Щетинин
Егор
M3338

1.1

$N = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot \ldots \cdot p_m^{k_m}$

$p_i > 2$, т.к. N - нечётное

По КТО ~~***~~ уравнение $x^2 \equiv_N 1$ равносильно

$x^2 \equiv_{p_1^{k_1}} 1$ и $x^2 \equiv_{p_2^{k_2}} 1$ .... $x^2 \equiv_{p_m^{k_m}} 1$.

Покажем, что каждое из этих уравнений имеет ровно 2 решения.

Рассмотрим p^k.

1) $k = 1$

$x^2 \equiv_p 1$, т.к $\mathbb{Z}/p\mathbb{Z}$ является полем, то это уравнение имеет ровно 2 корня $x = \pm 1$

2) $k > 1$

$x^2 \equiv_{p^k} 1 \Rightarrow x^2 \equiv_p 1 \Rightarrow x \equiv_p \pm 1$.

Мы уже знаем 2 решения $x \equiv_{p^k} \pm 1$

Покажем что других нет.

Если они и есть, то имеют вид

$x = \pm 1 + mp$, [illegible] $x \equiv \pm 1$

$$(\pm 1 + mp)^2 \equiv_{p^k} 1$$

$$\pm 2mp + m^2p^2 \equiv_{p^k} 0$$

$$\pm 2mp + m^2p^2 \vdots p^k$$

$$mp(\pm 2 + mp) \vdots p^k$$

$mp \pm 2 \not\vdots p$, т.к. $p > 2$, а $mp \vdots p$,

Значит $mp \vdots p^k \Rightarrow m \vdots p^{k-1}$, т.к. $k > 1$, то

$m \vdots p \Rightarrow m = 0 \Rightarrow x = \pm 1$ - ЧТД

Значит все уравнения

$x^2 \equiv_{p_i^{k_i}} 1$ имеют ровно 2 решения

их у нас n штук объединяем

и получаем как раз 2^n. ЧТД

1.2

$L(x) = e^{\sqrt{\log(x)\log\log(x)}}$ - ~~субэк~~

Функция субэкспоненциальна

если

$\forall c>0: \lim\limits_{x\to\infty} \frac{f(x)}{e^{cx}} = 0.$

~~$\forall a>0: \lim\limits_{x\to\infty} \frac{f(x)}{x^a} = \infty$~~

~~Докажем оба предела.~~

1) $\lim\limits_{x\to\infty} \frac{e^{\sqrt{\log(x)\log\log(x)}}}{e^x} = \lim\limits_{x\to\infty} e^{\cancel{x}\sqrt{\log(x)\log\log x} - x} =$

Покажем, что $\lim\limits_{x\to\infty} \cancel{x - \sqrt{\log x \log\log x}} =$

$\sqrt{\log x \log\log x} - x = -\infty$

$\sqrt{\log x \log\log x} \le \sqrt{\log^2 x} = \log x$

$\log x - x \to -\infty \Rightarrow$

$= 0$

Мы показали, что функция растет медленнее экспоненты. ЧТД

1.4.

1) $f(x) = x^4 - 2x^2 - 1$

Предположим, мы смогли разложить на два квадратных трехчлена.

$x^4 - 2x^2 - 1 = (x^2 + ax + b)(x^2 + cx + d) =$

$= x^4 + (a+c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd$

$$\begin{cases} a + c = 0 \\ ac + b + d = -2 \\ ad + bc = 0 \\ bd = -1 \end{cases} \Rightarrow \begin{cases} a = -c \\ -c^2 + b + d = -2 \\ a(d - b) = 0 \\ bd = -1 \end{cases}$$

$a(d - b) = 0$ $a = 0$ или $d = b$

1) $a = 0$, $c = 0$

$$\begin{cases} b + d = -2 \\ bd = -1 \end{cases} \Rightarrow b \quad b = -1 + \sqrt{2} \quad d = 1 + \sqrt{2}$$

иррац. иррац.

2) $b = d$

$b^2 = -1$ - невозможно. Неприводим. ЧТД

2) θ - корень

$\theta^4 = \theta^2 + 1$ $\Rightarrow$ что любую степень θ больше 3 можно представить как линейную комбинацию меньших степеней

Из этого следует, что ~~минимальная~~
~~кольца точно лежит в Q[~~

$Q(\theta)$ лежит в $Q[\theta]$

$Q[\theta]$ очевидно лежит в $Q(\theta)$ $\Rightarrow$

$\Rightarrow Q(\theta) = Q[\theta]$

3) $Z[\theta] = D$? D - целые алг. числа в $Q(\theta)$

$Z[\theta] \subseteq D$, т.к. и 1 и θ целые алг. числа

$D \subset Z[\theta]$?

1, 6 $\mathbb{Q}(\sqrt{-13})$

(размышления из 1.4)

$\mathbb{Q}(\sqrt{-13}) = \mathbb{Q}[\sqrt{-13}] = \mathrm{span}(1, \sqrt{-13})$

$x \in \mathbb{Q}(\sqrt{-13}) \Rightarrow x = a + b\sqrt{-13}$

$\cancel{a \in \mathbb{Q}}$ $a, b \in \mathbb{Q}$

$x = a + b\sqrt{-13}$ - $b, a \in \mathbb{Q}$

Рассмотрим моник с целыми коэф второй степени.

Мы рассматриваем вторую степень, т.к. все числа вида $a + b\sqrt{-13}$ являются корнями многочленов второй степени

$x^2 + a'x + b' = 0$, $b', a' \in \mathbb{Z}$

$$x_{1,2} = \frac{-a' \pm \sqrt{a'^2 - 4b'}}{2}$$

$$x = \frac{-a' \pm \sqrt{a'^2 - 4b'}}{2} = -\frac{a'}{2} \pm \frac{\sqrt{a'^2 - 4b'}}{2} = a + b\sqrt{-13}$$

$\cancel{a'^2 - 4b' =}$ $a', b' \in \mathbb{Z}$; $a, b \in \mathbb{Q}$

$\cancel{a'^2 - 4b' = -13 \cdot k^2, \text{ где } k \in \mathbb{N}}$

$\sqrt{a'^2 - 4b'} = \sqrt{-13} \cdot k$, где $k \in \mathbb{N}$, ведь a' и $b' \in \mathbb{Z}$

$a'^2 - 4b' = -13 \cdot k^2$

Покажем, что a' - чётное

$a'^2 - 4b' = -13k^2$

От обратного.

$a = 2n+1$, $n \in Z$

$(2n+1)^2 - 4b' = -13k^2$

$4(n^2+n-b') = -13k^2-1$

$\vdots 4$

k	k^2	$-13k^2-1$
0	0	3
1	1	2
2	0	3
3	1	2

$-13k^2-1$ не делится на 4 ~~при~~ $\Rightarrow$

$\Rightarrow$ противоречие

Значит a' - чётно. $a' = 2m$, $m \in Z$

$x' = -m \pm \sqrt{m-b'} = a + b\sqrt{-13}$

$a = -m \Rightarrow a \in Z$

$\pm\sqrt{m-b'} = b\sqrt{-13}$

$k \in Z$

m и $b' \in Z \Rightarrow \sqrt{m-b'} = \pm\sqrt{-13k^2} =$

$b \in Q$

$= \sqrt{-13} \cdot \pm k \Rightarrow b = \pm k$ $b \in Z$

Мы показали, что a' и $b' \in \mathbb{Z}$

$x = a + b\sqrt{-13}$ $\Rightarrow$ все целые числа лежат в $\mathbb{Z}[\sqrt{-13}]^*$

Ответ: $x = a + b\sqrt{-13}$, где $a, b \in \mathbb{Z}$

* ~~Очевидно~~, что все числа вида $a + b\sqrt{-13}$, $a, b \in \mathbb{Z}$ являются целыми, т.к. мы можем привести ~~многочлен~~ многочлен, где они являются корнями:

$$(x - (a + b\sqrt{-13}))(x - (a - b\sqrt{-13})) = x^2 - 2ax + 13b^2 + a^2.$$

1.7 $D \equiv_4 1$

$\mathbb{Q}(\sqrt{D}) = \mathrm{span}(1, \sqrt{D})$ — как в 1.6

$x = a + b\sqrt{D}$ Аналогично 1.6, $a, b \in \mathbb{Q}$

$x^2 + a'x + b' = 0$, $a', b' \in \mathbb{Z}$

$$x = \frac{-a' \pm \sqrt{a'^2 - 4b'}}{2} = -\frac{a'}{2} \pm \frac{\sqrt{a'^2 - 4b'}}{2} = a + b\sqrt{D}$$

$$\frac{\sqrt{a'^2 - 4b'}}{2} = b\sqrt{D} \qquad a = -\frac{a'}{2}$$

$$\sqrt{a'^2 - 4b'} = 2b\sqrt{D}$$

$$a'^2 - 4b' = 4b^2 D \qquad D = 4k + 1$$

$\cancel{a'^2 - 4b' = 4b^2 D \quad a' = 2m \quad 4m^2 - 4b' = 4b^2 D \quad m^2 - b' = b^2(4k+1)}$

$b = \frac{c}{2}$ $\quad c \in \mathbb{Q}$

$$\underset{\mathbb{Z}}{a'^2} - 4b' = c^2 \underset{\mathbb{Z}}{D} \Rightarrow c^2 \in \mathbb{Z} \Rightarrow c \in \mathbb{Z}$$

$D = 4k+1$

$$a'^2 - 4b' = c^2(4k+1)$$

$$a'^2 - c^2 = 4(kc^2 - b')$$

$$a'^2 - c^2 \vdots 4 \Rightarrow a'^2 \underset{4}{\equiv} c^2 \Rightarrow a' \underset{2}{\equiv} c$$

$$x = a + b\sqrt{D} = -\frac{a'}{2} + \frac{c}{2}\sqrt{D} = \frac{-a' + c\sqrt{D}}{2}$$

$\cancel{-a' \underset{2}{\equiv} c \quad \ldots \quad = \frac{a + b\sqrt{D}}{2}}$

$$x = \frac{-a' + c\sqrt{D}}{2} \qquad a', c \in \mathbb{Z}$$

$$a' \underset{2}{\equiv} c \Rightarrow -a' \underset{2}{\equiv} c$$

~~Что~~ Осталось показать, что такие числа и вправду все целые

$$x = \frac{a+b\sqrt{D}}{2} \qquad a \equiv_2 b$$

Приведём монотик

$$\cancel{\left(x - \frac{a+b\sqrt{D}}{2}\right)\left(x - \frac{a-b\sqrt{D}}{2}\right)} =$$

$$\left(x - \frac{a+b\sqrt{D}}{2}\right)\left(x - \frac{a-b\sqrt{D}}{2}\right) =$$

$$= x^2 - ax + \frac{a^2 - b^2 D}{4} = \cancel{x}^2 - ax + \frac{a^2 - b^2(4k+1)}{4}$$

$$= x^2 - ax + b^2 + \frac{a^2 - b^2}{4} \qquad a^2 - b^2 \vdots 4, \text{ т.к. } a \equiv_2 b$$

монотик.

Доказали, что

$x \in \mathfrak{D}$ – мн-во целых $\mathbb{Q}(\sqrt{D})$ $D \equiv_4 1$ имеет вид

$x = \frac{a+b\sqrt{D}}{2}$, где $a \equiv_2 b$

Очевидно, что одним из базисов задающих такие числа является $\left\{1, \frac{1+\sqrt{D}}{2}\right\}$ – ЧТД