Теорія чисел - весняний семестр 2023 року
§9. Квадратичний закон взаємності.

1. Нехай p є непарним простим та $r_1, \ldots, r_{(p-1)/2}$ це всі квадратичні лишки за модулем p. Обчисліть добуток $r_1 \cdot r_2 \cdot \ldots \cdot r_{(p-1)/2} \mod p$. Також обчисліть добуток всіх квадратичних нелишків.

2. Для яких простих чисел p число 7 є квадратичним лишком за модулем p? Скористайтеся квадратичним законом взаємності.

3. Які прості числа p є простими елементами у кільці цілих $\mathcal{O}_K$ поля $K = \mathbb{Q}(\sqrt{5})$?

4. а) Покажіть, що $(-3/p) = 1$ коли $p \equiv 1 \mod 3$. Користуючись тим, що група $(\mathbb{Z}/p\mathbb{Z})^\times$ є циклічною, сконструюйте лишок x такий що $x^2 + 3 = 0 \pmod p$. Підказка: якщо $\rho \in (\mathbb{Z}/p\mathbb{Z})^\times$ це елемент порядка 3, то $(2\rho + 1)^2 = -3$.

   б)* Покажіть, що $(5/p) = 1$ коли $p \equiv 1 \mod 5$. Користуючись тим, що група $(\mathbb{Z}/p\mathbb{Z})^\times$ є циклічною, сконструюйте лишок x такий що $x^2 = 5 \pmod p$. Спробуйте діяти як в а).

Нехай p це непарне просте число. Зверніть увагу, що кількість лишків x які задовольніють рівнянню $x^2 = a \pmod p$ дорівнює $1 + \left(\frac{a}{p}\right)$. У наступному завданні ми порахуємо кількість розв'язків $(x, y) \in \mathbb{F}_p^2$ рівняння $y^2 = x^3 + x$.

5. Доведіть, що

   а) просте число $p > 2$ може бути представлене як сума двох квадратів цілих чисел тоді і тільки тоді коли $p \equiv 1 \pmod 4$;

   б) для простого $p \equiv 1 \pmod 4$ існує єдине представлення $p = a^2 + 4b^2$ з додатними цілими $a, b \in \mathbb{Z}$;

   с)*
   $$\sum_{x=0}^{p-1} \left(\frac{x^3 + x}{p}\right) = \begin{cases} 0, & p \equiv 3 \pmod 4 \\ -2a, & p \equiv 1 \pmod 4), \end{cases}$$
   де $a \in \mathbb{Z}$ є таким єдиним числом що $p = a^2 + 4b^2$ для деякого $b \in \mathbb{Z}$ і $a \equiv 1 \pmod 4$.
   Це обчислення було зроблено Карлом Фрідріхом Гауссом, автором квадратичного закону взаємності.