Nhắc lại một số thuật toán trong lý thuyết số

Trần Vĩnh Đức

HUST

Ngày 23 tháng 3 năm 2023

Nội dung

Định nghĩa

- Ước chung của hai số nguyên a và b là số nguyên d thỏa mãn:

$$d \mid a \quad \text{và} \quad d \mid b.$$

- Ta ký hiệu $\gcd(a, b)$ là ước chung lớn nhất của a và b.

Định nghĩa

- Ước chung của hai số nguyên a và b là số nguyên d thỏa mãn:

$$d \mid a \quad \text{và} \quad d \mid b.$$

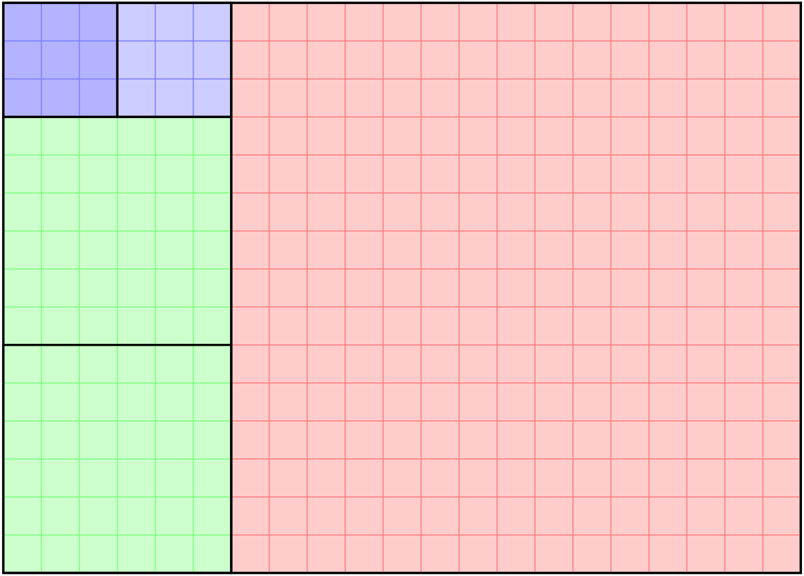
- Ta ký hiệu $\gcd(a, b)$ là ước chung lớn nhất của a và b.

Ví dụ

- $\gcd(12, 18) = 6$ vì $6 \mid 12$ và $6 \mid 18$ và không có số nào lớn hơn có tính chất này.
- $\gcd(748, 2014) = 44$ vì

$$\begin{aligned}\text{các ước của } 748 &= \{1, 2, 4, 11, 17, 22, 34, 44, 68, 187, 374, 748\},\\ \text{các ước của } 2024 &= \{1, 2, 4, 8, 11, 22, 23, 44, 46, 88, 92, 184, 253,\\ &\qquad 506, 1012, 2024\}.\end{aligned}$$

$\gcd(21, 15) = \gcd(15, 6) = \gcd(6, 3)$



Định lý (Thuật toán Euclid)

Xét a, b là hai số nguyên dương với $a \geq b$. Thuật toán sau đây tính $\gcd(a, b)$ sau một số hữu hạn bước.

1. *Đặt $r_0 = a$ và $r_1 = b$.*
2. *Đặt $i = 1$.*
3. *Chia r_{i-1} cho r_i, ta được*
$$r_{i-1} = r_i \cdot q_i + r_{i+1} \qquad \text{với} \qquad 0 \leq r_{i+1} < r_i.$$
4. *Nếu $r_{i+1} = 0$, vậy thì*
$$r_i = \gcd(a, b)$$
và thuật toán kết thúc.
5. *Ngược lại, $r_{i+1} > 0$, vậy thì đặt $i = i + 1$ và quay lại Bước 3.*

Định lý

Phép chia (Bước 3) của Thuật toán Euclid thực hiện nhiều nhất

$$\log_2(b) + 2 \quad \textit{lần.}$$

Thuật toán Euclid (dạng đệ quy)

EUCLID(a, b)
    if $b == 0$
        return a
    else
        return EUCLID$(b, a \mod b)$

Thuật toán Euclid mở rộng

- Thuật toán Euclid có thể mở rộng để tìm thêm một số thông tin.
- Cụ thể, chúng ta mở rộng thuật toán để tính thêm hệ số x, y thỏa mãn
$$d = \gcd(a, b) = ax + by.$$
- Các hệ số x, y có thể âm hoặc bằng 0. Các hệ số này sẽ có ích sau này khi tích phần tử nghịch đảo trong số học modun.

Thuật toán Euclid mở rộng

- *Input* : Cặp số nguyên dương (a, b)
- *Output*: Bộ ba (d, x, y) thỏa mãn

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

EXTENDED-EUCLID(a, b)
    if $b == 0$
        return $(a, 1, 0)$
    else
        $(d', x', y') =$ EXTENDED-EUCLID$(b, a \mod b)$
        $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$
        return (d, x, y)

Tính đúng đắn của thuật toán

- Thuật toán tìm (d, x, y) thỏa mãn

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

- Nếu $b = 0$, vậy thì
$$d = a = a \cdot 1 + b \cdot 0.$$

- Nếu $b \neq 0$, thuật toán EXTENDED-EUCLID sẽ tính (d', x', y') thỏa mãn

$$\begin{aligned} d' = d &= \gcd(b, a \mod b) \\ &= bx' + (a \mod b)y' \end{aligned}$$

- Và vậy thì

$$\begin{aligned} d &= b'x' + (a - b\lfloor a/b \rfloor)y' \\ &= ay' + b(x' - \lfloor a/b \rfloor y') \end{aligned}$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$x = y'$$
$$y = x' - \lfloor a/b \rfloor y'$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$x = y'$$
$$y = x' - \lfloor a/b \rfloor y'$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$x = y'$$
$$y = x' - \lfloor a/b \rfloor y'$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$x = y'$$
$$y = x' - \lfloor a/b \rfloor y'$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$
\begin{aligned}
x &= y' \\
y &= x' - \lfloor a/b \rfloor y'
\end{aligned}
$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2			
3	0	–			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$x = y'$$
$$y = x' - \lfloor a/b \rfloor y'$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2			
3	0	–	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$
\begin{aligned}
x &= y' \\
y &= x' - \lfloor a/b \rfloor y'
\end{aligned}
$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2	3	0	1
3	0	–	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$x = y'$$
$$y = x' - \lfloor a/b \rfloor y'$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1			
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	–	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$x = y'$$
$$y = x' - \lfloor a/b \rfloor y'$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3			
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	–	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$x = y'$$
$$y = x' - \lfloor a/b \rfloor y'$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1			
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	–	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$
\begin{aligned}
x &= y' \\
y &= x' - \lfloor a/b \rfloor y'
\end{aligned}
$$

Ví dụ

a	b	$\lfloor a/b \rfloor$	d	x	y
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	–	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào a và b, giá trị tính $\lfloor a/b \rfloor$, và giá trị trả về d, x, y.
- Bộ ba d, x, y được trả về trở thành bộ ba d', x', y' của mức tiếp theo từ công thức

$$x = y'$$
$$y = x' - \lfloor a/b \rfloor y'$$

Bài tập

Hãy tính giá trị

$$(d, x, y) = \text{EXTENDED-EUCLID}(899, 493).$$

Tính nghịch đảo

- Xét $n > 1$, nếu $\gcd(a, n) = 1$ thì ta có

$$\gcd(a, n) = 1 = ax + ny$$

- Vậy $ax = 1 \pmod{n}$. Tức là

$$x = a^{-1} \pmod{n}$$

Nội dung

Tính lũy thừa nhanh

Ví dụ

Giả sử ta muốn tính

$$3^{218} \pmod{1000}.$$

Đầu tiên, ta viết 218 ở dạng cơ số 2:

$$218 = 2 + 2^3 + 2^4 + 2^6 + 2^7.$$

Vậy thì 3^{218} trở thành

$$3^{218} = 3^{2+2^3+2^4+2^6+2^7} = 3^2 \cdot 3^{2^3} \cdot 3^{2^4} \cdot 3^{2^6} \cdot 3^{2^7}.$$

Để ý rằng, dễ tính các mũ

$$3\ ,\ 3^2\ ,\ 3^{2^2}\ ,\ 3^{2^3}\ ,\ 3^{2^4}\ ,\ \ldots$$

Ví dụ (tiếp)

Ta lập bảng

i	0	1	2	3	4	5	6	7
$3^{2^i} \pmod{1000}$	3	9	81	561	721	841	281	961

rồi tính

$$\begin{aligned} 3^{218} &= 3^2 \cdot 3^{2^3} \cdot 3^{2^4} \cdot 3^{2^6} \cdot 3^{2^7} \\ &\equiv 9 \cdot 561 \cdot 721 \cdot 281 \cdot 961 \pmod{1000} \\ &\equiv 489 \pmod{1000}. \end{aligned}$$

Thuật toán tính nhanh $a^b \pmod{n}$

MODULAR-EXPONENTIATION(a, b, n)

$c = 0$

$d = 1$

Biểu diễn $b = \langle b_k, b_{k-1}, \ldots, b_0 \rangle_2$

for $i = k$ **downto** 0

$c = 2c$

$d = (d \cdot d) \pmod{n}$

if $b_i == 1$

$c = c + 1$

$d = (d \cdot a) \pmod{n}$

return d

Ví dụ

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
d	7	49	157	526	160	241	298	166	67	1

- Kết quả tính $a^b \pmod{n}$ với

$$a = 7, \quad b = 560 = \langle 1000110000 \rangle, \text{ và } n = 561$$

- Giá trị được chỉ ra sau mỗi bước lặp.
- Kết quả cuối cùng bằng 1

Thuật toán đệ quy tính $a^b \mod n$

```
MODULAR-EXPONENTIATION(a, b, n)
    if  b == 0  then return  1
    if  b == 1  then return  a
    r = MODULAR-EXPONENTIATION(a, b/2, n)
    r = r * r
    if b  mod 2 == 1 then  r = r * a
    return  r
```

Định lý (Định lý Fermat nhỏ)

Xét số nguyên tố p và xét số nguyên a. Khi đó

$$a^{p-1} \equiv \begin{cases} 1 \pmod{p} & \textit{nếu } p \nmid a, \\ 0 \pmod{p} & \textit{nếu } p \mid a. \end{cases}$$

Ví dụ

Số $p = 15485863$ là số nguyên tố, vậy thì

$$2^{15485862} \equiv 1 \pmod{15485863}.$$

Vậy thì, không cần tính toán ta cũng biết rằng

số $2^{15485862} - 1$ *là bội số của* 15485863.

Nhận xét

Định lý Fermat nhỏ và thuật toán tính nhanh lũy thừa cho ta một phương pháp hợp lý để tính nghịch đảo theo modun p. Cụ thể

$$a^{-1} \equiv a^{p-2} \pmod{p}.$$

Thời gian tính toán của phương pháp này tương tự như dùng thuật toán Euclid mở rộng.