PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 130, Number 2, Pages 363–365
S 0002-9939(01)06100-7
Article electronically published on September 19, 2001

DETERMINISTIC PRIMALITY TEST FOR NUMBERS OF THE FORM $A^2.3^n + 1$, $n \geq 3$ ODD

PEDRO BERRIZBEITIA AND BORIS ISKRA

(Communicated by David E. Rohrlich)

Abstract. We use a result of E. Lehmer in cubic residuacity to find an algorithm to determine primality of numbers of the form $A^2 3^n + 1$, n odd, $A^2 < 4(3^n + 1)$. The algorithm represents an improvement over the more general algorithm that determines primality of numbers of the form $A.3^n \pm 1$, $A/2 < 4.3^n - 1$, presented by Berrizbeitia and Berry (1999).

1. Introduction

Deterministic test of primality for numbers of the form $A.3^n \pm 1$, where $n \in \mathbb{N}$, A even, $A/2 < 4.3^n - 1$, were first given by Lucas [Lu], and further studied by Williams [W1] and [W2], who explored in depth properties of certain Lucas sequences.

Berrizbeitia and Berry [BB] and independently Kirfel and Rødseth [KR], used the law of cubic reciprocity to produce an algorithm that determines the primality of these numbers. The use of the cubic reciprocity for this purpose was first introduced by Guthmann [G]. The theorem from which the algorithm is derived is the following:

Theorem 1.1. *Let $M = A.3^n \pm 1$. Assume $n \geq 2$, A even, $A/2 < 4.3^n - 1$. Let p be a prime $p \equiv 1 \pmod 3$ such that M is not a cube* $\bmod p$. *Let π be a prime of the ring $\mathbb{Z}[\omega]$ (where $\omega^2 + \omega + 1 = 0$) lying over p (i.e. $N(\pi) = p$). Let*

$$S_0 = Tr\left[\left(\frac{\overline{\pi}}{\pi}\right)^A\right]$$

where $Tr(\alpha) = Trace_{\mathbb{Q}(\omega)/\mathbb{Q}}(\alpha)$. Let S_i be given by

$$S_{i+1} = S_i^2(S_i - 3) \quad \textit{for} \quad i \geq 0. \tag{1.1}$$

Then M is prime if and only if $S_{n-1} \equiv -1 \pmod M$.

For a proof see [BB]. We note that in [BB] the extra condition that π be primary can be dropped when $n \geq 2$.

This theorem gives place to a deterministic primality test for numbers of the form $M = A.3^n \pm 1$ as follows:

- Find a prime $p \equiv 1 \pmod 3$ such that M is not a cube mod p.
- Find $\pi \in \mathbb{Z}[\omega]$ such that $\pi\overline{\pi} = p$.
- Compute $S_0 = Tr[(\overline{\pi}/\pi)^A] \bmod M$.
- Use the recurrence (1.1) to verify if $S_{n-1} \equiv -1 \pmod M$.

Received by the editors July 11, 2000.
2000 *Mathematics Subject Classification.* Primary 11A51, 11Y11.

- Declare M prime if the congruence holds and composite otherwise.

Some features of this test are:

- We start with a prime $p \equiv 1 \pmod 3$ to find the seed S_0.
- S_0 is obtained by finding the class mod M of a rational number, namely $Tr[(\overline{\pi}/\pi)^A]$.
- The recurrence used is $S_{i+1} = S_i^2(S_i - 3)$.

In this paper we will restrict to the subsequence of the numbers $A.3^n \pm 1$ given by, $A^2.3^n + 1$ where $A^2 < 4(3^n + 1)$, n odd. For these numbers we will produce a test with the following features:

- Any prime $p > 3$ can be used to provide the seed S_0.
- S_0 is obtained by finding the class mod M of an integer.
- The recurrence used is $S_{i+1} = S_i^3$.

2. The test

Our main theorem is based on the following theorem due to Emma Lehmer.

Theorem 2.1 (Lehmer)**.** *Let M and p be primes, $M \equiv 1 \pmod 3$, $4M = Q^2 + 27R^2$, and let $L(p) \subseteq \mathbb{Z}/p$ be given by*

$$L(p) = \{\mu^2 : \mu^2 \equiv r(\frac{9}{2u+1})^2 \pmod p, u \not\equiv 0, 1, -\frac{1}{2}, -\frac{1}{3} \pmod p,$$
$$r \equiv \frac{3u+1}{3u-3} \pmod p \text{ and } (r/p) = +1\}.$$

Then

$$p \text{ is a cube } \bmod M \Leftrightarrow p \mid QR \text{ or } p \mid Q^2 - \mu^2 R^2 \text{ for some } \mu^2 \in L(p).$$

For a proof see [Le]. Our algorithm will be based in the following theorem:

Theorem 2.2. *Let $n = 2k + 1$, $k \geq 1$, $M = A^2.3^n + 1$, A even, $A^2 < 4(3^n + 1)$. Let p be a prime, $p > 3$ and $L(p) \subseteq \mathbb{Z}/p$, as in Lehmer's theorem. Assume that $p \nmid A$ and that $\forall \mu^2 \in L(p)$, $A^2 3^{2(k-1)} \mu^2 \not\equiv 1 \pmod p$. Then*

$$M \text{ is prime } \Leftrightarrow p^{2\frac{M-1}{3}} + p^{\frac{M-1}{3}} \equiv -1 \pmod M.$$

Proof. Assume M is prime. The conditions $p \nmid A$ and

$$A^2.3^{2(k-1)}\mu^2 \not\equiv 1 \pmod p \qquad \forall \mu^2 \in L(p)$$

imply by Theorem 2.1 that p is not a cube mod M, therefore $p^{\frac{M-1}{3}}$ has order 3 mod M, from which

$$p^{2\frac{M-1}{3}} + p^{\frac{M-1}{3}} + 1 \equiv 0 \pmod M. \tag{2.1}$$

Conversely, let q be a prime divisor of M; then (2.1) holds mod q. It follows that $p^{\frac{M-1}{3}}$ has order 3 mod q which implies that $p^{A^2} = p^{\frac{M-1}{3^n}}$ has order 3^n mod q, then $3^n \mid q - 1$. Therefore every prime divisor of M is of the form $B.3^n + 1$, where B is even since M, hence q, are both odd. It follows that if M is not prime, then $M \geq (2.3^n + 1)^2$ which implies $A^2 \geq 4(3^n + 1)$. □

We note that if we add the extra condition that M is not a square, we can improve the bound for A to be $A^2 < 4(3^{n+1} + 2)$.

Note that if we let $S_0 = p^{A^2}$ and $S_{i+1} = S_i^3$, then equation (2.1) turns into $S_{n-1}^2 + S_{n-1} \equiv -1 \pmod M$.

In particular, for $p = 5$ and $p = 7$, $L(p) = \emptyset$, so we get the following corollary.

Corollary 2.3. *Let $M = A^2 3^n + 1$, $n \geq 3$ odd, $p = 5$ or 7, $p \nmid A$ and $A^2 < 4(3^n+1)$, A even. Let $S_0 = p^{A^2}$ and*

$$S_{i+1} = S_i^3 \quad \textit{for } i \geq 0.$$

Then

$$M \textit{ is prime } \Leftrightarrow S_{n-1}^2 + S_{n-1} \equiv -1 \pmod{M}.$$

References

[BB] P. Berrizbeitia and T. G. Berry *Cubic Reciprocity and Generalized Lucas-Lehmer Tests for Primality of $A.3^n \pm 1$*. Proc. Amer. Math. Soc. 127 **7** (1999) 1923–1925. MR **99j:**11006

[G] A. Guthmann. *Effective primality test for $N = k \cdot 3^n + 1$ and $N = k \cdot 2^m 3^n + 1$*. BIT **32** (1992) 529–534. MR **93h:**11008

[KR] C. Kirfel and Ø. Rødseth. *On the primality of $2h \cdot 3^n + 1$*. To appear. Discrete Math.

[Le] E. Lehmer. *Criteria for Cubic and Quartic Residuacity*. Mathematika **5** (1958) 20–29. MR **20:**1668

[Lu] E. Lucas. *Théorie des functions numériques simplement périodiques* Amer. J. Math. **1** (1878) 184–214, 289–321.

[W1] H. C. Williams. *The primality of $N = 2A.3^n - 1$*. Can. Math. Bull. **15** (1972) 585–589. MR **47:**121

[W2] H. C. Williams. *A Note on the Primality of $6^{2^n} + 1$ and $10^{2^n} + 1$*. Fibonacci Quart. **26** (1988) 296–305. MR **89i:**11013

Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Caracas, Venezuela

E-mail address: pedrob@usb.ve

Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Caracas, Venezuela

E-mail address: iskra@usb.ve