

### 3. Теорема Ферма год иона 3


Т. 1 (Эйлер, 1770) Ур-е  $x^3 + y^3 = z^3$  (\*)

не имеет ненулевого решения в целых числах.

Нормальные:  $\omega = \frac{-1 + \sqrt{3}i}{2}$  - куб. 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.  $\omega = \sqrt{-3}$ .
- 2)  $\mathcal{O}_L^\times = \{ \pm 1, \pm \omega, \pm \omega^2 \}$  - все корни 6-ой ст. из 1.
- 3)  $\lambda = 1 - \omega$  - простейший делитель  $\mathcal{O}_L$  и  $3\mathcal{O}_L = \lambda^2$ , где  $P = (\lambda)$ .

Д-во: см. Т-ем 1, 2 и лемму 1 и 3 § 2 (ANT 12) 

Далее, от прост. предположения, что  $(x, y, z)$  - решение  
ур-я (\*).

• Можно считать, что  $\text{НОД}(x, y, z) = 1$

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 мод. 9 и если  $3 \mid xyz$   $\square$

• Можно считать, что  $3 \mid z$ ,  $3 \nmid xy$  и ур. (\*) переписать в виде: (\*\*)  $x^3 + y^3 = (3^m z_0)^3$ , где  $3 \nmid xy z_0$ .

• Считаем,  $m$  - наим. возм. кат. число, гд. кр. (\*\*\*) имеет решение  $(x, y, z_0)$ .

Лемма 3  $\lambda \nmid xyz_0$ .

Д-во: Т.к.  $P = (\lambda)$  вращается в ДАЗЛ.  $\mathbb{Z}_L = P^2$

$\Rightarrow P \cap \mathcal{H} = 3\mathcal{H}$ . Если  $\lambda \mid xyz_0$ , то  $\lambda$  делит один

из сокращен, так  $\lambda$  - простое  $\mathbb{Z} = \mathbb{Z}$ . Например,  $\lambda | x$   
 $\Rightarrow x \in \mathbb{P} \cap \mathbb{Z} = 3\mathbb{Z} \Rightarrow 3 | x$ , условие  $\square$

Лемма 4 В  $\mathbb{Q}_\zeta$  имеем  $x^3 + y^3 = (x+y)(x+\omega y)(x+\omega^2 y)$ .  $\square$

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

Лемма 5  $x + \omega^i y \equiv x + \omega^j y \pmod{\lambda}$ . В частности,  $\forall i$   
 $\lambda | x + \omega^i y$ .

$\Delta$ -во:  $1 - \omega^{j-i} \equiv 0 \pmod{\lambda} \Rightarrow \omega^i y \equiv \omega^j y \pmod{\lambda} \Rightarrow$  равенство  
 $\text{но } \lambda | 3 | (3^m z_0)^3 \Rightarrow \lambda | x^3 - y^3 = \prod_{i=0}^2 (x + y \omega^i)$   $\square$

• По п.3 леммы 1  $\exists = \xi' \cdot \lambda^2$  где некот.  $\xi' \in \mathcal{O}_L^*$ .

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

Лемма 6  $x + \omega^i y \neq x + \omega^j y \pmod{\lambda^2}$ , если  $i \neq j \pmod{3}$ .

Д-во: Укаже  $y \pmod{1 - \omega^i} \equiv 0 \pmod{\lambda^2} \Rightarrow \lambda \mid y$  против  $\square$

меньше при необходимости  $y$  не  $\omega y$  или  $\omega^2 y$   $\lambda^k \mid \binom{m}{3}_{\mathbb{Z}_6}$

• Считаю, что  $\lambda^2 \mid x + y$ , но  $\lambda^2 \nmid x + \omega^i y$ ,  $i=1, 2$ .  $\left. \begin{aligned} &= x^2 + y^2 \\ &\Rightarrow k \geq 6. \end{aligned} \right\}$

Лемма 7  $(x + \omega^i y, x + \omega^j y) = (x)$  при  $i \neq j \pmod{3}$

Д-во Пусть  $\pi$  - простой делитель кольца  $\mathcal{O}_L$ . 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., с.ч.  $(x, y) = \mathfrak{f}$ . Аналогично для ост. случаев.  $\square$

Зам.  $\pi \mathcal{O}_L \cap \mathfrak{f} \stackrel{\text{чрп}}{\neq} \mathfrak{f} \Rightarrow \pi \mathcal{O}_L \cap \mathfrak{f} \neq \mathfrak{p} \mathfrak{f}$ . Если  $\pi \mid x$  и  $\pi \mid y \Rightarrow \mathfrak{p} \mid (x, y)$   
противоположно.

Методом Ферма (методом беск. спуска) мы показали,  
что ур.  $e$  (\*\*\*) :  $x^3 + y^3 = \varepsilon \lambda^{3n} z_0^3$

не имеет решений в  $\mathcal{O}_L$  таких, что  $n \in \mathbb{N}$

$x, y, z_0$  взаимно просты и  $\varepsilon \in \mathcal{O}_L^\times$ . Упрости систему,

предположив, что такое решение есть, мы

покажем, что есть решение и для  $n' < n$ .

В силу лемм 5-7 и факторизации в кольце  $\mathcal{O}_L$  имеем

$$x + y = \varepsilon_1 d_1^3 \lambda^{3n-2},$$

$$x + \omega y = \varepsilon_2 d_2^3 \lambda, \quad (**)$$

$$x + \omega^2 y = \varepsilon_3 d_3^3 \lambda,$$

где  $\varepsilon_i \in \mathcal{O}_L^\times$ ,  $\lambda \nmid d_i$ ,  $(d_i, d_j) = 1$ ,  $i, j \in \{1, 2, 3\}$ ,  $i \neq j$ .

Умножимся 2-е рав-во на  $\omega$ , 3-е рав-во на  $\omega^2$  и сложим все  
 умеем (учитывая  $1 + \omega + \omega^2 = 0$ ):

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

Делим (+5) на  $\lambda$ :

$$0 = \varepsilon_1 \alpha_1^3 \lambda^{3(n-1)} + \omega \varepsilon_2 \alpha_2^3 + \omega^2 \varepsilon_3 \alpha_3^3. \quad (+6)$$

Положим  $z_1 = \alpha_1 \lambda^{n-1}$ ,  $x_1 = \alpha_2$ ,  $y_1 = \alpha_3$ , перемножим

(+6) в виде:

$$x_1^3 + u_1 y_1^3 = u_2 z_1^3, \text{ где } u_1, u_2 \in \mathcal{O}_L^* \quad (+7)$$

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

$\pm 1 \pm u_1 \equiv 0 \pmod{\lambda^2}$ . Проверим, возможны ли значения  $u_1$ ,

получаем  $x_1 = \pm z_1$ . Меняя при необходимости  $y_1$  на  $-y_1$ ,

получаем соотношение:

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

где  $\varepsilon \in \mathcal{O}_L^\times$ ,  $x \nmid x_1, y_1$ , но  $z_1 = \lambda^{3(n-1)} z_0'$ ,  $\lambda \nmid z_0'$ ,  
противоречие  $\blacksquare$

Лемма 8 Если  $L = \mathbb{Q}[\zeta]$ , где  $\zeta$  - и.к.  $p$ -ой степени,  
 $p \nmid n$   $\forall a \in \mathcal{O}_L \exists b \in \mathbb{Z} : a^p \equiv b \pmod{p\mathcal{O}_L}$ .

Д-60: В силу т. Г.Д.Д (АВТ 12):  $a = b_0 + b_1 \zeta + \dots + b_{p-2} \zeta^{p-2}$ ,  
 $b_i \in \mathbb{Z}$ . Тогда  $a^p \equiv_{p\mathcal{O}_L} b_0^p + (b_1 \zeta)^p + \dots + (b_{p-2} \zeta^{p-2})^p =$   
 $= b_0^p + b_1^p \zeta^p + \dots + b_{p-2}^p \zeta^{(p-2)p} = b_0^p + b_1^p + \dots + b_{p-2}^p \in \mathbb{Z}$ .  $\blacksquare$   
 $\zeta^{p^k} = 1$