Nhập môn số học thuật toán

Trần Vĩnh Đức

HUST

Ngày 23 tháng 3 năm 2023

Tài liệu tham khảo

- J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer-Verlag – Undergraduate Texts in Mathematics, 2nd Ed., 2014.
- T. H. Cormen, C. E. Leiserson, R. L. Rivest, C. Stein. *Introduction to Algorithms*, Third Edition (3rd ed.). The MIT Press. 2009.
- H. H. Khoái, *Nhập môn số học thuật toán*

Nội dung

Ký hiệu

- $\mathbb{N} = \{1, 2, 3, \dots\}$
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Định nghĩa

Xét $a, b \in \mathbb{Z}$. Ta nói

b là ước của a, hay

a chia hết cho b

nếu có một số nguyên c sao cho

$$a = bc.$$

Ta viết $b \mid a$ để chỉ a chia hết cho b. Nếu a không chia hết cho b thì ta viết $b \nmid a$.

Ví dụ

- $847 \mid 485331$ vì $485331 = 847 \cdot 573$.
- $355 \nmid 259943$ vì $259943 =$

Định nghĩa

Xét $a, b \in \mathbb{Z}$. Ta nói

b là ước của a, hay

a chia hết cho b

nếu có một số nguyên c sao cho

$$a = bc.$$

Ta viết $b \mid a$ để chỉ a chia hết cho b. Nếu a không chia hết cho b thì ta viết $b \nmid a$.

Mệnh đề

Xét $a, b, c \in \mathbb{Z}$.

1. *Nếu $a \mid b$ và $b \mid c$, thì $a \mid c$.*
2. *Nếu $a \mid b$ và $b \mid a$, thì $a = \pm b$.*
3. *Nếu $a \mid b$ và $a \mid c$, thì $a \mid (b + c)$ và $a \mid (b - c)$.*

Bài tập

Hãy chứng minh mệnh đề trước.

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

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

Định nghĩa (Chia lấy dư)

Xét a, b là các số nguyên dương. Ta nói a chia cho b có thương là q và phần dư là r nếu

$$a = b \cdot q + r \qquad \text{với} \qquad 0 \le r < b.$$

Bài tập

Hãy chứng minh rằng các số q và r ở trên xác định duy nhất bởi 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.

Một số tính chất của hàm $\gcd$

$$\begin{aligned} \gcd(a, b) &= \gcd(b, a) \\ \gcd(a, b) &= \gcd(-a, b) \\ \gcd(a, 0) &= |a| \\ \gcd(a, ka) &= |a| \qquad \text{với mọi } k \in \mathbb{Z}. \end{aligned}$$

Thuật toán tính $\gcd(a, b)$

- Chia a cho b ta được

$$a = b \cdot q + r \qquad \text{với} \qquad 0 \le r < b.$$

- Áp dụng đẳng thức

$$\gcd(a, b) = \gcd(b, r).$$

Ví dụ: Tính $\gcd(2024, 748)$

$$
\begin{aligned}
2024 &= 748 \cdot 2 + 528 \\
748 &= 528 \cdot 1 + 220 \\
528 &= 220 \cdot 2 + 88 \\
220 &= 88 \cdot 2 + 44 \qquad \leftarrow \qquad \gcd = 44 \\
88 &= 44 \cdot 2 + 0
\end{aligned}
$$

Định lý (Thuật toán Euclid)

Xét a, b là hai số nguyên dương với $a \ge b$. 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*
$$r_{i-1} = r_i \cdot q_i + r_{i+1} \qquad \text{với} \qquad 0 \le r_{i+1} < r_i.$$
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

$$\log_2(b) + 2 \quad \text{lần.}$$

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' − ⌊a/b⌋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	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.
- Lời gọi thủ tục EXTENDED-EUCLID(99,78) trả về $(3, -11, 4)$ thỏa mãn $\gcd(99, 78) = 3 = 99 \cdot (-11) + 78 \cdot 14$.

Bài tập

Hãy tính giá trị

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

Nội dung

Định nghĩa

Xét số nguyên $m \geq 1$. Ta nói hai số nguyên a và b là đồng dư theo modun m nếu $a - b$ chia hết cho m, và viết

$$a \equiv b \pmod{m}$$

Số m được gọi là modun.

Đồng hồ có thể được viết theo như modun dùng modun $m = 12$:

$$6 + 9 = 15 \equiv 3 \pmod{12} \qquad \text{và} \qquad 2 - 3 = -1 \equiv 11 \pmod{12}$$

Mệnh đề

Xét số nguyên $m \geq 1$.

1. *Nếu $a_1 \equiv a_2 \pmod{m}$ và $b_1 \equiv b_2 \pmod{m}$, vậy thì*

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}, \quad \text{và}$$
$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}.$$

Bài tập

- Lấy $m = 5$ và $a = 2$. Rõ ràng $\gcd(2, 5) = 1$, vậy thì tồn tại nghịch đảo của a theo modun 5. Hãy tìm a^{-1}.

Ví dụ

- $17 \equiv 7 \pmod{5}$ vì $10 = 17 - 7$ chia hết cho 5.
- $19 \not\equiv 6 \pmod{11}$ vì $19 - 6 = 13$ không chia hết cho 11

Mệnh đề

Xét số nguyên $m \geq 1$.

1. *Nếu $a_1 \equiv a_2 \pmod{m}$ và $b_1 \equiv b_2 \pmod{m}$, vậy thì*

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}, \quad \text{và}$$
$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}.$$

2. *Xét số nguyên a. Vậy thì tồn tại số nguyên b thỏa mãn*

$$a \cdot b \equiv 1 \pmod{m} \text{ nếu và chỉ nếu } \gcd(a, m) = 1.$$

Nếu tồn tại số b như vậy thì ta nói b là nghịch đảo của a theo modun m.

Bài tập

- Lấy $m = 5$ và $a = 2$. Rõ ràng $\gcd(2,5) = 1$, vậy thì tồn tại nghịch đảo của a theo modun 5. Hãy tìm a^{-1}.
- Tương tự $\gcd(4,15) = 1$. Hãy tìm 4^{-1} theo modun 15.

Định nghĩa

Ta viết

$$\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \ldots, m-1\}$$

và gọi $\mathbb{Z}/m\mathbb{Z}$ là vành số nguyên modun m.

Nhận xét

Khi chúng ta thực hiện phép cộng hoặc nhân trong $\mathbb{Z}/m\mathbb{Z}$ ta luôn chia kết quả cho m và lấy phần dư.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Bảng: Cộng và nhân theo modun 5

Định nghĩa

Ta biết rằng a có nghịch đảo modun m nếu và chỉ nếu $\gcd(a, m) = 1$. Các số khả nghịch gọi là *đơn vị*. Ta ký hiệu tập mọi đơn vị bởi

$$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^* &= \{a \in \mathbb{Z}/m\mathbb{Z} : \gcd(a, m) = 1\} \\ &= \{a \in \mathbb{Z}/m\mathbb{Z} : a \text{ có nghịch đảo theo modun } m\}\end{aligned}$$

Tập $(\mathbb{Z}/m\mathbb{Z})^*$ được gọi là nhóm đơn vị theo modun m.

Ví dụ

Nhóm đơn vị theo modun 24 là

$$(\mathbb{Z}/24\mathbb{Z})^* = \{1, 5, 7, 11, 13, 17, 19, 23\}.$$

Bảng nhân của nhóm này xác định như sau:

$\cdot$	1	5	7	11	13	17	19	23
1	1	5	7	11	13	17	19	23
5	5	1	11	7	17	13	23	19
7	7	11	1	5	19	23	13	17
11	11	7	5	1	23	19	17	13
13	13	17	19	23	1	5	7	11
17	17	13	23	19	5	1	11	7
19	19	23	13	17	7	11	1	5
23	23	19	17	13	11	7	5	1

Ví dụ

Nhóm đơn vị theo modun 7 là

$$(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6\}$$

vì các từ 1 đến 6 đều nguyên tố cùng nhau với 7. Bảng nhân của nhóm này được xác định như dưới đây.

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Định nghĩa

Phi hàm Euler là hàm $\phi(m)$ định nghĩa bởi luật

$$\begin{aligned}\phi(m) &= \#(\mathbb{Z}/m\mathbb{Z})^* \\ &= \#\{0 \le a < m : \gcd(a, m) = 1\}.\end{aligned}$$

Ví dụ

$$\phi(24) = 8 \qquad \text{và} \qquad \phi(7) = 6.$$

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 = ⟨b_k, b_{k-1}, ..., b_0⟩_2
    for  i = k  downto  0
        c = 2c
        d = (d · d) (mod n)
        if  b_i == 1
            c = c + 1
            d = (d · a) (mod n)
    return  d
```


Nội dung

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

Định nghĩa

- Số nguyên tố là số nguyên lớn hơn 1, không chia hết cho số nguyên dương nào ngoài 1 và chính nó.
- Số nguyên lớn hơn 1 không phải số nguyên tố được gọi là hợp số.

Mệnh đề

Xét số nguyên tố p, và giả sử rằng tích ab của hai số a và b chia hết cho p. Vậy thì a hoặc b phải chia hết cho p.
Tổng quát hơn nếu

$$p \mid a_1 a_2 \cdots a_n,$$

vậy thì ít nhất một trong các số a_i phải chia hết cho p.

Định nghĩa

- Số nguyên tố là số nguyên lớn hơn 1, không chia hết cho số nguyên dương nào ngoài 1 và chính nó.

100 số nguyên tố đầu tiên

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541

Bài tập

Hãy chứng minh mệnh đề trước.

Định lý (Định lý cơ bản của số học)

Mọi số nguyên $a \geq 2$ đều phân tích được thành tích các số nguyên tố

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_r^{e_r}.$$

Hơn nữa phân tích này là duy nhất nếu các thừa số được viết với thứ tự không giảm.

Bài tập

Hãy chứng minh định lý trước.

Định nghĩa

- Định lý cơ bản của số học chỉ ra rằng trong phân tích thừa số nguyên tố của số nguyên dương a, mỗi số nguyên tố p xuất hiện với một số mũ nào đó.
- Ta ký hiệu số mũ này là $\mathrm{ord}_p(a)$ và gọi nó là cấp (hoặc số mũ) của p trong a.
- Để cho tiện, ta kí hiệu $\mathrm{ord}_p(1) = 0$ với mọi số nguyên tố p.

Ví dụ

Phân tích của 1728 là

$$1728 = 2^6 \cdot 3^3.$$

Vậy thì

$$\mathrm{ord}_2(1726) = 6, \qquad \mathrm{ord}_3(1726) = 3,$$

và

$$\mathrm{ord}_p(1728) = 0 \text{ với mọi số nguyên tố } p \geq 5.$$

Mệnh đề

Xét số nguyên tố p. Khi đó mọi phần tử a khác 0 của $\mathbb{Z}/p\mathbb{Z}$ đều có nghịch đảo, có nghĩa rằng, tồn tại b để

$$ab \equiv 1 \pmod{p}.$$

Ta ký hiệu giá trị b này bởi $a^{-1} \bmod p$, hoặc đơn giản là a^{-1} nếu p đã xác định.

Mệnh đề này chỉ ra rằng

$$(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, 3, 4, \dots, p-1\}.$$

Bài tập

Hãy chỉ ra thuật toán tính phần tử nghịch đảo a^{-1} của phần tử a trong nhóm $(\mathbb{Z}/p\mathbb{Z})^*$.

Trường hữu hạn $\mathbb{F}_p$

- Nếu p nguyên tố, vậy thì tập $\mathbb{Z}/p\mathbb{Z}$ với phép toán cộng, trừ, nhân và luật chia là một trường.
- Trường $\mathbb{Z}/p\mathbb{Z}$ chỉ có hữu hạn phần tử. Đây là trường hữu hạn và ta ký hiệu $\mathbb{F}_p$.
- Ta viết $(\mathbb{F}_p)^*$ cho nhóm $(\mathbb{Z}/p\mathbb{Z})^*$.
- Trong $\mathbb{F}_p$ người ta thường ký hiệu

$$a = b \text{ thay cho } a \equiv b \pmod{p}.$$

Ví dụ

$1^1 \equiv 1$	$1^2 \equiv 1$	$1^3 \equiv 1$	$1^4 \equiv 1$	$1^5 \equiv 1$	$1^6 \equiv 1$
$2^1 \equiv 2$	$2^2 \equiv 4$	$2^3 \equiv 1$	$2^4 \equiv 2$	$2^5 \equiv 4$	$2^6 \equiv 1$
$3^1 \equiv 3$	$3^2 \equiv 2$	$3^3 \equiv 6$	$3^4 \equiv 4$	$3^5 \equiv 5$	$3^6 \equiv 1$
$4^1 \equiv 4$	$4^2 \equiv 2$	$4^3 \equiv 1$	$4^4 \equiv 4$	$4^5 \equiv 2$	$4^6 \equiv 1$
$5^1 \equiv 5$	$5^2 \equiv 4$	$5^3 \equiv 6$	$5^4 \equiv 2$	$5^5 \equiv 3$	$5^6 \equiv 1$
$6^1 \equiv 6$	$6^2 \equiv 1$	$6^3 \equiv 6$	$6^4 \equiv 1$	$6^5 \equiv 6$	$6^6 \equiv 1$

Bảng: Các lũy thừa theo theo modun 7

Câu hỏi

Tại sao cột bên tay phải toàn nhận giá trị 1?

Nội dung

Định lý (Định lý Fermat nhỏ)

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

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

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.

Định nghĩa

Cấp của phần tử a theo modun p là số mũ $k > 0$ nhỏ nhất thỏa mãn

$$a^k \equiv 1 \pmod{p}.$$

Mệnh đề

Xét số nguyên tố p và xét số nguyên a không chia hết cho p. Giả sử $a^n \equiv 1 \pmod{p}$. Vậy thì n chia hết cho cấp của a theo modun p. Đặc biệt, $p-1$ chia hết cho cấp của a.

Bài tập

Hãy chứng minh mệnh đề trước.

Định lý (Định lý căn nguyên thủy)

Xét số nguyên tố p. Khi đó có tồn tại một phần tử $g \in \mathbb{F}_p^*$ thỏa mãn mọi phần tử của $\mathbb{F}_p^*$ đều là một lũy thừa nào đó của g. Tức là

$$\mathbb{F}_p^* = \{1, g, g^2, g^3, \cdots, g^{p-2}\}.$$

Các phần tử có tính chất này được gọi là căn nguyên thủy của $\mathbb{F}_p$ hoặc phần tử sinh của $\mathbb{F}_p^*$. Chúng là các phần tử của $\mathbb{F}_p^*$ có cấp $p-1$.

Ví dụ

Trường $\mathbb{F}_{11}$ có 2 là một căn nguyên thủy, bởi vì trong $\mathbb{F}_{11}$,

$$\begin{array}{ccccc} 2^0 = 1 & 2^1 = 2 & 2^2 = 4 & 2^3 = 8 & 2^4 = 5 \\ 2^5 = 10 & 2^6 = 9 & 2^7 = 7 & 2^8 = 3 & 2^9 = 6. \end{array}$$

nhưng 2 không phải căn nguyên thủy của $\mathbb{F}_{17}$, bởi vì trong $\mathbb{F}_{17}$

$$\begin{array}{ccccc} 2^0 = 1 & 2^1 = 2 & 2^2 = 4 & 2^3 = 8 & 2^4 = 16 \\ 2^5 = 15 & 2^6 = 13 & 2^7 = 9 & 2^8 = 1 & \end{array}$$

Bài tập

- Hãy tìm một căn nguyên thủy của trường $\mathbb{F}_{17}$.
- Hãy liệt kê tất cả các căn nguyên thủy của $\mathbb{F}_{17}$.