4. Теорема Ферма для регулярных простых

Опр 1 Пусть p-нч. простое, ξ – п.к. из 1 сб. p, $L = \mathbb{Q}[\xi]$.

Число p наз-ся регулярным, если p не делит h_L.

Напоминание: $h_L = |Cl(L)| = |Id(O_L)/P(O_L)|$.

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

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

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

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

Экспон. производящая ф-ция: $\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$

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

Нерегулярные иррегул. p: 37, 59, 67, 101, ...

Йенсен (1915): Существует бесконечно много иррегул. простых

Конечно ли число регул. простых неизвестно!

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

Использование ЭВМ (критерий Вандиверa) позволяет ЭВМ-ным тестом Ферма для всех доступных "малых" $p < 1\,000\,000$...

Уайлз, 1994 окончательное доказательство Великой теоремы Ферма

Фалтингс, 1983 конечность числа реш. урав.

гипотеза Мордела

Теорема (Куммер, 1847) Пусть p — нечётное простое число. Тогда у ур-я $x^p + y^p = z^p$ $(*)$ не имеет нетрив. целых решений.

- Считаем, что $(x, y) = (y, z) = (x, z) = 1$
- Считаем, что $p > 3$ (иначе зок-м).

Первый случай: p не делит ни xyz.

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

Пред, что $x \equiv y \equiv \pm z \pmod p$. Тогда по малой т. 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. сам y на $\pm z$ имеем $x \not\equiv_p \pm y$ ч.т.д.

Ключевая техническая лемма:

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

1-вои: Пусть $b_i = 0$. В силу Т. 6.2.1 $1, \xi, \dots \xi^{i-1}, \xi^{i+1}, \dots \xi^{p-1}$ — целый базис кольца O_L (т.к. $\sum_{i=0}^{p-1} \xi^i = 0$). Поэтому $\exists c_j \in \mathbb{Z}$: $a = \pi d$ и $d = \sum_{j=0}^{p-1} c_j \xi^j$ и $c_i = 0$. Из единств. разложения по базису: $b_j = \pi c_j \quad \forall j = 0, \dots p-1$ ∎

Вернемся к док-ву Теоремы в первом случае:

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

Целое решение $\prod_{i=0}^{p-1}(x + \xi^i y) = z^p$ (**). в O_L!

Лемма 2 Идеал $(x+\xi^i y)$ в O_L порождён $\mathfrak{B}$. простой.

Д-во: $P=(1-\xi)$ - простой идеал в O_L (лемма 6.2.1, АЛТ12)

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

Пусть, что $Q \trianglelefteq_{\text{прос}} O_L$: $Q \mid (x+\xi^i y, x+\xi^j y)$ для $1 \le i<j \le p-1$

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

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

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

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

$\Rightarrow x+y \in P$. Но $P \cap \mathbb{Z} = (p) \Rightarrow p \mid x+y$, противоречие

или $Q \mid (x,y) \Rightarrow 1 = (x,y) = ax+by \in Q$, $a,b \in \mathbb{Z}$, противоречие.

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

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

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

для всех $i = 0,\dots p-1$ $Q_i = (\alpha_i)$ для $\alpha_i \in \mathcal{O}_L$. Пусть $\alpha := \alpha_1$.

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

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

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

$(***)$ $x + \xi y - \xi^{2r} x - \xi^{2r-1} y \equiv 0 \pmod{p O_L}$.

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

а) $1 = \xi^{2r} \Rightarrow \xi y - \xi^{2r-1} y \equiv_{p O_L} 0$. По лемме 1 $p \mid y$, противор.

б) $\xi = \xi^{2r-1} \Rightarrow x - \xi^{2r} x \equiv_{p_L} O_L$. По лемме 1 $p \mid x$, противор.

в) $1 = \xi^{2r-1}$ и $\xi = \xi^{2r} \Rightarrow (x-y)(1-\xi) \underset{p O_L}{\equiv} 0 \Rightarrow p \mid x-y$, противоречие (см. начало док-ва). ∎

Второй случай: $p \mid xyz$ в (*).

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

Ключевая лемма (без док-ва)

Лемма 3 (Куммер) Пусть для $u \in O_L^*$ найдется $b \in \mathbb{Z}$: $u \equiv b \pmod{pO_L}$. Тогда $\exists v \in O_L^*$: $u = v^p$.

Зам 1 Док-во см. p-ад. числа см. например, гл. 5, §6 в Боревич-Шафаревич.

Зам 2 Очевидно вып-ся для $p = 3$, т.к. O_L^* конечна в этом сл. и легко понять, что $u \equiv b \pmod{pO_L} \Rightarrow u = \pm 1$ (см. упр 1 для $p = 5$).

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

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

Пусть от противного нашлись $x, y, z_0 \in O_L$ такие, что $(x), (y), (z_0)$ вз. прост с $\mathfrak{P}$, $u \in O_L^*$ и $m \geq 1$. Выберем среди них такие, что m - наименьшее нат. число. (метод беск. спуска). Как и в первом случае:

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

Из ОТА для идеалов $\Rightarrow \exists j \in \{0, \dots, p-1\}: \mathfrak{P} \mid (x + \xi^j y)$.

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

Если $x + \xi^i y \equiv_{\mathfrak{P}^2} (x + \xi^j y) \Rightarrow \xi^i y (1 - \xi^{j-i}) = \xi^i y \mathfrak{P} \equiv_{\mathfrak{P}^2} 0$

$\Rightarrow \mathfrak{P} \mid (y)$ при $j \neq_p i$, противоречие. Значит, числа $\frac{x + \xi^i y}{1 - \xi}$, $i = 0, \dots, p-2$, попарно не сравнимы по модулю $\mathfrak{P}$.

По лемме 6.2.1 $\prod N(P) = N_{L/\mathbb{Q}}(1-\xi) = p = |\mathbb{Z}/p\mathbb{Z}| = |O_L/P|$

св-во $f(P/p\mathbb{Z}) = 1$

Св-но, эти p чисел задают все см. классы в O_L/P.

В частности, $\exists j \in \{0,\dots p-1\}$: $\frac{x+\xi^j y}{1-\xi} \in P$. Заменяя y на $\xi^j y$, можем считать, что $x+y \in P^2$ и $x+\xi^i y \in P \setminus P^2$ для $i = 1,\dots p-1$. В частности, левая часть (*5) делится на $P^{p+1} \Rightarrow m \geq 2$ в (*5) и (*4).

Обозначим через $J = \text{Hod}(x)_1(y) \trianglelefteq O_L$. Т.к. $(P, (x)) = 1$ $\Rightarrow P \nmid J$. Значит, $\exists Q_0,\dots Q_{p-1} \trianglelefteq O_L$ такие, что $(x+y) = P^{p(m-1)+1} J Q_0$ и $(x+\xi^i y) = PJQ_i$, $i = 1 \dots p-1$.

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

$\forall I \trianglelefteq O_L : I \mid Q_i$ и $Q_j \Rightarrow PJI \mid (x+\xi^i y)$ и $(x+\xi^j y)$.

Тогда $y(1-\xi^{j-i}), x(1-\xi^{j-i}) \in PJI \Rightarrow x, y \in JI$, что противоречит выбору $y = \min(v_1(y))$. Подставляя в (5),

$y^p P^{pm} Q_0 \dots Q_{p-1} = P^{pm}(z_0)^p$. Из вз. простоты Q_i и однозн. разложения на эл-ты O_L, имеем $Q_i = R_i^p$ для некот. идеалов $R_i \trianglelefteq O_L$ для всех $i = 0, \dots p-1$. Из пр-ия $(x+y) = P^{p(m-1)+1} J R_0^p$ и $(x+\xi^i y) = PJ R_i^p$, $i = 1, \dots p-1$, выводим рав-во дробных идеалов:

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

$\Rightarrow (R_i/R_0)^p$ – целые дробные идеалы $\Rightarrow R_i/R_0$ тоже! $\forall i = 1 \dots p-1$.

$p \nmid h_L$

Таким образом, $\exists \alpha_i, \beta_i \in O_L$, $i=1\dots p-1$: $R_i/R_0 = (\alpha_i/\beta_i)$

Т.к. R_i и R_0 вз. прост с P, то можно ч., что $\alpha_i, \beta_i \notin P \ \forall i$.

Перепишем (*6)

(*7) $(x+\zeta y)(1-\zeta)^{p(m-1)} = u_i (x+y)(\alpha_i/\beta_i)^p$, $u_i \in O_L^*$, $i=1\dots p-1$

Используя рав-во $(x+\zeta y)(1+\zeta) - (x+\zeta^2 y) = \zeta(x+y)$, вычтем (*7) при $i=2$ из (*7) при $i=1$, ум. на $(1+\zeta)$. Получаем

$u_1(1+\zeta)(x+y)(\alpha_1/\beta_1)^p - u_2(x+y)(\alpha_2/\beta_2)^p = \zeta(x+y)(1-\zeta)^{p(m-1)}$. Отсюда

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

Обозначим $\alpha = \alpha_1\beta_2$, $\beta = \alpha_2\beta_1$, $\gamma = \beta_1\beta_2$. Т.к. $(1+\zeta) = \frac{1-\zeta^2}{1-\zeta} \in O_L^*$,

можно переписать последнее рав-во так:

(*8) $\alpha^p + \varepsilon\beta^p = \varepsilon'(1-\xi)^{p(m-1)}\gamma^p$, где $\varepsilon, \varepsilon' \in O_L^*$, а $\alpha, \beta, \gamma \in \mathfrak{P}_L|p$.

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

Т.к. (β) и I вз. просты, то (β) и $I^{p-1} = p\mathfrak{P}_L$ вз. просты $\Rightarrow$

$\exists \beta' \in O_L$: $\beta\beta' \equiv_{p\mathfrak{P}_L} 1$. Поэтому $\varepsilon \equiv_{p\mathfrak{P}_L} (-\alpha\beta')^p \equiv_{p\mathfrak{P}_L} c \in \mathbb{Z}$,

где посл. сравнение вып-ся в силу леммы 6.3.8 (ANT13).

Применяя лемму 3, получаем $\varepsilon \equiv \eta^p$ для нек. $\eta \in O_L^*$.

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

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

Упр 1 Д-ре лемму Кумнера (лемма 3) для $p = 5$.

Указ: пусть $\zeta = e^{\frac{2\pi i}{5}}$ – пр. к. 5-ой ст. из 1, $\mathcal{O}_L = \mathbb{Q}[\zeta]$.

а) Д-ть, что $\omega = \zeta + \zeta^{-1} = \frac{\sqrt{5}-1}{2}$ – фундамент. единица 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 (Прок Софи. Жермен) 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) Иссл-ть рав-ва Ферма – $x^p = y^p + z^p = (y+z)(y^{p-1} - y^{p-2}z + \dots - yz^{p-2} + z^p) \dots$