Э. Берендс

МАТЕМАТИЧЕСКИЕ ПЯТИМИНУТКИ

Лаборатория ЗНАНИЙ

Ehrhard Behrends

Fünf Minuten Mathematik

100 Beiträge der Mathematik-Kolumne der Zeitung DIE WELT

Mit einem Geleitwort von Norbert Lossau

3., aktualisierte Auflage

Springer Spektrum

Э. Берендс

МАТЕМАТИЧЕСКИЕ ПЯТИМИНУТКИ

Перевод с немецкого
Н. А. Шиховой
И. А. Маховой

5-е издание, электронное

Москва
Лаборатория знаний
2020

УДК 51(079)
ББК 22.1
Б48

Берендс Э.

Б48 Математические пятиминутки / Э. Берендс ; пер. с нем. — 5-е изд., электрон. — М. : Лаборатория знаний, 2020. — 379 с. — Систем. требования: Adobe Reader XI ; экран 10". — Загл. с титул. экрана. — Текст : электронный.

ISBN 978-5-00101-903-9

Книга представляет собой перевод широко известной зарубежному читателю книги для математического досуга. Ее автор — профессор математики Берлинского университета, блистательный популяризатор науки. В основу книги легли более 100 эссе, которые Э. Берендс публиковал в своей рубрике в газете «ДиВельт». Русское издание представляет собой перевод 3-го немецкого издания, в котором исправлены замеченные опечатки.

Книга написана живым и доступным языком, сложные математические факты излагаются под неожиданным углом зрения, при этом их научная составляющая не нарушается. Приводятся многочисленные исторические факты. Книга богато иллюстрирована. Автор поставил своей целью уверить читателя, что математика не сухой и нудный предмет, а, напротив, она полна очарования и достойна восхищения.

Книга адресована широкому кругу читателей, всем, кто готов занять свой досуг захватывающим и познавательным чтением.

УДК 51(079)
ББК 22.1

Деривативное издание на основе печатного аналога: Математические пятиминутки / Э. Берендс ; пер. с нем. — 3-е изд., испр. и доп. — М. : БИНОМ. Лаборатория знаний, 2015. — 376 с. : ил. — ISBN 978-5-9963-1735-6.

16+

Перевод немецкого издания
Fünf Minuten Mathematik
автора Ehrhard Behrends,
опубликованного издательством
Springer Spektrum

ISBN 978-5-00101-903-9

ПРЕДИСЛОВИЕ К ТРЕТЬЕМУ ИЗДАНИЮ

Для третьего немецкого издания был подготовлен ряд дополнений. Особенно следует отметить несколько фильмов, посвященных лотерее, экспоненциальному росту и размерности. Их легко найти в YouTube или при помощи QR-кодов, размещенных в книге.

Меня также очень порадовало то обстоятельство, что успех книги не ограничился Германией. К настоящему времени книга переведена на японский (2006), английский (2008), французский (2012) языки; в процессе подготовки переводы на итальянский, русский и турецкий.

Как нетрудно убедиться, уважаемые читатели, у математики много интересных аспектов, благодаря которым она стала важной составной частью нашей культуры, и вы можете наслаждаться ее красотой, даже не имея специальной подготовки.

Эрхард Берендс, Берлин, октябрь, 2012

ПРЕДИСЛОВИЕ КО ВТОРОМУ ИЗДАНИЮ

Книга Fünf Minuten Mathematik вызвала широкий интерес; появились переводы на японский и английский языки.

Переписка с переводчиком на английский язык Дэвидом Креймером оказалась особенно плодотворной. Он отметил опечатки, которым удалось проникнуть в текст; и в некоторых местах книги его вопросы привели к дополнениям, облегчающим понимание для математически неподготовленного читателя. Во второе издание вошли эти улучшения, а также многочисленные замечания, полученные от читателей.

Нужно еще сказать, что колонка «Пять минут математики» в газете *Die Welt* была переименована в «Математика в 2008 году». Теперь в нее пишут 12 авторов, каждый по одному месяцу, а я только координирую их работу.

Эрхард Берендс, Берлин, май, 2008

ПРЕДИСЛОВИЕ

В 2003 и 2004 годах появилась первая, а на тот момент и единственная регулярная колонка в общегерманской газете. Рубрика «Пять минут математики» выходила каждый понедельник в *Die Welt*, а через несколько недель эту колонку перепечатывали в *Berliner Morgenpost*.

За два года было опубликовано сто эссе о самых разных математических дисциплинах. Постоянные читатели колонки получили представление о криптографии и теории кодирования, познакомились с очарованием простых чисел и бесконечного, узнали, как математика работает в CD-плеерах и томографах, разобрались со знаменитой задачей Монти Холла и другими загадками теории вероятностей, — и это лишь несколько тем.

Всего в книге сто глав. Они тщательно выверены и дополнены примечаниями, таблицами и иллюстрациями, отчего объем текста увеличился почти вдвое.

Если вы хотите узнать больше о тех аспектах современной математики, для понимания которых не нужно специальных знаний, то обязательно найдете что-нибудь интересное на этих страницах. Автор особенно надеется убедить тех читателей, которые в детстве были травмированы школьной математикой, что это вовсе не тот иссушающе скучный предмет, который они помнят, а источник очарования и восхищения.

Эрхард Берендс, Берлин, июль, 2006

«ПЯТЬ МИНУТ МАТЕМАТИКИ» В ГАЗЕТЕ DIE WELT

Большинство людей не испытывают особой симпатии к математике. Числа и формулы кажутся им сложными, путанными, абстрактными и далекими от жизни. Возможно, действительно нужно обладать предрасположенностью вроде музыкальности, чтобы развить в себе страстный интерес к математике.

Тем не менее я убежден, что многие скептики живо интересовались бы этой царицей наук, если бы только кто-нибудь построил для них мост в захватывающее царство математики.

Такие мосты могли бы строить учителя, облекая уроки математики в увлекательные истории из повседневной жизни. Что, если обсуждение абстрактных кривых мотивировать поиском оптимальных сроков для опционов? Или если использовать геометрию для вычисления жизненного пространства в геометрически сложном жилище и количества рулонов обоев для него? А когда речь заходит о простых числах, внимание многих учеников обязательно привлечет история о криптографии и сложностях взлома секретных кодов.

Математика находится в центре нашей жизни. Она всюду, куда ни посмотришь: в сканере на кассе в магазине, в вычислениях процентов по закладной, в пин-коде кредитной карты, в компьютерном томографе и в дизайне автомобиля или самолета.

Математика отправляет зонды на дальние планеты и вдыхает жизнь в роботов. Именно она — движущая сила технологического прогресса, а еще — если позволить себе углубиться в предмет — математика невероятно увлекательна. И даже если в далекие школьные годы мост к ней построен не был, все равно у взрослых есть возможность приблизиться к математике.

Во-первых, в последние годы в СМИ науке и технологиям стало уделяться значительно больше внимания, хотя о математике этого, увы, не скажешь.

Только несколько газет и телепередач регулярно, или хотя бы от случая к случаю, рассказывают о связанных с математикой темах, а ведь остается еще больше тем, заслуживающих, чтобы о них рассказали. Такое впечатление, что для многих редакторов математика — запретная тема, табу.

Die Welt не страдает от такого подхода и не боится, например, посвятить целый разворот числу π (25 февраля 2006 г.).

Благодаря перу профессора Эрхарда Берендса еженедельная колонка «Пять минут математики» предоставила постоянную печатную трибуну для публикации сотни эссе о математике. Судя по большому числу читательских откликов, мы знаем, что колонка вызвала устойчивый интерес. О математике — упакованной в интересные истории — рассказывается точно и сжато, доходчиво и компетентно. И — о чудо из чудес! — несъедобный предмет математики вдруг обретает приятный вкус.

«Пять минут математики» заслуживают того, чтобы расширить круг читателей, не ограничиваясь подписчиками *Die Welt*, и нам приятно, что, издав книгу, издательство сделало доступным эту серию статей для широкой аудитории.

Профессор Берендс, строитель мостов, указывает путь через крепостной ров, населенный драконами математических страхов, к твердыне математики. Он умело излагает математическую суть, так что от абстракции не остается и следа.

Если мы собираемся повышать статус математики в общественном мнении, нам нужно больше таких авторов, и конечно же, больше изданий, где они могут выступить.

Д-р *Норберт Лоссау*,
главный научный редактор Die Welt,
автор колонки «Пять минут физики».

ВВЕДЕНИЕ

История этой книги началась 25 января 2002 г. во время обеда, который устроило Немецкое математическое общество, чтобы установить контакты между общественными деятелями и группой журналистов. Разговаривали о том, как воспринимает математику общественность. Одним из участников встречи был Норберт Лоссау, научный редактор газеты *Die Welt*, с которым я встретился еще раз через несколько месяцев. Беседы с ним привели к идее регулярной колонки, посвященной математике.

Я составил обширную презентацию, название «Пять минут математики» было принято, художник нарисовал логотип, и 12 мая 2003 г. колонка впервые увидела свет в *Die Welt*. Так и пошло — неделя за неделей; ритм нарушался, только если понедельник выпадал на праздник и газета не выходила. Через два года сто статей из колонки «Пять минут математики» привели к созданию другой рубрики.

Выбирая темы, я старался обращаться в основном к тем читателям, которые давно окончили школу и, возможно, забыли о математике, однако хотели бы что-нибудь узнать о ней. Правильно ли, что формула корней квадратного уравнения и умение рисовать графики — предел того, что сто́ит знать о математике? Где математика реального мира?

За два года мне удалось объять широкий спектр тем; в этом можно убедиться, просмотрев оглавление. Есть современные и классические, есть попроще и посложней. Читатель узнает, как математика пронизывает нашу жизнь, о чем бы речь ни шла — о лотерее, криптографии, томографии или об оценке страховых полисов.

Еще до выхода последней колонки я получил предложение от издательства Springer Verlag опубликовать все статьи в виде книги. Было множество причин приступить к этой работе тотчас же. Во-первых, в такой книге были заинтересованы многие постоянные читатели. Во-вторых, газетная статья ограничена постоянным объемом, вне зависимости от темы[1)]. Для некоторых тем ограничения в объеме означали, что важную информацию приходилось опускать, отчего совесть автора была нечиста.

Поэтому я рад, что формат книги позволил избавиться от этих ограничений. И наконец, роскошь свободного пространства означала, что слово удалось дополнить изображением: фотографиями, рисунками, графиками, таблицами...

Три аспекта я считаю особенно важными.

Математика полезна. Должно быть ясно, почему наш основанный на технологиях мир не может работать без математики. Этикетку «Математика внутри» можно наклеить на очень многие продукты.

Математика увлекательна. Кроме того что математика полезна, она чрезвычайно привлекательна интеллектуально. Непреодолимое желание довести решение задачи до конца может вызвать прилив огромного количества энергии.

Без математики нельзя понять мир. По словам Галилея, «книга природы написана на языке математики». В его время это было не более чем прозрение. Сейчас мы знаем, что математика — это мост, который ведет нас сквозь неизведанное в действительность, лежащую за пределами человеческого восприятия. Без математики было бы невозможно «знать, что держит мир вместе изнутри» (Гёте).

Я хочу поблагодарить доктора Лоссау за то, что он позволил мне в течение двух лет рассказывать читате-

[1)] По крайней мере, так сказали автору. То и дело приходилось немного урезать колонку.

лям *Die Welt* о математике. У меня остались чудесные воспоминания о нашем сотрудничестве.

Еще я выражаю признательность Эльке Берендс за большое число фотографий, в особенности за фотографии к гл. 6, 10, 15. И я благодарен коллегам Вагну Хансену (Копенгаген) и Робину Уилсону (Оксфорд) за предоставленные ими рисунки (к гл. 53 и 89).

И наконец, я хочу поблагодарить Тину Шерер и Альбрехта Вайса за то, что они исправили множество ошибок.

Глава 1

ГОСПОЖА УДАЧА

Представьте себе, что вы живете в большом городе, таком как Берлин или Гамбург. Вы едете в автобусе и замечаете, что один пассажир вышел, забыв зонтик. Вы берете его и собираетесь, вернувшись домой, набрать случайный телефонный номер: вдруг повезет и трубку возьмет хозяин зонтика?

Это, конечно же, надуманная история, и в реальной жизни такой план осмеяли бы как совершенно наивный. Но не смейтесь раньше времени: миллионы наших сограждан каждую субботу отмечают числа в лотерейном билете с надеждой угадать правильные, хотя вероятность успеха при этом составляет только 1/13 983 816. Шансы при этом еще меньше, чем отыскать хозяина зонтика, действуя согласно описанному плану: ведь случайных последовательностей из семи цифр «всего лишь» десять миллионов.

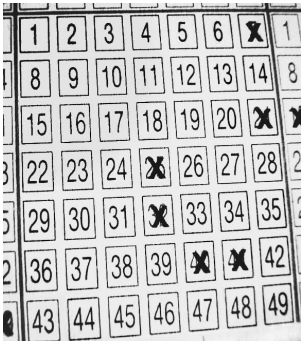
Многие участники лотереи воображают, будто они могут обмануть удачу, выбирая числа, которые редко выпадали в прошлом. Это бессмысленная стратегия: у случайности нет памяти. Даже если, например, числа 13 не было давно, шансы на его выпадение такие же, как и у других чисел. Некоторые участники разрабатывают собственные хитроумные системы, чтобы победить случай, но все такие попытки — только напрасная трата сил. Уже несколько десятилетий тому назад было доказано, что ни одна система не может обмануть госпожу удачу.

Напоследок хочется сказать хоть что-то позитивное. Кое-что участник лотереи все же может предпринять,

а именно, он может выбрать такую комбинацию чисел, которую вряд ли выберут большинство игроков. Тогда, если уж он каким-то чудом победит, ему скорее всего не придется делить выигрыш со многими. Однако сказать легче, чем сделать. В последнее время поразительно много участников выбирают числа, расположенные на карточке «крестиком».

В математике нет ни одной формулы, позволяющей выразить сладкое чувство предвкушения грядущих планов на то, как поступать с баснословным выигрышем. Удачи!

ПОЧЕМУ ИМЕННО 13 983 816?



Как же математики вычислили точное число 13 983 816 всех возможных комбинаций в лотерее? Выберем два числа, обозначим их n и k и предположим, что n больше k. Сколько различных k-элементных подмножеств содержится в множестве из n объектов?

Хотя на первый взгляд эта задача кажется математически абстрактной, она имеет непосредственное отношение к вопросу о лотерее, потому что, заполняя лотерейный билет, вы выбираете 6 чисел из 1, 2, 3, ..., 49, так что в этом случае $n=49$, $k=6$.

В жизни мы сталкиваемся и с другими примерами.

- При $n = 32$ и $k = 10$ речь идет о числе возможных раскладов в преферансе.
- В совещании приняли участие 14 человек, и, прощаясь, все пожали друг другу руки. Сколько всего было при этом рукопожатий? Здесь $n = 14$ и $k = 2$.

А теперь вернемся к общей задаче. Ее ответ выражается формулой, числитель которой равен $n \cdot (n-1) \cdots (n-k+1)$, а знаменатель равен $1 \cdot 2 \cdots k$. Неискушенному читателю числитель может показаться несколько устрашающим, но это просто произведение k целых чисел, из которых первое n, а каждое следующее на 1 меньше предыдущего. (Тот, кто хочет узнать, как появилась эта формула, может обратиться к гл. 29.)

В наших примерах получаются такие результаты:

- В задаче о лотерее нужно разделить $49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44$ на $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$. Так и появилось число 13 983 816.
- В задаче о числе раскладов в преферансе получается частное чисел $32 \cdot 31 \cdot 30 \cdot 29 \cdot 28 \cdot 27 \cdot 26 \cdot 25 \cdot 24 \cdot 23$ и $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10$, т. е. всего в преферансе возможно 64 512 240 раскладов. (Если учитывать расклады для всех игроков и их очередность, то это число существенно возрастет.)
- Задачу о рукопожатиях можно решить в уме: $14 \cdot 13$, деленное на $1 \cdot 2$, даст 91.

КОЛОДА КАРТ ВЫШИНОЙ ПОЧТИ В ЧЕТЫРЕ С ПОЛОВИНОЙ КИЛОМЕТРА

Осознать ничтожность шансов на лотерейный выигрыш помогает не только идея набирать наугад телефонный номер незнакомца. Есть и другие наглядные аналоги.[1)]

Вспомним, что толщина колоды карт составляет около одного сантиметра. Чтобы собрать вместе 13 983 816 карт, потребуется приблизительно 437 000 колод. Если их сложить в одну стопку, ее высота окажется примерно 4,37 км. Теперь предположим, что ровно одна из этих карт отмечена. Шансы выбрать эту карту наугад из четырехкилометровой колоды такие же, как шансы выиграть в лотерею.

ЛОТЕРЕИ В ИТАЛИИ

В лотерею играют почти в каждой стране, но правила очень различаются. В качестве примера сошлемся на лотерею в Италии. Там действуют две разновидности. В «обычном» варианте следует отметить крестиком 2, 3, 4 и 5 позиций в поле из 90 номеров. Разыгрываются 5 номеров, а прибыль зависит от того, сколько позиций вы отметили правильно. Если вы выбрали вариант с 5 крестиками, анализ похож на анализ в немецкой лотерее, только на этот раз надо выбрать «5» из «90», т. е. это $90 \cdot 89 \cdot \ldots \cdot 86 / 1 \cdot 2 \cdot \ldots \cdot 5 = 43\,949\,268$ возможностей, а вероятность угадать эту пятерку состав-

[1)] Еще одну иллюстрацию этой малой вероятности можно найти в гл. 83.

ляет 1/43 949 268, что значительно ниже аналогичной вероятности в нашей лотерее.

А еще есть «Суперлотерея», которая является разновидностью «6» из «90». В ней 622 614 630 миллионов возможностей выбора шести позиций, соответственно вероятность сверхприбыли — совсем крошечная.

Примечательно также, что существуют разные лотереи — как и в Германии, — которые должны быть отнесены к категории наименьшей вероятности выигрыша в случае выпадения джекпота. Поэтому можно набрать много вариантов, но только один из 6 правильных ответов приведет к весьма ощутимой выплате (около 100 млн евро). Иначе все автобусные караваны из соседних стран хлынули бы к итальянским лотерейным киоскам.

ФИЛЬМ НА ТЕМУ «ЭКСПОНЕНЦИАЛЬНЫЙ РОСТ»

2008 год был объявлен в Германии Годом математики. По этому поводу в Берлине прошла большая выставка «Mathema» в музее технологий. Там был также представлен экспонат в виде параболы из зерен риса и сделан фильм, который демонстрировал бесконечный рост: сколько же зерен риса понадобится? Вы найдете этот фильм в YouTube:

http://www.youtube.com/watch?v=KA-gN1h15Ko

или непосредственно с помощью следующего QR-кода:

Глава 2

ВОЛШЕБНАЯ МАТЕМАТИКА: ТЫСЯЧА И ОДНО ВОЛШЕБСТВО

Я предлагаю поиграть в «угадайку». Задумайте трехзначное число и запишите его два раза подряд. Например, если вы задумали 761, запишите 761 761. Игра начинается с того, что вы делите полученное шестизначное число на 7. Остаток от этого деления и становится вашим счастливым числом. Оно может быть равным только 0, 1, 2, 3, 4, 5, или 6, поскольку других остатков при делении на 7 не бывает. Теперь запишите ваше исходное число и остаток на открытке и отправьте в редакцию газеты *Die Welt*. Редактору нужно ваше счастливое число, чтобы именно столько банкнот в 100 евро выслать вам почтовым переводом.

Если вам не повезло и ваше счастливое число равно нулю, вы оказались в хорошей компании, потому что эта участь ожидает всех читателей газеты *Die Welt*. (Иначе издатель никогда не согласился бы опубликовать эту статью.)

```
761761 | 7
7      |---
06
 6
 61
 56
  57
  56
   16
   14
    21
    21
     0
```

Причина этого явления кроется в хорошо замаскированном свойстве целых чисел. А именно, записать трехзначное число подряд дважды — все равно что умножить его на 1001. Поскольку 1001 делится на 7, шестизначное число тоже будет делиться на 7.

Эта идея годится для маленького фокуса в небольшой компании, а обещание банкнот в 100 евро можно заменить на предсказание остатка.

Между прочим, математические факты находят себе место в шляпе фокусника не так уж редко. Нужно только найти противоречащий повседневному опыту математический результат, обоснование которого глубоко запрятано в некоторой теории.

Прислушайтесь к совету: волшебство — как духи́, упаковка почти столь же важна, как и содержание. Хотя умножение на 1001 эквивалентно записыванию числа

дважды, никому не должно прийти в голову, что такое умножение имеет место, иначе фокус станет тривиальным. Любители разнообразия могут вместо 7 взять 11 или 13, так как число 1001 раскладывается на произведение именно этих трех множителей. Только остаток вычислить будет несколько сложнее...

ИНЫЕ ВАРИАНТЫ: 1001, 10 0001, ...

Почему нужно задумывать именно *трех*значное число? Может быть, подойдет двузначное или четырехзначное?

Возьмем двузначное число n, записав его в виде xy. Если мы запишем это число два раза подряд, то получим четырехзначное число $xyxy$, что эквивалентно умножению исходного числа на 101. Но число 101 — простое, так что делителями числа $xyxy$ являются xy и 101. Поскольку в этом фокусе про число xy не известно ничего, нулевой остаток можно гарантировать только при делении на 101. К сожалению, просьба заняться делением на 101 убивает волшебство или по крайней мере заставляет заподозрить, что здесь что-то не так. Кроме того, деление на 101 может оказаться слишком сложным для ваших друзей и знакомых. Так что начинать с двузначного числа — не самая удачная идея.

Четырехзначные числа приводят нас к умножению на 10 001. Это число не является простым: ведь $10\,001 = 73 \cdot 137$, и оба этих сомножителя просты. Поэтому, если вы запишите четырехзначное число два раза подряд, получив восьмизначное, можете быть уверены, что результат делится на 73 и 137. Но кому хочется делить на 73?

У числа 100 001 тоже только два простых делителя — 101 и 9091, делить на них неудобно, поэтому пятизначные числа тоже не вполне походят для нашего фокуса. И так далее. Наконец, мы находим маленький делитель у числа 1 000 000 001 (оно делится на 7). Но стоит ли начинать волшебные фокусы фразой «Задумайте девятизначное число и запишите его два раза подряд, чтобы получить восемнадцатизначное»? Так что советую придерживаться первоначального варианта.

Вот таблица разложения на простые множители нескольких первых чисел вида $10\ldots01$:

Число	Разложение на простые множители
101	101
1001	$7 \cdot 11 \cdot 13$
10001	$73 \cdot 137$
100001	$11 \cdot 9091$
1000001	$101 \cdot 9901$
10000001	$11 \cdot 909091$
100000001	$17 \cdot 5882353$
1000000001	$7 \cdot 11 \cdot 13 \cdot 19 \cdot 52579$
10000000001	$101 \cdot 3541 \cdot 27961$
100000000001	$11 \cdot 11 \cdot 23 \cdot 8779 \cdot 4093$
1000000000001	$73 \cdot 137 \cdot 99990001$

Тем, кто хочет больше узнать об отношениях между математикой и волшебством, советую обратиться к книге Мартина Гарднера «Математические чудеса и тайны»[1)]. В этой книге математические фокусы описаны в гл. 24 и 86.

[1)] Минск: Современное слово, 2011.

Глава 3
СКОЛЬКО ЛЕТ КАПИТАНУ?

Математика, что совершенно справедливо, считается точной наукой. Ее строгие логические конструкции служили моделью для других наук, как естественных, так и гуманитарных. Знаменитый пример — главный труд Исаака Ньютона «Математические начала натуральной философии», который начинается с основных определений и аксиом о мире (что такое сила? что такое масса? каковы основные законы механики?), и из них выводится — строго дедуктивным образом — модель мира, которая произвела революцию в науке.

После Ньютона возникло представление о познании, которое сегодня кажется нам несколько наивным: все явления должны быть сведены к возможно более простой механической модели. Многие из нас до сих пор испытывают особое доверие к утверждениям, выраженным в математических терминах, а еще лучше — записанным в виде математических формул. Однако нередко бывает нужна здоровая доза скептицизма, поскольку полезных результатов можно ожидать только тогда, когда в их основе лежат четкие понятия. Так, все мы согласны с определением «скорости», тогда как «комфортная температура» — все же субъективное понятие. И поэтому формула для коэффициента комфорта, например, это просто уловка; одни находят ее забавной, а другие — возмутительной.

Итак, нужно всегда помнить о существовании естественных ограничений применения математики. Вне зависимости от того, сколько интеллекта задействовано, из недостаточной информации нельзя получить разумных результатов. Иногда «результат» совершенно невозможно вывести из условий задачи, она воспринимается как шутка: «Длина корабля 45 метров, а ширина 3. Сколько лет капитану?»

В такой ситуации все понимают, что подобные вопросы бессмысленны. Однако часто спрашивают что-то вроде

«Какова вероятность того, что Германия станет чемпионом мира?» А как можно вычислить шансы выиграть в лотерее производителя пива, если никто не знает, сколько всего призов и участников лотереи?

КОЭФФИЦИЕНТ КОМФОРТА И ЕГО РОДСТВЕННИКИ

Одна из формул, по которой вычисляют комфортность погоды, выглядит так:

$$T_к = (0.478 + 0.237\sqrt{v} - 0.12v)(T - 33),$$

где T — реальная температура в градусах по Фаренгейту, а v — скорость ветра.

Эта формула — прекрасный пример ложно понимаемой точности. Все согласятся, что когда дует пронизывающий ветер, нам холоднее. Но трудно найти двух человек, для которых «воспринимаемая температура» при -5 градусах по Фаренгейту и скорости ветра 7 км/ч совпадает с точностью до четырех знаков. Температура, которую мы ощущаем, зависит от чувствительности вашего организма, одежды, и множества других факторов.

Однако формулы для коэффициента комфорта, слепленные из различных параметров, дают температуру точно, до четырех значащих цифр. Конечно же, следует ожидать монотонности: чем сильнее ветер, тем ниже кажется температура. Но как бы то ни было, вместо формулы лучше было бы привести грубую таблицу значений, поскольку формула приводит к абсолютно неверному впечатлению, что здесь мы имеем дело с точной наукой.

$$h = Q(12 + 3s/8)$$

Рис. 3.1. Попытка математического юмора: оптимальная высота дамского каблучка как функция от количества выпитых напитков

Тем временем на сцене появляются толпы подражателей. Например, существуют формулы для высоты каблука (см. рис. 3.1) и уровня «напряженности» приключенческого романа. Такие «научные попытки» часто попадаются в газетах в разделе «Смесь». Читая газету за утренней чашкой кофе, мы поражаемся, какой жуткий вздор пытаются порой обосновать математическими формулами.

Глава 4

ГОЛОВОКРУЖИТЕЛЬНО БОЛЬШИЕ ПРОСТЫЕ ЧИСЛА

Конечно же, нет чисел проще натуральных, т. е. тех, которые мы используем при счете: $1, 2, 3, \ldots$ Некоторые из этих чисел обладают особым свойством: их нельзя записать в виде произведения меньших чисел. Это относится, например, к 2, 3, 5, к 101 и даже 1 234 271. Такие числа называются *простыми*; они привлекали к себе внимание с самого возникновения математики.

Как велики бывают простые числа? Более двух тысяч лет назад Евклид доказал, что простых чисел бесконечно много, а значит, они бывают сколь угодно большими.[1)] В основе знаменитого доказательства лежит следующая идея. Евклид описывает что-то вроде машины, в которую закладывают некоторые простые числа, а она в ответ выдает простое число, отличное от всех заложенных. Это подтверждает, что простых чисел бесконечно много.

Следствия из этого факта замечательны и даже головокружительны. Например, результат Евклида гарантирует, что существует настолько большое простое число, что для его записи потребовалось бы больше чернил, чем было произведено за всю историю человечества; конечно же, нам никогда не увидеть этого монстра воочию. В самом большом известном на данный момент (2006 г.) числе почти десять миллионов цифр[2)]. (Чтобы представить себе, насколько велико это число-рекордсмен, вообразите, что вы решили напечатать его в книге — для этого потребовалось бы более 800 страниц.) Большие простые числа используются

[1)] В гл. 54 рассказывается, как в наше время находят «очень большие» простые числа.

[2)] Наибольшим известным простым числом по состоянию на февраль 2011 г. является $2^{43112609} - 1$. Оно содержит 12 978 189 десятичных цифр и является простым числом Мерсенна. Его нашли 23 августа 2008 года на математическом факультете университета UCLA в рамках проекта по распределенному поиску простых чисел Мерсенна GIMPS.

в криптографии, а маленькими считаются числа всего только с несколькими сотнями цифр.

Одна из важнейших задач раздела математики — *теории чисел* — раскрывать секреты простых чисел, и поэтому великий математик Карл Фридрих Гаусс называл теорию чисел «королевой математики».

МАШИНА ЕВКЛИДА

Теперь опишем, как функционирует машина простых чисел Евклида. Пусть даны n простых чисел, которые обозначим $p_1, p_2, \ldots, p_n$. Если это вам кажется слишком абстрактным, то просто возьмите для примера четыре простых числа 7, 11, 13, 29, в этом случае $n = 4$, $p_1 = 7$, $p_2 = 11$, $p_3 = 13$ и $p_4 = 29$.

Теперь прибавим 1 к произведению этих простых чисел. Результат обозначим m. Таким образом,

$$m = p_1 \cdot p_2 \cdots p_n + 1.$$

В рассмотренном примере $m = 7 \cdot 11 \cdot 13 \cdot 29 + 1 = 29\,030$.

У каждого числа, а значит, и у m, есть по крайней мере один простой делитель, обозначим его p. Заметим, что он не может быть равен ни одному из чисел $p_1, p_2, \ldots, p_n$. Действительно, если m разделить на одно из этих чисел, получится остаток 1. (В нашем примере мы можем выбрать $p = 5$ — простой делитель числа 29 030. При этом число 5 не равно 7, 11, 13 или 29.)

Итак, мы видим, что для произвольного набора простых чисел $p_1, p_2, \ldots, p_n$ получается новое простое число, которого не было среди введенных. Значит, множество простых чисел не может быть конечным, поскольку любой конечный набор простых чисел, введенный в машину, приводит к простому числу, отличному от введенных.

На рис. 4.1 приведены несколько дополнительных примеров, в которых на выходе даются *все* простые делители числа $p_1 \cdot p_2 \cdots p_n + 1$. Обратите внимание на второй и третий примеры: вводимые простые числа не обязаны быть разными.

Генерирует ли машина Евклида *все* простые числа? Имеется в виду следующее: мы считаем известным, что

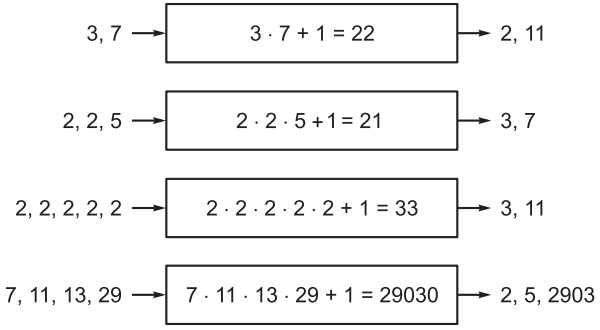


Рис. 4.1. Евклидова машина для генерирования простых чисел в действии

2 — простое число. Вводим его в машину, которая на выходе дает число 3 («произведение» одного числа — это само число, поэтому вывод равен $2 + 1$). Теперь мы можем ввести в машину числа 2 и 3, получив при этом 7, так что теперь мы можем работать с числами 2, 3 и 7. Эти три числа — возможные вводы, и мы не обязаны вводить их все одновременно, к тому же одно или несколько из них могут быть использованы больше одного раза. Возникает такой вопрос: каждое ли простое число возникнет на выходе из этой машины Евклида?

Ответ положительный, поскольку для каждого простого числа p число $p-1$ — это произведение нескольких (не обязательно различных) простых чисел $p_1, p_2, \ldots, p_r$. Поэтому при вводе $p_1, p_2, \ldots, p_r$ на выходе получится простое число p, ведь $p_1 \cdot p_2 \cdots p_r + 1 = p$. Это рассуждение может быть использовано для доказательства методом математической индукции утверждения о том, что все простые числа, не превышающие некоторого числа n, могут быть получены на машине Евклида, каким большим бы ни было число n.

Глава 5
ПРОИГРЫШ + ПРОИГРЫШ = ВЫИГРЫШ

Математика, и в особенности теория вероятностей, полна удивительных явлений. Когда какой-то результат резко контрастирует с общими ожиданиями, он называется *парадоксом*. Не так давно испанский физик Хуан Парондо пополнил зверинец таких парадоксов новым примером.

Рассмотрим две случайные игры, в которых игрок проигрывает игорному дому в среднем небольшую сумму. Игрок должен заплатить небольшой первоначальный взнос, чтобы принять участие в игре, а затем с вероятностью $\frac{1}{2}$ выигрывает или проигрывает один евро в каждом раунде игры. В другой игре шансы на победу зависят от предыдущего хода игры. Есть более или менее благоприятные раунды, но в среднем шансы все равно составляют 50 на 50.

Фокус вот в чем: если перед каждым раундом подбрасывать монетку, чтобы определить, играть первую или вторую игру, то у игрока есть выигрышная стратегия. Если игроку позволить играть достаточно долго, то может стать сколь угодно богатым. После открытия парадокса Парондо стали появляться сообщения, что теперь существует математическая теория для всех возможных ситуаций, в которых любое кажущееся проигрышным предложение заканчивается выигрышем. У каждого был такой опыт. Например, в шахматах вы можете пожертвовать почти любую фигуру и все равно победить.

Конечно же, такой теории не существует. Однако интересно, что все математические результаты, которые просачиваются сквозь стены академической башни из

слоновой кости в ежедневные газеты, почти всегда вселяют в читателей необоснованные надежды на грандиозный успех. Как многие помнят, так случилось с фракталами и с теорией хаоса. А вот у парадокса Парондо обнаружилось несколько интересных приложений. Например, он объясняет, как микроорганизм может чередовать две химические реакции, чтобы плыть против течения.

ТОЧНЫЕ ПРАВИЛА ВТОРОЙ ИГРЫ

Правила первой игры Парондо уже были описаны. Правила второй игры несколько сложнее.

Если сумма выигрыша к данному моменту делится на 3, то шансы неблагоприятны: с вероятностью 9/10 игрок теряет один евро, а с вероятностью 1/10 — выигрывает[1)].

Все не так плохо, когда сумма выигрыша не делится на 3. Тогда игрок выигрывает с вероятностью 3/4 и проигрывает с вероятностью 1/4.

Таким образом, для игрока ситуация благоприятна или неблагоприятна в зависимости от того, делится сумма выигрыша на 3 или нет. Можно показать, что эта игра абсолютно честная. Однако из-за того, что требуется первоначальный взнос, в длинной серии это проигрышная игра.

ПАРАДОКС!

В разных разделах математики имеются свои парадоксы. Как правило, их следует ожидать при описании явлений, недоступных нашему повседневному опыту: очень большие или очень малые числа, бесконечные множества и т. д.[2)]

Несколько удивляет, что парадоксы так часто появляются в теории вероятностей: ведь в ходе эволюции мы развили способность чувствовать многие аспекты случайности. Например, мы надежно умеем оценить

[1)]Например, из десятикарточной колоды можно наудачу вынимать одну. На девяти картах написано «Вы только что проиграли один евро!», а на одной — «Вы выиграли один евро!»

[2)]О некоторых парадоксах бесконечности говорится в гл. 15 и 70.

настроение собеседника, основываясь лишь на выражении лица, и неплохо умеем оценивать риски.

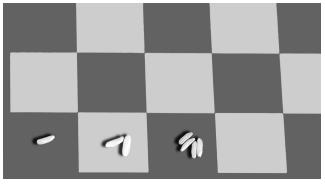
Хорошо известен парадокс дней рождения, описанный в гл. 11. Еще один хорошо известный пример — *парадокс перестановок*. Человек пишет десять писем и надписывает десять конвертов. Затем он раскладывает письма по конвертам в случайном порядке. Попадет ли хотя бы одно письмо в соответствующий конверт? Наивные представления говорят о том, что вероятность этого крайне мала. На самом деле, согласно теории вероятностей она составляет около 64%. Попробуйте сами! (Под маской выбора партнера в игре этот парадокс появляется в гл. 29.)

Глава 6

ИНТУИЦИЯ ПОДВОДИТ НАС, КОГДА РЕЧЬ ИДЕТ О БОЛЬШИХ ЧИСЛАХ

История человечества плохо подготовила нас к недавним открытиям в физике и математике. С точки зрения продолжения рода и выживаемости интересны только такие вещи, как средняя скорость, расстояния — не очень большие и не очень маленькие, — вообще, сравнительно небольшие числа. Поэтому сложно усвоить современные взгляды на природу вселенной, где при больших скоростях возникают удивительные явления. Можно сказать, что в нас встроен барьер, который мешает воспринимать некоторые математические истины.

Поговорим, например, о больших числах. В физике все же существует возможность представлять расстояния, далеко выходящие за рамки повседневного опыта и интуиции, с помощью подходящего масштаба. Например, можно представить миниатюрную модель Солнечной системы, в которой Солнце сжалось до размеров апельсина. В математике таких возможностей меньше, и наши способности вообразить, что происходит, быстро тают.



Особенно сложно осознать экспоненциальный рост. Многие слышали притчу о рисовом зернышке. Изобретатель шахмат обратился к своему правителю с просьбой, на первой взгляд необременительной. Он хотел, казалось, немного рису, но суммированному так, чтобы на первой клетке шахматной доски лежало одно зернышко риса, на второй — вдвое больше, на третьей — *еще* вдвое больше, и т. д. Оказалось, что через 64 шага число зерен превзойдет количество произведенного риса во всем мире за год.

Конечно же, раскладывание риса на шахматной доске не относится к повседневным занятиям. Другая аналогия, более близкая к реальной жизни,— это «письма счастья».

Допустим, вы получили письмо — одно из цепи распространяющихся, — в котором сказано, что вы должны разослать его копии десяти знакомым, указав свои имя и адрес. Предполагается, что они поступят так же. Каждому, чье имя окажется ниже уровня пяти поколений, полагается цветная открытка (или 100 евро, или еще что-нибудь). На первый взгляд — это великолепная идея, и наивные люди верят, что она должна принести выгоду (выраженную в открытках или евро). Чтобы сохранить жизнеспособность системы, посылая одну открытку, в результате вы должны получить огромную корзину почты (на самом деле корзины не хватит — если все игроки сделают то, что от них требуется, вам достанется более 100 000 открыток). Однако эта игра всегда прекращается еще на ранних этапах, поскольку слишком много людей получают слишком много писем от слишком большого числа друзей с требованием выслать десять писем.

Математики испытывают особое благоговение перед экспоненциальным ростом. Задачи, степень сложности которых растет экспоненциально относительно размеров входных данных, считаются особенно сложными. Так, например, пытаются показать, что задача взлома процедуры шифрования экспоненциально сложна.

ЭКСПОНЕНЦИАЛЬНЫЙ РОСТ I: РИСОВЫЙ ПОТОП

Сколько же всего рисовых зерен в притче о рисовом зернышке? Чтобы ответить на этот вопрос, нужно найти сумму $1+2+4+\cdots+2^{63}$. Такие вычисления удобно проводить по формуле *геометрической прогрессии*:

$$1 + q + q^2 + \cdots + q^n = \frac{q^{n+1} - 1}{q - 1} \quad \text{при } q \neq 1 \text{ и } n = 1, 2, \ldots.$$

В нашем случае

$$\frac{2^{64} - 1}{2 - 1} = 18\,446\,744\,073\,709\,551\,615 \approx 18 \cdot 10^{18}.$$

Так много риса!

Когда речь идет о таких больших числах, наша интуиция подводит нас. И правда, даже четырнадцать миллионов различных комбинаций в лотерее кружат нам

голову. Давайте хоть попытаемся представить себе такое количество риса. Грубо говоря, рисовое зернышко — это цилиндр диаметром 1 мм и длиной 5 мм. Таким образом, в кубическом сантиметре помещается 200 рисовых зерен[1)].

Теперь можно заняться математикой. Если в кубическом сантиметре 200 зерен, то в кубическом метре их $200 \cdot 100^3 = 2\,000\,000$, а в кубическом километре — $200 \cdot 100^3 \cdot 1000^3$. Поэтому, разделив число зерен на $2 \cdot 10^{17}$, мы вычислим объем рисовой кучи в кубических километрах. Оказывается, что их получится около 92 км^3.

Чтобы представить себе этот объем, сделаем так. Площадь Германии — 360 000 квадратных километров; если распределить рис, требующийся по условиям задачи, по всей этой территории, он покроет ее слоем толщиной в 25 сантиметров (25 см это 1/4000 км; $360\,000/4000 = 90$ км^3).

Не верите? Я тоже не верил, поэтому попробовал сам. Так появились рис. 6.1, 6.2 и 6.3.

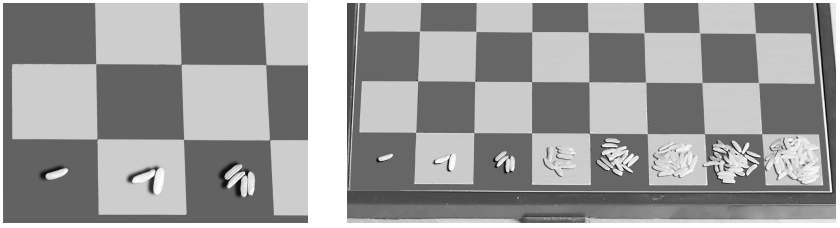


Рис. 6.1. Все начиналось вполне безобидно...

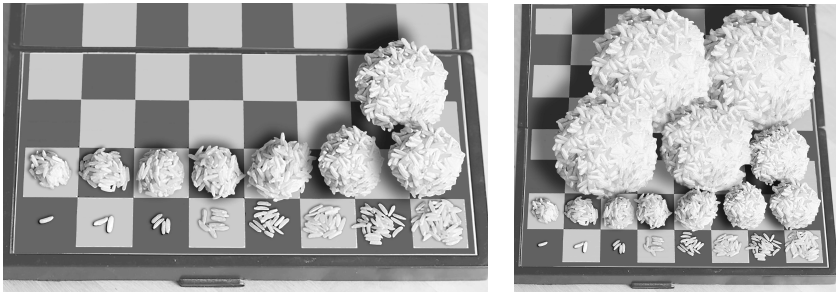


Рис. 6.2. ...но потом все пошло быстрее, чем предполагалось...

[1)] Даже больше, если их можно оптимально упаковать, но в этой притче они размещаются как попало.

Рис. 6.3. ...и в конце концов я сдался

ЭКСПОНЕНЦИАЛЬНЫЙ РОСТ II: СКОЛЬКО РАЗ ВЫ СМОЖЕТЕ СЛОЖИТЬ ЛИСТ БУМАГИ?

Прежде чем читать дальше, ответьте на один вопрос: как вы думаете, сколько раз можно перегибать лист бумаги пополам, чтобы получилась тетрадка? Большинство не могут угадать и говорят о слишком большом количестве раз.

Перегибая, нужно учитывать два момента. Во-первых, толщина тетрадки экспоненциально растет, удваиваясь после каждого перегиба. После пяти перегибов сложенный лист станет в 32 раза толще исходного листа, ведь $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$. Это составляет примерно один сантиметр[1)], и если бы вы смогли сложить еще 5 раз, то получили бы толщину 32 сантиметра.

Но это невозможно. Когда несколько слоев расположены один над другим и их толщина составляет d, то ситуации различаются для верхнего — т. е. для внутреннего после складывания — слоя и для нижнего. А именно, нижний нужно растянуть, чтобы он дал полукруг радиуса r. Длина окружности вычисляется по формуле $2\pi r$, поэтому нам понадобится длина πr. Например, если после пяти складываний получается толщина в один сантиметр, то нижний слой должен растянуться на $\pi/2 \approx 3,14$ сантиметров.

[1)] Речь идет, видимо, о листе бумаги, толщина которого составляет 1/32 см, т. е. ~0,3 мм. Для такого листа 5-е складывание было бы окончательным. Обычный лист писчей бумаги имеет толщину ~0,05 мм, и он выдерживает максимум 8 складываний. — *Прим. ред.*

После еще нескольких складываний растягивание больше невозможно. Практика показывает, что предел — восемь складываний. (На одной берлинской радиостанции решили это проверить, и 12 сентября 2005 года было проведено публичное складывание листа бумаги размером 33 на 49 футов. И в этом случае успешными были только восемь складываний.)

ФИЛЬМ НА ТЕМУ «ЭКСПОНЕНЦИАЛЬНЫЙ РОСТ»

2008 год был объявлен в Германии Годом математики. По этому поводу в Берлине прошла большая выставка «Mathema» в музее технологий. Там был также представлен экспонат в виде параболы из зерен риса и сделан фильм, который демонстрировал бесконечный рост: сколько же зерен риса понадобится? Вы найдете этот фильм в YouTube:

http://www.youtube.com/watch?v=KnQZ3Mg6upg

или непосредственно с помощью следующего QR-кода:

Глава 7

КЛЮЧ К ШИФРУ — В ТЕЛЕФОННОЙ КНИГЕ

Много веков люди мечтают о таком методе отправки секретных сообщений, чтобы они действительно оставались секретными. Реализация этой мечты под названием *криптография* стала ветвью математики, в которой сегодня ведутся интенсивные исследования.

Интересно, что развитие криптографических методов заставило некоторые математические специальности покинуть башни из слоновой кости и спуститься к людям. Возьмем теорию чисел, почтенную область математики, которая изучает обычные числа 1, 2, 3,.... В последние десятилетия внезапно возрос коммерческий интерес к простым числам, потому что новые результаты оказались чрезвычайно красноречивыми и немало поведали о безопасности передачи зашифрованных данных.

Криптография всегда была верным источником зрелищных сюрпризов. Все началось тогда, когда обнаружилось, что больше нет нужды хранить информацию, использованную при кодировании и декодировании секретных сведений. Под названием *криптография с открытым ключом* эта идея произвела революцию. Теперь безопасность зависит от вполне конкретной задачи о простых числах: всякий, кто сможет разложить на множители большое число, равное произведению двух простых, сможет прочитать зашифрованное сообщение. Легко видеть, что, например, 35 равно произведению двух простых чисел 7 и 5, но для числа 49 402 601 (оно равно произведению простых чисел 33 223 и 1487) все гораздо сложнее. Однако в серьезной криптографии рассматриваются числа с сотнями цифр. Обычно считается, что не существует

процедуры, позволяющей устанавливать множители таких больших чисел настолько быстро, чтобы взламывание шифра давало практическую пользу. Так, много шума произвело открытие, сделанное несколько лет тому назад: любое разложение на два множителя было бы легко выполнить на квантовом компьютере, если бы его когда-нибудь изобрели. А пока криптографы могут расслабиться, хотя они чувствовали бы себя гораздо увереннее, если бы можно было окончательно доказать, что используемые ныне системы действительно безопасны. Несмотря на огромные усилия, это до сих пор не сделано.

СЛУЧАЙНЫЕ КЛЮЧИ БЕЗОПАСНЫ!

Более полное описание взаимоотношений между криптографией и простыми числами можно найти в гл. 23.

Даже не используя простые числа, можно прийти к абсолютно безопасным процедурам кодирования, при условии что мы готовы допустить небольшое искажение. Вот самая известная из этих процедур. Подбросьте монету много, скажем 10 000, раз, и запишите результат в виде последовательности нулей и единиц. (Если вы слишком ленивы и не хотите самостоятельно бросать монетку, поручите компьютеру сделать это виртуально.) Последовательность будет выглядеть, например, так:

$$00101111011011100000\ldots.$$

Теперь ее можно использовать для кодирования сообщения. Для простоты будем считать, что оно тоже представляет собой последовательность нулей и единиц[1)].

Так что предположим, что закодированное сообщение начинается как-нибудь так:

$$10111001100000011000\ldots.$$

При кодировании будем действовать следующим образом: сначала над передаваемым сообщением запишем

[1)] Этого можно добиться, например, закодировав буквы и другие важные символы последовательностями из пяти нулей и единиц: $A = 00000$, $B = 00001$ и т. д. Поскольку $2^5 = 32$, таким образом можно закодировать 32 символа.

случайную последовательность:

00101111011011100000 . . .
10111001100000011000 . . . .

Построим третью последовательность. Когда друг над другом расположены одинаковые цифры (нули или единицы), запишем ноль, а если разные — единицу. В нашем случае получится такой результат:

10010110111011111000 . . . .

Теперь это закодированное сообщение можно передавать. Для принимающего, обладающего секретным ключом, расшифровка не представляет трудностей. Если например, первый символ в ключе ноль, а в закодированном сообщении — единица, то исходное сообщение должно начинаться с единицы (а ноль привел бы к нулю).

Эта процедура абсолютно безопасна. Причина в том, что все 10 000 возможных закодированных сообщений длины 10 000 равновероятно порождаются описанной процедурой. К сожалению, у этого метода кодирования есть два серьезных недостатка. Первый — получатель должен обладать секретным ключом, а ведь любой канал передачи подвержен атакам. Второй недостаток — ключ можно использовать только однажды. Если его использовать несколько раз, то его легко взломать посредством частотного анализа.

Математические методы открытого ключа не страдают этими пороками и потому широко используются в наши дни.

КРИПТОГРАФИЯ: НАУКА ТАЙН

Криптография — это область математики, в которой многие открытия не стали достоянием общественности. Важная часть современных исследований относится к вопросу о восстановлении разложения на множители числа, которое является произведением простых. На этом вопросе зиждется безопасность многих алгоритмов кодирования.

В некоторых частных случаях разложение на множители провести несложно. Но заранее неизвестно, в каких именно частных случаях исследования показывают, что разложение на множители не составляет труда. Поэтому

те, кто используют большие простые числа для кодирования, всегда пребывают в некоторой неуверенности.

Чтобы пояснить сказанное, приведем пример, идея которого восходит еще к Декарту. Предположим, мы нашли большое простое число p. Начав с него, среди дальнейших мы будем искать следующее простое число q. То есть будем считать, что $q = p + k$ для некоторого «малого» целого k.

В качестве примера рассмотрим случай $p = 23\,421\,113$, $q = 23\,421\,131$. При этом $k = 18$.

В реальных приложениях используются числа с несколькими сотнями цифр, но идея Декарта работает уже в нашем примере. Мы вычислим произведение $n = p \cdot q$, получив $n = 548\,548\,955\,738\,803$. Можно ли восстановить p и q по данному n? Если кажется справедливым, что $q = p + k$ для не слишком большого k, то можно схитрить вот так.

Ясно, что число k — четное, так как оба p и q — нечетные. Значит, можно записать $k = 2 \cdot l$. Число $p + l$, лежащее ровно посредине между числами p и q, будет играть важную роль в нашем рассказе. Обозначим его r. При этом $p = r - l$ и $q = r + l$. Кроме того, $n = (r - l) \cdot (r + l) = r^2 - l^2$, и поэтому $n + l^2 = r^2$. Итак, если к числу n добавить точный квадрат небольшого числа, то опять получится точный квадрат. Это наблюдение подсказывает следующую стратегию.

Будем прибавлять к n точные квадраты $l^2 = 1^2$, 2^2, 3^2 ... и каждый раз проверять, не является ли число $n + l^2$ точным квадратом. Компьютер сделает это быстро.

Получив нужный результат, запишем, что $n + l^2$ равно r^2. Остается заметить, что искомые множители p и q задаются формулами $p = r - l$ и $q = r + l$.

В нашем конкретном примере нужно проверить, нет ли среди чисел $548\,548\,955\,738\,803 + 1$, $548\,548\,955\,738\,803 + 4$, $548\,548\,955\,738\,803 + 9$, ... точного квадрата. На девятой попытке — после нескольких миллисекунд вычислений на компьютере — нас ждет удача:

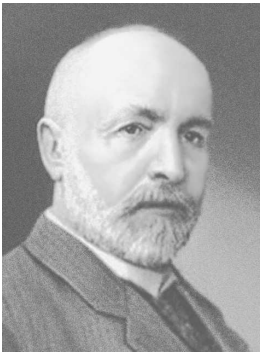
$$548\,548\,955\,738\,803 + 9^2 = 23\,421\,122^2.$$

Осталось только прибавить 9 к 23 421 122, а затем вычесть 9 из 23 421 122, чтобы получить нужные множители.

Глава 8

ДЕРЕВЕНСКИЙ ЦИРЮЛЬНИК, КОТОРЫЙ САМ СЕБЯ БРЕЕТ

Не так много немецких математиков известны за пределами своей науки. Но Георг Кантор, основатель теории множеств, несомненно, один из них. Почему теория множеств важна? Почему ее называют «математическим раем» и почему математика без нее невозможна?[1)] Причина в том, что эта наука позволила поставить математику на строгое дедуктивное основание.



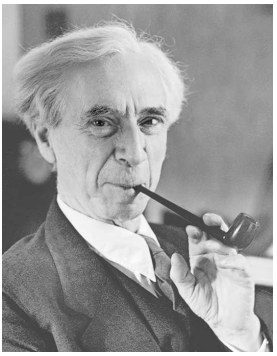


Рис. 8.1. Георг Кантор и Бертран Рассел

На поверхностный взгляд, теория множеств совершенно безобидна. Собирают вместе некоторые представляющие интерес объекты и получают новый объект под названием множество. Построение множеств происходит и в повседневной жизни. Понятно, например, что некоторые страны образовали множество «Европейский союз», а некоторые департаменты — множество «федеральное правительство». Однако если допустить образование новых объектов без всяких критериев проверки, могут возникнуть неприятности. Результат окажется бессмысленным, как было показано

[1)] По словам великого математика Давида Гильберта.

сто лет тому назад британским математиком и философом Бертраном Расселом. Его рассуждения основаны на логическом парадоксе, известном с древних времен: когда разрешается, чтобы утверждения ссылались сами на себя, возникновение логических противоречий неизбежно.

В хорошо известном варианте этого парадокса речь идет о деревенском цирюльнике, который бреет только тех, кто не бреет себя сам. А как же насчет самого цирюльника? Бреется ли он самостоятельно? Этого не может быть, ведь он бреет только тех, кто не может побриться сам. А если нет? Тогда его следует отнести к числу тех клиентов, которые не бреются самостоятельно. Вы можете вертеть это высказывание так и сяк; этот вопрос исключает логический ответ.

Запретив ссылающиеся на себя множества, теория множеств немного оправилась после шока, произведенного парадоксом Рассела, и сегодня она считается бесспорным фундаментом математики.

ТЕОРИЯ МНОЖЕСТВ В ДЕТСКОМ САДУ

Старшее поколение читателей помнит, что около 1960 г. в Германии был настоящий бум теории множеств. Причиной было потрясение: в 1957 г. Советский Союз запустил первый искусственный спутник Земли. Запад ответил серьезными усилиями по улучшению образования на всех уровнях, от детского сада до университета. К несчастью, управленцы в области образования позволили убедить себя, что для понимания математики необходимо знание теории множеств. В результате дошкольники строили «пересечения множеств зеленых фигурок и квадратных фигурок». Даже без теоретико-множественного языка большинство детей понимали, что это означало квадратные зеленые фигурки.

Теория множеств в Германии оказалась кратким эпизодом. Однако идет постоянный поиск способов улучшить математическое образование в школах, поскольку в наше время большинство учеников заканчивают школу с прочной ненавистью к математике и почти никто из них не понимает, о чем она.

ШЕРЛОК ХОЛМС В ЗАМЕШАТЕЛЬСТВЕ

Чтобы разобраться с парадоксом Расселла, нужно только понимать выражение «x является элементом M», где M — множество. Оно всего-навсего означает, что x принадлежит множеству M. Так, например, «14 является элементом множества четных чисел» и «11 является элементом множества нечетных чисел» — истинные утверждения, а «3/14 является элементом множества целых чисел» — нет.

Рассел рассмотрел множество тех множеств, которые не являются элементами себя. Оказывается, этот объект, обозначим его $\mathcal{M}$, обладает некоторыми странными свойствами. Например, можно задать наивный вопрос: является $\mathcal{M}$ элементом $\mathcal{M}$? Есть два варианта ответа.

Ответ «да» означал бы, что множество $\mathcal{M}$ обладает свойством, характеризующим элементы $\mathcal{M}$: оно не является элементом себя, и поэтому из «да» следует «нет».

Попробуем теперь ответить «нет». Это означает, что множество $\mathcal{M}$ не обладает свойством, характеризующим элементы $\mathcal{M}$ (а именно, быть элементом себя). Но если $\mathcal{M}$ не является элементом себя, оно должно входить в $\mathcal{M}$. Так что ответ должен быть «да».

Такая замысловатая форма рассуждения превосходит возможности логики в царстве теории множеств. Словно в ходе расследования преступления, когда известно, что преступник — один из двух персонажей A и B, Шерлок Холмс пришел к следующим выводам. Если предположить, что преступником является A, то в преступлении следует обвинить B; а если принять гипотезу о виновности B, то преступником оказывается A. Но ведь так не бывает!

Парадокс Рассела оказался большим потрясением для математического сообщества. Сегодня, спустя более ста лет, таких противоречий обычно избегают, запрещая ссылающиеся сами на себя определения. Такие определения ссылаются на определяемый объект, словно он уже известен.

Глава 9

УЙДИ, ПОКА ТЫ ВПЕРЕДИ

Представьте себе азартную игру, в которой вы проигрываете ставку с вероятностью 1/2 и получаете двойную ставку с той же вероятностью. Например, вы можете подбрасывать монетку, проигрывая, если выпадет «орел», и выигрывая, если выпадет «решка». Это, конечно же, справедливая игра, но можно ли победить удачу? Можно ли разбогатеть на такой игре? В принципе, для этого есть несколько способов. Первый простым смертным недоступен: если бы можно было заглянуть в будущее и знать результат подбрасывания монеты, то достаточно было бы просто принимать участие в игре только тогда, когда ожидается выигрыш. В среднем он случается в половине игр, так что можно неплохо обогатиться за один только вечер.

Второй способ гораздо сложнее и вовсе не такой прибыльный. Он хорошо известен игрокам. Идея проста. Поставьте один евро. Если вы выиграете, то станете на один евро богаче. Заканчивайте игру и ступайте домой. Если вы проиграете, то в следующий раз поставьте два евро. Если в этот раз удача будет с вами, то вы можете отправляться домой с чистой прибылью в один евро (четыре выигранных евро за вычетом трех проигранных). Но если вы проиграли и в этот раз, ставьте четыре евро. И опять, если вы выиграете, то станете на один евро богаче. Стратегия состоит в том, чтобы прекращать игру в случае выигрыша и удваивать ставку в случае проигрыша.

У этого метода есть два недостатка. Во-первых, предполагается, что ваши финансовые ресурсы безграничны (на тот случай, если вам предстоит большое число проигрышей

перед тем как вы наконец-то выиграете) и что игорный дом принимает сколь угодно большие ставки. Во-вторых, у вас будут большие проблемы, если посреди серии проигрышей крупье вздумает объявить выходной.

Идеи о невозможности предсказать будущее и о честности можно сформулировать с математической строгостью. Тогда можно строго доказать, что в случае ограниченности числа игр или размера ставки выигрышной стратегии не существует. Так что все предлагаемые системы победить удачу достоверно ничего не стоят. Ни один (честный) игрок не может стать богатым, если только ему не повезет.

Я ВЫИГРЫВАЮ ПОЧТИ ВСЕГДА

Теперь пора добавить несколько определений, чтобы точно сформулировать утверждение предыдущего раздела — теорему о моменте остановки. В простейшем варианте она касается *справедливых игр*, т. е. игр, в которых победы и проигрыши сбалансированы. Вспомните об игре с подбрасыванием монеты: если выпадает герб, вы выигрываете один евро, а если решка — проигрываете.

Нам требуется еще правило, которое определяет, когда мы прекращаем игру. Вот примеры таких правил:

Закончить после десятого круга.

Закончить, выиграв 100 евро.

Закончить после трех проигрышей.

Следует понимать, что таких *правил остановки* сколь угодно много. (Математики говорят о *моментах остановки* — это термин, один из важнейших в современной теории вероятностей.)

После того как правило остановки выбрано, можно будет определить *среднюю прибыль*: если играть в соответствии с этим правилом много раз, то прибыль будет примерно такой.

Теорема о моменте остановки гласит, что с*редняя прибыль в точности равна нулю, вне зависимости от сложности правила остановки*. По крайней мере, так обстоят дела, если дополнительно сделать реалистичное предположение, что размер ставки не может быть неограниченным.

Если ожидаемую прибыль и нельзя изменить в чью-либо пользу, можно изменить уровень *ощущаемой удачи*, чтобы в большинстве случаев выходить из казино с выигрышем в кармане. Вот простая стратегия достижения этой цели:

Придерживайтесь стратегии удвоения ставок, описанной выше, и играйте либо до тех пор, пока не получите один евро прибыли, либо пока не достигнете верхнего предела ставок, допустимого игорным домом. Затем прекратите игру и ступайте домой.

Чтобы проанализировать эту стратегию, рассмотрим один пример. Допустим, максимальный размер ставки составляет 1000 евро. В несчастливый вечер мы безуспешно ставим 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 евро. Десять раз подряд нам не повезло в игре с пятидесятипроцентными шансами на выигрыш. Вероятность такого печального стечения обстоятельств равна $(1/2)^{10}$, приблизительно одна тысячная. В противном случае, почти во всех случаях (а именно, приблизительно 999 раз из тысячи), мы покидаем казино с чистой прибылью (хотя и не такой впечатляющей, как проигрыш, ведь прибыль всегда составляет один евро). Конечно же, может случиться, что мы проиграем, и проигрыш при этом будет велик, так что утверждение о том, что в среднем чистая прибыль равна нулю, справедливо и в этом случае.

P. S. Весной 2006 г. бóльшая часть телеаудитории имела возможность узнать о математических реалиях, связанных с теоремой остановки. На *Stern TV* в программе Гюнтера Яуга, принял участие некто г-н Г., который утверждал, что обладает надежной стратегией игры. Действительно, он десять раз вышел из казино с выигрышем в кармане. Но, конечно же, это ничего не доказывает, ведь, как только что мы видели, можно устроить так, чтобы шансы на выигрыш составляли бы почти сто процентов. Г-н Г. не захотел заключить пари и убедиться, что его система пройдет строгую проверку. (Ставкой был рождественский бонус автора этой книги.)

Глава 10

МОЖЕТ ЛИ ОБЕЗЬЯНА СОЗДАТЬ ВЕЛИКОЕ ЛИТЕРАТУРНОЕ ПРОИЗВЕДЕНИЕ?

Начнем с мысленного эксперимента. Ваша годовалая дочка устроилась за компьютером и жизнерадостно нажимает на кнопки клавиатуры. Если разрешить ей заниматься этим достаточно долго, время от времени будут набраны осмысленные слова. Можно ли сказать, что ваша дочка умеет писать?

Этот вопрос касается философской проблемы, которой уделялось много внимания во времена зарождения теории вероятностей. Тогда еще не было персональных компьютеров и популярен был образ обезьяны за печатной машинкой (рис. 10.1). Можно строго доказать, что если обезьяне дать достаточно времени, то рано или поздно она напечатает любое литературное произведение, когда-либо увидевшее свет. Это обусловлено тем, что в последовательности случайных экспериментов может случиться любое событие с положительной вероятностью: все, что может случиться, обязательно случится (лишь бы времени было достаточно).

Давайте в качестве примера возьмем гл. 10, которую вы сейчас читаете. Даже она обязательно возникнет

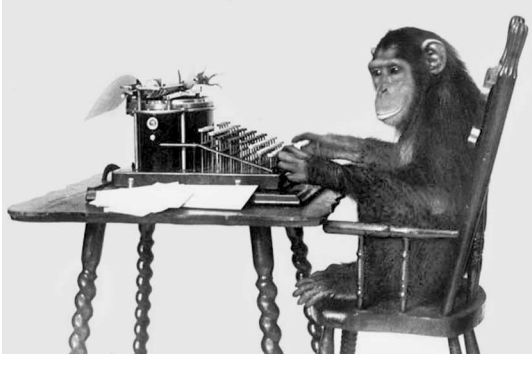


Рис. 10.1. Поэма? Роман?

как случайный продукт обезьяньей деятельности. Вопрос в том, следует ли из этого факта, что обезьяне можно приписать некоторую степень творческих способностей? Простого ответа здесь нет, ведь в конце концов обезьяна действительно напечатает данную главу, напишет «Фауст» и передовицу сегодняшней газеты.

Есть две причины утверждать, что случайность не заменит человеческое творчество. Первая — время. Какая польза в уверенности, что великие творения искусства рано или поздно увидят свет, если даже грубая прикидка показывает, что для этого потребуются бесчисленные эпохи. Целые армии печатающих обезьян, тысячелетиями не покидающие клавиатуры, почти наверное не осилят даже первой части «Фауста». Но решающая причина — другая. Кто возвестит: «Свершилось!», когда наконец появится сто́ящий текст? Без участия проницательного разума некому будет отсеять осмысленные произведения от гор случайных данных. Ведь и вы, скорее всего, не знаете, не напечатала ли ваша дочь басню на суахили.

СКОЛЬКО ВРЕМЕНИ НУЖНО ОБЕЗЬЯНЕ?

Попробуем оценить, сколько надо ждать, пока из обезьяньих экспериментов не появится нечто осмысленное. Начнем с одного результата теории вероятностей. Если вероятность того, что случайное событие осуществится с первой попытки, равна p, то в среднем нужно $1/p$ попыток, чтобы это событие произошло. Например, мы ожидаем, что один раз из 52 наугад вынутая из стандартной колоды карта окажется королем треф. Таким образом, время ожидания обратно $1/52$, а именно, равно 52.

Предположим, что мы ждем, пока появится слово «РУКА». Чтобы облегчить вычисления, позволим обезьянке напечатать четыре символа. Затем проверим, получилось ли слово «РУКА», и если нет, заправим в печатающее устройство новый лист бумаги. Если обезьяна нажимает только клавиши с буквами, и мы не делаем различия между строчными и прописными буквами («рУКа» засчитывается как успех), то для каждого удара по клавишам имеется 32 возможности. Четыре удара по клавишам могут дать

одно из $32 \cdot 32 \cdot 32 \cdot 32$ возможных «слов». Всего их 1 048 576, так что вероятность напечатать слово «РУКА» равна 1/1048576, а ожидаемое число попыток равно 1 048 576. Это ориентировочная величина, которую мы можем учитывать для планирования, но это, конечно же, только среднее значение. В действительности число попыток может оказаться и гораздо больше, и гораздо меньше.

Что это означает? Если давать обезьяне новую страницу каждые десять секунд, она сможет делать 6 попыток в минуту, т. е. 360 попыток в час или $8 \cdot 360 = 2880$ за рабочий день. Теперь нужно разделить 1 048 576 на 2880, чтобы получить ожидаемое число дней для получения слова «РУКА». Результат равен приблизительно 364, так что нужно ждать около года.

Но ведь слово «РУКА» не такое уж сложное. А что, если мы будем ждать фразы «СЕМЬ СИНИЦ В РУКЕ»? В ней 17 символов. Теперь мы должны учитывать еще и пробел, так что для каждого удара по клавишам есть тридцать три разные возможности, и вероятность каждого исхода равна 1/33. Поэтому вероятность того, что семнадцать ударов дадут «СЕМЬ СИНИЦ В РУКЕ» равна

$$\frac{1}{33^{17}} = \frac{1}{65273511648264442971824673},$$

а ожидаемое число попыток равно

$$65273511648264442971824673,$$

что составляет приблизительно 2×10^{23} лет, при условии восьмичасового рабочего дня и новой попытки каждые 10 секунд. Не похоже, что обезьяна доживет до успеха.

Глава 11

ПАРАДОКС ДНЕЙ РОЖДЕНИЯ

Мы уже говорили в этой книге о том, что человеческая интуиция не особенно хорошо приспособлена для овладения математическими истинами. В ходе эволюции нам требовалось освоить только самые элементарные факты, относящиеся к «пространству» и «числу». Это особенно верно в отношении такой математической дисциплины, как *теория вероятностей*, где наши ожидания и математические факты часто противоречат друг другу.

Один из примеров этого явления известен под названием «парадокс дней рождения». Предположим, что на вечеринке собрались двадцать пять человек. Каковы шансы на то, что у двух из них дни рождения совпадают? Вероятность этого события вычислить не так уж сложно, и как это ни удивительно, она составляет приблизительно 0,57.

Если поставить этот вопрос для произвольного числа n участников вечеринки, то окажется, что вероятность совпадения дней рождения у двух из участников становится довольно велика при сравнительно небольших n. А число 23 играет в этом случае особую роль. Это самое маленькое число из тех, для которых вероятность совпадения двух дней рождения больше 0,5. Этот результат противоречит нашей интуиции. Большинство людей полагают, что 50-процентная вероятность достигается при 183 участниках, что приблизительно равно половине от 365.

Те, кто не особенно доверяет математике, могут провести небольшое исследование. Если у вас есть ребенок школьного возраста, вам достаточно посмотреть календарь дней рождений класса во время следующего родительского дня. Если хотя бы у двух школьников дни рождения совпадают, это скорее правило, а не исключение.

Формализовать парадокс дней рождения можно, вычислив вероятность того, что среди n случайно выбранных чисел от 1 до 365 хотя бы два совпадают. Если вместо 365 взять другое число, то задача сложнее не станет, но

появятся новые интересные ее интерпретации. Например, вероятность того, что в случайно порожденном семизначном телефонном номере хотя бы одна цифра повторяется дважды, составляет 0,94. (В этом случае семь различных цифр выбираются из множества $0,1,\ldots,9$.) Может быть, это подойдет для заключения небольшого пари? Например, я могу поспорить — без особого риска, — что в вашем телефонном номере хотя бы одна цифра повторяется дважды.

КАК ВЫЧИСЛЯЮТ ВСЕ ЭТИ ВЕРОЯТНОСТИ?

Сформулируем задачу в общем случае.

Даны n объектов; выберем из этого набора r раз наудачу по одному объекту. Все объекты могут быть выбраны с равными вероятностями, и для любого не исключено, что он может быть выбран более одного раза.

Пример 1. *Дни рождения*. Здесь *объекты* — возможные дни рождения, т. е. $n = 365$. Тогда r — число участников вечеринки, а распределение дней рождения интерпретируется как *выбор из возможных дней рождения*.

Пример 2. *Слова*. Если напечатать наугад r-буквенное слово, то это можно формулировать как задачу выбора для случая $n = 32$.

Пример 3. *Номера телефонов*. Этот пример соответствует случаю $n = 10$ (поскольку цифр всего десять) и $r = 7$ (для семизначных номеров).

Возникает задача: вычислить вероятность того, что все выбранные элементы различны. Если она известна, то легко найти и вероятность того, что хотя бы два из них совпадают: для этого нужно только вычесть из единицы вероятность того, что они все разные. Например, если вероятность того, что все дни рождения встречаются только по одному разу, равна 0,65, то вероятность того, что есть хотя бы два совпадения, равна $1 - 0{,}65 = 0{,}35$, т. е. в 35% случаев.

Для решения задачи мы обратимся к следующему принципу:

вероятность = отношение числа благоприятных случаев к числу всех случаев.

Этот принцип вступает в игру всякий раз, когда все возможные объекты выбираются с одинаковой вероятностью. Число возможных случаев, т. е. число всевозможных способов выбора, равно n^r — произведению $n \times n \times \cdots \times n$ (всего r раз). Объясняется это тем, что для каждого из r объектов имеется n возможностей.

Перейдем к «благоприятным» случаям. Сколько таких наборов, что все объекты в них различны? При выборе первого объекта есть n возможностей. Выбирая второй, мы не можем взять тот, что был выбран первым, так что теперь есть только $n-1$ возможностей; а всего для первых двух объектов у нас $n \cdot (n-1)$ возможностей. Добавим третий, помня, что два объекта теперь под запретом, и получим $n(n-1)(n-2)$ вариантов выбора трех элементов без повторения.

Так все и продолжается; для r объектов есть

$$n(n-1)(n-2)\cdots(n-r+1)$$

способов их выбрать. Поэтому чтобы найти *отношение числа благоприятных случаев к числу всех случаев*, нужно вычислить дробь

$$\frac{n(n-1)(n-2)\cdots(n-r+1)}{n^r},$$

которую можно переписать в виде[1)]

$$1 \cdot \left(1-\frac{1}{n}\right) \cdot \left(1-\frac{2}{n}\right) \cdots \left(1-\frac{r-1}{n}\right).$$

Теперь должно быть ясно, как были получены описанные выше результаты. Появление числа 23 в парадоксе дней рождения объясняется тем, что вероятность события *ни одного совпадения для r человек* впервые опускается ниже границы 0,5 для $r = 23$. Действительно, число

$$\left(1-\frac{1}{365}\right) \cdot \left(1-\frac{2}{365}\right) \cdots \left(1-\frac{22}{365}\right) = 0{,}493$$

[1)] Мы воспользовались специальным приемом: записали дробь в виде произведения

$$\frac{n}{n} \cdot \frac{n-1}{n} \cdots \frac{n-r+1}{n},$$

а затем упростили каждый из сомножителей, воспользовавшись соотношением $\frac{x-y}{x} = 1-\frac{y}{x}$.

меньше 0,5, а число

$$\left(1-\frac{1}{365}\right)\cdot\left(1-\frac{2}{365}\right)\cdots\left(1-\frac{21}{365}\right)$$

равно 0,524.

Поскольку $1-0{,}493=0{,}507$, шансов на то, что хотя бы у двоих из двадцати трех гостей на вечеринке совпадают дни рождения, составляет 50,7%. Посмотрим, что будет, если гостей еще больше: для тридцати гостей они равны 71%, для 40 — уже 89%, а для 50 — целых 97%.

Шансы растут быстрее, чем подсказывает нам интуиция. Для иллюстрации этого явления мы построили две таблицы.

1	2	3	4	5	6	7	8	9	10
1,000	0,900	0,720	0,504	0,302	0,151	0,060	0,018	0,004	0,0004
0,000	0,100	0,280	0,496	0,698	0,849	0,940	0,982	0,9964	0.9996

В первой таблице идет речь о *совпадении цифр*. Чему равна вероятность того, что среди r наугад выбранных цифр хотя бы две одинаковые? В первой строке приведены значения r. Во второй — вероятность того, что все r выбранных наугад цифр различны, а в третьей — что хотя бы две из них совпадают.

Если вы захотите узнать, скажем, вероятность того, что в семизначном телефонном номере есть две одинаковые цифры, достаточно посмотреть в столбец $r = 7$: эта вероятность поразительно велика: она равна 0,94.

Следующая таблица относится к парадоксу дней рождения. В первой строке записано число гостей; во второй — вероятность того, что у них у всех разные дни рождения, а в третьей — дополнительная вероятность (того, что хотя бы у двух гостей дни рождения совпадают).

1	2	3	4	5	6	7	8
1,000	0,997	0,992	0,984	0,973	0,960	0,944	0,926
0,000	0,003	0,008	0,016	0,027	0,040	0,056	0,074
9	10	11	12	13	14	15	16
0,905	0,883	0,859	0,833	0,806	0,777	0,747	0,716
0,095	0,117	0,141	0,167	0,194	0,223	0,253	0,284
17	18	19	20	21	22	23	24
0,685	0,653	0,621	0,589	0,556	0,524	0,493	0,462
0,315	0,347	0,379	0,411	0,444	0,476	0,507	0,538

НИЧТО НЕ ПОВТОРЯЕТСЯ?

Хочется сказать об одном частном случае парадокса дней рождения. Если выбирают n объектов из n-элементного множества, то вероятность того, что каждый элемент выбран ровно однажды, равна $n!/n^n$. (Напомним, что $n!$ — это сокращенное обозначение для произведения $1 \cdot 2 \cdots n$.) Это число получилось бы, если в предыдущих примерах брать $r = n$.

Пример 1. Если из набора $1,2,\ldots,9$ девять раз выбирают целое число, то вероятность того, что все эти девять чисел окажутся различными, равна

$$\frac{9!}{9^9} = \frac{362\,880}{387\,420\,489} = 0{,}000936\ldots,$$

т. е. меньше одной тысячной.

Пример 2. Если одновременно бросить шесть игральных костей, то вероятность того, что на них выпадут разные числа, выражается дробью

$$\frac{6!}{6^6} = \frac{720}{46\,656} = 0{,}0154\ldots$$

Почти с такой же вероятностью в лотерее можно угадать три номера (см. гл. 40). Так что в среднем можно ожидать 6 разных чисел на 6 костях в 1 бросании из 65[1)].

P. S. В немецкой национальной сборной по футболу в 2006 г. было 23 человека — неплохие шансы на двойной день рождения. И правда, Мик Ханке и Кристоф Метцельдер празднуют свои дни рождения 5 ноября.

[1)] Если вероятность успеха случайного события равна p, то ожидаемое число попыток для осуществления этого события равно в среднем $1/p$, а $1/0{,}0154\cdots \approx 65$.

Глава 12
HORROR VACUI

Студенты-математики с большим уважением относятся к понятию «ничто», по крайней мере в начале учебы. Это не удивительно: ведь для того, чтобы число нуль встало в один ряд с такими числами, как семь или одиннадцать, понадобились столетия. Чтобы понять, почему это было так сложно, нужно вспомнить, что теория множеств, построенная Георгом Кантором, стала основанием современной математики. Согласно теории Кантора множество — это набор различных объектов, образующий новый объект. Это понятие привычно и нематематикам. Они же осознают, например, что США — это множество, состоящее из пятидесяти различных штатов, или что Европейский Союз — это множество, в которое входят двадцать семь государств–членов союза.

Все сложнее, когда мы строим набор, в который ничего не входит, например, множество всех граждан Германии, ростом выше трех метров. Не так-то легко осознать, что определенный таким образом объект совпадает с тем, что задан условием: «Все украинские пианисты, которые могут сыграть вальс-минутку Шопена за двадцать секунд». Оба этих примера описывают *пустое множество*.

Для теории множеств пустое множество (обозначается $\varnothing$) играет ту же роль, что нуль для целых чисел. Пустое множество может быть добавлено к произвольному множеству и размер последнего при этом не изменится; это ключевое свойство пустого множества. Всю математику можно построить, исходя из пустого множества. Например, целые числа возникают, если взять пустое множество в качестве нуля, а затем для числа 1 взять множество, единственным элементом которого является пустое множество. Для больших чисел такой способ построения оказывается несколько неуклюжим, однако принцип все тот же.

Понять, что же такое пустое множество, ни в какой мере не означает «разрешить все затруднения». Матема-

тики, изучая свойства множеств, большую роль отводят утверждениям вида «все элементы такого-то множества обладают таким-то свойством». Обычно полагают, что для пустого множества все такие высказывания истинны.

В большинстве случаев достаточно руководствоваться здравым смыслом. Например, если некто пообещал давать пять евро каждому встретившемуся в определенный день нищему, то он выполнит обещание, даже если не повстречает в этот день ни одного нищего.

ПУСТОЕ МНОЖЕСТВО ПОХОЖЕ НА НУЛЬ

Сейчас мы хотим пояснить, что понимается под утверждением: *пустое множество соответствует нулю*. Во-первых, надо знать, что *объединение* двух множеств A и B состоит из всех элементов, входящих в A или в B (возможно, в оба сразу, см. рис. 12.1). Например, если множество A состоит из элементов 2, 5, 6, а множество B состоит из элементов 6 и 8, то объединение A и B — это множество, в которое входят элементы 2, 5, 6, 8. Еще пример: если A обозначает жителей Парижа, а B — французов-блондинов, то объединение этих двух множеств включает, среди прочих, парижан-брюнетов и рыжих парижан.

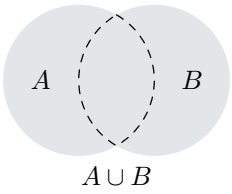


Рис. 12.1. Так можно представить себе объединение...

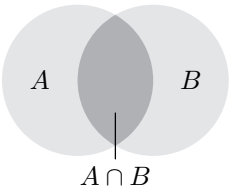


Рис. 12.2. ...а так — пересечение

Объединение двух множеств обозначается символом $A \cup B$. При этом для каждого множества A выполняется соотношение

$$A \cup \varnothing = A,$$

так как пустое множество не добавляет никаких элементов в объединение. Если рассматривать объединение множеств

как аналог сложения, то соотношению $A \cup \varnothing = A$ соответствует соотношение $x + 0 = x$ для чисел.

Для множества элементов, содержащихся одновременно в A и B, имеется обозначение $A \cap B$ (в описанном выше примере это множество парижан-блондинов, см. рис. 12.2).

Выражение $A \cap B$ читается «пересечение множеств A и B».

Поскольку в пустом множестве нет элементов, выполняется соотношение

$$A \cap \varnothing = \varnothing.$$

Если считать объединение множеств аналогом сложения, то пересечение множеств — аналог умножения. Иначе говоря, это соотношение соответствует правилу $x \cdot 0 = 0$ для чисел.

Латинское выражение «horror vacui» означает «боязнь пустоты». Это понятие возникло в древней натурфилософии, где был принят принцип «природа не терпит пустоты», означавший, что пустое место не может существовать. И действительно, хотя вакуум может существовать и существует, он стремится «всасывать» газы и жидкости.

Глава 13

ДОСТАТОЧНАЯ СЛОЖНОСТЬ МАТЕМАТИЧЕСКОЙ ЛОГИКИ НЕОБХОДИМА

В этой главе будем говорить о способности к логическим заключениям. Каждый день мы испытываем много впечатлений, и чтобы как-то их упорядочить, пытаемся выстроить некоторые логические соотношения. Рассмотрим например, очевидно верное утверждение: «Если сегодня Рождество, почта не работает». Никто не перепутает его с обратным утверждением: «Если почта не работает, то сегодня Рождество». Все же искушение путать такие пары утверждений очень велико. Вспомните только высказывание: «одежда красит человека». Богатые люди могут позволить себе дорого одеваться, однако мы не можем по одежде человека с уверенностью судить о его банковском счете.

И все становится еще сложнее в более абстрактных ситуациях. В этом отношении вспоминается «противоречие с трапецией». В 2003 г. вся страна задавалась вопросом, который возник в игре «Кто хочет стать миллионером»: можно ли считать прямоугольник трапецией? Если принять определение «трапеция — это четырехугольник с двумя параллельными сторонами», то верный ответ должен быть «да». Это было сложно объяснить уважаемому гражданину, реакции которого варьировались от злобных до агрессивных: «Как может математик утверждать, что каждая трапеция — прямоугольник?» Но ведь этого никто не утверждал...

Для полноты нужно добавить еще кое-что. Если для двух утверждений p и q всегда выполняется «q следует из p», то математики говорят, что p *достаточно для* q, а также что q *необходимо для* p. Эти две идеи легко спутать. И правда, можете ли вы определить истинность утверждения: «Чтобы фигура была трапецией, достаточно,

чтобы она была прямоугольником»? Правильный ответ ищите в сноске внизу[1)].

ТРАПЕЦИЯ ИЛИ НЕ ТРАПЕЦИЯ?

Чтобы в споре о трапеции дело не дошло до рукоприкладства, следует признать, что учебники и справочники и в самом деле могут вводить в заблуждение. Действительно, в определение трапеции часто вводят условие, что в ней не должно быть прямых углов.

С математической точки зрения в этом ограничении нет никакого смысла, поскольку оно очень неэкономично. Рассмотрим, например, утверждение, что сумма углов трапеции равна 360°. Предположим, что мы убедились в нем с помощью строгого геометрического доказательства. Теперь мы переходим к понятию «прямоугольник». Если мы вслед за всеми математиками будем считать прямоугольник частным случаем трапеции, то сможем немедленно провозгласить теорему: *сумма углов прямоугольника равна* 360°, так как это просто частный случай более общего, уже доказанного нами результата. А всем остальным придется проводить доказательство с самого начала. И то же самое относится ко всем утверждениям о трапециях.

Обычно в школьных учебниках трапецию изображают примерно так, как на рис. 13.1. Но на рис. 13.2 тоже изображены трапеции.

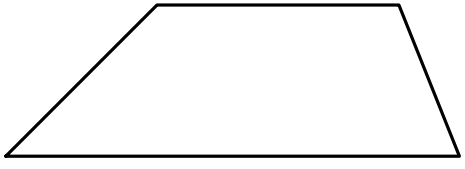


Рис. 13.1. «Типичная» трапеция

[1)]На самом деле утверждение «фигура является прямоугольником» достаточно для справедливости утверждения «фигура является трапецией».

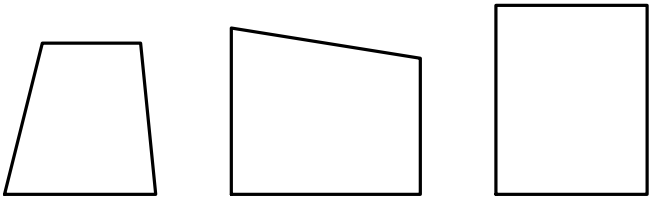


Рис. 13.2. Другие примеры трапеций

МЫСЛЯТ ЛИ СОБАКИ ЛОГИЧЕСКИ?

На рис. 13.3 вы видите объявление «Если собака лает, она не кусает. Наша собака не лает». Конечно же, оно висит как предупреждение. На самом деле здесь из «p влечет за собой q» («лает» влечет за собой «не кусает») сделан вывод, «не p влечет за собой не q» («не лает» влечет за собой «кусает»). Этот вывод нельзя назвать логическим, однако же объявление работает.

Рис. 13.3. Вы бы вошли?

Глава 14

МЕНЯТЬ ИЛИ НЕ МЕНЯТЬ? ПАРАДОКС МОНТИ ХОЛЛА

Теория вероятностей богата парадоксами: в ней много утверждений, противоречащих «здравому смыслу». Несколько лет назад широкой публике стал известен так называемый *парадокс Монти Холла*.

Если вы позабыли, то я напомню, о чем речь: ведущий популярного игрового шоу предлагает финалисту выбрать одну из трех дверей. За одной из них находится большой приз — новый автомобиль. За двумя другими — по болванчику в форме козлика. Допустим, играющий выбрал дверь под номером 1. После этого ведущий отворяет другую дверь, скажем, номер 3, и за ней стоит козлик. Мы добрались до главного. Игроку предлагается изменить свой выбор, в данном случае с номера 1 на 2. Следует ли ему принять предложение? В пользу неприятия говорит тот факт, что место большого приза не меняется, когда отворяют дверь 3. С другой стороны, отворив дверь, ведущий меняет ситуацию. Вопрос породил споры среди специалистов в разных областях математики. Задача попала в ведущие газеты и подробно обсуждалась нематематиками. Партия ДА и партия НЕТ осмеивали идеи друг друга как наивные/примитивные/смехотворные. У проблемы обнаружился и гендерный аспект.

Одним из первых защитников идеи принять предложение сменить дверь была американская журналистка Мэрилин вос Савант, знаменитая своим необыкновенно высоким IQ. В математическом сообществе раздавалось немало голосов, советовавших ей бросить эту тему и не заниматься вопросами, которые женщине все равно недоступны.

Кто же был прав? Оказывается, права была Мэрилин, утверждая, что играющий должен соглашаться на смену

двери, поскольку шансы на выигрыш при этом повышаются с $\frac{1}{3}$ до $\frac{2}{3}$. Сейчас мы все объясним.

АНАЛИЗ: ПОЧЕМУ СЛЕДУЕТ ПРЕДПОЧЕСТЬ ДРУГУЮ ДВЕРЬ?

Утверждение, что смена выбора двери предпочтительнее, — это только первое приближение к истине. Мы предлагаем подробный анализ задачи, так что это утверждение становится понятнее и вся ситуация проясняется. Дорога к этой цели не так проста, поскольку в пути попадаются довольно сложные явления.

ВЕРОЯТНОСТЬ

Вначале следует ознакомиться с некоторыми понятиями теории вероятностей. К счастью, нам не нужно разбираться с философскими аспектами вопроса «Что такое вероятность?».

Представьте процедуру генерирования случайных событий. Например, бросание игральной кости или извлечение карты из хорошо перетасованной колоды. Если повторять такой процесс много раз, то можно обнаружить некоторые «тенденции». Примерно в одной шестой части бросаний кости выпадает четверка, и примерно в одной четверти случаев из колоды извлекают карту червей. Для описания этого явления говорят, что в случае игральной кости вероятность выпадения четверки равна одной шестой, а в случае колоды карт вероятность извлечения карты червей равна одной четверти. И вообще:

- Вероятность возможного результата E в случайном выборе равна числу p, обладающему следующими свойствами: если случайный выбор повторять много раз, то в части p случаев будет получен результат E. Хотя это соотношение выполняется только приблизительно, оно становится все более и более точным с увеличением числа испытаний. Соотношение записывают в виде $P(E) = p$, и читают «вероятность E равна p»[1)].

[1)] Буква P напоминает о слове «вероятность», по-английски probability, а по-французски probabilité.

- В наших примерах P(выпадает четверка) $= \frac{1}{6}$, и P(выпадает карта червей) $= \frac{1}{4}$. Поскольку часть целого всегда принимает значения от нуля до единицы, то же самое можно сказать о вероятностях. Кроме этого, определение вероятности позволяет установить некоторые другие простые свойства. Например, если результат E всегда обеспечивает выполнение условий для другого результата F, то вероятность F не меньше вероятности E. Она просто никак не может оказаться меньше. Например, поскольку 4 — четное число, неудивительно, что при бросании кости вероятность выпадения четного числа (она равна 0,5) больше, чем вероятность выпадения четверки.

В парадоксе Монти Холла встречаются несколько вероятностей. Например, интересно было бы знать вероятности, с которыми большой приз (новый автомобиль) обнаруживается за разными дверями. Можно ли считать, что эти вероятности равны для всех трех дверей (по $\frac{1}{3}$)? Или для той двери, что ближе к выходу на сцену, вероятность больше? (В конце концов, не так-то легко поднять на сцену большой автомобиль.)

УСЛОВНЫЕ ВЕРОЯТНОСТИ

Теперь обсудим важный принцип «информация меняет вероятность». Вот пример. Вероятность выпадения четверки при бросании игральной кости равна одной шестой. Пусть теперь уже после того, как вы бросили кость, но еще до того, как увидели число на ней, вам сказали, что выпало четное число. Теперь вы понимаете, что на кости может оказаться только два, четыре или шесть, и поэтому вероятность выпадения четверки повышается до одной трети. Или допустим, вы получили дополнительную информацию, что выпало нечетное число. Тогда это явно не четверка, и вероятность ее выпадения снижается до нуля.

Итак, если вы получите дополнительную информацию, с вероятностью может произойти что угодно; она может увеличиться, уменьшиться или остаться неизменной.

Мы сталкиваемся с этим явлением в повседневной жизни[1]. Предположим, что каждый рабочий день вы ездите по одной и той же дороге. В левой полосе машины двигаются несколько быстрее, и вы хотите туда сместиться. Поэтому интересно знать, не собирается ли автомобиль перед вами на следующем перекрестке свернуть налево. (Если да, то вам следует сменить полосу, поскольку вы собираетесь двигаться прямо.) Предположим, что один из примерно двадцати водителей на этом перекрестке поворачивает налево, так что вы оцениваете вероятность того, что автомобиль впереди повернет налево, как 1/20. Но автомобильные номера несут информацию о том, в каком городе зарегистрирован автомобиль, и может случиться так, что номер автомобиля впереди указывает на то, что он зарегистрирован в том городе, до которого можно добраться, свернув налево. В таком случае вероятность того, что автомобиль повернет налево, конечно же, увеличивается.

Было бы полезно сформулировать все это точнее. Пусть E — некоторое событие; обозначим $P(E)$ его вероятность. И если F — дополнительная информация, будем обозначать как $P(E|F)$ новую вероятность того, что событие E осуществится с учетом F. Читается «вероятность события E при условии F», а число $P(E|F)$ называется «условной вероятностью события E при условии F».

В первом примере E обозначим выпадение четверки, а F — информацию о том, что число четное. Как мы уже видели, $P(E|F) = \frac{1}{3}$.

В общем случае процедура такая. Вначале находят величины $P(F)$ (вероятность события F) и $P(E \text{ и } F)$ (вероятность того, что осуществятся E и F). Тогда $P(E|F)$ определяется

[1] Я осмелюсь даже предположить, что способность корректировать вероятность при получении новой информации сыграла важную роль в ходе эволюции рода человеческого и в итоге стала непосредственно встроенной в мозг.

следующим образом:

$$P(E|F) := \frac{P(E \text{ и } F)}{P(F)}.$$

Проверим эту формулу на нашем примере. У нас $P(F) = \frac{1}{2}$, поскольку в половине бросаний выпадает четное число. Событие «E и F» означает, что выпавшее число четно и равно четырем. Это может произойти только тогда, когда выпадает четверка, так что $P(E \text{ и } F) = \frac{1}{6}$. Поэтому

$$P(E|F) = \frac{P(E \text{ и } F)}{P(F)} = \frac{1/6}{1/2} = \frac{1}{3}.$$

В следующем примере речь шла об извлечении карты наугад из стандартной колоды в 52 листа. Вероятность события E (извлечена дама бубен) равна $1/52$, ведь в колоде только одна такая карта. Однако если кто-то подсмотрел извлеченную карту и сообщил вам, что это дама, то вероятность того, что это дама бубен, возрастает до $1/4$. Если F — дама, то $P(F) = 4/52 = 1/13$ (в колоде четыре дамы) и $P(E \text{ и } F) = \frac{1}{52}$ (дама бубен только одна). Итак,

$$P(E|F) = \frac{P(E \text{ и } F)}{P(F)} = \frac{1/52}{1/13} = \frac{1}{4}.$$

ФОРМУЛА БАЙЕСА

Замечательно, что условные вероятности в какой-то мере могут быть обращены. Для этого используют *формулу Байеса*. Вот реальный пример.

Вскоре после визита друзей вы заметили, что исчез ваш любимый DVD. Вы знаете, что один из ваших друзей имеет привычку то и дело одалживать диски, не предупреждая об этом. Кого вам следует подозревать?

Для наших целей лучше всего использовать формулу Байеса следующим образом. Рассмотрим случайный эксперимент, в котором каждый исход можно отнести к одному из трех классов: B_1, B_2, B_3. Важно, что эти классы не перекрываются.

В примере с бросанием кости эти классы можно задать так:

B_1 — выпала единица или двойка;
B_2 — выпала тройка или четверка;
B_3 — выпала пятерка или шестерка.

Рассмотрим теперь возможный результат нашего эксперимента, который мы обозначим A. Например, мы можем интересоваться событием A — выпало простое число. Если известны условные вероятности $P(A|B_1)$, $P(A|B_2)$, $P(A|B_3)$, а также вероятности $P(B_1)$, $P(B_2)$, $P(B_3)$, то мы можем получить «обратные» условные вероятности $P(B_1|A)$, $P(B_2|A)$, $P(B_3|A)$:

$$P(B_1|A) = \frac{P(A|B_1)P(B_1)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + P(A|B_3)P(B_3)},$$
$$P(B_2|A) = \frac{P(A|B_2)P(B_2)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + P(A|B_3)P(B_3)},$$
$$P(B_3|A) = \frac{P(A|B_3)P(B_3)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + P(A|B_3)P(B_3)}.$$

Это и есть формулы Байеса [1].

Мы не собираемся доказывать здесь эту формулу. Однако для иллюстрации приведем пример. Классы B_1, B_2, B_3 останутся прежними: B_1 — выпала единица или двойка; B_2 — выпала тройка или четверка; B_3 — выпала пятерка или шестерка.

А в качестве A возьмем событие «выпало число больше трех». Выполнив описанные в предыдущем разделе вычисления, получим

$$P(A|B_1) = 0,$$
$$P(A|B_2) = \frac{1}{2},$$
$$P(A|B_3) = 1,$$

и, разумеется, $P(B_1) = P(B_2) = P(B_3) = \frac{1}{3}$.

[1] Если бы вместо трех классов мы выбрали n, т. е. $B_1, B_2, \ldots, B_n$, то формула Байеса приняла бы вид

$$P(B_i|A) = \frac{P(A|B_i)P(B_i)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + \cdots + P(A|B_n)P(B_n)},$$

где символ i можно заменить на один из символов $1, 2, \ldots, n$.

Допустим, кость брошена, и в результате событие A произошло (выпало число больше трех). Чему тогда равна вероятность, скажем, события B_2? Для ответа на этот вопрос воспользуемся формулой Байеса:

$$P(B_2|A) = \frac{P(A|B_2)P(B_2)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + P(A|B_3)P(B_3)} =$$

$$= \frac{(1/2)\cdot(1/3)}{0\cdot(1/3) + (1/2)\cdot(1/3) + 1\cdot(1/3)} = \frac{1}{3}.$$

Аналогично, пользуясь той же формулой Байеса, можно получить[1)], что $P(B|A) = 0$ и $P(B_3|A) = \frac{2}{3}$.

ЛУЧШАЯ СТРАТЕГИЯ В ПАРАДОКСЕ МОНТИ ХОЛЛА: СТАНДАРТНЫЙ ВАРИАНТ

После всех этих приготовлений мы, наконец, можем выяснить, выгодно ли сменить дверь. Начнем с вероятностей, относящихся к дверям, за которыми спрятан автомобиль. Мы используем следующие обозначения:

B_1 — автомобиль за дверью 1;
B_2 — автомобиль за дверью 2;
B_3 — автомобиль за дверью 3.

Мы будем считать, что все эти варианты равновозможны, так что

$$P(B_1) = P(B_2) = P(B_3) = \frac{1}{3}.$$

Пусть это несколько наивно, но если нет никаких доводов против, мы можем принять это предположение.

Теперь мы подошли к важному пункту — пора принимать решение. Играющий выбрал дверь 1, ведущий открыл козлика за дверью 3, и не ясно, что делать — сменить ли предпочтение с двери 1 на дверь 2. Теперь анализ.

Событие «ведущий открыл козлика за дверью 3» мы обозначим A. Мы хотим, пользуясь этой информацией, ответить на вопрос, где правдоподобнее находиться автомобилю: за дверью 1 или за дверью 2? С учетом этих обозначений, мы хотим знать соотношение между числами

[1)] В этом случае проще провести прямые вычисления, но результат, разумеется, был бы тот же.

$P(B_1|A)$ и $P(B_2|A)$. Если они одинаковы, то менять дверь нет смысла, но если второе из них больше, то следует сменить.

В этой ситуации естественно применить формулу Байеса. Но чтобы ее применить, надо знать величины $P(A|B_1)$, $P(A|B_2)$, $P(A|B_3)$.

Чему равна условная вероятность $P(A|B_1)$? Иначе говоря, если автомобиль за дверью 1, то чему равна вероятность того, что ведущий отворит дверь 3? Конечно же, он мог бы отворить дверь 2 (но только не дверь 1). Мы будем считать, что ведущий с равными вероятностями отворяет двери 2 и 3, и поэтому $P(A|B_1) = \frac{1}{2}$.

Еще проще вычислить $P(A|B_2)$. Если автомобиль за дверью 2, с какой вероятностью будет открыта дверь 3? Разумеется, она равна 1, так как ведущий не может отворить дверь 2 (за ней автомобиль), дверь 1 тоже под запретом, поскольку именно она выбрана играющим.

Так же легко вычислить $P(A|B_3)$. Эта вероятность равна нулю, поскольку ведущий не будет отворять дверь, за которой скрыт автомобиль. Итак,

$$P(A|B_1) = \frac{1}{2},$$
$$P(A|B_2) = 1,$$
$$P(A|B_3) = 0.$$

И теперь можно применять формулу Байеса:

$$P(B_1|A) = \frac{P(A|B_1)P(B_1)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + P(A|B_3)P(B_3)} = \\ = \frac{(1/2)\cdot(1/3)}{(1/2)\cdot(1/3) + 1\cdot(1/3) + 0\cdot(1/3)} = \frac{1}{3}$$

и

$$P(B_2|A) = \frac{P(A|B_2)P(B_2)}{P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + P(A|B_3)P(B_3)} = \\ = \frac{1\cdot(1/3)}{(1/2)\cdot(1/3) + 1\cdot(1/3) + 0\cdot(1/3)} = \frac{2}{3}.$$

Мы обозначили $P(B_1|A)$ вероятность выиграть, приняв стратегию «не менять выбор», а $P(B_2|A)$ — вероятность выиграть со стратегией «менять», так что расчеты показывают, что смена двери удваивает шансы на выигрыш.

ВСЯ ПРАВДА О ПАРАДОКСЕ МОНТИ ХОЛЛА

Если вы внимательно ознакомились с предыдущим анализом, то заметили, что для вывода «смена двери лучше, это удваивает шансы на выигрыш», нам потребовалось сделать несколько допущений. Например, мы положили $P(A|B_1) = \frac{1}{2}$. Но есть и другие варианты. Может случиться так, что ведущий только тогда отворяет дверь 3, когда это возможно (т. е. если это не выдает местоположения автомобиля). Чтобы исследовать более общий случай, мы положим $P(A|B_1) = p$, где p — некоторое число между нулем и единицей. Тогда анализ дает

$$P(B_1|A) = \frac{p}{1+p}, \quad P(B_2|A) = \frac{1}{1+p}.$$

Поскольку $p < 1$, первое из этих чисел всегда меньше второго, так что мы видим, что менять выбор всегда выгоднее, хотя выигрыш в вероятности может быть небольшим.

К этой задаче может быть и другой подход[1)]. Стратегия играющего может не учитывать намерений ведущего и заключаться просто в перемене выбора. Доводы такие.

Во время первоначального выбора (и это выполняется вне зависимости от того, изменится он в конце или нет) можно выиграть автомобиль с вероятностью $\frac{1}{3}$, поскольку автомобиль может с равными вероятностями оказаться за любой дверью.

[1)] Я благодарен профессору Дитеру Пуппе из Гейдельберга за эту идею.

При смене выбора выигрыш случается именно в том случае, когда первоначальный выбор был неправильным, т. е. с вероятностью $\frac{2}{3}$.

Эти доводы можно уточнить. Пусть p_1, p_2, p_3 обозначают вероятности, с которыми автомобиль стоит соответственно за дверью 1, 2, 3. Тогда если выбрана дверь 1, вероятность выиграть автомобиль без смены двери равна p_1, а вероятность выиграть автомобиль, сменив дверь, равна $p_2 + p_3$.

Возможно, что некоторые читатели озадачены фактом, что во втором рассуждении действия ведущего не играют роли. Следует рассмотреть эту сложность внимательнее, чтобы убедиться, что оба рассуждения верны.

В первом рассуждении ситуация была задана следующим образом. Выбрана дверь 1, дверь 3 (за которой козлик) отворена. И все вероятности вычислялись исходя из этой ситуации.

Во втором рассуждении ситуация иная. Действия ведущего роли не играют, и в любом случае следует менять выбор. Однако интуитивно сложно понять, что эта разная информация ответственна за разные вероятности.

Глава 15

В ОТЕЛЕ ГИЛЬБЕРТА ВСЕГДА ЕСТЬ СВОБОДНЫЕ НОМЕРА

Математикам часто приходится иметь дело с бесконечностью. Общепризнано, что в царстве бесконечности действуют законы, которые очень отличаются от привычных нам.

В дальнейшем мы будем рассматривать простейшее бесконечное множество, а именно множество натуральных чисел 1, 2, 3, ... Великий Галилео в своем труде «Discorsi» (1638 г.) поражался удивительному явлению, которое связано с этим множеством. Оказывается, натуральных чисел столько же, сколько их квадратов, т. е. чисел 1, 4, 9, 16, ... Действительно, можно записать обе последовательности одну под другой так, что между ними установится взаимно однозначное соответствие. Математическая подоплека такова: если убрать часть бесконечного множества, остаток получается того же «размера», что исходное множество.

Рис. 15.1. Отель Гильберта

Математик Давид Гильберт (1862–1943) придумал интересное описание этого явления, известное под названием «Отель Гильберта». Посмотрите на рис. 15.1. В этом отеле бесконечно много апартаментов, занумерованных числами

1, 2, 3, ... И вот, в выходной день отель полон. Поздно вечером прибывает гость и требует номер. Если обычный отель полон, то в нем нет свободных номеров, но в отеле Гильберта все иначе. Здесь у этой проблемы есть решение! Гость из номера 1 перебирается в номер 2, гость из номера 2 перебирается в номер 3 и т. д. Теперь номер 1 свободен, и место для ночлега находится для всех. Но потом в отель прибывает целый автобус с восемью отдыхающими, и всем нужно место. И эту проблему можно решить: теперь гость из номера 1 отправится в номер 9, и т. д.

Систематическое изучение бесконечных множеств началось только в девятнадцатом веке с пионерской работы Георга Кантора (1845–1918). Она встретила холодный прием у многих его коллег, убежденных в том, что математика должна ограничиваться изучением конкретных и конструктивных вещей. В наше время Кантор полностью реабилитирован, и бесконечность входит в число повседневных математических объектов, таких как целые числа, геометрические фигуры и вероятности.

СУМАТОШНАЯ НОЧЬ

Бурная ночь в отеле Гильберта еще не закончилась, нам есть еще о чем рассказать. На ближайшую станцию прибыл поезд, в котором *бесконечно много* пассажиров, и каждому из них нужен номер. Все они устали, и все они забронировали номера заранее.

Но отель полон. Что же делать? Решение есть. Автоматическая система предписывает гостю из номера 1 перебраться в номер 2, гостю из номера 2 в номер 4, гостю из номера 3 в номер 6, и т. д.; каждый гость переезжает в апартаменты с номером вдвое больше чем был. Теперь все апартаменты с нечетными номерами свободны, и все уставшие путешественники могут разместиться.

То, что мы описали, — не более чем мысленный эксперимент, иллюстрирующий некоторые явления, связанные с бесконечными множествами, однако мы должны упомянуть некоторые практические недостатки, присущие описанному явлению. Гость n из номера n переезжает в номер $2n$. Для малых n это несложно, но при больших n

придется преодолеть большое расстояние между старым и новым номерами. Если предположить, что постояльцы отеля Гильберта могут ходить только с ограниченной скоростью, то смена номеров не сможет осуществиться за конечное время.

Но эта проблема уже изначально была заложена в ситуацию. Если всех гостей предупреждают о грядущем переезде одновременно, то всё сработает: все могут переехать сразу же, и через десять минут воцарится покой. Но поскольку информация не может путешествовать быстрее света, гости из дальних комнат получат сигнал только через долгое время.

Глава 16

ЭТО УДИВИТЕЛЬНОЕ ЧИСЛО π

У числа π (произносят «пи») есть все шансы занять первое место в любом споре математиков о самом важном числе. Хорошо известно его значение в геометрии, и формулы, вроде «длина окружности равна π, умноженному на диаметр», знают все школьники.

Но это число появляется почти во всех областях математики, даже в тех, где окружностями и не пахнет. Оно важно для теории вероятностей, и это нашло свое отражение на банкноте, достоинством в десять немецких марок (см. гл. 25), где иллюстрируется вклад великого математика Гаусса.

У числа π есть много замечательных свойств. Если нужно использовать его в конкретной формуле, скажем, для числа семян, требующихся, чтобы засеять круглое поле, можно использовать приближение с малым количеством десятичных знаков; скажем, $\pi \approx 3{,}14$. Однако можно доказать, что точного значения π не может дать никакое конечное число десятичных знаков. Их потребуется бесконечно много. Действительно, π — *трансцендентное число*, а к ним относятся самые «трудные» в иерархии чисел. Этот факт был доказан в девятнадцатом веке, и таким образом была решена древняя задача о квадратуре круга (в гл. 33 об этом рассказывается подробнее).

Если нельзя выписать все цифры после запятой, почему бы не записать их как можно больше? Некоторые математики и IT-специалисты соревнуются — кто больше, используя компьютеры и тонкие теоретические результаты, получая все больше и больше знаков.

И наконец, следует сказать, что π произвело некоторое смятение и среди нематематиков. Существуют клубы фанатов числа π, а несколько лет назад появился фильм под названием «π». Да просто, наконец, настроение, которое дарит туалетная вода π от Живанши.

ЧИСЛО π В БИБЛИИ

Те, кто умеет читать между строк, могут найти ссылку на число π в Библии (Третья книга Царств, 7.23):

И сделал литое [*из меди*] *море, — от края его до края его десять локтей, — совсем круглое, вышиною в пять локтей, и снурок в тридцать локтей обнимал его кругом.*

Здесь «литое море» — это сосуд для святой воды, установленный перед храмом Соломона. Мы представляем его себе круглым, так что из Библии можно выделить следующую информацию:

длина окружности, деленная на диаметр, равна 3.

Это неплохое приближение числа π. Вавилоняне и египтяне пользовались гораздо лучшим приближением $\pi \approx 22/7 = 3{,}142\ldots$. Правда, неточность может объясняться тем, что сосуд измеряли не у самого края, а несколько ниже.

ПРИБЛИЗИТЕЛЬНЫЕ ОЦЕНКИ ЧИСЛА π

Некоторые факты о числе π можно объяснить и без больших познаний в математике. Допустим, есть круг, вписанный в квадрат, как на рис. 16.1, слева. Если бы нам вздумалось путешествовать вдоль круга, начав в точке, где он касается квадрата, и закончив в противоположной, мы бы проехали расстояние, равное половине длины окружности. Поэтому оно равно половине произведения диаметра и π, т. е. $\frac{1}{2} \cdot 2r \cdot \pi = \pi \cdot r$, где r — радиус (поэтому $2r$ — диаметр).

Рис. 16.1. π меньше четырех и больше трех

А вот если между теми же точками мы путешествовали бы вдоль квадрата, то преодолели бы расстояние $4 \cdot r$. Видно, что $\pi \cdot r$ меньше $4 \cdot r$, и если мы разделим это неравенство на r, то получим, что π меньше 4. Аналогично можно убедиться, что π больше 3. Для этого нужно описать окружность около шестиугольника (как на рис. 16.1 справа). Теперь путь между двумя противоположными точками *короче*, если путешествовать вдоль сторон шестиугольника. Нужно обойти три стороны, каждая длины r, и это показывает, что $3 \cdot r$ меньше $\pi \cdot r$. Поэтому число 3 должно быть меньше π.

Рисунки дают нам дополнительную количественную информацию: путь вдоль квадрата *гораздо* длиннее, чем вдоль окружности, а вот путь вдоль шестиугольника только *чуточку* короче. Это означает, что число π должно быть гораздо ближе к 3, чем к 4.

Глава 17
ВЫЧИСЛЯЕМАЯ СЛУЧАЙНОСТЬ

Удача — это что-то такое, что не может быть вычислено заранее: даже самый блестящий математик может только подсчитать вероятности проигрыша и выигрыша.

Но это только часть всей правды, поскольку неточность становится меньше и меньше с ростом числа случайных воздействий. Представьте себе монету, которая с равными вероятностями (по 50%) падает орлом или решкой. Подбрасывая такую монетку, вы принимаете решение «да» или «нет» строго наугад, ведь результат заранее предсказать невозможно. Однако если вы подбросите ее десять раз, подсчитаете число орлов и сделаете так несколько раз, то «средние» значения будут попадаться гораздо чаще. Гораздо вероятнее, что в результате окажется ровно пять орлов (25%), а не один (0,1%). Если увеличить число бросаний, то тенденция станет еще явственней, число орлов с большой вероятностью будет колебаться в узком коридоре около половины числа бросаний.

В основе этого явления лежит одна из важнейших предельных теорем теории вероятностей. Это теорема описывает сдвиг от непредсказуемого к детерминированному. Этот факт интересен не только с теоретической точки зрения. Например, можно вспомнить, что в соответствии с принципами квантовой механики в наномасштабе мир управляется случайными процессами. И только суперпозиция невообразимо многих случайных событий дает нам иллюзию того, что мы живем в детерминированном мире. Тот же принцип работает, давая возможность предсказывать результат президентских выборов после того, как становится известен малый процент голосов, поскольку правдоподобный результат можно получить на основании малой случайной выборки.

И наконец, на предельные теоремы полагаются покупатели в сети супермаркетов и управляющие общественным

транспортом. Совершенно неправдоподобно, чтобы внезапно все покупатели испытали потребность в покупке пекарского порошка или все те, кто живет возле одной из пригородных станций, решили отправиться поездом в 8.50 к центральному вокзалу.

НАЧНИТЕ СВОЙ СОБСТВЕННЫЙ БИЗНЕС

Предельных теорем — целый зоопарк. Все они говорят о том, что с ростом числа случайных воздействий остается все меньше места для случайности. Допустим, вы решили открыть игорное заведение на сельской ярмарке. Для простоты будем считать, что посетитель бросает одну игральную кость. Если выпадет шесть очков, он выигрывает 30 евро. В противном случае — ничего. Поэтому за каждую игру вам придется с вероятностью $\frac{1}{6}$ выплатить посетителю 30 евро, так что средняя выплата составит $\frac{1}{6} \cdot 30 = 5$ евро.

Поэтому за право играть следует взимать хотя бы эту сумму: вы же не хотите потерять деньги. Предположим, что входная плата составляет 7 евро. Сколько тогда вы получите с одного клиента? С вероятностью $\frac{1}{6}$ вы потеряете 23 евро (выплатите тридцать за выигрыш и возьмете семь за вход), а с вероятностью $\frac{5}{6}$ вам останется 7 евро. Поэтому каждый клиент в среднем приносит

$$-\frac{1}{6} \cdot 23 + \frac{5}{6} \cdot 7 = \frac{-23+35}{6} = 2 \text{ евро.}$$

Если в удачный день к вам придут 300 клиентов, можете рассчитывать на прибыль в $2 \cdot 300 = 600$ евро. А в соответствии с предельными теоремами теории вероятностей с таким числом игроков вы можете быть уверенным в этих 600 евро почти наверняка. Совершенно неправдоподобно, чтобы вдруг повезло столь большому числу играющих, что в кассе оказалось менее 550 евро. К сожалению, нет почти никакой надежды получить более 650 евро.

ИСЧЕЗАЮЩАЯ ВЕРОЯТНОСТЬ

В этом разделе мы рассмотрим *численный пример*, связанный с предельными теоремами. Вначале бросим

правильную монету десять раз. Следует ожидать, что при этом выпадет пять орлов. Точные значения вероятностей таковы:

Число выпадений орлов	Вероятность
Ровно 5	24,6%
От 4 до 6	54,2%
От 3 до 7	77,4%

Теперь подбросим монету сто раз:

Число выпадений орлов	Вероятность
Ровно 50	7,95%
От 45 до 55	72,9%
От 40 до 60	96,5%

И наконец, тысячу раз:

Число выпадений орлов	Вероятность
Ровно 500	2,52%
От 490 до 510	49,2%
От 480 до 520	80,6%
От 470 до 530	94,6%

Итак, хотя и неправдоподобно получить ровно пятьсот орлов, можно рассчитывать почти наверняка, что отклонение от этого числа составит не более 30, т. е. 6% от числа бросаний.

Исчезновение влияния случайности можно сделать очень наглядным. Предположим, ваша приятельница Мария играет в игру и с равными вероятностями выигрывает или проигрывает один евро. Результаты отдельных игр мы обозначим x_1, x_2, ..., а результат последовательности игр будет выглядеть примерно так: 1, 1, –1, 1, –1, ... Сложив первые n чисел этой последовательности, мы получим чистую прибыль или проигрыш после n-го раунда. В нашем примере эти результаты для $n = 1, 2, 3, 4, 5$ — это числа 1, 2, 1, 2, 1. А теперь, чтобы найти *средний* выигрыш,

результат после n-го шага нужно разделить на n, что даст $1{,}1, \frac{1}{3}, \frac{1}{2}, \frac{1}{5}, \ldots$.

Заметьте, что эти величины стремятся к нулю. На рис. 17.1 изображен график этих средних значений для отдельной последовательности игр. В начале удача и неудача чередуются, затем идет черная полоса, а потом график начинает понемногу расти. Но в длинной серии выигрыши и проигрыши *всегда* сравниваются, и средний выигрыш стремится к нулю.

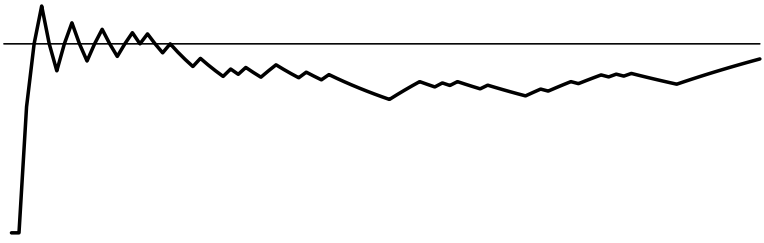


Рис. 17.1. Средний выигрыш стремится к нулю

Глава 18

МИЛЛИОННАЯ НАГРАДА: КАК РАСПРЕДЕЛЕНЫ ПРОСТЫЕ ЧИСЛА?

В этой главе мы снова будем обсуждать простые числа. Они ничуть не растеряли своего очарования за те две тысячи лет, что люди их изучают. (Напомним, что простые числа — это целые числа, которые нельзя представить в виде произведения меньших целых чисел; так что, например, 7 и 19 — простые числа, а 20 — нет.) Они привлекали даже Карла Фридриха Гаусса, одного из величайших математиков всех времен. Он хотел узнать, как простые числа распределены среди целых. Можно ли знать, сколько простых чисел находится в-о-о-о-н там?

Два факта известны точно. Во первых, простые числа выскакивают как грибы в лесу, без всякого правила. Если вы отметите простые числа среди первой сотни положительных целых, вы увидите, что в их расположении нет никакого порядка. Кроме того, ясно, что у большого числа меньше шансов оказаться простым, чем у маленького, ведь у большого потенциальных делителей больше.

Гаусс действовал прагматично, занимаясь тем, что сегодня мы называем «экспериментальной математикой» (и используем для этого компьютеры). Основываясь на конкретных вычислениях, он высказал гипотезу, которую в наше время называют теоремой о целых числах. Доля простых чисел, меньших заданного числа, может быть хорошо приближена. Для числа с k цифрами она почти точно равна $0{,}43/k$. (Ниже мы дадим точную формулу.) Таким образом, в пределах 1000, где $k = 3$, получается $0{,}43/3$, т. е. около 0,143 или 14,3%. В пределах 1 000 000 доля простых чисел равна только $0{,}43/6$, или 7,2%.

Гаусса давно уже не было, когда удалось строго доказать его гипотезу. В конце девятнадцатого века независимо друг от друга это сделали математики Ж. Адамар и Ш. Ж. Валле Пуссен.

Но это вовсе не конец истории. С тех пор появились описания распределения простых чисел, гораздо точнее

гауссовских. За решение одного из аспектов этой задачи в 2000 г. была назначена премия в миллион долларов.

ТЕОРЕМА О ПРОСТЫХ ЧИСЛАХ

На рис. 18.1 наглядно представлен рост простых чисел. График начинается слева, k-й отрезок изображает k-е простое число на высоте k. Например, четвертый отрезок (на рисунке он выделен) изображает четвертое целое число, т. е. 7, и поэтому абсцисса этого отрезка начинается в 7 и заканчивается в 11, — на следующем простом числе.

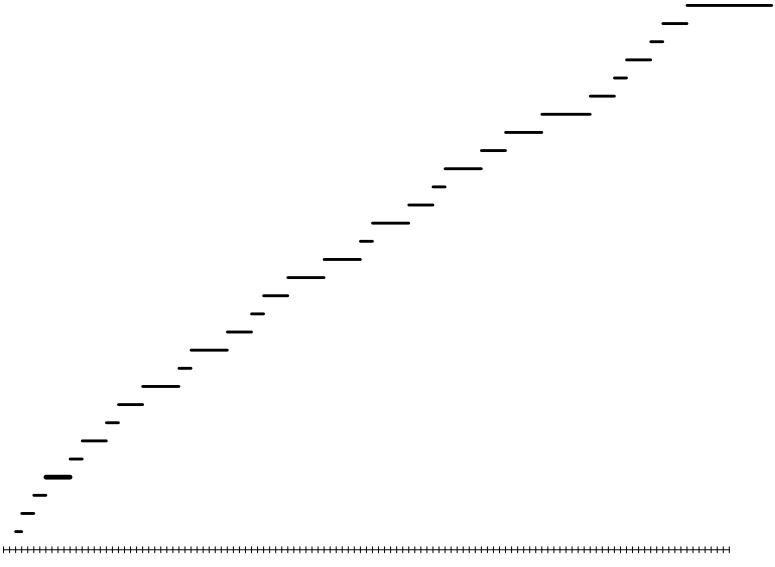


Рис. 18.1. Распределение простых чисел

Теорема о простых числах говорит о том, что для больших x высота графика, изображающего количество простых чисел, не превышающих x, очень хорошо аппроксимируется кривой $x/\ln x$.

Чтобы понять это утверждение, нужно знать, что такое $\ln x$ — натуральный логарифм[1)] числа x. Это то число y,

[1)] См. гл. 36.

для которого значение

$$(2{,}71828\ldots)^y$$

равно x. Упрощая, можно сказать, что логарифм k-значного числа можно приблизить числом $k/0{,}43$ (например, значение логарифма 8000 равно $8{,}987\ldots$, а $4/0{,}43 = 9{,}302\ldots$).

Чтобы убедиться в точности аппроксимации, рассмотрим несколько примеров. Для $x = 100\,000\,000$ существует 5 761 455 простых чисел, меньших x. Отношение $x/\ln x$ отличается от этого значения на 332 774, так что ошибка составляет около шести процентов. При $x = 10\,000\,000\,000$ существует 344 052 511 простых чисел, меньших x. А теорема о простых числах дает оценку на двадцать миллионов простых чисел меньше. Это большое расхождение, но ошибка лишь слегка превышает четыре процента.

Хотя в предыдущем обсуждении мы употребляли слова «очень хорошо аппроксимируется», более подробный анализ показывает, что можно придумать более сложные и точные формулы. Самые лучшие из них дают количество простых чисел, меньших x, с очень высокой точностью.

Например, существует формула, которая для $x = 100\,000\,000$ ошибается только на 754, и ошибка составляет около одной сотой процента. А для $x = 10\,000\,000\,000$ она ошибается только на 3104, и ошибка меньше одной тысячной процента.

Однако, чтобы строго оценить величину ошибки, требуется решить одну известную нерешенную задачу, *гипотезу Римана*. Именно за ее решение Математический институт Клэя обещает миллионное вознаграждение (подробности можно найти на сайте http://www.claymath.org).

Глава 19
ПЯТИМЕРНЫЙ ТОРТ

В последнее время, например в рецензиях на фильмы и книги, да и в бытовой речи, как неодобрительный эпитет употребляется выражение «плоский» или даже «прямолинейный». Имеется в виду, что предмет осуждения примитивен, без сложных ответвлений. Но что в действительности означают слова одно-, дву-, трехмерный? Что же такое *размерность*?

Говоря попросту, размерность геометрического объекта — это число параметров, требующихся для задания точки этого объекта. Возьмем, например, прямую линию. Зафиксируем на ней некоторую точку P. Тогда любую другую точку можно задать одним-единственным числом: достаточно указать расстояние от нее до точки P, используя положительные величины для точек справа от P и отрицательные — для точек слева. Поэтому прямая одномерна.

Точно так же можно показать, что поверхность Земли двумерна. Например, любую точку на ней можно задать широтой и долготой. В пространстве потребуется уже три числа, а если нужно определить точку одновременно в пространстве и времени, то понадобится уже четыре числа — они задают точку в пространстве-времени теории относительности.

Математики часто работают и с более высокими размерностями. Чтобы разобраться в той или иной ситуации, обычно достаточно рассмотреть дву- или трехмерный пример, включающий самые важные аспекты ситуации; точно так же как по двумерной фотографии возможно восстановить трехмерный оригинал. Таким образом, пятимерное, например, пространство — это просто множество точек, для задания которых требуется пять чисел.

Это все может звучать сложно и абстрактно, однако есть параллели с нашим повседневным опытом. Например, рецепт торта может быть задан количеством различных ин-

гредиентов в граммах. Если записать количества муки, сахара, масла, яиц и разрыхлителя в виде (200, 100, 80, 20, 3), то такое представление будет содержать самую важную информацию. В этом, конечно же, ничего захватывающего нет, но на самом деле в пяти измерениях тоже нет ничего сложного.

СКАЧОК В ПЯТОЕ ИЗМЕРЕНИЕ

У математиков такие же извилины в коре головного мозга, как и у других людей, поэтому они не могут изобразить более трех измерений. Однако они без труда работают с объектами высоких размерностей. Важна только способность визуализовать важные аспекты задачи в двуили на худой конец трехмерной картинке. Если важны расстояния, то картинка должна воспроизводить расстояния между точками аккуратно: точки, равноудаленные в действительности, должны быть равноудаленными и на картинке и т. д. Фактически эта работа напоминает работу составителей карт; они тоже изображают на картах только самые важные аспекты реальности.

Посмотрим, как математики подходят к изучению четвертого измерения. Сначала поупражняемся в трех измерениях. Как объяснить что такое поверхность куба (трехмерного) существу, которое знакомо только с двумя измерениями? Начнем с рис. 19.1.

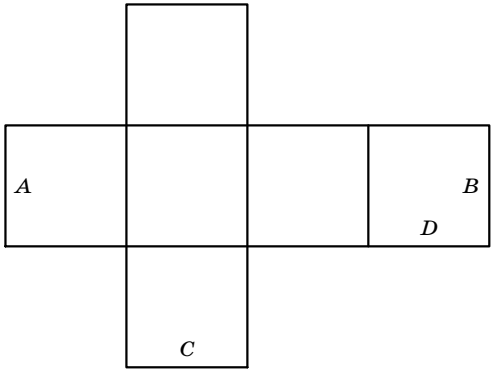
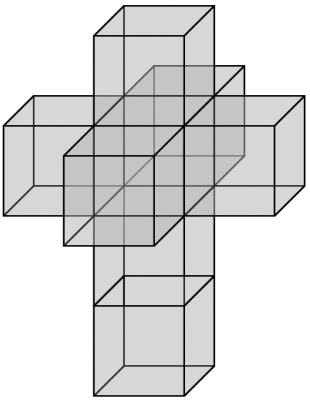


Рис. 19.1. Двумерное существо движется по этой поверхности

Здесь изображена развертка куба. Поместим наше двумерное существо (будем звать его Фердинандом) на развертку и отправим в путешествие, потребовав соблюдения следующих условий:

- По поверхности можно перемещаться свободно, но покидать ее нельзя.
- Если у тебя возникло впечатление, что ты сполз с фигуры, на самом деле ты тотчас же вернулся на нее, войдя с другой стороны. Более точно, если ты покинул поверхность на стороне A, то ты вошел в нее на стороне B, а если покинул ее на стороне C, то вошел на стороне D, и т. д.[1)]



Так Фердинанд может привыкнуть к поверхности куба, что для нас не представляет никаких сложностей. Он заметит, наконец, что у поверхности границ нет, она никогда не заканчивается. Однако поверхность конечна; ее можно окрасить ограниченным количеством краски. Освоившись, Фердинанд обнаружит некоторые другие характеристики поверхности. Например, каждой точке соответствует другая точка, наиболее удаленная от первой. В трехмерном мире это точки-антиподы.

Теперь повторим опыт в более высокой размерности. Теперь *мы* — трехмерные существа, желающие ознакомиться с четвертым измерением. Мы хотим развить в себе способности представить трехмерную поверхность четырехмерного куба. Для этого мы разместимся на соответствующем изображении, на объекте, напоминающем

[1)] Другие правила обусловлены тем, что фигура представляется сложенной в поверхность куба; они описывают перемещения по смежным сторонам.

детский снаряд для лазанья. У нас есть инструкция с «правилами лазанья»:

- Нельзя покидать снаряд.
- Если у тебя возникло впечатление, что ты сполз с фигуры, на самом деле ты тотчас же вернулся на нее, войдя с другой стороны. Например, покинуть верхушку — все равно что вернуться снизу.

Есть еще кое-какие правила, здесь не описанные.

Таким образом действительно можно изучить структуру геометрического объекта, недоступного непосредственному восприятию.

Закончим упоминанием о том, что художник Сальвадор Дали (1904–1989) обессмертил этот гиперкуб в своей картине «Распятие. Corpus Hypercubus», 1954. Возможно, она символизирует тот философский догмат, что понять можно только идею Бога, непосредственно он непостижим.

ФИЛЬМ НА ТЕМУ «ЧЕТВЕРТОЕ ИЗМЕРЕНИЕ»

2008 год был в Германии Годом математики. По этому поводу в музее технологий в Берлине проходила большая выставка Mathema и был отснят фильм: Как математики представляют четвертое измерение?

Вы можете пойти по ссылке

http://www.youtube.com/watch?v=xWRAEfhQ3gw

или воспользоваться непосредственно следующим QR-кодом:

Глава 20
КАЗНИТЬ НЕЛЬЗЯ ПОМИЛОВАТЬ

В математике термин *композиция* используется для того, чтобы обозначать новый объект, который возникает как результат действия над некоторыми двумя другими объектами. Например, из двух чисел x и y можно получить их сумму $x+y$ или произведение $x \cdot y$. В русском языке из двух слов *мясо* и *комбинат* образуется слово *мясокомбинат*. Точно так же из словосочетаний складываются осмысленные предложения.

Если, имея дело с композициями, мы хотим работать не с двумя, а с тремя элементами, возникает одна проблема. Складывая числа, допустим x, y и z, можно вначале построить сумму $x+y$, а затем прибавить z. С другой стороны, можно x прибавить к сумме $y+z$. Символически эти суммы трех слагаемых можно записать в виде $(x+y)+z$ или $x+(y+z)$. Если оба способа всегда приводят к одинаковым результатам, то говорят, что композиция *ассоциативна*. Это очень важное свойство; оно позволяет нам не утонуть в море скобок.

Хорошо известно, что сложение и умножение ассоциативны. Это означает, что верны равенства $(1+2)+3 = 1+(2+3)$ и $(3 \cdot 4) \cdot 5 = 3 \cdot (4 \cdot 5)$. Однако далеко не все важные правила построения композиций обладают этим замечательным свойством. Например, если из чисел x и y построить частное x/y, такая композиция ассоциативной не является. В этом можно убедиться, сравнив частные $(20/2)/2$ и $20/(2/2)$: они не совпадают, так как первое равно 5, а второе равно 20.

К счастью или нет, язык наш не ассоциативен, ведь от порядка, в котором мы складываем слова, зависит смысл предложения. Например, можно по-разному понимать, кто кого защищает, прочитав фразу «суды защищают законы».

Еще один пример описан в детской энциклопедии[1)].

[1)]Энциклопедия для детей. Т. 10. Языкознание. Русский язык. — М.: Аванта+, 1998. — С. 227–229. — *Прим. перев.*

Дана фраза: *Письма знакомой из Киева не заменят фотографии его любимой и милой дочери Марии*.

В условии дано простое предложение со сказуемым, выраженным глаголом *заменят*. При нем обязательно должны быть выражены подлежащее и прямое дополнение, кроме того, возможно и косвенное дополнение со значением адресата: *заменят кому-либо*. Адресат может вычленяться семью способами, включая нулевое его выражение: (*его* (*любимой* (*и милой* (*дочери* (*Марии*))))) или *знакомой из Киева* ...

Слева от сказуемого содержатся неоднозначные сочетания слов двух типов: 1) *письма знакомой* (чьи? или кому?); 2) *письма из Киева* или *знакомой из Киева*. В части предложения справа от сказуемого можно выделить следующие неоднозначные словосочетания: 1) *дочери Марии* — *дочери* (чьей?) *Марии* или *дочери по имени Мария*; 2) *любимой и милой дочери* — (*любимой и милой*) *дочери* или (*любимой*) *и* (*милой дочери*); 3) слово *его* может относиться только к ближайшему слову *любимой* или ко всей последующей группе слов; конструкция *фотографии X* имеет три смысла: а) фотографии, которые сделал *X*, б) фотографии, которые имеет *X*, в) фотографии, на которых изображен *X*.

ВСЕ ХОТЯТ СЭКОНОМИТЬ (ХОТЯ БЫ НА СКОБКАХ)

Ассоциативный закон позволяет нам сэкономить пару скобок. Однако в отсутствие ассоциативности неоднозначность, вызванная отсутствием скобок, может сказываться очень сильно. Она быстро растет с увеличением числа элементов. Если элементов три, скажем a, b и c, то приходится использовать скобки, чтобы определить, как следует понимать запись $a \circ b \circ c$: как $(a \circ b) \circ c$ или как $a \circ (b \circ c)$. Здесь символ $\circ$ означает какую-либо композицию. Для четырех элементов есть уже четыре возможности: понимать ли $a \circ b \circ c \circ d$ как $(a \circ b) \circ (c \circ d)$, $(a \circ (b \circ c)) \circ d$, $a \circ ((b \circ c) \circ d)$ или $a \circ (b \circ (c \circ d))$. Скобки необходимы, так как каждое из этих выражений может иметь различный смысл.

Без закона ассоциативности жизнь была бы гораздо сложнее. Без него нам пришлось бы обходиться без многих элементарных конструкций. Например, прежде чем использовать обозначение a^4 для выражения $a \circ a \circ a \circ a$, следует убедиться, что последнее определено однозначно. Как можно было бы определить выражение a^4, если бы смысл выражения $a \circ a \circ a \circ a$ зависел от порядка скобок?

Например, мы могли бы рассмотреть композицию $a \circ b = a^b$ для натуральных чисел. Она не ассоциативна, ведь почти для всех значений a даже такое простое выражение, как $a \circ a \circ a$, зависит от порядка скобок. Например, при $a = 3$ верны равенства $(3^3)^3 = 729$ и $3^{(3^3)} = 19\,683$. Для больших значений a отличия еще разительней: в числе $(9^9)^9$ «только» 77 цифр, а в $9^{(9^9)}$ — много миллионов. Это самое большое число, которое можно записать с помощью трех девяток.

КАЖДАЯ СЕЛЕДКА — РЫБА, НО НЕ КАЖДАЯ РЫБА — СЕЛЕДКА

Кроме ассоциативности композиции могут обладать еще одним свойством, которое математики считают очень важным: *коммутативность*. Говорят, что правило композиции коммутативно (выполняется закон коммутативности), если порядок элементов не имеет значения; иначе говоря, если всегда выполняется соотношение $a \circ b = b \circ a$. Хорошо известные примеры коммутативных композиций — сложение и умножение. А вот деление не коммутативно: 4, деленное на 2, вовсе не то же самое, что 2, деленное на 4. Композиция a^b, которую мы только что рассмотрели, тоже не коммутативна, поскольку 2^5, например, не равно 5^2. (На самом деле в этой композиции числа почти *никогда* нельзя менять местами. Конечно же, есть одно исключение $2^4 = 4^2$, но других двух разных натуральных чисел a и b, для которых $a^b = b^a$, не существует.)

В противоположность ассоциативности, которая почти всегда предполагается выполненной, во многих важных ситуациях коммутативность не имеет места. Приходится

работать с объектами вроде *некоммутативных групп* и *некоммутативных алгебр*, а это не так-то легко.

В нашем языке коммутативность, как и ассоциативность, не выполняется. Меняя порядок букв, получаем разные слова: «рысак» — вовсе не то же самое, что «крыса». Да и пару слов в предложении поменять местами можно не всегда. Еще капитан Врунгель с исключительной точностью установил, что каждая селедка — рыба, но не каждая рыба — селедка.

Есть и другие формальные параллели. Может быть, вы помните из школьных уроков математики, что существует *дистрибутивный закон*, который позволяет раскрывать скобки. Например, выражение $a \cdot (b + c)$ всегда равно $a \cdot b + a \cdot c$. Этому закону есть аналог и в русском языке: «десяти- и пятидесятирублевые банкноты» означает «десятирублевые и пятидесятирублевые банкноты».

И не забывайте про запятые! Заголовок этой главы стал уже хрестоматийным примером. А как бы вы расставили запятые в детском стихотворении Б. Заходера[1)]?

Очень-очень странный вид:
Речка за окном горит
Чей-то дом хвостом виляет
Песик из ружья стреляет
Мальчик чуть не слопал мышку
Кот в очках читает книжку
Старый дед влетел в окно
Воробей схватил зерно...

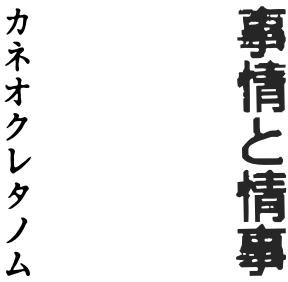
ДРУГИЕ ЯЗЫКИ

Как уже было упомянуто в предисловии к этому новому изданию, сейчас книга переведена и на другие языки. Именно эта глава всегда представляет для переводчиков особые затруднения, потому что именно здесь им приходится особенно напрягать свой интеллект. В оригинале, например,

[1)] Б. В. Заходер. Избранное. — М.: Детская литература, 1981. — *Прим. перев.*

можно найти фрагменты, не имеющие полных аналогов в переводах. Вот примеры из имеющихся в настоящее время переводов (в хронологическом порядке их появления):

- **Японский.** Данную статью было не так просто найти, потому что японцы изменили порядок: настоящая глава 20 в японском издании превратилась в раздел 42 из второго тома. На рисунке ниже вы можете увидеть варианты перевода. Слева заголовок представлен в шрифте Katakana. В зависимости от того, как читать, фраза может означать как «получить деньги и потом выпить», так и «Я получу деньги?». Справа приведен пример того, как может быть представлена одна и та же фраза в шрифте Kanji. Оригинал (вверху) и его перестановка (ниже) могут означать и «Ситуацию», и «Любовную интригу».



- **Английский.** Переводчик Дэвид Креймер представляет на наш суд два примера. Первый: one night stand, что означает «одноразовое явление» (чтобы оценить это, следует знать, что слова night stand — это просто «прикроватная тумбочка»). Второй пример был из области поп-культуры, который трудно комментировать.

  Некоммутативность языка иллюстрируется на таком примере: dog house (собачья конура) в противовес house dog (собачьи условия жизни).

- **Французский.** В качестве примера неассоциативности рассмотрим: paniers de fruits rouges: красные корзины для фруктов или корзины для красных фруктов? По-

хоже, также некоммутативно следующее: Gorge rouge (красное горло) в противовес rouge-gorge (малиновка).

- **Итальянский.** Итальянское издание еще только готовится, но эта глава уже переведена. Она начинается с fine settimana di vacanza: это «конец недели каникул» или «конец праздничных выходных»? В качестве примера некоммутативности было предложено soprattutto sotto (значительно ниже) или totto sottosopra (совершенно запутать).

Глава 21

ВОЗЬМИ МЕНЯ НА ЛУНУ

Обычно математики реагируют раздраженно, если собеседник, узнав об их профессии, спрашивает: «А разве в математике есть что-нибудь новое, не открытое?» Видимо, широкой публике неизвестно, что математика — это захватывающее приключение, которое требует огромных творческих способностей и завершается оно конкретным решением прикладных задач. Поэтому сегодня мы постараемся создать реалистичный образ, заглянув математику через плечо.

Чтобы понять нашу задачу, вообразите горную цепь, покрытую толстым слоем сияющего льда. Если вы хотите перебраться с одного пика на другой, той же высоты, теоретически нужно только уточнить направление и скатиться с горы: гравитация даст вам ускорение, а энергии, набранной во время спуска, хватит на подъем до следующего пика.

Аналогичная, хотя и более сложная ситуация возникает в космических путешествиях. Так же, как в примере с горными пиками, между некоторыми пунктами в космосе существуют пути, по которым можно перемещаться без затрат энергии, если разумно воспользоваться гравитационным притяжением Солнца, Луны и планет. И действительно, космические путешествия планируются с учетом таких технологий.

Конечно же, вначале требуется вычислить координаты нужных точек, а также найти минимальные коррекции курса, необходимые для поддержки правильного направления. Математические требования для таких вычислений огромны, и вполне можно сказать, что без развития теоретической и практической математики последних десятилетий и без невероятной производительности современных компьютеров такие вычисления были бы невозможны.

И это только одно из многих математических приложений, о которых мы могли бы рассказать.

МАТЕМАТИКА СО СКЛАДА

На протяжении столетий математика накопила огромный запас методов и результатов, которые стоят на полках готовыми к употреблению и использованию. Конечно же, большинство результатов последних столетий появились потому, что подоплека задачи представляла некоторое очарование для математического ума, а вовсе не с целью конкретных приложений.

Однако часто бывает так, что из практических приложений возникают задачи, которые можно решить, приспособив уже существующие математические инструменты.

Известным примером тому могут служить *конические сечения*. Это кривые, которые возникают при разрезании конуса острым ножом, — окружности, эллипсы, параболы и гиперболы. Об этих кривых многое было известно еще в Древней Греции, и одной из первых работ по этой теме около 200 лет до нашей эры стал труд «Конические сечения» Аполлония.

Семнадцать столетий спустя после развала византийской империи, математические знания Древней Греции стали

вызывать интерес в Центральной Европе. Однако большое число переводов и копий привело к тому, что за века накопилось много ошибок. Лучшие математики шестнадцатого и семнадцатого столетий занялись реставрацией, насколько это было возможно, оригинальных текстов. Так работа Аполлония стала известна в ученых кругах.

Труд Аполлония был крайне важен для астронома Иоганна Кеплера, который пытался привести космогонию Коперника в соответствие с результатами наблюдений. Коперник полагал, что планеты вращаются вокруг Солнца по круговым орбитам, но в начале семнадцатого века точность измерений позволила установить, что это не так. Поэтому Кеплер решил перейти от круговых орбит к эллиптическим. Все, что ему нужно было знать об эллипсах, он прочел у Аполлония.

Таких примеров множество. Теория относительности Эйнштейна (начало двадцатого века) немыслима без дифференциальной геометрии Римана (середина девятнадцатого века). А математика компьютерной томографии — развитой в 1960-х годах техники реконструирования трехмерного объекта по измерениям затухания лучей, проходящих сквозь этот объект в разных направлениях, — была полностью разработана за полвека до этого.

Но все это исключения. Как правило, теория, необходимая для успешного решения прикладной задачи, должна быть развита с момента постановки задачи. Это взаимодействие интеллектуальной притягательности и возможности решения конкретных задач делает математику столь привлекательной.

Глава 22

ОСТАТКИ СЛАДКИ

Если вы принесете домой 81 мармеладного мишку (рис. 22.1), чтобы раздать вашим пятерым детям, и попытаетесь разделить их поровну, то каждый ребенок получит по шестнадцать штук и один мишка останется (придется вам его украдкой съесть). Математики описывают это явление, говоря, что *остаток от* 81 *по модулю* 5 *равен* 1. Вообще, остаток числа m по модулю n — это остаток при делении числа m на n. Вычисления «по модулю» играют важную роль во многих областях математики.

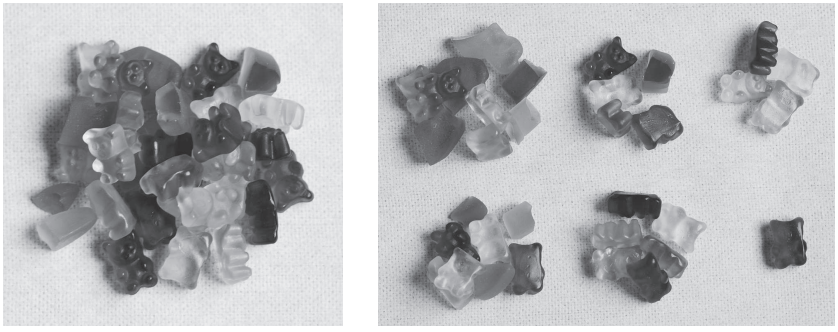


Рис. 22.1. 81 по модулю 5 равно 1

Нематематики тоже легко могут работать в этой технике во многих конкретных ситуациях. Например, если вы захотите знать, какой день недели наступит через 39 дней, интуиция вполне правильно подскажет вам вычислить остаток от 39 по модулю 7, т. е. 4. Поэтому через 39 дней будет тот же день недели, что и через 4. А который час будет через 50 часов? Легко! Вычисляем остаток от 50 по модулю 24, получаем 2, значит, через 50 часов будильник покажет то же время, что и через 2 часа.

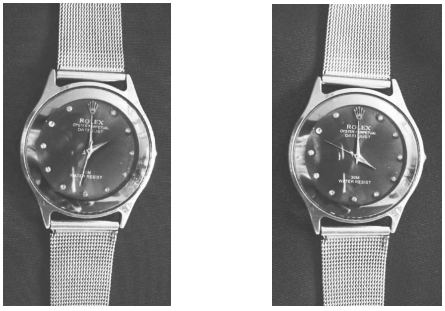


Рис. 22.2. Сейчас...и спустя 50 часов

До сих пор ничего особенного мы не сказали, а только ввели термин для одного хорошо известного метода вычислений. Однако математики видят подоплеку этой терминологии, и многие удивительные свойства чисел лучше всего формулировать в терминах *теории сравнений по модулю*. Рассмотрим один пример. Пусть n — простое число, а k — целое число между 1 и $n-1$ (включительно). Что произойдет, если k умножить на себя $n-1$ раз? Как это ни удивительно, но результат, взятый по модулю n, всегда равен 1. В примере с мармеладными мишками у нас было $n = 5$ (количество детей — простое число). Возьмем $k = 3$, тогда k (=3), умноженное на себя $n-1$ (=4) раз дает 81 — число мишек. То, что 81 по модулю 5 равно 1, следует из общего утверждения, которое мы сформулировали.

Тот факт, что в случае простого числа описанные вычисления по модулю всегда приводят к 1, был известен с давних пор. В семнадцатом веке его открыл французский математик Пьер Ферма. В наше время этот факт оказался особенно важным в криптографических приложениях, где используются простые числа с сотнями цифр (больше об этом можно прочитать в гл. 23).

ШЕСТЬЮ ШЕСТЬ — ОДИН

Остатки (т. е. числа 0, 1, ..., $n-1$) ведут себя как обычные числа при сложении и умножении, при условии что результат всегда приводится к остатку по модулю n.

Например, при сравнении по модулю 7 произведение 3 и 5 равно 1, поскольку $3 \cdot 5$ по модулю 7 равно 1. Аналогично, 4 плюс 6 равно 3, так как $6 + 4$ по модулю 7 равно 3.

Поэтому арифметика при сравнении по модулю очень похожа на обычную арифметику. Параллели особенно поражают, когда n — простое число. Тогда каждое число (кроме нуля) может быть умножено на некоторое число, причем в результате получится 1. В качестве примера возьмем число по модулю 7. Перебрав последовательно произведения $1 \cdot 6$, $2 \cdot 6$, $3 \cdot 6$, $4 \cdot 6$, $5 \cdot 6$, $6 \cdot 6$, мы получим остатки 6, 5, 4, 3, 2, 1 и убедимся, что $6 \cdot 6$ равно 1.

Это свойство не выполняется для чисел, не являющихся простыми. Например, если взять $n = 12$, то тщетны будут попытки найти число x, обладающее тем свойством, что $4 \cdot x$ равно 1 по модулю 12. Это обусловлено тем, что при делении $4 \cdot x$ на 12 всегда получается один из остатков 0, 4, 8.

Такое богатство арифметических свойств наводит на мысль о математическом значении теории сравнений по модулю. Например, выполняется свойство *коммутативности* сложения, т. е. $a + b$ всегда равно $b + a$ при сложении по некоторому модулю n.

Глава 23
СОВЕРШЕННО СЕКРЕТНО!

Простые числа уже появлялись в этой книге. Сейчас мы расскажем о том, как большие простые числа революционизировали *криптографию*, науку о секретных кодах.

Рис. 23.1. Классическая криптография: машина «Энигма»

Предположим, что вы установили простоту двух очень больших чисел (обозначим их p и q) и это известно только вам. Слово «большие» означает, что в этих числах по несколько сотен цифр. Затем вы вычислили произведение $p \cdot q$, получив в результате n.

Числа p и q спрятаны в числе n, как иголки в стоге сена. В частности, не существует метода найти множители p и q, зная их произведение n, за разумное время: даже самым быстрым компьютерам нужно для этого проработать несколько тысячелетий.

Именно этот факт использует современная криптография. Уже несколько веков известна теорема из теории чисел: можно осуществить ряд манипуляций над числом n таким образом, что этот процесс будет обратим, только если известны множители p и q. Поэтому, если ваша приятельница Мария хочет отправить вам секретное сообщение, вам достаточно сообщить ей число n и описать, как его использовать для кодирования ее сообщения, представленного в виде большого целого числа. Она перешлет вам результат этого преобразования и теперь никто, кроме вас,

Рис. 23.1.

не сможет разобраться в зашифрованном сообщении, а вы, зная p и q, с легкостью его расшифруете.

Революционная особенность этого процесса в том, что он проходит, можно сказать, на глазах у широкой публики. Кто угодно может знать число n, процедуру кодирования, и закодированное сообщение. Поэтому говорят о *криптографии с открытым ключом*.

С математической точки зрения едва затронутая здесь процедура кодирования с использованием числа n основана на арифметике сравнения по модулю, описанной в предыдущей главе. Даже математиков удивляет, что теория сравнения используется миллионы раз каждый день для отправки зашифрованной информации, например, через Интернет.

ШИФРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМА RSA

Чтобы разобраться, что понимают под криптографией с открытым ключом, нужно познакомиться с некоторыми терминами и основными математическими фактами. В принципе, так называемый алгоритм RSA[1)] работает следующим образом.

Основные принципы. Основная идея заключается в том, чтобы использовать арифметику сравнения по модулю, описанную в гл. 22. Нужно, например, знать, почему равенство $211 \mod 100 = 11$ корректно[2)]. И если у вас есть компьютер, вы можете убедиться, что

$$265\,252\,859\,812\,191\,058\,636\,308\,480\,479\,023 \mod 1\,459\,001 = 897\,362.$$

Факты

В гл. 22 мы упомянули поразительный факт: если n — простое число, а k — целое число между 1 и $n - 1$, то

[1)]Эту процедуру в 1977 г. разработали трое ученых Rivest, Shamir и Adleman; первые буквы их фамилий дали название алгоритма.

[2)]Здесь запись $211 \mod 100 = 11$ — сокращение для высказывания «211 по модулю 100 равно 11». Далее мы будем использовать более компактную запись.

всегда выполняется соотношение

$$k^{n-1} \mod n = 1.$$

Математики называют это утверждение *малой теоремой Ферма*[1]. Если умножить обе части уравнения на k, то получим

$$k^n \mod n = k.$$

Мы не собираемся здесь доказывать этот результат, а лишь используем его в дальнейшем обсуждении.

В качестве иллюстрации приведем численный пример. Если $n = 7$ и $k = 3$, то $k^n = 3^7 = 2187$. И действительно,

$$2187 \mod 7 = 3.$$

Нам понадобится обобщение теоремы Ферма для чисел, которые могут не быть простыми; впервые оно было доказано математиком Леонардом Эйлером (1707–1783). Чтобы сформулировать этот результат, нужно знать, что означает термин «взаимно простые числа»: два числа m и n называются *взаимно простыми*, если единственное число, которое делит и m, и n, — это единица. Таким образом, числа 15 и 32 взаимно просты, а числа 15 и 12 — нет (ведь у них есть общий делитель 3).

Для положительного числа n определим функцию $\phi(n)$ (читается «фи от эн») — количество целых чисел между 1 и n (включительно), взаимно простых с n. Например, для $n = 22$ числа

$$1, 3, 5, 7, 9, 13, 15, 17, 19, 21$$

взаимно просты с 22, поэтому $\phi(22) = 10$.

Теперь мы можем сформулировать результат Эйлера.

Если числа k и n взаимно просты, то

$$k^{\phi(n)} \mod n = 1.$$

Для «проверки» возьмем $n = 22$ и $k = 13$. При этом

$$k^{\phi(n)} = 13^{10} = 137\,858\,491\,849,$$

а 137 858 491 849 по модулю 22 действительно равно 1.

[1] Большая теорема Ферма относится к гораздо более сложной задаче — выяснить, существует ли уравнение вида $a^n + b^n = c^n$ с нетривиальными целыми решениями для $n > 2$. См. гл. 89.

Тем, кто предпочитает примеры, в которых можно все вычисления провести в уме, советуем попробовать $n = 6$ и $k = 5$. Тогда $\phi(6) = 2$ и $5^2 \mod 6 = 1$.

Следует отметить, что малая теорема Ферма — частный случай теоремы Эйлера. То есть если p — простое число, то у него нет общих делителей ни с одним меньшим целым числом (это по определению и означает простоту p). Поэтому все целые числа $1, 2, \ldots, p-1$ взаимно просты с p, так что $\phi(p) = p - 1$; в этом случае теорема Эйлера превращается в малую теорему Ферма.

АЛГОРИТМ RSA

Для начала нам потребуется найти два больших простых числа p и q, а затем вычислить произведение $p \cdot q = n$ (напомним читателю, что «больших» означает с несколькими сотнями цифр). Нам потребуется еще два дополнительных числа k и l таких, что произведение $k \cdot l$ равно 1 по модулю $\phi(n)$. Единственные числа между 1 и n, которые не взаимно просты с n, это p и q, поскольку они просты, и поэтому $\phi(n) = (p-1) \cdot (q-1)$.

Например, в случае $p = 3$ и $q = 5$ мы получаем $n = 15$. Между 1 и 15 есть следующие взаимно простые с 15 числа:

$$1, 2, 4, 7, 8, 11, 13, 14,$$

т. е. их ровно $8 = (3-1) \cdot (5-1)$. Значит, $\phi(15) = 8$.

Мы закончили все приготовления. Числа p, q и l должны быть скрыты за семью замками, а числа n и k могут быть доступны для всех заинтересованных сторон. Теперь, если кто-либо захочет отправить сообщение, его сначала следует перевести в строку чисел (например, используя стандартный код ASCII). Затем строку делят на блоки, скажем по 50 цифр.

Теперь можно проводить кодирование. Предположим, Мария хочет отправить закодированное сообщение своему брату Ивану. Если блок представляет число m, то она должна вычислить $m^k \mod n$ (мы обозначим результат r). Она в состоянии сделать это, поскольку n и k известны всем. Мария выполняет вычисление для всех блоков и отправляет Ивану результат (числа r). Заметьте, все желающие могут прочесть передаваемую последовательность.

Декодирование осуществляется следующим образом. Иван открывает сейф, в котором хранил числа p, q и l, и вычисляет $r^l \mod n$. При этом $r^l = (m^k)^l = m^{kl}$, а произведение $k \cdot l$ равно 1 по модулю $\phi(n)$. Поэтому существует целое число s такое, что $k \cdot l = s \cdot \phi(n) + 1$. Тогда

$$r^l \mod n = m^{kl} \mod n = m^{s\phi(n)+1} \mod n = m \cdot (m^{\phi(n)})^s \mod n.$$

По теореме Эйлера можем заключить, что число $m^{\phi(n)}$ (поэтому и s-я степень этого числа) равно 1 по модулю n. Итак,

$$r^l \mod n = m \mod n = m,$$

где последнее равенство верно в силу выбора числа $m < n$. Итак, мы действительно можем восстановить m по публично переданному сообщению r.

Но это восстановление может выполнить только тот, кому известно значение $\phi(n)$, т. е. $(p-1) \cdot (q-1)$. Каждый, кто смог установить числа p и q по n, тоже сможет прочитать сообщение. По этой причине задача факторизации привлекла так много внимания в последние годы[1)].

Здесь мы рассмотрим конкретный пример с небольшими числами (в серьезных приложениях используются гораздо большие числа). Мы выбрали числа $p = 47$ и $q = 59$, и опубликовали произведение $n = 47 \cdot 59 = 2773$. Теперь нужно выбрать числа k и l. Мы возьмем $k = 17$ и $l = 157$. Поскольку $\phi(n)$ равно $46 \cdot 58 = 2668$, а $17 \cdot 157 = 2669$ и поэтому равно 1 по модулю $\phi(n)$, наш выбор вполне удовлетворителен. Числа 2773 и 17 обнародованы, но 47, 59 и 157 сохраняются в полном секрете.

Наступает этап кодирования. Предположим, что сообщение превращено в число 1115. Мария заставляет компьютер вычислить для нее значение $1115^{17} \mod 2773$; результат равен 1379. Она пишет это число на открытке, и на следующий день эта открытка уже в почтовом ящике Ивана. Его компьютер вычисляет для него $1379^{157} \mod 2773$. Несколько миллисекунд — и результат готов: 1115. Если заклятой подруге Марии, зловредной Марго, удастся секретно скопировать содержание открытки, она все равно не сможет его расшифровать.

[1)] См., например, гл. 43.

Глава 24

ВОЛШЕБНАЯ МАТЕМАТИКА: ПОРЯДОК СРЕДИ ХАОСА

«Порядок среди хаоса» — подходящий девиз для математического волшебного фокуса, о котором я хочу рассказать в этой главе. Вам потребуется колода игральных карт, в которой красных и черных карт поровну. Стандартная колода в 52 листа вполне подойдет. Для начала вы должны расположить карты так, чтобы цвета чередовались, как показано на рис. 24.1.

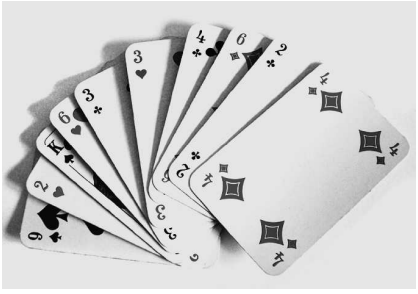


Рис. 24.1. Так нужно приготовить карты

А теперь мы позволим случаю трижды вмешаться в это расположение карт. На первом шаге кто-то снимает колоду приблизительно посредине. На втором шаге кто-то другой стасовывает обе половины вместе. Иногда в кино показывают, как это делают профессиональные игроки; они держат в каждой руке по половине колоды и постепенно отпускают и пролистывают концы карт обеих пачек так, чтобы они перемешивались, чередуясь между собой. И наконец, третий участник делит получившуюся колоду на две части так, чтобы разделенными оказались две карты одного цвета (рис. 24.2).

Части кладут одна на другую и отдают вам. Наивный человек подумал бы, что эти три случайных процесса приводят к хаотичной смеси карт, смешанных совершенно случайно. На первый взгляд так и кажется. Однако имеет

Рис. 24.2. ...сдвиньте, сложите, сдвиньте еще раз...

место замечательное явление. Оказывается, что карты 1 и 2 разного цвета, карты 3 и 4 — тоже, и карты 5 и 6, и т. д. Теперь вы можете как настоящий волшебник положить колоду карт под покрывало, пробормотать мистические заклинания а затем вынуть пары карт разных цветов словно по волшебству, хотя на самом деле нужно брать их по порядку сверху вниз (рис. 24.3).

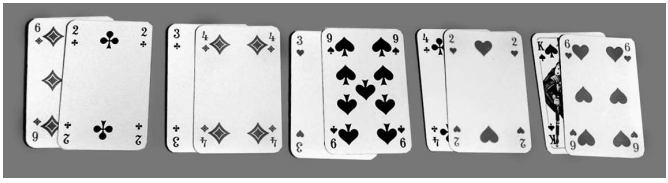


Рис. 24.3. ...и разложите попарно

У этого фокуса интересная математическая подоплека. Комбинаторными методами можно доказать, что после описанных трех случайных манипуляций карты будут расположены парами разноцветных карт, и это свойство математики называют *инвариантом* относительно произведенных манипуляций. Похоже, что фокусник Джилбрейт, который изобрел этот трюк в начале предыдущего столетия, сделал это методом проб и ошибок.

ВАРИАНТ ФОКУСА

Для тех, кто хочет добавить этот фокус в свой репертуар, опишем еще одну его разновидность. Напомним, что в оригинале процесс идет так.

- Приготовьте колоду карт (четное число карт двух чередующихся цветов).
- Снимите колоду и стасуйте обе части вместе.

- Снимите колоду в том месте, где есть две карты одного цвета и поменяйте обе части местами.

Тогда карты в каждой паре (карты 1 и 2, 3 и 4, 5 и 6 и т. д.) будут разных цветов.

А теперь разновидность. Приготовьте колоду карт так же, как в первом случае, и тоже снимите ее. Предупреждение: в этот раз нужно как-то выяснить, одного цвета нижние карты в каждой половине или разного. Это можно сделать, передавая карты для тасования. Следующий шаг тоже сохраняется: обе половины нужно стасовать вместе. Только в этот раз не нужно снимать колоду повторно.

Преимущество перед первым вариантом в том, что не нужно просить кого-то смотреть и снимать колоду в нужном месте — где соседствуют две карты одного цвета. Тогда никому и в голову не придет, что черные и красные карты распределены более регулярно, чем в случае хорошо стасованной колоды карт.

Может осуществиться один из двух случаев. В первом случае две нижние карты разных цветов, никаких поправок при этом не требуется, карты уже расположены как надо: в каждой паре они разного цвета. Во втором случае две нижние карты обе красные или обе черные. Все становится несколько сложнее. Пока вы произносите заклинания, передвиньте верхнюю карту вниз колоды. Тогда все равно все пары будут состоять из карт разных цветов. Конечно же, вы не обязаны перекладывать верхнюю карту вниз. Вместо этого можете составить первую пару из верхней и нижней карт, а затем действовать как раньше. Удачи в магии!

А где же математика? Она гарантирует, что трюк всегда работает. Можно *доказать*, что расположение карт будет таким, как предсказано. Однако для этого потребовалась бы довольно сложная теория, выходящая за рамки нашей книги.

Дополнение для третьего издания: лица, заинтересованные в теме «фокусы с математической подоплекой», главным образом читатели английского издания могут посетить сайт www.mathematics-in-europe.eu, который был создан автором этой книги. Там представлено большое разнообразие математических фокусов.

Глава 25

КАК ВСТУПИТЬ В КОНТАКТ С ГЕНИЕМ

Как распознать исключительное явление? Многие считают Карла Фридриха Гаусса (1777–1855) величайшим математиком из всех, когда-либо живших на Земле. До введения евро на банкноте достоинством в 10 марок был его портрет, а также графическое изображение некоторых его достижений. Например, на этой банкноте можно видеть знаменитую колоколообразную кривую — указание на вклад Гаусса в теорию вероятностей.

Вряд ли найдется хоть один математик, который с полной уверенностью может утверждать, что он вполне осознает феномен Гаусса. Его публикации установили стандарт математических исследований на десятилетия, а ведь от публикации многих своих результатов он отказался. Отчасти он сделал это, поскольку полагал, что современники не готовы воспринять их, а отчасти в силу того, что считал некоторые из своих открытий, сегодня рассматриваемые как прорыв, недостаточно интересными.

Так, например, он полагал (совершенно справедливо), что для неевклидовой геометрии время еще не пришло. Математики (и философы, такие как Кант) на протяжении тысячелетий были уверены, что возможен только один вид геометрии, а именно тот, который построил Евклид за две

Рис. 25.1. Гора Брокен в Гарце

с половиной тысячи лет до того, — геометрии, где сумма углов треугольника равна 180°, а для каждой прямой через точку, ей не принадлежащую, можно провести только одну параллельную прямую.

Гаусс, однако, понимал, что евклидова геометрия — только одна из многих возможных геометрий. В 1821 г., измеряя углы большого треугольника, он экспериментально проверял, что в нашем мире выполняется именно евклидова геометрия, по крайней мере в рамках допустимой экспериментальной погрешности. Вершинами треугольника, углы которого он измерял, были три горных пика: Брокен в Гарце (рис. 25.1), Инсельсберг в Тюрингии и Высокий Хаген неподалеку от Гёттингена.

И только годы спустя стало общепризнано, что для описания природы могут быть использованы неевклидовы геометрии, как, например, в общей теории относительности[1)].

Было бы несправедливо по отношению к Гауссу рассматривать его только как математика. Ничуть не менее он известен своими достижениями в физике (по магнетизму) и в астрономии, где он применял совершенно новые математические методы для вычисления небесных орбит. Он предсказал положение астероида Церера, и это сделало его имя знаменитым в круге профессиональных астрономов еще в молодости.

[1)] О неевклидовых геометриях подробнее написано в гл. 80.

Сегодня величие Гаусса продолжает подтверждаться, благодаря упоминанию его имени в связи с важными научными событиями. Не так давно одна из наиболее престижных в мире математических наград была названа в его честь; а самое важное событие в немецком математическом сообществе — это, конечное же, гауссовская лекция, которая проходит каждый семестр в разных университетах.

СЕМНАДЦАТИУГОЛЬНИК

В нежном восемнадцатилетнем возрасте Гаусс открыл удивительную связь между теорией чисел и геометрией. Речь идет о построении многоугольников, у которых все углы равны[1)]. По определению такие построения должны проводиться только при помощи циркуля и линейки.

Те, кто изучал геометрию в старших классах, может быть, помнят, что такое построение осуществить несложно, когда число сторон n равно 3. Чтобы построить равносторонний треугольник, нужно провести отрезок, установить раствор циркуля равным этом отрезку, и начертить две окружности с центрами в концах проведенного отрезка. Любая из двух точек пересечения этих двух окружностей может быть выбрана в качестве третьей вершины треугольника. Случай $n = 4$, т. е. квадрат, тоже не сложен, ведь имеется простая процедура построения прямого угла. А что происходит для других значений n?

Еще в античности было известно, что с помощью циркуля и линейки можно построить правильный пятиугольник ($n = 5$) и шестиугольник ($n = 6$). Можно ли сделать вывод, что можно построить любой многоугольник? Нет! Благодаря Гауссу сегодня точно известны значения n, для которых такое построение циркулем и линейкой возможно. Чтобы найти их, начинают с простых чисел, представимых в виде степени двойки, увеличенной на 1. Такие простые числа называются *простыми числами Ферма*. Наибольшее такое простое число, известное на сегодняшний день, равно 65 637; есть и другие примеры: $5 = 2^2 + 1$ и $17 = 2^4 + 1$. Если n — простое число Ферма или произведение двух

[1)] Математики называют такие многоугольники *правильными*.

различных таких простых чисел (оно может быть еще умножено на произвольную степень 2), то соответствующий правильный n-угольник построить можно. А для других значений n этого сделать нельзя. Например, число 7 нельзя записать в виде $2^k + 1$, значит, оно не является простым числом Ферма, и поэтому правильный семиугольник циркулем и линейкой построить нельзя. (Конечно, такой многоугольник можно построить приблизительно, но эта задача неинтересна с математической точки зрения.)

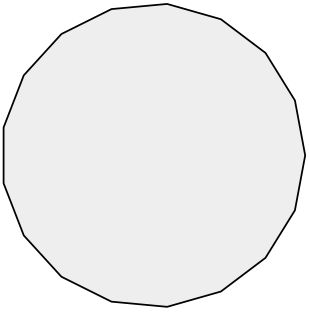


Рис. 25.2. 17-угольник

ПРЕВЗОЙТИ УЧИТЕЛЯ

До наших дней дошло много рассказов о великих личностях, и Гаусс не стал исключением. Такие истории ярко описывают его характер, даже если они и не вполне правдивые или вовсе апокрифические.

Один из самых известных анекдотов (рассказываю его в надежде, что хотя бы некоторые читатели с ним еще не знакомы): через несколько недель обучения в первом классе учителю Гаусса понадобилось занять класс, и он велел детям сложить первые сто натуральных чисел, т. е. вычислить сумму $1 + 2 + \cdots + 100$.

Через минуту Гаусс сказал учителю, что закончил, и объявил правильный ответ 5050. Вместо того чтобы, как все остальные школьники, уныло складывать все подряд, Гаусс перегруппировал слагаемые: вместо $1 + 2 + \cdots + 100$

он вычислял сумму

$$(1 + 100) + (2 + 99) + \cdots + (50 + 51).$$

Преимущество очевидно, ведь все слагаемые в скобках равны 101. Остается только умножить 101 на число слагаемых (т. е. 50), и с легкостью получить результат $50 \cdot 101 = 5050$.

Как и в других областях математики, да и реальной жизни тоже, этот пример показывает, что часто именно подход к задаче определяет, простая она или сложная.

Глава 26

О ПОЛУТОНАХ И КОРНЯХ ДВЕНАДЦАТОЙ СТЕПЕНИ

Существует устойчивое поверье, будто бы математиков особенно привлекает музыка. Однако оно утвердилось не во время опроса математиков на одной из последних конференций, что наводит на мысль о том, что математики не более склонны к музыке, чем, скажем, доктора или адвокаты. Все же тесная связь между этими двумя областями — математикой и музыкой — есть.

Более 2500 лет назад Пифагор знал, что две ноты, сыгранные одновременно на натянутых струнах, особенно приятно звучат, когда длины струн подчиняются простым математическим соотношениям. Например, если одна струна вдвое длиннее другой (и они сделаны из одного материала и натянуты одинаково), то короткая струна звучит ровно на октаву выше длинной (и как теперь знаем мы, частота высокого тона — число колебаний в секунду — вдвое выше, чем низкого). Для квинты отношение равно 2 к 3. Пифагорейцы построили на этом принципе всю музыкальную гамму, но для нас осталось неизвестным, что привело к обнаруживаемой во всех культурах связи между простыми математическими соотношениями и прелестью музыки.

К сожалению, пифагорейская гамма и связанные с ней музыкальные системы обладают одним решительным недостатком: когда мы переходим из одной тональности в другую, математические соотношения в новой гамме несколько отличаются от соотношений в старой.

Из этого недостатка родилась идея демократично разделить октаву на 12 частей. От одного полутона до соседнего частота увеличивается в $\sqrt[12]{2}$ раз, т. е. приблизительно в 1,059 463 094...раз. Примерно триста лет тому назад был изобретен равномерно темперированный строй. В своем произведении «Хорошо темперированный клавир» Иоганн Себастьян Бах (1685–1750) представил собрание пьес

(прелюдий и фуг), написанных в 24 мажорных и минорных тональностях. Он таким образом продемонстрировал, что можно играть в любой тональности, не перенастраивая инструмент.

Это изобретение ни в коей мере не исчерпало возможных связей между математикой и музыкой. В двадцатом веке многие композиторы использовали различные математические соотношения в своих сочинениях, начиная с метода настраивания и заканчивая большими формами. Например, композитор Янис Ксенакис (1922–2001) использовал вероятностные методы, теорию игр и теорию групп в качестве организационных принципов своих сочинений.

Однако какое высокое значение мы бы ни придавали математике, невозможно выразить математическими формулами нашу радость от сонат Шуберта или любимой популярной песенки.

ПИФАГОРОВА ИЛИ ХРОМАТИЧЕСКАЯ

Почему в нашем обсуждении возник корень двенадцатой степени из 2? Предположим, что октаву нужно разделить на n частей, где n — целое положительное число. Гитарному мастеру придется расположить n ладовых порожков на одной половине грифа, причем последний порожек окажется ровно посредине, чтобы дать звук на октаву выше (рис. 26.1). Если все музыкальные интервалы будут одного размера, то отношение частот звуков, издаваемых свободной струной и прижатой у первого порожка, должно быть таким же, как у звуков, издаваемых струной, прижатой у первого и второго порожков, и т. д.

Если это отношение обозначить x, то его можно вычислить прямо. Если одновременно (скажем, на двух одинаково настроенных гитарах) звучат две ноты, разделенные k полутонами, то отношение их частот равно x^k. В частности, n-я нота, звучащая на октаву выше, должна иметь частоту вдвое больше, поэтому выполняется уравнение $x^n = 2$. При равномерно темперированном строе $n = 12$, и поэтому $x^{12} = 2$ или $x = \sqrt[12]{2} = 1{,}059\ldots$. Таким образом, у нот C и C-диез отношение частот равно $1{,}059\ldots$, то же самое можно сказать о нотах C-диез и D, и т. д. Можно вычислить

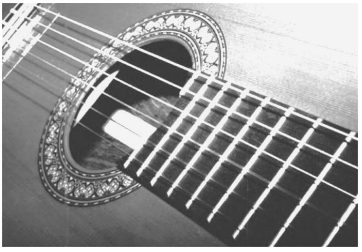



Рис. 26.1. Одинаково настроенные инструменты

отношение частот между любой парой нот. Например, для D и C оно равно

$$\mathrm{D} : \mathrm{C} = \mathrm{D} : \mathrm{C}^{\#} \times \mathrm{C}^{\#} : \mathrm{C} = 1{,}0594 \cdot 1{,}0594 \ldots = 1{,}12246 \ldots .$$

Следующая таблица показывает отношение частот для пифагоровой и равномерно темперированной гаммы до-мажор.

Нота	Пифагорава гамма	Равномерно темперированная гамма
C	1	1
D	1,12500	1,12246
E	1,26563	1,25992
F	1,33333	1,33484
G	1,50000	1,49831
A	1,68750	1,68179
B	1,89844	1,88775
C	2	2

Отношения частот практически совпадают, и нетренированное ухо вряд ли заметит разницу. В популярной музыке равномерное темперирование почти универсально, но когда музыку исполняют на старинных инструментах, музыканты часто стараются добиться такого же звучания, которое было во время сочинения произведения.

Глава 27

ВЕЧНО Я НЕ В ТОЙ ОЧЕРЕДИ!

Тема этой статьи — опять психология. Вам никогда не приходила в голову мысль, что другие очереди в супермаркете или на почте всегда продвигаются быстрее, чем та, в которой стоите вы? Может быть, вам станет легче, если вы узнаете, что другие думают точно так же, и причину мы вам сейчас объясним.

Представьте себе пять очередей на почте примерно одной длины; вам нужно выбрать одну из них. Вероятность того, что вы выберете ту, что будет продвигаться быстрее остальных, равна $\frac{1}{5}$ или 20%. Иначе говоря, с вероятностью 80% вы снова окажетесь в неправильной очереди. А если вы часто оказываетесь в такой ситуации, то неизбежно возникнет впечатление, что судьба несправедлива к вам.

Наши ожидания и действительность и впрямь часто расходятся из-за недостаточно развитой математической интуиции. Такой недостаток мы получили в ходе эволюции, и об этом часто идет речь в нашей книге. Например, нелегко осознать экспоненциальный рост, да и правильное интуитивное решение парадокса Монти Холла (гл. 14) для многих людей почти невозможно.

К задаче, упомянутой в начале этой главы, мы должны добавить, что ожидание в очередях подвергалось серьезным исследованиям в течение долгого времени: теория очередей (или теория массового обслуживания) — один из классических разделов теории вероятностей.

У теории очередей много приложений. Как только задача очередей совершенно изучена, это знание можно приложить

к таким разным ситуациям, как оптимальное планирование работы светофоров и передача пакетов данных до узловой точки в интернет-соединении.

ОЧЕРЕДИ

Как мы уже сказали, теория очередей — ветвь теории вероятностей. Ее типичные результаты приложимы к бизнесу. Представьте себе предприятие по обслуживанию населения. Клиентов принимают, обслуживают, и они уходят. Это может быть ресторан, металлоремонт — да что угодно. В эту же схему укладываются музей или туристический аттракцион.

Мы принимаем следующие предположения.

Клиенты прибывают в случайные моменты времени по одному. Слово «случайные» означает, что нельзя точно предсказать, когда прибудет следующий клиент, известен только средний интервал между прибытиями. (Для этого есть научный термин *экспоненциально распределенные моменты поступления*.) Считается, что клиенты не ходят группами[1)]. Однако нам известно время ожидания: *в среднем* один клиент прибывает каждые K секунд.

Когда клиент входит «в лавку», он обслуживается немедленно (служащих достаточно). Время обслуживания, как и моменты поступления, не могут быть предсказаны наверняка, однако известно ожидаемое значение, которое мы обозначим L — среднее число секунд, требующихся на обслуживание одного клиента.

В зависимости от ситуации эти условия более или менее точно отражают действительность. Они вполне подходят для крупного ресторана с большим штатом и достаточным количеством свободных столиков. И для исторического собора, посещаемого туристами, эти условия тоже выполняются.

Параметры K и L независимы, они определяются ситуацией. Малое значение K для собора означает, что его посещает много народа, а большое — что посетителей мало, они заходят только изредка. Параметр L служит

[1)] Это накладывает ограничение на наш пример с туристами, так что придется предположить, что все они путешествуют поодиночке.

мерой привлекательности. При малых L турист не тратит много времени на осматривание собора, а большие значения говорят о длительных посещениях (вспомните о базилике Святого Петра в Ватикане).

Задача в том, чтобы предсказать число клиентов в любой момент времени. Качественно ситуация ясна: большие K и малые L говорят о том, что в среднем в любой момент времени клиентов будет мало. Однако мы хотим знать точнее, чего ожидать: сколько диванов для клиентов разместить в предприятии металлоремонта? Сколько официантов нанять? Ответы на эти вопросы позволяет дать теория вероятностей.

Обозначим λ отношение L/K — столько клиентов в среднем находится в лавке в любой момент времени. Вероятность того, что в любой момент присутствует ровно k клиентов, задается формулой

$$\frac{\lambda^k}{k!}\,e^{-\lambda},$$

где $k!$ (читается «k факториал») обозначает произведение $1 \cdot 2 \cdots k$, а $e = 2{,}718\ldots$ — постоянная Эйлера, основание натуральных логарифмов[1)].

Например, $K = 60$ и $L = 120$. Это означает, что в среднем каждые 60 секунд приходит клиент и задерживается в среднем на 2 минуты. Здесь $\lambda = 2$, и можно вычислить вероятность того, что в любой момент времени в лавке будет ровно k клиентов. Некоторые значения мы приведем в таблице.

k	0	1	2	3	4	5
Вероятность	0,135	0,271	0,271	0,180	0,090	0,036

Так что если на предприятии металлоремонта есть четыре места для сидения, то стоящего клиента там можно будет увидеть очень редко: вероятность того, что клиентов не более четырех, равна $0{,}135 + 0{,}271 + 0{,}271 + 0{,}180 + 0{,}090 = 0{,}947$, а вероятность того, что их пять или больше, равна $1 - 0{,}947 = 0{,}053$, лишь несколько выше 5%.

[1)] Подробнее о ней можно прочитать в гл. 42.

Глава 28

НЕЗАСЛУЖЕННО НЕДООЦЕНЕННОЕ ЧИСЛО

Числа — это абстракции. У множества пяти груш и множества пяти яблок есть одно общее свойство, которое можно обнаружить и у других множеств: оказалось очень полезно ввести для него специальный символ. Такие абстракции возникают во всех человеческих культурах, и даже малыши могут работать с такими небольшими числами.

А что можно сказать про число ноль? Нет ничего особенного в том, что в некоторых множествах нет элементов; однако прошло несколько сотен лет, пока не возникла идея о пользе понятия и символа *ноль*. Например, в римской нумерации нуля не было, и на самом деле она совершенно не подходит для проведения арифметических операций. И только с введением нуля и позиционной системы счисления записывать большие числа стало просто и выполнять арифметические действия стало удобно.

Тот, кто выучил таблицу умножения и умеет складывать однозначные числа, может без труда справиться со всеми арифметическими операциями. Здесь у нуля важнейшая роль. Например, в записи числа 702 он использован для обозначения того факта, что в этом числе нет десятков (только 7 сотен и 2 единицы). И чем больше нулей в конце числа, тем большие значения выражают цифры перед ними: единица в числе 1000 значит больше, чем в числе 10.

Вначале в индийской позиционной системе вместо нуля был только специальный значок, свидетельствующий о том, что в этом месте ничего не записано. (Получалось меньше ошибок, чем если бы совсем ничего не было отмечено.) Роберт Каплан в книге «История нуля» [1)], которая читается на одном дыхании, пишет, что в то время в Индии ноль «был не цифрой — не более чем точкой или запятой». И только в начале шестнадцатого столетия ноль стал полноправным числом.

[1)] Die Geschichte der Null, Campus Verlag, 2000.

Для математиков роль нуля простирается гораздо дальше, за пределы участия в записи чисел. Действительно, ноль — одно из самых важных чисел. Ведь если прибавить его к какому-нибудь другому числу, оно не изменится, поэтому ноль называют *нейтральным элементом* или *единицей по сложению*. В мире чисел он находится в центре, как точка равновесия между положительными и отрицательными числами.

Даже сейчас роль нуля не выявлена вполне точно. В 2100 году задолго до Рождества начнется оживленный спор о том, когда именно начинается двадцать второй век. Ответ на этот вопрос зависит от того, как принято отсчитывать годы — начиная с 0 или с 1.

ПОИСК ВЕЛИКОГО НЕИЗВЕСТНОГО

Чтобы продемонстрировать, как используются свойства нуля при вычислениях, рассмотрим простую задачу сложения. Мы не будем выходить за рамки множества целых чисел, т. е. чисел

$$\ldots, -2, -1, 0, 1, 2, 3, \ldots.$$

Во-первых, нужно убедиться, что, как мы уже сказали, сложение с нулем не меняет число. Вне зависимости от значения y всегда выполняется соотношение $y + 0 = y$. Во-вторых, мы всегда можем «вернуться обратно к нулю». Это означает, что для любого числа y всегда можно найти такое число w, что $y + w = 0$. Например, можно выбрать $w = -5$, если дано $y = 5$, а для $y = -13$ нужно взять $w = 13$.

Обычно мы используем обозначение «$-y$» для числа w и называем число w *обратным по сложению* числу y. Отметьте, что мы уже выяснили, что $-(-13) = 13$. Это подтверждает правило «минус на минус дает плюс».

Теперь мы готовы решать алгебраические уравнения. Предположим, нужно найти число x такое, что выполняется равенство

$$x + 13 = 4299.$$

Неизвестное число x можно найти так: просто добавить число -13, обратное по сложению числу 13, к обеим сторонам уравнения. Исходное уравнение преобразуется

следующим образом:

$$(x + 13) + (-13) = 4299 + (-13).$$

Левую часть преобразуем к виду $x + (13 + (-13))$; это можно сделать в силу ассоциативности сложения[1)]. Сумму $(13 + (-13))$ можно заменить нулем (именно для этого мы и прибавляли число, обратное по сложению), а вместо $x + 0$ записать просто x (ведь 0 — единица по сложению). Итак, мы получили уравнение $x = 4299 + (-13)$, которое можно записать в более привычном виде $x = 4299 - 13$. Нам осталось воспользоваться математикой на уровне начальной школы, чтобы убедиться, что x равен 4286.

Может показаться, что эти рассуждения слишком сложны для такого незамысловатого результата. Даже математики просто вычитают 13 из обеих частей уравнения $x + 13 = 4299$. Однако мы показали таким образом решающую роль нуля: именно его свойства позволяют решать такие уравнения.

[1)] См. гл. 20.

Глава 29
Я ЛЮБЛЮ СЧИТАТЬ!

Комбинаторика — почтенная и старинная ветвь математики, играющая важную роль во многих ее областях. Первоначальная задача комбинаторики — подсчитывать число способов, которыми что-либо может осуществиться или быть сгруппировано, причем обычно речь идет о больших числах. Например, сколькими способами вы можете выбрать шесть чисел из сорока девяти в ближайшем лотерейном розыгрыше?

Представьте себе барабан и в нем 49 шаров, пронумерованных числами от 1 до 49 и хорошенько перемешанных. Вы 6 раз опускаете туда руку и вынимаете шар — это и есть ваши лотерейные номера.

Сколько же здесь возможностей? В первый раз их сорок девять, но во второй уже только сорок восемь, потом сорок семь и т. д. Всего имеется $49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44 = 10\,068\,347\,520$ способов вынуть шесть шаров. Но постойте! Все эти возможности не приводят к разным наборам. Если шесть шаров вынуты, то есть и другие способы вынуть те же шары, возможно, выбранные в другом порядке. Например, последовательность 2, 3, 34, 23, 13, 19 приводит к тому же набору, что и последовательность 23, 2, 34, 3, 13, 19. Шесть шаров можно вынуть $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$ различными способами; а именно, для первого шара есть шесть возможностей, для второго — пять, и т. д. Поэтому мы найдем истинное число различных способов выбрать числа для лотереи, разделив $10\,068\,347\,520$ на 720, что дает $13\,983\,816$ — именно это число мы встречали в гл. 1.

Если вы умеете считать, вы можете вычислять вероятности. Поскольку только один из $13\,983\,816$ возможных способов выбрать лотерейные номера даст большой выигрыш, вероятность угадать эти выигрышные номера равна $1/13\,983\,816$, — увы, она обескураживающе мала.

ЧЕТЫРЕ ОСНОВНЫЕ ЗАДАЧИ ПОДСЧЕТА

Подсчитывая, мы всегда рассматриваем количество некоторых способов выбора: всегда выбираем k элементов из n. Прежде чем двигаться дальше, нужно ответить на два ключевых вопроса: 1) важен ли порядок, в котором выбираются элементы; 2) можно ли один и тот же элемент выбрать более одного раза?

Существует по два ответа на каждый из этих двух вопросов, поэтому нужно различать четыре случая.

Случай 1. Порядок важен, допустим многократный выбор

Для примера подумаем, сколько всего четырехбуквеных «слов» (здесь словами мы называем любые сочетания букв, включая бессмысленные, такие как ЫЙЬЪ). Порядок букв важен, так как ДАНЯ вовсе не то же самое, что НАДЯ, а повторы допустимы, ведь мы не исключаем таких слов, как АЛЛА или ЛИЛЯ.

Число всех таких слов подсчитать несложно. Для каждой из k букв есть n возможностей, итого $n \cdot n \cdots n = n^k$. Поскольку в алфавите $n = 33$ буквы, а в словах, которые мы рассматриваем, $k = 4$ буквы, всего имеется

$$33^4 = 1\,185\,921$$

четырехбуквенных слов.

Рассмотрим еще один пример. Если мы будем выбирать четыре цифры из набора 0, 1, ..., 9, то получим четырехзначное число[1)]. Очевидно, что порядок имеет значение и что одна и та же цифра может повторяться несколько раз. В этом случае $n = 10$ и $k = 4$, так что всего имеется $10^4 = 10\,000$ возможностей. (Мы получили число различных пин-кодов для банковских карточек. Оно не такое уж большое, если учесть, как много людей пользуется банкоматами. Возможно, в вашем городе есть

[1)] Конечно же, если первая выбранная цифра оказалась нулем, то мы получим числа вроде 0233 или 0003. Мы можем либо договориться рассматривать и такие числа тоже, или подсчитывать количество целых чисел, в которых четыре или *меньше* цифр.

человек, пин-код банковской карточки которого совпадает с вашим[1]).)

У этой задачи есть важный вариант — когда на различных этапах выбора возникают разные множества. Например, сколькими способами можно заказать обед в ресторане, если предлагается 5 закусок, 7 блюд и 3 десерта? Чтобы получить ответ, достаточно просто составить произведение $5 \cdot 7 \cdot 3 = 105$. Доказательство то же, что в предыдущем примере.

Случай 2. Порядок важен, многократный выбор не разрешается

Типичный пример такой задачи (при $n = 20$ и $k = 11$) — выбор членов футбольной команды из двадцати студентов в группе.

Порядок выбора здесь важен, ведь если вратарь поменяется местами с нападающим, команда получится совсем другой. И ясно, что многократный выбор запрещен — один и тот же человек не может быть одновременно вратарем и нападающим.

Аналогичная задача возникает при выборе правления клуба: президента, вице-президента, секретаря, казначея. Порядок, конечно же, важен. Когда Мария — президент, а Иван — секретарь, это вовсе не то же самое, когда Иван — президент, а Мария — секретарь. И снова один человек не может занимать более одной должности, так что многократный выбор не разрешается.

В этом случае вычисления не сложные. Первый элемент мы можем выбрать n способами, второй — $(n-1)$ способами (поскольку первый элемент уже не участвует в выборах), третий — $(n-2)$ способами, и т. д., пока не будут выбраны все k элементов. Общее число возможностей равно произведению числа возможных способов на каждом шаге, т. е. числу

$$n \cdot (n-1) \cdots (n-k+1).$$

[1]) Строгое доказательство того, что обязательно найдутся люди с одинаковыми пин-кодами, основывается на *принципе Дирихле*, который мы обсудим в гл. 62.

Обратите внимание, что последний множитель свидетельствует о том, что в произведение входит k множителей.

Эта формула означает, что футбольную команду можно выбрать

$$20 \cdot 19 \cdots (20 - 11 + 1) = 20 \cdot 19 \cdots 10 = 6\,704\,425\,728\,000$$

способами.

И если есть восемь кандидатов в члены правления клуба, то выбрать правление возможно всего

$$8 \cdot 7 \cdot 6 \cdot 5 = 1680$$

способами.

Случай 3. Порядок не важен, многократный выбор не разрешается

Эта ситуация возникает чаще всего, и на самом деле она уже нам встречалась, когда мы обсуждали частный случай выбора шести чисел из сорока девяти. Есть и другие примеры.

- Сколько существует раскладов в преферансе (10 карт из 32)?
- Сколько рукопожатий случится, если все n участников встречи пожмут друг другу руки? Это число равно числу способов выбрать двух человек из n. В этом случае $k = 2$.
- У вас есть $n = 8$ книг и вы хотите взять $k = 4$ из них с собой в отпуск. Сколькими способами можно это сделать?

Мы уже нашли решение этой задачи, обсуждая лотерею в этой главе, и общая формула выглядит так:

$$\frac{n \cdot (n-1) \cdots (n-k+1)}{1 \cdot 2 \cdots k}.$$

Это выражение так часто встречается в математике, что для него ввели специальное обозначение:

$$C_n^k = \frac{n \cdot (n-1) \cdots (n-k+1)}{1 \cdot 2 \cdots k}.$$

Это символ читается «Це из эн по ка» и называется *биномиальным коэффициентом*.

Теперь мы можем провести вычисления из наших примеров: существует 64 512 240 раскладов в преферансе, а двадцать человек при встрече обмениваются $C_{20}^2 = \frac{20 \cdot 19}{1 \cdot 2} = 190$ рукопожатиями.

Случай 4. Порядок не важен, многократный выбор разрешается

Это довольно редкий случай. Представьте себе, что нужно распределить k шаров по n ящикам (см. рис. 29.1). Выбрать одно из n чисел — значит, решить, в какой ящик поместить очередной шар. В любом ящике может оказаться более одного шара, это и означает, что разрешается многократный выбор. И не имеет значения, поместили вначале один шар во второй ящик, а затем другой — в четвертый ящик, или сделали это в обратном порядке. Найти число таких способов не так просто. Ответ получается такой:

$$C_{n+k-1}^k.$$

Поэтому есть

$$C_{5+2-1}^2 = C_6^2 = \frac{6 \cdot 5}{1 \cdot 2} = 15$$

способов распределить два шара по пяти ящикам; а шесть шаров по десяти ящикам можно разложить

$$C_{10+6-1}^6 = C_{15}^6 = \frac{15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10}{6!} = 5005$$

различными способами.

И наконец, нужно отметить, что эта задача, которая на первый взгляд кажется чисто академической, очень важна в приложениях, например в физике элементарных частиц, когда нужно найти число способов, которыми можно распределить k электронов по n оболочкам.

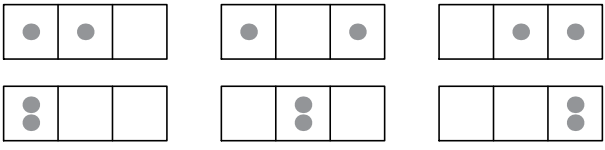


Рис. 29.1. Два шара в трех ящиках: $C_{3+2-1}^2 = C_4^2 = 6$ способов

Глава 30

ГЕНИЙ-САМОУЧКА. ИНДИЙСКИЙ МАТЕМАТИК РАМАНУДЖАН

Существует ли прямой путь к математической истине? Путь, ведущий к озарению без утомительного освоения техники и подробной проработки доказательств? По-видимому, в исключительных случаях это возможно, и судьба Шриниваса Рамануджана (1887–1920) тому пример. Мы сейчас расскажем о его драматичной истории.

Рис. 30.1. Ш. Рамануджан и Г. Х. Харди

Рамануджан вырос в бедной южной Индии. Основы математики он освоил самостоятельно, разбираясь с формулами, попадавшими ему на глаза. Без чьей-либо помощи он обнаружил замечательные соотношения в теории чисел: некоторые из них были известны европейским ученым, но большинство были новыми. У него не было университетского образования, и поэтому он не мог занять должность, соответствующую его способностям. Но все же ему удалось пробиться, и каждую свободную минуту, пока не был побежден физическим и умственным истощением, он посвящал поиску математической истины.

Только ряд счастливых совпадений привел к тому, что Рамандужан оказался в Кембриджском университете.

Он начал переписываться с некоторыми европейскими математиками, и один из них рассмотрел глубокие истины на исписанных формулами страницах. В Кембридже Рамандужан провел несколько чрезвычайно продуктивных лет, работая с ведущими специалистами. Но в силу чрезмерной нагрузки, неприспособленности к климату и других обстоятельств он заболел и в 1919 году вернулся в Индию, где на следующий год умер.

Каким чудесным образом Рамануджан подходил к истине, навсегда осталось загадкой, но история его жизни замечательна по другим причинам. Например, можно представить себе, сколько рамануджанов так и остались безвестными, поскольку их образование зависело от места рождения.

В НАШЕ ВРЕМЯ РАМАНУДЖАНУ ПОВЕЗЛО БЫ БОЛЬШЕ?

Для истории математики было удачей, что английский математик Г. Х. Харди (1877–1947) признал гения в авторе робкого письма из Индии. Письма от Рамануджана получали и другие выдающиеся математики, но не потрудились их внимательно прочитать.

То же самое вполне могло бы случиться и сегодня. Университетские математики нередко получают письма или электронные сообщения о суперактуальных открытиях, которые на поверку оказываются ошибочными или давно известными. Особенно популярны новые «доказательства» знаменитой последней теоремы Ферма, квадратуры круга и гипотезы Гольдбаха[1)]. И каждый раз, неизменно, в них встречаются элементарные ошибки. Однако ошибка может быть хорошо спрятана, и всегда требуется затратить время и энергию, для того чтобы убедить автора, что его доказательство не безупречно. А если просто отказаться отвечать, то поднимается шквал брани: «Отныне Вы лично и Ваш университет получаете черную метку за то, что у Вас нет ни способности, ни желания признать значение этой важной работы». Поэтому многие учреждения, например Académie Francaise, приняли стратегию просто игнорировать такие письма.

[1)] См. гл. 89, 33 и 49.

Однако на более простом, чем «Ферма—Квадратура—Гольдбах», уровне от непрофессионалов иногда исходят очень интересные мысли. В последние десятилетия не появилось ни одного Рамануджана, однако то и дело возникают оригинальные идеи, до которых можно дойти и без формального образования.

Закончим цитатой Рамануджана: «Уравнение для меня ничего не значит, если оно не выражает божественной мысли».

Глава 31

Я ТЕРПЕТЬ НЕ МОГУ МАТЕМАТИКУ, ВЕДЬ...

Ни для кого не секрет, что у большинства наших современников остались очень неприятные воспоминания о начальном и среднем математическом образовании. Дети идут в школу, исполненные энтузиазма. Им нравится считать и они не могут дождаться, когда наконец научатся считать до ста. Но где-то между 7 и 9 классами энтузиазм испаряется, интерес к математике пропадает, и только незначительное меньшинство находит математику захватывающей.

Причины такого положения вещей многообразны. Одна из них заключается в том, что прежде чем ученик доберется до интересных тем, ему нужно усвоить большой объем элементарных знаний. То же самое можно сказать и про другие области человеческого знания. Без грамматики и словаря — никаких французских романов, без гаммы до-мажор — никакой *Лунной сонаты*. Однако в математике особенно сильна опасность того, что ученик увязнет в технике, как если бы в музыкальной школе заставляли слишком много работать над гаммами и не давали заниматься музыкой.

Кроме того, с первого взгляда трудно понять, почему изучение математики за пределами элементарной арифметики делает нас более приспособленными к решению тех задач, которые могли бы сделать этот мир лучше. В одном сатирическом журнале однажды появился прекрасный пример задачи из реальной жизни:

если полкурицы снесут пол-яйца за полдня, то сколько яиц шесть кур снесут за четыре дня?

Дорогой читатель! Ты читаешь эту главу по доброй воле, и поэтому я не верю, что ненавидишь математику черной ненавистью. Однако было бы интересно знать, почему так много наших соотечественников испытывают

глубокую антипатию к этому предмету. Приветствуются все соображения о том, как изменить ситуацию.

МАТЕМАТИКА ОТСТУПАЕТ. ПОСЛЕСЛОВИЕ

Предыдущая колонка в газете вызвала необычайно много ответов читателей. Разброс мнений нельзя, конечно же, считать статистически представляющим все общество. Однако следует отметить, что два мнения возникали особенно часто.

- Математику не любят потому, что образование слишком продвинуто. Доказательства и логические структуры математики вводятся слишком рано и становятся центром внимания. Большинство учеников в замешательстве. Довольно часто эти замечания сопровождаются горькими воспоминаниями о циничных высказываниях учителей математики об уровне класса.
- Никогда не объясняют, для чего это все нужно. Многие читатели говорят, что учителя ничего не рассказывали о связи математики и реальной жизни. В лучшем случае, остаются воспоминания о приятной интеллектуальной игре.

Возможно, у меня слишком оптимистичный взгляд на вещи, но, по-моему, появилась тенденция к более позитивному взгляду на математику. Он то и дело проявляется в рекламе, и не только как декорация (сложно! требовательно!), но и как индикатор интеллектуальных притязаний. И давно уже не слышно политиков или медиазвезд, хвастающих, как плохо они успевали по математике. Многие люди, работающие в школах и университетах, видят, что такая тенденция нарастает.

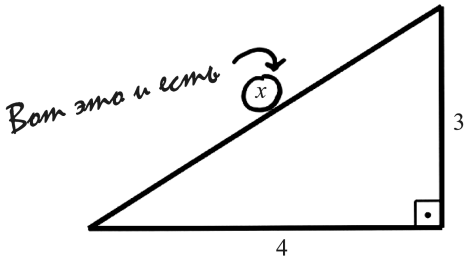
И вот что мы получили:

Четверо из трех немцев не знают арифметики

(Из объявления о наборе в частную школу)

...и можно вообразить ответы в тестах PISA[1)]:

Найдите x в этом прямоугольном треугольнике



Карикатурист Улли Штайн избрал эту тему предметом своих нападок и проиллюстрировал следующие два анекдота в своей книге о PISA.

Учитель: Это доводит меня до отчаяния. Восемьдесят процентов из вас ничего не понимают!

Ученик, обиженно: Но здесь нет столько присутствующих!

Официант: Вам пиццу разрезать на четыре или на восемь кусков?

Посетитель: На четыре, пожалуйста. Восемь я не осилю!

[1)]Program for International Student Assessment.

Глава 32

ПУТЕШЕСТВУЮЩИЙ КОММИВОЯЖЕР. СОВРЕМЕННАЯ ОДИССЕЯ

У одной фирмы есть интересы в нескольких немецких городах. Ее представитель должен объехать все эти города на автомобиле, чтобы всюду представить новый товар. Как правильно спланировать такое путешествие? Разумеется, так, чтобы коммивояжер посетил каждый город, причем ровно однажды, и проехал как можно меньшее расстояние. Задача отыскания такого оптимального маршрута известна (среди математиков) под названием «задача о коммивояжере». Название наводит на (неверную) мысль о том, что речь идет об очень частной проблеме. Но это не так, и вопросы, поднимаемые в этой задаче, приложимы ко многим задачам о планировании, например, оптимизации пути для компьютерно управляемой дрели при производстве монтажных плат.

Казалось бы, решение должно быть несложным, ведь число маршрутов конечно, можно их все измерить, сравнить и выбрать кратчайший. Теоретически это верно. Однако число возможных маршрутов так велико, что практически этот план неисполним. Хотя в реальной жизни задача коммивояжера, как и другие практические задачи планирования, заключается в отыскании оптимального (или почти оптимального) маршрута за разумное время, основной вопрос остается: насколько же сложна эта задача? Она не решена потому, что в истории математики не нашлось никого, способного найти эффективный алгоритм, или потому, что по существу сложна и поэтому неразрешима?

Хотя для коммивояжера, странствующего по белу свету, это может быть неинтересно, вам я раскажу, что задача сложна по существу, и поэтому ее относят к классу сложных задач, включающему те, на которых основана безопасность систем кодирования. Вот почему за нее обещана награда в миллион долларов.

ЗАДАЧА P=NP

Предположим, нужно посетить пятьдесят городов, и расстояния между ними заданы таблицей. Фирма, как всегда, хочет сэкономить и найти маршрут покороче. Бухгалтерию интересует еще и такой вопрос:

Существует ли замкнутый маршрут, проходящий через все города и не превышающий 2000 миль?

У этого вопроса есть два важных аспекта.

Нет никакой надежды решить эту задачу, проверив все возможные маршруты. Для пункта отправления есть 50 возможностей, для второго города — 49, для следующего — 48, и так далее. Всего возможностей существует

$$50 \cdot 49 \cdots 2 \cdot 1 =$$

$$=30414093201713378043612608166064768844377641568960512000000000000,$$

и анализ их всех был бы не под силу самому быстродействующему компьютеру.

Если нам повезет, мы все же сможем ответить на вопрос. Для этого просто выберем маршрут, который кажется довольно коротким, и проверим, не превышает ли его длина 2000 миль. Если не превышает, то мы добились успеха.

Другими словами, мы столкнулись с задачей, которую можно решить, только если очень повезет. Никто не ожидает, что без удачи решение можно будет найти быстро. То есть никто не верит, что кто-либо может придумать процедуру, которая будет давать решение задачи за разумное время. Как это ни скандально, до сих пор никто не смог доказать это утверждение. Специалисты говорят о «задаче P=NP», где символ P означает, что быстрая процедура существует[1)], а NP означает, что решение найдется при большом везении. За решение проблемы «P=NP» предложена награда в миллион долларов[2)].

[1)] Точнее, существует способ найти решение за количество времени, которое полиномиально зависит от входных данных.

[2)] Подробнее об этом написано в гл. 57.

ПРИМЕР

В следующем примере двадцать «городов» были смоделированы на компьютере с использованием алгоритма рандомизации. После этого предложенный маршрут (рис. 32.1) был построен при помощи описанного в гл. 60 метода имитации отжига.

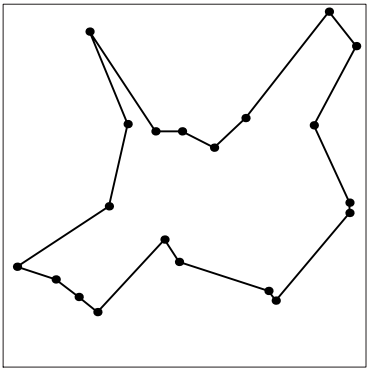


Рис. 32.1. Один из маршрутов коммивояжера

Глава 33
КВАДРАТУРА КРУГА

Придя из математики, выражение «квадратура круга» попало в повседневную речь и стало обозначать почти неразрешимую задачу. Математик, слыша эти слова, вспоминает захватывающую историю, продолжающую очаровывать профессионалов и любителей уже больше двух тысяч лет.

История эта началась в Древней Греции, где геометрия была поставлена на твердую основу в «Началах» Евклида. Древнегреческие математики потратили много сил, выясняя, что можно построить только циркулем и линейкой. Это ограничение, которое сегодня кажется довольно произвольным, было обусловлено представлением о том, что прямая и окружность — совершенные формы.

Многих из нас учили в старших классах выполнять такие построения: как разделить угол пополам, как построить правильный шестиугольник или даже прямоугольный треугольник по данной гипотенузе, используя окружности Фалеса, и т. д.

Некоторые из задач, поставленных греками, оказались довольно сложными. Одна из них — построить квадрат, площадь которого равна площади круга данного радиуса. Эта задача, известная под названием *квадратура круга*, не поддавалась попыткам решения на протяжении двух тысяч лет. И только в 1882 г. задача наконец сдалась, и вовсе не геометрии, как все ожидали, а алгебре.

На протяжении столетий алгебраисты прилежно анализировали природу чисел и выяснили точный смысл, в котором одни числа «легкие», а другие «трудные»[1)]. Уже давно было известно, что только некоторые «легкие» числа можно построить с помощью циркуля и линейки и что можно показать, что квадратура круга сводится

[1)]Об этих числах, которые называются соответственно алгебраическими и трансцендентными, подробнее можно прочитать в гл. 48.

к доказательству «трудности» числа π. Многие математики работали над этим вопросом, и в 1882 г. математик Карл Луи Фердинад фон Линдеманн опубликовал доказательство того, что π — действительно «трудное» число. Его имя навсегда связано с этим результатом, а в отличие от реальной жизни в математике «квадратура круга» действительно невозможна.

ПОСТРОЕНИЕ ЦИРКУЛЕМ И ЛИНЕЙКОЙ

Мы подробнее рассмотрим построения циркулем и линейкой. Наши инструменты — лист бумаги, циркуль и линейка, причем на листе бумаги изображен отрезок единичной длины. Нетрудно, например, начертить отрезок длины 2. Для этого нужно провести по линейке прямую линию, развести ножки циркуля на ширину заданного единичного отрезка, и отметить на прямой две единичных длины подряд. Продолжая, таким образом можно получить отрезки длины 3, 4, 5, ... Аналогично можно построить сумму любых двух уже построенных отрезков, а двигаясь в противоположном направлении — их разность.

Теперь в игру вступает отношение сторон подобных треугольников. Рассмотрим два луча с общим началом, пересеченных двумя параллельными прямыми (рис. 33.1).

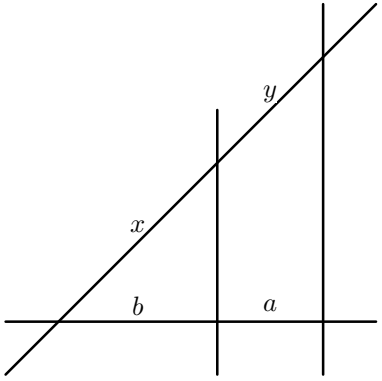


Рис. 33.1. Пропорциональное деление

По обобщенной теореме Фалеса

$$\frac{y}{x} = \frac{a}{b}.$$

Если y обозначает единичную длину, а отрезки a и b уже построены, то длина x равна $\frac{b}{a}$. Это означает, что для любой пары допускающих построение отрезков можно построить и их частное. То же самое относится и к произведению, поскольку в качестве единичной длины можно взять a, а в качестве уже построенных чисел — b и y. Тогда $x = b \cdot y$.

С учетом всех полученных соотношений мы делаем вывод, что можно построить любое число, которое можно получить из уже построенных с помощью операций сложения, вычитания, умножения и деления.

Но это еще не все — можно построить и некоторые корни. Чтобы в этом убедиться, рассмотрите прямоугольный треугольник на рис. 33.2. Хорошо известно, что квадрат высоты равен произведению двух отрезков, которые эта высота отсекает на гипотенузе: $h^2 = p \cdot q$.

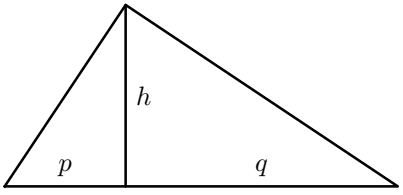


Рис. 33.2. В прямоугольном треугольнике $h^2 = p \cdot q$

Поэтому если длины p и q уже даны, то мы можем построить прямоугольный треугольник с гипотенузой $p+q$ и высотой h так, как изображено на рис. 33.3.

Вначале восставим перпендикуляр из точки F к отрезку AB так, как показано на рис. 33.3. Затем найдем точку M — середину отрезка AB — и построим полуокружность с центром в этой точке. Точку пересечения полуокружности и перпендикуляра обозначим C. Из курса элементарной геометрии известно, что ABC — прямоугольный треугольник. Поэтому два меньших треугольника подобны друг другу и большому треугольнику. Из подобия мы получаем

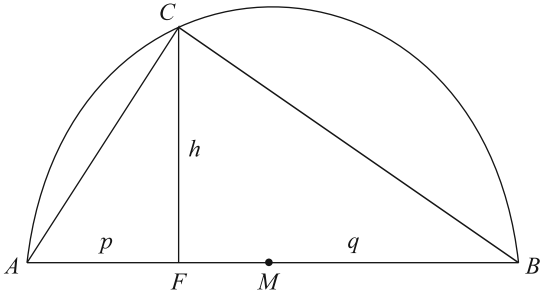


Рис. 33.3. Извлечение квадратного корня с помощью подобных треугольников

соотношение $h/q = p/h$, и несложные алгебраические преобразования дают $h^2 = p \cdot q$. Итак, h равно корню квадратному из $p \cdot q$. И если взять p равным единице, то нам удастся построить $\sqrt{q}$.

Комбинируя все сделанное до сих пор, мы можем построить довольно сложные числа. На самом деле — все числа, которые можно построить из 1, пользуясь операциями $+$, $-$, $\cdot$, $\div$, $\sqrt{}$; например, число

$$\frac{\sqrt{3-\sqrt{2}}}{5}+6.$$

Поскольку корень квадратный из корня квадратного — это корень четвертой степени, мы можем без труда строить корни четвертой, восьмой, шестнадцатой степени, и т. д., — любые корни степени двойки. Процедуры, которые мы описали, по-видимому, позволяют строить сколь угодно сложные числа. Отчего же среди них не может оказаться число π? Отчего бы не записать его в виде комбинации целых чисел и знаков $+$, $-$, $\cdot$, $\div$, $\sqrt{}$, пускай такая запись и займет целую страницу? Результат Линдеманна исключает такую возможность. Все числа, допускающие построение, гораздо «проще» числа π.

ПОСТРОЕНИЕ ТОЛЬКО ЦИРКУЛЕМ И ЛИНЕЙКОЙ

Условие «только циркулем и линейкой» следует понимать буквально. Например, если разрешить делать на линейке

отметки, ситуация изменится кардинально. Чтобы в этом убедиться, с помощью линейки с отметками мы разделим угол на три равные части. Алгебраическими методами доказано, что невозможно выполнить такое построение, пользуясь только циркулем и линейкой[1)].

Рассмотрим угол CBA (рис. 33.4). Как обычно, мы обозначаем угол тремя буквами, причем средняя обозначает вершину угла.

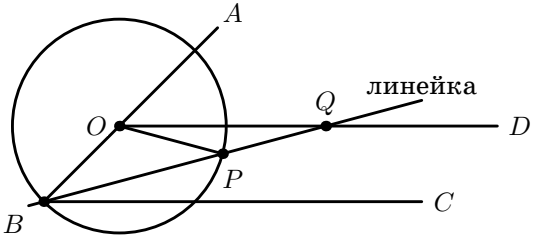


Рис. 33.4. Трисекция угла

Мы собираемся осуществить *трисекцию* этого угла — разделить его на три равные части — при помощи линейки, на которой сделаны две метки P и Q. Вначале мы отметим длину PQ на луче BA, начиная в точке B. Получим точку O, которая послужит центром окружности радиуса PQ. Конечно же, эта окружность пройдет через точку B. Затем построим прямую, проходящую через точку O параллельно BC, и рассмотрим луч OD.

Теперь нам понадобится линейка с делениями. Расположим ее так, чтобы она проходила через точку B, метка P оказалась на окружности, а метка Q — на луче OD, как показано на рис. 33.4.

Мы практически закончили. Осталось убедиться в том, что угол POQ в точности равен одной трети угла CBA.

Чтобы доказать это, удобно обозначить α величину угла POQ. Вначале заметим, что величина угла PQO тоже равна α. Это объясняется тем, что треугольник

[1)]Такие построения — циркулем и линейкой с небольшими модификациями — интенсивно изучались в семнадцатом веке под названием «построения методом вставки».

OPQ равнобедренный, ведь стороны PO и PQ равны (их длины равны радиусу окружности), и поэтому равны углы, лежащие напротив равных сторон.

Сумма всех углов треугольника OPQ равна 180°, два из них известны, и поэтому величина угла OPB должна быть равна 2α, поскольку OPB и OPQ в сумме дают 180°.

Треугольник BPO тоже равнобедренный: OP и OB равны радиусу окружности. Поэтому угол OBP тоже равен 2α.

Для последнего шага доказательства остается заметить, что угол QBC равен α. Этот угол должен быть равен углу OQB, ведь они являются внутренними накрест лежащими углами, образованными прямой (краем линейки), пересекающей два параллельных луча BC и OD. Поэтому угол OBC, равный сумме углов QBC и OBQ, равен 3α. Это и означает, что угол POQ равен одной трети угла CBO.

КУБАТУРА СФЕРЫ

Как мы видели, квадратура круга невозможна, если правила игры ограничивают нас только циркулем и линейкой, и поэтому в обыденной речи сложные задачи называют квадратурой круга.

В конце 2005 г. в ходе затяжных переговоров о составе новой немецкой правящей коалиции избранная канцлером Ангела Меркель, желая сделать заявление, сказала прессе, что переговоры были даже сложнее квадратуры круга — наверное, их следовало бы сравнить с кубатурой сферы. Видимо, речь шла о задаче превращения сферы в куб того же объема. Объем сферы радиуса r равен $\frac{4}{3} \cdot \pi \cdot r^3$, а объем куба со стороной l равен l^3, поэтому получается уравнение

$$\frac{4}{3} \cdot \pi \cdot r^3 = l^3$$

или, что то же самое,

$$l = r \sqrt[3]{\frac{4}{3} \cdot \pi}.$$

Другими словами, кубатура сферы требует построения отрезка $\sqrt[3]{\frac{4}{3}\pi}$. Если бы описанными нами методами можно было построить и отрезок π, то после этого квадратура круга не представляла бы трудностей.

Однако к кубатуре сферы это не относится, поскольку, вообще говоря, строить кубические корни с помощью циркуля и линейки нельзя.

Поэтому Ангела Меркель была совершенно права, говоря, что задача кубатуры сферы сложнее, чем задача квадратуры круга (хотя можно было бы возразить, что нет смысла говорить о сравнении степеней сложности, когда оба построения невозможны).

Глава 34

ШАГ В БЕСКОНЕЧНОСТЬ

Как можно объять необъятное? Как доказывают, например, что для *любого* положительного числа n сумма первых n натуральных чисел всегда равна $\frac{1}{2} \cdot n \cdot (n+1)$? Для начала выясним, есть ли шансы у этого утверждения быть истинным, проверив несколько чисел. Если $n = 4$, то сумма первых n натуральных чисел равна $1+2+3+4 = 10$; а подстановка $n = 4$ в формулу $\frac{1}{2} \cdot n \cdot (n+1)$ тоже дает $\frac{1}{2} \cdot 4 \cdot (4+1) = 10$. Мы можем проверять и другие числа, но как можно удостовериться, что формула верна *всегда*? Даже для десятитысячезначных чисел, даже для тех, для записи которых чернила нужно производить целый год?

Ответ, конечно же, не в том, чтобы приступить к проверке всех чисел подряд! Даже если вы сможете соединить все компьютеры в мире в одну сеть, вам не удастся продвинуться дальше двадцатизначных чисел.

Так как же быть? Математики доказывают истинность этого и аналогичных высказываний, используя метод под названием *индукция*. Доказательство по индукции состоит из двух шагов. На первом шаге нужно провести вычисления и показать истинность высказывания для наименьшего из допустимых значений n; в нашем случае для $n = 1$. Это просто, ведь «сумма» одного числа равна 1, и подстановка 1 в доказываемую формулу тоже дает $\frac{1}{2} \cdot 1 \cdot (1+1) = 1$. На втором шаге нужно доказать, что *если* утверждение истинно для некоторого числа, то оно должно быть истинно для следующего по порядку числа. (Вычисления для нашего примера мы проведем ниже.)

Поскольку утверждение истинно для $n = 1$, в силу второго шага метода оно должно быть истинно и для $n = 2$. А раз оно верно для $n = 2$, то должно выполняться для $n = 3$. А если оно выполняется для $n = 3$, то должно .... Вы

наверняка видели костяшки домино, выстроенные в ряд так, что если толкнуть первую, она толкнет соседнюю. Если первую костяшку уронить, то поочередно упадут и все остальные.

Самое интересное в индукции в том, что в нескольких строках доказательства можно установить истинность бесконечного числа утверждений. Это ключ почти ко всем математическим утверждениям, которые нужно доказывать для бесконечного числа случаев.

НЕДОСТАЮЩИЙ ШАГ ИНДУКЦИИ

Здесь мы проведем так называемый *шаг индукции* для доказательства формулы суммирования, которую мы привели в начале главы.

Нужно показать, что сумма $n + 1$ чисел, т. е. $1 + 2 + \cdots + n + (n + 1)$, выражается этой формулой, если согласно *предположению индукции* сумма первых n чисел задается формулой $\frac{1}{2} \cdot n \cdot (n + 1)$.

Согласно предположению индукции

$$1 + 2 + \cdots + n + (n + 1) = \frac{1}{2} \cdot n \cdot (n + 1) + (n + 1).$$

Но последнее выражение равно $\frac{1}{2} \cdot (n+1) \cdot (n+2)$ (на основе простейших алгебраических преобразований), а это и есть формула суммирования для $n + 1$.

Итак, мы показали, что если предположить истинность формулы для n, то она верна и для $n + 1$.

ОТКУДА БЕРЕТСЯ ФОРМУЛА?

Индукция — «официальный» способ проверки корректности некого утверждения для бесконечного количества натуральных чисел. Но прежде чем доказывать утверждение, нужно это утверждение как-то обнаружить! Как придумывают такие вещи?

Это креативный аспект математики. Нужна интуиция, опыт, удача, а часто еще блестящее умение сделать задачу наглядной. Посмотрим, как это работает в нашем

конкретном примере — утверждения о сумме первых n натуральных чисел:

$$1 + 2 + \cdots + n = \frac{n \cdot (n+1)}{2}.$$

С доказательством мы уже знакомы, а теперь выясним, откуда берется формула. Способов получить ее много, и мы рассмотрим два из них.

Одна возможность — представить сумму в виде суммы площадей, как изображено на рис. 34.1.

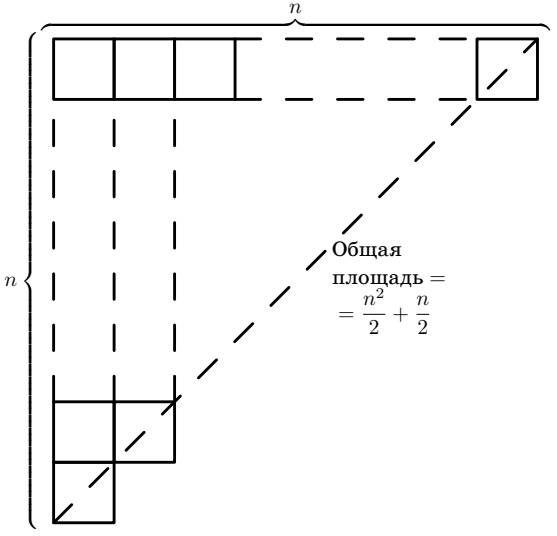


Рис. 34.1. Так «выглядит» формула $1 + \cdots + n = n(n+1)/2$

Мы начнем с маленького квадрата в нижнем левом углу рисунка. Сверху разместим еще два квадрата, еще выше — три, и т. д.; в верхнем ряду окажется n квадратов. Результат похож на половину шахматной доски. Площадь половины шахматной доски равна $n \cdot n/2$, но площадь квадратов больше нее на половину квадратиков на диагонали. Поэтому полученную величину нужно увеличить на $\frac{1}{2}n$. В результате имеем: сумма $1 + \cdots + n$ должна быть равна $n \cdot n/2 + n/2$. А это выражение равно $n \cdot (n+1)/2$.

Мы могли бы рассуждать иначе, примерно так, как это делал маленький Гаусс в истории из гл. 25. Запишем сумму $1 + \cdots + n$ в виде $(1 + n) + (2 + (n - 1)) + \ldots$, сгруппировав первое и последнее слагаемые, второе и предпоследнее, и т. д. Каждое сгруппированное выражение равно $n + 1$, а их количество составляет $n/2$, если n четно. Если же n нечетно, то таких слагаемых $(n - 1)/2$, да еще одинокое слагаемое $(n + 1)/2$ в конце.

Итак, для четных n сумма равна $(n + 1) \cdot n/2$, а для нечетных — $(n + 1) \cdot (n - 1)/2 + (n + 1)/2$, что после небольших алгебраических преобразований тоже принимает вид $(n+1) \cdot n/2$. Мы получаем одну формулу для суммы первых n чисел вне зависимости от того, четно n или нечетно.

ЕЩЕ ОДНО ДОКАЗАТЕЛЬСТВО ПО ИНДУКЦИИ

Приведем еще один пример утверждения, которое можно доказать по индукции: «n объектов можно упорядочить $1 \cdot 2 \cdot 3 \cdots n$ способами». Точнее, это означает, что при $n = 1$ есть только один способ; при $n = 2$ есть $1 \cdot 2 = 2$ способа; и т. д. Заметим еще, что для произведения $1 \cdot 2 \cdot 3 \cdots n$ есть специальное обозначение $n!$ (читается «n факториал»)[1)].

Для малых n это утверждение легко проверить непосредственно. Например, три объекта a, b, c можно упорядочить так: abc, acb, bac, bca, cab, cba. Этих способов действительно $3! = 6$.

«Строгое» доказательство по индукции могло бы выглядеть приблизительно так. *Во-первых*, показывают, что утверждение верно при $n = 1$. Это очевидно, поскольку один элемент можно упорядочить только одним способом. *Во-вторых*, фиксируют некоторое значение n, которое считают произвольным натуральным числом, и полагают (индуктивное предположение), что утверждение для него выполняется. *В-третьих*, показывают, что при выполненном индуктивном предположении утверждение выполняется для $n + 1$ объектов.

[1)] О способах упорядочивать объекты можно подробнее прочитать в гл. 29.

Сейчас мы так и сделаем. Представим, что n объектов — это n белых шариков, пронумерованных числами от 1 до n. А $(n+1)$-й объект — это красный шарик. Упорядочивая *все* $n+1$ шариков, поступим следующим образом. Вначале выберем расположение n белых шариков, Согласно индуктивному предположению это можно сделать $1 \cdot 2 \cdot 3 \cdots n = n!$ способами. Теперь посмотрим, куда положить красный шарик. Его можно положить в начало, после первого белого шарика, после второго, после третьего, и т. д.; последний способ — положить его в конце ряда. Так что для красного шарика есть $n+1$ позиций. Эти $n+1$ позиций возможны для *любого* расположения n белых шариков, поэтому всего имеется $(n+1) \cdot n!$ расположений всех $n+1$ шариков, или $(n+1)!$. В этом и состоит доказываемое утверждение для $n+1$ объектов.

Глава 35
МАТЕМАТИКА В ТВОЕМ CD-ПЛЕЕРЕ

Среди всех технических устройств, которые можно найти в обычном доме, именно CD-плеер — самый математический. Математика в нем важна в двух отношениях. Во-первых, исходный непрерывный сигнал — например, концерт в Берлинской филармонии — оцифровывают и превращают в набор нулей и единиц. Для этого сигнал дискретизируют примерно 44 000 раз в секунду; важная теорема об обработке сигнала гласит, что на таком уровне дискретизации сохраняется все, что может уловить человеческое ухо. Если бы наш слух был значительно лучше или хуже (в смысле воспринимаемых частот), то параметры CD-плеера были бы иными.

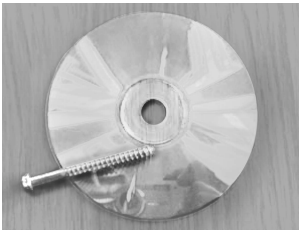
Другие математические требования к CD-плееру обусловлены тем, что ни процесс сжатия, ни процесс воспроизведения не свободны от ошибок: на диск может попасть пылинка, или его может поцарапать кошка. Это серьезная проблема, как может понять всякий, кому случалось потерять компьютерные данные (jpeg-изображение, html-сайт) в результате того, что среди передаваемых миллионов битов информации попался один неверный.

Если бы кто-то надеялся достичь совершенства для CD-плеера, то и аппарат, и диск оказались бы слишком дорогими. Но проблема была решена другими средствами, и ключевая фраза здесь — *теория кодирования*[1)]. Как можно передать сообщение, чтобы принимающая сторона могла его прочесть, даже если при передаче были возможны ошибки?

Как передать десятибуквенное сообщение азбукой Морзе так, чтобы если даже оно было повреждено из-за опечатки или атмосферного воздействия, все равно можно было бы гарантировать правильность его прочтения? Первое, что приходит в голову, — передать сообщение несколько

[1)] Мы будем обсуждать ее подробнее в гл. 98.

раз подряд, после чего принимающая сторона выберет ту версию, которая встречается чаще всех. Для CD-плеера такой способ был бы слишком громоздким, и поэтому пришлось разработать методы, для которых «надежная» версия переданного сигнала не намного длиннее оригинала.



Тем временем способ передачи сигнала стал настолько устойчив к ошибкам, что качество воспроизведения не страдает и в случае серьезных помех. Например, даже сильно поцарапанный диск можно слушать, и несовершенства будут неощутимы. Жалко, что такие технологии были недоступны во времена виниловых пластинок. Тогда было слышно каждую пылинку.

ТЕОРЕМА ОТСЧЕТОВ

Для того чтобы музыка или какой-нибудь другой акустический сигнал нашли путь от источника к вашей стереосистеме, предпринимаются следующие шаги. Во-первых, звук *оцифровывается*, т. е. преобразуется в очень длинную строку нулей и единиц. Это преобразование аналогового, или непрерывного, сигнала в цифровой, или дискретный, — решающий шаг, поскольку только после оцифровки может быть создана и передана без потери качества копия сигнала.

Метод оцифровки оказался успешным благодаря несовершенству человеческого слуха. В мире, где мы слышали бы сколь угодно высокие частоты, не было бы компакт-дисков. Но в действительности частоты выше 20 килогерц недоступны нашему восприятию, и поэтому оцифровка возможна. Она проходит в два этапа.

- Вначале сигнал проходит через фильтр, в котором все частоты выше некоторой неслышной (нам) подавляются. Мы не воспринимаем разницу между первоначальным и урезанным сигналами.
- Потом пользуются тем, что ограниченный по частоте сигнал может быть оцифрован и аккуратно восстановлен, если передается достаточное число раз в секунду.

Последний факт известен под названием *теоремы отсчетов*. Вот ее точная формулировка.

Если сигнал состоит из нескольких частот не выше f, то цифровой сигнал может быть воспроизведен, если промежутки времени между значениями сигналов не превышают $1/(2f)$.

Например, если самая высокая частота составляет 10 килогерц, то требуется промежуток дискретизации в $1/20\,000$, т. е. $20\,000$ отсчетов в секунду.

Если это кажется слишком абстрактным, теорему можно проиллюстрировать иначе. Представьте себе, что у вас есть видеокамера, фиксирующая несколько кадров в секунду. Ваш малыш качается на качелях, и вы хотите его запечатлеть. При нормальной частоте раскачивания сюжет можно воспроизвести реалистично. Но если частота слишком низкая, вас может постичь разочарование: может оказаться, что соседние кадры отличаются только небольшим смещением, хотя на самом деле произошел почти полный цикл, но камера не смогла его воспроизвести.

Теорему об отсчетах можно рассматривать как аналог руководства пользователя: вы должны выбрать такую-то частоту, чтобы аккуратно воспроизвести раскачивания с такой-то скоростью.

Глава 36
ЛОГАРИФМ. ВЫМИРАЮЩЕЕ ПЛЕМЯ

Читатели старшего поколения вспомнят — возможно, с ужасом — как они в школе учились работать с логарифмами. Здесь мы напишем некролог логарифмам. Конечно же, логарифмы остаются важной частью математики, но в среде инженеров и техников они постепенно исчезают.

Чтобы понять, для чего они нужны, нам придется вспомнить некоторые термины. Во-первых, нужно знать, как математики обозначают степени: если a и n — целые числа, то a^n обозначает n-кратное произведение множителей a. Таким образом, 3^4 обозначает произведение $3 \cdot 3 \cdot 3 \cdot 3$ (равное 81), а 10^6 равно миллиону. Если некоторое число умножить на себя n раз и потом еще m раз, то всего получится $m + n$ сомножителей, это наблюдение выражается формулой $a^{m+n} = a^n \cdot a^m$. Этот же закон для степеней выполняется, даже если определить возведение в степень для произвольных, не обязательно целых, показателей. Например, квадратный корень из a можно записать как $a^{1/2}$.

А теперь на сцену выходят логарифмы. Для простоты мы будем рассматривать логарифмы по основанию 10. Для положительного числа b логарифм b определяется как число m такое, что $10^m = b$. Выше мы видели, что логарифм миллиона равен 6, а логарифм тысячи — это, конечно же, 3. Важно помнить, что когда допускаются произвольные степени, у любого положительного числа логарифм есть.

Ключевой момент в теме «логарифмы»: согласно описанному выше закону для степеней *логарифм произведения равен сумме логарифмов множителей*. Это свойство позволяет переходить от умножения к сложению. Если нужно вычислить произведение $b \cdot c$, то можно по таблице найти логарифмы чисел b и c, сложить два результата, а затем выяснить, логарифм какого числа равен полученной сумме. Это и есть произведение.

В стародавние времена, когда компьютеров еще не было, именно так чаще всего и умножали; логарифмы были ломовой лошадью вычислений. Сложение гораздо проще умножения, поэтому переход от одного типа вычислений к другому упрощал жизнь тем, кто вел подсчеты карандашом на бумаге. У этой техники есть аналоги и в других областях нашей жизни, где задачу приходится привести к другому виду, чтобы можно было ее решить.

И еще один некролог, окончательный и бесповоротный. Для механизации логарифмических вычислений пользовались логарифмическими линейками, в свое время они были очень удобными (рис. 36.1). А сейчас они исчезли, и найти их можно только в музее.

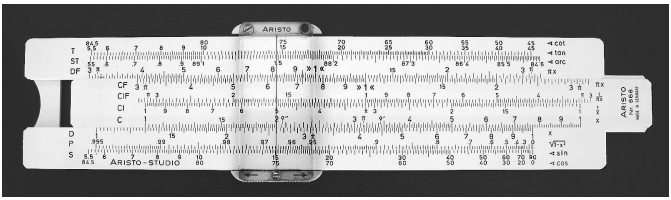


Рис. 36.1. Логарифмическая линейка

ТИПИЧНЫЙ РАСЧЕТ

Давайте рассмотрим пример вычислений, описанных в некрологе, как это делалось в те времена, когда калькуляторы еще не были широко распространены.

Допустим, нужно вычислить произведение $3{,}45 \cdot 7{,}61$. Ответ нам пока еще неизвестен, и мы обозначим его x:

$$x = 3{,}45 \cdot 7{,}61.$$

По закону степеней логарифм x равен сумме логарифмов чисел 3,45 и 7,61. Мы будем пользоваться десятичными логарифмами — так, как некоторые из нас делали в школе. Итак, логарифм 3,45 равен 0,53782, а логарифм 7,61 равен 0,88138. Эти числа следовало найти в таблице логарифмов. Поэтому логарифм (до сих пор все еще неизвестного) числа x равен

$$0{,}53782 + 0{,}88138 = 1{,}41920.$$

По определению логарифма $10^{\log x} = x$, поэтому

$$x = 10^{1,41920} = 26,25427.$$

Последнее число тоже можно найти в таблице логарифмов.

Результат вполне удовлетворительный, так как точное значение равно

$$3,45 \cdot 7,61 = 26,2545.$$

Поэтому можно забыть об умножении и для всех вычислений пользоваться сложением, как только задача переведена в мир логарифмов.

Глава 37

МАТЕМАТИКА, ДОСТОЙНАЯ НАГРАДЫ

Как? Вы не слышали о наградах для математиков? Возможно, это объясняется тем, что, как правило, суммы невелики. Да и будь они огромны, математические достижения обычно так сложно объяснить широкой публике, что новостные медиа и не беспокоят ее такими рассказами.

Рис. 37.1. Самая престижная награда в математике — медаль Филдса

Мы вкратце расскажем о самых важных наградах за достижения в математике. Любой математик, желающий обессмертить свое имя, должен сделать что-нибудь особенно впечатляющее, будучи еще довольно молодым. Лучше всего — двадцати с чем-нибудь лет. Тогда есть возможность получить медаль Филдса, присуждаемую каждые четыре года на Международном конгрессе математиков. Эта награда не делает человека богатым — она составляет приблизительно двадцать тысяч долларов. Однако лауреат премии может быть уверен в своем финансовом положении до конца дней, поскольку ему наверняка предложат лучшие позиции и затопят предложениями высокооплачиваемых должностей. Медаль Филдса часто называют аналогом Нобелевской премии для математиков. Однако эта медаль

может быть присуждена только тем математикам, кто еще не достиг сорокалетия. (Именно поэтому в 1998 г. в Берлине филдсовскую медаль не присудили вообще никому, поскольку самое, по-видимому, поразительное открытие предыдущего столетия в математике, доказательство теоремы Ферма, было сделано сорокапятилетним Эндрю Уайлзом.)

Однако существуют и награды, весьма внушительные в денежном выражении. Например, в 2000 г. институтом Клэя были назначены призы в миллион долларов каждый за решение семи конкретных сложных задач. Они все еще никому не присуждены, несмотря на то что за них брались многие из лучших в мире математических умов[1)].

В 2003 г. появилась премия на уровне Нобелевской. Абелевская премия финансируется богатым гражданином Норвегии, и возможно, когда-нибудь встанет в один ряд с Нобелевской и будет вручаться на ежегодной церемонии в Швеции. Первым обладателем этой премии стал Жан-Пьер Серр, и членам абелевского комитета было непросто объяснить непосвященным, что такого сделал Серр, что заслужил награду в 600 000 евро. Возможно, это объясняется тем, что вся наука стала узкоспециализированной: помните ли вы, за что была присуждена последняя Нобелевская премия по химии?

РАЗБОГАТЕТЬ НА МАТЕМАТИКЕ: ЕСТЬ ЛИ ШАНС У ЛЮБИТЕЛЯ?

Существует много математических задач, над которыми десятилетиями бьются лучшие умы человечества. О нескольких мы рассказываем в этой книге (гл. 18, 32, 49, 57).

За решение некоторых из этих задач можно, вдобавок к бессмертной славе, получить миллион долларов. Есть ли шанс у склонного к математике любителя? В истории математики известно несколько эпизодов, когда серьезные, даже выдающиеся результаты получили те, для кого

[1)] Одна из семи задач — проблема Пуанкаре, — была решена нашим соотечественником Григорием Перельманом в 2002 г., но от приза он отказался (см. гл. 93). — *Прим. перев.*

математика просто хобби. В этой книге мы рассказываем о двух из них — о Байесе и Бюффоне (гл. 50 и 59). Да и сам Пьер Ферма (см. гл. 89) был юристом, а профессиональным математиком не был.

Однако совершенно невероятно, чтобы по-настоящему сложную задачу решил любитель. Уровень слишком высок, и все очевидные подходы уже испробованы.

В других областях мы тоже не ожидаем великих достижений от тех, кто не работает там на высоком уровне. В Уимблдонском турнире никогда не победит теннисист-любитель, время от времени играющий по выходным. А тому, кто не потратил годы на учебу, никогда не поручат спеть партию Зигфрида в опере Вагнера.

Глава 38

ПОЧЕМУ ИМЕННО АКСИОМЫ?

Дети в возрасте от трех до шести часто надоедают родителям, постоянно задавая невинные вопросы вроде «Мама, как работает автомобиль?». Но если не использовать слова «мотор», «зажигание», «химическая реакция», то даже экспертам остается только сказать: «А вот так!». Конец дискуссии.

Точно так же с математикой. Можно задавать все больше и больше вопросов о ее основаниях, но в некоторый момент дискуссия становится бесплодной, и тогда просто договариваются: «А вот так». Аксиомы в математике так и возникают.

Первая система аксиом была построена более 2000 лет назад Евклидом (III век до н. э.; рис. 38.1). В своих «Началах» он построил аксиоматику геометрии. Описав основные понятия, такие как «точка» и «прямая», он

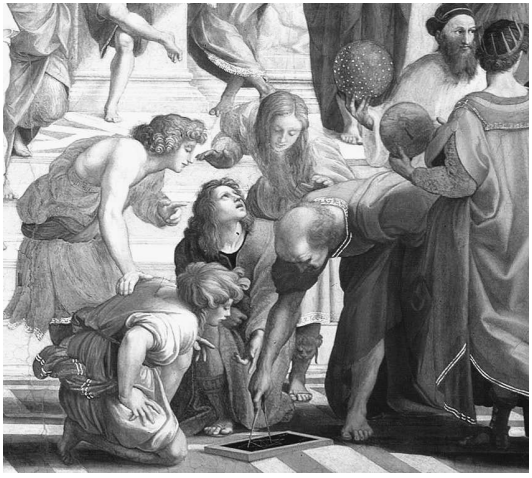


Рис. 38.1. Евклид в «Афинской школе» (фрагмент) (Рафаэль, 1510)

затем определил некоторые свойства этих объектов: «Через любые две точки проходит одна и только одна прямая», и т. д.

В наше время почти все области математики аксиоматизированы. Существуют аксиомы о самых разных объектах, таких как числа, векторы и вероятности.

После того как аксиомы установлены, можно отправляться в свободный поиск возможных следствий. Большинство математиков считают, что это гораздо интереснее, чем бесконечно спорить из-за основ.

Но одна вещь остается загадкой. Как получается — например, в геометрии, — что из небольшого количества аксиом можно развить прекрасно функционирующую математическую модель для описания реального мира? Огромный успех аксиоматического метода подвигнул мыслителей из других областей человеческого знания на попытки построить аксиоматику и для их наук. В великом труде Ньютона по механике (неспроста он называется «Математические начала натуральной философии») есть длинные пассажи, которые читаются как учебник по математике.

Если заменить слово «аксиома» на «правила игры», то получится очень полезная аналогия. Правила игры — шахмат, например, — фиксированы, и игроки не тратят интеллектуальных усилий на попытки придумать новые, улучшенные правила. Вместо этого шахматисты стараются проанализировать, можно ли в данной ситуации поставить мат. Точно так же математики хотят знать, есть ли у той или иной задачи решение в рамках некоторой аксиоматики.

ПРОГРАММА ГИЛЬБЕРТА

Хотя первой аксиоматике уже более двух тысяч лет, триумфальное шествие этого подхода началось только сто лет тому назад. Великий математик Давид Гильберт предложил подвести под математику прочное основание. Главная идея состояла в том, что этим достигались сразу две цели. Во-первых, пользуясь правилами дедукции, можно будет автоматически выводить из этих аксиом

математические теоремы, а во-вторых, можно будет опять-таки механически проверять истинность математических утверждений. Например, «да» будет ответом на вопрос «Существует ли целое число, квадрат которого равен 25?», а «нет» будет следовать из «Существует ли решение уравнения $x = x + 1$?».

Эта амбициозная программа закончилась провалом. Логик Курт Гёдель доказал свои теоремы о неполноте, смысл которых в том, что в математической теории всегда может существовать утверждение, которое нельзя ни доказать, ни опровергнуть. Эти теоремы говорят еще о том, что всегда существуют истинные утверждения, которые нельзя вывести из аксиом.

АКСИОМЫ — «ЗАКОНЫ» МАТЕМАТИКИ

Кроме аналогии между аксиомами математики и шахматными правилами можно найти параллели и в юриспруденции. После того как законы установлены, некоторые вещи можно делать, не опасаясь наказания. Для адвоката моральные суждения о таких действиях не так важны по сравнению с вопросом о том, допустимы ли действия с юридической точки зрения. Точно так же в математике трудно сказать, как предмет разовьется из данных аксиом. Иногда некоторые законы приводят к нежелательным результатам, и в этом случае законы можно переписать или изменить. Точно так же в математике можно модифицировать систему аксиом.

В противоположность шахматам, в юриспруденции моральный аспект имеет значение; то же самое можно сказать и о математике. Математические открытия могут быть использованы как во благо человечества, так и с бесчестными целями. Теорема оптимизации, например, может быть использована для создания не только улучшенных удобрений, но и биологического оружия.

Глава 39
КОМПЬЮТЕРНОЕ ДОКАЗАТЕЛЬСТВО

Сегодня мы собираемся обсудить почти философскую проблему, с которой математики столкнулись в ходе развития технологий: при каких обстоятельствах математическое утверждение может со всей определенностью считаться доказанным?

В течение последних двух тысяч лет было достигнуто понимание того, каким должно быть «строгое доказательство» в науке, основания которой уже установлены: доказываемое утверждение должно выводиться корректными дедуктивными рассуждениями из фундаментальных научных аксиом. Так была построена евклидова геометрия, да и многие другие области развивались по пути, проложенному Евклидом в его «Началах». Потребовалось много времени, для того чтобы все области математики были установлены на строгий аксиоматический фундамент, но к середине девятнадцатого века основания математики были вполне добротными. Было единодушие по вопросу о том, что считать истиной в математике. Все соглашались, что за достоверностью доказательств следит все математическое сообщество; истинно то, что получило благословение экспертов.

В 1970-х гг. эти стандарты были поставлены под вопрос в ходе решения знаменитой задачи о четырех красках[1)]. Впервые в истории математики решающую роль сыграли компьютеры, поскольку значительную часть вычислений, проведенных компьютером, по-видимому, невозможно выполнить «вручную», даже если потратить на это всю жизнь.

Полноценно ли это доказательство? В математическом сообществе мнения по этому вопросу разделились. Многим хотелось избежать компьютерного доказательства, и после его построения значительные усилия были потрачены

[1)] В этой задаче речь идет о раскраске карты; подробности здесь несущественны; см. гл. 99.

на поиск «классического» доказательства. Иногда такие поиски бывают плодотворными, но во многих случаях приходится полагаться на поток электронов.

У этой проблемы есть еще один аспект: ведь в наше время можно запрограммировать компьютеры таким образом, что они будут открывать и доказывать свои собственные, хоть и несложные, теоремы. И техника компьютерных доказательств может развиться в той же степени, что и умение компьютеров играть в шахматы. Вначале оно было слабым, и даже рядовые игроки обыгрывали компьютеры, а сейчас и чемпионы мира не всегда побеждают. Если все так и произойдет, у математиков возникнут большие проблемы.

ЛЕГКО ВИДЕТЬ, ЧТО...

Ответ на вопрос «Полноценно ли это доказательство?» зависит не только от того, к чему он относится, но и от математической подготовки беседующих. Например, если речь идет о натуральных числах (т. е. числах 1, 2, 3, ...), то доказательства часто проводят по индукции[1)]. Только этот метод позволяет доказывать факты о бесконечном.

Те, кому по роду своей математической деятельности часто приходится им пользоваться, предпочитают не тратить время и энергию на стандартные рассуждения. Поэтому нередко попадаются фразы вроде: «По индукции отсюда следует, что...», или даже попросту приводятся утверждения без всяких комментариев.

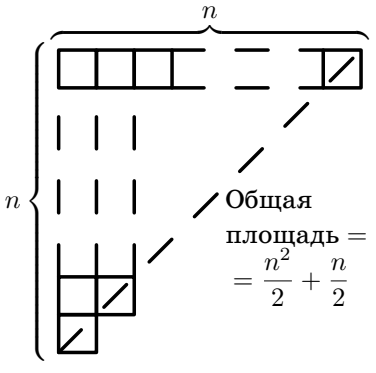
Такие ситуации вызывают ужас у неофитов в математике. В начале учебы они ожидают полных доказательств, а экспертам скучно выписывать все подробности. Со временем математики привыкают к пропускам в доказательствах. Хотя в сомнительных ситуациях подробности желательны, не стоит допускать, чтобы технические детали, с которыми читатель давно знаком, занимали бóльшую часть научной статьи.

[1)] См. гл. 34.

СПОСОБНЫ ЛИ КОМПЬЮТЕРЫ К МАТЕМАТИЧЕСКОМУ ТВОРЧЕСТВУ?

Прежде чем приступать к доказательству, нужно понимать, что именно вы хотите доказать. Например, если вы не подозреваете о том, что величина угла, вписанного в полукруг (такого, как угол C на рис. 33.3), составляет 90°, то не догадаетесь, как доказать это утверждение[1)].

Математики единодушны в том, что креативный аспект математического прогресса (откуда берутся утверждения, которые нужно доказывать?) во многих отношениях требует большего, чем умение строить доказательства этих утверждений.



Рассмотрим, например, утверждение о том, что сумма $1+2+\cdots+n$ первых n натуральных чисел[2)] равна $n\cdot(n+1)/2$. Прошли десятилетия с тех пор, как люди научились вполне строго доказывать это утверждение по индукции. Но до сих пор неясно, способен ли компьютер открыть этот факт самостоятельно. Мы, существа мыслящие, можем изобразить половину шахматной доски, и этот рисунок подскажет правильную формулу. Компьютеры же могут «видеть» только то, что в них заложено программой, и поэтому математики убеждены, что компьютеры никогда не отберут у них самую захватывающую часть работы.

[1)] Это теорема Фалеса, которую мы будем обсуждать в гл. 47.
[2)] Подробнее об этом см. в гл. 34.

Глава 40

ЛОТЕРЕЯ. МАЛЕНЬКИЕ ВЫИГРЫШИ

Когда математиков спрашивают о шансах выиграть в лотерее, обычно интересуются вероятностью выиграть джекпот. Об этой вероятности шла речь в гл. 1, и мы видели, что вероятность невелика — всего-то 1/13 983 816. Покупая по одному билету в неделю, выигрыша можно ждать в среднем около 270 000 лет. Чтобы надеяться выиграть джекпот хотя бы однажды, играя в лотерею еженедельно на протяжении 70 лет, нужно покупать около 4000 билетов в неделю.

Большинству из нас остается довольствоваться меньшим, и мы утешаемся лучшими шансами на выигрыш одного из меньших призов. Играя в лотерею, нужно угадать шесть чисел от 1 до 49. Джекпот предназначается тем, кто угадал все шесть номеров, но есть призы и для тех, кто угадал три, четыре или пять номеров. Шансы правильно угадать три номера нельзя назвать крохотными — около 0,018 или 1,8%. Вас может, конечно, постигнуть неудача, и вы ни разу не угадаете хотя бы три номера за год, но, к счастью, вероятность угадать три верных номера хотя бы однажды, имея 52 лотерейных билета, составляет около 61%.

Угадать четыре номера, конечно же, сложнее. Такая удача выпадает приблизительно на один билет из тысячи. Пять правильных номеров угадывают в двух билетах из ста тысяч. Конечно же, нужно еще рассмотреть номер-бонус, который дополнительно выбирается из 43 чисел, оставшихся после выбора шести выигрышных. С наивной точки зрения, бонус должен бы в огромной степени повышать шансы на выигрыш, но математические расчеты отрезвляют. Вероятность угадать пять номеров и еще один бонусный только в шесть раз выше вероятности верно угадать шесть номеров. А для шансов верно угадать четыре номера сразу или три номера и один бонусный ситуация еще хуже. Вероятность меняется только в 1,33 раза.

Однако же, как всегда покупая лотерейный билет, вы выигрываете в основном пару дней, посвященных мечтам об огромном богатстве, а еще получаете моральное удовлетворение от того, что деньги, не выплаченные на выигрыш, тратятся на значительные социальные проекты.

МАЛЫЕ ВЫИГРЫШИ. ВЫЧИСЛЕНИЯ

Введенные в гл. 29 понятия позволяют нам вычислить больше, чем просто вероятность выиграть большой приз. Напомним, что имеется C_n^k (читается «це из эн по ка») способов выбрать k элементов из n-элементного множества, и поэтому есть $C_{49}^6 = 13\,983\,816$ различных способов заполнить лотерейный билет.

Мы хотим вычислить вероятность угадать ровно три из шести номеров. Итак, сколько же существует способов выбрать шесть номеров из сорока девяти так, чтобы ровно три из них оказались правильными и три — неправильными? Нужно выбрать три номера из шести «счастливых», а также три номера из оставшихся сорока трех «несчастливых». Имеется $C_6^3 = 20$ способов выбрать три правильных и C_{43}^3 способов выбрать три неправильных номера. Поэтому всего имеется

$$C_6^3 \cdot C_{43}^3 = 20 \cdot 12\,341 = 246\,820$$

различных способов так угадывать номера в лотерее, что три из них окажутся верными, а три — неверными. Поскольку всего есть $13\,983\,816$ способов заполнить лотерейный билет, вероятность угадать верно ровно три номера равна

$$\frac{246\,820}{13\,983\,816} = 0{,}0176466\ldots;$$

она немного не дотягивает до $1{,}8\%$.

А чему равна вероятность не угадать ни одного номера? Все шесть номеров должны быть выбраны из множества сорока трех неправильных номеров, и соответствующая вероятность равна

$$\frac{C_{43}^6}{13\,983\,816} = \frac{6\,096\,454}{13\,983\,816} = 0{,}43587\ldots\,.$$

Результаты вычислений для любого числа угаданных номеров от нуля до шести сведены в таблицу:

k	Вероятность правильно угадать k номеров
0	0,436
1	0,413
2	0,132
3	0,018
4	0,001
5	$2 \cdot 10^{-5}$
6	$7 \cdot 10^{-8}$

БОНУС

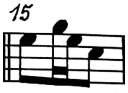
Как изменяются шансы, если учитывать бонусный номер? Давайте подсчитаем.

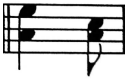
Выбрать 5 верных номеров можно $C_6^5 \cdot C_{43}^1 = 6 \cdot 43 = 258$ способами. Поэтому угадать 5 выигрышных номеров в 258 раз вероятнее, чем 6. Чтобы отметить в билете 5 верных номеров и один бонусный, нужно правильно угадать пять номеров из шести (это можно сделать C_6^5 способами), а также единственный бонусный номер (это можно сделать только одним способом). Всего получается шесть возможностей.

Выбрать же все 6 верных номеров можно только одним способом, поэтому можно сказать, что угадать 5 верных номеров и один бонусный в шесть раз вероятнее, чем угадать все 6 верных номеров.

Глава 41

ФОРМУЛЫ = КОНЦЕНТРАТ МЫСЛИ





Формулы — это язык математики. Столетиями вырабатывались специальные обозначения, чтобы знающие люди могли передавать свои мысли, экономя на записях. Точно так же, как запись девятой симфонии Бетховена может перевести в музыку, задуманную композитором, новозеландский оркестр, математические формулы понимаемы в разных культурах.

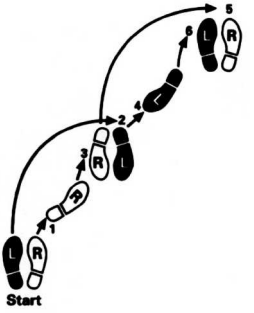
Как и нотная запись, математические формулы — изобретение современное. Нынешним студентам-математикам было бы сложно извлечь математическое содержание из работы Адама Ризе, написанной в шестнадцатом веке. Когда он писал об алгебре, он не использовал формул. Вместо этого все свои вычисления он записывал «прозой», которую нам в двадцать первом веке читать очень сложно.

Утверждение о том, что соотношение $3 \cdot x + 5 = 26$ выполняется для некоторого числа x, в одной из книг Ризе записывается следующим образом:

Возьми число и утрой его. Затем прибавь 5 *и получишь* 26. *Как велико число*?

Интересен и приведенный метод решения. Ризе берет наугад два различных значения для x и подставляет их в выражение, т. е. оба раза вычисляет $3 \cdot x + 5$. В зависимости от того, получились ли слишком большие или слишком маленькие результаты, и насколько «слишком», эти угаданные значения интерполируются, чтобы получить точное значение x.

Использование способов записи, разработанных с целью передавать идеи, присуще не только математике или музыке. Возможно, кто-то знаком со специальной нотацией танцевального шага, со способами записи шахматных



ходов, химическими формулами или с обозначениями на чертежах. Те, кто пользуется такими обозначениями, согласятся, что они упрощают коммуникацию. Даже в процессе творчества полезно подчеркнуть самое важное специальными обозначениями. Конечно же, насколько быстро удается понять, что именно выражает та или иная формула, зависит от уровня математической подготовки, но то же самое можно сказать и о музыкальных обозначениях, шахматных, и т. д.

И наконец, следует подчеркнуть, что никто из математиков не считает, что формулы заключают в себе основное содержание математики. Они просто средство записи и передачи идей. Точно так же для музыкантов способность воспринимать музыку — вовсе не то же самое, что умение читать и записывать ноты.

АЛГЕБРА ОСВОБОЖДАЕТСЯ ИЗ-ПОД ОПЕКИ ГЕОМЕТРИИ

Путь к современной системе обозначений в истории математики был достаточно долгим. Представьте себе, что в средние века кому-то потребовалось выразить мысль, что нужно найти такое число x, что $x^3 = 5$, например, если нужно было найти ребро куба объемом 5. Это можно было сделать только прозой: «Какое число, умноженное на себя трижды, дает 5?» Только вообразите, насколько трудно было выражать более изощренные действия, такие как вычисления сложных процентов.

Первый важный шаг к улучшенной системе обозначений был сделан во время итальянского Возрождения. В восемнадцатом веке был разработан стандарт, которым мы пользуемся до сих пор. В то время были даны имена самым важным математическим постоянным. В 1731 г. Эйлер ввел символ e для основания натуральных логарифмов[1)]. Из Англии пришла идея обозначать отношение длины окружности к диаметру, используя символ π, возможно

[1)] См. гл. 42.

потому, что греческая буква π соответствует латинской P, которой обозначают периметр[1)].

И еще одна проблема сдерживала развитие математических обозначений. До нашего времени почти все вычисления были ориентированы на геометрию. Выражения вроде x^5 или $x^3 + x$ считались лишенными смысла; первое — потому что не бывает пятимерных объектов, второе — потому что в нем складывают трехмерный объем x^3 и одномерную длину x, а это все равно, что складывать яблоки с грушами.

При Декарте математика перестала быть рабой геометрических интерпретаций. Математические результаты обрели новые применения. В наши дни задачи формулируются и решаются для тысяч переменных, например при оптимизации графика движения транспорта. И никому даже в голову не приходит, что еще пару столетий назад выражение x^5 было сложным для понимания.

[1)] Длина окружности — это специальное название для периметра круга.

Глава 42
БЕСКОНЕЧНЫЙ РОСТ

Инвесторам сейчас трудно, поскольку процентные ставки рекордно низки. Представьте себе банк в банановой республике, предлагающий баснословную процентную ставку 100%: через год вклад в один евро превращается в два. У вашей подруги Марии есть блестящая идея — извлечь всю выгоду из такой ситуации[1]. Она снимает свой вклад через полгода, получив 1,5 евро, и тотчас же снова вкладывает эти деньги. Еще через полгода она опять снимает вклад, и теперь у нее уже 2,25 евро. Если бы Мария снимала и перекладывала вклад чаще, четырежды в год, то в конце года у нее была бы более внушительная сумма в $1{,}25 \cdot 1{,}25 \cdot 1{,}25 \cdot 1{,}25 = 2{,}44$ евро. Марии интересно, как много можно получить, если играть в игру с перекладыванием денег еще чаще: ежедневно, или ежечасно, или даже ежесекундно.

Как ни удивительно, все более частое перекладывание денег не приводит к большей финансовой выгоде. Есть предел суммы, которая может быть получена таким образом. Это предельное число, до которого может увеличиться первоначальный вклад, — знаменитое число $e = 2{,}7182\ldots$.

Если обыватели ежедневно сталкиваются с цифрами $0, 1, 2, 3, \ldots, 9$, то математикам постоянно попадается число e, причем в самых неожиданных местах. В паре с π это самые важные числа в математике. Число e всегда прячется где-то рядом, когда речь идет об экспоненциальном росте (вспомните о бактериях) или о скорости радиоактивного распада (уран-235). Оно часто встречается и в теории вероятностей, в формуле для знаменитой колоколообразной кривой.

[1] Мы собираемся предположить, что банки чрезвычайно любезны с клиентами, и тем, кто забирает вклад досрочно, выплачивают соответствующую долю полагающихся процентов.

КАКОГО ЖДАТЬ ДОХОДА?

Следующая таблица демонстрирует поразительный факт, что, хотя увеличение частоты перекладывания вкладов ведет к увеличению дохода, есть предел суммы, которую можно получить таким образом. В первой строке стоит число периодов, на которые разбит год, т. е. сколько раз в году перекладывают вклад, а во второй — баланс в конце года; мы продолжаем считать, что банк предлагает ошеломляющую ставку — 100%.

Число n учета процентов	1	2	5	10	50	100
Баланс в конце года	2,000	2,250	2,488	2,594	2,692	2,705

С ростом n баланс в конце года приближается к числу $e = 2{,}718281828459045\ldots$.

ЭКСПОНЕНТА

Число e можно получить и по-другому. Описывая простейшую модель роста населения, приходят к задаче: *найти функцию, обладающую следующими свойствами*:

- Функция f должна иметь заранее заданное значение в 0. Подходящей нормировкой можно добиться, чтобы это значение было равно 1.
- Функция должна быть *дифференцируемой*. Это означает, что можно однозначно судить о скорости роста функции в каждой точке, а у ее графика не должно быть изломов.

Если скорость роста функции в точке x обозначить $f'(x)$, то должно выполняться соотношение

$$f'(x) = f(x).$$

В частности, это означает, что чем больше значение функции, тем быстрее она растет (см. рис. 42.1).

Для моделей роста населения это соотношение должно выполняться, поскольку ожидается, что с ростом населения

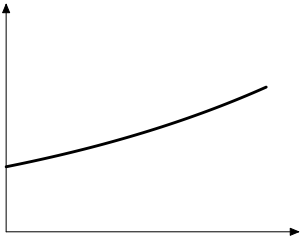


Рис. 42.1. Экспонента

скорость его роста тоже должна расти: ведь в большей популяции больше способных к воспроизводству пар.

Замечательно, что есть только одна функция, обладающая всеми этими свойствами, а именно функция, которая каждому числу x ставит в соответствие e^x. Поэтому число e можно задать следующим образом:

- На первом шаге установить, что описанная выше функция f действительно единственна.
- Затем определить число e как значение этой функции в точке $x = 1$. Поскольку $f(1) = e^1 = e$, мы действительно получаем желаемое число.

Преимущество этого метода заключается в том, что сразу же открывается важная область приложений числа e. Каждый раз, когда моделируют процесс роста или убывания (бактерий, радиоактивного распада и т. д.), возникают функции вида e^{ax}. Здесь a — число положительное, когда популяция растет, и отрицательное, когда уменьшается.

На рис. 42.2 и 42.3 представлены два типичных примера.

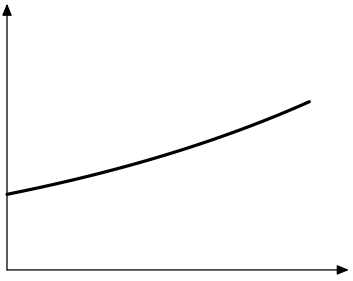


Рис. 42.2. Функция e^{ax} при $a > 0$: рост населения

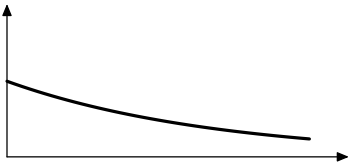


Рис. 42.3. Функция e^{ax} при $a < 0$: радиоактивный распад

В первом примере размер популяции (скажем, число жителей некоторой страны) описывается как функция от времени, а во втором моделируется количество радиоактивной субстанции в радиоактивно зараженном здании.

Глава 43

КАК КВАНТЫ ВЫЧИСЛЯЮТ?

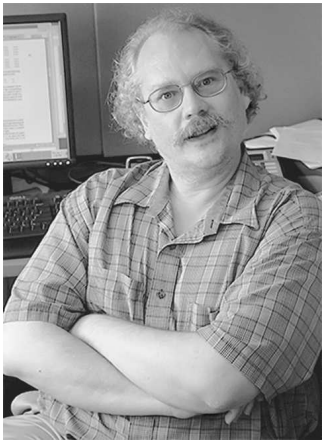
Несколько лет тому назад было много разговоров о квантовых компьютерах, а потом на этом фронте наступило затишье. Если бы удалось сделать такие компьютеры достаточно сложными, они, казалось бы, могли проявлять невероятные чудеса в вычислениях. Однако сейчас какой бы то ни было оптимизм в отношении таких компьютеров угас.

Тем не менее проводились интенсивные исследования возможностей квантовых вычислений. Ситуация напоминает сложившуюся в предыдущем столетии, когда до запуска первой космической ракеты было много рассуждений о том, что было бы, если бы были возможны космические путешествия.

В основе квантовых компьютеров лежат некоторые законы наномира, значительно отличающиеся от нашего повседневного опыта. В частности, согласно законам квантовой механики при взаимодействии квантовых систем вероятности того, что должно быть измерено в конце, могут находиться в суперпозиции контролируемым образом. Если преобразовать математическую задачу так, что решение может быть представлено на квантовом компьютере, то можно было бы работать с различными суперпозициями параллельно, так как количество возможностей экспоненциально растет с числом строительных кубиков, так называемых *квантовых битов* или *кубитов*.

К сожалению, есть много трудностей на пути создания квантового компьютера. Например, самые замечательные свойства квантового мира могут использоваться, только если система весьма серьезно защищена, ведь нарушить вычисления может любая заблудшая частица, например залетевшая из космоса. Кроме того, есть, по-видимому, непреодолимые проблемы с программированием: если промежуточные вычисления требуют некоторого результата, он

вначале должен быть закодирован. Но в квантовом мире каждое измерение изменяет состояние системы, причем первоначальное состояние не может быть восстановлено. Так что существует лишь небольшое число интересных математических вопросов, к которым применим данный метод. Обычно в математике требуются ответы, которые истинны всегда, а не с определенной вероятностью.



Одним из примеров, когда можно пытаться получить решение, является расшифровка секретных кодов. Действительно, интерес к квантовым компьютерам возрос, когда американец Питер Шор (это он на фотографии) разработал квантовый алгоритм для разложения больших чисел на простые множители, который был бы полезен для взлома кода RSA[1)]. За эту работу в 1998 г. Питер Шор был награжден премией Неванлинны на международном математическом конгрессе в Берлине.

ЧТО ТАКОЕ КУБИТ?

Самое важное понятие, связанное с квантовыми вычислениями, — это квантовый бит, или кубит. Термин должен напоминать нам о битах обычных компьютеров, где бит — единица хранения информации, которая может принимать одно из двух значений; обычно считают, что это нуль и единица. Для проведения сложных вычислений задействуют миллиарды битов.

Кубит — это квантовый аналог бита. Кубит можно представлять себе как черный ящик, который, получив запрос, отвечает нулем или единицей. Известны вероятности, с которыми ящик возвращает каждое из двух значений. В этом смысле «классический» бит — это специальный

[1)] О криптографии с открытым ключом можно почитать в гл. 7, а в гл. 23 можно найти подробности об алгоритме RSA.

кубит, о котором известно наверняка, что получится на выходе — нуль или единица.

Вероятностное определение отражает тот факт, что наномир управляется вероятностью, а не достоверностью. И только измерения определяют, которое из двух возможных значений конкретно реализовано.

Однако изображение кубита как черного ящика не подходит для описания взаимодействий множества кубитов. Для более четкой картины мы должны представить, что вероятность единицы или нуля на выходе определяется парой стрелок на плоскости. Квадрат длины стрелки с меткой 1 дает вероятность того, что на запрос будет дан ответ единица. Например, если длина стрелки с меткой 1 равна 0,8, то вероятность единицы равна $0{,}8 \cdot 0{,}8 = 0{,}64$. При этом вероятность нуля, разумеется, равна $1 - 0{,}64 = 0{,}36$, и длина стрелки с меткой 0 должна быть равна 0,6 (поскольку $0{,}6 \cdot 0{,}6 = 0{,}36$). На рис. 43.1 изображен кубит, для которого вероятности нуля и единицы примерно равны, так что можно считать, что он представляет собой монету, которую бросают, чтобы определить, что должно быть на выходе — 0 или 1.

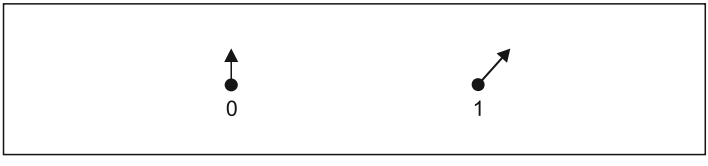


Рис. 43.1.

При взаимодействии двух кубитов их стрелки складываются по правилу сложения векторов[1)]. Так, два кубита с большими вероятностями единицы, направленными

[1)] Если при таком сложении получаются векторы, сумма квадратов длин которых не равна единице, то эти векторы нужно «нормировать», то есть умножить на число, чтобы по-прежнему можно было интерпретировать длины как вероятности. Например, если сумма векторов дает пару кубитов, для которых стрелки, соответствующие 0 и 1, имеют длины 0,3 и 0,4 соответственно, так что сумма квадратов равна $0{,}3 \cdot 0{,}3 + 0{,}4 = 0{,}25$, придется умножить каждый вектор на число $1/\sqrt{0{,}25} = 1/0{,}5 = 2$. Такое

в разные стороны, могут дать в результате кубит с очень маленькой вероятностью возврата единицы.

Рассмотрим пример на рис. 43.2. Слева изображены два кубита, у которых стрелка 0 располагается выше стрелки 1, но сами цифры не указаны, чтобы не загромождать рисунок. В результате сложения получается кубит (справа от знака равенства), который почти наверное возвращает нуль.

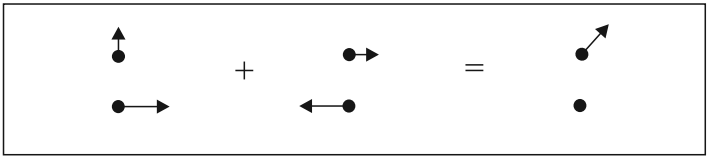


Рис. 43.2.

Именно этот принцип лежит в основе работы (все еще гипотетического) квантового компьютера. Чтобы ответить на некоторый вопрос, нужно задать его правильно запрограммированному квантовому компьютеру. Теоретически будет произведено огромное количество возможных ответов, но вероятности отдельных результатов устанавливаются таким образом, что вероятность выбора нужного результата, очень велика. Это технически сложно, и такие задачи все еще далеки от решения с помощью квантовых методов.

Огромные порядки задействованных величин происходят от взаимодействия кубитов. Допустим, что их два: Q_1 и Q_2. Каждый из них может принимать значения 0 или 1, так что всего имеется четыре возможности: 00, 01, 10, 11. Если понимать Q_1 и Q_2 как квантово-механическую систему, то имеется *четыре* соответствующие вероятностные стрелки. Например, если стрелка 00 особенно коротка, то вероятность того, что оба кубита одновременно окажутся в состоянии 0, крайне мала. В реалистичных криптографических приложениях понадобится несколько тысяч кубитов, которые дадут количество состояний, выражаемое числом с несколькими *тысячами* цифр. Это далеко превосходит современные технические возможности.

нормирование дает векторы длиной 0,6 и 0,8; и действительно, $0{,}6 \cdot 0{,}6 + 0{,}8 \cdot 0{,}8 = 0{,}36 + 0{,}64 = 1$.

Неудивительно, что тема «квантового компьютера» стала довольно обыденной. Вы не раз прочитаете, что теперь, обладая кубитами, можно действительно защитить закодированную информацию, применив настоящие квантово-теоретические факты. Но ее расшифровка оказывается бесполезной.

Достаточно заглянуть в гл. 6, чтобы в этом убедиться.

Там было проиллюстрировано, какое гигантское число 2 ^64. Однако здесь речь идет о 2 ^2000 состояниях, если вы хотите решать реальные криптографические задачи ...

Глава 44
КРАЙНОСТИ!

Какая скорость вращения приводит к наилучшей работе мотора? Как следует устроить лыжный трамплин, чтобы прыжок был как можно длиннее? Столетиями создавался зоопарк методов, позволяющих отвечать на такие вопросы про «самое большое» или «самое маленькое».

В простейших случаях в задачу входит конечное, сравнительно небольшое число вариантов выбора. Тогда можно просто перепробовать все возможности и выбрать самую подходящую. Все сложнее, когда нужно оптимизировать несколько непрерывно меняющихся параметров; например, при изучения расстояния, на которое улетает мяч, в зависимости от угла бросания.

Читатели, изучавшие математический анализ, могут вспомнить, что уже встречались с такими задачами. Для их решения нужно было взять производную подходящей функции, приравнять ее к нулю и решить уравнение относительно нужного параметра. Заметим, что этот метод позволяет решить задачу, в которой бесконечно много случаев (поскольку параметр изменяется непрерывно) с помощью одного только уравнения, и поэтому требует конечного времени. Этот удивительный факт был отмечен несколько веков тому назад; он и подтолкнул развитие дифференциального и интегрального исчислений.

Для случая, когда одновременно рассматриваются несколько параметров, принципиальных отличий нет. Все опять сводится к решению уравнений (хотя теперь они сложнее). С помощью современных высокоскоростных компьютеров теперь можно справиться с гораздо более сложными задачами, чем несколько десятилетий назад.

Но иногда возникают совершенно новые идеи. Не так давно в моде был метод имитации отжига[1)]. Представьте себе, что в густом тумане путешественник ищет самую

[1)] См. также гл. 60.

высокую вершину в округе. Он все время по возможности направляется вверх, но чтобы его путешествие не завершилось на невысоком холме, он иногда спускается вниз.

Нужно заметить, что математике можно предоставить решение задач, но не постановку целей. Решение задачи об оптимизации работы мотора в первом примере будет зависеть от того, чего нужно добиться: нужен ли самый мощный, самый экономичный, или самый экологичный мотор.

ТИПИЧНАЯ ЗАДАЧА ОБ ЭКСТРЕМАЛЬНЫХ ЗНАЧЕНИЯХ

Представьте себе, что вы путешествуете на велосипеде через Гарц. Вы выезжаете из отеля рано утром и возвращаетесь вечером. В наивысшей точке вашего путешествия велосипед располагается строго горизонтально. Действительно, если бы переднее колесо было выше заднего, впереди был бы подъем, а если ниже — то спуск.

Именно на эту идею опирается подход к решению задач об экстремальных значениях. Когда достигается максимум, то крутизна (или *наклон*) кривой должна быть равна нулю. Пользуясь терминологией гл. 13, можно сказать, что нулевой наклон — *необходимое* условие существования экстремального значения.

Чтобы воспользоваться этим знанием для *практического* вычисления экстремальных значений, нужны формулы для выражения наклона кривой. Эта необходимость оказалось одним из сильнейших импульсов для развития современной математики, а именно, *математического анализа*, независимо изобретенного Лейбницем и Ньютоном.

Рассмотрим пример: где функция $-x^2+6x+10$ достигает наибольшего значения? На рис. 44.1 видно, что график функции сначала поднимается, а затем опускается.

Но в какой же точке он достигает максимума? Воспользовавшись правилом нахождения производной, которое мы здесь обсуждать не будем, узнаем, что наклон в точке x задается выражением $-2x+6$. А оно обращается в нуль в точке $x = 3$. Поэтому максимальное значение тоже достигается в этой точке. (Решая такие задачи, нужно быть внимательным, чтобы случайно не спутать минимум

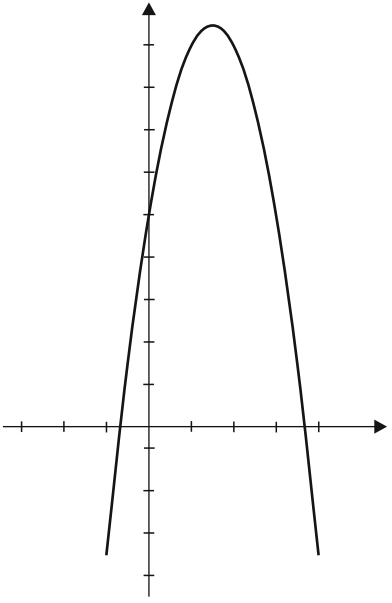


Рис. 44.1. Функция $-x^2 + 6x + 10 = y$

и максимум. В конце концов, велосипед располагается горизонтально не только в наивысшей, но и в самой низшей точке путешествия.)

Глава 45
БЕСКОНЕЧНО МАЛЫЕ?

Бесконечно малые величины расцвечивают математический пейзаж уже несколько веков. Они терроризировали всех, кто стремился установить всю математику на таком же прочном основании, какое было у алгебры и геометрии.

Бесконечно малые величины увидели свет в семнадцатом веке, когда они понадобились для развивающихся интегрального и дифференциального исчислений. Ньютон и Лейбниц независимо развили два подхода, и ни один из них не мог обойтись без «бесконечно малых».

Но что они должны были значить? Если число x положительно, то должно существовать еще меньшее число (например, $\frac{1}{2} \cdot x$). Поэтому наименьшего положительного числа не существует. Однако можно пойти по неверному пути, рассматривая все более мелкие величины.

Например, рассмотрим дугу окружности. Если мы зафиксируем точку на дуге и рассмотрим включающую эту точку часть дуги при все большем и большем увеличении, эта часть будет все больше и больше походить на отрезок, так что захочется удостовериться, правда ли, что в пределе она превратится в обыкновенный прямолинейный отрезок. Тогда можно было бы сказать, что на уровне бесконечно малых окружность *является* прямой линией.

Именно так рассуждал Лейбниц, когда переходил от кривых к касательным. Несмотря на то что его аргументации недоставало четкости, он смог сделать много интересных и полезных выводов. Многие из математиков — его современников — скептически относились к таким построениям, и только в девятнадцатом веке основания математического анализа были развиты в такой мере, что стало возможно отбросить понятие бесконечно малой (и бесконечно большой) величины. Здесь важную роль сыграл берлинский математик (здесь мы позволим автору,

тоже жителю Берлина, проявить местный патриотизм) Карл Теодор Вильгельм Вейерштрасс.

Исчезновение бесконечно малых никто не оплакивал. В частности, теперь новичкам в математике живется легче, им больше не нужно оперировать с такими туманными понятиями, овладевая основами математического анализа. Хотя никто не ожидает ренессанса бесконечно малых, несколько десятилетий назад была предпринята попытка такого ренессанса под названием *нестандартный анализ*. Но строгая проработка его понятий еще сложнее, чем любой другой подход к секретам дифференцирования и интегрирования.

МИР ЭПСИЛОН

Как же математики работают с бесконечно малыми в наши дни? В качестве примера рассмотрим последовательность чисел, обратных натуральным, т. е. $1, \frac{1}{2}, \frac{1}{3}, \ldots$. Интуитивно ясно, что эти обратные становятся «сколь угодно малыми» или «приближаются сколь угодно близко к 0».

Во времена Лейбница сказали бы, что эти обратные числа «постепенно обращаются в нуль», а сегодня такой оборот речи даже из уст абитуриента заслужил бы упрека. Расскажем, как строго формулировать идею бесконечно малых (осторожно: изложение становится несколько формальным).

ЗНАКОМСТВО С ε

Если дана последовательность положительных чисел $x_1, x_2, x_3, \ldots$, то говорят, что они *стремятся к нулю*, если числа постепенно становятся меньше любого положительного числа, как бы мало́ оно ни было. Точнее, для любого сколь угодно малого заданного числа ε (это греческая буква «эпсилон») существует номер n такой, что не только x_n, но и x_{n+1}, x_{n+2}, и все последующие числа в последовательности меньше ε. Чтобы установить такой факт, нужно только найти способ указывать подходящее значение n для любого заданного ε.

В нашем примере можно поступить так. Для заданного ε нужно найти такое значение n, что n больше $1/\varepsilon$. Например,

если $\varepsilon = 1/1000$, можно взять $n = 1001$. По правилам действий с неравенствами при этом n величина $1/n$ (и тем более $1/(n+1)$, $1/(n+2)$ и т. д.) меньше ε. Таким образом, мы установили корректность утверждения: «Числа, обратные натуральным, стремятся к нулю».

Общепризнанно, что это определение плохо усваивается с первого подхода. Это мнение относится ко всем, кому приходится усвоить его в первом семестре, где бы они ни изучали математику. В этом определении важно то, что оно делает корректным первоначально туманное важнейшее понятие, и в силу этого дальнейшие математические утверждения можно формулировать строго.

НЕСТАНДАРТНЫЙ АНАЛИЗ

В разделе математики под названием «нестандартный анализ», развитой в 1960 гг., числа представляют таким образом, что любое «классическое» число окружено «облаком» других неизмеримо близких к нему чисел. Числа, близкие к классическому нулю, называются *инфинитезимальными*.

В этом новом царстве чисел выполняются обычные правила: можно складывать и умножать, порядок сложения роли не играет и т. д. Нужно только привыкнуть к некоторым странным свойствам понятий «больше» и «меньше»: теперь не верно, что каждое число меньше какого-либо натурального числа $1, 2, 3, \ldots$.

Если привыкнуть к этому новому миру чисел, то многие вещи, с которыми новичкам обычно сложно разобраться, становятся очень простыми. Например, наклон функции — это больше не предел, как это обычно считается, а просто отношение прилегающей и противоположной сторон инфинитезимального треугольника, так же, как это представлял себе Лейбниц.

Однако, несмотря на такие преимущества, нестандартный анализ останется на полях истории математики. Чтобы понять, как этот подход основывается на прочном аксиоматическом фундаменте, нужно несколько лет учебы. Но числа и их свойства не могут ждать так долго: они нужны уже в первые недели первого семестра.

Глава 46

МАТЕМАТИКА В ПОЖАРНОЙ ЧАСТИ

Сегодня мы еще раз увидим, как можно математически смоделировать повседневный опыт. Мы рассмотрим такую задачу: как избежать некорректных решений, устанавливая процедуру выбора возможных откликов на данную ситуацию.

Типичный учебный пример процедуры принятия решения описывает действия оператора пожарной части, получившего телефонный звонок о том, что горит местная школа. Судя по голосу, звонивший был пьян. Какие действия должны быть предприняты в пожарной части? Продолжить партию в домино, рискуя, что школа сгорит дотла? Или направить четыре пожарные машины, хотя звонок был очень похож на розыгрыш?

Абстрактная теория, лежащая в основании этой задачи, заключается в том, что в нашем восприятии мира мы допускаем два вида ошибок. (Математики называют их ошибками первого и второго рода.)

(1) Мы верно воспринимаем происходящее, но делаем неверные выводы.

(2) Мы считаем гипотезу верной, хотя на самом деле она неверна.

Это звучит довольно абстрактно. Но каждый день в газетах или в повседневной практике мы встречаем ситуации, когда должны избежать таких ошибок. Стоит ли игнорировать ночью красный сигнал светофора (предположение: поблизости нет полицейских)? Как отнестись к идее познакомиться с хорошенькой девушкой, явившейся

на дискотеку с подозрительным типом (предположение: он приходится ей братом)?

Эволюция научила нас оценивать такие ситуации за доли секунды. Но оценки эти в большой мере зависят от нашего характера и жизненного опыта.

В математической статистике правильное оценивание ошибок составляет основу процедур принятия решений. Математика не в силах предупредить возникновение ошибок обоих родов, но можно попытаться так определить последствия принятия решений, чтобы минимизировать риски. Вот поэтому пожарные части отвечают на каждый сигнал, даже если «совершенно ясно», что он ложный.

ВСЕ БЕСПЛАТНО В ТЕАТР

Пример с пожарной частью — обычная иллюстрация ошибок двух родов. Но большинству из нас обычно не приходится сталкиваться с пожарами или с ложными вызовами, так что этот пример может показаться слишком абстрактным или нежизненным.

Поэтому хочется показать, как мы встречаемся с ошибками первого и второго рода в газетах. Например, не так давно появился репортаж о том, как департамент полиции Берлина прибыл в Немецкий театр из-за подозрения в массовых беспорядках. А на самом деле единственной причиной была стычка подвыпившего завсегдатая театра с другим зрителем. Пресса издевалась: «Полицейское государство! Неужели им больше нечем заняться?!» Предположение о массовых беспорядках оказалось неверным, и полицию обвинили в ошибке второго рода. Но что сказали бы журналисты, случись ошибка первого рода: «Люди бросались друг на друга! Куда смотрит полиция?!».

Еще более драматический пример появился 10 апреля 2006 года в берлинской газете «Daily mirror».

Операторы службы спасения не приняли всерьез звонок пятилетнего ребенка.

Поскольку звонок пятилетнего ребенка в службу 911 приняли за шутку, умерла его мать. Мальчик позвонил в службу спасения, когда она потеряла сознание. Но

ребенку велели прекратить играть с телефоном. Когда помощь, наконец, подоспела, было уже поздно.

Даже в личной жизни сложные решения подвержены ошибкам двух родов. Относительно гипотезы «Мне следует пройти ежегодную диспансеризацию» ошибка первого рода приведет к отказу от диспансеризации в предположении, что от нее больше вреда, чем пользы, хотя на самом деле если бы вы посетили доктора, то могли бы на раннем этапе выявить болезнь. Ошибку второго рода вы бы совершили, если бы, будучи совершенно здоровым, отправились на диспансеризацию и напрасно потеряли время и деньги.

Глава 47

ПЕРВОМУ ДОКАЗАТЕЛЬСТВУ УЖЕ 2500 ЛЕТ

Когда родилась математика? Это сложный вопрос. Все зависит от того, что понимать под математикой. Если имеют в виду способность справляться с простейшими вычислительными задачами, то рождение математики теряется где-то в темных доисторических веках. Уже во времена Вавилона и Древнего Египта проводились довольно изощренные вычисления. Сколько собрано пшеницы? Каким должен быть склон строящейся пирамиды?

Эти цивилизации разработали инструкции, как выполнять вычисления, необходимые для ответа на такие вопросы. Были разработаны приемлемые приближения числа π, а также открыто соотношение для прямоугольных треугольников, ныне известное как теорема Пифагора.

Историки математики обычно относят ее появление к середине первого тысячелетия до н. э. Тогда греческие математики перестали довольствоваться эмпирическими правилами и образцами вычислений. Им хотелось добраться до сути вещей, чтобы установить философское основание истины. Именно тогда появились первые доказательства, одним из самых ранних тому примеров служит теорема Фалеса: если вершина треугольника располагается на полуокружности так, что диаметр ее является самой длинной стороной треугольника, то треугольник прямоугольный (рис. 47.1). И это всегда правда, что можно доказать, основываясь на простых предположениях.

Тот способ рассуждения, который применялся при формулировке теоремы Фалеса, достиг наивысшей точки в «Началах» Евклида. В них были собраны все геометрические знания, известные в то время, и была дана модель построения науки, вызвавшая множество подражаний. Вначале идут очевидно истинные утверждения (аксиомы), а уже из них строго логически выводится все остальное. Точно так же, например, построена физика Ньютона;

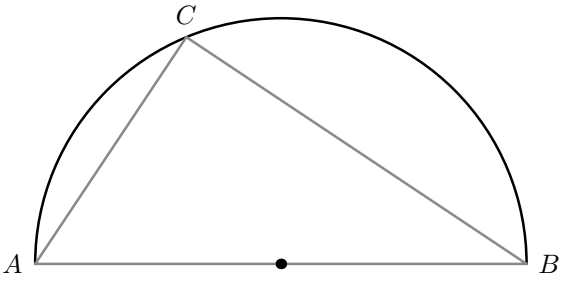


Рис. 47.1. Теорема Фалеса: угол C равен 90°

и даже Кант считал такой подход достойным подражания: «В любом частном учении о природе можно найти науки в собственном смысле лишь столько, сколько имеется в ней математики» (И. Кант. «Критика чистого разума»).

Такой «доказательный поиск истины», впервые осуществленный греческими математиками, привел к заметному успеху. В последние годы выяснилось, что все больше и больше явлений в нашей жизни могут быть описаны фактами, открытыми ранее математиками. Во времена Ньютона все было довольно просто: можно было ограничиться только векторами и функциями. Однако в наше время специалисты не могут обойтись без искривленных пространств, тензоров и вероятностных распределений.

Почему так происходит — вопрос открытый. Был ли Господь Всемогущий математиком? Или мы в состоянии понять только то, что поддается методам, имеющимся в нашем распоряжении? Эти вопросы второстепенны для математиков. Их пленяют и удовлетворяют поиски истин, которые останутся истинными навсегда.

ПОЛУОКРУЖНОСТИ И ПРЯМЫЕ УГЛЫ

Теорема Фалеса — прекрасный пример того, как можно проверить математическую истину с легкостью, если посмотреть на ситуацию под правильным углом. Еще раз сформулируем теорему (рис. 47.1).

Рассмотрим полуокружность над диаметром. Концы диаметра обозначим A и B. Теперь, если C — произвольная

точка на полуокружности, то треугольник ABC — прямоугольный с прямым углом C.

Доказательство начнем с того, что проведем вспомогательный отрезок, соединяющий центр окружности M и точку C, как показано на рис. 47.2.

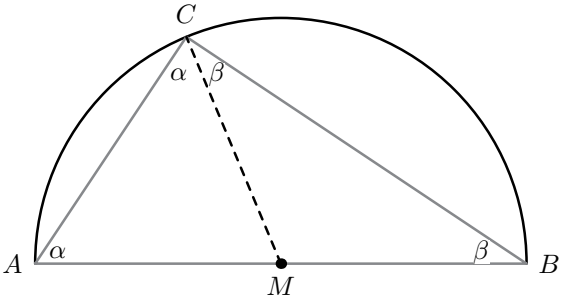


Рис. 47.2. Теорема Фалеса: доказательство

В треугольнике AMC две стороны равны, поскольку AM и CM являются радиусами окружности. Поэтому в треугольнике AMC угол A равен углу C. Такая же ситуация с треугольником MBC: угол B равен углу C. Поэтому, как отмечено на рисунке, угол C исходного треугольника ABC равен $\alpha + \beta$. Далее, сумма углов A, B и C треугольника ABC должна быть равна 180°, т. е.

$$\alpha + \beta + (\alpha + \beta) = 180^\circ,$$

а это выражение можно упростить до $2 \cdot (\alpha + \beta) = 180^\circ$ или $\alpha + \beta = 90^\circ$. Поэтому величина угла C равна 90°, что и требовалось доказать.

У теоремы Фалеса много приложений: например, можно доказать, что при помощи циркуля и линейки можно построить квадратный корень некоторого числа. Это подробно описано в гл. 33.

Глава 48

В МАТЕМАТИКЕ ЕСТЬ ТРАНСЦЕНДЕНТНОЕ, ХОТЯ НЕТ НИЧЕГО МИСТИЧЕСКОГО

Математики часто заимствуют термины в других областях и используют их так, что от первоначального значения ничего или почти ничего не остается. Непосвященных это озадачивает.

Так, часто считают, что трансцендентные числа имеют какое-то отношение к мистике и секретам нумерологии. И конечно же, многие нематематики очарованы числом π именно потому, что оно трансцендентно.

Чтобы понять, что такое трансцендентные числа, нужно разобраться с базовыми понятиями в иерархии чисел. Нам для начала достаточно обратиться к дробям, таким как $\frac{3}{8}$ и $-\frac{7}{19}$. Такие числа называются *рациональными*, а термин этот происходит от английского «ratio» — отношение (а не от латинского «ratio» — разум).

Для большинства повседневных задач рациональных чисел достаточно. Но для тех, кто интересуется точной математической теорией, без таких чисел, как π и квадратные корни, не обойтись.

Числа, которые не являются рациональными, называются, разумеется, *иррациональными*. Математика полна такими числами. Некоторые из них особенно просто описать. Они называются *алгебраическими*. Как даже неспециалисту видно из названия, эти числа как-то связаны с алгебраическими операциями: сложением, вычитанием, умножением и делением.

Числа, которые не являются алгебраическими, называются *трансцендентными*. Одних алгебраических методов для работы с такими числами недостаточно. Они часто возникают как предельные значения в тех или иных математических конструкциях.

И что теперь? Подробное изучение иерархии чисел привело к наглядным результатам. Самый известный из них — это, конечно же, доказательство невозможности квадратуры круга. Доказательство основано на том, что с помощью циркуля и линейки можно построить только относительно простые (а именно, некоторые алгебраические) числа, а для квадратуры круга требуется строить трансцендентные. Само их существование не было доказано до девятнадцатого века, так что неудивительно, что с задачей не могли справиться две тысячи лет.

ИЕРАРХИЯ ЧИСЕЛ

Трансцендентные числа — самые сложные в *иерархии чисел*, которая встречается в некоторых главах этой книги. Здесь мы опишем ее систематически.

Натуральные числа. Это самые простые числа 1, 2, 3, ... Еще в детстве усваивается понятие «число», и даже дошколята справляются с простейшими вычислениями.

Следует знать:

(1) При аксиоматическом построении натуральных чисел, в наши дни обычно начинают с *аксиом Пеано*. Они гласят, что в множестве натуральных чисел есть первое число и что всегда можно «продолжить счет». Очень важна аксиома индукции: верно любое утверждение, которое истинно для значения 1 и для которого можно доказать, что из его истинности для значения n следует истинность для значения $n+1$ (см. гл. 34).

(2) Множество натуральных чисел обычно обозначают $\mathbb{N}$ (от слова *Natural*).

Целые числа. Если рассмотреть все возможные разности натуральных чисел, то получим множество *целых чисел*. Так, целыми числами являются 3, 0, -12, поскольку

их можно получить, например, как разности $5-2$, $4-4$ и $2-14$. Целые числа полезны для простых вычислений в бизнесе, поскольку позволяют бухгалтерам записывать и дебет (отрицательные числа) и кредит (положительные).

Следует знать:

(1) Множество целых чисел обычно обозначают $\mathbb{Z}$ (Z — первая буква немецкого слова «Zahl», число).

(2) Каждое натуральное число — целое, но обратное неверно.

(3) Суммы, произведения и разности целых чисел — тоже целые. Но о частных этого сказать нельзя: хотя $44/11$ — целое число, $3/2$ — нет.

Рациональные числа. Число называется *рациональным*, если его можно записать в виде частного m/n, где m — целое, а n — натуральное число. Примеры: $33/12$ и $-1111/44$.

Следует знать:

(1) Множество рациональных чисел обычно обозначают $\mathbb{Q}$ (Q — первая буква английского слова «quotient» — частное).

(2) Если m — целое число, то его можно (хотя выглядит это несколько искусственно) записать в виде $m/1$. Поэтому целые числа являются рациональными.

Иррациональные числа. Числа, которые не являются рациональными, называются *иррациональными*. Для древнегреческих математиков было потрясением, когда они обнаружили существование таких чисел. Самый известный пример иррационального числа — квадратный корень из 2, о нем мы еще будем говорить в гл. 56. Для иррациональных чисел нет специального обозначения.

Алгебраические числа. Представьте себе игру. Первый игрок, Фердинанд, выбирает некоторое число x, а второй, Изабелла, пытается сделать из него нуль, пользуясь натуральными числами и символами $+, -, \cdot, \div$. При этом

число x может встречаться сколько угодно раз. Если Изабелле удастся дать подходящую формулу, которая дает нуль, то она выигрывает. В противном случае она проигрывает.

Вот несколько примеров.

- Фердинанд выбрал $x = 17$. Изабелла с легкостью выигрывает, предложив формулу $x - 17 = 0$. На самом деле, если Фердинанд выбирает натуральное число, Изабелла всегда может выиграть.
- На этот раз Фердинанд пытается остановить Изабеллу с числом $x = 21/5$. Но Изабелла не теряется. Она выдает формулу $5 \cdot x - 21 = 0$, и это доказывает, что x можно превратить в нуль согласно правилам. Изабелла всегда может выиграть, если x — рациональное число.
- Фердинад достает козырную карту — предлагает $x = \sqrt{2}$. Поразмыслив немного, Изабелла выдает $x \cdot x - 2 = 0$ — как раз то, что надо! Так что число $x = \sqrt{2}$ тоже можно превратить в нуль.

Числа x, которые можно таким образом преобразовать в нуль, называются *алгебраическими*. Мы видели в игре Фердинанда и Изабеллы, что целые, дроби и квадратный корень из 2 — алгебраические числа.

Трансцендентные числа. И наконец, те, кто знаком с алгебраическими числами, легко разберется, что такое трансцендентные числа. А именно, число называется *трансцендентными*, если оно не алгебраическое. Итак, число x — трансцендентное, если Изабелла (или кто-то другой) не в состоянии превратить x в нуль согласно описанным выше правилам, какой сложной ни была бы формула.

Важно отметить разницу между тем, как приходится доказывать, что число алгебраическое и что оно трансцендентное. Чтобы доказать, что число алгебраическое, нужно придумать формулу и доказать, что она превращает число в нуль. Чтобы доказать, что число трансцендентное, придется доказывать, что нуль никак нельзя получить ни

с какой формулой, какой бы сложной и длинной она ни была, протянись она хоть до Солнца.

Ясно, что доказать несуществование гораздо сложнее существования, и, действительно, только в середине девятнадцатого столетия удалось строго доказать трансцендентность некоторого числа.

Трансцендентны некоторые очень важные числа в математики. Самые известные из них — основание натуральных логарифмов e и число π (см. гл. 16 и 42).

Глава 49

КАЖДОЕ ЧЕТНОЕ ЧИСЛО РАВНО СУММЕ ДВУХ ПРОСТЫХ?

В этой книге мы часто писали о простых числах (это числа 2, 3, 5, 7, 11, ..., которые делятся только на себя и на 1). Хотя эти числа легко описать, с ними связаны некоторые очень сложные задачи. Одна из них оставалась неразрешенной на протяжении столетий. Это гипотеза Гольдбаха.

Христиан Гольдбах (1690–1764) был дипломатом и интересовался математикой. В 1742 г. он сообщил свою задачу великому математику Эйлеру. Гипотеза Гольдабаха легко формулируется.

Верно ли, что каждое четное число, большее 3, *можно записать в виде суммы двух простых чисел?*

Разберемся, что это значит. Рассмотрим четное число 30. Действительно, его можно записать в виде $7 + 23$, и оба числа 7 и 23 просты. Но число 30 можно представить в виде суммы двух простых и по-другому: $11 + 19$. И так обстоят дела для всех четных чисел, проверенных к настоящему моменту: их можно записать в виде суммы двух простых, и для больших чисел это можно сделать многими, многими способами.

В силу совершенно очевидных экспериментальных свидетельств казалось совершенно неприличным, что в математическом мире до сих пор нет доказательства этой гипотезы. Конечно же, такая теорема не имеет непосредственных приложений ни в какой области прикладной математики. Однако в этой книге мы уже показали, что математики вкладывают свои усилия не только в развитие методов, необходимых для приложений, но и для открытия общих законов в мире чисел, фигур и вероятностей.

Математиков пленяют задачи, долгое время не поддающиеся решению, которые бросили вызов великим умам прошлого. Не стоит забывать и о перспективе некоторой прибыли, поскольку за решение этой задачи назначена премия.

ВАЖНА ЛИ ГИПОТЕЗА ГОЛЬДБАХА?

Среди математиков нет согласия в том, насколько важна гипотеза Гольдбаха. Она, конечно же, интересна, потому что скрывает свой секрет уже на протяжении нескольких веков. Радость от ее решения сравнима только с радостью первых покорителей Эвереста или первого бегуна, пробежавшего стометровку меньше чем за десять секунд.

Чтобы осознать скептицизм в отношении значимости этой задачи, важно помнить, что простые числа определяются *мультипликативным* свойством: простое число нельзя записать в виде произведения двух меньших чисел. Более того, самый важный результат о простых числах связан с умножением: каждое натуральное число[1)] можно разложить на простые множители, и эти простые множители определяются единственным образом. А в гипотезе Гольдбаха речь идет о сумме простых чисел. Что, спросят критики, здесь интересного?

ЭКСПЕРИМЕНТАЛЬНАЯ ПРОВЕРКА

На рис. 49.1 горизонтальная ось представляет четные числа $z = 2, 4, 6, \ldots$, и над каждым таким числом z отмечена точка на высоте, которая соответствует числу способов, которыми z может быть представлено в виде двух простых. Например, выделенная точка в левой части графика расположена над числом 14 на высоте 2, поскольку число 14 можно записать в виде суммы двух простых чисел двумя способами: $3 + 11$ и $7 + 7$.

Гипотеза Гольдбаха эквивалентна утверждению о том, что на горизонтальной оси нет ни одного числа z такого, что точка над ним располагается на нулевой высоте. По виду графика можно предположить не только это. Хотя узор из точек представляется хаотичным, кажется, что даже для тех чисел z, у которых мало разложений на сумму двух простых (т. е. соответствующие точки располагаются внизу облака точек), график понемногу поднимается. Иначе говоря, не только каждое число должно быть представимо

[1)] Это числа 1, 2, 3, 4, ...

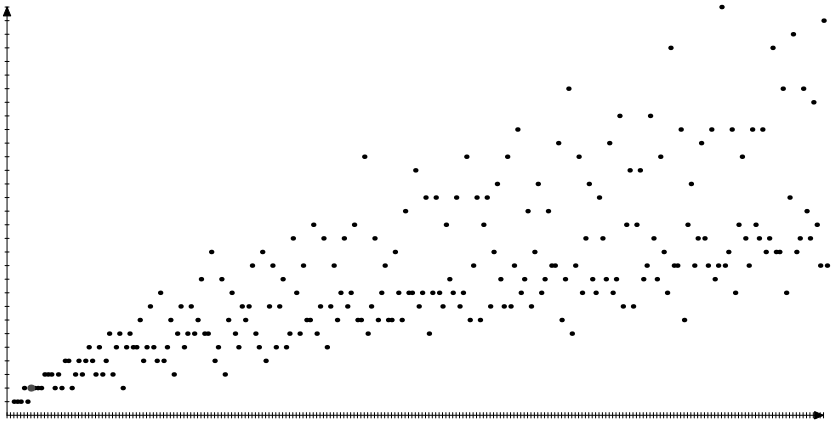


Рис. 49.1. Гипотеза Гольдбаха: первые 240 значений

в виде суммы двух простых, но даже число таких представлений должно быть сколь угодно большим для больших z.

«ДОКАЗАТЕЛЬСТВО» ГИПОТЕЗЫ ГОЛЬДБАХА

Гипотеза Гольдбаха — одна из тех знаменитых проблем, которые привлекали любителей математики. Однажды на факультет математики одного университета пришло письмо с таким «доказательством».

Во-первых, простых чисел бесконечно много[1)].

Во-вторых, при попарном сложении простых чисел получается бесконечно много сумм. Это и доказывает гипотезу Гольдбаха.

К сожалению, это доказательство никак нельзя назвать исчерпывающим. Конечно же, совершенно верно наблюдение о том, что бесконечно часто числа раскладываются в сумму двух простых, и этот факт доказан как нельзя лучше. Но отсюда далеко до доказательства, что *любое* число может быть представлено таким образом. Возможно, автор письма имел в виду следующее: если отметить

[1)] См. гл. 4.

бесконечно много элементов бесконечного множества, то они его исчерпают. Для конечных множеств это, безусловно так: если некто имеет пять конвертов и он наклеит пять марок на пять разных конвертов, то, конечно же, на каждом конверте окажется по марке. Но у бесконечных множеств другие законы, и поэтому гипотеза Гольдбаха до сих пор ждет своего доказательства (и предложенной за него награды).

Глава 50

ПОЧЕМУ МЫ НЕПРАВИЛЬНО ОБРАЩАЕМ УСЛОВНЫЕ ВЕРОЯТНОСТИ

Эволюция неплохо подготовила нас к оцениванию вероятностей. Мы умеем за доли секунды оценить ситуацию и решить: сыграть или удрать? Сбивать пламя или бежать в безопасное место? Мы также воспитываем в себе понимание того, что новая информация воздействует на вероятности некоторых событий. Например, даже если вы не знаете, интересуется ли классической музыкой ваша новая знакомая, вы, скорее всего, оцените шансы «за» ниже, если обнаружите, что она путает Шумана с Шубертом.

Эти довольно расплывчатые идеи можно выразить математически точно, используя понятие *условной вероятности*. В качестве математического примера рассмотрим вероятность выпадения четного числа при бросании правильной игральной кости. Она, конечно же, равна $\frac{1}{2}$. Однако если известно, что выпало простое число, то эта вероятность падает до $\frac{1}{3}$, так как между 1 и 6 только три простых числа — 2, 3, 5 — и только одно из них — 2 — четно.

В математике имеется формула, известная под названием *формулы Байеса*, которая позволяет обращать условные вероятности. Представьте себе бармена, которому по опыту известен процент посетителей, оставляющих чаевые. Допустим, в среднем это 40%, а для туристов это среднее увеличивается до 80%. Поэтому информация о том, что кто-то из посетителей — турист, увеличивает шансы на то, что он оставит чаевые. Формула Байеса позволяет сделать и обратный вывод: зная, что оставлены чаевые, можно вычислить вероятность того, что оставивший был туристом.

Впрочем, нельзя сказать, что вычисление вероятности получить чаевые — фундаментально важная задача. Однако те же самые методы применимы к гораздо более

важным вопросам. Знаменитый пример — эффективность медицинских тестов. Чему равна вероятность, что у меня определенная болезнь, если результат теста оказался положительным? Тех, кто имеет опыт получения положительного результата, можно утешить математически — эта вероятность гораздо меньше, чем подсказывает интуиция. Эволюция запрограммировала нас быть слишком пессимистичными в этом случае.

ТЕСТ НА КОРЬ

Мы уже говорили об условных вероятностях и формуле Байеса в гл. 14 (парадокс Монти Холла). Подчеркнем некоторые самые важные моменты.

- Если A и B — два возможных исхода случайного эксперимента, то $P(A|B)$ обозначает вероятность осуществления A, если известно, что произошло событие B. Например, пусть из стандартной колоды в 52 листа извлекают наугад карту. Обозначим A событие «валет пик», а B — «карта пик». Тогда вероятность A равна $1/52$, поскольку всего есть 52 карты, и с равными вероятностями может быть извлечена любая из них. Однако, если известно, что извлечена карта пик (осуществилось событие B), то вероятность валета пик увеличивается до $1/13$, поскольку в колоде 13 различных карт пик.
- В простейшем случае в формулу Байеса входят два события, A и B. Считается, что известна вероятность $P(B)$ того, что произойдет событие B, а также известны условные вероятности $P(A|\neg B)$ и $P(B|A)$[1]. Формула Байеса позволяет вычислить $P(B|A)$:

$$P(B|A) = \frac{P(A|B)P(B)}{P(A|B)P(B) + P(A|\neg B)(1 - P(B))}.$$

Теперь можно уточнить, о чем говорит наш медицинский пример, в котором речь идет о диагностике редкой болезни. Не будем вспоминать про СПИД или рак, пусть

[1] Здесь $\neg B$ обозначает событие, дополнительное к B (событие B не осуществляется). Так что если событие B — «карта пик», то $\neg B$ — «карта червей, бубен или треф».

это будет корь. Однажды утром у себя на лице вы обнаруживаете красноватую сыпь и немедленно хотите узнать, не заразились ли вы корью. Доктор назначает тест на корь, и его результат оказывается положительным. Больны вы или нет?

Обозначим A событие «тест на корь положителен», а B — событие «у меня корь». Чтобы воспользоваться формулой Байеса, нам нужно знать вероятности $P(B)$, $P(A|B)$ и $P(A|\neg B)$. Первая из них — вероятность того, что у взрослого человека есть корь. Среди взрослых это редкая болезнь, и мы можем положить $P(B) = 0{,}05$ или 5%.

Условная вероятность описывает надежность теста: чему равна вероятность того, что для больного человека тест дает положительный результат? Если бы тест был совершенным, эта вероятность была бы равна $1{,}0$ или 100%. Однако таких тестов не бывает, и можно только надеяться приблизиться к идеалу. Мы оптимистически положим эту вероятность равной $0{,}98$.

И наконец, нужно знать $P(A|\neg B)$ — вероятность того, что тест дает положительный результат, несмотря на то что вы здоровы. Было бы хорошо, чтобы это значение было равно нулю, но такая цель недостижима. Реалистично положить вероятность «фальшивого положительного» результата равной $P(A|\neg B) = 0{,}20$.

Теперь можно приступать к вычислениям. Мы хотим знать $P(B|A)$ — вероятность того, что при положительном результате действительно имеется заболевание. Воспользуемся формулой Байеса:

$$P(B|A) = \frac{P(A|B)P(B)}{P(A|B)P(B) + P(A|\neg B)(1 - P(B))} =$$

$$= \frac{0{,}98 \cdot 0{,}05}{0{,}98 \cdot 0{,}05 + 0{,}20 \cdot (1 - 0{,}05)} = 0{,}205\ldots .$$

Вероятность того, что вы в действительности больны, составляет отрадные 20%. Результат поражает. Большинство людей ожидает, что он окажется больше. Это обусловлено тем, что, оценивая вероятность, мы недооцениваем информацию о том, что сама по себе болезнь встречается очень редко.

ГЕОМЕТРИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ

Чтобы понять, почему мы ошибаемся, оценивая эти вероятности, рассмотрим рис. 50.1. Прямоугольник символизирует все возможные интересующие нас исходы. Маленький черный кружочек означает событие A — «корь». Кружочек очень маленький, потому что это очень редкая болезнь. Второй круг означает событие B — «тест положителен». Второй круг захватывает большую часть первого, ведь в случае болезни тест почти всегда дает положительный результат. Доля малого круга вне большого мала, поскольку мы считаем ничтожным число «фальшивых отрицательных» результатов.

Рис. 50.1.

Однако при всех этих условиях доля круга A, захваченного кругом B, невелика: положительный результат не означает, что у вас почти наверняка корь.

Глава 51
МИЛЛИОНЕР ИЛИ МИЛЛИАРДЕР?

В газетах и других СМИ часто встречаются очень большие числа: совокупный валовый продукт, национальный долг, и т. д. Можно считать, что почти все знают, что один миллион — это единичка с шестью нулями. Ведь без этого знания мы не могли бы планировать, как потратить огромную сумму, которую надеемся на следующей неделе выиграть в лотерею.

Числа в миллиардах сложно воспринимать, возможно, еще и потому, что политики или бизнесмены не объясняют важности больших чисел, которыми они разбрасываются. Если кто забыл: миллиард — это тысяча миллионов. Так что миллиардер может отдать тысячную долю своего состояния нищему и превратить того в миллионера.

Чтобы сделать все еще сложнее, в разных языках большие числа называются по-разному, а что еще хуже — одно и то же слово может иметь разные значения в разных странах. В американском английском, а в последнее время все чаще и в британском слово «биллион» означает то число, которое англичане или немцы[1)] называют «миллиардом». В США после миллиона идет биллион, затем триллион, квадрильон и так далее. В Германии миллиарды и биллиарды путаются, смазывая картинку, и легко впасть в замешательство.

К счастью, нам, немцам, повезло хотя бы в том, что в Германии терминология стабильна. Когда мы читаем про большие числа на британском английском или французском, например, то лучше было бы видеть числа, записанные цифрами, а не словами, особенно если литература старая. Действительно, какое-то время сосуществовали обе системы. В наши дни у французов тоже в ходу «миллиард», как у немцев, а британцы говорят «биллион» вслед за американцами. Поэтому

[1)] и россияне. — *Прим. ред.*

будьте скептиками, если вы в немецкой прессе читаете, что американский поп-идол — биллионер. По-немецки это просто «миллиардер». В реальной жизни квадрильоны вряд ли возникают, поскольку весь национальный валовой продукт может быть исчислен триллионами. Однако если бы мы хотели писать об общей сумме, хранящейся на счетах в Германии, то речь могла бы идти о квадрильонах.

Иногда математиков спрашивают о названиях еще больших чисел. Ответ не очень впечатляет, поскольку обычно большие числа выражаются просто как степени десятки. Очень немногие математики воспользуются словом «биллион», чтобы указать на число, записывающееся единицей с девятью нулями. Скорее всего, просто запишут десять в девятой степени (10^9). И если в разговоре зайдет речь о десяти в двадцатой степени, то совершенно необязательно справляться в латинском словаре о подходящей приставке.

ЧТО ЗНАЧАТ ДВА НУЛЯ?

К сожалению, природа не снабдила нас умением воспринимать большие числа. Конечно же, все знают разницу между десятью евро и тысячей. Но когда мы читаем, что свет проходит 5 870 000 000 000 миль (почти шесть триллионов) за год, способность воспринимать большие числа подводит нас. Будь в этом числе на два нуля больше или меньше — никакого впечатления это бы не произвело. Такие большие числа просто «непомерно» велики.

К несчастью, один из результатов такой неспособности — то, что нам сложно охватить некоторые реалии повседневной политической жизни. Заявление «дефицит Берлина составляет 59 253 104 304 евро»[1)] легче осмыслить, если прочитать его как «дефицит Берлина очень велик», а не пытаться переварить значение каждого из почти шестидесяти миллиардов. Тем не менее это же шестьдесят миллиардов евро! Если бы у кого-нибудь были такие деньги, он мог бы превратить в миллионеров всех жителей среднего немецкого города. А еще можно было бы заполнить

[1)] Берлинская газета «Tagesspiegel» от 22 марта 2006 года.

шестьсот ящиков объемом в кубический ярд купюрами в сто евро.

Тот день, когда все люди в мире будут одинаково понимать слово «миллиард», никогда не наступит. То же самое относится к праворульным и леворульным автомобилям и к ширине железнодорожного полотна. Раз уж общество поколениями привыкало к определенной системе, то находятся тысячи причин ничего не менять. В любом случае, это приводит к проблемам только для журналистов и переводчиков. Встретив слово «биллион», им приходится учитывать, когда и где оно было написано.

Глава 52

МАТЕМАТИКА И ШАХМАТЫ

Вы умеете играть в шахматы хоть немного? Или, по крайней мере, знаете правила? Некоторые аспекты математики проще объяснять, перенося их в другие рамки. Сегодня мы собираемся отправиться в мир шахмат.

Вначале рассмотрим правила игры. Они соответствуют аксиомам математики. Серьезных попыток изобрести новые правила игры в шахматы не предпринималось. Больше усилий направлено на то, чтобы понять, как пользоваться существующими правилами, чтобы выигрывать. Точно так же математики работают месяцами, даже годами, чтобы узнать, доказуем ли некоторый практический результат определенной теории.

Как известно, шахматные истины не зависят от какой-то отдельной доски или определенных игроков. Если в какой-то позиции возможен мат, то ее можно записать на бумаге (или при необходимости описать словами), и ничего не поделаешь. Точно так же, математические результаты не зависят от личностей, книг или языков. Локализовать математику действительно сложно. Платон полагал, что она вечна и находится в мире идей. Другие философы рассматривали ее просто как набор следствий, которые выводятся из условленных соглашений и которые иногда по случайности имеют полезные приложения.

Теперь мы подходим к решенным и нерешенным задачам. Даже новички быстро усваивают, что в эндшпиле король с поддержкой ладьи выигрывает против короля, оставшегося в одиночестве. Однако мы, по-видимому, никогда не узнаем, есть ли выигрывающая стратегия у белых в начале игры, ведь она слишком сложна. Точно

так же и в математике есть много нерешенных задач, и никому не известно, можно ли их решить (о некоторых из них, например о гипотезе Гольдбаха, мы рассказываем в этой книге).

Однако между математикой и шахматами есть фундаментальное различие, объясняющее, почему в ведущих университетах не бывает факультетов игры в шахматы. С помощью шахмат нельзя установить прочность моста или шансы выигрыша в лотерею. В отличие от математики шахматы неприложимы к проблемам реальности непосредственно. Почему же «книга природы написана языком математики» (Галилей), никто на самом деле не знает.

КАК СЛЕДУЕТ УЧИТЬ МАТЕМАТИКУ?

Есть и другие аналогии между математикой и шахматами. Рассмотрим университетское математическое образование. Как правило, математику учат, решая конкретные задачи: «докажите, что число x иррационально»; «покажите, что у данного дифференциального уравнения бесконечномерное пространство решений».

В шахматах тоже решают задачи: «черные начинают и выигрывают» (см. рис. 52.1); «как белые могут добиться преимущества, пожертвовав слона?».

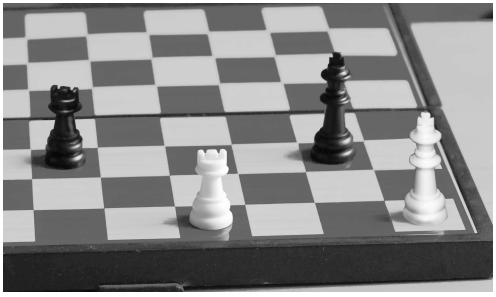


Рис. 52.1. Черные начинают и выигрывают

Однако каждый шахматист знает, что нельзя добиться совершенства, только решая задачи. Когда в реальной шахматной позиции вы ищете хороший ход, вы не знаете, есть ли здесь мат в три хода и может ли эффектная жертва решительно изменить ситуацию на доске.

Так и в математике в процессе обучения полезно включаться в ситуации, когда изначально неясно, что здесь можно доказать. Требуется творческое начало, для того чтобы решить, какие математические методы могут оказаться полезными. Такие ситуации гораздо ближе к тому, с чем профессиональные математики сталкиваются в работе, чем задачи типа «покажите, что ...»

Глава 53

«КНИГА ПРИРОДЫ НАПИСАНА ЯЗЫКОМ МАТЕМАТИКИ»

«Книга природы написана языком математики», — писал Галилей почти четыреста лет назад. Он имел в виду, что многие аспекты нашей жизни можно с успехом перевести на язык математики. Вообразите, например, что вы решили постелить ковровое покрытие в новой гостиной. Тогда вы можете оценить стоимость нового покрытия с помощью элементарной геометрии: нужно просто вычислить площадь прямоугольника.

При вычислении стоимости некоторые аспекты вашей реальной гостиной были выражены математическим языком. Эта же идея используется в инженерных проектах и естественных науках: представляющие интерес аспекты реальной задачи переводятся на язык математики, а затем задачу решают математическими методами. Последующий перевод на язык действительности должен — мы надеемся — давать ответ на жизненную задачу. Почти все ветви математики включаются в этот процесс: алгебра, геометрия, численные методы и теория вероятностей. Решаемые задачи могут быть сколь угодно сложными.

В конце концов, это напоминает ситуацию, когда иностранный турист в США переводит вопрос «Где здесь ближайшая заправка?» на английский: «Where can I find a gas station around here?», а затем надеется, что местный житель ему поможет. Решение, скорее всего, будет получено на английском языке, а потом его можно будет перевести на исходный язык.

В наше время никто не сомневается всерьез в правоте Галилея. Однако до сих пор идут споры о том, почему так происходит. Это тайна, в которую мы не можем проникнуть? Или Господь Бог — математик? Иначе говоря, устроен ли мир согласно математическим принципам, которые мы постепенно открываем? Или это просто обычай, и применимость математики иллюзорна?

На протяжении многих столетий математики и философы задавались этим вопросом, так и не получив удовлетворительного ответа на него. Мало надежды на то, что они когда-либо его получат.

МАТЕМАТИК КАК ПЕРЕВОДЧИК

Применение математики к задачам реального мира часто описывается как перевод: перевести суть задачи P в задачу P', получить решение L', а затем сформулировать обратный перевод L' в решение L как (возможное) решение исходной задачи. Этот процесс отображен на рис. 53.1.

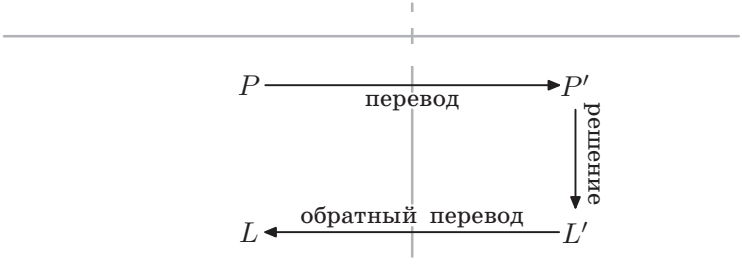
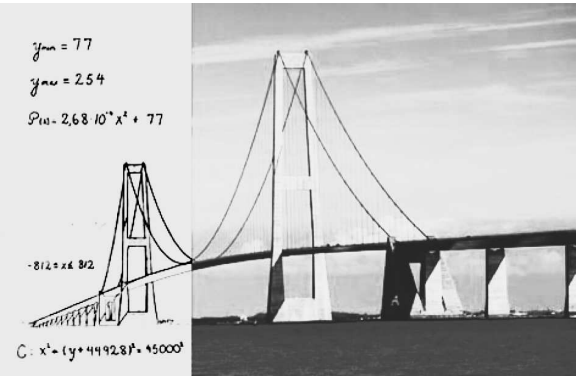


Рис. 53.1. Математика как искусство перевода

Это все очень похоже на другие методы перевода в математические модели из реального мира. Так, в гл. 36 уже говорилось, что самое главное достоинство использования логарифмов в том, что они переводят задачи на умножение в задачи на сложение. А бельгиец, прибывший в аэропорт Джона Кеннеди в Нью-Йорке, в поисках такси правильно сделает, если переведет эту задачу на английский язык, с тем чтобы с ней мог справиться американец.

Датский математик Вагн Лудсгаард Хансен изобразил роль математики в виде «моста в мир» на плакате, посвященном *международному году математики* 2000.

Справа на плакате изображен мост Большой Бельт — самый длинный подвесной мост в Европе (1624 м) и второй по длине в мире; уступая только мосту Акаси-Кайкё в Японии, он соединяет датские острова Фюн и Зеландию.



ЧТОБЫ РАСТИТЬ САД, СФЕРИЧЕСКАЯ ТРИГОНОМЕТРИЯ НЕ НУЖНА

Нужно заметить, что, создавая математические модели, приходится делать некоторые упрощающие предположения. Но если модель получается слишком простой, то результат будет малоприменим к моделируемой реальной ситуации; а если она будет слишком сложной, то вычисления будут слишком сложны или вовсе невозможны для практического применения. Мы не пользуемся сферической тригонометрией, разбивая грядки на огороде. Математическая теория полезна только тогда, когда строится подходящая модель.

Важно еще, что перевод на математический язык — только начало. Если, например, нужно определить тормозной путь автомобиля, требуется еще знание законов механики, поскольку именно они описывают соотношения между массами, силами и движением.

В сложных ситуациях может оказаться, что требуется много теорий о природе мира, чтобы прийти к конкретной математической задаче. И если решение не соответствует наблюдениям, то может быть неясно, какую из теорий придется модифицировать.

Глава 54

ПОИСК ПРОСТЫХ ЧИСЕЛ МЕРСЕННА

Ваш компьютер скучает? Вы хотите, чтобы ваше имя было вписано в анналы истории математики? Тогда отправляйтесь на сайт www.mersenne.org. Здесь вы обнаружите компьютерную сеть, созданную с целью найти очень большие простые числа.

Напомним, что простыми числами называются те, которые делятся только на себя и 1; к ним относятся, например, 3, 11 и 31. Известно, что простых чисел бесконечно много, поэтому среди них можно найти сколь угодно большие. Но это вовсе не означает, что примеры таких больших простых чисел легко привести. К задаче отыскания больших простых чисел использовались разные подходы, и самой эффективной оказалась смесь теоретических построений и обширных компьютерных вычислений.

С наивной точки зрения можно считать, что проверка простоты заданного большого числа несложна и не занимает много времени. Нужно просто проверить все меньшие числа — не являются ли они делителями. К сожалению, такой подход осуществим только для относительно малых чисел. Для больших чисел на такую проверку начинает требоваться все больше времени, по порядку сравнимого с возрастом вселенной.

Поэтому при поиске наибольших известных простых чисел рассматривают только кандидатов специального вида. Эти числа возникают при многократном умножении числа 2 на себя и последующем вычитании единицы. Например, числа 31 и 63 получаются как $2\cdot2\cdot2\cdot2\cdot2-1$ и $2\cdot2\cdot2\cdot2\cdot2\cdot2-1$. Такие числа называются *числами Мерсенна*. Они так названы в честь Св. отца Марина Мерсенна (1588–1648), портрет которого вы видите на следующей странице. Этот человек служил науке и Церкви.

Чтобы проверить, является ли некоторое число Мерсенна простым, существует специальный тест, который

можно провести за разумное время, даже если число очень велико. Нужно только провести проверку на делимость для очень большого числа. Лучше всего это делать с помощью большой компьютерной сети, и тест Мерсенна занимается как раз тем, что согласовывает работу разных участников такой сети.

Время от времени открывают новое рекордное простое число Мерсенна. В 2004 г. чемпиона открыли в ноябре. В нем было более шести миллионов цифр. Повезло некоему Майклу Шаферу — именно на его компьютере тест показал положительный результат. Как сооткрыватель сорокового числа Мерсенна он прославился наряду с другими профессиональными математиками.

РЕКОРДСМЕНЫ СРЕДИ ПРОСТЫХ ЧИСЕЛ

Рекорды в мире простых чисел быстро устаревают. Скорости компьютеров растут, сети ширятся, алгоритмы становятся все изощреннее, и поэтому открывают все новые простые числа. Так что неудивительно, что рекорд на время появления этой газетной статьи в 2004 г. был превзойден. Когда я пишу эти слова, рекордсменом[1)] считается число

$$2^{25\,964\,951} - 1.$$

Если вы хотите ознакомиться с современным положением вещей, отправляйтесь на www.mersenne.org, на этом сайте ведется книга рекордов.

Чтобы представить себе, насколько огромны эти числа, вспомним, что число 2^{10} равно 1024. Иначе говоря, 2^{10} приблизительно равно 10^3. Аналогично, можно считать, что $2^{20} \approx 10^6$, $2^{30} \approx 10^9$ и так далее. И вообще, число 2^n приблизительно равно числу, которое начинается с 1 и в котором $3 \cdot (n/10)$ нулей (по крайней мере если эта дробь выражает целое число). Для нашего примера

[1)] См. примечание на с. 19 (гл. 4).

$2^{25\,964\,951} - 1$ мы получаем число $3 \cdot (25\,964\,951)/10$, т. е. в нем около восьми миллионов цифр. Если отпечатать это число на таком листе бумаге, на котором по пятьдесят строк и в каждой из них по 100 знаков — всего по 5000 знаков на листе, — потребуется $8\,000\,000/5\,000 = 8\,000/5 = 1\,600$ страниц. Увесистый том.

ПРОВЕРКА НА ПРОСТОТУ

Как быстро проверить, является ли некоторое число n простым? Например, просто ли число 2 403 200 604 587?

Самый простодушный подход — проверить все числа m, меньшие n, не являются ли они делителями n. Для этого нужно примерно n вычислений, и для больших чисел это слишком много.

Поразмыслив, мы можем сэкономить немного времени. А именно, если n — не простое число и может быть представлено в виде $n = k \cdot l$, то оба числа k и l не могут быть больше квадратного корня из n. (Из неравенств $k > \sqrt{n}$ и $l > \sqrt{n}$ при помощи умножения мы сделали бы вывод, что $k \cdot l > \sqrt{n} \cdot \sqrt{n} = n$.) Поэтому если в интервале от 2 до $\sqrt{n}$ делителей нет, то их нет вовсе.

Экономия во времени разительна. Для числа порядка миллиона нам понадобилось не миллион вычислений, а только тысяча. Однако если в числе n несколько сотен цифр, то полученная экономия все равно недостаточна для того, чтобы метод стал практически пригодным: корень $\sqrt{n}$ настолько велик, что для проверки на простоту понадобилось бы несколько сотен лет.

Значит, мы должны найти другой путь. Процедура, применимая для открытия новых рекордов, применима только к числам вида $2^k - 1$. Она называется «тестом Люка–Лемера».

Введем обозначение $M_k = 2^k - 1$. Когда M_k является простым числом? Можно доказать, что оно простое только тогда, когда число k само простое. Правда, из простоты k вовсе не следует простота самого числа Мерсенна M_k. (Например, $M_{11} = 2^{11} - 1 = 2\,047 = 23 \cdot 89$.)

Поэтому выбирают простое число k и определяют числа $L_1, L_2, \ldots, L_k$, называемые *числами Люка–Лемера*, следу-

ющим образом: $L_1 := 4$, $L_2 := L_1^2 - 2 = 14$, $L_3 := L_2^2 - 2 = 194$, и т. д. Всегда выполняется соотношение $L_{l+1} = L_l^2 - 2$. Следовательно, M_k является простым числом ровно тогда, когда M_k делит L_{k-1}.

Посмотрим, как работает этот метод. Вычислим первые несколько чисел Люка–Лемера:

$$4, 14, 194, 37\,634, 1\,416\,317\,954, \ldots$$

Ясно, что числа в последовательности очень быстро растут. Однако нам интересно лишь, делятся ли они на M_k, поэтому достаточно рассматривать L_l по модулю M_k[1)].

Пример 1. Возьмем $k = 5$. Тогда $M_k = 2^5 - 1 = 31$. Поскольку 31 — простое число, тест должен быть положительным. Мы должны найти числа L_1, L_2, L_3, L_4 и проверить, делится ли последнее из них на 31. Вычисляя остатки этих чисел при делении на 31, получим последовательность 4, 14, 8, 0. Последнее число 0, значит, тест справедливо говорит нам о том, что 31 — простое число.

Пример 2. Теперь попробуем $k = 11$. Мы должны проверить число $M_{11} = 2\,047$. Вот остатки чисел $L_1, L_2, \ldots, L_{10}$ при делении на 2047:

$$4, 14, 194, 788, 701, 119, 1877, 240, 282, 1736.$$

Последнее из чисел не равно нулю, и это говорит о том, что M_{11} не может быть простым числом. (Кстати, заметьте: этот метод доказывает, что число M_{11} не простое, но он не дает ни одного делителя этого числа. Это особенность теста.)

[1)] Арифметика по модулю обсуждается в гл. 22.

Глава 55

БЕРЛИН, XVIII ВЕК: ОТКРЫТА САМАЯ КРАСИВАЯ ФОРМУЛА

Несколько лет назад среди математиков был проведен опрос: «Какая формула самая красивая?». Предлагались формулы из разных областей математики, а победила та, что была открыта швейцарским математиком Леонардом Эйлером в восемнадцатом веке. В то время Эйлер был придворным математиком при дворе Фридриха Великого в Берлине.

Чтобы понять эту формулу, вспомним самые важные числа в математике. Бесспорно, к ним относятся нуль и единица, ведь все оставшиеся числа можно из них построить. Кроме того, они проявляют особенные свойства в операциях с другими числами. Действительно, нуль является нейтральным элементом по сложению: прибавление нуля к другому числу не изменяет результат, и аналогично, единица является нейтральным элементом по умножению: для любого числа x выполняется тождество $1 \cdot x = x$.

Нам понадобится еще число π. Даже школьники знакомятся с этим числом, вычисляя площадь и длину окружности по данному радиусу. А для описания некоторых явлений роста существенную роль играет число $e = 2{,}71828\ldots$. Экспоненциальный рост (бактерии) и экспоненциальное убывание (радиоактивный распад) относятся к основным математическим моделям, и в обоих случаях возникает число e. И наконец, уже несколько столетий известно, что множество чисел, необходимых для решения алгебраических уравнений, должно включать *комплексные числа*, для чего требуется определить число i как *мнимый* корень из -1. Эти числа нужны не только для теоретических исследований. Действительно, комплексные числа входят в инструментарий многих практиков, например инженеров-электриков.

Поразительно, но существует тесная связь между числами $0, 1, \pi, e$ и i. А именно, если к единице прибавить e

в степени, равной произведению π и i, то получится нуль. Это и есть формула Эйлера:

$$0=1+e^{i\pi}$$

Эта формула имеет особое значение для математиков, поскольку символизирует единство математики. Есть что-то мистическое в том, что горстка чисел, используемых с самыми разными целями, связаны столь простым соотношением.

ВЫВОД САМОЙ ПРЕКРАСНОЙ ФОРМУЛЫ

В этой книге мы прояснили роль почти всех чисел, входящих в формулу Эйлера. В гл. 16 речь шла о числе π, в гл. 28 — о нуле, в гл. 42 — о e, а в гл. 94 — об i. Как же Эйлер открыл свою формулу?

Чтобы это понять, нужно знать несколько математических функций. Важную роль играет тот факт, что иногда сложные выражения могут быть хорошо приближены простыми. Например, если число x *достаточно мало*, то приблизительное значение квадратного корня из $1+x$ дает сумма $1+x/2$. Проверим это утверждение для $x=0{,}02$: значение $\sqrt{1{,}02}=1{,}00995$ очень близко к $1+\frac{0{,}02}{2}=1{,}01$. Если нужна более высокая точность, то можно добавить слагаемое, кратное x^2; можно добиться еще более высокой точности, добавив слагаемое с x^3.

Сейчас нам интересна экспоненциальная функция. Для e^z мы получим все лучшие приближения, взяв два, три или более слагаемых в разложении

$$1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\ldots$$

(напомним, что $2!=1\cdot 2$, $3!=1\cdot 2\cdot 3$ и т. д.) Ошибка становится все меньше по мере того, как берут все больше слагаемых, поэтому справедливо выражение

$$e^z=1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\ldots,$$

которое мы приводим без доказательства. Существуют аналогичные формулы для функций синуса и косинуса:

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \dots$$

$$\cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \frac{z^6}{6!} + \dots$$

Теперь воспользуемся формулой для e^z, чтобы выразить e^{ix}, где i — мнимая единица. Помня о том, что $i^2 = -1$ (см. гл. 94), получим:

$$\begin{aligned} e^{ix} &= 1 + ix + \frac{(ix)^2}{2!} + \frac{(ix)^3}{3!} + \dots = \\ &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{z^6}{6!} + \dots + \\ &\quad + i\left(x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots\right) = \cos x + i \sin x. \end{aligned}$$

А теперь возьмем значение $x = \pi$ и вспомним значения некоторых тригонометрических функций для этого угла, а именно $\cos \pi = -1$ и $\sin \pi = 0$. Вот теперь и получается $e^{i\pi} = -1$, а это и есть формула Эйлера.

Глава 56

ПЕРВОЕ ДЕЙСТВИТЕЛЬНО СЛОЖНОЕ ЧИСЛО

Есть две причины, почему числа, представимые в виде дроби, — *рациональные числа* — очень важны. Во-первых, их очень много и они так плотно расположены среди всех чисел, что практически каждое важное число может быть хорошо приближено рациональным. Например, можно достаточно точно определить количество семян, необходимое для засева круглого поля, приблизив число π дробью 314/100.

А во-вторых, с дробями легко работать. Даже довольно маленькому ребенку нетрудно объяснить, что такое дробь 5/11. Пифагорейцы в Древней Греции полагали, что все числа в арифметических и геометрических задачах должны быть рациональными. Этот принцип позволил пифагорейцам описать много важных явлений. Например, они ввели гамму, опираясь на наблюдение, что приятные слуху соотношения между тонами описываются простыми дробями[1)].

Поэтому оказалось тяжелым ударом, когда выяснилось, что даже в самых простых ситуациях могут возникать числа, которые не являются рациональными. Такие числа называются *иррациональными*. Самый известный пример — конечно же, квадратный корень из 2. Он возникает как длина диагонали квадрата с единичной стороной. Те, кто занимаются геометрией, неизбежно встречаются с этим числом.

Доказательство иррациональности нельзя назвать тривиальным. Компьютеры и обширные вычисления бесполезны. Из того что корень из двух нельзя записать в виде дроби с числителем и знаменателем в миллионы цифр, вовсе не следует, что его нельзя записать миллиардами.

[1)] См. гл. 26.

Поэтому придется проводить непрямое доказательство. Даже Шерлок Холмс часто и с успехом пользовался этим методом. Если вы делаете предположение, которое считаете истинным, и из него должен следовать некоторый вывод, на деле оказавшийся ложным, то исходное предположение тоже должно быть ложным.

Именно такой метод работает в нашем случае. Сейчас мы расскажем об этом подробнее, но вначале — история, связанная с иррациональностью квадратного корня из двух. Открыв существование иррациональных чисел, пифагорейцы поклялись хранить это в секрете, а первооткрыватель, некий Гиппосус, был казнен за то, что потряс основы математики.

ПОЧЕМУ $\sqrt{2}$ НЕЛЬЗЯ ПРЕДСТАВИТЬ В ВИДЕ ДРОБИ?

Квадратный корень из двух — это положительное число, квадрат которого равен 2. Для краткости обозначим его w. Немного поэкспериментировав, мы можем оценить его. Например, квадрат числа 1,4, т. е. $1{,}4 \cdot 1{,}4 = 1{,}96$, меньше 2, и поэтому число w должно быть больше 1,4. С другой стороны, квадрат числа 1,5 равен 2,25, а это слишком много. Поэтому w, конечно же, меньше 1,5.

Любой карманный калькулятор позволяет уточнить это значение. Для многих практических целей достаточно пользоваться приближением 1,414213562. Оно не точное, поскольку

$$1{,}414213562 \cdot 1{,}414213562 = 1{,}999999998944727844,$$

— до двух не хватает самой малости.

Вопрос о том, представим ли квадратный корень из двух в виде дроби, встал более двух тысяч лет назад[1)].

Следующее доказательство опирается только на тот факт, что

квадрат нечетного числа — тоже нечетное число, а квадрат четного числа — четное.

[1)] Заметьте, что любое число, которое допускает конечную десятичную запись, можно представить в виде дроби. Например, число 1,41 можно записать в виде 141/100. А число, которое нельзя записать в виде обычной дроби, не может иметь конечной десятичной записи.

Доказательство начинается с предположения о том, что число w можно записать в виде дроби. Затем мы будем выводить следствия из этого предположения, пока не придем к противоречию. (Так рассуждал бы Шерлок Холмс: если бы убийца покинул ресторан через кухню, его бы увидели повара. Они никого не видели. Значит, убийца вышел другим путем.)

Итак, запишем w в виде p/q, где p и q — натуральные числа. Можно считать, что мы сократили в этой дроби все возможные общие делители, так что хотя бы одно из чисел p и q должно быть нечетным.

Из соотношения $w = p/q$ мы заключаем, что $p = w \cdot q$. Возведем это равенство в квадрат, помня о том, что $w \cdot w = w^2 = 2$: получаем $2 \cdot q^2 = p^2$. Поэтому p^2 — четное число; а как мы уже заметили, это может быть, только если само p четно. А раз оно четно, то его можно записать в виде $2k$, а затем подставить в равенство $2 \cdot q^2 = p^2$. Это дает $2 \cdot q^2 = 4 \cdot k^2$. Умножив обе части равенства на $\frac{1}{2}$, получим $q^2 = 2 \cdot k^2$. Таким образом, число q^2, а значит и q, четно. Но этого не может быть: мы предположили, что сократили все общие множители числителя и знаменателя p и q, а теперь оказалось, что оба этих числа четны.

Таким образом, мы показали, что корень w не может быть записан в виде дроби. Даже если брать астрономически большие числа. Даже за 100 000 лет.

Глава 57

P=NP: НУЖНО ЛИ ВЕЗЕНИЕ В МАТЕМАТИКЕ?

В этой главе мы расскажем о задаче, за решение которой предложена награда в миллион долларов.

Для начала рассмотрим классификацию процедур решения. Все знают, что складывать проще, чем умножать. Этим словам можно придать более точный смысл, если рассмотреть количество цифр в заданных числах. При сложении n-значных чисел требуется n вычислительных операций, а при умножении — $n \cdot n$. Как правило, мы будем говорить, что алгоритму требуется *полиномиальное время работы*, если число операций не превышает некоторой степени n, т. е. не больше n^r при некотором фиксированном r.

Обычно считается, что такие задачи решать «просто», поскольку с ними можно справиться с помощью компьютера, даже для сравнительно больших n. Но встречаются и существенно более сложные задачи. Например, хорошо известна *задача о коммивояжере*, в которой требуется найти кратчайший маршрут, проходящий через несколько точек [1)].

Иногда ответ «сложной» задачи можно просто угадать, для чего требуется редкое везение. Например, разложить большое число на множители — сложная задача, но если удастся угадать один из сомножителей, то доказать, что он действительно сомножитель, нетрудно.

Всерьез, конечно же, никто не думает, что такие задачи можно считать простыми, поскольку удачливость требуется такая же, как для еженедельного угадывания выигрышных лотерейных номеров на протяжении всей жизни.

Поразительно, но никто не может доказать, что без удачи здесь действительно не обойтись. В последние десятилетия много усилий было направлено на решение этой задачи, а в 2000 г. была назначена премия в миллион долларов тому, кто ее решит. Но прежде чем браться за бумагу

[1)] См. гл. 32.

и карандаш, вспомните, что лучшие математики мира не смогли построить доказательство.

Мы должны здесь подчеркнуть, что определенный интерес в решении этой задачи обусловлен тем фактом, что ответ может значительно повлиять на безопасность современных шифровальных систем.

ЧТО ЖЕ ТАКОЕ P- И NP-ЗАДАЧИ?

Чтобы разобраться в задаче, мы должны вначале прояснить некоторые термины.

Что такое P-задача?

Чтобы сложить два трехзначных числа, нужно провести три элементарных сложения; в общем случае для n-значных чисел потребуется n операций сложения. Обычный метод умножения сложнее: придется выполнить $n \cdot n$ простых умножений, и потом еще несколько сложений. Для умножения потребуется не более $2n^2$ элементарных операций. Говорят, что задача (такая как «найти сумму» или «найти произведение») относится к типу P, если время ее решения с n-значными числами ограничивается выражением вида $c \cdot n^r$, где c и r — некоторые фиксированные постоянные. Буква P означает, что такие задачи могут быть решены за полиномиальное время. Например, если задача с n-значными входными данными может быть решена с помощью менее $1000 \cdot n^{20}$ элементарных операций, то она относится к типу P.

Хорошо известно, что задачи этого типа «сравнительно просты» и что обычно их можно решить с помощью компьютера за разумное время.[1)]

Что такое NP-задача?

Однако для некоторых задач требуются очень сложные методы решения. Чтобы определить оптимальный маршрут

[1)] Это только эмпирическое правило. Если ограничение имеет вид $1000 \cdot n^{20}$, то для решения задачи с пятизначными числами потребуется 95 367 431 640 625 000 операций. Компьютер не справится с таким количеством.

в задаче о коммивояжере с n городами, требуется сравнить $1 \cdot 2 \cdot 3 \cdots n$ возможных маршрутов, а это число не может быть ограничено выражением вида $c \cdot n^r$, какими бы большими ни были числа c и r.

Но если попытаться угадать решение, может повезти, и тогда задача решится быстро: нужно лишь угадать решение и проверить, затратив не более n операций, не слишком ли длинный получился маршрут.

В общем случае, задачу относят к типу NP (недерминистский полиномиальный), если методом угадывания при везении ее можно свести к полиномиальной.

Математиков раздражает, что до сих пор никто не смог доказать что класс P-задач и класс NP-задач не совпадают. Особенный интерес вызывает вопрос о том, принадлежит ли классу P задача «найти делитель целого числа» (как мы уже говорили, к классу NP, она, конечно же, относится). В гл. 23 мы обсуждали, как безопасность систем шифрования зависит от ответа на этот вопрос.

За решение задачи «P=NP?» математический институт Клэя назначил награду в миллион долларов. Подробности вы можете найти на сайте http://www.claymath.org.

Глава 58
ВАМ ВСЕГО ЛИШЬ 32 ГОДА!

С проблемами лучше всего разбираться, если подходить к ним с точки зрения оптимальности. Это относится и к математике, где много усилий тратится на создание огромного разнообразия способов представить рассматриваемые объекты так, чтобы можно было выбрать подходящие методы, когда возникает какая-либо задача.

Рассмотрим, например, целые числа. Мы привыкли записывать их в хорошо знакомой десятичной системе. Это означает, что мы задаем определенное число, указав, сколько нужно единиц, десятков, сотен, и т. д., чтобы его записать. Так, 405 — краткая запись числа «четыре сотни плюс нуль десятков плюс пять единиц.»

Это очень практичная форма представления, поскольку позволяет сложные вычисления свести к простым операциям умножения и сложения, на обучение которым в начальной школе ученики тратят так много времени.

Но почему система записи десятичная? Конечно же, потому, что у нас на руках десять пальцев; более глубокой причины нет. Существовали культуры, которые использовали систему счисления с основанием 12. В такой системе двенадцать символов-цифр (обозначим их 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B), а числа записываются с использованием степеней двенадцати. Нам показалось бы странно работать с подобными числами, но в такой системе, несомненно, есть преимущества. А именно, у двенадцати больше делителей, чем у десяти, и поэтому реже встречались бы ситуации, когда число приходится записывать дробью.

В наше время кроме десятичной системы широко распространены лишь системы с основаниями два и шестнадцать: двоичная и шестнадцатеричная системы. Обе используются в компьютерах. Двоичная система практична, поскольку в ней только две цифры (0 и 1), и поэтому числа легко представлять в электронном виде (*да* или *нет*; *высокое напряжение* или *низкое*). А шестнадцатеричная система

возникает, когда комбинируют четыре двоичные цифры в одну.

Например, число 50 записывается в шестнадцатеричной системе как 32 (т. е. дважды один плюс трижды шестнадцать). Так что 50-й день рождения превращается в 32-й: все зависит только от точки зрения.

ФОНТАН В НОВОЙ НАЦИОНАЛЬНОЙ ГАЛЕРЕЕ

Система с основанием 3 получила художественное представление в Берлинской национальной галерее. Фонтан во внутреннем дворике, разработанный американским минималистом Уотером де Мариа, включает несколько маленьких струй, которые бывают трех разных форм. Если эти формы интерпретировать как цифры в троичной системе счисления, то можно получить возможные комбинации цифр, представляющие все числа от нуля до $3 \cdot 3 \cdot 3 - 1 = 26$ в системе по основанию 3.

Рис. 58.1. Числа в троичной системе счисления

КАК ПЕРЕВОДИТЬ?

Те, кому понравилось переводить свой возраст или другие числа в шестнадцатеричную систему, могут использовать следующую процедуру. Допустим, задано число в привычной десятичной системе. Например, число 730.

Шаг 1. Разделим число на 16 и рассмотрим вначале получившийся остаток. В нашем примере 730, деленное на 16, равно 45, а остаток равен 10. Поскольку в шестнадцатеричной системе есть цифры 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, в разряде единиц в шестнадцатеричном представлении числа 730 стоит A. Это самая правая цифра в новом представлении.

Шаг 2. Теперь возьмем частное от деления, проведенного на первом шаге. Это было число 45. С этим числом поступим точно так же, как раньше с числом 730. Разделим 45 на 16 и запомним частное и остаток. 45 : 16 = 2, и остаток равен 13. Остаток дает цифру на месте шестнадцаток, вторую цифру справа, и поэтому это должна быть цифра D.

Процедура продолжается в том же духе все дальше, пока в результате деления не получится число меньше 16. Оно станет первой цифрой. В нашем примере хватило двух делений, поскольку второе частное 2, разумеется, меньше 16. Итак, мы выяснили, что десятичное число 730 в шестнадцатеричной системе записывается как $2DA_H$, индекс H указывает на то, что число записано в шестнадцатеричной системе. Без индекса возможны недоразумения. Например, в представлениях некоторых чисел, таких как 50-й день рождения, т. е. 32_H, не входят особые шестнадцатеричные цифры A, B, C, D, E, F.

Глава 59
ИГЛА БЮФФОНА

Сегодня мы вернемся на 250 лет назад и пересечем французскую границу. Там и тогда у науки был высокий социальный статус. Последними достижениями в зарождающихся естественных науках и математике интересовались многие дворяне, и некоторые из них добились значительных результатов. Каждому уважающему себя аристократу кроме конюшни с породистыми рысаками полагалось иметь научную лабораторию, и любой путешествующий ученый получал радушный прием.

Одним из таких энтузиастов науки был Жорж-Луи Леклерк, граф де Бюффон; он родился в 1707 г., а умер в 1788 г., за год до Французской революции. Сегодня множество его энциклопедических трудов, в которых было собрано знание того времени, почти забыто. Однако он обессмертил свое имя, войдя вместе со своим знаменитым экспериментом в историю математики.

Представьте себе плоскую поверхность, на которой через равные промежутки прочерчены параллельные прямые. Это может быть разлинованный лист бумаги, лежащий на столе, или дощатый пол. В ходе эксперимента подбрасывают иглу таким образом, что она падает на эту поверхность. Верьте или нет, но можно вычислить вероятность того, что игла пересечет одну из параллельных линий. Еще удивительнее, что эта вероятность выражается через число π — отношение длины окружности к ее диаметру. Этот факт позволяет вычислить значение π экспериментально. Для этого нужно только подбрасывать

иглу достаточно долго, чтобы вычислить вероятность пересечения одной линии достаточно точно.

Метод, описанный Бюффоном, известен почти во всех областях математики под названием *метод Монте-Карло*[1]. Капризы госпожи удачи укрощены и используются для подсчетов, вычисления интегралов и т. д. Конечно же, никто не бросает иглы в наше время, когда есть компьютеры, позволяющие моделировать миллионы случайных событий в мгновение ока.

Как жалко, что в наше время наука стала настолько сложной, что те, у кого много времени и денег, не могут распорядиться ими так, как удалось когда-то месье графу.

ФОРМУЛА ДЛЯ ВЫЧИСЛЕНИЯ ВЕРОЯТНОСТИ ПЕРЕСЕЧЬ ЛИНИЮ

Для того чтобы вывести формулу, связывающую число π и вероятность пересечь линию, нужно посмотреть на задачу с правильной точки зрения.

Вначале введем некоторые обозначения. Ширину досок обозначим d, а длину иглы — l. Чтобы гарантировать, что игла может пересечь только одну линию, будем считать, что l меньше d. Эта ситуация изображена на рис. 59.1.

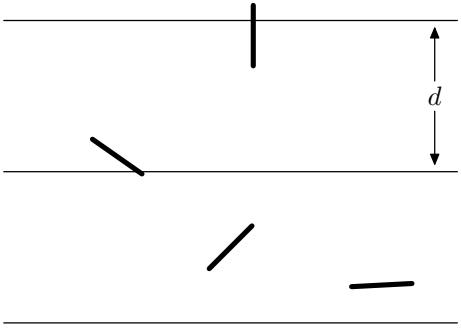


Рис. 59.1. Эксперимент с иглой

Пора подключать к работе случай. Представьте прямоугольник со сторонами 90 и $d/2$ в первом квадранте

[1] См. также гл. 73.

декартовой системы координат. Точку в этом прямоугольнике можно задать двумя числами, скажем α и y, причем α лежит между 0 и 90, а y — между 0 и $d/2$.

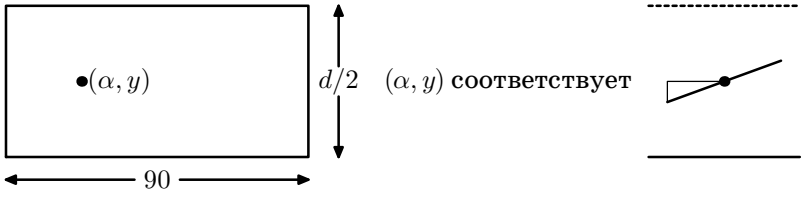


Рис. 59.2. Случайному бросанию соответствует точка в прямоугольнике

Числа α и y можно использовать для описания того, как именно игла упала на пол. Пусть y обозначает расстояние от середины иглы до ближайшей прямой, а α — угол между иглой и прямой. Эта ситуация изображена на рис. 59.2. Если угол α мал, то игла почти параллельна прямой, а если $\alpha = 90^\circ$, то перпендикулярна. Ясно, что для малых значений y (когда центр иглы близок к прямой), для того чтобы игла пересекла прямую, достаточно малых углов α. Для точного описания этой зависимости достаточно элементарной тригонометрии: игла пересекает прямую в точности тогда, когда вертикальная сторона изображенного на рисунке треугольника больше y. Но длина этой стороны, деленная на $l/2$, равна синусу угла α. Поэтому игла пересекает прямую ровно тогда, когда $\frac{l}{2} \cdot \sin\alpha$ больше y. Множество точек (α, y), для которых это верно, изображено на рис. 59.3.

Вместо того чтобы на самом деле бросать иглы, можно выбирать случайным образом точки на прямоугольнике и интерпретировать их как результаты реальных бросаний иглы. Вероятность того, что игла пересечет прямую, можно найти по рисунку: она равна отношению площади

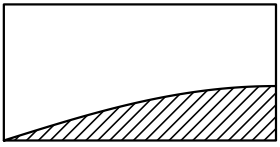


Рис. 59.3. Точки в заштрихованной области соответствуют «попаданию»

заштрихованной фигуры под графиком синуса к площади всего прямоугольника.

Эти площади можно вычислить, и тогда мы получим, что вероятность пересечь прямую на полу равна

$$\frac{2 \cdot l}{\pi \cdot d},$$

где d — ширина доски[1)].

Количественные оценки показывают, что эта формула имеет смысл. Вероятность должна быть больше для больших значений l и должна уменьшаться с ростом ширины доски d.

Довольно теорий, начинаем эксперимент с π! Мы подбрасываем вязальную спицу (длиной 10 дюймов) 1000 раз и отмечаем, сколько раз она пересекла прямую (когда ширина доски составляет 20 дюймов). Допустим, мы получили 320 пересечений. Это дает оценку вероятности P: она должна составлять приблизительно $320/1000 = 0{,}32$. И если мы рассмотрим выведенную ранее теоретическую формулу, а именно

$$P = \frac{2 \cdot 10}{20 \cdot \pi}$$

и выведем из нее π, то получим

$$\pi = \frac{2 \cdot 10}{20 \cdot P} \approx \frac{2 \cdot 10}{20 \cdot 0{,}32} = 3{,}125.$$

Таким образом, эксперимент с иглой позволил получить такую оценку: $\pi \approx 3{,}125$. По-видимому, эта оценка не так уж точна, но если вы хотите получить более точный результат, просто бросайте иглу дольше.

[1)] Эта формула получена интегрированием. Число π здесь возникает, поскольку радианная мера угла 90° составляет $\pi/2$.

Глава 60

ЖАРА И ХОЛОД: КОНТРОЛИРУЕМОЕ ОХЛАЖДЕНИЕ КАК СПОСОБ РЕШЕНИЯ ЗАДАЧ ОПТИМИЗАЦИИ

Не так давно в математику из внешнего мира проник технический термин. В производстве стекла «отжиг» — процесс постепенного охлаждения стекла с целью увеличить его твердость и снять возникшие в нем напряжения.

В математике «имитация отжига» стала универсальным методом решения сложных задач оптимизации. Идея заключается в том, чтобы найти такие числа, или параметры, которые делают искомую величину как можно больше. Скажем, выбраны параметры широта и долгота, а искомая величина — высота над уровнем моря в регионе. Задача состоит в том, чтобы найти наивысшую точку в регионе (а может стоять цель найти самую низкую точку). В задачу могут входить пропорции различных веществ в химической реакции, или же параметры мотора; возможно, требуется найти материал с особыми свойствами или условия, гарантирующие наивысшую эффективность.

Классический способ решения таких задач — использовать дифференциальные уравнения. Но такой подход часто не срабатывает, поскольку соотношения между начальными значениями и целевой функцией заведомо не известны или они слишком сложны для конкретных вычислений.

В таких обстоятельствах полезно воспользоваться имитацией отжига. Этот метод можно объяснить на примере, когда путешественник ищет наивысшую точку в холмистой местности. Представьте себе, что вокруг густой туман. Как найти самую высокую точку? Идти все выше и выше? Тогда может случиться так, что вы застрянете на вершине невысокого холмика, хотя могли бы достичь других высот. Суть метода — большую часть пути двигаться все выше, но время от времени делать шаг вниз. Это позволит найти действительно наивысшую точку. Вам только нужно убедиться, что, достигнув наивысшей точки, вы не уйдете оттуда. Этого можно добиться, позволив тенденции к спуску

стремиться к нулю. Здесь и выходит на сцену аналогия с контролируемым охлаждением.

В других задачах подход приблизительно такой же. Вместо того чтобы блуждать в тумане, вы путешествуете в поле параметров. Если поле не бескрайнее и у вас достаточно времени для вычислений, вы сможете решить вашу задачу оптимизации.

ПУТЕШЕСТВУЮЩИЙ КОММИВОЯЖЕР

При постановке оптимизационных задач часто используют аналогии с путешествиями. Например, давайте вспомним коммивояжера-путешественника из гл. 32. Скажем, речь идет о двадцати городах и требуется найти кратчайший путь, проходящий через каждый город ровно по одному разу. Пронумеруем города числами от 1 до 20 и будем записывать маршрут в порядке посещения городов. Так, последовательность

6, 1, 19, 2, 15, 12, 3, 5, 20, 11, 16, 10, 7, 13, 8, 4, 9, 17, 14, 18

обозначает маршрут, начинающийся в городе 6, затем ведущий в город 1, в город 19, и т. д. Мы будем считать, что в конце нужно вернуться в самый первый город, поэтому после посещения города 18 уставший коммивояжер отправится в город 6, завершив путешествие.

Число всех возможных маршрутов астрономически велико. Элементарная комбинаторика (см. гл. 29) говорит о том, что их 2 432 902 008 176 640 000. Нереалистично, чтобы компьютер мог вычислить длины всех этих маршрутов. Для того чтобы применить метод имитации отжига, можно представить себе каждый возможный маршрут как точку на холмистой местности; длина маршрута при этом соответствует высоте над уровнем моря. Наша цель — найти самую низкую точку.

При *имитации отжига* мы попытаемся найти решение, исходя из некоторого маршрута, скажем того, что привели выше (6, 1, 19, ...). Выберем наугад две позиции в списке и поменяем их местами. Например, если выбраны позиции

3 и 8, то поменяются местами города 19 и 5, что даст маршрут

6, 1, 5, 2, 15, 12, 3, 19, 20, 11, 16, 10, 7, 13, 8, 4, 9, 17, 14, 18.

Если такая перемена приводит к более короткому маршруту, то будем продолжать процесс, выбирая каждый раз наугад по две позиции. В противном случае вернемся к предыдущему варианту и попробуем еще раз. Однако есть еще одно правило. Будем с определенной вероятностью принимать маршрут длиннее предыдущего, и эта вероятность в начале процедуры выше, чем в конце. Это гарантирует, что мы не застрянем в локальном минимуме (и в самом деле найдем самую низкую точку, а не просто впадинку посреди плато).

Рассмотрим пример, в котором использована имитация отжига. На рис. 60.1 слева изображена область с отмеченными на ней двадцатью «городами». Расстояния между городами измеряются по прямой. В других задачах расстояния могут измеряться иначе, например вдоль существующих дорог или в зависимости от стоимости авиабилета. Предложен некоторый маршрут, и после этого можно запускать случайный процесс выбора. Результат такого случайного выбора изображен на рис. 60.1 справа.

Теперь применим алгоритм имитации отжига. Как мы уже сказали, текущий маршрут все время варьируется, и, как правило, метод оставляет только более короткие

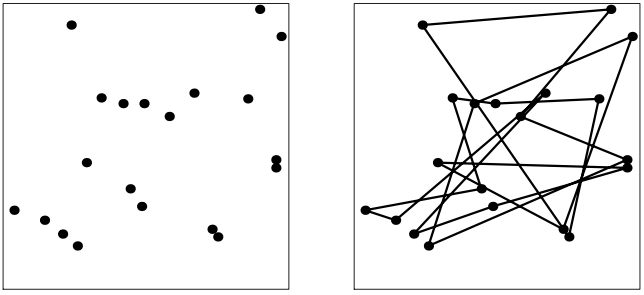


Рис. 60.1. Города и случайный маршрут

из предложенных альтернатив. После нескольких миллисекунд вычислений компьютер выдал рис. 60.2.

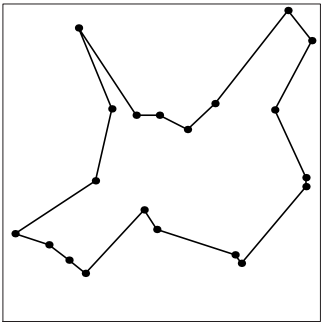


Рис. 60.2. Маршрут, построенный методом моделирования отжига

Этот маршрут выглядит многообещающе, и по-видимому, лучшего маршрута не существует. Нужно отметить, что никогда нельзя быть уверенным, что метод не пропускает наилучший маршрут. Гарантия выбора наилучшего маршрута потребовала бы гораздо больших затрат на вычисления и более сложной математической теории.

Глава 61
КТО НЕ ЗАПЛАТИЛ?

В математике иногда возникают такие ситуации, что можно строго доказать существование объекта, обладающего некоторыми свойствами, однако невозможно построить ни одного конкретного примера такого объекта. Такие доказательства называются *неконструктивными доказательствами существования*.

Например, рассмотрим классический результат о том, что существует бесконечно много простых чисел. Отсюда следует, например, что существует простое число, в котором более 100 триллионов цифр[1]. Однако мы крайне далеки от возможности записать такое число на бумаге. Рекордсмен среди открытых простых чисел состоит «всего лишь» из примерно десяти миллионов цифр. И мы можем считать, что на протяжении нашей жизни ситуация значительно не изменится.

Путь от доказательства существования к конкретным примерам часто бывает долгим и мучительным — если такой пример вообще может быть найден. Например, Георг Кантор, создатель теории множеств, доказал, что среди всех чисел большинство «крайне сложны», т. е. *трансцендентны*. Но потребовались серьезные усилия, чтобы доказать, что какое-то определенное число трансцендентно. (И еще труднее было доказать, что трансцендентны некоторые хорошо известные числа; математик, доказавший трансцендентность числа π, Линдеманн, обеспечил себе место на математическом Олимпе; см. гл. 48.)

Можно подумать, что такие задачи не возникают в «реальной» жизни, но это не так. За примером можно отправиться в ближайший джаз-клуб. Сотня завсегдатаев раскачиваются в ритме музыки. Кассир замечает, что за вход заплатили только девяносто человек. Можно быть

[1]О бесконечности множества простых чисел можно прочитать в гл. 4.

уверенным, что десять посетителей как-то пробрались, не заплатив, но как вы определите, кто именно?

КРОЛИКИ И КЛЕТКИ

Один из важных методов доказательства — *принцип кроликов и клеток*. Он часто используется в математических неконструктивных доказательствах существования.

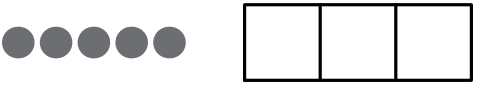


Рис. 61.1. Пять шаров и три ящика: хотя бы в одном ящике два шара

Идея проста. Допустим, в комоде есть n ящиков и имеется более n шаров, которые нужно в ящиках разместить. Тогда хотя бы в одном ящике окажется по меньшей мере два шара. Можно быть уверенным, что так оно и есть, даже не открывая ящики и не задумываясь, в каком ящике или в каких ящиках более одного шара.

Принцип ясен всем, даже тем, у кого нет опыта в раскладывании шаров по ящикам. Например, если вы рассовали три носовых платка по двум карманам, то хотя бы в одном кармане обнаружится не меньше двух платков.

А как же доказывают сам принцип кроликов и клеток? Замечательно, что его нельзя доказать прямо. Приходится доказывать то, что в логике называется противопоставлением, — это излюбленный метод Шерлока Холмса. Если мистер X — не преступник, то миссис Y должна была видеть его. Но миссис Y его не видела, поэтому мистер X должен быть преступником.

В нашем случае мы докажем следующее. Если в каждом ящике не более одного шара, то в комоде не более n шаров. Но в комоде более n шаров, и поэтому утверждение о том, что в каждом ящике «не более одного шара» не может быть истинным.

Типичное математическое приложение может выглядеть так. Даны одиннадцать случайных натуральных чисел.

Тогда ясно, что по крайней мере два из них заканчиваются на одну и ту же цифру. Просто нарисуйте в своем воображении такую картину: десять ящиков пронумерованы цифрами $0, 1, 2, \ldots, 9$, каждое из одиннадцати чисел помещено в ящик, соответствующий последней цифре.

Можно представлять себе n ящиков, в которых нужно разместить более n кроликов. Тогда по крайней мере в одном ящике окажется хотя бы пара кроликов. Видимо, тот, кто назвал «принципом кроликов и ящиков» этот метод доказательства, был большим любителем кроликов.

Глава 62

О ЧЕМ ГОВОРИТ СТАТИСТИКА?

Почти каждый день — и даже в серьезных газетах — можно найти информацию о последних статистических исследованиях: ученые открыли, что математики живут дольше физиков; кататься на велосипеде опаснее, чем ходить пешком; и т. д.

Откуда берутся такие утверждения? Что статистика может нам сказать? Увы, ответ разочаровывает, так что давайте рассмотрим конкретный пример.

Допустим, вы отправились в любимый магазин товаров для досуга и купили пару игральных костей. Продавец убеждает вас, что каждая кость совершенно сбалансирована. Придя домой, вы испытали эти кости и обнаружили, что при бросании одна кость все время падает тройкой вверх. Потребуете ли вы обменять кость? Сбалансирована ли она?

Рис. 62.1. Ничего подозрительного?

Простого ответа на этот вопрос нет, поскольку с некоторой (весьма малой) вероятностью на абсолютно правильной кости может выпасть тройка сто раз подряд. Обычно никто не ожидает осуществления крайне невероятных событий, и поэтому действуют следующим образом. Прежде чем проверять кость, выбирают множество M исходов, которое ожидается с вероятностью, скажем, 99%, если кость бросают 100 раз. Например, M может быть множеством исходов, в которых 3 выпадает не более 40 раз. Тогда если ваша новая кость дает 3 сто раз из ста (или даже хотя бы только 45), вы можете считать, что купили дефектную

вещь. Конечно же, вы можете ошибаться, но это крайне маловероятно (не больше 1%).

Обычно всему этому учат с использованием математических терминов вроде нулевой гипотезы и доверительных интервалов, но общая идея всегда одна: полагайте, что невероятные события не осуществляются.

Конечно же, правильность кости — достаточно безопасный пример, но бывают ситуации, когда в вопросах надежности на кону стоит гораздо больше. Эффективность нового лекарства; вероятность заболеть раком, живя неподалеку от ветрогенератора; опасность пассивного курения — все это оценивается статистически на основе того же принципа.

К сожалению, аккуратные и тщательно проработанные формулировки статистиков что-то теряют в пересказах журналистов. Причину легко понять: то, что можно утверждать честно в терминах доверительных интервалов, редко можно представить в виде хлесткой новости.

МЕНЯТЬ ЛИ МНЕ ПОСТАВЩИКОВ?

Для реалистического примера статистических методов возьмите на себя роль оптового покупателя радиодеталей. Только что вам доставили партию транзисторов. Правда ли, что процент дефектных товаров меньше 3%, как гарантирует производитель?

Конечно же, вы можете проверить каждый транзистор, но, во-первых, это заняло бы слишком много времени, а во-вторых, в процессе проверки транзисторы часто получают повреждения. Поэтому вы решаете проверить двадцать транзисторов. Результат: два из них дефектны.

Теперь покупатель рассуждает так. Насколько вероятен полученный результат, *если* доля дефектных товаров не превышает 3%? Он чертит табличку вроде той, что изображена ниже, в которой указаны вероятности того, что из двадцати транзисторов 1, 2, 3, 4 оказываются дефектными, если процент дефектов не превышает 3:

Число дефектных изделий	0	1	2	3	4
Вероятность	0,55	0,33	0,10	0,02	0,003

Ясно, например, что вероятность двух дефектных деталей из двадцати при данных условиях равна 0,1, или 10%.

Нельзя сказать, что это крайне невероятное событие, так что пока нет серьезных оснований для отказа от партии. Четыре дефектных транзистора — это уже тревожный сигнал. Конечно же, это не вовсе невозможный исход, поскольку мы все же допускаем три процента дефектных транзисторов, а это тридцать штук из тысячи. Так что может случиться так, что в выборке из двадцати транзисторов может оказаться больше ожидаемого числа дефектных, но все же полученный результат выглядит совершенно невероятным, и поэтому больше нельзя соглашаться с предположением «дефектных транзисторов не более 3%».

Уровень недоверия может быть выражен в числах[1)]. Следует меньше доверять поставщику, для которого нет позитивной истории сотрудничества. Даже с умеренно невероятным исходом было бы правильно не принимать партию. Но если на протяжении многих лет у вас с поставщиком были доверительные отношения, только крайне невероятный результат может быть поводом сомневаться в объявленном проценте дефектных товаров.

[1)] Существует технический термин *доверительный интервал*.

Глава 63
АРБИТРАЖ

Одно из ключевых слов в финансовой математике — *арбитраж*. О нем нужно знать две вещи. Во-первых, определение. Арбитраж — это возможность получить прибыль без риска и без вложений капитала. Например, если банк А продает доллары по 0,9 евро, а банк Б покупает доллары по 1 евро, то следует быстро где-нибудь одолжить 900 евро; потратить их на покупку 1000 долларов; тотчас же продать их, выручив 1000 евро; а затем вернуть позаимствованные 900 евро. Вуаля! — вы получили прибыль в 100 евро. Было бы еще лучше, если бы вы могли взять взаймы 9000 евро или даже 90 000 евро. Арбитраж — это как гусыня, несущая золотые яйца.

Увы, вторая вещь, которую нужно знать про арбитраж, — что его не бывает. Фундаментальный закон финансовой математики говорит о том же, что и повседневный здравый смысл: бесплатного сыра не бывает. Однако этот закон не такой строгий, как, скажем, законы физики. Если, например, обменный курс в Гонконге хоть немного отличается от курса во Франкфурте, то будут перемещены крупные суммы, чтобы воспользоваться возможностью арбитража. В процентах разница может быть минимальной, но для миллиардов евро она станет очень заметной. Мы с вами никогда не разбогатеем таким образом, поскольку банковские комиссионные платежи окажутся выше прибыли.

А теперь займемся математикой. Принцип «бесплатного сыра не бывает» работает как законы движения Ньютона или как второй закон термодинамики. Его цель — построить формулы цен для всех возможных опционов (подробнее об этом написано в следующей главе). Принцип арбитража играет большую роль в опционной торговле. Он используется следующим образом: только когда цена за некоторый опцион предполагает некоторое специальное

значение, арбитраж исчезает. Поэтому это и есть цена, которую следует назначить за опцион.

Несколько лет назад за вычисления — конечно же, очень сложные, — проведенные согласно этому принципу, была присуждена Нобелевская премия. Она стала наградой за вывод формулы Блэка–Шоулза, играющей большую роль в ценообразовании опционов.

АРБИТРАЖ КАК «ЗАКОН ПРИРОДЫ»

Принцип «арбитража не бывает» играет в финансовой математике такую же роль, как законы природы (например, сила равна произведению массы на ускорение) в физике. Его можно использовать для того, чтобы делать новые открытия.

Рассмотрим, например, договор, согласно которому в наступающем году я получаю гарантированную выплату в 100 000 евро. Платеж может быть связан, например, с переводом сложного портфеля акций, за который гарантированно будет получена сумма в 100 000 евро в конце оговоренного срока. Сколько я должен заплатить за такой контракт?

Предположим, что я могу взять кредит под 4% годовых[1)]. Принцип арбитража гласит, что стоимость контракта равна в точности $100\,000/1{,}04 = 96\,154$ евро. И вот почему.

- Что было бы, если бы контракт можно было купить дешевле, скажем, за 90 000 евро? Тогда я бы взял в банке в кредит 90 000 евро и купил бы контракт. Через год я получил бы свои 100 000 евро. Вернул бы кредит в банк: 90 000 евро и еще за проценты $90\,000 \cdot 0{,}04$, всего 93 600 евро. У меня бы осталось 6 700 евро — абсолютно безрисковая прибыль! Но поскольку арбитража не бывает, никто не предлагает таких контрактов за 90 000 евро. Те же рассуждения годятся для любой цены ниже 96 154 евро.
- А что произошло бы, если бы такие контракты продавались дороже, чем за 96 154 евро, скажем, за

[1)] И мы будем считать, что я могу получить 4% накоплений.

98 000 евро? Тогда я бы сам их продавал. Покупатель платит мне 98 000 евро. Я кладу 96 154 евро в банк на депозит, и оставляю себе 98 000 – 96 154 = 1 846 евро. Арбитраж! Я легко выполняю свои обязательства, поскольку в конце срока контракта мои 96 154 евро вырастут до 100 000 евро, которые я и выплачу своему клиенту.

Мораль такова. Для цен выше 96 154 евро существует арбитраж, и поэтому таких цен не бывает.

Есть только одна цена — 96 154 евро, — которая не приводит к арбитражу, и поэтому это и есть справедливая цена контракта.

Глава 64

ПРОЩАЙ, РИСК. ОПЦИОНЫ

Представьте себе, что вы владеете виноградником, где выращиваете каждый год около десяти тонн винограда. Вы продаете весь виноград виноделу, поскольку, хорошо разбираясь в выращивании винограда, не умеете делать вино.

К сожалению, вы не можете знать наверняка, сколько именно винограда можете поставить на рынок, собрав урожай. Чтобы гарантировать разумную выручку, вы хотите обеспечить себе что-то вроде «страхового полиса». Вы устанавливаете на свой виноград цену P, которая кажется вам разумной, а затем отправляетесь на поиски кого-нибудь, кто готов заключить с вами очередной контракт. Вы платите партнеру определенную сумму за подписание контракта. Если осенью цена на виноград будет меньше P, то партнер выплатит вам разницу. Если цена на виноград будет больше P, вы получаете доход и ваш партнер ничего вам не должен.

Такие соглашения заключаются каждый день десятками тысяч; они называются *опционами*. Это контракты,

направленные на то, чтобы уменьшить или вовсе исключить риск неопределенного дохода. Застраховать таким образом можно почти все: рыночные цены на виноград, сахарный тростник и золото; цены на доллары, электричество, акции телекоммуникационных компаний и т. д.

Опционы стали крайне удобным инструментом. Например, мы можете отправиться в свой банк и приобрести опцион на покупку десяти тысяч акций телекоммуникационной компании 3 октября по 20 евро за акцию. Если рыночная цена в этот день окажется меньше, то банк будет доволен, поскольку вы не станете покупать акции. Если рыночная цена будет выше, то банк заплатит вам разницу. И никто даже и не спросит, действительно ли вы купили акции или потратили деньги на отпуск.

Здесь вступает в игру математика, поскольку в таком контракте партнер должен знать, сколько контракт стоит для вас. Вычисляя это, нужно помнить принцип арбитража, о котором мы говорили в предыдущей главе. А именно, никто не может получить прибыль, не рискуя. После введения нужных параметров — процентных ставок, ожидаемых изменений на рынке акций, рыночных цен, сроков контракта — цену можно вычислить.

На рынке есть огромное число различных опционов, и каждый день появляются всё новые, так что у математиков много работы. Большие банки приглашают их на работу сотнями, а в университетах ведутся исследования и разрабатываются новые модели, позволяющие получать всё более точные предсказания.

Но нужно помнить: опционная торговля очень привлекательна, ведь если повезет, можно удвоить свои вложения за считанные недели. Но иногда обстоятельства складываются не так, как хотелось бы, и вы теряете свои деньги. Поэтому те, кого по выходным тянет делать ставки, могут предпочесть поставить несколько евро в национальной лотерее.

ПУТ ИЛИ КОЛЛ?

Международный язык финансов — можно сказать «разумеется» — английский. Некоторые термины вы встретите почти наверняка.

Если хотят что-то продать, то интересуются *опционами пут*. Так было с владельцем виноградника, о котором мы рассказывали. Нужно договориться с банком о деталях: сколько следует заплатить за виноград в конце срока действия контракта (это будет важно, конечно же, если цена окажется ниже указанной в контракте)? Это *страйк-цена*. Логично, что более высокая страйк-цена делает опцион дороже.

Наиболее распространены опционы двух стилей — европейский и американский опционы пут. Для европейского стиля дата контракта фиксирована. Например, размер выплат может зависеть от рыночной цены на виноград 31 октября. Если опцион американский, то можно отправляться в банк в любой момент до определенной даты, скажем, конца июля, и погасить контракт. Так поступают, если цены на виноград особенно низки.

Для тех, кто хочет что-нибудь купить, подходят *опционы колл*. Если 13 декабря мне понадобится пять тонн сахара, при помощи опциона колл я могу гарантировать цену, скажем, в 2000 евро. Если в декабре цены на сахар возрастут, и я должен буду заплатить 2500 евро, то банку придется выплатить мне разницу в 500 евро. В этом случае тоже есть две разновидности — американский и европейский опционы, и, как и раньше, чем ниже цена сделки, тем дороже опцион.

С опционами работают даже те, кто не нуждается в пяти тоннах сахара, а просто собирается разбогатеть путем чистых спекуляций. Постоянно растущая доля опционных сделок связана с их удобством.

Глава 65

ОТРАЖАЕТ ЛИ МАТЕМАТИКА РЕАЛЬНЫЙ МИР?

«Правильная» ли у нас математика? Наивный ответ — да, конечно же! Ведь многие математические законы складываются из нашего опыта в реальном мире, и мир отражает наши математические законы. Например, абстрактный результат «неравенства можно складывать» гармонирует с нашим опытом, что делать покупки в супермаркете дешевле, чем в бутике. Поскольку в супермаркете дешевле каждая вещь по отдельности, общий счет тоже будет меньше.

Но если перейти от обычных чисел к более сложным объектам, ответ становится не таким очевидным. Например, нужно знать точные фундаментальные законы функций, чтобы строго доказать, что непрерывная функция обязана в некоторой точке принять нулевое значение, если она принимает и отрицательные, и положительные значения. Это должно быть «очевидно» всем, но математики не довольны, пока не найдут выверенного доказательства. Еще сложнее показать, что на рис. 65.1 любой путь из точки A в точку B должен пересекать окружность.

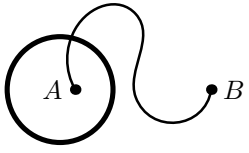


Рис. 65.1. Любой путь из A в B пересекает окружность

Действительно, все «знают», что должна быть точка, в которой путь пересекает окружность, однако четкого понимания задачи со строгими формулировкой и доказательством удалось достичь только 150 лет тому назад. Задача состоит из двух частей. Во-первых, нужно разобраться, что же такое путь, соединяющий две точки, и как

выразить тот факт, что на пути нет «разрывов». Во-вторых, после этих уточнений нужно доказать существование точки пересечения.

Иногда между формулировкой задачи и удовлетворительным решением проходит много времени. Хорошо известен пример из теории узлов[1)]. Здесь тоже все «знают», что некоторые узлы развязать нельзя, как ни старайся. Однако потребовалось много усилий, чтобы этот очевидный факт из нашего повседневного опыта обрел строгость математической теоремы.

Формулировка и доказательство «очевидных» фактов как математических теорем необходимы, поскольку мы не можем вполне доверять нашим опыту и интуиции. И все становится еще сложнее, когда мы вторгаемся в области, не поддающиеся чувственному восприятию. Возьмем, например, царство бесконечности. Здесь открываются поразительные законы. Например, на одной части прямоугольника помещается столько же точек, сколько на всем прямоугольнике, и этому утверждению можно придать совершенно строгий смысл.

Кроме того, для описания на современном научном уровне того, что происходит на космических или микроскопических расстояниях, требуются математические модели, совершенно недоступные непрофессионалу. Однако только такие модели могут описать четырехмерное пространство-время из общей теории относительности или законы квантовой механики.

В этом смысле математика предоставляет «корректные» строительные детали, но только после долгих поисков становится понятно, какие именно из них следует использовать для моделирования нашего мира.

УДВОЕНИЕ АПЕЛЬСИНА

Даже в математическом описании явлений, недоступных непосредственно нашему чувственному восприятию, есть следствия, согласующиеся с ожиданиями обычного человеческого разума. Однако иногда приходится осознавать, что

[1)] Подробнее о теории узлов можно прочитать в гл. 76.

существуют результаты, совершенно неожиданные с точки зрения повседневного опыта. Общепринятое понятие равенства бесконечных множеств говорит о том, что число элементов бесконечного множества не изменится, если удалить из него три или даже три тысячи элементов (см. гл. 78).

Ситуация может оказаться и еще более драматичной. В примере с бесконечностью можно утешить себя тем, что такие парадоксы появляются в областях, к работе с которыми эволюция нас не подготовила. Но бывают и парадоксы, относящиеся к самым элементарным понятиям. Знаменитый пример — *парадокс Банаха–Тарского*. В нем говорится о том, что, используя общепринятые методы, можно разделить шар — например, апельсин, — на кусочки таким образом, что из них можно сложить вдвое больший шар. См. рис. 65.2.

Рис. 65.2. Волшебство?

Требуется тщательный анализ, чтобы убедиться в истинности утверждения, которое на первый взгляд кажется полным бредом. Возможность удвоения апельсина обусловлена тем, что при «разрезании» сферы края кусочков становятся настолько зигзагообразными, что никак нельзя приписать им разумного понятия объема. И поэтому нельзя воспользоваться доводом о том, что как ни переставлять кусочки, объем остается неизменным.

Если когда-нибудь в будущем математические методы приведут к результатам, «несовместимым» с действительностью, то так или иначе потребуется перестройка оснований этой науки.

Глава 66

МАТЕМАТИКА, КОТОРУЮ СЛЫШНО

Сегодня мы расскажем о Жане Батисте Жозефе Фурье. В начале девятнадцатого века он построил анализ, который мы называем сегодня *анализом Фурье*. Его жизнь была полна событий, связанных с Французской революцией. Помимо прочего, Фурье участвовал в экспедиции Наполеона в Египет и написал научную работу, в которой впервые были систематизированы египетская история и культура.

Анализ Фурье — один из главных инструментов работы математиков и инженеров. В его основе лежит простое представление колебательных явлений. Мы ограничимся музыкальными звуками, т. е. звуковыми колебаниями. «Атомы» тона — синусоидальные волны различной частоты (рис. 66.1). Если хотите, можете услышать такой звук прямо сейчас. Присвистните: то, что вы услышите, — почти чистая синусоидальная волна.

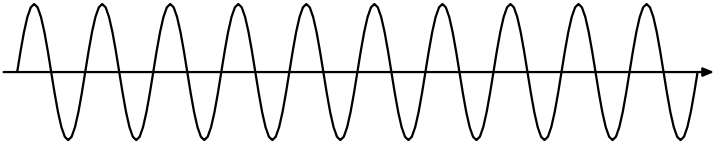


Рис. 66.1. Синусоида

Согласно теории различные синусоиды различной интенсивности должны складываться, чтобы дать нужную форму волны. Для музыкальных звуков начинают с синусоид основной частоты, добавляют синусоиду удвоенной частоты, возможно, капельку утроенной частоты, и т. д.

Наш слух позволяет убедиться в этом. Волна, состоящая из синусоиды и порции утроенной частоты, — хорошее приближение к так называемой квадратной волне. Чтобы мы могли услышать разницу между синусоидой

и квадратной волной, утроенная частота должна попадать в диапазон слышимых звуков, для большинства читателей ограниченных значением 15 килогерц. Поэтому разницу между двумя видами волн можно услышать при основной частоте до 5 килогерц.

Для этого нужен идеальный генератор частоты (возможно, у вас есть приятель-инженер). А может быть, у вас есть синтезатор или еще какой-нибудь электронный музыкальный инструмент? Тогда просто выберите формы волн «синусоидальная» и «квадратная», и можете начинать эксперимент.

Те, кому придется удовлетвориться качественной проверкой теории Фурье, могут обратить внимание на голоса, которые можно услышать на какой-нибудь вечеринке. Низкие мужские голоса гораздо легче разобрать, чем высокие женские. Это потому, что у мужских голосов больше обертонов в слышимом диапазоне, и у нас больше шансов различить их.

ЧЕРНЫЙ ЯЩИК

Есть и другие математические результаты, в корректности которых вы можете убедиться своими ушами, по крайней мере качественно. Вообразите черный ящик, на вход которого подаются сигналы, они как-то внутри ящика обрабатываются и подаются на выход. Любители электроники могут представить себе какой-то сложный электрический контур, в котором сигнал в одном месте подается, а в другом месте измеряется (рис. 66.2).

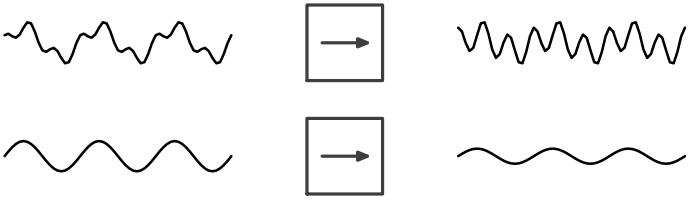


Рис. 66.2. Так работает «черный ящик»

Черный ящик должен обладать следующими свойствами.

- Он должен быть «линейным». То есть если интенсивность входного сигнала удваивается, интенсивность выходного тоже удваивается; а если на вход подается сумма двух отдельных сигналов, то на выходе должен получиться тот же результат, что от сложения выходов этих сигналов.
- Он должен быть «инвариантным по времени». То есть выход для любого заданного входа сегодня должен быть таким же, каким был вчера.

Для любителей электроники это означает, что в схеме нельзя использовать транзисторы (они нелинейны), и во время эксперимента нельзя вносить никаких изменений. Придется ограничиться резисторами, индукторами и конденсаторами, а сила тока и напряжение не должны быть слишком большими.

Хотя такие черные ящики описывают довольно разные ситуации, у них есть одно общее: синусоиды-кирпичики анализа Фурье проходят через черный ящик, почти не изменившись. Они могут ослабеть или выйти из фазы — но это все, что с ними может произойти.

Из всего сказанного следует, что (высокочастотный или низкочастотный) фильтр для акустических сигналов, который может быть описан как черный ящик с линейными свойствами, не изменяет характера синусоидальных волн. Если в такой фильтр свистнуть (это дает хорошее приближение к синусоидальному звуку), на выходе получится свист той же частоты. С другой стороны, звук голоса при пении может совершенно изменить свой характер; он может стать гораздо более приглушенным или, напротив, пронзительным.

РЕЦЕПТ ПЕРИОДИЧЕСКИХ ВОЛН: ФОРМУЛА ФУРЬЕ

Согласно теории Фурье для синусоид периодические колебания складываются. Каков же точный рецепт, т. е. в какой пропорции различные функции входят в результат?

Рассмотрим, например, функцию f, график которой изображен на рис. 66.3.

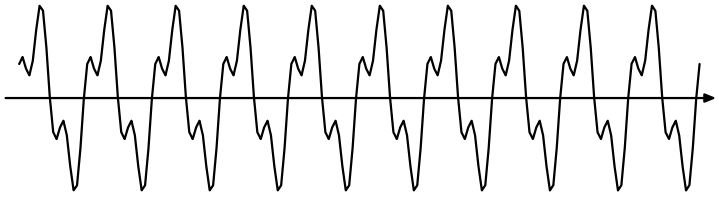


Рис. 66.3. Периодическая функция

Существует число p (период) такое, что значение функции в точке $x+p$ всегда совпадает с ее значением в точке x. Поэтому достаточно знать значения функции на некотором интервале I длины p, таком, как отрезок на рис. 66.4.

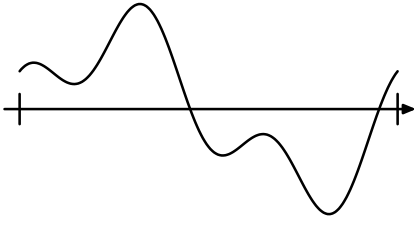


Рис. 66.4. Период функции f

Функции обычно нормируют и считают, что период равен 2π, тогда формулы получаются особенно простыми. Этого легко добиться, если подходящим образом выбрать единичный отрезок на оси абсцисс.

И наконец, нужно знать, что такое *интеграл*. Идея проста. Если функция g определена на некотором интервале, то интеграл функции g по этому интервалу равен площади области между графиком функции и осью абсцисс. При этом считают, что любая часть области, лежащая ниже оси абсцисс, имеет отрицательную площадь. Например, если область между положительной частью графика функции и осью абсцисс равна 4, а площадь между отрицательной частью и осью абсцисс равна 3, то значение интеграла равно $4-3=1$. А если обе части равны, то интеграл равен нулю. (На рис. 66.4 изображен график такой функции.)

Теперь мы можем вычислить «ингредиенты». Если функция f периодична с периодом 2π, то ее можно записать в виде

$$f = a_0 + a_1 \cos x + a_2 \cos(2x) + a_3 \cos(3x) + \cdots + \\ + b_1 \sin x + b_2 \sin(2x) + b_3 \sin(3x) + \ldots,$$

где sin и cos обозначают функции синус и косинус[1]. «Веса» $a_0, a_1, \ldots, b_1, b_2, \ldots$, использованные для построения функции f, определяются следующим образом:

- коэффициент a_0 равен интегралу функции f (на интервале от 0 до 2π), деленному на 2π;
- коэффициент a_1 равен интегралу функции $f(x)\cos x$ (на интервале от 0 до 2π), деленному на π;
- коэффициент a_2 равен интегралу функции $f(x)\cos(2x)$ (на интервале от 0 до 2π), деленному на π; ...
- коэффициент b_1 равен интегралу функции $f(x)\sin(x)$ (на интервале от 0 до 2π), деленному на π;
- коэффициент b_2 равен интегралу функции $f(x)\sin(2x)$ (на интервале от 0 до 2π), деленному на π; ...

Итак, если вы умеете брать интегралы, вы сможете определить количества всех частей, которые составляют периодическую функцию.

[1] Функция косинус на самом деле равна функции синус, сдвинутой по времени. Поэтому в формуле можно обойтись одними только синусами.

Глава 67
СЛУЧАЙ-КОМПОЗИТОР

В гл. 10 мы уже обсуждали тему «случай-писатель»: мартышка за печатной машинкой за достаточно большое время напечатает все шедевры мировой литературы.

В музыке случай эксплуатируется вполне реально. Моцарт (вы видите его портрет) снабдил нас методикой сочинения музыки при помощи игральных костей, основанной на следующих правилах. Бросьте две кости и подсчитайте общее число выпавших очков. Затем из набора под названием «первый такт» выберите такт с соответствующим номером из одиннадцати экземпляров, перенумерованных от 2 до 12. То же самое проделайте для такта 2, для такта 3, и т. д., пока не наберете 16 тактов.

Теперь остается соединить эти такты один за другим и воспроизвести результат. В получившейся пьесе не чувствуется, увы, рука мастера, но ее вполне можно принять за часть сонатины одного из современников Моцарта.

Для каждого из 16 тактов есть 11 возможностей, и потому доступны всего 176 тактов; их можно скомбинировать в одну пьесу 11^{16} различными способами. Однако некоторые из 176 тактов могут совпадать с некоторыми из других 176 тактов, поскольку Моцарт иногда использовал одни и те же строительные кирпичики по нескольку раз. Тем не менее остается 759 499 669 166 482 различные композиции. Поэтому после бросания костей можно быть практически уверенным, что получившаяся пьеса никогда раньше не исполнялась.

В современной музыке случай играет еще более важную роль. В музыке Ксенакиса, например, случай определяет

не только ноты и порядок их проигрывания, но и форму волны для воспроизведения звука.

Возможно, музыка Ксенакиса вызывает энтузиазм лишь у сравнительно небольшого количества слушателей. Однако интересно задать вопрос: какую роль сыграл случай в классической музыке? Что подвигло Шуберта в шестом такте вальса до-мажор перейти в тональность ми-мажор? Почему Моцарт решил написать в ля-миноре рондо «Турецкий марш» в финале сонаты ля-мажор? Это вопрос гению, который черпает свое вдохновение в ином мире, или результат работы некоторых нейронов в головном мозге?

Мы до сих пор не можем глубоко проникнуть в человеческий мозг. Но нас еще ждут сюрпризы: ведь в последние несколько десятилетий мы уже освоились с идеей, что случайные воздействия могут оказать продуктивное и стабилизирующее влияние на результат.

МОЦАРТ ИЗ КОМПЬЮТЕРА?

У того, кто возьмет на себя труд сочинить много пьес по методу Моцарта, через некоторое время возникнет впечатление, что все это уже можно было слышать раньше, даже если эти ноты до сих пор еще никогда не проигрывались именно в таком порядке. Причина в том, что наш мозг способен узнавать музыкальные структуры. Какие созвучия использовались и в каком порядке? Каким интервалам оказывается предпочтение? Если эти аспекты совпадают в двух сочинениях, то они кажутся нам похожими.

Этим знанием можно воспользоваться для того, чтобы после тщательного анализа сочинений Моцарта или Баха запрограммировать компьютер на сочинение музыки, которая звучит так же. Нужно просто вычленить важные аспекты музыкальной структуры и создать что-нибудь новое с такими же параметрами. С какой вероятностью, скажем, в пьесе до-мажор после нот соль и до идет си? А с какой вероятностью ми? Компьютер может учесть это знание: если ноты соль и до идут последовательно, то с предписанной вероятностью за ними пойдет си или ми.

Для среднего слушателя результат будет звучать «вроде Моцарта» или «вроде Баха». Разумеется, новых идей при этом нет и такую музыку никак нельзя назвать вдохновенной.

Основываясь на этом подходе, композитор Орм Финнендаль разработал метод создания гибридных композиций. Анализируют две композиции A и B[1)] и начинают гибридную композицию с параметрами A. Иными словами, все созвучия, ритмы и рисунок мелодии такие же, как в сочинении A. Затем параметры начинают постепенно менять, и к концу пьесы все параметры становятся такими, как в композиции B. В результате пьеса начинается в стиле A, а заканчивается в стиле B.

759 499 667 166 482 ВОЗМОЖНОСТИ?

Для последнего такта в первой части пьесы, созданной по методу Моцарта, т. е. для восьмого такта, есть возможность выбрать из одиннадцати вариантов. Однако все такты идентичны. Поэтому такт 8 заранее фиксирован. Аналогично, для самого последнего такта, шестнадцатого, тоже есть одиннадцать вариантов, но только два действительно различных такта. Для оставшихся четырнадцати тактов с номерами 1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15 действительно есть все одиннадцать вариантов, и поэтому, с учетом того, что для одного из тактов — возможностей только две, всего различных пьес

$$11^{14} \cdot 2 = 759\,499\,667\,166\,482.$$

Можно отметить, что различные произведения могут быть реализованы с разными вероятностями. Это связано с тем, что при бросании пары костей суммы 2 и 12 встречаются довольно редко: каждая из них появляется с вероятностью лишь $1/36$. Средние значения выпадают гораздо чаще; например, вероятность получить в сумме 7 равна $1/6$. Поэтому композиции, соответствующие очень большим или очень малым результатам бросания костей, крайне маловероятны.

[1)] Финнендаль экспериментировал с сочинениями композиторов Джоскина и Гесуальдо.

Глава 68

БЫВАЕТ ЛИ ИГРАЛЬНЫМ КОСТЯМ СОВЕСТНО?

В теории вероятностей бывают чрезвычайно запутанные темы. Допустим, много раз бросают игральную кость. С одной стороны, мы часто слышим, что после «большого» числа бросаний разные числа выпадают примерно одинаково часто. Но говорят еще, что у случая нет памяти, что на каждом бросании все вероятности остаются теми же, какими они были в самом начале.

Как такое может быть? Если кость бросали много раз и при этом не выпала шестерка, не должна ли кость приложить некоторые усилия, чтобы выполнилось первое условие и усреднить результат? Не должны ли увеличиться шансы на выпадение шестерки? Здесь мы встречаемся с той же философией, которая заставляет некоторых выбирать те номера в лотерейных билетах, которые давно не выпадали.

Это противоречие снимается замечанием о том, что «равные возможности» для всех чисел не обязательно приводят к одинаковым результатам: мы ожидаем, что с очень высокой вероятностью разных чисел будет *приблизительно* поровну. Можно вычислить, что в таком эксперименте шансы на то, что все шесть чисел будут выпадать примерно одинаково часто, составляют почти сто процентов. Однако может случиться (хотя вероятность этого исчезающе мала) и нечто крайне неправдоподобное; например, выпадут одни только тройки.

Проиллюстрируем сказанное следующим образом. Представьте себе огромное число параллельных вселенных, в которых проходит один и тот же эксперимент: игральную кость подбрасывают шестьсот раз. В большинстве миров все происходит так, как и должно быть: каждое из чисел от 1 до 6 выпадает примерно по 100 раз. Но найдется несколько миров, в которых результат окажется совершенно неожиданным. Например, выпадут одни тройки (доля таких миров составляет $0{,}000\ldots012$, причем перед

12 идет 466 нулей). Или не выпадет ни одной шестерки (доля таких миров равна 0,00...31, причем перед 31 идет 47 нулей).

Мораль: игральная кость неподкупна и у нее нет памяти. Если результаты неправдоподобны, это означает, что вы столкнулись с экспериментом в очень необычном мире.

НЕСОВЕРШЕННОЕ ПОНИМАНИЕ СЛУЧАЙНОСТИ

Описанное здесь непонимание природы случайности широко распространено. Детям, играющим в пачиси, совершенно ясно, что если шестерки давно не было, то теперь ее выпадения особенно стоит ждать. Не забудем про то мнение, что в Калифорнии следует ожидать серьезного землетрясения, поскольку с момента последней катастрофы прошло больше среднего промежутка времени.

В нашем несовершенном понимании природы случайности убеждает небольшой эксперимент. Возьмите листок бумаги и, не бросая монетку и не проводя еще каких-нибудь экспериментов в этом духе, придумайте и запишите последовательность результатов гипотетических бросаний, обозначая решку нулем, а орел — единицей. У вас получится что-то вроде этого:

1001110010110100011101010010110010100011100101100010100 0...

Настоящий генератор случайных чисел даст последовательность такого вида:

1101010011101000111101111111100111101001011011010011000...

Видите разницу? В действительно случайной последовательности следует ожидать длинных последовательностей решек или орлов. А когда мы сами строим случайную последовательность, бессознательно подгоняем результат.

Глава 69
КЛУБНИЧНОЕ МОРОЖЕНОЕ УБИВАЕТ!

Так происходит со всеми экспертными докладами: что бы вы ни пытались доказать, всегда найдется статистика, которая подтверждает ваше мнение. Вот несколько примеров.

Предположим, вам нужно выяснить посредством опроса, следует ли перестать считать Понедельник Святого Духа праздничным днем и вместо этого сделать его обычным рабочим понедельником. В зависимости от того, как сформулирован вопрос, можно ожидать услышать различные наборы ответов.

С точки зрения профсоюзов, формулировка должна быть иной, чем с точки зрения торговой палаты: одни во главу угла ставят стандарты жизни, а другие — привлекательность Германии для иностранных инвестиций. Внимания заслуживают точки зрения обеих сторон, но при формулировании вопроса должно быть принято решение, которое никогда уже нельзя будет исправить математическими методами.

Или представьте себе директора филиала, который нервничает по поводу предстоящей презентации в главном офисе. В прошлом году продажи возросли со 100 000 только до 101 000 евро, т. е. на один жалкий процент. Если он отобразит этот рост так, как на рис. 69.1 слева, то это будет выглядеть как застой.

Есть ли решение? Ему следует отобразить только верхушку графика так, как изображено на рисунке справа. Столбик, соответствующий прошлому году, поднимается от 90 000 до 100 000, а соответствующий этому году — от 90 000 до 101 000. Теперь второй столбик на 10% выше первого, и ситуация выглядит гораздо лучше.

Еще один метод дурачить людей — подобрать сложный набор статистических данных для нужных утверждений. Если научное исследование показало, что слишком большое потребление клубничного мороженого стабилизирует кровяное давление и вместе с тем в опасной степени поднимает

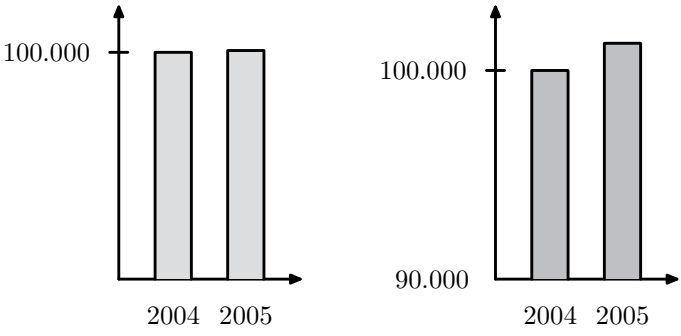


Рис. 69.1. Это вопрос представления...

уровень сахара в крови, то редактору придется выбирать между двумя заголовками: «Путь к здоровью — клубничное мороженое» или «Клубничное мороженое убивает нас».

Мораль в том, что путь к установлению и трактовке истины усеян подводными камнями. И в самом начале уже есть проблема — как найти общепринятое определение «истины». Затем дорогу к истине осаждают те, кто преследует свои собственные интересы. И если в конце концов удастся дойти до вопросов математической статистики, то может быть сформулирован безупречный взвешенный ответ, который потом будет проинтерпретирован кем угодно в соответствии со своими желаниями: «Клубничное мороженое может убить тебя!»

БОГАТЫЙ ИЛИ БЕДНЫЙ

Статистика действительно нуждается в защите от тех, кто видит в ней лишь удобный склад, в котором можно подобрать результаты, поддерживающие личные интересы. Вот еще несколько примеров.

Все дело в определении

Кого можно назвать бедным? Последние несколько лет, читая газетные сообщения, можно было составить мнение, что в Германии растет обнищание населения. Турист, незна-

комый с действительным положением вещей, ожидал бы встретить массы голодающих граждан, одетых в лохмотья.

Однако бóльшая часть этого явления существует только на бумаге[1)]. Причина — в определении понятия «бедный», согласно которому к бедным относят тех, у кого доход ниже среднего по стране. Но это самое знаменитое определение бедности; максимум, что оно позволяет, — приблизительно объяснить, что такое «чувствовать себя бедным». Может быть, и правда некоторые молодые люди полагают, что переживают лишения, если у них нет модных джинсов или мобильного телефона, но разве это означает настоящую бедность, требующую напряженного действия?

Случайное рассеяние

В этих главах мы часто говорили о капризах господина случая. И точно так же, как иногда случается получать всякий раз шесть очков, бросая игральную кость пять раз подряд, некоторые события, происходящие независимо в разных местах, дают совершенно неожиданные совпадения.

Предположим, что в Германии регистрируются заболевания редкой болезнью, примерно две тысячи случаев в год. Если для каждого случая воткнуть в карту булавку в той местности, где он зарегистрирован, в результате получится набор, похожий на порожденный генератором случайных чисел. Неудивительно, что там и сям возникают скопления булавок; понятно, что такое скопление может появиться поблизости от шоссе, или атомной электростанции, или городской свалки. Тогда-то оно становится аргументом для противников скоростных трасс или атомной энергетики, и все статистические доводы игнорируются.

[1)] Чтобы избавить издателя от гневных писем, скажем здесь, что в Германии, как и в других странах, бедные, конечно же, существуют.

Глава 70
ПРОЦВЕТАНИЕ ДЛЯ ВСЕХ

Мы уже говорили раньше, что, как заметил великий Галилео, бесконечность полна сюрпризов. Сегодня проведем мысленный эксперимент, разослав в бесконечность письма счастья.

Идея писем счастья привлекательна тем, что обещает нечто (почти) даром:[1)] я отправляю один евро по указанному адресу и не даю цепочке прерваться, рассылая копию письма десяти знакомым. Каждый из них, в свою очередь, рассылает ее десяти своим знакомым, и те тоже пишут по десять писем. Вот и набралась тысяча человек, каждый из которых должен отправить мне по одному евро. К сожалению, эта чудесная схема нарушается, когда новые знакомые заканчиваются и писать больше некому.

Но в бесконечном мире все не так. Пронумеруем знакомых числами $1, 2, 3, 4, \ldots$. Каждому числу соответствует какой-то человек, а числа могут быть сколь угодно большими.

И игра начинается. Первый человек отправляет письмо счастья следующим десяти, с номерами от 2 до 11. Каждый из них пишет еще десять писем, включая игроков 12–111. Каждый из ста человек должен отправить по десять писем для получателей с номерами 112–1111; и т. д.

Где-то в письме счастья есть фраза «отправь один евро человеку, имя которого стоит тремя «поколениями» раньше тебя в цепочке.» Итак, первый человек получает тысячу писем с приложенным евро от игроков 112–1111. Номера 2–11 тоже получат по одному евро, и когда все закончится, все в мире станут по крайней мере на 999 евро богаче, получив 1000 евро за один-единственный, ими отправленный (начиная с номера 112).

Конечно же, никто не может запретить нам играть в эту игру не с одним евро, а с десятью, с целой сотней

[1)] О письмах счастья мы уже рассказывали в гл. 6.

или даже больше. Не успев опомниться, мы все станем миллионерами. Может ли так случиться? Да, разумеется. Произойдет просто сдвиг денежных сумм от тех, у кого номер больше, к тем, у кого номер меньше. Но поскольку номера становятся бесконечно большими, все участники останутся довольны. Как жаль, что мир, в котором мы живем, конечен. С финансовой точки зрения бесконечный мир был бы раем.

ССУДИТЬ И ВЗЯТЬ ВЗАЙМЫ ОДНОВРЕМЕННО

Как вариант писем счастья можно рассмотреть другую схему самообогащения. Как и раньше, пронумеруем всех граждан числами $1, 2, 3, 4, \ldots$. Первому человеку нужна тысяча долларов, и поэтому он одалживает эту сумму у второго. К несчастью, этот второй — банкрот, поэтому он отправляется к третьему, берет у него взаймы две тысячи, из которых одну отдает первому, а вторую оставляет себе. Увы, капитал третьего гражданина тоже невелик. Чтобы ссудить две тысячи евро, он одалживает у четвертого три тысячи и одну оставляет себе, и т. д. Если бы в этой цепочке был последний участник, на нем повис бы чудовищный долг. Но в бесконечном мире все счастливы и довольны, а экономика жужжит дальше.

Если заменить слово «человек» словом «поколение» и вместо тысяч евро взять миллиарды, то мы получим довольно аккуратное описание финансовой политики Германии (и других индустриально развитых стран) в последние десятилетия. Национальный долг растет на порядки, и связь поколений в будущих поколениях зависит от предположения о последующих долгах, выплата которых отодвигается всё дальше и дальше в будущее.

Порочность этой схемы в том, что ссуды просто так не выдаются. Проценты по долгам тоже должны быть профинансированы за счет дальнейших займов. Это приводит к экспоненциальному росту долга и остается удивляться — как долго финансовые рынки будут соглашаться давать все больше и больше денег для того, чтобы система функционировала.

Такие технологии часто используются не только правительствами, но и обыкновенными мошенниками. Они обещают баснословные процентные ставки и берут первый миллион у как можно большего числа невинных доверителей. Затем живут на всю катушку, оставляя лишь суммы, достаточные для выплаты в конце года баснословных двадцати процентов. Проходит слух, что предприятие надежное, и к мошеннику текут все новые миллионы, достаточные чтобы выплатить проценты на следующем этапе и пуститься во все тяжкие. А когда один из первых клиентов хочет отозвать свой капитал — и с чего бы? — на это тоже хватает. Все это может длиться довольно долго, пока в один прекрасный день вся схема не терпит крах.

Глава 71
НИКАКОГО РИСКА, СПАСИБО!

Допустим, вы — директор банка. В ваш офис входит клиентка и объявляет, что хочет заключить с вами договор с первого января следующего года на покупку пятисот акций некой телекоммуникационной компании. Клиентка полагает, что к тому моменту цена на акцию не будет превышать 20 евро, и хочет, чтобы банк возместил разницу, если цена будет выше.

В наше время такие договоренности — вовсе не редкость. Они называются *опционами*. Гарантии, которые предоставляет клиентке такой договор, достаются ей не даром. После его подписания она должна будет выплатить премию банку. Как вам следует поступить с этими деньгами, чтобы 1 января выполнить обязательства по контракту?

Волшебное слово, в котором заключается решение задачи, — *хеджирование*. В математике финансов хеджирование сделок означает искусное страхование от рисков.

В основе лежит простая и продуманная идея: к сумме, полученной от вашей клиентки, вы добавляете деньги, взятые в долг под рыночный процент, и используете их — деньги клиентки и одолженные — для покупки акций той самой телекоммуникационной компании.

Для чего? Если акции вырастут к 1 января, то они будут достаточно ценными, чтобы вы могли сделать выплаты для покупателя опциона, и еще сможете вернуть взятую в долг сумму с процентами. Будет печально, если акции упадут в цене, но тогда покупатель опциона ничего от вас не потребует, и после продажи своего пакета вы сможете вернуть долг.

Итак, чтобы оградить себя от потерь в такой ситуации, приобретают пакет акций. Вне зависимости от развития событий ваша сделка работает и в случае роста, и в случае падения цен.

Математика вступает в игру, чтобы определить, какова справедливая цена опциона и сколько следует купить

акций. Основываясь на «естественном законе финансовых рынков» (см. гл. 63), а именно, что прибыли без риска не бывает, можно построить уравнение, которое дает решение этой задачи. Сложность в том, что нужно следить за рыночными курсами до истечения срока опциона. Поскольку цены акций и процентные ставки изменяются, нужно решать, не продать ли часть пакета или не взять ли в долг дополнительную сумму.

ХЕДЖ ДЛЯ ТЫСЯЧИ АКЦИЙ

Рассмотрим хеджирование на конкретном примере. Допустим, сейчас январь. Вы хотите приобрести опцион на покупку тысячи акций Интергалактического Предприятия в конце года. Если приобрести их сегодня, это обойдется в 10 000 евро. Однако цена в конце года неизвестна. Она может составить 16 000 евро, или только 8000, в зависимости от множества факторов. (Для простоты мы будем считать, что в конце года осуществится одна из этих возможностей и что мы не будем осуществлять дополнительных сделок в течение года.) В декабре в вашем распоряжении будет 12 000 евро, и если цена составит 8000 евро, то все будет в порядке. Но если цена окажется 16 000 евро, то вы захотите, чтобы банк выплатил вам разницу. Сколько банк может потребовать от вас за такую гарантию и что он будет делать с деньгами, которые вы ему уплатите?

Служащий банка, к которому вы обратились с предложением о покупке опциона, звонит в отдел кредитов и узнает, что внутренняя процентная ставка составляет 6%: за то, чтобы получить $E/1{,}06$ евро сегодня, придется выплатить E евро в конце года. Этой информации достаточно, чтобы рассчитать опционный контракт. В уплату за свои гарантии банк требует от вас выплатить $5000 - \frac{4000}{1{,}06} \approx 1226$ евро[1)].

Вы ставите в нужном месте свою подпись, и дальше события разворачиваются без вашего участия. Кредитное подразделение тотчас же вручает $4000/1{,}06 \approx 3774$ евро банковскому работнику, и теперь в его распоряжении

[1)] Эта сумма не включает банковской комиссии, здесь мы ее игнорируем.

1226 + 3774 = 5000 евро. На эти деньги он покупает 500 акций и забывает про них до декабря.

Допустим, что акции поднялись в цене. В банковском портфеле они теперь стоят 8000 евро (напомним, мы предположили, что в случае роста цен за тысячу акций дают 16 000 евро, а банк купил всего 500). Банк выплачивает вам условленные 4000 евро, и с теми 12 000 евро, которые вы выделили для покупки, вы можете теперь купить 1000 акций Интергалактики за 16 000 евро. У банковского работника остается 4000 евро, которые он возвращает в кредитный отдел.

Если же акции упали, то в банковском портфеле они составят 4000 евро, — только-только чтобы расплатиться с кредитным отделом. Вы же, покупатель опциона, не получаете вовсе ничего, так как ваших 12 000 евро вполне достаточно для покупки акций.

Мораль: используя стратегию хеджирования, вы смогли застраховать риск в 4000 евро за сравнительно небольшую сумму: всего за 1226 евро, ведь именно 4000 вы могли потерять, если бы акции упали в цене.

Глава 72

НОБЕЛЕВСКАЯ ПРЕМИЯ В МАТЕМАТИКЕ?

Бывает ли Нобелевская премия в математике? Еще несколько лет назад ответом было бы твердое и ясное «нет». У математиков есть своя престижная медаль Филдса, которую вручают раз в четыре года на Международном математическом конгрессе. Хотя вручаемая сумма очень скромна, обладатели этой награды могут быть уверены в финансовой стабильности, поскольку на них изливается поток предложений хорошо оплачиваемой работы. Награда лучшему молодому поэту в городе Ванн-Айкель и то больше.

Но в последние несколько лет все изменилось, хотя предыстория награды началась много миллионов лет назад. Тогда геологические процессы привели к образованию поблизости от норвежских берегов целого моря нефти; оно сделало очень богатой эту маленькую страну (всего четыре миллиона жителей).

Много лет спустя после образования этого моря в Норвегии родился один из самых блестящих математиков девятнадцатого века: Нильс Хенрик Абель (1802–1829). Его недолгая жизнь прошла в болезнях и нищете. Предложение академической должности (следует отметить, оно исходило не из родной Норвегии, а из Берлина) пришло слишком поздно. Он был так болен, что не смог его принять.

И только после его смерти на родине признали гениального математика. Чтобы почтить его память, в 2002 г. учредили Абелевскую премию. Ее присуждают ученым, оказавшим особенно большое влияние на развитие математики. Премия составляет около миллиона долларов — почти так же велика, как Нобелевская.

Впервые Абелевскую премию присудили Жан-Пьеру Серру, это было в 2003 г. Затем ее получили сэр Майкл Атья и Изадор Зингер (2004 г.), Питер Лакс (2005 г.), Леннат Карлесон (2006 г.) и Сриниваса С. Р. Варадхан (2007)[1)]. Берлин тоже имеет отношение к этой премии: норвежское посольство любезно финансировало поездку на церемонию награждения команде, выигравшей ежегодный конкурс «День математики», который проводят для берлинских студентов.

АБЕЛЬ И УРАВНЕНИЕ ПЯТОЙ СТЕПЕНИ

Значителен вклад Абеля в различные области математики. В качестве примера рассмотрим его результаты по решению полиномиальных уравнений.

Задача. Многие задачи в приложениях математики сводятся к задаче отыскания всех чисел, удовлетворяющих уравнению вроде $x^2 - 2{,}5x + 3 = 0$ или $x^7 - 1200x^6 + 3{,}1x - \pi = 0$. (Например, такие задачи часто попадаются инженерам. По расположению решений можно судить — останется ли система устойчивой или будет реагировать на малейшие помехи.) Функции, которые здесь появляются (т. е. $x^2 - 2{,}5x + 3$ и $x^7 - 1200x^6 + 3{,}1x - \pi$), называются *многочленами* или *полиномами*. В общем виде многочлены записывают так:

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

где n — некоторое натуральное число, а *коэффициенты* $a_n, a_{n-1}, \ldots, a_0$ — произвольные числа.

Самая большая степень в многочлене называется его *степенью*. В двух рассмотренных нами примерах степени многочленов равны 2 и 7, а степень многочлена общего вида $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ равна n. Мы считаем, что коэффициент a_n не равен нулю. (Если бы он был равен нулю, мы бы просто опустили слагаемое $a_n x^n$.)

Результаты. Только в девятнадцатом веке удалось установить, что у каждого многочлена $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ есть корни. Поскольку,

[1)] А также Джон Томпсон и Жак Титс (2008 г.), Михаил Громов (2009 г.). — *Прим. перев.*

например, у уравнения $x^2 + 1 = 0$ нет действительных корней, нужно поискать решение среди комплексных чисел (и найти решения $x = \pm i$). Если допустить комплексные корни, то окажется, что у многочлена $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ есть решения, даже если сами его коэффициенты — комплексные числа[1)]. Но из существования решений вовсе не следует, что существует простая формула, по которой их можно вычислить. На самом деле такая формула существует только для очень «маленьких» степеней многочлена. Вот несколько примеров.

- Первая степень. Задача заключается в том, чтобы найти число x такое, что $a_1 x + a_0 = 0$, где a_1 и a_0 — заданные постоянные. Такое уравнение относительно x умеют решать все, кто учил алгебру: $x = -a_0/a_1$.
- Вторая степень. Теперь стоит задача найти все значения x такие, что выполняется равенство

  $$a_2 x^2 + a_1 x + a_0 = 0,$$

  где a_2, a_1, a_0 заданы. Поколения школьников заучивали формулу корней квадратного уравнения; их два:

  $$x_1 = \frac{-a_1 + \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}, \quad x_2 = \frac{-a_1 - \sqrt{a_1^2 - 4a_2 a_0}}{2a_2}.$$

- Третья степень. В этом случае явная формула тоже есть, и называют ее *формулой Кардано*, по имени знаменитого итальянского математика Джироламо Кардано, опубликовавшего ее в 1545 г. в своем трактате «Ars Magna».

  Чтобы воспользоваться ею, нужно с помощью линейного преобразования привести уравнение третьей степени к виду

  $$x^3 - ax - b = 0.$$

  Тогда решение можно найти по формуле

  $$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 - \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 - \left(\frac{a}{3}\right)^3}}.$$

[1)] См. гл. 94.

- Четвертая степень. И здесь есть формула для решений, она строится по коэффициентам с использованием знаков +, –, ·, : и извлечением корней. Эта формула была открыта Людовиком Феррари (1522–1565), современником Кардано.

А что дальше? Почему нельзя построить пусть даже и сложные явные формулы для уравнений более высоких степеней? Интенсивные поиски таких формул начались в шестнадцатом веке и закончились только в девятнадцатом, когда Абель решил этот вопрос раз и навсегда.

Теорема Абеля о неразрешимости

В 1924 г. (в юном возрасте 22 лет) Абель показал, что нельзя ожидать результатов, аналогичных тем, что имеют место для степеней 2, 3, 4. Действительно, для уравнений пятой степени нельзя найти формулу — какой бы сложной она ни была, — выражающую решение через коэффициенты.

С тех пор математики знают, что во многих случаях самое большее, на что можно надеяться, — найти величину, сколь угодно близкую к решению.

Теперь добавим, что более подробную информацию об Абелевской премии (и таблице лауреатов вплоть до настоящего времени) вы найдете, пройдя по ссылке http://de.wikipedia.org/wiki/Abelpreis.

Премия дается за достижения математики в прикладных областях, и иногда бывает довольно трудно обеспечить нематематическую общественность этим призом, что рассматривается у лауреатов, как особенно достойная награда. Автор испробовал это на себе: соответственно в воскресенье перед выдачей премий в мае статья размером в целую страницу появилась в журнале «ДиВельт» с попыткой изображения математического закулисья.

Глава 73

СЛУЧАЙ-ВЫЧИСЛИТЕЛЬ: МЕТОД МОНТЕ-КАРЛО

Город Монте-Карло прославился автомобильными гонками, обилием знаменитостей и своими казино. Математики, размышляя за рулеткой над капризами госпожи Удачи, выбрали термин «метод Монте-Карло» для одного способа вычислений, в котором случай играет главную роль.

Рассмотрим, например, сложную фигуру F, лежащую внутри квадрата со стороной длины 1. Как найти площадь F? Классический подход состоит в том, чтобы разбить фигуру на меньшие, площади которых можно вычислить, и просуммировать результаты.

В методе Монте-Карло используется совершенно другой подход. Его самая главная составная часть — генератор случайных чисел, который задает случайные точки на квадрате. При этом важно, что генератор запрограммирован таким образом, что для всех точек квадрата вероятности быть сгенерированными равны. Такое распределение точек называется «равномерным». Сегодня компьютеры могут генерировать миллионы таких точек в секунду. В таких предположениях вероятность того, что выбранная наугад точка попадет в область F, пропорциональна площади последней.

Метод Монте-Карло позволяет экспериментально найти площадь фигуры. Например, если из миллиона сгенерированных точек ровно 622 431 попали на F, то вероятность «попадания» равна примерно 62,2%. Поэтому площадь F должна составлять примерно 62,2% от площади квадрата; последняя равна единице, поэтому в результате эксперимента установлено, что площадь F равна 0,622.

У этого метода есть и достоинства, и недостатки. Самое главное достоинство заключается в том, что метод Монте-Карло легко применим в крайне сложных и запутанных ситуациях; соответствующие программы написать нетрудно, поскольку самая важная их составляющая — генератор

случайных чисел — встроена практически во все существующие языки программирования. Но, к сожалению, не всегда можно полагаться на удачу. Может случиться так, что сгенерированные точки расположатся на квадрате не равномерно, и тогда вычисленная вероятность их попадания на фигуру F не будет соответствовать ее площади.

В силу такого эффекта результаты процедуры Монте-Карло следует интерпретировать аккуратнее, в духе «с 99-процентной вероятностью площадь лежит в пределах от 0,62 до 0,63».

Поэтому нет ничего удивительного в том, что математики по возможности стараются прибегать к точным процедурам. А вы хотели бы ездить по мосту, устойчивость которого гарантирована только с вероятностью 99%?

ВЫЧИСЛЕНИЕ ПЛОЩАДИ ПАРАБОЛИЧЕСКОЙ ФИГУРЫ МЕТОДОМ МОНТЕ-КАРЛО

Рассмотрим, как метод Монте-Карло может быть использован для вычисления площади под параболой. Найдем площадь фигуры, ограниченной параболой и осью абсцисс, когда x меняется от 0 до 1 (рис. 73.1).

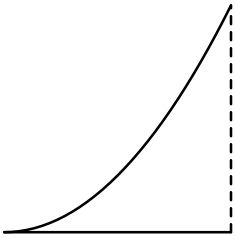


Рис. 73.1. Чему равна площадь под параболой?

Для этой задачи несложно найти и точное решение. Больше двух тысяч лет назад Архимед нашел формулу, которую сейчас выводят в курсе элементарного анализа. Пусть парабола задается функцией $f(x) = x^2$, ее первообразная равна $x^3/3$, и с учетом верхних и нижних пределов получаем площадь $\frac{1}{3}$.

С методом Монте-Карло вы можете забыть про анализ. Есть две разновидности этой процедуры.

Метод первый. Вначале фигуру F, площадь которой нужно вычислить, помещают в какой-нибудь прямоугольник R. В нашем случае мы можем взять квадрат с единичной стороной. Затем компьютер генерирует «много» случайных точек внутри этого квадрата так, чтобы они были равномерно распределены. Затем остается только подсчитать, сколько точек попало внутрь области F. Доля этих точек среди всех выражает отношение площади F к площади R, поскольку точки распределены равномерно.

На рис. 73.2 вы видите типичный пример распределения точек. Всего их 60, и 22 из них попали в область под параболой. Поэтому площадь этой области равна приблизительно 22/60, т. е. 0,366...

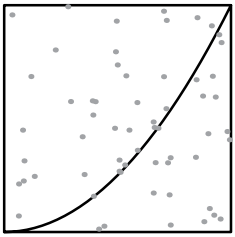


Рис. 73.2. Вычисление площади методом Монте-Карло

Это неплохой результат для такого небольшого числа точек. Компьютер легко сгенерирует много раз по столько точек; при этом точность и надежность вычислений повысятся.

Метод второй. Этот метод основан на теоретико-вероятностной интерпретации. Искомая площадь равна среднему выигрышу в игре, в которой наугад выбираются точка x из интервала $[0,1]$ и выплачивается сумма x^2. Чтобы воспользоваться этим фактом, можно написать компьютерную программу. Обнулим регистр памяти r и заставим компьютер генерировать случайные числа в диапазоне от 0 до 1. Каждое из этих чисел возводится в квадрат и суммируется в регистр r. (Например, если сгенерировано случайное число 0,22334455, то значение r должно

увеличиться на $0{,}22334455 \cdot 0{,}22334455 = 0{,}4988278801$.) Эта операция проделывается очень много раз, а затем результат делится на число сгенерированных случайных чисел (здесь мы обозначим его n). На «псевдокоде» эта программа выглядит так:

```
.
.
.
n:=10000;
r:=0;
for i=1 to n do
begin y:=random; r:=r+y*y; end;
r:=r/n;
.
.
.
```

Когда программа закончит работу, в регистре r будет храниться число, приблизительно равное площади под параболой. Мы свели в таблицу результаты нескольких компьютерных испытаний:

Число n испытаний	10 000	10 000	100 000	100 000
Регистр r	0,3338399	0,336283	0,33350	0,33304

Замечательно то, что можно получить значение, довольное близкое к истинному $0{,}3333\ldots$, не прибегая к интегрированию. Весь процесс занимает доли секунды, причем функции могут быть гораздо сложнее. Единственный минус — никогда нельзя быть на сто процентов уверенным в результате. Только зная результат заранее, можно сказать, насколько точной оказалась аппроксимация. А без этой информации остается только уповать на компьютер и законы теории вероятностей, и если речь идет о вопросах жизни или финансов, нужно семь раз отмерить, прежде чем один раз отрезать.

Глава 74
НЕЧЕТКАЯ ЛОГИКА

Совсем недавно в рекламе пылесосов и стиральных машин говорилось, что они оперируют с «нечеткой логикой». Идею такой логики в 1970 г. предложил профессор математики и информатики из Беркли Лофти Аскер Заде. Он построил математические основания для того способа рассуждений, которым мы пользуемся в повседневной жизни.

Математики обычно настаивают на строгости, и поэтому для них есть только «правда» и «ложь». Целое число может или быть простым, или не быть, и нет никаких промежуточных положений между этими двумя.

Но в повседневной жизни мы не ограничиваемся только черным и белым. В зависимости от доступной информации наши представления об истинности некоторого утверждения могут быть довольно расплывчатыми: безопасен ли выбранный способ передвижения? Перспективно ли данное предприятие?

Нечеткая логика призвана «очеловечить» математику, допуская, что о суждении можно сказать не только «истина» или «ложь», но оценить его любым значением от 1 (бесспорная абсолютная истина) до 0 (бесспорная абсолютная ложь). Например, значение 0,9 можно приписать утверждению, в истинности которого мы «почти уверены».

Замечательно, что бóльшая часть теорем классической логики может быть перенесена в нечеткие рамки. Например, нечеткие утверждения можно соединять: если утверждения p и q имеют высокие истинностные значения, то же самое можно сказать и об утверждении «p и q». Это вполне согласуется с нашим опытом и поэтому привлекает многих математиков.

Аналогичный подход можно использовать для контролирования более или менее сложных процессов. Предположим, робот должен уравновесить доску на горизонтальной пластине. Точное моделирование такой ситуации — крайне

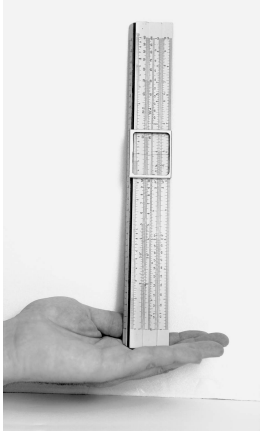
тонкая вещь, но его несложно втиснуть в рамки нечеткой логики. Можно поставить нечеткие значения в соответствие степеням отклонения доски от вертикали — что-то вроде «доска немного повернута влево», или «доска сильно развернута влево», и так далее. Если смещение влево составляет, скажем, 10 градусов, то значение для утверждения «немного влево» может быть равным 0,6, а для утверждения «сильно влево» — 0,4. (Поскольку нам кажется что 10 градусов — это скорее «немного», чем «сильно», — для «немного» нечеткое значение больше.) Кроме того, можно предусмотреть, как робот должен реагировать в ситуации «немного влево» или «сильно влево»: что-то вроде «подвинуть на дюйм вправо» или «на три дюйма влево», например. После этого проводится наблюдение за перемещением и его оценка: чем «истиннее» получился результат, тем больше устанавливается доля соответствующей реакции.

Такая процедура позволяет использовать такие человеческие знания, которые не могут быть выражены математической формулой. Однако для большинства математиков нечеткая логика — кустарное изделие. Для своих пылесосов они предпочли бы точную логику, даже если это не сказывалось бы на результатах работы.

НЕЧЕТКОЕ УПРАВЛЕНИЕ

Классическая теория управления — сложная математическая дисциплина. Большой вклад в ее развитие был сделан американским математиком Норбертом Винером (1894–1964), придумавшим слово «кибернетика». Идея состоит в контроле за оптимальной системой: желательно добиться, чтобы некоторые значения достигались как можно быстрее (или дешевле), при этом для управления процессом можно менять некоторые параметры. «Система» может представлять собой цепь химических реакций на фармацевтической фабрике, доменную печь или вражескую ракету, которую нужно сбить. Методы, разработанные в этой области, распространены неимоверно широко. Ситуация может быть довольно сложной: полная информация доступна не всегда, поскольку контроль может

осуществляться только с задержкой, или случайные помехи могут менять процесс непредсказуемым образом. Как правило, функции управления задаются очень сложными уравнениями, и точные решения доступны только в исключительных случаях.



Как мы уже говорили, *нечеткое управление* может сделать жизнь гораздо проще. За системой наблюдают, а потом оценивают, в какой мере текущая ситуация соответствует различным сценариям. Если уравновешиваемая доска наклонилась на пять градусов вперед, то это может привести к следующему распределению сценариев, описанных ранее («сильно отклонить назад», «не отклонять», «немного наклонить вперед», «сильно наклонить вперед»): 0,0; 0,2; 0,8; 0,0. Затем опрашивают «экспертов», что нужно предпринять в случае, если доска сильно отклонилась назад? Отклонить немного назад? и т. д. Если среди прочего выяснится, что ничего предпринимать не следует, когда отклонения нет[1)], и что при небольшом наклоне вперед нужно подвинуть доску на пять дюймов вперед, то эти две реакции комбинируются пропорционально их участию в описанном нами сценарии: «ничего не делать» — с коэффициентом 0,2; «подвинуть доску на пять дюймов вперед» — с коэффициентом 0,8. В результате доска будет перемещена на $0{,}8 \cdot 5 = 4$ дюйма.

Поразительно, что так можно работать с довольно сложными задачами управления. Решение может получиться «дерганным» по сравнению с классическим, но зато «нечеткость» гораздо проще в исполнении.

[1)] Конечно же, вы могли бы догадаться об этом сами, не прибегая к помощи экспертов.

Глава 75

СЕКРЕТНЫЕ ПОСЛАНИЯ В БИБЛИИ

Для математиков числа — это объекты, свойства которых нужно изучать и использовать в вычислениях. Математики не приписывают числам никаких мистических свойств. Однако с давних пор существует традиция, известная еще Пифагору, видеть в числах нечто большее. Например, числам могут приписывать некоторую значимость («парность — купель изменений», «тройка говорит о мудрости и знании»), а затем использовать это качество в ходе принятия решений.

Следует ли покупать дом, если сумма цифр в адресе — «несчастливое» число? Кого-то может смутить номер подержанной машины (покупать или не покупать) или дата рождения будущего супруга; числа есть всюду.

Особое распространение мистика чисел получила в девятнадцатом веке. Было такое популярное занятие: буквам алфавита приписывали определенные значения, и таким образом получали числа, соответствующие именам людей. Если в результате получалось 666, — «число зверя», о котором упоминается в Библии, — то это, несомненно, должно было что-то означать:

Здесь мудрость. Кто имеет ум, тот сочти число зверя, ибо число это человеческое; число его шестьсот шестьдесят шесть (Св. апостол Иоанн, Отк.13:18).

У этого метода есть уязвимое место. Существует так много способов сопоставить буквам цифры, что у подсчитывающего есть огромный простор, чтобы повлиять на результат. Например, в романе Толстого «Война и мир» удалось сопоставить с Наполеоном число 666, только если его имя записать не вполне верно как «Le Empereur».

Еще один всплеск числового мистицизма случился в 1997 г. после публикации книги М. Дрознина «Код Библии» (M. Drosnin. «The Bible Code»). Автор предложил теорию, что в оригинальной иудейской библии в зашиф-

рованном виде хранится много информации о событиях прошлого и будущего.

Споры добрались и до профессиональных математических журналов, поскольку вначале было неясно, как такое огромное количество столь точных предсказаний долго могло оставаться неизвестным. Но оказалось, что метод Дрознина приводит к аналогичным результатам для любого текста, лишь бы тот был достаточно длинным. Нужно только хорошо постараться.

Конечно же, такие игры не ограничиваются одной только Библией — существуют и современные варианты. Например, порицатели компании Microsoft при желании могут найти число 666 в имени Билла Гейтса. Для этого нужно только «правильно» записать имя как «B. & Gates» и сопоставить это с буквами в ASCII-кодах:

	B	.	&	G	A	T	E	S	Сумма
ASCII-код	66	190	38	71	65	84	69	83	**666**

Но это не единственный способ разоблачить Билла Гейтса[1]. Его полное имя — Уильям Генри Гейтс III, поэтому любой вправе посмотреть, что будет, если записать его как «BILL GATES 3», и вуаля:

	B	I	L	L	G	A	T	E	S	3	Сумма
ASCII-код	66	73	76	76	71	65	84	69	83	3	**666**

Следует признать, что здесь есть доля жульничества. Во-первых, ASCII-код цифры 3 равен вовсе не 3, а 51. А во-вторых, пропущен пробел между именем и фамилией, а его ASCII-код равен 32. Прямой перевод имени Билла Гейтса в числа ни разу не обнаружил ничего зверского.

ИСТОКИ МИСТИЦИЗМА У ПИФАГОРЕЙЦЕВ

Историю числового мистицизма можно проследить до глубокой древности. Впервые он обнаруживается у пифагорейцев, последователей Пифагора (около 500 г. до н. э.).

[1] Этот способ в 1995 году появился в журнале Harper.

В древних цивилизациях Египта и Междуречья числа были важным инструментом вычислений в астрономии, архитектуре, и никакого особого смысла им не придавали. Спустя два века после Пифагора греческие математики тоже не видели в них ничего мистического; в огромном математическом компендиуме, «Началах» Евклида, нет таких упоминаний.

После заката пифагорейской школы числовой мистицизм был почти забыт до появления нео-пифагорейцев в начале нашей эры. И с тех пор он прочно удерживает свое место в сокровищнице всего иррационального. Особенно в трудные времена, когда люди ищут объяснения своих проблем и помощи, а религия им кажется недостаточной, вдруг опять становится важно, что 1 — «хорошее» число, а 2 — «плохое».

Хотя для математиков во всем этом нет ни малейшего смысла, не сто́ит полагать, что у настоящих ученых обязательно есть иммунитет против мнений, которые в наше время многие считают иррациональными. Иоганн Кеплер, открывший, что планеты движутся по эллиптическим орбитам, пытался вывести расстояния от планет до Солнца через соотношения между вписанными одно в другое Платоновыми телами (кубом, тетраэдром, октаэдром, икосаэдром, додекаэдром). А великий Ньютон в поисках секретных сообщений, зашифрованных в Библии, проводил больше времени в своей алхимической лаборатории, чем тратил на написание книги «Principia Mathematica», — а ведь она торжественно открыла победоносное шествие математических методов в царство естественных наук.

ЗАКОН «МАЛЫХ ЧИСЕЛ»

«Мистические» связи иногда возникают лишь потому, что число малых чисел мало. Математик назвал бы этот принцип «законом малых чисел».

Математические доказательства бесспорны. Каждому, кто хочет разложить пять шариков в четыре ящика, придется поместить более одного шарика хотя бы в один ящик. Математики называют этот принцип «принципом Дирихле» (о роли этого принципа как метода доказатель-

ства можно прочитать в гл. 61). Согласно этому принципу при выявлении взаимосвязей между понятиями неизбежно довольно часто будет повторяться малое число. Например, хорошо известны такие тройки:

- три грации (Аглая, Ефросина и Талия),
- три царя (Каспар, Мельхиор и Валтасар),
- три мушкетера (Атос, Портос и Арамис),
- три времени (прошлое, настоящее и будущее).

Такое совпадение не означает вовсе ничего, но нумерологи считают, что когда в группу входят три элемента, — это очень важно.

Те, кто интересуется этим предметом, могут прочитать две очень интересные книги:

- Underwood Dudley: Die Macht der Zahl. Birkhäuser, 1999.
- Harro Heuser: Die Magie der Zahlen. Herder Spektrum, 2003.

Глава 76

НАСКОЛЬКО УЗЛОВАТЫМ МОЖЕТ БЫТЬ УЗЕЛОК?

Вообразите, что где-то в чулане у вас есть электрический провод-удлинитель. Вы включаете его самого в себя, т. е. вставляете вилку в розетку на другом конце удлинителя: получается замкнутый контур.

Если, перед тем как вы это проделали, удлинитель был более или менее запутанным, то теперь он станет безнадежно заузленным (рис. 76.1). Можно ли распутать узел, не вынимая вилку из розетки? Иначе говоря, можно ли превратить его в большую окружность? Понятно, что иногда это можно сделать, а иногда нельзя.

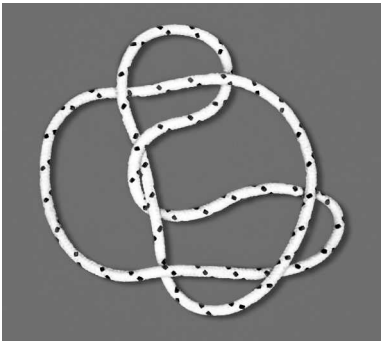
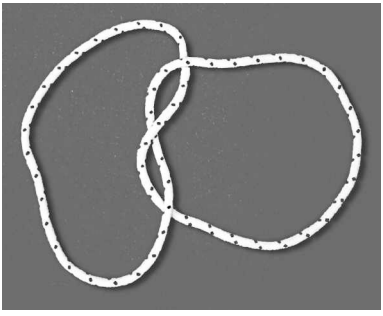


Рис. 76.1. Можно ли развязать этот узел?

Но в каких именно ситуациях? Этот вопрос занимал математиков несколько столетий. Конечно же, не как теория удлинителей, но как теория общих абстрактных узлов. Сразу же встает задача построить подходящий словарь для формулирования этого вопроса об узлах. Ее поставил еще Лейбниц, но удовлетворительное решение было получено только в конце девятнадцатого века. Точная формулировка достаточно сложна, так что мы ограничимся моделью с удлинителем.

Поразительно, но потребовалось несколько десятилетий, чтобы был получен ответ на один из самых простых вопросах об узлах. Факт, известный каждому, кто хотя бы раз пробовал завязать узел, был строго доказан лишь в 1930 г.: некоторые узлы развязать нельзя, как ни старайся. Вот простейший пример такого узла: лист клевера.



Задача классификации гораздо сложнее. Как разделить на категории огромное множество самых разных узлов? Над этим вопросом математики работают сейчас.

Развитие теории узлов важно для физики. В 1867 г. английский физик Ульям Томсон (позднее лорд Кельвин) предложил новую и оригинальную атомистическую теорию, в соответствии с которой атом представляется в виде извилистой линии в эфире; атомы можно представлять себе как перепутанные кольца дыма. Разнообразие всевозможных атомов тогда соответствовало бы различным базовым типам узлов. Так возникла задача классификации и началась систематическая разработка теории узлов.

В современной физике идеям Кельвина места не нашлось. Однако теория узлов стала жизненно необходимой для физики по другой причине. Она играет важную роль в *теории струн*, которая пытается объяснить базовую структуру материи.

ИНВАРИАНТЫ УЗЛОВ

Прошло 230 лет с формулировки вопроса «существуют ли узлы, которые нельзя развязать?» до его первого ре-

шения математиком Куртом Райдемайстером (1893–1771). В 1932 г. он предложил использовать *инварианты узлов*.

Вначале объясним идею инвариантов на простом примере.

Рассмотрим следующую простую «игру». На столе лежат десять камешков; ход игры заключается в том, чтобы выложить на стол семь камешков (из неограниченного запаса) или снять со стола семь камешков (если это возможно).

Задача. Может ли в некоторый момент игры на столе оказаться ровно 22 камешка?

Решение. Нет. Такого быть не может, и это можно доказать, используя несложный метод инвариантов. В каждый момент игры мы рассматриваем остаток от деления числа камешков на столе на семь[1)]. Тогда ясно, что должны выполняться три вещи.

- В начале игры остаток равен 3.
- Любой ход в этой игре не меняет остатка при делении на 7, поскольку камешки на столе добавляются или убираются по семь штук.
- Для числа 22 остаток от деления на 7 равен 1.

Таким образом, в ходе описанной процедуры невозможно получить число 22.

А теперь вернемся к теории узлов. Райдемайстеру пришло в голову использовать для узлов аналогичный подход. Вначале он определил то, что можно было бы назвать «простой ход в игре с узлами». Всего оказалось три различных вида «движений Райдемайстера». Это манипуляции с узлами вида «передвинуть одну петлю полностью над другой». Важно, что любая манипуляция над узлом может быть представлена в виде последовательности движений Райдемайстера.

А затем Райдемайстер определил инвариант — такое свойство узла, которое не может измениться при этих движениях. Если узел обладал этим свойством до движения, то будет обладать и после.

[1)]То есть, как было сказано в гл. 22, ищем сравнение этого числа по модулю семь.

К сожалению, инвариант этот сложнее, чем «остаток при делении на 7» из описанного нами примера. Инвариант Райдемайстера заключается в возможности раскрасить плоское изображение узла определенным образом.

Суть подхода Райдемайстера в том, что можно доказать следующие утверждения.

- Инвариант не меняется при движениях Райдемайстера.
- Замкнутый контур, т. е. не заузленный узел, нельзя раскрасить указанным образом.
- Некоторые узлы, такие как лист клевера, раскрасить можно.

Отсюда следует, что узел «лист клевера» развязать нельзя.

Надо заметить, что этот результат вовсе не дает ответа на все оставшиеся вопросы. Если узел можно раскрасить, то его нельзя распутать. Но обратное необязательно верно: во многих случаях этот метод не позволяет определить, можно ли распутать узел, поскольку существуют узлы, которые раскрасить нельзя, но распутать можно. Поэтому остается задача найти другие инварианты, позволяющие отличать узлы, которые распутать можно, от тех, которые распутать нельзя.

Поиск таких инвариантов составляет предмет многих исследований. Долгосрочная цель — *универсальный инвариант*, т. е. легко проверяемое свойство узлов, которому узел удовлетворяет в том и только том случае, когда его можно распутать. Но пока эта цель кажется очень далекой.

Глава 77

СКОЛЬКО МАТЕМАТИКИ НУЖНО ЧЕЛОВЕКУ?

Сколько математики нам в действительности нужно? Нам правда нужны квадратные уравнения, графики функций и интегралы? Разве не достаточно уметь считать и знать таблицу умножения, чтобы знать, сколько заплатить в бакалейной лавке и сколько оставить чаевых в ресторане? Некоторые готовы пойти еще дальше и передать даже эти вычисления карманным калькуляторам, которые теперь встраиваются в любой мобильный телефон.

Не стоит воспринимать такие радикальные предложения всерьез. С тем же успехом можно защищать отмену преподавания родного языка (ведь есть программы проверки правописания) или географии (на это есть Гугл). Тем не менее вполне правомерен вопрос о том, каким должно быть место математики в современной системе образования.

Я полагаю, есть *три момента*, которые обусловливают глубокое изучение предмета в школьной программе. Во-первых, нельзя спорить с тем, что математика *полезна* для решения конкретных задач реального мира. Начиная с вычислений в уме у прилавка в булочной, и переходя почти ко всем ветвям науки. Любому студенту, планирующему стать инженером, заниматься естественными, гуманитарными, социальными науками или медициной, требуется серьезная подготовка хотя бы по основам статистики. Компьютеры не заменят этой подготовки, какими удобными бы ни были программы. Человек, который не в состоянии провести простые вычисления, чтобы проверить результат работы компьютера, не заметит, если кассир в супермаркете нечаянно введет неверную цену, ошибившись в положении запятой. И даже самый совершенный программный пакет не снимает с пользователя ответственности; только пользователь может проверить, подходит ли данный пакет в данной ситуации, только пользователь может выяснить, на какие вопросы

позволяют ответить собранные данные; только пользователь может проинтерпретировать результаты. Без математики люди отдают себя на милость барышников и спекулянтов, а долговременные экономические планы, такие как покупка дома, превращаются в опасную азартную игру для тех, кто не в состоянии оценить величину задолженности.

Во-вторых, математика — невероятно захватывающее интеллектуальное приключение. Решение задач требует настойчивости и креативности — в процессе воспитания этим качествам невозможно уделить слишком много внимания. Ответственные за персонал в крупных компаниях любят повторять, что эти качества, которыми обладают студенты-математики, не менее важны, чем техническая осведомленность о делах фирмы. Математик привыкает возиться с задачей до тех пор, пока не будет получено решение. Без сомнения, это качество ценится высоко в любой профессии.

И в-третьих, нельзя забывать, что «наш мир построен на математических принципах». Со времен Галилео нам известно, что книга природы написана на языке математики. Поэтому всякий, кто желает познать глубинную сущность мира, должен быть знаком с числами, геометрическими объектами и вероятностью.

Математика играет важную роль во всех базисных концепциях естественных наук. Философ не осмелился бы на попытку вести речь об онтологии, не имея базовой математической подготовки для понимания теории относительности и теории вероятностей.

К сожалению, обучение в школе обычно ограничивается техническими приемами. Для того чтобы получать хорошие оценки, достаточно запомнить несколько рецептов; поэтому ученики с такой математической подготовкой так и не прикасаются к сути. Это словно бы учить французский язык, ограничившись исключительно грамматикой и не прочитав ни одного стихотворения Бодлера. Но это уже другая история[1)].

[1)] См. гл. 31.

ГДЕ ОБ ЭТОМ ПРОЧИТАТЬ

Большинство глав в этой книге можно рассматривать как иллюстрацию этих трех аспектов важности математики, которые мы сегодня обсуждали. Вот некоторые примеры:

- «Математика полезна»: гл. 1, 7, 9, 14, 21, 62, 63, 64, 71, 90, 91, 93, 98.
- «Математика увлекательна»: гл. 4, 15, 17, 18, 23, 33, 48, 49, 76, 99.
- «Математика — язык природы»: гл. 38, 47, 51.

Глава 78
МНОГО, БОЛЬШЕ, ЕЩЕ БОЛЬШЕ!

На рынке продают две корзины яблок, и вы хотите купить ту, где яблок больше. Как решить — которую? Первое, что приходит в голову, — подсчитать яблоки в обеих корзинах и сравнить результаты.

А если вы пока не умеете хорошо считать? Все равно можно провести сравнение, — просто вынимайте по одному яблоку из каждой корзины, пока одна из них не опустеет. В ней яблок было меньше.

Точно так же можно сравнивать размеры множеств, даже если нет возможности подсчитать количество их элементов. Эту идею основатель теории множеств Георг Кантор успешно применил к бесконечно большим множествам. Нужно только слегка подкорректировать пример с яблоками. Вместо того чтобы вынимать их парами, яблоки из первой корзины раскладывают в ряд. Затем яблоки из второй корзины тоже раскладывают в ряд параллельно первому, так чтобы напротив яблока из одной корзины лежало яблоко из другой. Точное соответствие рядов укажет на то, что яблок в корзинах поровну, если же точного соответствия нет, то это будет замечено сразу же.

Мы воспользуемся этим способом, чтобы показать, что нечетных чисел «столько же», сколько четных. Нужно только расставить элементы множеств $2, 4, 6, \ldots$ и $1, 3, 5, \ldots$ «в две шеренги», чтобы четное число 2 было напротив нечетного 1, четное 4 — напротив нечетного 3, четное 6 — напротив нечетного 5, и т. д. каждому четному числу будет соответствовать нечетное, на единицу меньшее.

Кантор обнаружил несколько удивительных явлений, связанных с размерами числовых множеств. Рассмотрим, например, множество рациональных чисел — их можно представить в виде дроби, т. е. отношения двух целых чисел, например $7/9$ или $1001/4711$. В этом множестве столько же элементов, сколько в множестве натуральных

чисел 1, 2, 3, ..., — и это вовсе не очевидно. На первый взгляд кажется, что дробей должно быть гораздо «больше», чем целых чисел.

Кантор также показал, что множество дробей ничтожно мало по сравнению с множеством всех чисел, — тех, которые можно представить в виде бесконечной десятичной дроби. Последних так много, что нет никакой возможности поставить им в соответствие натуральные числа 1, 2, 3 ....

Во многих отношениях бесконечности ведут себя как обычные числа. Например, их можно сравнивать так, что о любых двух бесконечных множествах можно сказать — они одного размера, или одно из них больше, «бесконечнее» другого. Арифметика бесконечных множеств полна подводных камней, парадоксы и неожиданные выводы встречаются на каждом шагу. И поэтому по большей части в математике имеют дело с множествами, которые «не слишком велики».

ДРОБЕЙ И НАТУРАЛЬНЫХ ЧИСЕЛ ПОРОВНУ

Мы уже говорили, что дробей и натуральных чисел поровну, и сейчас с помощью рисунка покажем, почему этот удивительный факт верен. Однако вначале нужно четко осознать, что утверждение «в множестве M столько же элементов, сколько натуральных чисел» означает, что через элементы множества M можно проложить такой маршрут, что по дороге встретится каждый элемент этого множества в точности по одному разу. Это верно, например, для множества четных чисел. На n-м шаге мы попадаем в число $2n$, при этом каждое четное число встречается ровно однажды; например, число 4322 — на 2161-м шаге.

Но как можно обойти все дроби, чтобы посетить каждую? Кантору пришла в голову такая идея. Запишем все дроби в следующем, вполне определенном, порядке. В первой строке запишем все дроби со знаменателем 1:

$$0, 1, -1, 2, -2, 3, -3, \ldots .$$

Знаки чередуются, так что отрицательные числа тоже попадают в эту строку.

Во второй строке запишем все (несократимые) дроби со знаменателем 2:

$$\frac{1}{2}, -\frac{1}{2}, \frac{3}{2}, -\frac{3}{2}, \frac{5}{2}, -\frac{5}{2}, \ldots .$$

В следующих строках запишем дроби со знаменателем 3, 4, 5, и т. д.

Получим бесконечную таблицу, в которой все дроби встречаются по одному разу. Например, дробь 12/1331 находится в 1331-й строке. Остается только проложить маршрут, проходящий через все эти дроби. Примитивный подход не сработает. Если отправиться вдоль первой строки, никогда не удастся добраться до ее конца, так что на этом пути никогда не встретится дробь $\frac{1}{2}$. Фокус в том, чтобы путешествовать вдоль диагоналей, как показано на рис. 78.1.

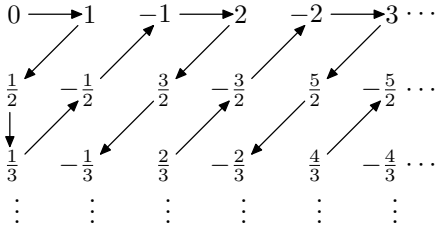


Рис. 78.1. Маршрут, который проходит через все дроби

Начинаясь в нуле, маршрут проходит через числа $1, \frac{1}{2}, \frac{1}{3}, -\frac{1}{2}, -1, \ldots$. Хотя нелегко сообразить, куда попадет путешественник, скажем, на десятитысячном шаге, все же ясно, что рано или поздно ему встретится каждая дробь. И поэтому натуральных чисел и дробей поровну.

Глава 79

ВЕРОЯТНО, ЭТО ВЕРНО

В последние десятилетия стало ясно, что роль случая заключается не только в том, чтобы вызывать непредсказуемые разрушения. В гл. 73 мы уже говорили о методе Монте-Карло, когда сложные вычисления поручаются случайному процессу. Сегодня мы расскажем о более фундаментальных вещах — о том, как случайность помогает устанавливать истину.

Например, рассмотрим большое число n, в котором несколько сотен цифр. Для криптографических приложений может быть важно знать, простое ли оно. Поскольку число большое, прямые методы проверки неприменимы, и нужно искать другие подходы к этому вопросы.

Из теории чисел известно, что если число n — не простое (т. е. составное), то по меньшей мере половина чисел между 1 и n обладает связанным с n легко проверяемым свойством P, а если n — простое, то чисел с таким свойством нет ни одного. (Точная природа P здесь для нас несущественна.) Теперь можно проверить число n на простоту, используя генератор случайных чисел, который выдает числа x между 1 и n, а затем проверяет, обладают ли они свойством P. Проверка дает отрицательный результат в двух случаях: если число n простое и если n составное, но так совпало, что число x относится к тем, которые не обладают свойством P. Если результаты многократных проверок оказались отрицательными, то крайне неправдоподобно, чтобы число n оказалось составным. После двадцати отрицательных тестов вероятность того, что число n не простое, равна приблизительно 2^{20}, т. е. одной миллионной.

Так математики приходят к утверждениям вроде «с ошеломляющей вероятностью это число просто». Во многих приложениях такие «практически простые» числа вполне подходят. А если кого-то тревожит, что «простое число» с вероятностью одна миллионная может оказаться

составным, то можно провести не двадцать, а сорок проверок, и получить «простое число», которое является составным с вероятностью одна триллионная. Хотя простота таких чисел не доказана математически строго, их вполне можно использовать во многих приложениях.

Более того, во многих случаях даже не нужно знать точную величину ошеломляющей вероятности. Если методика позволяет взламывать код с пятидесятипроцентной вероятностью, то кодировщику остается только молиться. А вы бы спокойно спали ночью, если бы у вашей входной двери снаружи висела связка ключей, половина из которых открывает замок?

Нужно подчеркнуть, что во многих приложениях все же лучше придерживаться классических методов, когда можно получить точное решение. Действительно, стали бы вы подниматься на девяносто пятый этаж здания, устойчивость которого «доказана» с вероятностью девяносто девять процентов?

ВЗЛАМЫВАНИЕ СЕКРЕТНЫХ КОДОВ С ВЫСОКОЙ ВЕРОЯТНОСТЬЮ

В связи с изложенным хочется рассказать об алгоритме Питера Шора, который позволял бы раскладывать на множители число, являющееся произведением больших простых чисел, если бы существовали квантовые компьютеры (см. гл. 23). Еще раз отметим, что современные методы шифрования считаются безопасными именно из-за сложности факторизации больших чисел[1)]. Поэтому в криптографическом мире алгоритм Шора был подобен бомбе.

Итак, предположим, что p и q — большие простые числа: обозначим их произведение n: $n = p \cdot q$. Нам понадобится еще случайное число x из промежутка от 1 до n, — с этим вполне справляются классические компьютеры со встроенными генераторами случайных чисел. Известно, что множители n легко найти, если знать некоторую характеристику числа x, называемую *период*, которая

[1)] Этот вопрос обсуждался в гл. 23.

обладает свойством P по крайней мере в половине случаев. Тогда квантовый компьютер можно запрограммировать так, чтобы он вычислял период с очень высокой вероятностью. Сам алгоритм заключается в следующем.

(1) Сгенерировать случайное число x из промежутка от 1 до n (это можно быстро сделать и на современных компьютерах).

(2) Вычислить кандидата для периода x на квантовом компьютере (это тоже было бы быстро, если бы квантовые компьютеры существовали).

(3) Повторять шаг (2), пока период x не обнаружится наверняка (такую проверку можно быстро выполнить и на современных компьютерах).

(4) Проверить, обладает ли период свойством P (и это тоже можно поручить современному компьютеру). Если результат отрицательный (число не обладает свойством P), вернуться к шагу (1) и взять другое случайное число x.

(5) Использовать число x, чтобы найти p и q, после чего без проблем взломать код.

Отметим, что случай играет важную роль *дважды*. Во-первых, период определяется только с некоторой вероятностью, а во-вторых, только половина (по меньшей мере) чисел x подходит для определения множителей числа n. В данном приложении это не такой серьезный недостаток — ведь не так уж важно, займет ли расшифровка закодированного сообщения на пару минут больше времени или меньше.

В последнее время разговоры о квантовых компьютерах поутихли. Во-первых, никто не знает, как справиться с огромными техническими проблемами, стоящими на пути по-настоящему интересных криптографических приложений. А во-вторых, оказалось поразительно сложно формулировать интересные задачи так, чтобы квантовый компьютер мог дать их решения с высокой вероятностью.

Глава 80

ЖИВЕМ ЛИ МЫ В СКРЮЧЕННОМ МИРЕ?

Один из пиков развития математики приходится на времена двухтысячелетней давности, когда Евклид создал системную компиляцию оснований планиметрии. Каковы соотношения между углами, образованными прямой, пересекающей пару параллельных прямых? Чему равна сумма углов треугольника? Трапеции? Что это значит — проводить построение циркулем и линейкой?

Точность подхода впечатляет, но в содержании нет ничего удивительного. Всякому ясно, что через две точки можно провести только одну прямую. Или что через точку P, не лежащую на прямой L, можно провести только одну параллельную ей прямую.

Другими словами, аксиомы Евклида призваны внести точность в повседневную действительность и выразить ее математически, поэтому его геометрия до середины девятнадцатого века воспринималась как бесспорная.

Но потом математики поставили под сомнение евклидову точку зрения на мир. Например, великий Карл Фридрих Гаусс (см. гл. 25) провел вычисления в огромном треугольнике, образованном пиками высоких гор (Брокен, Инзельберг и Высокий Хаген), чтобы убедиться, что на Земле сумма углов треугольника действительно составляет 180 градусов. В пределах точности измерений евклидова геометрия дала правильный ответ; а примечательно здесь то, что Гаусс считал необходимым сравнить теорию с действительностью.

В тридцатых годах девятнадцатого века Бойяи с Лобачевским независимо от Гаусса и друг от друга построили неевклидовы геометрии. Это было сделано формально, в том же духе, что и евклидова геометрия. Однако в этих геометриях сумма углов треугольника необязательно составляет 180°. Затем в 1850 г. Бернхард Риман развил

теорию, представив очень общую модель абстрактных геометрий.

На протяжении нескольких десятилетий эти идеи были известны только специалистам, но получили широкое распространение, когда общая теория относительности Эйнштейна продемонстрировала, что структура вселенной лучше всего моделируется геометрией Римана. Если бы вселенная была двумерной, то ее можно было представить себе волнистой поверхностью, кривизна которой в каждой точке определяется массой, сосредоточенной в этой точке.

Эта довольно абстрактная теория проверяется экспериментально. Измеренные кривизны крайне малы, меньше ошибки измерений в эксперименте Гаусса с треугольником в горах. Но даже столь малая разница между евклидовой и эйнштейновой геометриями может оказаться значимой в нашей повседневной жизни. Например, синхронизация спутников глобальной навигационной спутниковой системы (ГЛОНАСС) опирается на общую теорию относительности.

ТРЕУГОЛЬНИК С СУММОЙ УГЛОВ 270°

Нужно подчеркнуть, что в своих измерениях Гаусс в действительности имел дело с треугольником, стороны которого — прямолинейные отрезки, соединяющие горные пики. В конце концов, для измерений он пользовался собственными глазами, а поскольку в однородной среде свет распространяется по прямой, в результате получился треугольник с прямолинейными сторонами.

Однако большие треугольники на Земле можно получить и по-другому. Можно представить себе треугольник, который лежит на поверхности Земли и определяется тремя точками, попарно соединенными маршрутами кратчайшей длины по поверхности; сокращать путь, роя туннели сквозь земную кору, не разрешается.

Кратчайшие пути между двумя точками на сфере называются *дугами больших кругов*. Они соединяют точки вдоль круговых дуг, центры которых совпадают с центром сферы. (Возможно, вы интересовались, почему полет из Нью-Йорка в Гонконг проходит над Северным полюсом, а не над Гавайями, например. Дело в том, что дуга большого

круга, соединяющая эти два города, проходит неподалеку от Северного полюса.)

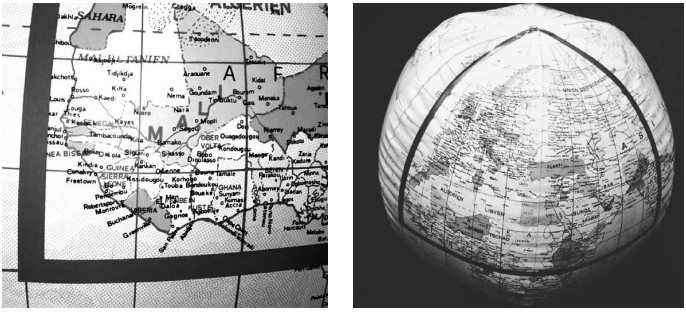


Рис. 80.1. Прямой угол и прямоугольный треугольник на Земле

Если дуги большого круга интерпретировать как прямые, то получится *сферическая тригонометрия*, к явлениям которой нужно еще привыкнуть. Например, несложно нарисовать треугольник, все три угла которого равны 90° (рис. 80.1). Так что в отличие от геометрии плоскости на сфере сумма углов треугольника может быть равна 270 градусов. Чтобы нарисовать такой треугольник, нужно начать с Северного полюса, двигаться вдоль большого круга до экватора, затем повернуть на запад или восток (по вкусу) и идти вдоль экватора около шести тысяч миль (точнее, ровно четверть окружности Земли), после чего повернуть на Север и вдоль дуги большого круга вернуться на Северный полюс.

Глава 81

БЫВАЮТ ЛИ В МАТЕМАТИКЕ СТАНДАРТЫ?

Вначале было слово. Как и в других областях человеческой деятельности, в математике обозначения и соглашения играют важную роль. Почему число, которое выражает отношение длины окружности к диаметру, обозначается именно π, и никак иначе? Почему два в степени нуль равно единице?

Есть много оснований для таких соглашений. Иногда они появляются в определенный момент и остаются в истории раз и навсегда, но гораздо чаще соглашения оттачиваются постепенно с самыми прагматическими целями. Например, при работе с соотношениями между элементами круга часто возникает число π: длина окружности в 2π раз больше радиуса, где π приблизительно равно $3{,}149\ldots$. Нет ни одной причины, по которой именно это число, а не какое-либо другое, с ним связанное, получило специальное обозначение. Можно было бы сэкономить много чернил, если бы собственное имя получило число, которое вдвое больше π, а именно $6{,}28\ldots$. Допустим, его обозначили бы ω, и тогда в историю вошло бы простое соотношение «длина окружности в ω раз больше радиуса». В высшей математике дважды π, т. е. ω, встречается гораздо чаще, чем π. Но теперь уже поздно! У попытки ввести такую реформу в математике не больше шансов, чем у идеи повсеместного распространения языка эсперанто или у предложения Джорджа Бернарда Шоу об упрощении английской орфографии.

Ситуация проще, когда математические соглашения основаны на целесообразности и возникают в результате просвещенной лени. Так, соглашение о том, что любое ненулевое число a, возведенное в нулевую степень, равно 1 ($a^0 = 1$), избавляет от необходимости запоминать сложные законы работы с экспонентой, с множествами частных случаев, так что нужно выучить только одну формулу и работать с ней.

В этой связи мы рассмотрим определение *трапеции*. В математике трапецией называют четырехугольник с парой параллельных сторон. Однако в школьных учебниках трапеции всегда рисуют так, что параллельны не вертикальные их стороны (как на рис. 81.1 в центре), а горизонтальные, причем верхняя короче нижней (на том же рисунке слева). Мало того, у этих трапеций всегда *ровно одна* пара параллельных сторон. У прямоугольника тоже есть параллельные стороны — целые две пары. Но если прямоугольник не считать трапецией, все результаты, уже доказанные для трапеций, пришлось бы передоказывать для прямоугольника, а это до крайности неэкономично.

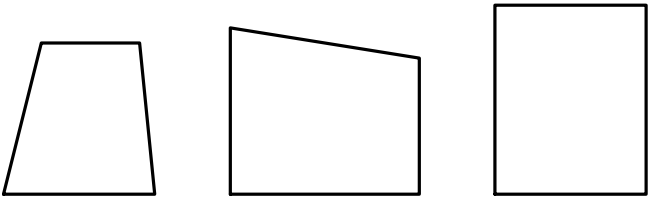


Рис. 81.1. Несколько трапеций

Нигде в мире не бывает математических стандартов. Когда предлагают новые термины или обозначения, математическое сообщество со временем их принимает или отвергает без особого шума: обычно математики тратят свою энергию на более важные вещи. Тем, кому математика кажется чем-то «данным свыше», довольно сложно представить компромиссы и соглашения, возникающие в математическом сообществе. В конце концов, прямоугольник тоже считается трапецией в силу общепринятого соглашения — у трапеции есть *по крайней мере* одна пара параллельных сторон, а не *ровно одна* пара, — а не потому, что Господь на небесах или совет мудрецов во время оно приняли такой закон.

ПОЧЕМУ 1 — НЕ ПРОСТОЕ ЧИСЛО?

После того как эта статься была опубликована в газете, мое внимание обратили на то, что на самом деле в Германии есть группа ученых, которые хотели бы ввести нормы

в математике вроде норм DIN (*Deutsche Industrie-Normen* — Немецкие индустриальные стандарты). Однако, хотя для введения таких норм есть вполне веские основания, уже много лет большинству профессиональных математиков такие предложения неизвестны.

Тому есть множество причин. Прежде всего, сказывается инерция: люди привыкают к терминологии и обозначениям, с которыми познакомились еще в школе. А кроме того, есть проблема здравого смысла и удобства. Например, если нужно записать утверждение «A — подмножество B», как лучше это сделать: $A \subset B$ или $A \subseteq B$? Второе обозначение представляется более разумным, поскольку понятие подмножества допускает, чтобы оба множества совпадали, и поэтому символ $\subseteq$, похожий на символ $\leqslant$ («меньше или равно»), кажется более подходящим чем $\subset$, который похож на символ $<$ («строго меньше»). Но эти доводы не сыграли никакой роли. Символ встречается так часто, что обозначение $\subseteq$ обычно уступает место обозначению $\subset$, и это экономит кучу места на доске. (Комиссия DIN, конечно же, выбрала бы $\subseteq$.)

И наконец, существуют еще проблемы, которые следовало бы назвать идеологическими. Так, смысл символа $\mathbb{N}$ зависит от того, относят нуль к натуральным числам или нет. Многие (например, логики) считают, что $\mathbb{N}$ обозначает множество $0, 1, 2, 3, \ldots$, но большинство математиков считают, что это множество $1, 2, 3, \ldots$.

В итоге не так важно, какое именно соглашение принято, нужно только внимательно читать введение в математический текст, чтобы знать, чего ждать на следующих страницах. Как правило, выбирают такие обозначения, которые упрощают формулировки в повседневной работе.

Если определить простое число как натуральное число, которое делится только на себя и единицу, то саму единицу придется считать простым числом. Но за это мы бы заплатили потерей утверждения о том, что любое целое число единственным способом представляется в виде произведения простых чисел: ведь теперь справедливо будет не только разложение $2 \cdot 3$, но и $1 \cdot 1 \cdot 2 \cdot 3$ — в первом два «простых» множителя, а во втором — четыре.

Единственность разложения на простые множители очень нужна математикам, поэтому единице не выдают пропуска в клуб простых чисел. Так что определение, проверенное обычаем и полезностью, выглядит так: простое число — это натуральное число больше 1, которое делится только на единицу и само на себя. Поэтому во всем мире, от Тувы до Вануату, от Дублина до Люблина, 2 — наименьшее простое число, что и гарантирует единственность разложения.

Глава 82

ВЗМАХ КРЫЛЬЕВ БАБОЧКИ

«Бабочка взмахнула крыльями в Греции, и во Флориде пронесся торнадо». Это утверждение из *теории хаоса* хорошо известно широкой публике, разве что слова «Греция», «Флорида», «торнадо» заменяются другими географическими названиями или видами бедствий. Что же именно означает это утверждение?

Если глубоко не копать, то оно, конечно же, верно, ведь все «так или иначе» зависит от всего. Однако эту зависимость невозможно описать точно, поскольку точное знание движения воздуха вокруг бабочки лежит за пределами наших возможностей.

Полет бабочки часто используют как иллюстрацию явления, присущего всем областям нашей жизни: небольшое изменение начальных значений некоторого процесса может значительно повлиять на его результат. Любой игрок в бильярд знает, что малейшее изменение направления кия приводит к драматическим изменениям в расположении шаров после удара.

Такие утверждения имеют скорее философский, нежели практический смысл. Начальное положение системы может быть нам известно только с некоторой (неизбежной) ошибкой, и поэтому мы никогда не достигнем значительного успеха в попытках подробно разглядеть будущее. Теперь нам кажутся наивными оптимистичные надежды Пьера де Лапласа (1749–1827), который в начале XIX в. описывал наш мир как огромную машину и верил в возможность установить все будущие и прошлые события по известному состоянию мира в настоящий момент.

Однако иногда такой «чувствительной зависимости от начального состояния» не возникает: например, движения

планет в отдаленном будущем можно предсказать чрезвычайно точно. А вот с погодой, напротив, наука быстро приходит к пределу своих предсказательных способностей. Если вы планируете свадьбу в июне, может случиться так, что вопрос о том, где ее проводить — на улице или в помещении — будет решаться в последнюю минуту. Не похоже, чтобы в этом отношении что-то изменилось в ближайшем будущем: мы не знаем, когда бабочке придет в голову взмахнуть крыльями.

ЛИНЕЙНОСТЬ И НЕЛИНЕЙНОСТЬ

Обсуждая теорию хаоса, часто приходится употреблять термин «линейность» — он появляется в самых разных областях, и может означать разные вещи. Когда говорят о компьютерных программах, «линейность» означает, что команды должны выполняться последовательно, по одной. Альтернативой служат параллельные вычисления, когда десятки или тысячи процессоров работают вместе, и множество команд выполняется одновременно.

Вплоть до последних десятилетий информацию, такую как в этой книге, обычно воспринимали «линейно»: читали строка за строкой, начиная с заголовка и заканчивая последней страницей. Но сегодня это все уже устарело — мы научились получать информацию по-другому. Любой путешественник по Интернету может перейти по ссылке к другому сайту, чтобы разобраться с каким-нибудь понятием, а затем вернуться или продолжить свое путешествие по всемирной паутине. Похоже, что такой метод восприятия информации лучше всего соответствует нашему способу мышления.

В математике и физике существует другое, более узкое понимание термина: процесс называется «линейным», если комбинация входных значений приводит к комбинации соответствующих выходных. Например, если система возвращает значение F в ответ на f, и значение G в ответ на g,

то вход $f+g$ на выходе приводит к $F+G$. Простым примером служит (не слишком сильное) растягивание пружинки. Если пружина растягивается на 5 дюймов под действием силы в 3 фунта, то сила в 6 фунтов должна приводить к растяжению на 10 дюймов. В естественных науках очень важны следующие факты:

- Многие физические процессы линейны в малых масштабах. Это объясняется тем, что большинство естественных процессов относительно равномерны, без резких скачков, и поэтому изображаются довольно гладкими графиками. Небольшой участок гладкой кривой довольно хорошо приближается прямой линией (касательной), и поэтому в малых окрестностях процессы выглядят линейными.
- С другой стороны, в природе не бывает процессов, которые линейны в строгом смысле. Если растянуть пружину сильнее некоторого предела, деформация ее структуры и напряжение металла приведут к тому, что процесс перестанет быть линейным; а если вы растянете пружину за предел прочности, то можете распрощаться с линейностью насовсем.
- Линейные приближения приводят к значительному упрощению анализа. Это объясняется тем, что можно сосредоточиться на особенно простых решениях, а их комбинации будут давать дополнительные решения. Например, звук трубы состоит из простых колебаний, — из основной частоты и ее гармоник. Более высокие частоты можно услышать, если изменить частоту амбушюра: труба зазвучит в основном тоне, в октаву, на две октавы выше основного тона, и т. д.

Поэтому нелинейное в принципе сложнее, чем линейное, и тому в современной математике есть бесчетное число примеров: нелинейные операторы, нелинейные дифференциальные уравнения в частных производных, и проч., и проч. Ясно, что большинство интересных проблем в нашем мире, связанных, например, с погодой, химическими реакциями и развитием космоса, приводят к нелинейным задачам. И именно такие задачи заставляют нас иметь дело с поистине хаотическими явлениями.

Глава 83
РАЗБОГАТЕТЬ ГАРАНТИРОВАННО

Вам когда-нибудь снились вещие сны? Скажем, снилось ли, что вам позвонила тетушка Мод, и на следующее утро телефон звонит — вот и она? Можно ли такие явления объяснить обычными процессами или здесь замешаны высшие силы? Такие случаи вовсе не опровергают основания современной науки, поскольку просто объясняются: если эксперимент с довольно малой вероятностью успеха проводить много раз, то можно ожидать, что иногда все-таки успех осуществится.

Чтобы лучше это осознать, представьте себе комнату, в которой много людей. Каждого из присутствующих просят задумать число от 1 до 6, а затем бросают игральную кость. Вне зависимости от того, какое число выпадет, окажется, что примерно одна шестая часть присутствующих (все те, кто задумал выпавшее число) правильно предсказали будущее. И в случае со звонком тетушки Мод примерно то же самое. Когда такому большому числу спящих снится так много снов, реальность и сон неизбежно когда-нибудь совпадут.

Иногда люди находят в своих гороскопах предсказания будущих событий, которые действительно осуществляются. Когда достаточно много людей прочитают такое предсказание (особенно если оно расплывчатое и может относиться почти к любому человеку), для некоторых из них оно обязательно осуществится.

Теперь мы опишем теоретическое и практическое применение этого явления. (Автор снимает с себя всякую ответственность за произошедшее, если кто-то испробует этот трюк на практике.) Разошлите сообщения тысяче интересующихся скачками человек с предсказанием результатов определенных скачек. Допустим, в них участвует десять лошадей, тогда вам нужно предсказать победу каждой из них в ста открытках. Вне зависимости от исхода скачек

сто получателей вашего сообщения получат правдивое предсказание. Этим ста вы отправите предсказания результата следующих скачек; причем десять адресатов узнают, что победит первая лошадь; еще десять — что победит вторая, и т. д. Таким образом, десять человек дважды получат правильные предсказания. Теперь наступает третий раунд: вы рассылаете десять сообщений десяти адресатам, одному из них обязательно повезет, и он уверится, что вы можете предвидеть будущее.

Спросите, сколько он готов заплатить за подсказку о результатах следующих скачек. Скорее всего, сумма будет больше, чем вы потратите на почтовые расходы.

Мораль такова. Каждый, кто делает большое число предсказаний, неизбежно иногда оказывается прав. И отчего бы среди всех тысяч тетушек Мод на свете не найтись одной, которая позвонит племяннику сегодня вечером?

ШЕСТ НА ШОССЕ

Явление, которое мы обсуждаем в этой главе, — еще одна иллюстрация того, что мы не в состоянии объять необъятно большие числа. Как еще можно объяснить тот факт, что, хотя вероятность выиграть в лотерее большой приз исчезающе мала (1 из 13 983 816, или примерно одна четырнадцатимиллионная), почти каждую неделю находится новый победитель?

Чтобы в этом разобраться, рассмотрим еще один пример. Представьте участок шоссе длиной 140 километров, — это примерно равно расстоянию от Москвы до Тарусы. В 140 километрах помещается $140 \cdot 1000 \cdot 100$ (четырнадцать миллионов) сантиметров. Вероятность того, что кто-то угадает определенный участок в 1 дюйм, который вы приметили на шоссе, примерно равна вероятности выиграть в лотерею. Допустим, ваш помощник устанавливает шест диаметром в один дюйм на шоссе, соединяющем Москву и Тарусу (рис. 83.1), а вы — разумеется, в качестве пассажира — с закрытыми глазами проезжаете вслепую от одного города до другого. Как вы думаете, попадете ли вы в шест, если по дороге бросите из окна монетку? Это кажется крайне неправдоподобным.

Рис. 83.1. Можно попасть в этот шест?

Каждую неделю миллионы людей выбрасывают свои деньги на лотерею. В нашей аналогии с шоссе это означает, что на протяжении многих недель стосорокакиллометровое шоссе заполнено автомобилями бампер к бамперу[1)], и в каждом автомобиле в какой-то момент пассажир выбрасывает из окна монетку. Теперь уже нельзя сказать, что совершенно невероятно, чтобы одна монетка из этого потока медяков не попала бы в шест.

ФИЛЬМ К ЭТОЙ ТЕМЕ

Помимо этой яркой иллюстрации вероятности победы в лотерее, рекомендуем посмотреть небольшой фильм. Его можно найти на YouTube:

http://www.youtube.com/watch?v=ODwm291It0E

или с помощью QR-кода.

[1)] Два миллиона лотерейных билетов и длина автомобиля 5 метров дадут сто миллионов метров или 100 000 километров — хватит два раза объехать вокруг Земли и еще останется.

Глава 84

НЕ ДОВЕРЯЙТЕ ТЕМ, КОМУ ЗА ТРИДЦАТЬ

Часто говорят, что самые крупные открытия в математике были сделаны очень молодыми людьми. Но так ли это?

Правда, что веками математику двигали вперед идеи совсем молодых людей, которые сегодня были бы студентами или даже старшеклассниками. Эварист Галуа (1811–1832) погиб на дуэли в нежном двадцатилетнем возрасте вскоре после того, как сделал революционное открытие в алгебре: как по виду полиномиального уравнения определить, можно ли его решить при помощи обычных операций сложения, умножения и извлечения корней. Можно еще вспомнить Нильса Генрика Абеля, о котором мы рассказывали в гл. 72. Этот норвежский математик прожил только 26 лет. Через два дня после его смерти пришло письмо с приглашением занять должность профессора в Берлинском университете. Абеля до сих пор считают самым выдающимся норвежским математиком, и несколько лет назад — с большим запозданием, к сожалению — была учреждена премия почти в миллион евро, носящая его имя. Эта Абелевская премия считается аналогом для математиков Нобелевской премии.

Существуют и современные примеры, и на любой большой конференции поразительно молодые ученые докладывают о своих очень зрелых результатах. Самая престижная математическая награда, медаль Филдса, предназначается именно таким людям. Медаль Филдса могут получить только те, кому не исполнилось сорока лет на момент ее получения. Награжденные могут претендовать на лучшие в мире математические кафедры.

Медальному комитету пришлось совершить над собой значительное усилие, чтобы на международном математическом конгрессе в 1998 г. наградить математика Эндрю Уайлза[1)]. Все соглашались, что он сделал самый важный вклад в математику прошлого столетия — доказал гипотезу Ферма, — но ему было уже далеко за сорок.

Поэтому не стоит слишком уж серьезно относиться к утверждению, что в математике, как в спорте, человек совершенно изнашивается, когда ему «за тридцать». Много известных математиков продолжают творческую деятельность на протяжении всей своей долгой жизни — например, Карл Фридрих Гаусс (1777–1855 г.).

Видимо, правильнее сравнивать математиков с дирижерами: работа с захватывающим материалом сохраняет серые клетки в прекрасной форме до почтенного возраста.

[1)] См. гл. 89.

Глава 85
РАВЕНСТВО В МАТЕМАТИКЕ

Что в математической задаче существенно, а что — только приправа? Точнее, хотелось бы понять, когда две ситуации можно считать «равными», чтобы ограничиться разбором только одной из них?

Итак, что же в математике понимают под равенством? Как ни удивительно — примерно то же самое, что в повседневной жизни, где равенство в смысле полной идентичности играет гораздо меньшую роль, чем равенство в определенном отношении.

Чтобы написать записку, салфетка так же хороша, как лист бумаги. Если стоит цель попасть этим вечером в оперу, небольшой автомобиль, лимузин и такси будут эквивалентны. Однако как только в игру включаются цена, время в пути, престижность, от этой эквивалентности не остается и следа.

Даже в элементарной математике дела обстоят приблизительно так же. Если вы хотите объяснить ребенку, что такое «пять», то можете с одинаковым успехом приводить в пример пять детей или пять яблок. Относительно сути «пятеричности» дети и яблоки эквивалентны.

Вся правда немного сложнее. Если в наше время хотят объяснить, что именно означает абстракция «пять», то обычно начинают с «эквивалентности относительно числа». При этом «пятеричность» — это совокупность всех объектов, которые эквивалентны множеству пальцев руки.

Этот принцип пронизывает всю математику. В геометрии два треугольника эквивалентны, если один можно наложить на другой сдвигом, поворотом и, возможно, переворотом. А в теории вероятностей совершенно неважно, чем пользоваться — правильной монетой или костью, чтобы принять решение, основываясь на случайности.

(Если решение принимается в зависимости от того, упадет монета орлом или решкой, то его можно принимать

в зависимости от того, четное или нечетное, например, число выпадет на кости.)

Только отношение эквивалентности вносит порядок в неизмеримое богатство математических объектов. Тот же принцип действует в каждом языке, лишь общее понимание тех или иных объектов делают общение возможным. Хотя для разных людей понятия «цветок» и «нечто прекрасное» могут различаться, язык все же функционирует именно благодаря идее эквивалентности.

Глава 86
ВОЛШЕБНЫЕ ИНВАРИАНТЫ

Что остается неизменным? На что можно положиться? На протяжении столетий математики искали инварианты, или, проще говоря, — величины, которые не меняются относительно некоторых определенных операций.

Возьмите колоду карт. Когда вы тасуете ее, имеется несколько инвариантов. Разумеется: не меняется общее число карт, а также число валетов, дам, и т. д. Ситуация изменится, если вместо тасования разрешается только разбивать колоду на две части — верхнюю и нижнюю — и менять их местами. Тогда неизменным остается еще относительный порядок карт. Если туз пик находился на три карты ниже дамы червей, то там он и останется.

Конечно же, мы должны правильно понимать слова «на три карты ниже». Если дама червей окажется в самом низу, то туз пик должен быть в колоде третьей картой сверху. То есть «на три карты ниже» следует понимать так, что если вы досчитали до самого низа, то нужно продолжать счет сверху.

Этот инвариант можно использовать для простого фокуса. Выньте из колоды королей и дам и разложите их в ряд, как показано на рис. 86.1. При этом важно, чтобы расстояние между картами одной масти (король пик и дама пик, король треф и дама треф, и т. д.) было в точности равно четырем. Если вы покажете эти карты зрителям мельком, то их расположение покажется более или менее случайным. Никто не заподозрит вас в жульничестве, и если вы разобьете колоду несколько раз (рис. 86.2), все поверят, что карты тщательно перетасованы.

Вы знаете, что расстояние между картами инвариантно: на четыре карты ниже первой лежит ей соответствующая. Поэтому легко составить пару, даже если карты под салфеткой или под столом; конечно же, нужно сделать вид, что вы стараетесь изо всех сил. Можно повторить процесс

Рис. 86.1. Подготовленные карты

и составить вторую пару (хотя в этот раз расстояние станет равным трем), а затем и третью (карты в ней разделены двумя другими), и четвертую.

Фокус основан на существовании некоторого порядка там, где, как кажется, царит хаос. В математике поиск неизменного стал лейтмотивом в исследованиях. Как только описан набор допустимых преобразований, начинается систематический поиск величин, не меняющихся при этих преобразованиях. Эта идея стала особенно важной как объединяющий принцип во многих ветвях геометрии. Его в 1872 г. предложил математик Феликс Клейн, и с тех пор он оказывает огромное влияние на все исследования.

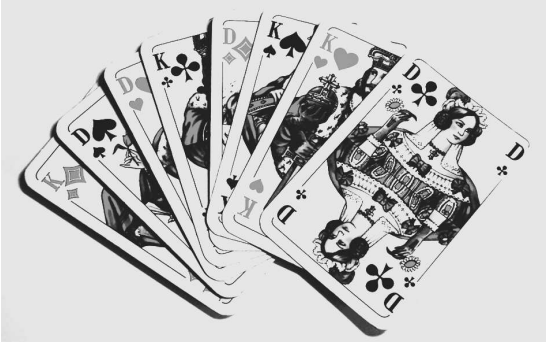


Рис. 86.2. Расклад после тасования

ПОДОПЛЕКА: ИНВАРИАНТ — РАССТОЯНИЕ ПО МОДУЛЮ

Используя арифметику по модулю, которую мы ввели в гл. 22, можно дать более четкое математическое описание принципа, лежащего в основе фокуса.

Если в колоде n карт и две из них находятся в позициях a и b (считая сверху), то число $(b-a)$ по модулю n является инвариантом. После разбивания колоды любое число раз разница значений позиций по модулю n не меняется.

Чтобы в этом убедиться, нужно использовать вычисления по модулю не только для положительных, но и для отрицательных чисел. В конце концов, как всем известно, неделю назад был тот же день недели, что сегодня, а 13 дней назад был вторник, если сегодня понедельник. Математически можно сказать, что -13 по модулю 7 равно 1.

Нужно учитывать эту тонкость, чтобы правильно понимать инвариант. Сейчас мы приведем пример, в котором используем тот факт, что -7 по модулю 10 равно 3. В колоде из десяти карт туз червей и валет бубен находятся в позициях 2 и 5 соответственно. Разность равна 3. Колоду разбивают в позиции 2. Теперь туз червей находится в десятой позиции — в самом низу, а валет перемещается в позицию 3. Разница (позиция второй карты минус позиция первой) теперь равна $3 - 10 = -7$. По модулю 10 это то же самое число 3, что и было раньше.

РИСОВАНИЕ НА РАСТЯГИВАЮЩЕЙСЯ ПОВЕРХНОСТИ

Для волшебных фокусов подходят не так много математических инвариантов. Их значение для любой теории в том, что инварианты отделяют существенное от несущественного. Мы покажем это на несколько необычном примере, для чего потребуется рисовать на поверхности, сделанной из эластичного материала[1)].

Нарисуем что-нибудь на этой поверхности — треугольник, кружок, несколько прямоугольников — все равно что. Теперь начнем деформировать поверхность — растягивать

[1)] Возможно, подойдет эластичная лента для фитнеса.

ее или сжимать в произвольных направлениях, как заблагорассудится. Маленький кружок может стать большим; прямой угол может стать тупым или острым.

Допустим, исходная фигура обладала тем свойством, что любые две точки можно было соединить кривой, которая полностью содержится внутри фигуры. (Это, например, треугольник или кружок, но не набор прямоугольников.) Тогда можно будет сделать то же самое и после того, как фигура изменится: *связность* инвариантна относительно деформаций.

Глава 87

МАТЕМАТИКА ИДЕТ В КИНО

Бывает так, что математика появляется в кино. Математики ходят на такие фильмы с определенной долей недоверия, потому что очень часто то, что появляется на экране, — не более чем популярные клише. Однако всегда интересно посмотреть, какие аспекты стараются подчеркнуть сценаристы и режиссеры.

Вспомним фильм 1992 года «Sneakers». Хорошие парни под предводительством Роберта Редфорда пытаются отобрать у плохого парня (Бен Кингсли) прибор, придуманный выдающимся математиком для взламывания любого секретного кода в мире.

Незадолго до ужасной гибели математика видели на конференции. Там он говорил примерно то, что обычно можно услышать на таких собраниях. Такое впечатление, что для разнообразия сценаристы и режиссер проделали серьезное исследование. Выступающие действительно говорят так, что каждый, изучавший математику хотя бы один семестр, может понять их. Математика в фильме выглядит довольно достойно, хотя возможности математиков по раскрытию всех в мире зашифрованных сообщений значительно преувеличены.

Преувеличение другого рода встречается в фильме с простым называнием «π», сюжет которого связан с глубоким математическим мистицизмом. Идея в том, что многие тайны зашифрованы с помощью цифр числа π, и если их читать в «правильном» порядке, многие поразительные явления получат вдруг свое объяснение. Возможно, это следует понимать метафорически: действительно, число π играет важную роль почти во всех областях математики и до сих пор некоторые тайны этого числа остаются нераскрытыми.

Если бы среди математиков провели опрос о самом любимом фильме на математическую тему, то первым, несо-

мненно, оказался бы фильм «Игры разума» с Расселом Кроу в главной роли. Фильм основан на биографии специалиста по теории игр Джона Нэша, написанной Сильвией Назар. Эмоциональные аспекты математики в фильме переданы особенно удачно. Непреодолимое желание решить задачу может стать всепоглощающим и даже опасным для жизни.

Мораль такова. Желающие вступить в брак с математиком должны быть готовы жить с человеком, который часто уносится в другой мир. Редкий математик умеет отвлечься хотя бы на день и отложить сражение с задачей до завтра.

Глава 88
ЛЕНИВАЯ ВОСЬМЕРКА: БЕСКОНЕЧНОСТЬ

Математики работают с бесконечностью постоянно. Она появляется в самых разных обличьях. Самая безобидная — та, что возникает при счете. Начинают с единицы, затем идет двойка, тройка, и т. д. Конца нет. Даже самые критически настроенные исследователи в области оснований математики соглашаются, что с такой бесконечностью проблем нет.

Все становится сложнее, если с бесконечностями работают как с новыми математическими объектами. Имеет ли смысл говорить о множестве всех простых чисел? Даже если никто не знает, как определить, является ли некоторое достаточно большое число простым? Сейчас принято считать, что говорить о таком множестве законно, и число противников этого мнения уменьшается.

Для тех, кто интересуется в основном математическими приложениями, такие вопросы по основаниям математики представляются вторичными. Для них «бесконечный» означает, что одна величина неизмеримо больше другой. Масса Солнца в некоторых ситуациях может считаться бесконечно большой по сравнению с массой Луны. Состояние Билла Гейтса бесконечно велико по сравнению с вашим банковским счетом, и т. д.

Постепенно привыкают работать с бесконечными величинами так же легко, как с конечными. Например, существует правило, что «бесконечное плюс конечное равняется бесконечному», и оно означает, в частности, что Билл Гейтс не станет богаче, если вы отдадите ему все свое состояние. Или что военный корабль не станет тяжелее, если на его палубу сядет блоха.

Эта идея позволяет упростить многие вычисления. Почти пятьсот лет назад Коперник рассмотрел задачу, которую можно решить, только обратившись к идее бесконечности. Чем можно объяснить, что положение звезд остается неизменным в то время как Земля вращается

Рис. 88.1. Так представляли бесконечную вселенную в средние века

вокруг Солнца? Коперник дал поразительно изящный ответ на этот вопрос: расстояние от Земли до ближайшей звезды бесконечно велико по сравнению с диаметром земной орбиты. Правда, такое объяснение явления вызвало множество теологических проблем (рис. 88.1). Внезапно во Вселенной не осталось места для Бога, и церкви понадобилось несколько столетий, чтобы принять коперниковскую модель Солнечной системы.

КАК РАБОТАТЬ С ∞

Чтобы обозначать бесконечность, математики используют «ленивую восьмерку» — символ ∞. Если изображать «обычные» числа в виде линии, бесконечно уходящей влево (отрицательные числа) и вправо (положительные), то символ ∞ размещают справа от изображения прямой (а $-\infty$ размещают слева). Это означает, что ∞ больше любого «обычного» числа.

Хотелось бы и привычные математические операции распространить на область бесконечного. Мы уже говорили, что сложение определяется таким образом, что сумма любого числа и бесконечности равна бесконечности[1)].

[1)] Это можно записать в виде $a + \infty = \infty$.

Произведение бесконечности и положительного числа — тоже бесконечность. Это можно записать в виде равенства $a \cdot \infty = \infty$ (для положительных a). Оно тоже представляется вполне правдоподобным: Билл Гейтс все равно останется неизмеримо богат, если по досадной оплошности его состояние уменьшится наполовину.

Однако определенная осторожность не помешает, поскольку от некоторых привычных правил придется отказаться. Рассмотрим, например, правило, позволяющее для «обычных» чисел из равенства $a + x = b + x$ делать вывод $a = b$. (Это абстрактное выражение самого привычного явления: если два человека празднуют свой сороковой день рождения одновременно, то они должны были родиться в один и тот же день сорок лет назад.)

Но как только мы договариваемся, что бесконечность прибавлять разрешается, это правило теряет силу: например, $10 + \infty = 1000 + \infty$ (обе суммы равны ∞), но отсюда нельзя, конечно же, заключить, что $10 = 1000$.

Глава 89

ПОЛЯ КНИГ ДОЛЖНЫ БЫТЬ ШИРЕ!

В этой книге уже не раз говорилось о том, что развитие математики не всегда направлено на полезные приложения. Даже когда никаких приложений не видно, мыслителя может мотивировать невероятное интеллектуальное свершение, если задача кажется непреодолимой.

Рис. 89.1. Пьер Ферма

Знаменитый пример — задача Ферма. Почти 400 лет назад в 1621 г. французский математик Баше перевел труд Диофанта «Арифметика» с греческого на латынь. Этот перевод прочел Пьер Ферма́ (1601–1665), юрист и математик-любитель, которого захватил вопрос о высокоразмерных вариантах *пифагоровых троек*. Это такие целые числа a, b, c, что сумма квадратов первых двух равна квадрату третьего ($a^2 + b^2 = c^2$). Таких троек бесконечно много, и самая известная из них — 3, 4, 5 (действительно, $3^2 + 4^2 = 9 + 16 = 25 = 5^2$). Треугольник, стороны которого удовлетворяют этому соотношению, — обязательно прямоугольный, и этим фактом можно воспользоваться для построения прямых углов, например, разбивая сад.

Ферма заинтересовался, что получится, если слово «квадрат» заменить на слово «куб» (третья степень), или еще более высокой степенью. Например, существуют ли целые числа a, b, c, которые удовлетворяют условию $a^4 + b^4 = c^4$? Ферма был убежден, что кроме тривиального решения, когда a и b равны нулю, других таких чисел не существует, и умел это доказать для четвертой степени. По-видимому, он полагал, что этот

же метод годится и для других степеней, поскольку на своем экземпляре книги диофантовой «Арифметики» написал (на латыни): «Я открыл этому поистине чудесное доказательство, но поля книги для него слишком узки».

Более трех столетий математики (и еще больше любители) пытались доказать гипотезу Ферма или найти контрпример. Эта задача стала, по-видимому, самой известной в истории математики. Огромные усилия по поиску доказательства объясняются, по крайней мере отчасти, своеобразным соревновательным духом — хотелось выиграть на интеллектуальном игровом поле: «Столь многие пытались и не преуспели. Если бы я решил ее...». С другой стороны, бестрепетный — и на протяжении веков напрасный — поиск решения привел к невероятному успеху в нашем понимании алгебры.

Сейчас весь мир знает, что Ферма был прав[1)]. В 1998 г. английский математик Эндрю Уайлз завершил доказательство, над которым он работал почти всю свою академическую жизнь. К сожалению, мы никогда не узнаем наверняка, удалось ли Ферма на самом деле найти доказательство. Однако методы, разработанные для доказательства Уайлзом и другими математиками, столь глубоки и требуют такого колоссального объема современных вычислительных средств, разработанных после Ферма, что совершенно невероятно, чтобы Ферма действительно нашел верное доказательство своей гипотезы.

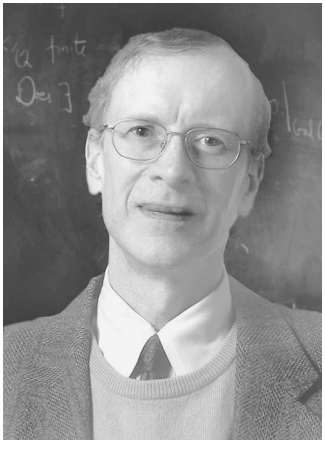


Рис. 89.2. Эндрю Уайлз

[1)] Не в том, что нашел доказательство, а в том, что не существует многомерных аналогов пифагоровых троек.

МЕТОД БЕСКОНЕЧНОГО СПУСКА

Задача Ферма — прекрасный образец того, насколько различны по сложности доказательства возможности что-то сделать и доказательства невозможности этого. Мы покажем это на примере степени 4. Предположим, что на самом деле существуют три натуральных числа a, b, c таких, что $a^4 + b^4 = c^4$. Тогда можно было бы написать компьютерную программу и надеяться, что рано или поздно эти числа найдутся. Если бы компьютер целый год не мог найти такие числа, стоило бы задуматься: возможно, в таких тройках числа астрономически велики, и тогда компьютер окажется бесполезным.

Но если вы подозреваете, что *решения нет*? Ни в стозначных числах, и ни в таких, для записи которых никаких чернил не хватит? Эта задача гораздо сложнее. Стратегия должна быть похожа на ту, которая использовалась для доказательства иррациональности квадратного корня из двух (см. гл. 56): предположим, что утверждение ложно (т. е. что квадратный корень из двух рационален), и найдем следствия, которые приведут к противоречию. Тогда доказываемое утверждение должно быть истинным.

В несколько измененном виде эта же идея может быть использована для доказательства гипотезы Ферма в специальном случае — когда степень равна 4. Для тех, кто освоил основные результаты теории чисел, достаточно будет одного бумажного листка. Название метода похоже на магическое заклинание: «бесконечный спуск».

Покажем, что *если* бы существовали натуральные числа a, b, c такие, что $a^4 + b^4 = c^4$, то нашлись бы натуральные числа d, e, f, обладающие тем же свойством, т. е. $d^4 + e^4 = f^4$, и еще одним дополнительным свойством: f меньше c. Иначе говоря, для каждой тройки, удовлетворяющей уравнению Ферма четвертой степени, есть другая тройка, удовлетворяющая уравнению для меньшего числа в правой части. Но такого не может быть, поскольку предполагается существование бесконечно убывающей последовательности натуральных чисел. Убывая, натуральные числа заканчиваются на единице, поэтому с какого большого числа c ни начинать, в бесконечно убывающей последовательности

окажется не более *c* чисел. Например, последовательность натуральных чисел, которая начинается с 5, может включать не более пяти чисел: 5, 4, 3, 2, 1. А если начать с 100 000, то последовательность может получиться подлиннее, но все равно постепенно придет к единице, тут-то все и кончится.

К сожалению, метод бесконечного спуска в уравнении Ферма годится только для некоторых степеней. Доказательство Уайлза основано на гораздо более глубоких результатах и методах, и в действительности только горстка математиков может всерьез утверждать, что они разобрались во всех его подробностях.

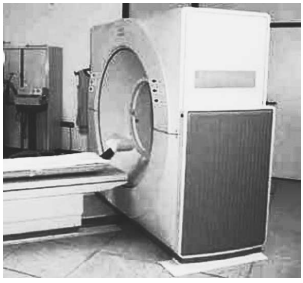
Глава 90

МАТЕМАТИКА: ЧТО У НАС ВНУТРИ

Математики — как сыщики, и об этом мы узнаём еще в школе. Например, x — неизвестная величина, про которую известно только, что $3x+5=26$. Шерлок Холмс придет на помощь! Если $3x+5=26$, то обязательно выполняется соотношение $3x=21$, и тогда x должен быть равен 7.

В компьютерной томографии возникают похожие задачи, хотя на более высоком уровне. Рассмотрим, например, несколько плоских фигур, — круг, эллипс и прямоугольник. Отправимся к стекольщику и закажем вырезать эти фигуры из стекла, толщиной в полдюйма[1)].

Посмотрим сквозь такую стеклянную фигуру, расположив ее ребром к свету. Если это круг, то вверху и внизу свету сквозь него нужно преодолеть меньшее расстояние, чем в середине, где нужно пройти путь в целый диаметр. Поэтому середина нам покажется темной (скорее всего, темно-зеленой), а края — светлыми. А посмотрев на ребро прямоугольника мы увидим равномерно яркую полосу.



Теперь главный вопрос: можно ли определить форму стеклянной фигуры, измерив и сравнив яркость света, который проходит сквозь нее с разных направлений? Да! И в этом состоит идея компьютерной томографии (сам томограф вы видите на фотографии). Этот метод диагностики решает задачу, похожую на нашу задачу со стеклышками. Тело человека с разных направлений просвечивают рентгеновскими лучами, измеряют интенсивность их поглощения, и по этим данным строят трехмерное изображение определенного органа, для которого требуется медицинское исследование.

[1)] Строго говоря, мы получим цилиндры и параллелепипед. — *Прим. ред.*

Это только общая идея; подробности крайне сложны. Чтобы создать прибор, который теперь стал обычным в медицинской практике, понадобилось объединить инженерное искусство, информационные технологии и серьезную математику. Идея этого прибора, возникшая в 1960 г., воплотилась уже через несколько лет. Одна из причин такой незамедлительности заключалась в том, что вся нужная математика была уже известна, она лежала на полке в кладовой интеллектуальных диковин и ждала своего часа. Почти сто лет назад математик Иоганн Радон (1887–1956) предложил процедуру определения формы освещенных предметов по данным об интенсивности света.

Компьютерный томограф — это не только высокие технологии, но и высокая математика. Исследования продолжаются, так как нужно повысить и скорость, и разрешение.

ОБРАТНЫЕ ЗАДАЧИ

Задача компьютерной томографии — это частный случай *обратной задачи*. Такие задачи возникают в различных приложениях. Например, измерив колебания земной коры в различных точках, можно точно определить, где именно произошло землетрясение и какова его интенсивность. Аналогично, измерение отраженной волны позволяет разведать положение и запасы подземных месторождений минералов.

У обратных задач есть типичные трудности, присущие в том числе и задачам компьютерной томографии. Например, зависимость решения от входных данных очень чувствительна: небольшая ошибка в измерениях — а ведь абсолютно точных измерений не бывает — может привести к серьезным погрешностям в результатах.

Для иллюстрации этих трудностей рассмотрим уравнение $0{,}0001 \cdot x = a$. Величина a известна, а x — неизвестное большое число. С математической точки зрения решение элементарно: $x = a/0{,}0001$. Однако в практических приложениях a может быть известно только приблизительно. Допустим, это длина, и ее значение измерено с точностью до 1 миллиметра. Но при вычислении x это дает ошибку в 10 000 раз больше, и компьютер выдаст решение с точностью в пределах 10 метров!

Глава 91
МОЗГ ВНУТРИ КОМПЬЮТЕРА

Математик-Франкенштейн? На протяжении столетий люди лелеяли надежду передать некоторые из человеческих интеллектуальных возможностей машинам. Нейронные сети, ставшие объектом изучения с 1960 г., представляют собой серьезную попытку воспроизвести структуру человеческого мозга и некоторые аспекты его функционирования, чтобы создать нечто, подобное человеческой мысли.

Кирпичиками нашего мозга служат нейроны — клетки, проводящие импульсы и формирующие центральную командную и контрольную структуру нервной системы. У человека около десяти миллиардов таких клеток, соединенных друг с другом триллионами связей, или *синапсов*. Компьютерный эквивалент нейрона — логическая структура, усиливающая или ослабляющая входной сигнал на основании некоторых контрольных сигналов. Ответ может колебаться в очень широких пределах в зависимости от реакции на контрольные сигналы; и установкой различных параметров можно добиться чрезвычайно широкого диапазона для возможных вариантов поведения.

При связывании таких структур число вариаций растет экспоненциально, и о таком наборе связей можно говорить как о *нейронной сети*.

Как выбирают различные параметры? Рассмотрим, например, вопрос о том, как банк может принимать решение: одобрить ли вашу заявку на кредитную карту, опираясь на доступные сведения о вас: возраст, доход, активы, кредитная история и т. д. В идеале нейронная сеть должна принимать всю эту информацию, а на выходе давать ответ «да» или «нет» так, чтобы одобрялись только кредитоспособные заявители.

После построения сети ее «обучают», подавая на вход данные, по которым уже другими способами получено решение — одобрять заявку или нет. В идеале нужно настроить

параметры таким образом, чтобы для всех элементов обучающего набора сеть выдавала правильное решение. Для этого требуется довольно сложная математика — в надежде на то, что, хорошенько обучившись, нейронная сеть будет давать правильный ответ на новые входные данные, неизвестные ранее ни банку, ни компьютеру.

Классическая математика довольно скептически относится к таким методам: ведь чтобы модель соответствовала действительности, параметры подгоняют без всякого понимания взаимосвязей между ними. Но ведь неизвестно, к чьему решению следует относиться с большим доверием: банковского служащего или хорошо обученной нейронной сети.

ПЕРЦЕПТРОН

Как же все-таки компьютер моделирует клетки человеческого мозга? Одна из первых моделей — *перцептрон*, его изучение началось в 1960 г. Проще всего его представить в виде черного ящика, в который с одной стороны входят несколько проводов, а с обратной выходит только один (рис. 91.1).

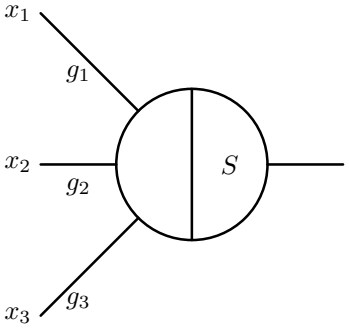


Рис. 91.1. Перцептрон

Перцептрон занимается тем, что умножает входные сигналы $x_1, x_2, \ldots$ на веса $g_1, g_2, \ldots$, складывает произведения и проверяет, не превосходит ли полученная сумма $g_1x_1 + g_2x_2 + \ldots$ некоторого порогового значения S. Если

да, то на выход подается единица; говорят, что перцептрон «среагировал». Если нет, то на выход подается нуль.

Рассмотрим случай, в котором есть два входа, пороговое значение S установлено равным 1, а оба весовых коэффициента равны 0,7. Если на один вход подается 1, а на другой 0, то сумма произведений входов и весов равна $0{,}7 \cdot 1 + 0{,}7 \cdot 0 = 0{,}7$, и это меньше порогового значения. Таким образом, на выход подается нуль, — перцептрон не реагирует. Однако если на оба входа подается единица, то получается сумма 1,4, и перцептрон реагирует.

В этой ситуации подходящим выбором весов и порогового значения мы добились, чтобы перцептрон моделировал логический элемент «И» (рис. 91.2).

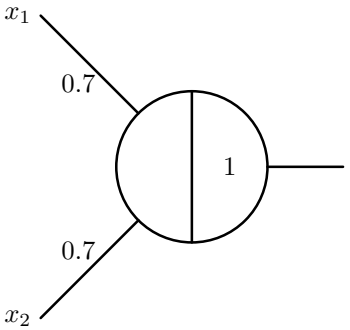


Рис. 91.2. Перцептрон как связь «И»

Но перцептрон способен на большее. Многие читатели помнят из школьного курса математики, что множество точек с координатами (x, y), удовлетворяющими уравнению $ax + by = c$, образует прямую на декартовой плоскости. Все те пары (x, y), для которых сумма $ax + by$ больше c, задают точки, лежащие по одну сторону от прямой, как изображено на рис. 91.3.

Вернемся к перцептрону. Пусть x, y — это входные значения, a, b — веса, а c — граничное значение. Такой перцептрон умеет определять, по какую сторону от прямой лежит заданная точка. Добавив логический элемент «И», можно соединить несколько перцептронов и смоделировать миниатюрный мозг, который выводит единицу, если точка

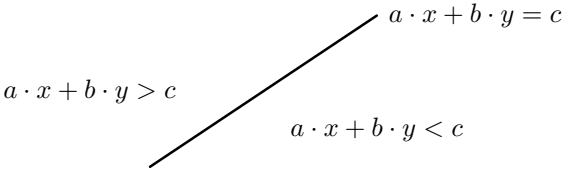


Рис. 91.3. Полуплоскость $ax + by < c$

лежит внутри заданного треугольника, и нуль — в противном случае. Если на вход подаются координаты точки, то, как видно из рис. 91.4, реализация не представляет трудностей. Точка лежит внутри треугольника ABC, если она правее прямой $G1$, левее прямой $G2$ и выше прямой $G3$.

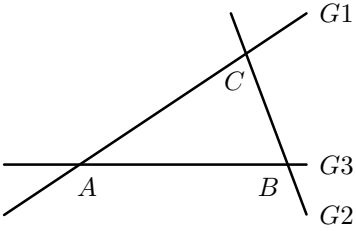


Рис. 91.4. Так перцептрон определяет, лежит ли точка в треугольнике

В более серьезных приложениях соединяют дюжины перцептронов, и речь идет о нейронной сети. Веса для входных сигналов выбираются методом проб и ошибок так, чтобы на выходе получался результат как можно ближе к правильному в тех случаях, когда он известен. В примере с кредитными картами если входные значения дохода, владения недвижимостью, времени работы на одном месте, и т. д., благоприятны, то нейронная сеть должна давать на выходе 1 (кредитоспособен), но кандидатов с данными, указывающими на риски, она должна отклонять.

Глава 92

COGITO, ERGO SUM

Рене Декарт (1596–1650) был замечательным человеком. Еще в юности он решил посвятить свою жизнь поиску истины. В его «Рассуждении о методе» содержится не только основание его философии (cogito, ergo sum — мыслю, следовательно, существую), но и важные приложения, призванные продемонстрировать новый метод.

Рис. 92.1. Рене Декарт

В одном из этих приложений речь идет о геометрии. В него включены положения, которым суждено было глубоко повлиять на развитие математики. Самое важное из них — это соединение алгебры и геометрии. Декарт обнаружил, что геометрические задачи можно переводить на язык алгебры и что, обратно, решение многих алгебраических уравнений допускает геометрическую интерпретацию. Этот подход оказался невероятно плодотворным, поскольку задачи, которые не решались одними методами, часто удавалось решить другими. Наглядное тому подтверждение —

доказательство невозможности квадратуры круга[1]. Когда удалось показать, что π относится к особенно сложным числам и что только относительно «простые» числа допускают построение с помощью циркуля и линейки, стало ясно, что такой вид геометрических построений не позволяет преобразовать круг в квадрат той же площади.

Однако для Декарта все это было делом далекого будущего. О числах было известно еще слишком мало. Даже на отрицательные числа поглядывали с подозрением, а среди решений уравнений различали «истинные» и «ложные» — в зависимости от того, были они положительными или отрицательными.

Стремительное развитие естественных наук в семнадцатом столетии было бы немыслимо без подготовительной работы, проделанной Декартом. Трудно поверить, что в математике он было просто «любителем» и самоучкой.

Нужно сказать, что «декартова система координат», с которой все знакомились в школе, в работах Декарта не встречается. Только в восемнадцатом веке стало общепризнано, что такая система могла объединить различные геометрические построения, которые становились при этом просто отдельными частными случаями.

«ПЕРЕВОД» ТЕОРЕМЫ ПИФАГОРА

Переход от геометрии к алгебре — чрезвычайно мощный метод; например, доказательство теоремы Пифагора становится очень простым, если вместо геометрических фигур обратиться к алгебраическим уравнениям.

Нужно доказать, что для прямоугольного треугольника со сторонами a, b, c выполняется соотношение $a^2 + b^2 = c^2$. Мы будем считать, что если a и b не равны, то b больше a (см. рис. 92.2).

Секрет доказательства в том, чтобы рассмотреть квадрат со стороной c, в который вписаны четыре экземпляра нашего треугольника.

Эти четыре треугольника не заполняют квадрат целиком: в центре остается еще маленький квадратик (на рис. 92.3 он

[1] См. гл. 33.

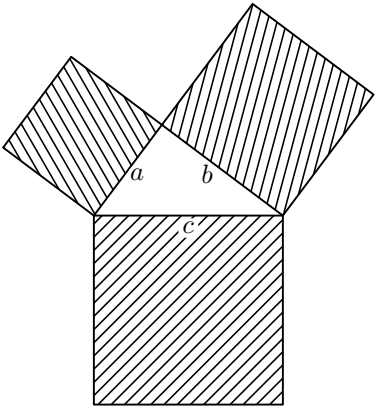


Рис. 92.2. Теорема Пифагора: $a^2 + b^2 = c^2$

белого цвета). Его сторона равна $b-a$, это видно из рисунка. Поэтому площадь большого квадрата равна учетверенной площади треугольника плюс еще площадь маленького квадратика со стороной $b - a$. Площадь прямоугольного треугольника с катетами a и b равна $\frac{1}{2}\,a \cdot b$, так что мы получаем соотношение

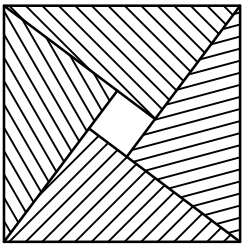


Рис. 92.3. Теорема Пифагора: так можно ее доказать

$$c^2 = 4 \cdot \frac{a \cdot b}{2} + (b - a)^2.$$

Теперь дело за алгебраическими трюками. Вспомнив, что

$$(a - b)^2 = a^2 - 2 \cdot a \cdot b + b^2,$$

можно доказать, что

$$c^2 = 4 \cdot \frac{a \cdot b}{2} + (b - a)^2 =$$

$$= 2 \cdot a \cdot b + b^2 - 2 \cdot a \cdot b + a^2 = a^2 + b^2.$$

Итак, мы показали, что $c^2 = a^2 + b^2$, заменив сложные геометрические рассуждения простыми алгебраическими.

Не следует судить по этому примеру и думать, что Декарт занимался только сравнительно простыми задачами. Напротив, большинство затронутых им вопросов настолько глубоки, что и сейчас — спустя почти четыреста лет — многие математики с трудом могли бы их решить.

Глава 93

ЕСТЬ ЛИ В МИРЕ ДЫРЫ?

Математический институт Клэя предлагает награды в один миллион долларов за решение некоторых не поддающихся никаким усилиям математических задач[1]. Теперь ученые сошлись во мнении, что первой покорилась гипотеза Пуанкаре. Ее доказательство стало настоящей сенсацией, ведь уже несколько поколений математиков скрежещут зубами в досаде на то, что не могут с ней справиться.

Для гипотезы Пуанкаре требуется понимать, что такое «пространство». Прежде чем перейти к трем измерениям, мы остановимся на двух — так будет легче представить себе ситуацию. Какие поверхности можно назвать «существенно» разными? Мы примем соглашение о том, что существенно разные поверхности — это те, которые нельзя преобразовать друг в друга непрерывными деформациями.

В этом смысле поверхность апельсина по существу не отличается от поверхности Земли или футбольного мяча. А вот поверхность спасательного круга совсем не такая (см. рис. 93.1). Работа над составлением каталога поверхностей началась в девятнадцатом столетии, и к настоящему моменту классификация поверхностей успешно завершена.

Рис. 93.1. Две существенно разные поверхности

А вот такой же вопрос для трех измерений остается пока без надежды на ответ. Чтобы объяснить, в чем

[1] См. гл. 57 и 37.

заключается гипотеза Пуанкаре, нужно освоиться с терминологией, а именно с понятием односвязности. Представьте свое жилище в печальном положении — мебель вынесли, межкомнатные двери сняли с петель, а входную дверь заперли. Возьмите длинную веревку, растяните ее по всем комнатам, как заблагорассудится, а затем свяжите два конца вместе. Если вы потянете за какую-нибудь петлю, то, возможно, вытянете всю веревку, но может случиться и по-другому: веревка зацепится и не поддастся, поскольку в вашем доме есть круговой проход через комнаты, как изображено на рис. 93.2 справа.

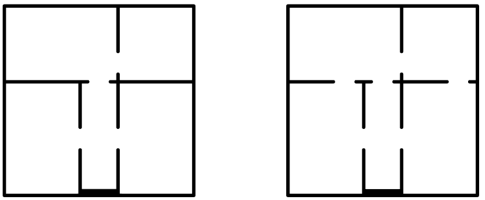


Рис. 93.2. Односвязна ли ваша квартира?

А теперь определение. Область в пространстве называется *односвязной*, если (как изображено на рис. 93.2 слева) веревке не за что зацепиться. (Это определение применимо и к двумерным поверхностям. Поверхность сферы, например, односвязна, а поверхность спасательного круга — нет.) Пуанкаре высказал гипотезу, что в пространстве есть только одна односвязная область, и в некотором техническом смысле она «не слишком велика».

Это было примерно в 1900 году. С тех пор достигнут огромный прогресс в понимании пространства, но проблема оставалась нерешенной. Это очень огорчительно, поскольку в то же время были решены другие, по всей видимости более сложные, задачи из других областей математики. Однако теперь наконец-то можно считать, что гипотеза Пуанкаре доказана. Это произошло благодаря озарению, посетившему русского математика Григория Перельмана, который решил эту задачу.

Успех идей Перельмана привел не просто к решению исходной задачи. У нас теперь есть полный каталог архи-

тектуры всевозможных пространств и даже конструктор, чтобы построить любое из них из кирпичиков всего восьми различных типов. Это предсказывал еще в 1970-х годах американский математик Уильям Тёрстон, но никакого продвижения по предложенной им программе не случилось до работы Перельмана.

Может случиться и так, что доказательство гипотезы Пуанкаре повлияет на наше знание о структуре Вселенной. Точно так же, как теория относительности Эйнштейна выиграла от углубленного понимания геометрии, достигнутого в девятнадцатом веке, так и предвидение Пуанкаре может когда-нибудь сыграть важную роль при описании Вселенной в целом. Поживем — увидим. Известно, что Вселенная локально трехмерна, а также существуют теории о том, что она конечна, но безгранична. Но предстоит еще много работы, прежде чем недостающие предположения о недостающих соотношениях подтвердятся теоретически и экспериментально.

Глава 94

ТАК ЛИ СТРАШНЫ КОМПЛЕКСНЫЕ ЧИСЛА?

Если какое-нибудь обычное число возвести в квадрат, получится положительный результат: трижды три — девять; минус четыре умножить на минус четыре — шестнадцать, тоже положительное число. Поэтому трудно вообразить число, квадрат которого отрицателен.

Эта тема доставила математикам много печали несколько столетий назад, когда началась работа над полиномиальными уравнениями. Решение задачи состояло из двух частей — обыкновенной и поразительной. Поэтому вовсе неудивительно, что в ходе работы над уравнениями, которые не решались старыми методами, возник новый вид чисел.

Возможно, читатель помнит что-то такое еще со школьной скамьи. Даже тех, кто овладел таблицей умножения, ставила в тупик невозможность найти число x такое, что $x + 3 = 1$. Правильное решение, а именно $x = -2$, было доступно только после знакомства с отрицательными числами. А ведь у отрицательных чисел тоже есть практический смысл: при работе с дебетом и кредитом, с отрицательными температурами и во многих других приложениях.

То же самое с комплексными числами. К отрицательным числам приходят, рассматривая уравнения, у которых иначе не было бы корней, и комплексные числа возникают в ходе решения уравнений вроде $x^2 + 1 = 0$, которому удовлетворяет число x, квадрат которого равен -1.

Поразительная часть вот в чем: этот новый вид чисел, к которым относятся квадратные корни из всех отрицательных чисел, обладает одним удивительным и очень приятным свойством. В него входят решения *всех* полиномиальных уравнений, и поэтому его уже не придется расширять по мере того, как решаемые нами уравнения становятся все сложнее.

Все это стало известно в восемнадцатом и девятнадцатом веках. С тех пор математики, инженеры и физики используют комплексные числа так же легко и привычно, как мы, простые смертные, имеем дело с числами вроде 3 или 12. Комплексные числа можно изображать как точки на плоскости, и, в принципе, с ними не больше проблем, чем с числами, которые нужны нам в повседневной жизни.

Что же в них хорошего? Комплексные числа так же нужны математикам, инженерам и физикам, как отрицательные числа — бухгалтерам.

Однако, чтобы работать с комплексными числами свободно, требуется своеобразная акклиматизация, и от них нет никакого проку в решении повседневных задач. Конечно же, решение назвать их «комплексными» и «мнимыми» было провальным с маркетинговой точки зрения. Такие названия придают им ореол мистичности, совершенно незаслуженный. Но те, кого они вводят в замешательство, окажутся в хорошей компании. Роберт Музиль в рассказе «The Confusions of Young Torless» так описывает раздражение от иррационального:

– Слушай, ты это вполне понял?

– Что?

– Эту историю с мнимыми числами?

– Да. Это же совсем не так трудно. Надо только запомнить, что квадратный корень из минус единицы — это еще одна величина при вычислении.

– Но вот в том-то все и дело. Такого же не существует...

– Совершенно верно. Но почему бы, несмотря на это, не попытаться произвести извлечение квадратного корня и при отрицательном числе?

– Но как же так, если с математической точностью знаешь, что это невозможно?

ЧТО НА САМОМ ДЕЛЕ НУЖНО ЗНАТЬ ПРО КОМПЛЕКСНЫЕ ЧИСЛА

Вы вполне разберетесь с комплексными числами, если усвоите следующие три факта.

- Их можно изображать на плоскости.

Представьте себе точку на плоскости с обычными прямоугольными координатами

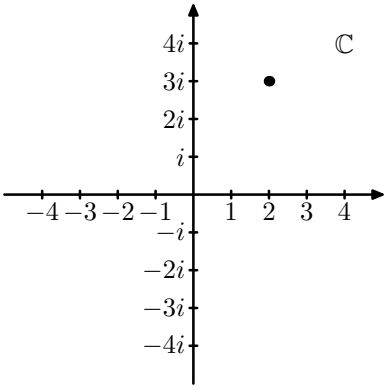


Рис. 94.1. Комплексная плоскость

Теперь от точек на плоскости перейдем к комплексным числам. Точке с координатами (x, y) поставим в соответствие число, которое записывается в виде $x + y \cdot i$. Так, на рис. 94.1 изображено число $2+3\cdot i$. Возможно, это выглядит несколько загадочно, но сложного ничего нет; важно лишь, что любую точку можно записать в виде числа (например, точка (12,14) записывается в виде числа $12 + 14 \cdot i$), и, обратно, любому комплексному числу соответствует ровно одна точка (так, числу $3 + 25 \cdot i$ соответствует точка (3,25)).

- С комплексными числами легко проводить вычисления.

Сложение определяется следующим образом. Например, чтобы сложить числа $2 + 3 \cdot i$ и $7 + 15 \cdot i$, достаточно сложить «действительные» части (без i) и «мнимые» (с i) по отдельности. Поэтому получается $9+18\cdot i$, так как $2+7 = 9$ и $3+15 = 18$. Аналогично, число $-9+5{,}5\cdot i$ является суммой чисел $-6 + 3 \cdot i$ и $-3 + 2{,}5 \cdot i$. Дальнейшие примеры были бы уже излишеством.

Умножаются комплексные числа как многочлены с той лишь оговоркой, что произведения $i \cdot i$ нужно заменять на -1. Давайте умножим $3 + 6 \cdot i$ на $4 - 2 \cdot i$. Обычные

вычисления дают результат $12-6\cdot i+24\cdot i-12i\cdot i$, и с учетом правила $i\cdot i$ получаем, что это произведение равно

$$12-6\cdot i+24\cdot i+12=24+18\cdot i.$$

Заметим, что, поскольку число i, умноженное на себя, дает -1, у уравнения $z^2=-1$ есть решение[1)].

- Теперь можно решить любое полиномиальное уравнение — линейное, квадратичное, кубическое, и т. д.

Это означает, что теперь не важно, какая у многочлена степень, какие у него коэффициенты — действительные или комплексные, — всегда найдется комплексное число вида $z=x+i\cdot y$, которое удовлетворяет уравнению. Например, можно быть уверенным, что существует комплексное число, удовлетворяющее уравнению $z^{10}-4z^3+9{,}2z-\pi=0$. Важность этого факта невозможно переоценить. Когда инженер изучает частотные характеристики электрического контура или огромной радарной антенны, всегда найдется комплексное решение, которое подскажет, нет ли подозрений в потере устойчивости системы.

Принципиальное значение комплексных чисел заключается в существовании решения для произвольного полиномиального уравнения. Это существование предполагали еще в семнадцатом веке, но первое строгое доказательство дал великий Карл Фридрих Гаусс в 1799 г.

[1)]Отметим, что привычная запись $z^2=z\cdot z$ выполняется не только для действительных чисел, но и для комплексных.

Глава 95
ЭШЕР И БЕСКОНЕЧНОСТЬ

Ценители изящных искусств достаточно холодно оценивают работы нидерландского художника-графика Маурица Корнелиса Эшера. Но мы в этой главе не собираемся обсуждать, до какой степени верно такое мнение. Бесспорно то, что картины Эшера интересны с математической точки зрения по многим причинам, и все они геометрической природы.

Первая интересная геометрическая тема — *замощения плоскости*. Цель замощения заключается в том, чтобы закрыть всю плоскость фигурами, которые составляют повторяющийся узор. Этот принцип замечательно демонстрируют паркеты. Если вы нарисуете квадрат, его можно бесконечно повторять во всех направлениях, как на бесконечной шахматной доске. Этот узор можно сделать интереснее, если искусно его раскрашивать, учитывать симметрию, вырезать кусочки с одной стороны и прикладывать их к другой. Вместо квадратов можно брать треугольники, параллелограммы, трапеции или шестиугольники. Так что плоскость можно замостить самыми разными способами.

Эшер подошел к этой задаче как математик. Сколько существует принципиально разных способов замощения, и как их можно описать? Хотя в математике он был любителем, ему удалось получить полную классификацию, и на его картинах изображены все возможные варианты. Это произвело огромное впечатление на математиков, работавших в этой же области.

Еще больше поражает успех Эшера в изображении бесконечности. Неважно, как велик ваш холст, — изобразить можно не полное замощение, а только его часть. Эшер нашел два решения этой проблемы. Первое — использовать поверхности без границы, отличные от плоскости; например, он замостил поверхность сферы, получив узоры, плавно перетекающие друг в друга. Во втором решении используются математические открытия

девятнадцатого века, о которых Эшеру сообщил математик Г. С. М. Коксетер. Имеются в виду неевклидовы геометрии, которые позволяют моделировать бесконечность на областях, для которых нужна только часть евклидовой плоскости. Так возникли знаменитые эшеровские мотивы со змеями и рыбами.

И наконец, надо рассказать о «невозможных» картинах Эшера, таких как конечная лестница, которая постоянно ведет вверх. Отдельные участки картины выглядят вполне привычно, но свести эти локальные восприятия в одно глобальное невозможно — такое трехмерное изображение противоречит действительности.

Даже если бы мы использовали термины «локальное» и «глобальное» в их математическом смысле, все равно оставался бы необъяснимый аспект, относящийся к психологии восприятия. При взгляде на картины Эшера становится ясно, что глаз обычно действует как молчаливый и ненавязчивый наблюдатель, отправляющий в мозг предварительно обработанные сообщения.

«СДЕЛАЙ САМ», КАК ЭШЕР

Хотите сами сделать эшеровскую гравюру? Например, вам нужен заполняющий плоскость узор для обоев или оберточной бумаги. Нет пределов возможностям, доступным предприимчивому любителю, хотя нужно сказать, что уже давно известно — имеется только двадцать восемь существенно разных методов построения (и все они используются в картинах Эшера).

За основу возьмите относительно простую картинку. На жаргоне паркетчиков она называется *CCC базового типа*. Чтобы ее получить, надо понять, что такое *C-линия*[1]. Это кривая, которая соединяет две точки A и B таким образом, что середина отрезка AB лежит на кривой, и поворот кривой на 180° вокруг этой точки приводит к той же самой кривой. Некоторые примеры вы видите на рис. 95.1.

[1] Буква C — сокращение от «center» (центр).

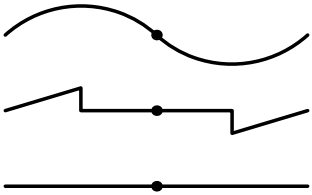


Рис. 95.1. Три C-линии

Теперь можно дать волю своей фантазии. Возьмите лист бумаги, отметьте на нем три точки P, Q, R и проведите несколько C-линий: одну из P в Q, другую из Q в R, и третью из R в P. Это могут быть любые C-линии, и при построении фигуры — обозначим ее F, — ограниченной этими линиями, вас сдерживает только ваша креативность. Заметьте, что вы можете замостить плоскость без зазоров и наложений копиями этой фигуры. Попробуйте! Сделайте дюжину экземпляров и вырежьте их из бумаги. Остается только поворачивать их и укладывать. Вместо того чтобы читать подробное описание, лучше один раз увидеть: на рис. 95.2 используются C-линии.

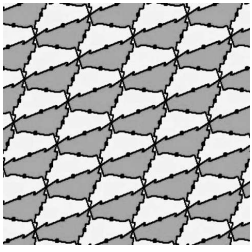


Рис. 95.2. Пример типа CCC

Если вам удастся сделать фигуру F в виде ангела, дьявола, рыбы, птицы — чего угодно, — ваш шедевр будет выглядеть как гравюра Эшера.

Если на ваш вкус тип CCC слишком сложен, попробуйте тип $TTTT$[1)]. Начните с параллелограмма. Обозначьте его вершины A, B, C, D, начав с левой нижней и двигаясь

[1)] Буква T означает «translation» — параллельный перенос.

против часовой стрелки. Нарисуйте какую вам заблагорассудится кривую, соединяющую точки A и D, и переместите ее копию вправо, чтобы та соединила точки B и C. Затем нарисуйте произвольную кривую, соединяющую точки A и B и переместите ее копию вверх, соединив точки D и C. У вас получилась своего рода «ячейка», копии которой теперь можно перемещать влево, вправо, вверх, вниз, чтобы замостить ими плоскость. По построению копии сомкнутся друг с другом без зазоров и наложений. На рис. 95.3 вы видите два примера замощения такого типа.

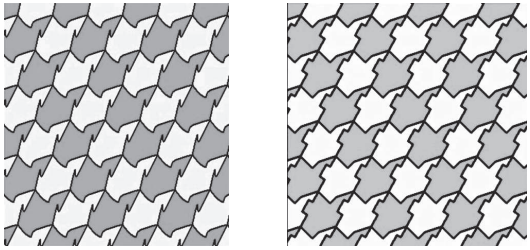


Рис. 95.3. Пример типа *TTTT*

Глава 96

В НАЧАЛЕ ЕДИНИЦА ВСТРЕЧАЕТСЯ ЧАЩЕ ДВОЙКИ

Замечали ли вы, рассматривая таблицу чисел, что фундаментальный закон равномерности нарушается? Казалось, разумно было бы предположить, что числа, у которых первая цифра 1, 2, и так далее, встречаются одинаково часто. Однако обычно это не так. Об этом говорит закон Бенфорда, названный так по имени физика Франка Бенфорда (1883–1948). Слово «закон» не стоит воспринимать слишком серьезно. Он не выполняется так же неотвратимо, как, скажем, ньютоновские законы небесной механики. Закон Бенфорда — скорее попытка количественного объяснения.

Здесь мы имеем дело с вариацией на тему «случай заметает свои следы». Для начала представьте себе простую игру в кости. «Доска» для игры состоит из примыкающих друг к другу полей, пронумерованных числами $0, 1, 2, \ldots$. Вы стартуете в 0, а затем продвигаетесь вперед на столько шагов, сколько очков выпало на игральной кости. Если на первых бросках выпали числа 1, 6, 2, то вы передвигаетесь на поле номер 1, затем на поле номер $7 (= 1 + 6)$, а затем на поле $9 (= 7 + 2)$.

Невозможно определить, попадете ли вы на определенном ходе на поле 101 с большей вероятностью, чем на поле 201, поскольку такие «далекие» поля кажутся равновероятными. Даже если кость неправильная, невозможно сделать предположение о том, где окажешься.

А теперь вернемся к закону Бенфорда. В нашей игре имеют место аддитивные случайные влияния. Как правило, факторы, оказывающие влияние, мультипликативны. (Например, удвоение осадков приводит к удвоению количества воды, доступной для орошения. На 2 нужно умножать, а не складывать.) Есть технический трюк, который превращает умножение в сложение: логарифмирование. Он приводит к тому, что логарифмы величин, которые мультипликативно зависят от влияющих на них случайных

факторов, должны быть распределены равномерно. А для самих величин это значит, что цифра 1 в начале числа должна появляться гораздо чаще, чем 2, а та, в свою очередь, чаще, чем 3, и т. д.

Почему так происходит? Возьмем двузначные числа. Если десятичные логарифмы чисел лежат между 1 и 2, то сами числа лежат между 10 и 100. (Логарифм 10 равен 1, а логарифм 100 равен 2.) Однако логарифм 20 равен приблизительно 1,3, так что примерно тридцать процентов логарифмов между 1 и 2 соответствуют числам от 10 до 19. Логарифм 30 равен примерно 1,5, поэтому двузначные числа, которые начинаются с цифры 2, представляют примерно 20% (1,5 – 1,3 = 0,2) логарифмов. Добравшись до 90, мы обнаружим, что логарифм этого числа равен примерно 1,95, и поэтому двузначные числа, начинающиеся с девятки, соответствуют только приблизительно 2,0 – 1,95 = 0,05 = 5% логарифмов.

Вы все еще сомневаетесь? Задумайте четырехзначное число и припишите перед ним единицу. Заставьте Google найти это (пятизначное) число. Проделайте то же самое с двойкой, тройкой, и так далее. Число результатов будет постепенно убывать, и это должно убедить самых закоренелых скептиков.

ЭКСПЕРИМЕНТ С ГУГЛОМ

Происхождение закона Бенфорда легко обнаружить, рассматривая таблицу логарифмов в библиотеке вашего города. Такие таблицы использовались для выполнения сложных вычислений[1)]. Бенфорд заметил, что страницы с логарифмами, начинающимися с маленьких цифр, замусолены больше, чем другие. Заинтересовавшись, Бенфорд подробно исследовал это явление и вывел свой закон. Как мы уже сказали, это не совсем «закон», и мы здесь его не доказываем, а только ищем способы объяснить его.

Но в том, что он действительно существует, нет никаких сомнений. Приведем результаты эксперимента, проведенного в декабре 2005 г. с поисковой системой

[1)] См. гл. 36.

Таблица 96.1

Результаты эксперимента с последовательностью цифр 3972

Поиск	13972	23972	33972	43972	53972	63972	73972	83972	93972
Реальное число результатов	389,000	232,000	136,000	117,000	71,400	65,300	44,600	54,100	42,300
Теоретическое значение (в процентах)	30,1	17,6	12,5	9,7	7,9	6,7	5,8	5,1	4,6
Теоретическое значение	346 000	203 000	144 000	112 000	91 000	77 000	68 000	59 000	53 000

Google. Была наугад выбрана случайная последовательность цифр 3972, и перед ней поочередно приписывались цифры от 1 до 9. В таблице (см. предыдущую страницу) указано число результатов, найденных в эксперименте, а также теоретическое (в процентах и в абсолютном выражении).

Реальные значения оказались несколько выше теоретических в начале таблицы и несколько ниже — в конце. Однако можно считать, что полученные результаты подтверждают теорию.

Выборы сфальсифицированы? В июле 2009 года возникло подозрение, что были махинации на выборах в Иране, и юридический закон Бенфорда дал задний ход, это случалось, разумеется, и раньше. Пришлось срочно латать образовавшуюся прореху.

Глава 97

ПОДСОЛНУХ И РАТУША В ЛЕЙПЦИГЕ

Золотое сечение — одно из важнейших чисел в математике. Напомним, что можно построить прямоугольник, в котором отношение длинной стороны к короткой равно отношению суммы обеих сторон к длинной. Такое отношение называется *золотым сечением*. Чтобы его вычислить, предположим, что короткая сторона равна 1, а длинную обозначим x. Тогда по определению

$$\frac{x}{1} = \frac{1+x}{x}.$$

Умножив обе стороны уравнения на x и перегруппировав слагаемые, получим квадратное уравнение

$$x \cdot x - x - 1 = 0.$$

По формуле корней квадратного уравнения получаем

$$x = \frac{1 \pm \sqrt{5}}{2}.$$

Из этих двух решений положительно только одно, и оно равно 1,6180....

Некоторые полагают, что прямоугольники, стороны которых находятся в таком отношении, особенно приятны

с эстетической точки зрения. И действительно, золотое сечение часто встречается в архитектуре, например в очертаниях древнегреческих храмов, а также современных зданий (например, башня лейпцигской ратуши разделена на секции в соответствии с золотым сечением). Однако в наше время все работают с бумагой международного стандарта A, для которого лист, сложенный пополам, сохраняет свои пропорции, и поэтому мы больше привыкли к отношению сторон, равному квадратному корню из двух, или 1,414....

Важность золотого сечения объясняется тем, что оно то и дело возникает почти во всех областях математики. Конечно, неудивительно встретить его в геометрии, поскольку оно и возникло как решение геометрической задачи. Но оно возникает и в чисто числовых задачах. Возьмем, например, знаменитую *последовательность Фибоначчи*. Она начинается с чисел 1, 1, а каждый новый член равен сумме двух предыдущих. Поэтому после 1, 1, идут числа 2, 3, 5, 8, 13, 21, и т. д. Отношение двух последовательных чисел все больше и больше приближается к золотому сечению; даже дробь 21/13 = 1,615... — уже неплохая аппроксимация.

Числа Фибоначчи встречаются и в природе, например в расположении семян в подсолнухе. А если у вас есть рулетка, то вы можете поискать золотое сечение у себя. Расстояние от локтя до кончиков пальцев, деленное на расстояние от локтя до запястья, — один из многих примеров.

Однако такие результаты быстро уводят в область предположений и домыслов. Может быть, отношение числа «плохих» персонажей из сказок братьев Гримм к числу «хороших» — тоже золотое сечение?

ЦЕПНЫЕ ДРОБИ

Золотое сечение замечательно еще в одном отношении. В этот раз речь пойдет об одном типе *аппроксимации*. Работая с числами, которые невозможно представить в виде дроби, бывает удобно заменять их дробями, у которых сравнительно небольшие числитель и знаменатель и которые хорошо приближают исходное число. Например, дробь $22/7 = 3{,}14285\ldots$ — хорошая аппроксимация числа π, с точностью до шести знаков оно равно 3,14159. Эта аппроксимация была известна еще 2500 лет назад в Древнем Египте, и она достаточна для многих приложений.

Самые лучшие рациональные аппроксимации получаются при использовании *цепных дробей*. Они возникают в результате довольно сложного процесса.

Записывают цепную дробь в виде конечной последовательности натуральных чисел, заключенной в квадратные скобки; такая запись понимается следующим образом:

$$[a_0] = a_0,$$

$$[a_0, a_1] = a_0 + \frac{1}{a_1},$$

$$[a_0, a_1, a_2] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}},$$

$$[a_0, a_1, a_2, a_3] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}},$$

$$[a_0, a_1, a_2, a_3, a_4] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}}}.$$

$$\ldots$$

Если такая запись кажется слишком абстрактной, рассмотрите следующие примеры:

$$[3,9] = 3 + \frac{1}{9} = \frac{28}{9},$$

$$[2,3,5,7] = 2 + \cfrac{1}{3 + \cfrac{1}{5 + \frac{1}{7}}} = \frac{266}{115}.$$

Если аппроксимировать число самой подходящей цепной дробью, то чем больше чисел в этой дроби, тем лучше аппроксимация. Дело в том, что все числа после первого появляются в знаменателе, и чем больше числа, тем быстрее растет знаменатель, тем больше верных цифр получается в десятичной записи числа.

Что касается золотого сечения, оно отличается от всех иррациональных чисел следующим свойством: оно хуже всех представляется цепной дробью в том смысле, что в его представлении участвуют самые маленькие числа, и поэтому для заданной точности нужно брать довольно много членов. И действительно, самые лучшие цепные дроби для золотого сечения — это $[1]$, $[1,1]$, $[1,1,1]$, $[1,1,1,1]$ и т. д. Этот факт играет значительную роль в КАМ-теории[1)]. Согласно этой теории колеблющаяся система, в которой отношение частот составляет золотое сечение, особенно нечувствительна к возмущениям.

ГОЛОВОЛОМКА

Хорошо известна одна головоломка, имеющая отношение к числам Фибоначчи. На рис. 97.1 вверху изображен треугольник, разрезанный на четыре части. После перекладывания частей получается такой же треугольник, но теперь в нем одна клеточка остается незаполненной.

Решение головоломки — в конце статьи.

[1)] Приставка КАМ образована тремя первыми буквами фамилий ученых, создавших эту теорию, — Андрея Колмогорова, Владимира Арнольда и Юргена Мозера.

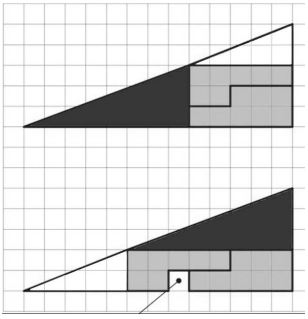


Рис. 97.1. Куда делся этот квадрат?

ИКОСАЭДР ПАЧОЛИ

Итальянский математик Лука Пачоли (1445–1517) открыл интересную связь между золотым сечением и платоновыми телами.

Возьмите три прямоугольника, стороны которых относятся в золотом сечении: длинная сторона длиннее короткой примерно в 1,618 раз.

Эти прямоугольники располагают так, что они пересекают друг друга в перпендикулярных направлениях, как изображено на рис. 97.2. Если прямоугольники деревянные, то для этого придется сделать распилы. А теперь сюрприз: если соединить вершины прямоугольников, то получится платоново тело, а именно икосаэдр.

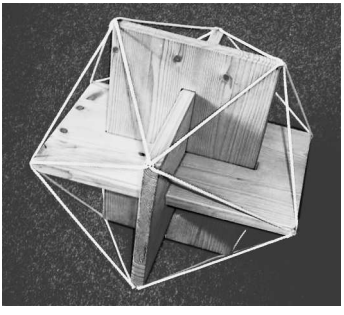


Рис. 97.2. Икосаэдр Пачоли

Это впечатляющий пример того, как то и дело в математике обнаруживаются удивительные связи между различными ее ветвями. Еще один такой пример мы видели в гл. 55, когда рассматривали «самую прекрасную формулу».

РЕШЕНИЕ ГОЛОВОЛОМКИ

Как же получается так, что кусочек плоскости исчезает при перекладывании частей? Дело в том, что фигура на рисунке — на самом деле вовсе не треугольник. У «треугольника» вверху гипотенуза немного вдавлена внутрь, а у «треугольника» внизу наоборот, немного выступает.

Вы можете сами убедиться в этом. У черного треугольника наклон гипотенузы составляет $\frac{3}{8} = 0{,}375$, а у белого — $\frac{2}{5} = 0{,}4$. Эти две дроби составлены из чисел Фибоначчи $2, 3, 5, 8$, и близость $\frac{2}{5}$ к $\frac{3}{8}$ объясняется именно сходимостью дробей, составленных из элементов последовательности Фибоначчи, к золотому сечению.

Глава 98

ОПТИМАЛЬНО УПАКОВАННАЯ ИНФОРМАЦИЯ

Необходимость обмена информацией между людьми с общими интересами возникает в самых разных областях. Как музыканты джаз-группы договариваются, в какой тональности они импровизируют? Как пары умудряются танцевать танго? Какой универсальный товарный код у товара, который покупатель хочет оплатить на кассе? В математике такие вопросы привели к созданию новой области, названной теорией кодирования. Она имеет дело с «оптимальной» упаковкой информации, причем термин «оптимальный» понимается в зависимости от ситуации.

Например, как можно передать сообщение, чтобы оставалась возможность его прочесть, даже если в ходе передачи оно будет повреждено? Первое, что приходит в голову, — передать сообщение несколько раз, скажем, пять. Крайне неправдоподобно, чтобы это сообщение было повреждено все пять раз в одном и том же месте, так что получатель сможет соединить неповрежденные куски из пяти экземпляров, чтобы составить нужный текст.

У этого метода есть серьезный недостаток — он до крайности неэкономичен. Существуют другие, более изящные решения этой задачи. Один из подходов требует использования компьютера. Сообщение буква за буквой переводится в строку из нулей и единиц. Можно считать, что каждый символ кодируется определенной последовательностью длины десять. Для простой проверки — успешно ли завершилась передача — можно добавить в код единицу или нуль, в зависимости от того, четно или нечетно число единиц в коде. Тогда получатель знает, что произошло что-то неладное, если «проверочная цифра» не соответствует

переданному коду. И теперь точность передачи может быть проверена за счет увеличения кода только на одну десятую. Правда, в случае ошибки не совсем ясно, где именно она локализована — в самом коде или в проверочной цифре — и как ее исправить. Но более изощренные системы кодирования справляются и с такими вопросами.

Высокое искусство теории кодирования — надежная передача сообщений даже по очень шумным каналам. Полученное сообщение может считаться корректным с очень высокой степенью надежности. Типичный пример успешных коммуникаций — изображения, полученные удаленными космическими зондами, например, с Марса. Кроме того, теория кодирования успешно применяется в вашем CD-плеере. Именно она позволяет воспроизводить вашу любимую песню, даже если диск случайно поцарапался.

КОДЫ, ИСПРАВЛЯЮЩИЕ ОШИБКИ

Проверочная цифра, как мы уже сказали, позволяет определить, не случилась ли где-нибудь ошибка при передаче сигнала. Если вы получили сообщение 011000001011, то знаете, что здесь что-то не так, поскольку в каждом пакете из одиннадцати цифр должно быть четное число единиц.

Обычно таких простых тестов достаточно, например, у кассы в супермаркете. Если там аппарат обнаруживает ошибку при считывании универсального товарного кода, то отказывается регистрировать товар, и кассиру остается только просканировать его еще раз.

Но иногда бывает важно знать, какой именно бит был передан неверно. Тогда можно исправить ошибку и восстановить исходное сообщение.

Первую простую реализацию такого кода описал Р. У. Хэмминг в 1948 г. В то время идея самокорректирующегося кода была революционной.

Чтобы ее понять, рассмотрим последовательность нулей и единиц длины 4, в общем виде она обозначается $a_1a_2a_3a_4$. Так, для последовательности 0110 получаются такие значения: $a_1 = 0$, $a_2 = 1$, $a_3 = 1$, $a_4 = 0$. Мы

добавим *три* проверочных бита, обозначив их a_5, a_6, a_7. Они определяются по следующим правилам:

- Если число единиц среди a_1, a_2, a_4 нечетно, то $a_5 = 1$, в противном случае $a_5 = 0$.
- Если число единиц среди a_1, a_3, a_4 нечетно, то $a_6 = 1$, в противном случае $a_6 = 0$.
- Если число единиц среди a_2, a_3, a_4 нечетно, то $a_7 = 1$, в противном случае $a_7 = 0$.

Затем передается последовательность символов $a_1a_2a_3a_4a_5a_6a_7$. В нашем примере, в котором требуется переслать последовательность 0110, расширенная последовательность имеет вид 0110110. Например, последняя цифра в ней a_7 — нуль, так как среди цифр a_2, a_3, a_4 (т. е. $1, 1, 0$) четное число единиц.

В чем мы выигрываем? Предположим, что в ходе передачи возникла ошибка, из-за которой изменился один бит. Мы знаем, что в каждой из последовательностей $a_1a_2a_4a_5$, $a_1a_3a_4a_6$ и $a_2a_3a_4a_7$ должно быть четное число единиц. Если бы ошибка была в бите a_1, то в последовательностях $a_1a_2a_4a_5$ и $a_1a_3a_4a_6$ было бы нечетное число единиц, а с последовательностью $a_2a_3a_4a_7$ было бы все в порядке. Так что при ошибке в бите a_1 получается такое число единиц для этих трех последовательностей: нечетно, нечетно, четно. А что для других битов?

- При ошибке в бите a_2: нечетно, четно, нечетно.
- При ошибке в бите a_3: четно, нечетно, нечетно.
- При ошибке в бите a_4: нечетно, нечетно, нечетно.
- При ошибке в бите a_5: нечетно, четно, четно.
- При ошибке в бите a_6: четно, нечетно, четно.
- При ошибке в бите a_7: четно, четно, четно.

Итак, зная, в какой из последовательностей $a_1a_2a_4a_5$, $a_1a_3a_4a_6$ или $a_2a_3a_4a_7$ неправильное число единиц, мы можем уверенно определить, в каком именно бите ошибка, исправить ее и восстановить исходное сообщение.

Пример. Предположим, что при передаче последовательности 0110110 произошла ошибка в первом бите, что привело к последовательности 1110110. Подсчитаем число единиц в $a_1a_2a_4a_5$, $a_1a_3a_4a_6$ и $a_2a_3a_4a_7$, т. е. в 1101,

1101 и 1100 — нечетное, нечетное, четное, так что следует сделать вывод, что ошибка в первом бите.

Обратите внимание, что код Хемминга не позволяет определить, сколько именно ошибок было сделано при передаче сообщения. Однако более изощренные самокорректирующиеся коды могут работать с последовательностями нулей и единиц произвольной длины, обнаруживая и исправляя две, три и даже больше ошибок. Как было сказано, такая способность к самокоррекции крайне важна для CD-плееров, поскольку выпускать абсолютно совершенные диски было бы слишком расточительно.

Глава 99

ЧЕТЫРЕХ КРАСОК ДОСТАТОЧНО

Возьмите лист бумаги и нарисуйте карту воображаемого континента, разместив на нем разные страны. Возьмите карандаши и раскрасьте эти страны так, чтобы никакие две страны с общим участком границы не были раскрашены в один цвет. Скоро вы обнаружите, что для карты всегда хватает четырех красок, как бы вы ни старались создать карту посложнее. Пример карты, для которой требуется четыре краски (и никак не меньше), вы видите на рис. 99.1.

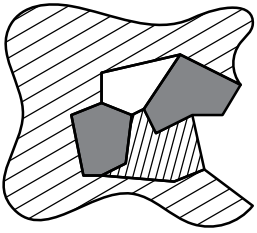


Рис. 99.1. Здесь нужно четыре краски (трех мало)

Это явление заметили еще в девятнадцатом веке. Однако математикам никогда не хватает экспериментальных наблюдений, как бы много их ни было. Нужно было доказать, что четырех красок хватит *всегда*, сколько бы ни было на карте стран и как бы сложно они ни располагались.

Попыток доказательства было много, однако задача оказалась твердым орешком. Математикам всего мира пришлось ждать до 1976 г., когда теорема о четырех красках была в конце концов доказана Кеннетом Аппелем и Вольфгангом Хакеном из Иллинойского университета. Почтовое отделение при этом университете гасило марки на письмах штемпелем со словами: «Четырех красок достаточно».

С этим доказательством была небольшая несостыковка, и из-за этого обсуждение задачи не прекращалось. До-

казательство было, несомненно, верным. Однако бóльшая часть рассуждений сводилась к обширным компьютерным вычислениям, которые были бы не под силу целой армии вычислителей из плоти и крови. Математики, на протяжении столетий полагавшиеся только на бумагу и карандаш, столкнулись с новой непривычной ситуацией и до сих пор не смирились с этим явлением. Даже если дюжина компьютеров подтвердит справедливость доводов, это не даст того удовлетворения, какое дает личная проверка шагов доказательства.

Для практических приложений теорема о четырех красках не представляет большого интереса. Она относится к категории теорем вроде «существует бесконечно много простых чисел» и «число π трансцендентно». Впечатляет в ней как раз то, что при очень простой формулировке решения пришлось ждать так долго, и оно наконец, было найдено. Навсегда. Для любого числа стран. Рано или поздно кто-нибудь найдет доказательство, не прибегая к компьютерным вычислениям, и тогда все будут довольны.

КАРТЫ И ГРАФЫ

Задача о четырех красках — прекрасный пример того, как математики могут находить самую суть задачи. При выборе цвета форма границы не играет никакой роли, важно лишь, чтобы у двух стран был общий участок границы. Поэтому задачу раскрашивания карты можно свести к задаче раскрашивания графа.

Каждую страну обозначают точкой на листе бумаги. Если у двух стран есть общий участок границы, их соединяют линией.

Такая система точек и линий называется *графом*[1)]. Графы встречаются не только в математике. Они полезны, чтобы изображать схемы метрополитена, например, или вычислительные блок-схемы.

Карту шестнадцати земель Германии можно преобразовать в граф, изображенный на рис. 99.2.

[1)] Это определение графа не имеет ничего общего с графиками функций, которые вы строили в школе.

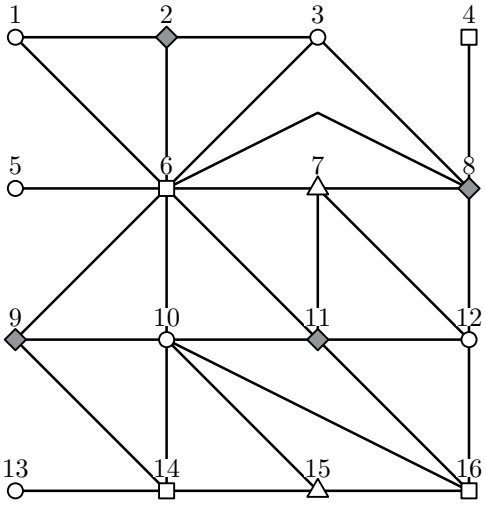


Рис. 99.2. Граф Германии

Числа на рисунке соответствуют следующим землям:

1. Гамбург
2. Шлезвиг-Гольштейн
3. Мекленбург — Передняя Померания
4. Берлин
5. Бремен
6. Нижняя Саксония
7. Саксония-Анхальт
8. Бранденбург
9. Северный Рейн — Вестфалия
10. Гессен
11. Тюрингия
12. Саксония
13. Саар
14. Рейнланд-Пфальц
15. Баден-Вюртембург
16. Бавария

Задача о раскраске звучит теперь так: можно ли раскрасить шестнадцать точек четырьмя красками так, чтобы никакие две точки, соединенные линией, не были одного цвета?

Такая раскраска для земель Германии показана на этом рисунке. Знаки ○, △, □, и ◆ соответствуют четырем разным краскам.

ВОЛК, КОЗА И КАПУСТА

Подходящее представление в виде графа может сделать задачу совсем простой, и примером тому служит классическая головоломка про волка, козу и капусту.

У крестьянина есть лодка, в которой ему нужно переправить через реку волка, козу и капусту. К сожалению, лодка слишком мала, и в ней помещается только один «пассажир». Дополнительная сложность в том, что некоторые пары нельзя оставлять на берегу вдвоем: коза может съесть капусту, а волк — козу.

Как организовать перевозки? Решение станет очевидным, если перевести задачу на язык графов. Мы назовем берега реки левым и правым и будем считать, что в начале все персонажи собрались на левом берегу. Как нужно действовать, чтобы волк не съел козу, а коза — капусту? Каждую возможную ситуацию мы изобразим точкой, и отметим возле нее персонажей, которые в этой ситуации находятся на левом берегу. На рис. 99.3 изображены все десять возможных ситуаций.

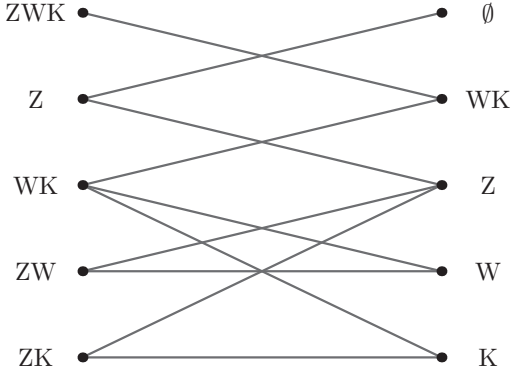


Рис. 99.3. Граф задачи о козе и капусте (Z — коза, W — волк, K — капуста)

Символ ∅ обозначает пустое множество (как в гл. 12) и указывает на то, что все пассажиры переправились на правый берег. Пять точек слева соответствуют ситуациям, когда крестьянин находится на левом берегу, а справа — когда он на правом берегу.

Например, вторая точка сверху в левом столбце с меткой «коза» означает, что коза и крестьянин — на левом берегу (и поэтому волк и капуста — на правом).

Точки, соответствующие запрещенным ситуациям, не изображены. Например, точка «коза, волк, капуста» в правом столбце означала бы, что крестьянин находится на правом берегу, а волк, коза и капуста — на левом, и в этом случае или коза бы съела капусту, или волк бы съел козу, или оба этих несчастья случились бы вместе. Поэтому такой точки на графе нет.

Теперь посмотрим на возможные переправы. Мы будем соединять любые две точки линией, если крестьянин может перейти из одного состояния в другое, перевезя одного пассажира. Например, линия, которая ведет из точки «волк, коза, капуста» слева в точку «волк, капуста» справа, означает, что крестьянин перевез козу с левого берега на правый, оставив пока волка и капусту. Обратите внимание, что из этой точки нельзя попасть ни в какую другую, поскольку для этого пришлось бы перевозить более одного пассажира, а по условию этого делать нельзя.

На языке графов задача звучит так. Есть ли путь, проходящий через допустимые точки из левой верхней точки (все на левом берегу) в правую верхнюю (все на правом)? Оказывается, есть, и по графу можно разобраться, каким должен быть порядок перевозок.

Глава 100

МАТЕМАТИКИ СТАНОВЯТСЯ МИЛЛИОНЕРАМИ

Когда поисковая система Google (Гугл) широко распространилась, ее основатели Сергей Брин и Лоуренс Пейдж вдруг оказались в рядах самых богатых людей планеты.

Тому, кто хочет повторить их успех, придется вначале получить в свое распоряжение гигантский компьютер и затем создать каталог всех веб-сайтов в мире. На сегодняшний день существует приблизительно двадцать миллиардов веб-страниц[1]. Для каждой страницы нужно завести индекс, отражающий все возможные показатели. Это сложная задача, но для команды талантливых программистов нет ничего невозможного. И разумеется, вся по-настоящему тяжелая работа досталась компьютеру.

Предположим, что все эти задачи успешно выполнены. Как ни огорчительно, этого мало, нужна еще конкурентоспособная поисковая система, поскольку Интернет поистине огромен. Несложно справиться с определенным запросом — скажем, на все страницы, содержащие слова «США» и «ураган», — и найти их все. Проблема в том, как отобразить эти результаты, ведь типичный поиск дает их от сотен тысяч до миллионов. Терпения пролистать все эти страницы не хватит никому. Поэтому хотелось бы, чтобы самые важные страницы отображались первыми. Те, кому «гуглить» приходится часто, знают, что Гугл удивительно успешно умеет справляться с этой задачей, и обычно удается найти искомое, просмотрев первую дюжину страниц или около того.

Секрет — в правильном понимании слова «важный». Идея в том, что важной считается та страница, на которую ссылаются много важных страниц. Будем изображать веб-страницу в виде точки и соединять две точки стрелкой, если

[1] Чтобы осознать это число, полезно вспомнить, что расстояние по поверхности Земли от Северного полюса до Южного составляет двадцать миллиардов миллиметров.

имеется ссылка с одной страницы на другую, на которую указывает стрелка. Тогда Интернет будет выглядеть как сеть из почти двух миллиардов точек, соединенных стрелками, которых больше миллиарда. Крохотный участок этой сети изображен на рис. 100.1.

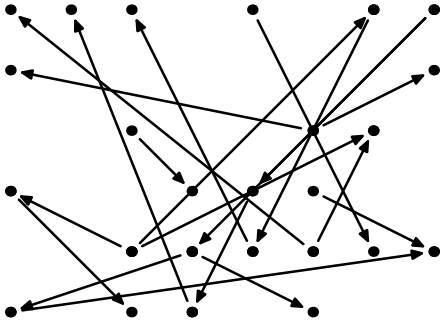


Рис. 100.1. Сеть ссылок на веб-страницы

Страницы, к которым ведет много стрелок, считаются «важными», в особенности если эти стрелки исходят из «важных» страниц. Если мы пронумеруем все страницы $1, 2, \ldots$ и присвоим вес W_i странице с номером i как меру важности этой страницы, то между этими числами должна существовать взаимосвязь.

Например, если на страницу 2 ссылается страница 5, а всего с нее имеются ссылки на три страницы, то страница 2 «унаследует» одну треть важности страницы 5. Возможно, на страницу 2 ссылается еще страница 7, и из нее выходят всего десять стрелок. Тогда страница 2 унаследует одну десятую важности W_7. Предположим, что других ссылок на страницу 2 нет. Тогда имеет место равенство

$$W_2 = \frac{W_5}{3} + \frac{W_7}{10}\,.$$

Большинство веб-сайтов связаны сложным образом, и потому в результате мы получаем более двадцати миллиардов уравнений с двадцатью миллиардами неизвестных $W_1, W_2, \ldots$.

Математика, которую мы учили в школе, здесь не поможет. Большинство читателей имели дело самое боль-

шее с двумя уравнения и двумя неизвестными. Но и для профессиональных математиков это число слишком велико, чтобы справиться с задачей обычными методами, хотя они с успехом применяются для оптимизационных задач с сотнями тысяч или даже несколькими миллионами переменных.

К цели ведет другой путь: «случайные блуждания». Представьте себе интернет-зависимую пользовательницу с навязчивым стремлением к веб-серфингу; будем звать ее Изабелла. Она стартует, скажем, со страницы http://www.pilotLZ.ru/. Затем она выбирает на этой странице случайную ссылку и переходит по ней. На новой странице Изабелла видит новый набор ссылок и одну из них выбирает наугад. Так начинается случайное блуждание по мировой паутине, в котором «более важные» страницы посещаются чаще, чем «менее важные». Замечательно, что относительные частоты посещений удовлетворяют построенной системе уравнений. Иначе говоря, важность страницы может измеряться долей времени, которое интернет-путешественник проводит на ней.

Однако провести такие вычисления, по-видимому, не проще, чем решить исходную задачу. И это действительно так, если требуется получить точные решения. Однако приблизительное решение (допустим, с точностью до пяти знаков) можно получить за несколько часов.

Теперь поисковая система вполне готова к работе: как только уровни важности вычислены, все остальное встает на место; нужно просто найти все страницы со словами «США» и «ураган», а затем вывести их в порядке убывания важности.

Так в первом приближении выглядит метод работы поисковой системы Google. Подробности и уточнения довольно сложны, и к тому же хранятся под таким же строгим секретом, как формула кока-колы. Уточнения могут потребоваться, если наша случайная путешественница Изабелла попадет на страницу, которая никуда не ссылается. Чтобы этого избежать, на каждом шаге поиска с некоторой вероятностью p все ссылки на странице игнорируются и вместо них пользователь переходит на случайную интернет-страницу. (Это может быть непросто

для Изабеллы, но при наличии директории всех веб-страниц проблем нет.) Говорят, что в поисковой системе Google используется значение $p = 0{,}15$, оно представляется разумным и, по-видимому, получено опытным путем. Кроме того, компания Google постоянно работает над устранением последствий «бомбардировок Google», — эта методика повышает важность веб-сайтов путем искусственного увеличения числа ссылок на одну из своих страниц.

Тем временем конкуренты Google тоже не дремлют. Идет постоянная работа по развитию новых подходов и вычислительных методов для оценивания «важности» веб-сайтов. Для различных пользователей и для различных комбинаций слов в запросе «важность» может быть разной. Но учет таких тонких материй приводит к проблеме — и у Гугла тоже — результаты поиска не удается получить за доли секунды.

ЧТО ЧИТАТЬ ДАЛЬШЕ

В последние годы появилось множество популярных книг по математике, некоторые из них уже упоминались на этих страницах. Здесь приводится небольшой список рекомендованного чтения для тех, кто хочет углубить свои знания. Полный регулярно обновляющийся обзор литературы можно найти в разделе «Rezensionen» на сайте www.mathematik.de.

M. Aigner, E. Behrends: *Alles Mathematik* (*Von Pythagoras zum CD-Player*). Vieweg+Teubner-Verlag, 2003 (3-е изд.)

Материалы лекций, прочитанных в берлинском научном обществе «Урания». Изложение ведется на более серьезном уровне, чем в настоящем издании, и требует более продвинутой математической подготовки.

M. Aigner, G. Ziegler: *Proofs from THE BOOK*. Springer-Verlag, 2010 (4-е изд.)

Собраны самые красивые математические доказательства. Для тех, кто уже немного знаком с математикой. [Имеется русский перевод: *М. Айгнер, Г. Циглер*. Доказательства из Книги. Лучшие доказательства со времен Евклида до наших дней. — М.: «БИНОМ. Лаборатория знаний», 2014.]

A. Beutelspracher: *Kryptologie*. Vieweg+Teubner-Verlag, 2008 (8-е изд.)

Для тех, кто хочет систематически изучить тему «Криптография».

A. Beutelspracher: *Mathematik für die Westentasche*. Pieper-Verlag, 2001.

Замысел этой книги напоминает замысел настоящего издания: множество коротких рассказов о различных аспектах математики, но совпадений между обеими книгами поразительно мало.

J. Bewersdorff: *Glück, Logik und Bluff*. Springer Spektrum Verlag, 2012 (6-е изд.)

В «Математических пятиминутках» речь шла о различных аспектах случайного и азартных игр. Тот, кто

хочет систематически продвинуться в математическом подходе к «игре», найдет в этой книге обзор важнейших положений.

A. Doxiadis: *Onkel Petros und die Goldbach-Vermutung*. Lübbe-Verlag, 2000.

В этом прекрасно написанном романе речь идет об ученом, который посвятил себя доказательству гипотезы Гольдбаха. О разрушении личности под влиянием увлечения математической задачей нигде лучше не написано. [Имеется русский перевод: *А. Доксиадис*. Дядя Петрос и проблема Гольдбаха. — Аст, 2002.]

U. Dudley: *Die Macht der Zahl*. Birkhäuser-Verlag, 1999.

Обязательное чтение для интересующихся мистикой чисел.

G. Glaeser, K. Polthier: *Bilder der Mathematik*. Spektrum-Verlag, 2010 (2-е изд.)

Пожалуй, никогда прежде математические понятия не были проиллюстрированы такими замечательными рисунками.

T. Gowers: *Mathematik*. Reclam-Verlag, 2011.

Автор — лауреат премии Филдса, очень плодовитый популяризатор математики в англоязычном мире. Рекомендуемая книга содержит немецкие переводы отдельных его работ.

P. Gritzman, R. Brandenberg: *Das Geheimnis des kürzesten Weges*. Springer-Verlag, 2005 (3-е изд.)

Это книга для сведущих в математике читателей, которые хотят больше узнать о математике, связанной с задачей коммивояжера.

H. Heuser: *Die Magie der Zahlen*. Herder-Spektrum, 2004 (2-е изд.)

Типичный Хойзер: написано отлично и очень информативно. О мистике чисел вы нигде не найдете больше.

R. Kanigel: *Der das Unendliche kannte*. Vieweg, 1995 (2-е изд.)

Это подробная биография гениального математика Рамануджана.

R. Kaplan: *Die Geschichte der Null*. Campus Verlag, 2003.

Очень информативная книга для тех, кто хочет больше узнать об истории нуля.

G. von Randow: *Das Ziegenproblem*. Rowohlt, 2004 (2-е изд.)

Задачу про козлика мы довольно подробно разобрали в гл. 14. Но еще больше информации о ведущем программы, козлах и вероятности можно найти в этой легко читающейся книге.

P. Ribenboim: *Die Welt der Primzahlen*. Springer-Verlag, 2011 (2-е изд.).

В настоящем издании мы много рассказывали о простых числах. Здесь эта тема излагается систематически.

M. du Sautoy: *Die Musik der Primzahlen*. C. H. Beck 2004 (4-е изд.), 2006.

... еще больше информации о простых числах.

S. Singh: *Fermats letzter Satz*. Carl Hanser, 1998, 2000.

Это одна из лучших популярных книг по математике. Читатель много узнает о математике и математиках из рассказа о задаче, которую решил Эндрю Уайлз, работая над теоремой Ферма. [Имеется русский перевод: *С. Сингх*. Великая Теорема Ферма. — М.: МЦНМО, 2000.]

S. Singh: *Geheime Botschaften*. Hanser, 2000, 2001.

Настолько же информативная и подробная, как книга о последней теореме Ферма, эта книга Сингха рассказывает об истории криптографии от античности до наших дней. Конечно же, в книгу включено подробное объяснение метода RSA, а также рассказ о работе шифровальной машины «Энигма» и о том, как англичане раскрыли ее секрет. [Имеется русский перевод: *С. Сингх*. Книга Шифров. — М.: Мир энциклопедий Аванта+, Астрель, 2009. — 464 с.]

G. Szpiro: *Die Keplersche Vermutung*. Springer-Verlag, 2011.

R. Taschner: *Der Zahlen gigantische Schatten*. Vieweg-Verlag, 2005 (3-е изд.)

Здесь можно найти многие из тем, обсуждавшихся в настоящем издании. Автор обратил свои знания в захватывающую и легко читающуюся книгу. К самым важным ее темам относятся: число и символы, число и музыка, число и время, число и пространство, числа и политика, число и материя, число и дух.

K. Wendland, A. Werner: *Facettenreiche Mathematik*. Vieweg+Teubner Verlag, 2011

Добавлено редактором русского перевода

Б. М. Писаревский, В. Т. Харин. О математике, математиках и не только. — М.: Лаборатория знаний, 2017 (4-е изд.).

Книга посвящена роли математики в познании человеком окружающего мира. На примере творческих биографий российских математиков XX века — А. Н. Колмогорова, С. Л. Соболева и А. Н. Тихонова — популярно рассказывается о достижениях современной математики.

К. Пиковер. Великая математика. От Пифагора до 57-мерных объектов. 250 основных вех в истории Математики. — М.: БИНОМ. Лаборатория знаний, 2015 (перевод с английского).

Великолепно иллюстрированное издание с краткой информацией к каждой иллюстрации. Для тех, кто любит математику, и для тех, кто еще не успел ее полюбить.

К. Дрёссер. Обольстить математикой. Числовые игры на все случаи жизни. — М.: Лаборатория знаний, 2018 (5-е изд.) (перевод с немецкого).

Книга написана легко, с юмором, а потому не следует опасаться математических сложностей: тут все понятно и вполне доступно для всех — и физиков, и лириков.

К. Дрёссер. Обольстить логикой. Выводы на все случаи жизни. — М.: Лаборатория знаний, 2017 (5-е изд.) (перевод с немецкого).

Эта книга полностью оправдывает свое название. Прочитав ее, вы поймете прелесть логического мышления и увидите, как логика помогает нам рассуждать и делать выводы даже в самых непростых жизненных ситуациях.

ОГЛАВЛЕНИЕ

Предисловие к третьему изданию 5
Предисловие ко второму изданию 6
Предисловие 7
«Пять минут математики» в газете Die Welt 8
Введение 10
Глава 1. **Госпожа удача** 13
Насколько вероятно выиграть главный приз в лотерее?
Глава 2. **Волшебная математика: тысяча и одно волшебство** 17
Фокус с числом 1001
Глава 3. **Сколько лет капитану?** 20
Математическая точность. Коэффициент комфорта
Глава 4. **Головокружительно большие простые числа** 22
Простых чисел бесконечно много. Доказательство Евклида
Глава 5. **Проигрыш + проигрыш = выигрыш** 25
Парадоксы теории вероятностей: Парронdo, дней рождения и перестановок
Глава 6. **Интуиция подводит нас, когда речь идет о больших числах** 28
Письма счастья. Рисовый сель
Глава 7. **Ключ к шифру — в телефонной книге** 33
Криптография с открытым ключом. Шифрование с помощью случайных чисел
Глава 8. **Деревенский цирюльник, который сам себя бреет** 37
Парадокс Рассела
Глава 9. **Уйди, пока ты впереди** 40
Правило остановки. Теорема о правиле остановки
Глава 10. **Может ли обезьяна создать великое литературное произведение?** 43
Шимпанзе за клавиатурой
Глава 11. **Парадокс дней рождения** 46
Насколько вероятно совпадение дней рождения?
Глава 12. **Horror vacui** 51
Пустое множество. Объединение и пересечение

Глава 13. **Достаточная сложность математической логики необходима** 54
Необходимость и достаточность
Глава 14. **Менять или не менять? Парадокс Монти Холла** 57
Задача про козлика. Условные вероятности. Формула Байеса
Глава 15. **В отеле Гильберта всегда есть свободные номера** 67
Отель Гильберта
Глава 16. **Это удивительное число π** 70
Число π в библии. Простые оценки
Глава 17. **Вычисляемая случайность** 73
Предельная теорема теории вероятностей
Глава 18. **Миллионная награда: как распределены простые числа?** 77
Распределение простых чисел. Теорема о простых числах. Гипотеза Римана
Глава 19. **Пятимерный торт** 80
Размерность. Четырехмерный куб (гиперкуб)
Глава 20. **Казнить нельзя помиловать** 84
Ассоциативный и коммутативный законы в математике и речи
Глава 21. **Возьми меня на Луну** 90
Конкретные приложения математики
Глава 22. **Остатки сладки** 93
a mod b. Вычисления по модулю. Теорема Ферма
Глава 23. **Совершенно секретно!** 96
Алгоритм RSA. Теорема Эйлера
Глава 24. **Волшебная математика: порядок среди хаоса** ... 101
Фокус Джилбрейта
Глава 25. **Как вступить в контакт с гением** 104
Гаусс. 17-угольник. Простые числа Ферма
Глава 26. **О полутонах и корнях двенадцатой степени** 109
Пифагорова и хроматическая гаммы
Глава 27. **Вечно я не в той очереди!** 112
Теория очередей
Глава 28. **Незаслуженно недооцененное число** 115
Ноль
Глава 29. **Я люблю считать!** 118
Некоторые комбинаторные результаты. Биномиальные коэффициенты
Глава 30. **Гений-самоучка. Индийский математик Рамануджан** 123
Удивительная судьба индийского математика

Глава 31. **Я терпеть не могу математику, ведь...** 126
Почему эту науку так не любят?
Глава 32. **Путешествующий коммивояжер. Современная Одиссея** 129
Задача о коммивояжере. P=NP?
Глава 33. **Квадратура круга** 132
Построения циркулем и линейкой
Глава 34. **Шаг в бесконечность** 139
Принцип индукции
Глава 35. **Математика в твоем CD-плеере** 144
Кодирование. Теорема отсчетов
Глава 36. **Логарифм. Вымирающее племя** 147
Умножение как сложение логарифмов
Глава 37. **Математика, достойная награды** 150
Абелевская премия. Медаль Филдса
Глава 38. **Почему именно аксиомы?** 153
Аксиоматика
Глава 39. **Компьютерное доказательство** 156
Задача о четырех красках
Глава 40. **Лотерея. Маленькие выигрыши** 159
Вероятность угадать 1, 2, ..., 6 правильных номеров
Глава 41. **Формулы = концентрат мысли** 162
Преимущество буквенных обозначений. Декарт
Глава 42. **Бесконечный рост** 165
Число e. Экспонента
Глава 43. **Как кванты вычисляют?** 169
Квантовый компьютер. Кубиты
Глава 44. **Крайности!** 174
Типичная задача об экстремальных значениях. Имитация отжига
Глава 45. **Бесконечно малые?** 177
Бесконечно малые величины. Нестандартный анализ
Глава 46. **Математика в пожарной части** 180
Ошибки первого и второго рода
Глава 47. **Первому доказательству уже 2500 лет** 183
Элементы Евклида. Теорема Фалеса
Глава 48. **В математике есть трансцендентное, хотя нет ничего мистического** 186
Иерархия чисел: натуральные, целые, рациональные... числа
Глава 49. **Каждое четное число равно сумме двух простых?** 191
Гипотеза Гольдбаха

Глава 50. **Почему мы неправильно обращаем условные вероятности** 195
Формула Байеса
Глава 51. **Миллионер или миллиардер?** 199
Обозначения на разных языках
Глава 52. **Математика и шахматы** 202
Правила игры и аксиомы
Глава 53. **«Книга природы написана языком математики»** 205
Математика и реальность. Как применяется математика?
Глава 54. **Поиск простых чисел Мерсенна** 208
Простые числа-рекордсмены
Глава 55. **Берлин, XVIII век: открыта самая красивая формула** 212
Разложение в ряд экспоненты, синуса и косинуса
Глава 56. **Первое действительно сложное число** 215
Иррациональность корня из двух
Глава 57. **P=NP: Нужно ли везение в математике?** 218
P- и NP-задачи
Глава 58. **Вам всего лишь 32 года!** 221
Разные системы счисления
Глава 59. **Игла Бюффона** 224
Эксперимент Бюффона по вычислению π
Глава 60. **Жара и холод: контролируемое охлаждение как способ решения задач оптимизации** 228
Имитация отжига. Задача о коммивояжере
Глава 61. **Кто не заплатил?** 232
Неконструктивное доказательство существования. Принцип кроликов и клеток
Глава 62. **О чем говорит статистика?** 235
Статистический контроль качества
Глава 63. **Арбитраж** 238
Опционы. Принцип арбитража для определения цены
Глава 64. **Прощай, риск. Опционы** 241
Опционы пут и колл
Глава 65. **Отражает ли математика реальный мир?** 244
Правдоподобны ли следствия из аксиом? Парадокс Банаха–Тарского
Глава 66. **Математика, которую слышно** 247
Анализ Фурье. Синус как собственная частота черного ящика
Глава 67. **Случай-композитор** 252
Игральные кости: метод Моцарта

Глава 68. **Бывает ли игральным костям совестно?** 255
Совпадение
Глава 69. **Клубничное мороженое убивает!** 257
Как лжет статистика
Глава 70. **Процветание для всех** 260
Письма счастья в бесконечном мире
Глава 71. **Никакого риска, спасибо!** 263
Хеджирование в финансовой математике
Глава 72. **Нобелевская премия в математике?** 266
Абелевская премия
Глава 73. **Случай-вычислитель: метод Монте-Карло** 270
Как вычисляют площади с помощью датчика случайных чисел
Глава 74. **Нечеткая логика** 274
Нечеткое управление
Глава 75. **Секретные послания в Библии** 277
Мистика чисел. Библейские коды. Закон малых чисел
Глава 76. **Насколько узловатым может быть узелок?** 281
Теория узлов. Инварианты узлов
Глава 77. **Сколько математики нужно человеку?** 285
Почему математика?
Глава 78. **Много, больше, еще больше!** 288
Иерархия бесконечностей. Диагональный метод Кантора
Глава 79. **Вероятно, это верно** 291
Вероятностное доказательство. Алгоритм Шора для квантового компьютера
Глава 80. **Живем ли мы в скрюченном мире?** 294
Неевклидова геометрия
Глава 81. **Бывают ли в математике стандарты?** 297
Математическая речь (за небольшим исключением) стандартизована
Глава 82. **Взмах крыльев бабочки** 301
Теория хаоса. Линейные задачи
Глава 83. **Разбогатеть гарантированно** 304
Феномен больших чисел
Глава 84. **Не доверяйте тем, кому за тридцать** 307
Правда ли, что математическая креативность с возрастом быстро убывает?
Глава 85. **Равенство в математике** 309
Тождество зависит от контекста
Глава 86. **Волшебные инварианты** 311
Математика и волшебство

Глава 87. **Математика идет в кино** 315
Как представлена математика в кинематографе
Глава 88. **Ленивая восьмерка: бесконечность** 317
Как математики работают с бесконечностью
Глава 89. **Поля книг должны быть шире!** 320
Задача Ферма. Бесконечный спуск
Глава 90. **Математика: что у нас внутри** 324
Компьютерная томография. Обратная задача
Глава 91. **Мозг внутри компьютера** 326
Нейронная сеть. Перцептрон
Глава 92. **Cogito, ergo sum** 330
Декарт. Декартовы координаты
Глава 93. **Есть ли в мире дыры?** 333
Гипотеза Пуанкаре
Глава 94. **Так ли страшны комплексные числа?** 336
Комплексные числа
Глава 95. **Эшер и бесконечность** 340
Морис Эшер. Паркеты
Глава 96. **В начале единица встречается чаще двойки** 344
Закон Бенфорда
Глава 97. **Подсолнух и ратуша в Лейпциге** 348
Золотое сечение. Последовательность Фибоначчи. Цепные дроби
Глава 98. **Оптимально упакованная информация** 354
Теория кодирования. Контрольные биты. Коды Хэмминга
Глава 99. **Четырех красок достаточно** 358
Задача о четырех красках. Графы
Глава 100. **Математики становятся миллионерами** 363
Алгоритмы Гугла
Что читать дальше 367

Минимальные системные требования определяются соответствующими требованиями программ Adobe Reader версии не ниже 11-й либо Adobe Digital Editions версии не ниже 4.5 для платформ Windows, Mac OS, Android и iOS; экран 10″

Научно-популярное электронное издание

Берендс Эрхард

МАТЕМАТИЧЕСКИЕ ПЯТИМИНУТКИ

Ведущий редактор *И. Маховая*
Технический редактор *Е. Денюкова*
Корректор *Е. Клитина*
Оригинал-макет подготовлен *Е. Ивлевой, О. Лапко* в пакете LaTeX 2$_\varepsilon$
Подписано к использованию 24.03.20.
Формат 125×200 мм

Издательство «Лаборатория знаний»
125167, Москва, проезд Аэропорта, д. 3
Телефон: (499) 157-5272
e-mail: info@pilotLZ.ru, http://www.pilotLZ.ru

МАТЕМАТИЧЕСКИЕ ПЯТИМИНУТКИ

Много ли математических знаний можно получить за 5 минут? Оказывается, не так уж и мало при наличии квалифицированного гида. Если читателю не повезло в школе с учителем математики и у него создалось впечатление о математике как об унылой научной дисциплине, посвященной исключительно манипуляциям с громоздкими формулами, то самое время открыть эту книгу – и математика засверкает своими неожиданно увлекательными гранями. Вы узнаете о криптографии и теории кодирования, о парадоксах, об удивительно простой формуле, связывающей знаменитые константы, о квантовых компьютерах, о странностях теории вероятностей, о непростых простых числах, о том, как выиграть в лотерею, и о многом, многом другом. В книге собрано 100 увлекательных эссе, автор которых – профессор математики Эрхард Берендс – ранее публиковал их еженедельно в газете «ДиВельт» в рубрике «Пять минут математики». Поэтому книгу можно читать, открыв на любой главе.

Если вы привыкли проводить досуг за интеллектуальными занятиями, то потратьте 5 минут из них на расширение своего математического кругозора – будет интересно! А если не привыкли к такому времяпрепровождению, то попробуйте – вдруг понравится?