Задача 7

(2) ~~Нехай~~ Якщо $p=2$, то $7 \equiv 1 \pmod 2$, $1^2 \equiv 1 \pmod 2$, тому 7 є кв. лишком за модулем 2.

Нехай $p \neq 2$:

За кв. законом взаємності:

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

Шукаємо такі (прості) p, щоб $\left(\frac{7}{p}\right)=1$

Якщо $p \equiv 1 \pmod 4$, то $\left(\frac{p}{7}\right)=1$

За модулем 7:

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

Тому тоді p повинно бути серед $1, 2, 4 \pmod 7$

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 7 \end{cases} \Rightarrow p \equiv 1 \pmod{\underset{\shortparallel}{28}\ 4\cdot 7}$$

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 2 \pmod 7 \end{cases} \overset{\text{КТЛО}}{\Longrightarrow} p \equiv 9 \pmod{28}$$

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 4 \pmod 7 \end{cases} \overset{\text{КТЛО}}{\Longrightarrow} p \equiv 25 \pmod{28} \equiv (-3) \pmod{28}$$

Тепер, якщо $p \equiv -1 \pmod 4$, то $\left(\frac{p}{7}\right) = -1$, а значить p повинно бути серед $3, 5, 6 \pmod 7$

$$\begin{cases} p \equiv -1 \pmod 4 \equiv 3 \pmod 4 \\ p \equiv 3 \pmod 7 \end{cases} \Rightarrow p \equiv 3 \pmod{28}$$

$$\begin{cases} p \equiv -1 \pmod 4 \\ p \equiv 5 \pmod 7 \end{cases} \overset{\text{КТЛО}}{\Longrightarrow} p \equiv 19 \pmod{28} \equiv -9 \pmod{28}$$

$$\begin{cases} p \equiv -1 \pmod 4 \\ p \equiv 6 \pmod 7 \equiv -1 \pmod 7 \end{cases} \Rightarrow p \equiv -1 \pmod{28}$$

Отже, 7 є кв. лишком для будь-якого простого вигляду $p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$