DOI:10.16515/j.cnki.32-1722/n.2018.02.0012

高次互反律和数 $h2^n \pm 1$ 的素性判定

黄丹丹

(金陵科技学院软件工程学院、网络安全学院,江苏 南京 211169)

摘 要:大素数在数据传输的安全性方面越来越重要,此外,现代密码学中许多密码协议的构造都依赖于大素数,例如,RSA公钥密码体制的生成就用到了大素数。主要给出了一类特殊形式整数 $h2^n \pm 1$(其中 h 不被17整除)的素性判定算法,该算法对固定的 h 只需两个递推序列,并且序列的首项只依赖于 h,而与 n 无关,算法的时间复杂性为确定性拟二次多项式时间。在算法的构造过程中主要利用了高次互反律,即八次和十六次互反律。

关键词:素数判定;高次互反律;时间复杂性;分圆域;梅森数

中图分类号:O156 **文献标识码**:A **文章编号**:1672-755X(2018)02-0050-04

Higher Reciprocity Law and Primality Tests for Numbers $h2^n \pm 1$

HUANG Dan-dan

(Jinling Institute of Technology, Nanjing 211169, China)

Abstract: Large prime numbers are becoming increasingly important in the security of digital transmission. In modern cryptography, many construction of cryptographic protocols are also based on large prime numbers. For instance, the generation of RSA public-key cryptosystem uses large primes. In this paper, we mainly described primality tests for numbers of the form $h2^n \pm 1$, where h is not divided by 17, by means of two recursive sequences with the first items depending only on h, not on n. Our test is deterministic and also runs in quasi-quadratic time. The techniques which we used are the higher reciprocity laws, especially of orders octic and bioctic.

Key words: primality testing; higher reciprocity law; computational complexity; cyclotomic field; Mersenne numbers

素数是数论中最古老的概念之一,早在公元前4世纪古希腊数学家欧几里得就证明了素数存在无穷多个。大素数在用于数据传输的安全性方面尤为重要,并已成为当今信息化社会不可或缺的一部分。无论在实践中还是研究问题本身,正确有效地判别素数是一个十分关键且有趣的问题。

关于判别素数的方法,不曾接受过数学专业训练的人会想到用试除法,例如17,至多尝试15次除法便知其为一个素数。但是,随着数的不断增大,这种原始的办法将变得越来越困难从而失效。例如数 $2^{216\,091}-1$,它是一个超过65 000位十进位的数,在1985年被证明是素数,如果采用的是试除法,即使耗费再多的人力和资源,在我们的有生之年恐怕也无法验证这一事实。

对于一般的数,判定其是否素数的问题在理论上已有重大突破。Agrawal,Kayal和Saxena[1]在2004

收稿日期:2018-06-15

基金项目:国家自然科学基金青年基金项目(11601202);金陵科技学院高层次人才科研启动基金(jit-b-201526)

作者简介:黄丹丹(1987—),女,安徽桐城人,讲师,博士,主要从事信息安全与密码学的理论研究,及其在网络安全中的实践应用。

年的 Annals of Mathematics 上正式公布了他们的算法，即著名的 AKS 算法。该算法是一个用于判定一般数素性的无条件确定性多项式时间算法。AKS 算法的时间复杂性是 $O^{\sim}(\log^{7.5}N)$比特运算，其中 N 是被测试的数。理论上，AKS 算法是目前最佳的素数判定算法，但在实际中鲜有人用，这是由于 AKS 算法的计算复杂度中多项式的次数太高，且算法占用内存偏大，从而并不实用。

相对一般数，特殊形式数的素性证明通常更有研究价值，且特殊素数在密码学中也很常用。特殊数的素性判定问题已经被不同时代的数学家所研究，如 Fermat，Mersenne，Lucas 等，其中 Lucas(1842—1891 年)关于这方面的研究成果最著名也最丰富，详细的内容可参考 Williams 的著作[2]。

Williams 给出了很多判定形为 $Ap^n\pm1$ 的数素性的充分或必要条件。尤其是对形如 $A2^n\pm1$ 的数，其中 A 不能被 5 整除，Berrizbeitia 等[3]于 2003 年巧妙地运用四次剩余及四次互反律得到了一个明确的素性算法，它是确定性拟二次多项式时间的，该算法在理论及实践中均是最佳的。

本文主要研究形为 $h2^n\pm1$ 数的素性判定问题，其中 h 不被 17 整除，且 h 为奇数；介绍了著名的 Lucas-Lehmer 素数判定法，以及八次和十六次互反律；给出了一个判定数 $h2^n\pm1$(其中 h 不被 17 整除，且 h 为奇数)的确定性拟二次多项式时间的素性算法。

1　相关工作

著名的 Lucas-Lehmer 素数判定法是用来判定梅森数的一个算法[4-5]。

命题 1　Lucas-Lehmer 素数判定法。令 $M_p=2^p-1$，其中 p 是奇素数。令 $u_0=4$，当 $k\geqslant1$ 时，$u_k=u_{k-1}^2-2$。则 M_p 为素数当且仅当 M_p 整除 u_{p-2}。

命题 1 的证明具体可参考文献[6]中的定理 4.2.6。关于数 $h2^n\pm1$，当 h 不被 5 整除时，Berrizbeitia 和 Berry[3]利用四次互反律导出了一个明确的拟二次多项式时间的素性算法，这是首次对数 $h2^n+1$ 和 $h2^n-1$ 两种情形同时进行处理，具体可参考文献[3]。

二次互反律在现实中很常见，以下介绍其的推广：八次和十六次互反律。

命题 2　令 $m=8$ 或 16，若 p 是一个与 m 互素的素数，α 是分 O_m 圆环中的一个本原元。则

$$\left(\frac{\alpha}{p}\right)_m=\left(\frac{(-1)^{(p-1)/2}}{\alpha}\right)_m$$

成立。

命题 2 是由 Berndt 等人给出的，其证明见参考文献[7]中的定理 14.3.1。

2　主要结果

本节重点介绍当 h 不被 17 整除时，用来同时判定数 $M=h2^n\pm1$ 的明确的素性算法。

下面将分圆域扩张 Q_{16}/Q 的伽罗华群记作 G，于是 $G\cong(Z/16Z)^*$，不妨设 $G=\{\sigma_{\pm i}\mid i=1,3,5,7\}$，其中 σ_c 是域 Q_{16} 上的一个自同构，通过将 ζ_{16} 映成 ζ_{16}^c 所得。在这种意义下，分圆域扩张 Q_8/Q 的伽罗华群 $\mathrm{Gal}(Q_8/Q)=\{\sigma_{\pm1}\mid i=1,3\}$，这里的映射 σ_c 均由 G 的元素限制在域 Q_8 上所得，即，σ_c 此时将 ζ_8 映成 ζ_8^c。

令 K_1，K_2 分别为分圆域 Q_8，Q_{16} 的极大实子域，则 $K_1=Q(\sqrt{2})$，$K_2=Q(\zeta_{16}+\zeta_{16}^{-1})$，且有 $\mathrm{Gal}(K_1/Q)=\{\sigma_i|_{K_1}\mid i=1,3\}$，$\mathrm{Gal}(K_2/Q)=\{\sigma_i|_{K_2}\mid i=1,3,5,7\}$。

下面对群环 $Z[G]$中的任一元素 τ 及分圆域 Q_{16} 中的任一非零元素 α，当 $\tau=\sum_{\sigma\in G}k_\sigma\sigma$ 时，将 τ 作用在代数 α 上定义为 $\alpha^\tau=\prod_{\sigma\in G}\sigma(\alpha)^{k_\sigma}$，这里 $k_\sigma\in Z$，也可写作 $\tau(\alpha)$。在 $Z[G]$中规定 $\sigma_1=1$。

为了导出判定 $M=h2^n\pm1$ 的素性算法，需要以下两个递推序列：

(1) $\{(T_k,N_k)\mid k\geqslant0\}$，当 $k\geqslant0$ 时，它有如下的递推关系式：

$$T_{k+1}=T_k^2-2N_k-4 \tag{1}$$

$$N_{k+1}=N_k^2-2T_k^2+4N_k+4 \tag{2}$$

(2) $\{(X_k,Y_k,Z_k,W_k)\mid k\geqslant 0\}$，当 $k\geqslant 0$ 时，它有如下的递推关系式：

$$X_{k+1}=X_k^2-2Y_k-8 \tag{3}$$

$$Y_{k+1}=Y_k^2-2X_kZ_k+2W_k-6X_k^2+12Y_k+24 \tag{4}$$

$$Z_{k+1}=2Z_k^2-2W_kY_k-4Y_k^2+8X_kZ_k-8W_k+12X_k^2-24Y_k-32 \tag{5}$$

$$W_{k+1}=W_k^2-2Z_k^2+4W_kY_k+4Y_k^2-8X_kZ_k+8W_k-8X_k^2+16Y_k+16 \tag{6}$$

还需引入一个记号，将关于 m 个变量 $x_1,\cdots,x_m$ 的初等对称多项式记为 $S_k(x_1,\cdots,x_m)$，具体定义如下：

$$S_k(x_1,\cdots,x_m)=\sum_{1\leqslant j_1<\cdots<j_k\leqslant m}x_{j_1},\cdots,x_{jk}$$

其中 $1\leqslant k\leqslant m$。记 $k^*=(-1)^{(k-1)/2}k$，其中 k 为任意的奇数。在下文中，$M^*=(\pm h)2^n+1$，用来对两个情形 $h\cdot 2^n\pm 1$ 同时处理的判定素性准则如下：

定理 1 令 $M=h\cdot 2^n\pm 1$，其中 $0<h<2^{n-6}$ 是一个奇数，h 不被 17 整除，且 $n\geqslant 7$。令 $\pi_1=1+2\zeta_8^3\in Q_8$，$\pi_2=1-\zeta_{16}+\zeta_{16}^5\in O_{16}$。令 $\{(T_k,N_k)\}$ 和 $\{(X_k,Y_k,Z_k,W_k)\}$ 为两个递推序列，其递推公式分别为(1)(2)和(3)(4)(5)(6)，它们对应的首项为 $(T_0,N_0)=(Tr_{K_1}/(\alpha_1^h+\bar{\alpha}_1^h),Nm_{K_1}/(\alpha_1^h+\bar{\alpha}_1^h))$ 及 $(X_0,Y_0,Z_0,W_0)=(Tr_{K_2}/(\eta),S_2(\eta,\sigma_3(\eta),\sigma_5(\eta),\sigma_7(\eta)),S_3(\eta,\sigma_3(\eta),\sigma_5(\eta),\sigma_7(\eta)),Nm_{K_2}/(\eta))$，其中 $\alpha_1=(\pi_1/\bar{\pi}_1)^{1+3\sigma_3}$，$\alpha_2=(\pi_2/\bar{\pi}_2)^{1+3\sigma_{-5}+5\sigma_{-3}+7\sigma_7}$，$\eta=\alpha_2^h+\bar{\alpha}_2^g$，且 $\bar{\pi}$ 表示复共轭映射 σ_{-1} 作用在元素 π 上。

则 M 为素数当且仅当 M 不被方程 $x^4\equiv 1(\mathrm{mod}\ 2^{n-3})$ 落在 $1<x<2^{n-3}$ 中的任何解整除，以及下列条件之一成立：

(Ⅰ) $M^*\equiv\pm 4(\mathrm{mod}\ 17)$，且 $T_{n-3}\equiv -N_{n-3}\equiv -4(\mathrm{mod}\ M)$；

(Ⅱ) $M^*\equiv\pm 2,\pm 8(\mathrm{mod}\ 17)$，且 $T_{n-3}\equiv N_{n-3}\equiv 0(\mathrm{mod}\ M)$；

(Ⅲ) $M^*\equiv\pm 3,\pm 5,\pm 6,\pm 7(\mathrm{mod}\ 17)$，且 $T_{n-3}\equiv 0(\mathrm{mod}\ M)$，$N_{n-3}\equiv -2(\mathrm{mod}\ M)$；

(Ⅳ) $M^*\equiv -1(\mathrm{mod}17)$，且 $X_{n-4}\equiv -8(\mathrm{mod}\ M)$，$Y_{n-4}\equiv 24(\mathrm{mod}\ M)$，$Z_{n-4}\equiv -32(\mathrm{mod}\ M)$，$W_{n-4}\equiv 16(\mathrm{mod}\ M)$.

定理 1 的证明主要用到八次和十六次互反律，在寻找合适的代数整数 π_1,π_2 时，充分利用了分圆域和分圆环的性质，可参考文献[8]。

可以看出，定理 1 中用来判定的递推序列的首项 (T_0,N_0) 和 (X_0,Y_0,Z_0,W_0) 仅依赖于 h，与 n 无关。特别地，当 $h=16^m-1$ 且 m 为奇数时，此时 $h\equiv -2\not\equiv 0(\mathrm{mod}\ 17)$，从而 h 固定后，对所有足够大 n 的算法只用两个固定的首项判定出 $M_n=h\cdot 2^n\pm 1$ 的素性。然而，Bosma[9] 的算法以及 Berrizbeitia 和 Berry[3] 给出的算法都需要无穷多个种子。

3 结 语

本文主要介绍了一个快速判定数 $M=h\cdot 2^n\pm 1$(其中 $0<h<2^{n-6}$ 是一个固定的奇数，h 不被 17 整除，$n\geqslant 7$)素性的算法，该算法是确定性拟二次时间的，也就是说，当判定数 $M=h\cdot 2^n\pm 1$(其中 h 不被 17 整除)的素性时，其计算复杂性仅为 $O^{\sim}(\log^2 M)$ 比特运算。

尽管 Agrawal 等[1] 已证明素数判定问题存在确定性多项式时间的算法，但该算法很不实用。本文的定理 1 以及 Bosma，Berrizbeitia 等所给出的工作结果说明对特殊数 $M=h\cdot 2^n\pm 1$，当 h 不被 3 整除，或 h 不被 5 整除，或 h 不被 17 整除时，分别存在相应的快速算法判定其素性。这些算法至多用到两个递推序列以及至多两个固定的首项，更重要的是，这些首项只依赖于 h(与 n 无关)。所以这类算法不仅是确定性的，且其时间复杂度为 $O^{\sim}(\log^2 M)$ 比特运算，从而十分有效。

参考文献：

[1] Agrawal M, Kayal N, Saxena N. PRIMES is in P[J]. Annals of Mathematics, 2004, 160(2):781－793

[2] Williams H C. Édouard Lucas and primality testing[M]. New York:John Wiley and Sons Inc., 1998

[3] Berrizbeitia P, Berry T. Biquadratic reciprocity and a Lucasian primality test[J]. Mathematics of Computation, 2004, 73:1559－1564

[4] Lehmer D H. On Lucas's test for the primality of Mersenne's number[J]. Journal of London Mathematics Society, 1935, 10:162－165

[5] Lucas E. Théorie des fonctions numériques simplement périodiques[J]. American Journal of Mathematics, 1878(1):184－240

[6] Crandall R, Pomerance C. Prime numbers: A computational perspective, second edition[M]. New York: Springer Science&Business Media, Inc., 2005

[7] Berndt B, Evans R, Williams K. Gauss and Jacobi Sums[M]. New York:John Wiley and Sons Inc, 1998

[8] Deng Y P, Huang D D. Explicit primality criteria for $h \cdot 2^n \pm 1$[J]. Journal de Théorie des Nombres de Bordeaux, 2016, 28(1):55－74

[9] Bosma W. Explicit primality criteria for $h \cdot 2^k \pm 1$[J]. Mathematics of Computation, 1993, 61:97－109

（责任编辑：谭彩霞）

（上接第 44 页）

因此，本研究得到如下结论：1）T 形多孔砖内部砖孔结构复杂，孔内部空气流动阻碍较大，具有良好的隔热保温性能。2）T 形多孔砖因其结构设计合理，在顺砌、顶砌时都有较好的热工性能。3）外保温 T 形多孔砖墙体能实现可观的节能经济效益，可大量推广应用在城市、小城镇和农村的民用建筑中。

参考文献：

[1] 苗存贤. T 形多孔砖孔型结构设计及其研究[J]. 砖瓦，2006(6)：45－47

[2] 王晓璐，徐雷，李鸿秋，等. 矩形孔节能页岩多孔砖墙体传热性能的三维数值计算研究[J]. 金陵科技学院学报，2018(1)：45－49

[3] 陶文铨. 数值传热学[M]. 2 版. 西安：西安交通大学出版社，2002

[4] 中华人民共和国建设部. GB 50019—2003：采暖通风与空气调节设计规范[S]. 北京：中国计划出版社，2003

[5] 黄榜彪，张贝，黄秉章，等. 污泥烧结页岩多孔砖墙体热工性能研究[J]. 新型建筑材料，2016(5)：30－34

[6] 翁丽芬，张楠，陈俊萍. 我国建筑能耗现状下的建筑节能标准解析及节能潜力[J]. 制冷与空调，2011(1)：10－14

[7] 张勇，张抗，张宁. 合肥市污水源热泵系统应用分析[J]. 工程与建设，2016(4)：502－504

（责任编辑：湛　江）