Số học 3 - Tính (a^b) % c

Số học 3 - Tính (a^b) % c

Nguồn: HackerEarth và 1 số bài viết trên Wikipedia

Người dịch: Bùi Việt Dũng

Xét bài toán tính $a^b \% c$, với $\%$ là dấu đồng dư thức và b có thể rất lớn (ví dụ $b \leq 10^{18}$).

Thuật toán "ngây thơ"

a^b có thể viết là $a.a.a.a...$ với b chữ a. Do đó ta có thể nhân b lần a để có được kết quả.

```
long long power(long long a, long long b, long long c) {
    long long ans = 1;
    for(int i = 1; i <= b; i++) {
        ans *= a;
        ans %= c;
    }
    return ans;
 }
```

Trong mỗi lần lặp, biến ans chứa kết quả được nhân với a. Ngoài ra, ta cần đảm bảo a sẽ không vượt quá c trong các lần lặp, vì thế ta lấy phần dư khi chia ans cho c (`ans = ans % c`). Ta làm được vậy là nhờ tính chất $(x.y)\%n = ((x\%n).(y\%n))\%n$.

Vì vậy trong code trên ta tính $(ans.a)\%c$ bằng cách tính $((ans\%c).(a\%c))\%c$.

Độ phức tạp của thuật toán: $O(b)$.

Thuật toán "chia để trị"

Dễ dàng nhận thấy thuật toán trên không hiệu quả, vì thế ta cần tìm thuật toán hiệu quả hơn. Ta có thể giải bài toán này với độ phức tạp $O(\log_2 b)$ bằng kĩ thuật **lũy thừa bằng cách bình phương (exponentiation by squaring)**. Kĩ thuật này chỉ cần $O(\log_2 b)$ lần bình phương và $O(\log_2 b)$ phép nhân để ra kết quả. Rõ ràng cách giải này hiệu quả hơn nhiều lần so với thuật toán "ngây thơ".

Ta biết rằng a^b có thể được viết dưới dạng:

$a^b = (a^{\frac{b}{2}})^2$ nếu b chia hết cho 2.

$a^b = a.(a^{[\frac{b}{2}]})^2$ nếu b không chia hết cho 2.

$a^b = 1$ nếu $b = 0$.

```
int sqr(int x) {
    return x*x;
}

int pow(int a, int b, int MOD) {
    if (b == 0) return 1 % MOD;
    else
        if (b % 2 == 0)
            return sqr(pow(a, b/2)) % MOD;
        else
            return a * (sqr(pow(a, b/2)) % MOD) % MOD;
}
```

Giả sử ta có $a = 2, b = 5, c = 5$, khi đó kết quả là $pow(2, 5, 5)$

1. Do b lẻ, nên hàm $pow(2, 5, 5)$ gọi hàm $pow(2, 2, 5)$ để tính $2.pow(2, 2, 5)$
2. Trong hàm $pow(2, 2, 5)$, do $b = 2$ chẵn nên $pow(2, 2, 5) = pow(2, 1, 5)^2$
3. Trong hàm $pow(2, 1, 5)$, do $b = 1$ lẻ nên $pow(2, 1, 5) = 2 * pow(2, 0, 5)$.
4. Trong hàm $pow(2, 0, 5)$, do $b = 0$ nên ta trả về 1.
5. Quay lại hàm $pow(2, 1, 5)$: hàm này trả về giá trị 2.
6. Quay lại hàm $pow(2, 2, 5)$: hàm này trả về giá trị 4.
7. Quay lại hàm $pow(2, 5, 5)$: hàm này trả về giá trị $(2.4^2)\%5 = 32\%5 = 2$.

Vậy ta có $2^5\%5 = 2$.

Độ phức tạp của thuật toán: $O(\log_2 b)$