ТЕОРЕМА 2: В пред. обозн.

$$|\alpha - \delta_k| < |\alpha - \delta_{k-1}| \quad \forall k > 1$$

доказательство: Имеем такое пред-ие

$$\alpha = \frac{\alpha_k P_{k-1} + P_{k-2}}{\alpha_k Q_{k-1} + Q_{k-2}}$$

$$\alpha_k = [q_{k+1} \dots]$$

отсюда: $|\alpha - \delta_{k-1}| = \left| \frac{\alpha_k P_{k-1} + P_{k-2}}{\alpha_k Q_{k-1} + Q_{k-2}} - \frac{P_{k-1}}{Q_{k-1}} \right| =$

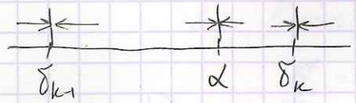
$$= \frac{|\alpha_k (-1)^k|}{(\alpha_k Q_{k-1} - Q_{k-2}) Q_{k-1}} - \frac{\alpha_k}{(\alpha_k Q_{k-1} - \alpha_{k-2}) Q_{k-1}} ;$$

$$|\alpha - \delta_k| = \left| \frac{\alpha_k P_{k-1} + P_{k-2}}{\alpha_k Q_{k-1} + Q_{k-2}} - \frac{P_{k-1}}{Q_{k-1}} \right| =$$

$$= \frac{1}{(\alpha_k Q_{k-1} + Q_{k-2}) Q_{k-1}} = \frac{Q_{k-1}}{\alpha_k Q_{k-1}} |\alpha - \delta_{k-1}| < |\alpha - \delta_{k-1}|$$

$Q_k > Q_{k-1}$, $\alpha_k > 1$ } дробь < 1

ч.доказ.



Опр: Число $\frac{a}{b} \in \mathbb{Q}$, где $b \in \mathbb{N}$, $a \perp b$ наилучшим приближением для числа $\alpha \in \mathbb{R}$, если

$$\forall x \in \mathbb{Z} \quad \forall y \in \mathbb{N}: \quad |\alpha - \frac{x}{y}| < |\alpha - \frac{a}{b}| \Rightarrow$$

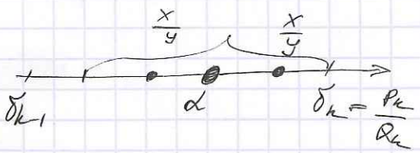
$$y > b$$

ТЕОРЕМА 3. Подх дроби δ_k суть наилучшие приближ. к ирр числу α.

доказ-во:

Пусть $|\alpha - \frac{x}{y}| < |\alpha - \frac{P_k}{Q_k}|$

по Т 2: картинка при k чётном



$$\Rightarrow 0 < |\delta_{k-1} - \frac{x}{y}| < |\delta_k - \delta_{k-1}| = \frac{1}{Q_k Q_{k-1}}$$

$$\frac{1}{y Q_{k-1}} < \frac{m}{y Q_{k-1}} \Rightarrow \frac{1}{y Q_{k-1}} < \frac{1}{Q_k Q_{k-1}} \Rightarrow Q_k < y$$

$y > Q_k$

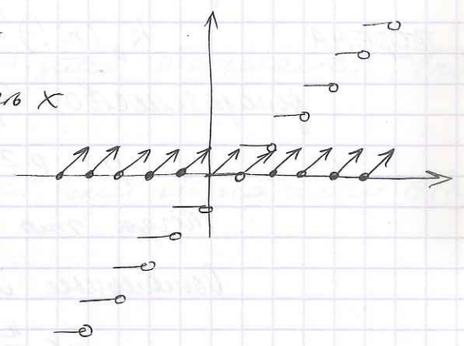
АРИФМЕТИЧЕСКИЕ ФУНКЦИИ

1) Целая и дробная часть

$x \in \mathbb{R}$ $\quad x = q + \lambda$ $\quad q \in \mathbb{Z}$ $\quad 0 \le \lambda < 1$

$q = [x]$ – цел. часть x

$\lambda = \{x\}$ – дробная часть x



ТЕОРЕМА 1) $[x + m] = [x] + m$ при $m \in \mathbb{Z}$

2) $\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$ $\quad n$-натур.

3) $[x+y] \ge [x] + [y]$

$[x+y] \le [x] + [y] + 1$

доказат-во: ① $x = q + \lambda$

тогда $x + m = \underbrace{q + m}_{\text{целое}} + \underbrace{\lambda}_{\text{дробное}}$

② Пусть $x = q + \lambda$ $\quad q \in \mathbb{Z}$ $\quad 0 \le \lambda \le 1$

$q = n \cdot h + r$, $0 \le r < n$, $h \in \mathbb{Z}$

Тогда

$[x] = q$, $\frac{[x]}{n} = h + \frac{r}{n}$

$h \in \mathbb{Z}$ $\quad 0 \le \frac{r}{n} < 1 \Rightarrow \left[\frac{[x]}{n}\right] = h$

С друг. стор $\quad \frac{x}{n} = \frac{n \cdot h + r + \lambda}{n} = h + \frac{r + \lambda}{n}$

$r < n$, $0 < \lambda < 1$ $\Rightarrow r + \lambda < n$ $\quad 0 \le \frac{r+\lambda}{n} < 1$

$\left[\frac{x}{n}\right] = h$

③ самим

Опр: Пусть p - прост. число, n - натур и k - такое что

$$p^k \mid n \;;\; p^{k+1} \nmid n \;,$$

тогда $k = k_p(n)$ - кратность p в n

ТЕОРЕМА $$k_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

доказательство: Пусть m - max

$(n-1)\cdot n$ $\quad p\cdot 1,\ p\cdot 2 \dots p\cdot m \le n$

Тогда то все множ $n!$ делятся на p

Остальные мн-ли не делятся на p, ясно, что

$$\left.\begin{array}{l} m < \frac{n}{p} \\ m - \text{усл} \\ m - \max \end{array}\right\} \Rightarrow m = \left[\frac{n}{p}\right]$$

Кроме того $k_p(n!) = k_p(p\cdot 1\cdot p\cdot 2 p\cdot 3 \cdots p\cdot n) =$

$$= k_p(p^m \cdot m!) = m + k_p(m!)$$

$$k_p(n!) = \left[\frac{n}{p}\right] + k_p(m!)$$

Аналогично:

$$k_p(m!) = \left[\frac{m}{p}\right] + k_p(\dots) =$$

$$= \left[\frac{\left[\frac{n}{p}\right]}{p}\right] + k_p(\dots) = \text{теор.} =$$

$$= \left[\frac{n}{p^2}\right] + k_p(\dots)$$

Продолжаем, получим:

$$k_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$ теор. доказана

пример: найдем число нулей в десятичной записи

$100!$ $\quad = k_{10}(100!)$

$$k = \min\{k_2(100!), k_5(100)\} =$$

$$= k_5(100) = \left[\frac{100}{5}\right] + \left[\frac{100}{5^2}\right] + \left[\frac{100}{5^3}\right] =$$

$$= 20 + 4 = 24.$$

Упр: 1) Разложить $160!$ на простые мн-ли.

2) Д-ть, что $100! > 10^{157}$

2) ЧИСЛО И СУММА ДЕЛИТЕЛЕЙ

Опр: Пусть n - нат. число, число его нат. делит обозначается $\tau(n)$

$$\tau(6) = 4$$

Опр: n - нат. число, Σ всех его нат делит обозначается $\sigma(n)$

$$\sigma(6) = 1+2+3+6 = 12$$

Опр: "Арифметическая фция"

$f: \mathbb{N} \to \mathbb{C}$ - мультипликативна, если

$$f(m\cdot n) = f(m)\cdot f(n) \text{ при } n \perp m$$

примеры:

1) $i(n) = 1$, $\forall x$

2) $e(n) = n$, $\forall n$

ТЕОРЕМА: Пусть f - мультипликат. фция

$$g(n) := \sum_{d \mid n} f(d) \qquad f\text{-мультипл.}$$

док-во: $m, n \in \mathbb{N} \qquad m \perp n$

Если $d \mid (m,n) \Rightarrow d = d_1 \cdot d_2 \;\Big|\; d_1 \mid m,\ d_2 \mid n,\ d_1 \perp d_2$

Отсюда

$$g(m\,n) = \sum_{d \mid (mn)} f(d) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 \cdot d_2) =$$

$$= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1)\, f(d_2) = \left(\sum_{d_1 \mid m} f(d_1)\right)\left(\sum_{d_2 \mid n} f(d_2)\right) =$$

$$= g(m)\cdot g(n)$$

следствие 1: τ и σ - мультипл. фции

$$\tau = \sum_{d \mid n} i(d) \qquad \sigma(n) = \sum_{d \mid n} e(d)$$

↑ мультипл. (сильно) ↑ сильно мультипл

Следствие: Если $n = p_1^{k_1} \cdots p_s^{k_s}$ – кан. разл. нат. числа на простые множители, то

$$\tau(n) = \prod_{i=1}^{s} (k_i + 1)$$

$$\sigma(n) = \prod_{i=1}^{s} \left(\frac{p_i^{k_i+1} - 1}{p_i - 1} \right)$$

Доказательство: Имеем

$p_i^{k_i} \perp p_j^{k_j}$ $\quad j \neq i$

$p_i^{k_i} \perp \prod_{j \neq i} p_j^{k_j}$

$$\tau(n) = \prod_{i=1}^{s} \tau(p_i^{k_i})$$

$$\sigma(n) = \prod_{i=1}^{s} \sigma(p_i^{k_i})$$

осуществ. индекс i и найдем $\tau(p^k)$ и $\sigma(p^k)$

где p-простое

очевидно: $1, p, p^2, \ldots, p^k$ – все делители p^k,

поэтому $\tau(p^k) = k+1$

$$\sigma(p^k) = 1 + p + p^2 + \ldots + p^k = \frac{p^{k+1}+1}{p-1}$$

3) Функция Мёбиуса

Опр: Ф-ия Мёбиуса $\mu : \mathbb{N} \to \mathbb{C}$

задаётся усл.

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1 \\ 0, & \text{если } \exists p > 1, \ p\text{-простое}, \ p^2 \mid n \\ (-1)^s, & \text{если } n = p_1 \cdot p_2 \cdots p_s \end{cases}$$

ТЕОРЕМА: 1) Ф. Мёбиуса – мультипл.

2) $\sigma(n) = \sum_{d \mid n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 0 \end{cases}$

3) пусть $g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu(d)\, g\left(\frac{n}{d}\right) \overset{(*)}{=} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) g(d)$

$d \mid n \Rightarrow n = dd'$, $d' = \frac{n}{d}$

↑ Ф-ла обращения Мёбиуса

доказ-во: 1) Пусть $m, n \in \mathbb{N}$ $\quad m \perp n$

Если $n = 1$ или $m = 1$ $\Rightarrow$

$\mu(mn) = \mu(m) \cdot \mu(n)$

Пусть $m, n > 1$ Если $p^2 \mid mn \Rightarrow p^2 \mid m$ или $p^2 \mid n$ (т.к. $m \perp n$)

В этом сл. $\mu(mn) = 0 = \mu(m) \cdot \mu(n)$

Пусть $m = p_1 p_2 \cdots p_s$; $n = q_1 \cdots q_n$

p_i, q_j – различные простые $\Rightarrow$

$$\mu(mn) = (-1)^{s+t} = (-1)^s \cdot (-1)^t = \mu(m) \cdot \mu(n)$$

2) $\sum_{d \mid 1} \mu(d) = \delta(1) = \mu(1) = 1$

Пусть $n > 1$ $\quad n = p_1^{k_1} \cdots p_s^{k_s}$ $\quad p_i$-разл. простые

т.к. p-нулят $\Rightarrow$ δ тоже нулят.

$$\delta(n) := \sum_{d \mid n} \mu(d)$$

Поэтому $\delta(n) = \delta\left(\prod_{i=1}^{s} p_i^{k_i}\right) = \prod_{i=1}^{s} \delta(p_i^{k_i})$

осуществ. индекс i:

$$\delta(p^k) = \sum_{\substack{p^i \mid p^k \\ i \leq k}} \mu(p^i) =$$

$$= \mu(1) + \mu(p) + \mu(p^2) \cdots \mu(p^k) =$$

$$= 1 + (-1) + 0 + 0 + \ldots + 0 = 0$$

$\Rightarrow \delta(n) = 0$ при $n > 1$.

3) ($\Rightarrow$) Имеем

$$\sum_{d \mid m} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d \mid m} \mu(d) \left[\sum_{c \mid \frac{n}{d}} f(c) \right] =$$

$$= \sum_{c \mid n} f(c) \left[\sum_{d \mid \frac{n}{c}} \mu(d) \right] = \quad \frac{n}{d} = cq \Rightarrow n = cdq$$

(2) $\Rightarrow \sum_{c \mid n} f(c)\, \delta\left(\frac{n}{c}\right) = f(n)$

1 только при $\frac{n}{c} = 1$, ост $= 0$

$\Leftarrow$) Имеем

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right) \overset{(*)}{=} \sum_{d|n} \sum_{c|\frac{n}{d}} \mu\left(\frac{n}{cd}\right) g(c) =$$

$n = dq$

$$= \sum_{c|n} g(c) \underbrace{\sum_{d|\frac{n}{c}} \mu\left(\frac{n}{cd}\right)}_{(2)} = \sum_{c|n} g(c)\,\delta\left(\frac{n}{c}\right) = g(n)$$

$c = n$

ч.т.д.

① φ_n - функция Эйлера

Опр: $\varphi(n)$ - кол-во нат. чисел $\le n$ и взаимнопрост с n

ТЕОРЕМА: 1) $\sum_{d|n} \varphi(d) = n$ [формула Гаусса]

2) φ - мультипликативна

3) $\varphi(p^k) = p^k - p^{k-1}$ при $k \ge 1$ и p-прост

$$\varphi(p_1^{k_1} \cdots p_s^{k_s}) = \prod_{i=1}^{s} p_i^{k_i} - p_i^{k_i - 1}$$

доказательство:

1) Пусть $A = \{1, 2, \dots n\}$

Если $d|m$ то $A_d := \{x \in A \mid НОД(x, n) = d\}$

разбиение: тогда

$$\bigcup_{d|n} A_d = A$$

$d_1 \neq d_2 \Rightarrow A_{d_1} \cap A_{d_2} = \varnothing$

$$n = |A| = \sum_{d|n} |A_d|;$$

(переходим на d)

но $|A_d| = |\{x \in A \mid \frac{x}{d} \perp \frac{n}{d}\}|$

$1 \le \frac{x}{d} \le \frac{n}{d} \Rightarrow |A_d| = \varphi\left(\frac{n}{d}\right)$

$$n = \sum_{d|m} \varphi\left(\frac{n}{d}\right) = \sum_{d|m} \varphi(d)$$

2) мультипликативность

Имеем $\varphi(n) \equiv n = \sum_{d|n} \varphi(d)$

Тогда по ф-ле обращ. Мёбиуса

$$\varphi(n) = \sum_{d|n} \mu(d)\, c\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$$

Если $n \perp m \Rightarrow \varphi(mn) = \sum_{d|mn} \mu(d) \cdot \frac{mn}{d} =$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2)\, \frac{mn}{d_1 d_2} =$$

$$= \left(\sum_{d_1|m} \mu(d_1) \cdot \frac{m}{d_1}\right)\left(\sum_{d_2|n} \mu(d_2)\, \frac{n}{d_2}\right) =$$

$$= \varphi(n)\,\varphi(m)$$

3) $\varphi(p^k) = ?$

Числа не превосх p^k и не взаимнопросты

$p, 2p, 3p, \dots p^{k-1} \cdot p$ - их $p^{k-1} \Rightarrow$

$\Rightarrow \varphi(p^k) = \underbrace{p^k}_{\text{все}} - p^{k-1}$, используя мультипл. φ получаем Эйлерову ф-ну.

СТРУКТУРА КОЛЬЦА ВЫЧЕТОВ $\mathbb{Z}_m$

Опр: Пусть $R_1 \dots R_s$ - кольца $\Rightarrow$

$\Rightarrow$ их прямая Σ - это кольцо $R = \bigoplus_{i=1}^{s} R_i =$

$= \{(r_1 r_2 \dots r_s) \mid r_i \in R_i\}$

с операциями

$(r_1 \dots r_s) + (r_1' \dots r_s') = (r_1 + r_1', r_2' \dots , r_s + r_s')$

$(r_1 \dots r_s) \times (r_1' \dots r_s') = (r_1 r_1', r_2 r_2' \dots r_s r_s')$

Его ноль - это набор из нулей.

$0 := (0, \dots, 0)$

Его '1' - это набор единиц

$1 := (1, \dots, 1)$

Теорема: $\exists\ m_1 m_2 \dots m_s \in \mathbb{N}$ и $m_i \perp m_j \ / i \neq j$

Пусть $m = m_1 m_2 \dots m_s$

Тогда $\mathbb{Z}_n \simeq \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{\dots} \oplus \mathbb{Z}_{m_s}$ — КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ.

доказ-во: $\varphi : \mathbb{Z}_m \to \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}$

по пр-лу:

$\varphi(x \pmod n) = (x \pmod{m_1}, \dots, x \pmod{m_s})$

ум-ся, что φ-биекция

Пусть $x = x' \pmod{m_i}, \forall i \Rightarrow$

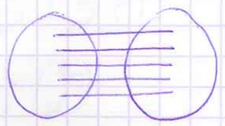
$\Rightarrow m_i \mid (x - x')\ \forall i \Rightarrow n = \prod_{i=1}^{s} m_i \mid (x - x') \Rightarrow$

$m_i \perp m_j\ \forall i \neq j$

$\Rightarrow x = x' \pmod n$

т.к. $|\mathbb{Z}_m| = m = \prod_{i=1}^{s} m_i = |\mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_s}| \Rightarrow$

$\Rightarrow \varphi$ - отобр "на"



Кроме того $\varphi(x+y) = \varphi(x) + \varphi(y)$ $\forall x, y \in \mathbb{Z}_m$

$\varphi(xy) = \varphi(x)\varphi(y)$

$x \pmod{m_k} + y \pmod{m_k} = (x+y) \pmod{m_k}$

ч.т.д.

конструктивное док-во (с построением)

Пусть $r_1 \dots r_s$ - набор остатков по $\mathbb{Z}_{m_1} \dots \mathbb{Z}_{m_s}$,

восстановить по нему $x \in \mathbb{Z} \mid x \pmod{m_i} = r_i\ \forall i$

$$\begin{cases} x = m_1 q_1 + r_1 \\ x = m_2 q_2 + r_2 \\ \dots \\ x = m_s q_s + r_s \end{cases} \qquad x = ?$$

Пусть $n_i = \frac{m}{m_i} = \prod_{j \neq i} m_j$ Тогда

$m = m_i n_i \quad m_i \perp n_i$

Сущ. реш. мин. диоф ур-ия

$m_i u_i + n_i v_i = 1$ где $v_i \in \mathbb{Z}$

Положим

$x := \sum_{i=1}^{s} r_i n_i v_i$

Тогда $x_0 = r_i \pmod{m_i} \quad \forall i$

т.к $n_i \cdot v_i = 1 = -m_i n_i$

$n_i v_i = 1 \pmod{m_i} \quad | \times r_i$

$r_i v_i n_i = r_i \pmod{m_i}$ с одной стороны

если $j \neq i$, то

$m_i \mid n_j \Rightarrow m_i \mid r_j v_j n_j \Rightarrow r_j v_j n_j = 0 \pmod{m_i}$

Если еще $x = r_i \pmod{m_i} \Rightarrow$ уже док. $\Rightarrow$

$x = x_n \pmod m \Rightarrow$

$x = x_0 + tm \quad t \in \mathbb{Z}$

(самое малое x - ост. от деления x_0 на m)

$x_0 = m \cdot t + x$

ч.т.д

ПРИМЕР: Как работать с больш. числами, ск-е 32 разр. арифметику?
$2^{32}-1$

ЛЕММА $НОД(2^k-1, 2^l-1) = 2^m-1$, $m = НОД(k,l)$

доказательство:

Ясно, что $a-1 \mid a^q-1 = (a-1)(1+a+\dots+a^{q-1})$

потому если $n \mid k \Rightarrow 2^n-1 \mid 2^k-1$

$a = l^n$ $l = n \cdot m \dots$

$2^n-1 \mid 2^l-1$

$\Rightarrow 2^n-1$ – общий дел., наибольший ли?

Пусть $N \mid 2^k-1, 2^l-1 \Rightarrow$

$$\Rightarrow \begin{cases} 2^k = 1 \pmod N \\ 2^l = 1 \pmod N \end{cases}$$

т.к. разрешимо н.Д. ур.

$kx+ly=n$ x,y – решение $\Rightarrow$

$\Rightarrow 2^n = 2^{kx+ly} = (2^k)^x \cdot (2^e)^y = 1^x \cdot 1^y \pmod N$ (1 = 1)

$\Rightarrow N \mid 2^n-1$

доказана лемма

а теперь пример: 32 31 29 27 25 – попарно +

по лемме числа $2^{32}-1$, $2^{31}-1$, $2^{29}-1$, $2^{27}-1$, $2^{25}-1$ – попарно вз-пр

$\Rightarrow$ по китайской Th

для $m = (2^{32}-1)(2^{31}-1)\dots(2^{25}-1)$

$Z_m \simeq Z_{(2^{32}-1)} \oplus \dots \oplus Z_{(2^{25}-1)}$

можно точно предст. в 32 разр. бинарной арифметике

Потому и Z_m можно представить число m;

$m = (2^{32}-1)(2^{31}-1)\dots(2^{25}-1) =$

$= 2^{32+31+\dots+25} + \dots - + - + \dots \leq 2^{143} \sim 10^{40}$

2^{144}

СЛЕДСТВИЕ Если $m = p_1^{k_1} \dots p_s^{k_s}$

p_i – разл. простые, то

$Z_m \simeq Z_{p_1^{k_1}} \oplus \dots \oplus Z_{p_s^{k_s}}$

(пр. Σ комм.)

СТРУКТУРА МУЛЬТИПЛИКАТ. ГР.-ПЫ КОЛЬЦА ВЫЧЕТОВ.

ТЕОРЕМА. Если $m_1 \dots m_s \in \mathbb{N}$ и попарно 1 $\Rightarrow$

$\Rightarrow Z_m^* = Z_{m_1}^* \times \dots \times Z_{m_s}^*$

доказ-во вост. из разл. Z_n & пр. Σ.

СЛЕДСТВИЕ: Если $m = p_1^{k_1} \dots p_s^{k_s}$ p_i – вз. прост

$$Z_m^* = Z_{p_i^{k_i}}^* \times \dots \times Z_{p_s^{k_s}}^*$$

Вопрос: Какова группа $Z_{p^k}^* = ?$

ТЕОРЕМА: Z_p^* – цикл. гр. порядка $p-1$, если p – прост.

Более общее: пусть K – поле $G \leq K^*$ $|G| < \infty \Rightarrow G$ – цикл. гр.

доказательство: G – конеч. абелева группа

тогда G – пр-ие примарных цикл. групп.

предположим, что в разлож. гр. G имеем 2 множителя порядка q^k и q^l $k \geq 0 \geq 1$ (q-прост)

$G = | \; x \; | \; x \dots |$

$Zq^k \quad Zq^l$

тогда ур-ие $x^{q^k}=1$ имеет $(q^k \cdot q^l)$ решений,
но $q^k \cdot q^l > q^k$

а в поле многочленов ст. n имеет не более чем n корней $\not\equiv$ с приколом. что $\underline{\underline{2}}$ ми-ля

$\Rightarrow$ для данного прост q $\exists$ $!_{\circ}$ ми-ле такого типа

G_q - кр. пр-ие групп взаимнопростых порядков, где q_i - различные простые

Ввиду изв. ф-ии

$$Z_p \times Z_{p^q} \simeq Z_{pq} \quad \text{если } p \perp q \Rightarrow$$

$\Rightarrow G_q$ - цикл. гр.-па.

ч.т.д.

ЗАМЕЧАНИЕ: Если p - простое, то

$Z_{p^k}^*$ - циклическая гр при $p \geq 3$

группа Z_8^* - не цикл. (упр)

Опр: Если $G = \{g\}$ - цикл. гр. порядка n, то $\forall$
$x \in G \; \exists! \, k(x) \mid \begin{cases} 0 \leq k(x) < n \\ g^{k(x)} = x \end{cases}$

это число - $k(x)$ - дискретный логарифм x по оси g
или индекс x по оси g

обозначение $\log_g x = \log_g x$ или $\underset{g}{ind} x$

ЗАМЕЧАНИЕ: $k \mapsto g^k \pmod N$, $k \in \mathbb{Z}$

легко вычислимо

ОБРАТНАЯ ФУНКЦИЯ:

$$X \to \log_g X$$

плохо вычислима

НЕ ЛИНЕЙНЫЕ ДИОФАНТОВЫ УР-НИЯ

ур-ие Эйлера.

$$x^2 + y^2 = n$$

Опр: Кольцо K нат-ли евклидовым, если

1) K - ассоц., комут. кольцо с "1" и без дел-ей "0"

2) сущ. ф-ия $N: K \setminus \{0\} \to \mathbb{Z}_{\oplus} [= \mathbb{N} \cup \{0\}]$

со св-ом

а) $N(ab) \geq N(a)$ и рво $\Leftrightarrow b \in R^*$

б) $\forall a, b \in K \setminus \{0\} \; \exists \, q$ и $r \in R$ со

св-ми $\begin{cases} a = bq + r \\ N(r) < N(b) \end{cases}$ или $r = 0$ ⟲

функция: N - норма на R

Примеры: 1) $R = \mathbb{Z}$

$N(b) = |b|$

2) $R = K(x)$ K-поле

$N(f(x)) = \text{ст. } f(x)$

3) —

ТЕОРЕМА. Кольцо целых гауссовых чисел

$$\Gamma = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

- евклидово отн $N(x) = N(a+bi) = |\alpha|^2 = a^2 + b^2$

док-во: Очевидно: Γ - ассоц, комут, с "1" ($\mathbb{C}$-поле)

'евклидовость': найдем Γ^* через

$\alpha \cdot \beta = 1$, $\alpha, \beta \in \Gamma \Rightarrow$

$\Rightarrow |\alpha\beta| = 1 \Rightarrow |\alpha|^2 \cdot |\beta|^2 = 1$

$(a^2+b^2)(c^2+d^2) = 1 \quad a, b, c, d \in \mathbb{Z}$

α → $(a, b) = \begin{bmatrix} (\pm 1, 0) \\ (0, \pm 1) \end{bmatrix} \Rightarrow \begin{bmatrix} \alpha = \pm 1 \\ \alpha = \pm i \end{bmatrix} \Rightarrow \Gamma^* = \{\pm 1, \pm i\}$

(≥ 0 над a, ≥ 0 над b) $\Rightarrow a^2 + b^2 = c^2 + d^2 = 1$ в $\mathbb{Z}$ числах

проверим свво:

а) $N(\alpha\beta) \geq N(\beta)$

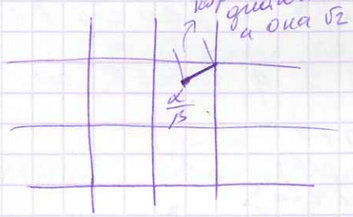
$'='$ $\Leftrightarrow$ $\alpha \in \Pi^*$

$\underbrace{|\alpha|^2}_{\in N} \cdot |\beta|^2 \geq |\beta|^2$ $\quad (\alpha\beta \neq 1)$

$'='$ $\Rightarrow$ $|\alpha|^2 = 1$ $\quad \alpha \in \Pi^*$

б) Пусть $\alpha, \beta \in \Pi$ $\quad \beta \neq 0$

тогда $\frac{\alpha}{\beta} \in \Pi$ и $\exists\, \gamma \in \Pi$



$\left|\frac{\alpha}{\beta} - \gamma\right| \leq \frac{1}{\sqrt{2}}$

тогда: обозначим r/β ρ число равное $\rho = \alpha - \beta\gamma \in \Pi^*$

Отсюда

$\alpha = \beta\gamma + \rho$

$|\rho| = |\alpha - \beta\gamma| = |\beta| \cdot \left|\frac{\alpha}{\beta} - \gamma\right| \leq$

$\leq \left(\frac{1}{\sqrt{2}}|\beta|\right)^2 < (|\beta|)^2$

$N(\rho) < N(\beta)$

ч.т.д.

СЛЕДСТВИЕ Т.к. всякое евкл. кольцо имеет алгоритм деления НОД, критерий разложимости и. ф. ур.

$ax + by = c$

$\text{НОД}(a,b) \mid c$

однозначность разл. на мн-ли

ТЕОРЕМА (Эйлера) Ур-ие $x^2 + y^2 = n$ при $n \in N$ разрешимо в целых числах $\Leftrightarrow$

в разложении числа n на простые множители двойки (простое) вида $(4k+3)$ входят с чётными показателями

примеры

1) $x^2 + y^2 = 2$ — разрешимо

$x = y = 1$

2) $x^2 + y^2 = 6 = 2 \cdot \underbrace{3}$

в кот ст. нечет $\Rightarrow$ неразрешимо

x	0	1	2	3
x^2	0	1	4	9

доказательство:

ом. 1) $\forall\, n = p$ - простое число, можно считать $p > 2$

$(\Rightarrow)$ Пусть $\exists\, x, y \in \mathbb{Z}$ $\quad x^2 + y^2 = p \Rightarrow$

$\Rightarrow \quad 0 < x, y < \sqrt{p} < p$

$x^2 \equiv -y^2 \pmod p$

$y \not\equiv 0 \pmod p$

$\mathbb{Z}_p$ - поле $\Rightarrow$ у обратим $\exists\, z \mid yz \equiv 1 \pmod p$

$(xz)^2 = -(yz)^2 \pmod p = -1 \pmod p$

Тогда $\text{ord}(xz) = 4$ в $\mathbb{Z}_p^*$

"//"

так как $-1 \neq 1 \pmod p$ ввиду нечетности p,

по порядок эл-а гр. делит порядок гр., т.е

$4 \mid |\mathbb{Z}_p^*| = p - 1$

$\Rightarrow p - 1 = 4k \Rightarrow p = 4k + 1$

$(\Leftarrow)$ пусть $p = (4k+1)$ - прост $\overset{?}{\Rightarrow}$ ур-ие разрешимо

$\Rightarrow |\mathbb{Z}_p^*| = p - 1 = 4k$

$\mathbb{Z}_p^*$ - цикл. гр.

$g^{4k} = 1$

$g^m \neq 1$, $m \leq 4k$

тогда $(g^{2k})^2 = 1$ $\quad g^{2k} = \begin{cases} 1 \\ -1 \end{cases}$ $\quad 2k < 4k$

$x^2 = 1 \Rightarrow x = \pm 1$ в поле

$g^{2k} \equiv -1 \pmod p$

$u = g^k \Rightarrow u^2 + 1 \equiv 0 \pmod p$

отсюда получим в $\Gamma \supset \mathbb{Z}$:

$u^2 + 1 = (u+i)\cdot(u-i)$

$p \mid (u+i)(u-i)$ в Γ

Если $p \perp u+i$ то $p \perp u-i$ тк

отобр $a+bi \mapsto a-bi$ это автоморфизм в Γ

Тк. Γ - евкл. кольцо $\Rightarrow$

$$\left.\begin{matrix} p \perp u+i \\ p \perp u-i \end{matrix}\right\} \Rightarrow p \perp (u+i)(u-i) = u^2+1 \equiv 0 \pmod p$$ ↯

$\Rightarrow p \not\perp u \pm i$ в Γ:

$\text{НОД}(p, u+i) \boxed{\notin \Gamma^*} = d$

Пусть $p = dd'$ $d' \subset \Gamma^*$

Если $d' \in \Gamma^* \Rightarrow p \mid (u+i)$ $p = d(d')^{-1}$

$$\underbrace{u+i}_{\text{целое}} = \underbrace{p}_{\text{целое (простое}} (\underbrace{m}_{\text{целое}} + \underbrace{n}_{\text{целое}} i) \Rightarrow$$

простое...

$\begin{cases} pn = 1 \\ pm = u \end{cases}$ — не может быть

$\Rightarrow d' \in \Gamma^*$ $p = dd' = (k+li)(m+ni)$

$k, l \in \mathbb{Z}$.

тогда $N(p) = p^2 \overset{(k^2+l^2)(k^2+l^2)}{=} N(d)\,N(d') =$

$= \underset{\overset{\vee}{1}}{(k^2+l^2)}\underset{\overset{\vee}{1}}{(n^2+m^2)}$

из единст. разл. нат. числа в пр-ие простых

$k^2 + l^2 = n^2 + m^2$

сл. 1) рассмотрен.

сл.2) Т n-составное

(⇒) Пусть $x, y \in \mathbb{Z} \mid x^2 + y^2 = n$

пусть d - НОД(x,y)

$x = x_0 d \quad y = y_0 d$

$x^2 + y^2 = (x_0^2 + y_0^2)\, d^2 = n \Rightarrow d^2 \mid n \quad n = md^2$?

$x_0^2 + y_0^2 = m \qquad x_0 \perp y_0$

Если $p \mid m$, то $x_0^2 + y_0^2 \equiv 0 \pmod p$

$x_0^2 = -y_0^2 \pmod p$

Пусть $p \mid n$ p простое (нечет)

Тогда $x_0^2 + y_0^2 \equiv 0 \pmod p$

Если $p \mid y_0 \to p \mid x_0$ но $x_0 \perp y$ $\Rightarrow$ невозм.

$\Rightarrow p \nmid y_0 \Rightarrow y_0 \not\equiv 0 \pmod p \Rightarrow \exists\, z \mid y_0 \cdot z \equiv 1 \pmod p \Rightarrow$

$\Rightarrow (x_0 \cdot z)^2 \equiv -1 \pmod p$, в этом сл.

$p = 4k+1$

Следоват, если $p = 4k+3$ и $p \mid \overset{d^2 m}{n} \Rightarrow p \mid d^2$

$\Rightarrow p^2 \mid d^2 \Rightarrow p$ входит в n с четным показателем

(⇐) предположение;

Число n разл на множ. вида

1) $p = 4k+1$ p-простое
3) $2 = p$
2) p^2, где $p = 4k+1$)

ур-ие
$$\left.\begin{matrix} x^2 + y^2 = p = 4k-1 \\ x^2 + y^2 = p^2 = (4k+1)^2 \\ x^2 + y^2 = 2 \end{matrix}\right\}$$ разрешимы в $\mathbb{Z}$

Осталось доказать, что если $x^2 + y^2 = m$, а $z^2 + t^2 = n$ $x, y, z, t \in \mathbb{Z} \Rightarrow$ ур-ие с правой частью разрешимо тоже $\Rightarrow mn = (\ldots)^2 + (\ldots)^2$

действительно $nm = \underset{\text{норма}}{N}(x+iy) + N(z+it) =$

$= N((x+iy)(z+it)) =$

$= N(xz - yt + i(yz+xt)) =$

$= \underbrace{(xz-yt)^2}_{\in\mathbb{Z}} + \underbrace{(yz+xt)^2}_{\in\mathbb{Z}}$

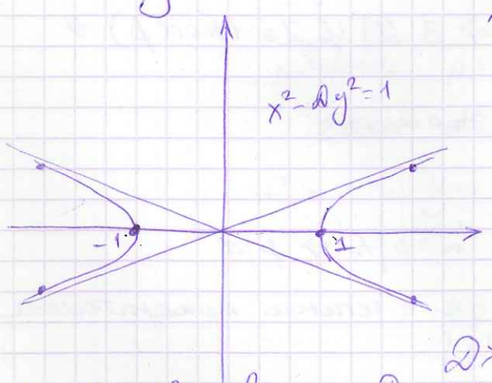
т. Эйлера док-на

УРАВНЕНИЕ ПЕЛЛЯ

$$x^2 - Dy^2 = 1 \qquad D \in \mathbb{N}.$$

Опр.: Число D - свободное от квадратов, если число $p^2 \nmid D$ $\forall p$ прост.

В ур-ии Пелля можно ограничиться, что D - свободно от квадратов



решения $(\pm 1, 0)$ тривиальные

$D > 1$

ТЕОРЕМА Пусть D - нат. число св. от квадратов, тогда ур-ие Пелля $x^2 - Dy^2 = \pm 1$ имеет ∞ много решений, каждое из них имеет вид $(\pm x_k, \pm y_k)$ ($\Leftrightarrow$ не тривиальное)

$k = 1, 2, 3 \ldots$

При этом $x_k + \sqrt{D}\, y_k = (x_1 + \sqrt{D}\, y_1)^k$

(x_1, y_1) – фундаментальное решение

Доказательство:

1) Стр-ра группы на мн-ве решений

Пусть $K = \{ a + b\sqrt{D} \mid a, b \in \mathbb{Q} \} \Rightarrow$

$\Rightarrow$ ут-ся, что $K \in \mathbb{R}$ K - подполе в поле вещ. чисел если $a + b\sqrt{D} = a' + b'\sqrt{D}$

a, b, a', b' - рац-ые

$a - a' = (b - b')\sqrt{D}$

если $b' - b \neq 0 \Rightarrow \sqrt{D}\left(\frac{a-a'}{b'-b}\right) \in \mathbb{Q}$ ↯ это неверно

$\Rightarrow \sqrt{D} = \frac{n}{m} \Rightarrow D = \frac{n^2}{m^2} \Rightarrow n^2 \cdot D = m^2$

$\exists\, p \mid D \Rightarrow p \mid D \quad p^2 \mid D$ ↯

$\Rightarrow b' = b$ и $a' = a \Rightarrow$ запись $a + b\sqrt{D}$ $a, b \in \mathbb{Q}$ однозначна

Очевидно, что K замкнуто отн $+, \times$ и образует коммут. ассоц. кольцо с 1, проверим аксиому У4

$a + b\sqrt{D} \neq 0$

$(a + b\sqrt{D})(x - y\sqrt{D}) = 1 = 1 + 0\sqrt{D}$

$$\begin{cases} ax + bDy = 1 \\ bx + ay = 0 \end{cases} \qquad \begin{vmatrix} a & bD \\ b & a \end{vmatrix}$$

$$x = \frac{a}{a^2 - Db^2};\ y = \frac{-b}{a^2 - Db^2}$$

$a^2 - Db^2 \neq 0$, т.к. иначе $\sqrt{D} = \frac{|a|}{|b|} \in \mathbb{Q}$

$\Rightarrow K$ - поле.

Сопоставим эл-ту $\alpha \in K$ лин. опер.:

$A(\alpha) : x \mapsto \alpha x \quad x \in K$

Его матрица в базисе $(1, \sqrt{D})$ имеет вид $A(x) \cdot 1 = \alpha = a + b\sqrt{D}$

$A(x)\sqrt{D} = \alpha\sqrt{D} = bD + a\sqrt{D}$

$$A(\alpha)_{1,\sqrt{D}} = \begin{pmatrix} a & bD \\ b & a \end{pmatrix} = M(\alpha)$$

Соотв M — изоморфизм поля K и мн-ва матриц.

$A(\alpha+\beta)x = (\alpha+\beta)x = \alpha x + \beta x = A(\alpha)x + A(\beta)x =$

$= (A(\alpha)+A(\beta))x \quad \forall x$

$A(\alpha+\beta) = A(\alpha)+A(\beta)$

$A(\alpha\beta)x = \alpha\beta x = \alpha(\beta x) = A(\alpha)\cdot(A(\beta)x) = (A(\alpha)A(\beta))x$

$A(\alpha\beta) = A(\alpha)\cdot A(\beta)$

Норма числа $\alpha \in K$

$N(\alpha) = \det M(\alpha) = \det A(\alpha) = a^2 - Db^2$

При том N — мультипликативна

$\det(M(\alpha\beta)) = \det M(\alpha)\cdot \det M(\beta) = N(\alpha)\cdot N(\beta)$

~~Решение~~

Решения ур-ия Пелля $a^2 - Db^2 = 1$ соотв матрицам

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix}$$ с определителем 1

мн-во таких матр обр. группу.

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix}^{-1} = \begin{pmatrix} a & -bD \\ -b & a \end{pmatrix}$$

Тогда и числа

$\alpha = a + b\sqrt{D} \quad a^2 - Db^2 = 1$

$a, b \in \mathbb{Z}$

образуют гр. отн. умнож. чисел. При этом

$\alpha^{-1} = a - b\sqrt{D}$

Числа $\alpha = a + b\sqrt{D}$ $a, b \in \mathbb{Z}$ $a > 0$

$a^2 - Db^2 = 1$ обр. подгр-пу Π

если еще $\beta = c + d\sqrt{D}$ $c, d \in \mathbb{Z}$

$c > 0 \quad c^2 - Dd^2 = 1 \Rightarrow \alpha\beta = \underbrace{(ac+bdD)}_{>0?} + (ad+bc)\sqrt{D}$

$>0?$: $a > \sqrt{D}|b|$ $(\leftarrow a^2 - Db^2 = 1)$

$c > \sqrt{D}|d|$ $(\leftarrow (2))$

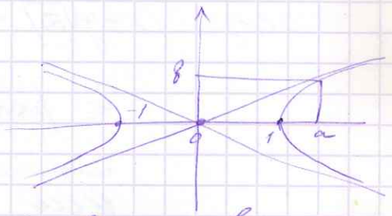
$\Rightarrow ac > D|bd| \Rightarrow ac + dbD > 0$

Утверждается, что гр $\Pi \simeq \mathbb{Z}_2 \times \mathbb{Z}_\infty$

$\mathbb{Z}_2 = \langle \pm 1 \rangle$, $\langle -1, 0 \rangle$ — реш

$-1 + 0\sqrt{D}$

$\mathbb{Z} = \langle \alpha \rangle$, $\alpha = ?$



Предположим, что $\exists$ хотя бы 1 нетривиальное решение

Тогда $\exists$ решение $\alpha = a + b\sqrt{D}$, где $a > 1$, $a \in \mathbb{N}$

$|\alpha|$ — min'ы

Утв-ся, что всякое другое полож. решение — степень числа α. Здесь, если $\beta = c + d\sqrt{D}$ - решение, $c > 1$

$c^2 - d^2D = 1 \Rightarrow$

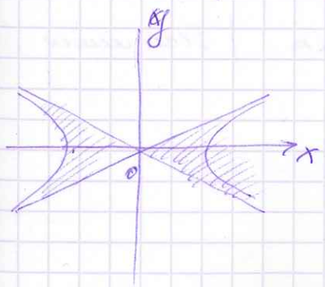
$\Rightarrow \beta \geq \alpha > 1$ как вещ. числа

Тогда $\exists\, k \mid \alpha^{k+1} \geq \beta \geq \alpha^k$

Тогда $\alpha > \underbrace{\beta \cdot \alpha^{-k}}_{\geq 1}$, но это отвечает решению, и меньше α ☺

$\Rightarrow \beta \cdot \alpha^{-k} = 1 \Rightarrow \beta = \alpha^k$

Итак, всякое решение от-но $\pm\alpha^k$, $k \in \mathbb{Z}$



$\alpha = x_1 + \sqrt{D}\, y_1$ — то это ФР.

2) Сущ-ие на пр. реш. $\frac{P_k}{Q_k}$ — как подх дробь к числу $\sqrt{D}$ такое

$$\left| \frac{P_k}{Q_k} - \sqrt{D} \right| < \frac{1}{Q_k^2}$$

$\exists\ \infty$ много несокр. дробей $\frac{x}{y}$ |

$$\begin{cases} \frac{x}{y} > \sqrt{2} & y>0 \\ \frac{x}{y} - \sqrt{2} < \frac{1}{y^2} \end{cases}$$

Тогда $|x - y\sqrt{2}| < \frac{1}{y}$

Пусть $|x+y\sqrt{2}| = |x - y\sqrt{2} + 2y\sqrt{2}| \le$

$$\le |x - y\sqrt{2}| + |2y\sqrt{2}| < \frac{1}{y} + 2y\sqrt{2} \le$$

$y \ge 1$

Итак

перемножим: $|x^2 - 2y^2| < \frac{1}{y}\cdot\left(\frac{1}{y} + 2y\sqrt{2}\right) =$

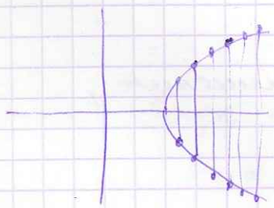
$$= \underbrace{\frac{1}{y^2}}_{\le 1} + 2\sqrt{2} \le 1 + 2\sqrt{2}$$

$|x^2 - 2y^2| = x^2 - 2y^2$ т.к. $\frac{x}{y} > \sqrt{2}$

Итак $\exists\ \infty$ несокр. дробей $\frac{x}{y} > 2$ | $\underbrace{x^2 - 2y^2}_{0} < 1 + 2\sqrt{2}$ $\underbrace{\quad}_{m}$

$x^2 - 2y^2 = m$ - гипербола их конечное число

$0 < m < 1 + 2\sqrt{2}$



но в общем на плоскости ∞ реш $\Rightarrow$
$\Rightarrow \exists\ n$ | $x^2 - 2y^2 = m$ имеет ∞ решений. x, y | $x \perp y$

$\exists\ \infty$ решений с различными x координатами

Тогда $\exists\ k, l$ | $0 \le k, l < m$ | бесконечно реш. | $\begin{cases} x \equiv k \pmod m \\ y \equiv l \pmod m \end{cases}$

Пусть (x_1, y_1) (x_2, y_2) $x_1 \ne x_2$

$$(x_1 + \sqrt{2}y_1)(x_2 - \sqrt{2}y_2) =$$

$$= \underbrace{x_1x_2}_{k^2} - 2y_1y_2 + (x_2y_1 - x_1y_2)\sqrt{2} \equiv \quad (\mathrm{mod}\ m)$$

$$= \left[(x_1^2 + y_1^2 2) + 0\cdot\sqrt{2}\right] (\mathrm{mod}\ m) =$$

$$= (m+0)\ (\mathrm{mod}\ 2) = 0$$

$\alpha\beta = m\gamma$

$N(\alpha\beta) = N(m\gamma)$

$N(\alpha)N(\beta) = N(m)N(\gamma)$

$m \cdot m = m^2 \cdot N(\gamma)$

$1 = N(\gamma) \Rightarrow \gamma$ - реш. ур. Пелля

коэф. $\gamma \Rightarrow$ реш. ур-ие Пелля, оно не тривиально

иначе $\gamma = \pm 1 \Rightarrow \alpha\beta = \pm m$

$\alpha\bar{\beta} = \pm m\bar{\beta}$

$\alpha \cdot m = \pm m\bar{\beta}$

$\alpha = \pm\bar{\beta}$ $\Rightarrow$ по x совпадают $\not\downarrow$ (или не так выбирали)

ЗАМЕЧАНИЕ. Лемма Дирихле, что ур-ие Пелля

$$x^2 - 2y^2 = 1 \quad (*)$$

т.е решения (x_1, y_1) ....

получается из разложения в цеп. дробь числа $\sqrt{2}$ ФСР

Там $x_1 = P_s$ $y_1 = Q_s$ где $\frac{P_s}{Q_s}$ - подх. дробь первая

и $\sqrt{D}$, удовл. ур-ию (*)

КОНЕЧНЫЕ ПОЛЯ И МНОГОЧЛЕНЫ.

гомоморфизмы колец, идеалы и фактор-кольца.

Опр: отобр $\varphi: R \to R'$ колец R и R' наз-ся гомоморфизмом колец, если

$$\left.\begin{aligned}\varphi(a+b) &= \varphi(a)+\varphi(b)\\ \varphi(ab) &= \varphi(a)\cdot\varphi(b)\end{aligned}\right\} \forall a,b \in R$$

Простейшие свва

$$\varphi(a) = \varphi(a-b+b) = \varphi(a-b)+\varphi(b) \Rightarrow$$

/прибавим $-\varphi(b)$/ $\Rightarrow \varphi(a)-\varphi(b) = \varphi(a-b)$

положим $b=a$, получим

$$0 = \varphi(0)$$

положим $a=0$

$$-\varphi(b) = \varphi(-b)$$

Опр: Пусть $\varphi: k \to R'$ – гом-м колец.

Подмн-во:

$$\ker\varphi = \{ a \in R \mid \varphi(a) = 0 \} \quad \text{– ядро}$$

$$\operatorname{Im}\varphi = \{ \varphi(a),\ a \in R \} \quad \text{– образ}$$

Предложение: ядро и образ – подкольца

доказ-во: подкольцо замкнуто отн. операций $\{+, -, \cdot\}$

ядра образа.

Im: $\varphi(a) \pm \varphi(b) = \varphi(a \pm b) \in \operatorname{Im}\varphi$

$\varphi(a)\cdot\varphi(b) = \varphi(a\cdot b) \in \operatorname{Im}\varphi$

Ker: $\varphi(a)=0$, $\varphi(b)=0 \Rightarrow$

$\varphi(a \pm b) = \varphi(a) \pm \varphi(b) = 0 \pm 0 = 0$

$\varphi(ab) = \varphi(a)\varphi(b) = 0\cdot 0 = 0$

Опр: Под-во I кольца R наз-ся "идеалом в R", если

1) $0 \in I$
2) $a,b \in I$ $\quad a-b \in I$
3) $a \in I$, $c \in R$ $\quad ac, ca \in I$

обозначение: $I \lhd R$

Упр: Идеал – подкольцо R

$$0, b \in I \Rightarrow 0-b = -b \in I \quad (1)$$

$$a \in I \Rightarrow a+b = a-(-b) \in I \quad (-)$$

примеры: 1) Если $\varphi: R \to R'$ – гомом. колец, то $\ker\varphi \lhd R$

2) $\langle m \rangle = \{ mk \mid k \in \mathbb{Z} \} \lhd \mathbb{Z}$

$0 := m\cdot 0$

$mk - ml = m(k-l) \in \langle m \rangle$ ($k-l \in \mathbb{Z}$)

$mk \cdot c \in \langle m \rangle$

3) Пусть $R = K[x]$

$P(x) \in K[x]$ – многочлен

$\langle P(x) \rangle$ – мн-во мн-в вида $P(x)\cdot H(x)$, $H(x) \in K[x]$

тогда $\langle P(x) \rangle \lhd R$

4) R – комм., $a_1 \dots a_s \in R$,

$$\langle a_1 \dots a_s \rangle = \{ a_1c_1 + a_2c_2 \dots + a_sc_s \mid c_i \in R \}$$

$\Rightarrow$ это идеал

$\Rightarrow$ идеалов не надо более (Юркин)

Теорема: Пусть I – идеал кольца R, тогда:

1) отношение ср-ни по модулю I:

$a \equiv b \pmod I \Leftrightarrow (a-b) \in I$ – это отнош. эквив.

2) оно согласовано с опер. кольца

3) мн-во R/I всех классов эв-ти отношения сравнимости по I обр. кольцо отн. индуцир. операций. – факторкольцо

4) если R – ас или комм с 1 $\Rightarrow$

R/I такое же кольцо

б) отобр $\varphi: R \to R/I$ по пр-лу $\varphi: a \to \tilde{a}$ – (факторизация) – гомоморфизм колец, причем $\ker\varphi = I$, $\operatorname{Im}\varphi = R/I$

$\{0\} \lhd R$

б) Если $\varphi: R \to R'$ — кольц. гомоморфизм колец $\Rightarrow$

$\Rightarrow R/\ker\varphi \cong \operatorname{Im}\varphi$

док-во: 1) обозначим $a \sim b \Leftrightarrow a \equiv b \pmod I$

Проверим: • $a \sim a \Rightarrow a-a=0 \in I$

• $(a \sim b \Rightarrow b \sim a) \Leftrightarrow (a-b) \in I \Rightarrow b-a=-(a-b) \in I$

• $(a \sim b,\ b \sim c \Rightarrow a \sim c) \Leftrightarrow$

$a-b \in I,\ b-c \in I \Rightarrow$

$\Rightarrow a-b+b-c=a-c \in I$

2) $a \sim a',\ b \sim b'$, надо пр-ть, что

$\begin{cases} a+b \sim a'+b' \\ ab \sim a'b' \end{cases}$ $\quad a+b \sim a'+b$ — выполн.

$a'+b \sim a'+b'$ — выш.

~~$a-a' \in I$~~ ~~$b-b' \in I$~~ ~~$\Rightarrow$~~ ~~a~~ но трансз.

$a+b \sim a'+b'$

$ab \sim a'b \sim a'b'$

↑ ↑

транзит.

Корректно определены операции на фактор-кольце:

$\tilde a + \tilde b = \widetilde{a+b}$

$\tilde a \cdot \tilde b = \widetilde{ab}$

Класс эк-ии $\tilde a = \{x \mid x \sim a$ т.е. $x-a \in I,\ x-a=c \in I,\ a+c,\ c \in I \Rightarrow \underbrace{a+I}\}$

класс смежности

3) R/I — кольцо т.к в анс. кольце есть обратный эл-т, поэтому все аксиомы верны и в фактор-кольце,

F.E: $\exists\ a+b=b+a$

$\widetilde{a+b}=\widetilde{b+a}$

$\tilde a + \tilde b = \tilde b + \tilde a$ — получили слож. С2

F.E: С3.

$\exists\ 0 \mid \forall a\ a+0=a$

$\exists\ \tilde 0\ \forall \tilde a \quad \tilde a + \tilde 0 = \tilde a$

$\widetilde{a+0}=\tilde a$

↑

нейтр. фактор кольца.

$\tilde 0 = \{x \in R \mid x-0 \in I \Rightarrow I\}$

4) аксиомы ассоц. ум., комут. ум., $\exists\ 1'$ не содерж. 0

отрицат. ρ-ба $\Rightarrow$ все ок!

если $a \sim b$ ↓↓ $[a]$ $\tilde a = \tilde b$

5) φ — гомом.

$\varphi(a+b)=\widetilde{a+b}=\tilde a+\tilde b=\varphi(a)+\varphi(b)$

$\varphi(ab)=\widetilde{ab}=\tilde a\cdot\tilde b=\varphi(a)\cdot\varphi(b)$

$\ker\varphi: \{a \in R \mid \varphi(a)=\tilde 0\}=\{a \in R \mid \tilde a=\tilde 0\}=$

$=\{a \in R \mid a-0 \in I\}=I$

б) Пусть $\varphi: R \to R'$ — кольц. гомом.

Обозначим гд $I=\ker\varphi$, зададим отобр.

$\tilde\varphi: R/I \to \operatorname{Im}\varphi$ по пр-лу:

$\tilde\varphi: \tilde a \mapsto \varphi(a)$

Корректно ли это отобр?

Тогда $\tilde a=\tilde b \Leftrightarrow a-b \in I=\ker\varphi \Leftrightarrow \varphi(a-b)=0 \Leftrightarrow$

$\Leftrightarrow \varphi(a)-\varphi(b)=0 \Leftrightarrow \varphi(a)=\varphi(b)$

Т. образом $\tilde\varphi$ — биз. одн. отобр.

более того: $\left.\begin{array}{l}\tilde a \hookrightarrow \varphi(a) \\ \tilde b \hookrightarrow \varphi(b)\end{array}\right\} \Rightarrow \begin{cases}\tilde a+\tilde b=\widetilde{a+b} \hookrightarrow \varphi(a+b)= \\ \quad =\varphi(a)+\varphi(b) \\ \tilde a\cdot\tilde b=\widetilde{ab} \hookrightarrow \varphi(ab)=\varphi(a)\varphi(b)\end{cases}$

$\Rightarrow \tilde\varphi$ — изоморфизм колец.

Пример: $\exists\ R = R[x]$, K - поле комплексных чисел

опр. $\varphi: R[x] \to \mathbb{C}$ по правилу.

$$\varphi: f(x) \to f(i) \leftarrow (i^2 = -1)$$

$\Rightarrow$ докажем, что φ - гомоморфизм колец:

$$\varphi(f(x)+g(x)) = f(i)+g(i) =$$
$$= \varphi(f(x))+\varphi(g(x))$$
$$\varphi(f(x)\cdot g(x)) = f(i)\cdot g(i) =$$
$$= \varphi(f(x))\cdot \varphi(g(x))$$

$\Downarrow$

Очевидно

$\operatorname{Im}\varphi = \mathbb{C}$ т.к. $\varphi(a+bi) = a+bi$, $a,b \in \mathbb{R}$

Найдем ядро:

поскольку, что $((x^2+1)\,h(x))$ то это будет

$$(i^2+1)\,h(i) = 0 \Rightarrow \langle x^2+1\rangle \in \operatorname{Ker}\varphi$$
$$\text{(}i^2+1=0\text{)}$$

Если $f(x) \in \operatorname{Ker}\varphi \Rightarrow f(i)=0$, по теореме Безу

$$(x-i) \mid f(x)$$

$f(x) \in \mathbb{R}[x] \Rightarrow$ * $f(-i)=0$

$$(x+i) \mid f(x)$$

$$(x-i) \perp (x+i) \Rightarrow (x^2+1) \mid f(x)$$

Таким образом

$\operatorname{Ker}\varphi = \langle x^2+1\rangle$, по теореме

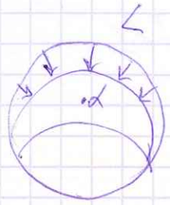
(б) имеем $R[x]/\langle x^2+1\rangle = \mathbb{R}[x]/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi = \mathbb{C}$

ТЕОРЕМА (о существ. корня) - Кронекер

$\exists$ K-поле; $p(x)$-неразложимый многочлен из $K[x]$, тогда $\exists$ поле L со свойствами:

а) $L \supset K$, как подполе

б) $L \ni \alpha \mid P(\alpha)=0$



с) L - min со свойствами а) и б) среди своих подполей.

со свойствами а и б и с поле L задается однозначно с точностью до изоморфизма.

доказательство:

1) Существование L. Пусть L - поле со свойствами а), б), с)

Пусть $\varphi: K[x] \to L$ - гомоморфизм подстановки

$$\varphi: f(x) \to f(\alpha)$$

Найдем ядро φ: очевидно, что

$\langle p(x)\rangle \subset \operatorname{Ker}\varphi$, т.к.

$$\varphi(p(x)\cdot h(x)) = p(\alpha)\cdot h(\alpha) = 0\cdot h(\alpha) = 0$$

докажем, что $\langle p(x)\rangle \supseteq \operatorname{Ker}\varphi$

Пусть $f(x) \in K[x]$ и $f(x)=0 \Rightarrow$

$\Rightarrow (x-\alpha) \mid f(x)$ /т. Безу/ в поле L

Сократим сторону $(x-\alpha) \mid p(x) \Rightarrow$

$\Rightarrow$ НОД$_L(p(x), f(x)) \mid (x-\alpha) \mid$ НОД$(\dots)$

Можно считать $d(x) \in K[x]$ по алг. Евклида.

$\Rightarrow$ ст $d(x) \geq 1$, т.к. $d(x) \mid p(x)$, но $p(x)$-неразложим в $K[x] \Rightarrow p(x) = \varepsilon\cdot d(x)$ $\varepsilon \in K$, $\varepsilon \neq 0$

Тогда $p(x) = \varepsilon\cdot d(x)$ $\quad f(x) = d(x)\cdot h(x) =$

$$= \varepsilon\cdot\varepsilon^{-1}p(x)\cdot h(x) \Rightarrow p(x) \mid f(x)$$

$f(x) \in \langle p(x)\rangle$

$\Rightarrow$ $\operatorname{Ker}\varphi = \langle p(x)\rangle$

тогда: $K[x]/\langle p(x)\rangle = K[x]/\ker\varphi \cong \operatorname{Im}\varphi \leq L$

обозначим $I = \langle p(x)\rangle = \ker\varphi$

ун-ся $K[x]/I \Rightarrow$ поле!

Все аксиомы поля кроме УА в $K[x]/I$

Проверим УА:

$$\tilde{f} \neq \tilde{0} \Rightarrow \exists \left(\tilde{f}\right)^{-1} \mid \tilde{f}\left(\tilde{f}\right)^{-1} = \tilde{1}$$

Т.к. $\tilde{f} \neq \tilde{0} \Rightarrow f \notin I \Rightarrow p \nmid f$, но

p-неразложимый $\Rightarrow p \perp f$, $\Rightarrow \exists\ u$ и $v \in K[x]$)

$$f\cdot u + pv = 1$$

Отсюда: $\tilde{1} = \widetilde{fu+pv} = \tilde{f}\cdot\tilde{u} + \tilde{p}\cdot\tilde{v} =$

$$= \tilde{f}\cdot\tilde{u} + \tilde{0}\cdot\tilde{v} = \tilde{f}\cdot\tilde{u}$$

$$\Rightarrow \tilde{u} = \left(\tilde{f}\right)^{-1}$$

Следовательно $\Rightarrow \operatorname{Im}\varphi$ - подполе в L

$\operatorname{Im}\varphi \supset K$, а

$a_0 + 0\cdot x \xrightarrow{\varphi} a_0 \in \operatorname{Im}\varphi$

$\forall x \xrightarrow{\varphi} \alpha \in \operatorname{Im}\varphi$

$p(\alpha) = 0$

Ввиду мин. $\operatorname{Im}\varphi = L$

$L \cong K[x]/\langle p(x)\rangle$ - ед-ен доказано.

ВСТАВКА - ЖЁЛТАЯ

о.в теоремы:

Поле $\mathbb{F}_{p^n}$ сов. с мн-ом корн. мн-на $x^{p^n}-x$ над $\mathbb{Z}_p$

Этот мн-н не имеет кр. корней

$$x^{p^n}-x \perp \left(x^{p^n}-x\right)' = -1$$

Поэтому $x^{p^n}-x$ - пр-ие различных нормир. неразл. над $\mathbb{Z}_p$ - мн-ов

Пусть $P_d(x)$ - пр-ие всех неразложимых, норм. делителей для $x^{p^n}-x$, имеющих ст d

По теор. Кронек. можно утв, что

$$\mathbb{F}_{p^d} \leq \mathbb{F}_{p^n} \Leftrightarrow \exists \text{ мин } P_d(x) \mid x^{p^n}-x \text{ и ст } P_d(x) = d$$

$$\Updownarrow$$

$$d \mid n$$

В итоге:

$$x^{p^n}-x = \prod_{d\mid n} P_d(x) \qquad (*)$$

$P_d(x)$ - пр-ие всех нормир. неразл. над $\mathbb{Z}_p$ мн-в ст d, его ст, ст $P_d(x) = d\cdot N_d$

Сравним ст. в (*)

$$p^n = \sum d\cdot N_d$$

применим ф-лу обращ. Мёбиуса для ф-ии $f(d) = d\cdot N_d$ $\Rightarrow$

$$f(n) = \sum_{d\mid n} \mu\left(\frac{n}{d}\right) p^d$$

$$\| \quad n\cdot N_n$$

$$N_n = \frac{1}{n}\sum_{d\mid n} \mu\left(\frac{n}{d}\right) p^d$$

ПРИМЕР: Кол-во неразложимых, норм. мн-ов ст 3 над $\mathbb{Z}_2$: теорема р-ка

$$N_2 = \frac{1}{3}\left(\mu(3)\cdot 2 + \mu(1)\cdot 2^3\right) =$$

$$= \frac{1}{3}\left(-2+2^3\right) = 2 \qquad \left\{ \begin{array}{l} x^3+x+1 \\ x^3+x^2+1 \end{array} \right. \text{ - базис поля пар. 8.}$$

$N_8 = 30$