Проблема Каталана.
I. Элементарное вступление

В 1844 г. бельгийский математик Е. Каталан [Cat] поставил следующую задачу.

Проблема Каталана. *Доказать, что все целочисленные решения уравнения*

$$x^p - y^q = 1, \qquad x, y, p, q \in \mathbb{Z}, \quad x > 1,\ y > 1,\ p > 1,\ q > 1, \tag{1}$$

исчерпываются набором $x = q = 3$, $y = p = 2$ (*т.е.* $3^2 - 2^3 = 1$).

Отметим, что достаточно ограничиться рассмотрением случая, когда p и q – различные простые числа; далее мы всюду считаем это соглашение выполненным.

Последнюю точку в решении проблемы Каталана поставил П. Михайлеску [Mi1], [Mi2] в 2002 г. В частности, он доказал следующий результат.

Критерий Михайлеску. *Пусть* p *и* q *– нечетные простые числа,* $p \neq q$, *и четверка* x, y, p, q *удовлетворяет уравнению Каталана* (1). *Тогда*

а) $p^{q-1} \equiv 1 \pmod{q^2}$ *и* $q^{p-1} \equiv 1 \pmod{p^2}$;

б) $q^2 \mid x$ *и* $p^2 \mid y$.

Замечание. Сравнения $p^{q-1} \equiv 1 \pmod{q}$ и $q^{p-1} \equiv 1 \pmod{p}$ следуют из малой теоремы Ферма (без всяких дополнительных ограничений на p и q, $p \neq q$).

Делимости $q \mid x$ и $p \mid y$ были доказаны Касселсом в 60-е годы; с их помощью Тайдеман доказал конечность количества решений уравнения (1), опираясь на линейные формы от двух и трех логарифмов. Однако, критерий Михайлеску позволяет ограничиться линейными формами от двух логарифмов и существенно снизить границу компьютерного перебора.

В качестве лирического отступления рассмотрим классический (или исторический) результат (доказательство мы заимствуем из [Se]).

Теорема 0 (Леви бен Гершон, около 1320). *Уравнения*

$$1) \quad 3^p - 2^q = 1 \qquad \textit{и} \qquad 2) \quad 2^p - 3^q = 1$$

не имеют решения в целых $p, q > 1$, *за исключением решения* $p = 2$, $q = 3$ *уравнения* 1).

В основу этих материалов лег цикл докладов Ю. В. Нестеренко на семинаре “Диофантовы приближения и трансцендентные числа” механико-математического факультета Московского университета. Настоящие конспекты являются адоптированным изложением В. В. Зудилина. Мы искренне благодарны Ю. А. Алексенцеву, Е. М. Матвееву и всем участника семинара за помощь и обсуждения. Особая благодарность М. Миньотту за предоставленные им материалы лекций по проблеме Каталана.

Доказательство. 1) Если $p = 2k+1$, то

$$2^q = 3^p - 1 = 3 \cdot 9^k - 1 \equiv 2 \pmod 4,$$

что для $q > 1$ невозможно.

Если $p = 2k$, то $2^q = 3^p - 1 = (3^k - 1)(3^k + 1)$, откуда $3^k - 1 = 2^u$ и $3^k + 1 = 2^v$. Поскольку $2^v - 2^u = (3^k + 1) - (3^k - 1) = 2$, имеем $v = 2$ и $u = 1$, откуда получаем единственное решение $q = u + v = 3$ и $p = 2$.

2) Если $q \geqslant 1$, то $3^q + 1$ не делится на 8. Действительно, если $q = 2k$, то $3^q + 1 = 9^k + 1 \equiv 2 \pmod 8$; если $q = 2k+1$, то $3^q + 1 = 3 \cdot 9^k + 1 \equiv 4 \pmod 8$. Поэтому $p \leqslant 2$ и, значит, $p = 2$. Последнее влечет $q = 1$, что невозможно.

Вклад самого Каталана в решении проблемы Каталана нельзя назвать значительным: он получил окончательный результат для уравнения $x^y - y^x = \pm 1$, что не сложнее рассмотренной выше теоремы Леви бен Гершона.

Теорема 1 (Лебег, 1850). *Пусть p – нечетное простое число. Тогда уравнение $x^p - y^2 = 1$ не имеет решений в целых $x, y > 1$.*

Доказательство. 1) Если y нечетно, то x четно ввиду $x^p = y^2 + 1$. Тогда $y^2 + 1 \equiv 2 \pmod 4$, в то время как $x^p \equiv 0 \pmod 8$.

2) Пусть y четно и, значит, x нечетно. Запишем $x^p = y^2 + 1 = (1 + iy)(1 - iy)$. Разложение на простые в кольце гауссовых чисел $\mathbb{Z}[i]$ единственно; кроме того, числа $1 + iy$ и $1 - iy$ (как элементы этого кольца) взаимно просты. Действительно, если λ делит $1 + iy$ и $1 - iy$, то λ делит их разность $(1 + iy) - (1 - iy) = 2$, а значит, и *четное* число y; таким образом, λ делит $1 + iy$ и y, в частности, λ делит $(1 + iy) - i \cdot y = 1$, т.е. $\lambda \in \{\pm 1, \pm i\}$ и $(1 + iy, 1 - iy) = 1$. Из единственности разложения на простые получаем, что $1 + iy = \varepsilon(u + iv)^p$, где ε – некоторая единица кольца $\mathbb{Z}[i]$, т.е. $\varepsilon \in \{\pm 1, \pm i\}$, а $u, v \in \mathbb{Z}$. Поскольку $\varepsilon = i^r$, причем $r \in \{0, 1, 2, 3\}$, а p – простое *нечетное* число, для некоторых $a, b \in \mathbb{Z}$ выполнено $r = 4a + pb$, т.е. $i^r = (i^b)^p$. Последнее означает, что без ограничения общности можно считать $\varepsilon = 1$, иными словами,

$$1 + iy = (u + iv)^p. \tag{2}$$

Таким образом, $x^p = (1+iy)(1-iy) = (u^2+v^2)^p$ и, значит, $x = u^2 + v^2$. Поскольку x нечетно, числа u, v имеют разную четность:

$$u \not\equiv v \pmod 2. \tag{3}$$

Раскрывая правую часть (2) с помощью бинома Ньютона и сравнивая вещественные части, находим

$$1 = \sum_{k=0}^{(p-1)/2} \binom{p}{2k} (-1)^k u^{p-2k} v^{2k} = u \cdot \sum_{k=0}^{(p-1)/2} \binom{p}{2k} (-1)^k u^{p-2k-1} v^{2k}. \tag{4}$$

Последнее равенство, в частности, означает, что u – обратимый элемент кольца $\mathbb{Z}$, т.е. $u = \pm 1$. Согласно (3) отсюда следует, что v четно, так что равенство (4) при переходе к остаткам от деления на 4 принимает вид

$$1 \equiv u^p \equiv (\pm 1)^p = \pm 1 \equiv u \pmod 4,$$

что приводит к единственной возможности $u = 1$. Подставляя $u = 1$, вычитая из обеих частей равенства (4) слагаемое, отвечающее $k = 0$ (и равное 1), и деля на v^2, находим

$$0 = \sum_{k=1}^{(p-1)/2} \binom{p}{2k} (-1)^k v^{2k-2} = -\frac{p(p-1)}{2} + \sum_{k=2}^{(p-1)/2} \binom{p}{2k} (-1)^k v^{2k-2} \tag{5}$$
$$= -\frac{p(p-1)}{2} + \sum_{k=2}^{(p-1)/2} \frac{p(p-1)}{2k(2k-1)} \binom{p-2}{2k-2} (-1)^k v^{2k-2}$$

Для $k = 2, 3, \ldots, (p-1)/2$ имеем

$$\operatorname{ord}_2 \left(\binom{p}{2k} (-1)^k v^{2k-2} \right) = \operatorname{ord}_2 \left(\frac{p(p-1)}{2k(2k-1)} \right) + \operatorname{ord}_2 \binom{p-2}{2k-2} + \operatorname{ord}_2 v^{2k-2}$$
$$\geqslant \operatorname{ord}_2 \left(\frac{p(p-1)}{2} \right) - \operatorname{ord}_2 k + 0 + (2k-2), \tag{6}$$

так как число v четно и 2 входит в неотрицательной степени в *целое* число $\binom{p-2}{2k-2}$. Несложный подсчет показывает, что $\operatorname{ord}_2 k \leqslant \log_2 k \leqslant 2k-3 < 2k-2$ для $k \geqslant 2$, так что оценка (6) может быть продолжена следующим образом:

$$\operatorname{ord}_2 \left(\binom{p}{2k} (-1)^k v^{2k-2} \right) > \operatorname{ord}_2 \left(\frac{p(p-1)}{2} \right)$$

для $k = 2, 3, \ldots, (p-1)/2$, что противоречит равенству (5). Теорема доказана полностью.

Случай $p = 2$ и $q = 3$ полностью разобран Эйлером. Случай $p = 2$ и $q > 3$ делается совершенно по-другому!

Теорема 2 (Эйлер). *Уравнение $x^2 - y^3 = 1$ имеет единственное решение $x = 3$, $y = 2$ в целых числах $x, y > 1$.*

Доказательство. 1) Если x четно, то $(x-1)(x+1) = y^3$ нечетно и $d = (x-1, x+1)$ делит $(x+1) - (x-1) = 2$, откуда $d = 1$. Таким образом, $x - 1 = a^3$, $x + 1 = b^3$, при этом оба числа $b > a$ нечетны, т.е. $b \geqslant a + 2$. Окончательно,

$$2 = (x+1) - (x-1) = b^3 - a^3 \geqslant (a+2)^3 - a^3 > 8,$$

что невозможно.

Замечание. Те же рассуждения показывают, что и в случае $x^2 - y^q = 1, q > 1$, число x не может быть четным.

2) Пусть $x = 2k + 1$, где $k > 1$ (при $k = 1$ без труда находим единственное решение $x = 3, y = 2$). Тогда $y = 2n$ и исходное уравнение $x^2 - y^3 = 1$ может быть записано (после деления обеих частей на 8) в виде

$$\frac{k(k+1)}{2} = n^3. \tag{7}$$

(Слева записано *треугольное* число, а справа – куб, так что по-существу Эйлер разобрался не только с уравнением $x^2 - y^3 = 1$.) Теперь мы также различаем два варианта в зависимости от четности k.

2.1) Если $k = 2m$, $m \geqslant 1$, то уравнение (7) принимает вид $m(2m+1) = n^3$, откуда $m = v^3$ и $2m+1 = u^3$, причем $(u, v) = 1$, так что $2v^3 + 1 = 2m + 1 = u^3$.

2.2) Если $k = 2m - 1$, $m > 1$, то уравнение (7) принимает вид $(2m-1)m = n^3$, откуда $m = v^3$ и $2m - 1 = u^3$, причем $(u, v) = 1$, так что $2v^3 - 1 = 2m - 1 = u^3$.

В обоих случаях мы получили уравнение

$$u^3 \pm 1 = 2v^3, \qquad (u, v) = 1, \quad u \geqslant 2, \ v \geqslant 1,$$

отсутствие решений у которого гарантируется следующим результатом.

Теорема 3 (Лагранж). *Уравнение $x^3 + y^3 = 2z^3$ не имеет решений в целых числах за исключением тривиальных наборов $x = y = z$ и $x = -y$, $z = 0$.*

В дальнейшем мы будем доказывать неразрешимость более общего уравнения над кольцом, содержащим $\mathbb{Z}$.

Обозначим через ρ корень третьей степени из единицы с положительной мнимой частью:

$$\rho = \frac{-1 + \sqrt{-3}}{2}, \qquad \rho^3 = 1, \quad \rho^2 + \rho + 1 = 0,$$

и рассмотрим поле $K = \mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$. Комплексное сопряжение обозначим штрихом, так что для $\alpha = a + b\rho$ имеем $\alpha' = a + b\rho^2$ и $\mathbf{N}(\alpha) = \alpha\alpha' = a^2 - ab + b^2 > 0$ для $\alpha \neq 0$. Кольцо целых над K представимо в виде $\mathbb{Z}_K = \mathbb{Z} + \mathbb{Z}\rho$, множество единиц (обратимых элементов) в нем $E(\mathbb{Z}_K) = \{\pm 1, \pm\rho, \pm\rho^2\} = \langle -\rho \rangle$ (т.е. $E(\mathbb{Z}_K)$ есть циклическая группа порядка 6, порожденная элементом $-\rho$). Два элемента кольца будем называть *ассоциированными*, если их отношение есть единица кольца; для записи будем использовать знак $\sim$. Отметим, что $\mathbb{Z}_K$ – кольцо с однозначным разложением на простые, причем (как и в случае кольца гауссовых чисел $\mathbb{Z}[i]$) все простые в $\mathbb{Z}_K$ имеют несложное описание:

а) $\varepsilon\sqrt{-3}$;

б) εp, где $p \equiv 2 \pmod 3$ – простое число в $\mathbb{Z}$;

в) $\varepsilon(x + y\sqrt{-3})$, где $x, y \in \mathbb{Z}$ и $\mathbf{N}(x + y\sqrt{-3}) = x^2 + 3y^2 = p \equiv 1 \pmod 3$ – простое число в $\mathbb{Z}$

(всюду ε – произвольный элемент $E(\mathbb{Z}_K)$). Нам понадобится только часть этой информации.

Лемма 1. *Число $1 - \rho \sim \sqrt{-3}$ простое в $\mathbb{Z}_K$; кроме того, $\pm(1-\rho) \sim \sqrt{-3}$ и $\pm(2+\rho) \sim \sqrt{-3}$.*

Ассоциированность следует из следующих соотношений:

$$\rho(1 - \rho) = \rho - \rho^2 = 2\rho + 1 = \sqrt{-3},$$
$$\rho(2 + \rho) = 2\rho + \rho^2 = 2\rho - \rho - 1 = -(1 - \rho).$$

Лемма 2. *Число* 2 *простое в* $\mathbb{Z}_K$.

Лемма 3. *Для любого* $\tau \in \mathbb{Z}_K$ *взаимно простого с* 2 *выполнено* $\tau^3 \equiv 1 \pmod 2$.

Доказательство. Действительно, все ненулевые остатки в $\mathbb{Z}_K$ при делении на 2 исчерпываются набором $1, \rho, \rho^2$. Поэтому $\tau^3 \equiv 1, \rho^3, \rho^6 = 1 \pmod 2$.

Как несложно заметить, теорема 3 является частным случаем следующего утверждения.

Теорема 3′. *Уравнение*

$$\xi^3 + \eta^3 + 2\varepsilon\zeta^3 = 0, \qquad \xi, \eta, \zeta \in \mathbb{Z}_K, \quad \varepsilon \in E(\mathbb{Z}_K), \quad (\xi, \eta, \zeta) = 1, \tag{8}$$

неразрешимо в $\xi, \eta, \zeta, \varepsilon$ *с* $\mathbf{N}(\xi\eta\zeta) > 1$.

Доказательство. Доказательство проводится методом спуска, придуманным Ферма для доказательства неразрешимости в целых числах уравнения $x^4 + y^4 = z^4$.

Предположим от противного, что существуют решения уравнения (8) с условием $\mathbf{N}(\xi\eta\zeta) > 1$ и выберем из этого множества решений одно с минимально возможной *высотой* $\mathbf{N}(\xi\eta\zeta)$. Сразу отметим, что условие $(\xi, \eta, \zeta) = 1$ ввиду однородности уравнения (8) и однозначности разложения на простые в $\mathbb{Z}_K$ можно записать в виде

$$(\xi, \eta) = (\xi, \zeta) = (\eta, \zeta) = 1. \tag{9}$$

Представим исходное уравнение в виде

$$-2\varepsilon\zeta^3 = \xi^3 + \eta^3 = (\xi + \eta)(\xi + \rho\eta)(\xi + \rho^2\eta) = (\xi + \eta)(\rho\xi + \rho^2\eta)(\rho^2\xi + \rho\eta) \tag{10}$$

и обозначим входящие в последнее произведение множители через α, β, γ. Согласно (10) по крайней мере один из этих множителей делится на 2; обозначим его через γ. Таким образом,

$$\{\alpha, \beta, \gamma\} = \{\xi + \eta, \rho\xi + \rho^2\eta, \rho^2\xi + \rho\eta\}, \qquad 2 \mid \gamma. \tag{11}$$

Несложная проверка показывает, что кроме равенства

$$\alpha\beta\gamma = -2\varepsilon\zeta^3, \tag{12}$$

вытекающего из (10), имеет место равенство

$$\alpha + \beta + \gamma = 0. \tag{13}$$

Докажем, что числа α, β на 2 не делятся. Если хотя бы одно из них делится на 2, то ввиду $\gamma \mid 2$ и (13) то же самое выполнено и для другого из них, так что каждое из чисел в (11) кратно 2 и этим свойством обладают также числа

$$\rho \cdot (\xi + \eta) - (\rho\xi + \rho^2\eta) = \rho(1 - \rho)\eta, \tag{14}$$

$$\rho^2 \cdot (\xi + \eta) - (\rho\xi + \rho^2\eta) = -\rho(1 - \rho)\xi \tag{15}$$

(ρ, ρ^2 – единицы кольца $\mathbb{Z}_K$). Таким образом, 2 делит числа $(1-\rho)\eta$ и $(1-\rho)\zeta$ и, значит, делит числа η, ζ по лемме 1. Последнее означает, что $(\eta, \zeta) \geqslant 2$, что невозможно согласно (9). Таким образом, число γ и только оно в наборе (11) делится на 2 в $\mathbb{Z}_K$.

Обозначим через $\delta \geqslant 1$ наибольший общий делитель чисел α, β; согласно только что доказанному число δ нечетно и согласно (13) и однозначности разложения на простые в $\mathbb{Z}_K$ выполнено

$$\delta = (\alpha, \beta) = (\alpha, \gamma) = (\beta, \gamma),$$

т.е. числа $\alpha/\delta, \beta/\delta, \gamma/\delta \in \mathbb{Z}_K$ попарно взаимно просты. Перепишем равенства (12) и (13) в виде

$$\frac{\alpha}{\delta} \cdot \frac{\beta}{\delta} \cdot \frac{\gamma}{\delta} = -2\varepsilon \left(\frac{\zeta}{\delta}\right)^3,$$
$$\frac{\alpha}{\delta} + \frac{\beta}{\delta} + \frac{\gamma}{\delta} = 0, \tag{16}$$

откуда

$$\frac{\alpha}{\delta} = \varepsilon_0 \xi_1^3, \quad \frac{\beta}{\delta} = \varepsilon_1 \eta_1^3, \quad \frac{\gamma}{2\delta} = \varepsilon_2 \zeta_1^3, \qquad \frac{\zeta}{\delta} = \xi_1 \eta_1 \zeta_1. \tag{17}$$

где ξ_1, η_1, ζ_1 попарно взаимно просты. Согласно (16) имеем $\varepsilon_0 \xi_1^3 + \varepsilon_1 \eta_1^3 + 2\varepsilon_2 \zeta_1^3 = 0$, т.е.

$$\xi_1^3 + \varepsilon_1' \eta_1^3 + 2\varepsilon_2' \zeta_1^3 = 0, \qquad \varepsilon_1' = \frac{\varepsilon_1}{\varepsilon_0}, \quad \varepsilon_2' = \frac{\varepsilon_2}{\varepsilon_0}. \tag{18}$$

Поскольку числа $\alpha/\delta, \beta/\delta$, а значит, и числа ξ_1, η_1, не делятся на 2, мы заключаем, что $\xi_1^3 \equiv 1 \pmod 2$ и $\eta_1^3 \equiv 1 \pmod 2$ согласно лемме 3. Подставляя эти сравнения в (18), получаем $\varepsilon_1' \equiv 1 \pmod 2$ или $\varepsilon_1' = \pm 1$, так как ε_1' – единица кольца $\mathbb{Z}_K$. Таким образом, уравнение (18) может быть записано в виде

$$\xi_1^3 + (\pm\eta_1)^3 + 2\varepsilon_2' \zeta_1^3 = 0.$$

Для получения противоречия осталось показать, что

$$1 < \mathbf{N}(\xi_1 \eta_1 \zeta_1) < \mathbf{N}(\xi \eta \zeta). \tag{19}$$

Отметим, что согласно (17) выполнено $\mathbf{N}(\xi_1 \eta_1 \zeta_1) = \mathbf{N}(\zeta/\delta)$.

Замечание. Для доказательства неравенства (19) мы приводим два способа – стандартный (недлинный) и элегантный (чуть длиннее, но классический).

Стандартный способ. Если $\mathbf{N}(\xi_1 \eta_1 \zeta_1) = \mathbf{N}(\zeta/\delta) = 1$, то ξ_1, η_1, ζ_1 – единицы кольца $\mathbb{Z}_K$ и $\xi_1^3, \eta_1^3, \zeta_1^3 \in \{\pm 1\}$. В частности, согласно (17) и тому, что $\varepsilon_1' = \varepsilon_1/\varepsilon_0 = \pm 1$, выполнено

$$\frac{\alpha}{\delta} = \pm\varepsilon_0 = \pm\frac{\beta}{\delta}.$$

Равенство $\alpha/\delta = -\beta/\delta$ невозможно, так как в подобном случае из (16) получим $\gamma = 0$, что противоречит (12). Поэтому в соответствии с (16)

$$\frac{\alpha}{\delta} = \varepsilon^*, \quad \frac{\beta}{\delta} = \varepsilon^*, \quad \frac{\gamma}{\delta} = -2\varepsilon^*, \qquad \text{где } \varepsilon^* \in E(\mathbb{Z}_K). \tag{20}$$

Подставляя эти соотношения в (14) с учетом (11), находим, что либо

$$\rho \cdot \varepsilon^*\delta - \varepsilon^*\delta = (\rho - 1) \cdot \varepsilon^*\delta,$$

либо

$$\rho \cdot \varepsilon^*\delta - (-2\varepsilon^*\delta) = (\rho + 2) \cdot \varepsilon^*\delta,$$

либо

$$\rho \cdot (-2\varepsilon^*\delta) - \varepsilon^*\delta = -(2\rho + 1) \cdot \varepsilon^*\delta$$

совпадает с $\rho(1-\rho)\eta$. Согласно лемме 1 это означает, что $\delta \sim \eta$. Аналогичная подстановка соотношений (20) в (15) с помощью леммы 1 приводит к ассоциированности $\delta \sim \xi$. Поскольку $(\xi, \eta) = 1$, мы окончательно получаем, что δ, а значит, и ξ, η являются единицами $\mathbb{Z}_K$.

Если $\mathbf{N}(\xi_1\eta_1\zeta_1) = \mathbf{N}(\zeta/\delta) \geqslant \mathbf{N}(\xi\eta\zeta)$, то $\mathbf{N}(\xi\eta\delta) \leqslant 1$ в виду мультипликативности нормы, так что ξ, η являются единицами $\mathbb{Z}_K$.

Итак, в обоих случаях $\mathbf{N}(\xi_1\eta_1\zeta_1) = 1$ и $\mathbf{N}(\xi_1\eta_1\zeta_1) \geqslant \mathbf{N}(\xi\eta\zeta)$ мы получили, что ξ, η – единицы в $\mathbb{Z}_K$. Следовательно, $\xi^3, \eta^3 \in \{\pm 1\}$, откуда $\xi^3 = \eta^3 = \pm 1$ (в противном случае $\zeta = 0$ в соответствии с (8), что невозможно, так как $\mathbf{N}(\xi\eta\zeta) \neq 0$). Таким образом, $\pm 2 = \xi^3 + \eta^3 = -2\varepsilon\zeta^3$, т.е. ζ^3 и, значит, ζ – единицы кольца $\mathbb{Z}_K$. Таким образом, $\mathbf{N}(\xi\eta\zeta) = \mathbf{N}(\xi)\mathbf{N}(\eta)\mathbf{N}(\zeta) = 1 \cdot 1 \cdot 1 = 1$, что противоречит предположению $\mathbf{N}(\xi\eta\zeta) > 1$. Тем самым, неравенство (19) и, как следствие, теорема доказаны.

Элегантный способ. Здесь нам потребуется еще одно вспомогательное утверждение о свойствах простого числа $\lambda = 1 - \rho \in \mathbb{Z}_K$.

Лемма. *Для любого $\alpha \in \mathbb{Z}_K$, не делящегося на простое $\lambda = 1 - \rho$, справедливо сравнение*

$$\alpha^3 \equiv \pm 1 \pmod{\lambda^4}.$$

Доказательство. Напомним, что $\mathbb{Z}_K = \mathbb{Z} + \rho\mathbb{Z}$. Согласно определению числа λ выполнено $\rho = 1 - \lambda \equiv 1 \pmod{\lambda}$ и, как следствие, $\rho^2 \equiv 1 \pmod{\lambda}$; кроме того, $\lambda \sim \sqrt{-3} \mid 3$ (именно, $-\rho^2\lambda^2 = 3$), так что в кольце $\mathbb{Z}_K$ существует в точности три класса вычетов по модулю λ, именно 0, 1 и -1 (проверка того, что $0 \not\equiv \pm 1$ и $1 \not\equiv -1$, тривиальна).

Итак, α не делится на λ, т.е. $\alpha \equiv \pm 1 \pmod{\lambda}$ или $\alpha = \pm 1 + \lambda\beta$, где $\beta \in \mathbb{Z}_K$. Следовательно, по модулю λ^4 имеем

$$\begin{aligned} \alpha^3 &= \pm 1 + 3\lambda\beta \pm 3\lambda^2\beta^2 + \lambda^3\beta^3 = \pm 1 - \rho^2\lambda^3\beta \mp \rho^2\lambda^4\beta^2 + \lambda^3\beta^3 \\ &\equiv \pm 1 - \rho^2\lambda^3\beta + \lambda^3\beta^3 = \pm 1 + \lambda^3(\beta^3 - \rho^2\beta), \end{aligned} \tag{21}$$

где мы вновь воспользовались тем, что $3 = -\rho^2\lambda^2$. Как было отмечено выше, $\rho^2 \equiv 1 \pmod{\lambda}$ и, значит,

$$\beta^3 - \rho^2\beta \equiv \beta^3 - \beta = \beta(\beta-1)(\beta+1) \equiv 0 \pmod{\lambda}.$$

Поэтому, продолжая цепочку сравнений (21), находим требуемое:

$$\alpha^3 \equiv \pm 1 + \lambda^3(\beta^3 - \rho^2\beta) \equiv \pm 1 + \lambda^3 \cdot \lambda \equiv \pm 1 \pmod{\lambda^4}.$$

Лемма доказана.

Вернемся к доказательству неравенства (19). Если $\mathbf{N}(\xi_1\eta_1\zeta_1) = \mathbf{N}(\zeta/\delta) = 1$, то ξ_1, η_1, ζ_1 – единицы кольца $\mathbb{Z}_K$ и $\zeta \sim \delta$. По определению δ является наибольшим общим делителем чисел в наборе (11) и согласно (14), (15) число δ делит как $\lambda\eta$, так и $\lambda\xi$. Последнее (ввиду взаимной простоты η и ξ) возможно только в двух случаях: $\delta \sim \lambda$ и $\delta \sim 1$. Рассмотрим каждый из них по отдельности.

Пусть $\delta \sim \lambda = 1 - \rho$. Поскольку $\zeta \sim \delta$, имеем $\zeta \sim \lambda$; в частности, λ делит ζ, т.е.

$$\xi^3 + \eta^3 = -2\varepsilon\zeta^3 \equiv 0 \pmod{\lambda^3}. \tag{22}$$

С другой стороны, $\lambda \nmid \xi$ и $\lambda \nmid \eta$ ввиду попарной взаимной простоты чисел ξ, η, ζ. Согласно лемме заключаем, что $\xi^3 \equiv \pm 1 \pmod{\lambda^4}$ и $\eta^3 \equiv \pm 1 \pmod{\lambda^4}$, а это дает возможность уточнить сравнения (22):

$$\xi^3 + \eta^3 \equiv 0 \pmod{\lambda^4}.$$

Последнее означает, что $-2\varepsilon\zeta^3 = \xi^3 + \eta^3$ делится на λ^4, что невозможно, так как

$$\mathbf{N}(\lambda^4) = 3^4 > 3^3 = \mathbf{N}(\lambda)^3 = \mathbf{N}(\zeta)^3 = \mathbf{N}(-2\varepsilon\zeta^3).$$

Полученное противоречие показывает, что случай $\delta \sim \lambda$ невозможен.

Пусть теперь $\delta \sim 1$, откуда также $\zeta \sim \delta \sim 1$, т.е. $\zeta \in E(\mathbb{Z}_K)$. Кроме того, $\xi_1\eta_1\zeta_1 = \zeta/\delta \sim 1$, так что $\xi_1, \eta_1, \zeta_1 \in E(\mathbb{Z}_K)$ и, как следствие, $\alpha \sim \alpha/\delta$, $\beta \sim \beta/\delta$ и $\gamma/2 \sim \gamma/(2\delta)$ также являются единицами. Поэтому из (14) и (15) вытекает, что каждое из чисел $\lambda\xi$ и $\lambda\eta$ является суммой двух единиц или суммой единицы и удвоенной единицы; непосредственная проверка (подобная проделанной выше в стандартном способе) показывает, что числа $\lambda\xi$ и $\lambda\eta$ имеют вид $\lambda \cdot \varepsilon$, где $\varepsilon \in E(\mathbb{Z}_K)$. Таким образом, $\xi, \eta \in E(\mathbb{Z}_K)$ и с учетом полученного включения $\zeta \in E(\mathbb{Z}_K)$ окончательно находим, что $\mathbf{N}(\xi\eta\zeta) = 1$. Последнее равенство противоречит выбору решения ξ, η, ζ уравнения (8).

Наконец, рассмотрение случая $\mathbf{N}(\xi_1\eta_1\zeta_1) \geqslant \mathbf{N}(\xi\eta\zeta)$ проводится так же, как и выше в стандартном способе. Это завершает доказательство теоремы $3'$.

Теорема 4 (Касселс, 1960). *Пусть p, q – простые числа, $p > q \geqslant 3$, и*

$$x^p - y^q = 1, \qquad x, y \in \mathbb{Z}, \quad |x| > 1, \ |y| > 1.$$

Тогда $p \mid y$ и $q \mid x$.

Замечание. Уравнения $x^p - y^q = 1$ и $(-y)^q - (-x)^p = 1$ равносильны, так что условие $p > q \geqslant 3$ не является ограничительным.

Лемма 4 (стара как Эйлер!). *Пусть q – нечетное простое число, $c \in \mathbb{Z} \setminus \{0, \pm 1\}$.*

1) *Наибольший общий делитель чисел $c-1$ и $(c^q-1)/(c-1)$ равен 1 или q.*

2) *Если $q \mid (c-1)$, то*

$$\frac{c^q - 1}{c-1} \equiv q \pmod{q(c-1)}.$$

Замечание. Во втором утверждении леммы равенство $(c^q - 1)/(c - 1) = q$ аозможно в одном единственном случае: $q = 3, c = -2$.

Доказательство. 1) Поскольку

$$\frac{c^q - 1}{c-1} = c^{q-1} + c^{q-2} + \cdots + c + 1 \equiv \underbrace{1 + 1 + \cdots + 1 + 1}_{q \text{ раз}} \equiv q \pmod{(c-1)},$$

заключаем, что

$$\left(\frac{c^q - 1}{c-1}, c - 1\right) = (q, c-1) \in \{1, q\}$$

ввиду простоты числа q.

2) Пусть $q \mid (c-1)$. Тогда

$$c^q - 1 = \big((c-1)+1\big)^q - 1 = \sum_{k=1}^{q} \binom{q}{k} (c-1)^k,$$

откуда

$$\frac{c^q - 1}{c-1} = \sum_{k=1}^{q} \binom{q}{k} (c-1)^{k-1} = q + \sum_{k=2}^{q} \binom{q}{k} (c-1)^{k-1} \equiv q \pmod{q(c-1)} \quad (23)$$

(действительно, при $k = 2, \ldots, q-1$ каждый биномиальный коэффициент делится на q и $(c-1)^{k-1}$ делится на $c-1$; при $k = q$ получаем, что $(c-1)^{q-1}$ делится на $(c-1)^2$, которое, в свою очередь, делится на $q(c-1)$).

Осталось разобраться с невозможностью равенства $(c^q - 1)/(c - 1) = q$. Последнее согласно (23) означает, что

$$0 = \sum_{k=2}^{q} \binom{q}{k} (c-1)^{k-2} = \frac{q(q-1)}{2} + (c-1) \sum_{k=3}^{q} \binom{q}{k} (c-1)^{k-3}. \quad (24)$$

Если простое число $q > 3$, то каждое слагаемое в последней сумме делится на q^2 (поскольку $c - 1$ делится на q), в то время как $q(q-1)/2$ делится на q, но не делится на q^2. Поэтому в случае $q > 3$ равенство (24) невозможно. Если $q = 3$, то равенство (24) перепишется в виде

$$0 = \frac{3 \cdot 2}{2} + (c-1) = c + 2,$$

т.е. мы получаем единственный исключительный случай $q = 3, c = -2$.

Лемма доказана полностью.

Лемма 5. *Пусть $\alpha > 1$ и $t > 0$ – произвольные вещественные числа. Тогда* $(1+t)^\alpha > 1 + t^\alpha$.

Доказательство слишком элементарно, чтобы его приводить.

Следствие 1. *Пусть $q \geqslant 3$ – нечетное целое. Тогда при $t > 0$ и $t < -1$ имеет место неравенство* $(1+t)^q > 1 + t^q$.

Доказательство. В случае $t > 0$ утверждение следует непосредственно из леммы 5 при $\alpha = q$. В случае $t < -1$ полагаем $\alpha = q$, $z = -t - 1 > 0$ и также применяем лемму 5.

Следствие 2. *Пусть p, q – нечетные целые, $p > q \geqslant 3$. Тогда при $w > 1$ и $w < 0$ имеет место неравенство*

$$(w^p - 1)^q > (w^q - 1)^p. \tag{25}$$

Доказательство. Если $w > 1$, то согласно лемме 5 с $\alpha = p/q > 1$ и $t = w^q - 1$ получаем $w^p > 1 + (w^q - 1)^{p/q}$, что после элементарных преобразований приводит к (25).

Если $w < 0$, то полагаем $\alpha = p/q$, $t = |w|^q$ и вновь воспользуемся леммой 5. Тогда $(1 + |w|^q)^{p/q} > 1 + |w|^p$ или, что то же самое, $(1 - w^q)^p > (1 - w^p)^q$, откуда следует (25). Лемма доказана.

Лемма 6. *В условиях теоремы 4 имеет место делимость $q \mid (y+1)$.*

Доказательство. Пусть от противного $q \nmid (y+1)$. Поскольку

$$x^p = y^q + 1 = (y+1) \cdot \frac{y^q + 1}{y+1},$$

в соответствии с леммой 4 (при $c = -y$) числа $y+1$ и $(y^q+1)/(y+1)$ взаимно просты. Следовательно, каждое из этих чисел является p-й степенью целого числа, так что $y + 1 = w^p$, причем $w \notin \{0, 1\}$ ввиду $x \neq 0$ и $y \in \mathbb{Z}$. Поэтому применение следствия 1 с $t = w^p - 1$ дает

$$x^p = y^q + 1 = (w^p - 1)^q + 1 < w^{pq},$$

откуда $x < w^q$, и в то же времяв соответствии со следствием 2

$$x^p = y^q + 1 > y^q = (w^p - 1)^q > (w^q - 1)^p,$$

откуда $x > w^q - 1$. Оценки $w^q - 1 < x < w^q$ ввиду целочисленности x и w^q противоречивы, что означает невозможность соотношения $q \nmid (y+1)$. Лемма доказана.

Лемма 7. *Пусть $k \in \mathbb{N}$ и*

$$\Delta(t) = \frac{t(t-1)\cdots(t-k+1)}{k!}$$

– (так называемый целозначный) многочлен. Тогда для любой дроби $p/q \in \mathbb{Z}$, где число q простое, имеет место включение

$$q^{k + \left[\frac{k}{q-1}\right]} \cdot \Delta\left(\frac{p}{q}\right) \in \mathbb{Z}.$$

Доказательство. Фактически исследование арифметических свойств целозначных многочленов и их производных положено в работах Зигеля. Положим

$$A = q^{k+\left[\frac{k}{q-1}\right]} \cdot \Delta\left(\frac{p}{q}\right) = q^{\left[\frac{k}{q-1}\right]} \cdot \frac{p(p-q)(p-2q)\cdots(p-(k-1)q)}{k!}.$$

Тогда для простых $l \neq q$ выполнено

$$\operatorname{ord}_l\big(p(p-q)(p-2q)\cdots(p-(k-1)q)\big) > \operatorname{ord}_l k!,$$

откуда $\operatorname{ord}_l A \geqslant 0$, в то время как

$$\operatorname{ord}_q A = \left[\frac{k}{q-1}\right] - \operatorname{ord}_q k! \geqslant 0,$$

поскольку

$$\operatorname{ord}_q k! = \left[\frac{k}{q}\right] + \left[\frac{k}{q^2}\right] + \left[\frac{k}{q^3}\right] + \cdots \leqslant \frac{k}{q} + \frac{k}{q^2} + \frac{k}{q^3} + \cdots = \frac{k}{q-1}$$

и это число является целым (т.е. равно своей целой части). Тем самым, $\operatorname{ord}_l A \geqslant 0$ для любого простого l, что и доказывает лемму.

Доказательство теоремы 4. Делимость $q \mid x$ следует из леммы 6. Это, в свою очередь, влечет

$$q^p \mid x^p = y^q + 1 = (y+1) \cdot \frac{y^q+1}{y+1}. \tag{26}$$

В то же время согласно второму утверждению леммы 4

$$\frac{y^q+1}{y+1} \equiv q \pmod{q(y+1)}, \tag{27}$$

откуда

$$\frac{y^q+1}{y+1} \equiv q \pmod{q^2}$$

и, значит, $(y^q+1)/(y+1)$ делится на q, но не делится на q^2. Таким образом, из (26) заключаем, что

$$y+1 = q^{p-1}u^p, \quad \frac{y^q+1}{y+1} = qv^p, \quad x = quv, \qquad (qu, v) = 1, \ v \neq 1.$$

Неравенство $v \neq 1$ вытекает из замечания к лемме 4, так как единственная исключительная пара $q = 3$, $y = 2$ возможно лишь в случае $p = 2$, $x = 3$, но $p > q$ по условию теоремы.

Подставляя равенство $y + 1 = q^{p-1}u^p$ в (27), получаем

$$qv^p = \frac{y^q+1}{y+1} \equiv q \pmod{q^p},$$

откуда

$$v^p \equiv 1 \pmod{q^{p-1}}. \tag{28}$$

С другой стороны, согласно теореме Эйлера (обобщающей малую теорему Ферма)

$$v^{\varphi(q^{p-1})} \equiv 1 \pmod{q^{p-1}}, \tag{29}$$

где $\varphi(q^{p-1}) = q^{p-2}(q-1)$ взаимно просто с p, так что сравнения (28) и (29) приводят к сравнению

$$v = v^{(p,\varphi(q^{p-1}))} \equiv 1 \pmod{q^{p-1}}.$$

Поскольку $v \neq 1$, последнее сравнение влечет оценку $|v-1| \geqslant q^{p-1}$ и, значит, $|v| \geqslant q^{p-1} - 1$. Это, в свою очередь, означает, что

$$|x| = q|uv| \geqslant q|v| \geqslant q^p - q. \tag{30}$$

Отметив выше некоторые следствия из доказанной делимости $q \mid x$, перейдем к доказательству "трудной половины теоремы" – делимости $p \mid y$. Предположим, что это не так, значит $p \nmid (x-1)$ и с учетом

$$y^q = x^p - 1 = (x-1) \cdot \frac{x^p - 1}{x-1},$$

а также леммы 4 получаем $x - 1 = z^q$ для некоторого целого z.

Полагая $\lambda = x^{p/q}$, перепишем исходное уравнение $x^p - y^q = 1$ в виде $\lambda^q - y^q = 1$, откуда (числа λ, x, y имеют одинаковые знаки)

$$\begin{aligned} |x^{p/q} - y| = |\lambda - y| &= \frac{1}{|\lambda^{q-1} + \lambda^{q-2}y + \cdots + \lambda y^{q-2} + y^{q-1}|} \\ &= \frac{1}{|\lambda|^{q-1} + |\lambda|^{q-2}|y| + \cdots + |\lambda|\,|y|^{q-2} + |y|^{q-1}} \\ &\leqslant \frac{1}{q \cdot (\min\{|\lambda|, |y|\})^{q-1}} = \frac{1}{q \cdot (\min\{|\lambda|^q, |y|^q\})^{(q-1)/q}} \\ &= \frac{1}{q \cdot (\min\{|x|^p, |y|^q\})^{(q-1)/q}}. \end{aligned} \tag{31}$$

Воспользуемся этими неравенствами, чтобы оценить $|x^{p/q} - y|$ в терминах z, определенной выше равенством $x = z^q + 1$. Согласно (30) выполнено

$$|z|^q = |x-1| \geqslant |x| - 1 \geqslant q^p - q - 1 \geqslant \frac{1}{2}q^p. \tag{32}$$

Далее, в случае $x > 0$ имеем $z > 0$ и $y > 0$, откуда

$$x^p > y^q = x^p - 1 = (1 + z^q)^p - 1 \geqslant z^{pq}$$

(последнее согласно лемме 5); если же $x < 0$, то $z < 0$ и $|x| = |z^q + 1| = |z|^q - 1$, откуда

$$|y|^q = |x^p - 1| = |x|^p + 1 > |x|^p = (|z|^q - 1)^p.$$

Таким образом, оценка

$$\min\{|x|^p, |y|^q\} \geqslant (|z|^q - 1)^p = |z|^{qp}(1 - |z|^{-q})^p \tag{33}$$

справедлива как для $x > 0$, так и для $x < 0$. Воспользуемся теперь оценкой (32) и неравенством Бернулли:

$$(1 - |z|^{-q})^p \geqslant (1 - 2q^{-p})^p \geqslant 1 - 2pq^{-p} \geqslant 1 - 2 \cdot 4 \cdot 2^{-p} = 1 - 2^{-p+3} \geqslant \frac{1}{2},$$

поэтому оценка (33) может быть записана следующим образом:

$$\min\{|x|^p, |y|^q\} \geqslant \frac{1}{2}|z|^{qp} \geqslant \frac{1}{q}|z|^{qp}.$$

Наконец, подставляя полученное неравенство в (31), заключаем, что

$$|x^{p/q} - y| \leqslant \frac{1}{q \cdot q^{-(q-1)/q}|z|^{p(q-1)}} = \frac{1}{q^{1/q}|z|^{p(q-1)}} \leqslant |z|^{-p(q-1)}. \tag{34}$$

Далее мы воспользуемся так называемым методом Рунге. Пользуясь формулой Тейлора, запишем

$$x^{p/q} = (z^q + 1)^{p/q} = z^p(1 + z^{-q})^{p/q} = \sum_{n=0}^{\infty} T_n, \tag{35}$$

где

$$T_n = \frac{(p/q)(p/q - 1)\cdots(p/q - n + 1)}{n!} z^{p-nq}.$$

Обозначим $N = [p/q] + 1$ и $\rho = [N/(q-1)]$. Тогда

$$z^{Nq-p} \cdot z^{p-nq} = z^{(N-n)q} \in \mathbb{Z} \qquad \text{для всех } n,\ 0 \leqslant n \leqslant N,$$

и

$$q^{N+\rho} \cdot \frac{(p/q)(p/q - 1)\cdots(p/q - n + 1)}{n!} \in \mathbb{Z} \qquad \text{для всех } n \geqslant 0$$

согласно лемме 7. Следовательно,

$$I = z^{Nq-p}q^{N+\rho} \cdot \left(y - \sum_{n=0}^{N} T_n\right) \in \mathbb{Z}. \tag{36}$$

Используя (35), это целое число можно представить и по-другому:

$$I = z^{Nq-p}q^{N+\rho} \cdot \left((y - x^{p/q}) + \sum_{n=N+1}^{\infty} T_n\right) = I_1 + I_2 + I_3,$$

где

$$I_1 = z^{Nq-p}q^{N+\rho}(y - x^{p/q}),$$

$$I_2 = z^{Nq-p}q^{N+\rho}T_{N+1}, \qquad I_3 = z^{Nq-p}q^{N+\rho}\sum_{n=N+2}^{\infty} T_n.$$

Оценив величин I_1, I_2, I_3, мы докажем, что $0 < |I| < 1$, и это будет противоречить включению (36).

Для $n \geqslant N+1 > p/q$ имеем

$$\frac{|T_{n+1}|}{|T_n|} = |z|^{-q} \cdot \frac{|p/q - n|}{n+1} = |z|^{-q} \cdot \frac{n - p/q}{n+1} < |z|^{-q} \leqslant 2q^{-p} \leqslant 2 \cdot 3^{-5} < 2^{-4},$$

где мы воспользовались оценкой (32). Поэтому

$$|I_3| \leqslant |z|^{Nq-p}q^{N+\rho} \cdot |T_{N+1}| \sum_{k=1}^{\infty}(2^{-4})^k = |I_2| \cdot \sum_{k=1}^{\infty} 2^{-4k} = |I_2| \cdot \frac{2^{-4}}{1-2^{-4}} = \frac{1}{15}|I_2|. \tag{37}$$

Согласно определению числа N получаем

$$\left|\frac{p}{q}\left(\frac{p}{q}-1\right)\cdots\left(\frac{p}{q}-N\right)\right| \leqslant N(N-1)\cdots 2 \cdot \left|\left(\frac{p}{q}-N+1\right)\left(\frac{p}{q}-N\right)\right| = N! \cdot \left|\left(\frac{p}{q}-N+\frac{1}{2}\right)^2 - \frac{1}{4}\right| \leqslant \frac{N!}{4}, \tag{38}$$

$$\left|\frac{p}{q}\left(\frac{p}{q}-1\right)\cdots\left(\frac{p}{q}-N\right)\right| \geqslant (N-1)(N-1)\cdots 1 \cdot \left|\frac{p}{q}-N+1\right| \cdot \left|\frac{p}{q}-N\right| \geqslant \frac{(N-1)!}{q^2} \tag{39}$$

(оценка $|p/q - k| \geqslant 1/q$ для целого k, дважды примененная в последнем неравенстве, вытекает из того, что дробь p/q как отношение двух простых чисел несократима). Применяя неравенства (34) и (39), находим

$$\frac{|I_1|}{|I_2|} = \frac{|x^{p/q} - y|}{|T_{N+1}|} \leqslant \frac{|z|^{-p(q-1)}}{|z|^{p-(N+1)q}(N-1)!/(q^2(N+1)!)} = q^2(N+1)^2|z|^{q(N+1-p)}. \tag{40}$$

Для продолжения последней оценки нам понадобится неравенство

$$N + 1 - p \leqslant -2, \tag{41}$$

для доказательства которого достаточно показать, что $N + 1 - p < -1$ (все числа целые!). Имеем

$$N+1-p = \left[\frac{p}{q}\right] + 2 - q \leqslant \frac{p}{q} + 2 - q = -1 - \frac{(p-3)(q-1)-3}{p} \leqslant -1 - \frac{2\cdot 2 - 3}{p} < -1,$$

что и требовалось.

Согласно (41) показатель $|z|$ в правой части (40) отрицателен, поэтому применима оценка (39) и мы получаем

$$\frac{|I_1|}{|I_2|} \leqslant q^2(N+1)^2|z|^{q(N+1-p)} \leqslant q^2(p-1)^2|z|^{-2q} \leqslant q^2(p-1)^2\left(\frac{1}{2}q^p\right)^{-2}$$
$$\leqslant \left(2(p-1)q^{-p+1}\right)^2 \leqslant \left(2\cdot 4\cdot 3^{-4}\right)^2 < \frac{1}{10}. \tag{42}$$

Наконец, согласно определению величины I_2 и неравенствам (38), (32) выполнено

$$|I_2| \leqslant |z|^{Nq-p}q^{N+\rho}|z|^{p-(N+1)q}\cdot\frac{N!/4}{(N+1)!} = |z|^{-q}\cdot\frac{q^{N+\rho}}{4(N+1)}$$
$$\leqslant 2q^{-p}\cdot\frac{q^{N+\rho}}{4(N+1)} = \frac{q^{N+\rho-p}}{2(N+1)}.$$

Остается отметить, что $N+1 = [p/q]+2 \geqslant 3$, так как $p > q$, и

$$N+\rho \leqslant N+\frac{N}{q-1} = N\left(1+\frac{1}{q-1}\right) \leqslant \left(\frac{p}{q}+1\right)\frac{q}{q-1} = \frac{p+q}{q-1}$$
$$= p - \frac{(p-1)(q-2)-2}{q-1} \leqslant p - \frac{4\cdot 1-2}{q-1} < p,$$

откуда

$$|I_2| \leqslant \frac{q^{N+\rho-p}}{2(N+1)} < \frac{q^0}{2\cdot 3} = \frac{1}{6}. \tag{43}$$

Собирая вместе оценки (37), (42) и (43), окончательно получаем

$$|I| \leqslant |I_1|+|I_2|+|I_3| = \left(1+\frac{|I_1|}{|I_2|}+\frac{|I_3|}{|I_2|}\right)\cdot|I_2| < \left(1+\frac{1}{10}+\frac{1}{15}\right)\cdot\frac{1}{6} = \frac{7}{36} < 1,$$
$$|I| \geqslant |I_2|-|I_1|-|I_3| = \left(1-\frac{|I_1|}{|I_2|}-\frac{|I_3|}{|I_2|}\right)\cdot|I_2| > \left(1-\frac{1}{10}-\frac{1}{15}\right)\cdot|I_2| > 0,$$

что противоречит тому, что I – целое число. Полученное противоречие завершает доказательство делимости $p \mid y$ и теоремы 4.

Следующее утверждение является ключевым в доказательстве неразрешимости уравнения

$$x^2 - y^q = 1 \tag{44}$$

в случае нечетного простого $q > 3$.

Теорема 5 (Нагелль, 1921). *Пусть q – нечетное простое (случай $q = 3$ не исключается) и пара $x > 1$, $y > 1$ удовлетворяет уравнению (44). Тогда y четно и $q \mid x$.*

Нам понадобится следующее вспомогательное утверждение.

Лемма 8. *Общее решение $x > 0$, $z \geqslant 0$ уравнения Пелля*

$$x^2 - dz^2 = 1, \qquad \text{где} \quad d = u^2 - 1,\ u \in \mathbb{Z},\ u \geqslant 2, \tag{45}$$

можно представить в виде

$$x + z\sqrt{d} = x_n + z_n\sqrt{d} = (u + \sqrt{u^2-1})^n, \qquad n = 0, 1, 2, \ldots .$$

Доказательство. Согласно результату Дирихле [Di, Дополнение VIII, § 142] общее решение уравнения $x^2 - dz^2 = 1$, где целое $d > 0$ не является квадратом, может быть представлено в виде $x + z\sqrt{d} = (x_1 + z_1\sqrt{d})^n$; при этом пара x_1, z_1 называется *фундаменательным решением*. Для доказательства леммы заметим, что $x_1 = u$, $z_1 = 1$ является фундаменательным решением уравнения (45), поскольку значение $z = 1$ у этого решения минимально возможное.

Доказательство теоремы 5. Отметим сразу, что четность y и, значит, нечетность x установлены в замечании в доказательстве теоремы 2.

Предположим, что $q \nmid x$, т.е. числа x, q взаимно просты. Записывая уравнение (44) в виде

$$x^2 = (y+1) \cdot \frac{y^q + 1}{y+1} \tag{46}$$

и пользуясь тем, что левая часть (46) на q не делится, согласно лемме 4 заключаем, что множители $y + 1$ и $(y^q + 1)/(y + 1)$ взаимно просты, так что

$$y + 1 = u^2, \quad \frac{y^q + 1}{y+1} = v^2, \quad x = uv, \qquad (u, v) = 1, \quad u, v \text{ нечетны}. \tag{47}$$

Используя (47), перепишем исходное уравнение в виде $x^2 - (u^2-1)^q = 1$ или

$$x^2 - dz^2 = 1, \tag{48}$$

где $d = u^2 - 1$. Это уравнение имеет целочисленное решение

$$x = uv, \quad z = (u^2-1)^{(q-1)/2},$$

которое в соответствии с леммой 8 можно представить в виде

$$x + z\sqrt{u^2-1} = (u + \sqrt{u^2-1})^n \tag{49}$$

для некоторого целого $n \geqslant 1$. Раскрывая суммирование в (49), получаем

$$x = \sum_{k=0}^{[n/2]} \binom{n}{2k} u^{n-2k}(u^2-1)^k, \tag{50}$$

$$z = \sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1} u^{n-2k-1}(u^2-1)^k.$$

Если n четно, то все слагаемые в правой части (50) кроме слагаемого, отвечающего $k = n/2$ делятся на u, т.е. $x \equiv (u^2-1)^{n/2} \equiv (-1)^{n/2} \pmod u$. Но число $x = uv$ делится на u, так что n нечетно. Поэтому

$$z \equiv \binom{n}{2k+1} u^{n-2k-1}(u^2-1)^k \Big|_{k=0} = nu^n = nu\big((u^2-1)+1\big)^{(n-1)/2}$$
$$\equiv nu \pmod{(u^2-1)} \equiv 1 \pmod 2,$$

так как n, u нечетны. В то же время $z = (u^2-1)^{(q-1)/2}$ делится на 2 (и даже на $8^{(q-1)/2}$). Полученное противоречие показывает, что взаимная простота x, q невозможна, и завершает доказательство теоремы.

Замечание. Оригинальное доказательство Нагелля теоремы 5 использовало следующую теорему (Штёрмер, 1897).

Пусть целое $d > 0$ не является квадратом и x, z – решение уравнения Пелля

$$x^2 - dz^2 = 1, \tag{51}$$

причем каждый простой делитель числа z делит d. Тогда x, z – фундаментальное решение уравнения (51).

В случае уравнения (48) с $d = u^2 - 1$ фундаментальным является решение $x_1 = u$, $z_1 = 1$, в то время как другое решение x, $z = (u^2-1)^{(q-1)/2}$ также удовлетворяет условию фундаментальности теоремы Штёрмера.

Теорема 6 (Ко Чао, 1965). *Если $q > 3$ – нечетное простое, то уравнение*

$$x^2 - y^q = 1 \tag{52}$$

не имеет решений в целых $x > 1$, $y > 1$.

На самом деле, теорема 6 была доказана Ко Чао еще в 1960 г., но на китайском языке. Далее мы приводим доказательство теоремы 6, основанное на идеях Чейна [Ch]. Более сложное, но оригинальное доказательство Ко Чао [Ko] (см. также [Mo, § 30]) излагается нами как "иное" доказательство теоремы 6. Здесь важно отметить, что в основе доказательства [Ko] лежит квадратичный закон взаимности, некоторое обобщение которого на круговые поля позволило Михайлеску [Mi1] получить существенное продвижение для общего уравнения Каталана.

Лемма 9 (обобщение леммы 4). *Пусть $q \geqslant 3$ – нечетное простое, а числа X, Y попарно взаимно просты. Тогда*

$$\left(X+Y, \frac{X^q+Y^q}{X+Y}\right) = \begin{cases} q, & \text{если } q \mid (X+Y), \\ 1 & \text{иначе.} \end{cases}$$

Доказательство теоремы 6. В теореме 5 доказано, что x нечетно и $q \mid x$. Перепишем уравнение (52) в виде

$$(|x|-1)(|x|+1) = y^q, \qquad (|x|-1, |x|+1) = 2,$$

откуда

$$x - 1 = 2a^q, \quad x + 1 = 2^{q-1}b^q \tag{53}$$

для некоторых целых (не обязательно положительных) $a \neq 0$ и $b \neq 0$, причем $(a, 2b) = 1$. Из (53) находим $a^q = 2^{q-2}b^q - 1$, откуда $|a|^q \geqslant 2^{q-2}|b|^q - 1 > |b|^q$ и, значит, $|a| > |b|$ или

$$|b| \leqslant |a| - 1. \tag{54}$$

Согласно (53) имеем

$$(a^2 + 2b) \cdot \frac{a^{2q} + (2b)^q}{a^2 + 2b} = a^{2q} + (2b)^q = \left(\frac{x-1}{2}\right)^2 + 2(x+1) = \left(\frac{x+3}{2}\right)^2. \tag{55}$$

Поскольку q делит x и $q > 3$, числа q и $x + 3$ взаимно просты, значит числа q и (55) также взаимно просты. В соответствии с $(a, 2b) = 1$ и леммой 9 получаем

$$\left(a^2 + 2b, \frac{a^{2q} + (2b)^q}{a^2 + 2b}\right) = 1,$$

откуда согласно (55) число $a^2 + 2b$ является полным квадратом:

$$a^2 + 2b = c^2, \qquad c \in \mathbb{Z}. \tag{56}$$

С другой стороны, применение оценки (54) дает неравенство $(|a|-1)^2 < |a^2+2b| < |a|^2$ в случае $b < 0$ и $|a|^2 < |a^2 + 2b| < (|a| + 1)^2$ в случае $b > 0$, т.е. равенство (56) невозможно. Полученное противоречие означает, что уравнение (52) не имеет решений в целых $|x| > 1$, $y > 1$. Теорема доказана.

Перед тем, как приводить доказательство из [Ko], напомним определение и свойства символов Лежандра и Якоби (все это подробно изложено в [Vi]).

Пусть p – нечетное простое. Целое число a, взаимно простое с p, называется *квадратичным вычетом* или *невычетом* в зависимости от того, разрешимо сравнение

$$x^2 \equiv a \pmod{p} \tag{57}$$

или неразрешимо. Отметим, что если a – квадратичный вычет, то сравнение (57) имеет в точности два решения по модулю p. Поэтому любая приведенная система вычетов по модулю p содержит $(p-1)/2$ квадратичных вычетов и $(p-1)/2$ квадратичных невычетов.

Символ Лежандра задается следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ – квадратичный вычет,} \\ -1, & \text{если } a \text{ – квадратичный невычет,} \end{cases}$$

а его обобщение – *символ Якоби* – определяется для целых нечетных $m = p_1 \times p_2 \cdots p_k$ и целых a, $(a, m) = 1$, по правилу

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right),$$

где в произведении в правой части участвуют символы Лежандра.

Предложение 1. *Имеют место следующие утверждения*:

1) *для простого p выполнено*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p};$$

2) *если $a \equiv a' \pmod{m}$, то $\left(\frac{a}{m}\right) = \left(\frac{a'}{m}\right)$;*
3) $\left(\frac{1}{m}\right) = 1$;
4) *выполнено*

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2} = \begin{cases} 1, & \text{если } m \equiv 1 \pmod{4}, \\ -1, & \text{если } m \equiv -1 \pmod{4}; \end{cases}$$

5) *выполнено*

$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8} = \begin{cases} 1, & \text{если } m \equiv \pm 1 \pmod{8}, \\ -1, & \text{если } m \equiv \pm 3 \pmod{8}; \end{cases}$$

6) *выполнено*

$$\left(\frac{a_1 a_2 \cdots a_l}{m}\right) = \left(\frac{a_1}{m}\right)\left(\frac{a_2}{m}\right)\cdots\left(\frac{a_l}{m}\right)$$

и, в частности,

$$\left(\frac{ab^2}{m}\right) = \left(\frac{a}{m}\right),$$

т.е. в числителе символа можно отбросить любой квадратичный множитель;

7) *если m, n – нечетные целые числа, то (квадратичный закон взаимности)*

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right),$$

иными словами, $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$, если оба числа m, n имеют вид $4l-1$, и $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$, если хотя бы одно из них имеет вид $4l+1$.

Иное доказательство теоремы 6. Согласно теореме 5 выполнено $x \equiv 0 \pmod{q}$, значит

$$y \equiv y^q \equiv -1 \pmod{q}.$$

Поэтому исходное уравнение

$$x^2 = y^q + 1 = (y+1)\cdot\frac{y^q+1}{y+1}$$

влечет

$$y + 1 = qu^2, \quad \frac{y^q+1}{y+1} = qv^2, \qquad (u, v) = 1.$$

Запишем исходное уравнение (52) по-другому:

$$x^2 - 2 = y^q - 1 = (y-1) \cdot \frac{y^q - 1}{y-1},$$

поэтому для произвольного простого делителя l числа $y-1$ сравнение $x^2 - 2 \equiv 0 \pmod{l}$ разрешимо, т.е. $\left(\frac{2}{l}\right) = 1$. Отсюда $l \equiv \pm 1 \pmod 8$ и число $y-1$ как произведение простых вида $8n \pm 1$ само имеет вид $8n \pm 1$. Таким образом, $y - 1 \equiv \pm 1 \pmod 8$ или

$$y \equiv 0 \text{ или } 2 \pmod 8.$$

Отметим, что $u^2 \equiv 1 \pmod 8$, поэтому $y + 1 = qu^2 \equiv q \pmod 8$, так что возможны два случая:

1) $q \equiv 3 \pmod 8$, если $y \equiv 2 \pmod 8$;
2) $q \equiv 1 \pmod 8$, если $y \equiv 0 \pmod 8$.

1) Поскольку $y \equiv 2 \pmod 8$, имеем $y^3 - 1 \equiv 7 \pmod 8$. Поэтому

$$x^2 = y^q + 1 \equiv y^\lambda + 1 \pmod{y^3 - 1}$$

и

$$\left(\frac{y^\lambda + 1}{y^3 - 1}\right) = 1, \tag{58}$$

где $q \equiv \lambda \pmod 3$ и $\lambda \in \{1, 2\}$ (для простого $q > 3$ сравнение $q \equiv 0 \pmod 3$ невозможно).

1.1) Если $\lambda = 1$, то

$$\left(\frac{y^\lambda + 1}{y^3 - 1}\right) = \left(\frac{y+1}{y^3-1}\right)_{\equiv 3 \pmod 4}^{\equiv 3 \pmod 4} = -\left(\frac{y^3 - 1}{y+1}\right) = -\left(\frac{-2}{y+1}\right)$$
$$= -\left(\frac{-1}{y+1}\right)_{\equiv 3 \pmod 4} \left(\frac{2}{y+1}\right)_{\equiv 3 \pmod 8} = -(-1) \cdot (-1) = -1,$$

что противоречит (58).

1.2) Если $\lambda = 2$, то

$$\left(\frac{y^\lambda + 1}{y^3 - 1}\right) = \left(\frac{y^2+1}{y^3-1}\right)^{\equiv 1 \pmod 4} = \left(\frac{y^3 - 1}{y^2+1}\right) = \left(\frac{-y-1}{y^2+1}\right)$$
$$= \left(\frac{-1}{y^2+1}\right)_{\equiv 1 \pmod 4} \left(\frac{y+1}{y^2+1}\right) = \left(\frac{y+1}{y^2+1}\right)_{\equiv 1 \pmod 4}$$
$$= \left(\frac{y^2+1}{y+1}\right) = \left(\frac{2}{y+1}\right)_{\equiv 3 \pmod 8} = -1,$$

что опять же противоречит (58).

Таким образом, случай 1) $q \equiv 3 \pmod 8$, $y \equiv 2 \pmod 8$ невозможен.

2) Среди приведенной системы вычетов $1, 2, \ldots, q-1$ по модулю q выберем квадратичный невычет p по этому модулю. Поскольку $q \equiv 1 \pmod 8$ и, значит, $\left(\frac{2}{q}\right) = 1$,

можно в случае необходимости разделить p на все входящие в него двойки, т.е. считать число p нечетным. Кроме того, $p \neq 1$, так как 1 – квадратичный вычет по модулю q. Таким образом, p – нечетное число, удовлетворяющее условиям $3 \leqslant p < q$ и $\left(\frac{p}{q}\right) = -1$.

Для каждого положительного $t \in \mathbb{Z}$ определим число

$$E(t) = \frac{(-y)^t - 1}{(-y) - 1} \in \mathbb{Z}. \tag{59}$$

Поскольку $y \equiv 0 \pmod 8$, выполнено $E(t) \equiv 1 \pmod 8$ для любого положительного $t \in \mathbb{Z}$. Отметим также еще одно свойство чисел (59), а именно

$$E(t+n) - E(t) = \frac{(-y)^{t+n} - (-y)^t}{(-y) - 1} = (-y)^t \cdot E(n),$$

откуда $E(t+n) \equiv E(t) \pmod{E(n)}$ и

$$E(kt+n) \equiv E(t) \pmod{E(n)}. \tag{60}$$

Кроме того, $E(1) = 1$.

В соответствии с выбором числа p выполнено $(q,p) = 1$. Запишем алгоритм Евклида для вычисления наибольшего общего делителя чисел p, q и индуцированные правилом (60) сравнения:

$$\begin{array}{ll} q = k_1 p + n_1, & E(q) \equiv E(r_1) \pmod{E(p)}, \\ p = k_2 n_1 + n_2, & E(p) \equiv E(n_2) \pmod{E(n_1)}, \\ n_1 = k_3 n_2 + n_3, & E(n_1) \equiv E(n_3) \pmod{E(n_2)}, \\ \dots\dots\dots & \dots\dots\dots \\ n_{s-2} = k_s n_{s-1} + n_s, & E(n_{s-2}) \equiv E(n_s) \pmod{E(n_{s-1})}, \\ n_{s-1} = k_{s+1} n_s + 1, & E(n_{s-1}) \equiv E(1) = 1 \pmod{E(n_s)}. \end{array} \tag{61}$$

Рассматривая сравнения в правой колонке (61) в обратном порядке, заключаем, что числа $E(n_{s-1})$ и $E(n_s)$ взаимно просты, откуда числа $E(n_{s-2})$ и $E(n_{s-1})$ взаимно просты и т.д., любые два соседних числа $E(n_j)$ и $E(n_{j+1})$ взаимно просты. Поэтому применение правил вычисления символа Якоби приводит к цепочке

$$\begin{aligned} \left(\frac{E(q)}{E(p)}\right) &= \left(\frac{E(n_1)}{E(p)}\right) = \left(\frac{E(p)}{E(n_1)}\right) = \left(\frac{E(n_2)}{E(n_1)}\right) = \left(\frac{E(n_1)}{E(n_2)}\right) = \left(\frac{E(n_3)}{E(n_2)}\right) = \cdots \\ &= \left(\frac{E(n_{s-2})}{E(n_{s-1})}\right) = \left(\frac{E(n_s)}{E(n_{s-1})}\right) = \left(\frac{E(n_{s-1})}{E(n_s)}\right) = \left(\frac{E(1)}{E(n_s)}\right) \\ &= \left(\frac{1}{E(n_s)}\right) = 1, \end{aligned} \tag{62}$$

где все ‘перевороты’ символов Якоби законны в связи с тем, что $E(t) \equiv 1 \pmod 8$.

С другой стороны,

$$E(q) = \frac{y^q + 1}{y + 1} = qv^2,$$

откуда

$$\left(\frac{E(q)}{E(p)}\right) = \left(\frac{qv^2}{E(p)}\right) = \left(\frac{q}{E(p)}\right)_{\equiv 1 \pmod 4} = \left(\frac{E(p)}{q}\right); \tag{63}$$

кроме того,

$$\begin{aligned} E(p) &= \frac{(-y)^p - 1}{(-y) - 1} = (-y)^{p-1} + (-y)^{p-2} + \cdots + (-y) + 1 \\ &\equiv \underbrace{1 + 1 + \cdots + 1 + 1}_{p \text{ раз}} \equiv p \pmod q, \end{aligned}$$

что вместе с соотношением (63) дает

$$\left(\frac{E(q)}{E(p)}\right) = \left(\frac{E(p)}{q}\right) = \left(\frac{p}{q}\right). \tag{64}$$

Таким образом, $\left(\frac{p}{q}\right) = 1$ согласно (62) и (64), а это противоречит выбору числа p. Полученное противоречие показывает, что случай 2) $q \equiv 1 \pmod 8$, $y \equiv 0 \pmod 8$ также невозможен, и завершает доказательство теоремы.

Список литературы

[Cat] Catalan E. C. Note extraite d'une lettre adressée à l'éditeur // J. Reine Angew. Math. 1844. V. 27. P. 192.

[Ca1] Cassels J. W. S. On the equation $a^x - b^y = 1$ // Amer. Math. J. 1953. V. 75. P. 159–162.

[Ca2] Cassels J. W. S. On the equation $a^x - b^y = 1$, II // Proc. Cambridge Phil. Soc. 1960. V. 56. P. 97–103.

[Ch] Chein E. Z. A note on the equation $x^2 = y^q + 1$ // Proc. Amer. Math. Soc. 1976. V. 56. P. 83–84.

[Di] Лежен Дирихле Г. П. Лекции по теории чисел. М.–Л.: ОНТИ, 1936.

[Ko] Ko Chao. On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$ // Sci. Sinica 1965. V. 14. P. 457–460.

[Le] Lebesgue V. A. Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$ // Nouv. Ann. Math. (1) 1850. V. 9. P. 178–181.

[Mi1] Mihăilescu P. A class number free criterion for Catalan's conjecture // J. Number Theory (to appear).

[Mi2] Mihăilescu P. Primary cyclotomic units and a proof of Catalan's conjecture. (submitted).

[Mo] Mordell L. J. Diophantine equations. Pure Appl. Math.. V. 30. London–New York: Academic Press, 1969.

[Na1] Nagell T. Sur l'impossibilité de l'équation indéterminée $z^p + 1 = y^2$ // Norsk Mat. Forenings Skrifter. 1921. V. 1. №4.

[Na2] Nagell T. Sur une équation à deux indéterminées // Norsk Vid Selsk Forh. 1934. V. 7. P. 136–139.

[Ri] Ribenboim R. Catalan's conjecture. Are 8 and 9 the only consecutive powers? New York: Acad. Press, 1994.

[Se] Серпинский В. 250 задач по элементарной теории чисел. М.: Просвещение, 1968.

[Vi] Виноградов И. М. Основы теории чисел. 8 изд. М.: Наука, 1972.