**SỐ HỌC THUẬT TOÁN**

**SỐ NGUYÊN**

Cho , phần nguyên của *x*, ký hiệu [*x*], là số nguyên lớn nhất nhỏ hơn hay bằng *x*.

}.

Ta có

.

Đăt

.

Với , có duy nhất cặp 2 số nguyên sao cho

,

*q* được gọi là thương số (quotient), ký hiệu ; *r* gọi là dư số (remainder), ký hiệu .

Cho .

Nếu có sao cho a = bc, thì a gọi là chia hết cho b, ký hiệu b|a ; và b gọi là ước số (divisor) của a.

Từ các định nghĩa trên, ta có kết quả sau:

Tập tất cả các ước số của là hữu hạn.

Và ta có thể chứng minh định lý sau.

**Định lý**

. a|a.

. a|b và b|c thì a|c.

. a|b và a|c thì a|(bx + cy).

. a|b và b|a thì a = ± b.

**SỐ NGUYÊN TỐ VÀ SỐ NGUYÊN TỐ CÙNG NHAU**

Cho

được gọi là ước số chung (common divisor) của a và b nếu có .

Tập tất cả các ước chung của 2 số nguyên a ≠ 0 và b ≠ 0 là tập hữu hạn.

Cho .

được gọi là ước chung lớn nhất (the greatest common divisor – **GCD**) của a và b, nếu d là một ước của a, b; và nếu c là một ước chung của a, b thì c ≤ d.

Vậy ta có

. , .

. Nếu gcd(a, b) = gcd(b, c) và nếu b là một ước của a thì gcd(a, b) = b.

Từ đó, ta có định nghĩa truy chứng sau:

gcd(ai, 1 < i ≤ k) ≡ gcd(a1, …, ak) = gcd(gcd(a1, …, ak-1), ak), ∀k ≥ 3.

Từ khái niệm ước số, ước chung, ta định nghĩa khái niệm bội chung và bội chung nhỏ nhất.

. . Số nguyên được gọi là bội chung (common multiple) của a và b nếu a|c và b|c.

. . Số nguyên được gọi là bội chung nhỏn nhất (the least commont multiple – **LCM**) của a và b nếu d là một bội chung của a, b, ký hiệu d = lcm(a, b), và nếu có bội chung d’ của a và b thì d’ ≥ d = lcm(a, b).

Một cách hình thức, ta viết

. .

. .

Quan hệ giữa ước chung lớn nhất và bội chung nhỏ nhất được thể hiện quả định lý sau.

**Định lý**. Cho , ta có .

Cho .

. a, b được gọi là nguyên tố cùng nhau (co-prime) nếu gcd(a, b) = 1.

. được gọi là số nguyên tố nếu gcd(d, a) = 1, ∀d = 2, …, a – 1, và a > 1.

Tập các số nguyên tố, ký hiệu P. Ta có

∀p ∈ P, p chỉ có 2 ước số là 1 và chính nó: 1|p và p|p.

Ta dễ dàng chứng minh định lý sau.

**Định lý**

. Nếu p ∈ P và không phải bội số của p, thì a nguyên tố cùng nhau với p, gcd(a, p) = 1.

. Hai số nguyên tố khác nhau thì nguyên tố cùng nhau.

**THUẬT TOÁN EUCLIDE**

**Định lý** (Euclide).

Cho . Đặt r-1 = a, r0 = b, ta có

,

với là số nguyên nhỏ nhất sao cho ,

và gcd(a, b) = rN.

Bezout, sau đó mở rộng định lý Euclide, gọi là Euclide mở rộng (Extended Euclide).

**Định lý** (Bezout).

Cho , và

;

;

.

Và ta có

;

.

Từ định lý Bezout, ta có định lý đảo.

. Giả sử có , thì mỗi ước chung d ≥ 1 của a, b đều là ước của 1. Vậy d = 1 hay gcd(a, b) = 1.

**ĐỒNG DƯ**

Cho , ta định nghĩa quan hệ đồng dư, ký hiệu ≡ (mod n), như sau:

a ≡ b (mod n) ⇔ a mod n = b.

Ta có

. a ≡ a (mod n).

. a ≡ b (mod n) ⇒ b ≡ a (mod n).

. a ≡ b (mod n) và b ≡ c (mod n) ⇒ a ≡ c (mod n).

. a ≡ b (mod n), c ≡ d (mod n) ⇒ a ± c ≡ b ± d (mod n).

. a ≡ b (mod n), c ≡ d (mod n) ⇒ ac ≡ bd (mod n).

. a ≡ b (mod n) ⇒ am ≡ bm (mod n).

Như vậy, quan hệ ≡ (mod n) là quan hệ tương đương (equivalence relation) và n gọi là mô-đun (modulus) của quan hệ này.

Với , tập các số nguyên mod n là tập các lớp tương đương (equivalence class), ký hiệu

.

Ta có thể chứng minh kết quả sau:

, ta có

. ad ≡ bd (mod n) ⇔ a ≡ b (mod n).

. ad ≡ 0 (mod n) ⇔ a ≡ 0 (mod n).

Và mở rộng định lý Bezout thành

Cho k ≥ 2 số nguyên dương đôi một nguyên tố cùng nhau a1, …, ak, tồn tai k số nguyên c1, …, ck sao cho: .

**ĐỊNH LÝ CƠ BẢN CỦA SỐ HỌC**

Với mọi số nguyên dương n ≥ 2, n có thể phân tích thành tích các ước nguyên tố nhỏ hơn nó:

.

Phân tích này là duy nhất.

Bây giờ,

Xét 3 số nguyên dương m, n, k ≥ 2, và các phân tích của nó

, ta có

. k = mn ⇔ kp = mp + np, ∀p ∈ P.

. m|n ⇔ mp ≤ np, ∀p ∈ P.

. k = gcd(m, n) ⇔ kp = min(mp, np), ∀p ∈ P.

. M = gcd(mi, i = 1,…, k) ⇔ Mp = min{(mi)p, i = 1, …, k}, ∀p ∈ P.

. k = lcm(m, n) ⇔ kp = max(mp, np), ∀p ∈ P.

. M = lcm(mi, i = 1, …, k) ⇔ Mp = max{(mi)p, i = 1, …, k},∀p ∈ P.

. gcd(m, n) = 1 ⇔ mpnp = 0, ∀p ∈ P.

. gcd(k, m) = 1 và gcd(k, n) = 1 ⇔ gcd(k, mn) = 1.

. gcd(km, kn) = k\*gcd(m. n).

. lcm(km, kn) = k\*lcm(m, n).

. d = gcd(m, n), m’ = m div d, n’ = n div d ⇒ gcd(m’, n’) = 1.

**PHƯƠNG TRÌNH DIOPHAN TUYẾN TÍNH VÀ PHƯƠNG TRÌNH ĐỒNG DƯ**

**Phương trình Diophant**

Cho , và phương trình Diophant tuyến tính .

. Nếu d không phải ước của c thì phương trình Diophant không có nghiệm.

. Nếu d là ước của c và ax0 + by0 = c thì nghiệm tổng quát của phương trình Diophant có dạng .

**Phương trình đồng dư**

Phương trình đồng dư

,

tương đương với phương trình Diophant

.

Ta tóm lược bằng định lý sau.

**Định lý**.

. Nếu d không phải ước của b, phương trình đồng dư không có nghiệm.

. Nếu d là ước của b, phương trình đông dư có nghiệm x = x1 + m’n, 0 ≤ n ≤ d – 1, với m’ = m div d.

. Nếu d = 1, phương trình đồng dư chỉ có 1 nghiệm duy nhất x = x1 = sb.