PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 8, August 2012, Pages 2653–2661
S 0002-9939(2011)11196-1
Article electronically published on December 20, 2011

GENERALIZED LUCAS-LEHMER TESTS USING PELL CONICS

SAMUEL A. HAMBLETON

(Communicated by Ted Chinburg)

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 $\mathcal{C} : X^2 - \Delta Y^2 = 4$ where Δ is a fundamental discriminant. Geometrically, points $\mathcal{P}$ and $\mathcal{Q}$ on Pell conics are added by taking the line parallel to $\overline{\mathcal{P}\mathcal{Q}}$, passing through the point $\mathcal{O} = (2, 0)$, and intersecting with $\mathcal{C}$ at $\mathcal{P} + \mathcal{Q}$. Algebraically this is

$$(x_1, y_1) + (x_2, y_2) = \Big(\frac{x_1x_2 + \Delta y_1y_2}{2}, \frac{x_1y_2 + x_2y_1}{2}\Big). \tag{1}$$

Multiplication by 2 and 3 is given by

$$\begin{aligned} 2(x, y) &= (x^2 - 2, xy), \\ 3(x, y) &= (x^3 - 3x, (x^2 - 1)y). \end{aligned} \tag{2}$$

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 $\mathcal{C} : X^2 - \Delta Y^2 = 4$, Δ be a fundamental discriminant, p be prime and N be an integer. Then:*

- *$\mathcal{C}(\mathbb{Z})$ is an abelian group with identity $\mathcal{O} = (2, 0)$, and point $\mathcal{T} = (-2, 0)$ of order 2. No other points have $y = 0$ or $x = \pm 2$. The inverse of (x, y) is $(x, -y)$.*
- *$\mathcal{C}(\mathbb{Z}/N)$ is an abelian group with identity $\mathcal{O}$.*
- *$\mathcal{C}(\mathbb{F}_p)$ is a cyclic group of order $p - \left(\frac{\Delta}{p}\right)$.*

Received by the editors June 11, 2009 and, in revised form, November 9, 2010 and March 15, 2011.
2010 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11G30.
Key words and phrases. Pell conics, Lucas-Lehmer, primality.

For multiplication by $m \geq 1$, including points of Equation (2), we define polynomials

$$f_0 = 2; f_1 = x; f_{i+1} = xf_i - f_{i-1}, \tag{3}$$

$$g_0 = 0; g_1 = 1; g_{i+1} = xg_i - g_{i-1}, \tag{4}$$

$$F_1 = 1; F_3 = x + 1; F_{2i+3} = xF_{2i+1} - F_{2i-1}. \tag{5}$$

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

$$f_m(x) = (x - 2)F_m(x)^2 + 2. \tag{6}$$

Proof. $m\mathcal{P} = \big(f_m(x), y \cdot g_m(x)\big)$ may be proved by induction using Equations (1), (3), and (4). To prove Equation (6), induction shows that

$$F_{2i-1}^2 - x \cdot F_{2i-1}F_{2i+1} + F_{2i+1}^2 = x + 2, \tag{7}$$

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

Corollary 1.3 is a direct result of Lemma 1.2. $\mathcal{C}(\mathbb{F}_p)[m]$ is used to denote the set of points $\mathcal{P}$ of $\mathcal{C}(\mathbb{F}_p)$ for which $m\mathcal{P} = \mathcal{O}$.

Corollary 1.3. *Let $\mathcal{C}$ be a Pell conic, $\mathcal{P} = (x, y) \in \mathcal{C}(\mathbb{F}_p)$, and p prime. Then for odd $m \geq 1$, $P \in \mathcal{C}(\mathbb{F}_p)[m] \backslash \mathcal{O}$ if and only if $F_m(x) \equiv 0 \pmod{p}$.*

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 $a^{N-1} \equiv 1 \pmod{N}$ but $a^{\frac{N-1}{q}} \not\equiv 1 \pmod{N}$ for every prime factor q of $N - 1$, then N is prime.*

Theorem 1.5. *Let $N \geq 5$ and $\mathcal{C} : X^2 - \Delta Y^2 = 4$ be a Pell conic defined over $\mathbb{Z}/N$ with $\left(\frac{\Delta}{N}\right) = -1$. Then N is prime if and only if for some point $\mathcal{P} \in \mathcal{C}(\mathbb{Z}/N)$, $(N + 1)\mathcal{P} = \mathcal{O}$, but $\frac{N+1}{q}\mathcal{P} \neq \mathcal{O}$ 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 $\mathcal{C} : X^2 - 12Y^2 = 4$ 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 $\mathcal{Q}$ will henceforth be used exclusively for a fixed generator of $\mathcal{C}(\mathbb{F}_p)$.

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

$$0 \longrightarrow 2\mathcal{C}(\mathbb{F}_p) \longrightarrow \mathcal{C}(\mathbb{F}_p) \xrightarrow{\theta} \{\pm 1\}^\times \longrightarrow 0, \tag{8}$$

where $\theta : (x, y) \mapsto \left(\frac{x+2}{p}\right)$.

Proof. Let $\mathcal{P}_1, \mathcal{P}_2 \in \mathcal{C}(\mathbb{F}_p)$. We must prove that $\theta(\mathcal{P}_1) \cdot \theta(\mathcal{P}_2) = \theta\big(\mathcal{P}_1 + \mathcal{P}_2\big)$. We will use the fact that $\theta(\mathcal{P}) = 1$ if and only if $\mathcal{P} \in 2\mathcal{C}(\mathbb{F}_p)$, but this also establishes that $\ker \theta = 2\mathcal{C}(\mathbb{F}_p)$. By Theorem 1.1, $\mathcal{C}(\mathbb{F}_p)$ is cyclic, generated by $\mathcal{Q}$, so there exist integers ℓ_1 and ℓ_2 such that $\mathcal{P}_1 = \ell_1\mathcal{Q}$ and $\mathcal{P}_2 = \ell_2\mathcal{Q}$. If $\theta(\mathcal{P}_1) = \theta(\mathcal{P}_2)$ then $\ell_1 \equiv \ell_2 \pmod 2$ so $\ell_1 + \ell_2$ is even and $\mathcal{P}_1 + \mathcal{P}_2 = (\ell_1 + \ell_2)\mathcal{Q} \in 2\mathcal{C}(\mathbb{F}_p)$ so that $\theta\big(\mathcal{P}_1 + \mathcal{P}_2\big) = 1$. If $\theta(\mathcal{P}_1) \neq \theta(\mathcal{P}_2)$ then $\ell_1 \not\equiv \ell_2 \pmod 2$ so $\ell_1 + \ell_2$ is odd and $\mathcal{P}_1 + \mathcal{P}_2 = (\ell_1 + \ell_2)\mathcal{Q} \notin 2\mathcal{C}(\mathbb{F}_p)$ so that $\theta\big(\mathcal{P}_1 + \mathcal{P}_2\big) = -1$. It follows that θ is a group homomorphism. $\theta(\mathcal{Q}) = -1$ since $\#\mathcal{C}(\mathbb{F}_p) = p - \left(\frac{\Delta}{p}\right) \equiv 0 \pmod 4$ and $\theta(2\mathcal{Q}) = 1$, so θ is surjective. □

It follows that if $p = 2^n h \pm 1$ is prime, where h is odd and $n \geq 2$, and the Pell conic $\mathcal{C} : X^2 - \Delta Y^2 = 4$ is chosen such that $p \equiv \left(\frac{\Delta}{p}\right) \pmod 4$, then:

- If $\left(\frac{x(\mathcal{P})+2}{p}\right) = 1$, then $\mathcal{P} \in 2\mathcal{C}(\mathbb{F}_p)$ and $2^{n-1}h\mathcal{P} = \mathcal{O}$.
- If $\left(\frac{x(\mathcal{P})+2}{p}\right) = -1$, then $\mathcal{P} \notin 2\mathcal{C}(\mathbb{F}_p)$ and $2^{n-1}h\mathcal{P} = \mathcal{T}$.

Observe that the order of $\mathcal{C}(\mathbb{F}_p)$ is equal to $2^n h$, so $2^{n-1}h\mathcal{P} = \mathcal{O}$ or $\mathcal{T}$. Now $\mathcal{P} = \ell\mathcal{Q}$, so $2^{n-1}h\mathcal{P} = 2^{n-1}h\ell\mathcal{Q} = \mathcal{O}$ if and only if $2^n h \mid 2^{n-1}h\ell$, because $\mathcal{Q}$ is the generator, if and only if ℓ is even. If $\left(\frac{x(\mathcal{P})+2}{p}\right) = -1$, then $2^{n-1}h\mathcal{P} = \mathcal{T}$.

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

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

For the following, $\left(\frac{\cdot}{\cdot}\right)$ will mean the Jacobi symbol.

Theorem 2.3. *Let $N = 2^n h \pm 1$ where $0 < h < 2^n$, h is odd and $n \geq 2$. Let $\mathcal{C} : X^2 - \Delta Y^2 = 4$ be a Pell conic satisfying $\left(\frac{\Delta}{N}\right) \equiv N \pmod 4$, and let $\mathcal{P} = (x, y) \in \mathcal{C}(\mathbb{Z}/N)$ be a point such that $\left(\frac{x+2}{N}\right) = -1$. 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, $2^{n-1}h\mathcal{P} = \mathcal{T}$. Conversely, suppose $2^{n-1}h\mathcal{P} = \mathcal{T}$ 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 $N = (2^n h_1 + 1)(2^n h_2 + 1)$ or $N = (2^n h_1 - 1)(2^n h_2 - 1)$, 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 $N = (2^n h_1 + 1)(2^n h_2 - 1)$, 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* Δ *such that* $\left(\frac{\Delta}{r-1}\right) = -1$ *and* $\left(\frac{\Delta}{r+1}\right) = 1$*.*
(3) *Find an integer* x *such that* $\left(\frac{x+2}{r-1}\right) = \left(\frac{x+2}{r+1}\right) = \left(\frac{x-2}{r+1}\right) = -\left(\frac{x-2}{r-1}\right) = -1$*.*
(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* $\mathcal{C} : X^2 - \Delta Y^2 = 4$ *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 $\left(\frac{x+2}{r-1}\right) = \left(\frac{x+2}{r+1}\right) = \left(\frac{x-2}{r+1}\right) = -\left(\frac{x-2}{r-1}\right) = -1$ then there exist points $\mathcal{P} \in \mathcal{C}(\mathbb{F}_{r\pm 1})$ such that $x = x(\mathcal{P})$ and $\mathcal{P} \notin 2\mathcal{C}(\mathbb{F}_{r\pm 1})$. Clearly, there exist points $\mathcal{P} \in \mathcal{C}(\mathbb{F}_{r\pm 1})$ such that $x = x(\mathcal{P})$ if and only if $\left(\frac{x^2-4}{r\pm 1}\right) = \left(\frac{\Delta}{r\pm 1}\right)$ if and only if $\left(\frac{x-2}{r\pm 1}\right) = \mp 1$. Part (4) then follows from Theorem 2.3. $\square$

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_i preceding $f_{r/2}$, as illustrated in the following example.

Example 2.5. The Pell conic $\mathcal{C} : X^2 - 28Y^2 = 4$ and points $(17, y) \in \mathcal{C}(\mathbb{Z}/r \pm 1)$ 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 $\mathcal{C} : X^2 - 28Y^2 = 4$ is suitable.
(3) $\left(\frac{19}{191}\right) = \left(\frac{19}{193}\right) = \left(\frac{15}{193}\right) = -\left(\frac{15}{191}\right) = -1$, so the points $(17, 50) \in \mathcal{C}(\mathbb{Z}/191)$ and $(17, 47) \in \mathcal{C}(\mathbb{Z}/193)$ have the required properties.
(4) To compute $f_{2^5 \cdot 3}(17)$ 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 $f_h(17) \pmod{191}$ and $f_h(17) \pmod{193}$, 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

$$(f_{t_{k+1}}, f_{1+t_{k+1}}) = \begin{cases} (f_{t_k}^2 - 2, f_{t_k} \cdot f_{1+t_k} - x) & \text{if } t_{k+1} \text{ is even,} \\ (f_{t_k} \cdot f_{1+t_k} - x, f_{1+t_k}^2 - 2) & \text{if } t_{k+1} \text{ is odd} \end{cases} \tag{9}$$

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

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 $p \equiv \left(\frac{\Delta}{p}\right) \pmod{m}$. Let μ_m denote the multiplicative group of m-th roots of unity, generated by ω. There is an exact sequence

$$0 \longrightarrow m\mathcal{C}(\mathbb{F}_p) \longrightarrow \mathcal{C}(\mathbb{F}_p) \xrightarrow{\phi} \mu_m \longrightarrow 0,$$

where $\phi : \mathcal{P} = \ell\mathcal{Q} \mapsto \omega^\ell$.

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

Lemma 3.2. *Let $p = m^n h \pm 1$ 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 $\left(\frac{\Delta}{p}\right) \equiv p \pmod{m}$. If $\mathcal{P} = (x, y) \in \mathcal{C}(\mathbb{F}_p)$ but $\mathcal{P} \notin m\mathcal{C}(\mathbb{F}_p)$, then $s \equiv f_{m^{n-1}h}(x) \pmod{p}$ satisfies $F_m(s) \equiv 0 \pmod{p}$. If $\mathcal{P} \in m\mathcal{C}(\mathbb{F}_p)$, then $s \equiv 2 \pmod{p}$.*

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

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

Lemma 3.3. *Let $N = m^n h \pm 1$, 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 $\left(\frac{\Delta}{N}\right) \equiv N \pmod{m}$. If there exists a $\mathcal{P} \in \mathcal{C}(\mathbb{Z}/N)$ such that $s \equiv f_{m^{n-1}h}(x(\mathcal{P})) \pmod{p}$ satisfies $F_m(s) \equiv 0 \pmod{N}$, then every prime factor q of N satisfies $q \equiv \left(\frac{\Delta}{q}\right) \pmod{m^n}$.*

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

Theorem 3.4. *Let $N = m^n h \pm 1$, 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 $\left(\frac{\Delta}{N}\right) \equiv N \pmod{m}$. Let $\mathcal{P} = (x, y) \in \mathcal{C}(\mathbb{Z}/N)$ and let $s \equiv f_{m^{n-1}h}(x) \pmod{N}$. Then:*

1. *If $F_m(s) \equiv 0 \pmod{N}$, then N is prime.*
2. *If $s \not\equiv 2 \pmod{N}$ and $F_m(s) \not\equiv 0 \pmod{N}$, then N is composite.*
3. *If $s \equiv 2 \pmod{N}$, then N is either prime or a Lucas pseudoprime. Another Pell conic is required.*
4. *If it is known that $\mathcal{P} \notin m\mathcal{C}(\mathbb{Z}/N)$, then N is prime if and only if $F_m(s) \equiv 0 \pmod{N}$.*

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 every prime factor q of N, and hence every factor, satisfies $q \equiv \pm 1 \pmod{m^n}$. If $N \equiv 1 \pmod{m}$, then N may factor as $N = (m^n h_1 + 1)(m^n h_2 + 1)$ or $N = (m^n h_1 - 1)(m^n h_2 - 1)$. These correspond to $h = \pm(h_1 + h_2) + h_1 h_2 m^n = h_1(m^n \pm 1) + h_2(m^n \pm 1) - m^n + (h_1 - 1)(h_2 - 1)m^n$. 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 $N = (m^n h_1 + 1)(m^n h_2 - 1)$. This corresponds to $h = h_2 - h_1 + h_1 h_2 m^n$. 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 $m^n h \mathcal{P} \neq \mathcal{O}$, so N is composite by Theorem 1.1. Case (3) follows from Lemma 3.2, noting that N may be a Lucas psuedoprime 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). □

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 $p = m^n h \pm 1$ 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 $\mathcal{C} : X^2 - \Delta Y^2 = 4$ is a Pell conic with the required property $\left(\frac{\Delta}{p}\right) \equiv p \pmod{m}$.

Corollary 3.6. *Let $p = m^n h \pm 1$ be prime where m is odd. Let $\mathcal{C} : X^2 - \Delta Y^2 = 4$ 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 $\mathcal{C}(\mathbb{F}_p) \simeq \mathbb{Z}/m^n h$, the proportion $\frac{1}{m}$ of the points of $\mathcal{C}(\mathbb{F}_p)$ are divisible by m. □

Remark 3.7. Let h be an integer. Neglecting the computation of the binary sequence B of Example 2.5 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

$$\begin{aligned} F_{4j-1} &= F_{2j+1} \cdot F_{2j-1} - F_{2j-1}^2 + 1, \\ F_{4j+1} &= F_{2j+1}^2 - F_{2j+1} \cdot F_{2j-1} - 1, \\ F_{4j+3} &= (x-1)F_{2j+1}^2 - F_{2j+1}F_{2j-1} + 1. \end{aligned} \tag{10}$$

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 $v_k = 2\lfloor u_k/2 \rfloor$:

$$\begin{aligned} V &= \{10, 110, 1100, 11000, 110000, 1100010, 11000110, 110001100\} \\ &= \{2, 6, 12, 24, 48, 98, 198, 398\} \qquad \text{in base 10.} \end{aligned}$$

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

$$(11)\quad F_{-1+v_{k+1}} = \begin{cases} F_{1+v_k}F_{-1+v_k} - F_{-1+v_k}^2 + 1 & \text{if } v_{k+1} \equiv 0 \pmod 4, \\ F_{1+v_k}^2 - F_{1+v_k}F_{-1+v_k} - 1 & \text{if } v_{k+1} \equiv 2 \pmod 4, \end{cases}$$

$$(12)\quad F_{1+v_{k+1}} = \begin{cases} F_{1+v_k}^2 - F_{1+v_k}F_{-1+v_k} - 1 & \text{if } v_{k+1} \equiv 0 \pmod 4, \\ (x-1)F_{1+v_k}^2 - F_{1+v_k}F_{-1+v_k} + 1 & \text{if } v_{k+1} \equiv 2 \pmod 4, \end{cases}$$

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

Example 3.9. We certify the primality of $N = 795^5 \cdot 1588 - 1$. Now $\left(\frac{13}{N}\right) = -1 \equiv N \pmod{795}$, so the Pell conic $\mathcal{C} : X^2 - 13Y^2 = 4$ is suitable for applying Theorem 3.4. The point $(11, 3)$ is the fundamental solution of $\mathcal{C}(\mathbb{Z})$. We must evaluate $s \equiv f_{795^4 \cdot 1588}(11) \pmod N$. The binary representation of $795^4 \cdot 1588$ is 1001000000111011001011110111000110101000101111010 0. As in Example 2.5 we recursively evaluate modulo N, the sequence of pairs

$$\begin{aligned} &\big\{(f_1(11), f_2(11)), (f_2(11), f_3(11)), (f_4(11), f_5(11)), (f_9(11), f_{10}(11)), \\ &\qquad \ldots, (f_{795^4 \cdot 794}(11), f_{795^4 \cdot 794+1}(11))\big\} \pmod N \text{ using Equation (9)} \\ &\equiv \big\{(119, 1298), (14159, 154451), (2186871698, 23855111399), \\ &\qquad \ldots, (363731798219995454, 244122496081218988)\big\} \pmod N, \end{aligned}$$

$$s \equiv 363731798219995454^2 - 2 \equiv 388011723344360862 \pmod N.$$

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

$$\begin{aligned} &\{(F_1(s), F_3(s)), (F_5(s), F_7(s)), (F_{11}(s), F_{13}(s)), \ldots, (F_{397}(s), F_{399}(s))\} \pmod N \\ &\equiv \{(1, 388011723344360863), (329280233123969461, 62155946453030219), \\ &\qquad \ldots, (139048125143085063, 364686195778250318)\} \pmod N. \end{aligned}$$

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

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

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

Theorem 4.2 relies on the cubic reciprocity law in the unique factorization domain $\mathbb{Z}[\omega]$ where ω is a primitive cube root of unity. See [3] for the following and for the other various identities of the cubic residue symbol $\left(\frac{\cdot}{\cdot}\right)_3$.

Theorem 4.1 (Eisenstein)**.** *If α and π are primes of $\mathbb{Z}[\omega]$ which are congruent to $\pm 1 \pmod 3$, then $\left(\frac{\pi}{\alpha}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3$.*

Below we simply associate the primality test [1] for $3^n h \pm 1$ 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 $N = 3^n h + \epsilon$, where $\epsilon = \pm 1$, h is even, not divisible by 3, $0 < h < 3^n$ and $n \geq 2$. Let $\alpha \in \mathbb{Z}[\omega]$ be a prime satisfying $\alpha \equiv \pm 1 \pmod 3$ and $\left(\frac{N}{\alpha}\right)_3 \neq 1$. Let $\beta = (\alpha/\alpha')^\epsilon = \beta_0 + \beta_1\omega$, $\mathcal{P}_\beta = (2\beta_0 - \beta_1, \beta_1)$, and $\mathcal{C} : X^2 + 3Y^2 = 4$. Let $s \equiv f_{3^{n-1}h}(x(\mathcal{P}_\beta)) \pmod N$. Then N is prime if and only if $s \equiv -1 \pmod N$.*

Proof. Since the norm of β is equal to 1, $\mathcal{P}_\beta \in \mathcal{C}(\mathbb{Z}/N)$. We must show that $\left(\frac{N}{\alpha}\right)_3 \neq 1$ implies that $\mathcal{P}_\beta \notin 3\mathcal{C}(\mathbb{Z}/N)$. Assuming that $\mathcal{P}_\beta \in 3\mathcal{C}(\mathbb{Z}/N)$, $x^3 - 3x - (2\beta_0 - \beta_1)$ is reducible modulo N so that β is a cubic residue modulo N, and hence modulo every primary prime divisor π of N meaning $\left(\frac{\beta}{\pi}\right)_3 = 1$. Now we show that this implies that $\left(\frac{\pi}{\alpha}\right)_3 = 1$ so that $\left(\frac{N}{\alpha}\right)_3 = 1$, a contradiction. If $\epsilon = 1$, then

$$\left(\frac{\beta}{\pi}\right)_3 = \left(\frac{\alpha\cdot\alpha'^{-1}}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3\left(\frac{\alpha'}{\pi}\right)_3^2 = \left(\frac{\alpha}{\pi}\right)_3\left(\frac{\alpha}{\pi'}\right)_3 = \left(\frac{\pi}{\alpha}\right)_3\left(\frac{\pi'}{\alpha}\right)_3 = \left(\frac{\pi\pi'}{\alpha}\right)_3 = 1$$

so that $\left(\frac{N}{\alpha}\right)_3 = 1$. If $\epsilon = -1$, then by the above calculation, $\left(\frac{\pi\pi'}{\alpha}\right)_3^2 = 1$ so that again $\left(\frac{N}{\alpha}\right)_3 = 1$. Therefore it must follow that $\mathcal{P}_\beta \notin 3\mathcal{C}(\mathbb{F}_N)$. Noting that $\left(\frac{-3}{N}\right) \equiv N \pmod 3$, the result follows from case (4) of Theorem 3.4. Note that $F_3(-1) \equiv 0 \pmod N$ if and only if $s \equiv -1 \pmod N$. $\square$

The first term of the recursion $T_{k+1} = T_k^3 - 3T_k$ in the statement of Theorem 4.2 according to [1] is the trace $\mathrm{Tr}(\beta^h)$ which is $f_h(x(\mathcal{P}_\beta))$ so that the computation of $s \equiv f_{3^{n-1}h}(x(\mathcal{P}_\beta)) \equiv f_{3^{n-1}}\big(f_h(x(\mathcal{P}_\beta))\big) \pmod N$ requires repeated multiplication by 3 on $X^3 + 3Y^2 = 4$ 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

1. P. Berrizbeitia, T. Berry, *Cubic reciprocity and generalised Lucas-Lehmer tests for primality of $A \cdot 3^n \pm 1$*, Proc. Amer. Math. Soc. **127** (1999), no. 7, 1923–1925. MR1487359 (99j:11006)
2. B. Gross, *An elliptic curve test for Mersenne primes*, J. Number Theory **110** (2005), no. 1, 114–119. MR2114676 (2005m:11007)
3. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990. MR1070716 (92e:11001)
4. F. Lemmermeyer, *Conics – A poor man's elliptic curves*, arXiv:math/0311306v1, preprint at http://www.fen.bilkent.edu.tr/~franz/publ/conics.pdf
5. R. Lidl, G. Mullen, G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, 65, Longman Scientific & Technical, 1993. MR1237403 (94i:11097)

6. H. Riesel, *Lucasian criteria for the primality of* $N = h \cdot 2^n - 1$, Math. Comp. **23** (1969), 869–875. MR0262163 (41:6773)
7. H. Williams, *Effective primality tests for some integers of the form* $A5^n - 1$ *and* $A7^n - 1$, Math. Comp. **48** (1987), no. 177, 385–403. MR866123 (88b:11089)

School of Mathematics and Physics, University of Queensland, St. Lucia, Queensland, Australia 4072

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