MATHEMATICS OF COMPUTATION
VOLUME 56, NUMBER 193
JANUARY 1991, PAGES 371–376

# A NOTE ON PERRIN PSEUDOPRIMES

STEVEN ARNO

ABSTRACT. The cubic recurrence $A(n+3) = A(n) + A(n+1)$ with initial conditions $A(0) = 3$, $A(1) = 0$, $A(2) = 2$, known as Perrin's sequence, is associated with several types of pseudoprimes. In this paper we will explore a question of Adams and Shanks concerning the existence of the so-called Q and I Perrin pseudoprimes, and develop an algorithm to search for all such pseudoprimes below some specified limit. As an example, we show that none exist below $10^{14}$.

## 1. INTRODUCTION

The cubic recurrence

$$A(n+3) = A(n) + A(n+1)$$

with initial conditions $A(0) = 3$, $A(1) = 0$, $A(2) = 2$ has several features which make it useful in the study of primes. Some of these features are quite old, dating back at least to an 1876 paper of Lucas [4] in which he examined $A(n)$ for $n > 0$ and proved that $n|A(n)$ if $n$ is a prime. Later, the sequence was reexamined by Perrin [5], and subsequently it became known as *Perrin's sequence.*

There are several types of pseudoprimes that one can associate with Perrin's sequence. Motivated by the discussion above, we define a pseudoprime to be a composite $n$ such that $n|A(n)$. The utility of this definition is of course dependent on the time it takes to calculate $A(n)$ modulo $n$, so it is fortunate that there is a simple $O(\log n)$ algorithm to do this [1]. This algorithm even gives us more than we requested. Given any integers $m$ and $n$, it provides a sextuple of the form

$$A(-n-1), A(-n), A(-n+1), A(n-1), A(n), A(n+1) \pmod m,$$

which we refer to as the *signature* of $n$ if $n = m$, and the *signature* of $n \pmod m$ if $n \neq m$ The following theorem describes the signature of a prime (see [1]).

**Theorem 1.** *Let* $f(x) = x^3 - x - 1$. *If* $f(x)$ *splits completely in* $(\mathbf{Z}/p\mathbf{Z})[x]$, *then we call* $p$ *an* $S$ *prime. The signature of an* $S$ *prime is*

$$1\ -1\ 3\ 3\ 0\ 2.$$

Received September 26, 1989; revised February 26, 1990 and March 19, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A41, 11B37.


0025-5718/91 $1.00 + $.25 per page

*If $f(x)$ has exactly one root in $\mathbf{Z}/p\mathbf{Z}$, then we call $p$ a $Q$ prime. The signature of a $Q$ prime is*

$$A \ -1 \ B \ B \ 0 \ C,$$

*where*

$$\begin{aligned} &B^3 - B - 1 = 0 \pmod p, \\ &A = B^{-2} + 2B \pmod p, \\ &C = B^2 - 2B^{-1} \pmod p. \end{aligned} \tag{1}$$

*If $f(x)$ is irreducible over $(\mathbf{Z}/p\mathbf{Z})[x]$, then we call $p$ an $I$ prime. The signature of an $I$ prime is*

$$0 \ -1 \ D' \ D \ 0 \ -1,$$

*where*

$$D' + D = -3 \pmod p, \qquad (D' - D)^2 = -23 \pmod p. \tag{2}$$

*Proof.* The proof is a simple computation. We illustrate by proving (1). Let $\mathbf{E}$ denote the algebraic closure of $\mathbf{Z}/p\mathbf{Z}$, and $\alpha_p$, $\beta_p$, $\gamma_p \in \mathbf{E}$ the roots of $f(x)$. Since the mapping $\phi\colon \mathbf{E} \to \mathbf{E}$ defined by $\phi(x) = x^p$ permutes the roots of $f(x)$, and $f(x)$ has exactly one root in $\mathbf{Z}/p\mathbf{Z}$, we can assume without loss of generality that $\alpha_p^p = \alpha_p$, $\beta_p^p = \gamma_p$, and $\gamma_p^p = \beta_p$. Define

$$C(n) = \alpha_p^n + \beta_p^n + \gamma_p^n,$$

and note that $A(n) = C(n) \pmod p$. It follows that

$$\begin{aligned} 0 &= C(p)C(-1) \\ &= C(p-1) + \alpha_p(\beta_p^{-1} + \gamma_p^{-1}) + \alpha_p^{-1}(\beta_p + \gamma_p) + 2 \\ &= C(p-1) + \alpha_p(\beta_p^{-1} + \gamma_p^{-1}) + \alpha_p^{-1}(\beta_p + \gamma_p) + 2\alpha_p\alpha_p^{-1} \\ &= C(p-1) + \alpha_p(C(-1) + C(1)) = C(p-1) - \alpha_p. \quad \square \end{aligned}$$

This theorem provides a simple way to strengthen our definition of a pseudoprime, i.e., a composite $n$ with an S, Q, or I signature. Note that a prime can have only one type of signature (assuming that $p \neq 23$). Indeed, from (2) we see that $D' \neq D$, which distinguishes I-type signatures, and from (1) combined with the fact that 3 is a solution of $f(x)$ if and only if $p = 23$, we distinguish between S- and Q-type signatures.

Combining our signature test with a quadratic character test leads to the notion of a Perrin pseudoprime. As is well known, one can evaluate a quadratic character in $O(\log n)$ steps, so the cost for this addition is relatively small. Our test is based on the following proposition (see [1]).

**Proposition 1.** *If $p$ is a $Q$ prime, then $(\frac{-23}{p}) = -1$. If $p$ is an $S$ or $I$ prime, $p \neq 23$, then $(\frac{-23}{p}) = 1$.*

**Definition.** An odd composite $n$ not divisible by 23 with an S (respectively Q or I) signature and an appropriate quadratic character $(\frac{-23}{n})$ is called an S (respectively Q or I) Perrin pseudoprime.

Our interest in Perrin pseudoprimes stems from a conjecture of Shanks which says that no Q or I Perrin pseudoprimes exist. If this were true, we would have an $O(\log n)$ primality test for 5/6 of the primes.

## 2. Searching for Q and I pseudoprimes

This section is devoted to the description of an algorithm for finding all Q and I pseudoprimes below some designated limit. In order to simplify our discussion, we specify the limit $10^{14}$. Our algorithm is based on the following theorem, which provides useful representations for certain types of pseudoprimes (see [1]).

**Theorem 2.** *Let $\omega_p$ denote the period of the sequence $\{A(n) \pmod p\}$. If an I prime $p$ divides an I pseudoprime $n$, then*

$$n = p + p\omega_p k, \quad \text{or} \quad n = p^2 + p\omega_p k$$

*for some integer $k$. If a Q prime $p$ divides a Q pseudoprime $n$, then*

$$n = p + p\omega_p k$$

*for some integer $k$.*

*Remark.* Various results about $\omega_p$ can be found in [1, 2]. For our purposes it will suffice to note that if $p$ is an S prime, then $\omega_p | p - 1$, if $p$ is a Q prime, then $\omega_p | p^2 - 1$, and if $p$ is an I prime, then $\omega_p | p^2 + p + 1$.

*Proof of Theorem* 2. If $n$ has an I signature modulo $n$, it has an I signature modulo $p$. By Theorem 1, this would require a triple of the form $D$, $0$, $-1$ to occur modulo $p$, where $D$ satisfies a quadratic equation. Since we are working over a field, there are at most two places where this can occur in the course of a given period $\omega(p)$. As two such places are known via Theorem 1, i.e., at $p$ and at $-p - 1 = p^2 \pmod{\omega_p}$, the first part of our theorem is established. The second part is proved similarly. □

*A general description of the algorithm.* Theorem 2 tells us that there are about $10^{14}/p\omega_p$ potential pseudoprimes that are multiples of a given Q or I prime $p$. If $p$ is of any reasonable size, we can check these multiples one-by-one. Further, since most Q and I primes have periods around $p^2$, only a small number of primes greater than $10^{14/3}$ require checking at all. With this in mind, we begin our attack by showing that if $n$ is a Q (respectively I) pseudoprime and $n < 10^{14}$, then $n$ is divisible by a Q (respectively I) prime $p$ such that $1 < p < 10^7$. This allows us to make full use of Theorem 2. If $p$ is small, however, the cost of checking potential multiples of $p$ can be prohibitive. Consequently, the next stage of our attack is devoted to showing that we can always assume that $p$ is of reasonable size.

It is instructive to understand why this algorithm will not work effectively for finding S Perrin pseudoprimes. First, it is possible that a Q or I prime

will divide an S pseudoprime (see [6]). This makes it difficult to exploit an S representation theorem like Theorem 2. Further, since S primes have small periods, the utility of such a representation theorem is greatly restricted in any case.

*A detailed description of the algorithm.* For the sake of simplicity we describe the algorithm only as it pertains to I pseudoprimes. The algorithm for Q pseudoprimes is exactly the same—just change every I to a Q, and every Q to an I in what follows.

Adams and Shanks show in [1] that no Q prime can divide any I pseudoprime. If we also knew that no S prime could divide any I pseudoprime, we would be able to invoke Theorem 2 directly, but this appears to be difficult to prove. In fact, it may not even be true. However, given a particular S prime $p$, it is usually easy to show that $p$ cannot divide any I pseudoprime. Indeed, if $p|n$, then $n$ must have an I signature modulo $p$. And since the sequence $\{A(m) \pmod p\}$ is periodic, one can check every triple in this sequence to see if such a signature occurs. Further, since the S primes have relatively small periods, this check can be done efficiently for S primes of reasonable size. This brings us to the first step of our algorithm.

*Step* 1. Show that no S prime $p$, $1 < p < 10^7$, can divide any I pseudoprime.

**Corollary.** *If $n$ is an I pseudoprime and $n < 10^{14}$, then $n$ is divisible by an I prime $p$ such that $1 < p < 10^7$.*

*Comment.* This is the most time-consuming part of our algorithm, taking roughly one day on one processor of a CRAY 2 (for both the Q and the I).

We are now in a position to use Theorem 2, though as pointed out above, direct use of this theorem can only be made if $p$ is large enough.

*Step* 2. Use Theorem 2 to check all potential multiples of I primes $p$ such that $300 < p < 10^7$.

**Corollary.** *Since we find no I pseudoprimes via Step 2, we conclude that if $n$ is an I pseudoprime and $n < 10^{14}$, then $n$ is divisible by an I prime $p$ such that $1 < p < 300$.*

*Comment* 1. The bound 300 is somewhat arbitrary. By raising this bound we would greatly reduce the time required for Step 2, but increase the time required for Steps 3, 4, and 5.

*Comment* 2. Instead of checking the signatures of potential pseudoprimes directly, one first sieves, using Q and S primes.

We now consider the case where $p$ is small. To circumvent the problems that arise here, let $\alpha$, $\beta$, and $\gamma$ be the roots of $f(x)$ over $\mathbf{C}$, and note that

$$\begin{aligned} A(mp) &= \alpha^{mp} + \beta^{mp} + \gamma^{mp} = (\alpha^m + \beta^m + \gamma^m)^p \pmod p \\ &= A(m) \pmod p. \end{aligned}$$

It follows that if $n = mp$ is a Perrin pseudoprime, then

$$p|(A(m), A(-m) + 1). \tag{3}$$

Hence, given any number $m$, we can find all prime multiples of $m$ that are potentially I pseudoprimes by finding the prime divisors of the gcd(3). We can then check the signatures of these numbers directly. This is our next step.

*Step* 3. Show that no prime multiple of an I prime $p$, $1 < p < 300$, is an I pseudoprime.

**Corollary.** *If $n$ is an I pseudoprime such that $n < 10^{14}$, then $n$ is divisible by at least two I primes $p_1$, $p_2$ such that $1 < p_1$, $p_2 < 300$.*

Now use the Chinese remainder theorem to modify Theorem 2: if $p_1$ and $p_2$ are two I primes which divide an I pseudoprime $n$, then for some integer $k$,

$$n = k\frac{p_1\omega_{p_1}p_2\omega_{p_2}}{d} + C,$$

where $d = (p_1\omega_{p_1}, p_2\omega_{p_2})$ and $C$ is easily calculated. We can now proceed as in Step 2.

*Step* 4. Use the modified version of Theorem 2 outlined above to check all potential multiples of products of distinct I primes $p_1$, $p_2$ such that $1 < p_1$, $p_2 < 300$.

**Corollary.** *If $n$ is an I pseudoprime less than $10^{14}$, then $n$ is divisible by the square of an I prime $p$ such that $1 < p < 300$.*

*Comment.* Step 4 would be quite long as described, since the progression for the primes 3 and 13 is still somewhat dense. However, by first applying Step 3 to numbers of the form $m = 3q$, where $q$ is an I prime less than 300, we will derive the corollary: if $n$ is an I pseudoprime such that $n < 10^{14}$, then either $n$ is divisible by at least two I primes $p_1$, $p_2$ such that $12 < p_1$, $p_2 < 300$, or $9|n$. It follows that we need to perform Step 4 only on pairs of distinct primes in the range $12 < p < 300$. This modification will significantly speed up Step 4, and can be extended if required.

*Step* 5. Use the method described for Step 1, i.e., check every triple in the sequence $\{A(m) \pmod n\}$ (with $n = p^2$) to show that 13 is the only small I prime whose square can divide any I pseudoprime. Also show that 13 cubed cannot divide any I pseudoprime.

**Corollary.** *If $n$ is an I pseudoprime such that $n < 10^{14}$, then $n$ is of the form $160p$, or $3 \cdot 169p$, for some prime $p$.*

*Comment.* It is now a simple matter to apply Step 3 with $m = 169$ and $m = 507$ to complete our search.

*Results.* Our implementation of this algorithm on a CRAY 2 was used to show that there are no Q or I Perrin pseudoprimes below $10^{14}$. A different algorithm

is given in [6], wherein it is shown that there are none below $50 \times 10^9$; it is simpler than ours, but less powerful as well.

## 3. Calculations

Some comments about the calculations are in order, since there are no pseudoprimes to list. There are 664579 primes less than $10^7$; 332466 Q primes, 221544 I primes, and 110569 S primes. As mentioned earlier, the search in Step 2 only involves those primes for which $p\omega_p < 10^{14}$, and the number of such primes relative to the potential number of primes is some indication of the strength of the method. It is therefore noteworthy that only 4255 of the Q primes and 1840 of the I primes satisfy this condition. Concerning Step 5, we note that 13 was the only I prime below 300 whose square could divide an I pseudoprime, while 97 was the only Q prime. As an example for Step 3, we note that $(A(281), A(-281) + 1) = 4496 = 2^4 \cdot 281$. Since a pseudoprime must be odd, we conclude that if there is one of the form $281p$, with $p$ prime, then it is $281^2$, which can be checked directly. Another example is given by $(A(97^2), A(-97^2) + 1) = 9560754560 = 2^7 \cdot 5 \cdot 7^3 \cdot 97 \cdot 449$. Since 449 is an S prime, we know from Step 1 that it does not divide a Q pseudoprime, and a simple check shows that neither $97^2 \cdot 5$, nor $97^2 \cdot 7$, are pseudoprimes. The entire running time for the search below $10^{14}$ was about 30 hours on one processor of a CRAY 2. Most of the time was spent in Step 1.

## Acknowledgments

I would like to thank Duncan Buell for supplying the gcd's that were required for Step 3, wherein arithmetic involving integers with several thousand bits is needed.

## Bibliography

1. W. Adams and D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. **35** (1982), 225–300.
2. W. Adams, *Characterizing pseudoprimes for third-order linear recurrences*, Math. Comp. **48** (1987), 1–15.
3. S. Lang, *Algebra*, Addison-Wesley, 1971.
4. E. Lucas, *Sur la recherche de grands nombres premiers*, A. F. Congrès du Clermont-Ferrand, 1876, pp. 61–68.
5. R. Perrin, *Item* 1484, L'Intermédiaire des Math. **6** (1899), 76–77.
6. D. Shanks, G. C. Kurtz, and A. C. Williams, *Fast primality test for numbers less than* $50 \times 10^9$, Math. Comp. **46** (1986), 691–701.

Supercomputing Research Center, 17100 Science Drive, Bowie, Maryland 20715-4300