

Aug 2 - 12.01.23
Aug 5 - 19.01.23
Aug 8 - 26.01.23
Aug 10 - 02.02.23
Aug 13 - 09.02.23

me.hse.ru/valkir/nth

12.01.23

Harada

J. P. Tayler, 9 січня 1814 р. — "последний зносит в гравюре"

146). Observatio per inductionem facta gravissima theoriam
residuorum biquadraturorum cum functionibus
lemniscatis elegantissime rectens. Pata si $a+bi$ est
Numerus primus, $a-1+bi$ per $2+2i$ divisibilis,
multitudo omnium solutionum congruentiae

$$1 \equiv x^2 + y^2 + xy + yx \pmod{a+bi}$$

inclusis $(x=\infty, y=\pm i)$; $(x=\pm i, y=\infty)$ fit $(a-1)^2 + b^2$

Найденение: Еслi $p = a^2 + b^2$ — простое, и $(a-1) + bi \vdash 2+2i$, то
уравнение $1 \equiv x^2 + y^2 + xy + yx \pmod{a+bi}$ имеет
 $(a-1)^2 + b^2 - 4$ решения в $\mathbb{Z}[i]$

Понятие: $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ — кольцо целых
рациональных чисел

Пусть p — простое. Тогда $\mathbb{Z}/p\mathbb{Z}$ — поле из $p-1$ -тих

$(\mathbb{Z}/p\mathbb{Z})^* = \{[1], [2], \dots, [p-1]\}$ — мульт. группа поле

Оп: $a \in (\mathbb{Z}/p\mathbb{Z})^*$ — квадр. вычет, еслi $\exists x \in (\mathbb{Z}/p\mathbb{Z})^*$, тиcо $x^2 = a$.

Число a — квадр. невычет

• $R = N = \frac{p-1}{2}$ — # бывших/невычетов

$[1], [2], \dots, [p-1] \rightsquigarrow \underbrace{R}_{\text{число групп } (p-1) \text{ из } \mathbb{Z}/p\mathbb{Z}} = W_p$

• Сколько раз встречается $RR/NR/RN/NN$ в W_p ?

• Моменты из R/N раз могут ли попасть в W_p ?

• S — произв. число групп L из R/N . Сколько раз S может встретиться
в W_p как подгруппа?

Циран: $l=3$ (Jacobsthal, 1906)

$$\begin{array}{cccc} RRR & RRN & RNR & RNN \\ NRR & NRN & NNR & NNN \end{array}$$

$p = 4k+3$ — простые явные формулы

$p = 4k+1$ — более сложные (некомпактные)

Лем: $p = a^2 + b^2 \rightarrow \alpha_p = |ab|$ — на самом деле $q-p$

Зад: @ проверка: $\forall p$ -простое $\exists! \alpha_p$

⑧ $p = a^2 + b^2 \Rightarrow p = (\alpha_p + b_i)(\alpha_p - b_i)$ — разл. на простые в $\mathbb{Z}[i]$

⑨ $(a-i) + bi : 2+2i \Leftrightarrow a = (-1)^{\frac{a_p+1}{2}} \cdot \alpha_p$ — я — это простое $a+bi$

Помимо: упомяну, как сейчас будем $\frac{a}{p}$ с простыми p

Число: будем считать длину $\kappa \pm 1$, но основная мысль будет та же

Число Тайса — Якобстхала

RRR

$x, x+1, x+2$

$$x = r^2, x+1 = s^2, x+2 = t^2 \quad \frac{1}{2} \text{ нецелое}$$

Помимо: $(r, s, t): s^2 = r^2 + 1, t^2 = s^2 + 1 \Leftrightarrow \begin{cases} s^2 - r^2 = 1 \\ t^2 - s^2 = 1 \end{cases}$

$$A^3 \ni (r, s, t); C = \{s^2 - r^2 = 1\} \cap \{t^2 - s^2 = 1\}$$

$$\begin{cases} s+r = u \\ s-r = u^{-1} \end{cases} \quad \begin{cases} t+s = v \\ t-s = v^{-1} \end{cases} \quad \simeq \text{Кривая } C \subset A^2 \text{ в коорд. } (u, v)$$

$$\frac{u+u^{-1}}{2} = s = \frac{v-v^{-1}}{2}$$

$$C': u+u^{-1} = v-v^{-1}$$

$$u^2v + v^2 = uv^2 - u$$

$$uv(u-v) + v^2 + u = 0$$

им.

$$\begin{array}{c} \approx \\ g^2 = x^3 - x \\ \approx \end{array}$$

$$x^2y^2 + x^2 + y^2 - 1 = 0$$

Число: C' — неявная кубическая кривая

Задача: $x^2y^2 + x^2 + y^2 - 1 = 0$ над $\mathbb{Z}/p\mathbb{Z}$ ищем сколько нечетных, сколько

решений y для которых $x^2y^2 + x^2 + y^2 - 1 = 0 \pmod{a+bi}$, т.к.

$$\mathbb{Z}[i]/(a+bi) = \mathbb{Z}/p\mathbb{Z}$$

Вопрос: Сколько точек над $\mathbb{Z}/p\mathbb{Z}$ на кривой $y^2 = x^3 - x$?

Отв: $p+1+2a$ (с учетом ∞)

Доказка (Харц): # точек на эллиптической кривой $< p+1+2\sqrt{P'}$

$$\bullet y^2 = x^3 - x \underset{(a_0)}{\approx} y^2 = x^3 + x$$

• $y^2 = x^3 + px + q$ — форма Вейерштрасса (наг \mathbb{C})

$$\bullet y^2 + a_2 xy + a_4 y = a_1 x^3 + a_3 x^2 + a_5 x + a_6 = E \text{ — канон. форма}$$

Вопрос: сколько точек на E ?

$$|E| = p+1 + \text{tr Fr}(\text{он же} \text{ tr Fr})$$

[19.01.23]

Безопасне в теории чисел

- Конгруэнции
- Квадратные корни
- Симметрия
- Концептуарий к лемме:
 - наше (лемма) = нечто
 - различные наше (лемма) = нечто

Онл: F_q — наше из q 2d-мн.

Вопрос: есть момент равенства q ?

Онл: $q = p^k$, где p — простое, $k \in \mathbb{N}$

Исп: ① $\text{char } F$ — простое число; ② $\dim_{F_p} F = k \Rightarrow |F| = p^k$

Вопрос: момент из ② соответствует наше из ④ 2d-мн?

Онл: если K — поле $F \Rightarrow |F| = |K|^t$, $t \in \mathbb{N}$ (F — БПнаг K)

Занер: $p = \text{char } F \Rightarrow F \supset \mathbb{F}_p$

Абстрактный Проблема

Нужно $\text{char } F = p$

Онл: $\Phi: F \ni x \mapsto x^p \in F$ — абстракт. Проблема

Исп: проверить, что Φ — групп. абел. [$x^p + y^p = (x+y)^p$]

Зад: Ищем неогр. множ. Φ собсн. с $\mathbb{F}_p \subset F$

Д-бо: $\Phi(x) = x \Leftrightarrow x^p = x \Leftrightarrow x^{p-1} = 1 \Leftrightarrow x \in \mathbb{F}_p$

① — МТФ

② — все корни $x^p - x$ лежат в \mathbb{F}_p ■

• Модуляция: $\Phi^k \in \mathbb{F}_{p^k}$, если такое есть

Исп: что делает, если \mathbb{F}_{p^k} не будет?

Вопрос: в каких комплексных температурных коэффициентах?

Ответ: • $\mathbb{Z}/P\mathbb{Z} = \mathbb{F}_P$ - искательные остатки

• Обобщение: R - одн. уединимости (акс, кашм. калькул с $1 \deg$ gen. 0)
 $\stackrel{v}{I}$ -угадай $\xrightarrow{\text{imp.}} R/I$ - кон. одн. gen. \Rightarrow кон. мод.

Пример: $|\mathbb{F}_P[x]/(f(x))| = P^{\deg f}$

$F:$ $\left\{ \begin{array}{l} \text{непр.} \\ \text{непр.} \end{array} \right.$

Исп: f - норм. пол. ф.

Задача: $\mathbb{F}_P[x]/(f(x)) = \mathbb{Z}[x]/(P, f(x))$

$$\begin{array}{ccc} & (\mathbb{Z}/P\mathbb{Z})[x] & \\ \mathbb{Z}[x] & \xrightarrow{\quad} & \mathbb{Z}[x] \\ \mathbb{Z}[x]/(f(x)) & \xleftarrow{\quad} & \end{array}$$

Квадратичные формулы

Одн: $q(x_1, \dots, x_n) = \sum_{i,j} a_{ij} x_i x_j, a_{ij} \in F$ — квадр. форма над F

Вопрос: Пусть $q(x_1, \dots, x_n)$ — квадр. форма над \mathbb{Z} . Какие числа можно получить как значения q в \mathbb{Z}^n ?

Пример: $n=2, q(x_1, x_2) = x_1^2 + x_2^2, q(x_1, x_2) = x_1^2 + 5x_2^2$

Зад: $\mathbb{Z}[x]/(f(x)) \cong \mathbb{Z}^2$, если $\deg f=2$ ($f(x)=x^2+d, d \in \mathbb{N}$)

Теор: $N \geq n = p_1^{k_1} \dots p_r^{k_r} = a^2 + b^2$, если все простые числа вида $p_i \equiv 3 \pmod{4}$ входят в четных степенях

Зад: p — простое вида $4k+1 \Rightarrow p = \left(\frac{q(r)}{2}\right)^2 + \left(\frac{q(n)}{2}\right)^2$, где $r+n$ — четное и нечетное соотв.

Одн: $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ — антипод лемонга

Сл-зап: $\left(\frac{x}{p}\right) = \begin{cases} 1, & x \text{ — квадр. четное} \\ -1, & x \text{ — квадр. нечетное} \end{cases}$

Исп: модуль квадр. групп F^* чисто-целевой

Д-зап: $x = y^k$, где y — одн.; x — четное $\Leftrightarrow k$ — четн., нечетное $\Leftrightarrow k$ — нечетн. ■

Зад: $\# \text{RRR} = \frac{1}{8} \sum_{i=1}^{P-3} \left(1 + \left(\frac{i}{P}\right)\right) \left(1 + \left(\frac{i+1}{P}\right)\right) \left(1 + \left(\frac{i+2}{P}\right)\right)$

Одн: $\Psi(a) = \sum_{m=1}^P \left(\frac{m}{P}\right) \left(\frac{m^2+a}{P}\right)$

Об-ва: • $\Psi(x) = \left(\frac{x}{P}\right) \Psi(ax^2) \Rightarrow \Psi(ax^3) = \Psi(ax^2) \quad (1)$

• $\sum_{a=1}^P \Psi^2(a) = \frac{P-1}{2} \left(\Psi^2(r) + \Psi^2(n) \right)$ модуль
кв. остр. модуль
кв. неост.
(такж., 1) (2)

• $\sum_{a=1}^P \Psi^2(a) = \left(1 + \left(\frac{-1}{P}\right)\right) \cdot P(P-1) \quad (= 0 \text{ при } P = 4k+3) \quad (3)$

Л-е: (2) = (3) $\Rightarrow P = \left(\frac{\Psi(1)}{2}\right)^2 + \left(\frac{\Psi(n)}{2}\right)^2$

Зад: $\Psi(1), \Psi(n)$ — rem

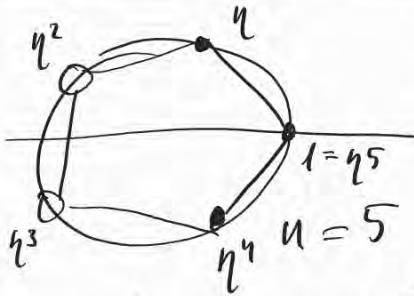
• $\Psi(1) = \sum_{m=1}^P \left(\frac{m}{P}\right) \left(\frac{m^2+1}{P}\right)$

Умн: разложение квадрата в сумму квадратов = теорема $\Psi(1)$

[26. 01. 23]

Круговые (циклические) поля

Комплексные корни из единицы $\sqrt[n]{1}$



$$\{1, 2, 3, 4\} = \mathbb{F}_5^*$$

(цикл. группа)

- 2, 3 – ее образующие

$$\begin{aligned} &\{1, 2, 3, 4\} \\ &\{2^0, 2^1, 2^2, 2^3\} \rightarrow \{2, 4, 3, 1\} \end{aligned}$$

• – генерат. элементы нового порядка
○ – не генерат. элементы нового порядка

Зад: проделать для $n=17$

Сумма Гаусса

Пусть η – первообр. корень степени P ($\eta = e^{\frac{2\pi i}{P}}$)

Пусть a – образующая \mathbb{F}_P^*

Зад: $(d, n) = \sum_{k=1}^{P-1} \eta^{r-a^{dk}}$ – сумма Гаусса

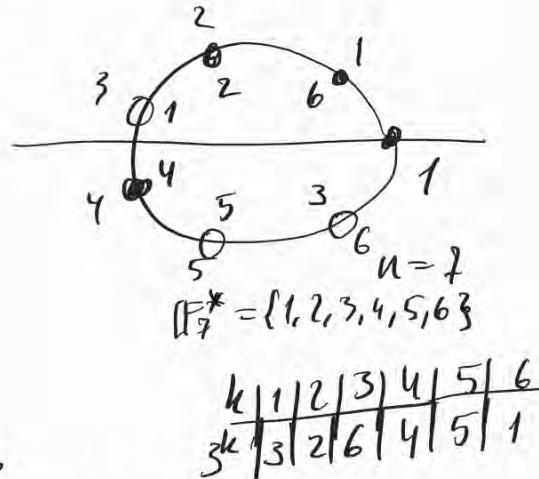
• $(2, r) = \sum_{k=1}^{P-1} \eta^{r-a^{2k}}$ – сумма \bullet (бикратн.)

• $(2, n) = \sum_{k=1}^{P-1} \eta^{n-a^{2k}}$ – сумма \circ (небикратн.)

Зад: $G(x, P) = (2, r) - (2, n)$ – сумма Гаусса, где $x: \mathbb{F}_P^* \rightarrow \mathbb{C}^*$ – линейн.

Зад: $G(x, P) = \sum_{a=1}^{P-1} x(a) e^{\frac{2\pi i a}{P}}$ – сумма Гаусса, где $x(a) = \left(\frac{a}{P}\right)$

Зад: показать: $\left(\frac{a}{P}\right)\left(\frac{b}{P}\right) = \left(\frac{ab}{P}\right)$ ($\Leftrightarrow a \mapsto \left(\frac{a}{P}\right)$ – линейн.)



$$\mathbb{F}_7^* = \{1, 2, 3, 4, 5, 6\}$$

$$\begin{array}{c|ccccc|c} k & | & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 3k & | & 3 & 2 & 6 & 4 & 5 & 1 \end{array}$$

Вопрос: как построить η ?

Зад: $(\mathbb{Q}(\eta) \ni (\sqrt{P} \text{ или } \sqrt{-P}), \text{ если } \eta \text{ постр. чиркулем и методом}$

Зад: $(z, r) - (z, n) = \pm i^{\frac{1-P}{2}} \cdot \sqrt{P} \quad (\Leftrightarrow G(x, P)^2 = \begin{cases} P, & P=4k+1 \\ -P, & P=4k-1 \end{cases})$

Д-бо: $(z, r) \cup (z, n)$ — корни квадр. у-ва с рациональными коэффициентами $x^2 = 2x + \beta$

$$\begin{cases} -1 = (z, r) + (z, n) = -1 \\ \beta = (z, r) \cdot (z, n) = A(z, r) + B(z, n) + C \quad (A, B, C \in \mathbb{Z}, A=B) \end{cases}$$

[Вложим]

$$\beta = \begin{cases} \frac{1-P}{4}, & P=4k+1 \\ \frac{1+P}{4}, & P=4k-1 \end{cases}$$

$$\text{Итого: } (P=4k+1) \quad x^2 + x + \frac{1-P}{4} = 0 \rightarrow \Delta = P \rightarrow x_1 - x_2 = \pm \sqrt{P}$$

Зад: разобраться с поиском знака (меняется ли η)

Квадратичный закон зависимостей

Теор (квадр. закон вз-ши):

$$P, q - \text{нечет. простые числа. Тогда } \left(\frac{P}{q}\right)\left(\frac{q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{q-1}{2}}$$

$$\begin{aligned} \text{Пример: } \left(\frac{59}{269}\right) &= \left(\frac{269}{59}\right) = \left(\frac{59 \cdot 4 + 33}{59}\right) = \left(\frac{33}{59}\right) = \left(\frac{3}{59}\right)\left(\frac{11}{59}\right) = \left(-\left(\frac{59}{3}\right)\right)\left(-\left(\frac{59}{11}\right)\right) = \\ &= \left(\frac{2}{3}\right) \cdot \left(\frac{4}{11}\right) = (-1) \end{aligned}$$

Д-бо: ① $x(a) = \left(\frac{a}{q}\right); \quad G(x, q)^2 = (-1)^{\frac{P-1}{2}} \cdot q \quad \text{нас } \mathbb{F}_P \quad (\text{проверено у Егора; } q=1)$
 $X: \mathbb{F}_q \rightarrow \{\pm 1\} \quad (\text{нужно в } \mathbb{F}_P)$

$$\text{② } y \in \mathbb{F}_P \Leftrightarrow y^{P-1} = 1$$

$$G(x, q)^{P-1} = (-1)^{\frac{P-1}{2}} \text{ нас } \mathbb{F}_P \quad (\text{проверено у Егора})$$

Надчленение: $f \in \mathbb{F}_P, y^2 \in \mathbb{F}_P \Rightarrow \left(\frac{f^2}{P}\right) = y^{P-1} \quad (y \in \mathbb{F}_P \Rightarrow \left(\frac{y^2}{P}\right) = 1, y \notin \mathbb{F}_P \Rightarrow \left(\frac{y^2}{P}\right) = -1)$

$$\left(\frac{y^2}{P}\right) = y^{P-1} = (-1)^{\frac{P-1}{2}}$$

$$\frac{1}{q} \cdot (-1)^{\frac{q-1}{2}} \text{ при } y = G(x, P)$$

02.07.23

D-бюл(праве.): $G(x) = \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \eta^a$, $\eta \in \overline{\mathbb{F}_p}$ — первообразн. корень в \mathbb{F}_q из 1

① $G(x)^2 = (-1)^{\frac{(q-1)}{2}} q \in \mathbb{F}_p$ ← \text{с. 318}

② $G(x)^{p-1} = \left(\frac{P}{q}\right)$ ← \text{прямое доказательство}

① $\Rightarrow \left(\frac{(-1)^{\frac{(q-1)}{2}} q}{p}\right) = 1 \Leftrightarrow G(x) \in \mathbb{F}_p$

② $\Rightarrow G(x)^{p-1} = 1 \Leftrightarrow G(x) \in \mathbb{F}_p$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \rightarrow \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

$$\left(\frac{a}{p}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \left(\frac{P}{q}\right) \blacksquare$$

D-бюл(1, праве.):

Помимо: $G(x)^P = G(x) \cdot \left(\frac{P}{q}\right)$ ($G(x) \neq 0$, иначе $G(x)^2 = (-1)^{\frac{q-1}{2}} G(x) \left(\frac{P}{q}\right)$)

$$\sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \eta^{ap} = [\beta = ap] = \sum_{\beta=1}^{q-1} \left(\frac{\beta \cdot p^1}{q}\right) \eta^\beta = \sum_{\beta=1}^{q-1} \left(\frac{\beta}{q}\right) \cdot \left(\frac{P}{q}\right) \cdot \eta^\beta = \left(\frac{P}{q}\right) \cdot \sum_{\beta=1}^{q-1} \left(\frac{\beta}{q}\right) \eta^\beta$$

$P, 2P, \dots, (q-1)p$ — non-pwd. mod q

Итого: $G(x)^P = G(x) \cdot \left(\frac{P}{q}\right) \Rightarrow G(x)^{P-1} = \left(\frac{P}{q}\right)$ ■

P-агонеские числа

• \mathbb{Z}_p — целые P-аг. числа

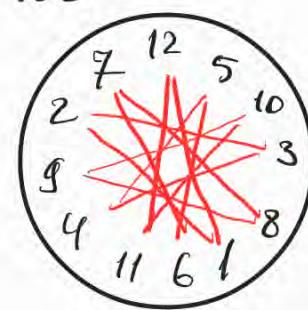
• $\mathbb{Z}_p \subset \mathbb{Q}_p$ — рациональные P-аг. числа

Пример: как устроены изоморфизмы \mathbb{Z}_{12Z}

$$\varphi: \mathbb{Z}_{12Z} \rightarrow \mathbb{Z}_{12Z}$$

φ -изом. $\Leftrightarrow \varphi(1) \in \{1, 5, 7, 11\}$

$((\varphi(1), 12) = 1$ — н. об. значение)



- $S^1 = \mathbb{R}/\mathbb{Z} \supset \mathbb{Q}/\mathbb{Z}$; $H_2 = \left\{ \frac{m}{2^n} | n=0,1,2,\dots; m \in \mathbb{Z} \right\} \subset \mathbb{Q}$

$$S_{H_2}^1 = H_2/\mathbb{Z}$$

Задача: вычислить $\text{Aut}(\mathbb{K}/\mathbb{Z}, H_2/\mathbb{Z})$

• А.Н.Паршин, "Факториальный метод"

P-аддитивные единицы числа \mathbb{Z}_p

Онп: $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z}$, $k \in \mathbb{N}$ — последовательность P-аддитивных единиц

Что это означает: $\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow \dots$

• $\mathbb{Z}_p \ni (a_0, a_1, a_2, \dots)$, где $a_k \equiv a_{k-1} \pmod{p^k}$

Как с этим работать: $a_0 = r_0$

$$a_1 = r_0 + p r_1$$

$$a_k = r_0 + p r_1 + \dots + p^k r_k$$

- От этого можно думать как о записи в p -важной системе счисл.
- Тогда получаем бесконечные числ-ти

$r = \dots r_2 r_1 r_0$ — бесконечная балльная дробь, p -адд. дробь

• Работают стандартные операции и умножение (исключение)

Пример: $p=2$:

$\begin{array}{r} (1) \ 1 \ 1 \\ + \quad \quad \quad 1 \\ \hline (0) \ 0 \ 0 \end{array}$	$(1) + 1 = 0 \in \mathbb{Z}_2$
	$(1) \cdot (1) = 1$ — <u>чтобы</u>

• $\mathbb{Z} \subset \mathbb{Z}_p$

Об-ва \mathbb{Z}_p : ① \mathbb{Z}_p — кольцо по сложению
(чтобы)

② $\mathbb{Z} \subset \mathbb{Z}_p$
 $n \mapsto (n \pmod{p}, n \pmod{p^2}, \dots)$ — отображение пол-ки (r_i), лем. 6 \mathbb{Z}

③ $\mathbb{Z}_p^* = \{ \dots r_2 r_1 r_0 \mid r_0 \in \mathbb{F}_p^* \}$

Вопрос: как устроено кольцо " p -адд. дробей"?

Предп: это \mathbb{K}_p

Натуральные числа \mathbb{N}_p

• $\mathbb{Z}_p \subset \mathbb{Q}_p$

Доп (некомп): ... $r_k r_{k-1} \dots r_1 r_0, r_{-1} r_{-2} \dots r_s \in \mathbb{Q}_p$

Вопрос: нормальны ли $(g) = 1$? Задача нахождения дроби?

03.02.23

Введение в ТЧ

- Р-аг. норма на \mathbb{Q}
- Полное квадратичное в \mathbb{Q}_P
- лемма Denzfeld

Дискретная норма на \mathbb{Q}

Пусть P -простой, K -поле

Опн: $\sigma: K \setminus \{0\} \rightarrow \mathbb{Z}$ — нормирование, если:

$$(1) \sigma(xy) = \sigma(x) + \sigma(y)$$

$$(2) \sigma(x+y) \geq \min\{\sigma(x), \sigma(y)\}$$

Пример: $\mathbb{R}(x) = \left\{ \frac{P(x)}{Q(x)} \mid Q(x) \neq 0; P(x), Q(x) \in \mathbb{R}[x] \right\}$

$f(x) \in \mathbb{R}(x) \rightsquigarrow \text{ord}_a f = : \sigma(f)$

Опн: a — точка полной кратности k , если $f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0, f^{(k)}(a) \neq 0 \Leftrightarrow$

$$\Leftrightarrow f(x) = (x-a)^k g(x), \text{ где } g(a) \neq 0$$

$$(1) \text{ord}_a(f_1 f_2) = \text{ord}_a f_1 + \text{ord}_a f_2$$

$$(2) \text{ord}_a(f_1 + f_2) \geq \min\{\text{ord}_a f_1, \text{ord}_a f_2\}$$

Нормирование на \mathbb{Q}

$\sigma: \mathbb{Q} \setminus \{0\} \rightarrow \mathbb{Z}$

$p \in \mathbb{N}$ -простое $\rightsquigarrow \sigma_p(q) = k$

$$q \in \mathbb{Q}, q = p^k \cdot \frac{m}{n}, m, n \in \mathbb{Z}$$

$$(1) \sigma(q_1 q_2) = \sigma(p^{k_1} \frac{m_1}{n_1} \cdot p^{k_2} \frac{m_2}{n_2}) = \sigma(p^{k_1+k_2} \cdot \frac{m_1 m_2}{n_1 n_2}) = k_1 + k_2 = \sigma(q_1) + \sigma(q_2)$$

$$(2) \sigma(q_1 + q_2) \geq \min\{\sigma(q_1), \sigma(q_2)\}$$

Зап: введение ортого. нормы на \mathbb{A}

P-аддитивная норма на \mathbb{Q}

Оп: $\|\cdot\|_p: \mathbb{Q} \rightarrow \mathbb{R}$ — P-адд. норма на \mathbb{Q} , если $\|q\|_p = \begin{cases} \frac{1}{p^{\nu_p(q)}}, & q \neq 0 \\ 0, & \text{иначе} \end{cases}$

Нормировано: $q \in \mathbb{Z} \Rightarrow \|q\|_p \leq 1$

• Адд. норма: $\|a\|_p = |q|$

Аксиома ограниченности

Аксиома (АП): $\forall \alpha \in \mathbb{K}, \|\alpha\| \Rightarrow \exists n \in \mathbb{N}: \|\alpha^n\| > 1$

Задача: $d(x, y) = \|x - y\|_p$

Оп: d_p — нормированная \mathbb{Q} -мат. нормы $\|\cdot\|_p$

¶

$\dots \Gamma_2 \Gamma_1 \Gamma_0 \Gamma_{-1} \dots \Gamma_K$

• $\Gamma, P, P^2 \in \mathbb{P}$

Пример: $x^2 - 10 = 0$ в \mathbb{Z}_3

$$1 + 0 \cdot 3 + 1 \cdot 3^2 = (0)101$$

$$10 = (1, 1, 10, 10, \dots)$$

Унг. no k:

$$k=0: x_0 = 1, 2$$

Мат: ищем x_{k+1} , ищем x_k

$$x_{k+1} \equiv x_k \pmod{p^{k+1}}; x_k^2 \equiv 10 \pmod{p^{k+1}}$$

$$\forall p \in \mathbb{Z} \Rightarrow x_{k+1} = x_k + a p^{k+1}, a \in \mathbb{F}_p \quad \text{и} \quad \frac{k+2}{1}$$

$$x_{k+1}^2 = x_k^2 + 2ax_k p^{k+1} + a^2 p^{2k+2} \equiv 10 \pmod{p^{k+2}}$$

$$x_k^2 - 10 + 2ax_k p^{k+1} \equiv 0 \pmod{p^{k+2}}$$

$$\frac{x_k^2 - 10}{p^{k+1}} + 2ax_k \equiv 0 \pmod{p}$$

$$\hookrightarrow a = \frac{10 - x_k^2}{2x_k p^{k+1}} \Rightarrow x_{k+1} = x_k + a p^{k+1}$$

Лемма Тензеля

Лемма (Тензеля): $f(x) \in \mathbb{Z}_p[x] - \text{мн-н}$ (пример: $x^2 - x_0$)

смво речи $\Leftrightarrow x_0 \bmod p$ -
квадр быв.

Если $\exists a \in \mathbb{Z}_p$, м.р.: (1) $f(a) \equiv 0 \pmod{p^n}$;
 (2) $\|f'(a)\|_p = p^{-k}$ где $k < \frac{n}{2}$,

то $\exists b \in \mathbb{Z}_p$, м.р.: (1) $b \equiv a \pmod{p^{n-k}}$
 (1) $f(b) \equiv 0 \pmod{p^{n+1}}$
 (2) $\|f'(b)\|_p = p^{-k}$

Доказ.: Б непр. леммы y ф однр. будем искать в \mathbb{Z}_p

Вопрос: $p=2 \Rightarrow x^2 \equiv 1 \pmod{8}$ илл. Ч решения - 1, 3, 5, 7 \Rightarrow
 \Rightarrow доказываем (?) по лемме и получаем 4 разл. реш. в $\mathbb{Z}_p \Rightarrow$
 \Rightarrow противор. с тем, что в \mathbb{Q}_p будет 2 реш.

• доказательство $\mathbb{R} = \text{лемма Ньютона}$:

$$f'(a)(x-a) = (y - f(a)); g = 0 \Rightarrow b = a - \underbrace{\frac{f(a)}{f'(a)}}$$

Доказ.: $b = a - \frac{f(a)}{f'(a)}$ — ходим поговаривать

Разл. f не содержит $(x-a)$ (Мейер)

$$f(x) = f(a) + (x-a)f'(a) + \dots$$

$$0 \pmod{p^n} \quad \|f'(a)\|_p = \frac{1}{p^k}$$

$$\begin{aligned} b = a + c \cdot p^{n-k} \Rightarrow f(b) &= f(a) + c \cdot p^{n-k} f'(a) + \overbrace{\frac{2(n-k)}{p} \cdots}^0 = \\ &\equiv f(a) + c \cdot p^n \left(\frac{f'(a)}{p^k} \right) \stackrel{\mathbb{Z}_p^*}{\bmod} p^{n+1} \stackrel{\text{помимо}}{\equiv} 0 \pmod{p^{n+1}} \end{aligned}$$

$$\theta \equiv \frac{f(a)}{p^n} + c \cdot u \stackrel{0 \pmod{p}}{\bmod} p$$

$$c \equiv \frac{-f(a)}{u p^n} \pmod{p} \Rightarrow b = a + c \cdot p^{n-k}$$

$$(b-a) = c \cdot p^{n-k} \rightarrow \text{бес} \bmod \text{нраво}$$

