Домашняя работа №2. Прохоренко Е.Ю. РК6-95

① а) $\phi(400) = \phi(2^2)\cdot\phi(2^2)\cdot\phi(5^2) =$ ~~[illegible]~~ $=$

$= \phi(2^4)\cdot\phi(5^2) = (2^4-2^3)(5^2-5^1) = (16-8)(20) = 8\cdot 20 = 160$

б) $\phi(567) = \phi(3^4)\cdot\phi(7) = (3^4-3^3)\cdot 6 = (81-27)\cdot 6 = 54\cdot 6 = 324$

в) $\phi(1716) = \phi(2^2)\cdot\phi(3)\cdot\phi(11)\cdot\phi(13) = (2^2-2^1)\cdot 2\cdot 10\cdot 12 = 40\cdot 12 = 480$

г) $\phi(29791) = \phi(31^3) = (31^3-31^2) = 28830$ (29791-961)

②

а) $3^{64} \bmod 67$

67 – p. м.т.Ф.: $3^{66} = 1 \bmod 67$

$3^{(66)+(-2)} \bmod 67 = \underset{1}{3^{66}}\cdot 3^{-2} \bmod 67 = 3^{-2} \bmod 67 = 9^{-1} \bmod 67$

$(9,67)=1$

$67 : 9 = 7$ (q_1), $67-63=4$
$9 : 4 = 2$ (q_2), $9-8=1$
$4 : 1 = 4$, $4-4=0$ — (1) НОД

		-7	-2
0	1	-7	15

[illegible]

1) $(9\cdot 15-1) : 67 = 2 \in Z$ ✓
2) $9\cdot 15 \bmod 67 = 1$ ✓

б) $2^{6001} \bmod 21$

т.Э.: $2^{\varphi(21)} = 1 \bmod 21 \Rightarrow [2^{12} = 1 \bmod 21]$

$\varphi(21) = 2\cdot 6 = 12$

$2^{500\cdot 12+1} \bmod 21 = \underset{1}{(2^{12})^{500}}\cdot 2 \bmod 21 = 2$

в) $16^{326} \bmod 189$

т.Э: $16^{\varphi(189)} \bmod 189 \Rightarrow [16^{108} = 1 \bmod 189)$

$\varphi(189) = \varphi(3^3)\varphi(7) = (3^3-3^2)\cdot 6 = (27-9)\cdot 6 = 18\cdot 6 = 108$

$16^{108\cdot 3+2} \bmod 189 = \underset{1}{(16^{108})^3}\cdot 16^2 \bmod 189 = 16^2 \bmod 189 = 256 \bmod 189 = 67$

г) $177^{1601} \bmod 100$

т.О: $177^{\varphi(100)+1} \bmod 100 \Rightarrow [177^{40} \equiv 1 \bmod 100]$

$\varphi(100) = \cancel{\varphi}\, 20 \cdot 2 = 40$

$177^{40 \cdot 40 + 1} \bmod 100 = 177 \bmod 100 = 77$.

3.

а) $\begin{cases} x \equiv 40 \bmod 137 \\ x \equiv 50 \bmod 113 \end{cases}$

$M = 15481$

$M_1 = 113$ | $N_1 = 113^{-1} \bmod 137 = 97$ $(97 \cdot 113 \bmod 137 = 1)$

$M_2 = 137$ | $N_2 = 137^{-1} \bmod 113 = 33$

$x_0 = (40 \cdot 113 \cdot 97 + 50 \cdot 137 \cdot 33) \bmod 15481 = -1193$

$\underset{(14288)}{}$

$\underline{x = -1193 + 15481\, k,\ k \in \mathbb{Z}}$

1) $(-1193 - 40) : 137 = 9 \in \mathbb{Z}$ ✓

2) $(-1193 - 50) : 113 = 11 \in \mathbb{Z}$ ✓

б) $\begin{cases} x \equiv 19 \bmod 24 \\ x \equiv 10 \bmod 75 \end{cases}$

$75 \mid 24$, $-72 \mid 3$; $24 \mid 3$, $-24 \mid 8$, 0

$M = 1800$

$M_1 = 75$ | $N_1 = 75^{-1} \bmod 24 =$

$M_2 = 24$ | $N_2 = 24^{-1} \bmod 75$ $(75, 24) \neq 1$ $x \in \varnothing$.

в) $\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 2 \bmod 5 \\ x \equiv 3 \bmod 7 \end{cases}$

$M = 105$

$M_1 = 35$ | $N_1 = 35^{-1} \bmod 3 = 2^{-1} \bmod 3 = 2$

$M_2 = 21$ | $N_2 = 21^{-1} \bmod 5 = 1^{-1} \bmod 5 = 1$

$M_3 = 15$ | $N_3 = 15^{-1} \bmod 7 = 1^{-1} \bmod 7 = 1$

$x_0 = (1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1) \bmod 105 = (70 + 42 + 45) \bmod 105 = 157 \bmod 105 = 52$

$\underline{x = 52 + 105\, k,\ k \in \mathbb{Z}}$

1) $(52 - 1) : 3 = 17 \in \mathbb{Z}$ ✓

2) $(52 - 2) : 5 = 10 \in \mathbb{Z}$ ✓

3) $(52 - 3) : 7 = 7 \in \mathbb{Z}$ ✓

2) $\begin{cases} 3x \equiv 5 \bmod 7 \Rightarrow x = 5 \cdot 3^{-1} \bmod 7 = 5 \cdot 5 \bmod 7 = 25 \bmod 7 = 4 \\ x \equiv 2 \bmod 6 \\ 2x = 1 \bmod 5 \Rightarrow x = 1 \cdot 2^{-1} \bmod 5 = 3 \end{cases}$

$-2 \bmod 7 = 5 \bmod 7$

$\Downarrow$

$\begin{cases} x = 4 \bmod 7 \\ x = 2 \bmod 6 \\ x = 3 \bmod 5 \end{cases}$

$M = 210$

$M_1 = 30$ $\quad N_1 = 30^{-1} \bmod 7 = 2^{-1} \bmod 7 = 4$.

$M_2 = 35$ $\quad N_2 = 35^{-1} \bmod 6 = 5^{-1} \bmod 6 = 5$

$M_3 = 42$ $\quad N_3 = 42^{-1} \bmod 5 = 2^{-1} \bmod 5 = 3$

$x_0 = (4 \cdot 30 \cdot 4 + 2 \cdot 35 \cdot 5 + 3 \cdot 42 \cdot 3) \bmod 210 = (480 + 350 + 378) \bmod 210 = 1208 \bmod 210 =$

$= 158$

$x = 158 + 210k, k \in Z$

$\begin{cases} (158-4) : 7 = 22 \in Z \checkmark \\ (158-2) : 6 = 26 \in Z \checkmark \\ (158-3) : 5 = 31 \in Z \checkmark. \end{cases}$