

4. Теорема Ферма для регулярных простых

Опр 1 Число p -ич. простое, ζ - н.к. из 1 ст. p , $L = \mathbb{Q}[\zeta]$.

Число p наз-ся **регулярным**, если p не делит h_L .
Напоминание: $h_L = |\text{Cl}(L)| = |\text{Id}(\mathcal{O}_L) / \mathfrak{p}(\mathcal{O}_L)|$.

Известно, что для $L = \mathbb{Q}[\zeta]$ $h_L = 1 \Leftrightarrow p \leq 19$.

Теорема (Куммер) Простое число p регулярно $\Leftrightarrow$
числителю всех чисел Бернулли $B_2, B_4, \dots, B_{p-3}$ не делится на p .

Опр 2 Числа Бернулли $B_0, B_1, \dots$ это рациональные коэф.-ы
в разложении $\sum_{n=0}^{N-1} x^n = \frac{1}{x+1} \sum_{k=1}^N \binom{N}{k} B_k x^{k-1}$.

Реккур. ф-ла: $B_0 = 1$, $B_n = -\frac{1}{n+1} \sum_{k=1}^n \binom{n+1}{k+1} B_{n-k}$, $n \in \mathbb{N}$.

Эксп. произвольная ф-ла: $\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$

Св-во: $B_1 = -\frac{1}{2}$ и $B_n = 0$ для всех нечётных $n > 1$.

Немаленькие простые p : 37, 59, 67, 101, ...

Йенсен (1915): Существует бесконечное число простых

Конечно ли число простых чисел? Известно!

Гипотеза (Зигель): $\frac{\text{число пр. } p}{\text{число всех } p} \rightarrow \frac{3}{5}$.

Использование ген. сообр. (критерий Вандивера)

позволяет ген-р т-му Ферма для всех гол.

"Малых" $p < 1\,000\,000 \dots$ Уайлз, 1994 доказ.
Фалтингс, 1983 конечное
реш.

Теорема (Куммер, 1847) Пусть p -простое простое число.

Тогда ур-е $x^p + y^p = z^p$ не имеет нетрив. целых решений.

Первый шаг: p не делит xyz .

• Следует, что $(x, y) = (y, z) = (x, z) = 1$

• Следует, что $p > 3$ (иначе доказано)

• Можно считать, что $p \nmid x - y, x + y$

Пред, что $x \equiv y \equiv \pm z \pmod{p}$. Тогда по малой ф. Ферма

$$z \equiv_p z^p = x^p + y^p \equiv_p x + y \equiv_p \pm 2z \Rightarrow \text{либо } z \equiv_p 0 \text{ либо } 3z \equiv_p 0.$$

Меняя при необх. сл. y на $\pm z$ можно $x \not\equiv_p y$ и т.д.

Ключевая техническая лемма:

Лемма 1 Пусть $a = b_0 + b_1 \zeta + \dots + b_{p-1} \zeta^{p-1} \in nO_L$, где $b_j \in \mathbb{Z}$,
 для некот. $n \in \mathbb{N}$. Если $\exists i \in \{0, \dots, p-1\} : b_i = 0 \Rightarrow n \mid b_j$
 для всех $j \in \{0, \dots, p-1\}$.

1-во: Пусть $b_i = 0$. В лемме Т. 6.2.1 $\{1, \zeta, \dots, \zeta^{i-1}, \zeta^{i+1}, \dots, \zeta^{p-1}\}$ —
 часть базиса кольца O_L (так $\sum_{i=0}^{p-1} \zeta^i = 0$). Поэтому
 $\exists c_j \in \mathbb{Z} : a = nd$ и $d = \sum_{j=0}^{p-1} c_j \zeta^j$ и $c_i = 0$. Из равенств.
 разложения по базису : $b_j = nc_j \quad \forall j = 0, \dots, p-1$ ■

Вернемся к док-ву Теоремы 1 и первом случае:

$$x^p + y^p = (-y)^p \left(\left(\frac{x}{-y} \right)^p - 1 \right) = (-y)^p \prod_{i=0}^{p-1} \left(\frac{x}{-y} - \zeta^i \right) = \prod_{i=0}^{p-1} (x + \zeta^i y) \Rightarrow$$

ищем разложение $\prod_{i=0}^{p-1} (x + \zeta^i y) = z^p \quad (\text{**}).$

Лемма 2 Углерод $(x + \zeta^i y)$ в O_L покрывае в 3. простот.

Д-во: $P = (1 - \zeta)$. - элемент ζ в O_L (лемма 6.2.1, атт 12)

Т.к. $\forall j \quad 1 - \zeta^j = u_j (1 - \zeta)$ где $u_j \in O_L^*$, то $P = (1 - \zeta^j) \forall j$.

Пред, что $Q \trianglelefteq_{\text{пр}} O_L$: $Q \mid (x + \zeta^i y, x + \zeta^j y)$ для $1 \leq i < j \leq p-1$

Тогда $Q \mid ((x + \zeta^i y) - (x + \zeta^j y)) = (\zeta^i y (1 - \zeta^{j-i})) = P \cdot (y)$

$\Rightarrow Q \mid P$ или $Q \mid (y)$. Аналогично, $Q \mid (\zeta^j (x + \zeta^i y) - \zeta^i (x + y \zeta^j))$

$= (\zeta^i x (1 - \zeta^{j-i})) = P \cdot (x) \Rightarrow Q \mid P$ или $Q \mid (x)$. Но $(x, y) = 1$

$\Rightarrow Q \mid P \Rightarrow Q = P$, но тогда $P = Q \ni x + \zeta^i y = x + y + \underbrace{(\zeta^i - 1)}_P y$

$\Rightarrow x + y \in P$. Но $P \cap \mathbb{Z} = (p) \Rightarrow p \mid x + y$, что невозможно.
 или $Q \mid (xy) \Rightarrow 1 - (xy) = ax + by \in Q, a, b \in \mathbb{Z}$, что невозможно.

В силу ОТА для идеалов в регулярн. кольцах, ф-н (**)
и леммы 2 имеем $(x + \xi^{-1}y) = Q_i^p$, $Q_i \in \mathcal{O}_L \forall i=0, \dots, p-1$

В группе $\text{Cl}(\mathcal{O}_L)$ имеем $\overline{Q_i^p} = \overline{Q_i}^p = \overline{(x + \xi^{-1}y)} = \overline{1}$.

Т.к. p -регулярное $\Rightarrow p \nmid |\text{Cl}(\mathcal{O}_L)| \Rightarrow \overline{Q_i} = \overline{1} \Rightarrow$ ← по л. 4.3.8

для всех $i=0, \dots, p-1$ $Q_i = (\alpha_i)$ для $\alpha_i \in \mathcal{O}_L$. Тогда $d := d_{\mathbb{A}}$.

Тогда $x + \xi y = u \alpha^p$ для $u \in \mathcal{O}_L^*$. В силу Т. 6.2.2 $u = \xi^r v$,
где $v \in L^+ = \mathbb{Q}[\xi + \xi^{-1}/2] \subset \mathbb{R}$. По лемме 6.3.8 (АНТ 13)

$\exists b \in \mathbb{Z} : \alpha^p \equiv b \pmod{p \mathcal{O}_L}$. Рассмотрим

$$x + \xi y = u \alpha^p \equiv_{p \mathcal{O}_L} \xi^r v b, \quad x + \xi^{-1} y = \overline{x + \xi y} \equiv_{p \mathcal{O}_L} \xi^{-r} v b \Rightarrow$$

$$v b \equiv_{p \mathcal{O}_L} \xi^{-r} (x + \xi y) \equiv_{p \mathcal{O}_L} \xi^r (x + \xi^{-1} y) \Rightarrow$$

$$(\ast\ast\ast) \quad x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0 \pmod{p \mathcal{O}_L}.$$

Напомним, что $p \geq 5$. Поэтому, если $1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ попарно различны, то по ключевой лемме 1, $p \nmid x$ и $p \nmid y$, противоречие с $\epsilon(x, y) = 1$. Остается рассмотреть след.

Возм.-сл

a) $1 = \zeta^{2r} \Rightarrow \zeta y - \zeta^{2r-1} y \equiv_{p \mathcal{O}_L} 0$. По лемме 1 $p \nmid y$, против.

b) $\zeta = \zeta^{2r-1} \Rightarrow x - \zeta^{2r} x \equiv_{p \mathcal{O}_L} 0$. По лемме 1 $p \nmid x$, против.

б) $1 = \zeta^{2r-1}$ и $\zeta = \zeta^{2r} \Rightarrow (x - y)(1 - \zeta)_{p \mathcal{O}_L} \equiv 0 \Rightarrow p \mid x - y$,

противоречие (см. начало доказательства). 

Второй случай: $p \nmid xyz$ в (*).

• Можно считать, что $p \mid z$ и $z = p^k z_0$, где $(p, z_0) = 1$.
 $= (p, x) = (p', y) = 1$.

Ключевая лемма (без док-ва)

Лемма 3 (Куммер) Пусть для $u \in \mathcal{O}_L^*$ найдется $b \in \mathbb{Z}$:

$$u \equiv b \pmod{p\mathcal{O}_L}. \text{ Тогда } \exists v \in \mathcal{O}_L^* : u = v^p.$$

Зам1 Две во все p -ад. числа см. например, гл. 5, § 6 в Боревице-Шфаревиче.

Зам2 Очевидно верно для $p=3$, т.к. $\mathcal{O}_L^*$ конечно в этом сл. и легко проверить, что $u \equiv b \pmod{p\mathcal{O}_L} \Rightarrow u = \pm 1$.

В силу леммы 6.2.1 (ANT12) в кольце $\mathcal{O}_L$ $p = P^{p-1}$, $P = (1-\zeta)$.

$$(*)4) \quad x^P + y^P = P^m (z_0)^P = u(1-\zeta)^{pm} (z_0)^P, \text{ где } u \in \mathcal{O}_L^*, m = k(p-1).$$

Тогда от противоположного нам есть $x, y, z_0 \in O_L$ такое, что $(x), (y), (z_0)$ вз. прости с P , $u \in O_L^\times$ и $m \geq 1$. Выберем среди них такое, что m - наименьшее н.ст. число (много есть случаев). Как и в первом случае:

$$(*)5) \quad \prod_{i=0}^{p-1} (x + \zeta^i y) = P^m (z_0)^P.$$

Из ОПА след. извлеч. $\Rightarrow \exists j \in \{0, \dots, p-1\} : P \mid (x + \zeta^j y)$.

Но $P = (1 - \zeta^{j-i}) \Rightarrow x + \zeta^i y \equiv_P x + \zeta^j y \Rightarrow P \mid (x + \zeta^i y) \forall i$.

Если $x + \zeta^i y \equiv_P (x + \zeta^j y) \Rightarrow \zeta^i y (1 - \zeta^{j-i}) = \zeta^j y P \equiv_P 0$

$\Rightarrow P \mid (y)$ при $j \neq_p i$, противоречие. Значит, числа

$\frac{x + \zeta^i y}{1 - \zeta}$, $i = 0, \dots, p-1$, попарно не сравнимы по модулю P .

По лемме 6.2.1 $IV(P) = N_{\mathbb{Q}}(1-\zeta) = p = |\mathbb{Z}/p\mathbb{Z}| = |\mathbb{O}_L/P|$
 м.б. $\exists$ $f(P/p\mathbb{Z}) = 1$

Сл-но, эти p чисел задают все см. классы в $\mathbb{O}_L/P$.
 В частности, $\exists j \in \{0, \dots, p-1\} : \frac{x + \zeta^j y}{1-\zeta} \in P$. Заменяя
 y на $\zeta^j y$, можем считать, что $x+y \in P$ и $x + \zeta^i y \in P \setminus P^2$
 для $i = 1, \dots, p-1$. В частности, левая часть (*) делится
 на $P^{p+1} \Rightarrow m \geq 2$ в (*) и (*').

Обозначим через $J = \text{НОД}(f(x), (y)) \leq \mathbb{O}_L$. Т.к. $(P, (x)) = 1$
 $\Rightarrow P \nmid J$. Значит, $\exists Q_0, \dots, Q_{p-1} \leq \mathbb{O}_L$ такие, что
 $(x+y) = P^{p(m-1)+1} J Q_0$ и $(x + \zeta^j y) = P^j Q_j, j = 1 \dots p-1$.

Заметим, что $Q_0, \dots, Q_{p-1}$ попарно вз. взаимно. Укажем $\exists i < j$ и

$$\# I \leq O_L : I \mid Q_i \cup Q_j \Rightarrow P \cap I \mid (x + z^i y) \cup (x + z^j y).$$

Тогда $y(1 - z^{j-i}), x(1 - z^{j-i}) \in P \cap I \Rightarrow x, y \in P \cap I$, что противоречит выбору $y = \min (W_1(y))$. Показавшаяся $\ell \in I$,

$\cap^P \cap^{P^m} Q_0, \dots, Q_{p-1} = \cap^{P^m} (z_0)^P$. Из вз. простых Q_i и означ. разности ℓ и $\ell \in O_L$, семей $Q_i = R_i^P$ для некот. идеалов $R_i \in O_L$ для всех $i = 0, \dots, p-1$. Из $\cap^{P^m} (x+y) = \cap^{P^{(m-1)+1}} \cap R_0^P$ и $(x+z^i y) = \cap R_i^P, i=1, \dots, p-1$, введем рав-во в больших идеалах:

$$(*)6) (x+z^i y) \cap^{P^{(m-1)+1}} = (x+y) (R_i/R_0)^P, i=1, \dots, p-1.$$

$$\Rightarrow (R_i/R_0)^P \text{ — идеалы больших идеалов} \Rightarrow R_i/R_0 \text{ тоже!}$$

$\forall i=1, \dots, p-1.$

Тогда образом, $\exists \alpha_i, \beta_i \in \mathcal{O}_L, i=1 \dots p-1, R_i/R_0 = (\alpha_i/\beta_i)$

Т.е. R_i и R_0 л.з. выраж. в $\mathbb{P}$, т.е. можно ч., что $\alpha_i, \beta_i \notin \mathbb{P} \forall i$.

Перемножив (*)

$$(*) (x + \frac{1}{3}y)(1-\frac{1}{3})^{p(m-1)} = u_i(x+y)(\alpha_i/\beta_i)^p, u_i \in \mathcal{O}_L^*, i=1 \dots p-1$$

Умножив раз-во $(x + \frac{1}{3}y)(1+\frac{1}{3}) - (x + \frac{1}{3}^2y) = \frac{1}{3}(x+y)$, получаем

(*) при $i=2$ из (*) при $i=$, умк. на $(1+\frac{1}{3})$. Получаем

$$u_1(1+\frac{1}{3})(x+y)(\alpha_1/\beta_1)^p - u_2(x+y)(\alpha_2/\beta_2)^p = \frac{1}{3}(x+y)(1-\frac{1}{3})^{p(m-1)} \quad \text{отсюда}$$

$$(\alpha_1/\beta_2)^p - \frac{u_2}{u_1(1+\frac{1}{3})}(\alpha_2/\beta_1)^p = \frac{1}{u_1(1+\frac{1}{3})}(1-\frac{1}{3})^{p(m-1)}(\beta_1/\beta_2)^p.$$

Обозначим $\alpha = \alpha_1\beta_2, \beta = \alpha_2\beta_1, \gamma = \beta_1\beta_2$. Т.е. $(1+\frac{1}{3}) = \frac{1-\frac{1}{3}^2}{1-\frac{1}{3}} \in \mathcal{O}_L^*$,

можем переписать последнее рав-во так:

$$(*)8) \quad \alpha^P + \varepsilon \beta^P = \varepsilon' (1 - \xi)^{P(m-1)} \gamma^P, \text{ где } \varepsilon, \varepsilon' \in O_L^\times, \alpha, \beta, \gamma \in O_L \setminus P.$$

$$\text{Поскольку } m \geq 2 \Rightarrow P(m-1) \geq P \Rightarrow \alpha^P + \varepsilon \beta^P \equiv_{pO_L} 0.$$

Так $(\beta) \in P$ вл. условие, то $(\beta) \in P^{\dagger+} = pO_L$ вл. условие $\Rightarrow$

$$\exists \beta' \in O_L : \beta \beta' \equiv_{pO_L} 1. \text{ Поэтому } \varepsilon \equiv_{pO_L} (-\alpha \beta')^P \equiv_{pO_L} \zeta \in \mathbb{Z},$$

где восп. сравнение вын-ств в силу лемм 6.3.8 (АНТ12).

Применяя лемму 3, получаем $\varepsilon \equiv \eta^P$ нек. $\eta \in O_L^\times$.

$$(*)8) \Rightarrow \alpha^P + (\eta \beta)^P = \varepsilon' (1 - \xi)^{P(m-1)} \gamma^P, \text{ совн. с } (*4),$$

но с меньшим $m' = m - 1$, что противоречит выбору m □

Упр 1 D-ре лемма Вурмера (лемма 3) годо $p=5$.

Указ: Пусть $\zeta = e^{\frac{2\pi i}{5}}$ - кор. к. 5-ой ст. и $\zeta \neq 1$, $L = \mathbb{Q}[\zeta]$.

а) D-р, что $\omega = \zeta + \zeta^{-1} = \frac{\sqrt{5}-1}{2}$ - функцион. элемент в $\mathcal{O}_L$,

т.е. $\mathcal{O}_L^* = \{ \pm \zeta^k \omega^n \mid k, n \in \mathbb{Z} \}$.

б) если $u \in \mathcal{O}_L^*$: $u \equiv_{5\mathcal{O}_L} c \in \mathbb{Z} \Rightarrow u = \pm \omega^n \in L^* = \mathbb{Q}[\omega] \subseteq \mathbb{R}$

в) $\pm \omega^n \equiv_{5\mathcal{O}_L} c \in \mathbb{Z} \Leftrightarrow 5 \mid n$.

Упр 2 (Пробл. Софи. Мермен) Пусть p и $q=2p+1$ - простые числа. Если $x^p + y^p + z^p = 0 \Rightarrow p \mid xyz$.

Указ: а) если $x \not\equiv 0 \pmod{q} \Rightarrow x^p \equiv \pm 1 \pmod{q}$

б) $x^p + y^p + z^p = 0 \Rightarrow q \mid xyz$

в) Если-то раз. на буги - $x^p = y^p + z^p = (y+z)(y^{p-1} - y^{p-2}z + \dots - yz^{p-2} + z^{p-1}) \dots$