Семинар 3. Суммы Гаусса и Якобшталя

Введение в теорию чисел, весенний семестр 2024 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Через p обозначается простое число.

Задача 1. Докажите, что символ Лежандра мультипликативен, то есть

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

для каждой пары ненулевых вычетов a и b.

Задача 2. (а) Пользуясь квадратичным законом взаимности, вычислите символ Лежандра:

$$\left(\frac{599}{701}\right).$$

(б) Является ли 449 квадратичным вычетом по модулю 701?

(в) Напишите явную формулу для символа Лежандра:

$$\left(\frac{-1}{p}\right).$$

(г) При каких условиях на p число 2 является полным квадратом по модулю p?

Задача 3. Для каждого p определим (квадратичную) сумму Гаусса формулой:

$$G(p) = \sum_{a\in\mathbb{F}_p\setminus\{0\}} \left(\frac{a}{p}\right) e^{\frac{2\pi i a}{p}}.$$

(а) Найдите $G(3)$.

(б) Покажите, что $G(5)^2 = 5$.

(в) Покажите, что $G(7)^2 = -7$.

(г) Докажите, что $|G(p)^2| = p$ для всех простых p.

Задача 4 ($\star$)**.** Пусть $a \in \mathbb{F}_p$. Определим сумму Якобшталя по формуле:

$$J(a) = \sum_{x\in\mathbb{F}_p\setminus\{0\}} \left(\frac{x}{p}\right)\left(\frac{x^2+a}{p}\right).$$

(а) Докажите, что $J(a) = \left(\frac{b}{p}\right) J(ab^2)$ для всех $x \in \mathbb{F}_p\setminus 0$.

(б) Докажите, что

$$\sum_{a=1}^{p} J^2(a) = \frac{p-1}{2}\left(J^2(R) + J^2(N)\right),$$

где R и N — произвольные квадратичные вычет и невычет, соответственно, по модулю p.

(в) Докажите, что

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

(г) Пусть $p = 4k+1$. Выведите из пунктов (б) и (в), что p представляется в виде суммы двух квадратов, выразив квадраты через суммы Якобшталя.

(д) Пусть $p = 4k+3$. Найдите простую явную формулу для сумм Якобшталя.

Задача 5 ($\star$)**.** Для слова S из букв R и N обозначим через $n_p(S)$ количество подслов вида S в слове W_p (определённом в листке для семинара 1).

(а) Проверьте, что

$$n_p(RRR) = \sum_{j=1}^{p-4} \prod_{i=1}^{3} \frac{1}{2} \left(1 + \left(\frac{i+j-1}{p} \right) \right)$$

(б) Выразите $n_p(RRR)$ через сумму Якобшталя $J(1)$.

(в) Выразите $n_p(S)$ через $J(1)$ для всех слов длины три.

Задача 6 ($\star$)**.** (а) Выразите количество решений уравнения $y^2 = x^3 - x$ над $\mathbb{F}_p$ через сумму Якобшталя $J(1)$.

(б) Как поменяется ответ, если вместо кривой $y^2 = x^3 - x$ рассмотреть кривую $y^2 = x^3 - ax$, где $a \in \mathbb{F}_p \setminus \{0\}$?