Квадратичні лишки

Тут і далі p — просте.

Означення. Число a називається квадратичним лишком за модулем p, якщо існує таке $x \in \mathbb{Z}$, що $a \equiv x^2 \pmod p$. У іншому випадку число a називається квадратичним нелишком. (Тут $(a, p) = 1$).

Символ Лежандра $\left(\dfrac{a}{p}\right)$ означає:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{якщо } a \text{ — квадратичний лишок} \\ -1, & \text{якщо } a \text{ — не квадратичний лишок.} \end{cases}$$

Критерій Ейлера. $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

Квадратичний закон взаємності [Ґаус]. Для різних непарних простих чисел p і q

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

Задачі.

1. Обчислити $\left(\dfrac{2}{31}\right)$, $\left(\dfrac{34}{43}\right)$, $\left(\dfrac{43}{991}\right)$, $\left(\dfrac{145}{2011}\right)$.
2. Довести, що, якщо число $p = 8k + 5$, то
   a) $2^{4k+2} \equiv -1 \pmod p$,
   b) рівняння $x^2 - 2 = py$ нерозв'язне в цілих числах.
3. Довести, що $\left(\dfrac{-3}{p}\right) = 1$, якщо $p = 6k + 1$ і $\left(\dfrac{-3}{p}\right) = -1$, якщо $p = 6k - 1$.
4. Чи має розв'язки конгруенція $18x^2 - 74x + 67 \equiv 0 \pmod{311}$?
5. Довести, що 3 є квадратичним нелишком за будь-яким простим модулем виду $4^n + 1$.
6. Довести, що простих чисел виду a) $8k+3$, b) $6k+1$ — нескінченна кількість.
7. Чи правда, що $1999 \mid 2^{999} - 1$?
8. Розв'язати рівняння в натуральних числах $y^5 = x^2 + 57$.
9. $x_1 = 7$, $x_{n+1} = 2x_n^2 - 1$. Довести, що $\forall n \in \mathbb{N} \quad 2003 \nmid x_n$ (не ділить).
10. Розв'язати рівняння в натуральних числах $4xy - x - y = z^2$.
11. Довести, що наступні твердження еквівалентні:
    i) існує $n \in \mathbb{N}$, що $p \mid n^2 - n + 3$,
    ii) існує $m \in \mathbb{N}$, що $p \mid m^2 - m + 25$.
12. Задача Оленки!