A Restricted Domain Lucas Probable Prime Test

Paul Underwood

November 9, 2022

Abstract

A Lucas probable prime test shall be presented with a restricted domain. The practical transformed version of it as a base 2 Euler probable prime test plus a simpler Lucas probable prime test is examined along with a "fused" probable prime test. The practical reduced domain Euler plus Lucas algorithm is given. Some statistical results are presented finally.

1 Introduction

There have been many publications regarding probable prime tests over the last forty years or so since the seminal paper of Baillie, Pomerance, Selfridge and Wagstaff (BPSW) [1]. The basic idea of BPSW is to perform a strong base 2 Fermat probable prime test in conjunction with an Lucas probable prime test with carefully chosen parameters.

The BPSW is very fast and reliable; It is $1+3$ Selfridges, where a Selfridge [2] is the time taken to do a Fermat probable prime test, and to date nobody has yet claimed the $30 offered for a counterexample or a proof that none exist. In contrast, Elliptic Curve Primality Proving (ECPP) [3, p368] is of the order $O(log(n)^{4+\epsilon})$ for some $\epsilon > 0$.

For the Lucas component of the BPSW test, parameters are chosen from $\mathbb{Z}$ by one of two methods, one given by Selfridge and the other by Pomerance in their paper. In this paper the domain of a parameter is restricted to 2^r for some integer r. Then r itself is restricted after the full Lucas probable prime test is transformed into a computationally efficient base 2 Euler probable prime test plus a simple Lucas probable prime chain test. The resulting restricted domain test is $1+2$ Selfridges and a brief look is taken to see how a "fused" probable prime test can be performed in 2 Selfridges.

A practical algorithm is given and finally some statistical results are also presented.

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 Domain Restriction

The domain of an LPRP test has its P restricted to 2^r for integer r and Q to 2. Thus $x^2 - 2^r x + 2 = 0$ where the Jacobi symbol of the discriminant $4^r - 8$ over n is the strong value of -1. The rationale is that a smaller domain will produce fewer pseudoprimes. Given that the multiplicative order of 2 over $\mathbb{Z}_n$ is much smaller then the domain of freely varying P across $\mathbb{Z}_n$, this seems a good way to greatly reduce the number of pseudoprimes. With the aid of a few choice GCDs, shown in the next section, finding a pseudoprime is very difficult. In a later section r itself is restricted, further diminishing the domain 2^r.

4 Transformation

The LPRP(n, 2^r, 2) test is strengthened into a 2-EPRP test of n and a test for $z^{\frac{n+1}{2}}$ equal to the Jacobi symbol of 2 over n working modulo n and $z^2 - (\frac{4^r}{2} - 2)z + 1$. That is a 2-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 $J(Q,n)Q \bmod n$ and dividing by Q which is assumed to be invertible mod n then $Q^{\frac{n-1}{2}} \equiv J(Q,n) \bmod n$. 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 $J(Q,n)$.

With the substitution of 2^r for P and 2 for Q, note that if either $\gcd(4^r - 2, n)$ or $\gcd(4^r - 4, n)$ is not 1 then over some factor of n the quadratic polynomial $z^2 - (\frac{4^r}{2} - 2)z + 1$ would be cyclotomic, making it easier to find pseudoprimes. Also note that trivially $\gcd(2^r, n) = 1$ for odd n.

5 Further Domain Restriction

The domain of P has already been restricted to 2^r. As shown in the previous section it is required that $\gcd(4^r - 4, n) = 1$ and $\gcd(4^r - 2, n) = 1$, but it is known that a 2-EPRP implies $2^{n-1} - 1 \equiv 0 \bmod n$. Hence by choosing r such that $\gcd((r-1)(2r-1), n-1) \leq 3$ by the extended Euclidean algorithm $M(r-1)(2r-1) + N(n-1) \leq 3$ for some integers M and N, the domain 2^r is further reduced and the two GCDs can be replaced with $\gcd(7, n) = 1$ and $\gcd(3, n) = 1$.

6 Fusion into 2 Selfridges

Combining back the 2-EPRP test with the LPRPC test for z by multiplication gives: $(2z)^{\frac{n+1}{2}} = 2 \pmod{n, z^2 - (\frac{4^r}{2} - 2)z + 1}$. 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 $2z$. 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: $(sz + t)(2z) = 2(as + t)z - 2s \pmod{n, z^2 - az + 1}$ where $a = \frac{4^r}{2} - 2$ 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 $as + 2t \bmod n$ and $t - s$ by $t + s \bmod n$. Thus it is 2 Selfridges.

7 A Practical Algorithm

A practical algorithm written in PARI/GP is now given which is $1 + 2$ Selfridges:

```
{RDPRP(n)=local(r,t,k);
if(n==2||n==3||n==7,return(1));
if(n<2||n%2==0||n%3==0||n%7==0||issquare(n),return(0));
k=kronecker(2,n);
if(Mod(2,n)^((n-1)/2)!=k,return(0));
r=0;t=Mod(4,n)^r;
while(kronecker(lift(t)-8,n)!=-1||gcd((r-1)*(2*r-1),n-1)>3,r++;t*=4);
Mod(Mod(z,n),z^2-(t/2-2)*z+1)^((n+1)/2)==k;}
```

The above code is only a guide; Some trial division could be performed as well for instance. Furthermore, like the BPSW test, the 2-EPRP and LPRPC tests can be made stronger.

8 Test Results

There are 118, 968, 378 odd numbers in Feitsma's list of 2-PSPs $\leq 2^{64}$ [4]. Of these 63, 912, 692 are 2-EPRP. No pseudoprimes were found with these against the RDPRP test of §7. All numbers $n \leq 5 \cdot 10^{13}$ pass the LPRPC(n, $\frac{4^r}{2} - 2$, 1) test for all applicable r, with and without the further GCD restriction given in §5, and for the 2 Selfridge version of §6.

By sampling Feitsma's list it was found that on average the domain of a 2-EPSP n was reduced to about $n^{0.408}$. If the GCD method with a strong discriminant were employed the domain of the exponent r itself would be reduced by a factor of about 0.16 making the domain of an LPRPC n about $n^{0.065}$. One could say that this paper's method is about $n^{0.935}$ times better than choosing P linearly.

On the other hand the counts of 2-PSPs that are also Euler pseudoprimes and pseudoprime for LPRP(n, P, 2) with $J(P^2 - 8, n) = -1$, $\gcd(P^2 - 2, n) = 1$, $\gcd(P^2 - 4, n) = 1$, $\gcd(P, n) = 1$ and $1 \leq P \leq \frac{n-1}{2}$ are tabulated as follows, along with the expectation of the total number of pseudoprimes for any r of this paper's test and the probability of the test RDPRP failing:

Digits	#2-EPSPs	Count	$10^{0.935 \times digits}$	Lower Expectation	Upper Expectation	Probability
4	11	0	5495	0	0	0
5	24	26	47315	0.000549509	0.004731574	10^{-13}
6	78	98	407380	0.000240562	0.002071225	10^{-15}
7	261	312	3507518	0.000088952	0.00076587	10^{-17}
8	696	1608	30188517	0.000053246	0.000458444	10^{-19}
9	1868	15072	260015956	0.000057966	0.000499081	10^{-21}
10	4776	101630	1778279410	0.000057151	0.000390861	10^{-23}

For example for all 10 digit numbers tested with the method presented in this paper have a total expectation of between 0.000057151 and 0.000390861 pseudoprimes. Consequently a 10 digit composite number has about 10^{-23} chance of passing the test RDPRP.

If a pseudoprime is found for some r then there will be spectacularly any number between $n^{0.2}$ and $n^{0.999\ldots}$ of other r failures due to the multiplicative order of 2 modulo n.

9 Conclusion

It has been shown empirically that a 2-EPRP test plus an LPRPC(n, $\frac{4^r}{2} - 2$, 1) test with $J(4^r - 8, n) = -1$ and by taking $\gcd(4^r - 2, n) = 1$ and $\gcd(4^r - 4, n) = 1$ makes any odd pseudoprimes very difficult to find: None were found. This is further rarefied by taking $\gcd((r-1)(2r-1), n-1) \leq 3$, and, like the BPSW test, by using a minimal suitable parameter value makes finding a pseudoprime with RDPRP a very rare prospect indeed.

The author offers a first prize of £100 sterling for a single r that passes the test RDPRP for a composite. This need not be a minimal r.

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.

[4] Jan Feitsma, "Pseudoprimes", `http://www.janfeitsma.nl/math/psp2/index`.

Email: *paulunderwood@mindless.com*