Задачи к спецкурсу "Введение в тригонометрические суммы" , 2015

Шкредов И.Д.

Предупреждение: задачи сильно разнятся по сложности.

1. Чему равна (полная) сумма символов Лежандра?

2. Найти сумму в зависимости от значения a

$$\sum_{x\in \mathbf{F}_p} \left(\frac{x(x+a)}{p}\right) .$$

3. Найти сумму в зависимости от значения дискриминанта b^2-4ac

$$\sum_{x\in \mathbf{F}_p} \left(\frac{ax^2+bx+c}{p}\right) .$$

4. Найти максимальное расстояние между двумя вершинами в графе Пэли.

5. Сколько существует вычетов в $\mathbb{Z}_p$ у которых сосед (правый/левый/оба) — невычет?

6. Пусть k — ненулевое число. Сумма

$$S(k) = \sum_{x\in \mathbf{F}_p} \left(\frac{x^3+kx}{p}\right)$$

называется *суммой Якобсталя*. Доказать, что

1) Для $p\equiv -1 \pmod 4$ эта сумма равна нулю, а для $p\equiv -1 \pmod 4$ сумма Якобсталя — четное число.

2) Имеем $S(a^2k) = \left(\frac{a}{p}\right) S(k)$.

3) Если $\left(\frac{k}{p}\right) = 1$ и $\left(\frac{l}{p}\right) = -1$, то

$$\left(\frac{1}{2}S(k)\right)^2 + \left(\frac{1}{2}S(l)\right)^2 = p\,.$$

Вывести отсюда, что любое простое вида $p\equiv -1 \pmod 4$ представляется в виде суммы двух квадратов.

7. (Дискретное преобразование Фурье) Пусть $f : \mathbb{Z}_N \to \mathbb{C}$ — некоторая функция. Определим преобразование Фурье формулой

$$\widehat{f}(r) = \sum_{x\in \mathbb{Z}_N} f(x)e(-rx)\,,$$

Тогда справедливы формулы

$$N\sum_x |f(x)|^2 = \sum_r |\widehat{f}(r)|^2 \qquad \textbf{(равенство Парсеваля)}\,.$$

$$f(x) = \frac{1}{N}\sum_r \widehat{f}(r)e(rx) \qquad \textbf{(формула обращения)}\,.$$

Пусть $g : \mathbb{Z}_N \to \mathbb{C}$ — другая функция. Тогда

$$N\sum_x f(x)\overline{g(x)} = \sum_r \widehat{f}(r)\overline{\widehat{g}(r)}$$

8. Пусть $f, g : \mathbb{Z}_N \to \mathbb{C}$ — некоторые функции. *Сверткой* функций f и g называется функция $(f * g)(x)$, вычисляемая по формуле

$$(f * g)(x) = \sum_s f(s)g(x-s)\,.$$

Преобразование Фурье свертки функций f и g, то есть $\widehat{(f*g)}(r)$ $(= (f*g)\widehat{\ }(r))$ вычисляется по формуле

$$\widehat{(f*g)}(r) = \widehat{f}(r)\widehat{g}(r)\,.$$

9. Выразить число решений уравнения $c_1x_1 + \cdots + c_kx_k = 0$, где $x_k \in A$ через преобразование Фурье характеристической функции A.

10. Пусть P — произвольная арифметическая прогрессия в $\mathbf{F}_p$ с шагом 1. Доказать, что $|\widehat{P}(r)| \leq \frac{4p}{|r|}$.

11. Пусть $A, B \subseteq \mathbf{F}_p$ и $|A||B| > p$. Доказать, что $(A-A)\cap(B-B) \neq \emptyset$. Придумать элементарное доказательство и доказательство с помощью анализа Фурье.

12. Если множество $E \in \mathbb{Z}_p$ такое, что $E + x \subseteq E$, $x \neq 0$, то $E = \mathbb{Z}_p$. Придумать элементарное доказательство и доказательство с помощью анализа Фурье.

13. Как связаны коэффициенты Фурье множества и его дополнения?

14. Пусть A — подмножество $\mathbf{F}_p$ размера меньше, чем $0.1\log p$. Доказать, что найдется такое $x \neq 0$ такое, что xA лежит от 0 до $p/2$.

15. Для произвольного множества $A \subseteq \mathbb{Z}_p$ положим $Q[A] := (A-A)/(A-A)\setminus\{0\}$. Доказать, что если $|A| > \sqrt{p}$, то $Q[A] = \mathbb{Z}_p$. Вывести отсюда оценку Виноградова для минимального квадратичного невычета.

16. Доказать

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2+$$

$$+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2\,.$$

17. Пусть

$$T(a) = \sum_{x\in\mathbf{F}_p} e(x^n + ax)\,.$$

Найти $\sum_a |T(a)|^2$.

18. Пусть

$$T(a) = \sum_{x\in\mathbf{F}_p} e(ax^n)\,.$$

Найти $\sum_a |T(a)|^2$.

19. Выражение

$$G(a) = \sum_{x\in\mathbf{F}_p} e(ax^2)$$

называется *суммой Гаусса.* Доказать, что

$$G(a) = \sum_{x \in \mathbf{F}_p} \left(\frac{x}{p}\right) e(ax) = \left(\frac{a}{p}\right) G(1)\,.$$

20. Выразить через суммы Гаусса триг. сумму $\sum_{x \in \mathbf{F}_p} e(ax^2 + bx + c)\,.$

21. Пусть $p > 2$ — простое число. Доказать, что

1) $G^2(1) = p$.
2) $|G(a)| = \sqrt{p}$.
3) (без доказательства).

$$G(1) = \begin{cases} \sqrt{p} & \text{если } p \equiv 1 \pmod 4 \\ i\sqrt{p} & \text{если } p \equiv 3 \pmod 4 \end{cases}$$

22. Пусть $a \neq 0$ — любое число. Возведением в квадрат доказать, что

$$|\sum_{x \in \mathbf{F}_p} e(ax^3)| \leq 2p^{3/4}\,.$$

23*. Пусть $a \neq 0$ — любое число. Доказать, что

$$|\sum_{x \in \mathbf{F}_p} e(ax^d)| \leq (d-1)\sqrt{p}\,.$$

24. Пусть Γ — мультипликативная подгруппа в $\mathbf{F}_p$. Доказать, что для всех $r \neq 0$ выполнено $|\widehat{\Gamma}(r)| < \sqrt{p}$.

25. Пусть Γ — мультипликативная подгруппа в $\mathbf{F}_p$, $|\Gamma| > p^{3/4}$. Доказать, что любой ненулевой элемент $\mathbf{F}_p$ представляется в виде суммы двух элементов Γ.

26. Доказать теорему Ферма в конечном поле, то есть, что для любого n и для всех достаточно больших p найдутся ненулевые $x, y, z \in \mathbf{F}_p$ такие, что $x^n + y^n \equiv z^n \pmod p$.

Нерешенные задачи.

1*. (Гипотеза Виноградова) Доказать, что минимальный квадратичный вычет/невычет в $\mathbb{Z}_p$ меньше чем p^ε для любого $\varepsilon > 0$.

2*. (Дискретная проблема Какеи для вычетов) Пусть $A \subseteq \mathbb{Z}_p^*$ — некоторое множество, $|A| = (p-1)/2$. Пусть также $|Q| = (p-1)/2$ — произвольное множество. Верно ли, что для некоторого $q \in Q$ минимальный элемент множества qA меньше чем p^ε для любого $\varepsilon > 0$?

3*. (Вопрос Алона) Пусть $A \subseteq \mathbb{Z}/p\mathbb{Z}$ — произвольное множество, $|A| \geq c\sqrt{p}$, где $c > 0$ — некоторая маленькая абсолютная константа (например, $c = 1/100$). Могут ли все числа из множества $A - A$ быть квадратичными вычетами/невычетами? Тот же вопрос, но пусть, дополнительно, известно, что все суммы $A - A$ — различные.

4*. (Возвращаемость на торах) Пусть множество $S \subseteq \mathbb{Z}_p$ — синдетическое, то есть расстояние между его любыми соседними элементами ограничено сверху некоторой абсолютной константой d. Доказать, что $S + S$ содержит арифметическую прогрессию длины $p^{\varepsilon(d)}$, где величина $\varepsilon(d) > 0$ зависит только от d.

5*. (Двойственные суммы–произведений) Пусть $A \subseteq \mathbb{Z}_p$ — произвольное множество, $|A| > p^\varepsilon$, $\varepsilon > 0$. Доказать, что найдется l, зависящее только от ε такое, что $(lA)^l = \mathbb{Z}_p^*$.