# Задачи (v12.07)

▷ Все уравнения рассматриваются по модулю $p > 2$, если явно не сказано иного.

▷ Напоминание:
• $\#\{x^2 = a\} = 1 + \left(\frac{a}{p}\right)$; • $\sum \left(\frac{a}{p}\right) = 0$; • $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; • $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$.

**Задача 1.** Будем говорить, что простое $p$ делит многочлен $f \in \mathbb{Z}[x]$, если $p \mid f(n)$ для некоторого $n$.
а) Опишите все простые делители многочлена $x^2 + 1$.
б) Докажите, что их бесконечно много.

**Задача 2.** а) Сколько решений (в зависимости от $d$ и $p$) имеет уравнение $x^2 + dy^2 = 1$?
б) Сколько у кривой $x^2 + dy^2 = 1$ бесконечно удаленных точек?

**Задача 3.** Выясните, для каких простых $(2/p) = 1$, рассматривая разбиение решений $x^2 + y^2 = 1$ на группы $\{(\pm x, \pm y), (\pm y, \pm x)\}$.

**Задача 4.** а) Найдите число точек на сфере $x^2 + y^2 + z^2 = 1$.
б) Выясните, пользуясь этим, для каких простых $(3/p) = 1$.

**Задача 5.** а) Чему равна сумма всех квадратичных вычетов mod $p$?
б) Чему равна сумма $k$-х степеней всех остатков mod $p$?

**Задача 6.** Пусть $a$ — случайный квадратичный вычет по модулю $p$. На сколько вероятность того, что $(a + 1)$ — тоже квадратичный вычет, отличается от $1/2$?

**Задача 7.** Сколько решений имеет уравнение $y^2 = x^3 - ax^2$?

**Задача 8.** Сколько решений имеет уравнение $y^2 = x^3 - x$ при $p = 4k+3$?

**Задача 9.** Пусть функция $e(p)$ такова, что для каждого кубического многочлена $f$ уравнение $y^2 = f(x)$ имеет не более $p + e(p)$ решений. Тогда каждое такое уравнение имеет не менее $p - e(p)$ решений.

**Задача 10.** Положим $S(x) = f(x)(f(x)^{(p-1)/2} - 1) - f'(x)(x^p - x)/2$.
а) Пусть $\left(\frac{f(a)}{p}\right) = 1$. Докажите, что $a$ — *кратный* корень многочлена $S$.
б) Пусть $\deg f = 3$. Докажите, что $\#\{y^2 = f(x)\} < 3p/2 + \text{const}$

Вместе с предыдущей задачей это доказывает и оценку снизу, в т. ч. существование решений.