ON AN ANALOGUE TO THE LUCAS-LEHMER-RIESEL TEST USING ELLIPTIC CURVES

Markus Kirschmer
Lehrstuhl D für Mathematik, RWTH Aachen University, Templergraben 64, D-52062 Aachen, Germany
markus.kirschmer@math.rwth-aachen.de

Michael H. Mertens
Lehrstuhl D für Mathematik, RWTH Aachen University, Templergraben 64, D-52062 Aachen, Germany
michael.helmut.mertens@rwth-aachen.de

Received: , Revised: , Accepted: , Published:

Abstract

Following an idea of B. H. Gross, who presented an elliptic curve test for Mersenne primes $M_p = 2^p - 1$, we propose a similar test with elliptic curves for generalized Thabit primes $K(h, n) := h \cdot 2^n - 1$ for any positive odd number h and any integer $n > \log_2(h) + 2$.

1. Introduction

In 1876, Édouard Lucas invented an efficient primality test for Mersenne numbers $M_p = 2^p - 1$ for prime numbers p. The test uses a recursion defined by

$$L_0 = 4, \quad L_{k+1} = L_k^2 - 2.$$

He showed that a given Mersenne number M_p for $p \geq 3$ is prime if and only if $L_{p-2} \equiv 0 \pmod{M_p}$ (cf. [6]). The general idea of the proof given in [9] is to interpret the recursion as squaring a point on the algebraic torus over $\mathbb{Q}$ associated to the quadratic field $\mathbb{Q}(\sqrt{3})$. This test was optimized by Derrick Henry Lehmer in 1935 (cf. [5]) and therefore it is known as Lucas-Lehmer test.
In 1969, H. Riesel proposed a test for so called generalized Thabit numbers

$$K(h, n) = h \cdot 2^n - 1 \text{ for } h \in \mathbb{N} \text{ odd and } n \in \mathbb{N}$$

using the Lucasian sequence

$$L_{k+1} := L_k^2 - 2$$

where the first value L_0 of the recursion depends on h and n (cf. [8]). Some special cases of his generalization, especially for $3 \nmid h$, had already been found by Lucas and Lehmer themselves. This test is referred to as the Lucas-Lehmer-Riesel test.
The idea of using elliptic curves for primality tests is due to Hendrik Lenstra. He invented a general primality test for integers. In 2005, Benedict H. Gross used the ideas of Lucas and Lenstra to create an elliptic curve test especially for Mersenne primes. It is based on doubling the point $P = (-2, 4)$ on the rational elliptic curve with Weierstrass equation

$$y^2 = x^3 - 12x.$$

In [2], R. Denomme and G. Savin developed similar primality tests for Fermat numbers $F_n = 2^{2^n} + 1$ and numbers of the form $2^{2^n} - 2^{2^{n-1}} + 1$ and $3^{2^n} - 3^{2^{n-1}} + 1$. These tests are also based on doubling some suitable point on a twisted rational elliptic curve.

In this paper, we will extend the algorithm of Gross to all generalized Thabit numbers $K(h, n)$ with $n > \log_2(h) + 2$. If h is disible by 3, we will usually not be able to work with a global point on some rational elliptic curve. Instead, we will be using quadratic twists of rational elliptic curves E_ε as it was done in [2]. The curves E_ε we are using have Weierstrass equations of the form

$$y^2 = x^3 - \varepsilon x,$$

where $\varepsilon \in \mathbb{Z}$ depends on h and n. We also give an algorithm to find appropriate values for ε.

All the primality tests mentioned above are based on the following idea. Let N be some integer such that the factorization of a sufficiently large factor of $N \pm 1$ is known. These algorithms then construct an element g in some suitable group (e.g. the reduction of some rational elliptic curve modulo N or $(\mathbb{Z}_F/N\mathbb{Z}_F)^*$ where $\mathbb{Z}_F$ denotes the ring of integers in some algebraic number field F). Then N is prime if and only if the order of g is sufficiently large. The survey article [7] by Carl Pomerance contains some more primality tests based on this idea.

The paper is organized as follows. A short proof of the Lucas-Lehmer-Riesel test is given in Section 2. In Section 3, we recall division polynomials and in Section 4, we summarize some properties of elliptic curves of the form E_ε. In Section 5, we prove our primality test for generalized Thabit numbers. Finally in Section 6, we compare the efficiency of the mentioned primality tests: the Lucas-Lehmer test to Gross' test using elliptic curves for Mersenne numbers (cf. [3]) and the Lucas-Lehmer-Riesel test to our test for generalized Thabit numbers.

Notation By $\mathbb{P}$ we denote the set of positive prime numbers.
For positive integers m, n let $\left(\frac{m}{n}\right)$ denote the Jacobi-Symbol. In particular, if n is prime, then $\left(\frac{m}{n}\right)$ coincides with the Legendre-Symbol.

For an elliptic curve E over a field K we set $E(L)$ the group of L-rational points of E for any extension field L of K and $\mathcal{O}$ as the point at infinity, the zero-element of E as an abelian group.
If $K = \mathbb{Q}$ and $p \in \mathbb{Z}$ is prime, we denote the reduction of E modulo p by $\widehat{E}$ and we set $E(p) := \widehat{E}(\mathbb{F}_p)$.
If $\mathcal{O} \neq P = (x_0, y_0)$ is a point of an elliptic curve E, we denote by $x(P) := x_0$ the projection to the first affine coordinate of P.

2. The Lucas-Lehmer-Riesel Test

At first we want to give a short proof of Riesel's original primality test for numbers of the form $K(h, n)$ (see [8]).
For this section, let $d \geq 2$ be a square-free integer, $F := \mathbb{Q}(\sqrt{d})$ the corresponding real quadratic number field and $\mathbb{Z}_F$ its ring of integers. Further, let $^-\colon F \to F$ denote the nontrivial Galois automorphism of F. The following theorem is well known from the theory of quadratic number fields, but essential for the further discussion of the Lucas-Lehmer-Riesel test. Thus we give a short proof here.

Theorem 2.1 (Fermat). *Let $\alpha \in \mathbb{Z}_F$ and let $p \in \mathbb{P}$ be an odd prime such that $\alpha\mathbb{Z}_F + p\mathbb{Z}_F = \mathbb{Z}_F$.*

1. *If $\left(\frac{d}{p}\right) = 1$ then $\alpha^{p-1} \equiv 1 \pmod{p\mathbb{Z}_F}$.*
2. *If $\left(\frac{d}{p}\right) = -1$ then $\alpha^{p+1} \equiv \alpha\overline{\alpha} \pmod{p\mathbb{Z}_F}$.*

Proof. Let $\varphi\colon \mathbb{Z}_F \to \mathbb{Z}_F/p\mathbb{Z}_F$ be the canonical epimorphism. If $\left(\frac{d}{p}\right) = 1$ then $\mathbb{Z}_F/p\mathbb{Z}_F \cong \mathbb{F}_p \times \mathbb{F}_p$ since p splits in $\mathbb{Z}_F$. By assumption, $\varphi(\alpha)$ is a unit, thus $\varphi(\alpha)^{p-1} = 1$. If $\left(\frac{d}{p}\right) = -1$ then p is inert in $\mathbb{Z}_F$. Thus $\mathbb{Z}_F/p\mathbb{Z}_F \cong \mathbb{F}_{p^2}$ and $\varphi(\overline{x}) = \varphi(x)^p$ for all $x \in \mathbb{Z}_F$. Hence $\varphi(\alpha^{p+1}) = \varphi(\alpha\overline{\alpha})$. □

From this fact, we can now derive the Lucas-Lehmer-Riesel test:

Proposition 2.2. *Suppose $p \in \mathbb{P}$ is an odd prime with $\left(\frac{d}{p}\right) = -1$. If there are $a, b, r \in \mathbb{Z}$ such that*

$$\alpha := \frac{(a + b\sqrt{d})^2}{r} \in \mathbb{Z}_F \text{ and } \left(\frac{r}{p}\right) \cdot \frac{a^2 - b^2 d}{r} = -1$$

then

$$\alpha^{(p+1)/2} \equiv -1 \pmod{p\mathbb{Z}_F}\,.$$

Proof. According to Theorem 2.1 we obtain modulo $p\mathbb{Z}_F$

$$\alpha^{(p+1)/2} = \frac{(a+b\sqrt{d})^{p+1}}{r^{(p+1)/2}} \overset{2.1}{\equiv} \frac{(a+b\sqrt{d})(a-b\sqrt{d})}{r^{(p-1)/2}\cdot r} \equiv \frac{a^2-b^2d}{r}\cdot\left(\frac{r}{p}\right) = -1\,. \qquad \square$$

Proposition 2.3. *Let $n \geq 2$ and let $h < 2^n$ be an odd number. Further let $K := K(h,n) = h\cdot 2^n - 1$ denote the corresponding generalized Thabit number. If $\gcd(K,d) = 1$ and if there are $a, b \in \mathbb{Z}$ such that*

$$\alpha := \frac{(a+b\sqrt{d})^2}{|a^2-b^2d|} \in \mathbb{Z}_F \quad \textit{and} \quad \alpha^{(K+1)/2} \equiv -1 \pmod{K\mathbb{Z}_F}$$

then K is prime.

Proof. Let p be some prime factor of $K(h,n)$. Then

$$\alpha^{(K+1)/2} \equiv -1 \pmod{p\mathbb{Z}_F}.$$

Let $\varphi\colon \mathbb{Z}_F \to \mathbb{Z}_F/p\mathbb{Z}_F$ be the canonical epimorphism and let

$$k = \min\{t \in \mathbb{N} \mid \alpha^t \equiv -1 \pmod{p\mathbb{Z}_F}\}\,.$$

The order of $\varphi(\alpha)$ in $(\mathbb{Z}/p\mathbb{Z}_F)^*$ is $2k$ since p is odd. Further, $\varphi(\alpha^{(K+1)/2-k}) = 1$ implies that $h\cdot 2^{n-1} = (K+1)/2 = k + 2kr = k(1+2r)$ for some $r \in \mathbb{Z}$. In particular, k is divisible by 2^{n-1}.
Let $\varepsilon := \left(\frac{d}{p}\right)$. Then $\varepsilon \neq 0$ since $\gcd(K,d) = 1$. Further, $\alpha\overline{\alpha} = 1$, so α is a unit in $\mathbb{Z}_F$. Thus, if $\varepsilon = 1$ then Theorem 2.1 shows that

$$\alpha^{(p-1)/2} = \frac{(a+b\sqrt{d})^{p-1}}{|a^2-b^2d|^{(p-1)/2}} \equiv \left(\frac{|a^2-b^2d|}{p}\right) \pmod{p\mathbb{Z}_F}$$

and if $\varepsilon = -1$ then

$$\alpha^{(p+1)/2} \equiv \frac{a^2-b^2d}{|a^2-b^2d|}\left(\frac{|a^2-b^2d|}{p}\right) \pmod{p\mathbb{Z}_F}\,.$$

In particular, $\alpha^{p-\varepsilon} \equiv 1 \pmod{p\mathbb{Z}_F}$. Thus we have

$$p+1 \geq p-\varepsilon \geq 2k \geq 2^n\,.$$

Furthermore, K is not a square since $K \equiv 3 \pmod 4$. So if K is not a prime, then K has two distinct prime factors p and q. We may assume that $p < q$. Then

$$K \geq p\cdot q \geq p(p+2) \geq (2^n-1)(2^n+1) = 2^n\cdot 2^n - 1 > h\cdot 2^n - 1 = K$$

gives the desired contradiction. Hence K must be prime. $\square$

Corollary 2.4 (Lucas-Lehmer-Riesel test). *Let $n \geq 2$ and let $h < 2^n$ be an odd integer. Suppose there exist $a, b \in \mathbb{Z}$ and some square-free integer $d \geq 2$ such that*

$$\alpha = \tfrac{(a+b\sqrt{d})^2}{r} \in \mathbb{Z}_{\mathbb{Q}(\sqrt{d})} \text{ and } \left(\tfrac{d}{K(h,n)}\right) = \left(\tfrac{r}{K(h,n)}\right) \cdot \tfrac{a^2-b^2d}{r} = -1$$

where $r = |a^2 - b^2 d|$.
Then the generalized Thabit number $K(h,n)$ is prime if and only if

$$L_{n-2} \equiv 0 \pmod{K(h,n)}$$

where $L_0 = \alpha^h + \overline{\alpha}^h \in \mathbb{Z}$ and $L_{s+1} := L_s^2 - 2$ for $s \geq 0$.

Proof. Let $F = \mathbb{Q}(\sqrt{d})$. Since $\alpha\overline{\alpha} = 1$ we have $\alpha^{-1} = \overline{\alpha}$. Hence it follows from

$$(\alpha^{h\cdot 2^s} + \alpha^{-h\cdot 2^s})^2 = \alpha^{h\cdot 2^{s+1}} + \alpha^{-h\cdot 2^{s+1}} + 2$$

that $L_s := \alpha^{h\cdot 2^s} + \alpha^{-h\cdot 2^s}$ for all $s \geq 0$. If $K(h,n)$ is prime, then Proposition 2.2 implies

$$\begin{aligned} L_{n-2} &= \alpha^{h\cdot 2^{n-2}} + \alpha^{-h\cdot 2^{n-2}} \\ &= \alpha^{-h\cdot 2^{n-2}}(\alpha^{h\cdot 2^{n-1}} + 1) \equiv 0 \pmod{K(h,n)\mathbb{Z}_F}\,. \end{aligned}$$

Since $L_{n-2} \in \mathbb{Z}$ this shows that $L_{n-2} \equiv 0 \pmod{K(h,n)}$ as claimed. Conversely, by Proposition 2.3 and the above calculation we see that the given conditions are also sufficient for the primality of $K(h,n)$. □

Given a generalized Thabit number $K(h,n)$, a triple (a,b,d) as in the Corollary above can be found by inspecting the fundamental units of various real quadratic number fields, see [8] for details.

Remark 2.5. *Suppose the notation of Corollary 2.4. Then the Lucas-Lehmer-Riesel test can be summed up as follows. Let $\varphi\colon \mathbb{Z}_F \to \mathbb{Z}_F/K(h,n)\mathbb{Z}_F$ denote the canonical epimorphism and set $\beta = \varphi(\alpha)$. Then $K(h,n)$ is prime if and only if β^h generates a cyclic subgroup of $(\mathbb{Z}_F/K(h,n)\mathbb{Z}_F)^*$ of order 2^n.*

3. Division Polynomials

In this section, let E be an elliptic curve over a field K with $\mathrm{char}(K) \neq 2, 3$ given by a Weierstrass equation of the form

$$y^2 = x^3 + ax + b, \quad a, b \in K.$$

Definition 3.1. *The* division polynomials $\psi_m \in \mathbb{Z}[x, y, a, b]$ *of the elliptic curve* E *are given via the recursion*

$$\begin{aligned}
\psi_0 &:= 0, \qquad \psi_1 := 1, \qquad \psi_2 := 2y, \\
\psi_3 &:= 3x^4 + 6ax^2 + 12bx - a^2, \\
\psi_4 &:= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3), \\
\psi_{2m+1} &:= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad (m \geq 2), \\
2y\psi_{2m} &:= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad (m \geq 3).
\end{aligned}$$

These polynomials have the following property.

Lemma 3.2. *Let* m *be a positive integer.*

1. *If one identifies* y^2 *with* $x^3 + ax + b$*, then* ψ_{2m+1}*,* ψ_{2m}/y *and* ψ_{2m}^2 *can be viewed as polynomials in* $\mathbb{Z}[x, a, b]$*.*
2. *Let* L/K *be a field extension and* $P = (x, y)$ *be a point on* $E(L)$*. If* $m \cdot P \neq \mathcal{O}$ *then* $\psi_m^2(x) \neq 0$ *and*

$$m \cdot P = \left(x - \frac{\psi_{m-1}(x)\psi_{m+1}(x)}{\psi_m^2(x)}, \frac{\psi_{2m}(x, y)}{2\psi_m^4(x)} \right).$$

In particular, $m \cdot P = (f_m(x, a, b), g_m(x, a, b)y)$ *for some rational functions* $f_m, g_m \in \mathbb{Q}(x, a, b)$*.*

Proof. See for example [4, Chapter 2, §§1-2]. □

4. Some properties of the curves E_ε

In the following, let E_ε^t be the (twisted) elliptic curve over $\mathbb{Q}$ given by

$$ty^2 = x^3 - \varepsilon x, \qquad \varepsilon, t \in \mathbb{Z} \text{ with } t \neq 0.$$

When $t = 1$, we will usually omit the superscript t. Then

$$\tau_{\varepsilon,t} \colon E_\varepsilon^t \to E_{\varepsilon t^2},\ (x, y) \mapsto (xt, yt^2) \tag{1}$$

is an isogeny. Further, E_ε^t defined over $\mathbb{Q}(i)$ has complex multiplication by the ring of Gaussian integers $\mathbb{Z}[i]$:

$$[i] : E_\varepsilon^t(\mathbb{Q}(i)) \to E_\varepsilon^t(\mathbb{Q}(i)),\ (x, y) \mapsto (-x, i \cdot y)$$

and the discriminant of E_ε^t is

$$\Delta(E_\varepsilon^t) = 2^6 \cdot \varepsilon^3 \cdot t^6.$$

This leads to the following lemma.

Lemma 4.1. *Let $q \in \mathbb{P}$ be a prime not dividing εt such that $q \equiv -1 \pmod 4$.*

1. *The reduction of E_ε^t modulo q is supersingular and the group $E_\varepsilon^t(q)$ has order $q+1$.*
2. *If ε is not a square modulo q, then the group $E_\varepsilon^t(q)$ is cyclic and the only point of order 2 in $E_\varepsilon^t(q)$ is $(0,0)$.*

Proof. Because of the isogeny $\tau_{\varepsilon,t}$ from equation (1), we may assume that $t = 1$. Let i be a primitive fourth root of unity in $\overline{\mathbb{F}}_q$. Then the reduction $\widehat{E}_\varepsilon$ of E_ε modulo q has complex multiplication by $[i]$ as well. Let Φ be the q-th power Frobenius endomorphism and $P = (x, y)$ a point of E_ε. We have

$$(\Phi \circ [i])(P) = (-x^q, i^q y^q) = (-x^q, -i \cdot y^q) \quad \text{and} \quad ([i] \circ \Phi)(P) = (-x^q, iy^q).$$

Therefore the endomorphism ring $\mathrm{End}(\widehat{E}_\varepsilon)$ is not commutative, hence $\widehat{E}_\varepsilon$ is supersingular by [10, Theorem V.3.1]. Thus the abelian group $E_\varepsilon(q)$ has order $q+1$ (cf. [10, exercise 5.10]). This proves the first claim.
Let $[q+1]$ denote the isogeny of E_ε which multiplies each point on E_ε by $q+1$. The kernel of $[q+1]$ is isomorphic to $\mathbb{Z}/(q+1)\mathbb{Z} \times \mathbb{Z}/(q+1)\mathbb{Z}$ by [10, Corollary III.6.4]. Since $\#E_\varepsilon(q) = q+1$ we have $E_\varepsilon(q) \leq \ker([q+1])$. In particular, $E_\varepsilon(q) \cong (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z})$ where $d_1 \mid d_2$ and $d_1 \cdot d_2 = q+1$. Furthermore $d_1 \mid (q-1)$ since the Weil-pairing is surjective and Galois-invariant (cf. [10, Proposition III.8.1]). Thus $d_1 \mid \gcd(q-1, q+1) = 2$, so either $E_\varepsilon(q)$ is cyclic or all 2-torsion points of $\widehat{E}_\varepsilon$ are $\mathbb{F}_q$-rational, which means all roots of $x^3 - \varepsilon x = x \cdot (x^2 - \varepsilon)$ lie in $\mathbb{F}_q$. But this is impossible because ε is not a square in $\mathbb{F}_q$. Hence the group $E_\varepsilon(q)$ must be cyclic. □

Lemma 4.2. *Let $q \in \mathbb{P}$ be a prime not dividing $2\varepsilon t$ and let $P = (x_0, y_0) \in E_\varepsilon^t(q)$. If $x_0 t$ is not a square in $\mathbb{F}_q$, then P is not divisible by 2 in $E_\varepsilon^t(q)$.*

Proof. It suffices to show that $P' := \tau_{\varepsilon,t}(P) = (x_0 t, y_0 t^2)$ is not divisible by 2 in $E_{\varepsilon t^2}(q)$. Let $Q = (x, y)$ be a point in $E_{\varepsilon t^2}(q)$ such that $2 \cdot Q \neq \mathcal{O}$. Then we have

$$x(2 \cdot Q) = \frac{(x^2 + \varepsilon t^2)^2}{4 \cdot y^2},$$

which is a square in $\mathbb{F}_q$. Since $x_0 t = x(P')$ is not, there cannot be any point $Q \in E_{\varepsilon t^2}(q)$ such that $2 \cdot Q = P'$. □

5. Generalized Thabit numbers

5.1. Choosing the curve

For our primality test for generalized Thabit numbers $K(h,n) = h \cdot 2^n - 1$ in Theorem 5.5 we need a (twisted) rational elliptic curve E such that

$$\#E(K(h,n)) = K(h,n) + 1 = h \cdot 2^n$$

and a point that generates the Sylow-2-subgroup of $E(K(h,n))$ provided that $K(h,n)$ is prime.

Proposition 5.1. *Let $n \geq 2$ and $h \in \mathbb{N}$ be odd. Suppose there exists a pair $(\varepsilon, x_0) \in \mathbb{Z}^2$ such that*

$$\left(\frac{\varepsilon}{K(h,n)}\right) = \left(\frac{x_0^2 - \varepsilon}{K(h,n)}\right) = -1\,.$$

Write $x_0(x_0^2 - \varepsilon) = ty_0^2$ for some $t, y_0 \in \mathbb{Z}$. Then $P = (x_0, y_0) \in E_\varepsilon^t(\mathbb{Q})$. If $K(h,n)$ is prime then

1. *$K(h,n)$ does not divide x_0.*
2. *The reduction of E_ε^t modulo $K(h,n)$ is supersingular and $E_\varepsilon^t(K(h,n))$ is cyclic of order $h \cdot 2^n$.*
3. *The reduction of P modulo $K(h,n)$ is not divisible by 2 in $E_\varepsilon^t(K(h,n))$ and $h \cdot P$ generates the Sylow-2-subgroup of $E_\varepsilon^t(K(h,n))$.*

Proof. If $K(h,n)$ would divide x_0, then

$$-1 = \left(\frac{x_0^2 - \varepsilon}{K(h,n)}\right) = \left(\frac{-\varepsilon}{K(h,n)}\right) = \left(\frac{-1}{K(h,n)}\right)\left(\frac{\varepsilon}{K(h,n)}\right) = (-1)^2$$

which is impossible. In particular, $K(h,n)$ does not divide $x_0(x_0^2 - \varepsilon) = ty_0^2$. Hence the second statement immediately follows from Lemma 4.1.
Further, $(x_0 t)(x_0^2 - \varepsilon) = t^2 y_0^2$ is a square modulo $K(h,n)$ but $x^2 - \varepsilon$ is not. So $x_0 t$ is also not a square. By Lemma 4.2 the point P is not divisible by 2 in $E_\varepsilon^t(K(h,n))$. Thus $h \cdot P$ generates the Sylow-2-subgroup of $E_\varepsilon^t(K(h,n))$. □

Note that different factorizations of $x_0(x_0^2 - \varepsilon)$ into $t \cdot y_0^2$ yield isomorphic curves.

If h is not divisible by 3 then one can easily find pairs (ε, x_0) satisfying the conditions in Proposition 5.1 for all generalized Thabit primes of the form $K(h,n)$ by quadratic reciprocity.

Example 5.2. *Suppose $n \geq 3$ and let $h \in \mathbb{N}$ be odd and not divisible by 3. Then either $K(h,n)$ is divisible by 3 or $(\varepsilon, x_0) := (12, -2)$ satisfies the conditions in Proposition 5.1. Moreover, $x_0^3 - \varepsilon x_0 = 4^2$. Thus we can work with the global point $P = (-2, 4)$ on the elliptic curve E_{12}. This is the setup used by B. Gross in [3] for Mersenne numbers $M_p = K(1,p)$ where $p \in \mathbb{P}$.*

If h is divisible by 3 then it is not possible to find such a pair (ε, x_0) which is independent from h and n. However, we have the following lemma.

Lemma 5.3. *Let $h \in \mathbb{N}$ be odd and let $n \geq 2$.*

1. *There exists a minimal prime $p \in \mathbb{P}$ such that $\left(\frac{p}{K(h,n)}\right) \neq 1$.*
2. *Either p is a proper divisor of $K(h,n)$ or $(\varepsilon, x_0) := (p, 1)$ satisfies the conditions in Proposition 5.1.*

Proof. The integer $K(h,n)$ is not a square in $\mathbb{Z}$ since $K(h,n) \equiv -1 \pmod 4$. Thus the existence of a minimal number $p \in \mathbb{N}$ satisfying $\left(\frac{p}{K(h,n)}\right) \neq 1$ follows from the Chinese Remainder Theorem. Since the Jacobi symbol is multiplicative in the first component, any nontrivial factorization of p would yield a smaller number d with $\left(\frac{d}{K(h,n)}\right) \neq 1$, which is a contradiction to the minimality of p. Hence p must be prime.
Moreover, since $1 < p < K(h,n)$ we know that either p is a proper divisor of $K(h,n)$ or $\left(\frac{p}{K(h,n)}\right) = -1$. In the latter case, the choice of p implies $\left(\frac{p-1}{K(h,n)}\right) = 1$ and therefore

$$\left(\frac{x_0^2 - \varepsilon}{K(h,n)}\right) = \left(\frac{-1}{K(h,n)}\right)\left(\frac{p-1}{K(h,n)}\right) = -1 \cdot 1 = -1$$

as claimed. □

If $n \geq 3$ and $h \in \mathbb{N}$ is odd but not divisible by 3 then

$$\min\left\{q \in \mathbb{P} \mid \left(\frac{q}{K(h,n)}\right) \neq 1\right\} = 3\,.$$

Hence, if we plug $(\varepsilon, x_0) = (3, 1)$ into Proposition 5.1, we end up with the point $P = (1,1)$ on the curve E_3^{-2}. Under the isogeny $\tau_{3,-2}$ from equation (1) this point corresponds to the point $(-2, 4)$ on the curve E_{12}. So Example 5.2 is just a special case of Lemma 5.3.

The curve E_{12} has rank 1. Similarly, the rational curves E_1^{30} and the one given by $7y^2 = x^3 + 1$ also have rank 1. These latter curves were used in [2] for primality tests of Fermat numbers and numbers of the form $2^{2^\ell} - 2^{2^\ell - 1} + 1$ respectively. So one might wonder what are the ranks of the rational curves E_p^{1-p}.

Proposition 5.4. *Let p be a prime. Then the rank of the rational elliptic curve E_p^{1-p} is at least 1.*

Proof. For $p = 2$ one can check the rank explicitly. So suppose $p \geq 3$ and let m be the product of all primes $\leq p$. Then by the Chinese Remainder Theorem, there exists a positive odd number h such that $p = \min\{q \in \mathbb{P} \mid \left(\frac{q}{K(h,3)}\right) \neq 1\}$. For $k \in \mathbb{N}$ let $a_k = K(h + km, 3) = k \cdot (8m) + (8h - 1)$. Then $p = \min\{q \in \mathbb{P} \mid \left(\frac{q}{a_k}\right) \neq 1\}$ for all k. The choice of p implies $\gcd(8m, 8h - 1) = 1$. Thus the sequence (a_k) contains infinitely many primes by Dirichlet's theorem on arithmetic progressions. But then Lemma 5.3 and Proposition 5.1 imply that the rank of the twisted rational curve E_p^{1-p} cannot be 0. □

It turns out that the smallest prime p such that E_p^{1-p} has rank 2 is $p = 7$.

5.2. An elliptic curve primality test for generalized Thabit numbers

Now we are able to prove the main theorem of this paper, which gives a primality test for numbers of the form $K(h, n)$.

Let (ε, x_0) a pair of integers that satisfies the conditions of Proposition 5.1. See Example 5.2 or Lemma 5.3 on how to find such a pair. Write $x_0^3 - \varepsilon x_0 = ty_0^2$ for some $y_0, t \in \mathbb{Z}$ and set $P = (x_0, y_0) \in E_\varepsilon^t(\mathbb{Q})$.

Now we recursively define a sequence of rational numbers as follows:

$$T_0 := x(h \cdot P) \text{ and } T_{k+1} := \frac{(T_k^2 + \varepsilon)^2}{4T_k(T_k^2 - \varepsilon)} \tag{2}$$

Then $T_k = x(h2^k \cdot P)$ for all $k \geq 0$. Also note that the initial value T_0 only depends on x_0 and ε. Moreover, it can be computed without knowing y_0 and t as explained in Remark 5.7 below.

Theorem 5.5. *Let $h \in \mathbb{N}$ be odd and $n > \log_2(h) + 2$ be some integer. Suppose $(\varepsilon, x_0) \in \mathbb{Z}^2$ satisfies the conditions of Proposition 5.1 and let (T_k) be the sequence defined in equation (2). Then the number $K(h, n) = h \cdot 2^n - 1$ is prime if and only if the following three conditions are met:*

- $\gcd(K(h, n), x_0) = 1$.
- *$T_k(T_k^2 - \varepsilon)$ is a unit in $\mathbb{Z}/K(h, n)\mathbb{Z}$ for all $0 \leq k \leq n - 2$.*
- $T_{n-1} \equiv 0 \pmod{K(h, n)}$.

Proof. Write $x_0^3 - \varepsilon x_0 = ty_0^2$ for some $y_0, t \in \mathbb{Z}$. Further let $Q = h \cdot P$ where P denotes the point $(x_0, y_0) \in E_\varepsilon^t(\mathbb{Q})$.
First, suppose that $K(h, n)$ is prime. Then $\gcd(x_0, K(h, n)) = 1$ by Proposition 5.1. This proposition also shows that the point Q generates the Sylow-2-subgroup of the cyclic group $E_\varepsilon^t(K(h, n)) \cong C_h \times C_{2^n}$. Hence Q has order 2^n, which implies $2^{n-1} \cdot Q = (0, 0)$ is the unique point of order 2. In particular, $2^k \cdot Q \neq (0, 0)$ for all $k \in$

$\{0,\dots,n-2\}$. The duplication formula shows that $T_k \equiv x(2^k \cdot Q) \pmod{K(h,n)}$, so we have that $T_{n-1} \equiv 0 \pmod{K(h,n)}$ and $T_k \not\equiv 0 \pmod{K(h,n)}$ for $0 \leq k \leq n-2$. Therefore T_k is invertible in $\mathbb{Z}/K(h,n)\mathbb{Z}$ for all $0 \leq k \leq n-2$. The same holds for $T_k^2 - \varepsilon$ since ε is not a square modulo $K(h,n)$.
Conversely, suppose that $K(h,n)$ is composite and satisfies the three conditions above. Let $q \leq \sqrt{K(h,n)}$ be the smallest positive prime divisor of $K(h,n)$. Note that by assumption $q \neq 2$ is coprime to x_0, $x_0^2 - \varepsilon$ and ε. So q does also not divide $x_0(x_0^2 - \varepsilon) = ty_0^2$. In particular, $\gcd(q, 2\varepsilon t) = 1$. Thus E_ε^t has good reduction modulo q. By assumption, $2^{n-1} \cdot Q$ has order 2 in $E_\varepsilon^t(q)$, so Q has order 2^n in $E_\varepsilon^t(q)$. Since $(0,0) \in E_\varepsilon^t(q)$ is the only point with x-coordinate 0, we get the trivial bound $\#E_\varepsilon^t(q) \leq 2q$. But then

$$2^n \leq \#E_\varepsilon^t(q) \leq 2q \leq 2\sqrt{K(h,n)} = 2^{\frac{n+\log_2(h)}{2}+1},$$

which is impossible by the choice of n. Hence q does not exist. □

If $h = 1$ and $(\varepsilon, x_0) = (12, -2)$ then the above primality criterion is the same as the one found by Gross in [3] for Mersenne numbers $M_p = K(1,p)$. Also note that if one chooses (ε, x_0) as in Example 5.2 or Lemma 5.3 then $x_0 \in \{1, -2\}$. Hence the condition $\gcd(K(h,n), x_0) = 1$ is always satisfied.

Remark 5.6. *The primality test given in Theorem 5.5 is based on the following idea. The candidate $K(h,n)$ is prime if and only if the reduction of $h \cdot P$ modulo $K(h,n)$ generates a cyclic subgroup of order 2^n. So it is completely analogous to the Lucas-Lehmer-Riesel test (see Remark 2.5).*

We close this section with a remark concerning the implementation of the above primality criterion.

Remark 5.7. *If $K(h,n)$ is prime then the order of $P = (x_0, y_0) \in E_\varepsilon^t(\mathbb{Q})$ is at least $2^n > h$ (see Lemma 4.1). So in particular, $m \cdot P \neq \mathcal{O}$ for any $1 \leq m \leq h$. Let $1 \leq m \leq h$ and $\alpha \in \mathbb{C}$ such that $\alpha^2 = t$. Then Lemma 3.2 and the change of coordinates*

$$E_\varepsilon^t(\mathbb{C}) \to E_\varepsilon(\mathbb{C}),\ (x,y) \mapsto (x, \alpha y)$$

show that $m \cdot P = (f_m, g_m y_0)$ for some $f_m, g_m \in \mathbb{Q}$ that only depend on ε, x_0 and $ty_0^2 = x_0^3 - \varepsilon x_0$. Thus without actually knowing t or y_0, one can compute $T_0 = x(h \cdot P) = f_h$ using "square and multiply" by adding at most $2\log_2(h)$ points.

Moreover, these calculations can be done directly in $\mathbb{Z}/K(h,n)\mathbb{Z}$. This has the advantage that if a necessary computation cannot be performed in $\mathbb{Z}/K(h,n)\mathbb{Z}$ (i.e. some nonzero element cannot be inverted) then $K(h,n)$ is immediately proven not to be prime. The same holds for the computation of $T_1, T_2, \dots$.

6. Efficiency

We have implemented our primality test for generalized Thabit numbers as well as the Lucas-Lehmer-Riesel test in MAGMA (see [1]) to compare the efficiency of both tests. All tests were performed on a Core i7, 940 running at 2.93 GHz.

In our primality test it is necessary to divide in the residue class ring $\mathbb{Z}/K(h,n)\mathbb{Z}$. Thus on the one hand the calculations in each step of the iteration are more complex than the calculations in the Lucas-Lehmer-Riesel test (four multiplications and one division versus one multiplication in the ring $\mathbb{Z}/K(h,n)\mathbb{Z}$) but on the other hand we know that, if the necessary division is not possible, $K(h,n)$ cannot be prime. So if $K(h,n)$ is composite, it might happen that the algorithm aborts without computing all values $T_0, T_1, \ldots, T_{n-1}$ modulo $K(h,n)$.

For example, $K(3, 100\,008)$ is composite and the Lucas-Lehmer-Riesel test as well as MAGMA's build-in primality test both take about 4 minutes to verify that. Our elliptic curve test (using $(\varepsilon, x_0) = (5, 1)$) recognizes this in virtually no time since already $T_4 \pmod{K(h,n)}$ does not exist.

To see how often such premature aborts occur, we have run the Lucas-Lehmer-test and our primality test using 27 different pairs (ε, x_0) for Mersenne primes in MAGMA to compute a list of all prime exponents $3 \leq p \leq 10\,000$, such that the Mersenne number $M_p = K(1,p) = 2^p - 1$ is prime. For some pairs (ε, x_0), there was no premature abort at all, for others there were up to five. Table 1 gives the chosen values ε (where $\varepsilon = 0$ represents the Lucas-Lehmer-test), the chosen initial values $T_0 = x_0$, the exponents p that yield an premature abort, and the time in seconds required for the test.

We see that it takes the elliptic curve tests about 50 times as long as the Lucas-Lehmer-test to do the task. This is easily explained by the fact that there were never more than four exponents out of 1 228 (i.e. the number of odd primes $\leq$ 10 000), which yielded an premature abort. So the possible advantage of the elliptic curve tests towards the Lucas-Lehmer-test does not play any significant role for the efficiency on average.

Similarly, we considered generalized Thabit numbers. We compared the Lucas-Lehmer-Riesel test (LLR) to Theorem 5.5 (where the pair (ε, x_0) was chosen as in Lemma 5.3) and measured the time needed to compute all exponents $\log_2(h) + 2 < n \leq 3\,000$ such that $K(h,n)$ is prime for all odd numbers $h \in \{1, \ldots 99\}$ using both tests. Additionally we calculated the ratio ρ of premature aborts that occurred using the algorithm from Theorem 5.5 to the number of composite generalized Thabit numbers in the tested range. The results are given in Table 2.

Note that $n \geq 3$, i.e. $\left(\frac{2}{K(h,n}\right) = 1$. So if $K(h,n)$ is divisible by 3, then Lemma 5.3 will immediately detect this. Hence we excluded all pairs (h,n) from the test for which Lemma 5.3 does find a nontrivial divisor since this would definitely favor our

algorithm. Moreover, any serious implementation of a primality test would test for small prime factors anyway.

By our experiments we conclude that our test is obviously less efficient than the Lucas-Lehmer-Riesel test. Although in some cases, where there are very many premature aborts (for example for $h = 11$ or $h = 71$) we are very close to its efficiency. We also see, that the value of ρ does indeed play a significant role for the velocity of our test. But still there are not enough premature aborts to compensate the fact that the calculations in each iteration step are much more expensive for our test compared to the Lucas-Lehmer-Riesel test.

ε	$T_0 = x_0$	Abort at	Time in sec.
0	-	-	71
-242	1	-	3544
-242	25	47, 191, 397, 1013	3550
-242	29	113, 4649	3550
-242	101	11	3548
-242	115	11, 23, 191, 5717, 6491	3537
-50	2	11, 37, 191	3542
-50	26	-	3541
-50	46	11, 23, 47, 1321	3543
-2	1	-	3540
-2	2	-	3539
-2	5	11, 37, 191	3540
-2	19	11, 23, 179	3540
-2	22	-	3539
-2	71	191, 9791	3529
3	1	23	3535
3	3	23	3534
3	27	11, 23, 47, 191, 743	3536
6	2	11, 37, 47, 191	3537
6	3	11, 37, 47, 191	3537
6	9	-	3536
6	33	23	3537
6	123	431, 3023	3535
27	5	37	3536
54	2	-	3534
75	9	37	3537
75	33	191, 4871	3536
243	1	11, 23, 47, 191, 743	3537

Table 1: Efficiency of the tests for Mersenne numbers

h	n for which $K(h,n)$ is prime	ρ (in %)	LLR (in sec)	Thm 5.5 (in sec)
1	3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281	66.3	8	67
3	4, 6, 7, 11, 18, 34, 38, 43, 55, 64, 76, 94, 103, 143, 206, 216, 306, 324, 391, 458, 470, 827, 1274	34.1	21	208
5	8, 10, 12, 14, 18, 32, 48, 54, 72, 148, 184, 248, 270, 274, 420, 1340, 1438, 1522, 1638, 1754, 1884, 2014, 2170, 2548, 2622, 2652, 2704	14.1	14	185
7	5, 9, 17, 21, 29, 45, 177	26.7	14	157
9	7, 13, 15, 21, 43, 63, 99, 109, 159, 211, 309, 343, 415, 469, 781, 871, 939, 1551	52.2	20	141
11	26, 50, 54, 126, 134, 246, 354, 362, 950, 1310, 2498	76.9	14	50
13	7, 23, 287, 291, 795, 2203	31.9	14	148
15	10, 14, 17, 31, 41, 73, 80, 82, 116, 125, 145, 157, 172, 202, 224, 266, 289, 293, 463, 1004, 1246, 2066, 2431, 2705	39.3	18	157
17	16, 20, 36, 54, 60, 96, 124, 150, 252, 356, 460, 612, 654, 664, 698, 702, 972, 1188, 1312	21.2	14	172
19	21, 41, 49, 89, 133, 141, 165, 189, 293, 305, 395, 651, 665, 771, 801, 923, 953	27.2	14	158
21	7, 10, 13, 18, 27, 37, 51, 74, 157, 271, 458, 530, 891, 1723, 1793, 1849, 1986, 2191, 2869	37.6	19	180
23	12, 46, 72, 244, 264, 544, 888, 1146	46.4	14	116
25	9, 11, 17, 23, 35, 39, 75, 105, 107, 155, 161, 215, 225, 335, 635, 651, 687, 1479, 1515, 1953, 2435, 2963	49.4	14	110
27	8, 10, 14, 28, 37, 38, 70, 121, 122, 160, 170, 253, 329, 362, 454, 485, 500, 574, 892, 962, 1213, 1580, 2642, 2708	43.8	20	172
29	16, 76, 148, 184	36.7	14	135
31	7, 11, 13, 23, 33, 35, 37, 47, 115, 205, 235, 271, 409, 739, 837, 887, 2189	31.9	14	146
33	8, 10, 22, 35, 42, 43, 46, 56, 91, 102, 106, 142, 190, 208, 266, 330, 360, 382, 462, 503, 815, 1038, 1651, 1855, 1858, 1992, 2232	25.6	22	243
35	10, 20, 44, 114, 146, 156, 174, 260, 306, 380, 654, 686, 702, 814, 906, 1196, 1316	47.7	14	116
37	2553	51.3	14	105

h	n for which $K(h,n)$ is prime	ρ (in %)	LLR (in sec)	Thm 5.5 (in sec)
39	24, 105, 153, 188, 605, 795, 813, 839, 2135, 2619	64.4	19	102
41	10, 14, 18, 50, 114, 122, 294, 362, 554, 582, 638, 758	57.8	14	91
43	31, 67, 251, 767, 1171, 1643	74.4	14	56
45	8, 9, 14, 15, 16, 22, 28, 29, 36, 37, 54, 59, 85, 93, 117, 119, 161, 189, 193, 256, 308, 322, 327, 411, 466, 577, 591, 902, 928, 946, 1162, 1428, 1708, 1724, 2063, 2922, 2951	43.9	28	226
47	14, 70, 78, 1374, 1824, 2158, 2654	40.2	14	129
49	9, 13, 15, 29, 33, 39, 55, 81, 95, 205, 279, 581, 807, 813, 2551, 2565	20.5	14	170
51	9, 10, 19, 22, 57, 69, 97, 141, 169, 171, 195, 238, 735, 885, 1287, 1365, 2026, 2211, 2361, 2889	63.4	18	102
53	8, 42, 50, 62, 362, 488, 642, 846, 2870	55.5	14	96
55	15, 33, 41, 57, 69, 75, 77, 131, 133, 153, 247, 305, 351, 409, 471, 1251, 1259, 2253, 2411, 2425, 2699	31.9	14	147
57	8, 10, 20, 22, 25, 26, 32, 44, 62, 77, 158, 317, 500, 713, 1657, 1790, 2761, 2794	37.5	19	178
59	12, 16, 72, 160, 256, 916, 1216, 1840	24.6	14	161
61	9, 13, 17, 19, 25, 39, 63, 67, 75, 119, 147, 225, 419, 715, 895, 1025, 1103, 1179, 1345, 1829	34.8	14	141
63	8, 11, 14, 16, 28, 32, 39, 66, 68, 91, 98, 116, 126, 164, 191, 298, 323, 443, 714, 758, 759, 1059, 1168, 1511, 1792, 2116	45.7	21	175
65	12, 22, 28, 52, 78, 94, 124, 162, 174, 192, 204, 304, 376, 808, 930, 972, 1714, 1776, 2176, 2568	44.6	15	122
67	9, 21, 45, 65, 77, 273, 677, 1049, 1721	36.5	14	138
69	9, 11, 13, 17, 19, 23, 29, 37, 49, 61, 79, 99, 121, 133, 141, 164, 173, 181, 185, 193, 233, 299, 313, 351, 377, 540, 569, 909, 1057, 1081, 1189, 1679, 2043, 2641	20.8	22	260
71	14, 410, 1390	72.4	14	61
73	11, 19, 71, 79, 131, 1167, 1191	30.6	14	151
75	18, 19, 20, 22, 28, 29, 39, 43, 49, 75, 85, 92, 111, 126, 136, 159, 162, 237, 349, 381, 767, 969, 1247, 1893, 1951, 2363, 2657	45.1	28	221

h	n for which $K(h,n)$ is prime	ρ (in %)	LLR (in sec)	Thm 5.5 (in sec)
77	14, 26, 58, 60, 64, 100, 122, 212, 566, 638, 1214, 2080	15.8	14	182
79	15, 43, 57, 61, 75, 145, 217, 247, 2803	55.1	14	98
81	11, 17, 21, 27, 81, 101, 107, 327, 383, 387, 941, 1665	55.3	19	132
83	10, 14, 18, 22, 24, 26, 28, 36, 42, 58, 64, 78, 158, 198, 206, 424, 550, 676, 904, 1276, 1374, 1536, 1642, 2124, 2796	29.0	14	154
85	11, 71, 113, 115, 355, 473, 563, 883, 1235	68.7	14	69
87	9, 10, 12, 22, 29, 32, 50, 57, 69, 81, 122, 138, 200, 296, 514, 656, 682, 778, 881, 1422, 1494, 1857	35.7	20	200
89	12, 24, 48, 52, 64, 84, 96, 1272, 2028	53.3	14	102
91	9, 13, 15, 17, 19, 23, 47, 57, 67, 73, 77, 81, 83, 191, 301, 321, 435, 867, 869, 917	20.3	14	172
93	10, 15, 18, 19, 24, 27, 39, 60, 84, 111, 171, 192, 222, 639, 954, 2400, 2587	45.6	19	153
95	26, 32, 66, 128, 170, 288, 320, 470, 1278, 1296, 1316, 1536, 1608	58.2	14	91
97	9, 45, 177, 585, 1409, 2617	34.0	14	142
99	11, 19, 25, 28, 35, 65, 79, 212, 271, 361, 461, 1237, 1297, 1577, 1747, 1901, 1943, 2741	31.1	19	197

Table 2: Efficiency of the tests for Thabit numbers

Acknowledgments

The authors would like to thank the anonymous referee and the editors for several helpful comments and suggestions.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I The user language. *Journal of Symbolic Computation*, 24:235–265, 1997.

[2] Robert Denomme and Gordan Savin. Elliptic curve primality tests for fermat and related primes. *Journal of Number Theory*, 128:2398–2412, 2008.

[3] Benedict H. Gross. An elliptic curve test for Mersenne primes. *Journal of Number Theory*, 110:114–119, 2005.

[4] Serge Lang. *Elliptic Curves - Diophantine Analysis*. Springer-Verlag, 1978.

[5] Derrick Henry Lehmer. On Lucas's test for the primality of Mersenne's numbers. *Journal of the London Mathematical Society*, 10:162–165, 1935.

[6] Édouard Lucas. Nouveaux théorèmes d'Arithmétique supérieur. *C.R. Acad. Sci. Paris*, 83:1286–1288, 1876.

[7] Carl Pomerance. Primality testing: variations on a theme of lucas. *Congressus Numerantium*, 201:301–312, 2010.

[8] Hans Riesel. Lucasian Criteria for the Primality of $\mathcal{N} = h \cdot 2^n - 1$. *Mathematics of Computation*, 23(108):869–875, 1969.

[9] Michael Rosen. A proof of the Lucas-Lehmer test. *American Mathematical Monthly*, 95:855–856, 1995.

[10] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.