欧拉函数和欧拉定理

一、欧拉函数的定义和性质

定义： 在小于等于 n 的正整数中，与 n 互质的数的个数。

$$\phi(n)=\sum_{i=1}^{n}[gcd(i,n)=1]$$

欧拉函数的性质：

性质一：

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

性质二：

ϕ是积性函数，但不是完全积性函数。（证明略）

$$\phi(pq)=\phi(p)\cdot\phi(q)\quad\ (gcd(p,q)=1)$$

性质三：

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

性质四（由性质二、三可证）：

$$\phi(x)=\prod_{i=1}^{r}(p_i-1)\cdot p_i^{\alpha_i-1}=x\cdot\prod_{i=1}^{r}(1-\frac{1}{p_i})$$

其中，正整数 x 唯一分解：$x=\prod_{i=1}^{r}p_i^{\alpha_i}$

性质五：

$$\sum_{i=1}^{n}i\cdot[gcd(i,n)=1]=n\cdot\frac{\phi(n)}{2}$$

可以证明若 $gcd(n,i)=1$ 则 $gcd(n,n-i)=1$

因此与 n 互质的数 $i,n-i$ 都是成对出现的。

性质六（由性质四可证）：

设 p 为质数，则有

$$\phi(i\cdot p)=p\cdot\phi(i)\ \ (i\ mod\ p=0)$$

性质七：

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

证明：设 n 个分数

$$\frac{1}{n},\ \frac{2}{n},\ \frac{3}{n}...\frac{n}{n}$$

将所有分数化简成最简分数，易得所有化简后的分母 $n_i|n$,而 n_i 出现的次数正好等于$\phi(n_i)$。

二、求解欧拉函数

求单个欧拉函数：

可一边分解质因数一边求欧拉函数，原理由性质四。

```
ll phi(ll n) {
    ll ans = n,temp = n;
    for (ll i = 2; i * i <= temp; i++){
        if (temp % i == 0){
            ans -= ans / i;//ans = ans * (i - 1) / i
            while (temp % i == 0) temp /= i;
        }
    }
    if (temp > 1) ans -= ans / temp;
    return ans;
}
```

由于欧拉函数是积性函数，所以可以用线性筛筛出。

三、欧拉定理

若 a 与 m 互质，则：

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

证明：

$$\begin{aligned} &\text{记}X_1, X_2 ... X_{\phi(m)}\text{为}[1, m]\text{与}m\text{互质的数} \\ &\text{可证明}aX_1, aX_2 ... aX_{\phi(m)}\text{模}m\text{后两两不同且与}m\text{互质} \end{aligned}$$

1、证明与m互质：

$$\because a\text{与}m\text{互质，}X_i\text{与}m\text{互质，所以}aX_i\text{显然与}m\text{互质。}$$

2、证明两两不同：

$$\begin{aligned} &\text{利用反证法，假设存在}1 \le i < j \le \phi(m) \\ &\text{使得}aX_i \equiv aX_j \ (mod \ m) \\ &\text{那么有 } m | a(X_j - X_i) \\ &\because gcd(a, m) = 1 \ \therefore m | (X_j - X_i) \\ &\text{又由假设 } 1 \le X_j - X_i < m \text{ ,矛盾} \end{aligned}$$

3、结论

$$\text{综上可得 } X_1X_2 ... X_{\phi(m)} \equiv aX_1aX_2 ... aX_{\phi(m)} \ (mod \ m)$$
$$\therefore a^{\phi(m)} \equiv 1 \ (mod \ m)$$

四、扩展欧拉定理（证明略）

$$a^c \begin{cases} \equiv a^{c \ mod \ \phi(m)} & gcd(a, m) = 1 \\ \equiv a^c & gcd(a, m) \ne 1, c < \phi(m) \\ \equiv a^{c \ mod \ \phi(m) + \phi(m)} & gcd(a, m) \ne 1, c \ge \phi(m) \end{cases}$$

五、费马小定理

即欧拉定理的特殊形式。

$$a^{p-1} \equiv 1 \pmod p$$

六、威尔逊定理（证明略）

当 p 是质数时，满足以下充分必要条件：

$$(p-1)! \equiv -1 \ (mod\ p)$$