# Euler-Frobenius Probable Prime Test

Paul Underwood

September 23, 2020

**Abstract**

Quick and reliable probable prime (PRP) tests are very useful in today's world where primes form the basis of many cryptosystems keeping electronic communication between computer entities secure. Mostly these tests do not constitute a proof of primality but are rather used because of the requirement for speed. Those tests which have no known counterexamples are of most interest. Such a test is given in this paper having no known counterexamples less than $2^{64}$ with minimal parameters.

## The Ansatz

Let $x^2 - 2x + 2^r = 0$. This has solutions $x = 1 \pm \sqrt{1 - 2^r}$. The PRP test presented here of $n$ consists of finding an appropriate value for $a := 2^r$ and initially performing an Euler PRPs sub-test $1 - a$ and a Frobenius PRP test [1] of $x$ over $x^2 - 2x + a$. The Jacobi symbol $J(1 - a, n)$ should be $-1$ in order to effect the Frobenius endomorphism. To prevent cyclotomy over factors of $n$ it is required that $\gcd(a - 2, n) = 1$ and $\gcd(a - 4, n) = 1$.

Since $x^2 - 2x + a = 0$ we can implement the Frobenius PRP test efficiently by computing the Euler PRP test $a^{\frac{n-1}{2}} = J(a, n) \pmod n$ and the binary chain Frobenius PRP test $x^{n+1} = 1 \pmod{n, x^2 - (\frac{4}{a} - 2)x + 1}$ the polynomial of which has the same discriminant of $1 - a$. Furthermore we can replace this Euler PRP test with $2^{\frac{n-1}{2}} = J(2, n) \pmod n$. This has the advantage for test verification for all $r$ for a given $n$ because we can use lists of known base 2 pseudoprimes efficiently.

To date, there are no counterexamples for any $r$ for all $n < 10^{12}$.

## The Algorithm

To test non-square odd $n$ for probable primality vary $r$ (minimally starting at 3) until a negative Jacobi symbol for $1 - a$ over $n$ is found:

1. If a 0 Jacobi symbol is found declare $n$ composite.
2. If $1 < \gcd(a - 2, n) < n$ then declare $n$ to be composite.
3. If $1 < \gcd(a - 4, n) < n$ then declare $n$ to be composite.

Having found a negative Jacobi symbol perform the following tests:

1. If $2^{\frac{n-1}{2}} \not\equiv J(2, n) \pmod n$ then declare $n$ to be composite.
2. If $(1 - a)^{\frac{n-1}{2}} \not\equiv -1 \pmod n$ then declare $n$ to be composite.
3. If $x^{n+1} \not\equiv 1 \pmod{n, x^2 - (\frac{4}{a} - 2)x + 1}$ then declare $n$ to be composite.

If all tests are passed then declare $n$ to be a probable prime.

## References

[1] J. Grantham, "A Frobenius probable prime test with high confidence", *Journal of Number Theory*, vol. 72, pp. 32–47, 1998.

*Email address: paulunderwood@mindless.com*