3. Теорема Ферма для показателя 3

Т. 1 (Эйлер, 1770) Ур-е $x^3+y^3=z^3$ (*)
не имеет ненулевого решения в целых числах.

Напоминание: $\omega=\frac{-1+\sqrt{3}i}{2}$ – прим. корень 3-ей ст. из 1.

Лемма 1 Пусть $L=\mathbb{Q}[\omega]$. Тогда
1) $\mathcal{O}_L=\mathbb{Z}[\omega]=\{a+b\omega \mid a,b\in\mathbb{Z}\}$ факториально. и $=\mathcal{PID}$.
2) $\mathcal{O}_L^*=\{\pm 1,\pm\omega,\pm\omega^2\}$ – мн-во корней 6-ой ст. из 1.
3) $\lambda=1-\omega$ – простой эл-т в $\mathcal{O}_L$ и $3\mathcal{O}_L=P^2$, где $P=(\lambda)$.

Д-во: См. Т-мы 1, 2 и лемму 1 из §2 (ANT 12) ▯

Далее, от прот. предположим, что (x,y,z) – решение ур-я (*).
(0,0,0)

- Можно считать, что $НОД(x,y,z)=1$

Лемма 2 $3 \mid xyz$.

Д-во: Если $3 \nmid x$, то легко проверить, что $x^3 \equiv \pm 1 \pmod 9$.
Рассм. теперь $(*)$ по $\mathrm{mod}\ 9$ имеем $3 \mid xyz$ ▣

- Можно считать, что $3 \mid z$, $3 \nmid xy$ и ур-е $(*)$ перепишется в виде: $(**)$ $x^3+y^3=(3^m z_0)^3$, где $3 \nmid xyz_0$
- Считаем, m – наим. возм. нат. число, для кот. $(**)$ имеет решение (x,y,z_0).

Лемма 3 $\lambda \nmid xyz_0$

Д-во: Т.к $P=(\lambda)$ встречается в разл. $3O_L = P^2$
$\Rightarrow P \cap \mathbb{Z} = 3\mathbb{Z}$. Если $\lambda \mid xyz_0$, то λ делит один

из сопр-ей, т.к. λ – простой эл-т. Например, $\lambda \mid x$
$\Rightarrow x \in P \cap \mathbb{Z} = 3\mathbb{Z} \Rightarrow 3 \mid x$, противоречие ▯

Лемма 4 В $\mathcal{O}_L$ имеем $x^3+y^3 = (x+y)(x+\omega y)(x+\omega^2 y)$ ▯

Д-во: Для простого p и первообр. корня ξ p-ой ст. из 1
имеем $t^{p-1} = \prod_{i=0}^{p-1} (t-\xi^i)$. Взяв $p=3$ и подставив
$t = -\frac{x}{y}$, получаем требуемое ▯

Лемма 5 $x+\omega^i y \equiv x+\omega^j y \ (\lambda)$. В частности, $\forall i$
$\lambda \mid x+\omega^i y$.

Д-во: $1-\omega^{j-i} \equiv 0 \ (\lambda) \Rightarrow \omega^i y \equiv \omega^j y \ (\lambda) \Rightarrow$ **Равенство**
по $\lambda \mid 3 \mid (3^m z_0)^3 \Rightarrow \lambda \mid x^3+y^3 = \prod_{i=0}^{2} (x+y\omega^i)$ ▯

По п.3 леммы 1 $3 = \varepsilon' \cdot \lambda^2$ для некот. $\varepsilon' \in O_L^*$.

(на самом деле, $3 = \lambda^2 \cdot (-\omega^2)$ как легко проверить)

Лемма 6 $x + \omega^i y \not\equiv x + \omega^j y \ (\lambda^2)$, если $i \not\equiv j \ (3)$.

Д-во: Иначе $y(1-\omega^{i-j}) \equiv 0 \ (\lambda^2) \Rightarrow \lambda \mid y$ против ▣

Меняя при необходимости y на ωy или $\omega^2 y$,

• Считаем, что $\lambda^2 \mid x+y$, но $\lambda^2 \nmid x + \omega^i y$, $i = 1, 2$.

Лемма 7 $(x + \omega^i y, x + \omega^j y) = (\lambda)$ при $i \not\equiv j$.

Д-во: Пусть π - простой делитель O_L. Если $\pi \mid x+y$ и $\pi \mid x + \omega y \Rightarrow \pi \mid \lambda y \Rightarrow$ либо $\pi = \lambda$, либо $\pi \mid y \Rightarrow \pi \mid x$, против. т.к. $(x, y) = 1$. Аналогично для ост. случаев. ▣

Методом Ферма (методом бесконечного спуска) мы покажем, что ур-е (***): $x^3+y^3=\varepsilon\lambda^{3n}z_0^3$ не имеет решений в O_L таких, что $n\in\mathbb{N}$ x,y,z_0 вз. λ и $\varepsilon\in O_L^*$. Именно сначала, предположив, что такое решение есть, мы покажем, что есть решение и для $n'<n$.

В силу лемм 5-7 и факторизуемости кольца O_L имеем

$$\begin{aligned} x+y &= \varepsilon_1\alpha_1^3\lambda^{3n-2},\\ x+\omega y &= \varepsilon_2\alpha_2^3\lambda, \qquad (*4)\\ x+\omega^2 y &= \varepsilon_3\alpha_3^3\lambda, \end{aligned}$$

где $\varepsilon_i\in O_L^*$, $\lambda\nmid\alpha_i$, $(\alpha_i,\alpha_j)=1$, $i,j\in\{1,2,3\}$, $i\neq j$.

Умножая 2-е рав-во на ω, 3-е рав-во на ω^2 и складывая имеем (учитывая $1+\omega+\omega^2=0$):

$$0=\varepsilon_1\alpha_1^3\lambda^{3n-2}+\omega\varepsilon_2\alpha_2^3\lambda+\omega^2\varepsilon_3\alpha_3^3\lambda \qquad (*5)$$

Делим $(*5)$ на λ:

$$0=\varepsilon_1\alpha^3\lambda^{3(n-1)}+\omega\varepsilon_2\alpha_2^3+\omega^2\varepsilon_3\alpha_3^3. \qquad (*6)$$

Полагая $z_1=\alpha_1\lambda^{n-1}$, $x_1=\alpha_2$, $y_1=\alpha_3$, перепишем $(*6)$ в виде:

$$x_1^3+u_1y_1^3=u_2z_1^3, \text{ где } u_1,u_2\in O_L^* \qquad (*7)$$

Заметим, что $n=2m\geq 2 \Rightarrow$ по модулю $(\lambda^2)=(3)$ (см. в тихе)

$\pm 1\pm u_1\equiv 0(\lambda^2)$. Перебирая все знаки u_1,

получаем $z_1 = \pm 1$. Меняя при необходимости y_1 на $-y_1$, получаем соотношение:

$$x_1^3 + y_1^3 = \varepsilon z_1^3,$$

где $\varepsilon \in O_L^*$, а x_1, y_1, но $z_1 = \lambda^{3(n-1)} z_0'$, $\lambda \nmid z_0'$, противоречие ▨

Лемма 8 Если $L = \mathbb{Q}[\xi]$, где ξ – п.к. p-ой степени, то $\forall a \in O_L \ \exists b \in \mathbb{Z} : a^p \equiv b \ (pO_L)$.

Д-во: В силу т. 6.1.1 (АЧТ12): $a = b_0 + b_1\xi + \dots + b_{p-2}\xi^{p-2}$, $b_i \in \mathbb{Z}$. Тогда $a^p \equiv_{pO_L} b_0^p + (b_1\xi)^p + \dots + (b_{p-2}\xi^{p-2})^p =$ ($\xi^p = 1$)

$= b_0^p + b_1^p + \dots + (b_{p-2})^p \in \mathbb{Z}$. ▨