[toc]

欧拉函数的定义

欧拉函数（Euler's totient function），即 $\varphi(n)$，表示的是小于等于 n 和 n 互质的数的个数。

比如说 $\varphi(1) = 1$。

当 n 是质数的时候，显然有 $\varphi(n) = n - 1$。

欧拉函数的一些性质

- 欧拉函数是积性函数。

  积性是什么意思呢？如果有 $\gcd(a, b) = 1$，那么 $\varphi(a \times b) = \varphi(a) \times \varphi(b)$。

  特别地，当 n 是奇数时 $\varphi(2n) = \varphi(n)$。

- $n = \sum_{d \mid n}{\varphi(d)}$。

  利用 莫比乌斯反演 相关知识可以得出。

  也可以这样考虑：如果 $\gcd(k, n) = d$，那么 $\gcd(\dfrac{k}{d},\dfrac{n}{d}) = 1, （ k < n ） $。

  如果我们设 $f(x)$ 表示 $\gcd(k, n) = x$ 的数的个数，那么 $n = \sum_{i = 1}^n{f(i)}$。

  根据上面的证明，我们发现，$f(x) = \varphi(\dfrac{n}{x})$，从而 $n = \sum_{d \mid n}\varphi(\dfrac{n}{d})$。注意到约数 d 和 $\dfrac{n}{d}$ 具有对称性，所以上式化为 $n = \sum_{d \mid n}\varphi(d)$。

- 若 $n = p^k$，其中 p 是质数，那么 $\varphi(n) = p^k - p^{k - 1}$。（根据定义可知）

- 由唯一分解定理，设 $n = \prod_{i=1}^{n}p_i^{k_i}$，其中 p_i 是质数，有 $\varphi(n) = n \times \prod_{i = 1}^s{\dfrac{p_i - 1}{p_i}}$。

  证明：

  - 引理：设 p 为任意质数，那么 $\varphi(p^k)=p^{k-1}\times(p-1)$。

    证明：显然对于从 1 到 p^k 的所有数中，除了 p^{k-1} 个 p 的倍数以外其它数都与 p^k 互素，故 $\varphi(p^k)=p^k-p^{k-1}=p^{k-1}\times(p-1)$，证毕。

  接下来我们证明 $\varphi(n) = n \times \prod_{i = 1}^s{\dfrac{p_i - 1}{p_i}}$。由唯一分解定理与 $\varphi(x)$ 函数的积性

$$ \begin{aligned} \varphi(n) &= \prod_{i=1}^{s} \varphi(p_i^{k_i}) \ &= \prod_{i=1}^{s} (p_i-1)\times {p_i}^{k_i-1}\ &=\prod_{i=1}^{s} {p_i}^{k_i} \times(1 - \frac{1}{p_i})\ &=n~ \prod_{i=1}^{s} (1- \frac{1}{p_i}) &\square \end{aligned} $$

如何求欧拉函数值

如果只要求一个数的欧拉函数值，那么直接根据定义质因数分解的同时求就好了。

```
int euler_phi(int n) {
  int m = int(sqrt(n + 0.5));
  int ans = n;
  for (int i = 2; i <= m; i++)
    if (n % i == 0) {
      ans = ans / i * (i - 1);
      while (n % i == 0) n /= i;
    }
  if (n > 1) ans = ans / n * (n - 1);
  return ans;
}
```

注：如果将上面的程序改成如下形式，会提升一点效率：

```
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;
    }
  if (n > 1) ans = ans / n * (n - 1);
  return ans;
}
```

如果是多个数的欧拉函数值，可以利用后面会提到的线性筛法来求得。

欧拉定理

与欧拉函数紧密相关的一个定理就是欧拉定理。其描述如下：

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

扩展欧拉定理

当然也有扩展欧拉定理

$$ a^b\equiv \begin{cases} a^{b\bmod\varphi(p)},,&\gcd(a,,p)=1\ a^b,&\gcd(a,,p)\ne1,,b<\varphi(p)\ a^{b\bmod\varphi(p)+\varphi(p)},&\gcd(a,,p)\ne1,,b\ge\varphi(p) \end{cases} \pmod p $$

可用于欧拉降幂