§9. Квадратичний закон взаємності

1. Нехай g — первісний корінь за модулем p, тоді квадратичні лишки за модулем p мають вигляд

$$g^2, g^4, \dots, g^{p-1} = 1.$$ Їх добуток

$$L \equiv_p \prod_{k=2}^{p-1} g^k \equiv_p g^{\sum_{k=2}^{p-1} k} \equiv_p g^{2\sum_{k=1}^{\frac{p-1}{2}} k} \equiv_p g^{\frac{p-1}{2}\cdot\frac{p+1}{2}} \equiv_p$$

$$\equiv_p \left(g^{\frac{p-1}{2}}\right)^{\frac{p+1}{2}} \equiv_p \left(\frac{g}{p}\right)^{\frac{p+1}{2}} \equiv_p (-1)^{\frac{p+1}{2}} \equiv_p \begin{cases} 1, & p \equiv_4 3; \\ -1, & p \equiv_4 1. \end{cases}$$

Квадратичні нелишки мають вигляд

$$g, g^3, \dots, g^{p-2}.$$ Їх добуток

$$N \equiv_p \prod_{k=1}^{p-2} g^k \equiv_p g^{\left(\frac{p-1}{2}\right)^2} \equiv_p \left(g^{\frac{p-1}{2}}\right)^{\frac{p-1}{2}} \equiv_p \left(\frac{g}{p}\right)^{\frac{p-1}{2}} \equiv_p$$

$$\equiv_p (-1)^{\frac{p-1}{2}} \equiv_p \begin{cases} 1, & p \equiv_4 1 \\ -1, & p \equiv_4 3 \end{cases};$$

$$L + N \equiv 0 \pmod p$$

2. Знайдемо символ Лежандра

$$\left(\frac{7}{p}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{7}\right) = (-1)^{\frac{3p+1}{2}} \left(\frac{p}{7}\right) =$$

$= [p - \text{непарне}] = (-1)^{\frac{p-1}{2}} \left(\frac{p}{7}\right)$.

За модулем 7 квадратичні лишки 1, 2 та 4; квадратичні нелишки $-1, -2$ та -4. Маємо:

· $\left(\frac{7}{2}\right) = \left(\frac{1}{2}\right) = 1$; $\left(\frac{7}{7}\right) = 0$;

· Для $p \neq 2$ та $p \neq 7$:

$$\left(\frac{7}{p}\right) = 1 \iff \begin{cases} p \equiv 1 \pmod 4; & p \equiv 1,2,4 \pmod 7, \\ p \equiv -1 \pmod 4; & p \equiv -1,-2,-4 \pmod 7. \end{cases}$$

$\iff p \equiv \pm 1, \pm 9, \mp 3 \pmod{28}$.

$$\left(\frac{7}{p}\right) = -1 \iff \begin{cases} p \equiv -1 \pmod 4; & p \equiv 1,2,4 \pmod 7, \\ p \equiv 1 \pmod 4; & p \equiv -1,-2,-4 \pmod 7. \end{cases}$$

$\iff p = \pm 15, \mp 5, \pm 11 \pmod{28}$,

за китайською теоремою про лишки.

3. Нехай $k = \mathbb{Q}(\sqrt{5})$, тоді $\mathcal{O}_k \in$ ООФ, тому, за твердженням 4, $p \in$ простим т.т.т.к. $\left(\frac{5}{p}\right) = -1$. Тоді, за квадратичним законом взаємності,

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\frac{p-1}{2}}\left(\frac{p}{5}\right) = (-1)^{p-1}\left(\frac{p}{5}\right) =$$

$= [p - \text{непарне}] = \left(\frac{p}{5}\right) = \begin{cases} 1, & p \equiv 1, -1 \pmod 5; \\ -1, & p \equiv \pm 2 \pmod 5. \end{cases}$

Відповідь: просте $p \in$ простим у кільці цілих $\mathcal{O}_k$ т.т.т.к. $p \equiv \pm 2 \pmod 5$ та $p \neq 2$.

4. а) Припустимо, $p \equiv 1 \pmod 3$, тобто $p = 3k+1$, $k \in \mathbb{N}$. p — просте, тому $(\mathbb{Z}/p\mathbb{Z})^\times \in$ циклічною. Нехай

g — первісний корінь за модулем p, тоді $\operatorname{ord}(g) = p-1 = 3k$; $\operatorname{ord}(g^k) = 3$. Тоді

$$0 = (g^k)^3 - 1 = \underbrace{(g^k - 1)}_{\neq 0}\left((g^k)^2 + g^k + 1\right) \Rightarrow (g^k)^2 + g^k + 1 = 0,$$

$$(2g^k+1)^2 = 4(g^k)^2 + 4g^k + 1 = 4\underbrace{\left((g^k)^2 + g^k + 1\right)}_{0} - 3 = -3,$$

тобто -3 — квадратичний лишок за модулем p, тобто $\left(\frac{-3}{p}\right) = 1$. ∎

б) Припустимо, $p \equiv 1 \pmod 5$, тобто $p = 5k+1$, $k \in \mathbb{N}$. p — просте, тому $(\mathbb{Z}/p\mathbb{Z})^\times$ є циклічною. Нехай g — первісний корінь за модулем p, тоді $\operatorname{ord}(g) = p-1 = 5k$; $\operatorname{ord}(g^k) = 5$.

Позначимо $p = g^k$. Тоді

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

$$- 2\left(p + \frac{1}{p}\right)\left(p^2 + \frac{1}{p^2}\right) = p^2 + \frac{1}{p^2} + 2 + p^4 + \frac{1}{p^4} + 2 -$$

$$- 2\left(p^3 + \frac{1}{p^3} + p + \frac{1}{p}\right) = p + p^2 + p^3 + p^4 + 4 - 2(p + p^2 +$$

$$+ p^3 + p^4) = 5 - (p + p^3 + p^2 + p + 1) \quad (*)$$

Але

$$0 = p^5 - 1 = \underbrace{(p-1)}_{\neq 0}(p^4 + p^3 + p^2 + p + 1) \Rightarrow p^4 + p^3 + p^2 + p + 1 = 0.$$

Отже,

$$\left(\left(p + \frac{1}{p}\right) - \left(p^2 + \frac{1}{p^2}\right)\right)^2 = 5, \text{ звідси } \left(\frac{5}{p}\right) = 1, \text{ що}$$

й треба було довести. ∎

5. а) (⇒) Припустимо, p — просте; $p = a^2 + b^2$, $a, b \in \mathbb{Z}$. Тоді $p \equiv a^2 + b^2 \pmod 4$, звідси рівно одне з чисел a та b парне. Без обмеження загальності, $a \equiv 0 \pmod 2$, тоді $a^2 \equiv 0 \pmod 4$; $b^2 \equiv 1 \pmod 4$, звідси $p \equiv a^2 + b^2 \equiv 0 + 1 \equiv 1 \pmod 4$, що й треба було довести.

(⇐) Припустимо, $p \equiv 1 \pmod 4$.