# Домашнее задание на 07.02 (Теория чисел)

Емельянов Владимир, ПМИ гр №247

**№1** Доказательство:

$\Rightarrow$ Пусть $p$ - простое, тогда по т.Вильсона:

$$(p-1)! \equiv -1 \pmod{p}$$

Но мы знаем, что:

$$p-1 \equiv -1 \pmod{p}$$

А значит:

$$(p-2)! \equiv 1 \pmod{p}$$

$\Leftarrow$ Пусть:

$$(p-2)! \equiv 1 \pmod{p}$$

докажем, что $p$ - простое.

Пусть $p$ - непростое, тогда существуют такие $a$ и $b$, что:

$$p = ab$$

А значит:

$$(p-2)! = (p-2)(p-3)\dots a \dots b \dots 2 \cdot 1$$

Поэтому:

$$p = ab \mid (p-2)!$$

Следовательно:

$$(p-2)! \equiv 0 \pmod{p}$$

Но по условию:

$$(p-2)! \equiv 1 \pmod p$$

Противоречие, значит $p$ - простое.

**№2** Чтобы решить систему

$$\begin{cases} x \equiv 4 \pmod{15} \\ x \equiv -1 \pmod{16} \\ x \equiv 11 \pmod{17} \end{cases}$$

воспользуемся к.т.о. . Единственное решение:

$$x = \sum_{i=1}^{k} M_i b_i \pmod M$$

Где:

$$M_i b_i = a_i \pmod{m_i}$$

$$M_1 = 16 \cdot 17 = 272 \equiv 2 \pmod{15}$$

$$M_2 = 15 \cdot 17 = 255 \equiv -1 \pmod{16}$$

$$M_3 = 15 \cdot 16 = 240 \equiv 2 \pmod{17}$$

$$M_1 b_1 \equiv a_1 \pmod{m_1} \Leftrightarrow 2b_1 \equiv 4 \pmod{15} \Rightarrow b_1 = 2$$

$$M_2 b_2 \equiv a_2 \pmod{m_2} \Leftrightarrow -b_2 \equiv -1 \pmod{16} \Rightarrow b_2 = 1$$

$$M_3 b_3 \equiv a_3 \pmod{m_3} \Leftrightarrow 2b_3 \equiv 11 \equiv -6 \pmod{17} \Rightarrow b_3 = -3$$

Найдём решение:

$$M = 15 \cdot 16 \cdot 17 = 4080$$

$$x = 272 \cdot 2 + 255 \cdot 1 + 240 \cdot (-3) = 79 \pmod{4080}$$

**Ответ:** $79 \pmod{4080}$

**№3** а) $x^2 - 1 \equiv 0 \pmod{15}$ Получаем:

$$(x-1)(x+1) \equiv 0 \pmod{15}$$

Разберём все возможные случаи:

$$\left[\begin{array}{l} \begin{cases} x-1 \equiv 0 \pmod 3 \\ x+1 \equiv 0 \pmod 5 \end{cases} \implies x = -11 \pmod{30} \\ \begin{cases} x-1 \equiv 0 \pmod 5 \\ x+1 \equiv 0 \pmod 3 \end{cases} \implies x = 11 \pmod{30} \\ x-1 \equiv 0 \pmod{15} \implies x = 1 \pmod{15} \\ x+1 \equiv 0 \pmod{15} \implies x = -1 \pmod{15} \end{array}\right.$$

**Ответ:** $\left[\begin{array}{l} x = 1 \pmod{15} \\ x = -1 \pmod{15} \\ x = -11 \pmod{30} \\ x = 11 \pmod{30} \end{array}\right.$

б) $x^2 - 1 \equiv 0 \pmod{56}$

$$56 = 8 \cdot 7$$

Получаем:

$$(x-1)(x+1) \equiv 0 \pmod{56}$$

Так $x-1$ и $x+1$ одновременно либо чётные, либо нечётные, то для искомого сравнения возможны только случаи:

$$\begin{cases} 7 \cdot 2 \mid x-1 \\ 2^2 \mid x+1 \end{cases} \quad \begin{cases} 7 \cdot 2^2 \mid x-1 \\ 2 \mid x+1 \end{cases} \quad \begin{cases} 7 \cdot 2 \mid x+1 \\ 2^2 \mid x-1 \end{cases} \quad \begin{cases} 7 \cdot 2^2 \mid x+1 \\ 2 \mid x-1 \end{cases}$$

Или когда:

$$56 \mid x-1 \text{ или } 56 \mid x+1$$

**№4** $\varphi(4^x 6^y) = 2\varphi(35^z)$ Это эквивалентно:

$$2^{2x+y}3^y(1-\frac{1}{2})(1-\frac{1}{3}) = 2\cdot 35^z(1-\frac{1}{5})(1-\frac{1}{7})$$

$$2^{2x+y}3^y\frac{1}{2}\frac{2}{3} = 2\cdot 35^z\frac{4}{5}\frac{6}{7}$$

$$2^{2x+y}3^{y-1} = 48\cdot 35^{z-1} = 2^4\cdot 3\cdot 5^{z-1}\cdot 7^{z-1}$$

Следовательно:

$$\begin{cases} 2x+y=4 \\ y-1=1 \\ z=1 \end{cases} \implies \begin{cases} x=1 \\ y=2 \\ z=1 \end{cases}$$

**Ответ:** $(x,y,z)=(1,2,1)$

**№5** Чтобы доказать, что отображение

$$\mathrm{Enc}_e(\bar{a}) = \overline{a^e}$$

взаимно однозначно отображает $\mathbb{Z}_n^*$ на себя, нам нужно показать, что оно является биекцией, то есть, что оно инъективно и сюръективно.

Для инъективности нам нужно показать, что если

$$\mathrm{Enc}_e(\bar{a_1}) = \mathrm{Enc}_e(\bar{a_2}),$$

то $\bar{a_1} = \bar{a_2}$.

Предположим, что

$$\overline{a_1^e} = \overline{a_2^e}.$$

Это означает, что

$$a_1^e \equiv a_2^e \mod n.$$

Так как $(e, \varphi(n)) = 1$, существует обратный элемент $d$ по модулю $\varphi(n)$, такой что

$$ed \equiv 1 \mod \varphi(n).$$

Теперь возьмем обе стороны уравнения $a_1^e \equiv a_2^e \mod n$ и возведем в степень $d$:

$$(a_1^e)^d \equiv (a_2^e)^d \mod n.$$

$$a_1^{ed} \equiv a_2^{ed} \mod n.$$

Так как $ed \equiv 1 \mod \varphi(n)$, мы можем записать:

$$a_1 \equiv a_2 \mod n.$$

Таким образом, $\bar{a_1} = \bar{a_2}$, что доказывает инъективность.

Теперь покажем, что отображение сюръективно. Для этого нужно показать, что для любого $\bar{b} \in \mathbb{Z}_n^*$ существует $\bar{a} \in \mathbb{Z}_n^*$, такое что

$$\mathrm{Enc}_e(\bar{a}) = \bar{b}.$$

Пусть $\bar{b} \in \mathbb{Z}_n^*$. Поскольку $(e, \varphi(n)) = 1$, существует $d$ такое, что

$$ed \equiv 1 \mod \varphi(n).$$

Теперь мы можем взять $\bar{a} = \overline{b^d}$. Тогда:

$$\mathrm{Enc}_e(\bar{a}) = \overline{(b^d)^e} = \overline{b^{de}}.$$

Так как $de \equiv 1 \mod \varphi(n)$, мы имеем:

$$b^{de} \equiv b \mod n.$$

Следовательно,

$$\mathrm{Enc}_e(\bar{a}) = \bar{b}.$$

Таким образом, для любого $\bar{b} \in \mathbb{Z}_n^*$ существует $\bar{a} \in \mathbb{Z}_n^*$, такое что $\mathrm{Enc}_e(\bar{a}) = \bar{b}$, что доказывает сюръективность.

Следовательно, искомое отображение - биекция.