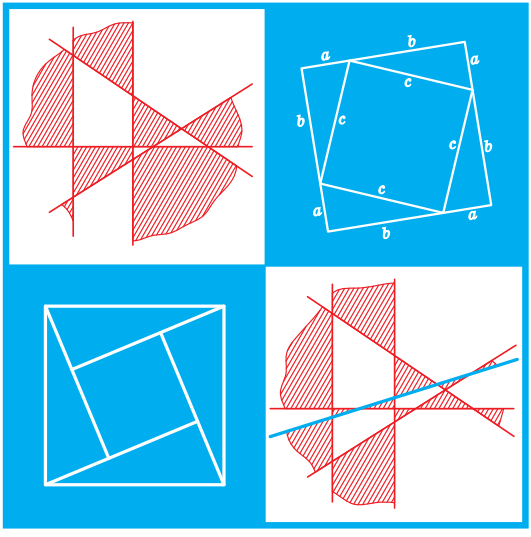
Библиотека
«Математическое просвещение»

В. А. Успенский

ПРОСТЕЙШИЕ ПРИМЕРЫ МАТЕМАТИЧЕСКИХ ДОКАЗАТЕЛЬСТВ



Издательство Московского центра
непрерывного математического образования
Москва • 2012

Серия основана в 1999 году.

Библиотека
«Математическое просвещение»

Выпуск 34

В. А. Успенский

ПРОСТЕЙШИЕ ПРИМЕРЫ МАТЕМАТИЧЕСКИХ ДОКАЗАТЕЛЬСТВ

Второе издание, стереотипное

Издательство Московского центра
непрерывного математического образования
Москва • 2012

УДК 511.1
ББК 22.130
У77

Успенский В. А.

У77 Простейшие примеры математических доказательств. — 2-е изд., стереотипное. — М.: Изд-во МЦНМО, 2012. — 56 с.

ISBN 978-5-94057-879-6

В брошюре доступным неспециалистам языком рассказывается о некоторых из основополагающих принципов, на которых строится наука математика: чем понятие математического доказательства отличается от понятия доказательства, принятого в других науках и в повседневной жизни, какие простейшие приёмы доказательства используются в математике, как менялось со временем представление о «правильном» доказательстве, что такое аксиоматический метод, в чём разница между истинностью и доказуемостью.

Для очень широкого круга читателей, начиная со школьников старших классов.

Первое издание книги вышло в 2009 году.

ББК 22.130

Серия «Библиотека „Математическое просвещение“»

Успенский Владимир Андреевич

ПРОСТЕЙШИЕ ПРИМЕРЫ
МАТЕМАТИЧЕСКИХ ДОКАЗАТЕЛЬСТВ

Выпуск 34

Серия основана в 1999 году

Редактор *М. Г. Быкова*
Тех. редактор *Д. Е. Щербаков*

Подписано к печати 13/IX 2011 г. Формат $60 \times 84\,{}^{1}\!/_{16}$. Бумага офсетная № 1.
Печать офсетная. Объём 3,50 (вкл.) печ. л. Тираж 2000 экз. Заказ .

Издательство Московского центра непрерывного математического образования.
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241 74 83.

Отпечатано в ППП «Типография „Наука“».
121099, Москва, Шубинский пер., 6.

ISBN 978-5-94057-879-6

МАТЕМАТИКА И ДОКАЗАТЕЛЬСТВА

Даже незнакомый с математикой человек, взяв в руки книгу по математике, может, как правило, сразу определить, что эта книга действительно по математике, а не по какому-нибудь другому предмету. И дело не только в том, что там обязательно будет много формул: формулы есть и в книгах по физике, по астрономии или по мостостроению. Дело в том, что в любой серьёзной книге по математике непременно присутствуют *доказательства*. Именно доказуемость математических утверждений, наличие в математических текстах доказательств — вот что нагляднее всего отличает математику от других областей знания.

Первую попытку охватить единым трактатом всю математику предпринял древнегреческий математик Евклид в III веке до нашей эры. В результате появились знаменитые «Начала» Евклида. А вторая попытка состоялась только в XX веке н. э., и принадлежит она французскому математику Николя́ Бурбаки́[1], начавшему в 1939 году издавать многотомный трактат «Начала математики». Вот какой фразой открывает Бурбаки свой трактат: «Со времён греков говорить „математика“ — значит говорить „доказательство“». Таким образом, «математика» и «доказательство» — эти два слова объявляются почти синонимами.

Казалось бы, можно возразить, что доказательства встречаются и в других сферах — скажем, в юриспруденции. Например, в суде каждая из спорящих сторон предъявляет свои доказательства (причём доказательства одной стороны нередко противоречат доказательствам другой стороны). Однако все согласны, что математические доказательства гораздо убедительнее тех, которые произносятся в судах.

Доказательства, собственно, встречаются во всех науках, даже в науках гуманитарных. Приведу два примера: первый из исторической науки, второй — из филологии.

[1] На самом деле такого математика не существует. Николя́ Бурбаки́ — это коллективный псевдоним группы математиков, подобно тому как «Козьма Прутков» — коллективный псевдоним группы писателей (но только, в отличие от группы Бурбаки, группы постоянного состава). Сказанное не послужило препятствием ни тому, чтобы г-н Бурбаки имел свой почтовый ящик на Международном съезде математиков в Москве в 1966 г. (причём почта из ящика исправно забиралась), ни тому, чтобы он получил гонорар, выписанный ему издательством «Мир» за осуществлённое в 1965 г. издание русского перевода первого тома его трактата. Рассказывают, что когда Американское математическое общество выпустило справочник, в котором Бурбаки был назван псевдонимом группы математиков, возмездие последовало незамедлительно: в одной из публикаций Бурбаки президент Американского математического общества был назван точно так же.

Первые шаги в науке великого российского математика Андрея Николаевича Колмогорова (1903—1987) были сделаны не в математике, а в истории[1] и относились к истории Новгородской земли XV века.

Колмогоровские разыскания содержали, в числе других достижений, ответ на вопрос, как брался налог с селений Новгородской земли — с селения в целом или же с каждого его двора. Опровергая господствующее мнение, Колмогоров доказал, что налог брался с селения в целом. Доказательство состояло в том, что в противном случае правило налогообложения должно было бы быть чересчур сложным. Проведённый Колмогоровым анализ новгородских писцовых книг, в которых наряду с другими сведениями записывались сведения о налогообложении, привёл к следующим результатам. Налог с больших селений всегда брался в целых единицах, к тому же в большинстве случаев — в круглых цифрах. Налог со средних селений брался, в основном, также в целых единицах. Налог с небольших селений мог составлять как целое, так и дробное число налоговых единиц, но это дробное число всегда имело вид целого числа с половиной. Более того, во многих случаях, когда налог с небольших селений брался в целых единицах, дворов в селении оказывалось больше, чем число налоговых единиц, взымаемых с селения. Кажется невероятным, чтобы налог был подворным и его ставки были столь хитроумны, чтобы достигнуть таких числовых эффектов!

Теперь пример из филологии. Долгое время предметом ожесточённых спекуляций служил вопрос о подлинности «Слова о полку Игореве», то есть вопрос о том, создано ли оно в XII—XIV веках, что и означает подлинность, или же является подделкой, относящейся, скорее всего, к XVIII веку. Андрей Анатольевич Зализняк (только личное знакомство с ним мешает мне назвать его великим лингвистом) доказал подлинность «Слова». Доказательство опирается на анализ раскрытых Зализняком тончайших закономерностей древнерусского языка. Невероятно, чтобы мог

[1] Над рукописями своих исторических исследований Колмогоров начал работать, когда ему было семнадцать с половиной лет, а закончил их в 1922 г., когда ему ещё не было девятнадцати. В то время он был студентом Московского университета. Эти рукописи долгое время считались утерянными, они были найдены и опубликованы лишь после смерти Колмогорова в книге: *Колмогоров А. Н. Новгородское землевладение XV в. Бассалыго Л. А. Комментарий к писцовым книгам Шелонской пятины*. — М.: Физматлит, 1994. (Да, книга имеет такое сложное библиографическое описание. Она состоит из двух самостоятельных сочинений, имеющих каждое своего автора.) После опубликования колмогоровские рукописи по истории получили высокую оценку специалистов.

существовать такой фальсификатор, который не только знал бы эти закономерности, иные из коих были обнаружены лишь недавно, но и скрыл своё знание от современников! (Это при том, что, как известно, незнание можно скрыть, знание скрыть невозможно.)

В обоих наших рассказах о доказательствах в гуманитарных науках мы употребили слово *невероятно*, а не слово *невозможно*. Дело в том, что в обоих случаях всё-таки остаётся некоторая, пусть весьма малая, вероятность того, что в действительности налог был подворным, а «Слово» — подделкой. Требуется ли ещё уменьшать эту вероятность? На мой взгляд, в приведённых примерах не требуется — но этот взгляд субъективен. И если кто-нибудь потребует сделать вероятность опровержения открытий, сделанных Колмогоровым и Зализняком, ещё ничтожнее, против этого будет трудно возразить. Вот, например, как реагировал на сообщение Колмогорова известный историк С. В. Бахрушин, когда работа была рассказана на занятиях его семинара в Московском университете. Пишет известный археолог, руководитель новгородской археологической экспедиции В. Л. Янин:

> Когда работа была доложена им [Колмогоровым] на семинаре, руководитель семинара профессор С. В. Бахрушин, одобрив результаты, заметил, однако, что выводы молодого исследователя не могут претендовать на окончательность, так как «в исторической науке каждый вывод должен быть обоснован несколькими доказательствами»(!). Впоследствии, рассказывая об этом, Андрей Николаевич добавлял: «И я решил уйти в науку, в которой для окончательного вывода достаточно одного доказательства». История потеряла гениального исследователя, математика навсегда приобрела его.

Думается, позиция Бахрушина имеет следующее объяснение. Он привык к тому, что обычно применяемые в исторической науке доказательства допускают, каждое в отдельности, ощутимую вероятность того, что доказанное утверждение не соответствует действительности; а посему, для уменьшения этой вероятности, требуется несколько доказательств. Возможно, он впервые услышал доказательство, уже в единственном числе делающее указанную вероятность пренебрежимо малой, — услышал, но не осознал.

Вернёмся, однако, к математике. Математические доказательства повсеместно признаются эталоном бесспорности. Выражения вроде «я тебе докажу математически», встречающиеся в русской

классической литературе, призваны продемонстрировать доказательство, которое нельзя оспорить.

Но что же такое доказательство? Доказательство — это рассуждение, которое убеждает того, кто его воспринял, настолько, что он делается готовым убеждать других *с помощью этого же рассуждения*. Так понимается доказательство всюду — и в истории, и в филологии, и в математике. Во избежание недоразумений и возможного возмущения просвещённых читателей (если таковые найдутся среди читателей этого текста) отметим, что есть и другое понимание того, что такое доказательство. По Бурбаки, например, доказательство — это цепочка символов, организованная по определённым правилам. Мы обсудим это другое понимание в заключительном разделе книги. Полагаем, однако, что наше понимание не является чем-то оригинальным, а отражает то стандартное употребление слова *доказательство*, которое имеет место и в средней, и в высшей школе. Те математические объекты, которые называет доказательствами Бурбаки, разумно называть *формальными доказательствами* — в отличие от содержательных, психологических доказательств, о которых мы здесь говорим. Формальные доказательства составляют предмет изучения математической логики. Заметим ещё, что, на наш взгляд, и Бурбаки не может избежать содержательных доказательств: ведь чтобы убедиться, что данная цепочка символов является формальным доказательством, требуется провести содержательное рассуждение, то есть именно психологическое доказательство.

Отличие математического доказательства от доказательств в других науках состоит в том, что в математике порог убедительности значительно выше. Можно сказать, что математические и нематематические доказательства имеют разные амбиции. Нематематические доказательства претендуют на то, чтобы убедить в следующем: доказываемое утверждение имеет место с подавляющей вероятностью, а предположение, что это не так, невероятно. Математические доказательства претендуют на то, чтобы убедить в следующем: доказываемое утверждение имеет место с необходимостью, а предположение, что это не так, невозможно. Так, уже отмечалось, что в приведённых выше примерах из истории и филологии оставалась возможность, пусть совершенно невероятная, что в действительности дело обстояло иным образом. И даже демонстрация нескольких доказательств, как того требовал Бахрушин, всего лишь повысила бы степень невероятности, но не превратила бы её в невозможность. В мате-

матических же доказательствах *невероятность* противоположного эффекта — то есть допущения того, что доказанное утверждение неверно, — заменяется на *невозможность*. Поэтому в математических доказательствах убедительность должна быть абсолютной, не оставляющей никакой возможности для противоположного суждения.

Предвидим протест или, по меньшей мере, удивление некоторых читателей. Как же так, такое важное математическое понятие, как доказательство, а имеет такое нечёткое определение — да и вообще не определение, а описание, пояснение. На это у нас два возражения. Во-первых, даже и в математике всё определить невозможно: ведь одни понятия определяются через другие, другие через третьи, и т. д. Но этот процесс не может продолжаться бесконечно. Поэтому мы вынуждены где-то остановиться. Во-вторых, понятие доказательства не есть математическое понятие (подобное, скажем, понятию действительного числа или понятию многоугольника); по отношению к математике оно не *внутреннее*, а *внешнее* и принадлежит не математике, а психологии (и отчасти лингвистике). Однако невозможно представить себе современную математику без повсеместного использования этого понятия.

Можно ли предложить разумную классификацию всевозможных доказательств, то есть убедительных рассуждений? Вряд ли. Тем более, что доказательство, как правило, состоит из нескольких (иногда очень многих) этапов, и на каждом этапе применяется свой способ убеждения. Можно, однако, среди схем доказательства выделить несколько часто повторяющихся; ниже некоторые из таких схем будут изложены. Чтобы не дезориентировать читателя, сделаем два предупреждения.

Предупреждение первое. Было бы глубоким заблуждением считать, что других методов доказательства не бывает! Да и само выделение схем достаточно условно. Ведь нередко случается, что одна схема «залезает» внутрь другой — скажем, внутри доказательства по индукции может встретиться доказательство от противного или наоборот.

Предупреждение второе. Все примеры, которые будут приведены ниже, содержат лишь очень простые и короткие доказательства. Многие доказательства, встречающиеся в математической науке, и гораздо сложнее, и гораздо длиннее: их длина может измеряться десятками, сотнями и даже тысячами страниц. Поясним, откуда могут взяться эти тысячи. Дело в том, что каждое доказательство опирается на какие-то факты, и если включить в него и полные

доказательства всех этих фактов, то тут-то и могут потребоваться тысячи страниц.

О ТОЧНОСТИ И ОДНОЗНАЧНОСТИ МАТЕМАТИЧЕСКИХ ТЕРМИНОВ

Прежде чем продолжить разговор о доказательствах, необходимо сказать несколько слов о математической терминологии.

Убедительность математических доказательств поддерживается отчётливостью, недвусмысленностью математических утверждений. Когда, например, говорят, что один общественный строй более прогрессивен, чем другой, то не вполне ясно, что в точности это означает. А вот когда говорят, что две прямые пересекаются, то ни у кого не возникает сомнения в смысле этих слов.

Для того чтобы математические суждения воспринимались как точные и недвусмысленные, необходимо, прежде всего, чтобы таковыми были те понятия, которые в этих суждениях используются. Суждения облекаются в словесную форму в виде предложений, а понятия — в виде терминов. Таким образом, каждый термин должен иметь ровно один точно очерченный смысл. Скажем несколько слов о том, что происходит в реальности с математическими терминами.

Надо признать, что точность смысла реально достигается лишь в профессиональных и высокоучёных математических текстах, в повседневной же практике — отнюдь не всегда. Чем точнее очерчен смысл термина — тем убедительнее использующие этот термин доказательства. Однозначности значений терминов также, к сожалению, не наблюдается.

Возьмём, к примеру, такой распространённый термин, как *многоугольник*. Он понимается по-разному — и как любая замкнутая ломаная, и как несамопересекающая замкнутая ломаная (и то, и другое ещё надо определять!), и как часть плоскости, ограниченная ломаной. Если вдуматься, то слова «часть плоскости, ограниченная ломаной» нуждаются в разъяснении, а тот факт, что такая часть существует, — ещё и в доказательстве, каковое оказывается довольно непростым (сам этот факт представляет собой частный случай так называемой *теоремы Жордана*, говорящей не только о ломаных, но и о замкнутых линиях вообще). Тем не менее именно в таком, достаточно наглядном и потому оставляемом без разъяснения, смысле термин *многоугольник* понимается в этой книге (а потому все приведённые здесь рассуждения о многоугольниках убедительны лишь постольку, поскольку ясен смысл термина).

Или возьмём термин *угол*. Вот несколько различных смыслов этого термина:

(1) два луча, исходящих из одной точки;

(2) угол в смысле (1) плюс одна из двух частей, на которые им разбивается плоскость;

(3) поворот луча;

(4) мера угла в смысле (1) (так понимается этот термин, когда говорят о сумме углов треугольника или произвольного выпуклого многоугольника);

(5) мера угла в смысле (2) (так понимается этот термин, когда говорят о сумме углов произвольного многоугольника, не обязательно выпуклого);

(6) мера угла в смысле (3) (так понимается этот термин, когда говорят об отрицательных углах и об углах, больших или равных 360°).

Заметим, что соотнесение углу как геометрической фигуре его меры как числа представляет собою, с позиций Высокой Науки, довольно сложную процедуру.

В дальнейшем изложении встретятся три важных неоднозначных термина. Это термины *натуральное число*, *натуральный ряд* и *равно́*.

Возможны два понимания того, что такое натуральное число, отличающиеся друг от друга в одном пункте: считать ли нуль натуральным числом. В школьных учебниках понятие натурального числа обычно выводят из пересчёта предметов, и потому натуральный ряд начинают с единицы. Но можно понимать натуральное число и как количество элементов какого-либо конечного множества. Поскольку одним из конечных множеств является пустое множество, вовсе не содержащее никаких элементов (например — множество ныне живущих динозавров), а количество элементов пустого множества есть нуль, то — при этом втором понимании — и наименьшее натуральное число есть нуль. При первом понимании понятие натурального числа совпадает с понятием целого положительного числа, при втором — с понятием целого неотрицательного числа. Подчеркнём, что каждое из указанных двух понятий имеет совершенно точное, недвусмысленное содержание, а двусмысленность заключается в терминологии, поскольку каждое претендует на то, чтобы его называли «натуральным числом». Чтобы избежать неясностей, первое понятие можно было бы называть *считательным натуральным числом*, а второе — *количественным натуральным числом*.

Натуральный ряд — это, по определению, множество всех натуральных чисел. Сообразно сказанному, есть два понятия натурального ряда: для одного из них натуральный ряд начинается с нуля, для другого — с единицы.

Каждая из двух точек зрения на то, что понимать под терминами *натуральное число* и *натуральный ряд*, имеет свои преимущества. Которую из них выбрать — дело вкуса. Но какую-то надо выбрать обязательно. Потому что невозможно ни говорить о доказательствах, ни тем более доказывать что-нибудь, не договорившись о значениях терминов. Чтобы не слишком уклоняться от школьной терминологии, мы будем начинать натуральный ряд с единицы. Впрочем, в некоторых из приводимых ниже примеров на тему «Индукция» удобнее относить к натуральным числам и ноль. Желающих начинать натуральный ряд с нуля призываем слегка переделать последующее изложение метода индукции — а именно, в базисе индукции надо положить $n=0$ вместо $n=1$.

Теперь о слове *равно́*. Основное значение этого термина в математике таково: говорят, что два предмета равны, если они совпадают. Именно этот смысл вкладывается и в выражающий равенство символ «=». Когда, например, пишут

$$3+5=8,$$

то эту запись понимают как выражающую такое утверждение: *предмет, обозначенный символом «*$3+5$*» совпадает с предметом, обозначенным символом «*8*»*. Казалось бы, никакое иное понимание и невозможно. К сожалению, возможно, и оно хорошо известно читателю. Это иное понимание появляется в школьном курсе геометрии. Там равными фигурами называют фигуры, которые могут и различаться, но совпадут после того, как одну из них переместить и совместить с другой. Именно так понимается, скажем, равенство отрезков AB и EF или треугольников ABC и EFG. И эти равенства записывают в виде $AB=EF$ и $\triangle ABC=\triangle EFG$ — так что смысл знака «=» здесь не тот, какой был указан выше.

Более грамотно было бы называть фигуры, совпадающие при совмещении, *конгруэнтными* и использовать для записи конгруэнтности не знак равенства «=», а специальный знак «$\cong$». Однако, чтобы не делать изложение излишне учёным, мы не будем употреблять ни термина *конгруэнтный*, ни знака «$\cong$», а довольствоваться школьной традицией (не такой уж, впрочем, и устойчивой, поскольку одно время в советских школах использовался именно термин «конгруэнтный»).

Итак, запись

$$AB = EF$$

вовсе не означает (а должна бы!), что отрезки AB и EF совпадают. Но что-то всё же при этом совпадает, а именно, их, отрезков, длины. Под психологическим давлением этого обстоятельства и длину отрезка AB нередко обозначают точно так же, как и сам отрезок, то есть посредством символа AB. И можно встретить такую запись известного неравенства, связывающего стороны треугольника:

$$AC < AB + BC.$$

Но это уже не лезет ни в какие ворота, и в этой книге длина отрезка AB будет обозначаться так, как ей и положено: $|AB|$.

ДОКАЗАТЕЛЬСТВА МЕТОДОМ ПЕРЕБОРА

Пример 1. Требуется доказать, что среди целых неотрицательных чисел, меньших числá 420, нет других корней уравнения

$$(x + 2008)(x - 3)(x - 216)(x - 548) = 0,$$

кроме чисел 3 и 216.

Доказательство: последовательно перебирая числа 0, 1, 2, 4, 5, 6, 7, ..., 213, 214, 215, 217, 218, 219, ..., 417, 418, 419 и подставляя их в уравнение, убеждаемся, что ни одно из них не обращает в нуль левую часть. Это есть типичное *доказательство методом перебора*. □

«Зачем же поступать так странно?» — возмутится читатель. Ведь достаточно опереться на следующее свойство произведения: если произведение равно нулю, то непременно равен нулю хотя бы один из сомножителей. Действительно, из указанного свойства вытекает, что если число является корнем нашего уравнения, то оно есть либо -2008, либо 3, либо 216, либо 548, а из этих четырёх чисел только 3 и 216 одновременно неотрицательны и меньше, чем 420. Читатель совершенно прав: его доказательство короче. Однако мы призываем читателя осознать тот факт, что предложенное нами доказательство совершенно убедительно, — а значит, совершенно безупречно. Кроме того, наше доказательство хотя и длиннее, но в определённом смысле проще: ведь оно не предполагает использования указанного выше свойства произведения. Представьте себе, что это свойство кому-либо неизвестно; тогда этот «кто-либо» поймёт наше доказательство, но не поймёт доказательства читателя. Мы преследовали и ещё одну, практическую цель: приучить

читателя не бояться доказательств методом перебора. Ведь хотя осуществление доказательства методом перебора может потребовать времени намного большего, чем проведение какого-нибудь хитроумного короткого доказательства, зато поиск такого хитроумного короткого доказательства может затянуться надолго...

Пример 2. Требуется доказать, что среди трёхзначных чисел нет числа, делящегося одновременно на 7, 11 и 13. Школьник младших классов, знакомый лишь с делением, может справиться с этой задачей, перебрав и испробовав все 900 трёхзначных чисел. Школьник старших классов знает (точнее — должен знать), что среди натуральных чисел выделяются *простые числа* и что *простым* называется всякое такое натуральное число, которое, во-первых, больше единицы и, во-вторых, делится только на единицу и на само себя. Так что числа 7, 11 и 13 — простые. А ежели школьник ещё более образован, то он знает, что число, делящееся на каждое из нескольких простых чисел, обязано делиться и на их произведение. Произведение $7 \cdot 11 \cdot 13$ равно 1001. Но никакое трёхзначное число не может делиться на 1001. □

Пример 3. Представим себе, что мы выдвинули такую гипотезу: уравнение $x^4 + y^4 = z^2$ не имеет решения в целых положительных числах, не превосходящих числа 100. В действительности указанное уравнение не имеет решения ни в каких целых положительных числах, так что наша гипотеза верна. Доказательство теоремы о неразрешимости нашего уравнения в целых положительных числах вполне элементарно. Так что в принципе читатель может доказывать гипотезу одним из двух способов. Первый способ: перебрать все десять тысяч пар $\langle x, y \rangle$, таких что $1 \leqslant x \leqslant 100$, $1 \leqslant y \leqslant 100$, возвести для каждой такой пары её составляющие в четвёртую степень, сложить и убедиться, что сумма не является полным квадратом. Второй способ: попытаться самостоятельно получить доказательство теоремы о неразрешимости уравнения. Второй способ труден, первый способ скучен. Конечно, можно поручить осуществление первого способа компьютеру; однако ведь можно взять вместо верхней границы 100 другую, настолько больш́ую, что и компьютеру перебор будет не под силу. Сейчас мы приведём реальный пример перебора, с которым не в состоянии справиться современные компьютеры. □

Пример 4. В 1742 г. российский математик Христиан Гольдбах выдвинул такую гипотезу: всякое натуральное число n, начиная с шести, есть сумма трёх простых чисел. Для небольших n гипотезу Гольдбаха можно проверить непосредственно; например,

$96 = 2 + 47 + 47$. С другой стороны, для очень больших *нечётных* чисел гипотеза тоже верна: как доказал в 1937 году И. М. Виноградов, гипотеза Гольдбаха верна для всех нечётных n, больших некоторого громадного n_0. Что касается самого этого n_0, то из анализа доказательства Виноградова вытекало, что в качестве n_0 можно взять, например, число $3^{14348907}$, требующее свыше шести с половиной миллионов знаков для своей десятичной записи. Оставалось, таким образом, проверить все нечётные числа от 7 до названного числа, и *для нечётных чисел* гипотеза Гольдбаха окажется либо доказанной, либо опровергнутой. Однако такая проверка совершенно нереальна. В 1989 г. китайские математики Ван и Чен понизили рубеж n_0 до числа, требующего всего лишь примерно 43 тысяч десятичных знаков для своей записи. Но и это число слишком велико для того, чтобы проверка оказалась в наши дни возможной — даже с помошью самой современной вычислительной техники. Есть серьёзные основания полагать, что осуществить столь большой перебор не удастся никогда. Остаётся надеяться, что со временем будет найдено другое, меньшее значение для n_0. □

Пример 5. Целые числа вида $n^2 + 1$ обладают следующим свойством: у них не бывает простых делителей вида $4k + 3$. Если перед читателем встанет задача проверить это свойство для предъявленного ему множества значений n (в другом варианте — для одного, но большого значения n), то что́ читатель предпочтёт — решать задачу перебором или же искать в математической литературе доказательство общей теоремы относительно чисел вида $n^2 + 1$, а то и пытаться самому сочинить такое доказательство? □

КОСВЕННЫЕ ДОКАЗАТЕЛЬСТВА СУЩЕСТВОВАНИЯ. ПРИНЦИП ДИРИХЛЕ

Самый естественный способ доказать, что объект с заданными свойствами действительно существует, — это его указать, назвать, построить (и, разумеется, убедиться, что он действительно обладает нужными свойствами). Чтобы доказать, например, что данное уравнение имеет решение, достаточно указать какое-то его решение. Такие доказательства существования чего-нибудь называются *прямыми* или *конструктивными*. Прямыми будут, например, приводимые в примерах 17 и 18 доказательства существования несоизмеримых отрезков, поскольку такая пара отрезков будет там указана.

Но бывают и *косвенные* доказательства, когда обоснование того факта, что искомый объект существует, происходит без прямого указания такого объекта.

Пример 6. В некоторой шахматной партии противники согласились на ничью после 15-го хода белых. Требуется доказать, что какая-то из чёрных фигур ни разу не передвигалась с одного поля доски на другое. (Термин «фигура» понимается здесь в широком смысле, включающем и пешки.) Рассуждаем так. Передвижения чёрных фигур по доске происходят лишь при ходах чёрных. Если такой ход не есть рокировка, передвигается одна фигура; если же ход есть рокировка, передвигаются две фигуры. Чёрные успели сделать 14 ходов, и лишь один из них мог быть рокировкой. Поэтому самое большое количество чёрных фигур, затронутых ходами, есть 15. А всего чёрных фигур 16. Значит, по крайней мере одна из них не участвовала ни в каком ходе чёрных. Отметим, что здесь мы не указываем такую фигуру конкретно (мы могли бы это сделать лишь в случае, если бы наблюдали шахматную партию или располагали её записью), а лишь доказываем, что она непременно существует. □

Пример 7. В самолёте летит 380 пассажиров. Докажите, что какие-то два из них отмечают свой день рождения в один и тот же день года. Рассуждаем так. Всего имеется 366 (включая 29 февраля) возможных дат для празднования дня рождения. А пассажиров больше; значит, не может быть, чтобы у всех у них дни рождения приходились на различные даты, и непременно случится так, что какая-то дата является общей по крайней мере для двух человек. Ясно, что этот эффект будет обязательно наблюдаться, начиная с 367 пассажиров. А вот при 366 пассажирах не исключено, что даты (числа и месяцы) их дней рождения будут для всех различны, хотя это и чрезвычайно маловероятно. (Кстати, теория вероятностей учит, что если случайно выбранная группа людей состоит более чем из 22 человек, то более вероятно, что у кого-нибудь из них будет общий день рождения, нежели что у всех у них дни рождения приходятся на разные дни года.) □

Логический прием, применённый нами в примере 7, носит название «*принцип Дирихлé*» — по имени знаменитого немецкого математика XIX в. Петера Густава Лежёна Дирихлé. Вот общая формулировка этого принципа:

если имеется n ящиков, в которых находятся в общей сложности по меньшей мере $n+1$ предметов, то непременно

найдётся ящик, в котором лежат по меньшей мере два предмета.

Чтобы увидеть, как приведённая формулировка используется в примере 7, надо мысленно представить себе 366 ящиков и надписать на каждом одну из 366 дат года, а затем, мысленно же, разместить по ящикам 380 пассажиров, помещая каждого пассажира в ящик с его датой рождения (всё делается только мысленно, так что никакого дискомфорта для пассажиров не будет). Тогда в каком-то из ящиков окажется более одного пассажира, и у этих пассажиров будет общий день рождения.

Для следующих двух примеров нам понадобится понятие счётного множества. Множество называется счётным, если его можно пересчитать, то есть назвать какой-то его элемент первым, какой-то элемент, отличный от первого, — вторым, какой-то, отличный от первых двух, — третьим, и так далее, причём все порядковые числительные должны быть использованы и ни один элемент множества не должен быть пропущен в этом пересчёте. Возьмём, к примеру, множество всех конечных цепочек, составленных из букв a и b, и запишем их в последовательность:

$$a, b, aa, ab, ba, bb, aaa, aab, aba, abb, \ldots, baaba, baabb, \ldots$$

(Высокая Наука относит к числу таких цепочек ещё и пустую цепочку, не содержащую ни одной буквы, но мы этого делать не будем, чтобы не пугать неискушённого читателя.) Правило расположения цепочек в последовательность мы выбрали таким (а могли бы выбрать и другим): группируем цепочки по длине (то есть по количеству составляющих букв), а в пределах группы располагаем цепочки в алфавитном порядке. Как только какое-либо множество удалось расположить в последовательность, так сразу возникает его пересчёт: член последовательности, стоящий на первом месте, объявляется первым; член, стоящий на втором месте, — вторым, и т. д. Простейшие примеры счётных множеств: натуральный ряд, множество всех простых чисел, множество всех рациональных чисел. Множество, являющееся бесконечным, но не являющееся счётным, называется *несчётным*. Сам факт существования несчётных множеств весьма принципиален, поскольку показывает, что бывают бесконечные множества, количество элементов в которых отлично от количества элементов натурального ряда. Открытие в XIX веке этого факта является одним из крупнейших открытий математики. В разделе «Доказательства от противного» будет приведён пример несчётного множества. Здесь мы заметим только, не

приводя доказательства, что множество всех действительных чисел является несчётным.

Пример 8. Можно предложить прямое доказательство существования иррациональных чисел — например, указать число $\sqrt{2}$ и доказать, что оно иррационально. Ниже будет приведено два таких доказательства — арифметическое в примере 11 и геометрическое в примере 19. Но можно предложить и вот какое *косвенное* доказательство. Множество всех рациональных чисел счётно, а множество всех действительных чисел несчётно; значит, бывают и числа, не являющиеся рациональными, то есть иррациональные. Конечно, надо ещё доказать счётность одного множества и несчётность другого, но это сделать сравнительно легко. Что касается множества рациональных чисел, то можно явно указать его пересчёт. Что же до несчётности множества действительных чисел, то его — при помощи представления действительных чисел в виде бесконечных десятичных дробей — можно вывести из несчётности множества всех двоичных последовательностей; а несчётность этого последнего множества будет доказана в примере 12, после чего будет намечен короткий путь, позволяющий получить несчётность множества действительных чисел. □

Пример 9. В предыдущем примере и прямое, и косвенное доказательства были приблизительно одинаковой степени сложности. Но вот ситуация, когда косвенное доказательство гораздо проще прямого. Действительное число называется *алгебраическим*, если оно является корнем многочлена с целыми коэффициентами; в противном случае оно называется *трансцендентным*. Прямое доказательство существования трансцендентных чисел состоит в предъявлении образца таких чисел. Такими образцами могут служить, например, известные числа e (основание натуральных логарифмов) и π (отношение длины окружности к диаметру). Однако доказать, что число e или число π (или какое угодно другое число) является трансцендентным, довольно сложно (так что какой-то образец найти просто, но трудно убедиться, что он действительно является образцом).

В то же время возможно следующее несложное *косвенное* доказательство существования трансцендентных чисел. Надо сравнить два множества, множество всех действительных чисел и множество всех алгебраических чисел, и убедиться, что первое из них несчётно, а второе счётно. Несчётность первого множества мы обсуждали в предыдущем примере. Счётность второго легко следует из того, что каждое алгебраическое число можно «назвать», то

есть присвоить ему некоторое имя. В качестве такого имени проще всего взять выражение, состоящее из двух частей: 1) из записи соответствующего многочлена и 2) из порядкового номера рассматриваемого числа среди корней этого многочлена (корни берутся в порядке возрастания). Такие имена уже нетрудно расположить в последовательность и тем самым — пересчитать. Раз множество всех алгебраических чисел счётно, а множество всех действительных чисел несчётно, то непременно бывают действительные числа, не являющиеся алгебраическими, то есть трансцендентные. □

ДОКАЗАТЕЛЬСТВА СПОСОБОМ «ОТ ПРОТИВНОГО»

Доказательства от противного устроены так. Делают предположение, что верно утверждение **B**, *противное*, то есть противоположное, тому утверждению **A**, которое требуется доказать, и далее, опираясь на это **B**, приходят к противоречию; тогда заключают, что, значит, **B** неверно, а верно **A**.

Пример 10. Этот пример встречается и в «Началах» Евклида, и в современных школьных учебниках. Пусть дан треугольник и два его неравных угла. Требуется доказать утверждение **A**: против большего угла лежит бóльшая сторона. Делаем противоположное предположение **B**: сторона, лежащая в нашем треугольнике против большего угла, меньше или равна стороне, лежащей против меньшего угла. Предположение **B** вступает в противоречие с ранее доказанной теоремой о том, что в любом треугольнике против равных сторон лежат равные углы, а если стороны неравны, то против большей стороны лежит больший угол. Значит, предположение **B** неверно, а верно утверждение **A**. Интересно, что прямое (то есть не «от противного») доказательство теоремы **A** оказывается намного более сложным. □

Пример 11. *Иррациональность квадратного корня из двух*, арифметическое доказательство. Обозначим этот корень буквой r и начнём рассуждать от противного. Итак, пусть число r рационально и таково, что $r^2 = 2$. Всякое рациональное число выражается дробью. Все выражающие число r дроби равны друг другу. Среди них найдётся несократимая дробь — доказательство этого простого факта составляет предмет примера 15. Пусть эта дробь есть $\frac{m}{n}$. Следовательно,

$$\left(\frac{m}{n}\right)^2 = 2.$$

Освобождаясь от знаменателя, имеем:

$$m^2 = 2n^2. \qquad (1)$$

Мы видим, что число m^2 чётно. Но квадрат любого нечётного числа всегда нечётен; значит, число m чётно: $m = 2k$ при некотором целом k. Подставляя $2k$ в (1) вместо m, получаем:

$$(2k)^2 = 2n^2, \tag{2}$$

и, после сокращения на 2:

$$2k^2 = n^2. \tag{3}$$

Совершенно так же, как мы убедились в чётности m, убеждаемся в чётности n. Итак, оба числа m и n чётны, и дробь $\frac{m}{n}$ можно сократить на 2 — а ведь мы выбрали её несократимой. Полученное противоречие доказывает, что число r не может быть рациональным, оно иррационально. Это и есть то арифметическое доказательство иррациональности числа $\sqrt{2}$, которое было упомянуто в примере 8. □

Пример 12. *Несчётность множества всех двоичных последовательностей. Диагональный метод*. Простейший пример несчётного множества — множество Ω всех двоичных последовательностей. Числовая последовательность называется *двоичной*, если каждый её член равен нулю или единице. Доказательство несчётности множества Ω очень знаменито и не слишком сложно. Сейчас мы его приведём. Оно проводится методом от противного.

Предположим, что Ω счётно, пересчитаем его и обозначим его n-й элемент через a_n. Этот элемент a_n есть двоичная последовательность $\alpha_{n,1}$, $\alpha_{n,2}$, $\alpha_{n,3}$, ... Таким образом, $\alpha_{n,k}$ есть k-й член n-й последовательности, а этот член равен либо нулю, либо единице. Сейчас мы предъявим такую двоичную последовательность b, которая не будет совпадать ни с одной из последовательностей a_n; тем самым мы получим противоречие с предположением, что мы пересчитали *все* последовательности. В качестве b мы укажем последовательность, которая отличается от a_1 своим 1-м членом, от a_2 — своим 2-м членом, от a_3 — своим 3-м членом, и так далее. Ясно, что такая последовательность b не может совпадать ни с a_1, ни с a_2, ни с a_3, и так далее. Указать такую b очень просто: достаточно взять последовательность β_1, β_2, β_3, ..., где $\beta_m = 1 - \alpha_{m,m}$. Противоречие, которое мы получили, и доказывает, что наше исходное предположение о счётности множества Ω является неверным.

Если каждую последовательности a_1, a_2, a_3, ... записать в строку, а эти строки расположить друг под другом, то получится

таблица, в которой члены $a_{m,m}$, лежащие в основе наших рассуждений, будут расположены на диагонали. Поэтому применённый метод доказательства называется *диагональным методом*. Диагональный метод был изобретён в XIX веке основателем теории множеств великим математиком Георгом Кантором. □

Несчётность множества всех действительных чисел. Сперва доказывается, что всякое подмножество счётного множества непременно конечно или счётно (предоставляем это читателю). Далее рассматривается множество таких действительных чисел, которые представимы как бесконечная десятичная дробь вида $0,\gamma_1\gamma_2\gamma_3\gamma_4\ldots$, в которой каждый десятичный знак γ_k равен 0 или 1. Множество таких чисел несчётно, что вытекает из примера 12. Но это множество образует подмножество множества всех действительных чисел, каковое, следовательно, несчётно. □

Чаще всего способ «от противного» используется для доказательства того, что объекта с заданными свойствами не существует. В самом деле, если требуется доказать, что что-то существует, то можно просто *предъявить* соответствующий объект (конечно, надо ещё доказать, что предъявлено именно то́, что надо, то есть что предъявленный объект обладает требуемыми свойствами). А как доказать, что чего-то нет? Хорошо, если это «что-то» надо искать среди конечного количества элементов — тогда можно попробовать метод перебора. А если среди бесконечного? Один из методов, применяемых в этом случае есть так называемый метод бесконечного спуска, речь о котором пойдёт в следующем разделе и который можно рассматривать как частный случай метода «от противного».

ПРИНЦИПЫ НАИБОЛЬШЕГО И НАИМЕНЬШЕГО ЧИСЛА И МЕТОД БЕСКОНЕЧНОГО СПУСКА

Принцип наибольшего числа утверждает, что *в любом непустом конечном множестве натуральных чисел найдётся наибольшее число*.

Принцип наименьшего числа формулируется так: *в любом непустом* (а не только в конечном!) *множестве натуральных чисел существует наименьшее число*.

Вторая формулировка принципа наименьшего числа: *не существует бесконечной убывающей* (то есть такой, в которой каждый последующий член меньше предыдущего) *последовательности натуральных чисел*.

Эти две формулировки принципа наименьшего числа равносильны. В самом деле, если бы существовала бесконечная убы-

вающая последовательность натуральных чисел, то среди членов этой последовательности не существовало бы наименьшего. Теперь представим себе, что удалось найти множество натуральных чисел, в котором наименьшее число отсутствует; тогда для любого элемента этого множества найдётся другой, меньший, а для него ещё меньший, и так далее, так что возникает бесконечная убывающая последовательность натуральных чисел.

Принцип наибольшего числа и обе формулировки принципа наименьшего числа с успехом применяются в доказательствах. Продемонстрируем это на примерах 13—15.

Пример 13. Доказать, что *любое натуральное число, большее единицы, имеет простой делитель*. Рассматриваемое число делится на единицу и на само себя. Если других делителей нет, то оно простое и тем самым является искомым простым делителем. Если же есть и другие делители, то берём из этих других наименьший. Если бы он делился ещё на что-то, кроме единицы и самого себя, то это что-то было бы ещё меньшим делителем исходного числа, что невозможно. □

Пример 14. Доказать, что *для любых двух натуральных чисел существует наибольший общий делитель*. Поскольку мы договорились начинать натуральный ряд с единицы (а не с нуля), то у любого натурального числа все его делители не превосходят самого этого числа и, следовательно, образуют конечное множество. Для двух чисел множество их общих делителей (то есть таких чисел, каждое из которых является делителем для обоих рассматриваемых чисел) тем более конечно. Найдя среди них наибольшее, получаем требуемое. □

Пример 15. Доказать, что *среди всех равных друг другу дробей непременно найдётся несократимая дробь.*

Первое доказательство — со ссылкой на пример 14, и тем самым с косвенным использованием принципа наибольшего числа. В нашем множестве дробей выберем произвольную дробь и найдём наибольший общий делитель d её числителя и знаменателя. Если $d=1$, то выбранная нами дробь уже несократима. Если $d\neq 1$, то сократим её числитель и знаменатель на это число d. Полученная дробь будет несократимой. Ведь если бы её можно было бы ещё сократить на какое-то число q, то произведение dq, большее числа d, было бы делителем числителя и знаменателя первоначальной дроби и d не было бы *наибольшим* общим делителем.

Второе доказательство — с использованием принципа наименьшего числа. Рассмотрим множество натуральных чисел, к которому

отнесём всякое число, являющееся знаменателем какой-нибудь из дробей нашей коллекции равных дробей. Найдём в этом множестве наименьшее число. Дробь с таким знаменателем будет несократима, потому что при любом сокращении и числитель, и знаменатель уменьшаются.

Третье доказательство — с использованием второй формулировки принципа наименьшего числа. Предположим, что в нашем множестве дробей нет несократимой. Возьмём произвольную дробь из этого множества и сократим её. Эту тоже сократим, и так далее. Знаменатели этих дробей будут всё меньшими и меньшими, и возникнет бесконечная убывающая последовательность натуральных чисел, что невозможно. □

Продемонстрированный в третьем доказательстве примера 15 вариант метода «от противного», когда возникающее противоречие состоит в появлении бесконечной последовательности убывающих натуральных чисел (чего, повторим, быть не может) называется *методом бесконечного* (или *безграничного*) *спуска*.

Пример 16. Вот ещё пример на метод бесконечного спуска. Выше, говоря о методе перебора, мы упомянули, что уравнение $x^4+y^4=z^2$ не имеет решений в натуральных числах. Стандартный способ доказательства этого факта состоит в доказательстве от противного: противоречие выводится из предположения, что существует тройка $\langle a, b, c\rangle$ натуральных чисел, являющаяся решением уравнения, то есть такая, что $a^4+b^4=c^2$. Для получения требуемого противоречия применяют метод безграничного спуска. Мы не будем здесь излагать, как именно осуществляется описываемое ниже построение[1], а ограничимся общей идеей. Идея же состоит в том, что указывается способ, следуя которому для каждой тройки натуральных чисел $\langle a, b, c\rangle$, служащей решением нашего уравнения, строится другая тройка натуральных чисел $\langle a', b', c'\rangle$, также служащая решением того же уравнения, но такая, что $c'<c$. Применяя этот метод, для тройки-решения $\langle a', b', c'\rangle$ можно построить тройку-решение $\langle a'', b'', c''\rangle$, а для этой тройки — тройку $\langle a''', b''', c'''\rangle$, и так далее. А тогда возникает невозможная убывающая последовательность натуральных чисел: $c>c'>c''>c'''>\ldots$ □

Напомним, что отрезок a называется *мерой* отрезка b, если a укладывается в b целое число раз. Возникает вопрос, для всяких

[1]Заинтересованный читатель найдёт это построение в главе 15 одной из лучших популярных книг по математике: *Г. Радемахер, О. Теплиц. Числа и фигуры. Опыты математического мышления*. Эта книга, в переводе с немецкого, выдержала в России несколько изданий, последнее — в 2007 г.

ли двух отрезков существует их *общая* мера, то есть такой отрезок, который является мерой для каждого из этих двух. Если какие-либо два отрезка имеют общую меру, то эти отрезки называются *соизмеримыми*, в противном же случае — *несоизмеримыми*. Итак, любые ли два отрезка соизмеримы? Этот вопрос имеет принципиальное значение: отношение несоизмеримых отрезков не может быть выражено рациональным числом, и потому именно явление несоизмеримости вызывает к жизни иррациональные числа. Тот факт, что несоизмеримые отрезки существуют, был известен ещё древним грекам и производил на них глубокое впечатление, а с открытием этого факта связан ряд легенд. Самым ранним примером несоизмеримых отрезков была такая пара: диагональ какого-нибудь квадрата и сторона этого же квадрата. Разумеется, тщетно пытаться доказать несоизмеримость двух отрезков методом перебора: ведь тогда пришлось бы перебрать *все* отрезки (что невозможно!) и про каждый из них убедиться, что он не является общей мерой рассматриваемых отрезков — в частности, общей мерой стороны и диагонали одного и того же квадрата.

Все известные доказательства несоизмеримости стороны и диагонали квадрата осуществляются способом «от противного». Мы приведём два доказательства — арифметическое и геометрическое. Обоим предпошлём следующее соображение. Если разрезать квадрат по диагонали, возникнут два равнобедренных прямоугольных треугольника, в каждом из которых эта диагональ будет служить гипотенузой, а стороны квадрата — катетами. Так что вопрос о соизмеримости или несоизмеримости стороны квадрата и его диагонали равносилен вопросу о соизмеримости или несоизмеримости катета и гипотенузы равнобедренного прямоугольного треугольника. Несоизмеримость катета и гипотенузы мы и будем доказывать.

Пример 17. *Несоизмеримость гипотенузы и катета равнобедренного прямоугольного треугольника*, арифметическое доказательство. Предположим противное: у гипотенузы и катета имеется общая мера. Пусть эта общая мера укладывается целое число m раз в гипотенузе и целое число n раз в катете. Тогда, по теореме Пифагора, $2n^2 = m^2$, откуда $\sqrt{2} = \frac{m}{n}$. Но этого не может быть, так как $\sqrt{2}$ есть число иррациональное, что было доказано в примере 11. □

Но известно и другое доказательство несоизмеримости гипотенузы и катета, чисто геометрическое, необыкновенно красивое и, возможно, древнее.

Пример 18. *Несоизмеримость гипотенузы и катета равнобедренного прямоугольного треугольника*, геометрическое доказательство. Рассуждать будем так. Для каждого равнобедренного прямоугольного треугольника Q мы построим другой равнобедренный прямоугольный треугольник Q′ с более коротким катетом и такой, что всякая общая мера катета и гипотенузы треугольника Q служит также общей мерой катета и гипотенузы треугольника Q′. Применяя к Q′ ту же конструкцию, получим равнобедренный прямоугольный треугольник Q″ с ещё более коротким катетом и такой, что всякая общая мера катета и гипотенузы треугольника Q′ служит также общей мерой катета и гипотенузы треугольника Q″. К треугольнику Q″ снова применяем ту же конструкцию, и т. д. Получаем бесконечную последовательность равнобедренных прямоугольных треугольников Q, Q′, Q″, Q‴, … со всё более и более короткими катетами. При этом всякая общая мера катета и гипотенузы исходного треугольника Q будет в то же время и общей мерой катета и гипотенузы треугольника Q′, а значит, и общей мерой катета и гипотенузы треугольника Q″, а значит, катета и гипотенузы треугольника Q‴, и т. д.

Это построение, которое мы осуществим ниже, и позволяет провести доказательство от противного. Действительно, предположим, что некоторый отрезок a является общей мерой для катета и гипотенузы треугольника Q. Тогда для каждого из треугольников $Q^{(k)}$ он является общей мерой катета и гипотенузы этого треугольника. Отсюда следует, что в катете каждого из этих треугольников он укладывается какое-то целое число раз. Пусть отрезок a укладывается n раз в катете треугольника Q, пусть, далее, этот отрезок укладывается n' раз в катете треугольника Q′, n'' раз в катете треугольника Q″, и т. д. Поскольку длины катетов уменьшаются, то $n > n' > n'' > n''' > \ldots$; таким образом, мы получаем бесконечную последовательность убывающих натуральных чисел, что невозможно. А это значит, что было неверным наше исходное предположение о наличии у катета и гипотенузы треугольника Q общей меры.

Осталось указать, как по треугольнику $Q = \triangle ABC$ строится треугольник Q′.

На гипотенузе BC исходного треугольника Q откладываем отрезок BD, равный катету (см. рис. 1). Из D восставим перпендикуляр к BC. Обозначим через E точку пересечения этого перпендикуляра с прямой, проходящей через точки A и C. Убедимся, что эта точка располагается между точками A и C, то есть на стороне AC, а не на продолжении этой стороны за точку A. Соединив прямой точки A и D (на рисунке эта прямая показана пунктиром),

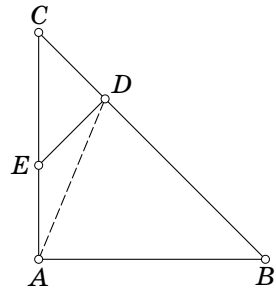


Рис. 1

получаем треугольник ADB. Этот треугольник равнобедренный по построению, и его углы BDA и BAD, прилежащие к равным сторонам, равны. В треугольнике не может быть ни двух прямых углов, ни двух тупых, поэтому угол BDA острый и, следовательно, меньше прямого угла BDE, а потому прямая DE не может идти внутри угла BDA. Значит, она проходит внутри угла ADC, в чём и требовалось убедиться.

Изучим наш рисунок более детально и установим три соотношения для разных отрезков. В прямоугольном (по построению) треугольнике CED угол ECD равен половине прямого угла, а общая сумма углов треугольника равна двум прямым; отсюда следует, что и угол CED равен половине прямого. Мы видим, что в треугольнике CED углы при его вершинах C и E равны; следовательно, этот треугольник равнобедренный с равными сторонами DE и DC, поэтому

$$|DE| = |DC|. \tag{1}$$

Далее, треугольники BEA и BED имеют общую сторону BE и равные стороны BA и BD; поскольку они прямоугольные, то сказанного достаточно для их равенства. Следовательно,

$$|EA| = |ED|.$$

Соединяя это равенство с (1), получаем второе из искомых соотношений:

$$|AE| = |DC|. \tag{2}$$

Наконец, третье соотношение. Поскольку, как только что доказано, $|DC| = |AE|$, то $|DC| = |AE| < |AC| = |AB|$. Итак,

$$|DC| < |AC| = |AB|. \tag{3}$$

Теперь уже нетрудно показать, что в качестве искомого треугольника Q' можно взять треугольник CED. Действительно: он прямоугольный по построению и равнобедренный, как показывает соотношение (1). Его катет короче катета исходного треугольника $\mathrm{Q}=\triangle ABC$, как показывает соотношение (3). Осталось убедиться, что всякая общая мера гипотенузы и катета треугольника ABC служит также и общей мерой для гипотенузы и катета треугольника CED. В самом деле, пусть некоторая общая мера сторон треугольника ABC укладывается p раз в его катете и q раз в его гипотенузе BC. Тогда она укладывается p раз в равном катету отрезке BD и $q-p$ раз в отрезке CD. Поскольку, согласно (2), отрезок AE равен отрезку CD, то и в AE эта общая мера укладывается $q-p$ раз. Значит, в отрезке EC она укладывается $p-(q-p)$ раз. Итак, эта мера укладывается целое число раз и в катете CD, и в гипотенузе EC треугольника CED, то есть является их общей мерой. □

Замечание. *Египетский треугольник и обратная теорема Пифагора.* Теорема Пифагора утверждает, что в любом прямоугольном треугольнике сумма квадратов катетов равна квадрату гипотенузы (понятно, что надо бы говорить о *длинах* катетов и гипотенузы, но слово «длина» для краткости часто опускается). Всякая тройка целых чисел, выражающих длины сторон какого-либо прямоугольного треугольника, называется *пифагоровой*. Пифагоровых троек бесконечно много, из них тройка $\langle 3, 4, 5\rangle$ имеет наименьшие члены, а прямоугольный треугольник с такими длинами сторон называется *египетским*. □

Происхождение названия таково. В Древнем Египте этот треугольник использовался в строительстве для построения прямого угла. Верёвка, разбитая на 12 равных частей, растягивалась так, чтобы три точки стали вершинами треугольника со сторонами длиною в 3, 4 и 5 частей. Треугольник оказывался прямоугольным. Тем не менее само существование египетского треугольника требует доказательства. Построить треугольник с длинами сторон 3, 4, 5 нетрудно, но вот почему он будет прямоугольным? Нередко можно услышать ответ: «По теореме Пифагора, потому что $3^2+4^2=5^2$». Ответ неточен. Ведь теорема Пифагора утверждает лишь то, что в прямоугольном треугольнике выполняется известное соотношение между длинами сторон. Но она не утверждает, что если это соотношение выполняется, то треугольник прямоугольный. Этот факт составляет содержание другой теоремы — теоремы, обратной к теореме Пифагора и называемой для краткости *обратной теоремой Пифагора*. Обратная теорема Пифагора гласит:

если в каком-то треугольнике сумма квадратов двух сторон равна квадрату третьей, то треугольник прямоугольный и против большей стороны лежит прямой угол.

Её доказательство чрезвычайно просто. Пусть длины сторон треугольника Δ суть a, b, c, причём $a^2+b^2=c^2$. На сторонах прямого угла отложим от его вершины O отрезки OX и OY, равные a и b соответственно. Возникает прямоугольный треугольник OXY, гипотенуза XY которого имеет, по теореме Пифагора, длину $\sqrt{a^2+b^2}$, то есть c. Таким образом, треугольники Δ и OXY имеют соответственно равные стороны и, следовательно, равны. Значит, трегольник Δ прямоугольный, и против стороны с длиной c лежит прямой угол. □

Пример 19. *Иррациональность квадратного корня из двух*, геометрическое доказательство. Предположим, что этот корень рационален и выражается дробью $\frac{m}{n}$. Тогда

$$\left(\frac{m}{n}\right)^2=2, \quad m^2=2n^2.$$

Рассмотрим равнобедренный треугольник с боковыми сторонами длины n и основанием длины m. По обратной теореме Пифагора этот треугольник прямоугольный, причём единичный отрезок укладывается в его катете n раз, а в гипотенузе m раз. Следовательно, единичный отрезок служит общей мерой катета и гипотенузы этого равнобедренного прямоугольного треугольника, так что они соизмеримы, чего не может быть: смотри пример 18. □

Замечание. Напомним, что геометрическая фигура называется *выпуклой*, если она обладает следующим свойством:

(α) *для любых двух точек фигуры отрезок, соединяющий эти точки, находится в пределах этой фигуры.*

В качестве полезного упражения рекомендуем читателю доказать, что для любой совокупности выпуклых фигур фигура, образованная их пересечением, непременно выпукла. В частности, если прямая пересекает выпуклый многоугольник, то она разбивает его на два выпуклых многоугольника. В самом деле, каждая из частей разбиения представляет собою пересечение исходного многоугольника с одной из тех двух полуплоскостей, на которые прямая разрезает плоскость, а всякая полуплоскость — выпукла. □

Пример 20. *Важное свойство выпуклого многоугольника*. Для того частного случая, когда геометрическая фигура является мно-

гоугольником, можно предложить и другое определение выпуклости. Именно, можно назвать многоугольник *выпуклым*, если для него выполняется свойство:

(β) *какую ни взять сторону многоугольника, многоугольник целиком лежит по одну сторону от неё, то есть от прямой, служащей её продолжением.*

Оба определения равносильны:

(1) из (α) вытекает (β);

(2) из (β) вытекает (α).

Утверждения (1) и (2) легко доказываются от противного. Доказательство для (1) сейчас изложим; доказать (2) предоставляем читателю. Итак, предположим, что в многоугольнике со свойством (α) нашлись две такие его точки P и Q, которые лежат по разные стороны от некоторой его стороны AB. Поскольку все точки отрезка AB принадлежат многоугольнику, ему будут принадлежать и все точки треугольников PAB и QAB. Таким образом, отрезок AB является общей стороной треугольников PAB и QAB, расположенных хотя и по разные стороны от этого отрезка, но целиком в пределах рассматриваемого многоугольника. Очевидно, что такого не может случиться, коль скоро AB является одной из сторон этого многоугольника. □

ИНДУКЦИЯ

Доказательства методом математической индукции

Метод математической индукции применяется тогда, когда хотят доказать, что некоторое утверждение выполняется для всех натуральных чисел.

Пример 21. Продемонстрируем метод математической индукции на простом примере. Пусть, например, мы хотим доказать, что всегда $1+2+3+\ldots+n=\frac{n(n+1)}{2}$. Рассуждаем так. Во-первых, для $n=1$ это утверждение верно; действительно, $1=\frac{1(1+1)}{2}$. Во-вторых, предположив, что наше утверждение верно для $n=k$, убеждаемся, что тогда оно верно и для $n=k+1$. Действительно,

$$1+2+3+\ldots+(k+1)=(1+2+3+\ldots+k)+(k+1)=$$
$$=\frac{k(k+1)}{2}+(k+1)=\frac{(k+1)[(k+1)+1]}{2}.$$

Значит, наше утверждение верно для всех значений n: действительно, оно верно для $n=1$ (это было наше «во-первых»), а тогда,

в силу «во-вторых», оно верно для $n=2$, откуда, в силу того же «во-вторых», оно оказывается верным и для $n=3$, и так далее. □

Пример 22. *Равенство Ададурова* (названо по имени нашедшего его российского математика XVIII века Василия Евдокимовича Ададурова):

$$1^3+2^3+3^3+\ldots+n^3=(1+2+3+\ldots+n)^2.$$

Доказываем по индукции. Для $n=1$ проверяем непосредственно. Предположим, что равенство верно при $n=k$. Докажем, что тогда оно верно и при $n=k+1$ (при этом используем результат примера 21):

$$\begin{aligned}
&[1+2+3+\ldots+k+(k+1)]^2=\\
&\quad=[1+2+3+\ldots+k]^2+2[1+2+3+\ldots+k](k+1)+(k+1)^2=\\
&\quad=1^3+2^3+3^3+\ldots+k^3+2\left[\frac{k(k+1)}{2}\right](k+1)+(k+1)^2=\\
&\quad=1^3+2^3+3^3+\ldots+k^3+k(k+1)^2+(k+1)^2=\\
&\quad=1^3+2^3+3^3+\ldots+k^3+(k+1)^3.
\end{aligned}$$

Проведённое рассуждение показывает, что наше равенство верно не только при $n=1$, но и при $n=2$, $n=3$, и так далее — и тем самым при всех n. □

Пример 23. Тем же способом легко убедиться в истинности при всех n равенства

$$1^2+2^2+3^2+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}.$$ □

Изложенный метод рассуждения требует установления двух фактов:

(1) интересующее нас утверждение верно для единицы;

(2) если интересующее нас утверждение верно для какого-то числа k, то оно верно и для следующего за ним числа $k+1$.

Если оба факта установлены, тогда, переходя от 1 к 2, от 2 к 3, и т. д., убеждаемся — подобно тому как мы в этом убедились в только что приведённом примере — в том, что рассматриваемое утверждение верно для *всех* натуральных чисел.

Первый факт называется *базисом индукции*, второй — *индукционным переходом* или *шагом индукции*. Индукционный переход включает в себя *посылку*, или *предположение индукции*, или *индукционное предположение*, и *заключение*. Смысл посылки:

рассматриваемое утверждение верно при $n=k$. Смысл заключения: рассматриваемое утверждение верно при $n=k+1$. Сам же индукционный переход состоит в переходе от посылки к заключению, то есть в заявлении, что заключение верно, коль скоро верна посылка. Весь в целом логический приём, позволяющий заключить, что рассматриваемое утверждение верно для всех натуральных чисел, коль скоро справедливы и базис, и переход, называется так: *принцип математической индукции*. Использование этого принципа и составляет *метод математической индукции*.

Таким образом, обстановка, позволяющая надеяться (всго лишь надеяться!) на успешное применение метода математической индукции, должна быть такова. Имеется некоторое утверждение **A**, зависящее от параметра, принимающего натуральные значения; требуется доказать, что **A** справедливо при всяком значении параметра. Так, в примере 21 утверждение **A** имело вид $1+2+$ $+3+\ldots+n=\frac{n(n+1)}{2}$. Сам параметр называется *параметром индукции*; говорят также, что происходит *индукция по данному параметру*.

Утверждение **A** при значении параметра, равном 1, принято обозначать через **A**(1), при значении параметра, равном 2, — через **A**(2), и так далее. В примере 21 **A**(10) есть $1+$ $+2+3+\ldots+10=\frac{10(10+1)}{2}$. Утверждения **A**(1), **A**(2), **A**(3), ... называют *частными формулировками*, утверждение «для всякого n имеет место **A**(n)» называют *универсальной формулировкой*. Таким образом, в наших теперешних обозначениях *базис индукции* есть не что иное, как частная формулировка **A**(1). А *шаг индукции*, или *индукционный переход*, есть утверждение «каково бы ни было n, из истинности частной формулировки **A**(n) вытекает истинность частной формулировки **A**($n+1$)».

Применение метода начинается с того, что формулируются два утверждения: базис индукции и её шаг. Здесь проблем нет. Проблема состоит в том, чтобы доказать оба эти утверждения. Если это не удаётся, это означает, что наши надежды на применение метода математической индукции не оправдались. Зато если нам повезло, если нам удалось доказать и базис, и шаг, то доказательство универсальной формулировки получаем уже без всякого труда, применяя следующее *стандартное рассуждение*.

> Утверждение **A**(1) истинно, поскольку оно есть базис индукции. Применяя к нему индукционный переход, получаем, что истинно и утверждение **A**(2). Применяя к нему индук-

ционный переход, получаем, что истинно и утверждение **A(3)**. Применяя к нему индукционный переход, получаем, что истинно и утверждение **A(4)**. Таким способом мы можем дойти до каждого значения n и убедиться, что **A**(n) истинно. Следовательно, для всякого n имеет место **A**(n), а это и есть та универсальная формулировка, которую требовалось доказать.

Принцип математической индукции заключается, по существу, в разрешении не проводить «стандартное рассуждение» в каждой отдельной ситуации. Действительно, стандартное рассуждение только что было обосновано в общем виде, и нет нужды повторять его каждый раз применительно к тому или иному конкретному выражению **A**(n). Поэтому *принцип математической индукции позволяет делать заключение об истинности универсальной формулировки сразу, как только установлены истинность базиса индукции и индукционного перехода.*

Пример 24. Чтобы у читателя не создалось впечатления, что принцип индукции используется только для доказательства равенств, докажем с помошью этого принципа важное неравенство

$$(1+\alpha)^n \geqslant 1+n\alpha,$$

где $\alpha \geqslant -1$. Базис индукции выполнен, поскольку при $n=1$ левая и правая части одинаковы. Шаг индукции начинаем с предположения, что утверждение верно при $n=k$; таким образом, посылка шага индукции есть $(1+\alpha)^k \geqslant 1+k\alpha$. Умножая это неравенство на неотрицательное число $1+\alpha$, имеем $(1+\alpha)^{k+1} \geqslant (1+k\alpha)(1+\alpha)$. Последнее неравенство переписываем так: $(1+\alpha)^{k+1} \geqslant 1+(k+1)\alpha+k\alpha^2$. Отбрасывая здесь в правой части неотрицательное слагаемое $k\alpha^2$, получаем $(1+\alpha)^{k+1} \geqslant 1+(k+1)\alpha$. А это и есть заключение шага индукции. Итак, мы проверили и базис, и шаг. Доказательство методом индукции завершено. □

Иногда приходится доказывать утверждение не для всех натуральных чисел, а для всех, начиная с некоторого числа. Как поступать в таких случаях, показано в примере 25.

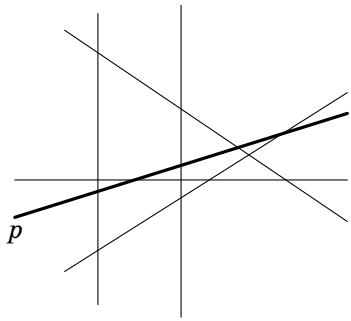
Пример 25. Требуется доказать, что сумма углов выпуклого n-угольника равна $2(n-2)d$, где d — прямой угол. Ясно, что утверждение, которое нужно доказать, имеет смысл лишь при $n \geqslant 3$. Чтобы иметь право применить метод индукции, надо косметически изменить формулировку: сумма углов выпуклого $(n+2)$-угольника равна $2nd$. Такая формулировка уже имеет смысл при всех натуральных n. Базис составляет здесь известная теорема о сумме

углов треугольника: сумма углов $(1+2)$-угольника равна $2\cdot 1\cdot d$. Чтобы вывести заключение индукционного перехода (сумма углов многоугольника с числом сторон $[(k+1)+2]$ равна $2(k+1)d$) из его посылки (сумма углов многоугольника с числом сторон $(k+2)$ равна $2kd$), поступаем так. В многоугольнике с числом сторон $[(k+1)+2]$ берём две вершины, соседствующие с одной и той же вершиной, и соединяем их диагональю. Эта диагональ разобьёт наш многоугольник на две части: на треугольник и на $(k+2)$-угольник. Сумма углов исходного многоугольника получается сложением суммы углов этого треугольника, каковая сумма есть $2d$, и суммы углов этого $(k+2)$-угольника, каковая сумма (посылка перехода!) есть $2kd$. Складывая, получаем $2(k+1)d$, то есть то́, что́ надо. □

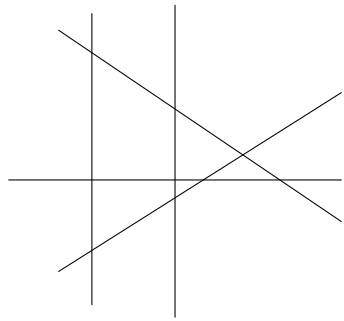
Иногда утверждение может и не содержать параметр в явном виде и требуется сообразительность, чтобы его туда ввести. На эту тему — примеры 26 и 27.

Пример 26. Дано конечное множество прямых на плоскости. Требуется доказать, что части, на которые плоскость разбита этими прямыми, можно раскрасить двумя красками, причём раскрасить *правильно*, то есть так, чтобы никакие две части, имеющие общую границу, не были бы одинакового цвета. Именно так, правильно, раскрашиваются географические карты, отражающие политическое или административное устройство какой-либо территории; поэтому всякое разбиение плоскости на части тоже будем называть *картой*. В подлежащем доказательству утверждении никакое натуральное число не упоминается, но сейчас мы такое число введём. С этой целью сформулируем наше утверждение слегка иначе, включив в него параметр n: всякую карту, образованную n прямыми, можно правильно раскрасить в два цвета. Вот теперь уже можно применять метод математической индукции.

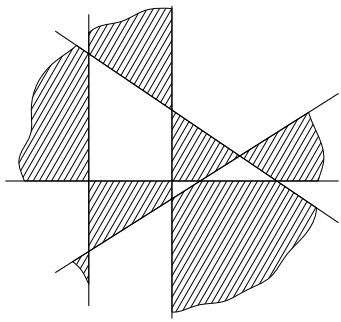
Базис справедлив: ведь в случае $n=1$ прямая ровно одна, и достаточно просто покрасить в разные цвета те две части, на которые она делит плоскость. Посылка индукционного шага состоит в предположении, что правильную раскраску можно всегда осуществить в случае k прямых. Заключение — в утверждении, что правильную раскраску всегда можно осуществить для $k+1$ прямых. Переход от посылки к заключению показан на рисунке 2, состоящем из пяти частей: 2а, 2б, 2в, 2г и 2д. Переход состоит в следующем. В карте, образованной $k+1$ прямыми, выделим одну из прямых — на рис. 2а она показана более толстой линией и помечена буквой p. Удалив эту прямую, получим карту, содержащую



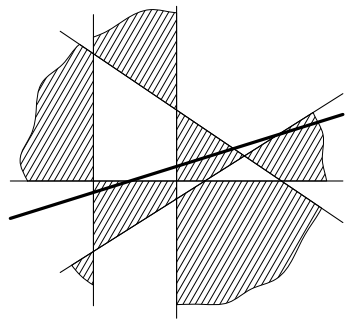
а)



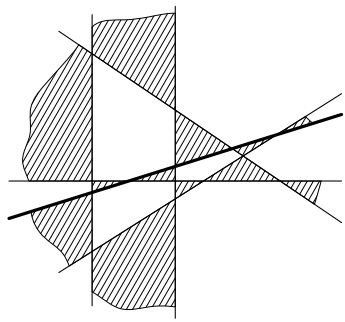
б)



в)



г)



д)

Рис. 2

k прямых, — она показана на рис. 2б. Согласно индукционному предположению, полученная карта допускает правильную раскраску — такая раскраска показана на рис. 2в. В раскрашенной карте восстанавливаем удалённую прямую (рис. 2г), отчего правильность раскраски, разумеется, нарушится. Однако она сохранится в каждой из полуплоскостей, на которые выделенная прямая разбивает плоскость; нарушения будут иметь место лишь там, где граница между участками проходит по прямой p. Поэтому если в одной из названных полуплоскостей раскраску не менять, а в другой заменить каждый из двух цветов на противоположный, то вся карта с $k+1$ прямой окажется правильно раскрашенной (рис. 2д). □

Пример 27. Выпуклый многоугольник целиком покрыт другим выпуклым многоугольником (например, на рисунке 3 многоугольник $ABCDEFG$ целиком покрыт многоугольником $IJKLMNOP$). Требуется доказать, что периметр внутреннего многоугольника не

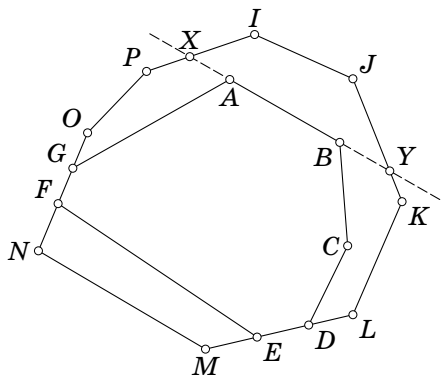


Рис. 3

превосходит периметра многоугольника внешнего. Будем доказывать данное утверждение методом математической индукции. Чтобы применить этот метод, надлежит ввести параметр. Сообразительности здесь потребуется несколько больше, чем в примере 26. Назовём *свободной* всякую сторону внутреннего многоугольника, которая не лежит ни на какой стороне внешнего многоугольника. (Так, на рисунке 3 свободными являются стороны AB, BC, CD, EF, GA, а стороны DE и FG не являются свободными.) В качестве параметра индукции возьмём количество свободных сторон, точнее говоря — количество свободных сторон плюс единица (поскольку свободных сторон может и не быть, а мы условились начинать

натуральный ряд не с нуля, а с единицы). Сформулируем теперь более развёрнуто то утверждение, которое мы собираемся доказывать индукцией по этому параметру: каково бы ни было натуральное число n, для всякой пары вложенных друг в друга выпуклых многоугольников с числом свободных сторон, равным $n-1$, периметр внутреннего многоугольника не превосходит периметра внешнего многоугольника.

В базисе индукции значение параметра равно единице, а это значит, что свободных сторон нет вовсе. Тогда утверждение очевидно: ведь в этом случае каждая сторона внутреннего многоугольника является частью какой-либо стороны внешнего многоугольника. Предположим теперь, что утверждение верно для всех случаев, когда имеется k свободных сторон. Докажем его для всех случаев, когда есть имеется $k+1$ свободная сторона. Итак, пусть R есть внутренний многоугольник, T — внешний, и количество свободных сторон есть $k+1$. Нам нужно доказать, что $p(\mathrm{R}) \leqslant p(\mathrm{T})$, где $p(\mathrm{R})$ и $p(\mathrm{T})$ — периметры многоугольников R и T. Берём одну из свободных сторон и продолжаем её в оба направления (на рисунке 3 в качестве такой свободной стороны выбрана сторона AB). Полученная прямая разрезает T на два многоугольника — также выпуклых, как это показано в замечании, непосредственно предшествующем примеру 20. Точки пересечения со сторонами многоугольника T обозначим буквами X и Y. Поскольку внутренний многоугольник выпукл, он, как это доказано в примере 20, целиком лежит по одну сторону от прямой XY. Следовательно, он целиком располагается внутри одного из тех двух многоугольников, на которые эта прямая разбивает T. Обозначим буквой S тот из многоугольников разбиения, который содержит R, так что R вложен в S, а S вложен в T. На рисунке 3 таковым промежуточным S является многоугольник $XYKLMNOP$ (а другим из двух многоугольников, на которые разбивается T, будет многоугольник $XIJY$). Обозначим через $p(\mathrm{S})$ периметр многоугольника S. На рисунке 3 видно, что $p(\mathrm{S}) \leqslant p(\mathrm{T})$, поскольку отрезок, стягивающий концы ломаной (на рисунке — отрезок XY), короче самой этой ломаной (на рисунке — ломаной $XIJY$). Если теперь рассмотреть пару вложенных многоугольников R и S, то можно заметить, что в этой паре количество свободных сторон на единицу меньше количества свободных сторон в паре R и T. Действительно, свободной перестала быть та сторона (на рисунке — сторона AB) многоугольника R, с которой мы начали построение. Поэтому, по предположению индукции, $p(\mathrm{R}) \leqslant p(\mathrm{S})$. Соединяя это неравенство с установленным ранее неравенством $p(\mathrm{S}) \leqslant p(\mathrm{T})$, приходим окончательно к требуемому неравенству $p(\mathrm{R}) \leqslant p(\mathrm{T})$. □

Принцип наименьшего числа может быть использован для построения нового варианта «стандартного рассуждения», призванного обосновать истинность универсальной формулировки. Вспомним, что мы обосновывали её, делая последовательные переходы от **A**(1) к **A**(2), от **A**(2) к **A**(3), и т. д. Теперь же будем рассуждать от противного. Покажем, как происходит рассуждение, на примере 26. Предположим, что бывают карты указанного вида, которые нельзя правильно раскрасить. Назовём число n «плохим», если возможна карта, образованная n прямыми, которую нельзя правильно раскрасить. По предположению, «плохие» числа существуют, следовательно, множество всех таких чисел не пусто. Применяя к нему принцип наименьшего числа, получаем, что существует наименьшее «плохое» число a. В силу базиса индукции $a \neq 1$. Значит, $a = k + 1$, где k — натуральное число. Так как a — наименьшее из «плохих» чисел, то k не является плохим; следовательно, всякую карту, образованную k прямыми, можно правильно раскрасить. Но тогда, в силу индукционного шага, можно правильно раскрасить и всякую карту, образованную $a = k + 1$ прямыми. Полученное противоречие убеждает нас, что исходное предположение о существовании карт, не допускающих правильной раскраски, не соответствует действительности. Тем самым мы получили доказательство того, что всякую карту, образованную прямыми, можно раскрасить правильно.

Полная индукция и неполная индукция

Метод *индукции*, в самом общем смысле, состоит в переходе от частных формулировок к формулировке универсальной. Различают *полную* и *неполную* индукцию. Метод математической индукции позволяет, применяя некоторое логическое рассуждение к произвольному натуральному числу, убедиться, что **A** истинно *для этого произвольного* числа, а тем самым — убедиться, что **A**(n) истинно для всех n. В этом смысле этот метод является методом *полной* индукции; слово *полная* означает, что мы лишь тогда считаем себя вправе объявить об истинности универсальной формулировки, когда мы убедились в её истинности для каждого отдельного значения n — во всей полноте этих значений, без исключения. Метод *неполной* индукции состоит в переходе к универсальной формулировке после проверки частных формулировок для отдельных, но не всех значений n.

Примеры неполной индукции встречаются на каждом шагу. Скажем, если не все, то многие знают, что Бенджамин Франклин

был президентом Соединённых Штатов. «Президент Франклин» — такое можно услышать и от кассира в банке, и с экрана телевизора, причём от персонажей, которых трудно заподозрить в глубоком знании американской политической истории. А откуда же известно это качество Франклина? Дело в том, что изображение Франклина мы видим на стодолларовой банкноте, а каждый знает, что на лицевой стороне долларовых банкнот помещены заключённые в овал портреты американских президентов. И действительно, на однодолларовой купюре изображён первый президент Джордж Вашингтон, на двухдолларовой — третий президент Томас Джефферсон, на пятидолларовой — шестнадцатый президент Авраам Линкольн, на двадцатидолларовой — седьмой президент Эндрю Джэксон, на пятидесятидолларовой — восемнадцатый президент Улисс Грант. Однако попытка установить порядковый номер президентства Франклина встречает непреодолимые затруднения. Дело в том, что Франклин не был президентом США. (Как не был президентом США и Александр Гамильтон, чей портрет украшает десятидолларовую купюру.)

Только что был приведён наглядный пример провала метода неполной индукции. Тем не менее любой человек в своей повседневной жизни постоянно применяет и не может не применять этот метод. Вот, например, вы покупаете яблоки; вам предлагают попробовать; вы пробуете, яблоко вам нравится, и вы покупаете два кило, применив неполную индукцию, то есть рассуждая так: «Если одно яблоко хорошее, то и все хороши». Однако ведь не исключено, что, в отличие от выбранного вами на пробу образца, все купленные яблоки окажутся плохими. Да, не исключено, но надкусить *все* яблоки вам не дадут, потому что надкус выводит яблоко из категории товаров.

Если магазин, закупающий яблоки ящиками, серьёзно подходит к делу, он подвергнет дегустации не одно, а несколько яблок (но, конечно, не все яблоки) из каждого ящика. Если результат дегустации оказался положительным, магазин закупает все ящики целиком, то есть на практическом уровне принимает решение «все яблоки хорошие» — таким образом, опять-таки применяет неполную индукцию. Сходная процедура применяется при контроле качества многих товаров. Чтобы полностью проверить, хорошо ли сделана, скажем, электрическая лампочка, нужно её разбить, то есть уничтожить как товар. Поэтому, полный контроль партии в тысячу лампочек предполагает тотальное уничтожение всей партии. Разработана математическая теория, которая указывает, сколько яблок из ящика или лампочек из тысячи надо опробовать,

чтобы при положительном результате их исследования можно было с большой вероятностью заключить об исправности всех яблок или всех лампочек партии.

Строго говоря, даже универсальные законы природы формулируются лишь на основе отдельных наблюдений — то есть на основе метода неполной индукции. Поэтому и наши практические решения (типа решения о качестве яблок или лампочек), и наши теоретические суждения (типа законов природы), если они высказаны в виде универсальных формулировок, верны не в абсолютном смысле, а — в лучшем случае — лишь с высокой степенью правдоподобия. Иное дело математика, истины которой признаются незыблемыми. А потому и метод неполной индукции, действующий в естественных науках, в математике не действует.

В математике нередко случается, что частная формулировка $\mathbf{A}(n)$ оказывается верной для отдельных значений n, и вместе с тем не удаётся найти таких значений, для которых частная формулировка была бы неверна. Тогда есть основание выдвинуть *гипотезу* об истинности универсальной формулировки — но всего лишь гипотезу, потому что то́, что́ не удалось найти сегодня, будет, может быть, обнаружено завтра. Вот три замечательных примера, показывающих, что метод неполной индукции не работает в математике.

Пример 28. *Числа Ферма*. Великий французский математик XVII в. Пьер Ферма́ изучал числа вида $2^{2^n}+1$; эти числа стали называть *числами Ферма*. Ферма полагал, что все эти числа суть числа простые. Для такого мнения, казалось бы, имелись основания: ведь при $n=0, 1, 2, 3, 4$ числа Ферма и в самом деле являются простыми. Однако в XVIII в. великий швейцарский (да и российский тоже) математик Леонард Эйлер обнаружил, что число $2^{2^5}+1$ есть произведение двух простых чисел 641 и 6 700 417. Более того, неизвестно, существуют ли простые числа Ферма помимо вышеуказанных пяти, открытых ещё самим Ферма. □

Пример 29. *Трёхчлен Эйлера*. Трёхчлен x^2+x+41, указанный Эйлером, принимает простые значения при $x=0, 1, 2, \ldots, 39$. Однако при $x=40$ его значением будет число составное, а именно 41^2. □

Пример 30. *Двучлен* x^n-1. Если брать различные значения n и разлагать двучлен на множители с целыми коэффициентами, то можно заметить, что у каждого из многочленов-сомножителей все его коэффициенты равны либо 1, либо -1. Например, $x^6-1=(x-1)(x+1)(x^2+x+1)(x^2-x+1)$. Была выдвинута гипотеза,

что это обстоятельство справедливо для любого n. Однако доказать эту гипотезу почему-то не удавалось. А в 1941 г. выяснилось, что, хотя высказанное свойство коэффициентов разложения действительно верно при всех n до 104 включительно, в разложении на множители двучлена $x^{105}-1$ среди сомножителей появляется многочлен, у которого некоторые из коэффициентов равны -2. □

ПРЕДСТАВЛЕНИЕ О МАТЕМАТИЧЕСКИХ ДОКАЗАТЕЛЬСТВАХ МЕНЯЕТСЯ СО ВРЕМЕНЕМ

Великий французский математик Анри Пуанкаре писал в 1908 г.:

> Если мы читаем книгу, написанную пятьдесят лет назад, то рассуждения, которые мы в ней находим, кажутся нам большей частью лишёнными логической строгости.

Для иллюстрации приведём рассуждение из книги «Введение в анализ бесконечных». Правда книга была опубликована в 1748 г., то есть не за 50, а за 160 лет до высказывания Пуанкаре; зато сам пример очень нагляден. В названной книге встречаются такие странные, по нынешним меркам, утверждения: «$e^x=(1+x/i)^i$, где i означает бесконечно большое число»; «так как дуга $2k\pi/i$ бесконечно мала, то $\cos\frac{2k}{i}\pi=1-\frac{2k^2}{i^2}\pi^2$»; «член x^2/i^2 может быть опущен без опасения, потому что даже после умножения на i он останется бесконечно малым». В наши дни, скажи студент такое на экзамене, он получил бы двойку. Однако автор книги не кто иной, как великий математик Эйлер, а взятые нами в кавычки цитаты составляют часть доказательства одной из знаменитых формул Эйлера, а именно формулы для разложения синуса в бесконечное произведение:

$$\sin x=x\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{4\pi^2}\right)\left(1-\frac{x^2}{9\pi^2}\right)\dots\left(1-\frac{x^2}{n^2\pi^2}\right)\dots$$

Формула Эйлера и поныне составляет одну из жемчужин математического анализа. В середине XX века даже выяснилось, что и процитированным «странным» утверждениям Эйлера можно придать точный смысл на основе так называемого *нестандартного анализа* — но это уже совсем другая история.

Мы видим, таким образом, что само понимание того, что является, а что не является доказательством, меняется со временем. Если вдуматься, ничего удивительного в этом нет. Ведь понятие доказательства основано на представлении об убедительности, а это представление исторически обусловлено. Для средневековых судов,

например, доказательства виновности и невиновности были — с нашей точки зрения — очень своеобразны: если человек мог выдержать в руке раскалённое железо, то он признавался невиновным; если брошенная в воду связанная женщина не тонула, то её объявляли ведьмой. Понятие математического доказательства имеет те же психологические основы, что и понятие доказательства юридического, и потому также зависимо от исторических обстоятельств.

Для математических текстов средневековой Индии, например, были характерны такие (возможно, восходящие к более древним временам) способы доказывания геометрических утверждений: предлагался чертёж, под которым было всего одно слово: «Смотри!». На рис. 4 воспроизведено подобное индийское доказательство

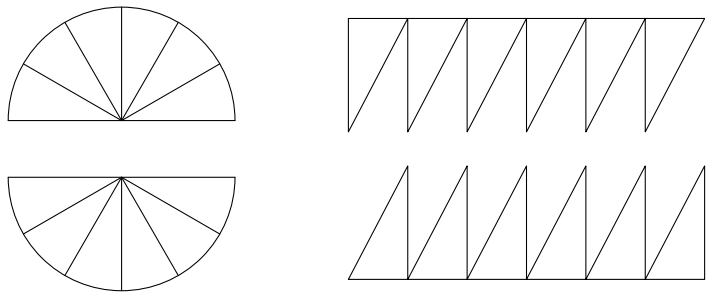


Рис. 4

формулы, выражающей площадь круга S через длину окружности l и радиус r.

Формула эта замечательна тем, что не использует числа π, осознание которого в качестве полноправного числа сталкивается с вполне естественными психологическими трудностями: ведь оно не представимо ни в виде дроби, ни даже в виде выражения с радикалами (то есть знаками корня), как это имеет место в случае диагонали единичного квадрата. Поэтому эта формула могла быть понятна и в древности. Найти её нетрудно. Поскольку $l = 2\pi r$, то в известной формуле площади круга число π можно заменить отношением длины полуокружности к радиусу:

$$S = \pi r^2 = \left(\frac{l}{2} : r\right) r^2 = \left(\frac{l}{2}\right) r.$$

Таким образом, площадь круга равна площади прямоугольника, основанием которого служит отрезок, равный по длине полуокружности этого круга, а высотой — его радиус.

Именно это наглядно показывает индийский чертёж, одновременно демонстрируя и доказательство. Сперва круг делится диаметром пополам, а потом каждый полукруг разрезается на большое и одинаковое для каждого полукруга количество равных секторов. Затем каждая из полуокружностей распрямляется, секторы превращаются в треугольники, и возникают две равные фигуры, по форме напоминающие пилу. Наконец, эти «пилы» так вставляются друг в друга, чтобы зубцы одной пилы полностью вошли в промежутки другой. Возникает прямоугольник, равный по площади исходному кругу и имеющий требуемые длины сторон. «Что за чушь, — скажет педант XXI века. — При распрямлении дуг секторы превратятся в Бог знает что и не смогут совпасть с промежутками между «зубцами», да и площади их исказятся. И прямоугольник выйдет кривобокий. Так что никакое это не доказательство».

Однако для индийцев это было доказательством. И его убедительность не испарилась с веками: ведь при разбиении на *очень большое* количество секторов все справедливо отмеченные педантом искажения будут почти незаметны. Так что при большом желании и готовности потрудиться индийское рассуждение можно облечь в форму, приемлемую и сегодня.

Для полноты картины приведём индийское доказательство теоремы Пифагора. Это тоже чертёж со словом «Смотри!». Заметим, что

$$a^2+b^2=ab+ab+(a-b)^2.$$

Поэтому теорему Пифагора, утверждающую, что для прямоугольного треугольника с катетами a и b и гипотенузой c справедливо равенство $a^2+b^2=c^2$, можно доказывать в форме:

$$c^2=ab+ab+(a-b)^2.$$

Последняя формула и доказывается рисунком[1] 5. Слева на рисунке квадрат с площадью c^2, составленный из четырёх одинаковых треугольников и квадрата со стороной $a-b$. Справа изображён тот же квадрат со стороной $a-b$, а треугольники уложены так, что образовались два одинаковых прямоугольника со сторонами a и b. Заметим, что — в отличие от предыдущего — это рассуждение полностью приемлемо и сегодня.

[1] Рисунок заимствован со с. 130 книги: *Ф. Кэджори*. История элементарной математики (с некоторыми указаниями для препод.) Пер. с англ. — Одесса: MATHESIS, 1910.

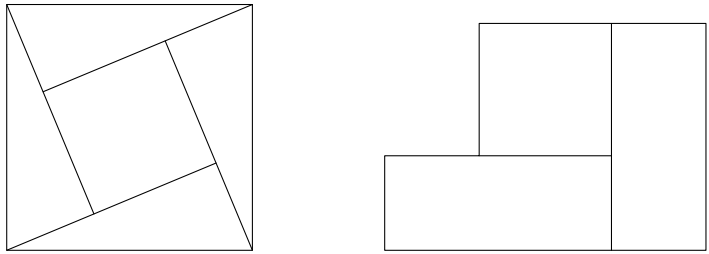


Рис. 5

Наш рисунок 5 с подписью «Смотри!» встречается в трудах индийского астронома и математика XII века Бха́скары. Можно предположить, что он встречался в ещё более ранних индийских текстах. В пользу такого предположения говорит, в частности, то, что левый чертёж из рисунка 5 мы находим в китайском трактате, датируемом не позже, чем III веком. Китайский текст, однако, не довольствуется призывом «Смотри!», а заменяет его алгебраическим пояснением. В упомянутом тексте предлагалось и другое — пожалуй, ещё более простое и наглядное доказательство теоремы Пифагора. Это второе доказательство показано на рисунке 6. Ки-

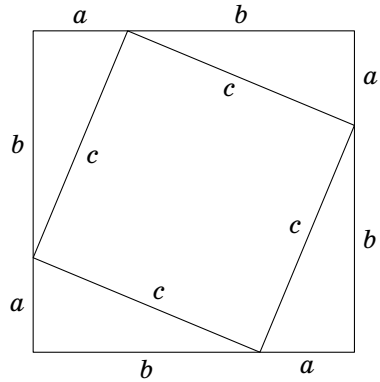


Рис. 6

тайский текст и в этом случае сопровождал чертёж необходимым пояснением; мы же, на индийский манер, ограничимся словом «Смотри!». Для точности укажем, что китайский чертёж состоял из наложенных друг на друга чертежей из наших рисунков 5 и 6, давая таким образом одновременно два доказательства теоремы Пифагора.

В древних египетских текстах встречаются рецепты оперирования с простыми дробями — не со всеми, а с некоторыми избранными: аликвотными (так принято называть дроби с числителем 1) и дробью 2/3. Встречаются также рецепты вычисления простейших площадей. Но все эти рецепты приводятся без какого бы то ни было обоснования. По-видимому, в то время не было психологической необходимости в таком обосновании. Убедительность заключалась в том, что рецепт, во-первых, исходил из авторитетного источника, как правило жреца, и во-вторых, был записан. (Не так ли подчас и мы относимся к медицинским рецептам?) Жившие в советское время помнят, что любое утверждение считалось полностью доказанным, коль скоро его удавалось обнаружить в каком-либо из текстов Маркса или Ленина. В сталинское же время ещё более неоспоримыми были тексты Сталина. (Так что официальная ментальность того времени недалеко ушла от ментальности Древнего Египта.)

Первые математические доказательства, в современном их понимании, приписывают древнегреческим мыслителям Фалéсу и Пифагору. Считается, что именно в Древней Греции в VII—VI веках до нашей эры возник новый, до того не встречавшийся обычай: сопровождать математический факт его обоснованием. Появилась потребность не просто сообщать данный факт, но и убеждать слушателя в его истинности, то есть проводить доказательство. По-видимому, сама идея необходимости убеждать слушателей появилась в дискуссиях в народных собраниях и в судах. (В этом смысле математика — младшая сестра юриспруденции.)

Древнегреческие доказательства были почти безупречны с современной точки зрения. Положение вещей стало меняться с XVII века, когда в математику вошли переменные величины, а вместе с ними — представление о предельном переходе. С сегодняшней точки зрения эти понятия и представления не были достаточно чёткими, а потому и относящиеся к ним доказательства XVII и XVIII веков кажутся теперь нестрогими: вспомним хотя бы приведённые выше цитаты из книги Эйлера. Замечательно, однако, что эти нестрогие доказательства приводили к строгим результатам, прочно вошедшим в арсенал современной математики.

Так продолжалось до 20-х годов XIX в., когда появились работы знаменитого французского математика Огюстена Луи Коши́; в его трудах понятие предела и опирающиеся на него понятия впервые стали приобретать ту логическую форму, которую они

имеют сегодня. Инициатива Коши была развита затем многими математиками, прежде всего, уже во второй половине XIX в., знаменитым немецким математиком Карлом Вейерштрассом. Но новые представления о необходимом уровне математической строгости входили в математику не сразу, о чём свидетельствует открывающее этот раздел высказывание Пуанкаре. Напрашивается предположение, что представления о строгости будут развиваться и впредь и то, что кажется строгим сегодня, не покажется таковым в будущем.

Уже сейчас видно одно из направлений, по которым может развиваться пересмотр представлений об убедительности математических доказательств. Дело в том, что само понимание того, что такое математическая истина, вызывает серьёзные затруднения. Ведь математические объекты, в отличие от объектов физических, не присутствуют в природе, они существуют лишь в умах людей. Поэтому говорить, что истина — это то, что соответствует реальному положению вещей, можно, в применении к математическим истинам, лишь с большой натяжкой.

Чтобы закончить этот раздел на оптимистической ноте, подчеркнём, что доказательства, содержащиеся в трудах Евклида и Архимеда, не потеряли свою убедительность за прошедшие тысячи лет.

ДВА АКСИОМАТИЧЕСКИХ МЕТОДА — НЕФОРМАЛЬНЫЙ И ФОРМАЛЬНЫЙ

Неформальный аксиоматический метод

Поиски большей убедительности математических доказательств привели к появлению так называемого аксиоматического метода. Вкратце он состоит в следующем. Выбираются основные положения рассматриваемой математической теории, которые принимаются без доказательств, а из них уже все остальные положения выводят чисто логическими рассуждениями. Эти основные положения получили название *аксиом*, а те, которые из них выводятся, — *теорем*. Ясно, что всякая аксиома также выводится из списка аксиом, поэтому удобно аксиомы рассматривать как частный случай теорем (в противном случае слову «теорема» надо было бы дать такое длинное определение: теорема — это то, что выводится из списка аксиом, однако в этот список не входит).

Первая попытка создать систему аксиом для какой-нибудь теории была предпринята Евклидом в III веке до н. э. Система аксиом из его «Начал» оставалась единственной системой аксиом геомет-

рии вплоть до конца XIX века, когда появились новые системы, отвечающие современным требованиям. Вот как Евклид определяет, что такое *точка* и что такое *прямая*: «точка есть то, что не имеет частей», «прямая линия есть та, которая равно расположена к точкам на ней». С современнных позиций эти определения непонятны и не могут быть использованы в доказательствах.

А как же определяются точка и прямая в современных аксиоматических системах? Ответ может удивить неискушённого читателя (искушённого читателя ничто не может удивить). Эти понятия не определяются никак. Не определяется и значение слов «точка лежит на прямой», «прямая проходит через точку». Если вдуматься, то чего-то подобного, то есть предъявления основных понятий без определения, и следовало ожидать — ведь всё определить невозможно: одно определяется через другое, другое через третье, и где-то приходится остановиться. Уж лучше сделать такую остановку честно и открыто. Спрашивается, а как же в таком случае можно использовать эти понятия в доказательствах. Вот тут на помощь и приходят аксиомы.

В аксиомах вместо определений основных понятий формулируются их главные, исходные свойства. На эти свойства и опираются доказательства. Поясним сказанное на примере. Среди основных понятий геометрии присутствуют такие: „точка“, „прямая“, „лежать на“, „лежать между“. Что такое точки и прямые, не разъясняется, а говорится лишь, что бывают такие объекты, одни называются *точками*, другие — *прямыми*. А про *лежать на* говорится, что это некоторое отношение между точками и прямыми. Это означает следующее: если взять произвольную точку и произвольную прямую, то осмысленно спросить, лежит ли эта точка на этой прямой; точка либо *лежит на* прямой, либо нет. А вот спрашивать, скажем, лежит ли прямая на прямой, бессмысленно: отношение „лежать на“ для пары прямых не определено — как не определено оно и для пары точек, и для пары ⟨прямая, точка⟩. *Лежать между* — это некоторое трёхместное отношение между точками; сказанное означает, что если даны три точки A, B, C, то точка B либо *лежит между* точками A и C, либо нет. Природа предметов „точка“ и „прямая“ и отношений „лежать на“ и „лежать между“ никак не раскрывается. Вместо этого в аксиомах формулируются основные свойства этих объектов и отношений и основные связи между ними.

Вот как выглядят некоторые из аксиом:

1. *На каждой прямой лежат по меньшей мере две точки.*

2. *Для двух различных точек не может существовать более одной такой прямой, что обе точки лежат на этой прямой.*

3. *Если три точки таковы, что одна из них лежит между двумя другими, то все эти три точки различны.*

4. *Если три точки таковы, что одна из них лежит между двумя другими, то все эти три точки лежат на одной прямой.*

5. *Для любых двух различных точек A и B существует такая точка C, что B лежит между A и C.*

Покажем на примере, как на основе аксиом проводят доказательства. Докажем, опираясь на выписанные пять аксиом, такую теорему:

На каждой прямой лежат по меньшей мере три точки.

Вот доказательство. Итак, пусть p — прямая. Надо обнаружить на ней три различные точки. По аксиоме 1 на ней лежат какие-то две различные точки; обозначим их A и B. По аксиоме 5 находим такую точку C, что B лежит между A и C. Согласно аксиоме 3 все они различны, а согласно аксиоме 4 все они лежат на одной прямой. Обозначим эту прямую буквой q. Точки A и B лежат на прямой p и в то же время лежат на прямой q. Но в силу аксиомы 2 две различные точки не могут лежать на двух различных прямых; следовательно, q совпадает с p. Поскольку через q была обозначена та прямая, на которой лежат все три точки A, B и C, а q совпадает с p, то все эти точки лежат на p. Вот мы и нашли на p три различные точки.

Казалось бы, тем же способом можно далее доказать, что на p лежат четыре точки: надо применить аксиому 5 к точкам B и C и получить такую точку D на той же прямой, что C лежит между B и D. Действительно, все точки B, C и D будут различны; однако ведь может случиться, что точка D совпадает с точкой A, — из аксиом не вытекает, что такое невозможно!

Ещё один пример. Дано множество N каких-то объектов. Задана операция, которая каждому объекту из N ставит в соответствие некоторый другой (а впрочем, может случиться, что и тот же самый) объект из того же N. Объект, ставящийся в соответствие объекту x, будем обозначать так: x'. Некоторый объект из N выделен особо, его будем обозначать так: 0. Всё это подчиняется двум аксиомам:

Аксиома I. *Если $x' = y'$, то $x = y$.*

Аксиома II. *Не существует такого x, что $x' = 0$.*

Требуется доказать утверждение

$$0'''' \neq 0''.$$

Доказываем от противного. Предположим, что

$$0'''' = 0''.$$

В силу первой аксиомы тогда

$$0''' = 0'.$$

В силу той же первой аксиомы получим

$$0'' = 0.$$

Но это противоречит второй аксиоме, потому что получается, что 0 есть результат применения операции $'$ к объекту $0'$. Точно так же доказывается различие любых двух объектов вида $0''\cdots'$, имеющих в своей записи различное количество штрихов. Поэтому выражения

$$0,\ 0',\ 0'',\ \ldots$$

часто используются в качестве обозначений натуральных чисел (включая нуль). Если принять эти обозначения, то видно, что только что была доказана формула $4 \neq 2$.

Заметим, что доказательства в обоих примерах понимались в соответствии с разъяснениями, предложенными в начальном разделе данного очерка, — как убедительные рассуждения. Специфика состояла в том, что мы не знали, о каких сущностях идёт речь. Мы не знали, что такое точка, прямая, отношение „лежать на“ и „лежать между“ в первом примере. Во втором примере мы не знали ни какие объекты образуют множество N, ни который из них выделен, ни в чём состоит операция штрих ($'$), ставящая в соответствие каждому объекту x объект x'. Мы знали лишь те свойства этих таинственных сущностей, которые были перечислены в аксиомах, и именно на эти свойства и только на них опирались в рассуждениях, образующих доказательства. Таким образом, сами наши доказательства были неформальными, психологическими доказательствами. Поэтому тот вариант аксиоматического метода, который был проиллюстрирован на двух примерах, принято называть *неформальным аксиоматическим методом*.

Формальный аксиоматический метод

Формальный аксиоматический метод отличается от неформального тем, что в нём совершенно чётко перечисляются не

только исходные понятия, не только записанные в виде аксиом исходные положения, но и дозволенные способы рассуждения. Точно указываются те логические переходы, которые разрешается делать. Более того: и аксиомы, и разрешённые логические переходы должны быть оформлены таким образом, чтобы первые могли использоваться, а вторые делаться чисто механически, чтобы мы могли не вникать в их содержание, — так, чтобы и то, и другое было доступно исполнительному лаборанту или, как уместнее сказать в наше время, компьютеру. Для этого нужно уметь оперировать с участвующими в доказательствах утверждениями, опираясь только на их внешний вид, а не на содержание, непонятное ни лаборанту, ни компьютеру. Такое оперирование довольно затруднительно, если утверждения записаны на *естественном языке*, то есть на одном из тех языков, которыми пользуются люди в повседневной жизни. Приходится записывать утверждения на специальном языке, отражающем структуру утверждений.

Скажем, тот факт, что из **A** следует **B**, на русском языке может быть записан многими разными способами: «из **A** следует **B**», «из **A** вытекает **B**», «если **A**, то **B**», «**B** верно при условии, что верно **A**», «**B** верно при условии, что справедливо **A**», «**B** справедливо при условии, что верно **A**», — и ещё многими другими, которые, без сомнения, сможет предложить любезный читатель. Заставить компьютер во всём этом разбираться было бы слишком накладно. А ведь помимо русского языка существуют ещё немало и других. В специальном, искусственном языке математической логики (точнее было бы сказать: в одном из орфографических вариантов такого языка) указанный факт записывается так:

$$(\mathbf{A} \Rightarrow \mathbf{B}).$$

Аналогично вместо того, чтобы анализировать все способы, которыми в русском языке можно выразить тот факт, что утверждение **A** неверно, пишут просто $\neg\mathbf{A}$.

Вот здесь очень важное отличие формального аксиоматического метода от неформального. Для неформального метода несущественно, на каком языке — на древнегреческом, русском или китайском — записаны утверждения. Для формального метода утверждений вне способов записи как бы не существует. Поэтому грамотнее говорить, что формальный метод имеет дело не с утверждениями, а с *предложениями*.

Посмотрим, например, в каком виде рассуждение «от противного» выглядит в рамках формального метода. На содержательном уровне это рассуждение происходит по следующей схеме:

из двух утверждений, (1) и (2):

(1) **B**,

(2) из утверждения **не-A** (то есть из отрицания утверждения **A**) следует утверждение **не-B** (то есть отрицание утверждения **B**)

— вытекает утверждение **A**.

В формальном методе указанное содержательное рассуждение оформляется в виде такого правила: если доказано предложение **B** и доказано предложение $(\neg\mathbf{A}\Rightarrow\neg\mathbf{B})$, то считается доказанным и предложение **A**.

Подобные правила носят название *правил вывода*. Они должны быть перечислены исчерпывающим образом. Их соединение с аксиомами приводит к тому, что некоторые предложения объявляются *доказуемыми*. Сперва доказуемыми объявляются все аксиомы, а затем провозглашается, что применение любого правила вывода к любым доказуемым предложениям даёт доказуемое предложение.

Проиллюстрируем сказанное на примере того, как в формальном методе доказывается утверждение $0''''\neq 0''$, содержательный вывод которого из аксиом-утверждений был проведён выше.

Прежде всего надо построить тот язык, в виде предложений которого будут записываться как аксиомы, так и все другие задействованные утверждения. Построение языка начинается с предъявления *алфавита*, то есть списка символов, которые мы собираемся использовать. Для наших целей удобен такой алфавит:

$$(\quad)\quad\Rightarrow\quad\neg\quad\exists\quad=\quad x\quad y\quad 0\quad '$$

Символы алфавита принято называть *буквами*, а цепочки букв — *словами*.

Каждое предложение, таким образом, является словом в только что определённом смысле. Придирчивый читатель может спросить, все ли слова являются предложениями, а если нет, то какой процедурой они, предложения, выделяются среди всех слов. Ответим ему так: для наших локальных целей это знать необязательно, и он может спокойно всюду заменить встречающийся ниже термин «предложение» (коль скоро он представляется ему непонятным) на термин «слово». (Как сказал ещё принц Гамлет, *слова, слова, слова*.)

Внимательный читатель заметит, что в выписанном алфавите отсутствует буква $\neq$. Она излишня, потому что вместо $a\neq b$ можно писать $\neg(a=b)$.

Слова вида 0, $0'$, $0''$, $0'''$, ... называют *нумералами*. Через $A(m)$ будем обозначать то слово, которое получается из слова A подстановкой нумерала m вместо x. Например, если A есть $))'yx\neg x''($, а m есть $0''$, то $A(m)$ есть $))'y0''\neg 0''''($. Через $A(m, n)$ будем обозначать то слово, которое получается из слова A одновременной подстановкой нумерала m вместо x и нумерала n вместо y. Сами такие подстановки будем обозначать записями $x \to m$, $y \to n$. Например:

если A есть $(x'' = x')$, а подстановка есть $x \to m$, то $A(m)$ есть $(m'' = m')$;

если A есть $(x'' = y')$, а подстановки суть $x \to m$, $y \to n$, то $A(m, n)$ есть $(m'' = n')$.

При помощи букв нашего алфавита запишем аксиомы в виде предложений:

Аксиома I: $(x' = y') \Rightarrow (x = y)$

Аксиома II: $\neg\exists x(x' = 0)$

Далее, сформулируем правила вывода. Каждое правило договоримся записывать в виде дроби, где в числителе — то предложение или те предложения, к которым это правило применяется, в знаменателе — результат применения. В скобках после названия правила пишем его условное обозначение. Правил будет четыре:

(1) Правило *modus ponens* (MP), оно же «правило *зачеркивания*»

$$\frac{A \Rightarrow B,\ A}{B}.$$

(2) Правило *обращения* ($\Rightarrow \neg$)

$$\frac{A \Rightarrow B}{\neg B \Rightarrow \neg A}.$$

(3) Правило *несуществования* ($\neg\exists$)

$$\frac{\neg\exists x A}{\neg A(m)}.$$

(4) Правило *конкретизации* (C), оно же «правило *перехода от общего к частному*»

$$\frac{A}{A(m,\ n)}.$$

Покажем, что предложение $\neg(0'''' = 0'')$ доказуемо. Для этого предъявим список из девяти доказуемых предложений, справа от каждого из них указав в квадратных скобках причину, по которой оно признаётся доказуемым. Если предложение является аксиомой, указываем номер аксиомы; если оно получается из

предыдущих предложений списка по одному из правил, указываем номера этих предложений в списке и это правило. Вот этот список:

1. $\neg\exists x(x'=0)$ [Ax. II]
2. $\neg(0''=0)$ $[1;\ \neg\exists : x\to 0']$

Временно прервём выписывание списка, чтобы сделать два комментария. Первый комментарий: мы только что установили доказуемость предложения $\neg(0''=0)$. На содержательном уровне это предложение выражает тот интересный факт, что два не равно нулю. Второй комментарий: уже выписанные две строки позволяют заметить одну важную особенность формального метода, отличающую его от метода неформального. Вспомним, что, излагая неформальный метод, аксиому II мы записали так: *Не существует такого x, что* $x'=0$. Ясно, что смысл аксиомы не изменился бы, выбери мы для неё такую запись: *Не существует такого y, что* $y'=0$. Поэтому доказательство утверждения $0''''\neq 0''$, предъявленное нами в рамках неформального метода, осталось бы прежним. А вот если бы мы в формальном методе заменили аксиому $\neg\exists x(x'=0)$ на аксиому на $\neg\exists y(y'=0)$, то получить предложение $\neg(0''=0)$ нам бы не удалось, поскольку правило $\neg\exists$ разрешает подстановку именно вместо буквы x, а не вместо буквы y. Формальный метод на то и называется формальным, что форма записи имеет здесь главенствующее значение. Продолжим список.

3. $(x'=y')\Rightarrow(x=y)$ [Ax. I]
4. $(0'''=0')\Rightarrow(0''=0)$ $[3;\ C\colon x\to 0'',\ y\to 0]$
5. $\neg(0''=0)\Rightarrow\neg(0'''=0')$ $[4;\ \Rightarrow\neg]$
6. $(0''''=0'')\Rightarrow(0'''=0')$ $[3;\ C\colon x\to 0''',\ y\to 0']$
7. $\neg(0'''=0')\Rightarrow\neg(0''''=0'')$ $[6;\ \Rightarrow\neg]$
8. $\neg(0'''=0')$ [5, 2; MP]
9. $\neg(0''''=0'')$ [7, 8; MP]

Остаётся заметить, что последним в списке стоит интересующее нас предложение $\neg(0''''=0'')$.

Если мы теперь запишем все эти 9 предложений друг за другом, разделив их каким-нибудь разделительным знаком, для определённости — решёткой #, то получим то, что называется *формальным доказательством* предложения $\neg(0''''=0'')$:

$$\neg\exists x(x'=0)\#\neg(0''=0)\#(x'=y')\Rightarrow(x=y)\#(0'''=0')\Rightarrow(0''=0)\#$$
$$\#\neg(0''=0)\Rightarrow\neg(0'''=0')\#(0''''=0'')\Rightarrow(0'''=0')\#$$
$$\#\neg(0'''=0')\Rightarrow\neg(0''''=0'')\#\neg(0'''=0')\#\neg(0''''=0'').$$

На этом примере состоялось знакомство с важнейшим понятием *формального доказательства*. Неформальные доказательства

(которые называют ещё содержательными или психологическими доказательствами) представляют собою убедительные рассуждения, то есть, прежде всего, тексты, состоящие из утверждений (не любые такие тексты, разумеется). Формальное же доказательство есть цепочка предложений, особым образом организованная. Читатель может возразить, что в начальном разделе статьи сообщалось, что формальное доказательство есть цепочка символов. Тут нет противоречия: ведь каждое предложение есть цепочка символов, и если составить их вместе, разделив каким-либо разделительным знаком, то снова возникнет не что иное, как цепочка символов, — как это и было видно на нашем примере. Таким образом, формальное доказательство есть слово, составленное из букв дополненного разделительным знаком алфавита.

Общее определение формального доказательства очевидно. *Формальное доказательство* есть такая цепочка предложений, каждое предложение которой либо является аксиомой, либо получается из каких-то предшествующих предложений цепочки применением одного из правил вывода.

Возьмём любое формальное доказательство, а в нём какое-либо его подслово (то есть часть слова, образованную подряд идущими буквами слова), не содержащее знака решётки и представляющее собою такую часть слова, которая ограничена решётками слева и справа, либо же начало слова, ограниченное решёткой справа, либо же конец слова, ограниченный решёткой слева. Всякое такое подслово является доказуемым предложением. Если это предложение представляет собою конец формального доказательства, то это формальное доказательство называется *формальным доказательством данного предложения*. Ясно, что предложение тогда и только тогда является доказуемым, когда оно имеет формальное доказательство.

Теорема Гёделя

Словосочетание «теорема Гёделя» довольно популярно, и не только в математической среде. И это совершенно заслуженно. Ведь теорема Гёделя (точнее, *теорема Гёделя о неполноте*) — не только одна из самых замечательных и неожиданных теорем математической логики, да и всей математики, но, пожалуй, единственная на сегодняшний день теорема теории познания.

Если говорить совсем грубо, теорема Гёделя утверждает, что не всё можно доказать, если говорить чуть более точно — что существуют истинные утверждения, которые нельзя доказать, а по-

дробнее — что такие утверждения найдутся даже среди утверждений о натуральных числах. Но эта формулировка заключает в себе некое противоречие. В самом деле, если мы обнаружили истинное утверждение, которое невозможно доказать, то откуда, спрашивается, мы знаем, что оно истинное? Ведь чтобы убеждённо заявлять о его истинности, мы должны эту истинность доказать. Но тогда как же можно говорить о его недоказуемости?

Разгадка в том, что в грубых, подобно приведённым, формулировках теоремы Гёделя смешиваются два понятия доказательства — содержательное (неформальное, психологическое) и формальное. Теорему Гёделя надлежит понимать в следующем смысле: существуют не имеющие формального доказательства утверждения, являющиеся тем не менее истинными, причём истинность их подтверждается содержательными доказательствами. Иными словами, эти утверждения доказуемы содержательно и недоказуемы формально. Отметим, что в применении к какому бы то ни было утверждению более корректно было бы говорить о формальных доказательствах не самого этого утверждения, а предложения, служащего записью этого утверждения в виде слова, составленного из букв подходящего алфавита. Однако мы этого делать не будем, чтобы не утяжелять изложения.

Указанный смысл нуждается в дальнейшем уточнении. Ведь понятие формального доказательства осмысленно лишь тогда, когда предъявлены аксиомы и правила вывода. Достаточно взять любое утверждение и включить его в число аксиом — и оно тут же сделается доказуемым формально. Точная, хотя и требующая разъяснений, формулировка теоремы Гёделя такова: *если язык достаточно богат, то какой бы список аксиом и какой бы список правил вывода ни предъявить, в этом языке найдётся истинное утверждение о натуральных числах, не имеющее формального доказательства*.

Жанр данного очерка не позволяет дать предложенной «точной» формулировке исчерпывающих объяснений. Но некоторые намётки всё же сделаем.

Под *утверждениями о натуральных числах* понимаются такие утверждения, которые помимо общелогических понятий (таких как «и», «если ..., то», «существует», «равно» и тому подобных) используют в своих формулировках лишь натуральные числа и операции сложения и умножения.

Под *достаточным богатством языка* понимается его способность выражать некоторые утверждения о натуральных числах. Чтобы было понятно, что имеется в виду, заметим, что тот язык,

на примере которого выше демонстрировался формальный аксиоматический метод, является «бедным»: в нём выразимы лишь очень простые утверждения о натуральных числах, а именно такие утверждения, которые можно сформулировать, используя лишь обозначения чисел (то есть нумералы), операцию штрих ($'$) и общелогические понятия «равно», «существует», «неверно, что», «если ..., то». Богатство же языка означает его способность выражать более сложные утверждения о числах: требуется, чтобы для любого перечислимого множества натуральных чисел в языке имелась формула, выражающая принадлежность к этому множеству натурального числа. Дальнейшие объяснения потребовали бы изложения основ математической логики и теории алгоритмов, а потому здесь мы остановимся.

ОГЛАВЛЕНИЕ

БИБЛИОТЕКА «МАТЕМАТИЧЕСКОЕ ПРОСВЕЩЕНИЕ»

1. В. М. Тихомиров
Великие математики прошлого и их великие теоремы

2. А. А. Болибрух
Проблемы Гильберта (100 лет спустя)

3. Д. В. Аносов
Взгляд на математику и нечто из неё

4. В. В. Прасолов
Точка Брокара и изогональное сопряжение

5. Н. П. Долбилин
Жемчужины теории многогранников

6. А. Б. Сосинский
Мыльные плёнки и случайные блуждания

7. И. М. Парамонова
Симметрия в математике

8. В. В. Острик, М. А. Цфасман
Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые

9. Б. П. Гейдман
Площади многоугольников

10. А. Б. Сосинский
Узлы и косы

11. Э. Б. Винберг
Симметрия многочленов

12. В. Г. Сурдин
Динамика звёздных систем

13. В. О. Бугаенко
Уравнения Пелля

14. В. И. Арнольд
Цепные дроби

15. В. М. Тихомиров
Дифференциальное исчисление (теория и приложения)

16. В. А. Скворцов
Примеры метрических пространств

17. В. Г. Сурдин
Пятая сила

18. А. В. Жуков
О числе π

19. А. Г. Мякишев
Элементы геометрии треугольника

20. И. В. Ященко
Парадоксы теории множеств

21. И. Х. Сабитов
Объёмы многогранников

22. А. Л. Семёнов
Математика текстов

23. М. А. Шубин
Математический анализ для решения физических задач

24. А. И. Дьяченко
Магнитные полюса Земли

25. С. М. Гусейн-Заде
Разборчивая невеста

26. К. П. Кохась
Ладейные числа и многочлены

27. С. Г. Смирнов
Прогулки по замкнутым поверхностям

28. А. М. Райгородский
Хроматические числа

29. С. Б. Гашков
Системы счисления и их применение

30. Ю. П. Соловьёв
Неравенства

31. В. Ю. Протасов
Максимумы и минимумы в геометрии

32. А. В. Хачатурян
Геометрия Галилея

33. А. М. Райгородский
Проблема Борсука

34. В. А. Успенский
Простейшие примеры математических доказательств

35. И. Д. Жижилкин
Инверсия

36. А. М. Райгородский
Остроугольные треугольники Данцера—Грюнбаума

37. В. В. Ерёмин
Математика в химии