

自由的百科全书

首页 分类索引

特色内容 新闻动态

最近更改 随机条目

帮助

帮助

维基社群 方针与指引

互助客栈

知识问答

字词转换 IRC即时聊天

联络我们

关于维基百科

资助维基百科

工具

链入页面 相关更改

上传文件

特殊页面

打印版本

固定链接

页面信息

维基数据项

引用本页

左侧跳顶连接

其他语言

العربية

Български Català

Čeština

Cymraeg

Dansk

Deutsch

Ελληνικά

Esperanto

Español فارسى

Suomi

Français

עברית

Magyar Italiano

日本語

Қазақша

条目 讨论 大陆简体 ▼

阅读 编辑 查看历史 搜索

Q

# 欧拉函数 嘴鲷

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 $\phi(q)=\prod^\infty (1-q^k)$ 的函数,详见"**欧拉函数 (复变函数)**"。

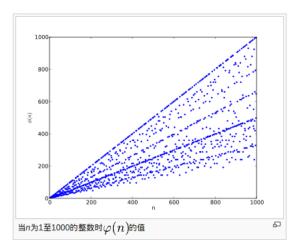
在数论中,对正整数n,**欧拉函数** $\varphi(n)$ 是小于或等于n的正整数中与n互质的数的数目。此函数以其首名 研究者歐拉命名,它又称为 $\phi$ 函数(由高斯所命名)或是欧拉总计函数 $^{[1]}$ (totient function,由西尔维斯特 所命名)。

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。

#### 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 牛成函数
- 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 [編輯]

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 [編輯]

 $\varphi(1) = 1$  (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(--对应)的 关系。(或者也可以从初等代数角度给出<mark>欧拉函数积性的简单证明</mark>)因此 $\wp(n)$ 的值使用算术基本定理便知,

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

한국어

Nederlands

Norsk bokmål

Português

Română

Русский Simple English

Српски / srpski

Svenska

Türkçe

Українська

Tiếng Việt

●编辑链接

其中 $\alpha_p$ 是使得 $p^{lpha}$ 整除n的最大整数lpha (这里 $lpha_{p_i}=k_i$ )。

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 $\wp(n)$  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 $d \mid n$ )。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:

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

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arphi(n)的公式:

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

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>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 $\mathbb{Z}/n\mathbb{Z}^{ imes}$ 

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 [編輯]

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:  $\sum_{d|n} \varphi(d) = n$ 

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((s)是黎曼(函数。推导过程如下:

$$\begin{split} \zeta(s) \sum_{f=1}^{\infty} \frac{\varphi(f)}{f^s} &= \left(\sum_{g=1}^{\infty} \frac{1}{g^s}\right) \left(\sum_{f=1}^{\infty} \frac{\varphi(f)}{f^s}\right) \\ &= \sum_{h=1}^{\infty} \left(\sum_{fg=h} 1 \cdot \varphi(g)\right) \frac{1}{h^s} \\ &= \sum_{h=1}^{\infty} \left(\sum_{fg=h} \varphi(g)\right) \frac{1}{h^s} &= \sum_{h=1}^{\infty} \left(\sum_{d|h} \varphi(d)\right) \frac{1}{h^s} \\ &\text{使用开始时的等式,就得到:} \sum_{h=1}^{\infty} \left(\sum_{fg=h} \varphi(d)\right) \frac{1}{h^s} &= \sum_{h=1}^{\infty} \frac{h}{h^s} \end{split}$$

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

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:

$$\sum_{n=0}^{\infty} \varphi(n)q^n$$
 q

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

其对于满足 |q|<1 的q收敛。

推导如下:

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

后者等价于:

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

### 欧拉函数的走势 [編輯]

随着n变大,估计arphi(n)的值是一件很难的事。当n为质数时,arphi(n)=n-1,但有时arphi(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 $\epsilon$ 可以被替换为:

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

 $\varphi$ 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]

$$1. \varphi(n^m) = n^{m-1} \varphi(n)$$

2. 
$$\forall a \in N, \forall n \in N, \exists l \in N$$
 使得  $[(a > 1 \land n > 1) \rightarrow (l | \varphi(a^n - 1) \land l \ge n)]$ 

3. 
$$\forall a \in N, \forall n \in N, \exists l \in N$$
 使得  $[(a > 1 \land n > 6 \land 4 \not \mid n) \rightarrow (l \mid \varphi(a^n - 1) \land l \geq 2n)]$ 

4. 
$$\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}$$

5. 
$$\sum_{\substack{1 \le k \le n \\ (k,n)=1}} k = \frac{1}{2} n \varphi(n) \text{ for } n > 1$$

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]

$$_{1.}\; arphi(n)>rac{n}{e^{\gamma}\; \log\log n+rac{3}{\log\log n}}$$
 , 其中 $n>2$  ,  $\gamma$  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,
$$arphi(n) \geq \sqrt{n}$$
。

4. 当
$$n$$
为质数时,显然有 $arphi(n)=n-1$ 。对于合数的 $n$ ,则有:

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

## 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

分类: 积性函数 同余

本页面最后修订于2014年10月19日 (星期日) 03:43。

本站的全部文字在知识共享署名-相同方式共享3.0协议之条款下提供,附加条款亦可能应用(请参阅使用条款)。 Wikipedia®和维基百科标志是维基媒体基金会的注册商标;维基™是维基媒体基金会的商标。 维基媒体基金会是在美国佛罗里达州登记的501(c)(3)免税、非营利、慈善机构。

隐私政策 关于维基百科 免责声明 开发者 Cookie声明 手机版视图



