An Extension to Perrin's Pseudoprime Test

Paul Underwood

September 14, 2023

Abstract

Perrin's pseudoprime test is herein made good in most cases by an inexpensive extension. When the simple extension cannot be employed then a similar suitable higher order test can be used as a substitute.

Introduction

Recurrence sequences, whereby a term in a sequence is formed by a fixed weighted sum of some of the preceding terms in the sequence, have been studied for many centuries. Fibonacci de Pisa circa 1200AD studied the recurrence relation $F_n = F_{n-1} + F_{n-2}$ for pairs of breeding rabbits. He asked "How many pairs exist after a certain number of periods given that the first period of any rabbit's life was for maturation?". He considered starting with one pair. At the end of the first period the rabbits had matured and so there was still only one pair. At the end of the second period the rabbits have reproduced somewhat hypothetically another pair so that there were two pairs, and so on. This forms a sequence of pairs: $1, 1, 2, 3, 5, 8 \ldots$, the so-called *Fibonacci Sequence*.

Édouard Lucas in the year 1878 [1] studied the general case of the Fibonacci Sequence $A_n = aA_{n-1} + bA_{n-2}$ with various starting pairs of numbers in the sequences. The *Lucas Sequence* is $2, 1, 3, 4, 7, 11 \ldots$ where $L_n = L_{n-1} + L_{n-2}$. He also studied higher order recurrence relations, for example the third order recurrence $P_n = P_{n-2} + P_{n-3}$ that starts $3, 0, 2, 3, 2, 5, 5, 7 \ldots$ noting that counting from 0 the prime p^{th} term is divisible by p. In 1899 François Olivier Raoul Perrin in an article of a French journal [2] asked whether there were any pseudoprimes to this property of the sequence. Adams and Shanks [3] studied the Perrin sequence in 1982 and wrote about "signatures" and reported the smallest Perrin pseudoprime $n = 521^2$. Steve Arno also studied Perrin signatures [4]. In a paper [5] Jon Grantham proved the infinity of the number of Perrin pseudoprimes. More recently there has been a paper by H. Stephan on how to find Perrin pseudoprimes [6].

Perrin's Sequence

Perrin's sequence $3, 0, 2, 3, 2, 5, 5, 7 \ldots$ can be formally defined by the recurrence relation $P_n = P_{n-2} + P_{n-3}$ with initial values $P_0 = 3$, $P_1 = 0$ and $P_2 = 2$.

The matrix form is $P_n = trace(M^n)$ where $M = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

The characteristic equation of M is $x^3 - x - 1 = 0$ which is given by the determinant $|x - M| = 0$.

It is not shown here that each binary digit of left-right binary exponentiation of M can be calculated with 6 multiplications and respectively 6 modular reductions plus sundry additions and subtractions.

The existence of Perrin pseudoprimes has hitherto made it a poor test when compared with the quicker Baillie-PSW [7] test which has no known counterexamples, although it is believed there are infinitely many counterexamples to the Baillie-PSW test albeit each with a large number of digits.

Extending Perrin's Test

A novel approach is taken; For $n \geq 9$ choose a small $k : 2 < k \leq \sqrt{n}$ with $x^n \not\equiv x \pmod{n, x^k - x - 1}$. The number of multiplications and modular reductions per bit of n for exponentiation is $k(k-1)$ for each k. Fortunately, the cubic character usually suffices and extremely rarely is the sextic or a higher degree character needed.

With the above non-equivalence condition met and $x^n \pmod{n, x^k - x - 1}$ already calculated there are two required checks: (i) $\gcd(A, n) = 1$ where A is the resulting coefficient of x^{k-1} from the exponentiation; (ii) Do the quick calculation $(x^n)^k \pmod{n, x^k - x - 1}$ and then check that $x^{kn} - x^n - 1 = 0 \pmod{n, x^k - x - 1}$.

Here is the function TPPPE written in the number theory package PARI/GP interpreted language [8]:

```
{
  kill(x);TPPPE(n)=my(k=2,X=x);
  while(X==x,k++;X=Mod(Mod(x,n),x^k-x-1)^n);
  gcd(polcoef(lift(lift(X)),k-1),n)==1&&X^k-X-1==0;
}
```

Conclusion

Substantial testing has been done without finding a single extended pseudoprime: $9 \leq n \leq 10^{11}$; All of Jan Feitsma's base 2 Fermat pseudoprimes less than 2^{64} [9] and all Perrin pseudoprimes provided by Holger Stephan at his internet website [10].

It should be noted that $x^{n\,k!} \equiv x \pmod{n, x^k - x - 1}$ for prime n. Whether this helps with a proof of sufficiency of the extended test presented in this paper remains to be seen.

References

[1] Lucas, É. (1878). "Théorie des fonctions numériques simplement périodiques". American Journal of Mathematics. The Johns Hopkins University Press. 1 (3): 197–240. American Mathematical Society. 39 (159): 255–300

[2] Perrin, R. (1899). "Query 1484". L'Intermédiaire des Mathématiciens. 6: 76.

[3] Adams, William; Shanks, Daniel (1982). "Strong primality tests that are not sufficient". Mathematics of Computation.

[4] Arno, Steve (1991). "A NOTE ON PERRIN PSEUDOPRIMES". https://www.ams.org/journals/mcom/1991-56-193/S0025-5718-1991-1052083-9/S0025-5718-1991-1052083-9.pdf

[5] Grantham, J. "There are Infinitely Many Perrin Pseudoprimes". https://arxiv.org/pdf/1903.06825.pdf

[6] Stephan, H. 'Millions of Perrin pseudoprimes including a few giants". https://arxiv.org/pdf/2002.03756.pdf

[7] Baillie, R; Wagstaff Jr., S. (1980). "Lucas Pseudoprimes". https://www.ams.org/journals/mcom/1980-35-152/S0025-5718-1980-0583518-6/S0025-5718-1980-0583518-6.pdf

[8] PARI/GP. https://pari.math.u-bordeaux.fr/

[9] Feitsma, J. http://www.cecm.sfu.ca/Pseudoprimes/

[10] H. Stephan, Perrin pseudoprimes. Data Sets, Weierstrass Institute Berlin (2019), http://doi.org/10.20347/WIAS.DATA.4

Email: paulunderwood@mindless.com