kaspersky.academy

Арифметика

Лекция 2. Сравнения

по модулю

Математика в кибербезопасности

Лекция 2. Сравнения по модулю

Сравнение чисел по модулю

Видео 1, 0:42 - 2:58

Сравнение чисел a и b по модулю m покажет, равны ли остатки от деления этих чисел на m:

5 / 3 = 1 | 2 – остаток
5 mod 3 = 2
$5 \equiv 2 \bmod 3$,
$\equiv$ - знак сравнимости чисел

Какие остатки от деления на m можно получить?

- Если $a \vdots m$, то $a \equiv 0 \bmod m$
- Если $a \equiv b \bmod m$, то a и b сравнимы по mod m
- Чисел a, сравнимых с b по mod m – бесконечное количество

Сложение и умножение чисел по модулю

Видео 1, 2:59 - 3:28

$5 \equiv 2 \bmod 3$
$4 \equiv 1 \bmod 3$

Сложение:
$(5 + 4) \bmod 3 \equiv 9 \bmod 3 \equiv 0 \bmod 3$

Умножение:
$5 \cdot 4 \bmod 3 \equiv 20 \bmod 3 \equiv 2 \bmod 3$

Что можно делать со сравнениями

Видео 1, 3:29 - 3:53

- Можно прибавлять к обеим частям число c: $a + c \equiv b + c \bmod m$
- Можно умножать обе части на число c: $a \cdot c \equiv b \cdot c \bmod m$

Вычитание чисел по модулю

Видео 1, 3:54 - 4:34

Операция «вычитание» – это сложение с числом, обратным по модулю по сложению

В целых числах $\mathbb{Z}$:
$2 + (-2) = 0$

a и b - обратные числа по сложению, если:
$a + b = 0$

Обозначение обратного числа:
$a = -b$
$b = -a$

Обратные числа по сложению

Видео 1, 4:35 - 6:07

a и b - обратные числа по сложению, если:
$a + b \equiv 0 \bmod m$

Тогда:
$b \equiv (m - a) \bmod m$

Если b – отрицательное число по mod m:
$b \bmod m \equiv (m + b) \bmod m$, где $b < 0$

Чтобы из отрицательного числа получить положительное, нужно взять обратное к нему по сложению:

$-2 \bmod 3 \equiv (3 - 2) \bmod 3 \equiv 1 \bmod 3$

Обратное число по сложению существует всегда

Деление чисел по модулю

Видео 1, 6:08 - 6:50

Операция «деление» - это умножение числа a на обратное к нему по умножению:

$6 / 2 = 6 \cdot 2^{-1} = 6 \cdot 1/2 = 6/2 = 3$

Обратные по умножению числа

Видео 1, 6:56 - 7:49

a, b – обратные, если $a \cdot b \equiv 1 \bmod m$

Пример:

$$2 \cdot 3 \equiv 1 \bmod 5$$

2 и 3 – обратные умножению по mod 5, то есть:

$$2 \equiv 3^{-1} \bmod 5$$
$$3 \equiv 2^{-1} \bmod 5$$

Как искать обратные по умножению числа

Видео 2, 0:00 - 1:25

Первый способ – подбором:

$$a = 4, m = 5$$
$$a \cdot b \equiv 1 \bmod m$$

Будем перебирать значения b:

$b = 1$: $4 \cdot 1 \bmod 5 = 4$
$b = 2$: $4 \cdot 2 \bmod 5 = 3$
$b = 3$: $4 \cdot 3 \bmod 5 = 2$
$b = 4$: $4 \cdot 4 \bmod 5 = 1$

Второй способ - с помощью расширенного алгоритма Евклида

НОД

Видео 2, 1:26-2:15

НОД (Наибольший Общий Делитель для целых чисел) – наибольшее число, на которое одновременно делятся несколько чисел

Если НОД (a, b) = 1, то a и b – взаимно простые числа

Обратное по умножению к числу a mod m будет существовать, если a и m– взаимно простые числа

Алгоритм Евклида

Видео №2, 2:16 - 3:45

Алгоритм Евклида используется для поиска наибольшего общего делителя двух целых чисел

Для любых целых чисел a, b:

$$\exists!\, q, r:$$
$$a = b \cdot q + r$$
$$r \geq 0$$

$$\text{НОД}(a, b) = \text{НОД}(b \cdot q + r, b) = \text{НОД}(a - b \cdot q, b) = \text{НОД}(r, b) = \text{НОД}(b, r)$$

Пример:

НОД (43, 15) = НОД (13, 15) = НОД (15, 13) = НОД (2, 13) = НОД (13, 2) = НОД (1, 2) = НОД (2, 1) = НОД (0, 1).

Наименьший общий делитель равен единице — значит числа 43 и 15 являются взаимно простыми

Расширенный алгоритм Евклида

Видео 2, 3:46 - 7:56

1. Выразим оба числа «друг через друга»
2. Коэффициенты выпишем в две строки
3. Вычитаем из первой строки вторую максимальное количество раз
4. Вычитаем из второй строки третью, пока не получим 0 в левом столбце

Пример: НОД (48, 15) = 3

Значит, эти числа не взаимно простые.

$$48 = 1 \cdot 48 + 0 \cdot 15$$
$$15 = 0 \cdot 48 + 1 \cdot 15$$

48	1	0	
15	0	1	
3	1	-3	НОД
0	-5	16	

Взаимно простые и обратные по умножению: используем расширенный алгоритм Евклида:

$$15 \cdot b \equiv 1 \bmod 43$$

b - ?

43	1	0	
15	0	1	
13	1	-2	
2	-1	3	
1	7	-20	НОД
0	-15	43	

Проверяем, что найденное число – обратно простое по умножению

$$НОД\ (43, 15) = 1$$
$$1 = 7 \cdot 43 - 20 \cdot 15$$
$$b = -20 \equiv (43 - 20) \bmod 43 \equiv 23 \bmod 43$$
$$23 \cdot 15 \equiv 1 \bmod 43$$
$$345 \equiv 1 \bmod 43$$

Значит, 23 и 15 – взаимно обратные числа.