欧拉函数 [编辑]

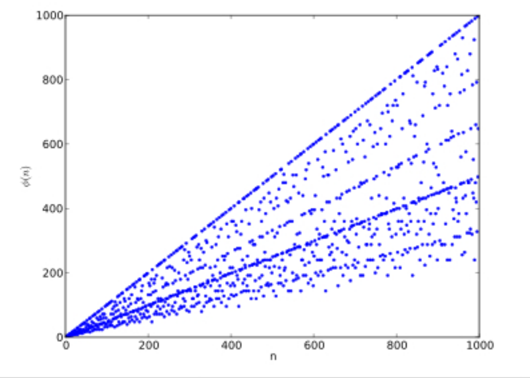
维基百科，自由的百科全书

本文介绍的是小于或等于*n*的正整数中与*n*互质的数的数目。关于形式为$\phi(q)=\prod_{k=1}^{\infty}(1-q^k)$的函数，详见"**欧拉函数 (复变函数)**"。

在数论中，对正整数*n*，**欧拉函数**$\varphi(n)$是小于或等于*n*的正整数中与*n*互质的数的数目。此函数以其首名研究者欧拉命名，它又称为**φ函数**（由高斯所命名）或是**欧拉总计函数**[1]（totient function，由西尔维斯特所命名）。

例如$\varphi(8)=4$，因为1,3,5,7均和8互质。

欧拉函数实际上是模*n*的同余类所构成的乘法群（即环$\mathbb{Z}/n\mathbb{Z}$的所有单位元组成的乘法群）的阶。这个性质与拉格朗日定理一起构成了欧拉定理的证明。



当*n*为1至1000的整数时$\varphi(n)$的值

目录 [隐藏]

1 历史：欧拉函数与费马小定理
2 欧拉函数的值
3 性质
4 生成函数
5 欧拉函数的走势
6 其他与欧拉函数有关的等式
7 与欧拉函数有关的不等式
8 参考来源
9 文献来源

历史：欧拉函数与费马小定理 [编辑]

1736年，欧拉证明了费马小定理[2]：

假若 p 为质数，a 为任意正整数，那么 a^p-a 可被 p 整除。

然后欧拉予以一般化：

假若 a 与 n 互质，那么 $a^{\phi(n)}-1$ 可被 n 整除。亦即，$a^{\phi(n)}\equiv 1 \pmod n$。

其中 $\phi(n)$ 即为欧拉总计函数。如果 n 为质数，那么 $\phi(n)=n-1$，因此，有高斯的版本[3]：

假若 p 为质数，a 与 p 互质（a 不是 p 的倍数），那么 $a^{p-1}\equiv 1 \pmod p$。

欧拉函数的值 [编辑]

$\varphi(1)=1$（小于等于1的正整数中唯一和1互质的数就是1本身）。

若*n*是质数*p*的*k*次幂，$\varphi(n)=\varphi(p^k)=p^k-p^{k-1}=(p-1)p^{k-1}$，因为除了*p*的倍数外，其他数都跟*n*互质。

欧拉函数是积性函数，即是说若*m*,*n*互质，$\varphi(mn)=\varphi(m)\varphi(n)$。证明：设*A*, *B*, *C*是跟*m*, *n*, *mn*互质的数的集，据中国剩余定理，$A\times B$和C可建立双射(一一对应)的关系。（或者也可以从初等代数角度给出欧拉函数积性的简单证明）因此$\varphi(n)$的值使用算术基本定理便知，

若$n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$

则$\varphi(n)=\prod_{i=1}^{r}p_i^{k_i-1}(p_i-1)=\prod_{p\mid n}p^{\alpha_p-1}(p-1)=n\prod_{p\mid n}\left(1-\frac{1}{p}\right)$。

其中α_p是使得p^α整除n的最大整数α（这里$\alpha_{p_i}=k_i$）。

例如$\varphi(72)=\varphi(2^3\times 3^2)=2^{3-1}(2-1)\times 3^{2-1}(3-1)=2^2\times 1\times 3\times 2=24$

性质 [编辑]

*n*的欧拉函数$\varphi(n)$也是循环群 C_n 的生成元的个数（也是*n*阶分圆多项式的次数）。C_n 中每个元素都能生成 C_n 的一个子群，即必然是某个子群的生成元。而且按照定义，不同的子群不可能有相同的生成元。此外， C_n 的所有子群都具有 C_d 的形式，其中*d*整除*n*（记作*d* | *n*）。因此只要考察*n*的所有因数*d*，将 C_d 的生成元个数相加，就将得到 C_n 的元素总个数：*n*。也就是说：

$$\sum_{d\mid n}\varphi(d)=n$$

其中的*d*为*n*的正约数。

运用默比乌斯反转公式来“翻转”这个和，就可以得到另一个关于$\varphi(n)$的公式：

$$\varphi(n)=\sum_{d\mid n}d\cdot\mu(n/d)$$

其中 μ 是所谓的默比乌斯函数，定义在正整数上。

对任何两个互质的正整数*a*, *m*（即 gcd(*a*,*m*) = 1），$m\geq 2$，有

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

即欧拉定理。

这个定理可以由群论中的拉格朗日定理得出，因为任意与*m*互质的*a*都属于环 $\mathbb{Z}/n\mathbb{Z}$ 的单位元组成的乘法群$\mathbb{Z}/n\mathbb{Z}^\times$

当*m*是质数*p*时，此式则为：

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

即费马小定理。

生成函数 [编辑]

以下两个由欧拉函数生成的级数都是来自于上节所给出的性质：$\sum_{d\mid n}\varphi(d)=n$。

由$\varphi(n)$生成的狄利克雷级数是：

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\frac{\zeta(s-1)}{\zeta(s)}.$$

其中ζ(*s*)是黎曼ζ函数。推导过程如下：

$$\begin{aligned}\zeta(s)\sum_{f=1}^{\infty}\frac{\varphi(f)}{f^s}&=\left(\sum_{g=1}^{\infty}\frac{1}{g^s}\right)\left(\sum_{f=1}^{\infty}\frac{\varphi(f)}{f^s}\right)\\&=\sum_{h=1}^{\infty}\left(\sum_{fg=h}1\cdot\varphi(g)\right)\frac{1}{h^s}\\&=\sum_{h=1}^{\infty}\left(\sum_{fg=h}\varphi(g)\right)\frac{1}{h^s}=\sum_{h=1}^{\infty}\left(\sum_{d\mid h}\varphi(d)\right)\frac{1}{h^s}\end{aligned}$$

使用开始时的等式，就得到：$\sum_{h=1}^{\infty}\left(\sum_{d\mid h}\varphi(d)\right)\frac{1}{h^s}=\sum_{h=1}^{\infty}\frac{h}{h^s}$

于是$\sum_{h=1}^{\infty}\frac{h}{h^s}=\zeta(s-1)$

欧拉函数生成的朗贝级数如下：

$$\sum^{\infty}\varphi(n)q^n \quad = \quad q$$

$$\sum_{n=1} \frac{}{1-q^n} = \frac{}{(1-q)^2}$$

其对于满足 |*q*|<1 的*q*收敛。

推导如下：

$$\sum_{n=1}^{\infty} \frac{\varphi(n) q^n}{1-q^n} = \sum_{n=1}^{\infty} \varphi(n) \sum_{r\geq 1} q^{rn}$$

后者等价于：

$$\sum_{k\geq 1} q^k \sum_{n|k} \varphi(n) = \sum_{k\geq 1} kq^k = \frac{q}{(1-q)^2}.$$

欧拉函数的走势 [编辑]

随着*n*变大，估计$\varphi(n)$的值是一件很难的事。当*n*为质数时，$\varphi(n)=n-1$，但有时$\varphi(n)$又与*n*差得很远。

在*n*足够大时，有估计：

对每个 ε > 0，都有*n* > *N*(ε)使得 $n^{1-\varepsilon} < \varphi(n) < n$

如果考虑比值：

$$\varphi(n)/n,$$

由以上已经提到的公式，可以得到其值等于类似$1-p^{-1}$的项的乘积。因此，使比值小的*n*将是两两不同的质数的乘积。由素数定理可以知道，常数 ε 可以被替换为：

$$C \log\log n/\log n.$$

φ就平均值的意义上来说是与*n*很相近的，因为：

$$\frac{1}{n^2}\sum_{k=1}^{n}\varphi(k) = \frac{3}{\pi^2} + \mathcal{O}\left(\frac{\log n}{n}\right)$$

其中的*O*表示大O符号。这个等式也可以说明在集合 {1, 2, ..., *n*} 中随机选取两个数，则当*n*趋于无穷大时，它们互质的概率趋于 $6/\pi^2$。一个相关的结果是比值$\varphi(n)/n$的平均值：

$$\frac{1}{n}\sum_{k=1}^{n}\frac{\varphi(k)}{k} = \frac{6}{\pi^2} + \mathcal{O}\left(\frac{\log n}{n}\right).$$

其他与欧拉函数有关的等式 [编辑]

1. $\varphi\left(n^m\right) = n^{m-1}\varphi(n)$
2. $\forall a \in N, \forall n \in N,\ \exists l \in N$ 使得 $[(a>1 \wedge n>1) \to (l|\varphi(a^n-1) \wedge l \geq n)]$
3. $\forall a \in N, \forall n \in N,\ \exists l \in N$ 使得 $[(a>1 \wedge n>6 \wedge 4 \not| n) \to (l|\varphi(a^n-1) \wedge l \geq 2n)]$
4. $\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}$
5. $\sum_{\substack{1\leq k\leq n \\ (k,n)=1}} k = \frac{1}{2} n\varphi(n) \text{ for } n>1$
6. $\sum_{k=1}^{n} \varphi(k) = \frac{1}{2}\left(1 + \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2\right)$
7. $\sum_{k=1}^{n} \frac{\varphi(k)}{k} = \sum_{k=1}^{n} \frac{\mu(k)}{k} \left\lfloor \frac{n}{k} \right\rfloor$
8. $\sum_{k=1}^{n} \frac{k}{\varphi(k)} = \mathcal{O}(n)$
9. $\sum_{k=1}^{n} \frac{1}{\varphi(k)} = \mathcal{O}(\log(n))$

与欧拉函数有关的不等式 [编辑]

1. $\varphi(n) > \frac{n}{e^{\gamma}\ \log\log n + \frac{3}{\log\log n}}$，其中$n > 2$，γ 为欧拉-马歇罗尼常数。
2. $\varphi(n) \geq \sqrt{\frac{n}{2}}$，其中$n > 0$。
3. 对整数n > 6，$\varphi(n) \geq \sqrt{n}$。
4. 当n为质数时，显然有$\varphi(n) = n - 1$。对于合数的n，则有：

$$\varphi(n) \leq n - \sqrt{n}$$

参考来源 [编辑]

- Milton Abramowitz、Irene A. Stegun， *Handbook of Mathematical Functions*， (1964) Dover Publications , New York. ISBN 0-486-61272-4. 24.3.2节.
- Eric Bach、Jeffrey Shallit， *Algorithmic Number Theory*, 卷 1, 1996, MIT Press. ISBN 0-262-02405-5, 8.8节，234页.
- Kevin Ford, The number of solutions of φ(x)=m, Ann. of Math. 150(1999), 283--311.
- 柯召，孙琦：数论讲义（上册），第二版，高等教育出版社，2001

文献来源 [编辑]

1. ^ Where does the word “totient” come from?
2. ^ Mathematical Thought From Ancient to Modern Times, 第 2 卷，p.608
3. ^ Mathematical Thought From Ancient to Modern Times, 第 3 卷，p.814