DOI: 10.13718/j.cnki.xdzk.2019.01.009

两种求二次剩余平方根算法的比较①

蔡兆政[1]，　瞿云云[2]，　包小敏[1]

1. 西南大学 数学与统计学院，重庆 400715；2. 贵州师范大学 数学与计算机科学学院，贵阳 550001

摘要：在模是大合数的情况下，求二次剩余平方根是一个困难问题. 目前已知的求二次剩余平方根的算法有两种，本文对 Cocks 和曹珍富的算法进行分析比较，结果表明由 Cocks 提出的算法效率更高，这对今后求二次剩余平方根时进行算法选择提供了帮助.

关　键　词：模；二次剩余；平方根；中国剩余定理

中图分类号：O211.4　　**文献标志码**：A　　**文章编号**：1673-9868(2019)01-0060-05

二次剩余是数论中的一个基本术语，高斯在其著作《算术研究》中就曾对其进行过讨论，其定义如下：

定义 1　设 $a \in Z_n^*$，其中 $Z_n^* = \{r \mid 1 \leqslant r < n, \gcd(r, n) = 1\}$. 若存在 $x \in Z_n^*$ 使得 $x^2 \equiv a \bmod n$，则称 a 是模 n 的二次剩余. 所有模 n 的二次剩余做成的集合记为 $QR(n) = \{x^2 \bmod n \mid x \in Z_n^*\}$.

当 n 是奇素数时，下面的定理给出了一个判别一个整数 a 是否是二次剩余的简单方法：

定理 1(欧拉准则)　设 p 是一个奇素数，则 a 是二次剩余当且仅当

$$a^{\frac{1}{2}} \equiv 1 \bmod p$$

当 n 是合数时，若不知道 n 的素因子分解，则判断一个整数 a 是否是二次剩余是困难的[1-4]；若知道 n 的素因子分解 $n = \prod_{i=1}^{k} p_i^{e_i}$，其中 p_i 为不同的素数，e_i 为正整数，$\gcd(a, n) = 1$，则可以通过计算 Jacobi 符号 $\left(\frac{a}{n}\right)$ 来判断 a 是否是二次剩余的(当且仅当所有的 Legendre 符号 $\left(\frac{a}{p_i}\right) = 1$，$a$ 是二次剩余的).

定义 2(Legendre 符号)　对于奇素数 m，若 $x^2 \equiv a \bmod \{m\}$ 有解，则记 $\left(\frac{a}{m}\right) = 1$；若 $a \mid m$，则记 $\left(\frac{a}{m}\right) = 0$；否则记 $\left(\frac{a}{m}\right) = -1$.

对于 $n = pq$，其中 p 和 q 是不同的奇素数，我们做如下标记：

$$\left(\frac{x}{n}\right) = \begin{cases} 0 & \gcd(x, n) > 1 \\ 1 & \left(\frac{x}{p}\right)\left(\frac{x}{p}\right) = 1\} \\ -1 & \left(\frac{x}{p}\right)\left(\frac{x}{p}\right) = -1 \end{cases}$$

显然，x 是模 n 的二次剩余等价于 $\left(\frac{x}{p}\right) = \left(\frac{x}{p}\right) = 1$.

① 收稿日期：2018-05-18

基金项目：国家自然科学基金项目(61462016)；贵州省科学技术基金项目(黔科合 J 字[2014]2125 号)；贵州省教育厅青年科技人才成长项目(黔教合 KY 字[2016]130.

作者简介：蔡兆政(1993-)，硕士研究生，主要从事编码理论和密码学的研究.

通信作者：包小敏，博士，教授，主要从事密码学和信息安全的研究.

定义 3(Jacobi 符号) 设 n 是一个奇正整数，n 的素因数分解如下

$$n=\prod_{i=1}^{k}p_i^{e_i}$$

对任意整数 a 定义 Jacobi 符号如下

$$\left(\frac{a}{n}\right)=\prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{e_i}$$

其中 $\left(\frac{a}{p_i}\right)$ 是 Legendre 符号. Jacobi 符号是 Legendre 符号的推广，需要注意的是，如果 $\gcd(a,n)>1$，那么 $\left(\frac{a}{n}\right)=0$；如果 $\left(\frac{a}{n}\right)=-1$，那么 a 是二次非剩余；但是 $\left(\frac{a}{n}\right)=1$ 时不能确定 a 是否为二次剩余，只有对于所有的 $\left(\frac{a}{p_i}\right)=1$ 成立时，a 是二次剩余.

1 模平方根的计算

本节讨论模平方根的计算问题. 设 a 是模 n 的二次剩余，根据模 n 分以下几种情况讨论计算 $a \bmod n$ 的平方根.

设 n 是一个奇素数，$a\in Z_n^*$，且 $\left(\frac{a}{n}\right)=1$. 首先考虑特殊情况，当 $p\equiv 3 \bmod n$ 时，$\frac{p+1}{4}$ 是整数

$$a=aa^{\frac{1}{2}}=a^{\frac{p+1}{2}}=(a^{\frac{p+1}{4}})^2$$

所以 $a^{\frac{p+1}{4}}$ 是 a 模 n 的一个平方根. 一般情况下，设 $p-1=2^h m$，其中 m 为奇数，$a\in (Z_n^*)^2$，$\gamma\in Z_n^*\backslash(Z_n^*)^2$. 对任意的 $\delta\in Z_n^*$，δ^m 的阶整除 2^h；因为 $a^{2^{h-1}m}=1$，所以 a^m 的阶整除 2^{h-1}；而 $\gamma^{2^{h-1}m}=-1$，则 γ^m 的阶恰好为 2^h. 生成元为 γ^m 的群是 Z_n^* 阶为 2^h 的子群，则存在偶数 $x(0\leqslant x<n)$，使得 $a^m=\gamma^{mx}$. 令 $k=\gamma^{\frac{mx}{2}}$，则 $k^2=\gamma^{mx}=a^m$. 由于 m 为奇数，设 $m=2t+1$，其中 t 为非负整数，而

$$(ka^{-t})^2=k^2a^{-2t}=a^m a^{-2t}=a^{m-2t}=a$$

即 ka^{-t} 为 $a \bmod n$ 的一个平方根.

若已知 n 的素因子分解，则由下面的定理 2，根据模为素数的情形分别求出模每个素因子的平方根，然后利用中国剩余定理求得模 n 的平方根.

定理 2[4] 设奇数 n 的因式分解为

$$n=\prod_{i=1}^{l}p_i^{e_i}$$

其中 $p_1,\cdots,p_l$ 为不同的素数，且 e_i 为正整数. 若 $\gcd(a,n)=1$，则当 $\left(\frac{a}{p_i}\right)=1$ 对于所有的 $i\in\{1,\cdots,l\}$ 成立时，$x^2\equiv a \bmod n$ 有 2^l 个解，其它情形没有解.

当模 n 为合数时，若 n 的素因子分解未知，则求模 n 的平方根是困难的[1-3]. 实际上我们有：

定理 3 求模 n 平方根的难度与分解 n 的难度是等价的，其中 n 是一个奇合数.

证 如果存在分解 n 素因子的多项式时间算法，那么根据定理 2 可以在多项式时间内计算出模 n 的平方根. 现假设存在一个计算模 n 平方根的多项式时间算法. 为了分解 n，首先检验 n 不是完全幂数，然后随机选取一个整数 $y\in Z_n^*$，令 $a=y^2 \bmod n$，利用假定的模 n 平方根算法求得一个 $x\in Z_n^*$，使得 $x^2\equiv a \bmod n$，即有 $x^2\equiv y^2 \bmod n$. 显然，x 和 y 的公因子是 n 的因子. 假设 x 和 y 互素. 如果 p 是 n 的一个因子，那么 p 整除 $x^2-y^2=(x+y)(x-y)$. p 要么整除 $x+y$ 或 $x-y$；要么同时整除两个因子，即 p 整除 $2x$ 和 $2y$. 由于 y 是随机的，则整除 x^2-y^2 的奇素数都有 $\frac{1}{2}$ 的概率整除 $x+y$ 或 $x-y$，且任意两个素数会有 $\frac{1}{2}$ 的概率整除不同的因子. 在这样的情况下，$\gcd(x-y,n)$ 可能是 n 的非平凡因子；若 $\gcd(x-y,n)$ 不是 n 的非平凡因子，则重新随机选取 y. 经过 k 次计算后，不能分解 n 的概率为 2^{-k}，那么存在分解 n 素因子的

多项式时间算法. 因此，求模 n 平方根的难度与分解 n 的难度是等价的.

在以下的讨论中，我们假设模 n 是一个特殊的整数- Blum 整数.

定义 4　若 p，q 是不同的奇素数，且 $p \equiv q \equiv 3 \bmod 4$，则称 $n = pq$ 为 Blum 整数.

由定理 2，同余方程 $x^2 \equiv a \bmod n$ 的解等价于同余方程组

$$\begin{cases} x \equiv a \bmod p \\ x \equiv a \bmod q \end{cases}$$

的解. 首先考虑 $x^2 \equiv a \bmod p$ 的解. 如果 $x^2 \equiv a \bmod p$ 有解，那么根据欧拉准则有 $a^{\frac{1}{2}} \equiv 1 \bmod p$，根据同余方程的性质，两边同乘以 a 得 $a \cdot a^{\frac{1}{2}} \equiv a \bmod p$，即 $a^{\frac{p+1}{2}} \equiv 1 \bmod p$，从而 $a^{\left(\frac{p+1}{4}\right)^2} \equiv 1 \bmod p$，又因为 $p \equiv 3 \bmod 4$，则 $\dfrac{p+1}{4}$ 是整数，所以 $x \equiv \pm a^{\frac{p+1}{4}} \bmod p$ 是 $x^2 \equiv a \bmod p$ 的两个解. 于是同余方程组有 4 个解. 而在 $QR(n)$ 中仅有一个为 $a^{\frac{1}{2}\left(\frac{\phi(n)}{4}+1\right)} \bmod n$，称作 a 的主平方根[4]，其中 $\phi(\cdot)$ 表示欧拉函数.

2　两种求二次剩余平方根的算法

文献[5－6]给出了两种求解二次剩余平方根的算法.

算法 1[5]

Input：大素数 p，q，整数 l，以及 s_{l+1}

Output：s_0

$a_1 \leftarrow \left(\dfrac{p+1}{4}\right)^{l+1} \bmod (p-1)$；

$a_2 \leftarrow \left(\dfrac{q+1}{4}\right)^{l+1} \bmod (q-1)$；

$b_1 \leftarrow s_{l+1}^{\,a_1} \bmod p$；

$b_2 \leftarrow s_{l+1}^{\,a_2} \bmod q$；

$s_0 \leftarrow CRT(b_1, b_2, p, q)$；//CRT 表示利用中国剩余定理求解的函数

return s_0

算法 2[6]

Input：大素数 p，q，整数 l，以及 s_{l+1}

Output：s_0

$w \leftarrow \left(\dfrac{\frac{\phi(n)}{4}+1}{2}\right)^{l+1} \bmod \phi(n)$

$s_0 \leftarrow s_{l+1}^{w} \bmod (p \times q)$；

return s_0

从表面上看，算法 2 的运算步骤简洁、直观；而算法 1 从表面上看起来不太直观，且运算比较繁杂，这是否说明算法 2 比算法 1 的效率高？接下来先对两种算法进行简单的介绍. 两种算法都是从 $s_{l+1} = s_0^{2^{l+1}} \bmod n$ 中计算出 s_0，每个 s_{i-1} 是 s_i 的主平方根. 分析算法 2，由前面的介绍可知 $s_{l+1} \bmod n$ 的主平方根为 $s_{l+1}^{\frac{1}{2}\left(\frac{\phi(n)}{4}+1\right)} \bmod n$，则 $s_{l+1}^{\left(\frac{1}{2}\left(\frac{\phi(n)}{4}+1\right)\right)^{l+1}} \bmod n$ 是 $s_{l+1} \bmod n$ 的 $l+1$ 次主平方根. 因为 Z_n^* 的阶为 $\phi(n)$，所以先模 $\phi(n)$ 约化指数 $\left(\dfrac{1}{2}\left(\dfrac{\phi(n)}{4}+1\right)\right)^{l+1}$，降低模指数运算的指数，然后计算得到 $s_{l+1} \bmod n$ 的 $l+1$ 次主平方根 s_0. 在算法 1 中，同样分别用模 $(p-1)$ 和模 $(q-1)$ 约化指数 $\left(\dfrac{p+1}{4}\right)^{l+1}$ 和 $\left(\dfrac{q+1}{4}\right)^{l+1}$，首先计算 s_{l+1} 模 p 和模 q 的 $l+1$ 次主平方根，然后使用中国剩余定理来计算 $s_{l+1} \bmod n$ 的 $l+1$ 次主平方根. 在下一节中，

将分析比较两种不同算法的运算次数，从理论层面分析比较这两种算法.

3 两种算法的分析比较

不难发现算法1与算法2主要进行了模整数的指数运算，由于 $p,q,n,\phi(n)$ 都很大，必须用多精度算术来执行 Z_n 上的运算，所需的时间将依赖于它们的二进制表示数位. 因为是选取差别很小的 p 和 q，所以设 p 和 q 是 $m=\lfloor \log_2 p \rfloor+1$ 位的大素数，则 n 和 $\phi(n)$ 约为 $2m$ 位的整数. 对于模指数运算 $x^c \bmod n$ 平均需要运行 $l-1$ 次模平方运算和 $\frac{3}{2}(l-1)$ 模乘运算，l 为 c 的二进制表示长度[7]. 假设计算机的计算位长为 w，则某个整数 r 在基 $W=2^w$ 表示下的长度 s 满足 $r=2^{ws}$. 那么在一次模平方运算中需要运行 $\frac{3}{2}s^2+\frac{1}{2}s$ 次乘法和 $3s^2+9s+3$ 次加法；在一次模乘法运算中要运行 $2s^2+s$ 次乘法和 $4s^2+4s+2$ 次加法，其中 s 为模在基 $W=2^w$ 表示下的长度[8-9]. 下面我们利用这些结论分别计算算法1和算法2的运行次数.

为了表述方便，令 $t=\log_2\{(l+1)\}-1$. 在算法1中，第一步，$p-1$ 为 m 位，则需要 t 次模平方运算和 $\frac{3}{2}t$ 次模乘运算，即 $t\left(\frac{9}{2}s^2+2s\right)$ 次乘法运算，$t(9s^2+15s+6)$ 次加法运算. 第一、二步的计算近似. 第三步，a_1 平均为 m 位，则需要 $(m-1)\left(\frac{9}{2}s^2+2s\right)$ 次乘法和 $(m-1)(9s^2+15s+6)$ 次加法. 第四步与第三步同理. 第五步，首先要计算 q 在 $Z_p{}^*$ 中的逆元 ${}_pq^{-1}$ 和 p 在 Z_q^* 中的逆元 ${}_qp^{-1}$，再计算 $(q_pq^{-1}b_1+p_qp^{-1}b_2)\bmod n$，现有的较好的模逆算法是Plus-minu扩展欧几里得算法[10]，最多需要 m^2 次加减法运算. 可得算法1求解 s_0 需要 $(t+m-1)(9s^2+4s)$ 次乘法运算，$(t+m-1)(18s^2+30s+12)+m^2$ 次加法运算.

用同样的方法计算得到算法2求解 s_0 需要 $(t+2m-1)\left(\frac{9}{2}\dot{s}^2+4\dot{s}\right)$ 次乘法运算，$(t+2m-1)(9\dot{s}^2+15\dot{s}+6)$ 次加法运算. 由于模 n 的长度是模 p 与模 q 的两倍，所以 $\dot{s}=2s$. 则算法2总共运行 $(t+2m-1)(18s^2+4s)$ 次乘法运算，$(t+2m-1)(36s+30s+6)$ 次加法运算.

从上面的分析可以得到算法2的运算次数明显比算法1的多. 最后，我们用Mathematic仿真实验，分别用算法1和算法2计算 s_0，为了方便统计实验结果，我们在同一个运行环境下，分别统计两种算法在1万次相同的输入下的运行时间，结果表明算法1比算法2用时少，而且结果很明显. 表1是两种算法在相同输入下的运行时间统计表，其中 $l=100$，T_1,T_2 分别表示算法1和算法2的运行时间.

表1 两种算法在相同输入下的运行时间统计表

p	q	s_{t+1}	s_0	T_1/s	T_2/s
379	383	103 572	99 425	0.093 6	5.631 6
983	991	589 438	386 709	0.093 6	68.952 442
1 999	2 003	3 670 516	2 590 196	0.192 0	300.613 9
9 931	9 967	19 834 925	60 368 572	0.468 0	—
999 983	999 979	332 131 240 224	842 302 977 551	15.553 3	—

4 结束语

二次剩余在密码学中有广泛应用[12-16]. 本文通过分析比较两种计算二次剩余平方根的算法，找到了相对较优的算法，这对今后求二次剩余平方根时进行算法选择提供了帮助，并且得到在计算模 n 的平方根时，将模 n 分解为两个二进制表示长度相等的模，再利用中国剩余定理进行求解，可以提高求模 n 二次剩余平方根的效率. 而近些年基于二次剩余构造密码方案是密码界研究的热点，无疑我们为后面学者对此热点的研究提供了方便.

参考文献：

[1] VICTOR S. A Computational Introduction to Number Theory and Algebra [M]. Cambridge: Cambridge University

Press Cambridge，2008.
[2] BUHLER J，WAGON S. Basic Algorithms in Number Theory [J]. Algorithmic Number Theory，MSRILibrary，2008：44：25－68.
[3] Cohen H. A Course in Computational Algebraic Number Theory [J]. Graduate Texts in Math，2000，26(2)：211－244.
[4] STINSON D R. Cryptography：Theory and Practice [M]. Florida ：Chemical Rubber Company Press ，1995.
[5] COCKS C. An Identity Based Encryption Scheme Based on Quadratic Residues. [J]. Cryptography and Coding，2001，2260：360－363.
[6] CAO Z F，ZHU H J，LU R X. Provably Secure Robust Threshold Partial Blind Signature [J]. Science in China Series F，2006，49(5)：604－615.
[7] 屈　晓. 基于公钥密码体制的模幂算法执行效率研究 [D]. 天津：天津大学，2014.
[8] 王金荣，周　赟，王红霞. Montgomery 模平方算法及其应用 [J]. 计算机工程，2007，33(24)：155－157.
[9] KAYA E，ACAR T，KALISK B S. Analyzing and Comparing Montgomery Multiplication Algorithms [J]. IEEE Microwave Magazine，1996，16(3)：26－33.
[10] 蒋　帅. 模逆运算及其时间复杂度分析 [D]. 济南：山东大学，2014.
[11] BLUM L，BLUM M ，SHUB M. A Simple Unpredictable Pseudo-Random Number Generator [J]. SIAM Journal on Computing，1986，15(2)：364－383.
[12] BLUM M，GOLDWASSER S. An Efficient Probabilistic Public Key Encryption Scheme Which Hides All Partial Information [J]. Process of Cryptography，1984：289－302.
[13] CHAI Z C，CAO Z F，DONG X L. Identity-Based Signature Scheme Based on Quadratic Residues [J]. Science in China Series F，2007(3)：373－380.
[14] 费如纯，王丽娜，于　戈. 基于离散对数和二次剩余的门限数字签名体制 [J]. 通信学报，2002，23(5)：65－69.
[15] 王志伟，张　伟. 基于二次剩余的新型盲签名方案 [J]. 计算机工程与科学，2010，32(9)：18－20.
[16] 邱卫国，陈克非，白英彩. 新型 Rabin 签名方案 [J]. 软件学报，2000，11(10)：1333－1337.

Comparison of Two Algorithms for Finding the Quadratic Residue Square Root

CAI Zhao-zheng[1]，　QU Yun-yun[2]，　BAO Xiao-min[1]

1. *School of Mathematics and Statistics，Southwest University，Chongqing 400715，China*；
2. *School of Mathematical Science，Guizhou Normal University，Guiyang，Guizhou 550001，China*

Abstract：In the case of a large composite number of modules，to find the quadratic residue root is a difficult problem. There are two kinds of algorithms that are known for finding the square root of quadratic residuals. In this paper，the two known algorithms are analyzed and compared，and the results show that the algorithm 1 proposed by Cocks is more efficient than the algorithm 2 proposed by Cao Zhenfu，et al.

Key words：module；quadratic residue；square root；Chinese remainder theorem

责任编辑　张　枸