一类广义欧拉函数的准确计算公式

廖群英
(四川师范大学 数学科学学院, 四川 成都 610066)

摘要:为将 Lehmer 同余式从模奇质数平方推广至模任意数的平方,Cai 等(CAI T X, FU X D, ZHOU X. Acta Aritmetica,2002,103(3):203－214.)定义了广义欧拉函数 $\varphi_e(n)$. 最近 Cai 等给出了 $e=3,4,6$ 时广义欧拉函数 $\varphi_e(n)$ 的计算公式. 利用初等数论与组合的方法和技巧,完全确定了一类广义欧拉函数的计算公式,即给出当 e 为 n 的特殊正因数时,$\varphi_e(n)$ 的准确计算公式,从而推广 Cai 等的相关主要结果,并由此给出 $\varphi_e(n)$ 为偶数的一个充分必要条件.

关键词:欧拉函数; 广义欧拉函数; 麦比乌斯函数
中图分类号:O156.1　　**文献标志码:**A　　**文章编号:**1001－8395(2019)03－0354－04
doi:10.3969/j.issn.1001－8395.2019.03.010

1 引言和主要结果

熟知正整数 n 的欧拉函数 $\varphi(n)$ 定义为序列 $1,2,\cdots,n$ 中与 n 互质的正整数的个数[1]. 该函数是 RSA 公钥密码体制得以建立的重要数学工具之一[2].

另一方面,早在 1637 年,法国数学家费马提出了如下的猜想:当 $n\geqslant 3$ 时,方程
$$x^n+y^n=z^n$$
没有正整数解(x,y,z). 而要证明费马大定理,实际上只需证明 $x^4+y^4=z^4$ 和 $x^p+y^p=z^p$(p 是奇素数)均无正整数解. 费马本人证明了 $n=4$ 的情形,而对于 n 为奇质数的情形的费马大定理的证明进展相当缓慢. 之后,数学家们称方程
$$x^p+y^p=z^p,\quad p\nmid xyz$$
没有正整数解为费马大定理第一情形,而方程
$$x^p+y^p=z^p,\quad p\mid xyz$$
没有正整数解为费马大定理的第二情形. 20 世纪初,文献[3]证明了:若 $p\nmid q_2(p)$ 且 $p\nmid q_3(p)$,则费马大定理第一情形成立,其中
$$q_2(p)=\frac{2^{\varphi(n)}-1}{p},$$
$$q_3(p)=\frac{3^{\varphi(n)}-1}{p},\quad p\neq 3.$$
1938 年,Lehmer[4] 证明了
$$q_2(p)\equiv q_3(p)\equiv 0(\bmod p)\Leftrightarrow$$
$$\sum_{r=1}^{\lfloor\frac{p}{n}\rfloor}\frac{1}{r}\equiv 0(\bmod p),\quad n\in\{2,3,4,6\}.$$
即对任意 $n\in\{2,3,4,6\}$,若
$$\sum_{r=1}^{\lfloor\frac{p}{n}\rfloor}\frac{1}{r}\equiv 0(\bmod p)$$
成立,则费马大定理第一情形成立,从而 Lemher 同余式
$$\sum_{r=1}^{\frac{p-1}{2}}\frac{1}{r}\equiv -2q_2(p)+pq_2{}^2(p)(\bmod p^2)$$
在证明费马大定理中起到至关重要的作用,其中 p 是奇质数,$\lfloor\frac{p}{n}\rfloor$ 表示下取整函数. 为将 Lehmer 同余式从模奇质数的平方推广至模任意整数的平方,文献[5－6]引入了广义欧拉函数的概念.

定义 1.1[5－6]　正整数 n 的广义欧拉函数定义为
$$\varphi_e(n)=\sum_{i=1,\gcd(i,n)=1}^{[\frac{n}{e}]}1,$$

收稿日期:2017－11－27　　接受日期:2018－01－08
基金项目:四川省科技厅科研重点项目(2016JY0134)
作者简介:廖群英(1974—),女,教授,主要从事编码和密码学理论的研究,E－mail:qunyingliao@sicnu.edu.cn

即 $\varphi_e(n)$ 等于序列 $1,2,\cdots,\left[\frac{n}{e}\right]$ 中与 n 互质的正整数的个数,其中 e 为正整数. 容易证明

$$\varphi_e(n) = \sum_{d\mid n}\mu\left(\frac{n}{d}\right)\left[\frac{d}{e}\right],$$

其中[·]是高斯取整函数,$\mu(n)$ 是麦比乌斯函数,即若 $n = \prod_{i=1}^{t} p_i^{\alpha_i}$, 且 $\alpha_i \geqslant 0 (i=1,2,\cdots,t)$,则

$$\mu(n) = \begin{cases} 1, & n = 1, \\ (-1)^t, & n \geqslant 2, \alpha_1 = \alpha_2 = \cdots = \alpha_t = 1, \\ 0, & n \geqslant 2, \exists \alpha_i > 1 (1 \leqslant i \leqslant t). \end{cases}$$

从而研究广义欧拉函数的计算公式及其性质,对于推广的 Lehmer 同余式的研究提供了理论参考.

对正整数 $n = \prod_{i=1}^{t} p_i^{\alpha_i}$, 其中 p_i 为不同的质数, 正整数 $\alpha_i \geqslant 1$. 为方便,记 $\Omega(n) = \sum_{i=1}^{t}\alpha_i$, $\omega(n) = t$,并规定 $\omega(1) = \Omega(1) = 0$,并记 $\gcd(a,b)$ 表示整数 a 和 b 的最大公因数.

由广义欧拉函数的定义易知 $\varphi_1(n) = \varphi(n)$ 且 $\varphi_2(n) = \varphi(n)/2 (n \geqslant 3)$. 最近, Cai 等[7-8]给出 $\varphi_e(n) (e=3,4,6)$ 的准确计算公式如下:

命题 1.1[7]　设 $n = 3^{\alpha}\prod_{i=1}^{t} p_i^{\alpha_i} > 3$, 其中 p_i 为质数且 $\gcd(p_i,3) = 1 (1 \leqslant i \leqslant t)$,则

$$\varphi_3(n) = \begin{cases} \dfrac{\varphi(n)}{3} + \dfrac{(-1)^{\Omega(n)}2^{\omega(n)-\alpha-1}}{3}, & \alpha = 0,1, \\ \quad p_i \equiv 2 \pmod 3), \quad 1 \leqslant i \leqslant t, & \\ \dfrac{\varphi(n)}{3}, & \text{其他}. \end{cases}$$

命题 1.2[8]　设 $n = 2^{\alpha}\prod_{i=1}^{t} p_i^{\alpha_i} > 4$, 其中 p_i 为质数且 $\gcd(p_i,2) = 1 (1 \leqslant i \leqslant t)$,则

$$\varphi_4(n) = \begin{cases} \dfrac{\varphi(n)}{4} + \dfrac{(-1)^{\Omega(n)}2^{\omega(n)-\alpha}}{4}, & \alpha = 0,1, \\ \quad p_i \equiv 3 \pmod 4), \quad 1 \leqslant i \leqslant t, & \\ \dfrac{\varphi(n)}{4}, & \text{其他}. \end{cases}$$

命题 1.3[8]　设 $n = 2^{\alpha}3^{\beta}n_1 > 6$, 其中 $n_1 = \prod_{i=1}^{t} p_i^{\alpha_i}$, p_i 为质数且 $\gcd(p_i,6) = 1 (1 \leqslant i \leqslant t)$,则

$$\varphi_6(n) = \begin{cases} \dfrac{1}{6}\varphi(n) + \dfrac{(-1)^{\Omega(n)}2^{\omega(n)+1-\beta}}{6}, & \alpha = 0, \\ \quad \beta = 0,1, p_i \equiv 5 \pmod 6)(1 \leqslant i \leqslant t), & \\ \dfrac{1}{6}\varphi(n) + \dfrac{(-1)^{\Omega(n)}2^{\omega(n)-1-\beta}}{6}, & \alpha = 1, \\ \quad \beta = 0,1, p_i \equiv 5 \pmod 6)(1 \leqslant i \leqslant t), & \\ \dfrac{1}{6}\varphi(n) - \dfrac{(-1)^{\Omega(n)}2^{\omega(n)-\beta}}{6}, & \alpha \geqslant 2, \\ \quad \beta = 0,1, p_i \equiv 5 \pmod 6)(1 \leqslant i \leqslant t), & \\ \dfrac{1}{6}\varphi(n), & \text{其他}. \end{cases}$$

当 $e=5$ 或 $e \geqslant 7$ 时,命题 1.1 ~ 1.3 的方法和技巧对于广义欧拉函数 $\varphi_e(n)$ 的计算公式的确定是无效的,因此上述 3 个命题也是迄今为止关于广义欧拉函数计算公式的最好结果. 欲给出一般情形下广义欧拉函数的准确计算公式,需要寻求新的方法和技巧.

另一方面,从命题 1.1 可以看出,当 $9 \mid n$ 时, $\varphi_3(n) = \dfrac{\varphi(n)}{3}$;命题 1.2 中当 $4 \mid n$ 时,有 $\varphi_4(n) = \dfrac{\varphi(n)}{4}$;命题 1.3 中当 $6^2 \mid n$ 时, $\varphi_6(n) = \dfrac{\varphi(n)}{6}$. 因此,一个很自然的问题如下.

问题 1.1　对任意整数 n 以及 n 的正因数 e, 是否都有 $\varphi_e(n) = \varphi(n)/e$ 呢?

本文利用广义欧拉函数的定义和初等数论的方法和技巧,基本解决了上述问题. 具体地讲,设正整数 n 的标准分解式为

$$n = p_1^{\alpha_1}\cdots p_t^{\alpha_t}, \quad \alpha_i \geqslant 2, \quad i = 1,2,\cdots,t,$$

其中 $p_1,\cdots,p_t$ 为不同的质数. 对 n 的绝大部分正因数 e,完全确定了相应的广义欧拉函数 $\varphi_e(n)$ 的准确计算公式. 即证明了如下主要结果.

定理 1.1　设正整数

$$n = p_1^{\alpha_1}\cdots p_t^{\alpha_t},$$

其中 $p_1,\cdots,p_t$ 为不同的质数,正整数 $\alpha_i \geqslant 1 (i=1,2,\cdots,t)$,则对 n 的正因数

$$e = p_1^{\beta_1}\cdots p_t^{\beta_t}, \quad 0 \leqslant \beta_i \leqslant \alpha_i - 1, \quad 1 \leqslant i \leqslant t,$$

有

$$\varphi_e(n) = \frac{\varphi(n)}{e}.$$

注记 1.1　在定理 1.1 中取 $p_1 = 3$ 且 $\alpha_1 \geqslant 2$,则得命题 1.1 公式中的第 2 种情形;取 $p_1 = 2, \alpha_1 \geqslant 2$,

则得命题1.2公式中的第2种情形;取 $p_1=2,p_2=3$ 且 $\alpha_1,\beta_1\geqslant 1$ 时,得命题1.3公式中的第4种情形.

另一方面,文献[7-8]还讨论了 $\varphi_e(n)(e=2,3,4,6)$ 的奇偶性,给出相应的 $\varphi_e(n)$ 为奇数的充分必要条件.基于定理1.1,本文给出当 e 为 n 的一些特殊正因数时,相应的 $\varphi_e(n)$ 为偶数的等价刻画.

定理1.2 1)条件同定理1.1,则 $\varphi_e(n)$ 为偶(奇)数当且仅当 $\varphi(n)/e$ 为偶(奇)数.特别地,当 e 为正奇数时,$\varphi_e(n)$ 为偶数当且仅当 $n\geqslant 3$.

2)对任意正整数 n,$\varphi_2(n)$ 为偶数当且仅当 n 至少含有3个不同的质因数,或者以下条件之一成立:

1) $n=2^\alpha,\alpha\geqslant 3$;

2) $n=2^\alpha p^\beta$,p 为奇质数,$\alpha\geqslant 2$ 或者 $\alpha=1$ 且 $4\mid p-1$;

3) n 为奇数且含有2个不同的奇质因数,或者 $n=p^\alpha$ 且 $p=4k+1$ 为奇质因数.

2 主要结果的证明

在证明主要结果之前,先给出如下引理.

引理2.1[1] 正整数 n 的标准分解式为

$$n=p_1^{\alpha_1}\cdots p_t^{\alpha_t},\quad \alpha_i\geqslant 1,\quad i=1,2,\cdots,t,$$

其中 $p_1,\cdots,p_t$ 为不同的质数,则 n 的欧拉函数

$$\varphi(n)=\prod_{i=1}^{t}(p_i^{\alpha_i}-p_i^{\alpha_i-1})=\prod_{i=1}^{n}p_i^{\alpha_i-1}(p_i-1).$$

定理1.1的证明 注意到,由 $n=p_1^{\alpha_1}\cdots p_t^{\alpha_t}$,以及 e 为 n 的正因数,可知必有

$$e=p_1^{\beta_1}\cdots p_t^{\beta_t},\quad 0\leqslant\beta_i\leqslant\alpha_i,\quad i=1,2,\cdots,t.$$

因此,由定义1.1可知 $\varphi_e(n)$ 等于不超过

$$\left[\frac{n}{e}\right]=\frac{n}{e}=p_1^{\alpha_1-\beta_1}\cdots p_t^{\alpha_t-\beta_t}=\prod_{i=1}^{t}p_i^{\alpha_i-\beta_i},$$

且与 n 互质的正整数的个数.注意到任意的 $\beta_i\leqslant\alpha_i-1$,故对任意正整数 $k\leqslant n/e$ 有

$$\gcd(k,n=\prod_{i=1}^{t}p_i^{\alpha_i})=1\Leftrightarrow$$
$$\gcd(k,\frac{n}{e}=\prod_{i=1}^{t}p_i^{\alpha_i-\beta_i})=1.$$

因此由引理2.1可得

$$\varphi_e(n)=\prod_{i=1}^{t}\varphi(p_i^{\alpha_i-\beta_i})=\prod_{i=1}^{t}p_i^{\alpha_i-\beta_i-1}(p_i-1)=\frac{\prod_{i=1}^{t}p_i^{\alpha_i-1}(p_i-1)}{e}=\frac{\varphi(n)}{e}.$$

这就完成了定理1.1的证明.

定理1.2的证明 1)由定理1.1可知 $\varphi_e(n)=\varphi(n)/e$,因此 $\varphi_e(n)$ 为偶数当且仅当 $\varphi(n)/e$ 为偶数.进而,当 e 为奇数时,$\varphi_e(n)=\varphi(n)/e$ 为偶数当且仅当 $\varphi(n)$ 为偶数.注意到 $\varphi(1)=\varphi(2)=1$,且当 $n\geqslant 3$ 时 $\varphi(n)$ 为偶数.故在满足定理1.1的条件下,$\varphi_e(n)$ 为偶数当且仅当 $n\geqslant 3$.

2)当 $n=2$ 时,$\varphi_2(2)=1/2$ 不是整数.因此 $n\geqslant 3$,此时 $\varphi(n)$ 为偶数且 $\varphi_2(n)=\varphi(n)/2$.从而 $\varphi_2(n)$ 为偶数当且仅当 $4\mid\varphi(n)$.又由 $n=p_1^{\alpha_1}\cdots p_t^{\alpha_t}$ 以及引理2.1可知

$$\varphi(n)=\prod_{i=1}^{t}(p_i^{\alpha_i}-p_i^{\alpha_i-1})=\prod_{i=1}^{t}p_i^{\alpha_i-1}(p_i-1).$$

故若 $t\geqslant 3$,即至少有2个 p_i 为奇质数,此时必有 $4\mid\varphi(n)$.若 $t=1,2$,则有以下2种情形.

情形一 若 n 为偶数,不妨设 $p_1=2$.

若 $t=1$,即 $n=2^\alpha$,则 $4\mid\varphi(n)$ 当且仅当 $8\mid n$,即 $\alpha\geqslant 3$,此即为1).

若 $t=2$,即 $n=2^{\alpha_1}p_2^{\alpha_2}$,其中 p_2 为奇质数,此时

$$\varphi(n)=2^{\alpha_1-1}p_2^{\alpha_2-1}(p_2-1).$$

故当 $\alpha_1=1$ 时,$4\mid\varphi(n)$ 当且仅当 $4\mid p_2-1$;而当 $\alpha_1\geqslant 2$ 时,显然有 $4\mid\varphi(n)$.此即为2).

情形二 若 n 为奇数,则 $p_i(i=1,2)$ 均为奇质数,从而 $2\mid p_i-1$.故当 $t=1$ 时,即 $n=p_1^{\alpha_1}$ 时,$4\mid\varphi(n)$ 当且仅当 $4\mid p_1-1$;而当 $t=2$ 时,显然有 $4\mid\varphi(n)$.此即为3).

这就完成了定理1.2的证明.

3 结束语

本文推广了Cai等[7-8]的部分结果,利用初等数论与组合的方法和技巧,完全确定了一类广义欧拉函数的计算公式,即给出当 e 为 n 的一些特殊类型的正因数时,$\varphi_e(n)$ 的准确计算公式.最后讨论了 $\varphi_e(n)$ 的奇偶性.

要特别说明的是,当正整数 n 的标准分解式为

$$n=p_1^{\alpha_1}\cdots p_t^{\alpha_t}$$

时,熟知 n 的任意正因数形如

$$d=p_1^{\beta_1}\cdots p_t^{\beta_t},\quad 0\leqslant\beta_i\leqslant\alpha_i,\quad 1\leqslant i\leqslant t.$$

而定理1.1中的正因数 e 的表达式中所有指数 $\beta_i\leqslant\alpha_i-1$.这是因为根据定义1.1可知 $\varphi_e(n)$ 为整数,要使得 $\varphi_e(n)=\varphi(n)/e$,则 $\varphi(n)/e$ 也必须要

为整数. 当某个 $\beta_i=\alpha_i$ 时,比如 $\beta_1=\alpha_1$,则由定理 1.1 的证明可知,此时

$$\frac{\varphi(n)}{e}=\left(1-\frac{1}{p_1}\right)\prod_{i=2}^{t}p_i^{\alpha_i-\beta_i-1}(p_i-1).$$

如果 $p_1=\max\{p_1,\cdots,p_t\}$,则上面式子的右边不是整数,从而矛盾.

比如当 $n=50=2\cdot 5^2$ 时,容易计算出 $\varphi(50)=20$. 如果 $e=5$,直接计算知道从 1 到 $n/e=10$ 中与 50 互质的整数恰有 4 个,即 1,3,7,9. 另一方面,由定理 1.1 的公式也可得出

$$4=\varphi_5(50)=\frac{\varphi(50)}{5}=\frac{20}{5}=4.$$

但是,如果 $e=5^2=25$,直接计算知道从 1 到 $\frac{n}{e}=2$ 中与 50 互质的整数恰有 1 个,从而

$$\varphi_{25}(50)=1\neq\frac{\varphi(50)}{25}=\frac{4}{5},$$

4/5 甚至都不是整数.

参考文献

[1] 冯克勤. 初等数论及其应用[M]. 北京:北京师范大学出版社,2003.

[2] 李铁牛,李红达. 基于欧拉函数秘密分享的 RSA 私钥的理性分布计算[J]. 计算机工程与科学,2010,32(9):11-17.

[3] SMITH D C. Fermat's Last Theorem (Case 1) and the Wieferich Criterion[J]. Math Comput,1990,54(190):895-902.

[4] LEHMER E. On congruences involving Bernouli numbers and the quotients of Fermat and Wilson[J]. Ann Math,1938,39:350-359.

[5] CAI T X, FU X D, ZHOU X. A congruence involving the quotients of Euler and its applications(I)[J]. Acta Aritmetica,2002,103(4):313-320.

[6] CAI T X, FU X D, ZHOU X. A congruence involving the quotients of Euler and its applications(II)[J]. Acta Aritmetica,2007,130(3):203-214.

[7] CAI T X, SHEN Z Y, HU M J. On the parity of the generalized Euler function(I)[J]. Adv Math(China),2013,42(4):505-510.

[8] SHEN Z Y, CAI T X, HU M J. On the parity of the generalized Euler function(II)[J]. Adv Math(China),2016,45(4):509-519.

The Explicit Formula for a Special Class of Generalized Euler Functions

LIAO Qunying

(*College of Mathematical Science*, *Sichuan Normal University*, *Chengdu* 610066, *Sichuan*)

Abstract: For a fixed positive integer n, in order to generalize the modulo from the square of prime numbers to the square of an arbitrary integer for the well known Lehmer congruence formula, Cai, et al (CAI T X, FU X D, ZHOU X. Acta Aritmetica, 2002, 130(3):203-214.), defined the generalized Euler function $\varphi_e(n)$ in 2007 and then determined the explicit formulas for $\varphi_e(n)$ ($e=3,4,6$) in 2013 and 2016. The present paper continues the study, obtains the computing formula of $\varphi_e(n)$ for some special divisor e of n, which is a generalization for the corresponding results of Cai, et al, and then gives a sufficient and necessary condition for $2\mid\varphi_e(n)$.

Keywords: Euler function; generalized Euler function; Möbius function

2010 MSC: 11A25; 11B65; 11B68

(编辑　周　俊)