A-I Лекция 9

Тригонометрические суммы. Уравнения над конечными полями

Енина Анна, 491 группа

Москва, 11 ноября 2025

Рассмотрим уравнения над конечным полем $\mathbb{F}_p$. Для начала изучим простое уравнение:

$$x^2 + y^2 \equiv 1 \pmod{p}$$

Количество решений этого уравнения в поле $\mathbb{F}_p$ обозначим как $N_p(x^2 + y^2 = 1)$.

Известно, что для уравнения $x^2 = a$ в конечном поле выполняется:

$$N_p(x^2 = a) = 1 + \left(\frac{a}{p}\right)$$

где $\left(\frac{a}{p}\right)$ – символ Лежандра.

Рассмотрим теперь более общее уравнение:

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

Количество решений можно выразить через сумму символов Лежандра:

$$N_p(x^2 + y^2 = 1) = \sum_{\substack{a,b \in \mathbb{F}_p \\ a+b=1}} N_p(x^2 = a) \cdot N_p(y^2 = b)$$

Используя свойства характеров конечных полей, получаем:

$$N_p(x^2 + y^2 = 1) = \sum_{a+b=1} \left(1 + \left(\frac{a}{p}\right)\right) \cdot \left(1 + \left(\frac{b}{p}\right)\right)$$

$$= \sum_{a+b=1} 1 + \sum_{a} \left(\frac{a}{p}\right) + \sum_{b} \left(\frac{b}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

В этой сумме второе и третье слагаемые равны нулю, а количество пар a, b, таких, что $a+b = 1$, равно p.

Опр. Пусть χ, λ - мультипликативные характеры. Тогда $J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b)$ - **матрица Якоби**.

Теорема. (свойства матрицы Якоби) Пусть χ, λ - не главные характеры, χ_0 - главный, тогда выполняются следующие утверждения:

1. $J(\chi_0, \chi_0) = p$
2. $J(\chi, \chi_0) = 0$
3. $J(\chi, \lambda^{-1}) = -\chi(-1)$
4. Если $\chi\lambda \neq \chi_0$, то $J(\chi, \lambda) = \frac{G(\chi) * G(\lambda)}{G(\chi\lambda)}$

Следствие. Пусть χ, λ такие, что $\chi\lambda \neq \chi_0$, тогда верно: $|J(\chi, \lambda)| = \sqrt{p}$

Пример: $N_p(x^2+y^2=1) = \begin{cases} p-1 & , p \equiv 1(4) \\ p+1 & , p \equiv 3(4) \end{cases}$

Теперь рассмотрим общий случай: $x^n + y^n = 1$ и пусть $p \equiv 1(m)$

Тогда

$$N_p(x^n + y^n = 1) = \sum_{a+b=1} N_p(x^n = a) N_p(y^n = b)$$

Используем $N(x^n = a) = \sum_{\chi^n = \chi_0}(\chi(a))$, и то, что n делит $p-1$, тогда при χ_1 - порождающий главный характер

из этого следует, что

$$N_p(x^n + y^n = 1) = \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} J(\chi^i, \chi^j)$$

Теорема.

Для уравнения $x^n + y^n = 1$ в конечном поле $\mathbb{F}_p$:

$$N_p(x^n + y^n = 1) = p + 1 + O_n(\sqrt{p})$$

Введем Обозначение:

Символ Ландау:

$$f(n) = o(g(n)) \quad \text{означает} \quad \exists C : |f(n)| < C|g(n)|$$

Свойства тригонометрических сумм

Сумма характеров:

$$\sum_{\chi=1}^{p} e^{2\pi i \frac{a\chi}{p}} = \begin{cases} p, & a \equiv 0 \pmod p \\ 0, & a \not\equiv 0 \pmod p \end{cases}$$

Общая постановка задачи:

Пусть $F(x_1, \ldots, x_n) \in \mathbb{F}_p[x_1, \ldots, x_n]$ — многочлен над конечным полем. Требуется найти количество решений:

$$N_p(F = 0) - ?$$

Для квадратичных форм:

$$F(x_1, \ldots, x_n) \approx O(p)$$

Метод тригонометрических сумм:

Используем формулу:

$$\sum_{x_1,\dots,x_n}\sum_{y} e^{2\pi i\frac{y}{p}F(x_1,\dots,x_n)} = \begin{cases} p, & F(x_1,\dots,x_n)\equiv 0 \pmod p \\ 0, & F(x_1,\dots,x_n)\not\equiv 0 \pmod p \end{cases}$$

Отсюда получаем формулу для количества решений:

$$N_p(F=0) = \frac{1}{p}\sum_{x_1,\dots,x_n}\sum_{y} e^{2\pi i\frac{y}{p}F(x_1,\dots,x_n)}$$

Асимптотическое поведение:

Теорема. (без д-ва) Для многочлена F общего положения:

$$N_p(F=0) = p^{n-1} + O(p^{n-1-\frac{1}{2}})$$

Теорема(Хассе-Вейла).

Рассмотрим многочлен $F \in \mathbb{F}_p[x,y]$. Количество решений уравнения $F=0$ оценивается как:

$$N_p(F=0) = p+1+O(\sqrt{p})(2g\sqrt{p})$$

Лемма. Пусть $d=(r,p-1)$, $z\neq 0$. Тогда:

$$N_p(x^r=z) = \sum_{s=0}^{d-1}\chi_s(z)$$

где $\chi_0,\chi_1,\dots,\chi_{d-1}$ — характеры, и $\chi^d=\chi_0$.

Д-во: Пусть $\mathbb{F}_p^* =< \eta >$ Рассмотрим замену переменных:

$$x^r = z, \quad z=\eta^k, \quad x=\eta^n$$

тогда и только тогда, когда $rn\equiv k(p-1)$

из этого следует:

$$N_p(x^r=z) = \begin{cases} d, & d\mid k \\ 0, & dk \end{cases}$$

С другой стороны:

Характер порядка d определяются как:

$$\chi_s(z) = e^{2\pi i \frac{ks}{d}} \quad \text{при } z = \eta^k, \quad 0 \le s \le d-1$$

$$\sum_{s=0}^{d-1} \chi_s(z) = \begin{cases} d, & d \mid k \\ 0, & dk \end{cases}$$

Уравнения над конечными полями

Теорема.

Рассмотрим линейную форму над конечным полем $\mathbb{F}_p$:

$$F(x_1, \ldots, x_n) = a_1 x_1 + \cdots + a_n x_n$$

где $a_i \in \mathbb{F}_p^*$ — ненулевые коэффициенты.

Обозначим количество решений уравнения $F = 0$ как:

$$N_p = N_p(F = 0)$$

Имеет место оценка:

$$|N_p - p^{n-1}| \le C(p-1)p^{\frac{n}{2}-1}$$

Док-во:

Выразим количество решений через тригонометрические суммы:

$$N_p(F) = p^{n-1} + \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \sum_{x_1, \ldots, x_r \in \mathbb{F}_p} e^{2\pi i \frac{y}{p}(a_1 x_1 + \cdots + a_r x_r)}$$

Или в более компактной форме:

$$N_p(F) = p^{n-1} + \frac{1}{p} \sum_{y \in \mathbb{F}_p^*} \prod_{i=1}^{n} \sum_{x_i \in \mathbb{F}_p} e^{2\pi i \frac{y a_i x_i^{r_i}}{p}}$$

Для каждого $x \in \mathbb{F}_p$:

$$\sum_{x\in\mathbb{F}_p} e^{2\pi i\frac{ax^r}{p}} = \sum_z N_p(x^r = z)e^{2\pi i\frac{az}{p}} = 1 + \sum_{z\neq 0}\sum_{s=0}^{d-1}\chi_s(z)e^{2\pi i\frac{az}{p}}$$

$$= 1 + \sum_{z=0}\chi_0(z)e^{2\pi i\frac{az}{p}} + \sum_{z\neq 0}\sum_{s=1}^{d-1}\chi_s(z)e^{2\pi i\frac{az}{p}} = \sum_{s=1}^{d-1} a(\chi_s)$$

Используя свойства характеров и сумм Гаусса, получаем:

$$|N_p - p^{n-1}| \leq \frac{1}{p}\sum_{y\neq 0}\left|\prod_{i=1}^{n}\sum_{j=1}^{d-1} G_a(\chi_{ij})\right| = \frac{1}{p}(p-1)Cp^{\frac{n}{2}}$$

При условии:

$$\prod_{i=1}^{n}|d_i| = 1$$

Количество решений квадратичных уравнений над конечными полями

Случай квадратичной формы

Теорема. Для уравнения суммы квадратов в конечном поле $\mathbb{F}_p$:

$$N_p(x_1^2 + \ldots + x_n^2 = 1) = \begin{cases} p^{n-1} + (-1)^{\frac{n-1}{2}\frac{p-1}{2}}p^{\frac{n-1}{2}}, & n \equiv 1 \pmod 2 \\ p^{n+1} + (-1)^{\frac{n}{2}\frac{p-1}{2}}p^{\frac{n}{2}-1}, & n \equiv 0 \pmod 2 \end{cases}$$

поле $\mathbb{F}_q$, где $q = p^s$ — степень простого числа.

Лемма. Пусть $m \in \mathbb{Z}$ и определим сумму:

$$S(m) = \sum_{x\in\mathbb{F}_q^*}\chi$$

в $\mathbb{F}_q$

Тогда:

$$S(m) = \begin{cases} -1, & q-1|m(p) \\ 0, & \text{q-1 m (p)} \end{cases}$$

Док-во:

рассмотрим случай $q-1|m(p)$

$$\forall x \in \mathbb{F}_q^* : x^{q-1} = 1$$

Для характера χ и $x \in \mathbb{F}_q^*$:

$$\chi^m = 1 \quad \Rightarrow \quad S(m) = (q-1) \cdot 1 = -1$$

Если существует $\alpha \in \mathbb{F}_q^*$ такой, что $\alpha^m \neq 1$, то:

$$S(m) = \sum (ax)^m = a^m \zeta(m)$$

что влечёт $\zeta(m) = 0$.

Следствие.

Пусть $\Phi(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ – многочлен от s переменных над конечным полем $\mathbb{F}_q$, причём $\deg \Phi \leq n \cdot (q-1)$.

Тогда сумма значений многочлена по всем точкам пространства:

$$\sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \Phi(x_1, \ldots, x_n) = 0$$

в $\mathbb{F}_q$.

Д-во:

Введём:

$$\Phi = (x_1^{k_1}, \cdots, x_s^{k_s})$$

Рассмотрим сумму мономов:

$$\sum_{x_1,\ldots,x_s \in \mathbb{F}_q} x_1^{n_1} \cdots x_s^{n_s} = \left(\sum_{x_1 \in \mathbb{F}_q} x_1^{k_1} \right) \cdots \left(\sum_{x_s \in \mathbb{F}_q} x_s^{k_s} \right)$$

$$k_1 + \cdots + k_s \leq n(q-1)$$

и $S \leq n$.

Если существует $k_i < d-1$, то для суммы:

$$\sum_{x \in \mathbb{F}_q} x^{k_i} = 0$$

при условии, что k_i не делится на q.

Теорема(Варинга). Пусть $F \in \mathbb{F}_q[x_1, \ldots, x_n]$ – многочлен от n переменных над конечным полем $\mathbb{F}_q$, где $q = p^s$, и пусть $\deg F = r < n$.

Тогда p делит $N_q(F)$

Док-во:

$$\Phi(x_1, \ldots, x_s) = 1 - F(x_1, \ldots, x_n)^{q-1}$$

и

$$\deg \Phi = r(q-1) < n(q-1)$$

Из того, что:

$$\sum_{x_1,\ldots,x_n \in \mathbb{F}_q} \Phi(x_1, \ldots, x_n) = N_q(F) \cdot 1 \Rightarrow p \mid N_q(F)$$

Теорема(Шавали). Пусть $F \in \mathbb{F}_q[x_1, \ldots, x_n]$ – многочлен от n переменных над конечным полем $\mathbb{F}_q$, и $\deg F = r < n$.

Тогда уравнение $F = 0$ имеет нетривиальное решение в $\mathbb{F}_q^{\infty}$.

Док-во: $F(0, \ldots, 0) = 0$, то:

$$N_q(F) \geq 1 \Rightarrow N_q(F) > p$$