Лекция 2. Великая теорема Ферма для малых показателей

Теорема 1 (Ферма)**.** *Для любого $n > 2$ не существует отличных от нуля натуральных чисел x, y, z таких, что $x^n + y^n = z^n$.*

1 Великая теорема Ферма при $n = 4$

1.1 Доказательство при $n = 4$

Это самый простой случай теоремы, доказать его можно, не выходя за пределы натуральных чисел. Доказательство, которое в свое время придумал Пьер Ферма*, основано на изобретенном им методе «бесконечного спуска», в сущности, одном из видов индукции. В первую очередь, как это часто бывает, рассуждая по индукции, удобно перейти к более общему уравнению $x^4 + y^4 = z^2$. Шаг будет заключаться в следующем: пусть из всех решений данного уравнения некоторое (положительное, так как знаки переменных неважны) решение (x, y, z) имеет наименьший z. Если по этому решению можно построить другое, с меньшим z, то теорема будет доказана.

Утверждение 1. Числа x, y, z попарно взаимнопросты (пишут $\ll x, y, z \gg = 1$, где под записью $\ll a_1, \ldots, a_n \gg$ понимается максимальный из попарных наибольших общих делителей a_i и a_j, $1 \leqslant i \neq j \leqslant n$).

Доказательство. Пусть какие-либо два числа из x, y, z делятся на простое число p. Тогда очевидно, что третье также делится на p. Тогда

$$x = p\overline{x}, y = p\overline{y}, z = p\overline{z},$$
$$p^4(\overline{x}^4 + \overline{y}^4) = p^2\overline{z}^2,$$
$$p^2(\overline{x}^4 + \overline{y}^4) = \overline{z}^2,$$
$$p \mid \overline{z}^2 \Rightarrow p \mid \overline{z} \Rightarrow \overline{z} = p\overline{\overline{z}},$$
$$\overline{x}^4 + \overline{y}^4 = \overline{\overline{z}}^2, \overline{\overline{z}} < z.$$

Противоречие с минимальностью z. □

Далее, (x^2, y^2, z) — пифагорова тройка. Число z обязательно нечётно, а среди x и y чётным без потери общности можно считать x. Тогда

$$x = 2x_1,$$
$$4x_1^2 = 2mn, y^2 = m^2 - n^2, z = m^2 + n^2,$$
$$y^2 \bmod 4 = 1 \Rightarrow 2 \nmid m, 2 \mid n \Rightarrow n = 2n_1,$$
$$x_1^2 = mn_1$$

*Это одно их тех редких его доказательств, что были записаны и дошли до нас

Далее, если $p \mid \gcd(m,n)$, то $p \mid \gcd(x,y) = 1$, значит m и n взаимно просты, поэтому m и n_1 тоже. Тогда $m = a^2, n_1 = b^2$ для каких-то натуральных a, b.

Из того, что $y^2 = m^2 - 4n_1^2 \Rightarrow y^2 + 4n_1^2 = m^2$ следует, что $(y, m, 2n_1)$ — пифагорова тройка. Тогда для каких-то взаимно простых натуральных q и r выполнено $m = q^2 + r^2, 2n_1 = 2qr$. Итак, $n_1 = qr$ и одновременно $n_1 = b^2$. Так как q и r взаинопросты, то они должны являться полными квадратами: $q = t^2, r = s^2$. Итого,

$$m = q^2 + r^2, m = a^2, q = t^2, r = s^2,$$
$$a^2 = t^4 + s^4.$$

Так как $a = \sqrt{m} \leqslant m \leqslant m^2 < z$, то тройка (t, s, a) даёт необходимое противоречие.

1.2 Роль случая $n = 4$ в общей задаче

Стоит отдельно отметить, что в общем случае теоремы Ферма, если $n > 2$, то либо $4 \mid n$, либо n имеет нечётный простой делитель. Если $n = 4k$, то соотношение $(x^k)^4 + (y^k)^4 = (z^k)^4$ противоречит только что проведённым рассуждениям. Аналогичное рассуждение полностью сводит задачу к рассмотрению только простых значений n.

Куммер в середине XIX века доказал теорему для широкого класса регулярных простых (предположительно их плотность в натуральном ряде не превосходит 40%, а в первой сотне нерегулярных простых только три: 37, 59, 67). Позже с помощью компьютера его доказательство было доработано для всех простых, не превосходящих 2521 (1954 г.), а позже 125,000 (1978 г.) и 4,000,000 (1993 г.). Однако полностью решить задачу используя машинные вычисления практически невозможно.

Упражнение 1. Если бы теорема Ферма была бы неверна и $x^n + y^n = z^n$, то $|x|, |y|, |z| > n$.

Это упражнение иллюстрирует, что компьютерный поиск контрпримера требовал бы проведения операций с числами порядка n^n, что для даже для n порядка 125,000 представляет вычислительно сложную задачу.

2 Числа Эйзенштейна

2.1 Норма и обратимые элементы

Для решения задачи при $n = 3$ необходимо исследовать структуру кольца $\mathbb{Z}[\omega]^*$ — так называемых чисел Эйзенштейна.

Упражнение 2. Пусть $\xi \neq 1$ — любой нетривиальный корень из единицы степени p (p — простое), тогда

$$x^p + y^p = (x + y)(x + \xi y) \ldots (x + \xi^{p-1} y).$$

$^*\omega = e^{\frac{2\pi}{3} i} = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$ — примитивный корень из единицы степени 3.

Таким образом, в кольце $\mathbb{Z}[\omega]$ выражение $x^3 + y^3$ раскладывается на линейные множители, что значительно облегчает анализ.

Стоит напомнить, что в общем случае $\mathbb{Z}[\xi_p]$ не является факториальным кольцом и основная теорема арифметики в нем не выполнена (первый такой пример при $p = 23$), что в свое время помешало Ламе построить доказательство для общего случая. Для некоторых простых можно доказать теорему из других соображений, в частности, Софи Жермен сделала это в случае, если p и $2p+1$ одновременно простые* и $p \nmid xyz$. Надо заметить, что случай $p \mid xyz$ сильно сложнее для анализа даже при $p = 3$ (в доказательстве существенно используется то обстоятельство, что 3 — не простое число в $\mathbb{Z}[\omega]$).

Упражнение 3 (сложное)**.** Найти разложения на простые множители 5 в $\mathbb{Z}[\xi_5]$ и p в $\mathbb{Z}[\xi_p]^\dagger$.

Итак, $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$, так как $\omega^2 = -1 - \omega$ (более строго, здесь сказано, что этот набор чисел является кольцом и что все числа такого вида лежат в $\mathbb{Z}[\omega]$, которое по определению есть минимальное кольцо, содержащее $\mathbb{Z}$ и ω). Невероятно удобная и естественная визуализация чисел Эйзенштейна — изображение их на комплексной плоскости, где они формируют полное замощение правильными треугольниками.

Определение 1. Нормой числа $z = a + b\omega$ называется $N(z) = a^2 - ab + b^2$. Легко убедиться, что $N(z) = a^2 + ab(\omega^2 + \omega) + b^2\omega^3 = (a + b\omega)(a + b\omega^2) = (a + b\omega)(a + b\overline{\omega}) = z\overline{z}$, то есть $N(z)$ — это квадрат привычной комплексной нормы.

Удобное свойство такой нормы — мультипликативность. В самом деле, очевидно, что $\forall a, b \in \mathbb{Z}[\omega] \to N(ab) = N(a)N(b)$. Стоит отметить, что это ни в коем случае не является аксимой нормы, и в других кольцах это свойство может не быть выполнено.

При исследовании евклидового кольца первоочередная задача заключается в описании его мультипликативной группы ведь основная теорема арифметики верна с точностью до умножения на обратимые элементы.

Утверждение 2. $a \in \mathbb{Z}[\omega]$ — обратим $\Leftrightarrow N(a) = 1$.

Доказательство. $N(a) = 1 \Rightarrow a\overline{a} = 1 \Rightarrow \overline{a}$ — обратный к a элемент.

Если $ab = 1$, то $ab\overline{ab} = 1 \Rightarrow N(a)N(b) = 1$. Произведение двух целых положительных чисел равно 1 тогда и только тогда, когда каждой из них равно 1, то есть $N(a) = 1$. □

$$N(a + b\omega) = 1 \Leftrightarrow a^2 - ab + b^2 = 1,$$
$$4a^2 - 4ab + 4b^2 = 4,$$
$$(2a - b)^2 + 3b^2 = 4.$$

*Такие простые в честь неё названы простыми Софи Жермен.

†В нефакториальных кольцах за определение простого берется свойство $p \mid ab \Rightarrow p \mid a$ или $p \mid b$.

Далее очевидно, что задача сводится к перебору целых значений b от -1 до 1. При фиксированном значении b для a существует не более двух возможных значений.

Упражнение 4. Перебрав варианты, показать, что обратимыми в кольце чисел Эйзенштейна являются элементы $1, -1, \omega, -\omega, 1+\omega, -1-\omega$.

Если записать эти элементы в другом виде, то можно увидеть, что все они представляют собой степени числа $1+\omega$, которое является примитивным корнем степени шесть из единицы. Это также означает, что мультипликативная группа кольца чисел Эйзенштейна изоморфна $\mathbb{Z}_6$.

2.2 Число λ

Дальнейшее исследование коснется важного числа $\lambda = 1 - \omega$. Первое наблюдение состоит в том, что $N(\lambda) = 3$.

Утверждение 3. Если норма числа $p \in \mathbb{Z}[\omega]$ — простое число, то само число p тоже простое.

Доказательство. Если p равно произведению двух неразложимых необратимых элементов a и b, то $N(p) = N(a)N(b)$, то есть какая-то из норм равна 1, а в этом случае или a или b — обратимый элемент, как было показано ранее*. □

Более того, тот факт, что норма числа λ равна 3, автоматически означает, что $3 = \lambda\overline{\lambda} = (1-\omega)(2+\omega)$ в этом кольце не является простым числом. Это обстоятельство помогает разобрать важный случай $3 \mid xyz$, который в общем случае ($n \mid xyz$) представляет наибольшую трудность (в частности, как было сказано выше, Софи Жермен удалось доказать вариант теоремы для обширного класса простых, но только при $n \nmid xyz$). С точки зрения делимости, λ, как и любое другое простое число, имеет ровно 12 делителей — 6 обратимых и 6 ассоциированных.

Естественным образом, решение уравнения Ферма (доказательство отсутствия решений) в числах Эйзенштейна автоматически решает задачу и в целых числах. Используя внутренние симметрии кольца, можно заметить, что домножение x, y или z на любой корень из единицы третьей степени (и даже шестой, так от этого меняется только знак соответсвующего слагаемого) не меняет множество решений. Так, например, если одно из чисел $x+y$, $x+y\omega$, $x+y\omega^2$ делится на какое-то число q, то без потери общности можно считать, что это число $x+y$, так как в противном случае, домножая x и y на нужную степень ω, можно получить тройку, все еще являющуюся решением уравнения Ферма и удовлетворяющую нужному свойству.

Утверждение 4. Пусть $x \in \mathbb{Z}[\omega]$, $\lambda \nmid x$. Тогда $x^3 \equiv \pm 1 \pmod 9$.

* В этом доказательстве использована как основная теорема арифметики, так и мультипликативность нормы, поэтому в произвольном кольце оно не проходит. Более того, можно убедиться, что в произвольном кольце утверждение неверно.

Упражнение 5.

(1) В $\mathbb{Z}[\omega]$ существует ровно 3 класса вычетов по модулю λ: $\{0, 1, -1\}$.

(2) В $\mathbb{Z}[\omega]$ существует ровно $N(p)$ классов вычетов по модулю p.

Доказательство. Если x не кратен λ, то $x = r\lambda \pm 1$. Тогда

$$x^3 = r^3\lambda^3 \pm 3r^2\lambda^2 + 3r\lambda \pm 1.$$

Учитывая, что $3\lambda^2 \equiv 0 \pmod 9$, необходимо показать, что $r^3\lambda^3 + 3r\lambda$ делится на 9.

$$r^3\lambda^3 + 3r\lambda = 3r\lambda - 3r^3\lambda\omega = 3\lambda(r - r^3\omega).$$

В свою очередь $r = 0, 1$ или $-1 \pmod \lambda$. Если $\lambda \mid r$, то при вынесении r выражение перед скобками делится на 9. Иначе $r = q\lambda \pm 1$, в этом случае $r^2 = q^2\lambda^2 \pm 2q\lambda + 1$. Тогда $\lambda \mid (r^2 - 1)$, то есть $r^2 = \lambda s + 1$. Итого,

$$3\lambda r(1 - r^2\omega) = 3\lambda r(1 - \omega - \lambda s\omega) = 3\lambda r(\lambda - \lambda s\omega) = 3\lambda^2(1 - s\omega) \equiv 0 \pmod 9$$

□

Замечание. Геометрический смысл утверждения заключается в том, что числа, кратные λ, но не кратные λ^2, в кубе не могут попасть на расстояние меньше 3 от чисел, кратных λ^4.

3 Великая теорема Ферма при $n = 3$

3.1 Основная теорема арифметики в $\mathbb{Z}[\omega]$

Утверждение 5. $\pm x^3 \pm y^3 \pm z^3 \neq 0$ при $\lambda \nmid xyz$.

Доказательство. Если ни одно из чисел x, y, z не делится на λ, то их кубы дают остаток ± 1 по модулю 9, а значит их сумма не сравнима с 0 по модулю 9, то есть не равна 0. □

Далее можно считать, что $\ll x, y, z \gg = 1$, значит ровно одно число делится на λ. Исследовать этот случай можно методом «бесконечного спуска», рассмотрев более общее уравнение $\varepsilon_1 x^3 + \varepsilon_2 y^3 + \varepsilon_3 z^3 = 0$, где $\varepsilon_1, \varepsilon_2, \varepsilon_3$ — произвольные обратимые, $xyz \neq 0, \ll x, y, z \gg = 1, \lambda \mid xyz$. Первое ключевое рассуждение заключается в следующем утверждении.

Утверждение 6. $\lambda^2 \mid xyz$.

Доказательство. Пусть без потери общности $z = -\lambda\overline{z}$. Тогда

$$\varepsilon_1 x^3 + \varepsilon_2 y^3 = \varepsilon_3 \lambda^3 \overline{z}^3, \lambda \nmid \overline{z}.$$

Тогда по модулю 9 левая часть есть $\pm\varepsilon_1 \pm \varepsilon_2$, а правая не равна 0 и делится на λ^3, но не на λ^4. По предыдущим утверждениям это противоречие. □

Прежде чем предпринять следующий шаг, необходимо внести ясность в вопрос об основной теореме арифметики в кольце чисел Эйзенштейна. Так как норма уже была введена, осталось только привести правило деления с остатком, согласующееся с нормой в смысле определения евклидового кольца.

Утверждение 7. Если $z_1, z_2 \in \mathbb{Z}[\omega]$, то $\exists \beta, \gamma \in \mathbb{Z}[\omega]\colon z_1 = z_2\beta + \gamma$, причём $N(\gamma) < N(z_2)$*.

Доказательство. $\frac{z_1}{z_2} = \frac{a+b\omega}{c+d\omega} = \alpha + \beta\omega, \alpha, \beta \in \mathbb{R}$. Пусть r, s являются округлёнными до ближайшего целого числами α, β. Тогда для числа $\gamma/z_2 = (\alpha - r) + (\beta - s)\omega$ верно, что $|\alpha - r|, |\beta - s| \leqslant 0.5$ (здесь число γ неявно определено через числа α, β, r, s, z_2)). В таком случае, сообразно с формулой для нормы, получается

$$N(\frac{\gamma}{z_2}) \leqslant |\alpha - r|^2 + |\alpha - r||\beta - s| + |\beta - r|^2 \leqslant \frac{3}{4} \Rightarrow N(\gamma) < N(z_2).$$

Итого $z_1 = z_2(r + s\omega) + \gamma$, $N(\gamma) < N(z_2)$. γ будет числом Эйзенштейна, так как все остальные числа в равенстве лежат в $\mathbb{Z}[\omega]$. $\square$

Упражнение 6 (сложное)**.** Найти норму в кольце $\mathbb{Z}[\xi_5]$.

3.2 Доказательство при $n = 3$

Теперь, автоматически получив основную теорему арифметики для кольца чисел Эйзенштейна, можно сформулировать второе ключевое утверждение, которое по сути является шагом метода «бесконечного спуска».

Утверждение 8. Если $\varepsilon_1 x^3 + \varepsilon_2 y^3 = \varepsilon_3 \lambda^{3k} z^3, k \geqslant 2$, причём $\lambda \nmid z$, то существуют числа $\overline{x}, \overline{y}, \overline{z}, \sigma_1, \sigma_2, \sigma_3$, являющиеся решенем уравнения $\overline{\sigma}_1 \overline{x}^3 + \overline{\sigma}_2 \overline{y}^3 = \overline{\sigma}^3 \lambda^{3k-3} \overline{z}^3$, причём $\lambda \nmid \overline{z}$.

Доказательство. По модулю 9 данное уравнение обращается в сравнение $\pm\varepsilon_1 \pm \varepsilon_2 \equiv 0 \pmod 9$, что конечно, заменяется обычным равенством, то есть $\varepsilon_1 = \pm\varepsilon_2$. Итак,

$$\pm\varepsilon_2 x^3 + \varepsilon_2 y^3 = \varepsilon_3 \lambda^{3k} z^3.$$

Далее, поделив на ε_2 и меняя при необходимости знак x, получаем

$$x^3 + y^3 = u\lambda^{3k} z^3,$$

$$(x + y)(x + y\omega)(x + y\omega^2) = u\lambda^{3k} z^3,$$

$$(x + y) - (x - y\omega) = y\lambda, (x + y) - (x + y\omega^2) = y\lambda(1 + \omega)$$

---

*Вообще говоря, норма нулевого элемента евклидового кольца не определена (для примера можно рассмотреть кольцо многочленов, которое тоже является евклидовым с нормой, равной степени многочлена). Но, работая с кольцами, аналогичными числам Эйзенштейна, как правило оставляют за нулевым элементом нулевую норму

Во-первых, невозможна ситуация, когда $\lambda^2 \mid (x+y, x+y\omega)$, так как в этом случае $\lambda^2 \mid y\lambda \Rightarrow \lambda \mid y$, но в то же время $\lambda \mid z$, противоречие. Аналогично, наибольший общий делитель любой другой пары скобок не делится на λ^2.

Во-вторых, в разложении $(x+y, x+y\omega)$ не существует никаких простых множителей, кроме λ. Если $p \mid (x+y, x+y\omega)$, то $p \mid y\lambda \Rightarrow p \mid y$. Однако, $p \mid (\omega(x+y) - (x+y\omega)) = -x\omega \Rightarrow p \mid x$, что невозможно, так как $(x,y) = 1$. Так как $x + y \equiv x + y\omega \equiv x + y\omega^2 \pmod{\lambda}$, то $\ll x, y, z \gg \in \{1, \lambda\}$.

Однако, так как правая часть уравнения делится на λ, то и левая тоже, значит каждая скобка делится на λ. Более того, в одну скобку λ входит в степени $3k-2 \geqslant 4$, а в остальные в степени 1. Без потери общности $\lambda^{3k-2} \mid (x+y)$.

$$
\begin{gathered}
x+y = \alpha\lambda^{3k-2}, x+y\omega = \beta\lambda, x+y\omega^2 = \gamma\lambda, \\
\ll \alpha, \beta, \gamma \gg = 1, \\
\alpha\beta\gamma = uz^3,
\end{gathered}
$$

По основной теореме арифметики:

$$
\begin{gathered}
x+y = \lambda^{3k-2}\alpha = \sigma_1\lambda^{3k-2}\overline{x}^3, \\
x+y\omega = \lambda\beta = \sigma_2\lambda\overline{y}^3, \\
x+y\omega^2 = \lambda\gamma = \sigma_3\lambda\overline{z}^3.
\end{gathered}
$$

Сложив с коэффициентами $1, \omega, \omega^2$, получаем 0 в левой, части, то есть

$$
\begin{gathered}
0 = \sigma_1\lambda^{3k-2}\overline{x}^3 + \sigma_2\omega\lambda\overline{y}^3 + \sigma_3\omega^2\lambda\overline{z}^3, \\
\overline{\sigma}_1\lambda^{3k-3}\overline{x}^3 = \overline{\sigma}_2\overline{y}^3 + \overline{\sigma}_3\overline{z}^3, \\
\ll \overline{x}, \overline{y}, \overline{z} \gg = 1.
\end{gathered}
$$

Что в точности и нужно доказать. □

Таким образом, если существует решение уравнения Ферма со степенью вхождения λ, равной k, то по доказанному можно за $k-1$ шаг перейти к решению со степенью 1, а таких решений нет.

4 Великая теорема Ферма при $n = 5$

4.1 План доказательства при $n = 5$

Первый важный вопрос уже фигурировал раньше в виде упражнения 6. Далее, необходимо немного исследовать структуру кольца $\mathbb{Z}[\xi_5]$.

Упражнение 7 (сложное)**.** Найти мультипликативную группу $\mathbb{Z}[\xi_5]$. Сперва может быть полезно найти обратимые из $\mathbb{Z}[\xi_5] \cap \mathbb{R}$.

Упражнение 8. Обобщить прием, использованный в утверждении 8, то есть найти способ скомбинировать уравнения

$$\begin{aligned} x + y &= \alpha_1 \lambda^q, \\ x + y\xi &= \alpha_2 \lambda, \\ &\dots, \end{aligned}$$

чтобы снизить степень делимости на λ. Найти, чему в этом случае равняется λ и найти разложение числа 5 на простые множители.

Упражнение 9. Доказать теорему Ферма при $n = 5$.