Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Сравнения и системы сравнений

Свойства сравнений $a \equiv b \ (mod\ m)$

- $a \equiv b \ (mod\ m)$ тогда и только тогда, когда a и b имеют одинаковые остатки от деления на m.
- Если $a \equiv b \ (mod\ m)$, то $ka \equiv kb \ (mod\ m)$ для любого $k \in \mathbb{Z}$.
- Если $ka \equiv kb \ (mod\ m)$ и $\text{НОД}(k, m) = 1$, то $a \equiv b \ (mod\ m)$.
- Если $a \equiv b \ (mod\ m)$, то $ka \equiv kb \ (mod\ km)$ для любого $k \in \mathbb{N}$.
- Если $ka \equiv kb \ (mod\ km)$, где $k, m \in \mathbb{N}$, то $a \equiv b \ (mod\ m)$.
- Если $a \equiv b \ (mod\ m)$ и $d | m$, то $a \equiv b \ (mod\ d)$.
- Если $a \equiv b \ (mod\ m)$ и $c \equiv d \ (mod\ m)$, то верно следующее:
  - $a + c \equiv b + d \ (mod\ m)$;
  - $a - c \equiv b - d \ (mod\ m)$;
  - $ac \equiv bd \ (mod\ m)$
- Если $a \equiv b \ (mod\ m)$, то для любого целого $n \geq 0$ выполняется $a^n \equiv b^n \ (mod\ m)$.
- Если $a \equiv b \ (mod\ m)$, то множество общих делителей чисел a и m совпадает с множеством общих делителей чисел b и m, в частности $\text{НОД}(a, m) = \text{НОД}(b, m)$.

Сравнение первой степени с одним неизвестным

- **Сравнение первой степени** с одним неизвестным:

  $ax \equiv b\ (mod\ m)$.

- **Решение**:
  - если $\text{НОД}(a, m) = 1$, то множеством решений является класс вычетов $a^{-1} \cdot b \in \mathbb{Z}_m$;
  - если $\text{НОД}(a, m) = \text{d} > 1$ и $d \nmid b$, то решений не существует;
  - если $\text{НОД}(a, m) = \text{d} > 1$ и $d|b$, то множеством решений являются d классов вычетов по модулю m, образующих один класс вычетов по модулю $\tilde{m} = \frac{m}{d}$:
    - $\tilde{a}^{-1} \cdot \tilde{b} \in \mathbb{Z}_{\tilde{m}}$;
    - $\left(\tilde{a}^{-1} \cdot \tilde{b} + \tilde{m}\right) \in \mathbb{Z}_{\tilde{m}}$;
    - …
    - $\left(\tilde{a}^{-1} \cdot \tilde{b} + \tilde{m}(d-1)\right) \in \mathbb{Z}_{\tilde{m}}$.

Пример решения сравнения $15x \equiv 20\ (mod\ 85)$

- Нахождение НОД(a, m):
  - $d = \text{НОД}(15{,}85) = 5.$
- Проверка делимости b на d:
  - 5 делит 20.
- Преобразование сравнения:
  - $15x \equiv 20\ (mod\ 85), \Rightarrow 3x \equiv 4\ (mod\ 17).$
- Решение нового сравнения:
  - $3^{-1}\ (\text{mod}\ 17) \equiv 6;$
  - $x \equiv 6 \cdot 4\ (\text{mod}\ 17) \equiv 7;$

q	r	y	m	a	y_2	y_1
–	–	–	17	3	0	1
5	2	−5	3	2	1	−5
1	2	6	2	1	−5	6
2	0		1	0	6	

Множество решений исходного сравнения:

- $x = 7\ (\text{mod}\ 85);$
- $x = 7 + 17(\text{mod}\ 85);$
- $x = 7 + 34\ (\text{mod}\ 85).$
- $x = 7 + 51\ (\text{mod}\ 85);$
- $x = 7 + 68\ (\text{mod}\ 85);$

Система сравнений

- Система сравнений:

$$- \begin{cases} x \equiv a_1 \pmod{n_1}, \\ x \equiv a_2 \pmod{n_2}, \\ \dots \\ x \equiv a_k \pmod{n_k}. \end{cases} \quad (*)$$

- Решение системы сравнений $(*)$ представляет собой восстановление натурального числа по его остаткам для различных модулей n_1, $n_2, \dots, n_k$.
- Алгоритмы решения систем сравнений основаны на китайской теореме об остатках.

- **Китайская теорема об остатках**. Пусть n_1, $n_2, \dots, n_k$ — попарно взаимно простые натуральные числа, $N = \prod_{i=1}^{k} n_i$, $N_i = {}^{N}/_{n_i}$ и целые числа u_i, v_i удовлетворяют равенствам $u_i N_i + v_i n_i = 1 \quad \forall\, i = 1, 2, \dots, k$. Тогда единственным решением по модулю N системы сравнений $(*)$ является следующее число:
  - $a \equiv \left(\sum_{i=1}^{k} a_i u_i N_i\right) \bmod N.$

Пример решения системы сравнений

- Решить систему сравнений $\begin{cases} x \equiv 2 \pmod 4, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod 7. \end{cases}$

- Решение:
  - $N = 4 \cdot 5 \cdot 7 = 140;$
  - $N_1 = {}^{140}/_{4} = 35;$
  - $N_2 = {}^{140}/_{5} = 28;$
  - $N_3 = {}^{140}/_{7} = 20;$
  - $a = (2 \cdot (-1) \cdot 35 + 3 \cdot 2 \cdot 28 + 2 \cdot (-1) \cdot 20) = 58.$

q	r	x	N_1	n_1	x_2	x_1
–	–	–	35	4	1	0
8	3	1	4	3	0	1
1	1	−1	3	1	1	−1
3	0		1	0	−1	

q	r	x	N_2	n_2	x_2	x_1
–	–	–	28	5	1	0
5	3	1	5	3	0	1
1	2	−1	3	2	1	−1
1	1	2	2	1	−1	2
2	0		1	0	2	

q	r	x	N_3	n_3	x_2	x_1
–	–	–	20	7	1	0
2	6	1	7	6	0	1
1	1	−1	6	1	1	−1
6	0		1	0	−1	

Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Криптографические методы защиты информации

Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru