ДОМАШНЯ РОБОТА №2
З ПРЕДМЕТУ
”МАТЕМАТИЧНІ ОСНОВИ КРИПТОЛОГІЇ”

ФІ-12 Бекешева Анастасія

1.

$$\varphi(14553)$$

$$\varphi(14553) = \varphi(3 \cdot 3 \cdot 3 \cdot 7 \cdot 7 \cdot 11) = 14553 \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{7}\right) \times \left(1 - \frac{1}{11}\right) = 7560$$

2.

$$5^8 2 \mod 24$$

Перевіримо чи є 5 та 24 взаємнопростими (знайдемо $\gcd(5, 24)$):
$24 = 5 \cdot 4 + 4, \quad 5 = 4 \cdot 1, \quad 4 = 1 \cdot 4 + 0, \quad \gcd(5, 24) = 1$

q_i		4	1	
u_i	0	1	-4	5
v_i	1	0	1	-1

Тепер порахуємо: $\varphi(24) = \varphi(2 \cdot 2 \cdot 2 \cdot 3) = 24 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 8.$

Отже $5^{82} = 5^{80} \cdot 25 \mod 24 = 1 \mod 4$

3.

$$\begin{cases} x = 2 \mod 5 \\ x = 8 \mod 13 \\ x = 2 \mod 9 \\ x = 5 \mod 7 \end{cases}$$

Перевіримо чи усі n_i попарно взаємнопрості:
$\gcd(5, 13) = 1, \gcd(5, 9) = 1, \gcd(5, 7) = 1, \gcd(13, 9) = 1, \gcd(13, 7) = 1, \gcd(9, 7) = 1$
Знайдемо M: $M = 5 \cdot 13 \cdot 9 \cdot 7 = 4095$. Отже $M_1 = 819, M_2 = 315, M_3 = 455, M_4 = 585$

$\gcd(5, 819) = 1$

q_i		163	1	
u_i	0	1	-163	164
v_i	1	0	1	-1

$\gcd(13, 315) = 1$

q_i		24	4	
u_i	0	1	-24	97
v_i	1	0	1	-4

$\gcd(9, 455) = 1$

q_i		50	1	1	
u_i	0	1	-50	51	-101
v_i	1	0	1	-1	2

$\gcd(7, 585) = 1$

q_i		83	1	1	
u_i	0	1	-83	84	-167
v_i	1	0	1	-1	2

Порахуємо N_i: $N_1 = 819^{-1} \mod 5 = -1, N_2 = 315^{-1} \mod 13 = -4,$
$N_3 = 455^{-1} \mod 9 = 2, N_4 = 585^{-1} \mod 7 = 2$. Знайдемо x за формулою
$x = a_1 N_1 m_1 + \cdots + a_n N_n M_n : x = -4048 \mod 4095 = 47$

4.

$$a = x^2 \mod 13$$

$\frac{p-1}{2} = \frac{13-1}{2} = 6$. Тобто 13 має 6 квадратичних лишків.

x	1	2	3	4	5	6	7	8	9	10	11	12
$x^2 \mod 13$	1	4	9	3	12	10	10	12	3	9	4	1

З таблиці легко бачити, що 1,3,4,9,10,12 є квадратичними лишками 13.

5.

$$\left(\frac{18}{53}\right) = ?$$

$$\left(\frac{18}{53}\right) = \left(\frac{2}{53}\right) \times \left(\frac{3}{53}\right) \times \left(\frac{3}{53}\right) = -\left(\frac{9}{53}\right) = -1$$

Отже 18 не є квадратичним лишком 53.

6.

$$\left(\frac{2}{8k+5}\right) = -1$$

$\left(\frac{2}{8k+5}\right) = (-1)^{\left(\frac{(8k+5)^2-1}{8}\right)} = (-1)^{8k^2+10x+3}$. Розглянемо $8k^2 + 10x + 3$: $8k^2$ та $10k$ завжди будуть парними, адже добуток парного числа з будь-яким іншим числом є парне число. Тобто $(8k^2+10x+3) \mod 2 = 8k^2 \mod 2 + 10k \mod 2 + 3 \mod 2 = 1$. Отже $(-1)^{8k^2+10x+3} = -1$. Іншими словами 2 є квадратичним нелишком за модулем p, де $p = 8k + 5$.