Lý thuyết số

Nguyễn Văn Hiệu
Khoa Công nghệ Thông tin

Nội dung

- Số nguyên tố và hợp số
- Số các ước, tổng và tích của chúng
- Sự phân bố của số nguyên tố
- Các phỏng đoán về số nguyên tố
- Ước số lớn nhất và bội số chung nhỏ nhất
- Đồng dư
- Thuật toán Euclid
- Hàm Euler
- Giải hệ phương trình
  - Phương trình Diophantine
  - Định lý thặng dư Trung hoa

Giới thiệu

Lý thuyết số liên quan đến đến các số, thường là số nguyên và các tính chất của chúng

- Phép chia hết trên các số nguyên
- Phép đồng dư trên các số nguyên

Một số ứng dụng

- Mật mã học
- Tạo số ngẫu nhiên
- Hàm băm
- Lý thuyết mã hóa

Số nguyên tố và hợp số(1)

$$n \in N, n > 1,$$

- n - **nguyên tố**, chỉ chia hết cho 1 và chính nó.
  - Các số nguyên tố: 2, 3, 5, 7, 11, 13, ...
  - Các số không nguyên tố: 4, 6, 8, 10, 12, ...
- n - **hợp số** nếu $n = a.\, b\,, 1 < a < n, 1 < b < n$
  - Các hợp số: 4 = 2.2, 6 = 2.3, 8 = 2.4, 9 = 3.3, 12 = 2.6, …
  - Các số a, b gọi **ước số** của n.
- n - **hợp số**, thì tồn tại ước a, $1 < a \leq \sqrt{n}$
  - $n = a.\, b,\, a \leq b,\, a^2 \leq a.\, b = n.$
- n- **hợp số**, thì tồn tại ước p, p - nguyên tố $p < \sqrt{n}$
  - p - ước nhỏ nhất của n, p = a.b với 1< a< p và 1< b < p => p nguyên tố

Số nguyên tố và hợp số(2)

$$n \in N, n > 1,$$

- n - **hợp số**, thì n có nhiều hơn 2 ước số
  - Số **12** có các ước: 1, 2, 3, 4 6, 12.
- **n - phân tích thành tích hữu hạn của các số nguyên tố**:

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}...p_s^{\alpha_s}, p_1 < p_2 < p_3 ... < p_s, p_i - nt, \alpha_i \in N$$

  - $6 = 2^1.\ 3^1$
  - $84 = 2^2.\ 3^1.7^1$

Số nguyên tố và hợp số(3)

$$n \in N, n > 1,$$

- Làm thế nào để phân tích n thành tích của các số nguyên tố

- Giải pháp:
  - Bắt đầu kiểm tra với n chia cho p (2|n, 3|n, 5|n,....)
  - Nếu tìm thấy p, thì lấy thương m
  - tiếp tục quá trình với m.
- Ví dụ
  - 7007 không chia hết cho 2, 3, 5, mà chia hết cho 7 với thương 1001
  - 1001 không chia hết cho 2, 3, 5, mà chia hết cho 7 với thương 143
  - 143 không chia hết cho 2, 3, 5, 7, mà chia hết cho 11 với thương 13
- Bài tập(15 phút)
  - Viết chương trình nhập vào n và đưa ra danh sách tích của các nguyên tố

Ước số, tổng và tích của chúng(1)

$$n \in N,\ n > 1,$$

- **Số các ước số** của n: $\tau(n) = \prod_{i=1}^{s}(\alpha_i + 1)$

$$84 = 2^2.3^1.7^1$$
$$\tau(84) = (2+1).(1+1).(1+1) = 12$$
$$\tau(84):\ 1, 2, 3, 4, 6, 7,\ 12, 14, 21, 28, 42, 84$$

- **Tổng các ước số** của n:

$$\sigma(n) = \prod_{i=1}^{s}(1 + p_i + \ldots + p_i^{\alpha_i}) = \prod_{i=1}^{s}\left(\frac{p_i^{\alpha_i+1} - 1}{p_i - 1}\right)$$

  - $\sigma(84) = \frac{2^3-1}{2-1}.\frac{3^2-1}{3-1}.\frac{7^2-1}{7-1} = 224$
  - $\sigma(84) = 1 + 2 + 3 + 4 + 6 + 7 + 12 + 14 + 21 + 28 + 42 + 84 = 224$

Ước số, tổng và tích của chúng(2)

$$n \in N,\ n > 1,$$

- **Tích của các ước số** của n: $\mu(n) = n^{\tau(n)/2}$
  - $84 = 2^2.3^1.7^1$
  - $\tau(84) = (2+1).(1+1).(1+1) = 12$
  - $\mu(84) = 84^6 = (1.84).(2.42).(3.28).(4.21).(6.14).(7.12) = 351298031616$
- n- **số hoàn hảo**, nếu $n = \sigma(n) - n$
  - n bằng tổng các ước số của n, ngoài trừ n.
  - $6 = 1 + 2 + 3$
  - $28 = 1 + 2 + 4 + 7 + 14$
- **Bài tập(10 phút)**: Tìm số hoàn hảo từ 1 đến n

Ước số, tổng và tích của chúng (3)

$$n \in N, n > 1,$$

- Bài tập (5 phút): Tìm số tự nhiên n có $\tau(n) = 10$

- Bài tập (5 phút): Tìm số tự nhiên nhỏ nhất có $\tau(n) = 10$

- Bài tập (3 phút): Số 1 có phải là số nguyên tố hay hợp số

Sự phân bố số nguyên tố (1)

$$n \in N, n > 1,$$

- $\pi(n)$ - số nguyên tố không vượt quá n.

- Phương pháp sàng Eratosthenes:
  - Viết các số tự nhiên từ 2 đến n
  - Xóa tất cả các số bội của 2 (trừ 2)
  - Xóa tất cả các số bội của 3 (trừ 3)
  - tiếp tục, cho đến khi xóa hết các hợp số

- **Bài tập**(7 phút): viết chương trình mô phỏng ràng Eratosthenes.
- Hiện nay lập bảng tìm được số nguyên tố với n = 100.000.0000

Sự phân bố số nguyên tố (2)

$$n \in N, n > 1,$$

- Số các nguyên tố của n, tiềm cận tới n/ln n, tức

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1$$

n	$\pi(n)$	$\frac{n}{\ln n}$
1000	168	145
10000	1229	1086
100000	9592	8686
1000000	78498	72382
10000000	664579	620420
100.000.000	5761455	5428681

Các phỏng đoán số nguyên tố(1)

- Fermat cho rằng các số nguyên tố $F(n) = 2^{2^n} + 1$
  - Đúng với n =1,2,3,4
  - Euler chỉ ra sai với n = 5, $F(5) = 2^{2^5} + 1 = \ 641 \ \times \ 6700417$

- Phóng đoán khác: $F(n) = n^2 - n + 41$
  - Đúng với n =1,2,..,40
  - Sai với n = 41, $F(41) = 41^2$

- Phóng đoán khác: $F(n) = n^2 - 79n + 1061$
  - Đúng với n =1,2,..,79
  - Sai với n = 80
- **Công thức tổng quát đang bỏ ngỏ (đợi các em:)**

Phỏng đoán số nguyên tố (2)

$$n \in N, n > 1,$$

- Còn nhiều điều thú vị về số nguyên tố
- **Phỏng đoán Goldbach**: Mọi số nguyên chẵn là tổng của 2 số nguyên tố
- **Phỏng đoán cặp số nguyên tố**. Có vô hạn cặp số nguyên tố (p, p+2)
- **Phỏng đoán của Legendre**: Tồn tại số nguyên tố giữa n^2 , $(n+1)^2$

Ước số chung lớn nhất và bội số chung nhỏ nhất(1)

$$n, m \in Z,\, n \neq 0 \,||\, m \neq 0,$$

- **Ước số chung lớn nhất** của n và m là d-số lớn nhất : $d \,|\, n \,,\, d \,|\, m$

- Ước số chung lớn nhất của gcd(42,72)
  - Các ước của 42: 1, 2, 3, 6, 7, 14, 21.
  - Các ước của 72: 1, 2, 3, 4, 6, 8, 9, 12, 24, 36.
  - gcd(42,72) =6

- Bội số chung nhỏ nhất của n, m là d - số nguyên dương nhỏ nhất:

$$n \,|\, d \,,\, m \,|\, d$$

- **n.m = lcm(m,n).gcd(m,n)**

Ước số chung lớn nhất và bội số chung nhỏ nhất (2)

Tìm ước số chung lớn nhất:

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}\dots p_s^{\alpha_s} \qquad m = p_1^{\beta_1}.p_2^{\beta_2}.p_3^{\beta_2}\dots p_s^{\beta_s}$$

- Ước số chung lớn nhất của n, m:

$$gcd(n,m) = p_1^{\min(\alpha_1,\beta_1)}.p_2^{\min(\alpha_2,\beta_2)}.p_3^{\min(\alpha_3,\beta_3)}\dots p_s^{\min(\alpha_s,\beta_s)}$$

- gcd(42, 72):
  - $72 = 2^3.3^2.7^0$

$$42 = 2^1.3^1.7^1$$

$$\gcd(72,42) = 2.3.1 = 6$$

Ước số chung lớn nhất và bội số chung nhỏ nhất(3)

Tìm bội số chung nhỏ nhất:

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}\dots p_s^{\alpha_s} \qquad m = p_1^{\beta_1}.p_2^{\beta_2}.p_3^{\beta_2}\dots p_s^{\beta_s}$$

- Bội số chung nhỏ nhất của n, m:

$$lcm(n,m) = p_1^{max(\alpha_1,\beta_1)}.p_2^{max(\alpha_2,\beta_2)}.p_3^{max(\alpha_3,\beta_3)}\dots p_s^{max(\alpha_s,\beta_s)}$$

- lcm(42, 72):
  - $72 = 2^3.3^2.7^0$

    $42 = 2^1.3^1.7^1$

    $lcm(72,42) = 2^3.3^2.7^1$

Thuật toán Euclid

- $n, m \in Z, m \neq 0 \implies \exists q, r \in Z, 0 < r < b : n = qm + r$
- $n = mq + r \implies \gcd(n, m) = gcd(m, r)$
    - n và m có chung tập ước số là u: $n = xu, m = yu,$
    - m và r có chung tập được số là u: $r = n - mq = xu - qyu = (x - qy)u$
- gcd(1804,328) = gcd(328, 164) = gcd(164,0) =164.

1804 = 328.5 + 164
328 = 164.2 + 0

- **Bài tập (5 phút):** cài đặt thuật toán Euclid

Thuật toán Euclid

- $$n, m \in Z, m \neq 0:$$
$$\begin{aligned} n &= mq_1 + r_1, \quad 0 < r_1 < m \\ m &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \\ &\dots \\ r_{s-2} &= r_{s-1} q_s + r_s, \quad 0 < r_s < r_{s-1} \\ r_{s-1} &= r_s q_{s+1} + 0, \end{aligned}$$

- $0 < r_s < r_{s-1} < \ldots < r_3 < r_2 < r_1 < m$

$$\implies \gcd(n, m) = r_s$$

- $d = \gcd(n, m) \implies \exists x, y \in Z: n.x + m.y = d$
    - $r_1 = n - q_1 m = \ldots = k_1 n + l_1 m$
      $r_2 = m - q_2 r_1 = \ldots = k_2 n + l_2 m$
      $\ldots \qquad \ldots \qquad \ldots.$
      $r_s = q_s r_{s-1} = \ldots = k_s n + l_s m$

Hàm số Euler $\varphi(n)$

- m, n - **nguyên tố cùng nhau** nếu gcd(m,n)=1
- $\varphi(n)$ số lượng số nguyên tố cùng nhau với n trong phạm vi từ 1 đến n
- $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6$
- $p - nt \implies \varphi(p) = p - 1$

vd: 84=2^2.3^1.7^1
=> phi(n)=84(1-1/2)(1-1/3)(1-1/7)=24

- n - hợp số, $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} \implies$

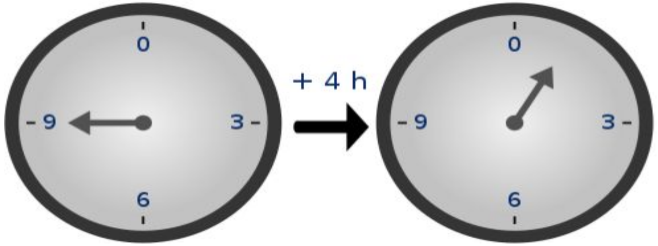
$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right)$$

Số học mô đun
(Modular Arithmetic)

Đồng dư (1)

$$n, a, b \in Z, n > 1$$

- Số a và b gọi **đồng dư theo môđun n** nếu có cùng số dư khi chia cho n (tức a-b chia hết cho n)
- Ký hiệu $a \equiv b\,(mod\, n)$



- Ví dụ $27 \equiv 12(mod\, 5)$ $27 = 12 + k.5$ $k = 3$
  - 27 chia 5 dư 2 và 12 chia 5 cũng dư 2
  - 27 - 12 chia hết cho 5
- Tính chất
  - Phản xạ $a \equiv a(mod\, n)$
  - Đối xứng $a \equiv b\,(mod\, n) \implies b \equiv a\,(mod\, n)$
  - Bắc cầu $a \equiv b\,(mod\, n), b \equiv c\,(mod\, n) \implies a \equiv c\,(mod\, n)$

Đồng dư (2)

Cho: $a \equiv c\,(mod\,n),\, b \equiv d(mod\,n)$

- Tính chất
  - Bảo toàn phép cộng

$$a + b \equiv c + d(mod\,n)$$

  - Bảo toàn phép trừ

$$a - b \equiv c - d(mod\,n)$$

  - Bảo toàn phép nhân

$$a.\,b \equiv c.\,d(mod\,n)$$

  - Bảo toàn phép mũ không âm

$$a^k \equiv c^k(mod\,n)$$

- Bảo toàn với đa thức với p(x) đa thức có các hệ số nguyên

$$p(a) \equiv p(b)(mod\,n)$$

Đồng dư(3)

- $$(a+b) mod\, n = [(a\, mod\, n) + (b\, mod\, n)] mod\, n$$
  $$(a-b) mod\, n = [(a\, mod\, n) - (b\, mod\, n)] mod\, n$$
  $$(a.b) mod\, n = [(a\, mod\, n).(b\, mod\, n)] mod\, n$$
  $$a^m\, mod\, n = (a\, mod\, n)^m\, mod\, n.$$
- Bài tập (7 phút): viết chương trình tính $a^m\, mod\, n$

Đồng dư (4)

- Định lý **Fermat**: p - số nguyên tố, a và p nguyên tố cùng nhau

$$a^{p-1} \equiv 1 (mod\, p)$$

  - Ở đây $a^k \, mod\, p = a^{k\, mod\, p-1} \, mod\, p$

- Định lý **Euler**: n và a nguyên tố cùng nhau

$$a^{\varphi(n)} \equiv 1 (mod\, n)$$

- Định lý Fermat là trường hợp riêng của định lý Euler:

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

Đồng dư (5)

- Minh họa về dấu hiệu chia hết cho 11
  - $z \in Z^+, z = a_n a_{n-1} \ldots a_0 = a_0 + a_1 10^1 + \ldots + a_n 10^n$
  - $t = a_0 - a_1 + a_2 - a_3 + a_4 - \ldots$
  - $z - t = a_1(10^1 + 1) + a_2(10^2 - 1) + a_3(10^3 + 1) + \ldots$
  - $(10^1 + 1) \equiv 0 \, mod \, 11, \ (10^2 - 1) \equiv 0 \, mod \, 11, \ (10^3 + 1) \equiv 0 \, mod \, 11, \ldots$
- $z - t \equiv 0 \, mod \, 11$
- $z \, mod \, 11 = t \, mod \, 11$
- Xem 3162819 chia hết cho 11 hay không

  9 - 1+ 8 - 2 + 6 - 1 + 3 = 22

Đồng dư (6)

- Bài tập 1(7 phút): Tìm dấu hiệu tương tự cho chia hết 7

- Bài tập 2(7 phút): Tìm dấu hiệu tương tự cho chia hết 13

Đồng dư (7)

- Minh họa về dấu hiệu chia hết cho 7
  - $10^0 \equiv 1\, mod\, 7,\ 10^1 \equiv 3\, mod\, 7,\ 10^2 \equiv 2\, mod\, 7,$

    $10^3 \equiv -1\, mod\, 7,\ 10^4 \equiv -3\, mod\, 7,\ 10^5 \equiv -2\, mod\ 7,$

    $10^6 \equiv 1\, mod\, 7,\ 10^7 \equiv 3\, mod\, 7,\ 10^8 \equiv 2\, mod\ 7,$
  - $t = (a_0 + 3a_1 + 2a_2 - 1a_3 - 3a_4 - 2a_5) + (\ldots)..$
- Xem 749 chia hết cho 7 hay không

  9 + 3.4 + 2.7 = 35

Nghịch đảo mô-đun (1)

- $a \in Z, m \in Z^+$

$$a.a^{-1}\,(mod\,m) = 1$$

  - a^{-1}- nghịch đảo mô-đun m của a

- a = 6, m = 17, $a^{-1} = 3$

- a = 2, m = 2, không tồn tại a^{-1}

- a^{-1} tồn tại khi và chỉ khi gcd(a, m) = 1.

Nghịch đảo mô-đun (2)

- Euclid
  - gcd(a, m) = 1, thì luôn tồn tại 2 số nguyên x và y thỏa mãn:

$$a.x + m.y = 1$$

  - $a.x \equiv 1 \,(mod\, m) \implies x = a^{-1}$

- Euler
  - gcd(a,m) =1, theo định lý Euler ta có:

$$a^{\varphi(m)} \equiv 1 (mod\, m)$$

  - Nếu m nguyên tố: $\varphi(m) = m - 1 \implies a^{m-1} \equiv 1 (mod\, m) \implies a^{m-2} \equiv a^{-1} (mod\, m)$
  - Nếu m bất kỳ: $a^{\varphi(m)-1} \equiv a^{-1} (mod\, m)$

Số Pitago và định lý cuối của Fermat

- (3,4,5) $a^2 + b^2 = c^2$

- $$a = (v^2 - u^2).r \quad b = 2uv.r \quad c = (v^2 + u^2).r$$
  $$a = (v^2 - u^2) \quad b = 2uv \quad c = (v^2 + u^2)$$
  $$v = 2,\ u = 1 : (3,4,5)$$
  $$v = 4, u = 3 : (7,24,25)$$
  $$v = 3, u = 2 : (5,12,13)$$
  $$\ldots$$

- (3,4,5)->(6,8,10)->(12,16,20)

- **Định lý cuối cùng của Fermat(chưa cm)**

$$a^n + b^n = c^n$$

Giải phương trình
(Solving equations)

Phương trình Diophantine (1)

- Phương trình Diophantine:

$$a, b, c \in Z : \ ax + by \ = c$$

- **Tìm nghiệm nguyên x và y** ?
  - d = gcd(a,b)
  - Theo Euclid: $\exists k, l \in Z : \ ka + lb \ = d$
- Phương trình có nghiệm khi và chỉ khi **c = q.d**

$$qka + qlb \ = qd \ = c.$$

- Nghiệm của phương trình: $x^{\cdot} = \ qk, \ y^{\cdot} = \ ql.$

- Nghiệm tổng quát: $x = x^{\cdot} \ + \ \frac{rb}{\gcd(a,b)}, \ y = y^{\cdot} \ - \ \frac{ra}{\gcd(a,b)}.$

Phương trình Diophantine(2)

- Ví dụ 1: Tìm nghiệm nguyên của phương trình

$$3\,x + 6y\; = 22$$

  - gcd(3, 6) = 3
  - 3 không phải ước của 22
  - **Phương trình không có nghiệm nguyên**

Phương trình Diophantine(3)

- Ví dụ 2: Tìm nghiệm nguyên của phương trình:

$$7x + 11y = 13$$

a b c

c=q.d
13=13.1

  - gcd(7,11) = 1.
d

$$11 = 1.7 + 4\,,\ 7 = 1.4 + 3,\ 4 = 1.3 + 1$$

$$1 = 4 - 3 = 4 - \underbrace{(7-4)}_{3} = -7 + 2.4 = -7 + 2.\underbrace{(11-7)}_{4} = -3.7 + 2.11$$

11-7=4
7-4=3
4-3=1

$$-3.7 + 2.11 = 1$$

k l

  - Nghiệm riêng: $x^{\cdot} = -39,\ y^{\cdot} = 26$

13.-3 13.2

  - Nghiệm tổng quát ??? $x = -39 + 11r\,,\ y = 26 - 7r$

Định lý thặng dư Trung Hoa(1)

- Hệ phương trình thặng dư

$$\begin{cases} x \equiv a_1 (mod\, m_1) \\ x \equiv a_2 (mod\, m_2) \\ \dots \\ x \equiv a_k (mod\, m_k) \end{cases} \quad \forall i = 1..k, j = 1..k, i \neq j : \gcd(m_i, m_j) = 1.$$

m1, m2,..., mk doi mot nguyen to cung nhau

- Hệ phương thặng dư có nghiệm duy nhất

$$x \equiv (a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_k M_k y_k)(mod\, M)$$

$$M = m_1 . m_2 . \dots . m_k$$

$$M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \dots, M_k = \frac{M}{m_k}$$

$y_i = M_i^{-1}$

$$y_1 \equiv M_1^{-1}(mod\, m_1), y_2 \equiv M_2^{-1}(mod\, m_2), \dots, y_k \equiv M_k^{-1}(mod\, m_k)$$

Định lý thặng dư Trung Hoa(2)

- Ví dụ 2: Giải hệ phương trình thặng dư

$$\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 3(mod\ 5) \\ x \equiv 5(mod\ 7) \end{cases}$$

- Hệ phương thặng dư có nghiệm duy nhất

$$M = 3.5.7 = 105,\ M_1 = 35, M_2 = 21, M_3 = 15$$

$$y_1 \equiv 35^{-1}(mod\ 3) \equiv 2^{-1}(mod\ 3) = 2,$$

$$y_2 \equiv 21^{-1}(mod\ 5) \equiv 1^{-1}(mod\ 5) = 1,$$

$$y_3 \equiv 15^{-1}(mod\ 7) \equiv 1^{-1}(mod\ 7) = 1,$$

$$x \equiv \left(\underbrace{2.35.2}_{140} + \underbrace{3.21.1}_{63} + \underbrace{5.15.1}_{75}\right) mod\ 105 \equiv 278(mod\ 105) \equiv 68(mod\ 105)$$

Tài liệu

- [V. M. P. Deisenroth, et. al., 2020] Mathematics for Machine Learning, Cambridge University Press.
- [E. Lehman, et. al. 2017] Mathematics for Computer Science, Eric Lehman Google Inc.
- [Gerard O’Regan,2016] Guide to Discrete Mathematics, Springer International Publishing Switzerland

Bài tập cần nộp của chương

Bài tập 1: Viết chương trình nhập vào n và đưa ra tích hữu hạn của các nguyên tố.

Bài tập 2: Tìm số hoàn hảo từ 1 đến n.

Bài tập 3 : viết chương trình mô phỏng ràng Eratosthenes. Lập bảng tìm được số nguyên tố với n = 100.000.0000

Bài tập 4: Cài đặt thuật toán Euclid

Bài tập 5: viết chương trình tính $a^m \, mod \, n$

Bài tập 6: Viết chương trình tìm nghiệm cho phương trình Diophantine.

Bài tập 7: Viết chương trình tìm nghiệm cho hệ phương trình thặng dư.

Cám Ơn!