Journal of Integer Sequences, Vol. 21 (2018),
Article 18.6.2

A Proof of the Lucas-Lehmer Test and its Variations by Using a Singular Cubic Curve

Ömer Küçüksakallı
Mathematics Department
Middle East Technical University
06800 Ankara
Turkey
komer@metu.edu.tr

Abstract

We give another proof of the Lucas-Lehmer test by using a singular cubic curve. We also illustrate a practical way to choose a starting term for the Lucas-Lehmer-Riesel test by trial and error. Moreover, we provide a nondeterministic test for determining the primality of integers of the form $N = hp^n - 1$ for any odd prime p. We achieve these by using the group structure on a singular cubic curve induced from the group law of elliptic curves.

1 Introduction

The largest primes known are given by expressions of the type $N = 2^n - 1$ since there is an efficient, deterministic primality test for such integers.

Theorem 1 (Lucas-Lehmer)**.** *Let $S_0 = 4$. If we define $S_k = S_{k-1}^2 - 2$ for all $k \geq 1$ recursively, then the integer $N = 2^n - 1$ is prime if and only if $S_{n-2} \equiv 0 \pmod{N}$.*

There are already several proofs of this fact in the literature [3, 4, 6, 8, 11, 12]. In this paper, we give another proof by using a singular cubic curve. Secondly, we illustrate a practical way to choose S_0 by trial and error for the Lucas-Lehmer-Riesel test, which is concerned with the integers of the form $N = h2^n - 1$. Finally, we give a nondeterministic test for determining the primality of integers of the form $N = hp^n - 1$ for an odd prime p.

2 Main results

Consider the projective curve

$$C : y^2 = 4x^3 + x^2.$$

Let K be an arbitrary field with $\mathrm{char}(K) \neq 2$. The curve C is a singular cubic curve defined over K that has a node at the origin. There are two distinct tangent lines at the origin, namely $y = x$ and $y = -x$. The cubic curve C and these tangent lines are illustrated in Figure 1.

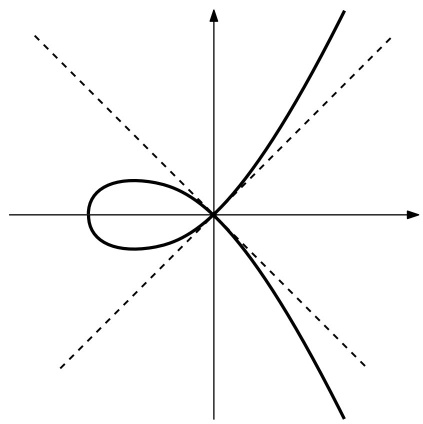

Figure 1: Cubic curve $C : y^2 = 4x^3 + x^2$.

The non-singular part of C with coordinates from K is denoted by $C_{\mathrm{ns}}(K)$. The group law of elliptic curves makes $C_{\mathrm{ns}}(K)$ into an abelian group. Moreover, we have the following characterization for this group.

Proposition 2. *The map $\psi : C_{ns}(K) \to K^*$ given by the formula $\psi(x, y) = \frac{y-x}{y+x}$ is a group isomorphism.*

Proof. See [13, Prop. III.2.5] and [13, Exer. 3.5]. ☐

There is a connection between the map $x \mapsto x^2 - 2$ and the duplication map on $C_{\mathrm{ns}}(K)$. To see this connection, we follow [5] and consider

$$\phi(z) = \frac{e^z}{(1 - e^z)^2}$$

and its derivative

$$\phi'(z) = \frac{e^z(e^z + 1)}{(1 - e^z)^3}.$$

It is easily verified that the cubic curve $C : y^2 = 4x^3 + x^2$ is parametrized by $x = \phi(z)$ and $y = \phi'(z)$. Note that $\psi((\phi(z), \phi'(z))) = e^z$ under the isomorphism of Proposition 2. It follows that $[n](\phi(z), \phi'(z)) = (\phi(nz), \phi'(nz))$ since $(e^z)^n = e^{nz}$.

The family of Dickson polynomials, denoted $\mathcal{D}_n(x)$, is a normalization of Chebyshev polynomials that is used in the theory of finite fields [7]. For each integer n, the polynomial $\mathcal{D}_n(x)$ is uniquely defined by the equation $\mathcal{D}_n(y+y^{-1}) = y^n+y^{-n}$ where y is an indeterminate. The first few examples of these polynomials are $\mathcal{D}_1(x) = x, \mathcal{D}_2(x) = x^2 - 2$ and $\mathcal{D}_3(x) = x^3 - 3x$. Note that $\phi(z) = 1/(e^z + e^{-z} - 2)$. Now, it is clear that

$$\mathcal{D}_n\left(\frac{1}{\phi(z)} + 2\right) = \mathcal{D}_n(e^z + e^{-z}) = e^{nz} + e^{-nz} = \frac{1}{\phi(nz)} + 2.$$

For any integer $n \geq 1$, define $f_n(x) := 1/(\mathcal{D}_n(1/x + 2) - 2)$. The rational function $f_n(x)$ satisfies the functional equation $f_n(\phi(z)) = \phi(nz)$ by the computation above. Let π_x be the projection to the first coordinate. Set $L(x) = 1/x + 2$. We write $\mathbf{P}^1(K) = K \cup \{\infty\}$. We have the following commutative diagram:

$$\begin{tikzcd}
C_{\mathrm{ns}}(K) \arrow[r, "{[n]}"] \arrow[d, "\pi_x"'] & C_{\mathrm{ns}}(K) \arrow[d, "\pi_x"] \\
\mathbf{P}^1(K) \arrow[r, "f_n"] \arrow[d, "L"'] & \mathbf{P}^1(K) \arrow[d, "L"] \\
\mathbf{P}^1(K) \arrow[r, "\mathcal{D}_n"] & \mathbf{P}^1(K)
\end{tikzcd}$$

For the case $n = 2$, we have

$$[2](x, y) = \left(\frac{x^2}{4x+1}, \frac{x^3(2x+1)}{y(4x+1)}\right).$$

The rational map f_2 associated with the duplication map on $C_{\mathrm{ns}}(K)$ is given by $f_2(x) = x^2/(4x+1)$. Recall that it satisfies the relation $f_2(x) = 1/(\mathcal{D}_2(1/x+2) - 2)$ where $\mathcal{D}_2(x) = x^2 - 2$.

There is a unique point of $C_{\mathrm{ns}}(K)$ of order two, namely $(-1/4, 0)$. Note that there are two points of order four, namely $(-1/2, i/2)$ and $(-1/2, -i/2)$. To see this, we can use $f_4(x) = f_2(f_2(x)) = x^4/((2x+1)^2(4x+1))$.

The following fact is the key argument to our alternative proof of Theorem 1.

Lemma 3. *Let p be an odd prime and let $P = (x, y)$ be a point of $C_{ns}(\mathbf{F}_{p^2})$. If $x \in \mathbf{F}_p$, then the order of P, denoted $o(P)$, satisfies the following:*

1. *$o(P)$ divides $p - 1$ if $y \in \mathbf{F}_p$, and*
2. *$o(P)$ divides $p + 1$ if $y \notin \mathbf{F}_p$.*

Proof. If both coordinates of P are in $\mathbf{F}_p$, then $\psi(x, y) = \frac{y-x}{y+x} \in \mathbf{F}_p^*$. We have $\psi(x, y)^{p-1} = 1$ and we conclude that $o(P)$ divides $p - 1$ by Proposition 2.

Now suppose that $x \in \mathbf{F}_p$ but $y \notin \mathbf{F}_p$. We have $y^p = -y$ because $y^2 = 4x^3 + x^2$. Observe that

$$\psi(x,y)^{p+1} = \left(\frac{y-x}{y+x}\right)^p \left(\frac{y-x}{y+x}\right) = \left(\frac{-y-x}{-y+x}\right)\left(\frac{y-x}{y+x}\right) = 1.$$

We conclude that $o(P)$ divides $p+1$ by Proposition 2. $\square$

A natural generalization of the Lucas-Lehmer test, namely the Lucas-Lehmer-Riesel test, is concerned with integers of the form $N = h2^n - 1$ for odd integers h. The recurrence relation is the same for this generalized test. However, the starting value S_0 varies depending on both h and n. Historically, the proof of this theorem was obtained in several steps:

1. If $h = 1$, and if $n \equiv 3 \pmod 4$ then pick $S_0 = 3$. [8]
2. If $h = 1$, and if $n \equiv 1 \pmod 2$ then choose $S_0 = 4$. [6]
3. If $h = 3$, and if $n \equiv 0, 3 \pmod 4$, then choose $S_0 = 5778$. [6]
4. If $h \equiv 1, 5 \pmod 6$, and if $3 \nmid N$, then choose $S_0 = w^h + w^{-h}$ where $w = 2 + \sqrt{3}$. [9]
5. Otherwise, h is a multiple of 3 and we follow [10] to choose S_0.

Unfortunately, there may not be any canonical value for S_0 even though the h value is fixed [2]. On the other hand, it is easy to choose S_0 by trial and error in practice by using the Jacobi symbol. For this purpose, we give the following method, which is inspired by [12].

Theorem 4. *Given $N = h2^n - 1$, with $n > 1$, h odd and $0 < h < 2^{n+1} - 1$, let D be a positive integer such that the Jacobi symbol satisfies $\left(\frac{D}{N}\right) = -1$ and $\left(\frac{D-1}{N}\right) = 1$. Define a sequence by*

$$S_0 = \mathcal{D}_h\left(\frac{2(D+1)}{D-1}\right) \quad \text{and} \quad S_k = \mathcal{D}_2(S_{k-1})$$

for $k \geq 1$. Then N is prime if and only if N divides S_{n-2}.

Proof. Suppose that N is prime. Then the Jacobi symbol reduces to the Legendre symbol. If $t = L^{-1}(\frac{2(D+1)}{D-1}) = (D-1)/4$, then $4t + 1 = D \pmod N$. Consider the point $P = (t, t\sqrt{D}) \in C_{\mathrm{ns}}(\mathbf{F}_{N^2})$. The order of P is a divisor of $N + 1 = h2^n$ by Lemma 3. We claim that $P \neq [2]Q$ for any $Q = (x, y)$ with $x \in \mathbf{F}_N$. Assume otherwise, i.e., $f_2(x) = t$ for some $x \in \mathbf{F}_N$. It follows that $x^2/(4x+1) = x^4/y^2 = (D-1)/4$ and therefore $y^2 = 4x^4/(D-1)$. This gives $y \in \mathbf{F}_N$ because $D - 1$ is a square modulo N. However, this is a contradiction because $P = [2]Q$ implies that P has both coordinates in $\mathbf{F}_N$. Thus, the point $[h]P$ has order precisely 2^n. Finally, the point $[2^{n-2}][h]P$ is of order 4. There are two such points, namely $(-1/2, \pm i/2)$. In either case the x-coordinate is $-1/2$. Thus $f_{2^{n-2}}(f_h(t)) = -1/2$ and as a result $\mathcal{D}_{2^{n-2}}(\mathcal{D}_h(s)) = L(-1/2) = 0$. This finishes the proof of necessity.

Suppose that N is composite. Let p be a prime factor of N with Jacobi symbol $\left(\frac{D}{p}\right) = -1$. In $C_{\mathrm{ns}}(\mathbf{F}_{p^2})$, we have $[p+1]P = \infty$ by Lemma 3. Therefore $[p+1][h]P = \infty$ as well. On the other hand, assume that $\mathcal{D}_{2^{n-2}}(S_0) \equiv 0 \pmod{N}$. It follows that $[h2^{n-2}]P = (-1/2, \pm i/2)$ and therefore $[2^n][h]P = \infty$ in $C_{\text{ns}}(\mathbf{F}_{p^2})$. If the order of $[h]P$ was a proper divisor of 2^n, then the equality $[2^{n-2}]P = (-1/2, \pm i/2)$ would not hold. We conclude that the order of $[h]P$ is precisely 2^n and therefore 2^n divides $p+1$. Thus $p+1 = 2^n k$ for some integer $k \geq 1$. From this point on, we follow [12]. We have $h2^n - 1 = N = (2^n k - 1)\ell$ for some integer ℓ. Reducing everything modulo 2^n, it is easily seen that $\ell = 2^n m + 1$ for some integer m. Since $N \neq p$, it is obvious that $m \geq 1$. If $k = m = 1$, then $h = 2^n$, which is a contradiction. Hence $k \geq 2$ or $m \geq 2$, and therefore $h \geq 2^{n+1} - 1$. $\square$

Remark 5. This proof constitutes an alternative proof for the Lucas-Lehmer test if we fix $h = 1$ and $D = 3$. In that case $N = 2^n - 1 \equiv 7 \pmod{24}$ for any integer $n \geq 3$. Clearly $\left(\frac{3}{N}\right) = -1$ and $\left(\frac{2}{N}\right) = 1$. Moreover $S_0 = \mathcal{D}_1(4) = 4$.

We also note that Lehmer's choice $S_0 = 5778$ for the case $h = 3$ and $n \equiv 0, 3 \pmod{4}$ is obtained by choosing $D = 5/4$. It follows that $2(D+1)/(D-1) = 18$ and therefore $S_0 = \mathcal{D}_3(18) = 5778$. Another choice could be $D = 5$, which would give $S_0 = 18$ according to the above theorem.

Now let us consider Riesel's choice $S_0 = \mathcal{D}_h(4)$ for the case $h \equiv 1, 5 \pmod{6}$, and $3 \nmid N$. This is obtained by choosing $D = 3$ in the above theorem. The facts $\left(\frac{3}{N}\right) = -1$ and $\left(\frac{2}{N}\right) = 1$ for $N = h2^n - 1$ can be verified easily by using the properties of the Jacobi symbol.

Now we give a test for determining the primality of integers of the form $N = hp^n - 1$ for an odd prime p. Unlike the previous theorem, it is not deterministic after S_0 is chosen. This theorem is inspired by the results of Williams, which are concerned with the primes $p = 3, 5$ and 7 [14, 15].

Theorem 6. *Let p be a prime and let $N = hp^n - 1$ be an odd integer, with $n > 1$ and* $\gcd(h, p) = 1$. *Let D be a positive integer such that the Jacobi symbol satisfies $\left(\frac{D}{N}\right) = -1$ and $\left(\frac{D-1}{N}\right) = 1$. Define the generalized Lucas sequence by*

$$S_0 = \mathcal{D}_h\left(\frac{2(D+1)}{D-1}\right) \quad \text{and} \quad S_k = \mathcal{D}_p(S_{k-1})$$

for $k \geq 1$. This sequence has the following properties:

1. *If $S_k \not\equiv 2 \pmod{N}$ for all $k \leq n$, then N is composite.*
2. *If $S_k \equiv 2 \pmod{N}$ for some positive minimal integer $k \leq n$ and $p^{2k} > N$ then N is prime.*

Proof. Suppose that N is prime. As in the proof of the previous theorem, let $P = (t, t\sqrt{D})$ with $t = L^{-1}(\frac{2(D+1)}{D-1}) = (D-1)/4$. The order of $P \in C_{\text{ns}}(\mathbf{F}_{N^2})$ is a divisor of $N+1 = hp^n$ by Lemma 3. It follows that the order of $[h]P$ is a divisor of p^n. Then we must have $[p^k]P = \infty$ for some $k \leq n$. This finishes the proof of the first part. Now, suppose that N is composite. Let q be a prime factor of N with the Jacobi symbol $\left(\frac{D}{q}\right) = -1$. In $C_{\text{ns}}(\mathbf{F}_{q^2})$, we have $[q+1]P = \infty$ by Lemma 3. Therefore $[q+1][h]P = \infty$, too. On the other hand, assume that

$\mathcal{D}_{p^k}(S_0) \equiv 2 \pmod{N}$ for some minimal positive integer k. It follows that the order of $[h]P$ is p^k. We conclude that p^k divides $q+1$, i.e., $q+1 = p^k\ell$ for some integer positive integer ℓ. We have $hp^n - 1 = N = (p^k\ell - 1)m$ for some integer m. Reducing everything modulo p^k, it is easily seen that $m = p^k a + 1$ for some integer a. Since $N \neq p$, it is obvious that $a \geq 1$. Hence $\ell \geq 1$ or $a \geq 1$, and therefore $p^{2k} \leq N$. $\square$

We remark that the inequality $p^{2k} > N$ in the second part of the above theorem can be improved as in [15]. We will leave it as it is for simplicity since this test is far from being deterministic in either case. On the other hand it is a common practice in algorithmic number theory to use a random element of a cyclic group since its order is expected to be large most of the time.

In order to make the above theorem deterministic, after S_0 is chosen, we need to prove that the congruence $\mathcal{D}_p(x) \equiv S_0 \pmod{N}$ has no solution if N is prime. It would then imply that P has order precisely p^n. In that case, we could replace the second part of the above theorem as: "Otherwise, $S_n \equiv 2 \pmod{N}$ and N is prime if $p^n > h$". This would give us a necessary and sufficient test if $p^n > h$. More precisely, we would be able to say that $N = hp^n - 1$ is prime if and only if $S_n \equiv 2 \pmod{N}$. This idea has already been accomplished by Berrizbeitia and Berry for $p = 3$ by using the cubic reciprocity law [1]. We hope that the isomorphism of Proposition 2 together with the higher degree reciprocity laws may shed some light in the future for the cases $p \geq 5$.

3 Acknowledgment

The author thanks S. Wong and an anonymous referee for their helpful comments and suggestions to improve this manuscript.

References

[1] P. Berrizbeitia and T. G. Berry, Cubic reciprocity and generalised Lucas-Lehmer tests for primality of $A \cdot 3^n \pm 1$, *Proc. Amer. Math. Soc.* **127** (1999), 1923–1925.

[2] W. Bosma, Explicit primality criteria for $h2^k \pm 1$, *Math. Comp.* **61** (1993), 97–109.

[3] J. W. Bruce, A really trivial proof of the Lucas-Lehmer test, *Amer. Math. Monthly* **100** (1993), 370–371.

[4] B. H. Gross, An elliptic curve test for Mersenne primes, *J. Number Theory* **110** (2005), 114–119.

[5] Ö. Küçüksakallı, Value sets of Lattès maps over finite fields, *J. Number Theory* **143** (2014), 262–278.

[6] D. H. Lehmer, An extended theory of Lucas' functions, *Ann. of Math. (2)* **31** (1930), 419–448.

[7] R. Lidl and H. Niederreiter, *Finite Fields*. Encyclopedia of Mathematics and Its Applications, Vol. 20, Second edition, Cambridge University Press, 1997.

[8] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–196.

[9] H. Riesel, A note on the prime numbers of the forms $N = (6a + 1)2^{2n-1} - 1$ and $M = (6a - 1)2^{2n} - 1$, *Ark. Mat.* **3** (1956), 245–253.

[10] H. Riesel, Lucasian criteria for the primality of $N = h \cdot 2^n - 1$, *Math. Comp.* **23** (1969) 869–875.

[11] M. I. Rosen, A proof of the Lucas-Lehmer test, *Amer. Math. Monthly* **95** (1988), 855–856.

[12] Ö. J. Rödseth, A note on primality tests for $N = h2^n - 1$, *BIT* **34** (1994), 451–454.

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Second edition, Graduate Texts in Mathematics, Vol. 106, Springer, 2009.

[14] H. C. Williams, The primality of $N = 2A3^n - 1$, *Canad. Math. Bull.* **15** (1972), 585–589.

[15] H. C. Williams, Effective primality tests for some integers of the forms $A5^n - 1$ and $A7^n - 1$, *Math. Comp.* **48** (1987), 385–403.

2010 *Mathematics Subject Classification*: Primary 11Y11; Secondary 11G20.
Keywords: elliptic curve, Jacobi symbol, Dickson polynomial, Lucas sequence.

Received May 29 2018; revised versions received May 30 2018; July 5 2018. Published in *Journal of Integer Sequences*, July 11 2018.

Return to Journal of Integer Sequences home page.