Теория чисел

ДЗ 7

Гольдберг Дмитрий Максимович

Группа БПМИ248

Задание 1

Выясните, разрешимо ли сравнение $x^2 \equiv 3 \pmod{143}$.

Решение:

Исходное сравнение равносильно системе

$$\begin{cases} x^2 \equiv 3 \pmod{13} \\ x^2 \equiv 3 \pmod{11} \end{cases}$$

Вычислим соответствующие символы Лежандра для проверки разрешимости сравнений

$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$$

$$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1$$

Оба равны 1, значит исходное сравнение разрешимо.

Ответ:

разрешимо

Задание 2

Выясните, разрешимо ли сравнение $x^2 \equiv 3 \pmod{119}$.

Решение:

Исходное сравнение равносильно системе

$$\begin{cases} x^2 \equiv 3 \pmod{7} \\ x^2 \equiv 3 \pmod{17} \end{cases}$$

Вычислим соответствующие символы Лежандра для проверки разрешимости сравнений

$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1 \Rightarrow \text{система не разрешима, значит исходное сравнение не разрешимо.}$$

Ответ:

нет

Задание 3

Вычислите сумму символов Якоби $\sum_{n=1}^{499}\left(\frac{n}{1001}\right)$.

Решение:

Заметим, что сумма символов Якоби $\sum_{n=1}^{1001}\left(\frac{n}{1001}\right) = 0$. Эту сумму можно переписать как

$$\sum_{n=1}^{499}\left(\frac{n}{1001}\right) + \sum_{n=500}^{1000}\left(\frac{n}{1001}\right) + \left(\frac{1001}{10001}\right) = 0.$$

Заметим, что $\left(\frac{n}{1001}\right) = \left(\frac{n-1001}{1001}\right) = \left(\frac{1001-n}{1001}\right) \cdot \left(-\frac{1}{1001}\right) = \left(\frac{1001-n}{1001}\right) \Rightarrow$

$$\Rightarrow \sum_{n=500}^{1000}\left(\frac{n}{1001}\right) = \sum_{n=1}^{501}\left(\frac{n}{1001}\right) = \sum_{n=1}^{499}\left(\frac{n}{1001}\right) + \left(\frac{500}{1001}\right) + \left(\frac{501}{1001}\right) = \sum_{n=1}^{499}\left(\frac{n}{1001}\right) + 2.$$

Подставляя в верхнюю сумму, получаем, что

$$2\sum_{n=1}^{499}\left(\frac{n}{1001}\right) + 2 = 0 \Rightarrow \sum_{n=1}^{499}\left(\frac{n}{1001}\right) = -1$$

Ответ:

-1

Задание 4

Пусть P —нечётное число, $P \geqslant 3$. Докажите, что $\left(\dfrac{2}{P}\right) = (-1)^{\left[\frac{P+1}{4}\right]}$.

Решение:

По свойтву символа Якоби

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}} = \begin{cases} 1, \text{ если } P \equiv \pm 1 \pmod 8 \\ -1, \text{ если } P \equiv \pm 3 \pmod 8 \end{cases}$$

Рассмотрим 4 случая:

1. $P \equiv 1 \pmod 8 \Rightarrow P = 8n+1$
   $\left[\frac{P+1}{4}\right] = \left[\frac{8n+2}{4}\right] = [2n+0.5] = 2n \Rightarrow (-1)^{\left[\frac{P+1}{4}\right]} = 1 = (-1)^{\frac{P^2-1}{8}}$
2. $P \equiv 7 \pmod 8 \Rightarrow P = 8n+7$
   $\left[\frac{P+1}{4}\right] = \left[\frac{8n+8}{4}\right] = [2n+2] = 2n+2 \Rightarrow (-1)^{\left[\frac{P+1}{4}\right]} = 1 = (-1)^{\frac{P^2-1}{8}}$
3. $P \equiv 3 \pmod 8 \Rightarrow P = 8n+3$
   $\left[\frac{P+1}{4}\right] = \left[\frac{8n+4}{4}\right] = [2n+1] = 2n+1 \Rightarrow (-1)^{\left[\frac{P+1}{4}\right]} = -1 = (-1)^{\frac{P^2-1}{8}}$
4. $P \equiv 5 \pmod 8 \Rightarrow P = 8n+5$
   $\left[\frac{P+1}{4}\right] = \left[\frac{8n+6}{4}\right] = \left[(2n+1)+\frac{1}{2}\right] = 2n+1 \Rightarrow (-1)^{\left[\frac{P+1}{4}\right]} = -1 = (-1)^{\frac{P^2-1}{8}}$

Получили, что $\left(\dfrac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}} = (-1)^{\left[\frac{P+1}{4}\right]}$, так как значения по соответствующим модулям одинаковые.

Ответ:

ч.т.д

Задание 5

Пусть $a, b \in \mathbb{N}$ и пусть $P = 4ab - 1$. Докажите, что сравнение $x^2 \equiv -a \pmod{P}$ неразрешимо.

Решение:

1. Пусть a —нечётное. Рассмотрим соответствующий символ Якоби

$$\left(\frac{-a}{P}\right) = \left(\frac{-1}{P}\right) \cdot \left(\frac{a}{P}\right) = -\left(\frac{a}{P}\right) = -\left(\frac{P}{a}\right) \cdot (-1)^{\frac{(P-1)\cdot(a-1)}{4}}$$

$$(-1)^{\frac{(P-1)(a-1)}{4}} = (-1)^{(ab-0.5)\cdot(a-1)} = (-1)^{(a-1)ab} \cdot (-1)^{(a-1)\cdot(-0.5)} = (-1)^{-\frac{a-1}{2}} = (-1)^{\frac{a-1}{2}}$$

Так как $P \equiv -1 \pmod{a} \Rightarrow -\left(\frac{P}{a}\right) = -\left(\frac{-1}{a}\right) = -(-1)^{\frac{a-1}{2}} \Rightarrow$

$$\Rightarrow \left(\frac{-a}{P}\right) = -\left(\frac{P}{a}\right) \cdot (-1)^{\frac{(P-1)\cdot(a-1)}{4}} = -(-1)^{\frac{a-1}{2}} \cdot (-1)^{\frac{a-1}{2}} = -1 \Rightarrow \text{сравнение неразрешимо}$$

2. Пусть a —чётно. Значит $a = 2^k \cdot n$, n —нечётное. Рассмотрим соответствующий символ Якоби

$$\left(\frac{-a}{P}\right) = -\left(\frac{a}{P}\right) = -\left(\frac{2}{P}\right)^k \cdot \left(\frac{n}{P}\right)$$

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}} = (-1)^{2a^2b^2-ab} = 1$$

$$\left(\frac{n}{P}\right) = 1(\text{считается также, как и в первом пункте})$$

$$\Rightarrow \left(\frac{-a}{P}\right) = -\left(\frac{a}{P}\right) = -\left(\frac{2}{P}\right)^k \cdot \left(\frac{n}{P}\right) = -1 \Rightarrow \text{сравнение неразрешимо}$$

Получили, что при всех a сравнение неразрешимо.

Ответ:

ч.т.д