LOTS AND LOTS OF PERRIN-TYPE PRIMALITY TESTS AND THEIR PSEUDO-PRIMES

Robert Dougherty-Bliss
Department of Mathematics, Rutgers University (New Brunswick)
robert.w.bliss@gmail.com

Doron Zeilberger
Department of Mathematics, Rutgers University (New Brunswick)
DoronZeil@gmail.com

Received: , Revised: , Accepted: , Published:

Abstract

We use *Experimental Mathematics* and *Symbolic Computation* (with Maple), to search for lots and lots of Perrin- and Lucas- style primality tests, and try to sort the wheat from the chaff. More impressively, we find quite a few such primality tests for which we can explicitly construct infinite families of pseudo-primes, rather, like in the cases of Perrin pseudo-primes and the famous Carmichael primes, proving the mere existence of infinitely many of them.

1. Preface: How it all Started thanks to Vince Vatter

It all started when we came across Vince Vatter's delightful article [14], where he gave a cute combinatorial proof, inspired by COVID, and social distancing, of the following fact that goes back to Raoul Perrin [8] (See also [9], [10], [13], [15]).

Perrin's Observation: Let the integer sequence $A(n)$ defined by

$$\begin{aligned} &A(1) = 0 \quad A(2) = 2 \quad A(3) = 3 \\ &A(n) = A(n-2) + A(n-3) \qquad \text{(for } n > 3\text{)}. \end{aligned}$$

Then, for every prime p, we have $p \mid A(p)$.

Perrin, back in 1889, was wondering whether the condition is *sufficient*, i.e. whether there are any *pseudo-primes*, i.e. *composite* n such that $A(n)/n$ is an integer. He could not find any, and as late as 1981, none was found ≤ 140000 (see [1]). In 1982, Adams and Shanks [1] *rather quickly* found the smallest Perrin pseudo prime, 271441, followed by the next-smallest, 904631, and then they found quite a few other ones. Jon Grantham [4] proved that there are *infinitely many* Perrin pseudo-primes, and finding as many as possible of them, became a computational challenge, see Holger's paper [6].

Another, older, primality test is that based on the Lucas numbers ([11], [12]).

Vince Vatter's Combinatorial Proof

Vatter first found a *combinatorial interpretation* of the Perrin numbers, as the number of circular words of length n in the alphabet $\{0, 1\}$, that *avoid* the *consecutive subwords* (aka *factors* in formal language lingo), $\{000, 11\}$.

More formally: the number of words, $w = w_1, \dots, w_n$, in the alphabet $\{0, 1\}$, such that for $1 \leq i \leq n-2$, $w_i w_{i+1} w_{i+2} \neq 000$, and also $w_{n-1} w_n w_1 \neq 000$ and $w_n w_1 w_2 \neq 000$ as well as for $1 \leq i \leq n-1$, $w_i w_{i+1} \neq 11$, and $w_n w_1 \neq 11$.

Then he argued that if p is a prime, all the p circular shifts are *different*, since otherwise there would be a non-trivial period, that can't happen since p is prime. Since the constant words 0^p and 1^p obviously can't avoid both 00 and 111, Perrin's theorem follows.

This proof is reminiscent of Solomon Golomb's [3] snappy combinatorial proof of Fermat's little theorem [G] that argued that there are $a^p - a$ non-monochromatic straight necklaces with p beads of a colors, and for each such necklace, the p rotations are all different (see also [16], p. 560).

When we saw Vatter's proof we got all excited. Vatter's argument transforms *verbatim* to counting circular words in *any* (finite) alphabet, and any (finite) set of forbidden (consecutive) patterns! More than twenty years ago one of us (DZ) wrote a paper, in collaboration with his then PhD student, Anne Edlin [2], that *automatically* finds the (rational) generating function in any such scenario, hence this is a cheap way to manufacture lots and lots of Perrin-style primality tests. We already had a Maple package, CGJ, to handle it, so all that remained was to *experiment* with many alphabets and many sets of forbidden patterns, and search for those that have only few small *pseudo-primes*.

This inspired us to write our first Maple package, PerrinVV.txt. See the front of the present article front of the present article for many such primality tests, inspired by sets of forbidden patterns, along with all the pseudoprimes less than a million.

2. An Even Better Way to Manufacture Perrin-style Primality Tests

After the initial excitement we got an *epiphany*, and as it turned out, it was already made, in 1990, by Stanley Gurak [5]. Take *any* polynomial $Q(x)$ with *integer coefficients*, and constant term 1, and write it as

$$Q(x) = 1 - e_1 x + e_2 x^2 - \cdots + (-1)^k e_k x^k \quad .$$

Factor it over the complex numbers

$$Q(x) \,=\, (1-\alpha_1 x)(1-\alpha_2 x)\cdots(1-\alpha_k x) \quad .$$

Note that $e_1, e_2, \ldots$ are the *elementary symmetric functions* in $\alpha_1, \ldots, \alpha_k$.

Defining

$$a(n) := \alpha_1^n \,+\, \alpha_2^n \,+\, \ldots + \alpha_k^n \quad ,$$

it follows thanks to Newton's identities ([7]) that $\{a(n)\}$ is an *integer sequence.* The generating function

$$\sum_{n=0}^{\infty} a(n)\, x^n \,=\, \frac{1}{1-\alpha_1 x} \,+\, \frac{1}{1-\alpha_2 x} \,+\, \ldots \,+\, \frac{1}{1-\alpha_k x} \quad ,$$

has denominator $Q(x)$ and *some* numerator, let's call it $P(x)$, with *integer coefficients*, that Maple can easily find *all by itself.*

So we can *define* an integer sequence $\{a(n)\}$ in terms of the rational function $P(x)/Q(x)$, where $Q(x)$ is *any* polynomial with constant term 1, and $P(x)$ *comes out* as above:

$$\sum_{n=0}^{\infty} a(n) x^n \,=\, \frac{P(x)}{Q(x)} \quad .$$

We claim that each such integer sequence engenders a *Perrin-style* primality test, namely

$$a(p) \equiv e_1 (mod\ p).$$

To see this, note that

$$(\alpha_1 + \cdots + \alpha_k)^p = a(p) \,+\, p\, A(p),$$

where

$$A(p) = \sum_{\substack{i_1+i_2+\cdots+i_k=p \\ i_1, i_2, \ldots i_k < p}} \frac{(p-1)!}{i_1! \cdots i_k!} \alpha_1^{i_1} \cdots \alpha_k^{i_k}$$

is a symmetric polynomial in the α_i. The fundamental theorem of symmetric functions [7] implies that $A(p)$ is an integer. Fermat's little theorem then gives

$$a(p) \equiv (\alpha_1 + \cdots + \alpha_k)^p = e_1^p \equiv e_1 (mod\ p).$$

So this is an even easier way to manufacture lots and lots of Perrin-style primality tests, and we can let the computer search for those that have as few small pseudoprimes as possible.

This is implemented in the Maple package `Perrin.txt`. Again, see the front of the present article for many such primality tests, inspired by this more general method (first suggested by Stanley Gurak [5]).

Searching for such primality tests with as few pseudo-primes less than a million, we stumbled on the following example.

The DB-Z Primality Test

Let

$$\sum_{n=0}^{\infty} a(n)\, x^n \;:=\; \frac{3x^4+5x^2+6x-7}{4x^7+x^4+x^2+x-1} \quad ,$$

or equivalently, the integer sequence defined by the initial values $1, 3, 4, 11, 16, 30, 78,$ and

$$a(n) = a(n-1) + a(n-2) + a(n-4) + 4a(n-7)$$

for $n > 7$. Then $a(p) \equiv 1 \pmod{p}$ for all primes p.

Manuel Kauers kindly informed us that the seven smallest DB-Z pseudo-primes are as follows.

- $1531398 = 2 \cdot 3 \cdot 11 \cdot 23203$
- $114009582 = 2 \cdot 3 \cdot 17 \cdot 1117741$
- $940084647 = 3 \cdot 47 \cdot 643 \cdot 10369$
- $4206644978 = 2 \cdot 97 \cdot 859 \cdot 25243$
- $7962908038 = 2 \cdot 191 \cdot 709 \cdot 29401$
- $20293639091 = 11 \cdot 3547 \cdot 520123$
- $41947594698 = 2 \cdot 3 \cdot 19 \cdot 523 \cdot 703559$

(This was a computational challenge posed by us to Manuel Kauers, and we offered to donate 100 dollars to the OEIS in his honor. The donation was made.)

After the first version of this paper was written, with the help of Manuel Kauers, we discovered an even better primality test.

The DB-Kauers primality test

Let

$$\sum_{n=0}^{\infty} a(n)\, x^n \;:=\; \frac{9x^5+16x^4+10x-6}{3x^6+9x^5+8x^4+2x-1} \quad ,$$

or equivalently, the integer sequence defined by initial conditions $2, 4, 8, 48, 157, 382$ and

$$a(n) = 2a(n-1) + 8a(n-4) + 9a(n-5) + a(n-6)$$

for $n > 6$. Then $a(p) \equiv 2 \pmod{p}$ for all primes p.

The smallest pseudoprime is $2,260,550,373 = 3 \cdot 103 \cdot 107 \cdot 68371$.

3. Perrin-Style Primality Tests with Explicit Infinite Families of Pseudo-Primes

We are particularly proud of the next primality test, featuring the *Companion Pell numbers* `https://oeis.org/A002203`. These numbers have been studied extensively, but as far as we know using them as a *primality test* is new. It is not a very good one, but the novelty is that it has an *explicit doubly-infinite* set of pseudoprimes.

The Companion Pell Numbers Primality Test Let

$$\sum_{n=0}^{\infty} a(n)\, x^n \;:=\; \frac{2x-2}{x^2+2x-1},$$

or equivalently, let $a(n)$ be the integer sequence defined by

$$a(1) = 2 \quad a(2) = 6$$
$$a(n) = 2a(n-1) + a(n-2).$$

Then $a(p) \equiv 2 \pmod{p}$ for all primes p.

Theorem 1. *The doubly-infinite family*

$$\{\, 2^i \cdot 3^j \mid i \geq 3\,,\, j \geq 0 \,\} \quad ,$$

are Companion-Pell pseudoprimes. In other words,

$$\frac{a(2^i \cdot 3^j) - 2}{2^i 3^j} \quad ,$$

is an integer if $i \geq 3$ and $j \geq 0$.

Proof. We will proceed by a kind of double-induction where we show that if the conclusion holds for n, it also holds for $2n$ and $3n$, provided that n is of the form stated in the theorem.

Let

$$\alpha_1 := 1 + \sqrt{2} \quad , \quad \alpha_2 := 1 - \sqrt{2}$$

be the roots of the characteristic equation for $a(n)$. It is routine to check that $a(n) = \alpha_1^n + \alpha_2^n$. Since $\alpha_1 \alpha_2 = -1$, we have the following recurrences:

$$a(2n) = a(n)^2 + 2(-1)^{n+1} \tag{1}$$
$$a(3n) = a(n)^3 + 3(-1)^{n+1} a(n). \tag{2}$$

Now define the sequence $b(n) = a(n) - 2$. Our goal is to show that $b(n)$ is divisible by n.

If we substitute $b(n)$ into (1) for even n, then we obtain

$$b(2n) = b(n)(b(n) + 4).$$

This gives

$$\frac{b(2n)}{2n} = \frac{b(n)}{n}\frac{b(n)+4}{2}.$$

If an even n divides $b(n)$, then both factors are integers, and therefore $2n$ divides $b(2n)$.

Substituting $b(n)$ into (2) when n is even yields

$$b(3n) = b(n)(b(n)^2 + 6b(n) + 12).$$

Therefore

$$\frac{b(3n)}{3n} = \frac{b(n)}{n}\frac{b(n)^2+6b(n)+12}{3}.$$

It is easy to prove that $b(n)$ is divisible by 3 when n is divisible by 6. Therefore, if an n divisible by 6 divides $b(n)$, then $3n$ divides $b(3n)$.

Since both $b(8)/8$ and $b(24)/24$ are integers, the theorem follows by induction. □

We now state without proofs (except for Theorem 4, where we give a sketch) a few other primality tests that have explicit infinite families of pseudoprimes.

Theorem 2. *Let*

$$\sum_{n=0}^{\infty} a(n)\, x^n \;:=\; \frac{x-2}{2x^2+x-1},$$

or equivalently, let $a(n)$ be the sequence defined by

$$a(1) = 1 \quad a(2) = 5$$
$$a(n) = a(n-1) + 2a(n-2).$$

Then $a(p) \equiv 1 \pmod p$ if p is prime. Furthermore, $\{2^i \,|i \geq 2\}$ are all pseudo-primes. That is, $a(2^i) \equiv 2^i \pmod{2^i}$ if $i \geq 2$.

Theorem 3. *Let*

$$\sum_{n=0}^{\infty} a(n)\, x^n \;:=\; \frac{2x-2}{2x^2+2x-1},$$

or equivalently, let $a(n)$ be defined by

$$a(1) = 2 \quad a(2) = 8$$
$$a(n) = 2a(n-1) + 2a(n-2).$$

Then $a(p) \equiv 2 \pmod p$ if p is prime. Furthermore, the following infinite families are all pseudo-primes:

$$\{3^i \mid i \geq 2\} \quad \{2 \cdot 3^i \mid i \geq 1\} \quad \{11 \cdot 81^i \mid i \geq 1\}$$
$$\{23 \cdot 3^{5i} \mid i \geq 1\} \quad \{29 \cdot 3^{4+12i} \mid i \geq 0\} \quad \{31 \cdot 3^{16i} \mid i \geq 1\}.$$

Theorem 4. *Let*

$$\sum_{n=0}^{\infty} a(n)\, x^n \ := \ \frac{2x^2+3}{2x^3+2x^2+1} \quad ,$$

or equivalently, let $a(n)$ *be defined by*

$$a(1)=0 \quad a(2)=-4 \quad a(3)=-6$$
$$a(n)=-2(a(n-2)+a(n-3)).$$

Then $a(p) \equiv 0 \pmod{p}$ *if* p *is prime. Furthermore, the following infinite families are all pseudo-primes:*

$$\{2^i \mid i \geq 2\} \quad \{3 \cdot 2^{4i} \mid i \geq 2\} \quad \{11 \cdot 2^{18i} \mid i \geq 2\} \quad \{13 \cdot 2^{17+20i} \mid i \geq 2\}.$$

Sketch of Proof. We use the *C-finite ansatz* [17]. It follows from the C-finite ansatz that

$$b(n)=a(2n)-a(n)^2$$

satisfies *some* recurrence. It turns out to be

$$b(n)=2b(n-1)+4b(n-3).$$

We now define

$$c(n) := \frac{b(n)}{2^{\lfloor n/2 \rfloor}},$$

and once again the C-finite ansatz implies that $c(n)$ satisfies some recurrence. (The even and odd terms are independently C-finite, and the interlacing of C-finite sequences is C-finite.) It turns out to be

$$c(n)=2c(n-2)+4c(n-4)+2c(n-6)$$

with initial conditions $-4,-4,-20,-24,-56,-76$. Note that $c(n)$ are manifestly *integers*. Going back to $a(n)$ we have the recurrence

$$a(2n)=a(n)^2+2^{\lfloor n/2 \rfloor}c(n) \quad ,$$

and it follows by induction that $a(2^i)/2^i$ are all integers. A similar argument goes for the other infinite families claimed. □

Theorem 5. *Let*

$$\sum_{n=0}^{\infty} a(n)\, x^n \ := \ \frac{2x^2+2x-3}{x^3+2x^2+x-1},$$

or equivalently, let $a(n)$ *be defined by*

$$a(1)=1 \quad a(2)=5 \quad a(3)=10$$
$$a(n)=a(n-1)+2a(n-2)+a(n-3).$$

Then $a(p) \equiv 1 \pmod{p}$ *for all primes* p*. Furthermore, the following infinite families are all pseudo-primes:*

$$\{3^i \mid i \geq 2\} \quad \{5 \cdot 3^{6+10\,i} \mid i \geq 0\} \quad \{5 \cdot 3^{8+10\,i} \mid i \geq 0\} \quad \{7 \cdot 3^{4+6\,i} \mid i \geq 0\}.$$

We found nine other such primality tests with infinite explicit families of presodoprimes. These can be viewed by typing `PDB(x);` in the Maple package `Perrin.txt`.

For fast computations and explorations using C programs, readers are welcome to explore the authors' GitHub repository.

Acknowledgment: Many thanks to Manuel Kauers for his computational prowess, and to the referee for a helpful remark.

References

[1] W. Adams and D. Shanks, Strong primality tests that are not sufficient, *Mathematics of Computation* **39** (1982), 255-300.

[2] A. E. Edlin and D. Zeilberger, The Goulden-Jackson Cluster method For cyclic Words, *Advances in Applied Mathematics* **25**(2000), 228-232.
`https://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/cgj.html` .

[3] S. W. Golomb, Combinatorial Proof of Fermat's "Little" Theorem, *The American Mathematical Monthly*, **63**(10), (Dec., 1956), 718.
`https://sites.math.rutgers.edu/~zeilberg/akherim/golomb56.pdf` .

[4] J. Grantham, There are infinitely many Perrin pseudoprimes, *Journal of Number Theory* **130** (2010), 1117-1128.

[5] S. Gurak, Pseudoprimes for Higher-Order Linear Recurrence Sequences, *Mathematics of Computation*, **55** (1990), 783-813.

[6] S. Holger, Millions of Perrin pseudoprimes including a few giants, arXiv:2002.03756 [math.NA]

[7] I. G. Macdonald, "Symmetric Functions and Hall Polynomials", Second Edition, Clarendon Press, Oxford, 1995.

[8] R. Perrin, Item 1484, *L'Intermèdiare des math* **6** (1899), 76-77.

[9] N. J. A. Sloane, The On-line Sequence of Integer Sequences, Sequence A001608,
`https://oeis.org/A001608` .

[10] N. J. A. Sloane, The On-line Sequence of Integer Sequences, Sequence A013998,
`https://oeis.org/A013998`

[11] N. J. A. Sloane, The On-line Sequence of Integer Sequences, Sequence A005854,
`https://oeis.org/A005845` .

[12] N. J. A. Sloane, The On-line Sequence of Integer Sequences, Sequence A000032,
`https://oeis.org/A000032` .

[13] I. Stewart, Tales of a Neglected Number, *Mathematical Recreations, Scientific American* **274**(6) (1996), pp. 102-103.

[14] V. Vatter, Social Distancing, Primes, and Perrin Numbers, , *Math Horizons*, **29**(1) (2022). https://sites.math.rutgers.edu/~zeilberg/akherim/vatter23.pdf .

[15] Wikipedia, Perrin Number, https://en.wikipedia.org/wiki/Perrin_number .

[16] D. Zeilberger, Enumerative and Algebraic Combinatorics, in: *Princeton Companion to Mathematics* (edited by W.T. Gowers), Princeton University Press, 2008, 550-561. https://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimPDF/enu.pdf .

[17] D. Zeilberger, The C-finite ansatz, *Ramanujan Journal* **31** (2013), 23-32. https://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/cfinite.html .