Теория чисел

ДЗ 3

Гольдберг Дмитрий Максимович

Группа БПМИ248

Задание 1

Докажите, что если длины сторон прямоугольного треугольника целые числа, то произведение этих длин делится на 60.

Решение:

Пусть a, b, c — искомые длины, при этом $a^2 + b^2 = c^2$. Заметим, что по модулю 8 квадраты могут давать остатки 0, 1, 4. При этом квадраты нечетных чисел дают дают остаток 1, квадраты четных чисел, некратных 4, дают остаток 4, квадраты чисел, кратных 4, дают остаток 0. Числа a и b не могут оба быть одновременно нечетными(так как правая часть не может быть сравнимой с 2 по модулю 8). Если одно из чисел a, b четное, а другое нечетное, то оставшееся число обязано делиться на 4(правая часть не может быть сравнимой с 5 по модулю 8). Получаем, что произведение a, b, c делится на 4.

Далее докажем делимость на 3. По модулю 3 квадраты дают остаток 0 или 1. Заметим, что квадраты чисел a, b не могут одновременно давать остаток 1 по модулю 3(правая часть не может быть сравнимой с 2 по модулю 3), значит какой-то из этих квадратов сравним с нулем по модулю 3, а значит и само число делится на 3(из таблицы остатков по модулю 3). Значит произведение делится на 3ю.

Далее докажем делимость на 5. По модулю 5 квадраты дают остатки 0, 1, 4. Если никакое из чисел a, b не делится на 5, то тогда одно из них должно давать остаток 1 по модулю 5, а другое 4(иначе не будет верно соотношение для суммы квадратов), но тогда c будет делится на 5(из арифметики остатков). Значит произведение делится на 5.

Итого, произведение делится на 3,4,5, значит делится на 60.

Ответ:

ч.т.д

Задание 2

Решите сравнения
а) $19x \equiv 2 \pmod{88}$
б) $102x \equiv 9 \pmod{165}$.

Решение:

1. Перепишем сравнение как диофантово уравнение и решим его
$$19x + 88y = 2$$
$$\begin{pmatrix} 19 & 88 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 19 & 12 \\ 1 & -4 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 7 & 12 \\ 5 & -4 \\ -1 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 7 & 5 \\ 5 & -9 \\ -1 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} 2 & 5 \\ 14 & -9 \\ -3 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} 2 & 1 \\ 14 & -37 \\ -3 & 8 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 1 \\ 88 & -37 \\ -19 & 8 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -74 \\ 16 \end{pmatrix} + t \cdot \begin{pmatrix} 88 \\ -19 \end{pmatrix}, t \in \mathbb{Z} \Rightarrow$$
$$x = -74 + 88t \Rightarrow x \equiv 14 \pmod{88}$$

2. Перепишем сравнение как диофантово уравнение и решим его
$$102x + 165y = 9$$
$$\begin{pmatrix} 102 & 165 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 102 & 63 \\ 1 & -1 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 39 & 63 \\ 2 & -1 \\ -1 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 39 & 24 \\ 2 & -3 \\ -1 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} 15 & 24 \\ 5 & -3 \\ -3 & 2 \end{pmatrix} \Rightarrow \begin{pmatrix} 15 & 9 \\ 5 & -8 \\ -3 & 5 \end{pmatrix} \Rightarrow \begin{pmatrix} 6 & 9 \\ 13 & -8 \\ -8 & 5 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} 6 & 3 \\ 13 & -21 \\ -8 & 13 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 3 \\ 55 & -21 \\ -34 & 13 \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -63 \\ 39 \end{pmatrix} + t \cdot \begin{pmatrix} 55 \\ -34 \end{pmatrix}, t \in \mathbb{Z} \Rightarrow$$
$$x = -63 + 55t \Rightarrow x \equiv 47 \pmod{55}$$
$$\Rightarrow x \equiv 47, 102, 157 \pmod{165}$$

Ответ:

1. $x \equiv 14 \pmod{88}$
2. $x \equiv 47, 102, 157 \pmod{165}$

Задание 3

Найдите все такие простые числа p, что $5^{p^2} \equiv 1 \pmod p$.

Решение:

Из МТФ следует, что $5^{p-1} \equiv 1 \pmod p$.

$$5^{p^2} =\equiv \left(5^{p-1}\right)^p \cdot 5^p \equiv 1^p \cdot 5^p \equiv 5^p \equiv 5^{p-1} \cdot 5 \equiv 1 \cdot 5 \equiv 5 \equiv 1 \pmod p$$
$$\Rightarrow 4 \equiv 0 \pmod p \Rightarrow p = 2$$

Ответ:

2

Задание 4

Найдите все основания a, для которых 15 — псевдопростое число.

Решение:

Имеем сравнение $a^{14} \equiv 1 \pmod{15}$, $(a, 15) = 1$. $15 = 5 \cdot 3$. Рассмотрим сравнение $a^{14} \equiv 1 \pmod{3}$. По МТФ $a^2 \equiv 1 \pmod{3} \Rightarrow \left(a^2\right)^7 \equiv 1^7 \pmod{3} \Rightarrow a^{14} \equiv 1 \pmod{3} \Rightarrow$ по модулю 3 подходят все a, взаимопростые с 3.

Рассмотрим сравнение $a^{14} \equiv 1 \pmod{5}$. По МТФ $a^4 \equiv 1 \pmod{5} \Rightarrow a^{14} \equiv \left(a^4\right)^3 \cdot a^2 \equiv a^2 \equiv 1 (\bmod 5) \Rightarrow a \equiv 1 \pmod{5}$ или $a \equiv 4 \pmod{5} \Rightarrow$ подходит a, равное 4, 11, 14

Ответ:

4, 11, 14

Задание 5

Не используя перебор, решите систему сравнений

$$\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 1 \pmod{13} \end{cases}$$

Решение:

Используя КТО, заключаем, что

$$x \equiv \sum_{i=1}^{2} b_i \cdot M_i \pmod{143} \equiv b_1 \cdot 13 + b_2 \cdot 11 \equiv \pmod{143}$$

$$b_1 \cdot 13 \equiv 2 \pmod{11} \Rightarrow b_1 = 1$$

$$b_2 \cdot 11 \equiv 1 \pmod{13}$$

Решим сравение с неизвестным b_2

$$11b_2 + 13y = 1$$

$$\begin{pmatrix} 11 & 13 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 11 & 2 \\ 1 & -1 \\ 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 2 \\ 6 & -1 \\ -5 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 \\ 6 & -13 \\ -5 & 11 \end{pmatrix} \Rightarrow$$

$$\begin{pmatrix} b_2 \\ y \end{pmatrix} = \begin{pmatrix} 6 \\ -5 \end{pmatrix} + t \cdot \begin{pmatrix} -13 \\ 11 \end{pmatrix}, t \in \mathbb{Z}$$

$$\Rightarrow b_2 = 6 - 13t \Rightarrow b_2 \equiv 6 \pmod{13} \Rightarrow b_2 = 6$$

$$\Rightarrow x \equiv 13 + 66 \equiv 79 \pmod{143}$$

Ответ:

$x \equiv 79 \pmod{143}$