A simpler alternative to Lucas–Lehmer–Riesel primality test

Pavel Atnashev
patnashev@gmail.com

February 14, 2023

Abstract This paper investigates application of Morrison primality test to numbers of $k \cdot 2^n - 1$ form and finds a simple general formula, which is equivalent to Lucas–Lehmer and Lucas–Lehmer–Riesel primality tests.

1 Introduction

There are two popular classes of deterministic primality tests: one deals with smooth numbers plus 1, the other deals with smooth numbers minus 1. Plus 1 tests are called $N-1$ tests and are based on the fact that for any prime p, $\varphi(p) = p - 1$. Since $N-1$ is a smooth number, there are ways to prove that it is exactly $\varphi(N)$, thus proving the primality of N. Minus 1 tests are called $N+1$ tests and are based on properties of Lucas sequences.

Lucas sequences are recursive integer sequences V_n and U_n with parameters P and Q satisfying the following relations:

$$V_0 = 2, \quad V_1 = P, \quad V_n = PV_{n-1} - QV_{n-2}$$

$$U_0 = 0, \quad U_1 = 1, \quad U_n = PU_{n-1} - QU_{n-2}$$

$$D = P^2 - 4Q \neq 0$$

There are many identities involving terms of Lucas sequences. Some of them are useful for this paper:

$$V_{2n} = V_n^2 - 2Q^n \tag{1}$$

$$V_{m+n} = V_m V_n - Q^n V_{m-n} \tag{2}$$

$$V_{mn} = V_m(P = V_n, Q = Q^n) \tag{3}$$

$$U_{2n} = U_n V_n \tag{4}$$

$$V_n^2 - DU_n^2 = 4Q^n \tag{5}$$

$$DU_n^2 = V_{2n} - 2Q^n \tag{6}$$

$$U_{p-\left(\frac{D}{p}\right)} \equiv 0 \pmod{p},\ p \nmid PQD \tag{7}$$

Of particular interest is (7), because by selecting P and Q in such a way that $\left(\frac{D}{N}\right) = -1$, we can have $U_{N+1} \equiv 0 \pmod{N}$ as a compositeness test. Unfortunately it doesn't work as a primality test, because there are so called Lucas pseudoprimes, which satisfy this condition but are not prime. But we can use the smoothness of $N+1$ to design additional criterias to prove primality.

Throughout this paper it is assumed that $\left(\frac{D}{N}\right) = -1$. Also, it is assumed that N does not have small factors, $(4PQD, N) = 1$.

Lucas–Lehmer–Riesel test. If $N = k \cdot 2^n - 1$, $k < 2^n$ and $V_{2^{n-2}} \equiv 0 \pmod{N}$, then N is prime. Q is fixed at 1, but P is chosen in a complicated process involving computing of V_k. The goal of this paper is to avoid that process.

2 Morrison test

There is a more general Morrison test [1, Theorem 16] for numbers with the smooth part of $N+1$ exceeding $\sqrt{N}$. When applied to $k \cdot 2^n - 1$ numbers it simplifies into the following statement:

Morrison test of $N = k \cdot 2^n - 1$ numbers. If $k < 2^n$ and there exist P, Q such that $U_{N+1} \equiv 0 \pmod{N}$ and $(U_{(N+1)/2}, N) = 1$, then N is prime.

There are several immediate problems with this test. First, U_n is more expensive to calculate than V_n. Thanks to (1), (2) and (3), V_n can be easily calculated for arbitrary n using methods like Montgomery ladder or differential addition chains. The fastest methods compute only V_n, and it is not possible to also obtain U_n. When U_n is absolutely necessary, one has to resort to slower methods.

The other problem is that due to [1, Theorem 9], if $\left(\frac{Q}{N}\right) = 1$, then $U_{(N+1)/2} \equiv 0 \pmod{N}$. In practice Q is almost always fixed at 1, because that simplifies formulas a lot. Since $\left(\frac{1}{N}\right)$ is always 1, $U_{(N+1)/2}$ is always divisible by N. Morrison test can't be used at all.

The solution to both problems is the choice of $Q = -1$. It is trivial to implement, one just needs to track parity in (1), (2) and (3). As for $\left(\frac{Q}{N}\right)$, its value is 1 if there exists quadratic root of -1, and -1 otherwise. But for prime N, quadratic root of -1 exists only if $\varphi(N) = N - 1$ is divisible by 4. But for our numbers $N+1$ is divisible by 4, therefore $\varphi(N) \equiv 2 \pmod{4}$. This means $\left(\frac{-1}{N}\right) = -1$.

If N is prime and $\left(\frac{Q}{N}\right) = -1$, then due to [1, Corollary 4], $V_{(N+1)/2} \equiv 0 \pmod{N}$ for any P (such that $\left(\frac{D}{N}\right) = -1$, of course). On the other hand, if $V_{(N+1)/2} \equiv 0 \pmod{N}$, then from (4) follows that $U_{N+1} \equiv 0 \pmod{N}$, from (5) follows that $DU^2_{(N+1)/2} \equiv -4 \pmod{N}$. If a divisor of N divides $U_{(N+1)/2}$, it has to divide 4 too, therefore $(U_{(N+1)/2}, N) = 1$. Since all conditions of Morrison test are fulfilled, N is prime.

All one needs to do to test if N is prime is to compute $V_{(N+1)/2} \pmod{N}$ and test whether it's zero. Note that this is actually not a new result. Rödseth in [2] gives a method to compute the starting value of Lucas–Lehmer–Riesel test, resulting in the following condition of primality:

$$V_{2^{n-2}}(V_k(P_R, Q_R)) \equiv 0 \pmod{N}, \quad Q_R = 1, \quad \left(\frac{P_R - 2}{N}\right) = 1, \quad \left(\frac{P_R + 2}{N}\right) = -1.$$

Consider $Q = -1$ and arbitrary P such that $\left(\frac{D}{N}\right) = -1$ where $D = P^2 - 4Q = P^2 + 4$. Compute $V_2 = P^2 - 2Q = P^2 + 2$. It has the following properties:

$$\left(\frac{V_2 - 2}{N}\right) = \left(\frac{P^2}{N}\right) = 1, \quad \left(\frac{V_2 + 2}{N}\right) = \left(\frac{D}{N}\right) = -1.$$

V_2 can be used as P_R, and because of (3) all indexes of V_m are even, therefore $Q^m = 1$. Lucas–Lehmer–Riesel test becomes

$$V_{2^{n-2}}(V_k(V_2)) = V_{2^{n-2} \cdot k \cdot 2} = V_{k \cdot 2^{n-1}} = V_{(N+1)/2} \equiv 0 \pmod{N}.$$

An implementation of Morrison test with $Q = -1$ and V sequence is mathematically indistinguishable from an implementation of Lucas–Lehmer–Riesel test with Rödseth starting value. The same can be said about Lucas–Lehmer test of numbers of $2^p - 1$ form, which can be expressed as Morrison test with $Q = -1$ and $P = \sqrt{2} = 2^{(p+1)/2}$.

This amazing result dims the novelty of this paper. Although it can still be seen as a simple explanation of the complex algorithm developed through centuries. It also can be useful to implementers who have access to good Lucas sequence libraries, because in that case the implementation can fit one line.

Also the expression $V_{(N+1)/2} \equiv 0 \pmod{N}$ is reminiscent of Proth's test for $k \cdot 2^n + 1$ numbers with the condition of primality $a^{(N-1)/2} \equiv -1 \pmod{N}$. In both cases starting values are selected with Legendre symbol.

References

[1] John Brillhart, D. H. Lehmer, and J. L. Selfridge. New Primality Criteria and Factorizations of $2^m \pm 1$. *Mathematics of Computation, 29*, pages 620–647, 1975. `https://doi.org/10.1090/S0025-5718-1975-0384673-1`.

[2] Öystein J. Rödseth. ”A note on primality tests for $N = h \cdot 2^n - 1$. *BIT Numerical Mathematics, 34*, pages 451–454, 1994. `https://doi.org/10.1007/BF01935653`.