

ĐỒNG DƯ THỨC:

THUẬT TOÁN LŨY THỪA NHỊ PHÂN – TÍNH DƯ CỦA LŨY THỪA

Tác giả: Phan Thành Hưng (PTNK, ĐHQG TP. HCM)

I. Giới thiệu

Cho bài toán sau:

“Tính giá trị biểu thức sau:

$$A^B \bmod M$$

hay tính phần dư của A^B khi chia cho M .”

II. Thuật toán

Thông thường, chúng ta có thể sử dụng định lý Fermat nhỏ, định lý Euler để thu nhỏ số mũ lại. Tuy nhiên, chúng đều phải dựa trên một số trường hợp cụ thể (ví dụ như định lý Fermat nhỏ chỉ dùng được với m là số nguyên tố, còn định lý Euler thì chỉ dùng được khi $\text{UCLN}(a, m) = 1$). Ngoài ra, nếu ta tìm cách tách số mũ ra thành tích nhiều số mũ nhỏ hơn, xong tính lũy thừa của a cho từng số một rồi nhân lại lấy dư thì sẽ rất tốn thời gian và dễ bị lộn dẫn tới kết quả sai. Ta muốn một cách làm vừa nhanh, vừa chính xác.

Trước khi bước vào thuật toán, ta cần tìm cách tìm ra một biểu thức tính dư của A khi chia cho M . Không khó để nhận ra biểu thức đó là:

$$A - M \times \text{Int}\left(\frac{A}{M}\right)$$

Trong đó, $\text{Int}\left(\frac{A}{M}\right)$ thực chất chính là phần nguyên của thương phép chia A cho M , và ta nhân nó lên M lần để tìm bội của M bé hơn A mà gần A nhất. Phần dư sẽ chính là hiệu giữa A và bội đó.

1. Thuật toán ngây thơ

Đối với một thuật toán thông thường, ta sẽ nhân A lên B lần, mỗi lần nhân lên như vậy ta lấy dư cho M ngay lập tức. Để làm như vậy, trước hết, ta khởi tạo biến D là biến lưu kết quả, rồi từ từ nhân B lần số A vào biến đó. Do ta chưa nhân lần nào hết nên giá trị khởi tạo của D là $A^0 = 1$.

Nhập vào máy tính như sau: $D = \frac{0ABMD}{B} + D \times A : D = D - M \times \text{Int}\left(\frac{D}{M}\right) : B = B - 1$

Với dữ liệu khởi tạo ban đầu là:

$$A = \text{cơ số}; B = \text{số mũ}; M = \text{phần dư}; D = 1$$

Sau khi nhập vào, ta bấm đầu bằng ($\equiv$) liên tục cho tới khi gặp lỗi **“Lỗi phép tính” (Math ERROR)** trong máy Casio thì dừng lại và thoát ra (nghĩa là lúc này B có giá trị là 0 và ta vừa lặp xong B lần phép nhân A với nhau). Kết quả sẽ nằm trong biến D .

Phân tích độ hiệu quả: Mỗi lần thực hiện đa câu lệnh thì ta đặt $B = B - 1$ và dừng lại khi $B = 0$ nên ta mất B lần thực hiện đa câu lệnh. Vậy ta cần thực hiện đa câu lệnh B lần để giải bài toán này. Nếu như đề bài cho B là một số rất lớn, ví dụ $5^{100000000}$ thì rõ ràng ta không thể dùng cách này được do sẽ phải bấm máy thực hiện tới 100000000 lần đa câu lệnh, có thể là bấm tới sáng hôm sau cũng chưa xong nữa ;))) $\Rightarrow$ ta cần tìm một thuật toán hiệu quả hơn.

2. Thuật toán tối ưu

Ta có một nhận xét sau:

$$A^B = \begin{cases} (A^2)^{B/2}, & \text{nếu } B \text{ là số chẵn} \\ A^{B-1} \times A, & \text{nếu } B \text{ là số lẻ} \end{cases}$$

Với trường hợp B là số lẻ, ta nhận thấy $A^B = A^{B-1} \times A$, mà $B - 1$ là số chẵn nên ta quay trở lại trường hợp số chẵn trên với A^{B-1} , nghĩa là nếu B là số lẻ thì

$$A^B = (A^2)^{(B-1)/2} \times A$$

Vậy ta có:

$$A^B = \begin{cases} (A^2)^{B/2}, & \text{nếu } B \text{ là số chẵn} \\ (A^2)^{(B-1)/2} \times A, & \text{nếu } B \text{ là số lẻ} \end{cases}$$

Ta có thể rút gọn thêm bằng nhận xét là với B là số lẻ thì: $\frac{B-1}{2} = \text{Int}\left(\frac{B}{2}\right)$,

còn nếu B là số chẵn thì: $\frac{B}{2} = \text{Int}\left(\frac{B}{2}\right)$

Do đó, ta rút gọn lại được thành:

$$A^B = \begin{cases} (A^2)^{\text{Int}\left(\frac{B}{2}\right)}, & \text{nếu } B \text{ là số chẵn} \\ (A^2)^{\text{Int}\left(\frac{B}{2}\right)} \times A, & \text{nếu } B \text{ là số lẻ} \end{cases} \quad (1)$$

Từ (1), ta viết ra được một thuật toán như sau:

Đặt $D = 1$
 Lập đa câu lệnh cho tới khi $B = 0$:
 – Nếu B là số lẻ thì gán $D \leftarrow D \times A \bmod M$
 – Gán $A \leftarrow A^2 \bmod M$
 – Gán $B \leftarrow \text{Int}\left(\frac{B}{2}\right)$

Trong thuật toán trên, ban đầu ta gán $D \rightarrow A^0 = 1$. Sau đó lặp lại tới khi $B = 0$ và trong mỗi lần lặp đa câu lệnh:

- Nếu B là số lẻ, nghĩa là rơi vào trường hợp $(A^2)^{\text{Int}(\frac{B}{2})} \times A$, ta nhân biến D cho A . Vậy sau khi nhân A thì phần còn lại là $(A^2)^{\text{Int}(\frac{B}{2})}$, y hệt trường hợp B là số chẵn.
- Lúc này, bài toán con của chúng ta là tính $(A^2)^{\text{Int}(\frac{B}{2})}$, ta sẽ thực hiện giống như cách ta thực hiện với A^B thôi. Do vậy ta gán $A \leftarrow A^2$ và $B \leftarrow \text{Int}\left(\frac{B}{2}\right)$ và quy về bài toán mới. Trong lúc thực hiện gán giá trị cho A và D ta liên tục chia lấy dư cho M .

Tuy nhiên, có một vấn đề là trong máy Casio, ta không thể tự tiện sử dụng thuật ngữ “nếu” được, đơn giản là vì máy tính Casio không hiểu “nếu” là cái gì ;o;. Vậy làm sao để nó biết khi nào B là số lẻ để mà cho D nhân với A đây?

Ta dựng một hàm $f(x)$ như sau:

$$f(x) = \begin{cases} 1, & \text{nếu } x = 0 \\ A, & \text{nếu } x = 1 \end{cases}$$

Gọi r là phần dư của B khi chia cho 2. Vậy nếu B là số chẵn thì $f(r) = f(0) = 1$, còn nếu B là số lẻ thì $f(r) = f(1) = A$. Dẫn tới việc ta chỉ cần gán $D \leftarrow D \times f(r)$ là được (nếu B chẵn thì $D \leftarrow D \times 1$, B lẻ thì $D \leftarrow D \times A$).

Vậy ta tạo hàm $f(x)$ như nào? Nhận thấy $x = 0$ thì $f(x) = 1$ và $x = 1$ thì $f(x) = A$ nên ta dễ dàng dựng được $f(x) = A^x$ sẽ thỏa mãn điều kiện ta cần. Do đó ta chỉ cần gán $D \leftarrow D \times A^r = D \times A^{B-2 \times \text{Int}(\frac{B}{2})}$. Vậy biểu thức tương đương với “nếu B lẻ thì $D \leftarrow D \times A$ ” là

$$D = D \times A^{B-2 \times \text{Int}(\frac{B}{2})}$$

Để cài đặt vào máy tính Casio, ta sẽ làm như sau:

$$D = \frac{0ABMD}{B} + D \times A^{B-2 \times \text{Int}(\frac{B}{2})} : D = D - M \times \text{Int}\left(\frac{D}{M}\right) : A = A^2 - M \times \text{Int}\left(\frac{A^2}{M}\right) : B = \text{Int}\left(\frac{B}{2}\right)$$

Bấm CALC, với dữ liệu khởi tạo ban đầu là:

$$A = \text{cơ số}; B = \text{số mũ}; M = \text{số chia dư}; D = 1$$

Sau khi nhập vào, ta bấm đầu bằng ($\square$) liên tục cho tới khi gặp lỗi “**Lỗi phép tính**” (**Math ERROR**) trong máy Casio thì dừng lại và thoát ra (nghĩa là lúc này B có giá trị là 0 và ta vừa lặp xong). Kết quả sẽ nằm trong biến D .

Dĩ nhiên là có thể dừng ngay khi thấy $B = 0$, không nhất thiết phải chờ Math ERROR (việc mình cố tình gây Math Error để khiến cho việc dừng đơn giản hơn).

Phân tích độ hiệu quả: Mỗi lần thực hiện đa câu lệnh thì ta đặt $B = \text{Int}\left(\frac{B}{2}\right)$ và dừng lại khi $B = 0$ nên ta mất khoảng $\approx \log_2 B$ lần thực hiện đa câu lệnh. Vậy ta cần thực hiện đa câu lệnh $\approx \log_2 B$ lần để giải bài toán này. Nếu như đề bài cho B là một số rất lớn, ví dụ $5^{100000000}$ thì ta chỉ phải bấm máy thực hiện $\approx \log_2 100000000 \approx 27$ lần đa câu lệnh, hoàn toàn có thể bấm được trong thời gian ngắn. Với $B = 10^{18}$ (1 tỉ tỉ) thì thuật toán trên chỉ mất khoảng 60 lần thực hiện đa câu lệnh!

BẢNG SO SÁNH SỐ LẦN LẬP CỦA 2 THUẬT TOÁN		
B	Số lần lặp (thuật ngây thơ)	Số lần lặp (thuật tối ưu)
10	10	≈ 3
100	100	≈ 7
10000	10000	≈ 14
100000	100000	≈ 17
10^9 (1 tỉ)	10^9	≈ 30
10^{12} (1 nghìn tỉ)	10^{12}	≈ 40

Có thể thấy, số lần lặp của thuật toán tối ưu ít hơn rất rất rất rất nhiều lần so với số lần lặp của thuật toán ngây thơ.

Điều kiện hoạt động: Do máy tính Casio chỉ lưu kết quả chính xác được tới $10^{15} - 1$, mà trong thuật toán của ta cần phải tính A^2 và $D \times A$ xong lấy dư cho M nên $A \in [0; M - 1]$. Do đó, để thuật toán chạy chính xác thì ta cần đảm bảo mọi phép tính trung gian không trả ra giá trị lớn hơn $10^{15} - 1$, nghĩa là $M \leq \sqrt{10^{15} - 1} \approx 31622776$.

TÓM TẮT THUẬT TOÁN:

$$D = \frac{0ABMD}{B} + D \times A^{B-2 \times \text{Int}\left(\frac{B}{2}\right)} : D = D - M \times \text{Int}\left(\frac{D}{M}\right) : A = A^2 - M \times \text{Int}\left(\frac{A^2}{M}\right) : B = \text{Int}\left(\frac{B}{2}\right)$$

Với dữ liệu khởi tạo ban đầu là:

$$A = \text{cơ số}; B = \text{số mũ}; M = \text{số chia dư}; D = 1$$

Điều kiện ràng buộc: $M \leq 31622776$.

Sau khi nhập vào, ta bấm đầu bằng ($\square$) liên tục cho tới khi gặp lỗi “**Lỗi phép tính**” (**Math ERROR**) thì dừng lại và thoát ra. Kết quả sẽ nằm trong biến D .