Домашнее задание 2

Асписов Дмитрий Алексеевич, БПИ226

8 октября 2024 г.

Задача 1

Найдите решение системы сравнений:

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 6 \\ x \equiv 5 \pmod 7 \end{cases}$$

Решение:

1. Находим значения произведений модулей M_i:

$$M = 5 \times 6 \times 7 = 210$$

$$M_1 = \frac{M}{5} = 42, \quad M_2 = \frac{M}{6} = 35, \quad M_3 = \frac{M}{7} = 30$$

2. Решаем для N_i из уравнений:

$$\begin{aligned} 42 \times N_1 &\equiv 1 \pmod 5 &&\Rightarrow 2 \times N_1 \equiv 1 \pmod 5 &&\Rightarrow N_1 = 3, \\ 35 \times N_2 &\equiv 1 \pmod 6 &&\Rightarrow 5 \times N_2 \equiv 1 \pmod 6 &&\Rightarrow N_2 = 5, \\ 30 \times N_3 &\equiv 1 \pmod 7 &&\Rightarrow 2 \times N_3 \equiv 1 \pmod 7 &&\Rightarrow N_3 = 4. \end{aligned}$$

3. Находим x:

$$x = (3 \cdot 42 \cdot 3) + (4 \cdot 35 \cdot 5) + (5 \cdot 30 \cdot 4) = 378 + 700 + 600 = 1678$$

Запишем решение в виде сравнения по модулю:

$$x \equiv 1678 \pmod{210}$$

$$\boxed{x \equiv 208 \pmod{210}}$$

Задача 2

Сколько решений в $\mathbb{Z}_5$ имеет система $x \equiv 3y \pmod 5$?

Решение:

Рассмотрим все возможные значения y в $\mathbb{Z}_5$ и найдём соответствующие x:

$$\begin{aligned}
&1)\ y = 0 \implies x = 3 \times 0 \equiv 0 \pmod 5,\\
&2)\ y = 1 \implies x = 3 \times 1 \equiv 3 \pmod 5,\\
&3)\ y = 2 \implies x = 3 \times 2 \equiv 1 \pmod 5,\\
&4)\ y = 3 \implies x = 3 \times 3 \equiv 4 \pmod 5,\\
&5)\ y = 4 \implies x = 3 \times 4 \equiv 2 \pmod 5.
\end{aligned}$$

Таким образом, для каждого значения y существует уникальное значение x. Поскольку y может принимать 5 различных значений в $\mathbb{Z}_5$, получаем:

$$\boxed{5 \text{ решений в } \mathbb{Z}_5}$$

Задача 3

Может ли при составном n выполняться сравнение $(n-1)! \equiv -1 \pmod n$?

Решение:

Нет, не можем.

Доказательство. Поскольку n — составное, мы можем его представить в виде:

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

Рассмотрим 3 случая:

1) Пусть $k > 1$, тогда $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ входят в $(n-1)!$ и $(n-1)! \equiv 0 \pmod n$
2) Пусть $k = 1$, $\alpha > 2$, тогда в $(n-1)!$ войдут $p^{\alpha-1}$, $p \implies (n-1)! \equiv 0 \pmod n$
3) Пусть $k = 1$, $\alpha = 2$, тогда мы получаем ещё два случая :
    1. $p = 2 \implies n = 4 \implies (n-1)! = 6 \equiv 2 \pmod 4$
    2. $p > 2 \implies p$ и $2p$ входят в $(n-1)! \implies (n-1)! \equiv 0 \pmod n$

Таким образом мы получили, что не существует составного $n : (n-1)! \equiv -1 \pmod n$

□