Модуль 6.3. Различные виды доказательств в математике

Понятие доказательства не принадлежит математике, математике принадлежит лишь его математическая модель — формальное доказательство.

Рассмотрим, как соотносятся неформальные доказательства и логический вывод. Логический вывод напоминает процесс мышления, но при этом мы не должны считать, что его правила суть правила человеческой мысли. Доказательство — это нечто неформальное; иными словами, это продукт нормального мышления, записанный на человеческом языке и предназначенный для человеческого потребления. В доказательствах могут использоваться всевозможные сложные мыслительные приемы, и хотя интуитивно они могут казаться верными, можно усомниться в том, возможно ли доказать их логически. Именно поэтому мы нуждаемся в формализации. Вывод — это искусственное соответствие доказательства: его назначение — достичь той же цели, на этот раз с помощью логической структуры, методы которой не только ясно выражены, но и очень просты.

Обычно формальный вывод бывает крайне длинен по сравнению с соответствующей «естественной» мыслью. Это, конечно, плохо — но это та цена, которую приходится платить за упрощение каждого шага. Часто бывает, что вывод и доказательство «просты» в дополнении друг к другу. Доказательство просто в том смысле, что каждый шаг «кажется правильным», даже если мы и не знаем точно, почему; логический вывод прост, потому что каждый из многочисленных его шагов так прост, что сомнения в правильности этих шагов не возникают, и поскольку весь вывод состоит из таких шагов, мы предполагаем, что он безошибочен. Каждый тип простоты, однако, привносит свой тип сложности. В случае доказательств — это сложность системы, на которую они опираются, а именно, человеческого языка; в случае логических выводов — это их грандиозная длина, делающая их почти невозможными для понимания.

Формальные доказательства в математике (в том числе и в математической логике) в большинстве случаев являются доказательствами вида «$\Gamma \vdash P$» или «не $\Gamma \vdash P$» для разных теорий первого порядка, множеств Γ и разных (классов) формул P.

Результат «$\Gamma \vdash P$» может доказываться посредством предъявления описания вывода формулы P из Γ. Однако в мало-мальски сложных случаях оно оказывается настолько длинным, что заменяется инструкцией по составлению такого описания, более или менее полной. Наконец, доказательство «$\Gamma \vdash P$» может вообще не сопровождаться предъявлением вывода P из Γ, хотя бы и неполного. В этом случае мы «не доказываем P, а доказываем, что существует доказательство P».

Результат «не $\Gamma \vdash P$» в редких случаях может устанавливаться чисто синтаксическим рассуждением, но обычно доказательство опирается на конструкцию модели, т. е. интерпретации, в которой Γ истинно, а P ложно.

Многие математики критикуют аксиоматический метод за то, ради чего он был создан: он избавляет математику от смысла. Потому что сначала мы избавляем математику от разных геометрических представлений, от интуиции. Переходя к формальной аксиоматической теории, мы, в общем-то, и логику изгоняем из математики. И в результате от содержательного доказательства остается лишь скелет, состоящий из формальных символов. Преимущество последнего ровно в том,

что мы не знаем, что такое «смысл» и «интуиция», но зато точно знаем, что такое манипуляции с конечными строками символов. Это и позволяет нам построить точную математическую модель сложного явления — доказательства — и подвергнуть ее математическому анализу.

Математическое доказательство изначально было психологическим процессом убеждения собеседника в верности того или иного утверждения. В формальной системе это не так: все свелось к чисто механическому процессу. Этот механический процесс способен выполнять компьютер. Однако, как и всякая модель, механический процесс передает лишь некоторые черты реальных доказательств. У такой модели есть свои границы применимости. Неверно думать, что формальные доказательства и есть «настоящие» математические доказательства или что математики на самом деле работают в рамках определенных формальных систем.

По словам Ю. И. Манина [1, с. 54], «в качестве средства общения, открытия, фиксации материала никакой формальный язык не способен конкурировать со смесью национального математического арго и формул, привычной для каждого работающего математика».

Отдельно стоит сказать о преподавании математики. Нет ничего хуже, чем строить обучение школьников и студентов на выполнении механических действий (алгоритмов) или же на построении формальных логических выводов. Так можно загубить в человеке любое творческое начало. Соответственно, при обучении математике не стоит подходить с позиции строгого аксиоматического метода в смысле Гильберта — не для того он был создан.

Определение доказательства было уточнено Н. Н. Непейводой. ***Доказательство*** — конструкция, синтаксическая правильность которой гарантирует семантическую.

Под это определение попадают все формальные доказательства. Но и некоторые неформальные доказательства. Например, использование диаграмм Венна для обоснования тождеств алгебры множеств (глава 2, параграф 2.2). В этих диаграммах нет предложений, нет правил вывода, не видно умозаключений, но они доказывают на хорошо подобранных системах множеств.

Перечислим различные методы математических доказательств. Надо, конечно, учитывать, что в сложном доказательстве могут сразу присутствовать несколько методов.

С точки зрения общего движения мысли все доказательства подразделяются на *прямые* и *косвенные*.

При прямом доказательстве задача состоит в том, чтобы подыскать такие убедительные аргументы, из которых по логическим правилам получается заключение. Другими словами, истинность утверждения выводится из истинности посылок без введения дополнительных предположений.

Непрямое (косвенное) доказательство истинности или ложности некоторого утверждения состоит в том, что оно достигается посредством опровержения некоторых других высказываний, несовместимых с доказываемым. Косвенные доказательства применяются в основном в математике.

1. **Аксиоматический метод**. Подразделяется на формальный и неформальный (см. главу 5, параграф 5.1).

2. **Доказательство методом перебора**. Такой метод часто применяют, когда количество вариантов незначительно для проверки данного утверждения, например, утверждения о каком-то свойстве натуральных чисел в ограниченном диапазоне. С использованием систем компьютерной алгебры проверка может быть проделана для очень больших чисел. Например, самая старая открытая проблема со времен античности: существуют ли нечетные совершенные числа? На конец 2014 года проверены все нечетные числа, меньшие 10^{300}. Нечетное совершенное число не обнаружено[1].

3. **Использование теоремы о дедукции**. Теорема о дедукции справедлива для исчисления высказываний (глава 5, параграф 5.3, теорема 3) и для теорий первого порядка (глава 5, параграф 5.4, теорема 7). Теорема служит обоснованием следующего приема, который часто используют в математических доказательствах. Для того чтобы доказать утверждение «Если A, то B», предполагают, что справедливо A и доказывают справедливость B.

Пример 1

Докажите, что для каждого целого n, если n четное, то n^2 тоже четное.

Доказательство. Так как n четное, то его можно представить в виде $n = 2m$, где m — целое число. Поэтому $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$, где $2m^2$ — целое число, т. е. n^2 четное.

4. **Доказательство импликаций с помощью контрапозиции**. Рассмотрим условное высказывание вида $A \supset B$, где A — конъюнкция посылок, B — заключение. Иногда удобнее вместо доказательства истинности этой импликации установить логическую истинность некоторого другого высказывания, равносильного исходному. Такие формы доказательства относятся к косвенным методам.

Контрапозицией формулы $A \supset B$ называется равносильная формула $\neg B \supset \neg A$. Поэтому если мы установим истинность контрапозиции, то тем самым докажем истинность исходной импликации.

Пример 2

На основе контрапозиции докажите, что если m и n — произвольные положительные целые числа, такие, что $m \times n \leqslant 100$, то либо $m \leqslant 10$, либо $n \leqslant 10$.

Доказательство. Контрапозицией исходному утверждению служит следующее высказывание: «Если $m > 10$ и $n > 10$, то $m \times n > 100$», что очевидно.

[1] Натуральное число n называется совершенным, если сумма его всех делителей равна $2n$.

Преимущества метода доказательства с помощью контрапозиции проявляются при автоматизированном способе доказательства, т. е. когда доказательство совершает компьютер с помощью специальных программных систем доказательства теорем (например, с помощью языка программирования Пролог).

При построении выводов не всегда целесообразно ждать появления искомого заключения, просто применяя правила вывода. Именно такое часто случается, когда мы делаем допущение A для доказательства импликации $A \supset B$. Мы применяем цепное правило и *modus ponens* к A и другим посылкам, чтобы в конце получить B. Однако можно пойти по неправильному пути, и тогда будет доказано много предложений, большинство из которых не имеет отношения к нашей цели. Этот метод носит название *прямой волны* и имеет тенденцию порождать лавину промежуточных результатов, если его запрограммировать для компьютера и не ограничить глубину.

Другая возможность — использовать контрапозицию и попытаться, например, доказать $\neg B \supset \neg A$ вместо $A \supset B$. Тогда мы допустим $\neg B$ и попробуем доказать $\neg A$. Это позволяет двигаться как бы назад от конца к началу, применяя правила так, что старое заключение играет роль посылки. Такая организация поиска может лучше показать, какие результаты имеют отношение к делу. Она называется *поиском от цели*.

5. **Доказательство с помощью противоречия (от противного)**. Частным случаем косвенных методов доказательства является приведение к противоречию (от противного). Метод доказательства основывается на следующем утверждении.

Если $\Gamma, \neg S \vdash F$, где F — любое противоречие (тождественно ложная формула), то $\Gamma \vdash S$.

В этом методе используются следующие равносильности:

- $A \supset B \equiv \neg(A \supset B) \supset (C\&\neg C) \equiv (A\&\neg B) \supset (C\&\neg C)$,
- $A \supset B \equiv (A\&\neg B) \supset \neg A$,
- $A \supset B \equiv (A\&\neg B) \supset B$.

Используя вторую из приведенных равносильностей для доказательства $A \supset B$, мы допускаем одновременно A и $\neg B$, т. е. предполагаем, что заключение ложно:

$$\neg(A \supset B) \equiv \neg(\neg A \vee B) \equiv A\&\neg B.$$

Теперь мы можем двигаться и вперед от A, и назад от $\neg B$. Если B выводимо из A, то, допустив A, мы доказали бы B. Поэтому, допустив $\neg B$, мы получим противоречие. Если же мы выведем $\neg A$ из $\neg B$, то тем самым получим противоречие с A. В общем случае мы можем действовать с обоих концов, выводя некоторое предложение C, двигаясь вперед, и его отрицание $\neg C$, двигаясь назад. В случае удачи это доказывает, что наши посылки ***несовместимы*** или ***противоречивы***. Отсюда мы выводим, что дополнительная посылка $A\,\&\,\neg B$ должна быть ложна, а значит, противоположное ей утверждение $A \supset B$ истинно. Метод доказательства от противного — один из самых лучших инструментов математика. «Это гораздо более «хитроумный» гамбит, чем любой шахматный гамбит: шахматист может пожертвовать пешку или даже фигуру, но математик жертвует *партию*» [2, с. 61].

Мы уже применяли в параграфе 3.4 главы 3 метод от противного при доказательстве тавтологичности некоторых импликаций. Следующие примеры более знамениты.

Теорема 3. Школа Пифагора. Докажем, что диагональ единичного квадрата является иррациональным числом.

Доказательство. Используя теорему Пифагора, переформулируем утверждение: *Не существуют два таких целых числа p и q, чтобы выполнялось отношение*

$$\sqrt{2} = \frac{p}{q}.$$

В самом деле, тогда мы приходим к равенству $p^2 = 2q^2$. Мы можем считать, что дробь p/q несократима, иначе мы с самого начала сократили бы ее на наибольший общий делитель чисел p и q. С правой стороны имеется 2 в качестве множителя, и потому p^2 есть четное число, и, значит, само p — также четное, так как квадрат нечетного числа есть нечетное число. В таком случае можно положить $p = 2r$. Тогда равенство принимает вид:

$$4r^2 = 2q^2, \quad \text{или} \quad 2r^2 = q^2.$$

Так как с левой стороны теперь имеется 2 в качестве множителя, значит q^2, а следовательно, и q — четное. Итак, и p, и q — четные числа, т. е. делятся на 2, а это противоречит допущению, что дробь p/q несократима. Итак, равенство $p^2 = 2q^2$ невозможно и $\sqrt{2}$ не может быть рациональным числом.

Теорема 4 (Евклида). Доказать, что простых чисел бесконечно много.

Доказательство. Предположим, что существует конечное множество простых чисел и p есть наибольшее из них: 2, 3, 5, 7, 11,…, p. Определим число $N = p! + 1$. Число N при делении на любое из чисел 2, 3, 5, 7, 11,…, p дает в остатке 1. Каждое число, которое не является простым, делится, по крайней мере, на одно простое число. Число N не делится ни на одно простое число, следовательно, N — само простое число, причем $N > p$. Таким образом, мы пришли к противоречию, которое доказывает, что простых чисел бесконечно много.

Софизм. Единица — наибольшее натуральное число.

Доказательство. От противного. Пусть $k > 1$ будет наибольшим натуральным числом; тогда имеем $k \cdot k = k^2 > k \cdot 1 = k$. Неравенство показывает, что k не является наибольшим натуральным числом. Следовательно, никакое целое число $k > 1$ не может быть наибольшим натуральным числом. Остается принять, что наибольшим натуральным числом является 1, так как только в этом случае мы не приходим к противоречию.

Попробуйте разобраться самостоятельно.

6. **Доказательство контрпримером**. Многие математические гипотезы имеют в своей основе форму: «Все объекты со свойством A обладают свойством B». Мы можем записать это в виде формулы:

$$\forall x\big(A(x) \supset B(x)\big),$$

где $A(x)$ обозначает предикат «x обладает свойством A», $B(x)$ — «x обладает свойством B». Если число возможных значений x является конечным, то в принципе доказательство может быть проведено с помощью разбора случаев, то есть непосредственной проверкой выполнимости гипотезы для каждого объекта. В случае если число объектов не является конечным, то такой возможности не существует даже в принципе. Однако для доказательства ложности гипотезы достаточно привести хотя бы один пример (называемый в этом случае *контрпримером*), для которого гипотеза не выполнима.

Знаменитых контрпримеров множество. Перечислим некоторые из них.

Пример 3

Ферма[1] предполагал, что все числа вида

$$p_k = 2^{2^k} + 1$$

простые. Первые пять чисел для $k = 0, 1, 2, 3, 4$ являются простыми. Он не смог проверить число $p_5 = 4\ 294\ 967\ 297$. Ферма был неправ, возможно, почти совсем неправ, дело в том, что все остальные числа, которые удалось проверить на простоту, оказались составными. Число p_5 было разложено на множители Эйлером.

Пример 4

Эйлер предположил (1769 г.), что для любого натурального числа $n > 2$ никакую n-ю степень натурального числа нельзя представить в виде суммы $(n-1)$ n-х степеней других натуральных чисел. То есть, уравнения:

$$\sum_{k=1}^{n-1} a_k^n = a_n^n$$

не имеют решения в целых числах. В 1966 году был найден для $n = 5$ контрпример

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Для $n = 4$ контрпример был найден в 1986 году:

$$2\ 682\ 440^4 + 15\ 365\ 639^4 + 1\ 879\ 760^4 = 206\ 156\ 734^4.$$

[1] Пьер Ферма (1601–1665 гг.) — французский математик, один из создателей аналитической геометрии, математического анализа, теории вероятностей и теории чисел.

Пример 5

В 1806 году Ампер[1] предпринял попытку доказать, что всякая «произвольная» функция дифференцируема всюду, за исключением «исключительных и изолированных» значений аргумента. Один из контрпримеров был найден в 1930 году ван дер Варденом[2] — пример непрерывной, но нигде не дифференцируемой функции:

$$v(x) = \sum_{n=0}^{\infty} \frac{\{10^n x\}}{10^n},$$

где фигурные скобки означают взятие дробной части.

7. **Метод математической индукции**. Дедукция как общенаучный метод является основным методом математики. Математическая индукция явно восходит к этой же идее. Аксиома индукции Пеано постулирует писать только первый и общий шаги доказательства и, таким образом, является по существу первым метаматематическим принципом. Хотя аксиома индукции формулируется для формальной арифметики, но, в сущности, она является фундаментальным архетипом математического мышления.

Отметим, что математическая индукция очень часто используется для доказательства гипотез, полученных с помощью индукции.

Доказательство становится таковым только в результате социального акта «принятия доказательства». Это относится к математике в той же мере, что и к физике, лингвистике или биологии. Представление о математическом доказательстве меняется со временем (см. [3, с. 370–390]). Однако со времени Евклида неизменной остается идеальная структура математического доказательства «неочевидной истины»: переход к ней от «очевидных» или установленных ранее посылок посредством серии явно выписанных «очевидно законных» элементарных умозаключений.

Формальный метод является хорошим приближением к традиционным математическим доказательствам. О различиях по форме и восприятию их человеком мы уже сказали. Но есть и другие серьезные различия, о которых пишет Ю. И. Манин [1, с. 54–55].

а) *Надежность принципов*. Не только математика, заложенная в специальные аксиомы теории множеств и арифметики Пеано, но даже логика языков первого порядка не является общепризнанной. В частности, после Брауэра[3] оспаривается закон исключенного третьего. С этих крайне критических позиций наши «доказательства» в лучшем случае выводят бессмыслицу из лжи.

[1] Андре-Мари Ампер (1775–1836 гг.) — знаменитый французский физик и математик.

[2] Бартель ван дер Варден (1903–1996 гг.) — голландский математик.

[3] Лёйтзен Брауэр (1881–1966 гг.) — голландский философ и математик. Положил начало новому направлению в математике — интуиционизму. Он подверг сомнению неограниченную приложимость в математических рассуждениях классического закона исключенного третьего и косвенных методов доказательства.

Быть совершенно глухим к этой критике математик не может себе позволить: вдумываясь в нее, следует по крайней мере осознать, что существуют объективно различные «степени доказательности» доказательств.

б) *Уровни доказательности*. Каждое предложенное доказательство апробируется на приемлемость математиками, иногда нескольких поколений. При этом подлежит уточнению и само доказательство, и его результат. Чаще всего доказательство является более или менее краткой схемой формального вывода в подходящем языке. Однако как уже было отмечено, иногда утверждение P устанавливается посредством доказательства того, что доказательство P существует. Эта иерархия доказательств существования доказательств в принципе может быть как угодно высокой. Мы снимаем ее с помощью высших логических или теоретико-множественных принципов, с которыми, однако, можно не соглашаться. Работы по конструктивной математике пестрят утверждениями типа: «не может не существовать алгоритма, вычисляющего x» там, где классический математик сказал бы просто «x существует» или, в крайнем случае, «x существует и эффективно вычислим».

в) *Ошибки*. Особенности человеческой психики делают формальные выводы практически не поддающимися проверке, даже если согласиться, что это идеальный вид доказательности. Два обстоятельства действуют в одну сторону с губительным эффектом: формальные выводы гораздо длиннее текстов на арго; скорость их сознательного чтения человеком гораздо ниже.

Нередко доказательство одной теоремы занимает пять, пятнадцать и даже сотни страниц. Длина соответствующих формальных выводов не поддается воображению.

Поэтому отсутствие ошибок в математической работе (если они не обнаружены), как и в других естественных науках, часто устанавливается по косвенным данным: имеет значение соответствие с общими ожиданиями, использование аналогичных аргументов в других работах. Разглядывание «под микроскопом» отдельных участков доказательства, даже репутация автора; словом, воспроизводимость в широком смысле слова, непонятные доказательства могут сыграть очень полезную роль, стимулируя поиски более доступных рассуждений.

Список литературы по модулю

[1] Манин Ю. И. Доказуемое и недоказуемое / Ю. И. Манин. — М. : Мир ; Советское радио, 1979. — 168 с.

[2] Харди Г. Г. Апология математики / Г. Г. Харди. — Ижевск : НИЦ «Регулярная и хаотическая динамика», 2000. — 104 с.

[3] Успенский В. А. Апология математики / В. А. Успенский. — СПб. ; Амфора, 2009. — 554 с.