第22卷第3期 数学研究与评论 Vol. 22 No. 3
2002年8月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Aug. 2002

Euler 函数 $\varphi(n)$ 的同余性*

王 瑞
(云南大学信息学院计算机科学系，云南 昆明 650091)

摘 要：本文引入模 p 子系的素化概念，得出 Euler 函数 $\varphi(n)$ 在某些素化系上的整体同余性质，并用于 Lehmer 问题的研究.

关键词：素化子系；幺素系；Lehmer 问题；同余关系.
分类号：AMS(2000) 11C/CLC O156
文献标识码：A **文章编号**：1000-341X(2002)03-0476-05

1 引 言

Euler 函数 $\varphi(n)$ 是重要的数论函数，除 Euler 定理及 $\varphi(n)$ 的计算式外，人们对它的了解甚少. 1932 年，Lehmer, D. H. 提出了一个与 $\varphi(n)$ 有关的著名猜想：[1,2,3]

不存在复合数 n 使得 $\varphi(n)|n-1$.

这个问题非常困难. 1962 年，柯召，孙琦仅证明：这样的复合数如果存在，至少是 12 个不同的奇素数的乘积[2]. 1980 年，Cohen 等利用计算机进一步证明了它至少是 14 个不同的奇素数的乘积[2]. 此后，一直没有什么实质性进展.

本文从研究 $\varphi(n)$ 的同余性出发，得到有关 $\varphi(n)$ 的某些有趣的同余性质和 Lehmer 猜想的若干支持性结果.

2 $\varphi(n)$ 的某些同余性

设 p 是奇素数，A_p 为模 p 的任一缩系，关于模 p 的子系，我们沿用文献[4]，[5]中的定义及符号：即模 p 的 k 次剩余系 $R_p(k)$、k 次非剩余系 $\overline{R}_p(k)$、q 阶系 $S_p(q)$、k 次 r-解系 $T_p^k(r)$、限制 $2k$ 次非剩余系 $\overline{R}_p(2k)_k$、限制 $2k$ 次 σ-解系 $T_p^{2k}(\sigma)$ 等，所不同的是 A_p 及其上述子系不再限制在模 p 的最小正缩系内. 由关于算术数列 $\{an+b\}((a,b)=1)$ 的素数无穷性的 Dirichlet 定理[1,3]，可假设模 p 的各子系中元素均为奇素数，统称为素化子系。

首先，给出

* 收稿日期：2000-02-21
作者简介：王 瑞(1960-)，男，教授.

定理 1 设 $S_p(q)=\{\sigma_1,\cdots,\sigma_{\varphi(q)}\}$[4,5] 是素化的，$q>2, q\mid p-1$，则

$$\varphi(n)\equiv\begin{cases}\gamma\ (\mathrm{mod}p)，\text{如果 } q=\gamma^{\alpha},\gamma \text{ 是素数},\alpha\in N,\\ 1\ (\mathrm{mod}p)，\text{如果 } q \text{ 含两个及以上的不同素因子}.\end{cases}\tag{1}$$

这里 $n=\sigma_1\cdots\sigma_{\varphi(q)}$.

证明 设 $F_q(x)$ 是有理数域 Q 上的 q 阶分圆多项式[1,2]. 由 q 阶系的定义[4,5] 及 $x^q-1=\prod\limits_{d\mid q}F_d(x)$ 的 Möbius 反演公式：[2]$F_q(x)=\prod\limits_{d\mid q}(x^d-1)^{\mu(q/d)}$，这里 $\mu(\cdot)$ 是 Möbius 函数. 不难证明：r 是 p 的 q 阶元的充分必要条件是 $F_q(r)\equiv 0(\mathrm{mod}\ p)$. 即知 $\sigma_1,\cdots,\sigma_{\varphi(q)}$ 是同余式 $F_q(x)\equiv 0(\mathrm{mod}\ p)$ 的全部 $\varphi(q)$ 个不同的解. 故 $\sigma_1,\cdots,\sigma_{\varphi(q)}$ 是同余式

$$G_q(x)=(x-\sigma_1)\cdots(x-\sigma_{\varphi(q)})-F_q(x)\equiv 0(\mathrm{mod}p)\tag{2}$$

的 $\varphi(q)$ 个不同的解. 因为 $F_q(x)$ 是首 1 的 $\varphi(q)$ 次整系数多项式[2,3]，所以 $G_q(x)$ 是次数 $<\varphi(q)$ 的整系数多项式. 故由素模同余式解数的 Lagrange 定理之推论[2,3] 知：$G_q(x)$ 的所有系数均含素因子 p. 于是，对任意整数 m，有

$$G_q(m)\equiv 0(\mathrm{mod}p).\tag{3}$$

特别地，有 $G_q(1)\equiv 0(\mathrm{mod}\ p)$，又由 $q>2$ 知 $2\mid\varphi(q)$. 故

$$\begin{aligned}G_q(1)&=(1-\sigma_1)\cdots(1-\sigma_{\varphi(q)})-F_q(1)=(-1)^{\varphi(q)}(\sigma_1-1)\cdots(\sigma_{\varphi(q)}-1)-F_q(1)\\&=(\sigma_1-1)\cdots(\sigma_{\varphi(q)}-1)-F_q(1)=\varphi(n)-F_q(1)\equiv 0(\mathrm{mod}p).\end{aligned}\tag{4}$$

再由分圆多项式性质[2,3]：

$$F_q(1)=\begin{cases}\gamma，\text{当 } q=\gamma^{\alpha},\ \gamma \text{ 是素数},\alpha\in N,\\ 1，\text{当 } q \text{ 含两个及以上的不同素因子},\end{cases}\tag{5}$$

立得(1)式. □

推论 1.1 对任意给定的奇素数 p，若 $k\not\equiv 0(\mathrm{mod}p)$，则方程

$$k\varphi(n)=n-1\tag{6}$$

在素化系 $S_p(q)(q\mid p-1, 2<q)$ 上均无解 n，这里 $n=S_q(q)$ 的所有元素之积.

证明 由定理 1 的证明，得

$$G_q(0)=(-1)^{\varphi(q)}n-F_q(0)=n-1\equiv 0(\mathrm{mod}p),\tag{7}$$

故若 $n=S_q(q)$ 的所有元素之积为方程(6)的解，即有 $k\varphi(n)\equiv 0(\mathrm{mod}p)$，而 $k\not\equiv 0(\mathrm{mod}p)$，所以 $\varphi(n)\equiv 0(\mathrm{mod}p)$，此与定理 1 的结论矛盾，该推论成立.

推论 1.2 方程

$$2^{\alpha}\varphi(n)=n-1,\alpha\in N\tag{8}$$

在素化系 $S_p(q)(q\mid p-1, q>2)$ 上均无解 n，p 为任意奇素数，$n=S_p(q)$ 的所有元素之积.

证明 仿推论 1.1 即得.

定理 2 设 $T_p^k(r)=\{\tau_1,\cdots,\tau_k\}$[4,5] 是素化的，$r\in R_p(k), k\geqslant 2, k\mid p-1$，则

$$\varphi(n)\equiv(-1)^k(1-r)(\mathrm{mod}p)\tag{9}$$

进一步，有

$$\varphi\left(\frac{n}{\tau_i}\right)\equiv(-1)^{k-1}\frac{1-\tau_i^k}{1-\tau_i}\ (\mathrm{mod}p), i=1,\cdots,k.\tag{10}$$

这里 $n=\tau_1\cdots\tau_k$.

证明 由 k 次 r-解系 $T_p^k(r)$ 的定义[4,5]知，$\forall\ \tau\in T_p^k(r)$，$\tau^k\equiv r(\mathrm{mod}\,p)$. 即 $\tau_1,\tau_2,\cdots,\tau_k$ 是同余式 $x^k-r\equiv 0(\mathrm{mod}\ p)$ 的全部 k 个不同的解. 故 $\tau_1,\cdots,\tau_k$ 是同余式

$$H(x)=(x-\tau_1)\cdots(x-\tau_k)-x^k+r\equiv 0(\mathrm{mod}\,p) \tag{11}$$

的 k 个不同的解. 因为 $H(x)$ 的次数 $<k$，即同余式(11)的解数 $k>H(x)$ 的次数，由关于模 p 的同余式解数的 Lagrange 定理之推论知[2,3]，$H(x)$ 的各项系数均含素因子 p. 故 $\forall\ m\in Z$，有 $H(m)\equiv 0(\mathrm{mod}\,p)$. 特别地，$H(1)\equiv 0(\mathrm{mod}\,p)$，即

$$\begin{aligned}H(1)&=(1-\tau_1)\cdots(1-\tau_k)-1+r=(-1)^k(\tau_1-1)\cdots(\tau_k-1)-1+r\\&=(-1)^k\varphi(n)-(1-r)\equiv 0(\mathrm{mod}\,p).\end{aligned} \tag{12}$$

于是，(9)式成立. 进一步，对任意给定的 $\tau_i\in T_p^k(r)$，由 $\tau_i^k\equiv r(\mathrm{mod}\ p)$ 知，$\tau_1,\cdots,\tau_{i-1},\tau_{i+1},\cdots,\tau_k$ 是同余式

$$\frac{x^k-\tau_i^k}{x-\tau_i}=x^{k-1}+x^{k-2}\tau_i+\cdots+\tau_i^{k-1}\equiv 0(\mathrm{mod}\,p) \tag{13}$$

的全部 $k-1$ 个解，故 $\tau_1,\cdots,\tau_{i-1},\tau_{i+1},\cdots,\tau_k$ 是同余式

$$Q(x)=(x-\tau_1)\cdots(x-\tau_{i-1})(x-\tau_{i+1})\cdots(x-\tau_k)-\frac{x^k-\tau_i^k}{x-\tau_i}\equiv 0(\mathrm{mod}\,p) \tag{14}$$

的 $k-1$ 个不同的解. 又因为 $Q(x)$ 是次数 $<k-1$ 的整系数多项式，再由素模同余式解数的 Lagrange 定理及其推论知，$Q(x)$ 的各项系数均能被 p 整除. 从而，对 $\forall\ m\in Z, m\neq\tau_i$，有 $Q(m)\equiv 0(\mathrm{mod}\,p)$，特别地，$Q(1)\equiv 0(\mathrm{mod}\,p)$. 即

$$\begin{aligned}Q(1)&=(1-\tau_1)\cdots(1-\tau_{i-1})(1-\tau_{i+1})\cdots(1-\tau_k)-\frac{1-\tau_i^k}{1-\tau_i}\\&=(-1)^{k-1}\varphi\left(\frac{n}{\tau_i}\right)-\frac{\tau_i^k-1}{\tau_i-1}\equiv 0(\mathrm{mod}\,p),\end{aligned} \tag{15}$$

即(10)成立，定理得证.

为了陈述下列推论的方便，将适合 $\tau\in T_p^k(1)$，$\tau\equiv 1(\mathrm{mod}\,p)$ 的元素取为奇素数，其余元素为正整数的 k 次 1-解系称为幺素的.

推论 2.1 同余方程

$$n\equiv 1(\mathrm{mod}\,\varphi(n)) \tag{16}$$

在幺素系 $T_p^k(1)(k\mid p-1, 2\mid k)$ 上均无解 n，这里 p 是 >3 的任一素数. $n=T_p^k(1)$ 的所有元素的乘积.

证明 由定理 2 的证明，得

$$H(0)=(-1)^k n-(-1)=n+1\equiv 0(\mathrm{mod}\,p), n=\tau_1\cdots\tau_k, 2\mid k, \tag{17}$$

$$(\tau_1-1)\cdots(\tau_k-1)\equiv 0(\mathrm{mod}\,p), \tag{18}$$

这里 $T_p^k(1)=\{\tau_1,\cdots,\tau_k\}$. 由关于 $T_p^k(1)$ 幺素的假设，不妨设 $\tau_1\equiv 1(\mathrm{mod}\,p)$，故知 τ_1 是奇素数，从而，有 $p\mid\varphi(n)$，$n=\tau_1\cdots\tau_k$，若(16)成立，得

$$n\equiv 1(\mathrm{mod}\,p) \tag{19}$$

此与(17)式矛盾. 推论得证.

推论 2.2 设 p 是奇素数，$D\equiv -1$，或 $1(\mathrm{mod}\,p)$，且 D 含 $pt+1$ 型素因子，则同余式

$$Dn\equiv\pm 1(\mathrm{mod}\,\varphi(Dn)) \tag{20}$$

在 $T_p^k(r)$ 上无解 n，这里 $(\mathrm{mod}p)-1, 1 \not\equiv r \in R_p(k), n = T_p^k(r)$ 的所有元素的乘积.

证明 由定理 2 的证明，可知

$$n \equiv (-1)^{k+1} r (\mathrm{mod}p). \tag{21}$$

因为 $r \not\equiv -1, 1(\mathrm{mod}p)$，所以无论 k 是奇数还是偶数，都有 $n \not\equiv -1, 1(\mathrm{mod}p)$. 从而，有 $Dn \not\equiv -1, 1(\mathrm{mod}p)$，但 $\varphi(Dn) \equiv 0(\mathrm{mod}p)$，此与(20)式相悖，推论成立.

下一个定理给出了 $\varphi(n)$ 和 $\sigma(n)$ 之间一个奇妙的同余关系.

定理 3 设 $T_p^k(r_i)$ 是素化系，$r_i \in R_p(k), i = 1, \cdots, (p-1)/k$，则

$$\varphi(n/L) \equiv (-1)^{\frac{(k-1)(p-1)}{k}} \sigma(L^{k-1}) (\mathrm{mod}p), \tag{22}$$

这里 L 是从 $T_p^k(r_i)(i = 1, \cdots, \frac{p-1}{k})$ 中分别取出一个元素所做的积，称为 k 次解类积；$n = \bigcup_{i=1}^{(p-1)/k} T_p^k(r_i)$ 的所有元素之积；$\varphi(m)$ 是 Euler 函数，$\sigma(m)$ 是 m 的诸正整因子之和.

证明 令 $A_p = \bigcup_{i=1}^{(p-1)/k} T_p^k(r_i), r_i \in R_p(k)$. 由 $R_p(k)$ 及 $T_p^k(r)$ 的定义[4,5]，不难知道：$T_p^k(r_1), \cdots, T_p^k(r_{(p-1)/k})$ 是模 p 缩系 A_p 的一个分类. 即 A_p 是模 p 的素化缩系，且 $T_p^k(r_i) \cap T_p^k(r_j) = \varnothing$，$r_i \not\equiv r_j(\mathrm{mod}p)$. 现令 $L = \prod_{i=1}^{(p-1)/k} \tau^{(i)}, \tau^{(i)} \in T_p^k(r_i), n_i = T_p^k(r_i)$ 的所有元素之积，由定理 2 的(10)式，得

$$\varphi\left(\frac{n}{L}\right) = \prod_{i=1}^{(p-1)/k} \varphi\left(\frac{n_i}{\tau^{(i)}}\right) \equiv (-1)^{\frac{(k-1)(p-1)}{k}} \prod_{i=1}^{(p-1)/k} \frac{(\tau^{(i)})^k - 1}{\tau^{(i)} - 1}$$

$$= (-1)^{(k-1)(p-1)/k} \sigma(L^{k-1}) (\mathrm{mod}p), \tag{23}$$

即(22)式成立. 定理得证.

一般地，有

定理 4 设 $T_p^{a_1}(r_1), \cdots, T_p^{a_s}(r_s)$ 是两两不相交的素化系，则

$$\varphi\left(\frac{n_1 n_2 \cdots n_s}{\tau_1 \tau_2 \cdots \tau_s}\right) \equiv (-1)^{a_1+a_2+\cdots+a_s-s} \sigma(\tau_1^{a_1-1} \cdots \tau_s^{a_s-1}) \ (\mathrm{mod}p), \tag{24}$$

这里 $n_i = T_p^{a_i}(r_i)$ 的所有元素之积，$\tau_i \in T_p^{a_i}(r_i), i = 1, \cdots, s$.

证明 仿定理 3 的证明即得.

推论 4.1 在定理 4 的假设下，若 $\frac{n_1 n_2 \cdots n_s}{\tau_1 \tau_2 \cdots \tau_s}$ 含有形如 $pt+1$ 的素因子，且 $\tau_1^{a_1-1} \cdots \tau_s^{a_s-1} \not\equiv (-1)^{a_1+\cdots+a_s-s} (\mathrm{mod}p)$，则 $\varphi\left(\frac{n_1 \cdots n_s}{\tau_1 \cdots \tau_s}\right) \nmid \frac{n_1 \cdots n_s}{\tau_1 \cdots \tau_s} - 1$.

证明 由假设及定理 2 可知 $p \mid \varphi\left(\frac{n_1 \cdots n_s}{\tau_1 \cdots \tau_s}\right), p \nmid \frac{n_1 \cdots n_s}{\tau_1 \cdots \tau_s} - 1$，即知该推论成立.

3 其他

仿第 2 节的方法，我们对模 p 的其他素化子系可得相应的 Euler 函数 $\varphi(n)$ 的同余性质. 下面仅给出结论，其证明略去.

定理 5 设 $\overline{R}_p(k)$ 是素化的[4,5,6]，$k \mid p-1, k > 1$，则

$$\varphi(n) \equiv (-1)^{\frac{(k-1)(p-1)}{k}} k \pmod{p} \tag{25}$$

这里 $n = \overline{R}_p(k)$ 的所有元素之积.

定理 6 设 $\overline{R}_p(2k)_t$ 是素化的[4,5],则

$$\varphi(n) \equiv (-1)^{\frac{p-1}{2k}} 2 \pmod{p} \tag{26}$$

这里 $n = \overline{R}_p(2k)_t$ 的所有元素之积. 等等.

参考文献:

[1] 华罗庚. 数论导引[M]. 北京: 科学出版社,1979.
HUA Lo-Keng. *Introduction to Number Theory* [M], Beijing: Science Press, 1979, (in Chinese)

[2] 柯 召,孙 琦. 数论讲义(上、下册)[M]. 北京: 高等教育出版社,1986.
KE Zhao, SUN Qi. *Lectures on Number Theory* [M]. Beijing: Advanced Education Press, 1986. (in Chinese)

[3] IRELAND K, ROSON M. *A classical introduction to modern number theory* [M]. NewYork: Spring-Verlag, 1982.

[4] WANG Rui. *Congruence relations for its subsystem of residue with mod p* [J]. Acta. Math. Sinica. 1997, **40**(6):947—950. (in Chinese)

[5] WANG Rui. *Combin-congruence law with power modules of prime* [J]. J. Math. Res & Exp., 2000, **20**(2). (in Chinese)

[6] WANG Rui. *Some structures of irreducible polynomials over UFD R* [J]. J. Math. Res. & Exp., 1999. **19**(2): 367—373. (in Chinese)

Congruence Properties of Euler's Function $\varphi(n)$

WANG Rui

(Dept. of Computer Science, Information College, Yunan University, Kunming 650091, China)

Abstract: In this paper, prime-subsystems with mod p are introducted, and congruence relations of Euler's function $\varphi(n)$ for some prime-subsystems are given. These properties are used for Lehmer's problem.

Key words: prime-subsystem; unite prime subsystem; Lehmer's conjecture; congruence relation.