Содержание

От издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Cambridge University Press очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Предисловие к третьему изданию

Читатели, изучающие математику и информатику, часто впадают в замешательство, когда их впервые просят серьезно потрудиться над математическими доказательствами, потому что они не знают «правил игры». Что от вас ждут, когда просят что-то доказать? Что отличает правильное доказательство от неправильного? Эта книга призвана помочь читателям узнать ответы на эти вопросы, разъясняя основные принципы, используемые при построении доказательств.

Многие читатели впервые знакомятся с математическими доказательствами на курсе геометрии в средней школе. К сожалению, школьников, изучающих геометрию, обычно учат думать о доказательстве как о пронумерованном списке утверждений и причин, а такое представление слишком ограниченно, чтобы быть полезным. Здесь есть поучительная параллель с информатикой. Ранние языки программирования поощряли аналогичный ограниченный взгляд на компьютерные программы в виде нумерованных списков инструкций. Теперь программисты-разработчики отошли от подобных языков и продвигают подход, называемый «структурным программированием». Обсуждение доказательств в этой книге основано на убеждении, что многие соображения, которые побудили программистов принять структурированный подход к программированию, применимы и к написанию доказательств. Можно сказать, что эта книга учит «структурированному доказательству».

В структурированном программировании компьютерная программа создается не путем перечисления инструкций друг за другом, а путем объединения определенных базовых структур, таких как конструкция `if-else` и цикл `do-while` языка программирования Java. Эти структуры объединяются не только путем перечисления по порядку, но и путем *вложения* друг в друга. Например, программа, созданная вложением конструкции `if-else` в цикл `do-while`, будет выглядеть так:

```
do
   if [условие]
      [Список операторов программы]
   else
      [Альтернативный список операторов программы]
while [условие]
```

Отступы в такой программе не являются абсолютно необходимыми, но это удобный метод, часто используемый в информатике для отображения основной структуры программы.

Математические доказательства также строятся путем объединения некоторых базовых структур доказательства. Например, при доказательстве утверждения вида «если *P*, то *Q*» часто используется то, что можно было бы назвать структурой «предполагать, пока»: мы *предполагаем*, что *P* истинно, *пока* не сможем прийти к заключению, что *Q* истинно, в этот момент мы отказываемся от предположения и заключаем, что утверждение «если *P*, то *Q*» истинно. Другой пример – структура «доказательства для произвольного *x*»: чтобы доказать утверждение вида «для всех *x* *P*(*x*)», мы *объявляем x как произвольный объект*, а затем *доказываем P*(*x*). Как только мы приходим к выводу, что *P*(*x*) истинно, мы отказываемся от объявления *x* как произвольного и заключаем, что утверждение «для всех *x* *P*(*x*)» истинно. Более того, чтобы доказать более сложные утверждения, эти структуры часто объединяют, не только перечисляя одну за другой, но также вкладывая одну в другую. Например, чтобы доказать утверждение вида «для всех *x* если *P*(*x*), то *Q*(*x*)», мы, вероятно, вложим структуру «предполагать, пока» в структуру «доказательства для произвольного *x*», получив следующее доказательство:

```
Пусть x произвольно.
   Предположим, что P(x) истинно.
      [Далее идет доказательство Q(x).]
   Таким образом, если P(x), то Q(x).
Таким образом, для всех x если P(x), то Q(x).
```

Как и раньше, мы использовали отступы, чтобы прояснить основную структуру доказательства.

Конечно, математики обычно не пишут свои доказательства в строгой форме с отступом. Наша цель в этой книге – научить читателей излагать доказательства обычным текстом, как это делают все математики. Тем не менее наш подход основан на убеждении, что если читатели хотят преуспеть в написании таких доказательств, они должны понимать основную структуру, которую имеют доказательства. Они должны усвоить, например, что выражения типа «Пусть *x* будет произвольным» и «Предположим, *P*» не являются изолированными шагами в доказательствах, а используются для введения структур доказательства «доказать для произвольного *x*» и «предполагать, пока». Начинающие математики нередко неправильно используют эти предложения в других целях. Такие ошибки аналогичны использованию в программе оператора `do` без парного оператора `while`.

Обратите внимание, что в наших примерах выбор структуры доказательства определяется логической формой доказываемого утверждения. По этой причине книга начинается с элементарной логики, чтобы познакомить читателей с различными формами математических выражений. В главе 1 обсуждаются логические связки, а в главе 2 представлены кванторы. В этих главах также представлены основы теории множеств, поскольку это важный предмет, который используется в остальной части книги (и во всей математике), а также потому, что он служит для иллюстрации многих логических выкладок, обсуждаемых в этих главах.

В главе 3 рассматриваются методы структурированного доказательства, упоминаются различные формы, которые могут принимать математиче-

ские утверждения, и обсуждаются структуры доказательства, подходящие для каждой формы. Примеры доказательств в этой главе по большей части выбраны не из-за их математического содержания, а из-за структур доказательства, которые они иллюстрируют. Это особенно верно в начале главы, когда мы только начинаем обсуждать некоторые методы, и в результате многие доказательства в этой части главы довольно тривиальны. По мере продвижения по главе доказательства становятся все более сложными и интересными с математической точки зрения.

Главы 4 и 5, посвященные отношениям и функциям, служат двум целям. Во-первых, они предоставляют материал, на котором читатели могут отрабатывать приемы доказательства из главы 3. И во-вторых, они знакомят читателей с некоторыми фундаментальными концепциями, используемыми во всех областях математики.

Глава 6 посвящена методу доказательства, который очень важен как в математике, так и в информатике: математической индукции. Изложение основано на методах из главы 3, которыми читатели должны были овладеть к этому моменту в книге.

После завершения главы 6 читатели должны быть готовы перейти к более существенным математическим темам. Две такие темы представлены в главах 7 и 8. Глава 7, новая в этом третьем издании, дает введение в теорию чисел, а в главе 8 мы обсуждаем бесконечные мощности. Эти главы развивают у читателей навык математических доказательств, а также дают представление о том, на что похожа более продвинутая математика.

Каждый раздел каждой главы заканчивается списком упражнений. Некоторые упражнения отмечены звездочкой; решения или подсказки для этих упражнений приведены в приложении. Упражнения, отмеченные символом P_D, можно выполнять с помощью программного обеспечения Proof Designer, которое бесплатно доступно в интернете.

Самыми большими изменениями в этом третьем издании являются добавление новой главы по теории чисел, а также более 150 дополнительных упражнений. Раздел о рефлексивных, симметричных и транзитивных замыканиях отношений был удален из главы 4 (хотя эти темы теперь включены в некоторые упражнения в разделе 4.4); он был заменен новым разделом в главе 5 о замыканиях множеств по функциям. По всему тексту также есть множество мелких изменений.

Я хотел бы поблагодарить всех, кто прислал мне комментарии к более ранним изданиям этой книги. В частности, Джон Коркоран и Раймонд Бут сделали несколько полезных предложений. Я также благодарен за советы Джонатану Сэндсу и нескольким анонимным рецензентам.

Введение

Что такое математика? Математика в старших классах школы в основном занимается решением уравнений и вычислением ответов на числовые задачи. Математика в средних и высших учебных заведениях занимается более широким кругом вопросов, включая не только числа, но также множества, функции и другие математические объекты. Их объединяет использование *дедуктивного мышления* для поиска ответов на вопросы. Когда вы решаете уравнение относительно x, вы используете заданную в уравнении информацию, чтобы *вывести* (deduce) значение x. Точно так же, когда математики решают другие виды математических задач, они всегда обосновывают свои выводы дедуктивными рассуждениями.

Дедуктивные рассуждения в математике обычно представляют в виде *доказательства*. Одна из основных целей этой книги – помочь вам развить ваши способности к математическому мышлению в целом и, в частности, вашу способность читать и записывать доказательства. В следующих главах мы подробно изучим, как строятся доказательства, но сначала давайте рассмотрим несколько примеров.

Не волнуйтесь, если у вас возникнут проблемы с пониманием этих доказательств. Они просто предназначены для того, чтобы дать вам почувствовать, на что похожи математические доказательства. В некоторых случаях вы можете выполнить многие шаги доказательства, но будете озадачены тем, почему эти шаги объединены именно таким образом, или как кто-то смог прийти к такому доказательству. Если это так, мы просим вас проявить терпение. Ответы на многие из этих вопросов будут даны позже в этой книге, особенно в главе 3.

Все наши примеры доказательств во введении будут включать простые числа. Напомним, что целое число больше 1 называется *простым*, если оно не может быть записано как произведение двух меньших положительных целых чисел. Если его можно записать как произведение двух меньших положительных целых чисел, то оно *составное*. Например, 6 – составное число, поскольку $6 = 2 \cdot 3$, а 7 – простое число.

Прежде чем мы сможем привести пример доказательства с участием простых чисел, нам нужно найти объект доказательства – некоторый факт о простых числах, правильность которого можно проверить с помощью доказательства. Иногда можно найти интересные закономерности в математике, просто попробовав вычислить несколько чисел. Например, рассмотрим табл. В.1. Для каждого целого числа n от 2 до 10 таблица показывает, являются n и $2^n - 1$ простыми или нет, и возникает удивительная закономерность. Оказывается, $2^n - 1$ – простое число как раз в тех случаях, когда n простое!

Таблица B.1. Закономерность вычисления простых чисел

n	n четное?	$2^n - 1$	$2^n - 1$ четное?
2	Да	3	Да
3	Да	7	Да
4	Нет: $4 = 2 \cdot 2$	15	Нет: $15 = 3 \cdot 5$
5	Да	31	Да
6	Нет: $6 = 2 \cdot 3$	63	Нет: $63 = 7 \cdot 9$
7	Да	127	Да
8	Да: $8 = 2 \cdot 4$	255	Нет: $255 = 15 \cdot 17$
9	Нет: $9 = 3 \cdot 3$	511	Нет: $511 = 7 \cdot 73$
10	Нет: $10 = 2 \cdot 5$	1023	Нет: $1023 = 31 \cdot 33$

Будет ли эта закономерность продолжаться? Заманчиво предположить, что так и есть, но это лишь догадка. Математики называют такие догадки *гипотезами*. Таким образом, мы имеем следующие две гипотезы:

Гипотеза 1. *Предположим, что n – целое число больше* 1 *и n простое. Тогда* $2^n - 1$ *– простое число.*

Гипотеза 2. *Предположим, что n – целое число больше* 1 *и n не является простым. Тогда* $2^n - 1$ *не является простым.*

К сожалению, если мы продолжим табл. B.1, то сразу обнаружим, что гипотеза 1 неверна. Легко проверить, что число 11 простое, но $2^{11} - 1 = 2047 = 23 \cdot 89$, поэтому $2^{11} - 1$ составное. Таким образом, 11 является *контрпримером* к гипотезе 1. Существование хотя бы одного контрпримера доказывает, что гипотеза неверна, но интересно отметить, что в этом случае существует много контрпримеров. Если мы продолжим проверять числа до 30, то найдем еще два контрпримера к гипотезе 1: 23 и 29 – простые числа, но $2^{23} - 1 = 8\,388\,607 = 47 \cdot 178\,481$ и $2^{29} - 1 = 536\,870\,911 = 2089 \cdot 256\,999$. Однако никакое число до 30 не является контрпримером к гипотезе 2.

Считаете ли вы, что гипотеза 2 верна? Найдя контрпримеры к гипотезе 1, мы делаем вывод, что эта гипотеза неверна, но наша неспособность найти контрпример к гипотезе 2 не еще доказывает, что она верна. Возможно, для нее тоже есть контрпримеры, но самый маленький из них больше 30. Продолжение проверки примеров может выявить контрпример, а если его нет, то это может повысить нашу уверенность в гипотезе. Но мы никогда не можем быть уверены в правильности гипотезы, если только проверяем примеры. Сколько бы примеров мы ни проверили, всегда есть вероятность, что следующий окажется первым контрпримером. Единственный способ убедиться в правильности гипотезы 2 – это доказать ее.

На самом деле гипотеза 2 верна. Вот доказательство гипотезы:

Доказательство гипотезы 2. Поскольку n не простое число, существуют натуральные числа a и b такие, что $a < n$, $b < n$ и $n = ab$. Пусть $x = 2^b - 1$ и $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}$. Далее

$$\begin{aligned} xy &= (2^b - 1)\cdot(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\ &= 2^b\cdot(1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) - (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\ &= (2^b + 2^{2b} + 2^{3b} + \cdots + 2^{ab}) - (1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b}) \\ &= 2^{ab} - 1 \\ &= 2^n - 1. \end{aligned}$$

Поскольку $b < n$, мы можем заключить, что $x = 2^b - 1 < 2^n - 1$. Кроме того, поскольку $ab = n > a$, отсюда следует, что $b > 1$. Следовательно, $x = 2^b - 1 > 2^1 - 1 = 1$, поэтому $y < xy = 2^n - 1$. Таким образом, мы показали, что $2^n - 1$ можно записать как произведение двух натуральных чисел x и y, оба из которых меньше $2^n - 1$, поэтому $2^n - 1$ не является простым.

Теперь, когда гипотеза доказана, мы можем назвать ее *теоремой*. Не волнуйтесь, если доказательство показалось вам непонятным. Мы вернемся к нему снова в конце главы 3, чтобы проанализировать, как он было построено. На данный момент наиболее важно понять, что если n – любое целое число больше 1, которое может быть записано как произведение двух меньших положительных целых чисел a и b, то доказательство дает нам способ (по общему признанию, несколько загадочный) записать $2^n - 1$ как произведение двух меньших натуральных чисел x и y. Таким образом, если n не является простым, то $2^n - 1$ также не должно быть простым. Например, предположим, что $n = 12$, тогда $2^n - 1 = 4095$. Поскольку $12 = 3\cdot 4$, мы можем подставить $a = 3$ и $b = 4$ в доказательство. Тогда согласно формулам для x и y, приведенным в доказательстве, мы будем иметь $x = 2^b - 1 = 2^4 - 1 = 15$ и $y = 1 + 2^b + 2^{2b} + \cdots + 2^{(a-1)b} = 1 + 2^4 + 2^8 = 273$. И как и предсказывают формулы в доказательстве, мы имеем $xy = 15\cdot 273 = 4095 = 2^n - 1$. Конечно, есть другие способы разложить 12 на произведение двух меньших целых чисел, и это может привести к другим способам факторизации 4095. Например, поскольку $12 = 2\cdot 6$, мы могли бы использовать значения $a = 2$ и $b = 6$. Попробуйте вычислить соответствующие значения x и y и убедитесь, что их произведение равно 4095.

Хотя мы уже знаем, что гипотеза 1 неверна, мы все же можем задать ей интересные вопросы. Если мы продолжим проверять простые числа n, чтобы убедиться, что $2^n - 1$ простое, продолжим ли мы находить контрпримеры к гипотезе – примеры, для которых $2^n - 1$ не является простым? Будем ли мы продолжать находить примеры, для которых $2^n - 1$ простое? Если бы существовал только конечный набор простых чисел, мы могли бы исследовать эти вопросы, просто проверив $2^n - 1$ для каждого простого числа n. Но на самом деле простых чисел бесконечно много. Евклид (около 300 г. до н.э.) привел доказательство этого факта в книге IX своих «Элементов». Его доказательство – одно из самых известных во всей математике[1]:

Теорема 3. *Простых чисел бесконечно много.*

Доказательство. Предположим, что существует только конечное количество простых чисел. Пусть $p_1, p_2, \ldots, p_n$ – список всех простых чисел. Пусть $m = p_1 p_2 \cdots p_n + 1$. Заметим, что m не делится на p_1, поскольку деление m на p_1 дает

[1] Евклид сформулировал теорему и доказательство несколько иначе. Для этой книги мы выбрали более современный подход.

частное $p_2p_3 \cdots p_n$ и остаток 1. Аналогично, m не делится на любое число из списка $p_2, p_3, \ldots, p_n$.

Теперь мы воспользуемся тем фактом, что каждое целое число больше 1 – либо простое, либо может быть записано как произведение двух или более простых чисел. (Мы увидим доказательство этого факта в главе 6 – см. теорему 6.4.2.) Ясно, что m больше 1, поэтому m либо простое, либо является произведением простых чисел. Предположим сначала, что m простое. Обратите внимание, что m больше, чем все числа в списке $p_1, p_2, \ldots, p_n$, значит, мы обнаружили простое число, которого нет в этом списке. Но это противоречит нашему предположению, что это был список *всех* простых чисел.

Теперь предположим, что m – произведение простых чисел. Пусть q будет одним из простых чисел в этом произведении. Тогда m делится на q. Но мы уже видели, что m не делится ни на одно из чисел в списке $p_1, p_2, \ldots, p_n$, поэтому мы снова приходим к противоречию с предположением, что в этот список включены все простые числа.

Поскольку предположение, что существует конечное число простых чисел, привело к противоречию, должно существовать бесконечно много простых чисел.

Напомним, что вы не должны беспокоиться, если некоторые аспекты этого доказательства кажутся загадочными. Прочитав главу 3, вы лучше подготовитесь к детальному пониманию доказательства. Затем мы вернемся к этому доказательству и проанализируем его структуру.

Мы видели, что если n не является простым, то $2^n - 1$ не может быть простым, но если n простое, то $2^n - 1$ может быть простым или составным. Поскольку простых чисел бесконечно много, существует бесконечно много чисел вида $2^n - 1$, которые, исходя из того, что мы знаем сейчас, *могут быть* простыми. Но сколько из них *являются* простыми?

Простые числа вида $2^n - 1$ называются *простыми числами Мерсенна* в честь отца Марѐна Мерсѐнна (1588–1648), французского монаха и ученого, изучавшего эти числа. Хотя было найдено много простых чисел Мерсенна, до сих пор неизвестно, бесконечно ли их много. Многие из самых больших известных простых чисел – простые числа Мерсенна. На момент написания этой книги (февраль 2019 г.) наибольшее известное простое число – это простое число Мерсенна $2^{82\,589\,933} - 1$, состоящее из 24 862 048 цифр.

Простые числа Мерсенна связаны с совершенными числами, что является предметом другой известной нерешенной проблемы математики. Положительное целое число n называется *совершенным*, если n равно сумме всех положительных целых чисел, меньших n, которые делят n. (Для любых двух целых чисел m и n мы говорим, что m делит n, если n делится на m; другими словами, если существует целое число q такое, что $n = qm$.) Например, существуют положительные целые числа меньше 6, которые делят 6. Это числа 1, 2 и 3, и при этом $1 + 2 + 3 = 6$. Следовательно, 6 – совершенное число. Следующее наименьшее совершенное число – 28. (Вы должны сами убедиться, что 28 совершенно, найдя все положительные целые числа меньше 28, которые делят 28, и сложив их.)

Евклид доказал, что если $2^n - 1$ – простое число, то $2^{n-1}(2^n - 1)$ совершенно. Таким образом, каждое простое число Мерсенна представляет собой совер-

шенное число. Более того, примерно через 2000 лет после доказательства Евклида швейцарский математик Леонард Эйлер (1707–1783), самый плодовитый математик в истории, доказал, что таким способом можно получить каждое четное совершенное число. Например, обратите внимание, что $6 = 2^1(2^2 - 1)$ и $28 = 2^2(2^3 - 1)$. Поскольку неизвестно, существует ли бесконечно много простых чисел Мерсенна, также неизвестно, существует ли бесконечно много четных совершенных чисел. Также неизвестно, существуют ли совершенные нечетные числа. Доказательства теорем Евклида и Эйлера см. в упражнениях 18 и 19 в разделе 7.4.

Хотя простых чисел бесконечно много, они встречаются тем реже, чем больше числа, которые мы рассматриваем. Например, существует 25 простых чисел от 1 до 100, 16 простых чисел от 1001 до 1100 и только шесть простых чисел от 1 000 001 до 1 000 100. В качестве нашего последнего вводного примера математического доказательства мы покажем, что существуют длинные отрезки последовательных положительных целых чисел, вообще не содержащие простых чисел. В этом доказательстве мы будем использовать следующую терминологию: для любого натурального числа n произведение всех целых чисел от 1 до n называется *факториалом* n и обозначается $n!$. Таким образом, $n! = 1 \cdot 2 \cdot 3 \cdots n$. Как и в случае с двумя предыдущими доказательствами, мы вернемся к этому доказательству в конце главы 3, чтобы проанализировать его структуру.

Теорема 4. *Для каждого натурального числа n существует последовательность из n последовательных натуральных чисел, не содержащая простых чисел.*

Доказательство. Предположим, что n – натуральное число. Пусть $x = (n + 1)! + 2$. Мы покажем, что ни одно из чисел $x, x + 1, x + 2, \ldots, x + (n - 1)$ не является простым числом. Поскольку это последовательность из n последовательных натуральных чисел, это доказывает теорему.

Чтобы убедиться, что x не является простым, обратите внимание, что

$$x = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1) + 2 = 2 \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1) + 1).$$

Таким образом, x можно записать как произведение двух меньших положительных целых чисел, поэтому x не является простым.

Аналогично имеем

$$x + 1 = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1) + 3 = 3 \cdot (1 \cdot 2 \cdot 4 \cdots (n + 1) + 1),$$

поэтому $x + 1$ также не является простым. В общем, рассмотрим любое число $x + i$, где $0 < i < n - 1$. Отсюда имеем

$$x + 1 = \ldots$$

поэтому $x + i$ не является простым.

Теорема 4 показывает, что иногда между одним и другим простыми числами есть длинные отрезки. Но простые числа также иногда встречаются близко друг к другу. Поскольку 2 – единственное четное простое число, единственная пара последовательных целых чисел, которые являются простыми, – это

2 и 3. Но есть много пар простых чисел, которые отличаются только на два, например 5 и 7, 29 и 31, 7949 и 7951. Такие пары простых чисел называются простыми *числами-близнецами*. Неизвестно, есть ли бесконечно много простых чисел-близнецов.

Недавно был достигнут значительный прогресс в вопросе о простых числах-близнецах. В 2013 году Итан Чжан (род. 1955) доказал, что существует натуральное число $d < 70\,000\,000$ такое, что существует бесконечно много пар простых чисел, различающихся на d. Усилиями многих других математиков в 2013–2014 гг. удалось снизить диапазон возможных значений d до $d \leq 246$. Конечно, если утверждение верно при $d = 2$, то существует бесконечно много простых чисел-близнецов.

Упражнения

Примечание. Решения или подсказки для упражнений, отмеченных звездочкой (*), приведены в приложении.

*1. (a) Разложите $2^{15} - 1 = 32\,767$ на произведение двух меньших натуральных чисел.
   (b) Найдите целое число x такое, что $1 < x < 232\,767 - 1$ и $232\,767 - 1$ делится на x.

2. Сделайте несколько предположений о значениях n, для которых $3^n - 1$ – простое число, или о значениях n, для которых $3^n - 2^n$ – простое число. (Вы можете начать с создания таблицы, подобной B.1.)

*3. Доказательство теоремы 3 дает метод нахождения простого числа, отличного от любого в данном списке простых чисел.
   (a) Используйте этот метод, чтобы найти простое число, отличное от 2, 3, 5 и 7.
   (b) Используйте этот метод, чтобы найти простое число, отличное от 2, 5 и 11.

4. Найдите пять последовательных целых чисел, которые не являются простыми.

5. Используйте таблицу B.1 и последующее обсуждение, чтобы найти еще два совершенных числа.

6. Последовательность 3, 5, 7 – это список из трех простых чисел, где каждая пара соседних чисел в списке отличается на два. Есть ли еще такие «тройные простые числа»?

7. Два различных натуральных числа (m, n) называются *дружественными*, если сумма всех натуральных чисел меньше n, делящих n, равна m, а сумма всех положительных целых чисел меньше m, которые делят m, равна n. Покажите, что пара (220, 284) дружественная.

Глава 1

Пропозициональная логика

1.1. Дедуктивное мышление и логические связки

Как мы показали во введении, доказательства играют центральную роль в математике, а дедуктивные выкладки являются основой, на которую опираются доказательства. Поэтому мы начинаем изучение математических выводов и доказательств с изучения того, как работает дедуктивное мышление.

Пример 1.1.1. Вот три примера дедуктивного мышления:

1. Завтра будет дождь или снег.
   Слишком тепло для снега.
   Значит, пойдет дождь.
2. Если сегодня воскресенье, то сегодня мне не нужно идти на работу.
   Сегодня воскресенье.
   Поэтому сегодня мне не нужно идти на работу.
3. Я пойду на работу завтра или сегодня.
   Я сегодня останусь дома.
   Поэтому пойду на работу завтра.

В каждом случае мы пришли к *заключению* из предположения, что некоторые другие утверждения, называемые *допущениями* или *посылками*, верны. Например, посылки в рассуждении 3 – это утверждения «Я пойду на работу завтра или сегодня» и «Я сегодня останусь дома». Вывод такой: «Я пойду на работу завтра», и он вроде бы следует из посылок.

Но действительно ли этот вывод сделан верно? В конце концов, разве не может случиться так, что я останусь сегодня дома, а завтра проснусь больным и снова останусь дома? Если это произойдет, вывод окажется ложным. Но заметьте, что в этом случае первая посылка, которая гласила, что я пойду на работу завтра или сегодня, также будет ложной! Хотя у нас нет гарантии, что вывод истинный, он может быть ложным только в том случае, если хотя

бы одна из посылок также ложная. *Если* обе посылки истинны, мы можем быть уверены в истинности вывода. В этом смысле заключение навязано нам посылками, и это критерий, который мы будем использовать для оценки правильности дедуктивного рассуждения. Мы говорим, что рассуждение *действительно*, если все посылки не могут быть истинными без истинного заключения. Все три рассуждения в нашем примере – действительные.

Вот пример недействительного дедуктивного рассуждения:

Виноват или дворецкий, или горничная.
Или виновата горничная, или виноват повар.
Следовательно, виноват или дворецкий, или повар.

Рассуждение недействительно, потому что вывод может быть ложным, даже если истинны обе посылки. Например, если горничная виновна, а дворецкий и повар невиновны, то обе посылки будут истинными, но вывод будет ложным.

Мы можем узнать больше о том, что делает рассуждение действительным, сравнивая три рассуждения в примере 1.1.1. На первый взгляд может показаться, что рассуждения 2 и 3 имеют много общего, потому что оба они касаются одного и того же предмета: посещения работы. Но с точки зрения используемых рассуждений наиболее похожи рассуждения 1 и 3. Оба они вводят две *возможности* в первой посылке, исключают вторую возможность с помощью второй посылки и затем делают вывод, что первая возможность должна иметь место. Другими словами, оба рассуждения имеют вид:

P или *Q*.
Не *Q*.
Следовательно, *P*.

Именно эта *форма*, а не предмет обсуждения делает рассуждения действительными. Вы можете увидеть, что рассуждение 1 имеет такую форму, если принять, что буква *P* обозначает утверждение «Завтра будет дождь», а *Q* – «Завтра будет снег». Для рассуждения 3 *P* будет означать «Я пойду на работу завтра», а *Q* – «Я пойду на работу сегодня».

Замена определенных утверждений в каждом рассуждении буквами, как мы это сделали для рассуждений 1 и 3, дает два преимущества. Во-первых, это не позволяет нам отвлекаться на аспекты рассуждений, не влияющие на их обоснованность. Вам не нужно ничего знать о прогнозировании погоды или привычке ходить на работу, чтобы признать, что рассуждения 1 и 3 верны. Это потому, что оба рассуждения имеют форму, показанную ранее, и вы можете сказать, что эта форма рассуждения верна, даже не зная, что означают *P* и *Q*. Если вы не согласны с этим, рассмотрите следующее рассуждение:

Либо стробонатор пропускает зажигание, либо механизм друмпеля не отрегулирован.
Я проверил регулировку механизма друмпеля, и с ним все в порядке.
Следовательно, стробонатор неисправен.

Если механик даст такое объяснение после осмотра вашей машины, вы все равно не поймете, почему машина не заводится, но у вас не будет претензий к его логике!

Возможно, более важно то, что из анализа формы рассуждений 1 и 3 становится ясно, что влияет на их обоснованность: это слова *или* (or) и *не* (not). В большинстве дедуктивных рассуждений и, в частности, в математических рассуждениях значения всего нескольких слов дают нам ключ к пониманию того, что делает часть рассуждения правильной или ошибочной. (Какие слова являются важными в рассуждении 2 в примере 1.1.1?) Первые несколько глав этой книги посвящены изучению этих слов и того, как они используются в математических записях и рассуждениях.

В этой главе мы сконцентрируемся на словах, используемых для объединения простых утверждений в более сложные. Мы продолжим использовать буквы для обозначения утверждений, но только для однозначных утверждений, которые являются истинными или ложными. Вопросы, восклицания и расплывчатые заявления не допускаются. Также будет полезно использовать символы, иногда называемые *соединительными символами* или *связками* (connective simbols), для обозначения некоторых слов, применяемых для объединения утверждений. Вот наши первые три соединительных символа и слова, которые они обозначают:

Символ	Значение
$\vee$	или (or)
$\wedge$	и (and)
$\neg$	не (not)

Таким образом, если P и Q обозначают два утверждения, тогда мы будем писать $P \vee Q$ для обозначения утверждения «P или Q», $P \wedge Q$ для «P и Q» и $\neg P$ для «не P» или «P является ложным». Утверждение $P \vee Q$ иногда называют *дизъюнкцией* P и Q, $P \wedge Q$ называют *конъюнкцией* P и Q, а $\neg P$ называют *отрицанием* P.

Пример 1.1.2. Запишите логические формы следующих утверждений:

1. Или Джон пошел в магазин, или у нас закончились яйца.
2. Джо собирается уйти из дома и больше не вернется.
3. Или Билл на работе, а Джейн нет, или Джейн на работе, а Билл нет.

Решения

1. Если мы назначим P обозначать утверждение «Джон пошел в магазин», а Q – «у нас закончились яйца», то общее утверждение можно было бы символически представить как $P \vee Q$.
2. Если мы назначим P обозначать утверждение «Джо собирается уйти из дома», а Q – «Джо не вернется», то мы могли бы символически представить это утверждение как $P \wedge Q$. Но эта запись упускает важную особенность утверждения, потому что она не означает, что Q – отрицательное утверждение. Мы могли бы улучшить запись, обозначив как R утверждение «Джо собирается вернуться», а затем записав утверждение Q

как $\neg R$. Подставив это в нашу первую запись посылки, мы получаем улучшенную запись $P \wedge \neg R$.

3. Пусть B означает утверждение «Билл на работе», а J – утверждение «Джейн на работе». Тогда первая половина утверждения «Билл на работе, а Джейн нет» может быть представлена как $B \wedge \neg J$. Аналогично, вторая половина – это $J \wedge \neg B$. Чтобы записать все утверждение, мы должны использовать связку «или», образуя дизъюнкцию, так что полная запись будет иметь следующий вид: $(B \wedge \neg J) \vee (J \wedge \neg B)$.

Обратите внимание, что при анализе третьего утверждения в предыдущем примере мы добавили круглые скобки при формировании дизъюнкции $B \wedge \neg J$ и $J \wedge \neg B$, чтобы однозначно указать, какие утверждения были объединены. Это похоже на использование круглых скобок в алгебре, в которых, например, произведение $a + b$ и $a - b$ будет записано как $(a + b) \cdot (a - b)$, причем скобки служат для однозначного указания того, какие величины должны быть перемножены. Как и в алгебре, в логике принято опускать некоторые скобки, чтобы наши выражения были короче и удобнее для чтения. Однако мы должны договориться о некоторых соглашениях о том, как читать такие выражения, чтобы они оставались однозначными. Согласно одному соглашению, символ $\neg$ всегда применяется только к утверждению, которое следует сразу после него. Например, $\neg P \wedge Q$ означает $(\neg P) \wedge Q$, а не $\neg(P \wedge Q)$. Позже мы увидим другие соглашения о скобках.

Пример 1.1.3. Какие английские предложения представлены следующими выражениями?

1. $(\neg S \wedge L) \vee S$, где S означает «Джон умен», а L означает «Джону повезло».
2. $\neg S \wedge (L \vee S)$, где S и L имеют те же значения, что и раньше.
3. $\neg(S \wedge L) \vee S$, причем S и L остаются прежними.

Решения

1. Джон не умен и ему повезло, или он умен.
2. Джон не умен, и ему повезло, или он умен. Обратите внимание, как расположение слова *или* в разговорном языке меняется в зависимости от того, где находятся круглые скобки.
3. Джон не умен и не удачлив, или Джон умен. Слово-союз *и* также зависит от различного возможного положения скобок.

Важно помнить, что символы $\wedge$, $\vee$ и $\neg$ на самом деле не соответствуют всем вариантам использования слов *и*, *или*, *не* в разговорном языке. Например, символ $\wedge$ нельзя использовать для обозначения слова *и* в предложении «Джон и Билл – друзья», потому что в этом предложении слово *и* не используется для объединения двух утверждений. Символы $\wedge$ и $\vee$ могут использоваться только *между двумя утверждениями*, чтобы образовать их конъюнкцию или дизъюнкцию, а символ $\neg$ может использоваться только *перед утверждением*, чтобы отрицать его. Это означает, что определенные строки букв и символов просто бессмысленны. Например, $P \neg \wedge Q$, $P \wedge \vee Q$ и $P \neg Q$ – все это «неграмматические» выражения на языке логики. «Грамматические» выражения, подобные приведенным в примерах 1.1.2 и 1.1.3, иногда называют *правильно*

построенными формулами или просто *формулами*. И снова, здесь полезно подумать об аналогии с алгеброй, в которой символы $+$, $-$, $\cdot$ и $\div$ могут стоять *между двумя числами* в качестве операторов, а символ – (минус) также может стоять перед числом, чтобы показать его отрицательность. Это единственный способ использования этих символов в алгебре, поэтому такие выражения, как $x - \div y$, не имеют смысла.

Иногда для записи выражений, представленных символами $\wedge$, $\vee$ и $\neg$, используются слова, отличные от *и*, *или*, *не*. Например, рассмотрим первое утверждение в примере 1.1.3. Хотя мы использовали выражение «Джон не умен и ему повезло, или он умен», альтернативным способом передачи той же информации было бы выражение: «Либо Джон не умен, но ему повезло, либо он умен». Часто слово *но* используется в разговорном языке для обозначения связки *и*, особенно когда есть некоторый контраст или конфликт между объединяемыми утверждениями. В качестве более яркого примера представьте, что синоптик заканчивает свой прогноз заявлением «Дождь *и* снег – только эти варианты можно ждать от завтрашней погоды». Это просто окольный способ сказать, что завтра будет дождь *или* снег. Таким образом, даже несмотря на то, что синоптик использовал слово *и*, значение, выраженное в его утверждении, является дизъюнкцией. Урок из этих примеров состоит в том, что для определения логической формы утверждения вы должны думать о смысле утверждения, а не просто переводить слово за словом в символы.

Иногда логические слова скрыты в математических обозначениях. Например, рассмотрим утверждение $3 \leq \pi$. Хотя с виду оно кажется простым утверждением, не содержащим логических связок, если вы прочитаете его вслух, то услышите слово *или*. Если мы назначим P обозначать утверждение $3 < \pi$ и Q для утверждения $3 = \pi$, тогда утверждение $3 \leq \pi$ будет записано как $P \vee Q$. В этом примере утверждения, представленные буквами P и Q, настолько короткие, что вряд ли имеет смысл сокращать их до отдельных букв. В таких случаях мы иногда не будем беспокоиться о замене утверждений буквами, поэтому мы также можем записать это утверждение как $(3 < \pi) \vee (3 = \pi)$.

В качестве немного более сложного примера рассмотрим утверждение $3 < \pi < 4$. Это утверждение означает $3 < \pi$ *и* $\pi < 4$, так что снова логическая связка была скрыта в математической нотации. Дополняя запись, которую мы только что разработали для $3 \leq \pi$, мы можем записать выражение как $[(3 < \pi) \vee (3 = \pi)] \wedge (\pi < 4)$. Знание логической формы утверждения может быть важно для понимания части математических рассуждений, связанных с этим утверждением.

Упражнения

*1. Запишите логические формы следующих утверждений:
   (a) У нас будут либо задания для самостоятельного чтения, либо домашняя работа, но у нас не будет одновременно домашней работы и теста.
   (b) Вы не пойдете кататься на лыжах или пойдете, но снега не будет.
   (c) $\sqrt{7} \not\leq 2$.

2. Запишите логические формы следующих утверждений:
   (a) Либо Джон и Билл оба говорят правду, либо ни один из них не говорит правду.
   (b) Я буду есть либо рыбу, либо курицу, но не буду есть рыбу и картофельное пюре одновременно.
   (c) Число 3 является общим делителем чисел 6, 9 и 15.
3. Запишите логические формы следующих утверждений:
   (a) Алиса и Боб не находятся в комнате одновременно.
   (b) Алисы и Боба одновременно нет в комнате.
   (c) Алисы или Боба нет в комнате.
   (d) Ни Алисы, ни Боба нет в комнате.
4. Запишите логические формы следующих утверждений:
   (a) Либо Ральф и Эд оба высокие, либо оба красивые.
   (b) И Ральф, и Эд либо высокие, либо красивые.
   (c) И Ральф, и Эд оба невысокие и некрасивые.
   (d) Ни Ральф, ни Эд не являются одновременно высокими и красивыми.
5. Какие из следующих выражений являются правильными формулировками?
   (a) $\neg(\neg P \vee \neg\neg R)$.
   (b) $\neg(P, Q, \wedge R)$.
   (c) $P \wedge \neg P$.
   (d) $(P \wedge Q)\ (P \vee R)$.

*6. Пусть P означает утверждение «Я куплю брюки», а S – утверждение «Я куплю рубашку». Какие разговорные предложения представлены следующими формулами?
   (a) $\neg(P \wedge \neg S)$.
   (b) $\neg P \wedge \neg S$.
   (c) $\neg P \vee \neg S$.
7. Пусть S означает утверждение «Стив счастлив», а G – «Джордж счастлив». Какие английские предложения представлены следующими формулами?
   (a) $(S \vee G) \wedge (\neg S \vee \neg G)$.
   (b) $[S \vee (G \wedge \neg S)] \vee \neg G$.
   (c) $S \vee [G \wedge (\neg S \vee \neg G)]$.
8. Пусть T означает «Налоги вырастут», а D – «Дефицит вырастет». Какие английские предложения представлены следующими формулами?
   (a) $T \vee D$.
   (b) $\neg(T \wedge D) \wedge \neg(\neg T \wedge \neg D)$.
   (c) $(T \wedge \neg D) \vee (D \wedge \neg T)$.
9. Определите посылки и выводы следующих дедуктивных рассуждений и запишите их логические формы. Как вы думаете, рассуждения верны? (Хотя при ответе на последний вопрос у вас будет только интуиция, в следующем разделе мы разработаем некоторые методы определения обоснованности рассуждений.)

(a) Джейн и Пит оба не выиграют приз по математике. Пит выиграет либо приз по математике, либо по химии. Джейн получит приз по математике. Следовательно, Пит получит приз по химии.
(b) Основное блюдо будет из говядины или рыбы. Гарниром будет либо горох, либо кукуруза. У нас не будет одновременно рыбы в качестве основного блюда и кукурузы в качестве гарнира. Поэтому у нас не будет одновременно говядины как основного блюда и гороха как гарнира.
(c) Либо Джон, либо Билл говорят правду. Либо Сэм, либо Билл лгут. Следовательно, либо Джон говорит правду, либо Сэм лжет.
(г) Либо продажи вырастут, и начальник будет доволен, либо расходы увеличатся, и начальник будет недоволен. Таким образом, продажи и расходы не могут увеличиться одновременно.

1.2. Таблицы истинности

В разделе 1.1 мы показали, что рассуждение действительно, если все посылки не могут быть истинными без наличия истинного заключения. Поэтому, чтобы понять, как слова *и*, *или* и *не* влияют на обоснованность рассуждений, мы должны понять, как они способствуют истинности или ложности содержащих их утверждений.

Когда мы оцениваем истинность или ложность утверждения, мы присваиваем ему один из ярлыков – *истина* или *ложь*, – и этот ярлык называется его значением истинности. Вполне очевидно, как слово *и* способствует значению истинности содержащегося в нем утверждения. Утверждение в форме $P \wedge Q$ может быть истинным, только если одновременно истинны и P, и Q; если либо P, либо Q является ложным, то $P \wedge Q$ также будет ложным. Поскольку мы предположили, что P и Q обозначают утверждения, которые либо истинны, либо ложны, мы можем свести все варианты возможных значений в табл. 1.1, называемую *таблицей истинности* для формулы $P \wedge Q$. Каждая строка в таблице истинности представляет одну из четырех возможных комбинаций значений истинности для утверждений P и Q. Хотя эти четыре возможности могут располагаться в таблице в любом порядке, лучше всего перечислять их систематически, чтобы мы могли быть уверены, что ни одна из возможностей не была упущена. Таблицу истинности для $\neg P$ также довольно легко построить, потому что для того, чтобы $\neg P$ было истинным, P должно быть ложным (табл. 1.2).

Таблица 1.1. Таблица истинности формулы $P \wedge Q$

P	Q	$P \wedge Q$
F	F	F
F	T	F
T	F	F
T	T	T

Таблица 1.2. Таблица истинности формулы ¬P

P	$\neg P$
F	T
T	F

Таблица истинности для $P \vee Q$ немного сложнее. Первые три строки, безусловно, должны быть заполнены, как показано в табл. 1.3, но могут возникнуть некоторые вопросы по поводу последней строки. Каким должно быть значение $P \vee Q$ – истинным или ложным в случае, когда P и Q оба истинны? Другими словами, какому из утверждений соответствует запись $P \vee Q$ – «P или Q, или оба» или же «P или Q, но не оба»? Первый способ интерпретации слова *или* называется *включающим или* (потому что он включает возможность того, что оба утверждения являются истинными), а второй – *исключающим или*. В математике *или* всегда включающее, если не указано иное, поэтому мы будем интерпретировать символ ∨ как включающее или (табл. 1.4). См. упражнение 3, чтобы узнать больше об исключающем или.

Таблица 1.3. Таблица истинности формулы P ∨ Q с неоднозначностью

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	?

Таблица 1.4. Таблица истинности исключающего или

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	T

Используя правила, изложенные в этих таблицах истинности, теперь мы можем разработать таблицы истинности для более сложных формул. Все, что нам нужно сделать, – это определить значения истинности составных частей формулы, начиная с отдельных букв и постепенно переходя к более сложным формулам.

Пример 1.2.1. Составьте таблицу истинности для формулы $\neg(P \vee \neg Q)$.

Решение

P	Q	$\neg Q$	$P \vee \neg Q$	$\neg(P \vee \neg Q)$
F	F	T	T	F
F	T	F	F	T
T	F	T	T	F
T	T	F	T	F