HÀM EULER

Hàm Euler, còn gọi là **phi-hàm** $\phi(n)$, cho số lượng số nguyên nằm trong phạm vi từ 1 đến n nguyên tố cùng nhau với n. Hai số được gọi là nguyên tố cùng nhau nếu ước chung lớn nhất của chúng bằng 1 (số 1 nguyên tố cùng nhau với mọi số nguyên).
Dưới đây là bảng giá trị $\phi(n)$ với một vài số nguyên:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8	12

Tính chất:

Các tính chất sau của $\phi(n)$ đủ để tính toán nó cho bất kỳ số nào:
+) Nếu p là số nguyên tố thì gcd(p,q)=1 với mọi $1 \le q < p$. Do đó:

$$\phi(p) = p - 1$$

+) Nếu p là số nguyên tố và $k \ge 1$, khi đó có đúng $\frac{p^k}{p}$ số nằm giữa 1 và p^k chia hết cho p. Điều này cho chúng ta:

$$\phi(p^k) = p^k - p^{k-1}$$

+) Nếu a, b nguyên tố cùng nhau thì:

$$\phi(a.b) = \phi(a).\phi(b)$$

Kết quả này là không tầm thường, nó là hệ quả của định lý phần dư Trung Hoa. Định lý phần dư Trung Hoa đảm bảo rằng với mỗi $0 \le x < a$ và mỗi $0 \le y < b$ thì tồn tại duy nhất $0 \le z < ab$ sao cho $z \equiv x(\text{mod } a), z \equiv y(\text{mod } b)$. Không khó chỉ ra được z nguyên tố cùng nhau với $a.b$ khi và chỉ khi x nguyên tố cùng nhau với a, y nguyên tố cùng nhau với b. Do vậy số lượng số nguyên tố cùng nhau với ab bằng tích của số lượng số nguyên tố cùng nhau với a với số lượng số nguyên tố cùng nhau với b.
+) Trong trường hợp tổng quát, khi a và b không nguyên tố cùng nhau ta có công thức:

$$\phi(ab) = \phi(a).\phi(b).\frac{d}{\phi(d)}$$

với $d = \gcd(a,b)$
Từ ba tính chất ở trên ta có thể tính $\phi(n)$ bằng cách phân tích n thành tích của các thừa số nguyên tố. Giả sử $n = p_1^{a_1}.p_2^{a_2} \dots p_k\hat{}(a_k)$, ở đây p_i là các thừa số nguyên tố của n:

$$\phi(n) = \phi(p_1^{a_1}).\phi(p_2^{a_2}) \dots \phi({p_k}_k^{a_k})$$
$$= (p_1^{a_1} - p_1^{a_1-1}).(p_2^{a_2} - p_2^{a_2-1}) \dots (p_k^{a_k} - p_k^{a_k-1})$$
$$= {p_1}_1^{a}.\left(1 - \frac{1}{p_1}\right).p_2^{a_2}.\left(1 - \frac{1}{p_2}\right) \dots p_k^{a_k}.\left(1 - \frac{1}{p_k}\right)$$
$$= n.\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Thực hiện:

1) Hàm tính $\phi(n)$ sử dụng phân tích thừa số nguyên tố với thời gian $O(\sqrt{n})$:

```
int phi(int n) {
    int result=n;
    for(int i=2;i<=n/i;++i) {
        if (n % i == 0) {
            while (n%i==0) n/=i;
```

```
            result -= result/i;
        }
    }
    if (n>1) result -= result/n;
    return result;
}
```

2) Tính giá trị của hàm Euler của tất cả các số từ 1 đến n trong thời gian $O(n \log \log n)$

```
void phi_1_to_n(int n) {
    vector<int> phi(n+1);
    for(int i=0;i<=n;++i) phi[i]=i;
    for(int i=2; i<=n;++i) {
         if (phi[i]==i) {
            for(int j=i; j<=n; j+=i)
                phi[j]-=phi[j]/i;
        }
    }
}
```

Tính chất tổng các ước:

Tính chất thú vị này được phát hiện bởi Gauss:

$$\sum_{d|n} \phi(d) = n$$

Chú ý rằng tổng lấy qua tất cả các ước d của n.

Ví dụ: 10 có các ước 1, 2, 5, 10. Ta có:

$$\phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10$$

Nhờ tính chất trên ta có thể tìm phi-hàm Euler của tất cả các số từ 1 đến n với thời gian $O(n \log n)$:

```
void phi_1_to_n(int n) {
    vector<int> phi(n+1);
    phi[0]=0;
    phi[1]=1;
    for(int i=2;i<=n;++i) phi[i]=i-1;
    for(int i=2; i<=n; ++i)
        for(int j=2;j<=n; j+=i)
            phi[j] -= phi[i];
}
```

Định lý Euler

Ứng dụng quan trọng nhất của hàm Euler là định lý Euler:

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

nếu a và m là nguyên tố cùng nhau.

Ngay lập tức ta có công thức:

$$a^n \equiv a^{n \bmod \phi(m)} \pmod{m}$$

(Công thức này thường dùng khi n là số cực lớn)