Везде далее p — нечетное простое число, a — ненулевой остаток по модулю p, все уравнения рассматриваются в остатках по модулю p.

Задача 2.1. Если числа k и $p-1$ взаимно просты, то уравнение $x^k = a$ имеет ровно одно решение для каждого a.

▷ *Теорема о первообразном корне* утверждает, что существует остаток θ такой, что $\operatorname{ord}_p \theta = p-1$ (ей можно пользоваться без доказательства).

Задача 2.2. а) Любой остаток по модулю p является степенью первообразного корня.
б) Для каждого делителя k числа $p-1$ в $\mathbb{Z}/p$ есть элемент порядка k.

▷ Как мы выяснили, символ Лежандра может быть вычислен при помощи *формулы Эйлера*,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Задача 2.3. Пусть $p-1$ делится на k.
а) Если уравнение $x^k = a$ имеет решение, то оно имеет ровно k решений.
б) Уравнение $x^k = a$ имеет в $\mathbb{Z}/p$ решение тогда и только тогда, когда $a^{\frac{p-1}{k}} = 1$.

Задача 2.4. Рассмотрим преобразование $\sigma\colon x \mapsto \frac{1}{1-x}$ множества $(\mathbb{Z}/p) \cup \{\infty\}$.
а) $\sigma^3 = \mathrm{Id}$;
б) число неподвижных точек отображения σ сравнимо с $p+1$ по модулю 3;
в) $\left(\frac{-3}{p}\right) = 1 \iff p = 3k+1$.

(Быть может кто-то сможет обобщить это вычисление на другие a?)