Квадратичный закон взаимности, p-адические числа

Напомним, что *символ Лежандра* $\left(\frac{a}{p}\right)$ определяется как

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p; \\ 1, & \text{если } a \text{ квадратичный вычет по модулю } p; \\ -1, & \text{если } a \text{ квадратичный невычет по модулю } p. \end{cases}$$

Как мы знаем, 1) $\#\{x \in \mathbb{F}_p \mid x^2 = a\} = 1 + \left(\frac{a}{p}\right)$; 2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; 3) $\sum_a \left(\frac{a}{p}\right) = 0$.

3.1. а) Найдите число решений уравнения $x^2 + y^2 = 1$ в $\mathbb{F}_p$ (возможно, по пути придется вычислить сумму $\sum_t \left(\frac{t}{p}\right)\left(\frac{1-t}{p}\right)$).

б) Выразите $\left(\frac{2}{p}\right)$ через остаток от деления p на 8 (указание: почти все решения предыдущего уравнения разбиваются на восьмерки $\{(\pm x, \pm y), (\pm y, \pm x)\}$).

3.2. Пусть p, q — нечетные простые числа. Обозначим через S_p^q число решений уравнения $x_1^2 + \ldots + x_q^2 = 1$ в $\mathbb{F}_p$.

а) $S_p^q = 0 \pmod q \iff \left(\frac{q}{p}\right) = -1$.

б) Вычислите S_p^q (должно получиться примерно p^{q-1}).

в) Выведите из предыдущих пунктов *квадратичный закон взаимности*:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

* * *

$\mathbb{Z}_p$ — кольцо целых p-адических чисел, $\mathbb{Q}_p$ — его поле частных.

3.3. а) Вычислите $1/4$ в $\mathbb{Z}_7$.

б) Вычислите первые 4 знака квадратного корня из 2 в $\mathbb{Z}_7$.

в) Сходится ли в $\mathbb{Q}_p$ ряд $1 - p + p^2 - p^3 + \ldots$? Если да, то к чему?

3.4. а) Если $f \in 1 + xk[[x]]$, то из f можно извлечь корень степени n.

б) Если $a \in 1 + p\mathbb{Z}_p$, $(n, p) = 1$, то из a можно извлечь корень степени n.

3.5. а) $\mathbb{R}^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{R}$.

б) $\mathbb{Z}_p^\times \cong (\mathbb{Z}/(p-1)\mathbb{Z}) \oplus \mathbb{Z}_p$ при $p \neq 2$.

в) Сформулируйте и докажите аналогичное утверждение про $\mathbb{Z}_2$.

г) Найдите $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

3.6. Пусть $u, v \in (\mathbb{Z}/p\mathbb{Z})^\times$.

а) Уравнение $ux^2 + vy^2 = 1$ имеет решение в $\mathbb{Q}_p$.

б) Уравнение $ux^2 + py^2 = 1$ имеет решение в $\mathbb{Q}_p \iff \left(\frac{u}{p}\right) = 1$.