

## CUBIC RECIPROCITY AND GENERALISED LUCAS-LEHMER TESTS FOR PRIMALITY OF $A \cdot 3^n \pm 1$

PEDRO BERRIZBEITIA AND T. G. BERRY

(Communicated by David E. Rohrlich)

ABSTRACT. Cubic reciprocity is used to derive primality tests analogous to the Lucas-Lehmer test for integers of the form  $A \cdot 3^n \pm 1$ . The test for  $A \cdot 3^n - 1$  is a minor improvement on a test derived by Williams by other means; the test for  $A \cdot 3^n + 1$  seems to be new.

The Lucas-Lehmer test for primality of the Mersenne number  $2^p - 1$  has been generalised by H. Williams to give primality tests for numbers of the form  $A \cdot k^n \pm 1$ , for various  $k$ , using techniques based on the classical derivation of the Lucas-Lehmer test itself (cf. [W1], [W2], [W3]). In this note, motivated by Rosen's derivation of the Lucas-Lehmer test via quadratic reciprocity (cf. [R]), we show how the theory of the cubic residue symbol leads to a very simple and conceptual derivation of generalised Lucas-Lehmer tests for the numbers  $A \cdot 3^n \pm 1$ . The resulting test for  $A \cdot 3^n - 1$  is a minor improvement on the test of [W1], though the derivation is completely different, while that for  $A \cdot 3^n + 1$  is, to our knowledge, new. A different type of test for  $A \cdot 3^n + 1$  using cubic reciprocity can be found in [G].

We first fix notation and recall some results for which a general reference is [IR]. Let  $\omega = e^{2\pi i/3}$ ,  $R = \mathbf{Z}[\omega]$ ; we shall denote the norm  $\mathbf{Q}(\omega) \rightarrow \mathbf{Q}$  by  $N$ , and the trace by  $Tr$ . Let  $\chi$  denote the cubic character on  $R$ . Then  $\forall a, b \in R$ ,  $a$  prime,  $b \not\equiv 0 \pmod{a}$ ,  $\chi_a(b)$  is a cube root of 1 uniquely defined by the condition  $\chi_a(b) \equiv b^{\frac{N(a)-1}{3}} \pmod{a}$ . If  $a, b \in R$  are *primary primes*, then the cubic reciprocity law  $\chi_a(b) = \chi_b(a)$  holds. Recall that primary is a normalization condition satisfied by  $x \in R$  when  $x \equiv 2 \pmod{3}$ .

Let  $M = A \cdot 3^n \pm 1$ , where we assume  $A$  is even and not divisible by 3. If  $M = A \cdot 3^n + 1$  assume  $M \neq (\frac{A}{2} \pm 1)^2$ . We first find a small rational prime  $l$  such that  $M$  is not a cube mod  $l$ . This can be done by direct search, since  $l$  is small. Note that  $l \equiv 1 \pmod{3}$ , since if  $l \equiv 2 \pmod{3}$ , then everything is a cube mod  $l$ . Now it is precisely rational primes  $\equiv 1 \pmod{3}$  which split in  $R$ , so  $l$  splits in  $R$  and we can write  $l = \pi \bar{\pi}$  for some irreducible  $\pi \in R$ ; choosing appropriately among associates, we may assume  $\pi$  to be primary. Let  $\tau = \bar{\pi}/\pi$ .

**Theorem.** *Let  $\{Q_k\}$  be the sequence defined by*

$$Q_0 = Tr(\tau^A); \quad Q_{k+1} = Q_k^2(Q_k - 3).$$

*Suppose  $A/2 < 4 \cdot 3^n - 1$ . Then  $M$  is prime if and only if  $Q_{n-1} \equiv -1 \pmod{M}$ .*

---

Received by the editors September 24, 1997.

1991 *Mathematics Subject Classification.* Primary 11A51, 11Y11.

*Proof.* We first give the proof for  $M = A \cdot 3^n - 1$ . Suppose that  $M$  is prime. By choice  $M$  is not a cube mod  $l$  and  $l = N(\pi)$ . It follows that  $M$  is not a cube mod  $\pi$ , whence  $\chi_\pi(M)$  evaluates to  $\omega$  or  $\omega^2$ . Since  $M \equiv 2 \pmod{3}$ , it is a primary prime in  $R$ , and applying the cubic reciprocity law, we find  $\chi_\pi(M) = \chi_M(\pi)$ , so  $\chi_M(\pi) = \omega$  or  $\omega^2$  also. Then, since

$$\chi_M(\pi) \equiv \pi^{\frac{M^2-1}{3}} \pmod{M},$$

we have

$$\pi^{\frac{M^2-1}{3}} \equiv \omega^i \pmod{M}$$

(where  $i$  is 1 or 2) which we can rewrite as

$$(\pi^{M-1})^{\frac{M+1}{3}} \equiv \omega^i \pmod{M};$$

that is,

$$\left(\frac{\pi^M}{\pi}\right)^{\frac{M+1}{3}} \equiv \omega^i \pmod{M}.$$

But  $\pi^M \equiv \bar{\pi} \pmod{M}$ , as can be seen either directly or by observing that complex conjugation must coincide with the Frobenius  $\phi(M)$  of the Galois group of  $\mathbf{Q}(\omega)$  over  $\mathbf{Q}$ . Thus, we obtain

$$\left(\frac{\bar{\pi}}{\pi}\right)^{\frac{M+1}{3}} \equiv \omega^i \pmod{M}$$

and finally

$$(1) \quad \tau^{\frac{M+1}{3}} \equiv \omega^i \pmod{M}.$$

Taking traces in equation (1), we find we have proved that  $M$  prime implies

$$\text{Tr}\left(\tau^{\frac{M+1}{3}}\right) = \text{Tr}\left(\tau^{A \cdot 3^{n-1}}\right) \equiv -1 \pmod{M}.$$

Now, set  $Q_k = \text{Tr}\left(\tau^{A \cdot 3^k}\right)$ . Thus  $M$  prime implies  $Q_{n-1} \equiv -1 \pmod{M}$ . The recurrence  $Q_k^3 = Q_{k+1} + 3Q_k$  follows easily from the definition of  $Q_k$ , using  $N(\tau) = 1$ , whence the sequence  $\{Q_k\}$  satisfies the recurrence given in the theorem and we are done.

Assume now  $Q_{n-1} \equiv -1 \pmod{M}$ . We shall show this implies that any prime divisor of  $M$  is greater than  $\sqrt{M}$  which clearly implies  $M$  prime. Suppose that  $q$  is a prime divisor of  $M$ . Let  $\delta$  be a prime of  $R$  lying over  $q$ . Thus  $\delta = q$  if  $q \equiv 2 \pmod{3}$  and  $\delta\bar{\delta} = q$  if  $q \equiv 1 \pmod{3}$ , and any congruence mod  $M$  in  $R$  implies the same congruence mod  $\delta$ . Then  $Q_{n-1} = (\text{Tr}(\tau))^{A \cdot 3^{n-1}} \equiv -1 \pmod{\delta}$  and this, together with  $N(\tau) = 1$ , implies  $\tau^{A \cdot 3^{n-1}} \equiv \omega^i \pmod{\delta}$ , where  $i = 1$  or  $2$ . It follows that  $\tau^A$  has order  $3^n$  in the group  $(R/\delta R)^*$ . This group has order  $N(\delta) - 1$  which is  $q - 1$  or  $q^2 - 1$  according to  $q \equiv 1$  or  $q \equiv 2 \pmod{3}$ . In the first case we get  $3^n$  divides  $q - 1$ , in the second case we get  $3^n$  divides  $(q - 1)(q + 1)$ , so we conclude that in all cases  $3^n$  divides either  $q + 1$  or  $q - 1$ . Under the hypothesis  $A/2 < 4 \cdot 3^n - 1$ , this implies  $q > \sqrt{M}$  (cf. [W1], Lemma 1) and the proof of the theorem for  $M = A \cdot 3^n - 1$  is complete.

The proof of the theorem for  $M = A \cdot 3^n + 1$  is slightly different, since now  $M \equiv 1 \pmod{3}$  and therefore splits in  $R$ . Assume  $M$  is prime, and choose  $\theta \in R$  to be a primary prime such that  $M = \theta\bar{\theta}$ . As before,  $M$  is not a cube mod  $l$ ,

hence not a cube mod  $\pi$ , so  $\chi_\pi(M) = \omega^i$ , where  $i = 1$  or  $2$ . Then  $\omega^i = \chi_\pi(\theta\bar{\theta}) = \chi_\pi(\theta)\chi_\pi(\bar{\theta}) = \chi_\theta(\pi)\chi_{\bar{\theta}}(\pi)$  (by cubic reciprocity)  $= \chi_\theta(\pi)\chi_\theta(\bar{\pi})^{-1} = \chi_\theta(\pi/\bar{\pi})$ . (This calculation can be found in [G]. It is reproduced in brief here for the convenience of the reader.) Thus  $\chi_\theta(\tau^{-1}) = (\tau^{-1})^{\frac{N(\theta)-1}{3}} = (\tau^{-1})^{\frac{M-1}{3}} \equiv \omega^i \pmod{\theta}$ . Taking traces, we obtain  $Q_{n-1} \equiv -1 \pmod{\theta}$ . Interchanging  $\theta$  and  $\bar{\theta}$  in the calculation we have just made, we also obtain  $Q_{n-1} \equiv -1 \pmod{\bar{\theta}}$ , whence  $Q_{n-1} \equiv -1 \pmod{M}$  as was to be proved. Finally,  $Q_{n-1} \equiv -1 \pmod{M}$  implies  $M$  prime follows as in the proof of the first case. The hypothesis  $M \neq (\frac{A}{2} \pm 1)^2$  is needed here to make the cited lemma of Williams apply in this case.

## ACKNOWLEDGEMENT

We thank H. Williams for a helpful discussion with the first author, which led to a considerable improvement on an earlier version of our Theorem 1.

## REFERENCES

- [G] A. Guthmann. *Effective primality tests for  $N = k \cdot 3^{n+1}$  and  $N = k \cdot 2^m 3^n + 1$* . BIT **32** (1992) 529-534. MR **93h**:11008
- [IR] K. Ireland and M. Rosen. *A classical Introduction to Modern Number Theory*. Springer-Verlag, Berlin, 1982. MR **83g**:12001
- [R] M. Rosen. *A proof of the Lucas-Lehmer test*. Amer. Math. Monthly **95** (1988) 855-856. MR **89i**:11011
- [W1] H. C. Williams *The primality of  $N = 2A3^n - 1$* . 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
- [W3] H.C. Williams *A class of primality tests for trinomials which includes the Lucas-Lehmer test*. Pacific J. Math **98** (1982) 477-494. MR **83f**:10008

DEPARTAMENTO DE MATEMATICAS PURAS Y APLICADAS, UNIVERSIDAD SIMÓN BOLÍVAR, CARACAS, VENEZUELA

*E-mail address:* pedrob@usb.ve

*E-mail address:* berry@usb.ve