Теория чисел - 2

6 декабря 2021 г. 13:13

Расширенный алг. Евклида

$a, b \quad d = \gcd(a,b)$
$ax+by \vdots d$

$12 \cdot 1 + 8 \cdot (-1) = 4$

Th. $\exists x,y \in \mathbb{Z}: ax+by=d.$

```
def ext_gcd(a,b):  # возвр. (x,y): ax+by = gcd(a,b)        O(log a + log b)
    if b==0:
        return (1,0)
    x1,y1 = ext_gcd(b, a % b)
    return (y1, x1 - (a//b)*y1)
```

$a = bk + r \qquad r = a \bmod b \qquad 0 \le r < b$

$x_1 \cdot b + y_1 \cdot r = \gcd(b,r) = \gcd(a,b)$

$(\quad)\cdot a + (\quad)\cdot b = \gcd(a,b)$

$x_1 b + y_1 (a - bk) = \gcd(a,b)$

$y_1 a + (x_1 - k y_1) b = \gcd(a,b)$

Линейное диоф. ур.-ие от двух пер.

$ax+by=c \qquad a,b,c$ – даны, x,y – ищем $\in \mathbb{Z}$

$\begin{cases} a=0 \\ b=0 \end{cases} \Rightarrow \begin{array}{l} c=0 \Rightarrow x,y \text{ – любые} \\ c \neq 0 \Rightarrow \text{реш. нет} \end{array}$

$\begin{cases} a \neq 0 \\ b \neq 0 \end{cases} \Rightarrow d = \gcd(a,b)$
$c \not\vdots d \Rightarrow$ решений нет
$c \vdots d \Rightarrow c = c_0 \cdot d$
$ax+by = c_0 \cdot d$
$x_0, y_0 = ext\text{-}gcd(a,b)$
$x_0 a + y_0 b = d \quad | \cdot c_0$
$x = x_0 \cdot c_0 \qquad y = y_0 \cdot c_0$ (какое-то из решений, их беск. много)

Быстрое возвед. в степень по модулю

a, k, m – даны
Вычислить $a^k \bmod m$.

$5^{16} \bmod 9$

$k = 1+2(1+2(0+2(0+2\cdot 1))) =$
$1 + 2\cdot 1 + 2^2 \cdot 0 + 2^3 \cdot 0 + 2^4 \cdot 1 =$
$= 10011_2$

$5^{2\cdot 2\cdot 2\cdot 2} \bmod 9 = \left(\left(\left(5^2\right)^2\right)^2\right)^2 \bmod 9 =$
$= \left(\left(\left(25\right)^2\right)^2\right)^2 = \left(\left(7^2\right)^2\right)^2 \bmod 9 = \left(4^2\right)^2 \bmod 9 = 7^2 \bmod 9 = 4 \bmod 9 = 4$

$a^k = a^{1+2(1+2(0+2(0+2)))} = a^{2^0} \cdot a^{2^1} \cdot a^{2^4}$

$(ab) \bmod m = \left((a \bmod m)\cdot(b \bmod m)\right) \bmod m$

```
def pow(a,k,m):
    if k==0:
        return 1 % m
    x = pow(a*a % m, k//2, m)
    if k%2==0:
        return x
    else:
        return x*a % m
```

$pow(a^2, k//2, m)$

$(a^2)^{k/k} \sim a^k$

$k = 2l+1$
$(a^2)^l = a^{2l}$
$a^k = a^{2l+1}$

$x \cdot (a ** (k \% 2)) \% m$

Time $= O(\log k)$ (арифм. операций)

Модульная арифметика

$a \underset{m}{\equiv} b$ (a сравнимо с b по модулю m) $\overset{def}{\Leftrightarrow} (a-b) \vdots m$

$a \underset{m}{\equiv} b \Leftrightarrow a$ и b дают один. ост. mod m

1). $\underset{m}{\equiv}$ – отн. эквивал.: рефл. $a \underset{m}{\equiv} a \quad \forall a$
симм. $a \underset{m}{\equiv} b \Rightarrow b \underset{m}{\equiv} a \quad \forall a,b$
транз. $a \underset{m}{\equiv} b, b \underset{m}{\equiv} c \Rightarrow a \underset{m}{\equiv} c \quad \forall a,b,c$

2). $\begin{cases} a \underset{m}{\equiv} b \\ c \underset{m}{\equiv} d \end{cases} \Rightarrow a+c \underset{m}{\equiv} b+d$

$(a+c)-(b+d) \vdots m ?$
$\underbrace{(a-b)}_{\vdots m} + \underbrace{(c-d)}_{\vdots m} \vdots m ?$

3). $\begin{cases} a \underset{m}{\equiv} b \\ c \underset{m}{\equiv} d \end{cases} \Rightarrow ac \underset{m}{\equiv} bd$

$a-b \vdots m$
$c-d \vdots m$
$ac - bd = ac - ad + ad - bd = a\underbrace{(c-d)}_{\vdots m} + d\underbrace{(a-b)}_{\vdots m} \vdots m$

Деление по модулю

a, b, m – даны

$x = a/b ? \qquad x \cdot b = a \qquad 5/3 = 5 \cdot \frac{1}{3}$

$x: \; x \cdot b \underset{m}{\equiv} a$
$(0 \le x < m)$

$x = b^{-1} \overset{def}{\Leftrightarrow} x \cdot b \underset{m}{\equiv} 1$ – обратный элемент к b mod m

$(a \cdot b^{-1}) \cdot b = a \cdot \underbrace{(b^{-1} \cdot b)}_{\underset{m}{\equiv} 1} \underset{m}{\equiv} a \cdot 1 = a$

4). $\begin{cases} a \underset{m}{\equiv} b \\ c \underset{m}{\equiv} d \end{cases} \Rightarrow \begin{cases} a \underset{m}{\equiv} b \\ c^{-1} \underset{m}{\equiv} d^{-1} \end{cases} \Rightarrow$

$\Rightarrow a c^{-1} \underset{m}{\equiv} b d^{-1}$

(1) $m \in P \quad m = p$
Утв. b^{-1} сущ. $\Leftrightarrow b \not\vdots p.$
Д-во: $\Rightarrow: b \vdots p \Rightarrow bx \not\underset{p}{\equiv} 1$
$\Leftarrow:$ из алгоритма
■

$p = 5$
$b = 3 \qquad b^{-1} = 2$
$2 \cdot 3 = 6 \underset{5}{\equiv} 1$

$b = 10$
$x \cdot 10 \underset{5}{\equiv} 1 \qquad \underbrace{10x - 1}_{\vdots 5} \vdots 5$

Th. (Малая теорема Ферма)
$p \in \mathbb{P}$
$a \not\vdots p$. Тогда $a^{p-1} \underset{p}{\equiv} 1$.

Дано $b \not\vdots p$. $b \cdot (\underbrace{\dots}_{?}) \underset{p}{\equiv} 1$. $b^{-1} = b^{p-2} \bmod p = pow(b, p-2, p)$ Time $= O(\log p)$
b^{p-2}

② m – произвольное $\in \mathbb{N}$

I. Th. (теорема Эйлера)
$a, m \in \mathbb{N}$
$gcd(a,m) = 1$
Тогда $a^{\varphi(m)} \underset{m}{\equiv} 1$, где $\varphi(m)$ – функция Эйлера.

$m = p_1^{d_1} \cdot p_2^{d_2} \cdot \dots \cdot p_k^{d_k}$ – разлож. на прост. $(p_i \neq p_j \ \forall i \neq j)$

$\varphi(m) = (p_1^{d_1} - p_1^{d_1-1})(p_2^{d_2} - p_2^{d_2-1}) \dots (p_k^{d_k} - p_k^{d_k-1})$

$m \in \mathbb{P}$, $m = p$
$\varphi(m) = \varphi(p) = p^1 - p^0 = p - 1$

b^{-1}? 1). $gcd(b,m) \neq 1 \Rightarrow$ обратный $\nexists$ $O(\log m)$
2). $b^{-1} := b^{\varphi(m)-1}$ нужно знать разлож.!

II. $x \cdot b + y \cdot m = 1$ $gcd(b,m) = 1$
$x, y = ext\_gcd(b,m)$
$xb + ym = 1$ $\quad xb - 1 = ym : m$
$\underbrace{ym}_{:m}$ $\quad xb \underset{m}{\equiv} 1$ $\quad x$ – обратн. к b

$b^{-1} := ext\_gcd(b,m)[0]$ Time $= O(\log m)$

1). $gcd(b,m) \neq 1 \Rightarrow$ нет обр.
2). $0 \leq b^{-1} < m \Rightarrow \% m$

Асимметричное шифрование

Симметричное шифрование: A: m – сообщ.
$x = Encode(m, key)$ – шифротекст
Шифр Цезаря (+3) key
m = а б ф а у э
x = г д ч г ш ь
m $\quad -3$
Б: $m = Decode(x, key)$

Асимметричное шифрование: A: m – сообщ.
$x = Encode(m, public\_key)$
Б: public_key – публичн. ключ (публикует на сайте)
private_key – приватный ключ
$m = Decode(x, private\_key)$

RSA (Rivest, Shamir, Adleman, 1977)
Б: p, q – два больших ($\sim 2^{1024}$) простых числа (радомн.)
(выбираем случ. число и проверяем на простоту за $\sim O(\log^2 p)$)
$n = pq \sim 2^{2048}$
e – случ., $0 < e < \varphi(n) = (p-1)(q-1)$, $gcd(e, \varphi(n)) = 1$
$d = e^{-1} \bmod \varphi(n)$
private_key $= \langle n, d \rangle$ public_key $= \langle n, e \rangle$
$Encode(m, \langle n, e \rangle) = (m^e) \bmod n$
$Decode(x, \langle n, d \rangle) = (x^d) \bmod n$
$(m < n)$

$x^d \bmod n \overset{?}{=} m$
$(m^e)^d \underset{n}{\equiv} m$ $\quad m^{ed} \underset{n}{\equiv} m$ $\quad gcd(n,n) = 1$
$m^{\varphi(n)} \underset{n}{\equiv} 1$
$\forall k \quad m^{k \cdot \varphi(n) + 1} \underset{n}{\equiv} m$

Противник: $n, e, m^e \bmod n \xrightarrow{?} m$
Не знает $\varphi(n)$! $\varphi(n) = (p-1)(q-1)$
Разл. n: $O(\sqrt{n})$, $M(\sqrt{n})$ Если $\exists k$: $ed = k \cdot \varphi(n) + 1$, то $m^{ed} \underset{n}{\equiv} m$.
$ed \underset{\varphi(n)}{\equiv} 1$

Замечание. Асимм. шифр. – медленное.
1). Рукопожатие: с помощью асимм. шифр. создают общий ключ key
2). Общаются с помощью симм. шифр. с помощью key