GENERALIZED LUCAS-LEHMER TESTS USING PELL CONICS

SAMUEL A. HAMBLETON

Abstract. Pell conics are used to write a Proth-Riesel twin-primality test. We discuss easy-to-find primality certificates for integers of the form $m^n h \pm 1$. The known primality test for $3^n h \pm 1$ is associated with $X^2 + 3Y^2 = 4$.

1. Introduction

Like elliptic curves, there is a group law on the Pell conics [4]. These are affine curves of genus 0 of the form $C : X^2 - \Delta Y^2 = 4$ where $\Delta$ is a fundamental discriminant. Geometrically, points $P$ and $Q$ on Pell conics are added by taking the line parallel to $PQ$, passing through the point $O = (2, 0)$, and intersecting with $C$ at $P + Q$. Algebraically this is

\[(x_1, y_1) + (x_2, y_2) = \left( \frac{x_1 x_2 + \Delta y_1 y_2}{2}, \frac{x_1 y_2 + x_2 y_1}{2} \right).\]

Multiplication by 2 and 3 is given by

\[2(x, y) = (x^2 - 2, xy),\]
\[3(x, y) = (x^3 - 3x, (x^2 - 1)y).\]

Lemmermeyer [4] considered the arithmetic of Pell conics indicating many interesting similarities with elliptic curves. The following theorem appears in [4] in a more general form. We use $\left( \frac{\Delta}{p} \right)$ to mean the Legendre symbol.

Theorem 1.1. Let $C : X^2 - \Delta Y^2 = 4$, $\Delta$ be a fundamental discriminant, $p$ be prime and $N$ be an integer. Then:

- $C(\mathbb{Z})$ is an abelian group with identity $O = (2, 0)$, and point $T = (-2, 0)$ of order 2. No other points have $y = 0$ or $x = \pm 2$. The inverse of $(x, y)$ is $(x, -y)$.
- $C(\mathbb{Z}/N)$ is an abelian group with identity $O$.
- $C(\mathbb{F}_p)$ is a cyclic group of order $p - \left( \frac{\Delta}{p} \right)$.
For multiplication by \( m \geq 1 \), including points of Equation (2), we define polynomials

\[
\begin{align*}
(3) & \quad f_0 = 2; f_1 = x; f_{i+1} = xf_i - f_{i-1}, \\
(4) & \quad g_0 = 0; g_1 = 1; g_{i+1} = xg_i - g_{i-1}, \\
(5) & \quad F_1 = 1; F_3 = x + 1; F_{2i+3} = xF_{2i+1} - F_{2i-1}.
\end{align*}
\]

**Lemma 1.2.** Let \( C \) be a Pell conic and \( P = (x, y) \in C(Z) \). Then for \( m \geq 1 \), \( mP = (f_m(x), y \cdot g_m(x)) \), and for odd \( m \geq 1 \),

\[
f_m(x) = (x - 2)F_m(x)^2 + 2.
\]

*Proof.* \( mP = (f_m(x), y \cdot g_m(x)) \) may be proved by induction using Equations (1), (3), and (4). To prove Equation (6), induction shows that

\[
F_{2i-1}^2 - x \cdot F_{2i-1}F_{2i+1} + F_{2i+1}^2 = x + 2,
\]

and using Equation (7) in another induction proves Equation (6). \( \square \)

Corollary 1.3 is a direct result of Lemma 1.2. \( C(F_p)[m] \) is used to denote the set of points \( P \) of \( C(F_p) \) for which \( mP = \emptyset \).

**Corollary 1.3.** Let \( C \) be a Pell conic, \( P = (x, y) \in C(F_p) \), and \( p \) prime. Then for odd \( m \geq 1 \), \( P \in C(F_p)[m] \) if and only if \( F_m(x) \equiv 0 \) (mod \( p \)).

Lemmermeyer [4] discussed primality proving using Pell conics, giving Theorem 1.5 as an analogue of Lucas’ theorem. It is assumed that the integers \( N \) are greater than 1 and coprime to 6.

**Theorem 1.4** (Lucas). If \( a^{N-1} \equiv 1 \) (mod \( N \)) but \( a^{N-1} \equiv 1 \) (mod \( N \)) for every prime factor \( q \) of \( N - 1 \), then \( N \) is prime.

**Theorem 1.5.** Let \( N \geq 5 \) and \( C : X^2 - \Delta Y^2 = 4 \) be a Pell conic defined over \( Z/N \) with \( \left( \frac{\Delta}{N} \right) = -1 \). Then \( N \) is prime if and only if for some point \( P \in C(Z/N) \), \( (N + 1)P = \emptyset \), but \( \frac{N+1}{q}P \neq \emptyset \) for every prime factor \( q \) of \( N + 1 \).

Lemmermeyer [4] remarked that there are Proth versions in which only part of \( N \pm 1 \) needs to be factored and commented that in the same way Gross [2] gave an elliptic curve ‘Lucas-Lehmer’ test, the Lucas-Lehmer test itself may be proved with the Pell conic \( C : X^2 - 12Y^2 = 4 \) and the point \((4, 1)\). This method is extended here to more general primality proving.

2. **Twin primes of the form \( 2^n h \pm 1 \)**

The theory of Pell conics is applied to a test similar to Riesel’s [6] generalization of the Lucas-Lehmer test to \( N = 2^n h - 1 \). Our test, however, also includes Proth’s Theorem. One advantage in their combination is a single primality certificate for a pair of twin primes. The uppercase letter \( \mathbb{Q} \) will henceforth be used exclusively for a fixed generator of \( C(F_p) \).

**Lemma 2.1.** Let \( p \) be an odd prime and let \( C : X^2 - \Delta Y^2 = 4 \) be a Pell conic such that \( p \equiv \left( \frac{\Delta}{p} \right) \) (mod 4). There is an exact sequence of group homomorphisms

\[
0 \rightarrow 2C(F_p) \rightarrow C(F_p) \xrightarrow{\theta} \{\pm 1\}^\times \rightarrow 0,
\]

where \( \theta : (x, y) \mapsto \left( \frac{x^2 + 2}{p} \right) \).
Lemma 2.2. Let $N = 2^n h + 1$, where $h$ is odd. Let $C : X^2 - \Delta Y^2 = 4$ be a Pell conic with $\Delta \equiv 1 \pmod{N}$. If there exists a $P \in C(\mathbb{Z}/N)$ such that $2^{n-1} h P = \mathcal{T}$, then every prime factor $q$ of $N$ satisfies $q \equiv \left( \frac{\Delta}{q} \right) \pmod{2^n}$.

Proof. Suppose $2^{n-1} h P = \mathcal{T}$ in $C(\mathbb{Z}/N)$. Let $q$ be a prime divisor of $N$. Let $o_q(P)$ denote the order of the point $P$ on $C : X^2 - \Delta Y^2 = 4$ over $\mathbb{F}_q$. Clearly we also have $2^{n-1} h P = \mathcal{T}$ in $C(\mathbb{F}_q)$. Therefore $o_q(P) | 2^n h$, but $o_q(P) \nmid 2^{n-1} h$. Since $h$ is odd, $2^n | o_q(P)$. Now $C(\mathbb{F}_q)$ is cyclic of order $q - \left( \frac{\Delta}{q} \right)$, so $o_q(P) | q - \left( \frac{\Delta}{q} \right)$. That is, $2^n | q - \left( \frac{\Delta}{q} \right)$ or simply $q \equiv \left( \frac{\Delta}{q} \right) \pmod{2^n}$. 

For the following, $(\cdot)$ will mean the Jacobi symbol.

Theorem 2.3. Let $N = 2^n h + 1$ where $0 < h < 2^n$, $h$ is odd and $n \geq 2$. Let $C : X^2 - \Delta Y^2 = 4$ be a Pell conic satisfying $\left( \frac{\Delta}{N} \right) \equiv N \pmod{4}$, and let $P = (x, y) \in C(\mathbb{Z}/N)$ be a point such that $\left( \frac{x^2 + 2y^2}{N} \right) = -1$. Then $N$ is prime if and only if $f_{2^n-1,h}(x) \equiv -2 \pmod{N}$, where $f_{2^n-1,h}(x)$ is the $2^{n-1}h$-th polynomial satisfying Equation (3).

Proof. If $N$ is prime, then by Lemma 2.1, $2^{n-1} h P = \mathcal{T}$. Conversely, suppose $2^{n-1} h P = \mathcal{T}$ while $N$ is composite. Then by Lemma 2.2 every prime factor $q$ of $N$, and hence every factor, satisfies $q \equiv \left( \frac{\Delta}{q} \right) \pmod{2^n}$. If $N \equiv 1 \pmod{4}$, then $N$ may factor as $N = (2^nh_1 + 1)(2^nh_2 + 1)$ or $N = (2^nh_1 - 1)(2^nh_2 - 1)$, so $h = \pm(h_1 + h_2) + h_1 h_2 2^n = (h_1 + h_2 - 1)(2^n \pm 1) \pm 1 + (h_1 - 1)(h_2 - 1)2^n \geq 2^n$ since $h_1$ and $h_2$ cannot both be 1 because $h$ is odd, a contradiction. If $N \equiv -1 \pmod{4}$, then $N$ may factor as $N = (2^nh_1 + 1)(2^nh_2 - 1)$, and we find that $h = h_2 - h_1 + h_1 h_2 2^n = h_2 + h_1 h_2 2^n - 1 \geq 2^n$, a contradiction. Therefore $N$ is prime.
We will assume from here on that $f$, $g$, and $F$ always refer to the polynomials defined in Equations (3), (4), and (5) respectively. We give an application of Theorem 2.3 to pairs of twin primes.

**Algorithm 2.4.** To certify the primality of a pair of twin primes of the form $2^n h \pm 1$:

1. Choose an integer $n \geq 2$ and a positive odd integer $h < 2^n$, and set $r = 2^n h$.
2. Find a fundamental discriminant $\Delta$ such that $\left(\frac{\Delta}{r}\right) = -1$ and $\left(\frac{\Delta}{r+1}\right) = 1$.
3. Find an integer $x$ such that $\left(\frac{x+1}{r}\right) = \left(\frac{x+1}{r+1}\right) = -1$.
4. Compute $f_{r/2}(x)$ modulo $r - 1$ and $r + 1$. If both $f_{r/2}(x) \equiv -2 \pmod{r \pm 1}$, then the points $(x, \cdot)$ and Pell conic $C : X^2 - \Delta Y^2 \equiv 4 \pmod{r}$ certify that $r \pm 1$ is a pair of twin primes.

**Proof.** If $r \pm 1$ are composite, then by Theorem 2.3, $f_{r/2}(x) \not\equiv -2 \pmod{r \pm 1}$, so we must prove that if $r \pm 1$ are prime and $\left(\frac{\Delta+1}{r}\right) = \left(\frac{\Delta+1}{r+1}\right) = -1$ then there exist points $P \in C(F_{r \pm 1})$ such that $x = x(P)$ and $P \not\in 2C(F_{r \pm 1})$. Clearly, there exist points $P \in C(F_{r \pm 1})$ such that $x = x(P)$ if and only if $\left(\frac{\Delta+1}{r \pm 1}\right) = \left(\frac{\Delta+1}{r \pm 1}\right)$ if and only if $\left(\frac{\Delta+1}{r \pm 1}\right) = \mp 1$. Part (4) then follows from Theorem 2.3. □

In Step (4) of Algorithm 2.4 it is unnecessary to evaluate, at the integer $x$ chosen in Step (3), each of the polynomials $f_t$ preceding $f_{r/2}$, as illustrated in the following example.

**Example 2.5.** The Pell conic $C : X^2 - 28Y^2 = 4$ and points $(17, y) \in C(Z/r \pm 1)$ certify the twin primes 191 and 193:

1. $r = 2^6 \cdot 3$.
2. $\left(\frac{28}{191}\right) = -1$ and $\left(\frac{28}{193}\right) = 1$, so $C : X^2 - 28Y^2 = 4$ is suitable.
3. $\left(\frac{19}{191}\right) = \left(\frac{19}{193}\right) = -1$, so the points $(17, 50) \in C(Z/191)$ and $(17, 47) \in C(Z/193)$ have the required properties.
4. To compute $f_{2^{3n}}(17)$ modulo 191 and 193, write $h = 3$ in binary as $b = 11$. The $k$-th term $t_k$ of a sequence $B$ is obtained by taking the first $k$ digits of $b$ from left to right, $B = \{1, 11\}$. To compute $f_h(17)$ (mod 191) and $f_h(17)$ (mod 193), for each $t_k \in B$, we wish to compute a sequence of pairs $(f_{t_k}(17), f_{1+t_k}(17))$ evaluated modulo 191 and 193, where

$$f_{t_k+1}(f_{1+t_k+1}) = \begin{cases} (f_{t_k}^2 - 2, f_{t_k} \cdot f_{1+t_k} - x) & \text{if } t_{k+1} \text{ is even}, \\ (f_{t_k} \cdot f_{1+t_k} - x, f_{1+t_k}^2 - 2) & \text{if } t_{k+1} \text{ is odd} \end{cases}$$

and $f_1(x) = x$ and $f_2(x) = x^2 - 2$. We have $f_3(17) \equiv 87$ (mod 191) and $f_3(17) \equiv 37$ (mod 193). Using $f_{2^{n-1}h} = f_{2^{n-1}}(f_h)$, we iterate terms of the sequences determined by repeated doubling, $n - 1 \equiv 5$ times, modulo 191 and 193: \{87, 118, 170, 57, 0, 189\} (mod 191) and \{37, 16, 61, 52, 0, 191\} (mod 193).

Equation (9) has been used by Williams [7] in the same way to efficiently evaluate Lucas sequences.

3. **EASY-TO-FIND PRIMALITY CERTIFICATES FOR $m^n h \pm 1$**

The main result of this section differs from the previous since we use solved Pell conics over integers to certify primes of the form $m^n h \pm 1$. The smallest non-trivial
point of $\mathcal{C}(\mathbb{Z})$ with $x, y > 0$, the fundamental solution, is usually a generator of $\mathcal{C}(\mathbb{F}_p)$. We begin with the main result which builds on a result of Williams [7].

The lemmas supporting Theorem 3.4 are included below. Remark 3.1 allows a comparison with Lemma 2.1.

Remark 3.1. Let $p$ be an odd prime, $m$ be an odd integer and $\mathcal{C} : X^2 - \Delta Y^2 = 4$ be a Pell conic such that $p \equiv \left(\frac{\Delta}{p}\right) (\bmod m)$. Let $\mu_m$ denote the multiplicative group of $m$-th roots of unity, generated by $\omega$. There is an exact sequence

$$0 \to m\mathcal{C}(\mathbb{F}_p) \to \mathcal{C}(\mathbb{F}_p) \to \mu_m \to 0,$$

where $\phi : \mathbb{P} = \ell \mathbb{Q} \to \omega^\ell$.

Proof. Let $\mathbb{P}_1, \mathbb{P}_2 \in \mathcal{C}(\mathbb{F}_p)$. Writing $\mathbb{P}_1 = \ell_1 \mathbb{Q}$ and $\mathbb{P}_2 = \ell_2 \mathbb{Q}$, $\phi(\mathbb{P}_1) \cdot \phi(\mathbb{P}_2) = \omega^{\ell_1} \omega^{\ell_2} = \omega^{\ell_1 + \ell_2} = \phi(\mathbb{P}_1 + \mathbb{P}_2)$. Again letting $\mathbb{P} = \ell \mathbb{Q}$, $\phi(\mathbb{P}) = 1$ if and only if $\omega^\ell = 1$, if and only if $m \mid \ell$, if and only if $\mathbb{P} \in m\mathcal{C}(\mathbb{F}_p)$. So $\ker(\phi) = m\mathcal{C}(\mathbb{F}_p)$. □

Lemma 3.2. Let $p = m^n h + 1$ be prime, where $m$ is odd, $h$ is even, not divisible by $m$ and $n \geq 2$. Let $\mathcal{C} : X^2 - \Delta Y^2 = 4$ be a Pell conic where $\left(\frac{\Delta}{p}\right) \equiv p (\bmod m)$. If $\mathbb{P} = (x, y) \in \mathcal{C}(\mathbb{F}_p)$ but $\mathbb{P} \notin m\mathcal{C}(\mathbb{F}_p)$, then $s \equiv f_{m^n-1h}(x) (\bmod p)$ satisfies $F_m(s) \equiv 0 (\bmod p)$. If $\mathbb{P} \in m\mathcal{C}(\mathbb{F}_p)$, then $s \equiv 2 (\bmod p)$.

Proof. If $\mathbb{P} \in m\mathcal{C}(\mathbb{F}_p)$, then $m^{n-1}h \mathbb{P} = m^n h \mathbb{Q} = \emptyset$ so that $s \equiv 2 (\bmod p)$. Points $\mathbb{P} \in \mathcal{C}(\mathbb{F}_p)$ satisfy $m^{n-1}h \mathbb{P} \in \mathcal{C}(\mathbb{F}_p)[m]$. Assuming $\mathbb{P} \notin \mathcal{C}(\mathbb{F}_p) \setminus m\mathcal{C}(\mathbb{F}_p)$ we must show that $m^{n-1}h \mathbb{P} \neq \emptyset$. Now $\mathbb{P} = \ell \mathbb{Q}$ for some positive integer $\ell$, so $m^{n-1}h \mathbb{P} = m^n h \mathbb{Q} = \emptyset$ if and only if $m^n h \mid m^{n-1}h \ell$, because $\mathbb{Q}$ is a generator, if and only if $m \mid \ell$. Since $\mathbb{P} \notin m\mathcal{C}(\mathbb{F}_p)$, $m \nmid \ell$, so $m^{n-1}h \mathbb{P} \in \mathcal{C}(\mathbb{F}_p)[m] \setminus 0$, and it follows that $s \equiv f_{m^n-1h}(x) (\bmod p)$ satisfies $F_m(s) \equiv 0 (\bmod p)$ by Corollary 1.3. □

The proof of Lemma 3.3 is similar to the proof of Lemma 2.2.

Lemma 3.3. Let $N = m^n h + 1$, where $m$ is odd, $h$ is even, not divisible by $m$ and $n \geq 2$. Let $\mathcal{C} : X^2 - \Delta Y^2 = 4$ be a Pell conic satisfying $\left(\frac{\Delta}{N}\right) \equiv N (\bmod m)$. If there exists a $\mathbb{P} \in \mathcal{C}(\mathbb{Z}/N)$ such that $s \equiv f_{m^{n-1}h}(x(\mathbb{P})) (\bmod p)$ satisfies $F_m(s) \equiv 0 (\bmod N)$, then every prime factor $q$ of $N$ satisfies $q \equiv \left(\frac{\Delta}{q}\right) (\bmod m^n)$.

For the purpose of certifying primes of the form $m^n h + 1$ in the case where it is not checked whether the point $\mathbb{P}$ belongs to $m\mathcal{C}(\mathbb{Z}/N)$, it should be assumed that the Pell conic satisfies $\Delta > 0$ and $\mathbb{P}$ is the fundamental solution of $\mathcal{C}(\mathbb{Z})$, reduced modulo $N$ to an element of $\mathcal{C}(\mathbb{Z}/N)$, in order to increase the chance that $\mathbb{P} \notin m\mathcal{C}(\mathbb{Z}/N)$.

Theorem 3.4. Let $N = m^n h + 1$, where $m$ is odd, $h$ is even, not divisible by $m$, $0 < h < m^n$ and $n \geq 2$. Let $\mathcal{C}$ be a Pell conic satisfying $\left(\frac{\Delta}{N}\right) \equiv N (\bmod m)$. Let $\mathbb{P} = (x, y) \in \mathcal{C}(\mathbb{Z}/N)$ and let $s \equiv f_{m^{n-1}h}(x) (\bmod N)$. Then:

1. If $F_m(s) \equiv 0 (\bmod N)$, then $N$ is prime.
2. If $s \equiv 2 (\bmod N)$ and $F_m(s) \equiv 0 (\bmod N)$, then $N$ is composite.
3. If $s \equiv 2 (\bmod N)$, then $N$ is either prime or a Lucas pseudoprime. Another Pell conic is required.
4. If it is known that $\mathbb{P} \notin m\mathcal{C}(\mathbb{Z}/N)$, then $N$ is prime if and only if $F_m(s) \equiv 0 (\bmod N)$.  

Proof. If $N$ is prime, then by Lemma 3.2, $F_m(s) \equiv 0 \pmod{N}$ or $s \equiv 2 \pmod{N}$. Conversely, suppose $F_m(s) \equiv 0 \pmod{N}$ while $N$ is composite. By Lemma 3.3 for every prime factor $q$ of $N$, and hence every factor, satisfies $q \equiv \pm 1 \pmod{m}$. If $N \equiv 1 \pmod{m}$, then $N$ may factor as $N = (m^nh_1 + 1)(m^nh_2 - 1)$. These correspond to $h = \pm(h_1 + h_2) + h_1h_2m^n = h_1(m^n \pm 1) + h_2(m^n \pm 1) - m^n + (h_1 - 1)(h_2 - 1)m^n$. Now $h_1$ and $h_2$ must be even since $h$ is even so that $h > m^n$, a contradiction, and $N$ must be prime. If $N \equiv -1 \pmod{m}$, then $N$ may factor as $N = (m^nh_1 + 1)(m^nh_2 - 1)$. This corresponds to $h = h_2 - h_1 + h_1h_2m^n$. If $h_1 = h_2 = 2$, then $h = 4 \cdot m^n$ so that $m \mid h$, a contradiction. Writing $h = h_2 + h_1(m^n - 1) + h_1(h_2 - 1)m^n$ and noting that $h_2$ must be even, $h > m^n$, a contradiction, so $N$ must be prime. This completes the proof of case (1). If the conditions of case (2) are satisfied, then $m^n\mathcal{P} \neq \emptyset$, so $N$ is composite by Theorem 3.1. Case (3) follows from Lemma 3.2 noting that $N$ may be a Lucas pseudoprime since the $f_i$ are terms of a Lucas sequence. If $N$ is prime and $\mathcal{P} \notin m\mathcal{C}(\mathbb{F}_N)$, then by Lemma 3.2, $F_m(s) \equiv 0 \pmod{N}$. This, together with case (1), completes the proof of case (4). \qed

Given that $N$ is prime and the Pell conic $\mathcal{C}$, with $\Delta > 0$ and $\left(\frac{\Delta}{N}\right) \equiv N \pmod{m}$, is randomly chosen while always using the fundamental solution of $\mathcal{C}(\mathbb{Z})$ reduced modulo $N$ to a point of $\mathcal{C}(\mathbb{Z}/N)$ as the point $\mathcal{P}$ of Theorem 3.4, this result leads to a primality certificate with a probability of $1 - \frac{1}{m}$. This attests to the occurrence of item (3) of Theorem 3.4 being unlikely. The $f_m(x)$ are in fact the Dickson polynomials of the first kind $D_m(x, a)$, with $a = 1$. The following comes from [5].

**Theorem 3.5 (Dickson).** Let $a \in \mathbb{F}_q^*$, where $q$ is the power of a prime. The Dickson polynomial $D_m(x, a)$ permutes the field $\mathbb{F}_q$ if and only if $\gcd(m, q^2 - 1) = 1$.

If $p = m^n + 1$ is prime and $m$ is odd while $h$ is even, then $\gcd(m, p^2 - 1) = m$ and $f_m(x) = D_m(x, 1)$ cannot permute $\mathbb{F}_p$. That is, there exists a $\mathcal{P} \in \mathcal{C}(\mathbb{F}_p)$ such that $\mathcal{P} \notin m\mathcal{C}(\mathbb{F}_p)$, where $\Delta : X^2 - \Delta Y^2 = 4$ is a Pell conic with the required property $\left(\frac{\Delta}{p}\right) \equiv p \pmod{m}$.

**Corollary 3.6.** Let $p = m^n + 1$ be prime where $m$ is odd. Let $\Delta : X^2 - \Delta Y^2 = 4$ be a Pell conic satisfying $\left(\frac{\Delta}{p}\right) \equiv p \pmod{m}$. Then the proportion $\frac{1}{m}$ of the points $\mathcal{P} \in \mathcal{C}(\mathbb{F}_p)$ satisfy $\mathcal{P} \in m\mathcal{C}(\mathbb{F}_p)$.

**Proof.** Let $\mathcal{Q}$ be the generator of the cyclic group $\mathcal{C}(\mathbb{F}_p)$. Suppose $\mathcal{Q} = m\mathcal{P}$. Then all of the elements of $\mathcal{C}(\mathbb{F}_p)$ are divisible by $m$, contradicting Theorem 3.5. Thus $\mathcal{Q}$ is not divisible by $m$. Under the isomorphism $\mathcal{C}(\mathbb{F}_p) \simeq \mathbb{Z}/m^n\mathbb{Z}$, the proportion $\frac{1}{m}$ of the points of $\mathcal{C}(\mathbb{F}_p)$ are divisible by $m$. \qed

**Remark 3.7.** Let $h$ be an integer. Neglecting the computation of the binary sequence $B$ of Example 3.5 and modular additions, the evaluation of $f_h$ modulo an integer $N$ requires at most $2\log_2(h)$ modular multiplications [5].

Induction may be used with Equations (5) and (7) to establish the identities

$$
\begin{align*}
F_{4j-1} &= F_{2j+1} \cdot F_{2j-1} - F_{2j-1}^2 + 1, \\
F_{4j+1} &= F_{2j+1}^2 - F_{2j+1} \cdot F_{2j-1} - 1, \\
F_{4j+3} &= (x-1)F_{2j+1}^2 - F_{2j+1}F_{2j-1} + 1.
\end{align*}
$$

We give an example showing how the $F_m$ may be computed using Equation (10).
Example 3.8. We show how $F_{795}(x)$ may be evaluated. The binary representation of $m = 795$ is $m_2 = 1100011011$. The $k$-th term $u_k$ of a sequence $U = \{u_k\}$ is obtained by taking the first $k + 1$ digits of $a$ from left to right from $k = 1$ up to, but not including $m_2$, to $k = \lfloor \log_2(m) \rfloor - 1$:

$$U = \{11, 110, 1100, 11000, 110001, 1100011, 11000110, 110001101\}.$$ 

Define a new sequence $V = \{v_k\}$ by $v_k = 2|u_k/2|$:

$$V = \{10, 110, 1100, 11000, 110001, 11000110, 11000110100\} = \{2, 6, 12, 24, 48, 98, 198, 398\} \text{ in base 10.}$$

The pairs $(F_{-1+v_k}, F_{1+v_k})$ may be evaluated recursively by using

$$F_{-1+v_k+1} = \begin{cases} 
F_{1+v_k} F_{-1+v_k} - F_2^2 + 1 & \text{if } v_{k+1} \equiv 0 \pmod{4}, \\
F_2^2 - F_1+v_k F_{-1+v_k} - 1 & \text{if } v_{k+1} \equiv 2 \pmod{4},
\end{cases}$$

$$F_{1+v_k+1} = \begin{cases} 
F_2^2 - F_1+v_k F_{-1+v_k} - 1 & \text{if } v_{k+1} \equiv 0 \pmod{4}, \\
(x-1)F_1^2 + F_{1+v_k} F_{-1+v_k} + 1 & \text{if } v_{k+1} \equiv 2 \pmod{4},
\end{cases}$$

which follow from Equations (10), until the value of $(F_{397}, F_{399})$ is known. Finally $F_{795} = F_{399} F_{397} F_{397}^2 + 1$.

Example 3.9. We certify the primality of $N = 795^5 - 188 - 1$. Now $(\frac{13}{N}) = -1 \equiv N \pmod{795}$, so the Pell conic $C : X^2 - 13 Y^2 = 4$ is suitable for applying Theorem 3.3. The point $(11, 3)$ is the fundamental solution of $C(\mathbb{Z})$. We must evaluate $s \equiv f_{795^{5},1588}(11) \pmod{N}$. The binary representation of $795^4 \cdot 1588$ is $100100000011011101101010001101111010001$. In Example 2.5 we recursively evaluate modulo $N$ the sequence of pairs

$$\{(f_1(11), f_2(11)), (f_3(11), f_3(11)), (f_4(11), f_5(11)), (f_5(11), f_9(11)), \ldots, (f_{795^{4}-794+1}(11))\} \pmod{N} \text{ using Equation } (9)$$

$$\equiv \{119, 1298, 14159, 154451, 2186871698, 23855111399, \ldots, 36373179821995454, 24412249608121898\} \pmod{N},$$

$$s = 36373179821995454^2 - 2 \equiv 88801172334360862 \pmod{N}.$$ 

To evaluate $F_{795}(s)$ (mod $N$), we proceed as in Example 3.8 using Equations (11) and (12):

$$\{(F_1(s), F_3(s)), (F_3(s), F_7(s)), (F_7(s), F_{11}(s)), \ldots, (F_{397}(s), F_{399}(s))\} \pmod{N}$$

$$\equiv \{(1, 388011723344360863), (329280233123969461, 62155946453030219), \ldots, (139048125143085063, 364686195778250318)\} \pmod{N}.$$ 

Now $F_{795}(s) = F_{399}(s) F_{397}(s) F_{397}^2 + 1 \equiv 0 \pmod{N}$, so $N$ is prime.

4. The primality test for $3^n h + 1$ using $X^2 + 3Y^2 = 4$ 

The recursions of both the classical Lucas-Lehmer test and that of the primality test for $3^n h + 1$ coincide with repeated duplication and repeated multiplication by 3 respectively. We have a geometric variation of the test of Berrizbeitia and Berry [1].

Theorem 1.2 relies on the cubic reciprocity law in the unique factorization domain $\mathbb{Z}[\omega]$ where $\omega$ is a primitive cube root of unity. See [3] for the following and for the other various identities of the cubic residue symbol $\left(\frac{\cdot}{3}\right)$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
Theorem 4.1 (Eisenstein). If α and π are primes of \( \mathbb{Z}[\omega] \) which are congruent to ±1 (mod 3), then \( (\frac{\alpha}{\omega})_3 = (\frac{\pi}{\omega})_3 \).

Below we simply associate the primality test \([\Pi]\) for \( 3^h h \pm 1 \) with the curve \( X^2 + 3Y^2 = 4 \). This avoids case (3) of Theorem 3.4 altogether, since one may not wish to accept 2 chances in 3 for obtaining a primality certificate.

Theorem 4.2. Let \( N = 3^h h + \epsilon \), where \( \epsilon = \pm 1 \), \( h \) is even, not divisible by 3, \( 0 < h < 3^\nu \) and \( n \geq 2 \). Let \( \alpha \in \mathbb{Z}[\omega] \) be a prime satisfying \( \alpha \equiv \pm 1 \) (mod 3) and \( (\frac{\alpha}{3})_3 \). Let \( \beta = (\alpha/\alpha')^r = \beta_0 + \beta_1 \omega, \beta_0 = (2\beta_0 - \beta_1, \beta_1) \), and \( \mathcal{C} : X^2 + 3Y^2 = 4 \).

Let \( s \equiv f_{3^{\nu-1}}(x(\mathcal{P}_\beta)) \) (mod \( N \)). Then \( N \) is prime if and only if \( s \equiv -1 \) (mod \( N )\).

Proof. Since the norm of \( \beta \) is equal to 1, \( \mathcal{P}_\beta \in \mathbb{C} \mathbb{Z}/N \). We must show that \( (\frac{\mathcal{P}_\beta}{3})_3 \). Therefore it must follow that \( \mathcal{P}_\beta \in \mathbb{C} \mathbb{Z}/N \). Noting that \( \mathcal{P}_\beta \not\equiv \mathbb{C} \mathbb{Z}/N \), the result follows from case (4) of Theorem 3.4. Note that \( F_0(1) = 0 \) (mod \( N \)) if and only if \( s \equiv -1 \) (mod \( N )\). \( \square \)

The first term of the recursion \( T_{k+1} = T_k^2 - 3T_k \) in the statement of Theorem 4.2 according to \([\Pi]\) is the trace \( \text{Tr}(\beta^k) \) which is \( f_k(x(\mathcal{P}_\beta)) \) so that the computation of \( s \equiv f_{3^{\nu-1}}(x(\mathcal{P}_\beta)) \equiv f_{3^{\nu-1}}(f_k(x(\mathcal{P}_\beta))) \) (mod \( N \)) requires repeated multiplication by 3 on \( X^2 + 3Y^2 = 4 \) over \( \mathbb{Z}/N \).

Acknowledgments

The author would like to thank Victor Scharaschkin for supervision of this project, which has been supported by the University of Queensland. Franz Lemmermeyer has given instructive advice about Pell conics and related topics and has suggested many improvements to the presentation of this material, for which the author is grateful.

References


SCHOOL OF MATHEMATICS AND PHYSICS, UNIVERSITY OF QUEENSLAND, ST. LUCIA, QUEENSLAND, AUSTRALIA 4072

E-mail address: sah@maths.uq.edu.au