① **Введение в теорию чисел** Лекция 2 19.01.2023

- конечные поля
- квадратичные формы
- символ Лежандра

Комментарий к Серру:
поле (Серр) = тело
коммутативное поле (Серр) = поле

• $\mathbb{F}_q$ – конечное поле из $q$ элементов

Вопрос: Чему может быть равно $q$?

$q = p^k$, $p$ – простое, $k \in \mathbb{N}$

$\underbrace{1+1+\dots+1}_{p \text{ – шт.}} = 0$ с таким $p$ – ом $\Rightarrow p = \operatorname{char}\mathbb{F}$

Упр. 1 $\operatorname{char}\mathbb{F}$ – простое

Упр. 2 $\dim_{\mathbb{F}_p}\mathbb{F} = k \Rightarrow |\mathbb{F}| = p^k$

$\mathbb{F}$ – векторное пр-во над $\mathbb{F}_p$ размерности $k$

Вопрос: Может ли поле из восьми элементов содержать в качестве подполя поле из четырёх элементов?

② **Определение**: автоморфизм Фробениуса поля характеристики $p$

$\Phi : \mathbb{F} \to \mathbb{F}$

$\Phi : x \mapsto x^p$

Биномиальная теорема: $(x+y)^p = x^p + y^p$

Упр. Проверьте, что $\Phi$ действительно автоморфизм.

$\mathbb{F}_{p^k} \subset \mathbb{F}$ Упр. дать полный ответ.

**Утверждение**: Множество неподвижных точек автоморфизма $\Phi^k$ совпадает с $\mathbb{F}_{p^k}$, если $x^p - x$ имеет не более $p$ корней

$\Phi : x \mapsto x^p = x \Leftrightarrow x \in \mathbb{F}_p$

малая теорема Ферма

Weil conjectures

$y^2 = x^3 - x$ над $\mathbb{F}_p$ $\quad \Phi : M^n \to M^n \rightsquigarrow H_*^i(M)$

③ Вопрос: В каких контекстах встречаются конечные поля?

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \rightsquigarrow \frac{R}{I}$ – область целостности

Упр. $R/I$ – конечная область $\Leftrightarrow$ целостности $\Leftrightarrow$ конечное поле

2, 3, 4 = $2^2$, 5, 7, 8 = $2^3$, 9 = $3^2$

**Примеры** $\mathbb{F} := \mathbb{F}_p[t]/(f(t)) = p^{\deg f}$ (неприводимый)

Упр. $\mathbb{F}$ – поле $\Leftrightarrow$ $f$ неприводимый

$\mathbb{Z}[t]/(p, f(t))$ $\quad (\mathbb{Z}/p\mathbb{Z})[t]$ $\quad \mathbb{Z}[t]$ $\quad \mathbb{Z}[t]/(f(t))$ $\quad \deg f = 2$ $\quad \simeq \mathbb{Z}^2$

④ • квадратичная форма $q(x_1, \dots, x_n)$ над полем $\mathbb{F}$

$q(x_1, \dots, x_n) = \sum_{i \le j} a_{ij} x_i x_j$ $\quad x_i x_j$, $i \ne j$ $\quad x_i^2$

Вопрос: Пусть $q(x_1, \dots, x_n)$ квадратичная форма с целыми коэффициентами. Какие целые числа можно получить в качестве значений формы $q$ на наборах $(x_1, \dots, x_n) \in \mathbb{Z}^n$?

$q : \mathbb{F}^n \to \mathbb{F}$

**Пример**: $n = 2$

$q(x_1, x_2) = x_1^2 + x_2^2$

$x_1^2 + 5x_2^2$

$u = x_1 + x_2 i$, $v = y_1 + y_2 i$, $uv = z_1 + z_2 i$

$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = z_1^2 + z_2^2$

⑤ **Пример** (теорема Ферма – Эйлера)

$\mathbb{N} \ni n = p_1^{k_1} \cdots p_e^{k_e} \stackrel{?}{=} a^2 + b^2$

$k_i$ нечётно $\Rightarrow p_i = 4k+1$

[J, стр. 12–13] Утв. $p$ – простое вида $4k+1$ $\Rightarrow p = a^2 + b^2$ единственным $p = a_{2+1}^2 + b^2$, $a$ чётно

$\Rightarrow p = \left(\frac{\varphi(r)}{2}\right)^2 + \left(\frac{\varphi(n)}{2}\right)^2$

$$\#\,RRR = \frac{1}{8}\sum_{i=1}^{p-3}\left(1+\left(\frac{i}{r}\right)\right)\left(1+\left(\frac{i+1}{p}\right)\right)\left(1+\left(\frac{i+2}{p}\right)\right) = \dots \frac{\varphi(-1)}{n} = \varphi(1)$$

**Определение**: $\varphi(a) = \sum_{m=1}^{p}\left(\frac{m}{p}\right)\left(\frac{m^2+a}{p}\right)$

(1) $\varphi(a) = \left(\frac{x}{p}\right)\varphi(ax^2) \Rightarrow \varphi^2(ax^2) = \varphi^2(ay^2)$

(2) $\sum_{a=1}^{p}\varphi^2(a) = \frac{p-1}{2}\left(\varphi^2(r) + \varphi^2(h)\right)$ (любой кв. вычет, любой невычет)

(3) $\sum_{a=1}^{p}\varphi^2(a) = \left(1+\left(\frac{-1}{p}\right)\right)p(p-1)$

**Следствие**: (2) = (3) $\Rightarrow p = \left(\frac{\varphi(1)}{2}\right)^2 + \left(\frac{\varphi(h)}{2}\right)^2$ при $p = 4k+3$

Упр. $\varphi(r)$, $\varphi(h)$ чётны

$$\varphi(1) = \sum_{m=1}^{p}\left(\frac{m}{p}\right)\left(\frac{m^2+1}{p}\right)$$

⑥ • символ Лежандра $\left(\frac{x}{p}\right)$, $p$-простое, $x \in \mathbb{F}_p^* = \langle y \rangle$ $\quad x^2 + d$, $d \in \mathbb{N}$

**Определение**: $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ $\quad x = y^k$ $\quad (y^k)^{\frac{p-1}{2}} = 1$, $k$ чётно

**Свойство**: $\left(\frac{x}{p}\right) = \begin{cases} 1, & \text{если } x \text{ – квадратичный вычет } (k \text{ чётно}) \\ -1, & \text{иначе } (k \text{ нечётно}) \end{cases}$

$|\mathbb{F}_p^*| = p - 1$

Упр. Любая конечная подгруппа группы $\mathbb{F}^*$ циклическая.

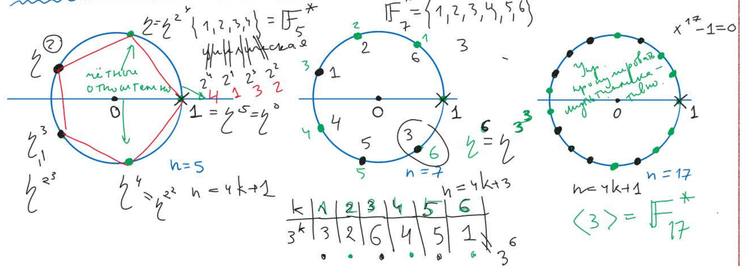
me.hse.ru/valkir/nth

## ① Введение в теорию чисел. Лекция 3. 26.01.2023

- квадратичный закон взаимности
- гауссовы суммы
- круговые (циклотомические) поля

30 марта 1796 г. первая запись Гаусса

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




| $k$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $3^k$ | 3 | 2 | 6 | 4 | 5 | 1 |

## ② Гауссова сумма $G(\chi)$, где $\chi: \mathbb{F}_p^* \to \mathbb{C}^*$ — гомоморфизм (характер)

**Определение:** $G(\chi) = \sum_{a=1}^{p-1} \chi(a) e^{\frac{2\pi i a}{p}}$

**Период Гаусса** $\eta$ — первообразный корень степени $p$

$\eta = e^{\frac{2\pi i}{p}}$

$a$ — образующая группы $\mathbb{F}_p^*$

$(2,h) = \sum_{k=1}^{\frac{p-1}{2}} \eta^{a^{2k}}$ (чётные степени) — период

$(2,r) = \sum_{k=1}^{\frac{p-1}{2}} \eta^{a^{2k}}$ (нечётные степени)

**Определение 2** Сумма Гаусса $G(\chi) = (2,r) - (2,h)$, где $\chi(a) = \left(\frac{a}{p}\right)$

Упр. $\left(\frac{q}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \Leftrightarrow a \mapsto \left(\frac{a}{p}\right)$ — гомоморфизм

## ③ Как построить $\eta$?

$\mathbb{Q}(\eta) \Rightarrow \sqrt{p}$ или $\sqrt{-p}$ $(p-1)/2$

**Утв.** $(2,r) - (2,h) = \pm i^{\frac{p-1}{2}} \sqrt{p}$

$\chi(a) = \left(\frac{a}{p}\right)$ (II)

$G(\chi)^2 = \begin{cases} p, & p = 4k+1 \\ -p, & p = 4k+3 \end{cases}$

**Дво:** $(2,r)$ и $(2,h)$ — корни квадратного ур-я с рациональными коэф.

$-A = (2,r) + (2,h) = -1$

$B = (2,r)\cdot(2,h) = A(2,r) + B(2,h) + C = \frac{1-p}{4}$ (если $p = 4k+1$)

$A, B, C \in \mathbb{Z}$

$x^2 + ax + \beta = x^2 + x + \frac{1-p}{4}$

$D = p$

$(x_1 - x_2)^2$

$x_1 - x_2 = \pm\sqrt{p}$

$\{x_1, x_2\} = \{(2,r), (2,h)\}$

(эсс→) Задача * Как Гаусс нашел знак?

## ④ (квадратичный закон взаимности)

**Тма** (Лежандр, 1798)

$p, q$ — нечётные простые числа

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

**Пример:**

$\left(\frac{59}{269}\right) = \left(\frac{269}{59}\right) = \left(\frac{59\cdot 4 + 33}{59}\right) = \left(\frac{33}{59}\right) =$

$= \left(\frac{3}{59}\right)\left(\frac{11}{59}\right) = -1$ т.к. (V)

(1) $\left(\frac{3}{59}\right) = -\left(\frac{59}{3}\right) = -\left(\frac{2}{3}\right) = 1 = -(-1)$

(2) $\left(\frac{11}{59}\right) = -\left(\frac{59}{11}\right) = -\left(\frac{4}{11}\right) = -\left(\frac{2}{11}\right)^2 = -1$

## ⑤

(1) $G^2(\chi) = (-1)^{\frac{q-1}{2}} q$

$\chi(a) = \left(\frac{a}{q}\right)$ $\quad \chi: \mathbb{F}_q^* \to \{\pm 1\} \Rightarrow G(\chi) \in \overline{\mathbb{F}_p}$

у Серра $q = \ell$ над $\mathbb{F}_p$

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

$G(\chi)^{p-1} = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$ в $\overline{\mathbb{F}_p}$ (II) $q^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}$

**Наблюдение:** $y \in \overline{\mathbb{F}_p}$, $y^2 \in \mathbb{F}_p \Rightarrow \left(\frac{y^2}{p}\right) = y^{p-1} = (-1)^{\frac{p-1}{2}}$

$y = G(\chi) \Rightarrow y^2 \overset{(1)}{=} (-1)^{\frac{q-1}{2}} q \Rightarrow \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) \overset{(2)}{=} (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)$

## ⑥ Работа над ошибками

Доказательство квадратичного закона взаимности (Серр, стр. 17-18)

(1) Определим сумму Гаусса $G(\chi) = \sum_{a=1}^{q-1}\left(\frac{a}{q}\right)\eta^a$ над $\overline{\mathbb{F}_p}$, где $\eta \in \overline{\mathbb{F}_p}$ — первообразный корень степени $q$ из единицы. Тогда

$G(\chi)^2 = (-1)^{(q-1)/2} q \in \mathbb{F}_p$

(2) $G(\chi)^{p-1} = \left(\frac{p}{q}\right)$ ← Проверяются прямым вычислением (см. Серр, д-ва лемм 1 и 2)

$\Rightarrow$ (1) $\Rightarrow \left(\frac{(-1)^{(q-1)/2} q}{p}\right) = G(\chi)^{p-1}$

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

$(-1)^{(p-1)/2}(-1)^{(q-1)/2}\left(\frac{q}{p}\right)$ ▨

## ① Введение в теорию чисел

Лекция 4 — 2 февраля 2023 г.

- p-адические числа
- $\mathbb{Z}_p \subset \mathbb{Q}_p$ — поле; кольцо целых
- метрики на $\mathbb{Q}$
- теорема Островского

не путать с $\mathbb{Z}/p\mathbb{Z}$

*Прошлый раз:* д-во квадратного закона взаимности

*Определение:* $G(X) = \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \eta^a$, где $\eta \in \overline{\mathbb{F}_p}$ — первообразный корень степени $q$ из 1.

(1) $G(X)^2 = (-1)^{\frac{q-1}{2}} q$ (задача 15, сем. 3)

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

*Д-во формулы (2)*

$$G(X)^p = G(X) \cdot \left(\frac{p}{q}\right) \Rightarrow$$

$$\sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \eta^{\boxed{a}\cdot b} = \sum_{b=1}^{q-1} \left(\frac{bp^{-1}}{q}\right) \eta^b = \left(\frac{p^{-1}}{q}\right) \sum_{b=1}^{q-1} \left(\frac{b}{q}\right) \eta^b = \left(\frac{p}{q}\right) G(X)$$

$p, 2p, \dots, (q-1)p$ — различны $\bmod q$

$\left(\frac{p}{q}\right)$

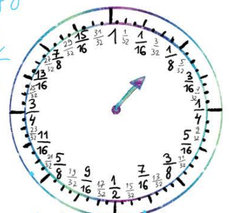
## ② Что такое время? Что такое часы?

$\mathbb{R} \xrightarrow{t \mapsto} S^1 = \mathbb{R}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ (топологическая группа)

*Пример:* как устроены изоморфизмы группы $\mathbb{Z}/12\mathbb{Z}$?

$\varphi: \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$

$\varphi$ — изоморфизм $\Leftrightarrow \varphi(1) = 1, 5, 7, 11$

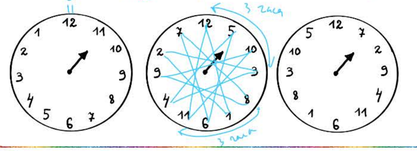


*Пример:* дана бесконечная система часов с периодами $1, \frac{1}{2}, \frac{1}{4}, \dots, \frac{1}{2^n}, \dots$

Как описать все возможные циферблаты?

$S^1_{H_2} = H_2/\mathbb{Z}$ — группа $\Rightarrow$ Найти $\mathrm{Aut}(H_2/\mathbb{Z}, H_2/\mathbb{Z})$

$H_2 \subset \mathbb{Q}$ состоит из чисел вида $\frac{m}{2^n}$, $n = 0,1,2,\dots$, $m \in \mathbb{Z}$




## ③ p-адические целые числа $\mathbb{Z}_p$

*Определение* $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z}$, $k \in \mathbb{N}$

*Что это означает:*

$$\mathbb{Z}/p\mathbb{Z} \leftarrow \mathbb{Z}/p^2\mathbb{Z} \leftarrow \mathbb{Z}/p^3\mathbb{Z} \leftarrow$$

$$\mathbb{Z}_p \ni r = (a_0, a_1, a_2, \dots)$$

$a_k \bmod p^k = a_{k-1}$

*Как с этим работать*

$a_0 =: r_0$

$a_1 = r_0 + r_1 p$

$\dots$

$a_k = r_0 + r_1 p + r_2 p^2 + \dots + r_k p^k$

Запись в p-ичной системе счисления $\longrightarrow$ $r = \dots r_2 r_1 r_0$

бесконечная влево „p-ичная дробь"

## ④ Упр. сложение и умножение в $\mathbb{Z}_p$ можно производить „в столбик" в p-ичной записи

*Пример:* $p = 2$

$\mathbb{Z} \subset \mathbb{Z}_p$

$(1) + 1 = 0$ в $\mathbb{Z}_2$

$(1) = -1$

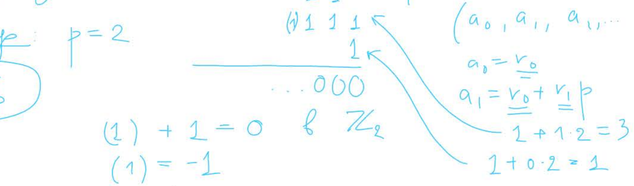
$(a_0, a_1, a_2, \dots)$

$a_0 = r_0$

$a_1 = r_0 + r_1 p$

$1 + 1 \cdot 2 = 3$

$1 + 0 \cdot 2 = 1$




*Упр.* $(1) \cdot (1) = 1$

*Свойства (упр.)*

(1) $\mathbb{Z}_p$ — кольцо

(2) $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$

$n \mapsto (n \bmod p, n \bmod p^2, \dots)$

Описать последовательности $\dots r_2 r_1 r_0$ в $\mathbb{Z}$.

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

*Вопрос:* как устроено подобную „периодическую дробь"?

## ⑤ Поле p-адических чисел $\mathbb{Q}_p \supset \mathbb{Z}_p$

$p^k\ p^{k-1}\ \dots\ p\ 1\ p^{-1}\ p^{-2}\ p^{-5}$

Неформальный смысл: $\dots r_k r_{k-1} \dots r_0, r_{-1} r_{-2} \dots r_{-5}$

*Вопрос* Почему $0,(9) = 1$?

$$\frac{9}{10} + \frac{9}{10^2} + \frac{9}{10^3} + \dots = 1$$

$$\left| 1 - \left(\frac{9}{10} + \dots + \frac{9}{10^k}\right) \right| \le \frac{1}{10^k}$$

$\downarrow$

$a$

$0 + \delta$

$\varepsilon = \frac{1}{n}$ $\quad 0 \in \left(-\frac{1}{n}, \frac{1}{n}\right)$

Аксиома полноты

~~Аксиома Архимеда~~

$9 + 9^2 + 9^3 + \dots + 9^k = a_k$

$\lim_{k \to \infty} a_k = a$

$9a + 9 = a$

$\to a = -\frac{9}{8}$

## ⑥