$k = 36217$
$c = 2002$
$d = 25$
$m = 2$
$x = 35$

Exercise 3

Синкевич Мария
гр. 0362

N1. $\varphi(36217) = 36216$

$\varphi(2002) = \varphi(2) \cdot \varphi(7) \cdot \varphi(11) \cdot \varphi(13) = 1 \cdot 6 \cdot 10 \cdot 12 = 720$
(разложение из Exercise 1)

$\varphi(25) = \varphi(5^2) = 25\left(1 - \frac{1}{5}\right) = 25 \cdot \frac{4}{5} = 20$

$\varphi(2) = 1$

$\varphi(35) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24$

Ответ: $\varphi(36217) = 36216$; $\varphi(2002) = 720$; $\varphi(25) = 20$; $\varphi(2) = 1$; $\varphi(35) = 24$.

N2. $x \equiv (25+5)^{36217^2} \bmod 35$; $x \equiv 30^{36217^2} \bmod 35$.

$k = 36217^2 \Rightarrow 30^k \bmod 35$

$\varphi(35) = \varphi(5) \varphi(7) = 4 \cdot 6 = 24$

$$\left.\begin{aligned} k &= 24n + b \\ k &= 36217^2 \end{aligned}\right| \Rightarrow 36217^2 = 24n + b$$

В $\mathbb{Z}_{35}$: $30^{36217^2} = 30^{24n+b} = 30^{24n} \cdot 30^b = 30^b$

$$\left.\begin{aligned} \varphi(24) &= \varphi(8) \cdot \varphi(3) = \varphi(8) \cdot 2 \\ \varphi(8) &= \varphi(2^3) = 8 \cdot \left(1 - \tfrac{1}{2}\right) = 4 \end{aligned}\right| \Rightarrow \varphi(24) = 4 \cdot 2 = 8$$

$$\left.\begin{aligned} &\varphi(24) = 8 \\ &\text{НОД}(36217, 24) = 1 \end{aligned}\right| \Rightarrow 36217^8 \equiv 1 \bmod 24$$

$\text{НОД}(36217, 24) = 1$
$36217 = 36217 \cdot 1$
$24 = 1 \cdot 3 \cdot 2^3$

В $\mathbb{Z}_{24}$: $b = 36217^2 = (36217^8)^{0,25} = 1^{0,25} = 1$

Тогда $30^{36217^2} \bmod 35 \equiv 30^1 \bmod 35 \equiv 30 \bmod 35$

Ответ: 30.

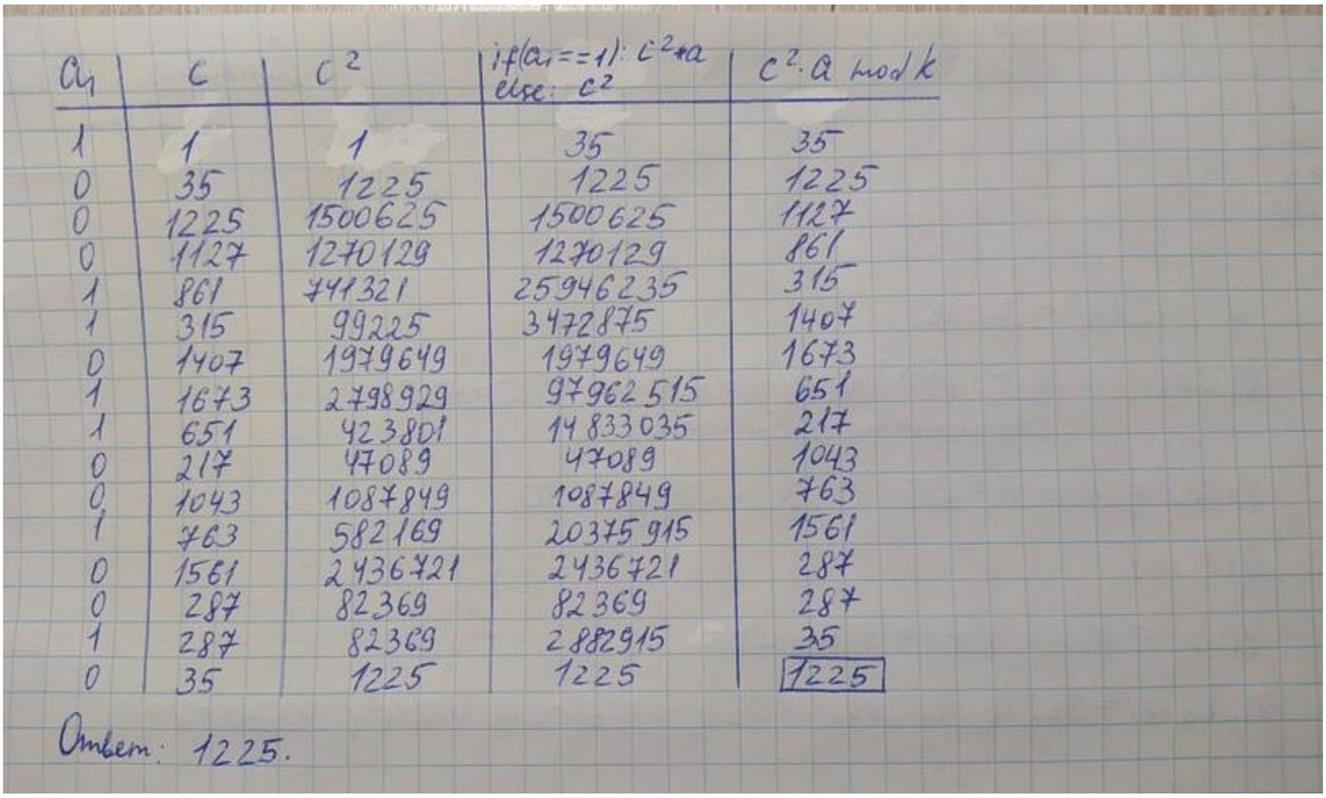
N3. $35^{36217+25} \bmod 2002$

$35^{36242} \bmod 2002$

$c = a^m \bmod k \Rightarrow \begin{aligned} a &= 35 \\ m &= 36242 \\ k &= 2002 \end{aligned}$

$36242_{10} = 1000110110010010_2$

36242	18121	9060	4530	2265	1132	566	283	141	70	35	17	8	4	2	1
0	1	0	0	1	0	0	1	1	0	1	1	0	0	0	1



a_1	c	c^2	if(a_1==1): c^2*a
			else: c^2
				$c^2 \cdot a$ mod k

1	1	1	35	35
0	35	1225	1225	1225
0	1225	1500625	1500625	1127
0	1127	1270129	1270129	861
1	861	741321	25946235	315
1	315	99225	3472875	1407
0	1407	1979649	1979649	1673
1	1673	2798929	97962515	651
1	651	423801	14833035	217
0	217	47089	47089	1043
0	1043	1087849	1087849	763
1	763	582169	20375915	1561
0	1561	2436721	2436721	287
0	287	82369	82369	287
1	287	82369	2882915	35
0	35	1225	1225	$\boxed{1225}$

Ответ: 1225.