PRIMALITY TESTS FOR $2^k n - 1$ USING ELLIPTIC CURVES

YU TSUMURA

Abstract. We propose some primality tests for $2^k n - 1$, where $k$, $n \in \mathbb{Z}$, $k \geq 2$ and $n$ odd. There are several tests depending on how big $n$ is. These tests are proved using properties of elliptic curves. Essentially, the new primality tests are the elliptic curve version of the Lucas-Lehmer-Riesel primality test.

1. Note

An anonymous referee suggested that Benedict H. Gross already proved the same result about a primality test for Mersenne primes using elliptic curve in [4].

2. Introduction.

There are mainly two types of primality tests. One of them applies to any integer and the other applies only to a special form of integer. Usually the latter is faster than the former because of its additional information. Among them, the Lucas-Lehmer primality test for Mersenne numbers $M_k = 2^k - 1$ is very fast. The test uses a sequence $S_i$ defined by $S_0 = 4$ and $S_{i+1} = S_i^2 - 2$ for $i \geq 1$. The primality test is that $M_k$ is prime if and only if $M_k$ divides $S_{k-2}$. For a proof, see for example [2]. Also see [1] and [8] for applications of the Lucas sequence for other primality tests. There is also a generalization of this test called the Lucas-Lehmer-Riesel test which applies to integers of the form $2^k n - 1$ with $n < 2^k$ (see [6] and [5]). This test also uses the sequence $S_i$ defined by the above recursion but with a different initial value $S_0$ depending $k$ and $n$.

In this paper we give several primality tests for integers of the form $2^k n - 1$ using elliptic curves. When $n$ is relatively small as in the Lucas-Lehmer-Riesel test, the primality test can be regarded as an analogue of the Lucas-Lehmer-Riesel test. The new test also uses a sequence defined by recursion. For the initial value, we need to take a proper elliptic curve and a point on it. This corresponds to the choice of an
initial value in the Lucas-Lehmer-Reisel test. However, when the new test applies to Mersenne numbers $2^k - 1$, there exist an elliptic curve and a point on it which are independent of $k$.

Now let us define the sequence. Let $p \equiv 3 \pmod{4}$ be a prime number and let $E$ be an elliptic curve defined by $y^2 = x^3 - mx$ for some integer $m \not\equiv 0 \pmod{p}$. Fix a point $Q = (x, y) \in E(\mathbb{F}_p)$ and denote $2^i Q = (x_i, y_i)$ for $i \geq 0$. On this curve, multiplication of a point by 2 is described as

\[
2(x, y) = \left(\frac{x^4 + 2mx^2 + m^2}{4(x^3 - mx)}, yR(x)\right) = \left(\frac{x^2 + m}{2y}, yR(x)\right)
\]

for some rational function $R(x)$. (See Example 2.5, page 52 in [7].)

Let us define a sequence $S_i$. Let $S_0 = x$ and $S_i = 4(x_{i-1}^3 - mx_{i-1})$ for $i \geq 1$, that is, $S_i$ is the denominator of $2^i Q$ when $i \geq 1$. Alternatively, we could omit a constant 4 in the definition of $S_i$. We refer to this sequence as the sequence $S_i$ with the initial value $Q = (x, y)$, or with the initial value $x$. Note that $S_i$ depends only on $x$ and $i$. ($S_i$ also depends on $m$. However, it will be clear from the context which $m$ is used.)

3. Group structure of $E(\mathbb{F}_p)$.

First, we analyze the structure of the group $E(\mathbb{F}_p)$, where $E$ is an elliptic curve defined by $y^2 = x^3 - mx$ for some integer $m \not\equiv 0 \pmod{p}$ and $p \equiv 3 \pmod{4}$ is a prime number. Assume $p + 1 = 2^k n$, where $k \in \mathbb{Z}$, $k \geq 2$ and $n$ is an odd integer.

**Theorem 3.1.** In this context, $\#E(\mathbb{F}_p) = p + 1$.

**Proof.** See Theorem 4.23, page 115 in [7].

**Theorem 3.2.** In this context, $E(\mathbb{F}_p) \cong \mathbb{Z}_{2^k n}$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-1} n}$ depending on whether $m$ is a non-quadratic residue or a quadratic residue modulo $p$.

**Proof.** By Theorem 3.1 we have $\#E(\mathbb{F}_p) = p + 1 = 2^k n$. Hence $E(\mathbb{F}_p) \cong \mathbb{Z}_{2^\alpha n_1} \oplus \mathbb{Z}_{2^\beta n_2}$ for some $n_1, n_2, \alpha, \beta \in \mathbb{Z}$ with $\alpha \leq \beta$ and $\alpha + \beta = k$ and $n_1 | n_2$ and $n_1 n_2 = n$. However, in general, $2^\alpha n_1$ must divide $p - 1$ by the group structure of elliptic curves. (See Theorem 4.3 and 4.4, page 98 in [7].) Note that $\gcd(\#E(\mathbb{F}_p), p - 1) = \gcd(p + 1, p - 1) = 2$. Therefore $n_1 = 1$ and $n_2 = n$. 


If $m$ is a quadratic non-residue (with Jacobi notation, $(\frac{m}{p}) = -1$), then only one root of $x^3 - mx$ is in $\mathbb{F}_p$. Hence $E[2] \not\subset E(\mathbb{F}_p)$. Therefore $\alpha = 0$ and $E(\mathbb{F}_p) \cong \mathbb{Z}_{2^n}$.

If $(\frac{m}{p}) = 1$, then $\sqrt{m} \in \mathbb{F}_p$. Hence all the roots of $x^3 - mx$ are in $\mathbb{F}_p$. Hence $E[2] \subset E(\mathbb{F}_p)$. So $\alpha \geq 1$. Since $p - 1 \equiv 2 \pmod{p}$ and $2^\alpha | p - 1$, we have $\alpha = 1$. Therefore $E(\mathbb{F}_p) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{k-1}}$.

□

The next theorem is essential to choose an initial value.

**Theorem 3.3.** Let $p \equiv 3 \pmod{4}$ be prime and let $E$ be an elliptic curve defined by $y^2 = x^3 - mx$ for some integer $m$. Assume $p+1 = 2^k$ for some integer $m$. Assume $p$ is not so small. More precisely, assume $p$ satisfies 

$$\lambda \sqrt{p} > (p^{1/4} + 1)^2.$$ 

Let $E$ be a curve defined by $y^2 = x^3 - mx$, where $m$ is a quadratic non-residue modulo $p$. Then $p$ is prime if and only if there exists a point $Q = (x, y)$ on $E$ such that 

$$\gcd(S_i, p) = 1$$

for $i = 1, 2, \ldots, k - 1$ and 

$$S_k \equiv 0 \pmod{p},$$

4. **Primality test for $p = 2^kn-1$ when $n$ is small.**

Using Theorem 3.3 we give primality tests for integers of the form $p = 2^kn-1$, where $k, n \in \mathbb{Z}$, $k \geq 2$ and $n$ is an odd integer. There are two primality tests. We distinguish them by the relative size of $n$ when compared with $2^k$. First, let us discuss the case when $n$ is relatively small.

**Theorem 4.1.** Fix $\lambda > 1$. Suppose $p = 2^kn-1$ with $k \geq 2$ and an odd integer $n \leq \sqrt{p}/\lambda$. Assume $p$ is not so small. More precisely, assume $p$ satisfies $\lambda \sqrt{p} > (p^{1/4} + 1)^2$. Let $E$ be a curve defined by $y^2 = x^3 - mx$, where $m$ is a quadratic non-residue modulo $p$. Then $p$ is prime if and only if there exists a point $Q = (x, y)$ on $E$ such that 

$$\gcd(S_i, p) = 1$$

for $i = 1, 2, \ldots, k - 1$ and 

$$S_k \equiv 0 \pmod{p},$$
where \( S_i \) is a sequence with the initial value \( S_0 = x \).

Proof. Suppose \( p \) is prime. Then by Theorem 3.2, \( E(\mathbb{F}_p) \cong \mathbb{Z}_{2^k} \). Then \( E(\mathbb{F}_p) \) has a point \( Q = (x, y) \) of order \( 2^k \). Hence \( S_i \), with the initial value this \( x \), satisfies the conditions of the theorem since \( S_i \) is the denominator of \( 2^i Q \).

Conversely, suppose there exists \( Q \) which satisfies the conditions. Assume \( p \) is composite and let \( r \) be a prime divisor such that \( r \leq \sqrt{p} \). Then we have \( \gcd(S_i, r) = 1 \) for \( i = 1, 2, \ldots, k-1 \) and \( S_k \equiv 0 \pmod{r} \). Hence in the reduction \( E(\mathbb{F}_r) \), \( Q \) has an order \( \geq 2^k \). Using the condition on \( n \), we have

\[
\lambda \sqrt{p} \leq p/n < 2^k \leq \#E(\mathbb{F}_r) \leq (\sqrt{r} + 1)^2 \leq (p^{1/4} + 1)^2
\]

Here the third inequality is by Hasse’s Theorem. However, we assumed that this does not happen. Therefore \( p \) is prime.

\[\square\]

To make Theorem 4.1 into a primality test, we need to find a point \( Q \) in the theorem. To this end we use Theorem 3.3. Let us first state the algorithm.

Algorithm. Let \( p \) be an integer of the form \( p = 2^k n - 1 \) with \( k \geq 2 \) and \( p, n \) satisfy the conditions of Theorem 4.1. To check whether \( p \) is prime, do the following steps.

1. Take \( x \in \mathbb{Z} \) such that \( \left( \frac{x}{p} \right) = -1 \) and find \( y \) such that \( \left( \frac{x^3 - y^2}{p} \right) = 1 \). Let \( m = (x^3 - y^2)/x \mod p \). Then \( Q' = (x, y) \) lies on the curve \( E : y^2 = x^3 - mx \), where \( m \not\equiv 0 \pmod{p} \). The following calculation is done in \( E(\mathbb{Z}_p) \). Let \( Q = nQ' \). If \( Q = \infty \), then \( p \) is composite. If not, go to Step 2.

2. Let \( S_i \) be the sequence with the initial value \( Q \). Calculate \( S_i \) for \( i = 1, 2, \ldots, k-1 \). If \( \gcd(S_i, p) > 1 \) for some \( i, 1 \leq i \leq k-1 \), then \( p \) is composite. If \( \gcd(S_i, p) = 1 \) for \( i = 1, 2, \ldots, k-1 \), then go to Step 3.

3. If \( S_k \equiv 0 \pmod{p} \), then \( p \) is prime. If not, \( p \) is composite.

Let us check why this algorithm works. In Step 1, we find an elliptic curve \( E : y^2 = x^3 - mx \) and a point \( Q \) on \( E \) whose \( x \)-coordinate is a quadratic non-residue. We have \( \left( \frac{m}{p} \right) = \left( \frac{(x^3 - y^2)/x}{p} \right) = \left( \frac{x}{p} \right) \left( \frac{x^3 - y^2}{p} \right) = -1 \cdot 1 = -1 \). Hence if \( p \) is prime, then \( Q' \) has order divisible by \( 2^k \) by Theorem 3.3. So the order of \( Q' \) is \( 2^k d \), where \( d|n \). Hence \( Q = nQ' \) has order \( 2^k \). Therefore if Step 1 concludes that \( p \) is composite, then \( p \) is really composite. Step 2 and Step 3 check if \( Q \) has order \( 2^k \). So if Step 2 or Step 3 concludes that \( p \) is composite, then \( p \) is really composite.
If the algorithm concludes \( p \) is prime, then \( S_1 \) satisfies the conditions of Theorem 4.1. Therefore \( p \) is really prime.

**Remark 4.2.** Since we know both coordinates of \( Q \), we can calculate \( nQ \) quickly.

**Remark 4.3.** Suppose this test concludes that \( p \) is composite because \( \gcd(S_i, p) > 1 \) for some \( i, 1 \leq i \leq k - 1 \) in Step 2. Then \( \gcd(S_i, p) \) might be a proper divisor of \( p \) though it might be \( p \) itself. This is the basic idea of the primality testing using elliptic curves proposed by Goldwasser and Kilian (see [3]).

5. Primality test for Mersenne numbers.

Let us apply the above algorithm for Mersenne numbers \( M_k = 2^k - 1 \). That is, we take \( n = 1 \) and suppose \( k \geq 3 \). In this case we do not have to choose the initial value and the elliptic curve as in Step 1. Note that since \( n = 1 \), the algorithm contains no elliptic curve calculation. Since \( S_i \) can be calculated using only the \( x \)-coordinate, we do not need to find \( y \). Actually, we can take \( E : y^2 = x^3 - 3x \) and a point \( Q \) with the \( x \)-coordinate \(-1\). Let us check this. Suppose \( M_k \) is prime. Since \( M_k \equiv 3 \pmod{4} \), we have \( \left( \frac{3}{M_k} \right) = -\left( \frac{M_k}{3} \right) = -1 \) by the quadratic reciprocity law. Hence we can take \( m = 3 \). Next, since \( M_k \equiv -1 \pmod{8} \), we have \( \left( \frac{(-1)^3 - 3(-1)}{M_k} \right) = \left( \frac{2}{M_k} \right) = 1 \). Hence \( \sqrt{2} \in \mathbb{F}_{M_k} \). Therefore \( Q = (-1, \sqrt{2}) \in E(\mathbb{F}_{M_k}) \).

In summary, the primality test for Mersenne numbers is the following.

**Algorithm for Mersenne numbers.**

Let \( p = 2^k - 1, k \geq 3 \). Let \( x_0 = -1, x_{i+1} = \frac{x_i^4 + 6x_i^2 + 9}{4(x_i^2 - 3x_i)} \) modulo \( p \) for \( i \geq 0 \). Define \( S_i = x_{i-1}^3 - 3x_{i-1} \) modulo \( p \) for \( i \geq 1 \).

To check the primality, do the following steps.

1. Calculate \( S_i \) for \( i = 1, 2, \ldots, k - 1 \). If \( \gcd(S_i, p) > 1 \) for some \( i, 1 \leq i \leq k - 1 \), then \( p \) is composite. If \( \gcd(S_i, p) = 1 \) for \( i = 1, 2, \ldots, k - 1 \), then go to Step 2.

2. If \( S_k \equiv 0 \pmod{p} \), then \( p \) is prime. If not, \( p \) is composite.

Therefore, we get a primality test which is an analogue of the Lucas-Lehmer test.

**Remark 5.1.** Note that for Mersenne numbers, the algorithm concludes that \( p \) is composite if and only if \( \gcd(S_i, p) > 1 \) for some \( i, 1 \leq i \leq k - 1 \). Hence as mentioned above, it might find a proper divisor of \( p \) as a value of \( \gcd(S_i, p) \).
6. PRIMALITY TEST FOR $p = 2^kn - 1$ WHEN $n$ IS LARGE.

Next, let us consider the case when $n$ is relatively large. For this case, we assume $n = q$ is prime for simplicity.

**Algorithm.** Let $p = 2^k q - 1$ with $k \geq 2$ and $q$ prime. Fix $\lambda > 1$ and assume $2^k \lambda \leq \sqrt{p}$ and $\lambda \sqrt{p} > (p^{1/4} + 1)^2$

To check if $p$ is prime or not, do the following steps.

(1) Take $x \in \mathbb{Z}$ such that \( \left( \frac{x^3 - y^2}{p} \right) = -1 \) and find $y$ such that \( \left( \frac{x^3 - y^2}{p} \right) \) = 1. Let $m = (x^3 - y^2)/x$ mod $p$. Then $Q = (x, y)$ lies on the curve $E : y^2 = x^3 - mx$. Then the following calculation is done in $E(\mathbb{Z}_p)$.

(2) If $2^k Q = \infty$, then go to Step 1 and take another $y$. If $2^k Q \neq \infty$, then go to Step 3.

(3) If $q(2^k Q) = \infty$, then $p$ is prime. If not, $p$ is composite.

**Theorem 6.1.** If we reach Step 3 in the above algorithm, it determines whether or not $p$ is prime.

**Proof.** We have \( \frac{m}{p} = \left( \frac{x^3 - y^2}{x} \right) = \left( \frac{x}{p} \right) \left( \frac{x^3 - y^2}{p} \right) = -1 \cdot 1 = -1 \).

If $p$ is prime, then by Theorem 3.2 we have $E(\mathbb{F}_p) \cong \mathbb{Z}_{2k_q}$. Since the $x$-coordinate of $Q$ is a quadratic non-residue, the order of $Q$ is divisible by $2^k$ by Theorem 3.3. By Step 2, we know that $2^k Q \neq \infty$. Hence $Q$ has order $2^k q$. So if $2^k q Q \neq \infty$, then $p$ is not prime.

Suppose we have $q(2^k Q) = \infty$ in Step 3 and $p$ is composite. Let $r$ be a prime divisor of $p$ such that $r \leq \sqrt{p}$. Since $2^k Q \neq \infty$ and $q(2^k Q) = \infty$, $Q$ has order divisible by $q$. Using the assumption on $k$, we have

\[
\lambda \sqrt{p} \leq p/2^k < q \leq \#E(\mathbb{F}_r) \leq (\sqrt{r} + 1)^2 \leq (p^{1/4} + 1)^2.
\]

Here the third inequality is by the Hasse’s Theorem. However, we assumed this inequality does not hold. Hence $p$ is prime.

**Remark 6.2.** Since we know $Q = (x, y)$, we can use the method of successive doubling when we multiply integers. Hence it is calculated quickly.

**Remark 6.3.** If we cannot proceed to Step 3, then this test will not stop. However, if $q$ is large prime, then it is likely that $Q$ has order $2^k q$. So after doing Step 2 several times if we could not proceed to Step 3, then it is likely $p$ is composite. Then we need to use another test to check if it is really composite. Or we should use this test after checking that $p$ is a probably prime by another test.
There exists a similar algorithm when \( n \) is not prime. However, the number of steps in the algorithm will increase. To see what happens, let us consider the case when \( n \) is a product of two primes. Let \( n = q_1q_2 \), where \( q_1, q_2 \) are (not necessarily distinct) primes.

**Algorithm.** Let \( p = 2^k q_1 q_2 - 1 \), where \( k \geq 2 \) and \( q_1, q_2 \) are primes.

Fix \( \lambda > 1 \) and assume \( 2^k \lambda \leq \sqrt{p} \) and \( \lambda \sqrt{p} > (p^{1/4} + 1)^2 \).

To check if \( p \) is prime or not, do the following steps.

1. Take \( x \in \mathbb{Z} \) such that \( \left( \frac{x}{p} \right) = -1 \) and find \( y \) such that \( \left( \frac{x^3 - y^2}{p} \right) = 1 \). Let \( m = (x^3 - y^2)/x \mod p \). Then \( Q = (x, y) \) lies on the curve \( E : y^2 = x^3 - mx \). Then the following calculation is done in \( E(\mathbb{Z}_p) \).

   (2) If \( 2^k Q = \infty \), then go to Step 1 and take another \( y \). If \( 2^k Q \neq \infty \), then go to Step 3.

   (3) If \( q_1(2^k Q) \neq \infty \) and \( q_2(2^k Q) \neq \infty \), then go to Step 4. Otherwise, go to Step 1 and take another \( y \).

   (4) If \( q_1 q_2(2^k Q) = \infty \), then \( p \) is prime. If not, \( p \) is composite.

The proof is almost the same as that of Theorem 6.1. You can replace \( q \) in the proof of Theorem 6.1 by \( q_1 q_2 \).

**Remark 6.4.** These tests in this section correspond to the primality tests using the factors of \( p + 1 \). (See [2]).

**References**

1. John Brillhart, D. H. Lehmer, and J. L. Selfridge, *New primality criteria and factorizations of \( 2^m \pm 1 \)*, Math. Comp. 29 (1975), 620–647. MR MR0384673 (52 #5546)
2. Richard Crandall and Carl Pomerance, *Prime numbers*, Springer-Verlag, New York, 2001, A computational perspective. MR MR1821158 (2002a:11007)
3. Shafi Goldwasser and Joe Kilian, *Primality testing using elliptic curves*, J. ACM 46 (1999), no. 4, 450–472. MR MR1812127 (2002c:11182)
4. Benedict H. Gross, *An elliptic curve test for Mersenne primes*, J. Number Theory 110 (2005), no. 1, 114–119. MR MR2114676 (2005m:11007)
5. Dale Husemöller, *Elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. MR MR2024529 (2005a:11078)
6. Hans Riesel, *Lucasian criteria for the primality of \( N = h \cdot 2^n - 1 \)*, Math. Comp. 23 (1969), 869–875. MR MR0262163 (41 #6773)
7. Lawrence C. Washington, *Elliptic curves*, second ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008, Number theory and cryptography. MR MR2404461 (2009b:11101)
8. Hugh C. Williams, *Édouard Lucas and primality testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts, 22, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR MR1632793 (2000b:11139)
DEPARTMENT OF MATHEMATICS, PURDUE UNIVERSITY 150 N. UNIVERSITY STREET, WEST LAFAYETTE, IN 47907-2067

E-mail address: ytsumura@math.purdue.edu