Định lý Wilson

Định lý Wilson

Nguồn: hackerearth

Định lý

Số tự nhiên $n > 1$ là số nguyên tố khi và chỉ khi $(n-1)! \equiv n-1 \ (mod \ n)$.

Ví dụ

- Với $n = 4$:
  $(n-1)! \ = 6 \ (n-1)! \ mod \ n \ = 2$
- Với $n = 5$:
  $(n-1)! \ = 24 \ (n-1)! \ mod \ n \ = 4 = n-1$, do n là số nguyên tố.
- Với $n = 6$:
  $(n-1)! \ = 120 \ (n-1)! \ mod \ n \ = 0$
- Với $n = 11$:
  $(n-1)! \ = 3628800 \ (n-1)! \ mod \ n \ = 10 = n-1$, do n là số nguyên tố.
- Với $n = 12$:
  $(n-1)! \ = 39916800 \ (n-1)! \ mod \ n \ = 0$

Chứng minh

Mệnh đề đúng với $n = 2$ và $n = 3$. Ta giả sử $n > 3$.

- **Chiều thuận:** nếu n là số nguyên tố thì $(n-1)! \equiv n-1 \ (mod \ n)$

Khi n là số nguyên tố thì $gcd(a, n) = 1$ với mọi $a < n$. Theo định lý Euler ta có:

$a * a^{n-2} = a^{n-1} \equiv 1 \ mod \ n$

Đặt $b = a^{n-2} \bmod n$. Với mỗi a thì b là duy nhất và $b < n$ để $a * b \ (mod \ n) \ = 1$, mặt khác $a = b$ khi và chỉ khi $a = 1$ hoặc $a = n-1$ nên ta có thể tạo ra $\frac{(n-2)}{2}$ cặp số a, b phân biệt như vậy. Nhân tất cả các cặp với nhau ta được

$2.3.4. . . (n-2) \ mod \ n = 1$

$\Rightarrow 1.2.3..(n-1) \; mod \; n = n-1$

$\Rightarrow (n-1)! \equiv n-1 \; (mod \; n)$

- **Chiều ngược:** nếu $(n-1)! \equiv n-1 \; (mod \; n)$ thì n là số nguyên tố

Nếu n là hợp số

$\Rightarrow$ tồn tại ước của n trong khoảng $(2; n)$

$\Rightarrow gcd((n-1)!, n) > 1$ do $(n-1)! = 1.2.3...(n-1)$

$\Rightarrow gcd((n-1)! \bmod n, n) > 1$

$\Rightarrow gcd(n-1, n) > 1$ (vô lý).

Vậy n phải là số nguyên tố.

- **Áp dụng**

Định lý Wilson cho ta cách tính nhanh $(n-1)! \; mod \; n$ khi n là số nguyên tố.

Luyện tập

- Factorial Again - HackerEarth