17 января 2023

Решение сравнений. Деление по модулю.

Что наша жизнь? Роман. — Кто автор? Аноним.
Читаем по складам, смеёмся, плачем… спим.

Н. М. Карамзин, «Два сравнения»

Напомню, целые числа a и b называют сравнимыми по модулю m, если они дают одинаковые остатки от деления на m. Это записывают так: $a \equiv b \pmod{m}$. При решении этого листка можно пользоваться всеми свойствами сравнений по модулю, которые мы доказывали на уроках.

1 Решите сравнения (т. е. найдите все решения по тому модулю, по которому производится сравнение, или докажите, что их нет):

a $5x \equiv 6 \pmod{11}$; b $2x \equiv 5 \pmod{13}$; c $4x \equiv 8 \pmod{12}$;
d $10x \equiv 5 \pmod{15}$; e $6x \equiv 2 \pmod{3}$; f $77x \equiv 1 \pmod{132}$.

2 $2x \equiv 5 \pmod{11}$. Какие решения у этого сравнения есть по модулю 22?

3 Решите систему сравнений:

$$\begin{cases} 2x + 3y \equiv 7 \pmod{13} \\ 3x + 4y \equiv 10 \pmod{13} \end{cases}$$

4 Докажите, что, если a и n взаимно просты, то у сравнения $ax \equiv b \pmod{n}$

a всегда есть решение; b есть единственное решение по модулю n.

Назовём *частным* от деления числа a на b по модулю n такое число c, что $a \equiv bc \pmod{n}$. Например, $1:3 \equiv 3 \pmod{4}$. Как и в арифметике целых чисел, деление по модулю возможно не всегда.

5 Составьте «таблицы деления» a по модулю 5 b по модулю 6. Пример (mod 4):

:	0	1	2	3
0	0/1/2/3	0	0/2	0
1	-	1	-	3
2	-	2	1/3	2
3	-	3	-	1

Заметьте, что результат деления не всегда однозначен!

6 Докажите, что если 1 делится на a по модулю n, то любое число делится на a по модулю n. В каком случае 1 не делится на a по модулю n?

Если 1 делится на a по модулю n, говорят, что a *обратимо* по модулю n. Результат деления $1:a \pmod{n}$ называется *обратным* к a остатком по модулю n и обозначается a^{-1}.

7 Найдите обратные остатки для:

a 1, 2, 3, 4, 5, 6 (mod 7); b 1, 3, 5, 7 (mod 8); c 2 (mod 9); d 16 (mod 31).

---

8 Докажите, что произведение k последовательных чисел всегда делится на $k!$.

9 Докажите, что $(C_n^0)^2 + (C_n^1)^2 + \cdots + (C_n^n)^2 = C_{2n}^n$.