Лекция 1. Диофантовы уравнения в истории математики

1 Введение

Изучение диофантовых уравнений исторически было одним из древнейших подходов к математике. С этой точки зрения, эта область уникальна тем, что даёт представление о пути, по которому шли математики прошлого, и помогает сформировать представление о том, на чем строятся и как были получены современные результаты. И, хотя на первый взгляд может быть неясно, какой практический смысл имеет, например, описание всех решений диофантового уравнения $x^a - y^b = 1$ или результат, известный как Великая теорема Ферма, однако конструкции и методы, полученные при исследовании этих и многих других схожих вопросов (а Великой теоремой Ферма занимались практически 350 лет), во многом составляют фундамент современной математики, в особенности алгебры.

Теорема Пифагора, известна уже как минимум 2500 лет. Довольно естественно, что математики древности, старавшиеся, если возможно, не выходить за пределы целых положительных чисел, пришли к задаче об отыскании всех прямоугольных треугольников с целыми стронами. Примеры таких треугольников (в частности самый знаменитый — египетский треугольник с соотношением сторон 3:4:5) известны по крайней мере 4000 лет. Вопрос о том, были ли результаты этих исследований напрямую применены на практике (некоторые авторы полагают, что древние использовали пифагоровы тройки для построения прямого угла) по большей части остаётся спорным, как и вопрос о практической пользе другой задачи, уходящей корнями в древность — задаче о построенях циркулем и линейкой, однако, с точки зрения математики, в процессе рещения этих задач (одно из древнейших дошедших до нас решений задачи о пифагоровых тройках принадлежит Евклиду; теория построений циркулем и линейкой оконачательно сформировалась в начале XIX века) было получено много других результатов, ставших неотъемлемыми частями современной математики.

2 Задача о пифагоровых тройках

2.1 Задача о пифагоровых тройках. Классическое решение

Задача о пифагоровых тройках ставится как задача об отыскании всех натуральных решений уравнения $x^2 + y^2 = z^2$. Это задача интересна также тем, что среди ее решений моно найти применение разных классических техник из разных областей математики. Классический подход к решению задачи — рассмотрение остатков и применение основной теоремы арифметики.

Нахождение всех натуральных решений, очевидно, решает задачу и для $x, y, z \in \mathbb{Z}$, если не рассматривать решения, где одно из слагаемых равно нулю. Также разумно сузить круг рассматриваемых троек до взаимно простых, то есть таких, что $(x, y, z) = 1$, так как все остальные тройки могут быть получены из взаимно простых домножением на число.

Утверждение 1. Если $x, y, z \in \mathbb{N}$ — пифагорова тройка, $(x, y, z) = 1$, то $(x, y) = 1$.

Доказательство. Докажем от противного. Пусть x и y делятся на какое-то простое число p. Тогда $x = p \cdot x', y = p \cdot y'$, следовательно

$$x^2 + y^2 = p^2 \cdot \left(x'^2 + y'^2\right) = z^2 \Rightarrow p \mid z^2 \Rightarrow p \mid z.$$

Из этого следует, что $(x, y, z) \neq 1$, противоречие. □

В доказательстве утверждения стоит выделить неявно используемое утверждение, которое, по сути, является одной из формулировок основной теоремы арифметики для целых чисел.

Утверждение 2. Если число p простое и $p \mid a \cdot b$, то либо $p \mid a$, либо $p \mid b$.

Следующий шаг заключается в рассмотрении чётности слагаемых. Никакие два числа не могут быть чётными, так как тройка взамно проста. Также все три не могут быть нечётными, так как сумма двух нечётных чисел есть чётное число. Таким образом, ровно одно из чисел чётное.

Утверждение 3. Если $(x, y, z) = 1$, то z нечётно.

Доказательство. Легко видеть, что квадраты натуральных чисел дают только остатки 0 и 1 при делении на 4. Если x и y нечётные, то

$$x^2 \equiv y^2 \equiv 1 \pmod 4 \Rightarrow z^2 \equiv 2 \pmod 4,$$

противоречие. □

Теперь без потери общности y — чётное число: $y = 2k$. Тогда

$$4k^2 = z^2 - x^2 = (z - x)(z + x) = \frac{z - x}{2} \cdot \frac{z + x}{2}.$$

В последней части равенства оба числа целые в силу нечётности z и x.

Утверждение 4. $(\frac{z+x}{2}, \frac{z-x}{2}) = 1$.

Доказательство. Если какое-то число делит одновременно $\frac{z+x}{2}$ и $\frac{z-x}{2}$, то оно делит и их сумму, то есть z. Также оно должно делить и их разность, то есть x. Значит $(\frac{z+x}{2}, \frac{z-x}{2}) \mid (x, z) = 1$, откуда следует утверждение. □

Из предыдущих утверждений следует, что k^2 есть произведение двух взаимно простых чисел.

Утверждение 5. Числа $\frac{z-x}{2}$ и $\frac{z+x}{2}$ являются квадратами натуральных чисел.

Доказательство. Пусть $k = p_1^{\alpha_1} \cdot \ldots \cdot p_q^{\alpha_q}$. Тогда, если $p_i \mid \frac{z+x}{2}$, то $p_i^{2\alpha_i} \mid \frac{z+x}{2}$. В самом деле, если это не так, то $p_i \mid \frac{z-x}{2}$ и одновременно $p_i \mid \frac{z+x}{2}$, что входит в противоречие с условием $(\frac{z-x}{2}, \frac{z+x}{2}) = 1$. Отсюда $\frac{z-x}{2} = \prod\limits_{i \in I} p_i^{2\alpha_i}$, $I \subset \{1, \ldots, q\}$, то есть $\frac{z-x}{2}$ является полным квадратом. Аналогичные рассуждения проходят и для $\frac{z+x}{2}$. □

Таким образом,

$$\frac{z+x}{2} = m^2, \frac{z-x}{2} = n^2,$$
$$z = m^2 + n^2, x = m^2 - n^2, y = 2mn$$

Упражнение 1. Если m и n — взаимно простые разной чётности, $m > n$, то числа $m^2 + n^2$, $m^2 - n^2$, $2mn$ взаимно просты.

Вывод. *Все решения диофантова уравнения $x^2 + y^2 = z^2$ имеют вид*

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2,$$

где m, n —взаимно простые натуральные числа разной чётности, $m > n$; при этом каждой такой паре n, m соответсвует решение.

2.2 Задача о пифагоровых тройках. Алгебро-геометрическое решение

Ключевое наблюдение в этом решении таково: ненулевой (возможно тривиальной или не взаимно простой) пифагоровой тройке x, y, z можно сопоставить рациональные числа $\alpha = \frac{x}{z}$ и $\beta = \frac{y}{z}$, причем $\alpha^2 + \beta^2 = 1$, то есть точка (α, β) лежит на единичной окружности.

Более того, верно и обратное. Если рациональная точка $(\frac{a_1}{b_1}, \frac{a_2}{b_2})$ лежит на единичной окружности, то $\forall L \in \mathbb{N}$ такого, что $L\frac{a_1}{b_1}$ и $L\frac{a_2}{b_2}$ — целые, тройка $(L\frac{a_1}{b_1}, L\frac{a_2}{b_2}, L)$ — пифагорова.

Таким образом задача поиска рациональных точек окружности оказывается эквивалентной задаче нахождения всех пифагоровых троек. Для описания всех рациональных точек окружности используется следующий классический прием.

Пусть O — тривиальная рациональная точка, имеющая координаты $(0, -1)$. Пусть (α, β) — рациональная точка и l — прямая, проходящая через нее и через точку O. Уравнение l имеет вид:

$$y = k \cdot x - 1$$

Утверждение 6. $k \in \mathbb{Q} \Leftrightarrow \alpha, \beta \in \mathbb{Q}$.

Замечание. Двум особым случаям $\alpha = 0, \beta = 1$ и $\alpha = 0, \beta = -1$ соответствуют значения $k = \infty$ и $k = 0$.

Доказательство. $k = \frac{\beta+1}{\alpha} \in \mathbb{Q}$, если $\alpha, \beta \in \mathbb{Q}$. В обратную сторону: пересечение прямой l и единичной окружности может быть найдено из уравнения $x^2 + (kx-1)^2 = 1$. Отсюда

$$x^2 + k^2x^2 - 2kx + 1 = 1$$
$$x^2 + k^2x^2 - 2kx = 0$$
$$x^2 \cdot (1 + k^2) = 2kx$$
$$x \cdot (1 + k^2) = 2k$$
$$x = \frac{2k}{1+k^2}$$
$$y = kx - 1 = \frac{2k^2}{k^2+1} - 1 = \frac{k^2-1}{k^2+1}$$

Очевидно, что $k \in \mathbb{Q} \Rightarrow x, y \in \mathbb{Q}$. Также очевидно, что $(-1, 0)$ — тривиальное решение, поэтому сокращение при решении уравнение было произведено правомерно. □

Если $k \in \mathbb{Q}$, то $k = \frac{m}{n}, m, n \in \mathbb{Z}, n \neq 0$. Тогда $\alpha = \frac{2mn}{m^2+n^2}, \beta = \frac{m^2-n^2}{m^2+n^2}$. При выборе числа $L = m^2 + n^2$, получаем пифагорову тройку $(2mn, m^2 - n^2, m^2 + n^2)$. Как видно, соотношения получаются те же, что и в предыдущем решении, однако получены они совершенно иными методами.

2.3 Задача о пифагоровых тройках. Решение в гауссовых целых числах

Здесь и далее все рассматриваемые кольца будут коммутативными, будут содержать единицу и не будет иметь делителей нуля.

Определение 1. Кольцом *гауссовых чисел* $\mathbb{Z}[i]$ называется подкольцо поля $\mathbb{C}$, состоящее из чисел с целой вещественной и мнимой частью.

Определение 2. Ненулевой элемент кольца a называется *обратимым*, если $\exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1$

Определение 3. Ненулевой необратимый элемент кольца a называется *неразложимым*, если из того, что $a = b \cdot c$ следует, что один из элементов b, c обратим.

Определение 4. Кольцо называется *факториальным*, если для любой ненулевой необратимый элемент представляется в виде произведения неразложимых элементов, причем единственным образом*.

*С точностью до обратимых элементов (в $\mathbb{Z}[i]$ это $1, -1, i, -i$), которые составляют *мультипликативную группу* кольца. Элементы кольца, отличающиеся домножением на обратимый, называются *ассоциированным* (обозначение: $a \sim b$). В дальнейшем, все рассуждения будут проводиться с точностью до умножения на обратимые элементы. Ремарки, подобные этой, будут, как правило, опускаться.

Хорошо известно, что наличия в кольце нормы и деления с остатком достатоно для выполнения большинства свойств целых чисел. Кольцо, в котором введена целочисленная норма и определено деление с остатком, называется *евклидовым*. Кольцо гаусовых чисел *евклидово*, его норма унаследованна из поля $\mathbb{C}$. Любое евклидово кольцо факториально, значит каждый неразложимый элемент является *простым*, то есть удовлетворяет свойству из утверждения 2. Таким образом, делимость в кольце гауссовых чисел устроена привычным образом, то есть выполнена основная теорема арифметики.

Гауссовы числа удобно представлять как целочисленную решетку на комплексной плоскости. Сопряженные числа получаются друг из друга поворотом на 90 градусов, поэтому с точки зрения теории делимости можно ограничиться рассмотрением свойств чисел первой четверти.

Простые гауссовы числа без мнимой части будут простыми и в кольце $\mathbb{Z}$. Обратное неверно, в чем можно убедиться на примере $2 = (1+i)(1-i)$. Более того, так как $1+i$ и $1-i$ ассоциированы, то число 2 можно считать точным квадратом. Точно так же, число $5 = (2+i)(2-i)$ перестает быть простым в гауссовых числах, однако, точным квадратом оно уже не будет.

В гауссовых числах уравнение $x^2 + y^2 = z^2$ переписывается как $(x + yi)(x - yi) = z^2$.

Упражнение 2. $(1 + i) \mid (a + bi) \Leftrightarrow a$ и b — одной чётности.

Упражнение 3. Если x, y — взаимно просты в $\mathbb{Z}$, то они взаимно просты и в $\mathbb{Z}[i]$. Более того, для любых $x, y \in \mathbb{Z}$ верно, что $\gcd_{\mathbb{Z}}(x, y) = \gcd_{\mathbb{Z}[i]}(x, y)$.

Утверждение 7. Если $x, y \in \mathbb{Z}$ — взаимно простые разной чётности, то гауссовы числа $x + yi$ и $x - yi$ взаимно просты.

Доказательство. Пусть $x + yi$ и $x - yi$ имеют общий простой делитель p, то есть $p \mid (x + yi), p \mid (x - yi)$. Тогда $p \mid 2x, p \mid 2y$. Так как x, y — разной чётности, то p не может быть ассоциированным с $1 + i$ и не может делить число 2. Тогда $p \mid x, p \mid y$. Противоречие. □

Из утверждения 7 следует, что числа $x + yi$, $x - yi$ являются точными квадратами. Пусть $x+yi \sim (m+ni)^2$, тогда $x+yi \sim m^2-n^2+2mni$. Отсюда, с точностью до порядка x, y и их знаков, вытекает $x = m^2-n^2, y = 2mn, z = m^2 + n^2$, как и в предыдущих решениях.

3 Экскурс в историю математики

3.1 Великая теорема Ферма

Методы, подобные описанным выше (конечно, не в современной математической формулировке, а в традиционной записи того времени), довольно глубоко развил древнегреческий математик Диофант Александрийский, живший примерно в III веке нашей эры. Из 13 томов его «Арифметики»

до нас дошли только первые 6. Его труды, будучи обнаружены в Ватиканской библиотеке Рафаэлем Бомбелли в XVI веке, были частично включены в его труд «Алгебра» и позже полностью изданы, оказав большое влияние на некоторых математиков того времени. Именно на полях «Арифметики», в главе, посвященной исследованию задачи о пифагоровых тройках, Пьер Ферма сделал знаменитое замечание о том, что никакую другую степень нельзя представить в виде суммы двух таких же степеней и он «нашел поистине чудесное доказательство этой теоремы, однако поля книги слишком узки, чтобы его привести». Впоследствии, Ферма опубликовал доказательство для уравнения $x^4 + y^4 = z^2$ (что, очевидно, представляет собой более общий случай), но доказательство общего случая так и не было найдено. Так родилась Великая теорема Ферма, на доказательство которой потребовалось более 350 лет.

Современные Ферма математики в основном были увлечены активно развивающейся дисциплиной математического анализа, однако, эта задача необычайно заинтересовала математиков следующих поколений. Случай $n = 3$ был разобран (с некоторыми оговорками, связанными с основной теоремой арифметики) Эйлером. Доказательство для $n = 5$ было найдено независимо Лежандром и Дирихле, позже альтернативные доказательства нашли Гаусс, Лебег, Ламе, что еще раз показывает внимание, уделяемое великой проблеме.

В 1847 году Габриэлем Ламе была предпринята попытка доказательства общего случая, основанная на идее рассмотрения кольца чисел, подобных гауссовым, но включающего комплексный примитивный корень n-й степени из единицы. Формально, рассматривалось минимальное кольцо, содержащее одновременно целые числа и комплексный корень n-й степени из единицы, обозначаемый, обычно ξ_n или, когда из контекста ясен порядок, просто ξ. Существование такого кольца легко обосновать — так как поле $\mathbb{C}$ есть кольцо, содержащее целые числа и ξ, а пересечение двух колец является кольцом, то среди всех подходящих подколец $\mathbb{C}$ найдется наименьшее по включению. Такая конструкция часто используется в алгебре, а искомое кольцо обозначается как $\mathbb{Z}[\xi]$ (что согласуется с использованным ранее обозначением $\mathbb{Z}[i]$ для гауссовых чисел).

Полученное кольцо $\mathbb{Z}[\xi]$ гораздо сложнее описать, по сравнению с гауссовыми числами. Легко видеть, что кольцо чисел вида $a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{n-2}\xi^{n-2}$ содержит искомое кольцо*. Однако точнее определить, какая наивысшая степень в действительности нужна, не так просто.

Упражнение 4 (сложное)**.** Если n — простое число, то $1, \xi, \ldots, \xi^{n-2}$ линейно независимы.

Замечание. Смысл этого утверждения в том, что для простых значений n придется задействовать все степени ξ вплоть до $n - 2$.

* В самом деле, если $\xi \neq 1$ и $\xi^n - 1 = 0$, то $\xi^{n-1} + \ldots + \xi + 1 = 0$. Поэтому при умножении чисел такого вида от степеней n и выше можно избавиться, используя равенство $\xi^n = 1$, а ξ^{n-1} выражается из предыдущего равенства.

Так или иначе, в этом кольце, выражение $x^n + y^n$ разложится на линейные множители: $(x + y)(x + y\xi) \dots (x + y\xi^{n-1})$. Кажется, что для решения задачи осталось только аккуратно доказать, что все эти числа взаимно просты и являются точными n-ми степенями. Однако, в этом месте появляется другое, гораздо более неприятное препятствие.

Утверждение 8. Кольцо $\mathbb{Z}[\xi_{23}]$ — не факториально.

Это утверждение, технически довольно сложное, в смысловом плане тем не менее одозначно сводит все предудыщие попытки доказательства на нет, так как основная теорема арифметики оказывается необходимым в рассуждениях инструментом. Ошибочное предположение факториальности построенного кольца, практически сразу же отмеченное Жозефом Лиувиллем, оказывается серьезным пробелом в доказательстве Ламе, пробелом, восполнить который так и не удастся.

Более того, даже для малых значений n, структура кольца оказывается очень и очень сложной.

Утверждение 9. Кольцо $\mathbb{Z}[\xi_5]$ — факториально и содержит бесконечное количество обратимых элементов.

Замечание. Удивительный факт также состоит в том, что описание всех обратимых элеметов $\mathbb{Z}[\xi_5]$ сводится к описанию всех целых решений уравнения Пелля: $x^2 - 5y^2 = 1$, что приводит к исследованию таких объектов, как цепные дроби, и изучению приближений иррациональных чисел рациональными.

Великая теорема в итоге, после огромного числа неудачных попыток, была доказана в 1994 году Эндрю Уайлсом. Примечательно, что первый вариант доказательства он опубликовал в 1993 году, но в нем был обнаружен серьезный пробел, который удалось, тем не менее, оперативно устранить. Однако, потребовалось достаточно много времени для того, чтобы математическое сообщество окончательно признало факт доказательства, что впрочем есть здоровый скептицизм, накопленный за 357 полных неудачных попыток лет. Доказательство построено на теории элиптических кривых, разделе алгебрической геометрии, не имея практически ничего общего с приведенными выше попытками. Так, за века, проведенные над решением задачи, не только были развиты и отточены известные еще древним идеи и методы, но и придуманы совершенно новые подходы и концепции, нашедшие применение во многих других областях математики.

3.2 Наследие иных методов

В итоге, из элементарных подходов, помогших тремя разными способами решить задачу о пифагоровых тройках, развились совершенно разные науки. Классическая арифметика и теория делимости, с которых все начиналось, в конечном итоге стали неиссякаемым источников задач и различных техник, породив в том числе и саму Великую теорему Ферма.

Алгебраическая геометрия была развита в основном в XX веке, развив теорию элептических кривых и много других красивых разделов, открыв в конечном итоге путь к решению задачи, стоявшей больше трех столетий. Еще одним примечательным для этой науки уравнением стало безобидное с виду $x^a - y^b = 1$. Удивительный результат касательно этой, окончательно решенной в 2002 году проблемы, таков.

Утверждение 10. Если x, y, a, b — натуральные числа, $a, b > 1$, то $x = 3, a = 2, y = 2, b = 3$.

Гауссовы же числа, введенные в мнографии Карла Фридриха Гаусса «Теория биквадратичных вычетов» также стали необходимым инструментом в математическом арсенале. С их помощью могут быть решены различные задачи о суммах квадратов, например, какие числа могут быть представлены в виде суммы двух квадратов и сколькими способами. С этой задачей связана еще одна, описание которой начинается казалось бы совсем изделека.

Первое известное доказательство того, что простых числе бесконечно много предложил еще Евклид. Сейчас это рассуждение знакомо каждому школьнику: если простые числа исчерпываются каким-то набором $p_1, \ldots, p_n$, то наименьший простой делитель числа $p_1 \cdot \ldots \cdot p_n + 1$ не может входить в этот набор по очевидным причинам. Поэтому это «новое» простое число, не входящее в наш набор, что влечёт противоречие.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ... После недолгого созерцания первых нескольких простых чисел можно заметить, что нечётные простые, имеющие остаток 1 от деления на 4 встречаются не реже тех, что имеют остаток 3. Нет ни какой-либо видимой закономерности, ни очевидной причины для того, чтобы какие-то из этих чисел когда-нибудь закончились. Возникает вопрос: конечно ли количество простых вида $4k + 3$? Ответ отрицательный, и это не очень сложно доказать, используя знакомый прием.

Утверждение 11. Существует бесконечно много простых чисел вида $4k + 3$.

Доказательство. Пусть простые вида $4k + 3$ исчерпываются каким-то набором $p_1, \ldots, p_n$. Тогда число $4p_1 \cdot \ldots \cdot p_n - 1$, имея остаток 3 по модулю 4, не делится ни на одно из чисел $p_1, \ldots, p_n$. Значит, все его простые делители имеют вид $4k + 1$. Но тогда оно само имеет остаток 1 по модулю 4, так как два числа вида $4k + 1$ при умножении дают число того же вида. Противоречие. □

Легко видеть, что с простыми вида $4k+1$ этот метод не сработает и нужно придумывать что-то новое. Ответ на этот вопрос неожиданным образом возвращает к задаче о числах, представимых в виде суммы двух квадратов, что в свою очередь приводит нас к гауссовым числам.

Примечательно, что выполнена гораздо более общая (вместе с тем, гораздо более сложная) теорема.

Теорема 1 (Дирихле)**.** *Если $a, b \in \mathbb{N}$ — взаимно простые, то существует бесконечно много простых чисел вида $ak + b$.*

3.3 Задачи о простых

Простые числа, естественно, стали источником огромного числа математических задач. В их числе древнейшая, однако, все еще не решенная, проблема простых-близнецов. Вопрос: конечно ли число соседних простых чисел, отличающихся ровно на 2. Из теоремы о законе распределения простых чисел, доказанная в конце XIX столетия Адамаром, следует, что n-е простое число асимптотически имеет порядок $n \cdot \ln n$. Промежуток же между соседними простыми числами растет асимптотически не медленнее, чем $\ln n$. Функция бесконечно растущая, и кажется, что это весомый аргумент в пользу того, что количество простых-близнецов все-таки конечно.

Однако, ошеломляющие, притом совсем недавние (2013 год), результаты Итана Чжана показывают, что для некоторого $N < 7 \cdot 10^7$ существует бесконечно много простых, отстоящих друг от друга ровно на N. К 2014 году совместными усилиями Теренса Тао и проекта Polymath константа $7 \cdot 10^7$ была последовательно улучшена до 4680, затем до 600 и, наконец до 246. Используя широко известные недоказанные, но предположительно верные, гипотезы, оценку улучшили до $N = 12$, а позже и до $N = 6$.

Методы, используемые в этих работах относятся к очень современному разделу математики — аддитивной комбинаторике, который, можно сказать, складывается прямо сейчас. Так, одна из древнейших математических проблем может в скорейшем времени оказать решенной, породив, как и все перечисленные необычайно короткие и простые в постановке задачи, большой и очень плодотворный раздел математики.

Следующая примечательная задача состоит в описании совершенных чисел.

Определение 5. Число n называется совершенным, если $\sum\limits_{d|n} d = n$.

Упражнение 5 (простое)**.** Если $2^n - 1$ — простое, то число $2^{n-1}(2^n - 1)$ — совершенное.

Упражнение 6 (посложнее)**.** Все чётные совершенные числа представляются в виде $2^{n-1}(2^n - 1)$, где $2^n - 1$ —простое.

Упражнение 7 (открытая проблема)**.** Доказать, что нечётных совершенных чисел не существует.

Более того, неизвестно даже, бесконечно ли количество чётных совершенных чисел, то есть неизвестно, конечно ли число простых вида $2^n - 1$ — простых чисел Мерсенна.

Если же полюбопытствовать и задать очень похожий вопрос: конечно ли число простых вида $2^n + 1$, то очень скоро выяснится, что n в свою очередь тоже должно быть степенью двойки.

Утверждение 12. Если n не является степенью двойки, то $2^n + 1$ — составное.

Доказательство. Если n не является степенью двойки, то оно представляется в виде $n = rs$, где r нечётно. Тогда $2^n + 1 = 2^{rs} + 1 = (2^s)^r + 1 = (2^s + 1)(2^{s(r-1)} - 2^{s(r-2)} + \ldots + 1)$. Оба множителя, очевидно, отличны от 1, значит $2^n + 1$ — составное. □

Так, сменой знака «+» на «−» получается другая все ещё открытая проблема — вопрос существовании бесконечного количества простых чисел Ферма. При том, что сам Ферма предполагал, что все числа такого вида просты, что было опровергнуто Эйлером (из числа $2^{32} + 1$ он выделил множитель 641), на сегодняшний день не известно никаких простых чисел Ферма, кроме первых четырёх.

Еще одна гипотеза о простых числах — гипотеза Гольдбаха-Виноградова: любое чётное число представляется в виде суммы двух простых чисел. В начале XX века совершенно неожиданным открытием стало доказательство того, что любое число представляется в виде суммы $k < 700$ простых чисел. Но вскоре после этого Виноградов доказал еще более потрясающее утверждение: любое нечётное число представляется в виде суммы 3-х простых чисел. Для чётных чисел тем самым, достаточно четырёх простых. Вопрос о том, достаточно ли двух, остаётся открытым.

3.4 Математическая революция XIX века

Наконец, еще один плодотворнейший раздел, в корне преобразивший в свое время алгебру, о котором уже упоминалось. К началу XIX века были хорошо известны четыре задачи, стоявшие со времен античности.

Имея единичный отрезок:

- Построить круг площади 1 (построить отерзок длины π).
- Построить куб объёма 2 (построить отрезок длины $\sqrt[3]{2}$).
- Разбить данных угол на три равных.
- Найти все правильные многоугольники, которые можно построить

К тому моменту сформировалась достаточно развитая алгебра, чтобы снять второй и третий вопросы (по сути, стало известно, какие длины отрезков можно построить, однако, долго было не понятно, является ли π таким числом). С последней задачей дела обстояли сложнее.

Античным геометрам были известны способы построения 3-х и 5-и угольника (можно показать, что для решения задачи достаточно выяснить, какие простые n-угольники можно построить). В 1796 году Гаусс нашел способ построить 17-угольник (и завещал изобразить его на своей могиле). Более того, позже он сформулировал полный критерий построимости многоугольника цикрулем и линейкой, который вновь отсылает нас к задаче о простых числах Ферма.

Еще одна очень простая в постановке задача, долгое время волновавшая умы математиков состоит в решении уравнений в радикалах. Каждый знает формулу корней квадратного уравнения через его коэффициенты. Также весьма известна аналогичная формула для корней кубического уравнения — формула Кардано. Для уравнения четвёртой степени аналогичная формула носит имя Феррари. К XVII веку эти формулы были уже хорошо известны и велись активные поиски общей формулы для уравнения n-й или хотя бы 5-й степени. В начале XIX века произошёл ряд продвижений в этой задаче. Сперва было доказано, что общей формулы нет для всех n, но было неясно, можно ли найти какой-то конкретный многочлен, корни которого бы не выражались в радикалах. Построить такой многочлен удалось Галуа, он же развил полную теорию, получившую после его имя, описывающую полный критерий разрешимости уравнения в радикалах. На тот момент открытие было потрясающего масштаба. Снятие бывших открытыми с античности проблем, связанных с разрешимостью, ознаменовало настоящую математическую революцию и создание той алгебры, которую мы знаем сейчас.