Семинар 3. Суммы Гаусса и Якоби

Введение в теорию чисел, весенний семестр 2023 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Определение 1. *Пусть p простое число.* Характер (по модулю p) — *это гомоморфизм $\mathbb{F}_p^* \to \mathbb{C}^*$ мультипликативных групп.*

Характер χ называется нетривиальным, *если существует $a \in \mathbb{F}^*$, такое что $\chi(a) \neq 1$.*

Если χ — это характер, определим сопряженный характер *по формуле $\overline{\chi}(a) = \overline{\chi(a)}$.*

Определение 2. *Пусть χ — это характер. Определим его сумму Гаусса $G(\chi)$ по формуле*

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

(Объясните, в каком смысле нужно понимать возведение комплексного числа в степень $a \in \mathbb{F}_p$.)

Задача 1. Докажите что сумма Гаусса удовлетворяет следующим свойствам:

(а) $\overline{G(\chi)} = \chi(-1) G(\overline{\chi})$;

(б) Если χ нетривиальный, то:

$$G(\chi) G(\overline{\chi}) = \chi(-1) p;$$

(в) Если χ нетривиальный, то модуль комплексного числа $G(\chi)$ равен $\sqrt{p}$.

Определение 3. *Пусть χ и φ — два характера. Определим их сумму Якоби по формуле*

$$J(\chi, \varphi) = \sum_{a \in \mathbb{F}_p \setminus \{0,1\}} \chi(a) \varphi(1-a).$$

Задача 2. Пусть χ, φ и $\chi\varphi$ — нетривиальные характеры.

(а) Верна следующая формула:

$$J(\chi, \varphi) = \frac{G(\chi) G(\varphi)}{G(\chi\varphi)}.$$

(б) Модуль комплексного числа $J(\chi, \varphi)$ равен $\sqrt{p}$.

Задача 3. Вспомните определение гамма- и бета-функций из курса анализа. Объясните, почему сумму Гаусса и сумму Якоби можно рассматривать как аналоги гамма- и бета-функции, соответственно? Аналогом какого утверждения является пункт (а) предыдущей задачи?

Задача 4. Пусть p — простое число вида $4k+1$. Зафиксируем первообразный корень g по модулю p, и обозначим через χ характер, который переводит g в i.

(а) Квадрат характера χ совпадает с символом Лежандра.

(б) Если $J(\chi, \chi^2) = a + bi$, то $p = a^2 + b^2$.

(в) Как связанны между собой $J(\chi, \chi^2)$ и $J(\chi, \chi)$?

Задача 5. Пусть p — простое число вида $4k+1$. Докажите что количество решений уравнения $y^2 = x^3 - x$ над $\mathbb{F}_p$ равно

$$p + J(\chi, \chi^2) + \overline{J(\chi, \chi^2)}.$$

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

Задача 6. Пусть $a \in \mathbb{F}_p$. Определим сумму Якобсталя по формуле:

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

Выразите $I(a)$ через суммы Якоби.

Задача 7. Сформулируйте и докажите аналоги задач 4 и 5 для простых вида $3k+1$.