数论—欧拉函数、欧拉定理、费马小定理

欧拉函数

定义

欧拉函数（Euler's totient function），记为 $\varphi(n)$，表示 $1 \sim n$ 中与 n 互质的数的个数。

也可以表示为：$\varphi(n) = \sum\limits_{i=1}^{n}[\gcd(i,n)=1]$.

例如：

$\varphi(1)=1$，即 $\gcd(1,1)=1$；
$\varphi(2)=1$，即 $\gcd(1,2)=1$；
$\varphi(3)=2$，即 $\gcd(1,3)=1$，$\gcd(2,3)=1$；$\ldots$

性质

1. 欧拉函数是积性函数；即如果 $\gcd(a,b)=1$，那么 $\varphi(a\times b)=\varphi(a)\times\varphi(b)$。
2. 由唯一分解定理，设 $n=\prod\limits_{i=1}^{s}p_i^{k_i}$，其中 p_i 是质数，有 $\varphi(n)=n\times\prod\limits_{i=1}^{s}\dfrac{p_i-1}{p_i}$。
3. 当 n 是质数的时候，显然有 $\varphi(n)=n-1$（定义）。

实现

根据性质 2 可以写出：

```
int euler_phi(int n) {
    int ans = n;
    for (int i = 2; i * i <= n; i++) {
        if (n % i == 0) {
            ans = ans / i * (i - 1);
            while (n % i == 0) n /= i;
        }
    }
```

```
    return n > 1 ? ans / n * (n - 1) : ans;
}
```

线性筛求欧拉函数

注意到在线性筛中，每一个合数都是被最小的质因子筛掉。

比如设 p_1 是 n 的最小质因子，$k = n/p_1$，即 $kp_1 = n$；
那么线性筛的过程中 n 通过 $k \times p_1$ 筛掉。

观察线性筛的过程，我们还需要处理两个部分，下面对 $k \bmod p_1$ 分情况讨论：

- 如果 $k \bmod p_1 = 0$，那么 k 包含了 n 的所有质因子；有：

$$\varphi(n) = n \times \prod_{i=1}^{s} \frac{p_i - 1}{p_i}$$

$$= p_1 \times k \times \prod_{i=1}^{s} \frac{p_i - 1}{p_i}$$

$$= p_1 \times \varphi(k)$$

- 如果 $k \bmod p_1 \neq 0$，这时 k 和 p_1 是互质的，根据欧拉函数性质；有：

$$\varphi(n) = \varphi(p_1) \times \varphi(k)$$

$$= (p_1 - 1) \times \varphi(k)$$

```
int primes[N], cnt;
bool is[N];

int phi[N];
int get_phi(int n) {
    phi[1] = 1;
    for (int i = 2; i <= n; ++i) {
        if (!is[i]) primes[++cnt] = i, phi[i] = i - 1;
        for (int j = 0; primes[j] <= n / i; ++j) {
            is[primes[j] * i] = 1;
            if (i % primes[j]) phi[primes[j] * i] = phi[i] * (primes[j]
- 1);
            else {
                phi[primes[j] * i] = phi[i] * primes[j];
                break;
            }
```

```
        }
    }
}
```

欧拉定理

前置知识

前置知识１：完全剩余系

完全剩余系（最小非负完全剩余系），定义为：$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$.

具体的定义为 整数集 $S = \{r_1, r_2, \dots, r_s\}$，满足：

1. 任意不同元素 $r_i \not\equiv r_j \pmod m$.
2. 任意 $a \in \mathbb{Z}$，存在 $r_i \equiv a \pmod m$.

也就是模 m 意义下的完全剩余系包含 $0 \sim m-1$ 内的所有整数，长度为 m。

前置知识２：简化剩余系

简化剩余系，定义为：$\Phi_m = \{r \in \mathbb{Z}_m : r \perp m\}$.

具体的定义为 整数集 $S = \{r_1, r_2, \dots, r_s\}$，满足：

1. 任意 $r_i \perp m$.
2. 任意不同元素 $r_i \not\equiv r_j \pmod m$.
3. 任意 $a \perp m$，存在 $r \equiv a \pmod m$.

也就是模 m 意义下的简化剩余系包含 $0 \sim m-1$ 内所有与 m 互质的整数，长度为 $\varphi(m)$。

前置知识３：欧拉定理的引理

若 $a \perp m$，且有 $S = \{r_1, r_2, \dots, r_s\}$ 为一个简化剩余系，
则 $S' = \{ar_1, ar_2, \dots, ar_s\}$ 也是一个简化剩余系。

证明：

1. 对于任意 r_i：由 $a \perp m$、$r_i \perp m$，得 $ar_i \perp m$（互质性质）.
2. 对于任意两个不同元素：由 $r_i \not\equiv r_j \pmod m$、$a \perp m$，得 $ar_i \not\equiv ar_j \pmod m$.
3. 由 $|S'| = |S|$ 及 (2) 得：任意 r_i 一定有与其对应的 ar_j ；
   因为对于任意 $t \perp m$，存在 $r_i \equiv t \pmod m$，也一定存在 $ar_j \equiv t \pmod m$.

满足简化剩余系的定义，因此 S' 是一个简化剩余系。

定义

若 $\gcd(a,m)=1$，则 $a^{\varphi(m)} \equiv 1 \pmod m$。

证明

设 $S=\{r_1,r_2,\cdots,r_{\varphi(m)}\}$ 为模 m 意义下的简化剩余系，
则 $S'=\{ar_1,ar_2,\cdots,ar_{\varphi(m)}\}$ 也为模 m 意义下的简化剩余系.

因为 $a \perp m$，所以 $r_1r_2\dots r_{\varphi(m)} \equiv ar_1ar_2\dots ar_{\varphi(m)} \pmod m$，
即 $r_1r_2\dots r_{\varphi(m)} \equiv a^{\varphi(m)}r_1r_2\dots r_{\varphi(m)} \pmod m$.

因为 $r_1r_2\dots r_{\varphi(m)} \perp m$（互质性质），所以可以约去;
即 $a^{\varphi(m)} \equiv 1 \pmod m$.

应用

指数取模

$a^k \equiv a^{k \bmod \varphi(p)} \pmod p$

证明:

$$
\begin{aligned}
a^{u+v\varphi(p)} &\equiv a^u a^{v\varphi(p)} && \pmod p && (1)\\
&\equiv a^u (a^{\varphi(p)})^v && \pmod p && (2)\\
&\equiv a^u (1)^v && \pmod p && (3)\\
&\equiv a^u && \pmod p && (4)
\end{aligned}
$$

费马小定理

若 p 为素数，由于 $\varphi(p)=p-1$，代入欧拉定理可立即得到费马小定理:
若 p 为素数，$\gcd(a,p)=1$，则 $a^{p-1} \equiv 1 \pmod p$。

Reference

[1] https://oi-wiki.org/math/number-theory/euler/

[2] https://oi-wiki.org/math/number-theory/sieve/

[3] https://oi-wiki.org/math/number-theory/fermat/

[4] https://zhuanlan.zhihu.com/p/581822244

[5] https://zhuanlan.zhihu.com/p/536214853

[6] https://zhuanlan.zhihu.com/p/577742188

[7] https://blog.csdn.net/weixin_43145361/article/details/107083879

[8] https://baike.baidu.com/item/简化剩余系/3712809

合集：学习笔记

标签：算法 ，学习笔记