Проблема Каталана.
II. Критерий Михайлеску

Настоящая глава посвящена доказательству следующего обобщения теоремы Касселса.

Теорема 1 (Михайлеску, 1999). *Если p и q – нечетные простые числа, а ненулевые числа x, y связаны соотношением $x^p - y^q = 1$. Тогда $q^2 \mid x$, $p^2 \mid y$ и*

$$p^{q-1} \equiv 1 \pmod{q^2}, \qquad q^{p-1} \equiv 1 \pmod{p^2}. \tag{1}$$

Различные версии этого утверждения с дополнительными ограничениями на нечетные простые параметры p, q берут начало с работы Инкери [In]. В случае $p \equiv q \equiv 3 \pmod 4$ теорема 1 была доказана О'Нейлом [ON] в 1995 г., а случай $p \not\equiv q \pmod 4$ был разобран Штайнером [St] в 1998 г. Однако доказательство Михайлеску [Mi1] не различает простые числа p, q в зависимости от остатка по модулю 4. Поэтому следующее далее доказательство не опирается на предыдущие результаты в этом направлении; по-существу оно воспроизводит (с некоторыми изменениями) оригинальное доказательство из [Mi1].

Замечание. Как несложно заметить, в предположениях теоремы 1 достаточно показать, что

$$x \equiv 0 \pmod{q^2}, \qquad p^{q-1} \equiv 1 \pmod{q^2}. \tag{2}$$

Действительно, переписывая уравнение Каталана в виде $(-y)^q - (-x)^p = 1$, из (2) получаем также $p^2 \mid y$ и $q^{p-1} \equiv 1 \pmod{p^2}$.

Условие (1) определяет так называемые *пары Вифериха*; непосредственные вычисления показывают, что среди простых p, q, удовлетворяющих неравенству $3 \leqslant q < p < 10^6$, имеется ровно три пары Вифериха:

$$p = 4871,\ q = 83, \qquad p = 18787,\ q = 2903, \qquad p = 318917,\ q = 911. \tag{3}$$

(Мы ссылаемся здесь на вычисления Миньотта, хотя ничто не мешает проделать их самостоятельно.)

Для доказательства теоремы 1 нам понадобятся некоторые факты из алгебраической теории круговых полей. Пусть p – нечетное простое число, $\zeta = \zeta_p = e^{2\pi i/p}$ – примитивный корень степени p из единицы. Как известно, минимальным многочленом числа ζ является

$$x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 = \prod_{j=1}^{p-1} (x - \zeta^j), \tag{4}$$

все корни которого – сопряженные к ζ – исчерпываются набором $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. Таким образом, степень расширения (*кругового поля*) $\mathbb{Q}(\zeta)$ над $\mathbb{Q}$ равна $p - 1$.

Отметим, что $\mathbb{Q}(\zeta)$ – нормальное поле (каждое число входит в поле со всеми своими сопряжениями). Для любого $\alpha \in \mathbb{Q}(\zeta)$ существует единственное представление

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}, \qquad \text{где} \quad a_0, a_1, \ldots, a_{p-2} \in \mathbb{Q}. \tag{5}$$

Все автоморфизмы поля $\mathbb{Q}(\zeta)$ суть $\sigma_c\colon \zeta \mapsto \zeta^c$, $c = 1, 2, \ldots, p-1$. Их действие на произвольный элемент (5) поля $\mathbb{Q}(\zeta)$ имеет вид

$$\sigma_c\colon \alpha \mapsto \alpha^{\sigma_c} = a_0 + a_1\zeta^c + \cdots + a_{p-2}\zeta^{c(p-2)}, \qquad c = 1, 2, \ldots, p-1.$$

Непосредственно из определения следует, что $\sigma_c \cdot \sigma_{c'} = \sigma_d$, где $d \equiv cc' \pmod{p}$; отсюда, в частности, следует, что $\sigma_c^{-1} = \sigma_{c'}$, где $cc' \equiv 1 \pmod{p}$. Группа Галуа $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_c : c = 1, 2, \ldots, p-1\}$ является циклической: если g – первообразный корень по модулю p, то $G = \langle \sigma_g \rangle_{p-1}$.

Доказательство следующего непростого утверждения можно найти в книге [BS].

Предложение 1. *Кольцом целых поля $\mathbb{Q}(\zeta)$ является $\mathbb{Z}[\zeta]$.*

Согласно (4) после подстановки $x = 1$ выполнено

$$p = \prod_{j=1}^{p-1}(1-\zeta^j) = (1-\zeta)^{p-1}\prod_{j=1}^{p-1}\frac{1-\zeta^j}{1-\zeta}. \tag{6}$$

Лемма 1. *Для любого целого j число $(1-\zeta^j)/(1-\zeta)$ является единицей кольца $\mathbb{Z}[\zeta]$.*

Доказательство. Действительно, достаточно доказать утверждение для целых положительных j. Имеем

$$\frac{1-\zeta^j}{1-\zeta} = 1 + \zeta + \zeta^2 + \cdots + \zeta^{j-1} \in \mathbb{Z}[\zeta],$$
$$\frac{1-\zeta}{1-\zeta^j} = \frac{1-\zeta^{jj'}}{1-\zeta^j} = 1 + \zeta^j + \zeta^{2j} + \cdots + \zeta^{(j'-1)j} \in \mathbb{Z}[\zeta],$$

где $jj' \equiv 1 \pmod{p}$. Таким образом, элемент $(1-\zeta^j)/(1-\zeta)$ обратим в кольце $\mathbb{Z}[\zeta]$ и, значит, является единицей.

Согласно лемме 1 соотношение (6) можно переписать в виде $p = \varepsilon(1-\zeta)^{p-1}$, где $\varepsilon \in E(\mathbb{Z}[\zeta])$, или после перехода к идеалам

$$(p) = (1-\zeta)^{p-1}.$$

При этом идеал $(1-\zeta)$ прост, поскольку $\mathbb{Z}[\zeta]/(1-\zeta) \simeq \mathbb{Z}/p\mathbb{Z}$ и последний объект является не кольцом, а полем.

Предложение 2. *Корни из единицы в поле $\mathbb{Q}(\zeta)$ образуют циклическую группу $\langle -\zeta \rangle_{2p}$.*

Замечание. Как следует из леммы 1 и предложения 2 элементы

$$\pm\zeta^n \cdot \frac{1-\zeta^j}{1-\zeta} \in \mathbb{Z}[\zeta], \qquad n, j \in \mathbb{Z}, \tag{7}$$

являются единицами кольца $\mathbb{Z}[\zeta]$. На самом деле, верно и обратное: группа единиц $E(\mathbb{Z}[\zeta])$ порождается множеством (7).

Предложение 3. *Пусть q – простое нечетное число, $q \neq p$, принадлежащее показателю f по модулю p, т.е. f – наименьшее положительное целое, для которого $q^f \equiv 1 \pmod p$. Тогда $(q) = \mathfrak{q}_1 \cdots \mathfrak{q}_e$, где $e = (p-1)/f$, а $\mathfrak{q}_1, \ldots, \mathfrak{q}_e$ – простые идеалы в $\mathbb{Z}[\zeta]$. Более точно, имеет место разложение*

$$x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 \equiv h_1(x) \cdots h_e(x) \pmod q,$$

где все многочлены $h_1(x), \ldots, h_e(x)$ неприводимы над $\mathbb{F}_q$; при этом $\mathfrak{q}_j = (q, h_j(\zeta))$, $j = 1, \ldots, e$.

Замечание. Сразу отметим, что любому простому идеалу $\mathfrak{q}$ в $\mathbb{Z}[\zeta]$ отвечает ровно одно простое число $q \in \mathbb{Z}$, делителем которого является $\mathfrak{q}$.

Лемма 2. *Пусть простой идеал $\mathfrak{q} \subset \mathbb{Z}[\zeta]$ не делит p. Тогда числа $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ попарно несравнимы по модулю $\mathfrak{q}$.*

Доказательство. Предположим от противного, что $\zeta^k \equiv \zeta^l \pmod{\mathfrak{q}}$ для $0 \leqslant l < k \leqslant p-1$. Тогда $\zeta^{k-l} \equiv 1 \pmod{\mathfrak{q}}$, так как $\zeta^{-l} \in E(\mathbb{Z}[\zeta])$, откуда

$$(1-\zeta) \cdot \frac{1-\zeta^{k-l}}{1-\zeta} \in \mathfrak{q}. \tag{8}$$

Но $(1-\zeta^{k-l})/(1-\zeta)$ – единица кольца $\mathbb{Z}[\zeta]$ согласно лемме 1, так что включение (8) означает, что $1-\zeta \in \mathfrak{q}$ или $(1-\zeta) \subset \mathfrak{q}$. Однако последнее вложение ввиду простоты идеала $\mathfrak{q}$ приводит, к $p \in (p) = (1-\zeta)^{p-1} \subset \mathfrak{q}$, что противоречит условию леммы.

Следствие. *Если $\alpha \notin \mathfrak{q} \mid q$, q – нечетное простое, в условиях леммы 2 и целое число f опрелено в предложении 3, то существует единственное n, $0 \leqslant n \leqslant p-1$, такое, что $\alpha^{(q^f-1)/p} \equiv \zeta^n \pmod{\mathfrak{q}}$.*

Замечание. Приведенное сравнение является аналогом сравнения

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

для символа Лежандра.

Доказательство. Отметим, что если $\mathfrak{q} = \mathfrak{q}_j$ в обозначениях предложения 3, то факторкольцо $\mathbb{Z}[\zeta]/\mathfrak{q}_j \simeq \mathbb{F}_q[x]/(h_j(x))$ является полем, изоморфным $\mathbb{F}_{q^f}$. Поэтому порядок любого элемента $\alpha \pmod{\mathfrak{q}}$ делит порядок мультипликативной группы поля $\mathbb{F}_{q^f}$, т.е. $\alpha^{q^f-1} \equiv 1 \pmod{\mathfrak{q}}$. Таким образом,

$$\prod_{n=1}^{p-1} \left(a^{(q^f-1)/p} - \zeta^n\right) = \alpha^{q^f-1} - 1 \in \mathfrak{q}$$

и ввиду простоты идеала $\mathfrak{q}$ хотя бы один из множителей в произведении слева лежит в $\mathfrak{q}$. Остается заметить, что только один из множителей $a^{(q^f-1)/p} - \zeta^n \in \mathfrak{q}$, так как все эти множители попарно несравнимы по модулю $\mathfrak{q}$ согласно лемме 2.

Для любого $\alpha \notin \mathfrak{q}$ определим в соответствии со следствием к лемме 2 символ

$$\left(\frac{\alpha}{\mathfrak{q}}\right) = \zeta^n.$$

Несложная проверка, как и для символа Лежандра, показывает, что имеют место следующие свойства.

Свойство 1. *Если* $\alpha \equiv \beta \pmod{\mathfrak{q}}$, *то*

$$\left(\frac{\alpha}{\mathfrak{q}}\right) = \left(\frac{\beta}{\mathfrak{q}}\right).$$

Свойство 2. *Для любых* $\alpha, \beta \notin \mathfrak{q}$ *выполнено*

$$\left(\frac{\alpha\beta}{\mathfrak{q}}\right) = \left(\frac{\alpha}{\mathfrak{q}}\right)\left(\frac{\beta}{\mathfrak{q}}\right).$$

Как уже отмечалось, факторкольцо $F = \mathbb{Z}[\zeta]/\mathfrak{q}$ является полем, изоморфным полю $\mathbb{F}_{q^f}$. Через $\widetilde{\alpha}$ будем обозначать образ элемента $\alpha \in \mathbb{Z}[\zeta]$ при естественном вложении $\mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]/\mathfrak{q} = F$. Приведенные выше свойства означают, что отображение

$$\chi_{\mathfrak{q}} \colon \widetilde{\alpha} \mapsto \left(\frac{\alpha}{\mathfrak{q}}\right)^{-1} \tag{9}$$

является характером мультипликативной группы F^* (т.е. $\chi_{\mathfrak{q}} \colon F^* \to \mathbb{C}^*$ – гомоморфизм).

Наряду с введенным ранее корнем из единицы $\zeta = \zeta_p = e^{2\pi i/p}$ нам также понадобится другой корень из единицы $\zeta_q = e^{2\pi i/q}$, где q – (единственное) простое число, лежащее в идеале $\mathfrak{q}$. Определим для характера (9) гауссову сумму

$$S(\chi_{\mathfrak{q}}) = \sum_{\widetilde{\alpha} \in F^*} \chi_{\mathfrak{q}}(\alpha) \cdot \zeta_q^{\mathrm{Tr}(\widetilde{\alpha})} \in \mathbb{Z}[\zeta_p, \zeta_q], \tag{10}$$

где $\mathrm{Tr}(\alpha) = a_0 + a_1 + \cdots + a_{p-2}$ для $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \in \mathbb{Z}[\zeta]$. Согласно лемме 2 из сравнения

$$\widetilde{\alpha} \equiv \alpha \pmod{\mathfrak{q}}, \qquad \widetilde{\alpha} = \widetilde{a}_0 + \widetilde{a}_1\zeta + \cdots + \widetilde{a}_{p-2}\zeta^{p-2} \in \mathbb{Z}[\zeta],$$

и целочисленности $a_l, \widetilde{a}_l$ следует, что $\widetilde{a}_l \equiv a_l \pmod{q}$ для каждого $l = 0, 1, \ldots, p-2$; поэтому $\mathrm{Tr}(\widetilde{\alpha}) \equiv \mathrm{Tr}(\alpha) \pmod{q}$, т.е. величина $\zeta_q^{\mathrm{Tr}(\widetilde{\alpha})}$ в (10) определена корректно. Наконец, включение $S(\chi_{\mathfrak{q}}) \in \mathbb{Z}[\zeta_p, \zeta_q]$ получаем ввиду $\chi_{\mathfrak{q}}(\alpha) \in E(\mathbb{Z}[\zeta_p]) \subset \mathbb{Z}[\zeta_p]$ и $\mathrm{Tr}(\widetilde{\alpha}) \in \mathbb{Z}$.

Лемма 3. *Пусть* $\varphi(\mathfrak{q}) = S(\chi_{\mathfrak{q}})^p$. *Тогда* $\varphi(\mathfrak{q}) \in \mathbb{Z}[\zeta_p]$.

Доказательство. Хорошо известно, что

$$[\mathbb{Q}(\zeta_p, \zeta_q) : \mathbb{Q}(\zeta_p)] = [\mathbb{Q}(\zeta_q) : \mathbb{Q}] = q - 1.$$

Это означает неприводимость многочлена $x^{q-1} + x^{q-2} + \cdots + x + 1$ как над $\mathbb{Q}$, так и над $\mathbb{Q}(\zeta_p)$. Следовательно, любой автоморфизм $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ единственным образом продолжается до автоморфизма $\widehat{\tau}$ поля $\mathbb{Q}(\zeta_p, \zeta_q)$ над $\mathbb{Q}$, действующего тождественно на $\mathbb{Q}(\zeta_p)$. Каждый такой автоморфизм $\widehat{\tau}$ определяется действием на ζ_q и ζ_p. Именно, если $\tau_c \in \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})\colon \zeta_q \mapsto \zeta_q^c$, то $\widehat{\tau}_c\colon \zeta_q \mapsto \zeta_q^c$ и $\widehat{\tau}_c\colon \zeta_p \mapsto \zeta_p$. Автоморфизмы $\widehat{\tau}_c$ порождают циклическую группу $\langle \widehat{\tau}_g \rangle_{q-1}$, изоморфную $(\mathbb{Z}/q\mathbb{Z})^*$; здесь g – первообразный корень по модулю q. Для доказательства леммы достаточно проверить, что порождающий автоморфизм $\widehat{\tau} = \widehat{\tau}_g$ переводит $\varphi(\mathfrak{q})$ в себя. Действительно, применяя линейность следа, получаем

$$\begin{aligned} S(\chi_{\mathfrak{q}})^\tau &= \sum_{\widetilde{\alpha} \in F^*} \chi_{\mathfrak{q}}(\widetilde{\alpha}) \cdot \zeta_q^{g \operatorname{Tr}(\widetilde{\alpha})} = \sum_{\widetilde{\alpha} \in F^*} \chi_{\mathfrak{q}}(g)^{-1} \chi_{\mathfrak{q}}(g\widetilde{\alpha}) \cdot \zeta_q^{\operatorname{Tr}(g\widetilde{\alpha})} \\ &= \chi_{\mathfrak{q}}(g)^{-1} \sum_{\widetilde{\alpha} \in F^*} \chi_{\mathfrak{q}}(g\widetilde{\alpha}) \cdot \zeta_q^{\operatorname{Tr}(g\widetilde{\alpha})} = \chi_{\mathfrak{q}}(g)^{-1} \cdot S(\chi_{\mathfrak{q}}) \end{aligned}$$

и поскольку $\big(\chi_{\mathfrak{q}}(g)^{-1}\big)^p = (\zeta_p^n)^p = 1$, находим

$$\varphi(\mathfrak{q})^\tau = \big(S(\chi_{\mathfrak{q}})^\tau\big)^p = S(\chi_{\mathfrak{q}})^p = \varphi(\mathfrak{q}).$$

Это завершает доказательство леммы.

Вернемся теперь к рассмотрению группы автоморфизмов $G = \{\sigma_c : c = 1, 2, \ldots, p-1\}$ поля $\mathbb{Q}(\zeta_p)$ над $\mathbb{Q}$. В дальнейшем будет удобно рассматривать следующее действие элементов множества

$$\mathbb{Z}[G] = \{\lambda = \lambda_1\sigma_1 + \cdots + \lambda_{p-1}\sigma_{p-1} : \lambda_1, \ldots, \lambda_{p-1} \in \mathbb{Z}\}$$

на $\alpha \in \mathbb{Q}(\zeta_p)$: для $\lambda \in \mathbb{Z}[G]$ полагаем

$$\lambda\colon \alpha \mapsto \alpha^\lambda = \prod_{c=1}^{p-1} (\sigma_c \alpha)^{\lambda_c}.$$

Определим

$$\theta = \sum_{c=1}^{p-1} c\sigma_c^{-1} = \sum_{c=1}^{p-1} c\sigma_{c'} \in \mathbb{Z}[G], \qquad cc' \equiv 1 \pmod{p}. \tag{11}$$

Предложение 4 (соотношение Штикельбергера). *Пусть простой идеал* $\mathfrak{q}$ *делит простое число* $q \neq p$. *Тогда* $\mathfrak{q}^\theta = \big(\varphi(\mathfrak{q})\big)$.

Доказательство этого частного случая теоремы Штикельбергера [Sti] можно найти в [IR, гл. 14, § 4]. В дальнейшем нам понадобится следствие из предложения 4 (далее мы опять будем опускать индекс p в записи примитивного корня из единицы $\zeta = \zeta_p = e^{2\pi i/p}$).

Следствие. *Для любого идеала* $\mathfrak{a} \subset \mathbb{Z}[\zeta]$ *идеал* $\mathfrak{a}^\theta \subset \mathbb{Z}[\zeta]$ *является главным.*

Доказательство. Запишем каноническое разложение идеала $\mathfrak{a}$ в произведение простых идеалов: $\mathfrak{a} = \mathfrak{p}^{k_0}\mathfrak{q}_1^{k_1}\cdots\mathfrak{q}_r^{k_r}$, где $\mathfrak{p} = (1-\zeta) \ni p$ (так как $\mathfrak{p}^{p-1} = (p)$), а для остальных идеалов ввиду простоты можно применять предложение 4. Тогда

$$\mathfrak{a}^\theta = \big((1-\zeta)^\theta\big)^{k_0}\big(\mathfrak{q}_1^\theta\big)^{k_1}\cdots\big(\mathfrak{q}_r^\theta\big)^{k_r} = \big((1-\zeta)\big)^{k_0}\big(\varphi(\mathfrak{q}_1)\big)^{k_1}\cdots\big(\varphi(\mathfrak{q}_r)\big)^{k_r}$$

является главным идеалом как произведение главных идеалов.

Замечание. Если образ любого идеала в $\mathbb{Z}[\zeta]$ под действием $\tau \in \mathbb{Z}[G]$ является главным идеалом, то говорят, что τ *аннулирует группу классов идеалов* $\mathbb{Z}[\zeta]$. Элемент (11) неединственный обладает этим свойством. В обозначениях

$$\theta' = \sum_{c=1}^{p-1} \frac{c}{p}\sigma_c^{-1} = \frac{1}{p}\theta \in \mathbb{Q}[G]$$

(так называемый *элемент Штикельбергера*) и $\theta_n = (\sigma_n - n)\theta'$ для $n \in \mathbb{Z}$ согласно теореме Штикельбергера [Sti] (см. также [IR, предложение 15.3.2]) каждый элемент θ_n лежит в $\mathbb{Z}[G]$ и аннулирует группу классов идеалов $\mathbb{Z}[\zeta]$. Фактически мы далее пользуемся этим свойством только для $\theta = -\theta_p$, в то время как Михайлеску [Mi1] применяет теорему Штикельбергера в полном объеме.

Наконец, закончим подготовительную часть следующим несложным наблюдением. Как обычно, говорят, что простое число $q \in \mathbb{Z}$ *неразветвлено над полем* $K \supset \mathbb{Q}$, если все компоненты в разложении главного идеала $(q) \subset \mathbb{Z}_K$ на простые идеалы в $\mathbb{Z}_K$ входят в первой степени; в противном случае говорят, что простое число q *разветвлено над полем* K. Так, любое простое число $q \in \mathbb{Z}$ неразветвлено над полем $\mathbb{Q}$; согласно предложению 3 любое простое число $q \neq p$ также неразветвлено над полем $\mathbb{Q}(\zeta_p)$.

Лемма 4. *Пусть простое число* q *неразветвлено над полем* $K \supset \mathbb{Q}$ *и для* $\alpha, \beta \in \mathbb{Z}_K$ *имеет место сравнение*

$$\alpha^q \equiv \beta^q \pmod{q}. \tag{12}$$

Тогда $\alpha^q \equiv \beta^q \pmod{q^2}$.

Доказательство. Пусть $(q) = \mathfrak{q}_1 \ldots \mathfrak{q}_e$ – разложение в произведение различных простых идеалов в $\mathbb{Z}_K$, и пусть $\mathfrak{q}_j$ – произвольный множитель в этом произведении. Тогда

$$\alpha^q \equiv \beta^q \pmod{\mathfrak{q}_j} \tag{13}$$

согласно (12). Покажем, что

$$\alpha^q \equiv \beta^q \pmod{\mathfrak{q}_j^2}. \tag{14}$$

Если $\alpha \in \mathfrak{q}_j$, то $\beta \in \mathfrak{q}_j$ согласно (13) и, следовательно, $\alpha^q \equiv \beta^q \pmod{\mathfrak{q}_j^q}$. Поэтому считаем $\alpha \notin \mathfrak{q}_j$. Записывая $\beta = \alpha + \xi$ в $\mathbb{Z}_K$ и подставляя в (12), находим

$$\alpha^q \equiv \beta^q \equiv \alpha^q + \xi^q \pmod{\mathfrak{q}_j},$$

откуда $\xi \in \mathfrak{q}_j$. Таким образом,

$$\beta^q = (\alpha + \xi)^q = \alpha^q + q\alpha^{q-1}\xi + \nu\xi^2, \qquad \nu \in \mathbb{Z}_K,$$

откуда ввиду делимостей $\mathfrak{q}_j \mid q$ и $\mathfrak{q}_j \mid \xi$ получаем сравнение (14). Окончательно, ввиду попарной взаимной простоты идеалов $\mathfrak{q}_1, \dots, \mathfrak{q}_e$ и, значит, $\mathfrak{q}_1^2, \dots, \mathfrak{q}_e^2$ из сравнений (14) находим

$$\alpha^q \equiv \beta^q \pmod{\mathfrak{q}_1^2 \cdots \mathfrak{q}_e^2 = q^2},$$

что и требовалось.

Доказательство теоремы 1. Согласно теореме Касселса $p \mid y$, откуда $x^p \equiv x \equiv 1 \pmod p$ и

$$\frac{x^p - 1}{x - 1} = pu^q, \tag{15}$$

$$x - 1 = p^{q-1}v^q, \tag{16}$$

$$y = puv, \qquad (u, pv) = 1.$$

Используя разложения (4), (6), перепишем равенство (15) в виде

$$\prod_{j=1}^{p-1} \frac{x - \zeta^j}{1 - \zeta^j} = u^q. \tag{17}$$

Представление $x = 1 + pt$, $t \in \mathbb{Z}$, приводит к включениям

$$\frac{x - \zeta^j}{1 - \zeta^j} = \frac{1 + pt - \zeta^j}{1 - \zeta^j} = 1 + t\frac{p}{1 - \zeta^j} = 1 + t\prod_{\substack{k=1 \\ k \neq j}}^{p-1}(1 - \zeta^k) \in \mathbb{Z}[\zeta], \qquad j = 1, 2, \dots, p-1. \tag{18}$$

Кроме того, числа в (18) попарно взаимно просты, так как

$$\frac{x - \zeta^j}{1 - \zeta^j} - \frac{1 - \zeta^k}{1 - \zeta^j} \cdot \frac{x - \zeta^k}{1 - \zeta^k} = \frac{\zeta^k - \zeta^j}{1 - \zeta^j}, \qquad 1 \leqslant j < k \leqslant p - 1,$$

а числа

$$\frac{1 - \zeta^k}{1 - \zeta^j}, \quad \frac{\zeta^k - \zeta^j}{1 - \zeta^j} = -\zeta^j\frac{1 - \zeta^{k-j}}{1 - \zeta^j}, \qquad 1 \leqslant j < k \leqslant p - 1,$$

в соответствии с леммой 1 являются единицами кольца $\mathbb{Z}[\zeta]$. Следовательно, согласно (17) для каждого $j = 1, 2, \dots, p - 1$ идеал в $\mathbb{Z}[\zeta]$, порожденный элементом $(x - \zeta^j)/(1 - \zeta^j)$, является точной q-й степенью. В частности (для $j = 1$),

$$\left(\frac{1 - \zeta^{-1}x}{1 - \zeta^{-1}}\right) = \left(\frac{x - \zeta}{1 - \zeta}\right) = \mathfrak{a}^q. \tag{19}$$

Согласно следствию из предложения 4 выполнено $\mathfrak{a}^\theta = (\alpha)$ для некоторого $\alpha \in \mathbb{Z}[\zeta]$, откуда в соответствии с (19) получаем

$$\left(\frac{1-\zeta^{-1}x}{1-\zeta^{-1}}\right)^\theta = \varepsilon\alpha^q,$$

где ε – единица кольца $\mathbb{Z}[\zeta]$, или

$$(1-\zeta^{-1}x)^\theta = (1-\zeta^{-1})^\theta\varepsilon\alpha^q. \tag{20}$$

Положим $\lambda = (1-\zeta^{-1})^\theta = (1-\bar{\zeta})^\theta$ и заметим, что $|\lambda\varepsilon| = |\overline{\lambda\varepsilon}|$. Поэтому $\eta = \overline{\varepsilon\lambda}/\varepsilon\lambda \in \mathbb{Q}(\theta)$ удовлетворяет условию $|\eta| = 1$, т.е. $\eta = (-\zeta)^t$ для некоторого целого t согласно предложению 2. Ввиду простоты (значит, и взаимной простоты) чисел p, q число t может быть представлено в виде $t = pm + qn$. Тогда $\eta = (-\zeta)^{pm+qn} = (-1)^{pm}(-\zeta)^{qn} = (-1)^{qm}(-\zeta)^{qn} = \delta^q$ с $\delta \in \langle -\zeta\rangle_{2p} \subset E(\mathbb{Z}[\zeta])$, где мы также воспользовались нечетностью чисел p, q. Таким образом, равенство (20) и сопряженное к нему принимают вид

$$(1-\zeta^{-1}x)^\theta = \varepsilon\lambda\alpha^q, \qquad (1-\zeta x)^\theta = \overline{\varepsilon\lambda}\bar{\alpha}^q = \varepsilon\lambda(\delta\bar{\alpha})^q. \tag{21}$$

Обозначим теперь через $\mathfrak{q} \subset \mathbb{Z}[\zeta]$ произвольный простой делитель числа q. Поскольку

$$(1-\zeta^{-1})^{\sigma_c} = 1-\zeta^{-c} = (1-\zeta)\cdot\frac{1-\zeta^{-c}}{1-\zeta}, \qquad c = 1, 2, \ldots, p-1,$$

причем $(1-\zeta^{-c})/(1-\zeta) \in E(\mathbb{Z}[\zeta])$ согласно лемме 1, выполнено

$$\lambda = (1-\zeta^{-1})^\theta = \varepsilon'\cdot\prod_{c'=1}^{p-1}(1-\zeta)^{c'} = \varepsilon'\cdot(1-\zeta)^{p(p-1)/2}, \qquad \varepsilon' \in E(\mathbb{Z}[\zeta]).$$

Следовательно, $\varepsilon\lambda \notin \mathfrak{q}$. Воспользуемся равенствами (21) и делимостью $q \mid x$, вытекающей из теоремы Касселса:

$$\varepsilon\lambda\big(\alpha^q - (\delta\bar{\alpha})^q\big) = (1-\zeta^{-1}x)^\theta - (1-\zeta x)^\theta \equiv 1-1 \equiv 0 \pmod{q},$$

откуда $\alpha^q - (\delta\bar{\alpha})^q \equiv 0 \pmod{q}$. Согласно лемме 4 последнее сравнение принимает вид $\alpha^q - (\delta\bar{\alpha})^q \equiv 0 \pmod{q^2}$ и, значит,

$$(1-\zeta^{-1}x)^\theta - (1-\zeta x)^\theta = \varepsilon\lambda\big(\alpha^q - (\delta\bar{\alpha})^q\big) \equiv 0 \pmod{q^2}. \tag{22}$$

С другой стороны,

$$(1-\zeta^{-1}x)^\theta \equiv 1-x\sum_{c=1}^{p-1}c\zeta^{-c'} \pmod{q^2}, \qquad (1-\zeta x)^\theta \equiv 1-x\sum_{c=1}^{p-1}c\zeta^{c'} \pmod{q^2}, \tag{23}$$

где мы вновь воспользовались делимостью $q \mid x$. Таким образом, сравнения (22) и (23) означают, что

$$x \sum_{c=1}^{p-1} c(\zeta^{c'} - \zeta^{-c'}) = x \sum_{c=1}^{p-1} c(\zeta^{c'} - \zeta^{p-c'})$$

делится на q^2. Если предположить, что $q^2 \nmid x$, то

$$\beta = \sum_{c=1}^{p-1} c(\zeta^{c'} - \zeta^{p-c'}) \in \mathbb{Z}[\zeta] \tag{24}$$

делится на q. Число β в (24) представлено как многочлен степени не выше $p-1$ от ζ; как следует из леммы 2, делимость $q \mid \beta$ означает, что коэффициент при каждой степени ζ в (24) делится на q. В то же время $c' = 2$ для $c = (p+1)/2$ и $c' = p-2$ для $c = (p-1)/2$, откуда коэффициент при ζ^2 в (24) равен $(p+1)/2 - (p-1)/2 = 1$. Поэтому предположение $q^2 \nmid x$ неверно, т.е. $q^2 \mid x$.

Согласно (16), делимости $q \mid x$ и малой теореме Ферма выполнено

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

откуда в соответствии с леммой 4 получаем $v^q \equiv (-1)^q \pmod{q^2}$. Учитывая теперь установленную делимость $q^2 \mid x$, окончательно находим

$$p^{q-1} \equiv -p^{q-1} v^q = -(x-1) \equiv 1 \pmod{q^2}.$$

Тем самым, соотношения (2) и, следовательно, теорема доказана полностью.

Список литературы

[BS] Боревич З. И., Шафаревич И. Р. Теория чисел. 2 изд. М.: Наука, 1972.

[In] Inkeri K. On Catalan's conjecture // J. Number Theory 1990. V. 34. P. 142–152.

[IR] Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987; Ireland K., Rosen M. A classical introduction to modern number theory. Graduate Texts in Math. V. 87. New York–Heidelberg–Berlin: Springer, 1982.

[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).

[ON] O'Neil T. Improved upper bounds on the exponents in Catalan's equation 1995. (manuscript).

[Sch] Schwarz W. A note on Catalan's equation // Acta Arith. 1995. V. 72. P. 277–279.

[St] Steiner R. Class number bounds and Catalan's equation // Math. Comp. 1998. V. 67. №223. P. 1317–1322.

[Sti] Stickelberger L. Über eine Verallgemeinerung von der Kreistheilung // Math. Ann. 1890. V. 37. P. 321–367.

[Wa] Washington L. C. Introduction to cyclotomic fields. New York: Springer-Verlag 1982.