$a^b \bmod m$

Nhiều cách làm:

- Định lý Fermat nhỏ
- Định lý Euler
- Tách b thành tích nhiều số nhỏ hơn
  xử lý từng cái xong nhân lại

$15^{300} \bmod 18$

$$15^{\underline{300}} = (\underbrace{15^5})^{\underline{60}} \equiv 9^{60} \pmod{18}$$

$$= (9^6)^{10} \equiv \boxed{9^{10}} \pmod{18}$$

$$= (9^5)^2 \equiv 9^2 \ (m18)$$

$$\equiv \underline{9} \ (m18)$$

$$\underline{15^{300}} \text{ mod } \underline{16}$$

$$15^{300} \equiv (-1)^{300} \ (m16)$$

$$\equiv 1 \ (m16)$$

Thuật toán:

$$a^b \ \underline{\text{mod } m}$$

$$\underset{\substack{\uparrow \\ D}}{1} \times \underbrace{a \times a \times \dots \times a}_{b \text{ lần}}$$

Quy trình:

Lặp lại b lần, mỗi lần ta lại nhân a vào kết quả và lấy dư cho m luôn

VD:

$\underline{15^3}$ mod 18

D là biến lưu kết quả: $D = 1$

→ Lặp lại 3 lần:

- Lần 1:

$$D \leftarrow (\underbrace{\overset{1}{D} \times 15}_{15}) \text{ mod } 18$$

$\rightarrow D = 15$

- Lần 2

$$D \leftarrow (\underbrace{\overset{15}{D} \times 15}_{225}) \text{ mod } 18$$

$\rightarrow D = 9$

- Lần 3:

$$D \leftarrow (\underbrace{\overset{9}{D} \times 15}_{135}) \text{ mod } 18$$

$\rightarrow \boxed{D = 9}$

$1 \times 15 \times 15 \times 15 = 15^3$

$D = 9 \Rightarrow$ kết quả

$a \bmod b = a - \underbrace{\text{Int}\left(\frac{a}{b}\right)} \times b$

CÀI ĐẶT VÀO MÁY CASIO:

$\frac{0}{B} + D \times A : \ldots$

$D = \boxed{D \times A} : D - M \times \text{Int}\left(\frac{D}{M}\right) : B = B - 1$

$\frac{0}{B}$ ⟨ Nếu $B \neq 0 \Rightarrow 0$

Nếu $B = 0 \Rightarrow \frac{0}{0}$?? → MATH Error

Kết quả nằm trong D.

$D = 1$; $A = a$; $B = b$; $M = m$

Số vòng lặp cần chạy : b

$15^{300 \leftarrow b}$

$b = 300$ vòng lặp

↪ QUÁ CHẬM

Thuật toán Lũy thừa nhị phân

Xét:

a^b

Nếu b chẵn

$$a^b = (a^2)^{b/2}$$

Nếu b lẻ

$$a^b = a^{\overset{\text{chẵn}}{b-1}} \cdot a = (a^2)^{\frac{b-1}{2}} \cdot a$$

$$a^b = \begin{cases} (a^2)^{b/2}, & \text{nếu } b \text{ chẵn} \\ (a^2)^{\frac{b-1}{2}} \cdot a, & \text{nếu } b \text{ lẻ} \end{cases}$$

Nếu b lẻ : nhân a vào kq luôn

Ta có:

nguyên ↓

- Nếu b chẵn: $\frac{b}{2} = \text{Int}\left(\frac{b}{2}\right)$

$$\Updownarrow$$

- Nếu b lẻ: $\frac{b-1}{2} = \text{Int}\left(\frac{b}{2}\right)$

$$b = 2k+1$$

$$\begin{cases} \frac{b-1}{2} = \frac{2k+1-1}{2} = \frac{2k}{2} = k \\ \text{Int}\left(\frac{B}{2}\right) = \text{Int}\left(\frac{2k+1}{2}\right) = \text{Int}\left(\frac{2k}{2} + \frac{1}{2}\right) \end{cases}$$

$$= \text{Int}(k + 0{,}5)$$

$$= \text{Int}(k{,}5)$$

$$= k$$

$$\Rightarrow \frac{b-1}{2} = \text{Int}\left(\frac{b}{2}\right)$$

$$\Rightarrow a^b = \begin{cases} \boxed{(a^2)^{\text{Int}\left(\frac{b}{2}\right)}} & \text{, nếu b chẵn} \\ (a^2)^{\text{Int}\left(\frac{b}{2}\right)} \cdot a & \text{, nếu b lẻ} \end{cases}$$

Quy trình:

```
D = 1
lặp lại cho tới khi B = 0
    nếu B lẻ: D ← D × A
    A ← A^2
    B ← Int(B/2)
```

Nếu B lẻ

$D \leftarrow D \times A$

Nếu B chẵn

$D \leftarrow D \times 1$

Tạo g(x) sao cho

nếu x lẻ: $g(x) = x$

nếu x chẵn: $g(x) = 1$

$$\boxed{D = D \times \underbrace{g(B)}}$$

Nếu B lẻ → $g(A) = A$ → $D \times A$

Nếu B chẵn → $g(A) = 1$ → $D \times 1$

How to tạo hàm $g(x)$

$A^{\textcircled{1}} = A$

$A^{\textcircled{0}} = 1$

A lẻ → dư $\textcircled{1}$ khi chia 2

chẵn → dư $\textcircled{0}$

$g(x) = x^{\text{dư của } x \text{ khi chia } 2}$

nếu x lẻ thì → $x^1 = x$

chẵn → $x^0 = 1$

$x - 2\mathrm{Int}\left(\frac{x}{2}\right)$

$\Rightarrow g(x) = x^{x - 2\mathrm{Int}\left(\frac{x}{2}\right)}$

$\rightarrow D \leftarrow D \times A^{B - 2\mathrm{Int}\left(\frac{B}{2}\right)}$

CÀI ĐẶT

$D = \boxed{D \times A^{B-2\mathrm{Int}\left(\frac{B}{2}\right)}} : A = A^2 - M\mathrm{Int}\left(\frac{A^2}{M}\right) : \underline{B = \mathrm{Int}\left(\frac{B}{2}\right)}$

$\frac{0}{B} + \dots$

Λ

$\underline{D - M\mathrm{Int}\left(\frac{D}{M}\right)}$

Gán $D = 1$; $A = a$; $B = b$; $M = m$

Thực hiện tới khi báo lỗi MATH Error

Kq nằm trong biến D.

Bao nhiêu vòng lặp

$\frac{\frac{\frac{B}{2}}{2}}{2}\dots$ mất bnhiêu lần chia

$\approx \log_2 B$ lần

Với B lớn tới 10^{13} thì mất

$\log_2 B \approx \underline{43}$ vòng lặp

Tính :

15^{300} mất ≈ $\log_2 300 \approx 8$ lần lặp

VD cách hoạt đ

$15^{300} \bmod 18$ | D = 1

$15^{300} = (15^2)^{150}$ ~~$\equiv 9^{150}$~~

→ 9^{150} | D = 1

$9^{150} = (9^2)^{75}$ ~~$\neq ((9^2)^{74}).9$~~

→ 9^{75} | D = 1

$9^{75} = 9^{74} . 9 = \boxed{(9^2)^{37}} . 9$

$(9)^{37}$ | D = 9

$9^{37} = 9^{36} . 9 = (9^2)^{18} . 9$

9^{18} | D = 9

$9^{18} = (9^2)^{9}$

$= 9^{9}$

⋮

$9^1 = 9^0 . 9 = (9^2)^0 . 9$

$(9^2)^{\boxed{0}}$ | D = $9 \times 9 = 9 \pmod{18}$

$= 9^0$ ← b = 0

$15^{300} = 9$