Теория чисел

ДЗ 4

Гольдберг Дмитрий Максимович

Группа БПМИ248

Задание 1

Докажите, что p — простое тогда и только тогда, когда

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

Решение:

1. Докажем слева направо. Пусть p — простое, тогда по теореме Вильсона

$$(p-1)! \equiv -1 \pmod p$$
$$(p-1)\cdot(p-2)! \equiv -1 \pmod p$$
$$-1\cdot(p-2)! \equiv -1 \pmod p$$
$$(p-2)! \equiv 1 \pmod p \Rightarrow \text{ доказали}$$

2. Докажем справа налево. Пусть $p = p_1^{\alpha_1}\cdot ... \cdot p_n^{\alpha_n}$. Тогда по КТО исходное сравнение равносильно системе сравнений

$$\begin{cases} (p-2)! \equiv 1 \pmod{p_1^{\alpha_1}} \\ ... \\ (p-2)! \equiv 1 \pmod{p_n^{\alpha_n}} \end{cases}$$

Рассмотрим произвольное сравнение из системы $(p-2)! \equiv 1 \left(\bmod p_i^{\alpha_i}\right)$. Заметим, что $p_i^{\alpha_i} \leqslant p-2$(так как $p_i^{\alpha_i}$ член разложения на простые множители и $(p-1, p) = 1$). Тогда в выражении $(p-2)! = (p-2)\cdot(p-1)\cdot ... \cdot 1$ обязательно встретится множитель, в точности равный $p_i^{\alpha_i} \Rightarrow$ левая часть сравнения обнулится и мы получим противоречие. Значит p обязано быть простым.

Ответ:

ч.т.д

Задание 2

Решите систему сравнений

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

Решение:

По КТО

$$x \equiv \sum_{i=1}^{3} b_i \cdot M_i \pmod{4080}$$
$$M_1 = 272; M_2 = 255; M_3 = 240$$
$$b_1 \cdot 272 \equiv 4 \pmod{15} \Rightarrow b_1 = 17$$
$$b_2 \cdot 255 \equiv -1 \pmod{16} \Rightarrow b_2 = 1$$
$$b_2 \cdot 240 \equiv 11 \pmod{17} \Rightarrow b_3 = 31$$
$$\Rightarrow x \equiv 4624 + 255 + 7471 \pmod{4080}$$
$$\Rightarrow x \equiv 79 \pmod{4080}$$

Ответ:

$x \equiv 79 \pmod{4080}$

Задание 3

Решите сравнения

$$а)\ x^2 - 1 \equiv 0 \pmod{15}\ б)\ x^2 - 1 \equiv 0 \pmod{56}$$

Решение:

1. По КТО перепишем сравнение как систему

$$\begin{cases} x^2 \equiv 1 \pmod 3 \\ x^2 \equiv 1 \pmod 5 \end{cases} \Longleftrightarrow \begin{cases} \left[\begin{smallmatrix} x \equiv 1 \pmod 3 \\ x \equiv -1 \pmod 3 \end{smallmatrix}\right. \\ \left[\begin{smallmatrix} x \equiv 1 \pmod 5 \\ x \equiv -1 \pmod 5 \end{smallmatrix}\right. \end{cases}$$

(1)

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \end{cases} \Rightarrow x \equiv 1 \pmod{15}$$

(2)

$$\begin{cases} x \equiv -1 \pmod 3 \\ x \equiv -1 \pmod 5 \end{cases} \Rightarrow x \equiv -1 \pmod{15}$$

(3)

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv -1 \pmod 5 \end{cases} \Rightarrow x \equiv 4 \pmod{15}$$

(4)

$$\begin{cases} x \equiv -1 \pmod 3 \\ x \equiv 1 \pmod 5 \end{cases} \Rightarrow x \equiv 11 \pmod{15}$$

2. По КТО перепишем сравение как систему

$$\begin{cases} x^2 \equiv 1 \pmod{2^3} \\ x^2 \equiv 1 \pmod 7 \end{cases} \Longleftrightarrow \begin{cases} \left[\begin{smallmatrix} x \equiv 1 \pmod{2^3} \\ x \equiv -1 \pmod{2^3} \\ x \equiv 3 \pmod{2^3} \\ x \equiv 5 \pmod{2^3} \end{smallmatrix}\right. \\ \left[\begin{smallmatrix} x \equiv 1 \pmod 7 \\ x \equiv -1 \pmod 7 \end{smallmatrix}\right. \end{cases}$$

(1)

$$\begin{cases} x \equiv 1 \pmod{2^3} \\ x \equiv 1 \pmod 7 \end{cases} \Rightarrow x \equiv 1 \pmod{56}$$

(2)

$$\begin{cases} x \equiv -1 \pmod{2^3} \\ x \equiv 1 \pmod 7 \end{cases} \Rightarrow x \equiv 15 \pmod{56}$$

(3)

$$\begin{cases} x \equiv 3 \pmod{2^3} \\ x \equiv 1 \pmod 7 \end{cases} \Rightarrow x \equiv 43 \pmod{56}$$

(4)

$$\begin{cases} x \equiv 5 \pmod{2^3} \\ x \equiv 1 \pmod{7} \end{cases} \Rightarrow x \equiv 29 \pmod{56}$$

(5)

$$\begin{cases} x \equiv 1 \pmod{2^3} \\ x \equiv -1 \pmod{7} \end{cases} \Rightarrow x \equiv 41 \pmod{56}$$

(6)

$$\begin{cases} x \equiv -1 \pmod{2^3} \\ x \equiv -1 \pmod{7} \end{cases} \Rightarrow x \equiv -1 \pmod{56}$$

(7)

$$\begin{cases} x \equiv 3 \pmod{2^3} \\ x \equiv -1 \pmod{7} \end{cases} \Rightarrow x \equiv 27 \pmod{56}$$

(8)

$$\begin{cases} x \equiv 5 \pmod{2^3} \\ x \equiv -1 \pmod{7} \end{cases} \Rightarrow x \equiv 13 \pmod{56}$$

Ответ:

1. $x \equiv 1; -1; 4; 11 \pmod{15}$
2. $x \equiv 1; -1; 15; 43; 29; 41; 27; 13 \pmod{56}$

Задание 4

Решите уравнение $\varphi(4^x 6^y) = 2\varphi(35^z)$

Решение:

$$\varphi\left(2^{2x+y} \cdot 3^y\right) = 2\varphi(7^z \cdot 5^z)$$
$$\varphi\left(2^{2x+y}\right) \cdot \varphi(3^y) = 2\varphi(7^z) \cdot \varphi(5^z)$$
$$\left(2^{2x+y} - 2^{2x+y-1}\right) \cdot \left(3^y - 3^{y-1}\right) = 2 \cdot \left(7^z - 7^{z-1}\right) \cdot \left(5^z - 5^{z-1}\right)$$
$$2^{2x+y-1} \cdot (2-1) \cdot 3^{y-1} \cdot (3-1) = 2 \cdot 7^{z-1} \cdot (7-1) \cdot 5^{z-1} \cdot (5-1)$$
$$2^{2x+y} \cdot 3^{y-1} = 2^4 \cdot 3 \cdot 7^{z-1} \cdot 5^{z-1}$$
$$\Rightarrow y - 1 = 1 \Rightarrow y = 2$$
$$2x + y = 4 \Rightarrow x = 1$$
$$z - 1 = 0 \Rightarrow z = 1$$

Ответ:

$(x, y, z) = (1, 2, 1)$

Задание 5

Пусть $n \in \mathbb{N}, n \geqslant 2, e \in \mathbb{Z}, (e, \varphi(n)) = 1$. Докажите, что отображение

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

взаимно однозначно отражает $\mathbb{Z}_n^*$ на себя.

Решение:

Докажем инъективность. Пусть $\mathrm{Enc}_e(a) = \mathrm{Enc}_e(b) \iff a^e \equiv b^e \pmod n$. Так как $(e, \varphi(n)) = 1 \Rightarrow \exists\ d : e \cdot d \equiv 1 \pmod{\varphi(n)} \Rightarrow e \cdot d = t \cdot \varphi(n) + 1$. Тогда $(a^e)^d \equiv (b^e)^d \pmod n \Rightarrow a^{t \cdot \varphi(n)+1} \equiv b^{t \cdot \varphi(n)+1} \pmod n \Rightarrow a \equiv b \pmod n$(по теореме Эйлера). Так как a и $b \in \mathbb{Z}_n^*$, то $a = b$. Доказали

Докажем сюръективность. Опять же, так как $(e, \varphi(n)) = 1 \Rightarrow \exists\ d : e \cdot d \equiv 1 \pmod{\varphi(n)} \Rightarrow e \cdot d = t \cdot \varphi(n) + 1$. Для сюръективности надо доказать, что для любого $k \in \mathbb{Z}_n^*\ \exists a^e : a^e \equiv k \pmod n$. Для любого k можем взять $a = k^d \pmod n$($d -$ обратный вычет по $\varphi(n)$)$\Rightarrow \left(k^d\right)^e \equiv k \pmod n \Rightarrow k^{t \cdot \varphi(n)+1} \equiv k \pmod n \Rightarrow k \equiv k \pmod n$(по теореме Эйлера). Доказали.

Значит отображение биективное.

Ответ:

ч.т.д