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

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Теоретико-числовые алгоритмы

Алгоритмы вычисления наибольшего общего делителя

Наибольший общий делитель

- **Наибольшим общим делителем** целых чисел $a, b \in \mathbb{Z}$ ($\text{НОД}(a, b)$) называется такое целое число $d \geq 1$, которое удовлетворяет следующим условиям:
  - d есть общий делитель a и b;
  - если $d' \in \mathbb{Z}$ есть любой общий делитель a и b, то d делится на d'.
- Если $\text{НОД}(a, b) = 1$, то a и b называются взаимно простыми числами.
- Целое число p , делители которого исчерпываются числами ± 1 и $\pm p$, называется **простым числом**.
- **Основная теорема арифметики**. Каждое натуральное число $n > 1$ может быть записано в виде произведения простых чисел, не обязательно различных, а именно: $n = p_1 p_2 \dots p_k$, причём эта запись единственна с точностью до порядка сомножителей.

Деление с остатком в кольце целых чисел

- **Теорема**. Для заданных чисел $a, b \in \mathbb{Z}$, $b > 0$ существуют числа $q, r \in \mathbb{Z}$, такие, что $a = qb + r$, $0 \le r < b$.
- **Теорема**. В $\mathbb{Z}$ для любых двух целых чисел a и b существует $d = \text{НОД}(a, b)$. Более того, существуют целые числа u, v, такие, что $au + bv = d$.
- Запись $au + bv = d$ будем называть **целочисленной линейной комбинацией** a и b.

- Алгоритмы нахождения наибольшего общего делителя целых чисел:
  - алгоритм Евклида.
  - расширенный алгоритм Евклида.

Алгоритм Евклида

Вход: целые числа $a \geq b > 0$.

Выход: $d = \text{НОД}(a, b)$.

Шаг 1. Пока $b \neq 0$, выполнять следующее:

Шаг 1.1. Вычислить $r \leftarrow a \bmod b$.

Шаг 1.2 Присвоить $a \leftarrow b$, $b \leftarrow r$.

Шаг 2. Возврат (a).

Расширенный алгоритм Евклида

Вход: целые числа $a \geq b > 0$.

Выход: $d = \text{НОД}(a, b)$ и целые x, y, такие, что $ax + by = d$.

Шаг 1. Полагаем $x_2 \leftarrow 1, x_1 \leftarrow 0, y_2 \leftarrow 0, y_1 \leftarrow 1$.

Шаг 2. Пока $b \neq 0$, выполнять следующее:

Шаг 2.1. $q \leftarrow [{}^{a}/_{b}], r \leftarrow a - qb, x \leftarrow x_2 - qx_1, y \leftarrow y_2 - qy_1$.

Шаг 2.2. $a \leftarrow b, b \leftarrow r, x_2 \leftarrow x_1, x_1 \leftarrow x, y_2 \leftarrow y_1, y_1 \leftarrow y$.

Шаг 3. $d \leftarrow a, x \leftarrow x_2, y \leftarrow y_2$ и возврат (d, x, y).

Пример работы расширенного алгоритма Евклида

- **Вход**: целые числа $1120 \geq 73 > 0$.

q	r	x	y	a	b	x_2	x_1	y_2	y_1
–	–	–	–	1120	73	1	0	0	1
15	25	1	-15	73	25	0	1	1	-15
2	23	-2	31	25	23	1	-2	-15	31
1	2	3	-46	23	2	-2	3	31	-46
11	1	-35	537	2	1	3	-35	-46	537
2	0			1	0	-35		537	

- **Выход**: $-35 \cdot 1120 + 537 \cdot 73 = \text{НОД}(1120, 73) = 1.$

Некоторые теоретико-числовые свойства колец классов вычетов

Нахождение обратных элементов по модулю n

- При проведении криптографических преобразований возникает задача нахождения обратных элементов в кольце $\mathbb{Z}_n$, а именно: по данному элементу $a \in \mathbb{Z}_n^*$ найти $a^{-1} \in \mathbb{Z}_n^*$ или же $a^{-1} \pmod{n}$.
- Пусть $xn + ya = d = \text{НОД}(n, a)$. Если $d = 1$, то верно следующее:
  - $xn + ya = 1$;
  - $(xn + ya) \bmod n \equiv 1 \bmod n$;
  - $ya \equiv 1 \bmod n$;
  - $y = a^{-1} \pmod{n}$.

Алгоритм вычисления $a^{-1} \pmod{n}$.

Вход: $n > a > 0,\ a, n \in \mathbb{Z}$.

Выход: $a^{-1} \pmod{n}$.

Шаг 1. Используя расширенный алгоритм Евклида, найти целые числа x, y, такие, что $xn + ya = d = \text{НОД}(n, a)$.

Шаг 2. Если $d > 1$, то $a^{-1} \pmod{n}$ не существует.

Шаг 3. Если $d = 1$, то возврат (y).

Пример нахождения обратного элемента по модулю n

- Найти $13^{-1} \pmod{267}$.
- **Вход**: целые числа $267 > 13 > 0$.

q	r	y	n	a	y_2	y_1
–	–	–	267	13	0	1
20	7	−20	13	7	1	−20
1	6	21	7	6	−20	21
1	1	−41	6	1	21	−41
6	0		1	0	−41	

- **Выход**: $13^{-1} \pmod{267} = -41 = 226.$

Функция Эйлера

- **Функцией Эйлера** $\varphi(m)$, $m \in \mathbb{N}$ называется число натуральных чисел, не превосходящих m и взаимно простых с m.
- **Теорема**. Пусть $\text{НОД}(k, l) = 1$, тогда $\varphi(kl) = \varphi(k) \cdot \varphi(l)$.
- **Теорема**. Пусть $m = p^k$, где p — простое число, тогда $\varphi(m) = p^{k-1}(p-1)$.
- **Теорема**. Пусть число m имеет каноническое разложение $m = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$, тогда $\varphi(m) = p_1^{k_1-1} p_2^{k_2-1} \dots p_l^{k_l-1}(p_1 - 1)(p_2 - 1) \dots (p_l - 1)$.

$$|\mathbb{Z}_{\boldsymbol{m}}^*| = \boldsymbol{\varphi(m)}$$

Примеры нахождения $|\mathbb{Z}_m^*|$

- $\mathbb{Z}_{55}^*$:
  - $55 = 5 \cdot 11, \Rightarrow \left|\mathbb{Z}_{55}^*\right| = \varphi(5 \cdot 11) = 4 \cdot 10 = 40.$
- $\mathbb{Z}_{1024}^*$:
  - $1024 = 2^{10}, \Rightarrow |\mathbb{Z}_{1024}^*| = \varphi\left(2^{10}\right) = 2^9 \cdot (2-1) = 512.$
- $\mathbb{Z}_{243000}^*$:
  - $243000 = 2^3 \cdot 3^5 \cdot 5^3, \Rightarrow$
    $|\mathbb{Z}_{243000}^*| = \varphi\left(2^3 \cdot 3^5 \cdot 5^3\right) = 2^2 \cdot 3^4 \cdot 5^2 \cdot (2-1) \cdot (3-1) \cdot (5-1) = 64800.$

Теорема Эйлера и малая теорема Ферма

- **Теорема Эйлера**. Пусть натуральное число $a \in \mathbb{Z}_n$. Если $\text{НОД}(a, n) = 1$, то верно следующее сравнение $a^{\varphi(n)} \equiv 1 \pmod{n}$.
- Теорема Эйлера определяет альтернативный способ вычисления $a^{-1} \in \mathbb{Z}_n^*$:
  - $a^{\varphi(n)} \equiv 1 \pmod{n}$;
  - $a \cdot a^{\varphi(n)-1} \equiv 1 \pmod{n}$;
  - $a^{\varphi(n)-1} = a^{-1} \pmod{n}$.
- Следствием из теоремы Эйлера является малая теорема Ферма.
- **Малая теорема Ферма**. Если p — простое число, то для любого ненулевого числа $a \in \mathbb{Z}_p$ верно $a^{p-1} \equiv 1 \pmod{p}$.

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