Amazing Q is Negative 3 Test

Paul Underwood

November 21, 2022

Abstract

A Lucas restricted domain probable prime test is presented. It is hoped that someday it will be proven to be a foolproof test of primality.

1 Introduction

The probable prime test of Baillie, Pomerance, Selfridge and Wagstaff (BPSW) [1] is a quick and has had no counterexamples during the passed forty years, It is $1 + 3$ Selfridges, where a Selfridge [2] is the time taken to do a Fermat probable prime test. It is $O(log(n)^2)$ compared to the primality tests based on Elliptic Curves Primality Proving (ECPP) [3, p368] which are $O(log(n)^{4+\epsilon})$ for some $\epsilon > 0$.

This paper is about Lucas probable prime tests over $x^2 - 3^r x - 3$. We shall see that this can be broken down into $1 + 2$ selfridges and combined back into a 2 selfridges test.

2 Definitions

A Fermat probable prime (PRP) is an n for which $a^n \equiv a \bmod n$ for some a. It is called a-PRP. If $\gcd(a, n) = 1$ it can be divided by a:

$$a^{n-1} \equiv 1 \pmod{n}.$$

There are Fermat pseudoprimes (PSP) to the PRP test such as 341 which is 2-PSP. There are also Carmichael (absolute pseudoprime) numbers for which $a^n = a \bmod n$ for all bases a; For example 561.

An Euler probable prime (EPRP) is one for which $a^{\frac{n-1}{2}} \equiv J(a, n) \bmod n$, where $J(a, n)$ is the Jacobi symbol of a over n.

A *strong* Fermat probable prime (SPRP) [3, pp136-138] is calculated as follows. Let $n = 2^s d + 1$ where d is odd. Compute $a^d \bmod n$. If it is ± 1 declare n do be a-SPRP. Square up to $s - 1$ times checking for equivalence to -1. If so declare n to be a-SPRP.

A (proper) Lucas probable prime (LPRP) is test of odd n over the quotient ring $\mathbb{Z}_n[x]/(x^2 - Px + Q)$ with a strong Jacobi symbol of the discriminant $P^2 - 4Q$ over n, i.e. equal to -1 so that the square root of the discriminant has no solution in $\mathbb{Z}_n$ which ensures the Frobenius automorphism forms the augmented solutions for x:

$$x = \frac{P \pm \sqrt{P^2 - 4Q}}{2}.$$

An LPRP is calculated thusly: $x^{n+1} \equiv Q \pmod{n, x^2 - Px + Q}$ such that $x^2 = Px - Q$ is repeatedly used to calculate powers of x, usually by a left-right binary exponentiation method. The general LPRP(n, P, Q) test has many pseudoprimes, for example LPRP(51, 17, 25). The Q value could be restricted to 2 and then test LPRP(n, P, 2), but again there are many pseudoprimes which can be found easily, for example LPRP(1387, 511, 2).

An LPRP(n, P, 1) test can be very efficiently calculated by a Lucas binary exponentiation chain and is denoted in this paper as an LPRPC [3, p147].

Define a *strong* Lucas probable prime chain (SLPRPC) test as follows. Let $n = 2^t e - 1$ where e is odd. Calculate the chain up to the power of e. If it is ± 1 declare n to be SLPRPC. Square the chain up to $t - 1$ times further checking for a result of -1 and if this is the case declare n to be SLPRPC.

3 The Raw Test

The domain of an LPRP test is restricted to $P = 3^r$ and $Q = -3$. Thus the test for n such that $\gcd(6, n) = 1$ is essentially

$$x^{n+1} \equiv -3 \pmod{n, x^2 - 3^r x - 3}.$$

where the Jacobi symbol of the discriminant $9^r + 12$ over n is the strong value of -1, with $\gcd(r - 1, n - 1) = 1$.

4 Transformation

The LPRP(n, 3^r, -3) test is strengthened into a base -3 EPRP test of n and a test for $z^{\frac{n+1}{2}}$ equal to the Jacobi symbol of -3 over n working modulo n and $z^2-(\frac{9^r}{-3}-2)z+1$. That is a 3-EPRP and an LPRPC test. This can shown with x^2-Px+Q companion matrix calculations:

$$\begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}^{n+1} = \begin{pmatrix} P^2-Q & -PQ \\ P & -Q \end{pmatrix}^{\frac{n+1}{2}} = \begin{pmatrix} \frac{P^2}{Q}-1 & -P \\ \frac{P}{Q} & -1 \end{pmatrix}^{\frac{n+1}{2}} \begin{pmatrix} Q & 0 \\ 0 & Q \end{pmatrix}^{\frac{n+1}{2}}.$$

The characteristic equation of the left hand matrix of the product (the determinant of which is 1) is $z^2-(\frac{P^2}{Q}-2)z+1=0$.

The right hand matrix of the product raised to power of $\frac{n+1}{2}$ is equivalent $J(Q,n)Q$ mod n and dividing by Q which is assumed to be invertible mod n then $Q^{\frac{n-1}{2}} \equiv J(Q,n)$ mod n. Consequently working over $\mathbb{Z}_n[z]/(z^2-(\frac{P^2}{Q}-2)z+1)$ that $z^{\frac{n+1}{2}}$ should also be equivalent to $J(Q,n)$. Now a substitution is made of 3^r for P and -3 for Q.

We want to avoid $z^2 \pm z+1$ in our testing because otherwise finding counterexamples becomes easier. It seems that only z^2-z+1, which has discriminant -3, needs to be avoided for $Q=-3$. Thus $z^2-(-3^{2r-1}-3+3-2)z+1$ is key and $3^{2r-2}+1=0$ should be avoided. That is $3^{4(r-1)}=1$ can be avoided by taking $\gcd(r-1,n-1)$.

5 Making it 2 Selfridges

Combining back the base -3 EPRP test with the LPRPC test for z by multiplication gives: $(-3z)^{\frac{n+1}{2}}=-3 \pmod{n, z^2-(-3^{2r-1}-2)z+1}$. It is now shown that this can be computed with 2 Selfridges.

Let $sz+t$ be the intermediate value during left-right binary exponentiation of the base $-3z$. For squaring: $(sz+t)^2 = s(as+2t)z+(t-s)(t+s) \pmod{n, z^2-az+1}$ and multiplying by the base where the current bit is a 1 in the binary expansion: $(sz+t)(-3z)=-3(as+t)z+3s \pmod{n, z^2-az+1}$ where $a=-3^{2r-1}-2$ which in practice is assumed to be small. Left-right exponentiation at each stage is then dominated by the two multiplications and two modular reductions i.e. s by $as+2t$ mod n and $t-s$ by $t+s$ mod n. Thus it is 2 Selfridges.

6 Conclusion

Verification of the test is ongoing and the author see no reason why it should fail, with $\gcd(r-1,n-1)=1$ avoiding z^2-z+1, despite the consensus from the mathematical community that it will fail eventually.

References

[1] R. Baillie and S. S. Wagstaff, Jr., "Lucas pseudoprimes", *Mathematics of Computation*, vol. 35, pp. 1391–1417, October 1980.

[2] A. O. L. Atkin., "Intelligent primality test offer", *Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Proceedings of a Conference in Honor of A. O. L. Atkin, International Press*, pp. 1–11, 1998.

[3] R. Crandall and C. Pomerance, *Prime Numbers, A Computational Perspective, 2nd Ed.* Springer, 2005.

Email: *paulunderwood@mindless.com*