An elliptic curve test for Mersenne primes

Benedict H. Gross*

Harvard University, Cambridge, MA 02138, USA

Received 8 August 2003; revised 8 September 2003
Communicated by D. Goss
Available online 28 October 2004

Abstract

Let \( \ell \geq 3 \) be a prime, and let \( p = 2^\ell - 1 \) be the corresponding Mersenne number. The Lucas–Lehmer test for the primality of \( p \) goes as follows. Define the sequence of integers \( x_k \) by the recursion

\[
x_0 = 4, \quad x_k = x_{k-1}^2 - 2.
\]

Then \( p \) is a prime if and only if each \( x_k \) is relatively prime to \( p \), for \( 0 \leq k \leq \ell - 3 \), and \( \gcd(x_{\ell-2}, p) > 1 \). We show, in the Section 1, that this test is based on the successive squaring of a point on the one-dimensional algebraic torus \( T \) over \( \mathbb{Q} \), associated to the real quadratic field \( k = \mathbb{Q}(\sqrt{3}) \). This suggests that other tests could be developed, using different algebraic groups. As an illustration, we will give a second test involving the successive squaring of a point on an elliptic curve.

If we define the sequence of rational numbers \( x_k \) by the recursion

\[
x_0 = -2, \quad x_k = \frac{(x_{k-1}^2 + 12)^2}{4 \cdot x_{k-1} \cdot (x_{k-1}^2 - 12)},
\]

then we show that \( p \) is prime if and only if \( x_k \cdot (x_k^2 - 12) \) is relatively prime to \( p \), for \( 0 \leq k \leq \ell - 2 \), and \( \gcd(x_{\ell-1}, p) > 1 \). This test involves the successive squaring of a point on the elliptic curve \( E \) over \( \mathbb{Q} \) defined by

\[
y^2 = x^3 - 12x.
\]

We provide the details in Section 2.

*Fax: +1-617-495-5132.
E-mail address: gross@math.harvard.edu.
The two tests are remarkably similar. For example, both take place on groups with good reduction away from 2 and 3. Can one be derived from the other?

© 2004 Elsevier Inc. All rights reserved.

Keywords: Mersenne prime; Elliptic curve

1. Lucas–Lehmer

If \( \ell \geq 3 \) is a prime, and \( p = 2^\ell - 1 \) is the corresponding Mersenne number, then

\[ p \equiv 7 \pmod{24}. \]  

We will exploit this congruence throughout the paper.

In this section, we will consider the Lucas–Lehmer test for the primality of \( p \). Lucas’s original paper is [Lu], and Lehmer’s addition is given in [Le]. A good modern treatment, similar to the one given here, can be found in [R].

Let \( A = \mathbb{Z} + \mathbb{Z}\sqrt{3} \) be the ring of integers, of discriminant 12, inside the real quadratic field \( k = \mathbb{Q}(\sqrt{3}) \). Let \( \sigma \) be the non-trivial automorphism of \( k \), for which

\[ \sigma(\sqrt{3}) = -\sqrt{3}. \]

The ring \( A \) has class number 1 and fundamental unit

\[ \varepsilon = 2 + \sqrt{3}. \]

The unit \( \varepsilon \) is totally positive and satisfies \( \varepsilon \cdot \varepsilon^\sigma = 1 \). It provides an integral point on the algebraic torus \( T \) mentioned in the introduction.

Let \( q \) be a prime number, and let \( T(q) \) be the subgroup of \( (A/q)^* \) consisting of elements of norm 1 to \( (\mathbb{Z}/q)^* \). By reduction \( (\mod q) \), we may consider \( \varepsilon \) as an element of the finite group \( T(q) \).

**Proposition 1.2.** If \( q \equiv 7 \pmod{24} \) then \( T(q) \) is cyclic of order \( q + 1 \), and \( \varepsilon \) is not a square in \( T(q) \).

**Proof.** Since \( q \equiv 7 \pmod{12} \) we have \( \left( \frac{3}{q} \right) = -1 \) by quadratic reciprocity. Hence \( q \) remains prime in \( A \) and \( A/q \) is a field with \( q^2 \) elements. Since the norm \( (A/q)^* \to (\mathbb{Z}/q)^* \) is surjective, \( T(q) \) is cyclic of order \( q + 1 \).

The element \( \varepsilon \) is not a square provided

\[ \varepsilon^{\frac{q+1}{2}} \equiv -1 \pmod{q}, \]

by Euler’s criterion. But

\[ \varepsilon = \beta/\beta^\sigma \]
in \( k \), with \( \beta = 3 + \sqrt{3} \) satisfying \( \beta^6 = 6 \). Writing this identity as
\[
\varepsilon = \frac{\beta^2}{6}
\]
and reducing (mod \( q \)) then gives
\[
\varepsilon^{\frac{q+1}{2}} = \frac{\beta^{q+1}}{6^{\frac{q+1}{2}}}
\equiv 6/6^{\frac{q+1}{2}} \quad \text{as} \quad \beta^p \equiv \beta^q
\equiv \left( \frac{6}{q} \right) = -1.
\]
The last identity follows from the congruence \( q \equiv 7 \) (mod 24) and quadratic reciprocity. This completes the proof. \( \square \)

Now define the (Lucas) sequence of integers \( x_k \) by the formula
\[
x_k = \text{Tr}(\varepsilon^{2k}).
\]
The first few terms are
\[
x_0 = 4, \quad x_1 = 14, \quad x_2 = 194, \quad x_3 = 37634.
\]
The integers \( x_k \) can be computed via the recursion
\[
x_k = x_{k-1}^2 - 2.
\]

**Proposition 1.3.** If the Mersenne number \( p = 2^\ell - 1 \) is prime, then \( x_k \not\equiv 0 \) (mod \( p \)) for \( 0 \leq k \leq \ell - 3 \) and \( x_{\ell-2} \equiv 0 \) (mod \( p \)).

Conversely, let \( p = 2^\ell - 1 \) be a Mersenne number. If \( x_k \) is a unit (mod \( p \)) for \( 0 \leq k \leq \ell - 3 \) and gcd\((x_{\ell-2}, p) > 1\), then \( p \) is prime.

**Proof.** If \( p \) is prime, then by (1.1) and Proposition 1.2, the group \( T(p) \) is cyclic of order \( p + 1 = 2^\ell \). Since \( \varepsilon \) is not a square in \( T(p) \), it is a generator. Hence \( \varepsilon^{2^\ell-2} \) has order 4 in \( T(p) \), and satisfies the polynomial \( x^2 + 1 \equiv 0 \) (mod \( p \)). In particular, \( x_{\ell-2} = \text{Tr}(\varepsilon^{2^{\ell-2}}) \equiv 0 \) (mod \( p \)). No smaller power of \( \varepsilon \) has order 4, so \( x_k \) is a unit (mod \( p \)) for \( 0 \leq k \leq \ell - 3 \).

For the converse, assume that \( q \) is a prime factor of \( p = 2^\ell - 1 \) which divides \( x_{\ell-2} \). Then \( \varepsilon^{2^{\ell-2}} \) has order 4 (mod \( p \)), so \( \varepsilon \) has order \( 2^\ell = p + 1 \) in the group \( T(q) \). Since \( T(q) \) has order \( q \pm 1 \), depending on the behavior of \( q \) in \( A \), this forces \( q = p \). Hence \( p \) is prime. \( \square \)
Corollary 1.4. Assume that \( p = 2^\ell - 1 \) is prime. Then the order \( B = \mathbb{Z} + p\mathbb{Z}\sqrt{3} \) of index \( p \) in \( A \) has class number 2 and fundamental unit \( \eta = \varepsilon^{2^\ell - 1} \).

Proof. Let \( \hat{A} = A \otimes \hat{\mathbb{Z}} \) and \( \hat{B} = B \otimes \hat{\mathbb{Z}} \) be the profinite completions of these rings. In general, we have an exact sequence \([L-P-P]\)

\[
1 \to A^*/B^* \to \hat{A}^*/\hat{B}^* \to \text{Pic}(B) \to \text{Pic}(A) \to 1.
\]

In this case, \( \text{Pic}(A) = 1 \) and

\[
\hat{A}^*/\hat{B}^* = (A/p)^*/(\mathbb{Z}/p)^*.
\]

Since \( \varepsilon \) has order \( 2^{\ell - 1} \) in \( (A/p)^*/(\mathbb{Z}/p)^* \), the quotient \( \text{Pic}(B) \) has order 2. Also \( \eta = \varepsilon^{2^\ell - 1} \) is the smallest power of \( \varepsilon \) which lies in \( B^* \). \( \square \)

Since the fundamental unit of \( B \) is so large, the continued fraction of the quadratic irrationality \( p \cdot \sqrt{3} \) is quite complicated, when \( p \) is prime. Can this be converted into a primality test?

2. Elliptic curves

Let \( E \) be the elliptic curve over \( \mathbb{Q} \) defined by

\[
y^2 = x^3 - 12x = x(x^2 - 12).
\]

Then \( E \) has discriminant \( \Delta = 2^{12} \cdot 3^3 \) and conductor \( N = 2^5 \cdot 3^2 = 288 \). In Cremona’s tables \([C, \text{p. 123}]\), \( E \) is the curve \( 288 - A2 \).

The Mordell–Weil group

\[
E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z}/2
\]

is generated by the points

\[
P = (-2, 4) \quad \text{of infinite order},
\]

\[
Q = (0, 0) \quad \text{of order 2}.
\]

The curve \( E \) has good reduction at all primes \( q > 3 \). It has complex multiplication by the ring of Gaussian integers, defined over \( \mathbb{Q}(i) \). An automorphism of order 4 is given by

\[
\varphi(x, y) = (-x, iy).
\]
In particular, \( E \) has supersingular reduction at all primes \( q > 3 \) with \( q \equiv 3 \pmod{4} \), and at these primes the group \( E(q) \) of points over \( \mathbb{Z}/q \) has order \( q + 1 \) [S2, p. 184].

**Proposition 2.1.** If \( q \equiv 7 \pmod{24} \) then \( E(q) \) is cyclic of order \( q + 1 \), and \( P = (-2, 4) \) is not divisible by 2 in \( E(q) \).

**Proof.** The group \( E(q) \) is the kernel of the isogeny \( F - 1 \) on \( E \) in characteristic \( q \) [S1, p. 131], where

\[
F(x, y) = (x^q, y^q).
\]

Hence \( E(q) \) is cyclic if \( F - 1 \) is not divisible by any prime \( \ell \) in the ring \( \text{End}(E) \). Otherwise, \( E(q) \) contains the group \((\mathbb{Z}/\ell)^2\) killed by multiplication by \( \ell \).

Since \( F^2 = -q \) in \( \text{End}(E) \), the only rational prime \( \ell \) which can divide \( F - 1 \) is \( \ell = 2 \). Indeed, the quotient must be an algebraic integer. But 2 divides \( F - 1 \) if and only if \( \left( \frac{12}{q} \right) = +1 \), when all 2-torsion is rational over \( \mathbb{Z}/q \). Since \( q \equiv 7 \pmod{12} \), \( \left( \frac{12}{q} \right) = -1 \), and \( E(q) \) is cyclic.

A point \((x, y)\) lies in \( 2E(q) \) provided both \( x \) and \( x^2 - 12 \) are squares in \( (\mathbb{Z}/q)^* \) [S1, p. 280–282]. Since \( q \equiv 7 \pmod{24} \), \(-2\) is not a square and \( P = (-2, 4) \) is not divisible by 2. \( \square \)

Now define a sequence of rational numbers \( x_k \) by the formula

\[
x_k = x(2^k \cdot P).
\]

The first few terms are

\[
x_0 = -2, \quad x_1 = 4, \quad x_2 = \frac{49}{4}, \quad x_3 = \frac{6723649}{1731856}.
\]

The rational numbers \( x_k \) can be computed (cf. [S1, p. 59]) via the recursion

\[
x_k = \frac{(x_{k-1}^2 + 12)^2}{4 \cdot x_{k-1} \cdot (x_{k-1}^2 - 12)}.
\]

**Proposition 2.2.** If the Mersenne number \( p = 2^\ell - 1 \) is prime, then the rational numbers \( x_k(x_k^2 - 12) \) are \( p \)-adic units for \( 0 \leq k \leq \ell - 2 \) and \( x_{\ell-1} \equiv 0 \pmod{p} \).

Conversely, let \( p = 2^\ell - 1 \) be a Mersenne number. If \( x_k(x_k^2 - 12) \) is relatively prime to \( p \) for \( 0 \leq k \leq \ell - 2 \) and \( \gcd(x_{\ell-1}, p) > 1 \), then \( p \) is prime.

**Proof.** If \( p \) is prime, then by (1.1) and Proposition 2.1, the group \( E(p) \) is cyclic of order \( p + 1 = 2^\ell \). Since \( P \) is not divisible by 2 in \( E(p) \), it is a generator. Hence

\[
2^{\ell-1} \cdot P \equiv Q \pmod{p}
\]
with \( Q = (0, 0) \) the unique point of order 2. In particular, \( x_{\ell - 1} = x(2^{\ell - 1}P) \equiv 0 \pmod{p} \). No smaller multiple of \( P \) has order 2, so \( x_k(x_k^2 - 12) \) is a \( p \)-adic unit for \( 0 \leq k \leq \ell - 2 \).

For the converse, assume that the rational number \( x_k(x_k^2 - 12) \) is relatively prime to \( p \) for \( 0 \leq k \leq \ell - 2 \) and that \( q \) is a prime factor of \( p = 2^\ell - 1 \) which divides \( x_{\ell - 1} \). Then \( 2^{\ell - 1}P \) has order 2 in \( E(q) \), so \( P \) has order \( 2^\ell = p + 1 \) in \( E(q) \). But the order of \( E(q) \) has the form \( q + 1 - a_q \) with \( |a_q| \leq 2\sqrt{q} \) [S1, p. 136]. Hence

\[
p + 1 \leq q + 1 + 2\sqrt{q}.
\]

This forces \( q = p \), so \( p \) is prime. \( \square \)

Acknowledgments

It is a pleasure to thank Hendrik Lenstra, who first introduced elliptic curves into the field of primality testing, for his suggestions. I also want to thank Curt McMullen, who read an earlier version of this paper, for his editorial comments.

References