kaspersky.academy

Арифметика

Лекция 3. Уравнения в целых числах

Математика в кибербезопасности

Лекция 3. Уравнения в целых числах

Операции сложения по модулю - аддитивная операция

Видео 1:13 - 1:51

Арифметическая операция будет аддитивной, если выполняется равенство:

$$(a + b) \bmod m \equiv a \bmod m + b \bmod m$$

Пример:

$$(35 + 28) \bmod 3 \equiv \underbrace{35 \bmod 3}_{2} + \underbrace{28 \bmod 3}_{1} \equiv (2 + 1) \bmod 3 \equiv 0 \bmod 3$$

Операции умножения по модулю - мультипликативная операция

Видео 1:52 - 2:38

Арифметическая операция будет мультипликативной, если выполняется равенство:

$$(a \cdot b) \bmod m \equiv a \bmod m \cdot b \bmod m$$

Пример:

$$(50 \cdot 703) \bmod 7 \equiv \underbrace{50 \bmod 7}_{1} \cdot \underbrace{703 \bmod 7}_{3} \equiv 1 \cdot 3 \bmod 7 \equiv 3 \bmod 7$$

Возведение в степень по модулю

Видео 2:41 - 4:11

$$2^{2020} \bmod 7 = \underbrace{2 \bmod 7 \cdot 2 \bmod 7 \cdot \ldots \cdot 2 \bmod 7}_{2020\ \text{раз}}$$

Пример возведения числа по модулю в огромную степень:

$$2^{1023} \bmod 5 \equiv ?$$
$$2^4 \equiv 1 \bmod 5$$
$$2^{1023} \bmod 5 \equiv \underbrace{2^4 \cdot 2^4 \cdot \ldots \cdot 2^4}_{255\ \text{раз}} \cdot 2^3 \bmod 5 \equiv \underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{255\ \text{раз}} \cdot 2^3 \bmod 5 \equiv 2^3 \bmod 5 \equiv 8 \bmod 5$$

Решение уравнений в модульной арифметике

Видео 4:13 - 5:22

$$5x \equiv 3 \bmod 7$$

Чтобы найти x, нужно избавиться от 5 в левой части.

Умножим обе части на $5^{-1} \bmod 7$:

$$5^{-1} \equiv 3 \bmod 7$$
$$3 \cdot 5x \equiv 3 \cdot 3 \bmod 7$$
$$x \equiv 9 \bmod 7$$
$$x \equiv 2 \bmod 7$$

Китайская Теорема об Остатках (КТО). Решение системы сравнений

Видео 5:30

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \dots \\ x \equiv a_n \bmod m_n \\ \\ 0 \le a_i < m_i \end{cases}$$

m_1, m_2, ... m_n - попарно взаимно простые (любые два числа взаимно просты)
Решение системы будем искать по модулю $M = m_1 \cdot m_2 \cdot \dots \cdot m_n$

Решим систему уравнения **подбором:**

Пример решения 1:

$$\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \end{cases}$$

1. Перемножим все модули:
   $M = 2 \cdot 3 \cdot 5 = 30$

   Каким может быть x?

$$\begin{cases} x \equiv 1 \bmod 2 \rightarrow x = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25,.. \\ x \equiv 2 \bmod 3 \rightarrow x = 2, 5, 8, 11, 14, 17, 20, 23, 26,.. \\ x \equiv 3 \bmod 5 \rightarrow x = 3, 8, 13, 18, 23, 28, 33,.. \end{cases}$$

Ответ: $x \equiv 23 \bmod 30$, значит, наименьшее число, которое может быть решением системы – 23

Алгоритм решения:

1. Перемножим все модули:
   $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n = 7 \cdot 8 \cdot 5 = 280$
2. Найдем M_i: $M_i = \frac{M}{m_i}$
3. Используем расширенный алгоритм Евклида:
   $M_i^{-1} \equiv (M_i \bmod m_i)^{-1} \bmod m_i$
4. Умножим и сложим целые числа: $x \equiv (a_1 \cdot M_1 \cdot M_i^{-1} + \ldots + a_n \cdot M_n \cdot M_n^{-1}) \bmod M$

Пример решения 2:

$$\begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 4 \bmod 8 \\ x \equiv 2 \bmod 5 \end{cases}$$

1. Перемножим все модули:
   $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n = 7 \cdot 8 \cdot 5 = 280$
2. Найдем M_i:
   $M_1 = \frac{280}{m_1} = \frac{280}{7} = 40$
   $M_2 = \frac{280}{m_2} = \frac{280}{8} = 35$
   $M_3 = \frac{280}{m_3} = \frac{280}{5} = 56$
3. Используем расширенный алгоритм Евклида:
   $M_i^{-1} \equiv (M_i \bmod m_i)^{-1} \bmod m_i$
   $M_1^{-1} \equiv (40 \bmod 7)^{-1} \bmod 7 \equiv 5^{-1} \bmod 7 \equiv 3 \bmod 7$
   $M_2^{-1} \equiv 3 \bmod 8$
   $M_3^{-1} \equiv 1 \bmod 56$

4. Умножим и сложим целые числа:
   $x \equiv (a_1 \cdot M_1 \cdot M_i^{-1} + \ldots + a_n \cdot M_n \cdot M_n^{-1}) \bmod M$
   $x \equiv (3 \cdot 40 \cdot 3 + 4 \cdot 35 \cdot 3 + 2 \cdot 56 \cdot 1) \bmod 280 \equiv 892 \bmod 280 \equiv 52 \bmod 280$

Ответ: $x \equiv 52 \bmod 280$