Арифметика VI: Суммы Гаусса и Якоби

Задача 1. а) Чему равна сумма k-х степеней всех корней n-й степени из единицы в $\mathbb{C}$?
б) Чему равна сумма k-х степеней всех элементов $\mathbb{F}_p$? в*) ...$\mathbb{F}_q$?

▷ Все переменные далее лежат в $\mathbb{F}_p$. Через $\#\{F(x)=0\}$ обозначается число решений уравнения $F(x)=0$.

Задача 2. Пусть F — однородный многочлен степени d от n переменных.
а) $\#\{F=0\} = \sum_{x\in\mathbb{F}_p^n}(1-F^{p-1}) \pmod p$.
б) Если $d<n$, уравнение $F(x)=0$ имеет ненулевое решение ("т-ма Шевалле–Варнинга").

Задача 3. Чему равна сумма а) $\sum\limits_t \left(\frac{t}{p}\right)$; б) $\sum\limits_t \left(\frac{t}{p}\right)\left(\frac{t+c}{p}\right)$; в) $\sum\limits_{s+t=1} \left(\frac{s}{p}\right)\left(\frac{t}{p}\right)$?

Задача 4. а) Сколько решений имеет уравнение $x^2+y^2=1$?
б) Сколько точек может быть на квадрике в $\mathbb{P}^2(\mathbb{F}_p)$?

▷ **Определение 1.** *Мультипликативным характером* по модулю n называется гомоморфизм $\chi\colon (\mathbb{Z}/n)^\times \to \mathbb{C}^\times$; будем также рассматривать χ как отображение $\mathbb{Z}\to\mathbb{C}$, нулевое на необратимых остатках. Пример: квадратичный характер $\left(\frac{-}{p}\right)$.

Задача 5. а) Нетривиальный характер по модулю p, такой что $\chi^d=1$, существует тогда и только тогда, когда $d|p-1$. В этом случае он может быть задан формулой $\left(\frac{-}{p}\right)_d\colon \lambda^n \to \exp(2\pi i n/d)$, где λ — некоторая образующая $\mathbb{F}_p^\times$. б) $\#\left\{x^d=a\right\} = \sum\limits_{\chi^d=1}\chi(a)$.

Задача 6. $\#\left\{x^3+y^3=1\right\} = p-2+2\,\mathrm{Re}\sum\limits_{x+y=1}\left(\frac{x}{p}\right)_3\left(\frac{y}{p}\right)_3$.

▷ **Определение 2.** Комплексное число

$$J_a(\chi,\chi') = \sum_{x+y=a}\chi(x)\chi'(y).$$

называется *суммой Якоби* (соответствующей данной паре характеров). Вместо $J_1(\chi,\chi')$ будем писать просто $J(\chi,\chi')$.

▷ **Определение 3.** Напомним, что *суммой Гаусса*, соответствующей характеру χ по модулю p, называется комплексное число

$$g_a(\chi) = \sum \chi(t)\zeta_p^{at},$$

где ζ_p — примитивный корень степени p из 1. Вместо $g_1(\chi)$ будем писать просто $g(\chi)$.

Задача 7. Пусть χ — нетривиальный характер.
а) $g_a(\chi) = \chi(a^{-1})g(\chi)$; б) $\sum_a g_a(\chi)\overline{g_a(\chi)} = (p-1)p$; в) $|g(\chi)| = \sqrt{p}$.

Задача 8. а) $J(\chi,\chi') = \dfrac{g(\chi)g(\chi')}{g(\chi\chi')}$ (если произведение $\chi\chi'$ нетривиально).
б) $|J(\chi,\chi')| = \sqrt{p}$, $J(1,1)=p$, $J(1,\chi)=0$, $J(\chi,\chi^{-1}) = -\chi(-1)$ (считая, что $\chi,\chi',\chi\chi'\neq 1$).

Задача 9. а) $\#\{x^3+y^3=1\} \approx p-2\pm 2\sqrt{p}$;
б) $\#\{x^n+y^n=1\} \approx p+1-\#\{x^n+1=0\} \pm (n-1)(n-2)\sqrt{p}$.

Задача 10. а) Если $p=4k+1$, то p представимо в виде суммы двух квадратов целых чисел ("рождественская теорема Ферма"). Указание. Если $a+bi = J(\chi,\chi^2)$, то $p=a^2+b^2$.
б) $\#\{y^2=x^3-x\} = p+2a$. в) $a = \dfrac{1}{2}\dbinom{2k}{k} \pmod p$ ("явная формула Гаусса").