Số học 4.5 - Nghịch đảo modulo

Số học 4.5 - Nghịch đảo modulo

Nguồn: e-maxx

Người dịch: Nguyễn Thành Trung (RR)

Định nghĩa:

Xét số nguyên dương m. Xét các số nguyên trên modulo m (từ 0 đến $m-1$).

Với một số nguyên a, ta gọi nghịch đảo modulo m (modular multiplicative inverse) của a là a^{-1} là số nguyên thoả mãn:

$$a \cdot a^{-1} \equiv 1 \pmod m$$

Ta cần chú ý rằng không phải lúc nào a^{-1} cũng tồn tại. Ví dụ, với $m = 4, a = 2$, ta không thể tìm được a^{-1} thoả mãn đẳng thức trên.

Có thể chứng minh rằng a^{-1} luôn luôn tồn tại nếu $gcd(a, m) = 1$.

Trong bài viết này, mình sẽ trình bày 2 cách khác nhau để tìm nghịch đảo modulo, dựa trên các kiến thức đã được trình bày ở các bài viết trên VNOI:

- Extended Euclid
- Tính a^b % c bằng chia để trị
- Phi hàm Euler

Extended Euclid

Như đã trình bày trong bài viết Số học 1, nếu $gcd(a, m) = 1$, ta luôn luôn tìm được 2 số nguyên x và y thoả mãn:

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

Vì ta đang làm việc trên modulo m, ta có thể bỏ $m*y$ và viết lại đẳng thức trên như sau:

$$a*x \equiv 1 \pmod m.$$

Do đó, x chính là a^{-1}.

Cài đặt:

```
int x, y;
int g = extended_euclidean(a, m, x, y);
if (g != 1) cout << "No solution!";
else {
    x = (x % m + m) % m;
    cout << x << endl;
}
```

Tính nghịch đảo modulo bằng a^b % c

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

$$a^{phi(m)} \equiv 1 \pmod m.$$

Với Phi hàm Euler đã được giải thích ở bài viết Số học 4.

Trong trường hợp m là số nguyên tố, $phi(m) = m - 1$, nên ta có:

$$a^{m-1} \equiv 1 \pmod m.$$

Nhân cả 2 vế với a^{-1}, ta được:

- Với m bất kỳ, $a^{phi(m)-1} \equiv a^{-1} \pmod m$,
- Với m nguyên tố, $a^{m-2} \equiv a^{-1} \pmod m$.

Như vậy, ta có thể dùng thuật toán Tính a^b % c bằng chia để trị để tính nghịch đảo modulo với độ phức tạp $O(\log m)$.

Tính tất cả nghịch đảo modulo m

Trong trường hợp m là số nguyên tố, ta cũng có thể tính tất cả nghịch đảo modulo của toàn bộ $[1, m - 1]$ với độ phức tạp $O(m)$ như sau:

```
r[1] = 1;
for(int i = 2; i < m; ++i)
    r[i] = (m - (m/i) * r[m%i] % m) % m;
```

Chứng minh:

$$m\%i = m - floor(m/i) * i$$

$$m\%i \equiv -floor(m/i) * i \pmod m$$

Nhân cả 2 vế với nghịch đảo modulo của i và nghịch đảo modulo của $m\%i$:

$$r[i] \equiv -floor(m/i) * r[m\%i] \pmod m$$

Các bài luyện tập

- UVa 11904 - One Unit Machine
- Hackerrank - Longest Increasing Subsequence Arrays
- Codeforces 300C - Beautiful Numbers
- Codeforces 622F - The Sum of the k-th Powers
- Codeforces 717A - Festival Organization