Теория чисел $\mathbb{Z}_m$

- $a, b, m \in \mathbb{Z}$, $m \neq 0$ $\quad a \underset{m}{\equiv} b \quad (a-b) \vdots m \qquad a \underset{m}{\equiv} a;\ a \underset{m}{\equiv} b, b \underset{m}{\equiv} c \Rightarrow a \underset{m}{\equiv} c$

  $a \underset{m}{\equiv} b \Rightarrow b \underset{m}{\equiv} a$

  $\begin{matrix} a \equiv b \\ c \underset{m}{\equiv} d \end{matrix} \Rightarrow \begin{matrix} a+c \underset{m}{\equiv} b+d \\ ac \underset{m}{\equiv} bd \end{matrix}$

- алгоритм Евклида $\text{НОД}(a,b) = \gcd(a,b) = \max d: d|a, d|b$

  $\gcd(a,b) = \gcd(a-kb, b) \quad \forall k \in \mathbb{Z}$

```
gcd(a,b):
    if b==0: return a
    else: return gcd(b, a mod b)        // a<b -> swap
                                        иначе (a,b)->(b,<b)
```

Количество арифм. операций:

$a \geq b$. 1). $a \geq 2b \quad (b, \underbrace{a \bmod b}_{<b \leq \frac{a}{2}})$

2). $2b > a \geq b \quad a \bmod b = a - b < a - \frac{a}{2} = \frac{a}{2}$

$b > \frac{a}{2}$

$\text{Time} = O(\log|a| + \log|b|)$

- Расширенный алгоритм Евклида

Lm. $\begin{cases} d|a, d|b. \\ \exists x,y: ax+by=d \end{cases} \Longleftrightarrow d = \gcd(a,b)$

Д-во $\boxed{\Leftarrow}$ $\gcd(a,b)|a \quad \gcd(a,b)|b$

$\exists x,y: ax+by = \gcd(a,b)$ – ?

$\boxed{\Rightarrow}$ $d|a, d|b \Rightarrow d$ – общ. дел. a, b

$\underbrace{ax}_{\vdots \gcd(a,b)} + \underbrace{by}_{\vdots \gcd(a,b)} = d \Rightarrow d \vdots \gcd(a,b) \Rightarrow d \geq \gcd(a,b) \Rightarrow d = \gcd(a,b)$

▨

```
ext_gcd (a,b): —> (x,y): ax+by=gcd(a,b)
    if b==0:
        return (1,0)
    else:
        x',y' = ext_gcd(b, a mod b)
        return (y', x'-y'*(a div b))
```

$a = k \cdot b + r \quad 0 \leq r < b$

$x' \cdot b + y' \cdot \underset{}{r} = \gcd(b,r) = \gcd(a,b)$

$\| + y'kb - y'kb$

$(-y'k + x') \cdot b + y' \cdot \underbrace{(r+kb)}_{a}$

- Линейное диофантово уравнение

$a, b, c \in \mathbb{Z}$

$x, y = ?\quad \underbrace{ax}_{\vdots d} + \underbrace{by}_{\vdots d} + \underbrace{c}_{\vdots d} = 0$

1). $d := \gcd(a,b) \quad c \not\vdots d \Rightarrow$ решений нет

2). $c = k \cdot d$

$(x', y') = \text{ext\_gcd}(a,b)$

$x'a + y'b = d \quad | \cdot (-k)$

$\underbrace{(-kx')}_{x} a + \underbrace{(-ky')}_{y} b + \underbrace{kd}_{c} = 0$

Деление по модулю $a/b \underset{m}{\equiv} x \Leftrightarrow a \underset{m}{\equiv} bx \qquad \textcircled{b^{-1}} \quad b \cdot (b^{-1}) \underset{m}{\equiv} 1$

$x = (b^{-1}) \cdot a$

① • $m = p \in \mathbb{P}$ $\qquad$ **Th.** (Малая теорема Ферма) $p \in \mathbb{P}$, $a \not\vdots p$ ($\gcd(a,p)=1$) $\Rightarrow a^{p-1} \underset{p}{\equiv} 1$

$b \cdot (\ldots) \underset{p}{\equiv} 1$

$b \cdot (b^{p-2}) \underset{p}{\equiv} 1 \quad (b \not\vdots p)$

$b^{-1} := b^{p-2} \bmod p \quad (b \not\vdots p)$

$\text{Time} = O(\log p)$ (арифм. опер.)

```
power (x,d,m):
    if d==0:
        return 1 mod m
    else:
        y = x*x mod m
        z = power (y, d div 2, m)
        return z if d mod 2 == 0 else
            (z*x) mod m
```

$x^d \quad (x^2)^{d/2}$

$x^{2k} = (x^2)^k$

$x^{2k+1} = (x^2)^k \cdot x$

• $m \in \mathbb{Z}$ $\qquad$ **Th.** (теорема Эйлера) $m \in \mathbb{Z}$, $\gcd(a,m) = 1 \Rightarrow a^{\varphi(m)} \underset{m}{\equiv} 1 \qquad \varphi(m)$ – функция Эйлера

$\varphi(p) = p-1$

$(b^{-1}) := b^{\varphi(m)-1} \bmod m$

$\gcd(b,m) = 1$

$\left[\gcd(b,m) = d > 1 \Rightarrow \underbrace{bx}_{\vdots d} \underset{m}{\equiv} \underbrace{1}_{\vdots d} \quad \underbrace{bx}_{\vdots d} - \underbrace{1}_{\not\vdots d} = \underbrace{m \cdot k}_{\vdots d}\right]$ (?!)

Проблема: чтобы вычислить $\varphi(m)$, нужно знать разложение m на простые. Его умеем искать, например, за $O(\sqrt{m})$.

Если знаем $\varphi(m)$, то $\text{Time} = O(\log \varphi(m)) = O(\log m)$

$\varphi(m) \leq m$

② $m \in \mathbb{Z}$ Расширенный алг. Евклида.

$b \cdot x \underset{m}{\equiv} 1 \Leftrightarrow b\underline{x} + my = 1 \qquad \gcd(b,m) = 1$

$(x,y) = \text{ext\_gcd}(b,m) \qquad \text{Time} = O(\log m)$

$b^{-1} := x \bmod m$

Замечание $m = 6 \quad 2^{-1}$ не сущ. $\quad 2 \cdot x \underset{6}{\not\equiv} 1 \qquad ax \underset{m}{\equiv} b$

$4/2 \underset{6}{\equiv} 2 \quad 2 \cdot 2 \underset{6}{\equiv} 4 \qquad \Updownarrow$

$ax + my - b = 0$ – лин. диоф. ур-ие

Проверка на простоту и разложение на мн-ли

1). $m \begin{matrix} \nearrow \in \mathbb{P} \\ \searrow \notin \mathbb{P} \end{matrix}$ $\qquad$ 2). $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \quad p_i \in \mathbb{P}$

```
for (i=2; i*i <= m; ++i)
    if m % i == 0:
        //m - не простое; break
m-простое
```

$\text{Time} = O(\sqrt{m})$

Все известные алгоритмы разлож. на мн-ли работают за $\omega(\log^c m) \ \forall c > 0$

$\text{Time} = O(\sqrt{m}) \rightsquigarrow O(\sqrt[4]{m}) \rightsquigarrow 2^{c(\log m)^{\alpha} \cdot (\log\log m)^{1-\alpha}}$ α, c – конст.

$2^{\log m \cdot \ldots}$

$2^{\sqrt{\log m}}$

$\text{Time} = O(\log^2 m)$ $\quad$ Тест Миллера-Рабина (проверка на простоту)

вероятн. алг.

$m \in \mathbb{P} \rightarrow$ выдаст „$\in \mathbb{P}$"

$m \notin \mathbb{P} \rightarrow$ выдаст „$\notin \mathbb{P}$" с вер. $\geq \frac{3}{4}$

(ошибётся с вер. $\leq \frac{1}{4}$)

Повторим k раз $\Rightarrow \Pr\{\text{ошибка}\} \leq \frac{1}{4^k}$

Тест Ферма: $1 < a < m \quad a^{m-1} \underset{m}{\equiv} 1? \qquad \not\equiv 1 \Rightarrow m \notin \mathbb{P}$

$(a,m) = 1$? $\qquad \equiv 1 \Rightarrow$??

если не так $\Rightarrow m \notin \mathbb{P}$

$\exists$ детерм. тест $\text{Time} = O(\log^c m) \quad c \sim 6$

Криптография

Симметричное шифрование: $\overset{\text{сообщение}}{m} \longrightarrow x = \text{Encode}(m, \text{key})$

x – шифротекст

Шифр Цезаря: key = сдвиг алфавита

$m = \text{Decode}(x, \text{key}) \leftarrow x$

Ключи нужно менять!

Асимметричное шифрование:

$A \longleftarrow Б$

public key – знают все

private key – хранит у себя

$x = \text{Encode}(m, \text{public\_key}) \xrightarrow{Б \quad A} m = \text{Decode}(m, \text{private\_key})$

RSA (Rivest, Shamir, Adleman 1977)

– работает не очень быстро по сравн. с симметричн. шифр.

1). $A \rightleftarrows Б$ – общаются с помощью асимметр. шифр. и вырабат. key – общий ключ

2). $A \rightleftarrows Б$ – общаются с помощью симм. шифр., используя key

---

RSA: Алиса генерирует public и private key

p, q – большие случайные (различные) простые числа // выбираем случ. – провер.

$n := p \cdot q \qquad e$ – число от 1 до $\varphi(n) - 1$

$\varphi(n) = (p-1)(q-1) \qquad \gcd(e, \varphi(n)) = 1$

$d := e^{-1} \bmod \varphi(n)$ – умеем за $O(\log \varphi(n))$

2048 бит

$n \sim 2^{2048}$

$\sqrt[4]{2^{2048}} = 2^{512}$

Функция Эйлера $\varphi(n)$:

$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \quad p_i \in \mathbb{P}$ различн., $\alpha_i > 0$

$\varphi(n) = p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1} \times (p_1 - 1)(p_2 - 1) \ldots (p_k - 1)$

$\varphi(p) = (p-1)$

$\text{Encode}(m, (n,e)) = m^e \bmod n = x \qquad \left[m < n\right]$ $\gcd(m,n) = 1$

$\text{Decode}(x, (n,d)) = x^d \bmod n \overset{?}{=} m$

$x^d = (m^e)^d = m^{ed} \underset{n}{\equiv} m$?

$ed \underset{\varphi(n)}{\equiv} 1 \qquad ed = \varphi(n) \cdot k + 1$

$m^{ed} = m^{\varphi(n) \cdot k + 1} \underset{n}{\equiv} 1^k \cdot m = m$

т. Эйлера $m^{\varphi(n) \cdot k} \underset{n}{\equiv} 1$

Противник видит:

$m^e \bmod n, e, n \overset{?}{\longrightarrow} m$