第10卷 第2期 华东交通大学 Vol. 10 No. 2
1993年 6月 Journal of East China Jiaotong University Jun. 1993

计算正整数模的平方剩余个数的公式

凌鄂生 李鹤年

（宣传部） （宜春师专）

摘 要

$\varphi(m)$ 是正整数 m 的欧拉函数值，当 m 的标准分解式是 $m=2^{\alpha}p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$，$\alpha=0$ 或 1 时，m 的平方剩余的个数是 $\varphi(m)\div 2^n$ 个。当 m 的标准分解式是 $m=2^{\alpha}p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ 时，m 的平方剩余的个数是 $\varphi(m)\div 2^{n+1}$ 个。当 m 的标准分解式是 $m=2^{\alpha}p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$，$\alpha>2$ 时，m 的平方剩余的个数是 $\varphi(m)\div 2^{n+2}$ 个。

关键词：欧拉函数；正整数的标准分解式；平方剩余；平方非剩余；简化剩余系；原根

对于一个已知的正整数 m，它有多少个平方剩余和平方非剩余？它们的个数与 m 有何关系？本文将给出一个公式来解决这些问题。有了这样一个公式，在需要求出 m 的全部平方剩余或全部平方非剩余时可以减少重复计算而且在理论上也有一定的价值。

若给出了同余方程 $x^2\equiv a \pmod m$，$(a, m)=1$ (1)

并且假设它有解，p_1，p_2，…，p_n 是 m 的两两不相等的全部奇素因数，$n\geqslant 0$。

众所周知，（Ⅰ）若 $m=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ 或 $m=2^{\alpha}p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ 是模 m 的标准分解式，则同余方程 (1) 式的解的个数是 2^n 个。（Ⅱ）若 $m=2^{\alpha}p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ 是模 m 的标准分解式，则同余方程 (1) 式的解的个数是 2^{n+1} 个。（Ⅲ）若 $m=2^{\alpha}p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$，$\alpha\geqslant 3$ 是模 m 的标准分解式，则同余方程 (1) 式的解的个数是 2^{n+2} 个。

本文中将要涉及的欧拉函数 $\varphi(m)$ 是指小于 m 的非负整数 0，1，2，…，m−1 中与 m 互质的数的个数。众所周知，若 $m=q_1^{\beta_1}q_2^{\beta_2}\cdots q_n^{\beta_n}$ 是 m 的标准分解式时，$\varphi(m)=q_1^{\beta_1-1}q_2^{\beta_2-1}\cdots q_n^{\beta_n-1}(q_1-1)(q_2-1)\cdots(q_n-1)$。

定理 正整数 $m>1$ 时，欧拉函数 $\varphi(m)=m$ 的平方剩余的个数$\times 2^i$，其中（Ⅰ）m 的标准分解式是 $m=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ 或 $m=2p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ 时 $i=n$。（Ⅱ）m 的标准分解式是 $m=2^2p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ 时，$i=n+1$。（Ⅲ）m 的标准分解式是 $m=2^{\alpha}p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$，$\alpha\geqslant 3$ 时，$i=n+2$。

证明 （Ⅰ）作同余方程 (1) 式。由于 (1) 式是有解的，并且 $m=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ 或 $m=2p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_n}$ 是模 m 的标准分解式，因此，由以上所述可知 (1) 式对模 m 来说有 2^n 个解。又因为

本文于 1992 年 12 月 11 日收到

$(a, m)=1$，所以使（1）式成立的任一整数 x_0 一定适合 $(x_0, m)=1$。由此可知（1）式中模 m 的任一简化剩余系中必有 2^n 个数使同余方程（1）式成立。

众所周知，使同余方程（1）式有解的整数 a 称为（1）式的模 m 的平方剩余。又设 b 是模 m 的另一平方剩余，并且 $a\not\equiv b\ (\mathrm{mod}m)$。根据以上所证可知，在模 m 的任一简化剩余系中也有 2^n 个数 x_1 使 $x_1^2\equiv b\ (\mathrm{mod}m)$ 成立。

由于 $a\not\equiv b\ (\mathrm{mod}m)$，所以使 $x_0^2\equiv\ (\mathrm{mod}m)$ 和 $x_1^2\equiv\ (\mathrm{mod}m)$ 成立的 x_0 和 x_1 一定适合 $x_0\not\equiv x_1\ (\mathrm{mod}m)$，否则，显然与 $a\not\equiv b\ (\mathrm{mod}m)$ 矛盾。

再设 m 的平方剩余总共有 $t\geqslant 1$ 个，把它们记为 $a_1, a_2, a_3, \cdots a_t$，再用它们作 t 个同余方程：$x^2\equiv a_1\ (\mathrm{mod}m)$，$x^2\equiv a_2\ (\mathrm{mod}m)$，…，$x^2\equiv a_t\ (\mathrm{mod}m)$　　(2)

根据以上的证明知道，这 t 个同余方程的每一个方程在模 m 的同一简化剩余系中都分别有 2^n 个数使其成立。又因为当 $i\neq j$ 时，$a_i\not\equiv a_j\ (\mathrm{mod}m)$，$1\leqslant i, j\leqslant t$，所以在模 m 的同一个简化剩余系里分别使（2）式中不同的同余方程成立的数关于模 m 是两两不同余的。这样一来就证明了模 m 的同一个简化剩余系里共有 $2^n t$ 个数分别使（2）式的每一个同余方程成立。另一方面，模 m 的任一简化剩余系中任何一个数一定使（2）式的一个同余方程成立。众所周知，模 m 的任一简化剩余系中共有 $\varphi(m)$ 个数，故以上所证表明了 $\varphi(m)=2^n t$ 成立。这就证明了本定理的（Ⅰ）式成立。

同理可证本定理的（Ⅰ）式和（Ⅱ）式成立。

推论 1　在上述定理的假设条件下，（Ⅰ）当 $m=2p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ 或 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ 时，模 m 的平方剩余的个数是 $\varphi(m)\div 2^n$ 个，平方非剩余的个数是 $\varphi(m)(1-2^{-n})$ 个；（Ⅱ）当 $m=2^2p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ 时，模 m 的平方剩余的个数是 $\varphi(m)\div 2^{n+1}$，平方非剩余的个数是 $\varphi(m)(1-2^{-n-1})$ 个；（Ⅲ）当 $m=2^\alpha p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$，$\alpha\geqslant 3$ 时，模 m 的平方剩余的个数是 $\varphi(m)\div 2^{n+2}$ 个，平方非剩余的个数是 $\varphi(m)(1-2^{-n-2})$ 个。

推论 2　当 $m=p^\alpha$ 或 $m=2p^\alpha$ 是模 m 的标准分解式，并且 p 是奇素数时，模 m 的平方剩余的个数是 $\frac{1}{2}\varphi(m)$ 个，平方非剩余的个数也是 $\frac{1}{2}\varphi(m)$ 个。

推论 3　当 p 为奇素数，$\alpha>0$ 时，只有 $m=4$，$m=p^\alpha$ 或 $2p^\alpha$ 时，模 m 的平方剩余的个数才与它的平方非剩余的个数相等。否则，除 $m=2$ 外，模 m 的平方剩余的个数都小于它的平方非剩余的个数。

因为只有 $n=0$ 时，$2^{-n}\varphi(m)>(1-2^{-n})\varphi(m)$，这时 $m=2$。只有 $n=1$ 时，$2^{-n}\varphi(m)=(1-2^{-n})\varphi(m)$，这时 $m=p^\alpha$ 或 $m=2p^\alpha$。当 $n>1$ 时，$2^{-n}\varphi(m)<(1-2^{-n})\varphi(m)$。

因为，只有 $n=0$ 时，$2^{-n-1}\varphi(m)=(1-2^{-n-1})\varphi(m)$，这时 $m=4$。当 $n>0$ 时，$2^{-n-1}\varphi(m)<(1-2^{-n-1})\varphi(m)$。

因为，当 $n\geqslant 0$ 时，$2^{-n-1}\varphi(m)<(1-2^{-n-1})\varphi(m)$。

推论 4　只有 $m=2, 3, 4, 6, 8, 12, 24$ 时，模 m 的平方剩余只有一个数为 1。只有模 $m=2$ 时，m 没有平方非剩余。

因为，$2^{-n}\varphi(m)=2^{-n}p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_n^{\alpha_n-1}(p_1-1)(p_2-1)\cdots(p_n-1)=1$ 成立。只有 $n=0$ 时，$m=2$ 和 $n=1$，$\alpha_1=1$，$p_1=3$ 时，$m=3, 6$ 这两种情况。

因为 $2^{-n-1}\varphi(m)=2^{-n}p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_n^{\alpha_n-1}(p_1-1)(p_2-1)\cdots(p_n-1)=1$ 成立，只有 $n=0$ 时 $m=4$ 和 $n=1$，$\alpha_1=1$，$p_1=3$ 时，$m=12$ 这两种情况。

因为 $2^{-n-2}\varphi(m)=2^{\alpha-n-3}p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_n^{\alpha_n-1}(p_1-1)(p_2-1)\cdots(p_n-1)=1$ 成立，只有 $n=0$，$\alpha=3$ 时，$m=8$ 和 $n=1$，$\alpha_1=1$，$\alpha=3$，$p_1=3$ 时，$m=24$ 这两种情况。

因为 $n\geqslant 0$，要使 $(1-2^{-n})\varphi(m)=(1-2^{-n-1})\varphi(m)=(1-2^{-n-2})\varphi(m)=0$ 成立，只有 $n=0$ 时，$(1-2^{-n})\varphi(m)=0$ 成立，这时 $m=2$，所以，只有模 $m=2$ 没有平方非剩余。

推论 5 当 $m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$，并且 $\alpha>3$ 是 m 的标准分解式时，模 m 的平方剩余的个数是偶数。

因为，$\alpha>3$ 时，$2^{-n-2}\varphi(m)=2^{\alpha-n-3}p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_n^{\alpha_n-1}(p_1-1)(p_2-1)\cdots(p_n-1)$ 总是偶数。

推论 6 当 $m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$，并且 $\alpha=0$，1，2，3 是模 m 的标准分解式时，（Ⅰ）若其中有一个奇素因数 $p_i=4t+1$　$1\leqslant i\leqslant n$，则模 m 的平方剩余的个数是偶数；（Ⅰ）若其中所有的奇素因数 $p_i=4t+3$，$i=1$　2，…，n，则模 m 的平方剩余的个数是奇数。

因为，这时模 m 的平方剩余的个数都是公式 $2^{-n}p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_n^{\alpha_n-1}(p_1-1)(p_2-1)\cdots(p_n-1)$ 计算的结果。由此可见：（Ⅰ）若其中有一个奇素因数 $p_i=4t+1$，$1\leqslant i\leqslant n$，则计算的结果显然是偶数；（Ⅰ）若其中所有的奇素因数都是 $p_i=4t+3$，$i=1$，2，…，n，则计算的结果显然是奇数。

众所周知，模 $m>1$ 有原根的充分与必要条件是 $m=2$，4，p^{α}，$2p^{\alpha}$，其中 p 为奇素数。

推论 7 当整数 $m>2$ 时，模 m 有原根的充分与必要条件是模 m 的平方剩余的个数与它的平方非剩余的个数相等。

由推论 1 和推论 4 显然又可得下面的结果。

推论 8 模 m 的平方剩余的个数可以整除它的平方非剩余的个数，并且除 $m=2$ 外，平方非剩余的个数是平方剩余的个数的奇数倍。

利用推论 3 来证明模 $m>2$ 有原根的必要条件是 $m=4$，p^{α}，$2p^{\alpha}$ 显得特别简单。

定理 当 $m>2$ 时模 m 有原根的必要条件是 $m=4$，p^{α}，$2p^{\alpha}$，其中 p 是奇素数。

证明 设 m 有原根 g，那么 g 是平方非剩余，并且 $g, g^2, \cdots, g^{\varphi(m)}$ 是模 m 的简化剩余系，又因为 $m>2$，所以，$\varphi(m)$ 是偶数。这样一来，在这个简化剩余系中 $\frac{1}{2}\varphi(m)$ 个数：$g^2, g^4, \cdots, g^{\varphi(m)}$ 都是模 m 的平方剩余。另外 $\frac{1}{2}\varphi(m)$ 个数：$g, g^3, \cdots g^{\varphi(m)-1}$ 都是模 m 的平方非剩余。因此由推论 3 得 $m=4$，p^{α}，$2p^{\alpha}$．其中 p 是奇素数。

参 考 文 献

[1] 柯召，孙琦．数论讲义．第三版，北京：高等教育出版社，1988：第一册 30～93
[2] 陈景润．初等数论．北京：科学出版社，1978：第 2 册 78～87

The Formula for the Numbers of Quadretic Residue of Positive Integers

Iing Esheng　　Li Henian

ABSTRACT

$\varphi(m)$ is Euler function. If $m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, that is the standard facorization of m, and $\alpha=0$ or 1, then a Quadratic residue of m is $\varphi(m) \div 2^n$. If $m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, m has $\varphi(m) \div 2^{n+1}$. If $m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, and $\alpha>2$, then m has $\varphi(m) \div 2^{n+2}$

Key words: Euler Function; the Standard Factorization of Positive Integers; Quadratic Residue; Quadratic Non－residue; Simplified Residue System; Primitive Root