Везде далее p — нечетное простое число.

▷ *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 было доказано, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Задача 1.1. Сравнение $ax^2 + bx + c \equiv 0 \mod p$ имеет (при $a \not\equiv 0 \mod p$) ровно $1 + \left(\frac{D}{p}\right)$ решений, где $D = b^2 - 4ac$.

Задача 1.2. а) Количество квадратичных вычетов по модулю p четно тогда и только тогда, когда $p = 4k + 1$.

б) Если a — квадратичный вычет, то и a^{-1} — квадратичный вычет.

в) Количество квадратичных вычетов по модулю p четно тогда и только тогда, когда -1 — квадратичный вычет по модулю p.

▷ Таким образом, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Задача 1.3. Если $p = 4k + 1$, то $(2k)!$ — корень из -1 по модулю p.
(Указание. Ср. с теоремой Вильсона.)

Задача 1.4. а) Если $a^2 + b^2$ делится на $p = 4k + 3$, то и a, и b делятся на p;

б) для $p = 4k + 1$ это неверно.