ДОМАШНЯ РОБОТА №3
З ПРЕДМЕТУ
”МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ”

ФІ-12 Бекешева Анастасія

1.

$$x^2 = 12 \mod 89$$

$89 = 8 \cdot 11 + 1$. $(12, 89) = 1$. Знайдемо символ Лежандра $\left(\frac{12}{89}\right) = (-1)^{990}\left(\frac{6}{89}\right) =$
$= (-1)^{990}\left(\frac{3}{89}\right) = (-1)^{44}\left(\frac{2}{3}\right) = -1 \Longrightarrow$ Так як 12 є квадратичним нелишком 89, не існує x, що задовольнятиме цю конгруецнію.

2.

$$x^2 = 70 \mod 73$$

$73 = 8 \cdot 9 + 1$. $(70, 73) = 1$. Знайдемо символ Лежандра $\left(\frac{70}{73}\right) = (-1)^{666}\left(\frac{35}{73}\right) =$
$= \left(\frac{5}{73}\right)\left(\frac{7}{73}\right) = 1$. $70^{18} = -1 \mod 73$ Шукаємо квадратичні нелишки за $\mod 73$:
$\left(\frac{2}{73}\right) = (-1)^{666} = 1, \left(\frac{3}{73}\right) = (-1)^3 6\left(\frac{1}{3}\right) = 1, \left(\frac{4}{73}\right) = \left(\frac{2}{73}\right) \cdot \left(\frac{2}{73}\right) = 1, \left(\frac{5}{73}\right) =$
-1. $5^{36} = -1 \mod 73$. Отже $70^{18} \cdot 5^{36} = 1 \mod 73$. Обчислюємо $70^9 \cdot 5^{18} = -1$
$\mod 73$. $70^9 \cdot 5^{18} \cdot 5^{36} = 1 \mod 73$. $70^{10} \cdot 5^{54} = (70^5 \cdot 5^{27})^2 = 70 \mod 73 \Longrightarrow x = \pm 70^5 \cdot 5^{27}$
$\mod 73 = \pm 17 \mod 73$.

3.

$$x^2 = 32 \mod 119$$

$119 = 7 \cdot 17$. Знайдемо символ Лежандра $\left(\frac{32}{7}\right) = \left(\frac{2^5}{7}\right) = (-1)^6 = 1, \quad \left(\frac{32}{17}\right) =$
$\left(\frac{2^5}{17}\right) = (-1)^{36} = 1$. Отже $x^2 = 32 \mod 7, x^2 = 32 \mod 17$. $7 = 4 \cdot 1 + 3$.
$x = \pm 32^{1+1} \mod 7 = \pm 2 \mod 7$. $17 = 8 \cdot 2 + 1$. $32^{2^3 \cdot 1} = 1 \mod 17$. $32^4 = -1 \mod 17$.
Шукаємо квадратичні нелишки за $\mod 17$: $\left(\frac{2}{17}\right) = (-1)^{36} = 1, \left(\frac{3}{17}\right) = -1$. Отже
$3^8 = -1 \mod 17$. $32^4 \cdot 3^8 = 1 \mod 17$. Обчислюємо $32^2 \cdot 3^4 = 1 \mod 17$,
$32^1 \cdot 3^2 = -1 \mod 17$. Отже $32^2 \cdot 3^8 \cdot 3^2 = (32 \cdot 3^5)^2 = 8 \mod 17 \Longrightarrow x = \pm 32 \cdot 3^5$
$\mod 17 = \pm 7 \mod 17$.

$$\begin{cases} x = 2 \mod 7 \\ x = 7 \mod 17 \end{cases}, \quad x = 2 \cdot 17(17^{-1} \mod 7) + 7 \cdot 7(7^{-1} \mod 17), \quad x = 58 \mod 119$$

$$\begin{cases} x = 2 \mod 7 \\ x = -7 \mod 17 \end{cases}, \quad x = 2 \cdot 17(17^{-1} \mod 7) - 7 \cdot 7(7^{-1} \mod 17), \quad x = 44 \mod 119$$

$$x = \pm 58 \mod 119, \quad x = \pm 44 \mod 119$$