文章编号: 2095-4298(2015)01-0052-03

应用容斥原理推广欧拉函数

林才雄
(华南师范大学 数学科学学院,广东 广州 510631)

摘要: 利用容斥原理对欧拉函数进行了推广,得出如下结论:1) 给出了欧拉函数的 3 种初步推广,即函数 $\varphi_{r;k}(m)$, $\Omega_{r;k;l}(m)$, $H_{r;k;l}(m)$,找到并证明了 $r=0$ 的 3 个表达式;2) 进一步推广了欧拉函数,得到并证明了函数 $\varphi_{r;k}(m)$, $\Omega_{r;k;l}(m)$, $H_{r;k;l}(m)$ 中 r 取 1,2,3 的表达式与 $r=0$ 的倍数关系.

关键词: 欧拉函数;容斥原理;推广

中图分类号: O157.1　　**文献标识码:** A　　**doi:** 10.3969/j.issn.2095-4298.2015.01.008

Popularization of the Euler function by using the principle of inclusion-exclusion method

Lin Caixiong
(School of Mathematical Sciences, South China Normal University, Guangzhou 510631, Guangdong, China)

Abstract: The purpose of this paper is to popularize the Euler function by using the principle of inclusion-exclusion method. The following are the main conclusions: 1) Give three initial promotion of the Euler function, found and proved the expressions when $r=0$; 2) Obtained and proved the multiple relationships among those expressions of the three functions when r takes 1,2,3 and r takes 0.

Key words: Euler function; inclusion-exclusion method; popularization

欧拉函数 $\varphi(n)$ 是数论中一个重要的函数,是数学家欧拉首先提出的. 欧拉函数 $\varphi(n)$ 表示不大于自然数 n 且与 n 互质的自然数的个数. 易知 $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$. 该函数在很多领域中有广泛的应用,如在离散数学中求循环群的生成元[1],在计算机网络安全中的 RSA 公开密钥密码体制中的应用[2]等.

虽然关于欧拉函数的研究有很多,如欧拉函数的性质、方程、算法实现以及欧拉函数在数论[3]、抽象代数[4]方面的推广等等,但在组合数学方面目前尚未见相关的结果. 因此,本文尝试利用容斥原理[5],对欧拉函数进行若干推广.

1　欧拉函数的推广之一

引理 1　$(x-a_1)(x-a_2)\cdots(x-a_l)=x^l-\sigma_1 x^{l-1}+\cdots+(-1)^{l-1}\sigma_{l-1}x+(-1)^l\sigma_l$,其中

$$\sigma_i=\sum_{1\leqslant j_1<\cdots<j_i\leqslant l} a_{j_1}a_{j_2}\cdots a_{j_i},\quad i=1,2,\cdots,l.$$

引理 2　$1-a^m=(1-a)(1+a+\cdots+a^{m-1})$, $m\in\mathbf{N}_+$.

引理 3[6]　自然数 $1,2,\cdots,n$ 的 m ($m\in\mathbf{N}_+$) 次幂和式 $\sum_{i=1}^{n} i^m$ 是关于 n 的一个 $m+1$ 次的有理多项式,即 $\sum_{i=1}^{n} i^m=\sum_{i=1}^{m+1} a_i n^i$,其中

$$a_i\in\mathbf{Q},\quad i=1,2,\cdots,m+1.$$

定义 1　设 m ($m\geqslant 2$) 为自然数, $p_1,p_2,\cdots,p_k$ 是互异的质数,且都是 m 的因数,记 $1,2,\cdots,m$ 中不能被 $p_1,p_2,\cdots,p_k$ 中的任何一个整除的自然数的 r 次方和为 $\varphi_{r;p_1,\cdots,p_k}(m)$,简记为 $\varphi_{r;k}(m)$.

定理 1　设 m ($m\geqslant 2$) 为自然数, $p_1,p_2,\cdots,p_k$ 是互异的质数,且都是 m 的因数,则 $1,2,\cdots,m$ 中不能被 $p_1,p_2,\cdots,p_k$ 中的任何一个整除的自然数的个数为

$$\varphi_{0;k}(m)=m\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).\tag{1}$$

证　记 $S=\{1,2,\cdots,m\}$, $A_i=\{S$ 中 p_i 的倍

收稿日期: 2014-04-26
作者简介: 林才雄,男,硕士研究生,主要从事竞赛数学和初等数学方面的研究,E-mail:1002101656@qq.com.
引文格式: 林才雄. 应用容斥原理推广欧拉函数. 江苏师范大学学报:自然科学版,2015,33(1):52-54.
Lin Caixiong. Popularization of the Euler function by using the principle of inclusion-exclusion method. J Jiangsu Norm Univ: Nat Sci Ed, 2015,33(1):52-54.

数$\}$，$i=1,2,\cdots,k$，则由容斥原理得

$$\varphi_{0;k}(m)=\sum_{\substack{a\in S\\ a\notin A_1\cup\cdots\cup A_k}}1$$
$$=|S|-w_1+w_2-\cdots+(-1)^k w_k,$$

其中

$$w_i=\sum_{1\leqslant j_1<j_2<\cdots<j_i\leqslant k}|A_{j_1}\cap A_{j_2}\cap\cdots\cap A_{j_i}|,$$
$$A_i=\left\{p_i,2p_i,\cdots,\frac{m}{p_i}\cdot p_i\right\},\qquad i=1,2,\cdots,k,$$
$$A_{j_1}\cap A_{j_2}=\left\{p_{j_1}p_{j_2},2p_{j_1}p_{j_2},\cdots,\frac{m}{p_{j_1}p_{j_2}}\cdot p_{j_1}p_{j_2}\right\},$$

$\cdots$，

$$A_1\cap A_2\cap\cdots\cap A_k=\left\{p_1p_2\cdots p_k,2p_1p_2\cdots p_k,\cdots,\frac{m}{p_1p_2\cdots p_k}p_1p_2\cdots p_k\right\},$$
$$1\leqslant j_1<j_2<\cdots<j_i\leqslant k,$$

所以

$$\varphi_{0;k}(m)=m-\sum_{i=1}^{k}\frac{m}{p_i}+\sum_{1\leqslant i<j\leqslant k}\frac{m}{p_ip_j}-\cdots+(-1)^k\cdot\frac{m}{p_1p_2\cdots p_k}$$
$$=m\left(1-\sum_{i=1}^{k}\frac{1}{p_i}+\sum_{1\leqslant i<j\leqslant k}\frac{1}{p_ip_j}-\cdots+(-1)^k\cdot\frac{1}{p_1p_2\cdots p_k}\right).$$

由引理 1 可得(1)式.

定理 2　设 $m(m\geqslant2)$为自然数，$p_1,p_2,\cdots,p_k$ 是互异的质数，且都是 m 的因数，则

a) 当 $r=1$ 时，

$$\varphi_{r;k}(m)=\varphi_{1;k}(m)=\frac{m}{2}\varphi_{0;k}(m);$$

b) 当 $r\geqslant2$ 时，

$$\varphi_{r;k}(m)=\left(a_{r+1}n^r+(-1)^k p_1p_2\cdots p_k\cdot\sum_{i=1}^{r-1}\left(a_in^{i-1}\prod_{j=1}^{k}\sum_{l=0}^{r-i-1}p_j^l\right)\right)\varphi_{0;k}(m),$$

其中 $a_{r+1},a_r,\cdots,a_1$ 是自然数 $1,2,\cdots,m$ 的 r 次幂和公式的降幂系数.

根据自然数的 2 次、3 次、4 次幂和公式，即

$$\sum_{i=1}^{m}i^2=\frac{2m^3+3m^2+m}{6},$$
$$\sum_{i=1}^{m}i^3=\frac{m^4+2m^3+m^2}{4},$$
$$\sum_{i=1}^{m}i^4=\frac{6m^5+15m^4+10m^3-m}{30}.$$

由定理 2-b)可得以下 3 个结论：

1) 当 $r=2$ 时，

$$\varphi_{2;k}(m)=\frac{2m^2+(-1)^k p_1p_2\cdots p_k}{6}\varphi_{0;k}(m);$$

2) 当 $r=3$ 时，

$$\varphi_{3;k}(m)=\frac{m^3+(-1)^k\cdot mp_1p_2\cdots p_k}{4}\varphi_{0;k}(m);$$

3) 当 $r=4$ 时，

$$\varphi_{4;k}(m)=\frac{1}{30}\left(6m^4+10m^2\cdot(-1)^k p_1p_2\cdots p_k-(-1)^k p_1p_2\cdots p_k\prod_{j=1}^{k}(1+p_j+p_j^2)\right)\cdot\varphi_{0;k}(m).$$

2　欧拉函数的推广之二

定义 2　设 $m(m\geqslant2)$为自然数，$p_1,p_2,\cdots,p_k,q_1,q_2,\cdots,q_l(k,l\in\mathbf{N}_+)$是互异的质数，且都是 m 的因数，记 $1,2,\cdots,m$ 中不能被 $p_1,p_2,\cdots,p_k$ 中的任何一个整除，但能被 $q_1,q_2,\cdots,q_l$ 同时整除的自然数的 r 次方和为 $\Omega_{r;p_1,\cdots,p_k,q_1,q_2,\cdots,q_l}(m)$，简记为 $\Omega_{r;k;l}(m)$.

下面给出 $\Omega_{0;k;l}(m)$的表达式及其证明，并类比 $\varphi_{r;k}(m)$给出 $\Omega_{r;k;l}(m)$在 $r=1,2,3$ 情况下的表达式.

定理 3　设 $m(m\geqslant2)$为自然数，$p_1,p_2,\cdots,p_k,q_1,q_2,\cdots,q_l$ 是互异的质数，且都是 m 的因数，则 $1,2,\cdots,m$ 中不能被 $p_1,p_2,\cdots,p_k$ 中的任何一个整除，但能被 $q_1,q_2,\cdots,q_l$ 同时整除的自然数的个数

$$\Omega_{0;k;l}(m)=\frac{m}{q_1q_2\cdots q_l}\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).\qquad(2)$$

证　记

$$S=\left\{q_1q_2\cdots q_l,2q_1q_2\cdots q_l,\cdots,\frac{m}{q_1q_2\cdots q_l}\cdot q_1q_2\cdots q_l\right\},$$
$$A_i=\{S\text{ 中 }p_i\text{ 的倍数}\},\quad i=1,2,\cdots,k,$$

则由容斥原理得

$$\Omega_{0;k;l}(m)=\sum_{\substack{a\in S\\ a\notin A_1\cup\cdots\cup A_k}}1$$
$$=|S|-w_1+w_2-\cdots+(-1)^k w_k,$$

其中

$$w_i=\sum_{1\leqslant j_1<j_2<\cdots<j_i\leqslant k}|A_{j_1}\cap A_{j_2}\cap\cdots\cap A_{j_i}|,$$
$$A_i=\left\{p_i,2p_i,\cdots,\frac{m}{q_1q_2\cdots q_lp_i}\cdot p_i\right\},\qquad i=1,2,\cdots,k,$$
$$A_{j_1}\cap A_{j_2}=\left\{p_{j_1}p_{j_2},2p_{j_1}p_{j_2},\cdots,\frac{m}{q_1q_2\cdots q_lp_{j_1}p_{j_2}}p_{j_1}p_{j_2}\right\},$$

$\cdots$，

$$A_1\cap A_2\cap\cdots\cap A_k$$
$$=\left\{p_1p_2\cdots p_k,2p_1p_2\cdots p_k,\cdots,\frac{m}{q_1q_2\cdots q_lp_1p_2\cdots p_k}p_1p_2\cdots p_k\right\},$$
$$1\leqslant j_1<j_2<\cdots<j_i\leqslant k,$$

所以

$$\Omega_{0;k;l}(m)=\frac{m}{q_1q_2\cdots q_l}-\sum_{i=1}^{k}\frac{m}{q_1q_2\cdots q_lp_i}+\cdots$$

$$+(-1)^k\cdot\frac{m}{q_1q_2\cdots q_lp_1p_2\cdots p_k}$$
$$=\frac{m}{q_1q_2\cdots q_l}\Big(1-\sum_{i=1}^{k}\frac{1}{p_i}+\sum_{1\leqslant i<j\leqslant k}\frac{1}{p_ip_j}-\cdots+(-1)^k\cdot\frac{1}{p_1p_2\cdots p_k}\Big).$$

故由引理 1,可得(2)式.

类比 $\varphi_{r;k}(m)$ 的证明及结论,可以得到 $\Omega_{r;k;l}(m)$ 在 $r=1,2,3$ 情况下的 3 个重要结论.

定理 4 设 $m(m\geqslant 2)$ 为自然数,$p_1,p_2,\cdots,p_k$,$q_1,q_2,\cdots,q_l$ 是互异的质数,且都是 m 的因数,则

1) 当 $r=1$ 时,
$$\Omega_{1;k;l}(m)=\frac{m}{2}\Omega_{0;k;l}(m);$$

2) 当 $r=2$ 时,
$$\Omega_{2;k;l}(m)=\frac{2m^2+(-1)^kp_1p_2\cdots p_k}{6}\Omega_{0;k;l}(m);$$

3) 当 $r=3$ 时,
$$\Omega_{3;k;l}(m)=\frac{m^3+(-1)^kmp_1p_2\cdots p_k}{4}\Omega_{0;k;l}(m).$$

3 欧拉函数的推广之三

定义 3 设 $m(m\geqslant 2)$ 为自然数,$p_1,p_2,\cdots,p_k$,$q_1,q_2,\cdots,q_l(k,l\in\mathbf{N}_+)$ 是互异的质数,且都是 m 的因数,记 $1,2,\cdots,m$ 中不能被 $p_1,p_2,\cdots,p_k$ 中的任何一个整除,但能被 $q_1,q_2,\cdots,q_l$ 中至少一个整除的自然数的 r 次方和为 $H_{r;p_1,\cdots,p_k,q_1,q_2,\cdots,q_l}(m)$,简记为 $H_{r;k;l}(m)$.

下面通过逆向思考,给出 $H_{0;k;l}(m)$ 的表达式及其证明,并类比 $\varphi_{r;k}(m)$ 给出 $H_{r;k;l}(m)$ 在 $r=1,2,3$ 情况下的表达式.

定理 5 设 $m(m\geqslant 2)$ 为自然数,$p_1,p_2,\cdots,p_k$,$q_1,q_2,\cdots,q_l$ 是互异的质数,且都是 m 的因数,则有 $1,2,\cdots,m$ 中不能被 $p_1,p_2,\cdots,p_k$ 中的任何一个整除,但能被 $q_1,q_2,\cdots,q_l$ 中至少一个整除的自然数的个数为
$$H_{0;k;l}(m)=m\prod_{i=1}^{k}\Big(1-\frac{1}{p_i}\Big)\Big(1-\prod_{j=1}^{l}\Big(1-\frac{1}{q_j}\Big)\Big).$$

证 用集合 A 表示 $1,2,\cdots,m$ 中不能被 $p_1,p_2,\cdots,p_k,q_1,q_2,\cdots,q_l$ 中的任何一个整除的自然数之集,用集合 B 表示 $1,2,\cdots,m$ 中不能被 $p_1,p_2,\cdots,p_k$ 中的任何一个整除的自然数之集. 显然 $H_{0;k;l}(m)=|B|-|A|$. 则由定理 1 可得
$$|A|=\varphi_{0;k+l}(m)=m\prod_{i=1}^{k}\Big(1-\frac{1}{p_i}\Big)\prod_{j=1}^{l}\Big(1-\frac{1}{q_j}\Big),$$
$$|B|=\varphi_{0;k}(m)=m\prod_{i=1}^{k}\Big(1-\frac{1}{p_i}\Big),$$
于是
$$H_{0;k;l}(m)=|B|-|A|=m\prod_{i=1}^{k}\Big(1-\frac{1}{p_i}\Big)\Big(1-\prod_{j=1}^{l}\Big(1-\frac{1}{q_j}\Big)\Big).$$

同样地,类比 $\varphi_{r;k}(m)$ 的证明及结论,也可得到 $H_{r;k;l}(m)$ 在 $r=1,2,3$ 情况下的 3 个重要结论.

定理 6 设 $m(m\geqslant 2)$ 为自然数,$p_1,p_2,\cdots,p_k$,$q_1,q_2,\cdots,q_l$ 是互异的质数,且都是 m 的因数,则

1) 当 $r=1$ 时,
$$H_{1;k;l}(m)=\frac{m}{2}H_{0;k;l}(m);$$

2) 当 $r=2$ 时,
$$H_{2;k;l}(m)=\frac{2m^2+(-1)^kp_1p_2\cdots p_k}{6}H_{0;k;l}(m);$$

3) 当 $r=3$ 时,
$$H_{3;k;l}(m)=\frac{m^3+(-1)^kmp_1p_2\cdots p_k}{4}H_{0;k;l}(m).$$

参考文献:

[1] 樊守德. 从欧拉函数的角度给出有限循环群生成元的计数公式[J]. 科技资讯,2011(29):242.

[2] 王伟,辛小龙,陈涛. 基于孙子定理和欧拉函数口令验证方案[J]. 现代电子技术,2006(1):60.

[3] 周尚超. Euler 函数的推广[J]. 华东交通大学学报,2007,24(4):131.

[4] 周敏娜. 关于欧拉函数的推广[J]. 绍兴文理学院学报,1997,17(6):491.

[5] 曹汝成. 组合数学[M]. 广州:华南理工大学出版社,2000:47.

[6] 陈景润,黎鉴思. 关于幂和公式的一般性质[J]. 数学研究与评论,1986,6(1):43.

[责任编辑:史成娣]