Г. Н. Берман

ЧИСЛО и НАУКА О НЁМ

MCMLIV

Г. Н. Берман

ЧИСЛО И НАУКА О НЁМ

ОБЩЕДОСТУПНЫЕ ОЧЕРКИ ПО АРИФМЕТИКЕ НАТУРАЛЬНЫХ ЧИСЕЛ

Издание второе исправленное

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1954

ОТ ИЗДАТЕЛЬСТВА.

Первое издание книги «Число и наука о нём» вышло в свет в 1948 г. (кроме того, в 1949 г. был отпечатан дополнительный тираж). Настоящее, второе издание книги выходит после смерти автора Георгия Николаевича Бермана (последовавшей 9 февраля 1949 г.). При подготовке настоящего издания к печати Издательство сочло необходимым учесть замечания, высказанные в рецензиях и письмах читателей, и внесло в текст книги некоторые уточнения и исправления.

Г. Н. Берман. Число и наука о нём.

Редактор *А. З. Рывкин.* Техн. редактор *Н. Я. Мурашова.*
Обложка, титул. заставки и концовки художника *В. А. Селенгинского.*
Корректор *Л. О. Сечейко.*

Сдано в набор 29/IX 1953 г. Подписано к печати 3/II 1954 г. Бумага 84×108¹/₃₂. Физ. печ. л. 10,25. Условн. печ. л. 8,4. Уч.-изд. л. 7,77. Т-00317. Тираж 50 000. Цена 2 р. 35 к. Заказ № 830.

Государственное издательство технико-теоретической литературы
Москва, Б. Калужская ул., 15.

4-я типография им. Евг. Соколовой Союзполиграфпрома
Главиздата Министерства культуры СССР. Ленинград, Измайловский пр., 29.

Памяти
НИКОЛАЯ БОРИСОВИЧА
ГОФМАНА,
павшего смертью храбрых

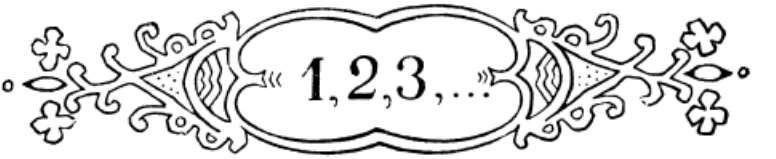
ИЗ ПРЕДИСЛОВИЯ АВТОРА К ПЕРВОМУ ИЗДАНИЮ.

Существует много книг — хороших книг, — задача которых возбудить интерес к математике. У этой книжки цель иная: удовлетворить тех, кто уже интересуется математикой, но не имеет достаточной подготовки, чтобы читать специальную литературу. Поэтому читатель не найдёт здесь ни математических головоломок, ни забавных анекдотов. Книжка эта посвящена общедоступному, но серьёзному изложению некоторых глав учения о целых числах. Для её понимания достаточно знать арифметику и немного алгебры в объёме примерно VIII—IX классов средней школы. Дать материал для чтения начинающим учителям, студентам педагогических училищ, а главное старшим школьникам, работающим в математических кружках, — вот к чему стремился автор.

Книга эта ни в коем случае не является учебником. Поэтому автор, чтобы сделать её живее, сознательно отказался от систематического изложения основ учения о числе. Но, возможно, студенты-математики увидят в ней удобный трамплин для прыжка из уютной элементарной арифметики в серьёзную и чопорную теорию чисел.

Автор благодарит всех, кто содействовал написанию и опубликованию этой книги. Особенно благодарен автор проф. А. Ф. Берманту, внимательно прочитавшему рукопись и давшему ряд ценных указаний.

Москва
1947 г.



ВВЕДЕНИЕ.

Понятие натуральных чисел возникло из потребностей счёта на самых ранних ступенях развития человеческого общества, задолго до появления понятий дробных и отрицательных чисел. Натуральными называются числа: один, два, три, четыре, пять, шесть и т. д. Современный человек знакомится с ними ещё в дошкольном возрасте.

И всё же, несмотря на свою привычность и повседневность, натуральные числа обладают многими свойствами, далеко не общеизвестными. Существует целая наука — теория чисел, — которая занимается их изучением. Наука эта обладает интересной особенностью: задачи её кажутся простыми и понятными; о результатах её можно рассказать всякому достаточно грамотному человеку. Но путь решения задач, способы достижения результатов порою очень трудны и сплошь да рядом недоступны даже лучшим математикам. Недаром крупнейший немецкий математик Гаусс (1777—1855) говорил, что арифметика — царица математики. Он имел в виду, разумеется, не элементарную арифметику, а именно теорию чисел, которую называют иначе высшей арифметикой и на дальнейшее развитие которой оказали большое влияние труды самого Гаусса.

Натуральных чисел бесконечно много: среди них нет наибольшего. Нам это кажется ясным. В самом деле, какое бы большое число мы ни взяли, если мы прибавим к нему единицу, то получим число ещё большее. Эта бесконечность числового ряда создаёт значительные трудности при логическом обосновании арифметики.

В этой книжке основы арифметики (аксиомы и простейшие правила) не рассматриваются.

Ряд натуральных чисел — чисел, которые служат для пересчитывания предметов, — начинается с единицы, а не с нуля. Нуль вводится вместе с отрицательными числами для того, чтобы сделать операцию вычитания возможной и в тех случаях, когда вычитаемое равно или больше уменьшаемого. Положительные целые, отрицательные целые числа и нуль образуют систему целых чисел, основные правила действий над которыми рассматриваются в начале школьного курса алгебры. Здесь в основном будет говориться о свойствах натуральных чисел. Но там, где это может упростить изложение, будут использованы и отрицательные числа и нуль.

Какие же свойства натуральных чисел мы будем рассматривать? Прежде всего — различные способы их записи и обозначения, развитие и взаимную связь этих способов. Далее — вопросы, которые возникают при делении целых чисел друг на друга (делимость, общий наибольший делитель, разложение на простые множители и т. д.). В заключительных главах будут разобраны некоторые свойства простых чисел.

Учением о простых числах занимались лучшие русские математики: Чебышев, Золотарёв и другие. В двадцатом веке самые крупные, самые блестящие результаты в этой области были получены советскими математиками: Л. Г. Шнирельманом и особенно академиком И. М. Виноградовым. Об этих результатах будет рассказано в последней главе этой книжки.

ГЛАВА I.

НАША СИСТЕМА СЧИСЛЕНИЯ.

Первобытному человеку считать почти не приходилось. «Один», «два» и «много» — вот все его числа. Но нам — современным людям — приходится иметь дело с числами буквально на каждом шагу. Нам нужно уметь правильно назвать и записать любое число, как бы велико оно ни было. Если бы каждое число называлось особым именем и обозначалось в письме особым знаком, то запомнить все эти слова и знаки было бы никому не под силу. Как же мы справляемся с этой задачей? Нас выручает хорошая система обозначений. Совокупность немногих названий и знаков, позволяющая записать любое число и дать ему имя, называется системой счисления, или нумерацией.

Наша нумерация использует для записи чисел десять различных знаков. Девять из них служат для обозначения первых девяти натуральных чисел (1, 2, 3, 4, 5, 6, 7, 8, 9), десятый не обозначает никакого числа; он представляет собою просто пробку, «пробельный материал» при записи чисел. Значок этот называют нулём и обозначают 0.

Итак, мы имеем девять значков для обозначения первых девяти чисел и десятый значок — нуль — «позиционную пробочку» *). Значки эти называются цифрами.

Как же с помощью десяти цифр записать любое число? Подумаем сначала, как бы мы стали пересчитывать большое число одинаковых предметов, например спичек. Мы сначала

*) О слове «позиционная» см. примечание на стр. 9.

разложили бы наши предметы на кучки по десяти в каждой. Получилось бы некоторое количество десятков (и, может быть, осталось бы несколько предметов, не вошедших в целые десятки). Далее нам пришлось бы пересчитать кучки (десятки). Если бы и кучек (десятков) было очень много, мы сгруппировали бы их тоже в десятки и т. д.

Таким путём мы приходим к основной идее нашей системы счисления — к мысли о единицах различных разрядов. Десять единиц образуют один десяток: иными словами, десять единиц первого разряда образуют одну единицу второго разряда. Десять единиц второго разряда образуют одну единицу третьего. Вообще, десять любых единиц образуют единицу следующего разряда.

Несмотря на всю свою кажущуюся простоту, такая система счисления прошла очень долгий путь исторического развития. В её создании принимали участие многие народы.

Возникает законный вопрос: почему стали раскладывать предметы на десятки, а не на пятки или дюжины? Почему единицы каждого разряда в десять, а не в восемь и не в три раза больше единиц предыдущего разряда?

Счёт десятками получил особенно широкое распространение потому, что люди располагают естественной «счётной машиной», связанной с числом десять: именно — десятью пальцами на руках.

Записать какое-нибудь число, например «пятьдесят семь», пользуясь десятью основными значками и некоторыми связующими словами, можно хотя бы так: «5 единиц второго разряда и 7 простых единиц». Но такой способ записи громоздок. Удобнее и короче было бы записывать числа без помощи слов, одними знаками (цифрами). И в самом деле, мы записываем число «пятьдесят семь» так: 57. Эти две цифры, поставленные рядом, обозначают сумму двух чисел: правое (в нашем примере 7) даёт число простых единиц, а левое (5) — число единиц второго разряда (десятков). Если написаны три цифры подряд, то крайняя правая обозначает простые единицы, следующая (средняя) — единицы второго разряда (десятки), а крайняя левая — единицы третьего разряда, т. е. сотни; значит, 238 обозначает сумму двух сотен, трёх десятков и восьми единиц. Вообще, из двух написанных рядом цифр левая выражает единицы, в десять раз бо́льшие, чем правая. Не только сама цифра, но и её место,

её позиция*) имеют значение. Поэтому нашу нумерацию называют позиционной нумерацией.

Напишем по нашей нумерации число «сто два». Здесь одна единица третьего разряда (сотня) и две простые единицы. Записать это так: «12» — нельзя: ведь так записывается число «двенадцать». Писать «1 2», оставляя место для отсутствующего разряда, неудобно; можно подумать, что здесь широко написанное число «двенадцать» или просто два числа: «один» и «два». Как, далее, отличить в записи следующие числа: «двенадцать» и «сто двадцать»; где оставлять при этом пустое место? Для устранения этих неудобств и введена «позиционная пробка» — цифра нуль. Её пишут на месте отсутствующего разряда. С её помощью числа «двенадцать», «сто два» и «сто двадцать» напишутся по-разному (12; 102; 120).

Позиционная десятичная нумерация известна была индусам полторы тысячи лет назад (а может быть, и раньше); в Европу её занесли арабы, вторгшиеся в Испанию в VIII веке нашей эры. Арабская нумерация распространилась по всей Европе и, будучи проще и удобнее остальных систем счисления, о которых речь будет в следующей главе, быстро их вытеснила. До сих пор наши цифры принято называть арабскими. Впрочем, за 1000 лет все цифры, кроме единицы и девятки, сильно изменились. Приводим для сравнения наши (называемые «арабскими») и настоящие арабские цифры:

Скажем несколько слов о принятых у нас наименованиях чисел. Названия первых шести разрядов (единицы, десятки,

*) Слово «positio» (позйцио) значит по-латыни «положение».

сотни, тысячи, десятки тысяч, сотни тысяч) очень древни и у разных народов звучат по-разному. Думать о происхождении этих названий — дело филолога, а не математика. Слово «миллион» сравнительно недавнего происхождения. По-итальянски millione (миллио́нэ) есть увеличительное от mille (ми́лле), что значит «тысяча». По-русски ему могло бы соответствовать несуществующее слово «тысячища». Придумал слово «миллион» известный венецианский путешественник XIII в. Марко Поло, которому нехватило обыкновенных чисел, чтобы рассказывать о необычайном изобилии людей и богатств далёкой Небесной Империи *). Теперь миллионами, десятками и сотнями миллионов называют единицы седьмого, восьмого и девятого разрядов. Тысяча миллионов называется биллионом или миллиардом, а далее, для построения числовых наименований, единых во всём мире, используются латинские числительные. Чтобы лучше понять, как строятся названия этих числовых гигантов, вспомним, что каждые три разряда образуют к л а с с: простые единицы, десятки и сотни образуют первый класс; тысячи, их десятки и сотни — второй класс; миллионы — третий класс, биллионы — четвёртый и т. д.

Чтобы назвать единицу какого-нибудь класса, начиная с четвёртого, надо уменьшить номер класса на два и к полученному числу, названному по-латыни, прибавить окончание «иллион». Так, единица пятого класса называется «триллион», потому что $5 - 2 = 3$, а 3 по-латыни tres (трэс); в сложных же словах tres переходит в tri (звучит так же, как наше «три»). Возьмём единицу двадцать второго класса. Это будет, как нетрудно сообразить, единица 64-го разряда (единице двадцать второго класса предшествует 21 класс, т. е. $21 \times 3 = 63$ разряда). Значит, запишется это число так:

1 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000

Как же его назвать? От номера класса отнимаем двойку: $22 - 2 = 20$; двадцать по-латыни viginti (вигинти); значит, наше число следует назвать «вигинтиллион».

Построенные таким образом названия мало удобны. Латынь знают не все. Кроме того, названия очень больших чисел громоздки и неудобопроизносимы. Даже хороший латинист вряд ли назовёт число, записанное в виде единицы с пятью

*) Так в старину называли Китай.

миллионами нулей. Впрочем, и записать такое число практически невозможно.

Почему же не реформируют, не изменят способа называть и записывать большие числа? Неужели нельзя внести сюда рационализацию? — Конечно, можно, и даже сравнительно легко. Но в этом нет ни малейшей надобности. Большие числа, подобные написанному выше гиганту, встречаются только в сборниках математических курьёзов, да в некоторых отделах теории чисел...

Позвольте, позвольте, — перебьёт читатель: а физика, а астрономия? Ведь за большими числами даже кличка установилась: «астрономические» числа!

Терпенье, читатель! Сейчас будет речь и об «астрономических» числах. Но раньше приведём таблицу наименований единиц высоких разрядов не столько для пользы (польза от неё, как мы скоро увидим, невелика), сколько для удовлетворения любопытства.

1 000 000 000	(единица	10	разряда	или 4	класса)	— биллион,
1 000 000 000 000	(»	13	»	» 5	»)	— триллион,
1 000 000 000 000 000	(»	16	»	» 6	»)	— квадриллион,
1 000 000 000 000 000 000	(»	19	»	» 7	»)	— квинтиллион.

Далее следуют: секстиллион, септиллион, октиллион, нониллион, дециллион, ундециллион и т. д.

В некоторых странах, например во Франции, биллионом называют не тысячу, а миллион миллионов, т. е. единицу 13-го разряда; триллионом называют миллион этих «крупных» биллионов (наш квинтиллион) и так далее, считая классы не по три, а по шесть разрядов. Это несколько упрощает наименование больших чисел.

Поговорим теперь об «астрономических числах»; причём, прежде чем забираться на небо, поищем их на земле. Чему равны, например, поверхность, объём и масса земного шара? Заглянув в учебник географии, находим:

Поверхность земного шара	—	509 000 000 $км^2$,
Объём » »	—	1 070 000 000 000 $км^3$,
Масса »	»	— 6 000 000 000 000 000 000 000 тонн.

Последнее число (масса) представляет собою 6 единиц 22-го разряда, т. е. шесть секстиллионов.

Все эти числа обладают одной особенностью; это — числа «круглые», оканчивающиеся нулями. Разумеется, ни поверхность, ни объём Земли не могут быть выражены таким «круглым» числом квадратных и кубических километров.

«Круглота» здесь кажущаяся. Ведь все геодезические измерения на земной поверхности — приближённые, хотя и производятся очень тщательно; поэтому и числа для поверхности и объёма земного шара суть числа приближённые.

Рассмотрим внимательнее число 509 000 000 (пятьсот девять миллионов). Шесть нулей справа не обозначают здесь отсутствия тысяч и низших разрядов. Этих разрядов мы либо не знаем, либо сознательно не пишем, так как такая точность нам не нужна. Мы округляем результат, мы говорим: число квадратных километров земной поверхности складывается из пятисот девяти миллионов и какого-то числа тысяч, сотен, десятков и единиц, но какого именно — точно не указываем.

В практической жизни при счёте предметов, которых очень много, например жителей какой-либо страны или красных кровяных телец в крови человека, а также при измерении различных величин удаётся определить только первые 3 — 4 верные цифры результата. При точнейших измерениях современной физики, которые сопровождаются предосторожностями, превосходящими самые смелые выдумки технической фантазии, удаётся получить семь, в редчайших случаях — восемь верных цифр; если получается целое число бо́льше чем с восемью цифрами, то приходится дописывать на конце нули. Значит, любое большое число, данное практически, можно записать как произведение не более чем восьмизначного (а чаще — трёх-четырёхзначного) числа на «единицу с нулями» *) (например, поверхность земли 509 000 000 $км^2$ можно записать так: $509 \times 1\,000\,000$ или $509 \cdot 1\,000\,000$). Числа до миллиарда нетрудно и назвать и записать; следовательно, всё дело в том, чтобы рационально записывать и называть числа, изображаемые единицей с большим числом нулей.

Тут нам на помощь приходит понятие степени. Число, изображаемое единицей с нулями, является степенью десяти. Например, сто есть вторая степень десяти ($100 = 10^2$), тысяча — третья степень десяти ($1000 = 10^3$). Вообще, число, изображаемое единицей с нулями, представляет собою такую степень десяти, сколько у него нулей; это можно записать следующим образом:

$$\underbrace{10\,000\ldots\ldots\ldots0000}_{p \text{ нулей}} = 10^p.$$

*) Так коротко называют число, которое имеет первую цифру 1, а все остальные — нули, например 10, 100, 1000, 10 000 000 и т. д.

Можно сказать и так: единица n-го разряда представляет собою $(n-1)$-ю степень десяти (например, миллион — единица 7-го разряда — равняется 10^6).

Эти соображения позволяют очень коротко и удобно называть и записывать все числа, которые даются нам наукой и жизнью. Рассмотрим, например, массу земного шара. Вот число, которым она выражается:

6 000 000 000 000 000 000 000 тонн.

Теперь мы его можем записать так $6 \cdot 10^{21}$ тонн, а назвать: «шесть на десять в двадцать первой» (подразумевается: степени). Это и коротко и удобно.

Чтобы привыкнуть к этой системе обозначений и названий, рассмотрим несколько примеров.

После первой мировой войны 1914—1918 гг. в ряде стран, в том числе и у нас, была хозяйственная разруха, сопровождавшаяся обесцениванием денег. Приходилось выпускать огромные массы бумажек всё более и более высокой номинальной стоимости. Это явление, называемое инфляцией, сопровождалось у нас несколько раз деноминацией, т. е. выпускались деньги сравнительно невысокой номинальной стоимости, причём объявлялось, что один рубль нового выпуска равняется сотне или тысяче рублей предыдущего. Эти деноминации приводили к тому, что на денежных знаках не приходилось печатать очень большие числа: дальше миллионов дело не шло. Но в Германии, где инфляция не сопровождалась деноминацией, существовали боны и даже почтовые марки необычайно высокого номинального достоинства: в десятки и сотни миллиардов марок. На рис. 1 читатель видит несколько почтовых марок с «астрономической» номинальной стоимостью. Высший номинал почтовой марки,

Рис. 1.

выпущенной в Германии, — пятьдесят миллиардов, т. е. $5 \cdot 10^{10}$ марок; боны бывали ещё более высокого достоинства.

Классическим примером числового гиганта является награда, которую, если верить старинной легенде, потребовал себе изобретатель шахматной игры. Он, гласит предание, просил за первую клетку доски одно зерно риса, за вторую — два, за третью — четыре и т. д., за каждую последующую — в два раза больше, чем за предыдущую. Эта скромная на вид просьба оказалась невыполнимой: все житницы мира не могут вместить риса, затребованного хитрым изобретателем. Действительно, за первую клетку ему следовало получить одно зерно, т. е. $2-1$. За первую и вторую ему следовало $1+2=3=2 \cdot 2-1$ зерно. За первые три клетки $1+2+4=7=2 \cdot 2 \cdot 2-1$ зёрен. Мы видим, что за некоторое число a первых клеток придётся отдать

$$\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{a \text{ раз}} - 1, \text{ т. е. } 2^a - 1 \text{ зёрен.}$$

Значит, за все 64 клетки изобретателю причитается $2^{64} - 1$ зёрен *). Число 2^{64} легче всего вычислить, пользуясь сочетательным свойством умножения: ведь 2^{64} есть произведение 64 двоек; их можно соединить в группы из 20, из 20, из 20 и из 4 двоек; мы получим:

$$2^{64} = 2^{20} \cdot 2^{20} \cdot 2^{20} \cdot 2^4.$$

Вычислить $2^{10} = 1024$ нетрудно. Помножив 1024 на себя, получим $2^{20} = 1\,048\,576$. Следовательно,

$$2^{64} = 1\,048\,576 \times 1\,048\,576 \times 1\,048\,576 \times 16.$$

Остаётся сделать скучное, но не трудное умножение. Окончательно получим:

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

Число это читается так: восемнадцать квинтиллионов четыреста

---

*) Читатели, знакомые с прогрессиями, сообразят, что числа зёрен, приходящиеся на каждую клетку, образуют геометрическую прогрессию со знаменателем 2, т. е. $\div 1, 2, 4, \ldots, 2^{63}$. Сумма членов такой прогрессии равна $\frac{2^{64}-1}{2-1} = 2^{64} - 1$.

сорок шесть квадриллионов семьсот сорок четыре триллиона семьдесят три биллиона семьсот девять миллионов пятьсот пятьдесят одна тысяча шестьсот пятнадцать. Оно приблизительно равно $18 \cdot 10^{18}$ (читается так: «восемнадцать на десять в восемнадцатой»).

Вспомним известную задачу-шутку о самом большом числе, которое можно записать с помощью трёх девяток.

Ответом этой задачи служит не наивное число 999 и не внушительное 9^{99} или 99^9, а «трёхэтажный» гигант 9^{9^9}. Запись его с помощью нашей системы счисления приблизительно такова: $4 \cdot 10^{369\,693\,099}$ (четыре на десять в триста шестьдесят девять миллионов шестьсот девяносто три тысячи девяносто девятой; его и по сокращённому способу назвать трудно!):

$$9^{9^9} \approx 4 \cdot 10^{369\,693\,099}$$

($\approx$ — знак приближённого равенства).

Рядом с таким числом исполином «астрономические» числа кажутся жалкими карликами. Рассмотрим, например, расстояние до самых далёких небесных объектов — галактик, доступных современным телескопам. Галактики — это грандиозные звёздные системы, состоящие из миллиардов звёзд; они так далеки, что свет от них до нас доходит почти в 1 миллиард лет; это значит, что они отстоят от нас почти на 10^{22} километров.

Итак, расстояние до галактик, доступных современным телескопам, равно 10^{22} *км* или $10^{22} \cdot 10^5 = 10^{27}$ *см* (в 1 *км* содержится $100\,000 = 10^5$ *см*). В физике все длины принято выражать в сантиметрах, поэтому и мы выразили это расстояние в сантиметрах. Это число нетрудно назвать: ведь 10^{27} равно одной единице двадцать восьмого разряда или одной единице десятого класса. Отнимая от десяти два, получим восемь (см. стр. 10 — как называть большие числа). Значит, название нашей единицы должно происходить от латинского octo (восемь), т. е. расстояние до галактик, доступных современным телескопам, равно одному октиллиону сантиметров.

Подведём итог этой главе. Для обозначения и записи чисел мы пользуемся позиционной десятичной нумерацией. Позиционной она называется потому, что значение цифры зависит от её положения — места в ряду других цифр написанного числа; десятичной — потому, что из двух написанных

рядом цифр левая обозначает единицы, в десять раз бо́льшие, чем правая. Для обозначения и записи чисел в пределах миллиарда эта система очень удобна. Для записи очень больших чисел она неудобна (получаются очень «длинные» числа), а для их названий — практически совсем неприменима. Чтобы устранить эти неудобства, пользуются понятием *степени* числа. Представляя число в виде произведения относительно небольшого числа на степень десяти, мы без труда записываем и называем все числа, встречающиеся в науке и в жизни.

ГЛАВА II.

КАК СЧИТАЛИ НАШИ ПРЕДКИ?

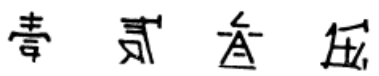
ак люди считали и как называли числа до изобретения письменности, мы точно не знаем. Об этом можно только догадываться. Несомненно одно: человечество овладевало счётом очень медленно. На ранних ступенях общественного развития люди обходились тремя числами: «один», «два», «много». Прошли, вероятно, многие тысячи лет, прежде чем это «много» отодвинулось дальше. Во всяком случае, ко времени изобретения письменности люди умели уже неплохо считать.

Четыре тысячи лет назад наиболее развитые народы (египтяне, холдеи) умели писать и пользовались не только целыми, но и простейшими дробными числами. Больше того, тогда уже существовали школы, в которых обучали искусству счёта.

В первобытном письме букв не было. Каждая вещь, каждое действие изображалось картинкой. Постепенно картинки упрощались; наряду с изображениями предметов и действий появились особые фигуры, обозначающие различные свойства вещей, а также значки для слов, соответствующих нашим предлогам и союзам. Так возникла письменность, называемая иероглифами; при иероглифической записи каждому значку соответствует не звук, как у нас, а целое слово. Специальных знаков (цифр) для записи чисел тогда не было, но словам «один», «два», «семнадцать» и т. д. соответствовали определённые иероглифы. Их было не так уж много, потому что больших чисел люди тогда не знали. В некоторых странах (например, в Китае и Японии) иероглифическое письмо сохранилось до наших дней.

Вот японские иероглифы, изображающие числа:

Ещё более замысловаты китайские иероглифы:



При иероглифической записи говорить о системе счисления не приходится: никакой системы нет. Впрочем, в древнем Египте намечалось нечто, напоминающее отдалённо нашу современную нумерацию.

На следующей ступени развития появляются буквы, обозначающие звуковые элементы слов. К этому времени люди умеют уже хорошо считать, во всяком случае, они уже знают тысячи и десятки тысяч. Появляются ц и ф р ы, т. е. особые значки для некоторых чисел, причём любое число (в известных пределах) может быть записано с помощью этих значков. Цифрами обычно служат те же буквы алфавита. Такого рода нумерации были у древних евреев, греков, у римлян и у наших предков славян. Мы остановимся на римской и на славянской нумерациях.

Римские цифры общеизвестны; вот они:

I	V	X	L	C	D	M
1	5	10	50	100	500	1000

Знаки эти, собственно, не цифры, а заглавные латинские буквы: «и», «вэ», «икс», «эль», «це», «де» и «эм». Но они играли роль цифр: с их помощью римляне могли записать любое число до миллиона. Вот как это делалось. Два и три записывались соответственно так: II, III (т. е. две единицы, три единицы). Четыре записывалось IV: единица, поставленная слева, «отнималась» от пяти. Наоборот, единицы, по-

ставленные справа, прибавлялись: пять, шесть, семь и восемь записывались так:

V, VI, VII, VIII.

Далее приходилось вводить значок X. Девять записывалось следующим образом: IX (от десяти отнимается единица), а десять, одиннадцать и т. д. так:

X, XI, XII, XIII, XIV.

Пятнадцать получалось комбинированием значков десятки и пятёрки: XV; двадцать, тридцать — с помощью десяток:

XX, XXX.

Для сорока и выше приходилось вводить знак L. Сорок один, например, писали так: XLI (десять отнимается, а единица к пятидесяти прибавляется). Для девяноста использовался знак сотни C, именно, 90 записывалось так: XC. Заметим, что 49 и 99 писали не так: XLIX, XCIX, а так: IL, IC. Сто два писалось CII, триста семьдесят четыре — CCCLXXIV и т. д. Большое число, например 29 635, записывали следующим образом:

$$XXIX_{m}DCXXXV$$

(маленькая буква *m**) обозначала тысячи).

Здесь мы видим уже вполне разработанную нумерацию, очень экономную (с помощью семи цифр записываются числа до миллиона), но неудобную: сравнительно небольшие числа записываются длинно, и никакого облегчения при вычислениях не получается: письменных вычислений производить невозможно, и считать фактически приходится в уме.

Славянская нумерация сходна с латинской тем, что тоже использует для записи чисел буквы алфавита. Она не так экономна, в ней употребляется больше (27) знаков, но сама запись гораздо систематичнее и позволяет значительно упростить выполнение действий. В отличие от римской она пользуется не заглавными, а строчными буквами, снабжёнными к тому же особым знаком — титлом (҃) (который, впрочем, употреблялся и в обычном письме для сокращения слов).

---

*) Начало латинского слова mille (ми́лле) — тысяча.

Вот славянские цифры:

Числа одиннадцать, двенадцать, ... записывались соответственно так: АІ, БІ, ...; двадцать один, двадцать два, ... — КА, КБ ... и т. д. Титло ставилось только над одной из цифр. Порядок цифр при записи числа был такой же, как в его устном названии. Мы говорим, например, «пятнадцать» (по славянски — пятьнадесять), — называя вперед цифру единиц, потом десяток. Славяне так и писали: ЄІ, т. е. впереди писали пятёрку, а за нею десяток. Наоборот, в числе «двадцать три» мы сперва называем десятки, потом единицы; у славян это отражалось в письме: писали КГ. Место цифры, её положение в числе не имело значения.

С помощью этих знаков легко записывались большие числа. Число 29 946 записывалось, например, таким образом: ≠КА ЦМЅ (знак ≠ обозначал тысячи). С помощью повторения знака ≠ можно было записывать очень большие числа. Вот как, например, записывалось число 20 178 073: ≠≠К ≠РОН ЗГ.

Нетрудно видеть, что эта система записи позволяет выполнять действия «столбиками», почти так же, как это делаем мы теперь.

Скажем несколько слов о названиях чисел в древней Руси. Числа до тысячи назывались почти так же, как сейчас *). Десять тысяч называлось «тьма», и число это считалось столь огромным, что тем же словом обозначалось всякое неподдающееся учёту множество. В более позднее время (XVI—XVII вв.) появилась своеобразная система наименования чисел, так называемое «великое словенское число»; в этой системе чйсла до 999 999 называются почти так же, как теперь. Слово «тьма» обозначает не десять тысяч, а миллион. Кроме того, появляются следующие названия: «тьма тем» или «легион» (т. е. миллион миллионов или по теперешнему триллион, т. е. 10^{12}); легион легионов («леодр»), который мы теперь должны записать с помощью единицы с 24 нулями (септиллион — 10^{24}); наконец, леодр леодров («во́рон»), т. е. по нынешнему 10^{48}. Про это число наши предки говорили, что «более сего несть разумевати». Впрочем, иногда (рукопись XVII в.) упоминалась ещё «колода», равная десяти «во́ронам» (10^{49}), но при этом оговаривалось, что «сего числа несть больше» **).

Позиционная нумерация возникла, повидимому, в древнем Вавилоне. Там она приняла такую своеобразную форму, что о ней стоит поговорить подробнее; это будет сделано немного дальше. От вавилонян позиционная нумерация перешла к индусам.

У индусов, как и у многих древних народов, первыми математиками были жрецы. Они ведали календарём и праздниками, следили за небесными светилами и должны были уметь предсказывать различные явления на небе (затмения и т. п.). Для этого нужно было обладать известными математическими познаниями. От существовавшей в старину связи математики с религией сохранился курьёзный пережиток — числовые суеверия; и в наше время есть люди, которые считают, что число 3 приносит счастье, а 13 — несчастье («чортова дюжина»).

---

*) Была небольшая разница в произношении: например, один назывался «един», двадцать — «двадесять» и т. д.

**) См. брошюру проф. А. В. Васильева — «Целое число» или книгу В. Беллюстина «Как постепенно дошли люди до настоящей арифметики».

Три тысячи лет назад индусы уже пользовались хорошо разработанной нумерацией, хотя в памятниках того времени и не упоминаются числа, бóльшие 100 000. В позднейших произведениях индийской письменности встречаются значительно бóльшие числа — до ста квадриллионов (10^{17}). В одной из сравнительно «молодых» легенд о Будде (ей меньше тысячи лет) говорится, что он знал названия чисел до 10^{54}. Впрочем, индусы, повидимому, не представляли себе ясно бесконечности натурального ряда, они полагали, что существует какое-то наибольшее число, известное только богам. Доказательство бесконечности числового ряда — заслуга древнегреческих учёных.

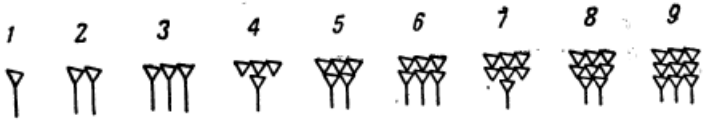
Совершенно особый интерес, как мы уже упоминали, представляет вавилонская математика. Вавилонская нумерация зародилась почти четыре тысячи лет назад, просуществовала полторы тысячи лет (с XVIII до III в. до н. э.) и пользовалась широким распространением на всём Ближнем Востоке. Она оказала влияние на китайскую, индийскую и греческую математику. Даже в современной науке, как мы увидим, остался её заметный след.

Вавилоняне писали палочками на пластинках из мягкой глины и обжигали потом свои «рукописи». Получались прочные кирпичные «документы», частично уцелевшие до нашего времени; их нередко находят при раскопках в Месопотамии (нынешний Ирак). Поэтому изучить вавилонскую историю вообще и математику в частности удалось довольно хорошо.

На рубеже XIX и XVIII вв. (до нашей эры) произошло слияние двух народов: сумерийцев и аккадян. Каждый из этих народов имел достаточно развитую торговлю, весовые и денежные единицы. Правда, торговля была мелкая, считать приходилось немного, и разработанной нумерации ни один из этих народов не имел. Единицей веса у сумерийцев была «мина» $\left(\text{приблизительно } \frac{1}{2}\ кг\right)$. Денежной единицей служила мина серебра. У аккадян основная единица — «шекель» — была в шестьдесят раз меньше (разумеется, не точно, а приблизительно в шестьдесят раз, но примитивные весы того времени не улавливали разницы). После слияния этих народов «имели хождение» обе системы единиц: минами и шекелями пользовались так, как мы теперь пользуемся килограммами и граммами. А в денежном обращении мины и шекели

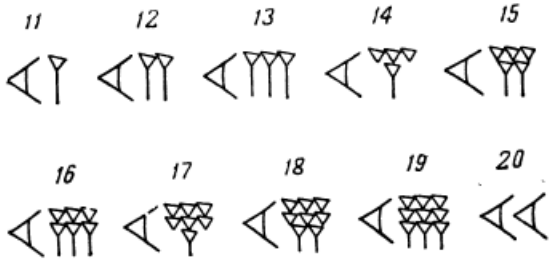
играли роль наших рублей и копеек, с той только разницей, что более крупная единица равнялась не ста, а шестидесяти мелким единицам. Торговля и хозяйство развивались, обороты росли. Как нам кроме граммов и килограммов нужны тонны, так там появилась более увесистая единица — «талант». Естественно, что раз отношение «шестьдесят» было уже привычным в хозяйственных расчётах, новую единицу установили в шестьдесят раз крупнее имеющейся. Один талант был равен шестидесяти минам.

Как же вавилоняне записывали числа? Они писали палочками, вдавливая их в мягкую глину, поэтому основным графическим элементом был у них клинышек ▽ или ◁. Для обозначения единицы использовался один клинышек, поставленный вертикально: ▽; начертание чисел от единицы до девяти естественно и понятно:



Каждое число до девяти включительно изображалось соответствующим количеством клинышков, расположенных столь разумно, что при чтении не приходилось их пересчитывать: количество их сразу бросалось в глаза.

Для десяти был особый знак ◁. Запись чисел второго десятка тоже понятна:



Мы видим, что и эти знаки очень наглядны. Теперь читатель без труда запишет сам любое число в пределах первой

сотни. Например, числа 37 и 54 запишутся так:

Числа восьмого и девятого десятков записываются довольно громоздко; но в них ведь не было надобности. Числá, большего пятидесяти девяти, благодаря наличию трёх единиц, вавилонянам записывать вообще не приходилось.

Первоначально мины обозначались более крупными значками, чем шекели. Например, 20 мин 37 шекелей записывалось так:

В более поздние времена все знаки записывались совершенно одинаково, и только положение знака показывало, какие единицы он обозначает. Например, 2 таланта 13 мин 41 шекель записывалось так:

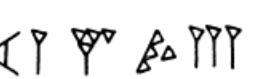
Если приходилось иметь дело только с одной какой-нибудь мерой, то и тогда её никак не обозначали. Сопровождающий текст позволял сразу догадываться, о каких мерах идёт речь.

На рубеже XVIII в. до н. э. появляются чисто математические тексты: таблицы для облегчения вычислений, правила решения задач и т. п. Высокого развития достигает астрономия. В связи с этим приходится, во-первых, всё чаще и чаще сталкиваться с большими числами, а во-вторых, от чисел именованных перейти к отвлечённым. Вместо того, чтобы придумывать другую, используют для новых целей уже разработанную нумерацию. Теперь запись

обозначает не обязательно 1 талант 23 мины 15 шекелей — совершенно так же записывается отвлечённое число, содер-

жащее одну единицу третьего, 23 единицы второго и 15 единиц первого разряда, причём единицы каждого последующего разряда в шестьдесят раз крупнее единиц предыдущего. Запись

обозначает, по нашему, $1 \cdot 60^2 + 23 \cdot 60 + 15$, т. е. 4995. Аналогично записываются четырёх-, пяти-, вообще многозначные числа. Например, запись



обозначает $2 \cdot 60^3 + 11 \cdot 60^2 + 4 \cdot 60 + 43$, т. е. 471 883. Наибольшее число, которое встречается в вавилонских «рукописях», равно $60^8 + 10 \cdot 60^7$. Вавилонская нумерация — вполне разработанная нумерация с основанием 60 — шестидесятиричное счисление.

Как же обозначали вавилоняне нуль? Как записывали они число 3605, равное $1 \cdot 60^2 + 5$, т. е. содержащее одну единицу третьего, пять единиц первого и совсем не содержащее единиц второго разряда? Они в течение сотен лет вовсе не пользовались знаком разделения. В нужных случаях они оставляли между цифрами более широкий промежуток:

означало у них 3605, а

— 65

Но клинописное письмо очень неудобно для оценки величины промежутков между цифрами, а необходимость переписывать всё от руки приводила к частым опискам. Знак разделения был необходим, и он появился. Начиная с некоторого времени (точную дату установить невозможно), на вавилонских кирпичиках появляется значок  , соответствующий нашему нулю.

Теперь 3605 записывают так:

а 65 так:

— смешать их больше нельзя.

Однако, введя «позиционную пробку» в середине чисел, вавилоняне так и не додумались ставить её на конце. И до самого падения вавилонской культуры числа «единица», «шестьдесят», «три тысячи шестьсот» записывались одинаково:  . Записывать шестьдесят так:  вавилонянам не приходило в голову. Только индусы, заимствовавшие у них позиционную нумерацию, научились правильно использовать знак нуля и, введя вместо шестидесяти основание десять, дали счислению его современную форму.

Вавилонская (шестидесятиричная) система счисления удержалась до сих пор при измерении углов и времени. Шестую часть окружности делят на 60 градусов, градус на 60 минут, минуту на 60 секунд. Точно так же час делится на 60 минут, минута на 60 секунд, подобно тому, как талант делился на 60 мин, а мина на 60 шекелей. Скажем, кстати, несколько слов о происхождении названий «минута» и «секунда». Минута (minuta) значит по-латыни: «маленькая»; а секунда (secunda) значит: «вторая». Минуты это были «partes minutae primae» (па́ртэс мину́тэ при́мэ) — «впервые малые части», а секунды — «partes minutae secundae» (па́ртэс мину́тэ секу́ндэ) — «вторые малые части» градуса или часа.

Подведём итоги. Человечество овладевало счётом медленно. Много столетий понадобилось человечеству для того, чтобы от чисел «один», «два» и «много» перейти к десяткам и сотням. Даже научившись писать, люди долго не имели разработанной нумерации и записывали числа с помощью иероглифов.

У древних евреев, а через них у греков, римлян и славян возникла нумерация с помощью букв алфавита. Эта нумерация просуществовала приблизительно две тысячи лет и была достаточна для целей практики.

Почти четыре тысячи лет назад в Вавилоне возникла позиционная нумерация. В Индии она приняла форму позиционной десятичной нумерации с применением «позиционной пробки» — нуля. У индусов эту систему записи чисел заимствовали арабы, ставшие в VIII — IX вв. н. э. одним из самых культурных народов мира. От арабов переняли её европейцы (отсюда — название: арабские цифры).

В наше время позиционная десятичная нумерация совершенно достаточна для нужд науки и практики. При написании же очень больших чисел удобно пользоваться знаком показателя степени.

ГЛАВА III.

ДЛЯ ЧЕГО И КАК АРХИМЕД СЧИТАЛ ПЕСОК?

III в. до н. э. на острове Сицилия жил математик совершенно исключительной одарённости. И сейчас, более чем через две тысячи лет после его кончины, имя его известно любому школьнику. Это был Архимед. Замечательный геометр, механик, физик и военный инженер, он оставил среди своих многочисленных творений удивительное сочинение по арифметике. Называется оно «Псаммит или исчисление песку в пространстве, равном шару неподвижных звёзд».

Архимед впервые убедительно показал, что для любого количества предметов, как бы велико оно ни было, можно найти соответствующее ему число; можно для любого числа указать его место в ряду уже известных чисел, построить числа ещё бо́льшие и назвать все эти числа. Иными словами, он построил научную систему счисления.

Архимед доказывает, что если предположить наполненный песком шар, равный аристархову *) шару неподвижных звёзд, то и тогда среди чисел можно найти такие, которые превосходят число песчинок, заполняющих этот шар. Для того чтобы заранее устранить всякие возможные возражения против доказательства этого предложения, Архимед принимает радиус сферы неподвижных звёзд в мириаду, т. е. в десять тысяч раз бо́льшим, чем расстояние от Земли до Солнца, а последнее полагает равным мириаде мириад стадий, т. е.

*) Архимед опирается здесь на воззрения выдающегося древнегреческого астронома Аристарха Самосского (конец IV в. — 1-я половина III в. до н. э.), полагавшего, что Солнце неподвижно и находится в центре сферы неподвижных звёзд, что Земля обращается по окружности, в центре которой находится Солнце.

АРХИМЕД

Один из античных бюстов, считавшихся изображением Архимеда.

по-нашему $150 \cdot 10^7$ *км* *). Это — в десять раз больше среднего расстояния от Земли до Солнца, для которого современные измерения дают приблизительно $150 \cdot 10^6$ *км*. Таким образом, радиус сферы неподвижных звёзд, в пересчёте на наши меры, Архимед принимал равным $15 \cdot 10^{12}$ *км*, что значительно превосходило даже аристархов радиус сферы неподвижных звёзд. Это примерно в три раза меньше фактического расстояния до ближайшей к нам звезды. Значит, принятый Архимедом радиус сферы неподвижных звёзд примерно в 650 миллионов раз меньше, чем расстояние до галактик, доступных нашим современным телескопам.

Теперь нетрудно вычислить объём «шара неподвижных звёзд». Он равен

$$\frac{4}{3}\pi R^3 \approx 4 \cdot 15^3 \cdot 10^{36} = 135 \cdot 10^{38} \text{ км}^3 **).$$

Остаётся подсчитать, сколько в этот объём можно вместить песчинок. Архимед считал, что в объёме макового зерна может вместиться мириада (10 000) песчинок (иными словами, он рассматривал весьма тонкий песок — лёгкую пыль). Поперечник макового зерна он считал равным одной сороковой части дюйма ***), т. е. по-нашему $\frac{1}{2}$ *мм*.

Считая, для простоты, что зерно имеет форму кубика, мы видим, что в одном кубическом миллиметре содержится 8 маковых зёрен или 80 000 песчинок; в кубическом метре — в 10^9 (в биллион) раз больше, т. е. $8 \cdot 10^{13}$, а в кубическом километре — ещё в 10^9 больше, т. е. $8 \cdot 10^{13} \cdot 10^9 = 8 \cdot 10^{22}$ песчинок. Остаётся перемножить число кубических километров «шара неподвижных звёзд» ($135 \cdot 10^{38}$) и число песчинок в одном кубическом километре ($8 \cdot 10^{22}$). Это даст, примерно, 10^{68} песчинок — число и по нашим современным масштабам громадное.

Мы без труда решили архимедову задачу. Но во времена Архимеда не было названий для чисел, бо́льших десяти тысяч,

---

*) Греческая стадия равнялась приблизительно 150 метрам. От слова «стадия» происходит «стадион»: первоначально — разделённая на стадии дорожка, на которой состязались бегуны. Слово «мириада» значит десять тысяч. Слов для обозначения чисел, бо́льших чем 10 000, в греческом языке не было.

**) Мы считаем, для простоты расчётов, $\pi = 3$. Эта неточность не влияет на существо результата.

***) Греческий дюйм равнялся приблизительно 2 *см*.

не было десятичной системы счисления, не было знака показателя, не было разработанных правил действий. Заслуга Архимеда именно в том, что он выдумал, как называть большие числа и как производить с ними вычисления (при вычислениях он пользовался только свойствами арифметической и геометрической прогрессий, которые и в то время были известны). Это вычисление очень интересно, но говорить о нём в нашей небольшой книжке нет возможности *). Мы рассмотрим только архимедову систему счисления.

Для первого десятка тысяч, т. е. до первой мириады, Архимед использует существовавшие тогда греческие числительные. Далее он называет числа до мириады мириад подобно тому, как мы называем числа до тысячи тысяч. Так число 85 643 911 Архимед назовёт: «восемь тысяч пятьсот шестьдесят четыре мириады три тысячи девятьсот одиннадцать». Все числа от единицы до мириады мириад он называет «числами первыми». Простую единицу он называет «единицей чисел первых», а мириаду мириад единиц чисел первых — «единицей чисел вторых». Итак, «единица чисел вторых» — это 10^8. Теперь нетрудно назвать числа до мириады мириад «единиц чисел вторых», т. е. по-нашему до 10^{16}. Это число Архимед называет «единицей чисел третьих» и т. д. Мы видим здесь позиционную систему счисления с основанием 10^8, но разработаны только названия, а не написание чисел, в котором Архимед для решения своей задачи не нуждался. Единица каждого разряда у Архимеда в 10^8 раз больше единицы предшествующего разряда.

Таким образом можно дойти до единицы любых чисел вплоть до мириадо-мириадных. Единица n-х чисел будет равна, как легко сообразить, $10^{8(n-1)}$ (например, единица десятых чисел — $10^{8(10-1)} = 10^{72}$; единица сто двадцать четвёртых чисел — $10^{8(124-1)} = 10^{984}$ и т. д.). Счёт можно довести до мириады мириад чисел мириадо-мириадных, т. е. до $10^8 \cdot 10^{8\,(100\,000\,000-1)} = 10^{8 \cdot 10^8}$. Этих чисел Архимеду вполне достаточно для решения его задачи. Мы видели, в самом деле, что решением служит $10^{63} = 10^7 \cdot 10^{8(8-1)}$, т. е. тысяча мириад единиц чисел восьмых.

---

*) Интересующиеся с удовольствием прочтут сами «Псаммит», который, начиная с 1824 г., неоднократно издавался в русском переводе. Последнее издание: «Исчисление песчинок (Псаммит)», перевод Г. Н. Попова, М.—Л., 1932 г.

Но Архимед на этом не останавливается. Как мы, кроме единиц различных разрядов, вводим единицы различных классов, так он вводит числа различных периодов. Все числа до $10^{8 \cdot 10^8}$ он называет числами первого периода. Мириаду мириад чисел мириадо-мириадных он называет «единицей первых чисел второго периода». Затем вводятся вторые, третьи числа и т. д. до мириадо-мириадных чисел второго периода. Мириада мириад мириадо-мириадных чисел второго периода ($10^{2 \cdot 8 \cdot 10^8}$) образует единицу первых чисел 3-го периода. Единицей первых чисел четвёртого периода будет число $10^{3 \cdot 8 \cdot 10^8}$. Вообще единицей первых чисел n-го периода будет число $10^{(n-1) \cdot 8 \cdot 10^8}$, а единицей m-х чисел n-го периода — число $10^{(n-1) \cdot 8 \cdot 10^8 + m \cdot 8 - m}$. Так Архимед доходит до мириады мириад мириадо-мириадных чисел мириадо-мириадного периода, т. е. до числа $10^{8 \cdot 10^{16}}$. На этом Архимед останавливается. Но продолжать его путь нетрудно. Вслед за периодами можно ввести какие-нибудь циклы или периоды второго порядка и т. д.

Архимедову систему счисления удобно представить в форме следующей таблицы:

Первый период — от 1 до $10^{8 \cdot 10^8} - 1$.

Первые числа — от 1 до $10^8 - 1$.

Вторые числа — от 10^8 до $10^{16} - 1$.

. . . . . .

m-е числа — от $10^{(m-1) \cdot 8}$ до $10^{8m} - 1$.

. . . . . .

Мириадо-мириадные числа — от $10^{8 (10^8 - 1)}$ до $10^{8 \cdot 10^8} - 1$.

Второй период — от $10^{8 \cdot 10^8}$ до $10^{2 \cdot 8 \cdot 10^8} - 1$.

Первые числа — от $10^{8 \cdot 10^8}$ до $10^{8 \cdot (10^8 + 1)} - 1$.

. . . . . .

Третий период — от $10^{2 \cdot 8 \cdot 10^8}$ до $10^{3 \cdot 8 \cdot 10^8} - 1$.

. . . . . .

N-й период от $10^{(N-1) \cdot 8 \cdot 10^8}$ до $10^{8N \cdot 10^8} - 1$.

Первые числа — от $10^{(N-1) \cdot 8 \cdot 10^8}$ до $10^{(N-1) \cdot 8 \cdot (10^8 + 1)} - 1$.

. . . . . .

m-е числа — от $10^{(N-1) \cdot 8 \cdot 10^8 + 8m - 8}$ до $10^{(N-1) \cdot 8 \cdot 10^8 + 8m} - 1$.

. . . . . .

Мириадо-мириадные числа — от $10^{8 \cdot N \cdot 10^8 - 8}$ до $10^{8 \cdot N \cdot 10^8} - 1$

. . . . . .

Мириадо-мириадный период от $10^{(10^8 - 1) \cdot 8 \cdot 10^8}$ до $10^{8 \cdot 10^{16}} - 1$.

Для того чтобы лучше разобраться в архимедовом счислении и оценить его достоинства, посмотрим, как с его помощью можно назвать числовые гиганты, о которых говорилось в главе I.

Как было показано на стр. 14, изобретатель шахматной игры потребовал

18 446 744 073 709 551 615

зёрен. Разобьём это число на «архимедовы разряды», т. е. на группы по 8 цифр

1844 6744 0737 0955 1615.

Здесь, очевидно, тысяча восемьсот сорок четыре единицы третьих чисел, шесть тысяч семьсот сорок четыре мириады семьсот тридцать семь единиц вторых чисел, девятьсот пятьдесят пять мириад тысяча шестьсот пятнадцать единиц первых чисел. Это название немногим длиннее нашего (восемнадцать квинтиллионов... и т. д., см. стр. 14).

Для числа 9^{9^9} хватило бы чисел первого периода. Но число $10^{10^{10}}$ будет уже равняться единице чисел пять тысяч мириад первых (5000 0001-х) периода тринадцатого.

Вот какое удобное орудие счёта создал Архимед две тысячи двести лет тому назад!

ГЛАВА IV.

НЕ ДЕСЯТКАМИ, А ПЯТКА́МИ ИЛИ ДЮЖИНАМИ.

При современном состоянии науки нельзя, повидимому, придумать систему счисления, которая была бы удобнее позиционной. Но в основу позиционной системы счисления можно ставить разные числа.

При решении различных задач могут оказаться удобными позиционные системы счисления с различными основаниями. Возможно, что некоторые системы, например двенадцатиричная, и в целом оказались бы несколько лучше десятичной. Но привычка считать десятками так велика, а обязательный переход к новой системе счисления вызвал бы такую ломку всех привычек и такие материальные расходы, что вряд ли подобную реформу можно было бы признать целесообразной.

Есть, впрочем, одна система счисления, настолько своеобразная, её преимущества перед десятичной в одних вопросах и недостатки в других так резко бросаются в глаза, что стоит её рассмотреть подробнее. Это — двоичная система, или система при основании 2. Ей будет посвящена следующая глава. А в этой главе поговорим о позиционных недесятичных системах вообще и научимся переходить от одной из таких систем к другой.

Кроме счёта десятками, в быту довольно широко распространён счёт пятка́ми. В Китае принято считать пятка́ми, причём пятки́ группируются в пары; получается своеобразная система счисления, в которой каждая единица чётного порядка в пять, а нечётного — в два раза больше предыдущей. Орудием счёта служат китайские счёты (рис. 2).

Не задерживаясь далее на этой сложной системе счисления с двойным основанием, отражающей счёт с помощью двух рук, рассмотрим чистую пятиричную систему, т. е. позицион-

ную систему с основанием пять. Эта система использует для записи всех чисел только пять знаков — цифр: знаки для чисел «одно», «два», «три», «четыре» и позиционную пробку — знак для нуля. Для обозначения этих первых четырёх чисел и нуля можно воспользоваться хотя бы нашими цифрами: **1, 2, 3, 4, 0,** но напечатанными жирным шрифтом.

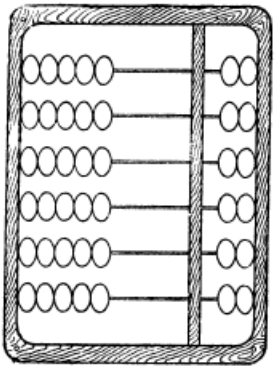


Рис. 2.

Число «пять», являющееся одним «пятко́м», т. е. одной единицей второго разряда, придётся записать так: **10** (как наше «десять»), поставив на месте отсутствующих простых единиц нуль.

Запишем по пятиричной системе число 387 (триста восемьдесят семь; обычный, светлый шрифт указывает на обычную, десятичную запись). Прежде всего выясним, сколько в нашем числе пятёрок (единиц второго разряда) и сколько простых единиц. Чтобы это узнать, поделим 387 на пять. Частное даст число пятёрок, остаток — число простых единиц:

$$\begin{array}{r} 387 : 5 = 77. \\ -\,35 \\ \hline 37 \\ -\,35 \\ \hline 2 \end{array}$$

Итак, в нашем числе 2 простые единицы и 77 единиц второго разряда. Но каждые пять единиц второго разряда составляют единицу третьего разряда; очевидно, в семидесяти семи единицах второго разряда содержится некоторое количество единиц третьего разряда. Чтобы найти его, повторяем операцию деления: делим 77 на 5:

$$\begin{array}{r} 77 : 5 = 15 \\ -\,5 \\ \hline 27 \\ -\,25 \\ \hline 2 \end{array}$$

Остаток (2) даёт число единиц второго разряда, частное же — число единиц третьего. Ищем, сколько в пятнадцати едини-

цах третьего разряда содержится единиц разряда четвёртого:

$$15 : 5 = 3.$$

Пятнадцать единиц третьего разряда состоят целиком из единиц четвёртого разряда. Отсутствие остатка указывает, что «свободных» единиц третьего разряда нет. Что касается трёх единиц четвёртого разряда, то ясно, что в них содержаться единицы высших разрядов не могут. Значит, число 387 состоит из трёх единиц четвёртого разряда, не содержит вовсе единиц третьего разряда, содержит две единицы второго и две единицы первого разрядов, т. е. может быть записано так: **3022**.

Все действия могут быть сгруппированы вместе:

$$\begin{array}{r|l} 387 & 5 \\ \hline -35 & 77 \\ \hline 37 & 5 \\ -35 & 27 \\ \hline \mathbf{2} & 25 \\ & \mathbf{2} \end{array} \qquad \begin{array}{r|l} 5 & \\ \hline -15 & 5 \\ \hline 15 & \mathbf{3} \\ \mathbf{0} & \end{array}$$

Напечатанные жирным шрифтом числа (остатки и последнее частное) нужно ещё переписать в обратном порядке.

Решим теперь обратную задачу. Пусть число дано в пятиричной системе: **2341**. Найти его десятичное выражение.

Подумаем, что́ обозначает каждая из цифр этого числа. Стоящая справа единица обозначает просто 1. Стоящая на втором (справа) месте четвёрка обозначает четыре пятка́, т. е. $4 \cdot 5$; следующая за ней тройка обозначает три «пять раз взятых пятка́», т. е. $3 \cdot 5^2$; наконец, крайняя левая двойка обозначает $2 \cdot 5^3$. Следовательно,

$$\mathbf{2341} = 2 \cdot 5^3 + 3 \cdot 5^2 + 4 \cdot 5 + 1 = 346.$$

Заметим, что и написанное по десятичной системе число, например 3208, может быть дано в аналогичной форме: $3 \cdot 10^3 + 2 \cdot 10^2 + 0 \cdot 10 + 8$. (В 3-м слагаемом этого выражения $(0 \cdot 10)$ множитель «нуль» есть число целое, но не натуральное.)

Вообще, если в основание системы счисления положено число m, то $abcdk$ *) обозначает:

$$a \cdot m^4 + b \cdot m^3 + c \cdot m^2 + d \cdot m + k.$$

*) Здесь, в отличие от принятой в алгебре записи, выражение $abcdk$ обозначает не произведение чисел a, b, c, d и k, а число, записанное в некоторой позиционной системе счисления с помощью цифр a, b, c, d, k.

В нашем быту остались кое-какие пережитки счёта дюжинами. Английский фут, как и русский, делится на 12 дюймов. Ряд товаров упаковывается в тару дюжинами, а для дюжины дюжин в торговле имеется специальное наименование — гросс. Надо сказать, что двенадцатиричная система счисления в некотором отношении лучше десятичной: двенадцать имеет четыре целых делителя (не считая 1 и самого числа 12): 2, 3, 4, 6, тогда как 10 — только два (2 и 5). Поэтому при двенадцатиричной системе было бы больше «круглых» чисел, а это позволило бы установить больше сокращённых приёмов выполнения действий. Но в общем выигрыш был бы невелик.

В двенадцатиричной системе счисления, кроме нуля и цифр от одного до девяти, пришлось бы ввести ещё цифры для обозначения десяти и одиннадцати. Обозначим условно эти цифры значками **X** и Λ. Запишем, например, число 1443 по двенадцатиричной системе:

$$\begin{array}{r|l} 1443 & 12 \\ \hline 12 & \underline{12} \\ \hline 24 & 120 \\ \hline 24 & \underline{120} \\ \hline \mathbf{3} & \mathbf{0} \end{array} \qquad \begin{array}{l} \\ \hline 12 \\ \hline \mathbf{10} \end{array}$$

Последнее частное равно десяти, остатки: нуль и три. Следовательно, $1443 = \mathbf{X03}$.

Во всех рассмотренных задачах указывались системы счисления и требовалось выразить заданные числа. Можно ставить и другие задачи. Например, по данной записи действий над числами установить, в какой системе счисления сделана запись. Вот пример такой задачи: дана запись

$$\begin{array}{r} \times\ \mathbf{121} \\ \mathbf{22} \\ \hline + \mathbf{242} \\ \mathbf{242} \\ \hline \mathbf{3212} \end{array}$$

В какой системе счисления она справедлива?

Внимательно приглядываясь к выполнению действий, мы замечаем, что $\mathbf{2}+\mathbf{4}$ дают какое-то число, оканчивающееся

единицей *). Но «два» и «четыре» дадут «шесть», как бы мы их ни записывали. Значит, знака для числа «шесть» в этой системе счисления нет. Но цифру **4** (четыре) мы в данной записи находим. Следовательно, система счисления может быть либо пятиричной, либо шестиричной. Записав число «шесть» в обеих этих системах, получим **11** (пятиричная) и **10** (шестиричная). Следовательно, в указанном примере, где $2+4$ даёт число, оканчивающееся единицей, система счисления — пятиричная. Вот ещё лёгкий пример: в какой системе счисления $3 \times 3 = 10$? Читатель сообразит, что это возможно только при основании девять.

Не всегда, однако, по виду действия можно однозначно установить, в какой системе счисления справедлива запись. Например, равенство $122 \times 3 = 366$ справедливо в любой системе счисления с основанием, бо́льшим шести.

Но случается и так, что по «жали́ким остаткам» какого-либо действия удаётся не только установить систему счисления, в которой произведена запись, но и восстановить действие. Вот пример: пусть известны лишь некоторые цифры действия (остальные заменены звёздочками):

$$\begin{array}{r} \times\ \ *\ *\ \mathbf{2} \\ \quad\ \ *\ \mathbf{2} \\ \hline \quad *\ \mathbf{0}\ \mathbf{0}\ * \\ +\ \ *\ *\ *\ \mathbf{1} \\ \hline \quad *\ *\ *\ *\ \mathbf{1} \end{array}$$

По какой системе счисления это написано? Как восстановить пропущенные цифры?

Смотрим прежде всего на последние цифры множимого и множителя и на последнюю цифру результата. Мы видим, что число «четыре» (дважды два) в этой системе счисления оканчивается единицей, т. е. для него нет специального знака. Это возможно только при основаниях, не превосходящих четырёх, т. е. при основаниях 2, 3 или 4. При основании «2» число «четыре» (квадрат основания) запишется так: **100**; при основании «3» число «четыре» запишется так: **11** (т. е. $\mathbf{3 \cdot 1 + 1}$). Наконец, при основании «4» число «четыре» (само основание) запишется так: **10**. Значит, искомым основанием

*) Предполагается, что цифры обозначают те же числа, что и в нашей системе счисления, т. е. что **1** есть знак для единицы, **2** — для числа «два» и т. д.

может быть только число «три». «Три» и будет ответом на первый вопрос задачи.

Обозначив далее вторую цифру множимого через x и учитывая единицу в уме, получим, что $2x+1$ даёт число, оканчивающееся нулём; это возможно только при $x=1$ *). Точно так же найдём, что первая цифра множимого равна единице. Значит, множимое равно **112**, т. е. числу «четырнадцать».

Левая цифра множителя при умножении на два даёт число, оканчивающееся единицей. Но $2\cdot 0=0$; $2\cdot 1=2$; $2\cdot 2=11$. Значит, эта цифра может равняться только двум, множитель равен **22** (восемь) и всё действие запишется так:

$$\begin{array}{r} \times\ 112 \\ \hline 22 \\ \hline 1001 \\ +\ 1001 \\ \hline 11011 \end{array}$$

или в нашей системе счисления

$$\begin{array}{r} \times\ 14 \\ \hline 8 \\ \hline 112 \end{array}$$

Для проверки запишем 112 в троичной системе счисления:

$$\begin{array}{r|l} 112 & 3 \\ \hline -\ 9 & 37 \\ \hline 22 & -\ 3 \\ \hline -\ 21 & 7 \\ \hline 1 & -\ 6 \\ \hline & 1 \end{array} \qquad \begin{array}{r|l} 3 & \\ \hline -\ 12 & 3 \\ \hline 12 & -\ 4 \\ \hline 0 & 3 \\ \hline & 1 \end{array} \qquad \begin{array}{r|l} 3 & \\ \hline -\ 3 & 3 \\ \hline 1 & \end{array}$$

Получается как раз **11011**.

Перейдём от примеров к общим выводам. Чем меньше основание системы счисления, тем, очевидно, более громоздкой становится запись чисел и действий над ними. Вот, например, как выглядит умножение двадцати трёх на семнадцать в десятичной и в троичной системах счисления:

$$\begin{array}{r} \times\ 23 \\ \hline 17 \\ \hline 161 \\ +\ 23 \\ \hline 391 \end{array}$$

$$\begin{array}{r} \times\ 212 \\ \hline 122 \\ \hline 1201 \\ +\ 1201 \\ \hline 212 \\ \hline 112111 \end{array}$$

*) x может равняться **0**, или **1**, или **2** (ведь система-то счисления — троичная). Но $2\cdot 0+1=1$; $2\cdot 1+1=10$; $2\cdot 2+1=12$. Значит, x должен равняться **1**.

Запись в троичной системе занимает больше места, чем в десятичной, и является, следовательно, более громоздкой. Что касается самого процесса письменного счёта, то нетрудно видеть, что в троичной системе он гораздо проще, чем в десятичной.

Действительно, чтобы считать «столбиками», как это обычно принято, нам приходится помнить наизусть «таблицу сложения» и «таблицу умножения». «Таблицу сложения» мы осваиваем в течение двух-трёх лет постепенно; с заучиванием таблицы умножения у всякого, вероятно, связаны не очень приятные воспоминания.

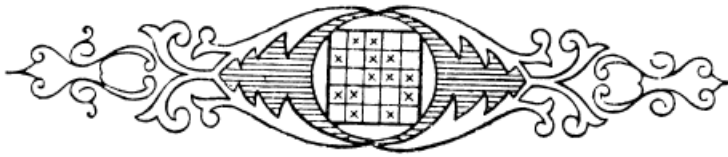
При маленьком основании и таблица сложения и таблица умножения значительно проще, чем у нас. Вот эти таблицы при основании «3»:

$$\begin{array}{lll} 0+0=0; & 1+0=1; & 2+0=2 \\ 0+1=1; & 1+1=2; & 2+1=10 \\ 0+2=2; & 1+2=10; & 2+2=11 \end{array}$$

$$\begin{array}{lll} 0\times 0=0; & 1\times 0=0; & 2\times 0=0 \\ 0\times 1=0; & 1\times 1=1; & 2\times 1=2 \\ 0\times 2=0; & 1\times 2=2; & 2\times 2=11 \end{array}$$

Ясно, что заучить эти таблицы значительно проще, чем наши.

Наименьшее натуральное число, которое может служить основанием системы счисления, есть «два». В этой системе действия должны выполняться особенно просто. В следующей главе мы увидим, что это действительно так. При позиционной нумерации с основанием «два» почти все выкладки выполняются автоматически: получается своеобразная «арифметика, в которой не нужно считать».



ГЛАВА V.

АРИФМЕТИКА, В КОТОРОЙ НЕ НУЖНО СЧИТАТЬ.

Система счисления, в основание которой положено число «два», обладает многими замечательными свойствами. Она заслуживает того, чтобы на ней задержаться. В ней используются только два знака для записи чисел: знак для единицы (1) и позиционная пробка — нуль (0).

В этой главе, как и в предыдущей, числа, изображённые по двоичной системе, будут напечатаны жирным шрифтом, а числа, записанные по десятичной — обыкновенным.

Для единицы мы имеем знак **1**. Число «два», будучи основанием системы счисления, станет единицей второго разряда и запишется так: **10**. Число «три», состоящее из единицы второго разряда (два) и простой единицы, запишется так: **11**. «Четыре» является квадратом двух, т. е. единицей третьего разряда, поэтому оно запишется так: **100**. Что касается числа восемь, равного двум в кубе, то его придётся записать, как нашу тысячу: **1000**.

Мы видим, что наши однозначные числа оказываются в двоичной арифметике трёх- и даже четырёхзначными. В дальнейшем мы увидим, что запись действий тоже занимает значительно больше места, чем наша. Всё это делает двоичную систему практически мало пригодной. Но простота выполнения действий в этой системе поистине изумительна.

Начнём со сложения. Сложим, например, **10110** и **1101** (т. е. 22 и 13).

Напишем эти числа одно под другим, как при обычной записи:

$$\begin{array}{r} \mathbf{10110} \\ +\ \mathbf{1101} \\ \hline \end{array}$$

Если в каком-либо столбике имеется одна единица (вторая цифра — нуль), то пишем её под чертой. Если же имеются две единицы, как в третьем столбике, то зачёркиваем их, внизу ставим нуль, а сверху, над следующим разрядом, приписываем единицу. Далее делаем то же со следующим разрядом, учитывая и надписанные сверху единицы. Всё действие выглядит так:

```
  111
 10110
+ 1101
------
100011
```

По существу делается то же, что и в обычной записи, но считать совершенно не приходится: ставятся только палочки да нулики, и палочки перекрещиваются. Вот более сложный пример (справа он же записан в десятичной системе счисления):

```
  111 11                12
 1111111               ----
 101101                 45
+ 11011               + 27
  10001                 17
 101011                 43
--------              ----
10000100              132
```

Зачеркнув две единицы в крайнем правом столбце, мы ставим сверху над вторым столбцом (над чертой) добавочную единицу; зачеркнув ещё две единицы, ставим ещё добавочную единицу. Больше единиц в правом столбце нет. Поэтому под чертой пишем нуль. То же случится со вторым столбцом справа; при этом нужно учитывать и единицы, стоящие над верхней чертой. В третьем столбце (справа) имеются три единицы; две из них мы зачеркнём, поставив единицу над четвёртым столбцом, а третью снесём под нижнюю черту, и так далее.

Запись, сравнительно с нашей десятичной, очень громоздка. Но выполняется действие автоматически.

Вычитание производится проще всего, если пользоваться «правилом дополнения». Десятичным дополнением данного числа называется разность между ближайшей

бо́льшей степенью десяти («единицей с нулями») и данным числом. Так, например, десятичным дополнением числа 7 будет 3, числа 89 — число 11, для числа 6385 десятичным дополнением будет 3615, для числа 580 — число 420. Чтобы найти дополнение, нужно все цифры данного числа вычесть из девяток, последнюю (не считая нулей на конце) — из десяти. Теперь нетрудно заменить вычитание сложением: вместо того чтобы вычитать какое-либо число из данного, достаточно прибавить к последнему десятичное дополнение вычитаемого и вычесть степень десяти. Например, вычитая 5883 из 11021, расположим действие так:

$$\begin{array}{r} 11021 \\ +\ 4167 \\ \hline 15188 \end{array} \quad 15188 - 10000 = 5188.$$

Подобно десятичному дополнению вводится и двоичное дополнение. Двоичным дополнением данного числа называют разность между ближайшей степенью двух и данным числом. Находить двоичное дополнение числа, записанного по двоичной системе счисления, ещё проще, чем находить дополнение десятичное. Пусть, например, нужно найти двоичное дополнение числа **11 010 111 000**. Последнюю правую единицу и все следующие за ней нули (если они есть) оставляем без изменений, а во всём остальном — заменяем единицы нулями, а нули — единицами. Если в результате получаются нули спереди, то их просто зачёркиваем — вплоть до первой единицы. Так, из числа **11 010 111 000** получается число

00101001000

т. е. **101 001 000**. Это и есть двоичное дополнение числа **11 010 111 000**.

Умея находить двоичные дополнения, мы сумеем автоматически выполнять вычитание. Вычтем, например, **11 011** из **1 110 001**:

1 110 001 — 11 011 = ?

Находим двоичное дополнение вычитаемого. Получим:

00101 = 101

Заменяем теперь вычитание сложением:

$$\begin{array}{r} \overset{1}{1}110001 \\ +\quad 101 \\ \hline 1110110 \end{array} - 100000 = 1010110$$

В десятичной системе запись вычитания этих же чисел будет короче: $113 - 27 = 86$.

При сложении и вычитании чисел, данных в двоичной системе, громоздкая запись совершенно обесценивает ту автоматичность, которой отличается выполнение действий. Но при умножении эта автоматичность бросается в глаза, и громоздкая запись не маскирует необычайной простоты самого действия.

Таблица умножения в двоичной системе счисления имеет следующий вид:

$$0 \times 0 = 0;\ 0 \times 1 = 0;\ 1 \times 0 = 0;\ 1 \times 1 = 1.$$

Запись действия располагаем так же, как и при обычной записи.

Перемножим, например, числа **111 001 101** и **1 101 101**:

$$\begin{array}{r} 111001101 \\ \times\quad 1101101 \\ \hline 1\,1 \\ 111111111 \\ 111111111111 \\ \hline 111001101 \\ 111001101 \\ +\quad 111001101 \\ 111001101 \\ 111001101 \\ \hline 1100010001001001 \end{array} \qquad \begin{array}{r} 461 \\ \times\ 109 \\ \hline 4149 \\ +\ 461 \\ \hline 50249 \end{array}$$

(Под множителем при двоичном умножении мы пишем две черты, чтобы оставить между ними место для единиц, которые получатся в результате сложения и которые при обычном умножении мы держали бы в уме.)

Десятичная запись гораздо короче (она дана рядом с двоичной, справа). Но выполнение десятичного умножения многозначных чисел требует известной квалификации. Нужны годы работы, чтобы научить ребёнка безошибочно выполнять такое умножение. Между тем, двоичное умножение выполняется совершенно автоматически.

Самым трудным из арифметических действий является, несомненно, деление. Всякий помнит, вероятно, каким сложным ему казалось деление в детстве. Да и взрослый человек вряд ли испытает особое удовольствие, деля, например, 8 663 545 198 на 87 995. В средние века деление считалось столь трудной операцией, что людям, искусным в этом действии, давалась учёная степень.

А в двоичной системе счисления и деление выполняется совершенно автоматически! Правда, простота и автоматичность покупаются здесь ценою чрезвычайно громоздкой записи. В качестве примера разделим **11 011 101** на **10 111**. Действие располагаем так же, как при обычном делении, но каждый раз под делимым будем подписывать не произведение делителя на соответствующую цифру частного, а двоичное дополнение этого произведения (при этом нули спереди можно и не зачёркивать):

```
  1 11
  11011101 | 10111
+ 01001    | 1001
  --------
  100100
- 100000 1
  ------
    100101
  +  01001
     ------
    101110
  -  100000
     ------
       1110
```

```
- 221 | 23
  207 | 9
  ----
   14
```

В частном получается **1001** и в остатке **1110**. Справа дано выполнение деления этих же чисел в обычной (десятичной) записи. Сразу видно, что двоичная система практически неприменима потому, что запись очень громоздка. Но что-то считать, что-то пробовать, что-то замечать — здесь совершенно не приходится.

На необычайную простоту и своеобразие двоичной системы счисления первый из европейцев обратил внимание знаменитый философ и математик Г. В. Лейбниц (1646—1716). Но китайцам она, повидимому, была известна значительно раньше.

Двоичная система счисления имеет разнообразные применения в различных отделах математики. Рассказать о них в этой книжке, рассчитанной на читателя без специальной подготовки, очень трудно. Вместо этого мы дадим несколько задач, в которых особенности этой системы выступают очень ярко.

Большинство применений двоичной системы основано на следующем её свойстве: во всех остальных системах счисления нужно указывать, сколько единиц каждого разряда входит в состав данного числа (например, называя или записывая число девятьсот пятьдесят один, мы отмечаем, что оно содержит девять сотен, пять десятков и одну единицу); в двоичной же системе единица любого разряда может либо присутствовать (тогда непременно в единственном числе), либо отсутствовать. Нет надобности говорить, что в двоичном разложении некоторого числа имеется столько-то единиц третьего разряда, столько-то второго, столько-то первого. Достаточно сказать: есть единица третьего разряда, нет — второго есть — первого. Этим число вполне определено: в рассмотренном примере мы имеем число **101** = 5. Чему, например, равно число, в котором есть единица десятого разряда, нет — ни девятого, ни восьмого, ни седьмого, есть — шестого и пятого, нет — четвёртого и всех низших? Ответ получается сразу: это будет число **1 000 110 000**, т. е. 560.

Всё это можно выразить иначе. Рассмотрим ряд чисел, начинающийся с единицы, из которых каждое в два раза больше предыдущего (геометрическую прогрессию):

1,	2,	4,	8,	16,	32,	64,	128,	256,	512, ...
1	2	3	4	5	6	7	8	9	10 ...

Любое число может быть представлено в виде суммы нескольких членов этого ряда. Например, 19 равно сумме первого, второго и пятого чисел ряда (номера членов проставлены под ними); сто равно сумме третьего, шестого и седьмого членов и т. д. Действительно, всякое число можно записать в двоичной системе счисления: тогда единицы укажут на присутствующие, а нули — на отсутствующие члены этой прогрессии (19 = **10011**, 100 = **1 100 100**).

Теперь нетрудно объяснить следующий фокус с угадыванием числа. Вы предлагаете товарищу задумать какое-нибудь число от 1 до 31, затем даёте ему картонную табличку, изображённую на рис. 3, и предлагаете, не показывая вам

№1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
№2	2	3	6	7	10	11	14	15	18	19	22	23	26	27	30	31
№3	4	5	6	7	12	13	14	15	20	21	22	23	28	29	30	31
№4	8	9	10	11	12	13	14	15	24	25	26	27	28	29	30	31
№5	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Рис. 3.

таблицу, сказать, в каких строчках имеется число. Как только он назовёт номера строк, вы сейчас же называете задуманное число.

Составлена эта таблица очень просто. В первой строке помещены все те числа (от 1 до 31), в двоичной записи которых на первом справа месте стоит единица (т. е. все нечётные числа). Во второй строке помещены те числа, в двоичном разложении которых на втором месте справа стоит единица. Число «три», например, которое в двоичной системе счисления записывается так: **11**, помещено и в первую и во вторую строку, так как у него и первая справа и вторая цифра — единицы. Так же построены и остальные строки. В последней, пятой строке помещены все те числа (в пределах от 1 до 31), у которых на пятом месте двоичного разложения стоит единица, т. е. числа от 16 до 31.

Пусть, например, задумано число 29. Загадывающий видит это число в первой, третьей, четвёртой и пятой строках. Назвав вам эти строки, он тем самым невольно указывает, что в двоичное разложение задуманного числа входят единицы первого, третьего, четвёртого и пятого разрядов. Вы знаете, что единицами этих разрядов в двоичной системе счисления служат числа 1, 4, 8 и 16 (они выписаны в первом столбце каждой строки). Теперь легко восстановить почти мгновенно задуманное число: нужно только сложить в уме эти несколько небольших чисел, что и даст 29.

Для выполнения следующего эффектного фокуса нужно научиться быстро запоминать несколько двузначных чисел (т. е. количество цифр, соответствующее двум телефонным номерам; запомнить сразу два телефонных номера нетрудно, тем более, что держать их в памяти придётся всего несколько минут). Фокус состоит в следующем. Вы предлагаете товарищу нарисовать квадратик из 5×5 клеток и расставить в его клетках произвольным образом крестики. Затем в течение полуминуты смотрите внимательно на квадрат и возвращаете его товарищу. Через пять минут вы беретесь нарисовать напамять расположение крестиков, и это вам удаётся сразу. Окружающим кажется, что это очень просто, но предложите любому в течение полуминуты запомнить расположение крестиков в квадрате: можете быть уверены, что никто этого не сможет сделать.

В чём же секрет быстрого запоминания расположения крестиков на квадратной таблице? Легче всего разобрать это на примере. Пусть вам дали следующее расположение крестиков:

	×	×		
×		×	×	
		×	×	×
×	×			×
	×		×	

Считайте, что крестики это — единицы, а пустые клетки — нули. Тогда на каждую строку можно смотреть как на число, записанное по двоичной системе. В нашем примере мы имеем следующие числа:

1100,
10110,
111,
11001,
1010

(нули, стоящие впереди единиц, пропущены). Прочитать эти числа легко, вот они: **1100** = 12,
10110 = 22,
111 = 7,
11001 = 25,
1010 = 10.

При некотором навыке этот перевод из двоичной системы в десятичную выполняется почти мгновенно. Остаётся запомнить серию чисел: 12—22—07—25—10. На перевод из двоичной системы в десятичную и на запоминание этой серии достаточно после небольшой тренировки полуминуты.

Через пять минут, когда расположение крестов у всех исчезло из памяти, вы продолжаете помнить серии чисел: 12—22—07 и 25—10 (как бы два телефонных номера). По этим числам можно сразу восстановить первоначальную таблицу: нужно только написать их одно под другим в двоичной системе счисления и заменить единицы крестиками.

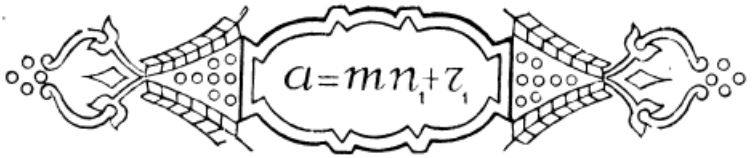
Эта возможность использовать двоичную систему счисления в качестве приёма запоминания квадратных таблиц применяется в шифровальном деле и в конспиративном письме. Как это осуществляется, подробно рассказано в книге Я. И. Перельмана «Живая математика» *).

Читатель обратит внимание на то, что во всех наших рассуждениях есть одна нестрогость. Мы несколько раз употребляли выражение: «всякое число (целое) можно записать в позиционной системе счисления с любым основанием». Верно ли это? Рассуждения, которыми мы пользовались в предыдущей главе, записывая одно и то же число при различных основаниях, показывают, что, повидимому, — верно. Более основательно этот вопрос будет разобран дальше, в конце главы VI (стр. 63); там возможность изображения любого числа в позиционной системе с любым основанием будет строго доказана.

В заключение заметим следующее. Как с помощью десятичной системы счисления можно записывать не только целые числа, но и дробные (десятичные дроби), точно так же можно ввести двоичные, троичные и т. д. дроби. Дроби эти имеют любопытные приложения, но эта книжка посвящена только целому числу и поэтому дробей мы касаться здесь не будем.

---

*) Гостехиздат, М. — Л., 1946 г.



ГЛАВА VI.

ОБЩАЯ МЕРА.

Сложение и умножение — два прямых действия — обладают следующим важным свойством: эти действия всегда выполнимы в целых числах. Точнее говоря, если даны два любых натуральных числа, то всегда можно найти натуральное число, равное их сумме, и натуральное число, равное их произведению. Иначе обстоит дело в случае двух обратных действий: вычитания и деления. Не всегда можно найти натуральное число, равное разности двух данных натуральных чисел (например, не существует натурального числа, равного $5 - 8$ или $6 - 6$). Точно так же, не всегда удаётся найти натуральное число, равное частному двух натуральных чисел (например, не существует натурального числа, равного $5 : 8$). Но между вычитанием и делением есть существенная разница. Узнать, вычитается ли одно натуральное число из другого, очень просто. Существует один единственный универсальный «признак вычитаемости»: если число b больше числа a или равно ему, то из a нельзя вычесть b, т. е. нельзя найти натуральное число, равное $(a - b)$. Наоборот, при делении часто бывает нелегко узнать, делится число a на b или нет (т. е. будет частное $\frac{a}{b}$ натуральным числом или нет).

Но этого мало. Из любого натурального числа, кроме единицы, можно вычитать некоторые другие натуральные числа (именно — все числа, меньшие его). При этом различных возможных вычитаемых у числа N будет всегда ровно $N - 1$ (например, для числа 5 «возможными вычитаемыми» будут числа 1, 2, 3, 4, т. е. всего $N - 1 = 5 - 1 = 4$ числá).

В случае же деления дело обстоит гораздо сложнее. Существует число, имеющее только один делитель, — это единица; существуют числа, имеющие два делителя: единицу и самого себя: таковы числа 2, 3, 5, 7 и другие. Наконец, существуют числа, имеющие больше двух делителей: так, например, число 6 имеет четыре делителя (1, 2, 3 и 6). Числа, имеющие ровно два делителя, обладают многими замечательными свойствами. Их называют простыми или первоначальными числами.

Таким образом, уже самый поверхностный обзор арифметических действий над натуральными числами выдвигает две задачи, которые кажутся очень привлекательными, потому что на вид они очень просты. Первая из них — найти признаки («признаки делимости»), позволяющие узнать, делится ли одно число на другое (так, чтобы в частном получилось натуральное число). Вторая задача — изучить свойства простых чисел. Обе задачи, особенно вторая, значительно труднее, чем это кажется с первого взгляда. При изучении этих задач математики столкнулись с многими новыми вопросами. Некоторые из этих вопросов не решены и по сей день, хотя простыми числами математики занимаются уже больше двух тысяч лет. Признаки делимости и учение о простых числах составляют основной предмет учения о делимости — очень важной главы той теории чисел, о которой говорилось во введении к этой книжке.

Для того чтобы хоть немного познакомиться с некоторыми вопросами теории чисел, нужно вспомнить и продумать ряд основных определений и теорем из школьного курса арифметики.

Если существует натуральное число n, равное частному от деления числа a на b, т. е. такое, которое при умножении на b даёт a, то говорят, что a кратно b или что a делится на b. Число b называют делителем числа a. Так, например, 6 кратно двум; 15 делится на 5 и т. д. Тот факт, что b является делителем a, записывают в виде формулы следующим образом:

$$a = bn, \text{ где } n \text{ — натуральное число.}$$

В учении о делимости приходится постоянно пользоваться тремя теоремами арифметики, которые представляют собою, так сказать, «разменную монету» большинства дальнейших рассуждений. Мы остановимся здесь на них, хотя это, быть

может, и скучно, для того, чтобы в последующих главах они не отвлекали нашего внимания от сути дела. Вот эти теоремы:

Теорема 1. Если a делится на b, а b в свою очередь делится на c, то a делится на c.

Теорема 2. Если алгебраическая сумма (т. е. сумма или разность) нескольких чисел равна нулю или делится на число N, и все слагаемые, кроме одного, о котором ничего не известно, кратны N, то и это слагаемое тоже делится на N.

Теорема 3. Если произведение двух целых чисел a и b делится на число m, не имеющее с a общих делителей (кроме единицы, разумеется), то b делится на m.

Первые две теоремы совершенно ясны. Если 36 делится на 9, а 9 в свою очередь делится на 3, значит, и 36 должно разделиться на 3. Точно так же, если $3 - x - 9 + 81 = 0$, то ясно, что x должен быть кратным трём. Доказывать эти теоремы нужно не для того, чтобы убедить кого-то в их справедливости, а для того, чтобы показать их связь с ещё более простыми предложениями. Читатель докажет их без труда. Что касается третьей теоремы, то она, несмотря на кажущуюся простоту, доказывается более сложно. Мы к ней ещё вернёмся (на стр. 62—63).

Прежде чем итти дальше, задержимся немного на делении с остатком. Если умножение на целое число можно рассматривать как повторное сложение, то деление естественно рассматривать как повторное вычитание. Чтобы разделить, например, 20 на 5, будем вычитать 5 из 20: после первого вычитания получим 15, после второго — 10, после третьего — 5, после четвёртого получим нуль (при рассмотрении вопросов делимости удобно к натуральным числам присоединить число нуль, рассматривая, таким образом, все целые неотрицательные числа). Итак, здесь возможно четыре последовательных вычитания; это и значит, что частным от деления 20 на 5 является число 4; кому приходилось считать на счётах или на арифмометре, тому этот взгляд на деление покажется особенно естественным. Нетрудно сообразить, что количество повторных вычитаний равно числу, которое при умножении на делитель (т. е. на повторное вычитаемое) даёт делимое (исходное число).

Поскольку в этой и ближайших главах наряду с натуральными числами будет рассматриваться число нуль, нужно сказать несколько слов о свойствах этого, в некоторых

отношениях исключительного, числа. Никакое число нельзя делить на 0. Действительно, чему может быть равно $a:0$ при $a \neq 0$? Никакому числу такое частное равняться не может; ведь всякое число, умноженное на нуль, даст 0, а не a. Если же мы нуль попробуем делить на нуль, то в качестве частного сможем взять любое число, ибо любое число при умножении на 0 даёт 0. Ввиду этих обстоятельств в математике делить на нуль «строго воспрещается». Напротив, сам нуль можно делить на какое угодно число (неравное нулю), причём частным всегда будет нуль. Говоря о делении целых, но не обязательно натуральных чисел, мы приходим к выводу, что нуль делится на любое неравное нулю целое число без остатка, потому что $0:a=0$, а нуль считается целым числом. На этом основании принято говорить, что нуль есть кратное любого числа.

Повторное вычитание оказывается применимым и тогда, когда делимое не является кратным делителя*). В этом случае последнее вычитание приведёт не к нулю, а к некоторому числу, меньшему делителя, — к так называемому остатку. Будем, например, делить 17 на 5 способом последовательного вычитания. Вычитаем 5 из 17 первый раз — получаем 12, вычитаем второй раз — получаем 7, вычитаем третий раз — получаем 2. Дальше вычитать невозможно. Значит, частным от деления 17 на 5 будет 3 (число последовательных вычитаний), а в остатке получится число 2.

Последовательное вычитание числа b из числа a, при котором получается частное n и остаток r, можно «перевести на язык формул», записав его так:

$$\underbrace{a-b-b-\ldots-b}_{n \text{ раз}}=r \quad (0<r<b);$$

*) Слово «делитель» имеет в арифметике два значения. Во-первых, делителем называют число, на которое делят другое число. Когда мы пишем $a:b$, то b называем делителем, даже если не знаем, что a должно разделиться на него (т. е. и в том случае, когда $a:b$ не есть целое). С другой стороны, всякое число, кратное которого равно a, мы называем делителем a даже и в том случае, когда непосредственно о делении нет речи. В последнем случае вместо слова «делитель» употребляют иногда слово «множитель». Например, выражения «разложить данное число на простые множители» и «найти все простые делители данного числа» — значит по существу одно и то же. Эта двусмысленность при внимательном отношении к делу никогда не ведёт к путанице.

приведение подобных членов даёт: $a - bn = r$ или $a - r = bn$, что формулируется следующим образом: если из числа a, которое при делении на b даёт остаток r, вычесть этот остаток, то разность $a - r$ будет делиться на b.

Более важно такое расположение членов в нашей формуле:

$$a = bn + r \qquad (0 < r < b).$$

Это — основная формула, определяющая деление с остатком. При этом существенно, что r меньше b. Если r равняется нулю, то деление выполняется нацело. Чтобы не исключать и этого случая, мы в нашу последнюю формулу подставим и знак равенства ($r = 0$), присоединив его к знаку неравенства. Формула будет выглядеть так:

$$a = bn + r \qquad (0 \leqslant r < b).$$

Из хода рассуждений ясно, что числа n и r определяются по числам a и b единственным образом. Иными словами, если даны два числа a и b, причём $a > b$, то единственным образом определяются частное n и остаток r; остаток этот неотрицателен (т. е. положителен или равен нулю) и всегда меньше делителя.

Оставим теперь современные учебники арифметики и посмотрим, как две с лишним тысячи лет назад подходил к вопросу о делимости один из крупнейших греческих математиков — Евклид. В своём сочинении «Начала», состоящем из 13 частей («книг»), он подвёл итог математическим знаниям того времени и систематизировал их. «Начала» Евклида были так хорошо разработаны, что до самого недавнего времени, всего 100 лет назад, в школах Англии геометрию изучали прямо по книге Евклида, как по учебнику. В основном «Начала» были посвящены именно геометрии, но в них рассматривались и арифметические вопросы: пятая книга была посвящена теории пропорций, десятая — классификации иррациональных величин, а седьмая, восьмая и девятая — арифметике целых чисел. В «Началах», между прочим, рассматривается разыскание общей меры двух отрезков и родственное ему разыскание общего наибольшего делителя двух целых чисел. Тот приём нахождения общего наибольшего делителя двух чисел, которым мы пользуемся в настоящее время, так и называется а л г о р и т м о м Е в к л и д а*).

*) Алгоритмом называется правило, которое позволяет автоматически решать какой-нибудь математический вопрос, выполнять определённое вычисление и т. д.

Общею мерой двух отрезков называют такой третий отрезок, который на каждом из данных укладывается целое число раз. Найдём, например, общую меру отрезков AB и CD на рис. 4. Отложим меньший отрезок CD на большем AB

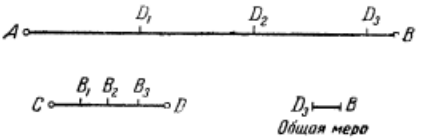


Рис. 4.

от точки A столько раз, сколько окажется возможным. Если CD уложится некоторое число раз без остатка, то он, очевидно, и будет общею мерой. Если же, как на нашем рисунке, останется некоторый остаток D_3B, то придётся искать общую меру меньшего из данных отрезков (CD) и остатка (D_3B), т. е. на CD откладывать от точки C один за другим отрезки, равные D_3B. На рис. 4 отрезок D_3B откладывается на CD ровно четыре раза. Сам отрезок CD укладывается на AB три раза с остатком, равным D_3B. Значит, D_3B укладывается на AB ровно $4 \cdot 3 + 1 = 13$ раз. Итак, D_3B укладывается целое число раз и на AB (13 раз) и на CD (4 раза). Он и есть общая мера этих отрезков.

Не всегда разыскание общей меры проходит так быстро и так гладко. Может случиться, что остаток не уложится целое число раз на меньшем отрезке. Тогда получится некоторый новый отрезок,— второй остаток,— который придётся откладывать вдоль первого остатка. Если какой-нибудь из остатков — пятый, десятый, сотый, тысячный,... уложится целое число раз на предыдущем, то он и будет общею мерой двух исходных отрезков.

Может случиться и хуже. Может оказаться, что такое последовательное откладывание очередного остатка на предыдущем никогда не кончится. Каждый раз будет получаться новый остаток. В этом случае общей меры у данных отрезков найти нельзя; её не существует. Так, например, известно, что сторона квадрата и его диагональ не имеют общей меры.

В арифметике целых чисел тоже можно поставить вопрос об общей мере двух чисел, т. е. о таком числе, которое в каждом из данных «помещается» целое число раз, т. е. на него делятся без остатка оба данных числа. В отличие

от отрезков такая общая мера у целых чисел всегда существует: именно число 1, которое «укладывается» целое число раз в любом целом числе. Но, кроме единицы, пара чисел может иметь и другие «общие меры». Например, 6 и 20 имеют «общею мерой» число 2: оба они делятся на два.

Вообще, любое число, на которое делятся без остатка оба данных числа, служит их общею мерой. Поэтому, естественно, возникает вопрос обо всех общих делителях двух данных чисел и, в частности, об их общем наибольшем делителе.

Общим наибольшим делителем двух данных чисел называется наибольшее число, на которое делятся оба этих числа. Если общий наибольший делитель двух чисел равен единице, то числа эти называются взаимно-простыми. Например, 8 и 9 — числа взаимно-простые. Точно так же взаимно-простыми будут числа 12 и 35. Вот как определяет взаимно-простые числа сам Евклид: «Если из двух неравных целых чисел последовательно меньшее вычитается из большего и остаток до тех пор не измеряет точно предыдущего, пока он не равен единице, то данные числа суть числа между собою взаимно-простые».

Этот отрывок очень содержателен. Он не только даёт определение взаимно-простых чисел, но и показывает, как вычислять общий наибольший делитель. Поэтому, как мы уже говорили, приём вычисления общего наибольшего делителя называется алгоритмом Евклида.

Переведём на современный математический язык и разберём внимательнее эту чрезвычайно сжатую формулировку Евклида.

Пусть даны два натуральных числа a и b, из которых a больше b; требуется найти их общий наибольший делитель. По Евклиду, нужно из большего вычитать меньшее до тех пор, пока не получится остаток; вместо этого мы просто разделим a на b; при этом получится некоторое частное m_1 и некоторый остаток r_1, что мы можем записать так:

$$a = bm_1 + r_1 \qquad (0 \leqslant r_1 < b).$$

Остаток r_1 меньше, чем b. Может случиться, что b точно разделится на этот остаток. Тогда правая часть написанного равенства, как сумма двух чисел, делящихся на r_1, сама будет делиться на r_1, а значит, и равное ей число a тоже разделится на r_1. Остаток r_1 будет общим делителем чисел

a и b. С другой стороны, переписав наше равенство так: $r_1 = a - bm_1$, мы видим, что всякий делитель чисел a и b будет делителем числа r_1; следовательно, этот делитель будет не больше r_1, а это как раз и значит, что r_1 будет общим наибольшим делителем чисел a и b.

Пусть, например, $a = 24$, $b = 16$. Поделив 24 на 16, получим в частном 1 ($m_1 = 1$), а в остатке 8 ($r_1 = 8$). Но 8 есть делитель 16. Значит, 8 и будет общим наибольшим делителем чисел 16 и 24. Действительно, проверим это. Вот все делители чисел 16 и 24:

Делители числа 16	1 2 4 8 16
Делители числа 24	1 2 3 4 8 12 24
Общие делители чисел 16 и 24	1 2 4 8

Наибольшим из общих делителей чисел 16 и 24 является, как мы и нашли, число 8.

Но может случиться, что меньшее из данных чисел b не делится на r_1. Прежде чем разобрать этот случай, обратим внимание на одно важное обстоятельство. Допустим, что a при делении на b даёт остаток r_1. Мы уже видели, что на математическом языке этот факт записывается так:

$$a = bn + r_1 \qquad (0 < r_1 < b).$$

Любой делитель чисел a и b будет делителем r_1, или, иными словами, любой общий делитель пары a и b будет в то же время делителем пары b и r_1; следовательно, общий наибольший делитель чисел a и b будет в то же время общим наибольшим делителем чисел b и r_1. Мы получаем следующую теорему.

Теорема. Общий наибольший делитель двух чисел равен общему наибольшему делителю меньшего числа и остатка, полученного при делении большего из данных чисел на меньшее.

Вооружённые этой теоремой, вернёмся к рассмотрению того случая, когда при делении a на b получается остаток r_1, на который b точно не разделится. Тогда придётся при делении b на r_1 найти второе частное m_2 и второй остаток r_2. Именно это и имеет в виду Евклид, когда говорит о после-

довательном применении повторного вычитания (по-нашему: деления с остатком). Значит, получатся уже два равенства:

$$a = m_1 b + r_1 \qquad (0 < r_1 < b),$$
$$b = m_2 r_1 + r_2 \qquad (0 < r_2 < r_1).$$

При этом новый остаток r_2 будет меньше нового делителя, т. е. первого остатка r_1. Таким образом, получается важный результат: $r_2 < r_1$.

Будем применять этот приём последовательно, как нам советует Евклид. Разделим r_1 на r_2. Получим новое очередное частное m_3 и новый остаток r_3, обязательно меньший, чем r_2:

$$r_3 < r_2.$$

Спрашивается, окончится ли когда-нибудь этот ряд последовательных действий, или же возможно бесконечное повторение их, как это случается иногда при нахождении общей меры двух отрезков? Легко сообразить, что такое бесконечное повторение ряда действий в данном случае невозможно.

В самом деле, мы видели, что первый остаток r_1 меньше числа b. Второй остаток r_2 меньше r_1 и так далее:

$$b > r_1 > r_2 > r_3 > r_4 > \ldots$$

Все эти числа — b, r_1, r_2, r_3, ... — целые и положительные, и каждое из них по крайней мере на единицу меньше предшествующего, так что они все различны. Но различных целых положительных чисел, меньших b, существует не так уже много: всего $b - 1$. Следовательно, рано или поздно наши деления с остатком закончатся, и последнее деление будет уже без остатка.

Обозначим число последовательных делений с остатком буквою n:

1-е деление: $a = bm_1 + r_1 \qquad (0 < r_1 < b)$,
2-е деление: $b = r_1 m_2 + r_2 \qquad (0 < r_2 < r_1)$,
3-е деление: $r_1 = r_2 m_3 + r_3 \qquad (0 < r_3 < r_2)$,
. . . . . .
n-е деление: $r_{n-2} = r_{n-1} m_n + r_n \quad (0 < r_n < r_{n-1})$;

следующее, «эн плюс первое» деление непременно будет выполняться нацело:

$(n+1)$-е деление: $r_{n-1} = r_n m_{n+1}$.

Теперь ко всем полученным равенствам применим только что найденную теорему об общем наибольшем делителе (стр. 58). Из первого равенства мы видим, что общий наибольший делитель чисел a и b равен общему наибольшему делителю чисел b и r_1. Но этот общий наибольший делитель равен, в силу второго равенства, общему наибольшему делителю чисел r_1 и r_2. Итак, общий наибольший делитель чисел a и b равен общему наибольшему делителю чисел r_1 и r_2. Рассмотрев третье равенство, убедимся, что он равен общему наибольшему делителю чисел r_2 и r_3. Дойдя последовательно до n-го равенства, убедимся, что общий наибольший делитель чисел a и b равен общему наибольшему делителю чисел r_{n-1} и r_n. Но r_{n-1}, как мы видели, делится без остатка на r_n. Значит, r_n является общим наибольшим делителем чисел r_{n-1} и r_n, и, следовательно, общим наибольшим делителем чисел a и b. Значит, евклидов алгоритм действительно ведёт к цели.

Как расположить действия при практическом вычислении общего наибольшего делителя, видно из следующего примера. Найдём общий наибольший делитель чисел $a = 729$ и $b = 522$.

Начинаем действие ближе к правому краю листа:

$$
\begin{array}{rl}
a = \ldots\ldots\ldots & \begin{array}{r|l} 729 & 522 \\ \hline 522 & 1 \end{array} \ldots\ldots\ldots = b \\
& \begin{array}{r|l} 522 & \mathbf{207} \\ \hline 414 & 2 \end{array} \ldots\ldots\ldots = r_1 \\
& \begin{array}{r|l} 207 & \mathbf{108} \\ \hline 108 & 1 \end{array} \ldots\ldots\ldots = r_2 \\
& \begin{array}{r|l} 108 & \mathbf{99} \\ \hline 99 & 1 \end{array} \ldots\ldots\ldots = r_3 \\
& \begin{array}{r|l} 99 & \mathbf{9} \\ \hline 99 & 11 \end{array} \ldots\ldots\ldots = r_4
\end{array}
$$

В этом примере выполнять деления приходится $n + 1 = 5$ раз. Четвёртый остаток ($r_4 = 9$) и есть общий наибольший делитель чисел 729 и 522.

При нахождении общего наибольшего делителя двух чисел мы, выполняя последовательное деление, обращаем внимание только на остатки при отдельных операциях деления. Частные нас не интересуют. Поэтому-то остатки в предыдущем примере и напечатаны жирным шрифтом. Но в некоторых вопро-

сах бывают важны последовательные частные; мы эти вопросы рассматривать здесь не будем *).

Вернёмся к столбику равенств, с которыми мы имели дело при разыскании общего наибольшего делителя. Вот этот столбик:

$$\begin{aligned}
a &= bm_1 + r_1;\\
b &= r_1 m_2 + r_2;\\
r_1 &= r_2 m_3 + r_3;\\
&\cdots\cdots\cdots\\
r_{n-3} &= r_{n-2} m_{n-1} + r_{n-1};\\
r_{n-2} &= r_{n-1} m_n + r_n.
\end{aligned}$$

Здесь a и b — два данных числа (a больше чем b), m_1, m_2 и т. д.— последовательные частные, r_1, r_2 и т. д.— последовательные остатки.

Перепишем этот столбик «шиворот-навыворот», т. е. начиная с последнего равенства, причём каждое из равенств напишем в немного изменённой форме, решив его относительно крайнего правого члена. Получим столбик:

$$r_n = r_{n-2} - r_{n-1} m_n; \qquad (1)$$

$$r_{n-1} = r_{n-3} - r_{n-2} m_{n-1}; \qquad (2)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_3 = r_1 - r_2 m_3; \qquad (n-2)$$

$$r_2 = b - r_1 m_2; \qquad (n-1)$$

$$r_1 = a - bm_1 \qquad (n)$$

(все равенства мы перенумеровали). Подставим теперь в равенство (1) выражение для r_{n-1} из равенства (2); мы получим:

$$r_n = r_{n-2} - (r_{n-3} - r_{n-2} m_{n-1})\, m_n$$

или

$$r_n = (1 + m_{n-1} m_n)\, r_{n-2} - m_n r_{n-3}.$$

Последний остаток r_n, являющийся общим наибольшим делителем чисел a и b, выражается через числа r_{n-2} и r_{n-3}, причём коэффициентами при r_{n-2} и r_{n-3} в этом выражении

*) Последовательные частные нужны, например, при разложении данного числа в непрерывную дробь, где тоже применяется алгоритм Евклида.

являются целые числа (положительные или отрицательные). Обозначим эти числа через A_1 и B_1:

$$A_1 = 1 + m_{n-1}m_n;$$
$$B_1 = -m_n.$$

Тогда последнее равенство запишется так:

$$r_n = A_1 r_{n-2} + B_1 r_{n-3}.$$

Перейдём теперь к равенству (3) нашего столбика (оно фактически не написано и заменено точками, но читатель без труда восстановит его). Это равенство выражает r_{n-2} через r_{n-3} и r_{n-4}. Подставляя его в выражение для r_n и делая приведение подобных членов, мы получим:

$$r_n = A_2 r_{n-3} + B_2 r_{n-4},$$

где A_2 и B_2 — опять некоторые целые числа (положительные или отрицательные). Повторяя эту операцию n раз, мы дойдём, наконец, до соотношения

$$r_n = Aa + Bb, \qquad (*)$$

т. е. выразим общий наибольший делитель r_n двух любых целых чисел a и b через эти числа в виде суммы этих чисел, предварительно умноженных на некоторые целые коэффициенты A и B.

Это выражение (*) для общего наибольшего делителя двух целых чисел играет очень важную роль в теории чисел, и мы в этой книжке ещё не один раз с ним встретимся.

Вот первое применение равенства (*).

Рассмотрим два взаимно-простых числа a и m (т. е. таких, что их общий наибольший делитель равен единице). Предположим, что произведение ab данного числа a и некоторого целого числа b делится на m. Что можно сказать о делимости b на m?

Применим только что разобранное свойство общего наибольшего делителя двух чисел, который выражается через эти числа по формуле (*), причём коэффициентами разложения будут целые (положительные или отрицательные) числа. Следовательно, равенство (*) перепишется так:

$$1 = Ac + Bm.$$

(r_n в нашем случае равен единице, потому что a и m — взаимно-простые!)

Умножив обе части последнего равенства на b, получим:

$$b = Aab + Bmb.$$

Оба члена правой части делятся на m: первый — потому что ab делится на m по условию, а второй — содержит множитель m явно. Следовательно, и левая часть, т. е. число b, разделится на m.

Мы получили доказательство теоремы третьей, о которой говорилось в начале этой главы (стр. 53).

С последовательным делением — правда, несколько иного рода — мы уже встречались при переводе числа из одной системы счисления в другую (стр. 37). Там, в отличие от евклидова алгоритма, все делители были одинаковы. Остановимся на этом делении несколько подробнее.

Предположим, что нам дано какое-нибудь число a и основание системы счисления m. Само число a может быть задано в какой-либо иной системе счисления, записано римскими цифрами или дано ещё как-нибудь иначе. Возникает принципиальный вопрос: можно ли число a записать в позиционной системе с основанием m? Как это делать практически, мы знаем; все примеры, с которыми приходилось сталкиваться в главах IV и V, как будто подтверждают такую возможность. Остаётся рассмотреть вопрос с общей, теоретической точки зрения — доказать теорему в общем виде.

Итак, нужно число a записать в системе с основанием m. Делим a на m. В результате, как мы знаем, единственным образом определятся частное n_1 и остаток r_1:

$$a = mn_1 + r_1.$$

Частное n_1 показывает, сколько в числе a содержится групп по m единиц, т. е. единиц второго разряда. Остаток r_1 даёт число свободных единиц первого разряда. Если число n_1 меньше основания системы счисления, то задача решена: наше число состоит из n_1 единиц второго и r_1 единиц первого разряда и запишется так:

$$n_1 r_1 \ ^*).$$

Если же n_1 больше m, то повторяем ту же операцию: делим n_1 на m и получаем в частном какое-то число n_2 и в остатке r_2.

---

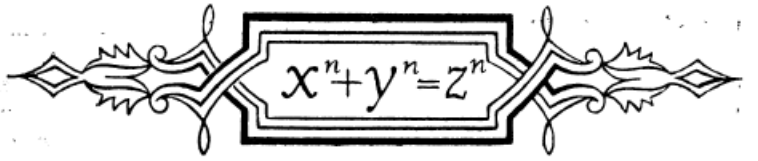
*) Здесь, как и в главе IV (см. стр. 37), $n_1 r_1$ обозначает не произведение чисел n_1 и r_1, а просто две рядом написанные цифры, как, например, цифры 3 и 5 в числе 35.

Частное показывает число единиц третьего разряда, а остаток — число единиц второго. Если n_2 меньше m, то задача решена: искомая запись числа a в системе с основанием m будет выглядеть так:

$$n_2 r_2 r_1$$

(т. е. $n_2 m^2 + r_2 m + r_1$). Если же n_2 больше, чем m, то снова повторяем деление.

Но число a — данное, вполне определённое. Если мы рассмотрим ряд степеней целого числа m, большего единицы, именно: m, m^2, m^3, ..., то в этом ряду обязательно найдётся степень с таким показателем — назовём его q, — что m^q будет больше, чем a. Значит, после q последовательных делений на m наши деления закончатся, и мы получим единственное, вполне определённое представление числа a в позиционной системе с основанием m. Это мы и хотели доказать.



ГЛАВА VII.

УРАВНЕНИЯ, КОТОРЫМИ ЗАНИМАЕТСЯ АРИФМЕТИКА.

Название этой главы может вызвать недоумение: ведь уравнениями занимается алгебра; какие же могут быть уравнения в арифметике? Но, оказывается, есть особый род уравнений, вернее, особая точка зрения на некоторые уравнения, по самой сути дела, по самому духу своему стоящая к арифметике гораздо ближе, чем к алгебре. Что же это за уравнения?

Рассмотрим следующую простую задачу.

В артели было несколько квалифицированных рабочих и несколько чернорабочих. Каждый квалифицированный рабочий получил за проделанную работу 210 р., а каждый чернорабочий — 150 р. Всего артель получила 1740 р. Сколько в артели было квалифицированных рабочих и сколько чернорабочих?

Уравнение этой задачи составляется очень просто: если квалифицированных рабочих было x, а чернорабочих y, то первые получили $210x$, а последние — $150y$ рублей. Сумма этих количеств должна равняться общему заработку артели; это сразу даёт уравнение:

$$210x + 150y = 1740,$$

или, по сокращении на 30,

$$7x + 5y = 58.$$

Но дальше получается неприятность: никаких данных для составления второго уравнения нет. В аналогичных задачах, которыми пестрят задачники Шапошникова и Вальцева и другие, всегда даётся некоторое дополнительное условие:

или общее количество рабочих, или отношение числа квалифицированных к числу неквалифицированных, или что-нибудь ещё в этом роде. Тогда можно составить второе уравнение и без труда решить полученную простую систему. В нашем примере данных для составления второго уравнения нет. Нужно решать единственное уравнение

$$7x + 5y = 58.$$

С точки зрения алгебры вопрос ясен: уравнение имеет бесчисленное множество решений; каждому произвольно взятому числу x соответствует определённое число y, которое вычисляется по формуле

$$y = \frac{58 - 7x}{5}.$$

Но такое решение задачи нас удовлетворить не может. Ведь число рабочих каждой категории должно быть целым положительным (в крайнем случае, одно из неизвестных может равняться нулю — артель может состоять из рабочих одной категории).

Таким образом, из бесконечного множества решений уравнения $7x + 5y = 58$ нас интересуют только такие пары значений x и y, когда оба неизвестных являются натуральными числами (легко видеть, что при $x = 0$ или $y = 0$ второе неизвестное получается дробным, а потому нулевые решения можно не рассматривать). Это позволит выделить некоторое определённое решение и довести задачу до конца.

Будем давать неизвестному x целые значения и вычислять соответствующие значения y. Проб придётся сделать не так уж много, потому что при $x > 8$ второе неизвестное станет отрицательным, а такое решение нас не устраивает. Составляем табличку:

x	0	1	2	3	4	5	6	7	8
$y = \frac{58 - 7x}{5}$	$\frac{58}{5}$	$\frac{51}{5}$	$\frac{44}{5}$	$\frac{37}{5}$	6	$\frac{23}{5}$	$\frac{16}{5}$	$\frac{9}{5}$	$\frac{2}{5}$

Только при $x = 4$ второе неизвестное получает целое положительное значение ($y = 6$). При любом другом значении x число y будет либо дробным, либо отрицательным. Следова-

тельно, задача имеет одно единственное, вполне определённое решение:

квалифицированных рабочих было 4;
чернорабочих » 6.

Дополнительное условие (целочисленность решения) заменило нам второе уравнение.

Разобранная задача привела к одному уравнению с двумя неизвестными. Возможны и такие задачи, в которых одно уравнение связывает больше чем два неизвестных. Некоторые задачи приводят к системам с числом уравнений, меньшим числа неизвестных. Подобные уравнения или системы уравнений называются неопределёнными, потому что, если нет дополнительных условий, они имеют бесконечное множество решений: одному или нескольким неизвестным можно дать любые значения; тогда уже определяются значения остальных. Неопределённые уравнения с их бесконечным числом решений весьма полезны в высшей математике при изучении кривых линий и поверхностей.

Иначе обстоит дело в том случае, когда искомые величины, помимо неопределённого уравнения, должны удовлетворять добавочным условиям. Наиболее важным и изученным является тот случай, когда разыскиваются целые решения. В нашем примере это как раз и было. Чаще, правда, разыскиваются не только натуральные, но все целые решения — как положительные, так и отрицательные. Иногда, напротив, на решения накладываются ещё более жёсткие ограничительные условия.

Такого рода исследование неопределённых уравнений носит название неопределённого анализа. Оно называется также диофантовым анализом по имени замечательного греческого математика — Диофанта, жившего в III в. н. э. в городе Александрии (больше о его жизни ничего не известно). Диофант оставил книгу, на которой воспитывались творцы современной теории чисел. Нужно заметить, что он занимался разысканием не только целых, но и рациональных (т. е. целых и дробных) решений неопределённых уравнений. Решением неопределённых уравнений в целых числах и исследованием полученных решений стали значительно позже заниматься индусы. Впрочем, трудно сказать, когда впервые возник неопределённый анализ; во всяком случае, в XII в. н. э. у индийского математика Бха́скара мы встречаем вполне

разработанную методику целочисленного решения неопределённых уравнений первой степени.

К задачам неопределённого анализа индусов привели вопросы практической жизни. При решении различных задач, связанных с календарём, им часто приходилось разыскивать некоторый промежуток времени, содержащий как целое число лет, так и целое число суток. Это приводило к неопределённым уравнениям, у которых интерес представляли только целые решения.

Разберём несколько задач на неопределённые уравнения, чтобы выяснить основные их особенности; ограничимся при этом уравнениями первой степени, потому что решение неопределённых уравнений высших степеней, хотя бы даже второй, представляет значительные трудности.

Задача первая. Требуется пятирублёвку разменять полтинниками *), двугривенными и пятачками так, чтобы всего было 20 монет.

Составляем уравнение. Пусть x — число пятачков, y — число двугривенных, z — число полтинников. Тогда общая сумма, равная 500 копеек, выразится так: $5x + 20y + 50z$; с другой стороны, по условию, $x + y + z = 20$. Больше никаких данных нет. Следовательно, решение задачи сводится к решению в целых числах системы:

$$5x + 20y + 50z = 500;$$
$$x + y + z = 20.$$

Число неизвестных (три) больше числа уравнений (два); значит, система уравнений — неопределённая. Сократив первое уравнение на 5 и вычтя из него второе, получим единственное уравнение с двумя неизвестными:

$$3y + 9z = 80.$$

Остаётся решить это уравнение в целых числах. Но приглядываясь к нему внимательнее, мы видим, что при любых целых значениях y и z левая часть уравнения должна делиться на 3; правая же часть (80) на 3 не делится. Следовательно, не существует таких целых y и z, которые удовлетворяли бы нашему уравнению. Это — пример неопределённого уравнения, неразрешимого в целых числах. Поэтому неразрешима и при-

*) Полтинник — раньше употреблявшаяся монета в 50 копеек.

ведшая к нему задача. Разменять пятирублёвку двадцатью монетами указанного достоинства невозможно.

Задача вторая. Найти натуральное число, которое при делении на 3 даёт остаток 2, а при делении на 5 — остаток 3.

Обозначим искомое число через x. Если частное от деления x на 3 обозначим через y, а частное от деления на 5 — через z, то получим (см. стр. 53):

$$x = 3y + 2;$$

$$x = 5z + 3.$$

По смыслу задачи x, y и z должны быть целыми (больше того — натуральными) числами. Значит, нужно решить в целых числах неопределённую систему уравнений.

Разыскание самого числа x не вызывает затруднений. При любых целых y и z будет целым и x. Поэтому приходится решить следующее единственное уравнение с двумя неизвестными:

$$5z - 3y + 1 = 0.$$

Найдя все целые положительные значения y или z из этого уравнения, сразу получим и все целые положительные значения x.

Из уравнения $5z - 3y + 1 = 0$ находим:

$$y = \frac{5z + 1}{3}.$$

Одно решение очевидно: при $z = 1$ получим

$$y = \frac{5 \cdot 1 + 1}{3} = 2;$$

и z и y получаются целые. Им соответствует решение $x = 8$.

Найдём все остальные решения. Для этого введём вспомогательное неизвестное u, полагая $z = 1 + u$. Мы получим:

$$5(1 + u) - 3y + 1 = 0,$$

т. е.

$$5u = 3y - 6$$

или

$$5u = 3(y - 2).$$

Правая часть последнего уравнения при любом целом y делится на 3. Значит, и левая должна делиться на 3. Но число 5 — взаимно-простое с числом 3; поэтому u должно разделиться на 3 *), т. е. иметь вид $3n$, где n — целое число. В этом случае y будет равняться

$$\frac{15n}{3}+2=5n+2,$$

т. е. тоже целому числу. Итак, $z=1+u=1+3n$, откуда

$$x=5z+3=8+15n.$$

Получилось не одно, а бесконечное множество значений для x, т. е. решений нашей задачи:

$$x=8+15n,$$

где n — целое число (положительное или нуль):

$$n=0,\ 1,\ 2,\ 3,\ \ldots$$

Проверка показывает, что все эти решения годятся **).

Задача третья. Куплены дыни по 7 р. и арбузы по 4 р. за штуку, всего на сумму 53 р. Сколько куплено дынь и сколько арбузов?

Одно уравнение составляется сразу; вот оно:

$$7x+4y=53$$

(через x обозначено число дынь, а через y — арбузов).

По смыслу задачи ясно, что x и y должны быть одновременно целыми положительными числами. Имеем

$$y=\frac{53-7x}{4}.$$

---

*) Вспомним теорему третью предыдущей главы (стр. 51).

**) Все решения этой задачи образуют неограниченно продолжаемую арифметическую прогрессию с первым членом 8 и разностью 15:

8, 23, 38, 53, 68, 83, ...

Даём x значения от 1 до 7 (при $x > 7$ для y получатся отрицательные значения). Вычисляем соответствующие значения y:

x	1	2	3	4	5	6	7
$y = \frac{53 - 7x}{4}$	$11\frac{1}{2}$	$9\frac{3}{4}$	8	$6\frac{1}{4}$	$4\frac{1}{2}$	$2\frac{3}{4}$	1

Получаются два решения задачи:

$$1) \begin{cases} x = 3; \\ y = 8; \end{cases} \quad \text{и} \quad 2) \begin{cases} x = 7; \\ y = 1. \end{cases}$$

Во всех остальных случаях хотя бы одно из неизвестных дробно или отрицательно. Следовательно, задача имеет два решения: либо куплено 3 дыни и 8 арбузов (это стоит $3 \cdot 7 + 8 \cdot 4 = 53$ р.), либо 7 дынь и 1 арбуз (это стоит $7 \cdot 7 + 1 \cdot 4$, т. е. тоже 53 р.).

Итак, в задачах на неопределённые уравнения мы сталкиваемся с самыми разнообразными случаями: задача может быть совсем неразрешимой, может иметь бесконечное множество решений, может иметь несколько определённых решений; в частности, она может иметь одно единственное решение.

Отметим разницу во взглядах на решение уравнения: с одной стороны — в алгебре, с другой — в неопределённом анализе. В алгебре господствует стремление охватить уравнение возможно шире, найти все мыслимые его решения. Для того чтобы сделать алгебраические уравнения разрешимыми во всех случаях, приходится вводить новые виды чисел: иррациональные, комплексные. В неопределённом же анализе рассматриваются только целые числа. Правда, от отрицательных чисел в неопределённом анализе отказаться нельзя, — без них пришлось бы рассматривать слишком много частных случаев, а употребление отрицательных чисел позволяет получить очень удобные общие формулы. Но так как в неопределённом анализе рассматриваются только целочисленные решения, то для их нахождения можно использовать

свойства целых чисел: делимость, кратность, разложение на простые множители, нахождение общего наибольшего делителя и так далее. Это — понятия, относящиеся не к алгебре, а к арифметике. Поэтому неопределённый анализ рассматривается обычно не как раздел алгебры, а именно как раздел арифметики. Таким образом, оправдано название настоящей главы этой книги.

Перейдём к более внимательному разбору неопределённого уравнения первой степени с двумя неизвестными. После обычной «обработки», которой принято подвергать уравнение (освобождение от знаменателей, приведение подобных членов и т. д.), такое уравнение может быть записано в виде

$$ax + by = c. \qquad (*)$$

Здесь a, b, c — данные целые (положительные или отрицательные) числа; x и y — неизвестные, но принимающие только целые значения (тоже — положительные, отрицательные или нуль).

Рассмотрим прежде всего случай, когда неопределённое уравнение неразрешимо (как в разобранной выше задаче первой на стр. 68).

Найдём общий наибольший делитель чисел a и b. Обозначим его через d (если a и b — взаимно-простые числа, то d равно 1). Тогда a будет равно произведению d на некоторое целое число m, а b — произведению того же d на целое число n:

$$a = md; \qquad b = nd.$$

При этом m и n обязательно будут числами взаимно-простыми. В самом деле, если бы они в свою очередь имели общий делитель k, не равный единице, то произведение kd было бы делителем и числа a и числа b, а потому d не было бы наибольшим делителем этих двух чисел.

Каковы бы ни были целые числа x и y, левая часть уравнения (*) должна делиться на d, потому что оба слагаемых ax и by на него делятся. Значит, и правая часть этого уравнения должна делиться на d. Отсюда можно сделать такой вывод: если свободный член неопределённого уравнения не делится на общий наибольший делитель коэффициентов при неизвестных, то уравнение (*) неразрешимо. В задаче первой на стр. 66 мы пришли к уравнению

$$3y + 9z = 80;$$

здесь общий наибольший делитель коэффициентов равен 3; свободный же член (80) на 3 не делится; следовательно, уравнение неразрешимо. Мы видели, что задача первая действительно не имеет решений.

Если нам даётся неопределённое уравнение (*), то мы прежде всего должны посмотреть, не принадлежит ли оно к случаю, который только что рассмотрен. Если принадлежит, то мы говорим, что это уравнение не может иметь никаких целочисленных решений, и больше нам с этим уравнением делать нечего. Таким образом, мы можем считать достойными изучения только такие уравнения, все члены которых делятся на общий наибольший делитель коэффициентов при неизвестных. Тогда мы можем все члены уравнения сократить на этот делитель. Получится уравнение, у которого коэффициенты при неизвестных — числа взаимно-простые. Поэтому в дальнейших рассуждениях мы будем считать, что в уравнении

$$ax + by = c \qquad (*)$$

числа a и b не только целые, но и взаимно-простые. Уравнения первой степени называют иначе линейными уравнениями *). Уравнения, все члены которых имеют одинаковое измерение, т. е. одинаковую сумму показателей при неизвестных, называют однородными. Например, уравнения $x^2 + 2xy = y^2$ или $x^3 + y^3 = 3xy^2$ будут однородными. Однородные уравнения обладают многими интересными свойствами и решаются они обычно проще неоднородных. В случае линейных уравнений однородным будет уравнение, не содержащее свободного члена, который является членом нулевого измерения. Например, уравнения

$$2x + 3y = 0; \qquad x - 3y = 2z; \qquad x - y = u - v$$

будут однородными; уравнения же

$$2x + 3y = 5; \qquad x - 3y + 1 = 2z; \qquad x - y = u - v + 100$$

— неоднородные.

Рассмотрим в качестве первого примера такие два уравнения:

$$2x + 3y = 5 \quad \text{и} \quad 2x + 3y = 0.$$

---

*) Это название происходит оттого, что в аналитической геометрии (отдел, с которого обычно начинают изучение высшей математики) уравнение $ax + by = c$ изображает прямую линию.

У этих уравнений одинаковые коэффициенты при неизвестных. В этом случае второе уравнение называют однородным уравнением, соответствующим первому (неоднородному) уравнению. Занимаясь линейным неопределённым уравнением $ax + by = c$, естественно сначала рассмотреть однородное уравнение, т. е. положить $c = 0$:

$$ax + by = 0.$$

Удобнее записать это уравнение так:

$$ax = by\ *).$$

Решить его очень просто. Раз правая часть (by) *делится на* b, *значит и левая* (ax) *должна делиться на* b. *Но* a — число взаимно-простое с b; следовательно, x должен быть кратным b (вспомним теорему третью предыдущей главы на стр. 53).

Итак,

$$x = bn.$$

Чтобы найти y, мы подставляем найденное выражение для x в уравнение $ax = by$. Получим:

$$abn = by, \quad \text{откуда} \quad y = an.$$

Здесь n должно быть непременно то же самое, что в выражении для x.

Следовательно, решение нашего однородного уравнения имеет вид:

$$\left.\begin{aligned} x &= bn, \\ y &= an, \end{aligned}\right\} \qquad (**)$$

где n — любое целое число. Обратно, при любом целом n найденные выражения для x и y будут целыми и будут обращать данное уравнение в тождество. Следовательно, формулы $(**)$ полностью решают однородное уравнение.

Те задачи, которые впервые привели индийских астрономов к неопределённым уравнениям (о чём упоминалось на стр. 68, в начале этой главы), приводили как раз к однородным уравнениям.

---

*) Читателю, быть может, не нравится, что вместо $ax = -by$ мы написали $ax = by$. По существу, конечно, сделано следующее. Сначала написано $ax = -by$. Затем положено: $b_1 = -b$, что даёт $ax = b_1 y$. Наконец, b_1, обозначающее совершенно произвольное число, заменено буквою b.

С однородными неопределёнными уравнениями нередко приходится иметь дело и в современной технике. В качестве примера приведём вопрос о числе зубцов у зубчатых колёс. Для плавной работы пары сцепленных зубчатых колёс необходимо, чтобы числа их зубцов были обратно пропорциональны числам оборотов каждого из колёс в единицу времени. Например, если одно из колёс делает 50, а другое — 80 оборотов в минуту, то число x зубцов первого колеса должно относиться к числу y зубцов второго, как 80 к 50; это записывается так:

$$\frac{x}{y}=\frac{80}{50} \quad \text{или} \quad 5x=8y.$$

Получилось однородное уравнение, которое легко решается в целых числах. По формулам (**)

$$x=8n, \quad y=5n,$$

где n — любое целое число.

Переходим теперь к неоднородным неопределённым уравнениям первой степени, т. е. к уравнениям вида

$$ax+by=c.$$

Все решения такого уравнения можно, как мы увидим, записать в виде двух формул, содержащих произвольное целое число n (подобно формулам (**) в случае однородного уравнения). Эти формулы мы будем называть *общим решением* уравнения (*), а каждую пару значений неизвестных, которая получается при некотором выбранном значении n, — *частным решением*. В однородном уравнении $5x=8y$ решение

$$x=8n, \quad y=5n$$

будет общим, а решение

$$x=24; \quad y=15,$$

полученное из предыдущего при $n=3$, — частным.

Предположим, что путём подбора удалось найти одно (частное) решение уравнения $ax+by=c$, т. е. найти два целых числа x_0 и y_0, удовлетворяющих соотношению

$$ax_0+by_0=c.$$

Применим приём, употребительный в алгебре и использованный нами в начале главы при решении числовых задач. Именно, введём новые вспомогательные неизвестные u и v, связанные с нашими прежними неизвестными — иксом и игреком, т. е. положим

$$x = x_0 + u; \qquad y = y_0 + v.$$

Подставляя эти выражения в уравнение $ax + by = c$, мы получим:

$$a(x_0 + u) + b(y_0 + v) = c.$$

Раскроем скобки и перегруппируем иначе члены:

$$ax_0 + by_0 + au + bv = c.$$

Вычитая из этого равенства тождество $ax_0 + by_0 = c$, получим:

$$au + bv = 0 \quad \text{или} \quad au = -bv.$$

Это — однородное уравнение, соответствующее неоднородному уравнению $ax + by = c$. Его решение мы можем написать по формулам (**) сразу; вот оно:

$$\left.\begin{aligned} u &= -bn, \\ v &= an. \end{aligned}\right\} \text{*)}$$

Следовательно,

$$x = x_0 + u = x_0 - bn;$$
$$y = y_0 + v = y_0 + an.$$

Такой вид должно иметь любое решение уравнения $ax + by = c$. С другой стороны, подставив найденные значения x и y в наше уравнение (*), мы убедимся, что при любом n они ему удовлетворяют. В самом деле:

$$a(x_0 - bn) + b(y_0 + an) = ax_0 + by_0,$$

а это число равно c, так как x_0 и y_0 удовлетворяют уравнению (*).

Следовательно, мы нашли общее решение неоднородного уравнения.

---

*) Здесь перед b стоит знак «минус», которого не было в формулах (**), потому что рассматриваемое уравнение имеет вид не $au = bv$, а $au = -bv$; у коэффициента b стоит знак «минус».

Мы получили замечательный результат: общее решение линейного неоднородного уравнения равно сумме его частного решения и общего решения соответствующего однородного уравнения. Этот простой результат является, однако, очень важным. Достаточно сказать, что аналогичные теоремы встречаются в самых различных отделах высшей математики.

Каким же образом найти числа x_0 и y_0, т. е. хотя бы одно решение неопределённого уравнения (*)? Практически, если коэффициенты a, b и c этого уравнения невелики, то лучше всего просто подобрать это решение, давая одному из неизвестных, например x, последовательно значения 0, 1, 2, 3, ..., пока и для второго, y, не получится целое значение; мы так уже поступали при решении задачи третьей (стр. 71). Если же коэффициенты эти велики, то приходится в той или иной форме использовать алгоритм Евклида. Так, по существу, поступали уже индусы, так же поступают и современные математики. Как применить алгоритм Евклида к решению уравнения (*), лучше всего будет видно на числовом примере.

Требуется решить уравнение

$$331x - 169y = 5.$$

Найдём сначала какое-нибудь частное решение этого уравнения.

Постараемся свести данное уравнение к уравнению с меньшими коэффициентами. С этой целью *делим больший коэффициент* (331) *на меньший* (169). Получаем в частном 1 и в остатке 162. Значит,

$$331 = 169 + 162 \quad \text{или} \quad 331x = 169x + 162x.$$

Наше уравнение можно теперь преобразовать так:

$$162x + 169x - 169y = 5 \quad \text{или} \quad 162x + 169(x - y) = 5.$$

Введём вспомогательное неизвестное, — приём, которым мы уже пользовались, — именно, положим

$$x - y = z. \tag{1}$$

Получим уравнение с меньшими коэффициентами:

$$162x + 169z = 5.$$

Заметим, что вспомогательное неизвестное z вошло в равенство (1), связывающее z со старыми неизвестными

x и y, с коэффициентом 1. То же самое можно сказать и о неизвестном y, входившем в исходное уравнение с меньшим по абсолютной величине коэффициентом.

Повторяем с полученным уравнением снова тот же приём: делим его больший коэффициент при неизвестном на меньший; иными словами, *делим меньший коэффициент исходного уравнения* (169) *на первый остаток* (162). Получим в частном 1 и в остатке 7, т. е. $169z = 162z + 7z$. Наше уравнение переписывается так:

$$7z + 162z + 162x = 5 \quad \text{или} \quad 162(x + z) + 7z = 5.$$

Вводим новое вспомогательное неизвестное, полагая

$$x + z = u. \tag{2}$$

[Обратим внимание на то, что в уравнении (2) и u (новое неизвестное) и x (то старое неизвестное, которое в предыдущем уравнении имело меньший коэффициент) имеют коэффициентом единицы!]

Мы получим:

$$162u + 7z = 5.$$

Делим снова больший коэффициент на меньший, т. е. *делим первый остаток исходного уравнения* (162) *на второй его остаток*; в частном получится 23, а в остатке 1. Следовательно, $162u = 7 \cdot 23u + u$, и наше уравнение примет вид

$$u + 7 \cdot 23u + 7z = 5 \quad \text{или} \quad u + 7(23u + z) = 5.$$

Введём последнее вспомогательное неизвестное, положив

$$23u + z = v. \tag{3}$$

(И здесь новое неизвестное v и одно из старых, z, — именно то, которое входило в предыдущее уравнение с меньшим коэффициентом, имеют коэффициент 1. Так будет всегда — читатель без труда докажет сам, почему.)

Наше уравнение примет теперь особенно простой вид

$$u + 7v = 5.$$

Полученное уравнение выгодно отличается от предыдущих тем, что коэффициент при одном из неизвестных равен 1. Это не случайное свойство нашего примера; так должно быть всегда. Действительно, пробежав глазами все строки

нашего рассуждения, которые напечатаны курсивом, читатель убедится, что мы фактически вычисляли общий наибольший делитель двух коэффициентов при неизвестных в исходном уравнении, и цепочка наших действий окончится тогда, когда один из коэффициентов очередного уравнения станет равен этому общему наибольшему делителю. Вспомним теперь, что мы рассматриваем только такие уравнения, коэффициенты которых — взаимно-простые числа *). Следовательно, их общий наибольший делитель равен 1 и последнее в цепи упрощённых уравнений обязательно будет иметь одним из коэффициентов единицу.

Последнее уравнение ($u + 7v = 5$) даёт нам:

$$u = 5 - 7v.$$

При любом целом v будет целым и u. Положив v равным, например, нулю, получим $u = 5$. Теперь остаётся пройтись «снизу вверх» по всем равенствам, отмеченным номерами (3), (2), (1). При этом каждое подлежащее определению неизвестное будет иметь коэффициентом единицу (мы всё время обращали внимание на это обстоятельство!). Поэтому все неизвестные, в том числе и x и y, будут целыми числами. В нашем примере мы получим:

$$\begin{aligned} v &= 0; \\ u &= 5; \\ z = v - 23u &= -115; \\ x = u - z &= 5 - (-115) = 120; \\ y = x - z &= 120 - (-115) = 235. \end{aligned}$$

Итак, частным решением нашего уравнения будет:

$$x_0 = 120, \quad y_0 = 235.$$

Мы уже видели, как найти общее решение этого уравнения. Для этого мы рассматриваем соответствующее однородное уравнение

$$331x - 169y = 0;$$

*) Если они имеют общий делитель, отличный от единицы, то, как мы знаем, либо уравнение неразрешимо, либо его можно на этот делитель сократить.

здесь $a = 331$, $b = 169$. Поэтому [см. формулы (**) на стр. 72] общим решением неоднородного уравнения $331x - 169y = 5$ будет:

$$x = 120 + 169n; \quad y = 235 + 331n.$$

Этот приём решения несколько громоздок, но на нём стоило остановиться по двум причинам: во-первых, он ясно выявляет связь между решением неопределённого уравнения и алгоритмом Евклида; во-вторых, он показывает, что при любых взаимно-простых коэффициентах при неизвестных уравнение имеет решение. Практически такой приём не доводится до конца; получив вспомогательное уравнение со сравнительно небольшими коэффициентами, последнее решают подбором. Самый ход решения можно рационализировать: выкладки при этом упростятся, но существо дела замаскируется *).

Существуют готовые формулы решения неопределённого уравнения первой степени с двумя неизвестными, но их вывод и применение основаны на использовании непрерывных дробей, с которыми читатель, быть может, незнаком. Заметим, что теория непрерывных дробей тоже связана с алгоритмом Евклида, так что и в этом случае без него обойтись нельзя.

Мы уже говорили, что первой книгой о неопределённых уравнениях было сочинение Диофанта (III в. н. э.). Есть основания полагать, что за 500 лет до Диофанта Архимед умел решать такие уравнения. В средние века ими занимались индусы и отчасти арабы. В Европе первым стал изучать целочисленные решения неопределённых уравнений французский математик Баше де-Мезириак, издатель и комментатор сочинений Диофанта (начало XVII в.).

Уже Диофант наряду с линейными уравнениями (уравнениями первой степени) рассматривал квадратные и кубические неопределённые уравнения. Решение их, как правило, сложно. Остановимся на одной задаче, ставшей классической.

Вот эта задача: найти такие прямоугольные треугольники, все три стороны которых выражаются целыми числами.

Теорема Пифагора позволяет сразу составить уравнение для этой задачи. Если длины катетов мы обозначим через x

---

*) Такой упрощённый путь решения неопределённого уравнения дан, например, во II части учебника алгебры Киселёва и в книге Я. Перельмана «Занимательная алгебра».

и y, а длину гипотенузы — через z, то получим:

$$x^2 + y^2 = z^2.$$

Это — неопределённое уравнение (уравнение одно, а неизвестных три). Оно однородное, второй степени. Одно его решение известно всем: катеты — 3 и 4, а гипотенуза — 5 единиц («египетский треугольник»). Но знание частного решения позволяет решить полностью только линейные уравнения. Здесь же для полного решения придётся искать какой-то искусственный приём.

Будем искать три числа x, y, z, удовлетворяющие пифагорову *) уравнению и не имеющие ни одного общего множителя, кроме 1 **). Важно найти именно эти решения, потому что из любого «взаимно-простого» решения x_0, y_0, z_0 сейчас же получается серия составных решений nx_0, ny_0, nz_0, где n — любое целое число. Обратно: если найдём какое-нибудь «составное» решение p, q, r, то, полагая $p = ax_0$, $q = ay_0$, $r = az_0$, где a — общий наибольший делитель чисел p, q и r, подставив ax_0, ay_0, az_0 в уравнение и сократив его на a^2, убедимся, что x_0, y_0, z_0 образуют «взаимно-простое» решение. Таким образом, найдя все «взаимно-простые» решения, мы будем знать и все вообще решения пифагорова уравнения.

Но если x, y и z — взаимно-простые числа, то они не могут быть все три чётными. Два из них тоже не могут быть чётными, потому что тогда одна часть равенства будет делиться на 2, а другая нет. Все три нечётными быть не могут, потому что сумма двух нечётных чисел — чётна. Следовательно, либо нечётны оба катета, либо нечётны один из катетов и гипотенуза.

Покажем, что оба катета не могут выражаться нечётными числами. Действительно, если один из них выражается числом $2q + 1$, а другой — числом $2p + 1$ (где q и p — целые числа), то сумма их квадратов равна

$$(2q+1)^2 + (2p+1)^2 = 4q^2 + 4q + 1 + 4p^2 + 4p + 1 = \\ = 4(q^2 + q + p^2 + p) + 2.$$

*) Пифагор сам не занимался этим уравнением, но оно связано с теоремой Пифагора, и поэтому такое название уравнения оправдано.

**) Такие три числа называются взаимно-простыми. Мы видим, что это название применяется не только к паре чисел, как на стр. 57, но и к тройке, четвёрке и большему количеству целых чисел.

Эта сумма, очевидно, делится на 2 и не делится на 4. Но квадрат любого чётного числа делится на 4, а квадрат любого нечётного не делится на 2. Следовательно, сумма квадратов двух нечётных чисел не может быть ни квадратом чётного, ни квадратом нечётного числа, т. е. вообще не может быть квадратом целого числа.

Итак, если все три стороны прямоугольного треугольника выражаются взаимно-простыми целыми числами, то возможно только такое «распределение чётности»: один из катетов — чётное число, а другой катет и гипотенуза — нечётные.

Будем чётный катет обозначать через x, а нечётный — через y; тогда мы вправе положить $x = 2v$, и наше уравнение запишется так: $4v^2 + y^2 = z^2$, или так: $4v^2 = z^2 - y^2$, или, наконец, так:

$$4v^2 = (z + y)(z - y).$$

Сумма и разность двух нечётных чисел всегда чётны. Положим поэтому

$$z + y = 2u, \quad z - y = 2t.$$

Нетрудно видеть, что u и t — числа взаимно-простые, причём одно из них чётное, а другое нечётное. Действительно, выразив z и y через u и t, получим: $z = u + t$, $y = u - t$. Если бы u и t имели общий делитель, то его имели бы и z и y, что противоречит предположению об их взаимной простоте; точно так же u и t не могут быть одной чётности, потому что тогда z, равный их сумме, был бы чётным, что, как мы видели, невозможно.

Подставляя в уравнение $4v^2 = (z + y)(z - y)$ вместо суммы и разности неизвестных числа $2u$ и $2t$, мы получим:

$$4v^2 = 4ut \text{ или } v^2 = ut.$$

Но это возможно только в том случае, если u и t порознь являются квадратами, т. е. если $u = a^2$; $t = b^2$. Действительно, в произведение ut (равное квадрату числа v) все простые множители входят парами *). Если бы в u имелся какой-нибудь непарный множитель, то такой же множитель должен был бы быть и в t, чтобы в произведение $ut = v^2$ он вошёл парой. А это невозможно, потому что числа u и t

*) Подробно о разложении на простые множители будет рассказано в главе XI (стр. 132).

взаимно-простые и общих множителей не имеют. Итак, в u все простые множители должны входить парами; то же можно сказать и про t. Следовательно, и u и t являются квадратами. Заметим ещё, что в силу взаимной простоты и различной чётности чисел $u(=a^2)$ и $t(=b^2)$ сами числа a и b тоже будут взаимно-простые и различной чётности. Таким образом,

$$z = t + u = b^2 + a^2;$$
$$y = t - u = b^2 - a^2.$$

Получается следующий результат: гипотенуза прямоугольного треугольника с целочисленными взаимно-простыми сторонами обязательно должна быть суммой, а один из катетов — разностью квадратов двух одних и тех же целых чисел, тоже взаимно-простых и притом различной чётности. Но и обратно: сумма и разность квадратов любых целых чисел a и b дают решение пифагорова уравнения, потому что в этом случае второй катет автоматически получается целым числом:

$$x^2 = z^2 - y^2 = (b^2 + a^2)^2 - (b^2 - a^2)^2 =$$
$$= b^4 + 2a^2b^2 + a^4 - b^4 + 2a^2b^2 - a^4 = 4a^2b^2,$$

откуда

$$x = 2ab, \text{ т. е. } x \text{ есть целое число.}$$

Следовательно, наиболее общее «взаимно-простое» решение пифагорова уравнения будет определяться формулами:

$$x = 2ab,$$
$$y = b^2 - a^2,$$
$$z = b^2 + a^2,$$

а все без исключения решения, как простые, так и составные, — формулами:

$$x = 2abn,$$
$$y = (b^2 - a^2)n,$$
$$z = (b^2 + a^2)n.$$

Здесь n — совершенно произвольное натуральное число, а a и b — любые целые числа, выбор которых ограничен лишь следующими условиями: 1) b больше a, 2) b и a — взаимно-простые, 3) b и a — различной чётности.

Мы видим, что «выбор» получился больший, чем в тех случаях, которые мы до сих пор рассматривали. Оно и

понятно. Там одно соотношение связывало два неизвестных, а здесь — три. Связь, ограничение, естественно, стали слабее.

Рассмотрим некоторые числовые решения пифагорова уравнения. Если $n = 1$ (решения «взаимно-простые»), то мы получим следующий ряд решений:

$a = 1$

b	x	y	z
2	4	3	5
4	8	15	17
6	12	35	37
8	16	63	65
10	20	99	101
...	...	...	...

$a = 2$

b	x	y	z
3	12	5	13
5	20	21	29
7	28	45	53
9	36	77	85
11	44	117	125
...	...	...	...

$a = 3$

b	x	y	z
4	24	7	25
8	48	55	73
10	60	91	109
14	84	187	205
16	96	267	285
...	...	...	...

Далее можно написать таблички для $a = 4$, $a = 5$ и т. д. Умножая любую строку (т. е. все числа строки) каждой из табличек на произвольное натуральное число, мы получим новые серии решений. Например, умножая третью строку второй таблички последовательно на 2, 3, 4, ..., получим следующие решения:

n	x	y	z
1	28	45	53
2	56	90	106
3	84	135	159
4	112	180	212
5	140	225	265
...	...	...	...

Никаких иных решений, кроме полученных этим путём из наших табличек, задача иметь не может.

После уравнения $x^2 + y^2 = z^2$ естественно рассмотреть уравнения $x^3 + y^3 = z^3$; $x^4 + y^4 = z^4$ и т. д. Математики XVI и начала XVII в. пытались решить эти уравнения в целых числах, но безуспешно.

П. ФЕРМА

Так обстояло дело до середины XVII в., когда француз Ферма́, рассмотревший это уравнение в общем виде, т. е. в форме

$$x^n + y^n = z^n,$$

где n — любое целое число, пришёл к выводу, что при любом n, большем двух, задача неразрешима в целых числах (при $n = 1$ её решит любой шестиклассник, а решение её при $n = 2$, т. е. решение пифагорова уравнения, мы только что разобрали).

Пьер Ферма́ (1601 — 1665 гг.), крупный юрист, видный общественный деятель своей родины — города Тулузы, — занимался математикой в часы досуга. О жизни его известно мало, книг он не печатал. Оставшиеся после него рукописи были изданы его сыном уже после смерти отца. Ферма́ состоял в переписке почти со всеми выдающимися математиками той эпохи; такой крупный учёный, как Паскаль, считал его лучшим математиком своего времени. Одновременно с Декартом Ферма́ заложил основы аналитической геометрии, вместе с Паскалем — основы теории вероятностей. Но лучшие его открытия принадлежат теории чисел.

На полях книги Диофанта Ферма́ сделал следующую надпись (на латинском языке): «Ни куб на два куба, ни квадрато-квадрат и вообще никакая, кроме квадрата, степень, не может быть разложена на сумму двух таких же; я нашёл удивительное доказательство этому. Однако ширина полей не позволяет здесь его осуществить».

Эту теорему Ферма́ оставил недоказанной. И не только эту: Ферма́ формулировал много интересных теорем, но доказательства их не оставил. Часто он умышленно посылал теоремы своим знакомым без доказательства, тем самым предлагая им трудную задачу для решения. Современники часто с ними не справлялись, но в течение XVIII и XIX вв. все эти теоремы были доказаны. Все, кроме двух! Одна из них — только одна из всего богатого наследия Ферма́ — оказалась неверной *): один раз и этому гению изменило математическое чутьё. А вторую, ту, которая была написана на полях книги Диофанта и о которой мы сейчас говорили, до сих пор не удалось ни доказать, ни опровергнуть.

---

*) О ней будет сказано дальше, см. стр. 124.

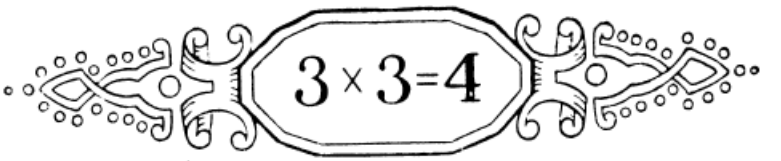
Лучшие математики пробовали на ней свои силы. Эйлер дал доказательства того, что уравнения $x^3+y^3=z^3$ и $x^4+y^4=z^4$ неразрешимы в целых числах, т. е. доказал теорему Ферма́ для $n=3$ и $n=4$ *). Лежандр и Дирихле доказали её для $n=5$, Ламэ́ — для $n=7$. В середине прошлого века Куммеру с помощью трудной и тонкой теории удалось показать, что теорема Ферма́ может быть неверна лишь для некоторых исключительных значений n. Так, например, он доказал, что она верна для всех n, меньших 100 **). Но полного доказательства её справедливости он всё же не дал.

Теорема эта сама по себе не имеет большого принципиального значения. Но она породила огромную литературу, привела к открытию новых теорий и методов решения задач и вообще сыграла такую роль в развитии математики, что ей присвоили наименование Великой теоремы Ферма́.

---

*) Доказательство теоремы для $n=4$ дал, по существу, сам Ферма́.

**) В настоящее время она доказана для всех n, меньших 619 (и для ряда бо́льших значений).



ГЛАВА VIII.

АРИФМЕТИКА, В КОТОРОЙ «ТРИЖДЫ ТРИ — ЧЕТЫРЕ».

Мы уже рассматривали (на стр. 39) арифметику, в которой $3 \times 3 = 10$. Это — система счисления при основании 9. Разумеется, и в этой и во всякой другой системе счисления три раза повторенное число три будет равно девяти; но в девятиричной системе счисления само число девять, будучи единицей второго разряда, выглядит так: **10**. Поэтому и получилась парадоксальная запись.

Теперь мы собираемся говорить не о способе записи. Мы покажем, что существует такая точка зрения, вполне разумная и в некоторых случаях полезная, при которой три, умноженное на три, даёт четыре. Чтобы понять возможность такой точки зрения, вернёмся на время к линейным неопределённым уравнениям, которые рассматривались нами в предыдущей главе.

Рассмотрим уравнение

$$ax + by = c,$$

где a, b, c — целые числа, причём a и b — взаимно-простые. По существу, при решении важно найти только x. Тогда y определится сразу:

$$y = -\frac{ax - c}{b}.$$

При этом x нужно искать с таким расчётом, чтобы выражение, которому равен y, было целым. Но это выражение, наверное, будет целым, если $ax - c$ разделится на b или, иначе, если ax при делении на b даст остаток c. (Действи-

тельно, если ax при делении на b даёт остаток c, то это значит, что $ax = bm + c$; отняв отсюда c, получим bm, очевидно, делящееся на b.)

В этой задаче нахождение y, когда x уже найдено, не представляет никакой трудности, и мы можем y вообще не рассматривать. А задачу — найти x — можно поставить так, что в ней y совсем не будет участвовать. По существу, здесь поставлена следующая задача: найти такое x, чтобы произведение ax при делении на b давало остаток c.

Для начала предположим, что $a = 1$. Это, очевидно, простейший случай, и отправляться нужно именно от него. Тогда наша задача примет вид: найти все числа x, которые при делении на данное число b дают остаток c. Несмотря на кажущуюся простоту, такая постановка вопроса оказалась очень плодотворной. Её развил и превратил в стройную систему Гаусс (1777—1855 гг.), которому удалось сделать на этом пути много важных открытий.

Итак, нас интересуют все числа, дающие при делении на некоторое определённое число данный остаток. Если, например, число, на которое делят [его называют модуль *)], равно 7, а требуемый остаток равен 2, то искомыми числами будут:

2, 9, 16, 23 и т. д.

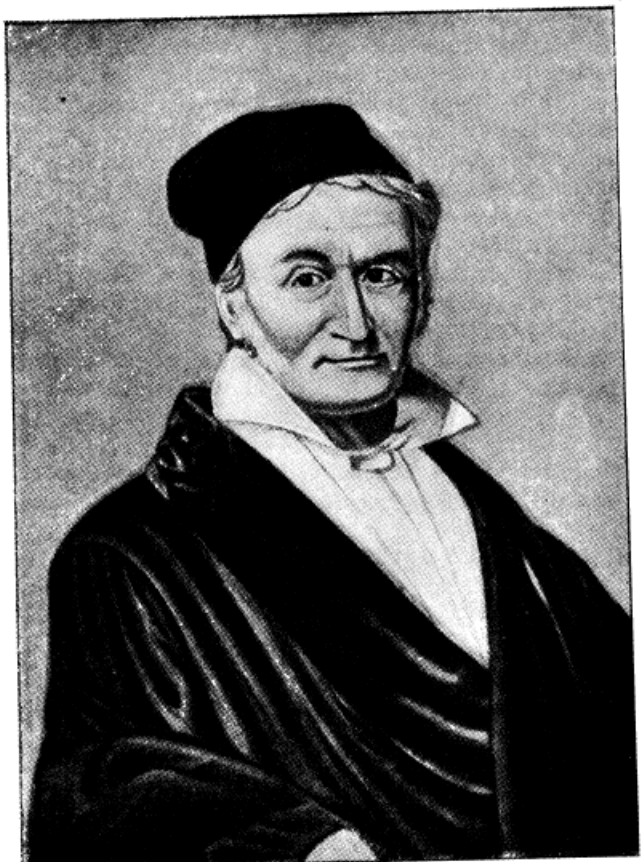
Они образуют неограниченно продолжаемую арифметическую прогрессию, первый член которой равен 2, а разность — 7.

Числа, дающие при делении на модуль равные остатки, называют равноостаточными или сравнимыми по этому модулю. Следовательно, числа 2, 9, 16, 23 и т. д. сравнимы друг с другом по модулю 7. Точно так же числа 1 и 27 сравнимы по модулю 13, число 103 сравнимо с 3 по модулю 10.

Понятие сравнения, введённое Гауссом, нашло такое широкое применение в математике, что для него пришлось ввести специальное обозначение (его придумал тот же Гаусс).

---

*) Слово «мо̀дуль» происходит от латинского modulus (мо́дулюс), что значит «мерка»; употребляется оно обычно в смысле «делитель». Постоянные, которые входят в знаменатель различных физических и технических формул, часто называются модулями: например, модуль упругости и т. д.



К. Ф. ГАУСС

Если a и b при делении на m дают равные остатки, т. е. если a сравнимо с b по модулю m, то пишут

$$a \equiv b \pmod{m};$$

читается это так: «a сравнимо с b по модулю m». Знак сравнения ($\equiv$) напоминает знак равенства. Это не случайно: свойства сравнений похожи на свойства равенств.

Кроме сравнений, содержащих известные, данные числа, например $2 \equiv 5 \pmod 3$, $1000 \equiv 1 \pmod{37}$ и т. д., приходится рассматривать сравнения, содержащие неизвестные. При этом возможны три случая: либо сравнение справедливо при л ю б ы х целых значениях входящих в него букв, либо оно справедливо только при н е к о т о р ы х, либо оно не может быть справедливым н и п р и к а к и х значениях входящих в него букв. Например, сравнение $ax \equiv 2a \pmod a$ справедливо при любых целых x и a (ax и $2a$ оба дают при делении на a остаток, равный нулю; значит, они сравнимы). Напротив, сравнение $2x \equiv 3 \pmod 5$, справедливое при $x = 4$ (ибо $2 \cdot 4 = 8$ даёт при делении на 5 остаток 3), не выполняется при $x = 5$, потому что тогда $2x$ равно 10; это число делится на модуль 5 без остатка. Наконец, сравнение $2x \equiv 1 \pmod 2$ не выполняется ни при каком целом x: левая часть его ($2x$) делится на модуль, а правая — нет.

Решить сравнение, значит — найти все удовлетворяющие ему значения неизвестных (или доказать его невозможность). Сами значения неизвестных, удовлетворяющие сравнению, называются его р е ш е н и я м и.

Сравнения, как и уравнения, могут быть первой, второй и т. д. степени, могут содержать одно, два и т. д. неизвестных. Вот несколько примеров сравнений:

$2x + 3y \equiv 5 \pmod{21}$ (сравнение первой степени с двумя неизвестными),

$x^2 + 5x - 3 \equiv 0 \pmod 3$ (квадратное сравнение с одним неизвестным).

Рассмотрим простейшие свойства сравнений. Возьмём сравнение $a \equiv b \pmod m$ и попробуем «перевести» его на привычный нам язык равенств. Это нетрудно сделать. Ведь сравнение $a \equiv b \pmod m$ обозначает, что $a - b$ делится на m без остатка, т. е. что $a - b$ равно произведению m на произвольное целое число n. Обратно: если $a - b = mn$, где n — целое число, то при делении a на m и b на m получатся

одинаковые остатки. В самом деле, допустим, что при делении на m число a даёт остаток r_1, а число b — остаток r_2. Это значит, что имеют место равенства: $a = pm + r_1$; $b = qm + r_2$, где p, q, r_1 и r_2 — числа целые, а r_1 и r_2, кроме того, оба меньше m. Допустим, что $r_1 > r_2$. Вычитая второе равенство из первого, получим:

$$a - b = (p - q)m + r_1 - r_2,$$

или

$$r_1 - r_2 = (a - b) - (p - q)m = mn - (p - q)m = m(n - p + q).$$

Следовательно, разность $r_1 - r_2$ есть число, кратное m. Эта разность меньше m, потому что и уменьшаемое и вычитаемое — положительные числа, меньшие m; значит, она может быть равна только нулю, и значит, $r_1 = r_2$. Но равноостаточность a и b по модулю m записывается как раз так: $a \equiv b \pmod m$.

Итак, равенство $a - b = mn$ (или $a = b + mn$) и сравнение $a \equiv b \pmod m$ обозначают совершенно одно и то же. Где нужно, можно вместо равенства писать сравнение, где нужно — вместо сравнения равенство. То и другое выражают одну мысль, только, так сказать, на разных языках.

Покажем теперь, что сравнения по одному и тому же модулю можно складывать, вычитать и перемножать (левую часть — с левой, правую — с правой). Рассмотрим два сравнения:

$$a \equiv b \pmod m \quad \text{и} \quad c \equiv d \pmod m.$$

Первое, как мы знаем, равносильно равенству $a = mn_1 + b$, а второе равенству $c = mn_2 + d$; сложив (или вычтя) эти равенства, мы будем иметь: $a \pm c = m(n_1 \pm n_2) + b \pm d$; переведя результат на язык сравнений, мы получим:

$$a \pm c \equiv b \pm d \pmod m.$$

А это как раз и значит, что сравнения можно почленно складывать (и вычитать).

Если равенства $a = mn_1 + b$ и $c = mn_2 + d$ мы перемножим, то получим:

$$ac = m^2 n_1 n_2 + mn_1 d + mn_2 b + bd =$$

$$= m(mn_1 n_2 + n_1 d + n_2 b) + bd.$$

Обозначая выражение в скобках, которое, очевидно, является целым числом, одной буквой n, мы будем иметь:

$$ac = mn + bd.$$

Это значит, что $ac \equiv bd \pmod{m}$, т. е. что сравнения по одному и тому же модулю можно перемножать. Разумеется, складывать и перемножать можно не только два, но и любое число сравнений. Отсюда сейчас же получается следствие: сравнение, не содержащее неизвестных, можно возвести в любую степень *).

Так же просто можно показать, что к обеим частям сравнения можно прибавить, от обеих частей отнять одно и то же число и обе части умножить на одно и то же число *). Например, из $a \equiv b \pmod{m}$ следует $a + c \equiv b + c \pmod{m}$. Действительно, сложим сравнения

$$a \equiv b \pmod{m} \quad \text{и} \quad c \equiv c \pmod{m}$$

(первое дано, а второе — очевидно); получим

$$a + c \equiv b + c \pmod{m},$$

что и требовалось доказать.

Указанные свойства сравнений позволяют производить над ними почти все преобразования, которые мы производим над уравнениями. В частности, можно переносить члены с одной стороны (или, лучше сказать, из одной части) сравнения в другую, изменив, разумеется, знаки на обратные. Это, вместе с приведением подобных членов, позволяет приводить все сравнения к виду:

$$(\text{некоторый многочлен}) \equiv 0 \pmod{m}.$$

Например, сравнение

$$x^2 \equiv 1 - x \pmod{4}$$

приводится к виду

$$x^2 + x - 1 \equiv 0 \pmod{4};$$

сравнение

$$3x - y + 5 \equiv y + 10 \pmod{7}$$

— к сравнению

$$3x - 2y - 5 \equiv 0 \pmod{7}$$

и т. д. В частности, любое сравнение первой степени с одним неизвестным можно привести к виду

$$ax + b \equiv 0 \pmod{m},$$

*) Умножение на выражение, содержащее неизвестное, как и в случае обыкновенных уравнений, может привести к посторонним решениям.

где a, b и m — заданные целые числа (m, кроме того, положительно).

Но в некотором отношении сравнения всё-таки «хуже» равенств. Сокращать их на общий множитель можно не всегда. Рассмотрим этот вопрос внимательнее.

Сравнение $22 \equiv 12 \pmod 5$, несомненно, справедливо: и 22 и 12 при делении на 5 дают остаток 2. Если мы разделим обе его части на 2, то получим $11 \equiv 6 \pmod 5$; это тоже справедливо: и 11 и 6 при делении на 5 дают в остатке 1. Кажется всё благополучно. Вот, однако, другой пример: $14 \equiv 10 \pmod 4$; действительно, и 14 и 10 при делении на 4 дают в остатке 2. Если же мы разделим обе части сравнения на 2, то получим $7 \equiv 5 \pmod 4$, что неверно: ведь 7 при делении на 4 даёт остаток 3, а 5 — единицу. В чём же дело?

В первом примере оба члена сравнения взаимно-просты с модулем. Во втором же оба члена и модуль имеют общий множитель, именно 2. Это и привело во втором примере к неблагополучию *).

Сформулируем наши наблюдения в форме теорем и докажем их.

Теорема первая. Если обе части сравнения взаимно-просты с модулем и имеют общий множитель, то сравнение можно сократить на этот множитель.

Пусть в сравнении

$$ad \equiv bd \pmod m$$

обе части делятся на d, а модуль не только не делится, но и взаимно-прост с d, т. е. не имеет делителей, общих с d и не равных 1. Из данного сравнения следует:

$$ad - bd \equiv 0 \pmod m,$$

т. е. $d(a-b)$ должно делиться на m. Но d, по условию, взаимно-просто с m. Следовательно, $a-b$ должно делиться на m, т. е. должно иметь место сравнение $a \equiv b \pmod m$, что и требовалось доказать. И здесь приходится использовать теорему третью главы VI (на стр. 53).

Теорема вторая. Если обе части сравнения и модуль имеют общий множитель, то справедливо сравнение,

---

*) Вопрос читателю: может ли одна часть сравнения быть взаимно-простой с модулем, а другая — нет?

которое получается путём деления обеих частей данного сравнения и его модуля на этот общий множитель. (Иными словами, в этом случае можно сокращать обе части сравнения, но одновременно и модуль).

Возьмём сравнение

$$ad \equiv bd \pmod{md},$$

в котором обе части и модуль делятся на d. Переводим мысль, выраженную сравнением, на язык равенств:

$$ad = md \cdot n + bd.$$

Сокращение этого равенства на d даёт:

$$a = mn + b;$$

а это, в переводе на язык сравнений, значит:

$$a \equiv b \pmod{m},$$

что и требовалось доказать.

Доказанная только что теорема объясняет, почему второй пример $14 \equiv 10 \pmod 4$ привёл нас при сокращении к абсурду. Обе стороны этого сравнения и его модуль (4) делятся на 2. Значит, нужно было не забыть сократить на 2 и модуль, что дало бы $7 \equiv 5 \pmod 2$, а это, очевидно, справедливо (и 7 и 5 при делении на 2 дают в остатке 1).

Но если, с точки зрения возможности сокращения, сравнения «хуже» равенств, то у них есть и такие свойства, которые позволяют делать преобразования, невыполнимые в случае равенств. Вот важнейшее из этих свойств: к любой части сравнения можно прибавить, от любой части сравнения можно отнять любое число, кратное модулю.

Действительно, прибавим к обеим частям сравнения

$$a \equiv b \pmod{m}$$

(или отнимем от них) очевидное сравнение $cm \equiv 0 \pmod{m}$; мы получим:

$$a \pm cm \equiv b \pmod{m};$$

аналогично можно было бы получить:

$$a \equiv b \pm cm \pmod{m}.$$

Посмотрим, какую пользу можно извлечь из этого свойства.

Возьмём сравнение

$$13x \equiv 16 \pmod 7. \qquad (1)$$

Вычтем из левой части $7x$: это — число, кратное модулю. Мы получим:

$$6x \equiv 16 \pmod 7.$$

Далее, из правой части вычтем число 14, тоже кратное модулю. Получим:

$$6x \equiv 2 \pmod 7.$$

Сократив на 2 (модуль не делится на 2), мы получим совсем простое сравнение:

$$3x \equiv 1 \pmod 7. \qquad (2)$$

Из сравнения (1) мы получили сравнение (2), справедливое при тех же значениях неизвестного x, при которых было справедливо исходное сравнение (1). Такие два сравнения называются эквивалентными, или равносильными. Но сравнение (2) проще сравнения (1) — в этом его преимущество.

Разберём несколько задач, при решении которых станет наглядной полезность сравнений.

Задача первая. Найти остаток от деления числа $1532^5 - 1$ на 9.

Для решения этой задачи не нужно делать утомительное умножение и скучное деление. Рассуждаем так:

1530 делится на 9 (сумма его цифр делится на 9); следовательно, 1532 даёт при делении на 9 остаток 2; это мы можем записать в форме сравнения

$$1532 \equiv 2 \pmod 9.$$

Мы знаем, что сравнения можно почленно перемножать; в частности, обе части сравнения можно возвести в одну и ту же степень. Возведём написанное сравнение в пятую степень; мы получим:

$$1532^5 \equiv 32 \pmod 9.$$

Вычтем из правой части 27 (число, кратное модулю):

$$1532^5 \equiv 5 \pmod 9.$$

Если теперь от обеих частей сравнения отнять по единице, то получится:

$$1532^5 - 1 \equiv 4 \pmod 9;$$

а это значит, что $1532^5 - 1$ даёт при делении на 9 остаток 4. Наша задача решена.

Задача вторая. Найти последние две цифры числа 9^{9^9}.

Рассмотрим сначала, каковы последние две цифры у первых десяти степеней девятки. Найти их просто:

$9^1 = \quad 9$
$9^2 = \quad 81$
$9^3 = \ldots.29$
$9^4 = \ldots.61$
$9^5 = \ldots.49$
$9^6 = \ldots.41$
$9^7 = \ldots.69$
$9^8 = \ldots.21$
$9^9 = \ldots.89$
$9^{10} = \ldots.01$

Указаны только последние цифры произведений. Остальные их цифры нас не интересуют, и тратить время на их вычисление нет надобности.

Последнее число (9^{10}), оканчиваясь на 01, даёт при делении на 100 в остатке единицу, что мы теперь умеем записать так:

$$9^{10} \equiv 1 \pmod{100}.$$

Если мы возведём обе части этого сравнения в произвольную целую степень p, то увидим, что всякая степень числа 9^{10}, т. е. число 9^{10p}, будет сравнима с 1 по модулю 100.

Рассмотрим, далее, произвольную степень девяти 9^N. Обозначим число десятков в N через p, число единиц — через q; иными словами, положим $N = 10p + q$. Мы только что доказали, что

$$9^{10p} \equiv 1 \pmod{100}.$$

Умножив обе части этого сравнения на 9^q, получим слева:

$$9^{10p} \cdot 9^q = 9^{10p+q} = 9^N,$$

а справа 9^q, т. е.

$$9^N \equiv 9^q \pmod{100}.$$

Последнее равенство показывает, что любая степень девяти (N) сравнима по модулю 100 с такой степенью девяти, показатель которой (q) равен остатку от деления первоначально данного показателя на 10, т. е. обе эти степени девяти

имеют те же две последние цифры *). Таким образом, наша задача упрощается. Последние две цифры числа 9^{9^9} обязательно должны быть те же, что и у числа 9^a, где a — остаток от деления «двухэтажного» показателя 9^9 на 10. Но остаток от деления любого числа на 10 равен последней цифре десятичной записи этого числа. Для числа 9^9 он равен 9 (см. табличку степеней девятки, данную выше).

Следовательно,

$$9^{9^9} \equiv 9^9 \pmod{100},$$

т. е. 9^{9^9} и 9^9 имеют те же последние две цифры. Смотрим снова в табличку первых десяти степеней девятки: видим, что 9^9 оканчивается на 89. Значит, и 9^{9^9} оканчивается на 89.

После вопроса о преобразованиях сравнений и действиях над ними было бы естественно заняться решением сравнений первой степени с одним неизвестным. Но мы этого делать не будем. Заметим только, что решение любого сравнения может быть сведено к решению неопределённого уравнения. Возьмём, например, сравнение

$$7x \equiv 3 \pmod{9}.$$

Это сравнение показывает, что разность $7x - 3$ делится на 9, т. е. равна произведению 9 на некоторое целое число y:

$$7x - 3 = 9y \text{ или } 7x - 9y = 3.$$

Получилось неопределённое уравнение, которое мы умеем решать в целых числах (см. предыдущую главу).

Взглянем теперь на сравнения с совершенно новой точки зрения. Зададим какой-нибудь определённый модуль, например $m = 5$. При делении любого числа на 5 могут получиться следующие остатки: 0, 1, 2, 3 и 4. Все натуральные числа можно разбить на пять категорий, в зависимости от того, какой остаток получается при делении этих чисел на 5. Числа каждой категории образуют неограниченно продолжаемую арифметическую прогрессию с разностью, равной мо-

*) Если два числа сравнимы, т. е. равноостаточны по модулю 100, то это значит, очевидно, что у одного из них в десятичной записи те же последние две цифры, что и у другого.

дулю, т. е. в нашем примере — пяти. Вот эти пять прогрессий:

$$\begin{aligned}
&\div 1,\ 6,\ 11,\ 16,\ 21,\ 26,\ 31,\ \ldots\\
&\div 2,\ 7,\ 12,\ 17,\ 22,\ 27,\ 32,\ \ldots\\
&\div 3,\ 8,\ 13,\ 18,\ 23,\ 28,\ 33,\ \ldots\\
&\div 4,\ 9,\ 14,\ 19,\ 24,\ 29,\ 34,\ \ldots\\
&\div 5,\ 10,\ 15,\ 20,\ 25,\ 30,\ 35,\ \ldots
\end{aligned}$$

Ясно, что каждое число непременно войдёт в одну, и только в одну, из этих прогрессий. Такие прогрессии называют классами по модулю пять. Аналогичным путём все натуральные числа можно разбить на классы и по любому другому модулю.

Все числа, входящие в состав написанных выше прогрессий (т. е. все без исключения числа натурального ряда), называются вычетами*) по модулю 5; каждый из них может служить свободным членом сравнения $x \equiv a \pmod 5$, имеющего решения.

Если бы мы взяли сравнение второй степени, например,

$$x^2 \equiv a \pmod 3,$$

то убедились бы, что некоторые числа, например $a = 1$, являются вычетами, потому что сравнение $x^2 \equiv 1 \pmod 3$ имеет решения; другие числа, например 2, не являются вычетами: можно доказать, что сравнение $x^2 \equiv 2 \pmod 3$ совсем не имеет решений. Говорят, что 2 есть квадратичный невычет по модулю 3. Для сравнений первой степени каждое натуральное число есть вычет.

Возьмём из каждого класса, т. е. из каждой прогрессии, написанной выше, по одному числу; например, возьмём следующие числа:

из первой прогрессии	. . . . .	6,
» второй »	. . . . .	2,
» третьей »	. . . . .	28,
» четвёртой »	. . . . .	14,
» пятой »	. . . . .	10.

Взятые таким образом числа называются представителями классов по модулю пять, а их совокупность — полной системой вычетов по модулю 5.

*) Слово «вычет» должно напоминать о том, что при изучении целых чисел мы смотрим на деление, как на повторное вычитание.

Полная система вычетов по данному модулю обладает многими замечательными свойствами. Мы рассмотрим одно из них; чтобы оно стало нагляднее, сделаем ещё упрощение. Именно, вместо взятых наудачу представителей классов, возьмём в качестве таковых наименьшие положительные вычеты, соответствующие различным классам. В нашем примере это будут числа: 1, 2, 3, 4, 5. Заменим последний вычет, равный модулю, сравнимым с ним по этому модулю числом 0. Получим следующую систему чисел:

$$1,\ 2,\ 3,\ 4,\ 0.$$

Будем над числами такой системы производить сложение, вычитание и умножение по обычным правилам, но каждый полученный результат заменять наименьшим положительным вычетом того же класса. Сложив, например, 3 и 4, мы получим 7; наименьший вычет класса, представителем которого служит 7, равен 2. Поэтому напишем: $3 + 4 = 2$. Чтобы эта запись не слишком резала глаза, будем указывать модуль, по которому все числа были разбиты на классы. Будем писать: $3 + 4 = 2 \pmod 5$. Точно так же, помножив 2 на 3, получим 6; число 6 принадлежит первому классу по модулю 5; оно по этому модулю сравнимо с единицей. Поэтому будем писать: $2 \times 3 = 1 \pmod 5$. Чтобы вычесть четыре из трёх, заменим тройку ближайшим бо́льшим представителем того же класса — восьмёркой. Получим $8 - 4 = 4$, или, по модулю 3,

$$3 - 4 = 4;$$

проверяем: если $3 - 4 = 4$, то $4 + 4$ (сумма разности и вычитаемого) должна равняться 3; и в самом деле, $4 + 4$ равно 8, т. е. числу, сравнимому с 3 по модулю 5.

Ясно, что при таком соглашении, в результате действий над числами системы наименьших неотрицательных вычетов по некоторому модулю, мы всегда будем получать числа той же системы. Важнее другое: все свойства действий (сложения, вычитания и умножения) полностью сохраняются. Сохраняются переместительный и сочетательный законы сложения и умножения, распределительный закон умножения относительно сложения, сохраняются все правила действий со скобками. Более того, оказывается, что каждое уравнение первой степени с одним неизвестным имеет решение, принадлежащее той же системе вычетов. Получается своеобразная арифметика, очень похожая на обычную, но, во-первых, без

действия деления, а, во-вторых, и это главное, не с бесконечным множеством чисел, а только с . . . пятью!

Можно сделать своеобразные «счёты», наглядно иллюстрирующие эту арифметику. Вырежем из картона два кружка, один побольше, другой поменьше. На каждом из них в вершинах правильного вписанного пятиугольника напишем цифры 1, 2, 3, 4, 0, наложим меньший кружок на больший так, чтобы центры их совпали, и скрепим кружки кнопкой (рис. 5).

Рис. 5.

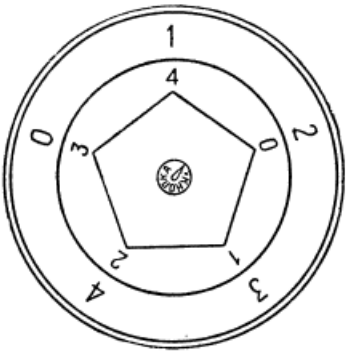


Рис. 6.

Теперь для сложения двух чисел поступаем так: замечаем на большем кружке слагаемое и ставим против него нуль меньшего кружка. На меньшем кружке мысленно отмечаем второе слагаемое. Против него на большем кружке и будет сумма. Сложим, например, 2 и 4. Против двойки большего кружка ставим нуль малого (рис. 6). Четвёрке малого кружка соответствует единица большего. Значит, по модулю пять, $2 + 4 = 1$.

Чтобы умножить 4 на 3, поступаем так. Сначала поставим оба кружка в исходное положение (т. е. чтобы одинаковые числа стояли друг против друга). Затем поворачиваем 3 раза (т. е. число раз, равное множителю) меньший кружок на угол, равный $\frac{4}{5}$ окружности (здесь числитель равен множимому, а знаменатель — модулю), и смотрим, против какого числа большего кружка станет нуль меньшего (рис. 7). Видим, что он придётся против двойки. Значит, в этой арифметике $4 \times 3 = 2$.

Пользуясь этими «счётами» (или обычными сложением и умножением с последующей заменой результатов наименьшими

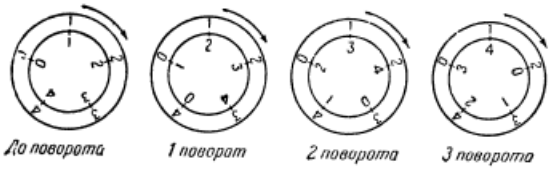


Рис. 7.

соответствующими им вычетами по модулю 5), получим такие таблицы сложения и умножения (по модулю 5):

Таблица сложения

$0+0=0$	$1+0=1$	$2+0=2$	$3+0=3$	$4+0=4$
$0+1=1$	$1+1=2$	$2+1=3$	$3+1=4$	$4+1=0$
$0+2=2$	$1+2=3$	$2+2=4$	$3+2=0$	$4+2=1$
$0+3=3$	$1+3=4$	$2+3=0$	$3+3=1$	$4+3=2$
$0+4=4$	$1+4=0$	$2+4=1$	$3+4=2$	$4+4=3$

Таблица умножения

$0\times0=0$	$1\times0=0$	$2\times0=0$	$3\times0=0$	$4\times0=0$
$0\times1=0$	$1\times1=1$	$2\times1=2$	$3\times1=3$	$4\times1=4$
$0\times2=0$	$1\times2=2$	$2\times2=4$	$3\times2=1$	$4\times2=3$
$0\times3=0$	$1\times3=3$	$2\times3=1$	$3\times3=4$	$4\times3=2$
$0\times4=0$	$1\times4=4$	$2\times4=3$	$3\times4=2$	$4\times4=1$

Из этой таблицы умножения мы видим, что $3\times3=4$; мы нашли ту арифметику, которая была обещана в начале главы.

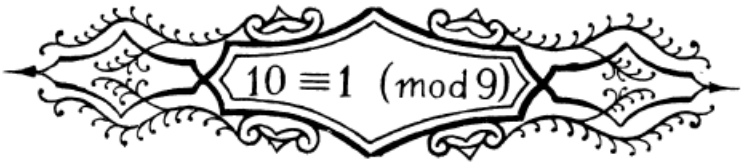
В наших примерах мы имели дело с системами чисел, в которых установлены только три действия: сложение, вычитание и умножение. Такие числовые системы называются в математике «кольцами». Совокупность всех целых чисел (положительных и отрицательных, включая нуль) тоже образует кольцо, но это кольцо содержит бесконечное множество элементов. Кольцом же является совокупность всех многочленов всевозможных степеней относительно единственной буквы x с целыми коэффициентами: сумма, разность и произведение многочленов подобного рода являются в свою очередь такими многочленами; деление же, напротив, приводит сплошь да рядом к алгебраическим дробям. Совокупность натуральных чисел не является кольцом, потому что

разность двух натуральных чисел может и не быть натуральным числом: например, 5—8 = —3, а «минус три» — число хотя и целое, но не натуральное.

Кроме числовых систем с тремя действиями, можно рассматривать системы, в которых выполняются все четыре действия, причём результатом всегда будет число той же системы. К таким системам относится совокупность всех рациональных (т. е. и целых и дробных) чисел: их сумма, разность, произведение и частное оказываются тоже рациональными числами. Подобные числовые системы называются полями, или телами. Говорят, что все рациональные числа образуют поле (тело). Все действительные числа, т. е. рациональные и иррациональные вместе, также образуют поле; поле образует и совокупность комплексных чисел. При изучении полей, как и в обычной арифметике, «строго воспрещается» делить на нуль.

Кроме колец и тел, рассматривают иногда числовые системы, в которых осуществимы только два действия: сложение и вычитание. Умножение и деление могут дать числа, не принадлежащие к изучаемой системе. Такие системы называют группами.

Говоря о кольцах, мы упомянули вскользь о «кольце многочленов». Это выражение кажется бессмысленным, потому что мы сказали сейчас, что кольцом называют некоторую совокупность чисел, а многочлены числами не являются. Но дело в том, что к группам, кольцам и телам можно подойти шире, рассматривая не только системы чисел, но и системы любых вещей, знаков, величин, над которыми производятся какие-то действия. Изучением групп, колец и тел различной природы, т. е. систем с двумя, тремя или четырьмя действиями, независимо от вещей, из которых они построены, занимается высшая алгебра. Арифметика, напротив, в первую очередь интересуется свойствами самих чисел. Эта её черта особенно ярко проявляется в учении о простых числах, которыми мы займёмся в следующих главах.



ГЛАВА IX.

РАЗДЕЛИТСЯ ИЛИ НЕТ?

От тел и колец, т. е. от вопросов, принадлежащих скорее алгебре, вернёмся снова к арифметике: займёмся признаками делимости. Признаки делимости на 2, 3, 4, 5, 6, 8, 9, 10, 25 всем известны. Заметим только, что в различных системах счисления признаки делимости выглядят по-разному. Вот, например, признак делимости на два: «на два делятся все числа, последняя цифра которых чётна». Предположим, что мы пользуемся троичной системой счисления; в ней число «десять» записывается так: **101**, т. е. оканчивается нечётной цифрой — единицей; тем не менее и в троичной, и в любой другой системе счисления число «десять» будет делиться на 2, потому что делимость на два есть внутреннее свойство числа десять, совершенно не зависящее от того, как это число записывать. Следовательно, признак делимости, имеющий место в десятичной системе, в другой системе счисления может оказаться неверным. Есть, разумеется, и такие предложения о делимости, которые справедливы в любой системе счисления, хотя бы, например, такая теорема: «Разность между кубом любого нечётного числа и самим числом делится на шесть»; ими мы займёмся в следующей главе.

Остановимся сначала на хорошо знакомых вещах: рассмотрим признак делимости на 9. Он поможет нам лучше понять те методы, которыми пользуются при выводе всевозможных иных признаков делимости.

Признак делимости на 9 основывается на том, что всякое число, имеющее в нашей системе счисления вид единицы

с нулями (всякая степень десяти), даёт при делении на 9 остаток 1. Действительно,

$$\underbrace{100\ldots00}_{n\text{ нулей}} = 10^n = \underbrace{99\ldots9}_{n\text{ девяток}} + 1.$$

Первое слагаемое, составленное сплошь из девяток, очевидно, делится на 9. Поэтому в остатке от деления 10^n на 9 будет обязательно единица.

Рассмотрим, далее, какое-нибудь произвольное число, например, 4351. Каждая тысяча даёт при делении на 9 остаток единицу. Значит, четыре тысячи дадут остаток 4. Точно так же три сотни при делении на 9 дадут остаток 3, пять десятков — 5, да ещё останется 1 (число единиц в данном числе). Следовательно,

$$4351 = (\text{число, делящееся на } 9) + 4 + 3 + 5 + 1.$$

Если бы «хвост» $4+3+5+1$, представляющий собой «сумму цифр» данного числа, делился на 9, то и всё число разделилось бы на 9. Отсюда вывод: если «сумма цифр» данного числа делится на 9, то и само число разделится.

Слова «сумма цифр» мы взяли в кавычки, потому что, строго говоря, складывать цифры нельзя: ведь цифра — это значок, с помощью которого записывается число. Складываются, разумеется, числа, изображаемые отдельными цифрами данного многозначного числа; но для краткости условились говорить «сумма цифр».

Повторим то же рассуждение, пользуясь понятием сравнения. 10 при делении на 9 даёт в остатке 1, т. е. 10 и 1 сравнимы по модулю 9:

$$10 \equiv 1 \pmod 9.$$

Возводим обе части сравнения в произвольную степень m; получим:

$$10^m \equiv 1^m \pmod 9.$$

Умножив обе части этого сравнения на любое число N, получим:

$$N \cdot 10^m \equiv N \pmod 9.$$

Полученный результат можно сформулировать так: произведение любого числа N на степень десяти даёт при делении на 9 тот же остаток, что и само число N.

Рассмотрим теперь число, составленное из цифр a, b, ..., k, l, т. е. число

$$ab \ldots kl.$$

Это — не произведение чисел a, b и т. д., а число, содержащее l единиц, k десятков и т. д. Его можно записать и так:

$$a \cdot 10^n + b \cdot 10^{n-1} + \ldots + k \cdot 10 + l.$$

Напишем столбиком ряд сравнений, справедливых на основании только что сказанного:

$$\left.\begin{array}{ll} a \cdot 10^n & \equiv a \\ b \cdot 10^{n-1} & \equiv b \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \\ k \cdot 10 & \equiv k \\ l & \equiv l \end{array}\right\} \pmod 9.$$

Сложим почленно эти сравнения. Слева мы получим

$$a \cdot 10^n + b \cdot 10^{n-1} + \ldots + k \cdot 10 + l,$$

т. е. данное нам число, а справа — сумму его цифр. Следовательно, любое число и сумма его цифр сравнимы по модулю 9, т. е. либо одновременно делятся на 9, либо нет.

Признак делимости на 9 используется в следующем поучительном фокусе. Предложите товарищу написать незаметно для вас любое трёх- или четырёхзначное число, состоящее из различных цифр. Пусть он переставит цифры в каком хочет ином порядке; тогда он получит новое число. Меньшее из этих двух чисел пусть он вычтет из большего. Теперь предложите ему зачеркнуть одну цифру полученной разности и назвать вам сумму незачёркнутых цифр. Вы сейчас же сможете назвать зачёркнутую цифру.

В самом деле: и первоначальное, и «перевёрнутое» числа имеют одну и ту же сумму цифр; иными словами, они при делении на 9 дают одинаковые остатки, и, следовательно, их разность делится на 9. Но если эта разность делится на 9, то значит, на 9 в свою очередь делится её сумма цифр. Вам сказана сумма всех цифр, за исключением одной. Следовательно, зачёркнутая цифра должна дополнять названную вашим товарищем сумму до ближайшего кратного девяти.

Если, например, было написано число 2365, а после перестановки получилось 3652, то их разность будет 1287; разность эта, а значит, и сумма её цифр $1+2+8+7=18$ делятся на 9. Если зачёркнута цифра 2, то останутся цифры, дающие в сумме $1+8+7=16$. Услышав от товарища, что получилось 16, вы дополняете это число до ближайшего бóльшего, кратного 9, т. е. до 18 (из кратных девяти: $1\cdot 9=9$; $2\cdot 9=18$; $3\cdot 9=27$ и т. д.; ближайшим, бóльшим шестнадцати будет 18). Полу́чите, очевидно, $18-16=2$, т. е. как раз зачёркнутую цифру. Если сумма незачёркнутых цифр сама окажется кратной девяти, то, очевидно, и зачёркнутая цифра должна быть кратной девяти, т. е. равняться или 9, или 0. В этом случае вам так и придётся сказать: «зачёркнуто либо девять, либо нуль».

Займёмся теперь признаком делимости на 11. Он основан на тех же соображениях, что и признак делимости на 9. Как 10; 100; 1000 и т. д. (т. е. единица с любым числом нулей) при делении на 9 дают в остатке единицу, точно так же 100; 10 000; 1 000 000 (вообще — единица, с чётным числом нулей) при делении на 11 дают в остатке единицу *). Иными словами,

$$100^n \equiv 1 \pmod{11}.$$

Рассмотрим теперь какое-нибудь число, например, 57 385. Разобьём его на грани по две цифры в каждой справа налево, как это делается при извлечении квадратного корня. При этом в крайней левой грани может получиться и одна цифра (что как раз имеет место в нашем примере: 5'73'85). Что́ представляет собой первая грань? — Пять десятков тысяч ($5\times 10\,000$). Каждый десяток тысяч даст при делении на 11 остаток 1, значит, пять десятков тысяч дадут при делении на 11 остаток 5. Следующая грань (73) представляет собой 73 сотни. Каждая сотня даст при делении на 11 остаток 1. Значит, 73 сотни дадут в остатке 73. Остаётся ещё крайняя правая грань: 85. Значит, наше число равно

$$57\,385 = (\text{число, делящееся на } 11) + 5 + 73 + 85,$$

т. е. числу, делящемуся на $11+$«сумма граней». Отсюда получается следующее правило:

---

*) Предлагаем читателю доказать это.

Если сумма граней делится на 11, то и всё число разделится на 11.

В нашем примере сумма граней равна $5 + 73 + 85 = 163$. Полученный результат не делится на 11; значит, и 57 385 не разделится на 11. Если при сложении граней получится большое число, то его в свою очередь можно разбить на грани и испытать их сумму; в нашем примере имеем: $163 = 1'63$. Складываем грани; $1 + 63 = 64$ — не делится на 11; значит, и исходное число не делится на 11.

Ещё пример:

563 035 делится на 11. Действительно, разбиение на грани даёт 56'30'35 (здесь первая грань состоит из двух цифр). Складываем грани $56 + 30 + 35 = 121$. Сумма граней делится на 11; значит, и 563 035 делится на 11.

Не следует думать, что для каждого числа существует единственный признак делимости. Вот ещё признак делимости на 11. Сложим отдельно все цифры данного числа, стоящие на чётных местах, и все цифры, стоящие на нечётных, и из бóльшего итога вычтем меньший *). Если разность делится на 11 (или равна нулю; нуль делится на любое число), то и данное число разделится на 11.

Рассмотрим пример. Пусть дано число 8 230 541. На нечётных местах (считая справа) стоят цифры: 1 (на первом месте), 5 (на третьем), 3 (на пятом), 8 (на седьмом); складывая эти цифры, получим $1 + 5 + 3 + 8 = 17$. На чётных местах стоят цифры: 4 (на втором), 0 (на четвёртом), 2 (на шестом); их сумма равна $4 + 0 + 2 = 6$. Разность $17 - 6 = 11$ делится на 11. Значит, и число 8 230 541 разделится.

Пусть читатель подумает сам, как доказать этот признак делимости. Рассуждение будет особенно просто, если использовать понятие сравнения.

Рассмотрим задачу, связанную с признаками делимости на одиннадцать.

Задача. Написать наименьшее делящееся на 11 шестизначное число, первая цифра которого 7 и все цифры различны.

---

*) Понятно, что в этом случае безразлично, считать ли цифры справа налево или слева направо: если число цифр в числе нечётное, то каждая цифра будет одинаковой чётности и слева и справа, а если число цифр чётное, то при счёте слева и справа чётность цифр изменится, но сумма чётных цифр останется равной или не равной сумме нечётных цифр.

Пишем вслед за семёркой четыре цифры, начиная с нуля, в порядке их роста: 70 123. Ясно, что таким образом мы получим наименьшее число нужного нам вида. Остаётся приписать последнюю цифру так, чтобы всё число разделилось на 11.

Сумма цифр, стоящих на нечётных местах (считая слева), равна $7+1+3=11$; сумма цифр, стоящих на чётных местах, равна 2. Чтобы разность сумм цифр, стоящих на чётных и нечётных местах, делилась на 11 или равнялась нулю, последняя цифра должна быть девяткой ($7+1+3=0+2+9$). Значит, искомое число — 701 239.

Совершенно аналогичен признак делимости на 37. Число 1000 и все его степени (т. е. числа, изображаемые единицей с числом нулей, кратным трём) дают при делении на 37 остаток, равный 1. Действительно, 999 делится на 37 (получается 27). Значит,

$$1000 \equiv 1 \pmod{37} \text{ и } 1000^n = 10^{3n} \equiv 1 \pmod{37}.$$

Если при испытании делимости на 11 мы разбивали число на грани по две цифры в каждой, то при испытании делимости на 37 приходится делить его на грани по три цифры в каждой, тоже справа налево. При этом в крайней левой грани могут получиться одна, две или три цифры. Если сумма граней делится на 37, то и всё число разделится. Например, 25 012 делится на 37: разбивая на грани, получим 25'012; сумма граней равна $25+12=37$.

Переходим к признакам делимости на 7 и на 13. Они основаны на том, что 1001 делится на 7 и 13; кстати, 1001 делится и на 11, так что мы, мимоходом, получим третий признак делимости на 11.

Рассмотрим какое-нибудь число, например 357 285. Это число содержит 357 тысяч и 285 простых единиц. Его можно записать так: $357\,000+285$. Прибавим и отнимем от нашего числа число его тысяч, т. е. 357; от этого ничего не изменится; сделаем далее простые преобразования:

$$357\,285 = 357\,000 + 285 + 357 - 357 =$$

$$= 357(1000+1) + 285 - 357 = 357 \cdot 1001 - (357 - 285).$$

Первое слагаемое, очевидно, делится на 1001; значит, судьба нашего числа зависит от выражения в скобках; но в скобках стоит разность между числом тысяч данного числа

и числом его простых единиц *). Если эта разность делится на 7, 11 или 13, то и само число разделится. Заметим, что число тысяч может оказаться меньше числа простых единиц; тогда, разумеется, из бóльшего вычитаем меньшее.

Рассмотрим число 208 824 525. В нём 208 824 тысячи и 525 простых единиц. Вычитаем из числа тысяч число единиц: 208 824 — 525 = 208 299. Нужно узнать, делится ли на 7, 11 или 13 это число. Повторяем наш приём. Теперь число единиц (299) больше числа тысяч (208). Вычитаем из бóльшего меньшее: 299 — 208 = 91. Полученное число (91) делится на 7 и на 13, но не делится на 11. Значит, и 208 824 525 делится на 7 и на 13, но не делится на 11.

Со свойствами числа 1001 связан любопытный арифметический фокус. Предложите кому-нибудь написать какое угодно трёхзначное число так, чтобы вы не видели, какое. Предложите, далее, приписать к этому числу справа такое же число (если, например, было задумано 167, то получится 167 167). Предложите разделить результат на 7. Всё благополучно разделится, хотя, казалось бы, взятое наугад число вовсе не обязано делиться на 7. Результат предложите разделить на 11; снова всё благополучно разделится! Наконец, последний результат предложите разделить на 13. Деление пройдёт без остатка, и в результате получится первоначально задуманное число.

Секрет фокуса очень прост. Приписав справа от задуманного числа его самого, мы тем самым умножаем его на 1001 (если, например, задумано число 167, то будем иметь $167\,167 = 167\,000 + 167 = 167\,(1000 + 1) = 167 \cdot 1001$). Но $1001 = 7 \cdot 11 \cdot 13$. Значит, разделив 167 167 последовательно на 7, 11 и 13, мы разделим его на 1001. Сперва мы умножили задуманное число на 1001, а потом разделили. Понятно, что все деления прошли благополучно, и в итоге получилось само задуманное число.

Мы говорили уже, что в разных системах счисления признаки делимости на одно и то же число — различны. Так, например, в системе счисления с основанием 3 число, оканчивающееся нечётной цифрой, может делиться на 2. Установим признак делимости на 2 в троичной системе счисления. Число 3 при делении на 2 даёт остаток 1. То же

*) Имеются в виду не разряды, а классы тысяч и простых единиц.

можно сказать о любой степени трёх, потому что всякая степень трёх, не содержа множителем двойку, при делении на 2 даёт в остатке единицу. Повторив те же рассуждения, которыми мы пользовались при выводе обычного признака делимости на 9, убедимся, что в троичной системе счисления на 2 делятся такие, и только такие, числа, сумма цифр которых делится на 2. Число **10 201** *), например, сумма цифр которого равна четырём, должно делиться на 2. Действительно, число **10 201** равно $1 \cdot 3^4 + 0 \cdot 3^3 + 2 \cdot 3^2 + 0 \cdot 3 + 1 = 81 + 18 + 1 = 100$, а сто, очевидно, на 2 делится.

Найдём все системы счисления, в которых признаком делимости любого числа на данное число a является делимость его суммы цифр на число a.

Заметим прежде всего, что этот признак делимости можно сформулировать иначе, именно так: разность между любым числом и суммой его цифр должна делиться на a. Действительно, в этом (и только в этом!) случае из делимости любого числа на a будет следовать делимость на a суммы его цифр и наоборот.

Обозначим основание искомой системы счисления буквой n. Число n, как основание системы счисления, запишется так: **10**; его сумма цифр равна единице. Значит, $n - 1$, разность между числом и его суммой цифр, должна делиться на a, что запишется следующим образом: $n - 1 = ma$, где m — любое натуральное число (или нуль). Отсюда следует, что искомое основание n системы счисления должно равняться увеличенному на единицу кратному числа a:

$$n = ma + 1.$$

Обратно: из этого равенства следует, что любая степень n при делении на a даст в остатке единицу. В самом деле, наше равенство выражает совершенно то же, что сравнение

$$n \equiv 1 \pmod{a};$$

возведя это сравнение в любую степень k, получим:

$$n^k \equiv 1 \pmod{a}.$$

Но если любая степень основания системы счисления даёт при делении на a в остатке единицу, то, повторив слово

*) Жирный шрифт, как и в главах IV и V, обозначает число, записанное в недесятичной, в данном случае в троичной системе счисления.

в слово вывод обычного признака делимости на 3 или на 9, убедимся, что делимость суммы цифр некоторого числа на a обеспечит делимость на a самого этого числа.

Итак, наш признак делимости будет иметь место во всех системах счисления, основание которых на единицу больше произвольного кратного числа a. Например, делимость суммы цифр будет обеспечивать деление числа на 9 не только в десятичной ($10 = 1 \cdot 9 + 1$), но и в девятнадцатиричной ($19 = 2 \cdot 9 + 1$), и в двадцативосьмиричной ($28 = 3 \cdot 9 + 1$), и во всех системах с основанием, равным $9m + 1$. Ни в каких иных системах счисления этот признак делимости не будет иметь места.

Вот ещё задача: найти наименьшее основание системы счисления, в которой имеют место следующие признаки делимости:

1°. Если сумма цифр некоторого числа делится на 5, то и само число разделится на 5.

2°. Если число, образованное двумя последними цифрами произвольного числа, делится на 7, то и само число разделится на 7.

Из предыдущей задачи мы знаем, что первому условию можно удовлетворить, взяв в качестве основания системы счисления число вида $5m + 1$:

$$n = 5m + 1.$$

Займёмся вторым условием. Если делимость некоторого числа на 7 обусловливается делимостью на 7 числа, образованного его двумя последними цифрами, то, значит, единица третьего разряда $\mathbf{100} = n^2$ должна делиться на 7 *); тогда и любое число единиц третьего разряда будет делиться на 7, и вопрос сведётся к исследованию второго и первого разрядов. Итак, n^2 должно делиться на семь: $n^2 = 7p$. Чтобы правая часть равенства была точным квадратом, число p должно равняться 7, умноженному на точный квадрат: $p = 7k^2$; мы будем иметь $n^2 = 49k^2$ или $n = 7k$.

Для определения n получилось два линейных уравнения с тремя неизвестными:

$$n = 7k \text{ и } n = 5m + 1.$$

*) Так, в десятичной системе счисления признак делимости на 4 или на 25 заключается в делимости на эти числа нашей единицы третьего разряда — сотни.

Приравнивая друг другу правые части, получим одно неопределённое линейное уравнение с двумя неизвестными:

$$7k = 5m + 1 \text{ или } 7k - 5m = 1.$$

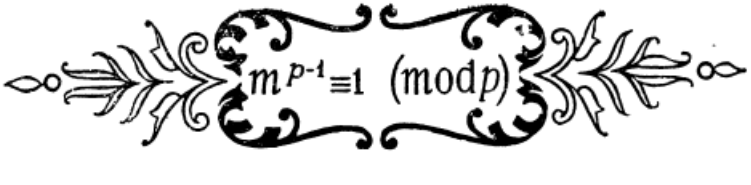
Решать такие уравнения в целых числах мы умеем. Без особого труда найдём:

$$m = 4 + 5t;\ k = 3 + 7t,$$

где t — любое целое число; следовательно, $n = 21 + 49t$. Наименьшее положительное значение $n = 21$ получится при $t = 0$.

Число 21 и будет ответом на нашу задачу. Наименьшим основанием системы счисления, в которой имеют место данные выше признаки делимости, является число 21.

Разобрав вопрос о связи признаков делимости с различными системами счисления, мы перейдём к таким теоремам о делимости чисел, которые от системы счисления не зависят.



ГЛАВА X.

ЕЩЁ О ДЕЛИМОСТИ; «БОЛЬШАЯ» ТЕОРЕМА, КОТОРУЮ ЗОВУТ «МАЛОЙ».

Разбирая на стр. 81 задачу о пифагоровых треугольниках, мы были вынуждены использовать предложения, подобные следующему: «сумма или разность двух чётных или двух нечётных чисел представляют собой числа чётные». Эти предложения, несомненно, относятся к учению о делимости; но в отличие от признаков делимости, разобранных в предыдущей главе и существенно связанных с выбором системы счисления, здесь выбор системы счисления не играет никакой роли.

В качестве первого примера рассмотрим разность между квадратом нечётного числа и единицей, т. е. выражение $m^2 - 1$, где m — число нечётное. Нетрудно убедиться, что при любом (нечётном) m эта разность должна разделиться на 8. Действительно, она разлагается на множители:

$$m^2 - 1 = (m - 1)(m + 1).$$

Раз m — число нечётное, значит оба множителя в правой части будут чётными, причём, очевидно, соседними чётными числами, потому что разность между ними равна $m + 1 - (m - 1) = 2$. Но из двух соседних чётных чисел одно обязательно делится на 4*). Значит, один из множителей делится на 4, да ещё второй введёт двойку. Всё произведение будет делиться на $2 \cdot 4 = 8$.

*) Действительно, если одно из них, будучи чётным, не делится на 4, то при делении на 4 оно может давать в остатке только 2, т. е. иметь вид $4n + 2$. Но чётными соседями этого числа будут числа $(4n + 2) \pm 2$, т. е. $4n$ и $4n + 4$; оба они кратны четырём.

Можно рассуждать и иначе: раз m по условию нечётное число, значит, его можно записать в виде $2k+1$, где k — произвольное число (натуральное или нуль). Получим:

$$m^2-1=(2k+1)^2-1=4k^2+4k+1-1=4k(k+1).$$

Из двух соседних чисел k и $k+1$ одно обязательно чётное. Значит, в состав нашего выражения, кроме коэффициента 4, войдёт ещё множитель, равный двум, т. е. в составе его будет множитель, равный $4\cdot 2=8$, что мы и хотели доказать.

Давая в выражении m^2-1 числу m различные натуральные значения, получим следующие числа, кратные восьми:

m	1	3	5	7	9	. . .
m^2-1	0	8	24	48	80	. . .

В качестве второго примера рассмотрим разность между кубом любого числа и самим числом. Эта разность, как нетрудно показать, делится на 6. Действительно, возьмём произвольное число m. Разность между кубом и самим числом равна m^3-m. Разлагая на множители, получим:

$$m^3-m=m(m-1)(m+1)=(m-1)m(m+1).$$

Иными словами, разность между кубом натурального числа и самим числом всегда представляет собой произведение трёх стоящих подряд натуральных чисел. Из трёх же стоящих подряд натуральных чисел по крайней мере одно — чётное (делится на 2) и одно делится на 3 *). Следовательно, разность между кубом натурального числа и самим числом делится на $2\cdot 3=6$, что мы и хотели доказать.

В качестве третьего примера рассмотрим задачу, обошедшую все школьные олимпиады и конкурсы: «показать, что выражение m^5-5m^3+4m при любом натуральном m делится на 120». Для $m=1$ и $m=2$ это очевидно, потому что при $m=1$ или 2 наш трёхчлен равняется нулю, а нуль

*) Действительно, рассмотрим три числа, стоящие подряд: k, $k+1$, $k+2$. Первое имеет вид либо $k=3n$, либо $k=3n+1$, либо $k=3n+2$, потому что при делении на 3 возможны только такие остатки: 0, 1, 2. Если $k=3n$, то вопрос ясен. Если $k=3n+1$, то $k+2=3n+3$ делится на 3. Если, наконец, $k=3n+2$, то $k+1=3n+3$ тоже делится на 3. Во всех возможных случаях одно из трёх стоящих подряд чисел оказывается кратным числа 3.

принято считать кратным любого числа, стало быть, и ста двадцати; поэтому будем считать, что $m > 2$.

Сделаем следующие очевидные преобразования:

$$m^5 - 5m^3 + 4m = m(m^4 - 5m^2 + 4) =$$
$$= m(m^4 - 4m^2 - m^2 + 4) = m[(m^4 - 4m^2) - (m^2 - 4)] =$$
$$= m[m^2(m^2 - 4) - (m^2 - 4)] = m(m^2 - 4)(m^2 - 1) =$$
$$= (m - 2)(m - 1)m(m + 1)(m + 2).$$

При любом m наш трёхчлен разлагается на пять множителей, представляющих собой (при m, большем двух) пять последовательных натуральных чисел. В последовательности пяти натуральных чисел найдётся по меньшей мере два соседних чётных; значит, трёхчлен будет делиться на 8. Далее, в последовательности пяти чисел имеется по крайней мере одно, делящееся на 3 (уже три первых множителя, как мы видели, обеспечивают делимость на 3). Наконец, соображениями, совершенно аналогичными тем, которые сделаны в примечании к предыдущему примеру, убеждаемся, что произведение пяти стоящих подряд натуральных чисел должно делиться на 5. Итак, наш трёхчлен делится на взаимно-простые числа 8, 3 и 5; он раздслится и на их произведение, т. е. на 120. Вот несколько различных значений m и соответствующих значений трёхчлена:

m	1	2	3	4	5	. . .
$m^5 - 5m^3 + 4m$	0	0	120	720	2520	. . .

Разобранные примеры, несмотря на некоторую искусственность, очень поучительны. Они подводят нас к двум любопытным теоремам. Прежде всего, мы видим, что разность $m^3 - m$ делится на 3. Так же можно доказать, что $m^5 - m$ делится на 5, хотя доказательство несколько громоздко. Непосредственно очевидно, что $m^2 - m$ делится на 2. Напротив, $m^4 - m$ может при некоторых m и не делиться на 4: именно, при $m = 2$ мы получим $m^4 - m = 16 - 2 = 14$, т. е. число, на 4 не делящееся. Возникает вопрос: при каких же именно значениях a разность $m^a - m$ делится на показатель a при любом m, а при каких — нет. Эту задачу

решил уже знакомый нам Ферма. Ей будет посвящён конец настоящей главы.

Вторая теорема, к которой подводят наши примеры, состоит в следующем. Мы видели, что произведение трёх последовательных натуральных чисел делится не только на 3 (это понятно), но и на 6, т. е. на произведение $1 \cdot 2 \cdot 3$. Точно так же произведение пяти последовательных натуральных чисел делится не только на 5, но и на 120, т. е. на произведение $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$. Читатель без всякого труда докажет, что произведение четырёх последовательных натуральных чисел делится на $1 \cdot 2 \cdot 3 \cdot 4 = 24$. Оказывается, имеет место следующая общая теорема:

Произведение m последовательных натуральных чисел

$$k(k+1)(k+2)\ldots(k+m-1)$$

делится без остатка на произведение m первых последовательных натуральных чисел, т. е. на

$$1 \cdot 2 \cdot 3 \cdot 4 \ldots (m-1)m.$$

Элементарное арифметическое доказательство этой теоремы довольно громоздко; поэтому говорить о нём мы не будем. Для читателей, знакомых с теорией соединений и биномом Ньютона, заметим, что частное $\dfrac{k(k+1)(k+2)\ldots(k+m-1)}{1 \cdot 2 \cdot 3 \ldots (m-1)m}$ равно числу сочетаний из $(k+m-1)$ элементов по m или же коэффициенту при $(m+1)$-м члене разложения бинома $(a+b)^{k+m-1}$. Следовательно, это частное должно быть целым числом, т. е. $k(k+1)\ldots(k+m-1)$ должно делиться без остатка на $1 \cdot 2 \cdot 3 \ldots (m-1)m$.

В разобранных выше примерах разыскивались конкретные делители некоторых выражений при каком угодно (целом) значении величины n, входящей в эти выражения. Часто вопрос ставится иначе: даётся некоторое выражение и требуется выяснить, может ли оно вообще при произвольном n иметь делители (отличные, разумеется, от него самого и от единицы) или же всегда является числом простым. Такого рода выражения изучались в надежде найти признаки, позволяющие по виду числа, по его строению решить вопрос: простое оно или нет. Примером подобного исследования может служить совсем простая теорема, найденная француженкой Софи Жермен:

«Всякое число вида n^4+4, где $n > 1$, является составным».

Докажем эту теорему. Имеем:

$$n^4+4=n^4+4n^2+4-4n^2=(n^2+2)^2-(2n)^2=$$
$$=(n^2+2-2n)(n^2+2+2n)=$$
$$=[(n-1)^2+1][(n+1)^2+1].$$

При целом n оба множителя — целые числа. При $n>1$ ни один из них не равен 1 и, следовательно, n^4+4 является числом составным. При $n=1$ мы имеем исключительный случай: $n^4+4=1^4+4=5$ — число простое.

Простые числа занимают математиков буквально тысячелетия. Древние греки интересовались ими две с половиной тысячи лет тому назад. Многие пытались найти признаки, позволяющие по строению числа установить — простое оно или составное. Достичь некоторого успеха на этом пути удалось впервые Ферма́. В 1640 г. ему удалось доказать теорему, которая так поразила и обрадовала его, что он написал по поводу её открытия (в письме к Френиклю): «Меня озарило ярким светом».

В чём же состоит эта теорема Ферма́?

Мы уже видели, что при любом m двучлен m^3-m делится на 3, двучлен m^5-m делится на 5. Ферма́ показал, что при любом простом p двучлен m^p-m делится на p, каково бы ни было число m. Этот скромный с виду результат привёл к важным обобщениям и породил довольно значительную литературу; его считают одной из основных теорем теории чисел. И всё же эту теорему называют «малой», в отличие от «великой теоремы Ферма́», о которой было рассказано в конце главы VII.

Сам Ферма́ формулировал свою теорему не совсем так, как это было сделано выше. Выражение m^p-m можно преобразовать, взяв m за скобку; получится $m(m^{p-1}-1)$. Если m кратно p, то теорема очевидна. Важен и интересен только тот случай, когда m не делится на p. Но в таком случае m и p взаимно-просты, потому что только те числа могут иметь общие множители с простым числом p, которые ему кратны. В случае взаимно-простых m и p должна делиться на p разность $m^{p-1}-1$. Так и была сформулирована теорема самим Ферма́: «Если p просто, а m не делится на p, то $m^{p-1}-1$ делится на p».

Эту же мысль можно выразить на языке сравнений. Раз $m^{p-1}-1$ делится на p, значит, m^{p-1} и 1 сравнимы по

модулю p, что, как мы знаем, записывается так:

$$m^{p-1} \equiv 1 \pmod{p}.$$

В этой форме теорема Ферма́ даётся в современных курсах теории чисел.

Разберём несколько примеров. Положим $m = 2$; тогда в качестве p можно будеть взять любое простое нечётное число, т. е. любое простое, за исключением самого числа 2. В следующей таблице даны значения p, 2^{p-1}, $2^{p-1} - 1$ и показано, что $2^{p-1} - 1$ всегда содержит множителем p.

$n = 2$

p	3	5	7	11	13	17
2^{p-1}	4	16	64	1024	4096	65 536
$2^{p-1} - 1$	$3 = 3 \cdot 1$	$15 = 5 \cdot 3$	$63 = 7 \cdot 9$	$1023 = 11 \cdot 93$	$4095 = 13 \cdot 315$	$65\,535 = 17 \cdot 3855$

Если p не является простым числом (например, $p = 15 = 3 \cdot 5$), то число $2^{p-1} - 1$ не будет обязательно обладать этим свойством. Действительно, $2^{15-1} - 1 = 2^{14} - 1 = 16\,384 - 1 = 16\,383$ не делится на 15. Точно так же n не должно делиться на p. Если при $n = 2$ мы возьмём в качестве p тоже 2, то у нас ничего не выйдет: $2^{2-1} - 1 = 1$ не делится на 2.

Вот ещё примеры:

	$n = 3$	$n = 5$	$n = 10$
$p = 2$	$3^{2-1} - 1 = 2 = 2 \cdot 1$	$5^{2-1} - 1 = 4 = 2 \cdot 2$	—
$p = 3$	—	$5^{3-1} - 1 = 24 = 3 \cdot 8$	$10^{3-1} - 1 = 99 = 3 \cdot 33$
$p = 5$	$3^{5-1} - 1 = 80 = 5 \cdot 16$	—	—
$p = 7$	$3^{7-1} - 1 = 728 = 7 \cdot 104$	$5^{7-1} - 1 = 15\,624 = 7 \cdot 2232$	$10^{7-1} - 1 = 999\,999 = 7 \cdot 142\,857$
$p = 11$	$3^{11-1} - 1 = 59\,048 = 11 \cdot 5368$	$5^{11-1} - 1 = 9\,765\,624 = 11 \cdot 887\,784$	$10^{11-1} - 1 = 9\,999\,999\,999 = 11 \cdot 909\,090\,909$

Мы видим, что n не обязано быть простым (например, в третьем столбце $n = 10 = 2 \cdot 5$). Но оно не должно

делиться на p. Поэтому при $n = 3$ не рассматривается значение $p = 3$, при $n = 5$ — значение $p = 5$, при $n = 10$ — значения $p = 2$ и $p = 5$. Читатель сам убедится путём подсчёта, что в этих случаях утверждение теоремы не выполняется.

Переходим к доказательству теоремы Ферма́. Начнём с того, что рассмотрим полную систему наименьших положительных вычетов числа p, т. е. все остатки, которые могут получиться при делении различных чисел на p (кроме остатка, равного нулю). Вот эти вычеты:

$$1,\ 2,\ 3,\ \ldots,\ p-2,\ p-1. \qquad (1)$$

Помножим каждый из них на число m, не делящееся на p. Получим

$$1m,\ 2m,\ 3m,\ 4m,\ \ldots,\ (p-2)m,\ (p-1)m. \qquad (2)$$

Все эти числа различны, ни одно из них не равно нулю. Но этого мало: все они дают при делении на p разные остатки. Действительно, если am и bm, где a и b — различные числа из ряда (1), т. е. меньшие p, дают при делении на p одинаковые остатки, то разность $am - bm = m(a-b)$ должна делиться на p. Число m взаимно-просто с p. Следовательно, $a-b$ должно делиться на p. А это невозможно, потому что разность $a-b$ не равна нулю и заведомо меньше p (и a и b — положительные числа, меньшие p). Полученное противоречие показывает, что исходное предположение о возможности одинаковых остатков при делении чисел ряда (2) на p — неверно. Следовательно, все эти остатки различны, и так как их ровно $p-1$, то они равны числам ряда (1), т. е. 1, 2, 3, ..., $p-1$, только взятым в каком-то другом порядке.

Но это значит, что каждое число ряда (2) сравнимо по модулю p (равноостаточно) с одним, и только одним, из чисел ряда (1). Обозначим число из ряда (2), сравнимое с 1, через k_1, число, сравнимое с 2, — через k_2 и т. д., число, сравнимое с $p-1$, — через k_{p-1}. Получим следующий ряд сравнений:

$$\left.\begin{aligned} k_1 &\equiv 1 \\ k_2 &\equiv 2 \\ k_3 &\equiv 3 \\ &\ldots\ldots \\ &\ldots\ldots \\ k_{p-2} &\equiv p-2 \\ k_{p-1} &\equiv p-1 \end{aligned}\right\} \pmod{p}.$$

Перемножим теперь все эти сравнения, что, как мы знаем, делать можно. Получим:

$$k_1 k_2 \ldots k_{p-1} \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}. \qquad (*)$$

Переходим к центральному пункту доказательства. Числа $k_1, k_2, \ldots, k_{p-1}$ представляют собой все числа ряда (2), только взятые в другом порядке. Произведение их не зависит от порядка множителей; поэтому

$$k_1 k_2 \ldots k_{p-1} =$$
$$= 1m \cdot 2m \cdot 3m \ldots (p-1)m = m^{p-1} \cdot 1 \cdot 2 \cdot 3 \ldots (p-1).$$

Заменяя произведение в левой части сравнения (*) равной ему величиной, получим:

$$m^{p-1} \cdot 1 \cdot 2 \cdot 3 \ldots (p-1) \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}.$$

Все члены произведения $1 \cdot 2 \ldots (p-1)$ меньше первоначального числа p, а потому взаимно-просты с ним. Значит, сравнение можно на них сократить. Получится:

$$m^{p-1} \equiv 1 \pmod{p},$$

что и требовалось доказать.

Это доказательство можно изложить, не используя понятия сравнения, что и было сделано самим Ферма́, жившим без малого за 200 лет до Гаусса — изобретателя теории сравнений. Такое доказательство очень громоздко. Существует любопытное доказательство теоремы Ферма́, связанное с превращением простой дроби в периодическую десятичную. Но оно, во-первых, длинно, а во-вторых, не совсем подходит к теме этой книжки, посвящённой целым числам *).

Для читателей, знакомых с биномом Ньютона, можно привести ещё одно доказательство теоремы Ферма́.

Напишем по формуле Ньютона разложение двучлена $(m+1)^p$, где m — целое, а p — простое число:

$$(m+1)^p = m^p + pm^{p-1} + \frac{p(p-1)}{1 \cdot 2} m^{p-2} + \ldots + pm + 1.$$

Все коэффициенты бинома Ньютона, т. е. числа вида $\frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \cdot 3 \ldots k}$ — числа целые. Мало того, все они,

*) Изложено оно в книге Радемахера и Теплица «Числа и фигуры», которая вообще очень интересна.

кроме первого и последнего, делятся на p. Действительно, мы уже знаем, что в дроби $\frac{p(p-1)\dots(p-k+1)}{1\cdot 2\cdot 3\dots k}$ числа, стоящие в знаменателе, должны полностью сократиться с множителями числителя. Но p взаимно-просто со всеми числами 1, 2, 3, ..., k. Значит, числа эти должны полностью сократиться с множителями произведения $(p-1)(p-2)\dots$ $\dots(p-k+1)$, а множитель p останется нетронутым. Итак,

$$(m+1)^p = m^p + (\text{число, делящееся на } p) + 1.$$

Это равенство показывает нам следующее. Если при каком-нибудь значении m двучлен $m^p - m$ делится на p, то на p обязательно разделится и $(m+1)^p - (m+1)$, т. е. такой же двучлен, но с основанием, на единицу бóльшим (потому что из делимости вычитаемого и разности на некоторое число следует делимость на это число и уменьшаемого). Если $m = 1$, то $m^p - m = 1 - 1 = 0$ наверное делится на p (нуль делится без остатка на любое число). Значит, и $(m+1)^p - (m+1)$, т. е. $2^p - 2$, будет делиться на p, а отсюда, в свою очередь, будет следовать, что $3^p - 3$ делится на p и т. д. до произвольного значения m *). Следовательно, $m^p - m$ при любом m и простом p делится на p («малая» теорема Ферма́).

Эта теорема была открыта Ферма́ в связи со следующей задачей: он искал такие выражения, содержащие букву n, которые были бы простыми числами. В связи с этим Ферма́ формулировал любопытную «теорему», которая оказалась неверной (см. стр. 87). Вот эта «теорема».

Ферма́ рассматривал числа вида $2^{2^n}+1$, где n — произвольное целое число. Вот какие числа он получил, полагая n равным 0, 1, 2, 3, 4:

n	0	1	2	3	4
$2^{2^n}+1$	$2^1+1=3$	$2^2+1=5$	$2^4+1=$ $=17$	$2^8+1=$ $=257$	$2^{16}+1=$ $=65\,537$

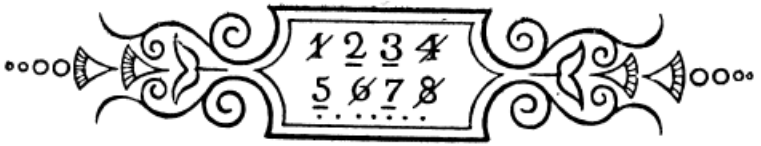
*) Напомним, что подобное рассуждение называется полной математической индукцией.

Все числа в нижней строке этой таблички (3, 5, 17, 257, 65 537) — числа простые. Ферма́ утверждал, что и при бо́льших значениях n получатся простые числа. При $n = 5$ Ферма́ получил число 4 294 967 297, которое он, Ферма́, не сумел разложить на множители и думал, что оно тоже простое. Однако Эйлер, о котором речь будет дальше, убедился, что 4 294 967 297 делится на 641, т. е. не является простым числом. Таким образом, Эйлер показал, что Ферма́ ошибся *).

Это неверное предложение очень поучительно. Своеобразное «чутьё» подсказывает талантливым математикам, в каком направлении вести исследование. Мы увидим в следующей главе, что числа Ферма́, т. е. простые числа вида $2^{2^n}+1$, оказались весьма замечательными, и изучение их привело впоследствии к крупным открытиям. Далее математик работает подобно любому учёному-естественнику: он делает предположения (гипотезы), проверяет их путём наблюдения и своеобразного математического опыта, ищет аналогии и т. п. Но, получив результат путём догадки или опыта, математик обязан строго доказать его. В противном случае всегда остаётся опасение, что высказанное утверждение может оказаться ошибочным.

---

*) Легко разделить 4 294 967 297 на 641, когда заранее знаешь, что делить нужно именно на 641. Но делить десятизначное число на все простые числа подряд (а простых чисел уже в пределах первой сотни — двацать пять штук), не имея при этом ни достаточно больших таблиц простых чисел, ни иных вспомогательных средств, — очень трудная работа.



ГЛАВА XI.

ЭРАТОСФЕНОВО РЕШЕТО.

В предыдущих главах нам нередко встречались простые, или первоначальные, числа. Мы говорили уже, что простым называется число, имеющее только два делителя: самого себя и единицу. Единица, имеющая только один делитель, к простым числам не причисляется. Числа 2, 3, 5, 7, 11, очевидно, — простые. Напротив, числа 4, 6, 8, 9 — составные.

Прежде чем ставить общие задачи, связанные с простыми числами, рассмотрим простые числа в пределах хотя бы от единицы до тысячи и постараемся путём непосредственного обзора подметить простейшие их свойства.

Как же найти все простые числа в пределах первой тысячи? Для этого поступают следующим образом: выписывают все числа от единицы до тысячи. Зечёркивают единицу (она не является простым числом). Затем подчёркивают число 2 и зачёркивают все числа, кратные двум (чётные), т. е. все числа через одно; получается таблица такого вида:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

и так далее.

Далее подчёркивают первое из оставшихся незачёркнутыми чисел (3) и зачёркивают все числа «через два на третье» (т. е. кратные трём); затем подчёркивают 5 (четыре уже за-

чёркнуто) и зачёркивают все числа, кратные пяти («через четыре на пятое») и так далее. Получается следующая таблица:

~~1~~	~~2~~	~~3~~	~~4~~	~~5~~	~~6~~	~~7~~	~~8~~	~~9~~	~~10~~
~~11~~	~~12~~	~~13~~	~~14~~	~~15~~	~~16~~	~~17~~	~~18~~	~~19~~	~~20~~
~~21~~	~~22~~	~~23~~	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	~~29~~	~~30~~
~~31~~	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	~~37~~	~~38~~	~~39~~	~~40~~
.	.	.	.	.	.	.	.	.	.
	.	.	.	.	.	.	.	.	.

Таким образом, мы вычеркнем все составные числа и получим таблицу простых чисел (она приложена в конце книги на стр. 163).

Впервые такую таблицу составил древнегреческий математик Эратосфен (III в. до н. э.). Он писал числа на папирусе, натянутом на рамку, и не зачёркивал, а прокалывал составные числа. Получалось нечто вроде решета, сквозь которое как бы «просеивались» все составные числа, а простые оставались. Поэтому таблицу простых чисел до сих пор зовут «эратосфеновым решетом».

Приглядываясь к эратосфенову решету, мы замечаем, что в начале таблицы простые числа расположены гораздо гуще, чем, например, вблизи тысячи. Так, в первом десятке (от 1 до 10) мы встречаем четыре простых числа: 2, 3, 5, 7. А между простыми числами 997 и 1009 имеется одиннадцать составных чисел подряд. Если зайти достаточно далеко, то можно найти какой угодно длинный числовой промежуток, т. е. сколь угодно длинный ряд натуральных чисел, состоящий сплошь из чисел составных.

Докажем, например, что существует числовой промежуток, состоящий из ста составных чисел подряд. Для этого рассмотрим число, представляющее собой произведение всех натуральных чисел от 1 до 101, т. е. число

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \ \ldots \ 99 \cdot 100 \cdot 101.$$

Это — очень большое число. Оно равно приблизительно $95 \cdot 10^{158}$, т. е. значительно больше обычных «астрономических» чисел. (Но оно ничтожно мало рядом с числом 9^{9^9},

см. стр. 15.) Обозначим это число буквой A. Рассмотрим теперь ряд чисел:

$$A+2,\ A+3,\ A+4,\ A+5,\ \ldots,\ A+99,\ A+100,\ A+101.$$

Это — серия из ста целых чисел подряд. Каждое из них — составное. Возьмём, например, первое из них, т. е. $A+2$; оно делится на 2. Действительно, A, имея по условию множителем 2, делится на 2. Само число 2 (второе слагаемое), очевидно, делится на 2. Следовательно, и сумма разделится на 2, т. е. будет числом составным. Точно так же $A+3$ разделится на 3, $A+4$ — на четыре и т. д.; наконец, $A+101$ разделится на 101, потому что в A входит множителем 101. Таким образом, все числа найденного нами ряда — числа составные; что́ мы и хотели доказать.

Точно так же доказывается, что можно найти какой угодно длинный ряд (содержащий хотя бы тысячу или миллион чисел), состоящий сплошь из составных чисел.

При этом, естественно, возникает мысль: может быть, начиная с некоторого числа, все числа являются составными? Может быть, существует лишь конечное, ограниченное количество простых чисел, а всё остальное бесконечное множество чисел суть числа составные? Может быть, существует самое большое простое число? Что же это за число?

Подобные вопросы занимали уже древних математиков. Евклид, о котором говорилось в главе VI, занимался этой задачей и дал полное её решение. Ему удалось доказать, что число простых чисел бесконечно, что не существует наибольшего простого числа. Докажем это предложение.

Мы будем, следуя Евклиду, доказывать его с помощью приёма, который называется «доказательством от противного» *). Иными словами, допустив, что существует наибольшее простое число, мы в результате правильных рассуждений придём к противоречию. Это и покажет, что предположение о существовании наибольшего простого числа неправильно, что такого числа нет.

Итак, предположим, что существует наибольшее простое число. Обозначим его через p. Рассмотрим число, представляющее произведение всех простых чисел, т. е. число $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ldots p$. Прибавив к этому числу единицу, по-

*) В настоящее время имеется много различных доказательств теоремы о бесконечности множества простых чисел.

лучим число $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ldots p + 1$, которое, конечно, гораздо больше, чем p.

Попытаемся разделить его на какое-либо простое число (мы предполагаем, что p самое большое простое число). Число $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ldots p + 1$ состоит из двух слагаемых. Первое слагаемое $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ldots p$, как произведение всех простых чисел, делится на любое простое число, а второе слагаемое (единица) при делении на любое целое число, кроме единицы, даёт в частном нуль и в остатке единицу; значит, и сумма $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ldots p + 1$ при делении на любое простое число даст в остатке единицу.

Следовательно, предположив, что p — самое большое простое число, мы пришли к противоречию, так как в этом случае составленное нами число ни на одно из простых чисел не делится.

Значит, число $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ldots p + 1$ или само является простым, или делится на простое число, отличное от 2, 3, 5, 7, 11, ..., p, и, значит, большее чем p. Таким образом, предположив, что p — наибольшее простое число, мы доказали, что существует простое число, ещё большее. Это противоречие убеждает нас, что исходное предположение неправильно, т. е. что наибольшего простого числа быть не может: число простых чисел бесконечно.

Все простые числа, начиная с трёх, можно разбить на две категории. Одни (например, 5, 13, 17) имеют вид $4n + 1$; другие (например, 3, 7, 11) имеют вид $4n - 1$. Никакого иного вида нечётное число (а все простые числа, кроме числа 2, нечётны) иметь не может, так как при делении нечётного числа на 4 возможны остатки, равные только 1 или 3. Разумеется, не всякое число вида $4n \pm 1$ простое, но всякое простое число имеет один из этих видов. Спрашивается: в каждом ли из этих классов содержится бесконечное множество простых чисел, или же один из них конечен, а другой — нет? Оба они быть конечными, разумеется, не могут.

Исследование показало, что и тех и других чисел бесконечно много. Для чисел вида $4n + 1$ доказательство этого утверждения несколько громоздко, и мы ограничимся тем, что докажем бесконечность множества простых чисел вида $4n - 1$.

Докажем предварительно следующее вспомогательное предложение (лемму): «Произведение нескольких чисел вида $4n + 1$ само есть число вида $4n + 1$».

Рассмотрим два числа этого класса: $4a+1$ и $4b+1$. Перемножим их:

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 =$$
$$= 4(4ab + a + b) + 1 = 4k + 1,$$

где через k обозначено целое число $4ab + a + b$. Мы видим, что произведение двух множителей вида $4n+1$ обязательно имеет тот же вид. Присоединяя третий, четвёртый и т. д. множители, мы убедимся, что то же самое можно сказать о произведении любого числа таких множителей.

Перейдём теперь к теореме о числах вида $4n-1$ и применим к ней евклидов приём доказательства. Допустим противное — что простых чисел вида $4n-1$ — конечное количество, например m. Обозначим их $p_1, p_2, \ldots, p_m$. Рассмотрим число

$$A = 4 \cdot p_1 \cdot p_2 \ldots p_m - 1.$$

Оно должно иметь хотя бы один (простой) множитель вида $4n-1$, потому что оно само имеет вид $4n-1$, а произведение множителей вида $4n+1$, как мы видели, должно иметь вид $4n+1$. Итак, среди простых множителей числа A должно быть некоторое $p = 4n-1$. Но p не может равняться ни одному из чисел $p_1, p_2, \ldots, p_m$, потому что ни на одно из этих чисел наше A не делится; это p — простое число вида $4n-1$. Следовательно, числами $p_1, p_2, \ldots, p_m$ не исчерпываются все простые числа вида $4n-1$; а это противоречит нашему исходному предположению. Таким образом, простых чисел вида $4n-1$ бесконечно много.

Числа вида $4n-1$ образуют арифметическую прогрессию с первым членом 3 и разностью 4 ($\div 3, 7, 11, 15, \ldots$). Доказанную только что теорему можно было бы сформулировать и так: в бесконечной арифметической прогрессии

$$\div 3, 7, 11, 15, 19, \ldots$$

содержится бесконечное же множество простых чисел.

Спрашивается, нет ли ещё прогрессий, обладающих тем же свойством? Мы видели, что прогрессия с первым членом 1 и разностью 1 (сам натуральный ряд) содержит бесконечное количество простых чисел. То же самое говорилось (хотя мы и не доказывали этого) о прогрессии $\div 1, 5, 9, 13, 17, 21, \ldots$, т. е. о числах вида $4n+1$.

Вопрос о количестве простых чисел в той или иной арифметической прогрессии занимал многих математиков, особенно на рубеже XVIII и XIX столетий. Решил его полностью Лежён-Дирихле (1805—1859 гг.), который доказал, что любая арифметическая прогрессия, первый член и разность которой взаимно просты, содержит среди своих членов бесконечное множество простых чисел. Оговорка относительно взаимной простоты первого члена и разности очень существенна: если они имеют общий множитель, отличный от единицы, то, очевидно, все члены прогрессии будут содержать этот множитель и, следовательно, будут числами составными.

Изложить доказательство Дирихле элементарно — совершенно невозможно.

Упомянем, кстати, ещё об одной проблеме, которая естественно возникает при внимательном рассмотрении эратосфенова решета и которая до сих пор не решена. Среди простых чисел встречаются «числа-близнецы», т. е. пары соседних нечётных чисел, являющихся одновременно простыми. Таковы, например, числа 5 и 7, числа 11 и 13, числа 17 и 19 и т. д. В начале «решета» подобные пары встречаются довольно часто, но по мере продвижения в область бóльших чисел, их становится всё меньше и меньше. В первой сотне имеется 8 таких пар (3 и 5; 5 и 7; 11 и 13; 17 и 19; 29 и 31; 41 и 43; 59 и 61; 71 и 73); между числами 501 и 600 — только две пары (521 и 523; 569 и 571). Дальше они встречаются очень неравномерно, но в общем — всё реже и реже, значительно реже, чем сами простые числа. Впрочем, известны и весьма солидные пары «близнецов», например 5 971 847 и 5 971 849. Спрашивается, будет ли среди этих пар последняя? Этого до сих пор не удалось установить. Мало того, до сих пор не намечено даже пути, следуя которому можно было бы приблизиться к решению этой проблемы.

Важнейшим вопросом, связанным с простыми числами, является вопрос о возможности разложения любого числа на простые множители, т. е. о возможности представления любого числа в виде произведения простых чисел и притом единственным образом. Эта возможность кажется нам совершенно очевидной, и мы в предыдущих главах неоднократно её использовали. Но в действительности предложение о разложении на простые множители является теоремой, которую нужно и можно доказать. Она настолько важна в теории

чисел, что её нередко называют «основной теоремой арифметики». Вот как она формулируется: «Всякое натуральное число разлагается единственным образом на простые множители». Докажем эту теорему.

Предварительно докажем вспомогательную теорему (лемму). Именно, докажем, что из делимости произведения kl на простое число p следует, что хотя бы один множитель (либо k, либо l, а может быть и оба) делится на p.

Действительно, число k либо делится на p, — и тогда теорема доказана, — либо нет. Если k не делится на p, то числа k и p взаимно-просты, потому что k, не делясь на p, не содержит его в числе своих множителей, а p, будучи простым, никаких иных множителей, кроме единицы и самого p, не имеет. Но если k взаимно-просто с p, а произведение kl делится на p, то l должно делиться на p (теорема третья главы VI, стр. 51). Следовательно, l делится на p.

Эта лемма без труда распространяется на любое число множителей: если произведение $ab \ldots h$ делится на простое число p, то на него делится по крайней мере одно из чисел a, $b, \ldots, h$.

Переходим теперь к доказательству самой теоремы — доказательству того, что всякое натуральное число разлагается единственным образом на простые множители. Здесь, собственно, не одно, а два утверждения: утверждается, во-первых, возможность разложения на простые множители и, во-вторых, единственность такого разложения.

Что разложение возможно, это очевидно. Пусть дано некоторое число N. Если оно простое, то теорема доказана, ибо его можно считать собственным единственным простым множителем. Если же оно составное, то разделится на какое-то простое число p, меньшее чем N. В частном получится число N_1, тоже меньшее чем N. Если N_1 просто, то $N = p_1 N_1$, и теорема доказана. Если же N_1 не является простым числом, то оно разделится на некоторое простое число p_2, меньшее чем N_1, и в частном получится N_2, тоже меньшее чем N_1. Числа N_1, N_2, N_3 и т. д. всё время уменьшаются, и число их не может быть бесконечным. Поэтому дойдём до последнего частного — числа p_m — уже простого, и получим представление числа N в виде произведения простых чисел $p_1 p_2 \ldots p_m$.

Это всё очень просто и почти очевидно. Существенной является вторая часть теоремы, именно утверждение, что разложение числа N на простые множители единственно. Пред-

положим, что нам удалось двумя путями разложить число N на простые множители: первый метод дал разложение

$$N = p_1 p_2 \ldots p_r,$$

а второй — разложение

$$N = q_1 q_2 \ldots q_s,$$

где все p и q — простые числа.

Имеем, очевидно,

$$p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s. \qquad (*)$$

Левая часть этого равенства делится на p_1; значит, и правая, т. е. произведение $q_1 q_2 \ldots q_s$, на него разделится. Но в силу леммы один из множителей $q_1, q_2, \ldots, q_s$ должен разделиться на p_1. Допустим, что q_1 делится на p_1 (мы всегда можем перенумеровать числа q именно таким образом). Число q_1, будучи простым, делится только на единицу и на самого себя; следовательно,

$$q_1 = p_1.$$

Поделив обе части равенства $(*)$ на $p_1 = q_1$, получим:

$$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s.$$

Повторив это же рассуждение, получим:

$$q_2 = p_2,$$

а после нового сокращения придём к соотношению

$$p_3 p_4 \ldots p_r = q_3 q_4 \ldots q_s.$$

Точно так же найдём, что $q_3 = p_3$; $q_4 = p_4; \ldots; q_s = p_s$. Следовательно, множителей q столько же, сколько множителей p, каждое q равно некоторому p, т. е. оба разложения числа N на простые множители — тождественны.

Как практически разлагать числа на простые множители, читатели помнят из школьного курса. Так, например, разложение числа 8316 на простые множители выполняется следующим образом:

8316	2
4158	2
2079	3
693	3
231	3
77	7
11	11

$$8316 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 \cdot 11 = 2^2 \cdot 3^3 \cdot 7 \cdot 11.$$

Любое число N можно, таким образом, представить единственным образом в форме

$$N = p_1^{\alpha} p_2^{\beta} \dots p_m^{\lambda},$$

где $p_1, p_2, \dots, p_m$ — простые числа, а $\alpha, \beta, \dots, \lambda$ — некоторые показатели. Такое представление числа N иногда называют «каноническим разложением числа на сомножители».

Прежде чем расстаться с основной теоремой арифметики, сделаем ещё одно замечание. Мы определили простое число как такое, которое не имеет делителей, кроме самого себя и единицы. Далее, мы доказали, что если произведение нескольких чисел делится на простое число, то на него непременно разделится хотя бы один из множителей (лемма к основной теореме). Можно было бы доказать теорему, обратную этой лемме, именно — доказать, что всякое число, на которое обязательно делится хотя бы один множитель делящегося на него произведения нескольких чисел, не имеет иных множителей, кроме единицы и самого себя. Поэтому именно последнее свойство можно принять за определение простого числа. Так часто и делают: именно, простым числом называют число, на которое произведение может делиться только в том случае, если на него делится один из множителей; а число, не имеющее иных делителей, кроме себя и единицы, называют неразложимым. Пользуясь этими терминами, мы можем лемму сформулировать так: «Всякое неразложимое число — просто»; а обратную ей теорему так: «Всякое простое число — неразложимо». Обе эти теоремы можно соединить в одну: термины «простое число» и «неразложимое число» — значат одно и то же.

Искушённый различными арифметическими сюрпризами читатель не станет спрашивать: «зачем было вводить два термина, если они обозначают одно и то же?» Читатель чувствует, конечно, что здесь скрыт какой-то подвох. Ведь если есть «арифметики», в которых трижды три — четыре и $\mathbf{3 \cdot 3 = 10}$, то почему бы не быть и такой арифметике, в которой простые числа не являются неразложимыми, а неразложимые — простыми?..

Правда, такая арифметика кажется невероятной. Ведь именно лемма, смысл которой, по существу, и состоит в отождествлении понятий простоты и неразложимости, позволила нам доказать, что разложение любого числа на простые множители — единственно. Неужели возможны такие «арифметики», в которых одно и то же число разлагается на неразложимые

множители несколькими различными путями, т. е. имеет несколько канонических разложений?

Оказывается, что возможны. Существуют такие числовые системы, в которых разложение чисел на неразложимые множители не единственно, а на простые — не всегда возможно. Именно наличие этих систем и привело к необходимости различать числа простые и числа неразложимые. Правда, те числовые системы, которые привели к установлению этих понятий, очень сложны, и говорить здесь о них, несмотря на всю их важность для высших отделов теории чисел, невозможно. Но мы рассмотрим простой искусственный пример, который поможет разобраться в существе дела.

Рассмотрим ряд всех чётных положительных чисел, т. е. числа

2, 4, 6, 8, 10, 12, 14, 16, 18 и т. д.

Этот ряд многими свойствами напоминает натуральный ряд. Так, например, в нём всегда выполняются обычные сложение и умножение; это значит, что сумма и произведение двух или нескольких чётных чисел дают снова число чётное. Вычитание меньшего числа из большего тоже всегда возможно. Наконец, деление с остатком (последовательное вычитание) совершенно аналогично обычному делению с остатком.

В этой числовой системе некоторые числа имеют только два делителя (рассматриваются, разумеется, только чётные делители). Таковы числа 4, 6, 10, 14 и многие другие, делящиеся только на два и на себя. Любое число вида $4n+2$ (где n — обычное натуральное число) будет в нашей системе иметь только два делителя. Числа такого вида и будут, с точки зрения этой системы, числами неразложимыми. Число 2, подобное единице в ряду натуральных чисел, имеет только один делитель (самого себя). Наконец, числа 8, 12, 16, вообще числа вида $4n$, имеют несколько делителей.

Пока аналогия с обычным натуральным рядом полная. Но дальше начинается расхождение. Рассмотрим число 420, принадлежащее к нашей системе (чётное). Его можно двумя путями разложить на множители, неразложимые с точки зрения нашей системы. Действительно, имеем: $420 = 6 \cdot 70$ и $420 = 14 \cdot 30$. Числа 6, 14, 30 и 70 неразложимы (ни одно из них не является произведением двух чётных же чисел.) Следовательно, возможно два разложения числа 420 на неразложимые далее множители.

Какие же числа будут играть в нашей системе роль простых? Нетрудно сообразить, что это будут числа вида $2p$,

где p — простое число в обычном смысле (с точки зрения арифметики натурального ряда). Всякое простое число будет в нашей системе неразложимым. Но не всякое неразложимое будет простым. Числа 30, 42, 70, будучи неразложимыми, не будут простыми. Лемма, предшествующая основной теореме арифметики, для них не выполняется. Поэтому-то и получилась возможность разлагать число на неразложимые дальше множители несколькими способами.

Другим парадоксом этой числовой системы будет то, что не всякое число можно будет разложить на простые множители, т. е. представить в виде произведения чисел вида $2p$, где p — обычное первоначальное число. То же число 420, разложимое двумя путями на «неразложимые» множители, не может быть разложено на «простые» множители.

Чтобы закончить главу об эратосфеновом решете, скажем несколько слов о попытках найти общую формулу, которая давала бы при всех целых значениях величины n, входящей в неё, только простые числа. «Охота» за такими формулами началась ещё в классической древности и до сих пор не увенчалась успехом. Существуют различные формулы, содержащие некоторую величину n и дающие при различных целых значениях n простые числа. Но все они при некотором значении n «перестают действовать». Так, например, выражение

$$A = n^2 - 79n + 1601$$

даёт простые числа при любом n, не превосходящем 79. Например, при $n = 0$ мы получим $A = 1601$, при $n = 1$ будет $A = 1523$, при $n = 2$ будет $A = 1447$, — всё числа простые. Наконец, при $n = 39$ получим $A = 41$, — тоже простое число. Далее, при значениях n от 40 до 79 получаются те же значения A, но в обратном порядке: при $n = 40$ будет $A = 41, \ldots$, при $n = 78$ будет $A = 1523$, при $n = 79$ будет $A = 1601$. Но при $n = 80$ формула «отказывается служить»! В этом случае получим:

$A = 80^2 - 79 \cdot 80 + 1601 = 1681 = 41^2$ — число составное.

Вот ещё интересный пример *). Если в выражение

$$N = \frac{2^p + 1}{3}$$

*) Этот пример указан мне проф. А. Ф. Бермантом.

вместо p подставлять различные простые нечётные числа до 31, то значения N тоже будут простыми числами. Приводим табличку значений p и соответствующих значений N:

p	$N=\frac{2^p+1}{3}$	p	$N=\frac{2^p+1}{3}$
3	3	17	43 691
5	11	19	174 761
7	43	23	2 796 203
11	683	29	178 956 771
13	2731	31	715 827 883

Но формула «отказывается служить» при $p=37$; при этом $N=\frac{2^{37}+1}{3}=45\,812\,984\,491$ — число составное; оно разлагается на 2 простых множителя, именно:

$$45\,812\,984\,491 = 1777 \cdot 25\,781\,083.$$

В конце предыдущей главы мы говорили о знаменитой ошибке Ферма́, связанной с «охотой за формулой», дающей простые числа. Ферма́ считал, что при любом целом неотрицательном n выражение $2^{2^n}+1$ даёт простое число. Если математическое чутьё обмануло Ферма́ в том отношении, что его утверждение оказалось неправильным, то во всяком случае оно подвело его к очень важной и интересной проблеме. Оказалось, что если и не все числа вида $2^{2^n}+1$ являются простыми, то те из них, которые просты, обладают рядом замечательных свойств. Мы уже говорили, что ими занимался Эйлер, который и обнаружил ошибку Ферма́. Но самый любопытный результат, относящийся к этим числам, был получен Гауссом. Он связан с известной геометрической задачей — с построением помощью циркуля и линейки правильных многоугольников.

Уже в древности умели строить правильные трёх-, четырёх- и пятиугольники. Пользуясь возможностью делить любой угол пополам, без труда строили 8-, 16-, вообще 2^n-угольники; далее 6-, 12-, вообще $2^n \cdot 3$-угольники, 10-, 20-, вообще $2^n \cdot 5$-угольники. Отнимая от одной шестой части окружности одну десятую часть её, получали одну пятнадцатую: т. е. строили правильный вписанный пятнадцатиугольник, а за ним 30-, 60-, вообще $2^n \cdot 15$-угольники. Но все попытки по-

строить циркулем и линейкой правильный семи- или одиннадцатиугольник оканчивались неудачей.

Так продолжалось более двух тысяч лет. Более двух тысяч лет все попытки математиков построить циркулем и линейкой правильные многоугольники, которых не умели строить в древности, оканчивались неудачей. И только в 1796 г. девятнадцатилетний Гаусс неожиданно для всего математического мира нашёл способ построения циркулем и линейкой правильного семнадцатиугольника, а через пять лет опубликовал решение задачи о правильных многоугольниках в общем виде.

Гаусс доказал следующую замечательную теорему: циркулем и линейкой можно построить только такие правильные многоугольники (с простым числом сторон), у которых число сторон есть «простое число Ферма́», т. е. число вида $2^{2^n}+1$ (при тех значениях n, разумеется, при которых эта формула даёт простое число, что, как мы знаем, осуществляется не всегда). При $n=2$ получается правильный 17-угольник, при $n=3$ — правильный 257-угольник. Если число сторон правильного многоугольника — простое, но не является числом Ферма́, то его построение классическими средствами — циркулем и линейкой — невозможно. Правильные многоугольники с семью, с одиннадцатью, с тринадцатью сторонами построить циркулем и линейкой нельзя, а с 17 и 257 сторонами — можно!

Сам Гаусс, решив задачу в общем виде, дал разработанный до конца метод построения только для семнадцатиугольника. Следующими после 17 «числами Ферма́» являются 257 и 65 537. Законченное построение многоугольника с 257 сторонами дал Ришело (оно занимает 80 страниц), а многоугольник с 65 537 сторонами построил (по гауссову же методу) Гермес (рукопись занимает довольно объёмистый ручной чемодан и хранится в Гёттингене). Теория чисел оказалась любопытнейшим образом связанной с геометрией.

После смерти Гаусса ему поставили в Гёттингене памятник на пьедестале, имеющем форму правильной 17-угольной призмы.

ГЛАВА XII.

ЧАСТО ИЛИ РЕДКО?

Рассматривая эратосфеново решето, мы видим, что сначала промежутки между последовательными простыми числами невелики, но по мере продвижения в ряду натуральных чисел они, как правило, становятся больше и больше. Иными словами, по мере движения вдоль ряда натуральных чисел простые числа встречаются всё реже и реже (см. таблицу в конце этой книжки). Если среди чисел первого десятка мы находим четыре простых числа, то между 1001 и 1010 имеется только одно: 1009.

Евклид доказал, что простых чисел бесконечно много: как бы далеко мы ни зашли в натуральном ряду, нам будут попадаться простые числа. С другой стороны, «острова», состоящие сплошь из составных чисел, будут, как правило, становиться «длиннее», простые числа будут встречаться реже и реже. Каков же закон распределения простых чисел? Как узнать, например, сколько их содержится между 1 000 000 и 10 000 000, не пересчитывая их непосредственно? Эта задача принадлежит к числу труднейших, и до сего времени до конца она не решена. Сложность задач, связанных с распределением простых чисел, стала у математиков поговоркой. О ней знают и нематематики. Даже поэты упоминают о ней. Валерий Брюсов писал в одном из своих известных стихотворений:

...Но пред Эдипом загадка Сфинкса:
Простые числа всё не разгаданы ...

Разберём пример, который позволит лучше освоиться с самой постановкой вопроса. Рассмотрим бесконечную

геометрическую прогрессию:

$$\div\div 1,\ 2,\ 4,\ 8,\ 16,\ 32,\ \ldots,$$

где каждое последующее число в два раза больше предыдущего. Число членов здесь бесконечно. Как же расположены эти числа по отношению к ряду всех натуральных чисел? Легко видеть, что вначале они «сидят» очень густо. В промежутке от 1 до 10 мы имеем четыре таких числа (1, 2, 4, 8). В промежутке от 30 до 40 мы имеем уже только одно (32). Наконец, в промежутке от 1025 до 2025 (промежуток в целую тысячу) нет ни одного числа нашего ряда. Нетрудно показать, что если зайти в натуральном ряду достаточно далеко, то можно найти сколь угодно длинный числовой промежуток («остров»), не содержащий ни одного члена нашей прогрессии.

Всё это очень напоминает свойства простых чисел. Но есть и существенная разница. Закон распределения чисел ряда 1, 2, 4, 8, 16, ... в ряду натуральных чисел очень прост. Нетрудно написать формулу, позволяющую найти число членов этого ряда между двумя любыми натуральными числами. Действительно, число членов нашего ряда, не превосходящих числа N, равно увеличенной на единицу целой части двоичного логарифма числа N (читатель, знакомый с логарифмами, сам докажет это).

Наоборот, закон распределения чисел ряда

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ \ldots$$

(простых чисел) необычайно сложен: за длинной серией составных чисел может последовать серия, богатая простыми числами. Например, после промежутка в 11 составных чисел

998, 999, 1000, 1001, 1002, 1003, 1004, 1005, 1006, 1007, 1008

следует промежуток

1009, 1010, 1011, 1012, 1013, 1014, 1015, 1016, 1017, 1018, 1019

тоже из 11 чисел, содержащий три простых: 1009, 1013 и 1019.

Мы видели, что промежутки между простыми числами становятся всё больше и больше и делаются в конце концов сколь угодно длинными. Но встречаются, и тоже достаточно

Л. ЭЙЛЕР

далеко, неожиданные «сгустки» простых чисел. По соседству с тысячей, например, вслед за промежутком в 11 составных следует серия из 11 чисел, из которых 3 простых. Значит, на 22 числа приходится три простых — более 13 процентов, что совсем не так уж мало! Далее, есть основания полагать, что в ряду натуральных чисел как угодно далеко встречаются пары соседних простых чисел — «числа-близнецы», о которых уже упоминалось в предыдущей главе. Поэтому наличие огромных «островов», свободных от простых чисел, почти ничего не даёт нам для суждения о том, насколько часты последние среди всех натуральных чисел. И всё-таки...

И всё-таки уже Эйлер (1707—1783 гг.), замечательнейший математик XVIII столетия *), полагал, что простые числа встречаются «бесконечно реже, чем целые». Как понимать эти слова Эйлера? Они означают следующее: рассмотрим какое-нибудь натуральное число N, простое или составное. Рассмотрим все простые числа, не превосходящие N, т. е. числа

$$2,\ 3,\ 5,\ \ldots,\ p$$

(если N простое, то последним в этом ряду будет само $N = p$, в противном случае — некоторое число (простое), меньшее N). Допустим, что всего будет n простых чисел, не превосходящих N. Если, например, исходить из $N = 10$, то простыми числами, меньшими чем 10, будут 2, 3, 5, 7; таких чисел будет всего 4; значит, в этом примере $n = 4$. Читатель сам подсчитает, что при $N = 19$ $n = 8$; при $N = 30$ $n = 10$ и т. д.

Само число n мало что даёт для интересующей нас задачи, но отношение $\frac{n}{N}$ как раз и показывает, какую долю составляют простые числа, не превосходящие данного числа, по отношению ко всем натуральным числам, его не превосходящим. Отношение $\frac{n}{N}$ вполне характеризует густоту, или, выражаясь научным языком, «плотность» простых чисел среди натуральных. В следующей таблице приведён ряд значений N и соответствующих значений n и $\frac{n}{N}$. В последней строке

*) Эйлер более 30 лет жил и работал в России, являясь членом Петербургской Академии наук.

показано, какой процент составляет число n по отношению к N:

N	10	100	1000	100 000	1 000 000	1 000 000 000
n	4	25	168	9592	78 498	50 847 478
$\frac{n}{N}$	0,4	0,25	0,168	0,09592	0,078 498	0,050 847 478
%	40%	25%	$\approx 17\%$	$\approx 9{,}6\%$	$\approx 8\%$	$\approx 5\%$

(Значок $\approx$, поставленный перед некоторыми числами последней строки, заменяет слово «приблизительно»; например, $\approx 17\%$ читается: «приблизительно 17 процентов».) Мы видим, что «плотность», густота простых в ряду всех натуральных чисел становится меньше и меньше, если мы рассматриваем всё бóльшие и бóльшие числовые промежутки.

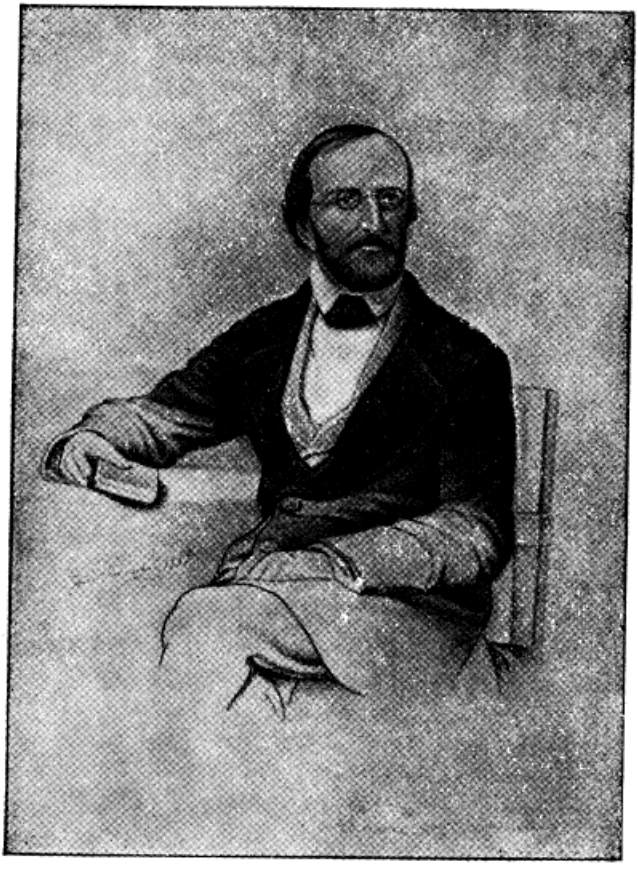
Слова Эйлера о том, что простые числа встречаются бесконечно реже, чем целые, надо понимать так: если рассматривать очень большое количество N последовательных натуральных чисел, то отношение $\frac{n}{N}$ будет очень малым числом; точнее, если мы выберем какое-нибудь очень малое значение для $\frac{n}{N}$, например одну миллионную, одну миллиардную и т. д., то всегда можно будет найти такое большое натуральное число, что при всех значениях N, которые его превосходят, наше требование будет выполняться, т. е. $\frac{n}{N}$ будет меньше, чем указанная малая дробь.

Эйлер доказал своё утверждение не вполне строго. Первое безупречное доказательство этого факта нашёл французский математик А. М. Лежандр, опубликовавший его в 1798 г.

Таким образом, вопрос о плотности простых чисел был решён в том смысле, что удалось установить неограниченное убывание этой плотности при возрастании числа N.

Установив это, математики поставили задачу — научиться вычислять n по данному N. Иными словами, они задались целью найти аналитическое выражение (формулу) количества простых чисел, не превосходящих данного натурального числа.

Эту задачу средствами современной математики решить ещё не удалось. Тогда её заменили двумя другими задачами: во-первых, стали искать формулу для отыскания n по заданному N, не точную, а приближённую, но такую, чтобы при больших N ошибка была ничтожно мала, и тем меньше, чем



Л. ДИРИХЛЕ

больше N; во-вторых, пытались найти те закономерности, которым подчиняются самые уклонения истинного закона распределения простых чисел от этой формулы. Обеим этим задачам уже полтораста лет, и занимались ими лучшие математики и за границей и у нас.

Первую простую формулу, приближённо выражающую число простых чисел, меньших, чем заданное натуральное число N, дал Лежандр; он получил её «путём подбора», причём она достаточно хорошо давала n для любых N, бо́льших чем 1000 и меньших чем 400 000. (Во времена Лежандра таблицы простых чисел были составлены только до $N = 400\,000$; в наше время эратосфеново решето доведено до $N = 9\,000\,000$.)

Вот формула Лежандра:

$$n = \frac{N}{2{,}3025 \log_{10} N - 1{,}08366},$$

причём берётся, разумеется, целая часть неправильной дроби, вычисленной по этой формуле. Рассмотрим табличку, дающую соответствующие различным N значения n, вычисленные по формуле Лежандра и подсчитанные непосредственно по таблице:

N	10	100	1000	10 000	100 000
n по Лежандру .	8	28	171	1230	9587
n истинное . . .	4	25	168	1229	9592

Начиная с $N = 1000$ «наблюдённые» и вычисленные значения n очень близки друг к другу, причём уклонения получаются «двусторонние»: при некоторых значениях N «наблюдённое» значение чуть больше вычисленного, при других—чуть меньше. Доказать справедливость формулы Лежандра в общем виде не удалось ни ему самому, ни другим математикам.

В середине прошлого века интерес к проблемам теории чисел в значительной мере усилился. Крупную роль сыграли работы Л. Дирихле (1805—1859 гг.). Дирихле работал главным образом в области математического анализа (так называются главы математики, посвящённые изучению непрерывно изменяющихся величин: дифференциальное исчисление, интегральное исчисление и т. п.). Но попутно он занимался и

теорией чисел и, прилагая к ней последовательно методы анализа (в этом — его большая заслуга), получил ряд интересных результатов. Мы говорили уже, что он доказал справедливость Великой теоремы Ферма́ при $n=5$ и $n=14$ и что им же доказано наличие бесконечного множества простых чисел в любой арифметической прогрессии со взаимно-простыми первым членом и разностью. Им же были получены важные результаты в учении о неопределённых уравнениях второй степени. С лёгкой руки Дирихле *) математики разных стран начали применять аналитические методы к изучению натуральных чисел.

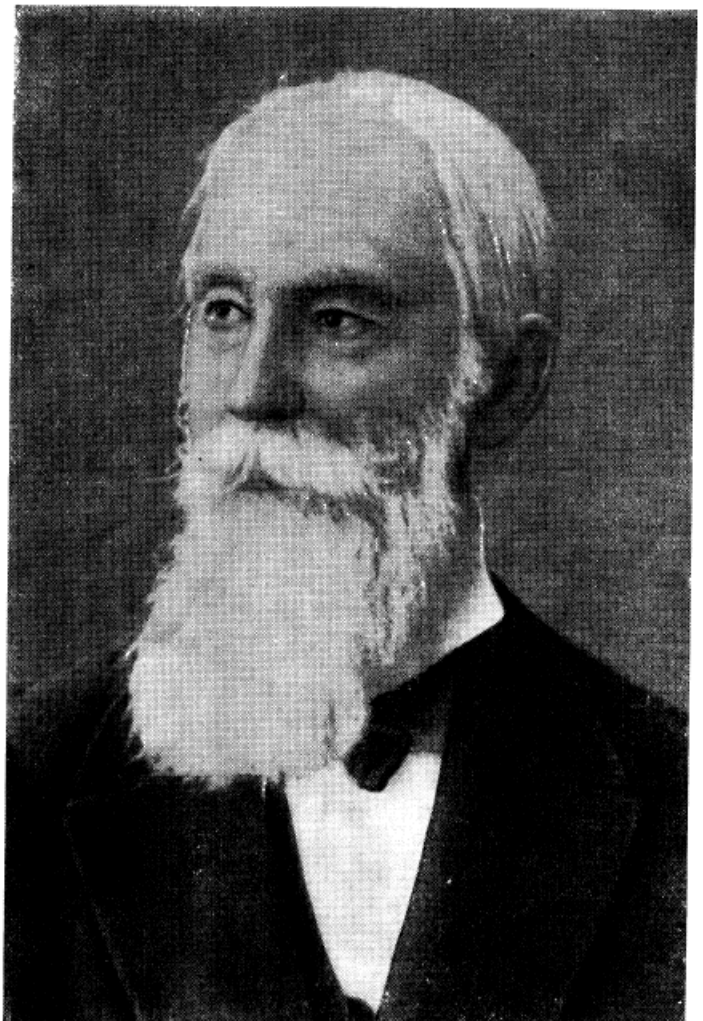
Французский математик Бертран, исходя из «опытов» с эратосфеновым решетом, высказал предположение, что между любым числом и числом, вдвое бо́льшим, имеется по крайней мере одно простое число. (Точнее, если $2x>7$, то между x и $2x-2$ всегда имеется простое число.) Он не сумел доказать это предложение, но, опираясь на него, доказал ряд важных теорем арифметики и алгебры. Предложение о том, что между числами x и $2x$ (при $x>1$) имеется по крайней мере одно простое число, получило у математиков наименование «постулата Бертрана» **). Доказать постулат Бертрана удалось в 1852 г. Чебышеву.

Пафнутий Львович Чебышев (1821—1894 гг.) по справедливости считается гордостью русской науки. Полвека работал он в самых разнообразных областях математики и везде получил выдающиеся результаты. Но самое важное в его деятельности — то, что он ставил совершенно новые вопросы, быстро привлекавшие к себе внимание многих математиков, в первую очередь — его учеников. Он создал русскую математическую школу, представители которой до сих пор занимают ведущее положение в науке.

Чебышеву не удалось найти формулу, которая позволяла бы по данному N точно находить соответствующее значение «плотности» $\frac{n}{N}$. Мы говорили уже, что и теперь, спустя сто лет после работ Чебышева по теории чисел, эта задача

*) Дирихле первый стал с и с т е м а т и ч е с к и применять к изучению натуральных чисел методы анализа непрерывных величин. Но отдельные результаты на этом пути получили до него Эйлер и Гаусс.

**) Латинское слово postulatum (постула́тум) значит «требование». В старых руководствах формулировка аксиом обычно начиналась словами: «потребуем, чтобы...».



П. Л. ЧЕБЫШЕВ

считается неразрешимой (средствами современной науки, разумеется: наука будущего безусловно её решит). Но Чебышев доказал, что при очень больших значениях N отношение $\frac{n}{N}$ мало отличается от величины $\frac{0{,}43429\ldots}{\log_{10} N}$, причём точность формулы тем больше, чем бóльшие значения N рассматриваются. Такого рода формулы, справедливые только приблизительно, но дающие тем бóльшую точность, чем больше значения входящих в них величин, носят название а с и м п т о т и ч е с к и х формул. Значит, можно сказать, что Чебышев дал асимптотическую формулу для плотности распределения простых чисел. Ему же удалось дать асимптотическую формулу для вычисления самого числа n простых чисел, не превосходящих данного N, но в эту формулу входит знак интеграла, и мы приводить её здесь не будем.

Чебышев справедливо считается создателем асимптотических законов распределения простых чисел. У него был, правда, предшественник, который чисто «опытным» путём — путём внимательного изучения эратосфенова решета — нашёл те же формулы, но доказать их правильности он не сумел и не публиковал их. Это был Гаусс.

После открытия асимптотических формул стал вопрос об оценке их точности и о тех закономерностях, которые можно подметить в самом уклонении «наблюдённых» значений числа n от вычисленных по этим формулам. Подобного рода вопросами занимались и сам Чебышев, и Адамар, и Ландау, а в последнее время — английские математики Гарди и Литтлвуд. Вопрос об отклонениях от формул Чебышева оказался чрезвычайно трудным. Но и здесь кое-что удалось сделать.

В приводимой здесь таблице в первой строке, отмеченной буквой N, даны значения натуральных чисел, а во второй, отмеченной буквой A, — соответствующие им значения для n, вычисленные по формуле Чебышева; наконец, в третьей строке — точные значения n

N	2	5	10	100	1 000	10 000	100 000	1 000 000	10 000 000	100 000 000
A	1	4	6	29	178	1246	9630	78 628	664 918	5 762 209
n	1	3	4	25	168	1229	9592	78 498	664 579	5 761 455

Мы видим, что разница между A и n с ростом N возрастает, но доля, которую эта разница составляет от числа N, убывает и убывает быстро. При $N = 1000$, например,

$$A - n = 178 - 168 = 10;$$

эти 10 составляют $\frac{1}{10}$ процента от тысячи. При $N = 1\,000\,000$ будем иметь:

$$A - n = 78\,628 - 78\,498 = 130$$

(больше чем при $N = 1000$); но эти 130 по отношению ко всему рассматриваемому миллиону составляют лишь $0{,}013\,\%$ — почти в 8 раз меньше, чем в случае $N = 1000$. Именно это отношение характерно для оценки качества приближённого соотношения. Мы видим, что для формулы Чебышева это отношение очень мало; стало быть, она хороша: чем больше рассматриваемые числа, тем эта формула лучше (асимптотический закон).

С другой стороны, мы замечаем, что A всегда больше n, и это справедливо не только для чисел, помещённых нами в табличку, но и для всех чисел N, для которых были подсчитаны соответствующие им A и n. Казалось естественным ожидать, что формула Чебышева даёт всегда несколько «завышенный» результат. До 1914 г. было много попыток доказать это утверждение, т. е. доказать, что $A \geqslant n$ при любом N. Но в 1914 г. Литтлвуд показал, что существуют такие числа (такие значения N), при которых n должно быть обязательно больше A, причём в дальнейшем при ещё больших значениях N будут встречаться и такие N, при которых $A > n$, и такие, при которых $n > A$; иными словами, уклонения от чебышевской формулы будут не только ничтожно малы, но будут носить совершенно случайный характер, давая результат, то чуть-чуть больший, то чуть-чуть меньший истинного.

Каково же то наименьшее натуральное число, для которого чебышевская формула даёт результат, меньший чем нужно? Товарищ Литтлвуда по работе, математик Гарди, показал, что это число невероятно велико. Оно не меньше чем 10^{700}. Казалось при этом, что подойти как-то ближе к этому числу невозможно. И только совсем недавно, в 1933 г., английскому математику Скьюзу удалось показать, что (если сделать некоторые дополнительные предположения) можно оценить то число, при котором впервые в числовом ряду чебышевская

формула даёт результат, меньший истинного. Это число равно приблизительно $10^{10^{10^{9.4}}}$.

Число, данное Скьюзом, значительно превосходит все ранее указанные числовые гиганты и в этом смысле его можно назвать «числом-рекордсменом». Именно, число 9^{9^9}, о котором говорилось в первой главе, и даже такое огромное число как $10^{8 \cdot 10^{16}}$, до которого дошёл в своём «Псаммите» Архимед, очень и очень малы по сравнению со скьюзовским гигантом.

ГЛАВА XIII.

ПРОБЛЕМА ГОЛЬДБАХА.

В предыдущей главе мы познакомились с вопросом распределения простых чисел среди всех натуральных. Оказалось, что простые числа, расположенные сравнительно густо в начале натурального ряда, в дальнейшем становятся всё реже и реже, промежутки между ними становятся всё больше и больше. В этих промежутках попадаются числа, представляющие собой сумму двух простых чисел. Вот, например, числа первого десятка: 1 (в счёт не идёт); 2 (простое); 3 (простое); 4 ($4 = 2 + 2$ — сумма двух простых); 5 (простое); 6 ($3 + 3$ — сумма двух простых); 7 (простое); 8 ($3 + 5$ — сумма двух простых); 9 ($2 + 7$ — сумма двух простых); 10 ($3 + 7$ — сумма двух простых). Мы видим, что все числа первого десятка или являются простыми, или представляют собой сумму двух простых. Но уже 27 представить в виде такой суммы не удаётся. Зато 27 можно записать как сумму трёх простых слагаемых: $27 = 3 + 11 + 13$. Спрашивается, для какого натурального числа трёх простых слагаемых не будет уже достаточно? Какое наименьшее число будет суммой не меньше чем четырёх, пяти и т. д. простых слагаемых?

Подобные задачи можно ставить применительно не только к простым числам. Математиков давно интересует вопрос, как заданное число записать в виде суммы некоторого числа квадратов. Если это возможно, то сколькими способами осуществляется разложение? Те же вопросы можно поставить для разложения числа на сумму кубов и т. д. Возникает своеобразная область теории чисел, в которой вместо делителей и множителей приходится иметь дело со слагае-

мыми и суммами. Её называют аддитивной теорией чисел, производя название от латинского слова additio (адди́цио), что значит «сложение». Что касается той части теории чисел, которая имеет дело с множителями и делителями (учение о делимости и т. д.), то она носит название мультипликативной теории чисел (от латинского multiplicatio — мультиплика́цио, — что значит «умножение»).

Вернёмся к простым числам, именно к задаче о представлении любого числа в виде суммы некоторого количества простых. Этой задачей более двухсот лет тому назад занялся член Петербургской Академии наук Хр. Гольдбах. Он перепробовал очень много чисел, пытаясь разложить их на сумму простых, и пришёл к убеждению, что трёх слагаемых всегда достаточно. Не сумев доказать это предложение, не найдя даже путей к доказательству, он написал о нём своему другу Эйлеру, с которым уже без малого 15 лет переписывался и который был тогда в зените славы. В письме от 7 июня 1742 г. Гольдбах сообщил Эйлеру, что рискует высказать следующее предположение: «любое число, большее пяти, представляет собой сумму трёх простых». Эйлер ответил, что считает безусловно верной теоремой утверждение, что каждое чётное число есть сумма двух простых. Отсюда, как простое следствие, получается утверждение Гольдбаха (почему?). Впрочем, и Эйлер доказательства не дал.

Итак, поставлена следующая задача (её называют «проблемой Гольдбаха»): требуется доказать или опровергнуть предложение: «всякое число, большее единицы, является суммой не более трёх простых чисел». Ни современники Гольдбаха и Эйлера, ни даже математики прошлого — XIX — столетия почти ничего не смогли сделать для решения этой задачи. Правда, Г. Кантор, один из оригинальнейших математиков прошлого века, терпеливо перепробовал все чётные числа от 2 до 1000, а Обри — от 1000 до 2000; они убедились, что в этих пределах любое чётное число является суммой двух простых. В 1911 г. Е. Меле показал, что подавляющее число чётных чисел от 4 до 9 000 000 являются суммами двух простых; исключений может быть не больше четырнадцати (т. е. для 4 499 986 чётных чисел утверждение Гольдбаха наверняка справедливо). Наконец, на рубеже XX века появляется ряд работ, пытающихся наметить пути решения этой проблемы или связать её с другими задачами математики. Но для строгого её доказательства ничего сделать не

удалось, и в 1912 г. крупнейший знаток теории чисел Э. Ландау высказал на международном конгрессе математиков предположение, что эта задача средствами современной математики вообще неразрешима!..

В 1923 г. двум английским математикам — Гарди и Литлвуду, о которых мы уже говорили, — удалось добиться некоторого сдвига в попытках найти решение гольдбаховской задачи. Им удалось связать проблему Гольдбаха с одной из труднейших и интереснейших задач специальной главы высшей математики, называемой теорией аналитических функций. Эта задача тоже до конца не решена, но открывшаяся связь между двумя, казалось бы, разнородными ветвями науки оказалась плодотворной и привела к ряду открытий.

Решительный перелом наступил в 1930 году. Советскому математику Льву Генриховичу Шнирельману (1905—1938 гг.), талантливому учёному, удалось так видоизменить задачу, что с помощью им же придуманных путей он сумел её решить. Именно, видя бесплодность попыток доказать утверждение Гольдбаха в его первоначальном виде, Шнирельман поставил родственную задачу, на вид более сложную, но по существу значительно более простую. Он, как говорят математики, «ослабил» требования задачи Гольдбаха. Гольдбах требует, чтобы каждое натуральное число являлось суммой не более трёх простых. Можно потребовать, чтобы каждое натуральное число было суммою не более четырёх, пяти, ..., ста простых. Эти требования, очевидно, слабее гольдбаховских: число, разложимое в сумму ста, может не разлагаться в сумму трёх простых.

Наконец, можно, что и сделал Шнирельман, поставить вопрос так: существует ли какое-то вполне определённое, но нам неизвестное целое число (обозначим его буквою C), такое, что любое натуральное число можно представить в виде суммы не более чем C простых слагаемых?

Иными словами, каково бы ни было натуральное число N, всегда можно написать

$$N = p_1 + p_2 + p_3 + \ldots + p_n,$$

где p_1, p_2, ..., p_n — простые числа, а n наверное меньше (или в крайнем случае равно) C. Если удастся доказать, что $C = 3$, то утверждение Гольдбаха будет доказано. Эту «ослабленную» теорему Гольдбаха Шнирельману удалось доказать полностью. Само, пока неизвестное, число C с тех пор

Л. Г. ШНИРЕЛЬМАН

И. М. ВИНОГРАДОВ

называют «числом Шнирельмана» или «константой Шнирельмана» (слово constanta — константа — значит по-латыни «постоянная»). Значит, утверждение Гольдбаха можно сформулировать и так: «константа Шнирельмана равна трём». Но этого мало. Самый точный анализ метода Шнирельмана, сделанный разными математиками (Романов, Ландау, Хейльборн, Риччи), позволил получить оценку константы Шнирельмана; будучи очень большой, она постепенно была уменьшена до 67.

Отсюда до гольдбаховской тройки, конечно, очень далеко! Но важно то, что это доказано для л ю б ы х чисел, сколь бы велики они ни были. Относительно какого-нибудь числа вроде

$$835\,042\,000\,000\,000\,000\,000\,000$$

или нашего знакомца 9^{9^9}, для записи которого нужно 30 томов, тоже можно утверждать, что 67 простых слагаемых достаточно для их представления. Даже скьюзовский гигант $10^{10^{10^{34}}}$ можно на основании доказательства Шнирельмана представить в виде суммы не более 67 простых слагаемых (некоторые из этих слагаемых сами неизмеримо велики: гораздо больше числа 9^{9^9}). Значит, результат Шнирельмана является огромным достижением; а главное — проложены новые пути, найдены новые способы подхода к решению старой задачи. Значит, можно ждать и новых результатов. Так оно и получилось.

В 1937 г. академик Иван Матвеевич Виноградов, ныне Герой Социалистического Труда и лауреат Сталинской премии, тогда уже известный всему учёному миру своими работами по аддитивной теории чисел, почти полностью решил проблему Гольдбаха, ещё так недавно считавшуюся недоступной.

Результат, полученный И. М. Виноградовым, можно сформулировать так: для всех достаточно больших нечётных чисел проблема Гольдбаха решена полностью; или так: константа Шнирельмана для достаточно больших нечётных чисел не превосходит трёх.

Почему же решение И. М. Виноградова нельзя считать полным, окончательным решением проблемы Гольдбаха; откуда взялось то злополучное «почти», о котором упоминалось выше? Дело в том, что Эйлер и Гольдбах утверждали, — и это для сравнительно небольших чисел подтвердилось на опыте, — что любое чётное число является суммой двух простых. Отсюда уже, как следствие, вытекало, что любое нечётное есть сумма не более чем трёх простых. Виноградов же

доказал именно последнее утверждение о нечётных числах; отсюда непосредственно следует, что для любого чётного достаточно четырёх простых слагаемых; но достаточно ли двух, — этот вопрос остаётся открытым. Кроме того, по Виноградову, утверждение Гольдбаха справедливо для всех достаточно больших нечётных чисел, иными словами, начиная с некоторого большого числа, которое некоторое время оставалось неизвестным.

В 1939 г. оно было вычислено молодым советским математиком К. Г. Бороздкиным. Это большое число может быть записано так:

$$e^{e^{e^{41,\,96}}},$$

где число e есть основание натуральных логарифмов: $e=2{,}7182\ldots$ Остаётся значительно снизить найденное К. Г. Бороздкиным число и тогда непосредственно проверить все меньшие числа, — работа, которой занимались Кантор и Обри в пределах первых двух тысяч.

Мы задержались на проблеме Гольдбаха не только потому, что она очень интересна с разных точек зрения, но и потому ещё, что ею смело может гордиться русская наука. Эта проблема была поставлена в Петербурге — нынешнем Ленинграде; первый сдвиг в её решении сделал Л. Г. Шнирельман, и решил её академик — И. М. Виноградов.

ТАБЛИЦА ПРОСТЫХ ЧИСЕЛ, НЕ ПРЕВОСХОДЯЩИХ 6000.

2	331	751	1217	1697	2221	2719	3299	3803	4357	4943	5503
3	337	757	1223	1699	2237	2729	3301	3821	4363	4951	5507
5	347	761	1229	1709	2239	2731	3307	3823	4373	4957	5519
7	349	769	1231	1721	2243	2741	3313	3833	4391	4967	5521
11	353	773	1237	1723	2251	2749	3319	3847	4397	4969	5527
13	359	787	1249	1733	2267	2753	3323	3851	4409	4973	5531
17	367	797	1259	1741	2269	2767	3329	3853	4421	4987	5557
19	373	809	1277	1747	2273	2777	3331	3863	4423	4993	5563
23	379	811	1279	1753	2281	2789	3343	3877	4441	4999	5569
29	383	821	1283	1759	2287	2791	3347	3881	4447	5003	5573
31	389	823	1289	1777	2293	2797	3359	3889	4451	5009	5581
37	397	827	1291	1783	2297	2801	3361	3907	4457	5011	5591
41	401	829	1297	1787	2309	2803	3371	3911	4463	5021	5623
43	409	839	1301	1789	2311	2819	3373	3917	4481	5023	5639
47	419	853	1303	1801	2333	2833	3389	3919	4483	5039	5641
53	421	857	1307	1811	2339	2837	3391	3923	4493	5051	5647
59	431	859	1319	1823	2341	2843	3407	3929	4507	5059	5651
61	433	863	1321	1831	2347	2851	3413	3931	4513	5077	5653
67	439	877	1327	1847	2351	2857	3433	3943	4517	5081	5657
71	443	881	1361	1861	2357	2861	3449	3947	4519	5087	5659
73	449	883	1367	1867	2371	2879	3457	3967	4523	5099	5669
79	457	887	1373	1871	2377	2887	3461	3989	4547	5101	5683
83	461	907	1381	1873	2381	2897	3463	4001	4549	5107	5689
89	463	911	1399	1877	2383	2903	3467	4003	4561	5113	5693
97	467	919	1409	1879	2389	2909	3469	4007	4567	5119	5701
101	479	929	1423	1889	2393	2917	3491	4013	4583	5147	5711
103	487	937	1427	1901	2399	2927	3499	4019	4591	5153	5717
107	491	941	1429	1907	2411	2939	3511	4021	4597	5167	5737
109	499	947	1433	1913	2417	2953	3517	4027	4603	5171	5741
113	503	953	1439	1931	2423	2957	3527	4049	4621	5179	5743
127	509	967	1447	1933	2437	2963	3529	4051	4637	5189	5749
131	521	971	1451	1949	2441	2969	3533	4057	4639	5197	5779
137	523	977	1453	1951	2447	2971	3539	4073	4643	5209	5783
139	541	983	1459	1973	2459	2999	3541	4079	4649	5227	5791
149	547	991	1471	1979	2467	3001	3547	4091	4651	5231	5801
151	557	997	1481	1987	2473	3011	3557	4093	4657	5233	5807
157	563	1009	1483	1993	2477	3019	3559	4099	4663	5237	5813
163	569	1013	1487	1997	2503	3023	3571	4111	4673	5261	5821
167	571	1019	1489	1999	2521	3037	3581	4127	4679	5273	5827
173	577	1021	1493	2003	2531	3041	3583	4129	4691	5279	5839
179	587	1031	1499	2011	2539	3049	3593	4133	4703	5281	5843
181	593	1033	1511	2017	2543	3061	3607	4139	4721	5297	5849
191	599	1039	1523	2027	2549	3067	3613	4153	4723	5303	5851
193	601	1049	1531	2029	2551	3079	3617	4157	4729	5309	5857
197	607	1051	1543	2039	2557	3083	3623	4159	4733	5323	5861
199	613	1061	1549	2053	2579	3089	3631	4177	4751	5333	5867
211	617	1063	1553	2063	2591	3109	3637	4201	4759	5347	5869
223	619	1069	1559	2069	2593	3119	3643	4211	4783	5351	5879
227	631	1087	1567	2081	2609	3121	3659	4217	4787	5381	5881
229	641	1091	1571	2083	2617	3137	3671	4219	4789	5387	5897
233	643	1093	1579	2087	2621	3163	3673	4229	4793	5393	5903
239	647	1097	1583	2089	2633	3167	3677	4231	4799	5399	5923
241	653	1103	1597	2099	2647	3169	3691	4241	4801	5407	5927
251	659	1109	1601	2111	2657	3181	3697	4243	4813	5413	5939
257	661	1117	1607	2113	2659	3187	3701	4253	4817	5417	5953
263	673	1123	1609	2129	2663	3191	3709	4259	4831	5419	5981
269	677	1129	1613	2131	2671	3203	3719	4261	4861	5431	5987
271	683	1151	1619	2137	2677	3209	3727	4271	4871	5437	
277	691	1153	1621	2141	2683	3217	3733	4273	4877	5441	
281	701	1163	1627	2143	2687	3221	3739	4283	4889	5443	
283	709	1171	1637	2153	2689	3229	3761	4289	4903	5449	
293	719	1181	1657	2161	2693	3251	3767	4297	4909	5471	
307	727	1187	1663	2179	2699	3253	3769	4327	4919	5477	
311	733	1193	1667	2203	2707	3257	3779	4337	4931	5479	
313	739	1201	1669	2207	2711	3259	3793	4339	4933	5483	
317	743	1213	1693	2213	2713	3271	3797	4349	4937	5501	

ОГЛАВЛЕНИЕ

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1954