MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 1–15

Characterizing Pseudoprimes for Third-Order Linear Recurrences

By William W. Adams*

Dedicated to Daniel Shanks on the occasion of his 70th birthday.

Abstract. This paper continues the work begun by D. Shanks and myself in [1] where certain cubic recurrences were used to give a very strong primality test. A complete characterization of the pseudoprimes for this test is given in terms of the periods of the corresponding sequences. Then these results are used to produce various types of pseudoprimes. A discussion of open problems is included.

1. Introduction. In [1], D. Shanks and I presented a pseudoprimality test that was manifestly very strong. Unfortunately, it appears that pinning down just how strong is problematical. However, in [3] computations are reported on that further show that the pseudoprimes for this test are extremely sparse. In the present paper characterizations of these pseudoprimes will be given in terms of the periods of the given recurrent sequences. Then examples of pseudoprimes for certain sequences will be given together with the method for constructing them.

The notation will be carried over directly from [1, Section 12]. Thus, r, s are integers, $A(-1) = s$, $A(0) = 3$, and $A(1) = r$. For any integer n, set

$$A(n+3) = rA(n+2) - sA(n+1) + A(n).$$

Set

$$f(X) = X^3 - rX^2 + sX - 1 = (X-\alpha)(X-\beta)(X-\gamma),$$

and let $K = \mathbf{Q}(\alpha, \beta, \gamma)$, d = discriminant of f, I_K the integers of K. We have

$$A(n) = \alpha^n + \beta^n + \gamma^n.$$

Associated to $A = A_f$, we have three types of "signatures" of $n \bmod m$ (at least, when f is a noncyclic irreducible cubic); that is, special forms for the sextuple of integers $A(-n-1)$, $A(-n)$, $A(-n+1)$, $A(n-1)$, $A(n)$, $A(n+1)$ read mod m [1, Section 13]. Each rational prime p, $p \nmid d$, has one of these signatures, called S, Q, I which correspond respectively to $f(x)$ split mod p, the product of a linear and irreducible quadratic, mod p, irreducible mod p [1, Section 14], respectively. The point is that it is difficult for a composite to have one of these signatures.

Received January 13, 1986.
1980 *Mathematics Subject Classification*. Primary 10A25, 10A35, 12A30.
*Partially supported by NSF Grant MCS 83-01431.

0025-5718/87 $1.00 + $.25 per page

The paper is organized as follows. In Section 2 we give the characterization of these pseudoprimes. In [1, Section 17] we established a certain p-adic congruence for primes p and here, in Section 3, we show that remarkably the corresponding congruence holds for any pseudoprime as well. In Section 4 the so-called "outsiders" of [1] for pseudoprimes are characterized. Also in [1] the primality tests were strengthened by certain other criteria and in Section 5 we discuss these so-called "acceptable" signatures in order to guarantee that the examples constructed in Section 6 do satisfy these more stringent conditions. Finally in Section 7 various open problems are discussed.

I would like to acknowledge my indebtedness to D. Shanks for his help and insight which have been so useful to me in the preparation of this paper. I would also like to thank J. Sonn for many helpful discussions. I would finally like to thank the Technion in Israel for their hospitality and stimulating atmosphere during the preparation of this paper.

2. Characterizing Pseudoprimes. We call a composite n a *pseudoprime A* (PSP A) if n has either an S, Q or I signature mod n (just say n has an S, Q or I signature). We denote by $W(m)$ the period of $A(n) \bmod m$.

For a composite integer $n > 0$, write $n = p_1^{\nu_1} \cdots p_t^{\nu_t}$ as its prime factorization.

LEMMA 1. *Let $T = S$, Q or I. Then n has a T signature if and only if for each i, $1 \leqslant i \leqslant t$, n has a T signature* mod $p_i^{\nu_i}$.

This follows immediately from the definition of signature. Of course, each of the primes will have their own signatures. The point is to see how various primes with various signatures can be combined to obtain n as a PSP A. We need some lemmas concerning the period of $A(n)$.

LEMMA 2. *Let $\varepsilon_1, \varepsilon_2 \in I_K$, $\mathfrak{A}$ be an integral ideal of I_K, $m \geqslant 1$ be a rational integer in $\mathfrak{A}$. Assume $\varepsilon_1 \equiv \varepsilon_2 \pmod{\mathfrak{A}^i}$. Then for all $j \geqslant 0$,*

$$\varepsilon_1^{m^j} \equiv \varepsilon_2^{m^j} \pmod{\mathfrak{A}^{j+i}}.$$

Proof. Use induction on j, the case $j = 0$ being the assumption. Assuming the result for $j - 1$, we have $\delta \in \mathfrak{A}^{j+i-1}$ such that $\varepsilon_1^{m^{j-1}} = \varepsilon_2^{m^{j-1}} + \delta$. Then

$$\varepsilon_1^{m^j} = \left(\varepsilon_2^{m^{j-1}} + \delta\right)^m = \varepsilon_2^{m^j} + m\delta\varepsilon_2^{m^{j-1}(m-1)} + \delta^2\rho$$

for some $\rho \in I_K$. Since $m\delta$, $\delta^2 \in \mathfrak{A}^{j+i}$, we are done. □

LEMMA 3. *Let m be an integer such that* $\gcd(m, 2d) = 1$. *Then for all $j \geqslant 1$,*

$$W(m^j) \mid m^{j-1}W(m).$$

Proof. From Theorem 7 of [1] we see that this follows directly from Lemma 2 for the case $\varepsilon_1 = \alpha^{W(m)}, \beta^{W(m)}, \gamma^{W(m)}$, $\varepsilon_2 = 1$, $\mathfrak{A} = mI_K$, $i = 1$. □

LEMMA 4. *Assume $n = p^\nu k$ with* $\gcd(p, 2d) = 1$ *and p prime. Then n has a signature* mod p^ν *implies* $W(p^\nu) = W(p)$.

Proof. Suppose n has a T signature mod p^ν ($T = S, Q$ or I). From Lemma 3 we have that $W(p^\nu) \mid p^{\nu-1}W(p)$. Moreover, we have from [1, Theorem 7] that

$$\begin{aligned}
&W(p^\nu) \mid p^\nu k - 1 && \text{if } T = S,\\
&W(p^\nu) \mid p^{2\nu}k^2 - 1 && \text{if } T = Q,\\
&W(p^\nu) \mid p^\nu\left(p^\nu k^2 + k\right) + 1 && \text{if } T = I.
\end{aligned}$$

Since $p^{\nu-1}$ is prime to each of the three numbers on the right, we see that $W(p^\nu) \mid p^{\nu-1}W(p)$ implies $W(p^\nu) \mid W(p)$. Then we are done since $W(p) \mid W(p^\nu)$. □

We now state the main result:

THEOREM 1. *Let n be a positive integer. Let p be a prime such that $p \mid n$, $p \nmid 2d$ and write $n = p^\nu k$ ($p \mid k$ is permissible). In the table below, for p being of the listed type (S, Q or I) (column 1) and ν satisfying the listed condition (column 2) we have that n has the listed signature (column 3) mod p^ν if and only if $W(p^\nu) = W(p)$ and the condition listed in the last column is true. If p is an S prime, then $f(x) \equiv (x-a)(x-b)(x-c) \pmod{p^\nu}$ for integers a, b, c, and the condition listed in the last column is for some permutation of a, b, c.*

p	ν	n	Condition: $W(p^\nu) = W(p)$ and
S	–	S	$k \equiv 1 \pmod{W(p)}$
S	–	Q	$a^{k-1} \equiv 1$, $b^k \equiv c \pmod{p^\nu}$
S	–	I	$a^k \equiv b$, $b^k \equiv c \pmod{p^\nu}$
Q	even	S	$k \equiv 1 \pmod{W(p)}$
Q	odd	S	$k \equiv p \pmod{W(p)}$
Q	even	Q	$k \equiv p \pmod{W(p)}$
Q	odd	Q	$k \equiv 1 \pmod{W(p)}$
Q	–	I	impossible
I	0 mod 3	S	$k \equiv 1 \pmod{W(p)}$
I	1 mod 3	S	$k \equiv p^2 \pmod{W(p)}$
I	2 mod 3	S	$k \equiv p \pmod{W(p)}$
I	–	Q	impossible
I	0 mod 3	I	$k \equiv p, p^2 \pmod{W(p)}$
I	1 mod 3	I	$k \equiv 1, p \pmod{W(p)}$
I	2 mod 3	I	$k \equiv 1, p^2 \pmod{W(p)}$

Proof. First consider the case where p is an S prime. Then for some integers a_0, b_0, c_0 we have that $f(x) \equiv (x-a_0)(x-b_0)(x-c_0) \pmod{p}$. We have assumed that $p \nmid d$ and thus the factorization of f lifts uniquely to a factorization $f(x) \equiv (x-a)(x-b)(x-c) \pmod{p^\nu}$ for integers a, b, c. Now assume n has some signature mod p^ν. By Lemma 4 and Corollary 8 of [1] we have $W(p^\nu) = W(p)$ and $W(p) \mid p-1$, and so by Theorem 7 of [1],

$$a^p \equiv a, \quad b^p \equiv b, \quad c^p \equiv c \pmod{p^\nu}. \tag{1}$$

If n is S mod p^ν, then from Theorem 7 of [1] we have $p^\nu k \equiv 1 \pmod{W(p)}$ and so $p \equiv 1 \pmod{W(p)}$ implies $k \equiv 1 \pmod{W(p)}$. If n is Q mod p^ν then from Theorem 3 of [1] there is a permutation of a, b, c so that $a^{p^\nu k} \equiv a$, $b^{p^\nu k} \equiv c \pmod{p^\nu}$ and then (1) yields the desired conclusion. Finally, if n is I, then Theorem 3 of [1] says that for some permutation of a, b, c we have $a^{p^\nu k} \equiv b$, $b^{p^\nu k} \equiv c \pmod{p^\nu}$ and again (1) yields the desired result.

We now consider the converse for S primes p. If $k \equiv 1 \pmod{W(p)}$, then since p is S we have $p \equiv 1 \pmod{W(p)}$ and thus $p^\nu k = n \equiv 1 \pmod{W(p)}$. Since by hypothesis $W(p^\nu) = W(p)$ we see that $n \equiv 1 \pmod{W(p^\nu)}$, which by Theorems 3, 7 of [1] shows that n has an S signature mod p^ν. Now assume that $a^{k-1} \equiv 1$, $b^k \equiv c \pmod{p^\nu}$. Since $W(p^\nu) = W(p)$ we have that (1) holds and so $a^{n-1} \equiv 1$, $b^n \equiv c \pmod{p^\nu}$. Then $abc \equiv 1 \pmod{p^\nu}$ implies $c^n \equiv a^{-n}b^{-n} \equiv a^{-1}c^{-1} \equiv b \pmod{p^\nu}$. Then

again by Theorem 3 of [1] we see n has a Q signature mod p^ν. The statement that $a^k \equiv b$, $b^k \equiv c \pmod{p^\nu}$ implies that n has an I signature mod p^ν follows in exactly the same way.

Now assume that p is a Q prime. Again, of course, Lemma 4 says $W(p^\nu) = W(p)$ if n has some signature. If n has an S signature then by Theorem 7 of [1], $n = p^\nu k \equiv 1 \pmod{W(p)}$. Then Corollary 8 of [1] and the hypothesis that p is a Q prime yields $p^2 \equiv 1 \pmod{W(p)}$ so that $k \equiv 1 \pmod{W(p)}$ if ν is even and $k \equiv p \pmod{W(p)}$ if ν is odd. Now assume n has a Q signature mod p^ν. Let $\mathfrak{P}$ be any prime of K lying over p. Then from Theorem 3 of [1] there is a permutation of the roots α, β, γ of $f(x)$ such that $\alpha^n \equiv \alpha$, $\beta^n \equiv \gamma$, $\gamma^n \equiv \beta \pmod{\mathfrak{P}^\nu}$. Also from Theorem 7 and Corollary 8 of [1], $\alpha^{p^2} \equiv \alpha$, $\beta^{p^2} \equiv \beta$, $\gamma^{p^2} \equiv \gamma \pmod{\mathfrak{P}}$. Combining these two relations yields $\alpha^k \equiv \alpha$, $\beta^k \equiv \gamma$, $\gamma^k \equiv \beta \pmod{\mathfrak{P}}$ if ν is even and $\alpha^{pk} \equiv \alpha$, $\beta^{pk} \equiv \gamma$, $\gamma^{pk} \equiv \beta \pmod{\mathfrak{P}}$ if ν is odd. Also from Theorems 3, 6 of [1] we have that $(\alpha^p, \beta^p, \gamma^p)$ is a 2-cycle permutation of $(\alpha, \beta, \gamma) \bmod \mathfrak{P}$. If $\beta^p \equiv \beta$, $\alpha^p \equiv \gamma$, $\gamma^p \equiv \alpha \pmod{\mathfrak{P}}$, then $\alpha \equiv \gamma^p \equiv \beta^{np} \equiv \beta^n \equiv \gamma \pmod{\mathfrak{P}}$, contradicting the hypothesis that $p \nmid d$. Similarly, $\gamma^p \equiv \gamma$, $\alpha^p \equiv \beta$, $\beta^p \equiv \alpha \pmod{\mathfrak{P}}$ is impossible. Thus $\alpha^p \equiv \alpha$, $\beta^p \equiv \gamma$, $\gamma^p \equiv \beta \pmod{\mathfrak{P}}$. Then if ν is even we see $\alpha^p \equiv \alpha^k$, $\beta^p \equiv \beta^k$, $\gamma^p \equiv \gamma^k \pmod{\mathfrak{P}}$ and so $k \equiv p \pmod{W(p)}$. Similarly, if ν is odd we see that $pk \equiv p \pmod{W(p)}$ and so $\gcd(p, W(p)) = 1$ yields the result. Finally, it was noted in Proposition 13 of [1] that n cannot have an I signature mod p and so cannot have one mod p^ν either.

We now prove the converse for Q primes p. We are assuming $k \equiv 1, p \pmod{W(p)}$. Since p is a Q prime we have $p^2 \equiv 1 \pmod{W(p)}$. Thus $n = p^\nu k \equiv 1 \pmod{W(p)}$ if ν is even and $k \equiv 1 \pmod{W(p)}$, or if ν is odd and $k \equiv p \pmod{W(p)}$; $n \equiv 1 \pmod{W(p)}$ and $W(p) = W(p^\nu)$ imply n has an S signature. Moreover, we see $n = p^\nu k \equiv p \pmod{W(p)}$ if ν is odd and $k \equiv 1 \pmod{W(p)}$, or if ν is even and $k \equiv p \pmod{W(p)}$. This, with $W(p) = W(p^\nu)$, implies that $\alpha^n \equiv \alpha^p$, $\beta^n \equiv \beta^p$, $\gamma^n \equiv \gamma^p \pmod{\mathfrak{P}^\nu}$. Since p has a Q signature, there is a permutation of α, β, γ such that $\alpha^p \equiv \alpha$, $\beta^p \equiv \gamma$, $\gamma^p \equiv \beta \pmod{\mathfrak{P}}$. We show that these last congruences hold mod $\mathfrak{P}^\nu$ as well by showing by induction that for $1 \leqslant \mu \leqslant \nu$ we have them mod $\mathfrak{P}^\mu$. We have that $W(p^\nu) = W(p)$ and $W(p) \mid p^2 - 1$, so $\alpha^{p^2} \equiv \alpha$, $\beta^{p^2} \equiv \beta$, $\gamma^{p^2} \equiv \gamma \pmod{\mathfrak{P}^\nu}$. Assume we know the result for μ: $\alpha^p \equiv \alpha$, $\beta^p \equiv \gamma$, $\gamma^p \equiv \beta \pmod{\mathfrak{P}^\mu}$ for $\mu < \nu$. Then from Lemma 2, $\beta^{p^2} \equiv \gamma^p \pmod{\mathfrak{P}^{\mu+1}}$ and so $\beta^{p^2} \equiv \beta \pmod{\mathfrak{P}^\nu}$ implies $\gamma^p \equiv \beta \pmod{\mathfrak{P}^{\mu+1}}$. Similarly for the other two congruences. Thus we have $\alpha^p \equiv \alpha$, $\beta^p \equiv \gamma$, $\gamma^p \equiv \beta \pmod{\mathfrak{P}^\nu}$ and $\alpha^n \equiv \alpha^p$, $\beta^n \equiv \beta^p$, $\gamma^n \equiv \gamma \pmod{\mathfrak{P}^\nu}$, which combine to yield $\alpha^n \equiv \alpha$, $\beta^n \equiv \gamma$, $\gamma^n \equiv \beta \pmod{\mathfrak{P}^\nu}$. Since this is true for all $\mathfrak{P} \mid p$ and p is unramified, we see from Theorem 3 of [1] that n has a Q signature mod p^ν, as desired.

Finally, we consider the case where p is an I prime. If n has a signature then by Lemma 4 again, $W(p^\nu) = W(p)$. If n has an S signature then $n = p^\nu k \equiv 1 \pmod{W(p)}$. Since p is an I prime we have $p^3 \equiv 1 \pmod{W(p)}$. These two congruences yield the desired results. Now assume n has an I signature mod p^ν. Then for some permutation of α, β, γ we have $\alpha^n \equiv \beta$, $\beta^n \equiv \gamma$, $\gamma^n \equiv \alpha \pmod{\mathfrak{P}^\nu}$. Since p is an I prime we have $W(p) \mid p^3 - 1$ and so $\alpha^{p^3} \equiv \alpha$, $\beta^{p^3} \equiv \beta$, $\gamma^{p^3} \equiv \gamma \pmod{\mathfrak{P}}$. If, for example, $\nu \equiv 0 \pmod 3$, we see $\alpha^k \equiv \beta$, $\beta^k \equiv \gamma$, $\gamma^k \equiv \alpha \pmod{\mathfrak{P}}$. Now $(\alpha^p, \beta^p, \gamma^p)$ is a 3-cycle permutation of (α, β, γ). If $\alpha^p \equiv \beta \pmod{\mathfrak{P}}$ we see

$\alpha^k \equiv \alpha^p$, $\beta^k \equiv \beta^p$, $\gamma^k \equiv \gamma^p \pmod{\mathfrak{P}}$ and so $k \equiv p \pmod{W(p)}$. If $\alpha^p \equiv \gamma \pmod{\mathfrak{P}}$, then $\alpha^{p^2} \equiv \gamma^p \equiv \beta \pmod{\mathfrak{P}}$ and so $k \equiv p^2 \pmod{W(p)}$. The other cases all follow similarly.

In the converse situation for I primes p we assume $k \equiv 1, p, p^2 \pmod{W(p)}$ and $W(p^\nu) = W(p)$. All the various cases are similar (or simpler) and so we will just consider the case where $\nu \equiv 2 \pmod 3$ and $k \equiv 1 \pmod{W(p)}$. We have $W(p^\nu) = W(p) \mid p^3 - 1$ and so $\alpha^{p^3} \equiv \alpha$, $\beta^{p^3} \equiv \beta$, $\gamma^{p^3} \equiv \gamma \pmod{\mathfrak{P}^\nu}$. We may assume, since α is an I prime, that $\alpha^p \equiv \beta$, $\beta^p \equiv \gamma$, $\gamma^p \equiv \alpha \pmod{\mathfrak{P}}$. Then from Lemma 2 we have $\alpha^{p^\nu} \equiv \beta^{p^{\nu-1}} \pmod{\mathfrak{P}^\nu}$ and so, $\alpha^{p^3} \equiv \alpha$, $\beta^{p^3} \equiv \beta \pmod{\mathfrak{P}^\nu}$ and $\nu \equiv 2 \pmod 3$ implies $\alpha^{p^\nu} \equiv \beta^p \pmod{\mathfrak{P}^\nu}$ and $\alpha^{p^2} \equiv \beta^p \pmod{\mathfrak{P}^\nu}$. Similarly, $\gamma^{p^2} \equiv \alpha^p \pmod{\mathfrak{P}^\nu}$. Then $\alpha^{p^\nu} \equiv \beta^p \equiv \alpha^{p^2} \equiv (\gamma^{p^2})^p \equiv \gamma \pmod{\mathfrak{P}^\nu}$. Since $k \equiv 1 \pmod{W(p^\nu)}$ we have then $\alpha^n = \alpha^{p^\nu k} \equiv \gamma \pmod{\mathfrak{P}^\nu}$. Similarly, $\gamma^n \equiv \beta$, $\beta^n \equiv \alpha \pmod{\mathfrak{P}^\nu}$. This is true for all $\mathfrak{P} \mid p$ and so we see n has an I signature mod p^ν, as desired. □

As an example, the most interesting composite discovered in [3] for the Perrin Sequence ($d = -23$, $r = 0$, $s = -1$) was $n = 24306384961 = 19 \cdot 53 \cdot 79 \cdot 89 \cdot 3433$. From Appendix I of [1] we see that 19, 53, 79, and 89 are all Q primes. Moreover, for $p = 19, 53, 79, 89$ we verify that $n/p \equiv p \pmod{p^2 - 1}$. In fact, for each of these p, $W(p) = (p^2 - 1)/2$ as is recorded in Appendix I of [1]. Finally, $p = 3433$ is an S prime and we can check that $n/p \equiv 1 \pmod{3432}$. Of course, $W(3433) \mid 3432$. Thus from Theorem 1 we see that n has an S signature.

We note from [3] up to 50×10^9, that 24306384961 is the only PSP Perrin that was not a product of S primes. All 55 have S signatures.

We also have

COROLLARY. *Let $p \nmid 2d$ be a prime, $\nu \geqslant 1$ be an integer. Then p^ν has a signature if and only if $W(p^\nu) = W(p)$.*

Proof. Indeed, this is the case $k = 1$ of Theorem 1. □

The signature can be read off the table of Theorem 1. For example, if p is a Q prime then p^ν has a Q signature if ν is odd and an S signature if ν is even (assuming $W(p^\nu) = W(p)$).

3. The n-Adic Congruence. In Theorem 14 of [1] it was shown that if p is a prime, $p \nmid 2d$, then for all $j \geqslant 1$,

$$A(p^j) \equiv A(p^{j-1}) \pmod{p^j}.$$

We thus obtained $\lim_{j \to \infty} A(p^j)$ existing in the p-adic integers. These limits are Abelian integers and have interesting applications (see [11]). In this section we will show that this result is not peculiar to primes, but holds more generally. We prove here

THEOREM 2. *Let $n, m > 1$ be integers such that $\gcd(m, 2d) = 1$ and $m \mid n$. Assume n has a signature* mod m *(either S, Q or I). Then for all $j \geqslant 1$,*

$$A(n^j) \equiv A(n^{j-1}) \pmod{m^j}.$$

Proof. Let $\mathfrak{P}$ be any prime ideal of I_K and assume $\mu \geqslant 1$ is the largest integer such that $\mathfrak{P}^\mu \mid m$. Then by Theorem 3 of [1] we see that $(\alpha^n, \beta^n, \gamma^n)$ is a permutation of (α, β, γ) mod $\mathfrak{P}^\mu$. In Lemma 2 let ε_1 be any one of $\alpha^n, \beta^n, \gamma^n$, and let ε_2 be the one of α, β, γ corresponding to it in the permutation, $\mathfrak{A} = \mathfrak{P}^\mu$ and the m of Lemma

2 is the n here. Then $\mathfrak{P}^{\mu} \mid m \mid n$ implies $n \in \mathfrak{P}^{\mu} = \mathfrak{A}$ and thus by Lemma 2, $\varepsilon_1^{n^j} \equiv \varepsilon_2^{n^j} \pmod{\mathfrak{P}^{\mu(j+1)}}$. This is true for $\varepsilon_1 =$ each of α^n, β^n, γ^n, and so we obtain

$$\alpha^{n^{j+1}} + \beta^{n^{j+1}} + \gamma^{n^{j+1}} \equiv \alpha^{n^j} + \beta^{n^j} + \gamma^{n^j} \pmod{\mathfrak{P}^{\mu(j+1)}},$$

i.e., $A(n^{j+1}) = A(n^j) \pmod{\mathfrak{P}^{\mu(j+1)}}$. Since this is true for all $\mathfrak{P} \mid m$, the result of the theorem follows. □

COROLLARY. *If* $\gcd(n, 2d) = 1$ *and* n *has a signature, then for all* $j \geqslant 1$,

$$A(n^j) \equiv A(n^{j-1}) \pmod{n^j}.$$

4. Outsiders. In [1] we defined the concept of an "outsider". This was important in constructing PSP A and in a sieving process described in Section 4 of [1].

We recall the definition of an outsider: Let p be a prime, and k be an integer. If

$$A(kp) \equiv A(1) \pmod{p} \quad \text{and} \quad A(-kp) \equiv A(-1) \pmod{p}, \tag{2}$$

but

$$k \not\equiv p^j \pmod{W(p)} \qquad (j = 0, 1, 2, \ldots),$$

then k is called an *outsider* for p.

It should be recalled that if $k \equiv p^j \pmod{W(p)}$, (2) does hold. This is because we know from [1] that $A(kp) \equiv A(k) \pmod{p}$ and so, writing $k = p^j + aW(p)$, we see

$$\begin{aligned} A(kp) \equiv A(k) = A\big(p^j + aW(p)\big) &\equiv A\big(p^j\big) \equiv A\big(p^{j-1}\big) \\ &\equiv \cdots \equiv A(1) \pmod{p}. \end{aligned}$$

Similarly, $A(-kp) \equiv A(-1) \pmod{p}$. Thus the outsider k's for p are in some sense the exceptional case. This was important in the sieving, since it was shown in [1] that they really are exceptional.

This is strengthened here because as a Corollary of Theorem 1 we see that we may in fact characterize those $n = kp$ where n has a signature mod p and k is an outsider for p.

THEOREM 3. *Assume* $n = kp$ *has a signature* mod *the prime* p *where* $p \nmid 2d$. *Then* k *is an outsider for* p *if and only if* n *has a* Q *or* I *signature and* p *is an* S *prime.*

Proof. If k is an outsider for p we may simply look at the table of Theorem 1 to see that only those two cases are allowable. Conversely, assume n is Q or I and p is S. Then from Theorem 1, $b^k \equiv c \pmod{p}$. If $k \equiv p^j \pmod{W(p)}$ we have $b^k \equiv b^{p^j} \equiv b \pmod{p}$, i.e., $b \equiv c \pmod{p}$, which contradicts the assumption that $p \nmid d$. □

5. Acceptable Signatures. In [1] we strengthened the primality test by adding an extra condition. These conditions will be recalled. Let $n > 1$ be an integer with $\gcd(n, 2d) = 1$. Write $n = p_1 \cdots p_t$ as its prime factorization.

First we say n has an *acceptable S signature* if and only if n has an S signature and $(\frac{d}{n}) = 1$ ((-) is the Jacobi symbol). For a prime $p \nmid d$ we have $(\frac{d}{p}) = -1$ if and only if p is a Q prime. Thus S primes have acceptable S signatures. Moreover, we see

> *n has an acceptable S signature if and only if n has an S signature and the number of Q primes p_i $(1 \leqslant i \leqslant t)$ is even.*

Similarly we say n has an *acceptable Q signature* if and only if n has a Q signature and $(\frac{d}{n}) = -1$. We obtain

n has an acceptable Q signature if and only if n has a Q signature and the number of Q primes p_i $(1 \leqslant i \leqslant t)$ is odd.

The definition for I primes is more complicated. See [4] for the necessary theory. Suppose n has an I signature. Then from the definition of an I signature, Eq. (137) of [1], we have an integer b satisfying $b^2 \equiv d \pmod{n}$. Since n is odd, we may assume b and d have the same parity. Then, since $d \equiv 0,1 \pmod 4$, we see that $b^2 \equiv d \pmod{4n}$. Write $d = b^2 - 4cn$. Then $F_n = nx^2 + bxy + cy^2$ is a quadratic form of discriminant d representing n. Consider the group of all classes of forms of discriminant d. Then there will be a subgroup of this group of index 3 which will represent S primes and not I primes. The two nontrivial cosets of this S subgroup will represent I primes but not S primes. We say n has an *acceptable I signature* if and only if F_n does not lie in the S subgroup.

Now the S and I primes p are the primes that split completely in $F = \mathbf{Q}(\sqrt{d})$ (we ignore, as usual, the primes $p \mid 2d$) and are distinguished by whether each factor from F splits or is inert in K, respectively. Thus, the Frobenius map for K/F distinguishes the S and I primes giving the index 3 subgroup noted above. (The correspondence between forms and ideal classes is a multiplicative isomorphism.) For example, if $n = pq$ where p is S and q is I and n has an I signature, we write $pI_F = \mathfrak{p}\mathfrak{p}'$, $qI_F = \mathfrak{q}\mathfrak{q}'$ in F and we see F_n must correspond to one of $\mathfrak{p}\mathfrak{q}$, $\mathfrak{p}\mathfrak{q}'$, $\mathfrak{p}'\mathfrak{q}$, $\mathfrak{p}'\mathfrak{q}'$. Since the classes of forms for $\mathfrak{p}$, $\mathfrak{p}'$ are S and for $\mathfrak{q}$, $\mathfrak{q}'$ are I, we see F_n must be an I form and so n has an acceptable I signature.

In passing, we note that although this test seems complicated, in practice the primality test is run for certain small discriminants where the group of forms can be given explicitly. Then checking acceptability is simply done by reducing the form F_n and comparing the result to the explicit list. In particular, for the much discussed cases of $d = -23$, -31, -44 in [1] the full group of forms has order 3 and the subgroup of S forms consists of just the identity form.

6. Construction of Examples. In this section we will show how the above can be used to construct acceptable signatures if we do not take as given in advance the particular recurrence. This answers a question left open in [1] concerning the existence of acceptable Q and I signatures.

We begin by constructing a composite with an acceptable Q signature. We will get $n = pq$ with p an S prime and q a Q prime. We noted in Section 5 that an n with a Q signature of this shape is automatically acceptable. From Theorem 1 we see the conditions that must be satisfied are q is a Q prime and

$$p \equiv 1 \pmod{W(q)} \tag{3}$$

and

$$f(X) \equiv (X-a)(X-b)(X-c) \pmod p \qquad (a, b, c \in \mathbf{Z}),$$

where

$$a^{q-1} \equiv 1 \pmod p, \quad b^q \equiv c \pmod p, \quad abc \equiv 1 \pmod p.$$

This latter condition is equivalent to

$$a^{q-1} \equiv 1 \pmod p, \quad b^{q+1} \equiv a^{-1} \pmod p, \quad b^q \equiv c \pmod p. \tag{4}$$

First choose any recurrence f_0 and a Q prime for f_0. For example, f_0 is Perrin and $q = 11$. Then $W(q) = 120$ and $r_0 = 0$, $s_0 = -1$.

Next choose any prime p satisfying (3). In the example, $p = 241$ is the least such prime. Now solve the equations (4) for a, b, c. Let g be a primitive root mod p. Assume $a \equiv g^{\nu} \pmod{p}$ and $b \equiv g^{\mu} \pmod{p}$. Then we need to solve

$$\nu(q-1) \equiv 0 \pmod{p-1} \quad \text{and} \quad \mu(q+1) \equiv -\nu \pmod{p-1}.$$

These can usually be solved. For our example,

$$10\nu \equiv 0 \pmod{240} \quad \text{and} \quad 12\mu \equiv -\nu \pmod{240},$$

and we see $\nu = 24t$ and $\mu \equiv -2t \pmod{20}$. Take, for example, $t = 1$ so $\nu = 24$, $\mu = 18$. Then $g = 7$ gives $a \equiv 7^{24} \equiv 36$, $b \equiv 7^{18} \equiv 236$, $c \equiv 236^{11} \equiv 162 \pmod{241}$. Thus

$$f_1(X) \equiv (X-36)(X-236)(X-162) \equiv X^3 - 193X^2 + 22X - 1.$$

So $r_1 = 193$, $s_1 = 22$. Now by the Chinese Remainder Theorem (CRT) solve

$$r \equiv r_0 \pmod{q}, \qquad s \equiv s_0 \pmod{q},$$
$$r \equiv r_1 \pmod{p}, \qquad s \equiv s_1 \pmod{p}.$$

In our example, this gives $r \equiv 1639 \pmod{11 \cdot 241 = 2651}$, $s \equiv 263 \pmod{2651}$. Thus for

$$f(X) = X^3 - 1639X^2 + 263X - 1,$$

$n = 2651 = 11 \cdot 241$ has an acceptable Q signature. Indeed, one can check that 1964 is a root of $f(X)$ mod 2651 and the signature of 2651 is

$$170 \quad 263 \quad 1447 \quad 1447 \quad 1639 \quad 2086$$

for which the definition, Eqs. (134) and (135) of [1], for a Q signature are valid.

In computing the signature of 2651 we note that $W(2651) = \operatorname{lcm}(W(11), W(241)) = \operatorname{lcm}(120, 40) = 120$. Then since $2651 \equiv 11 \pmod{120}$, we see that the signature of 2651 is the same as the signature of 11 mod 2651.

In the above example, we have from Theorem 3, since $p = 241$ is an S prime, that 241 is an outsider for 11. We now give an example of a composite n with a Q signature where no outsiders are present. From Theorems 1 and 2 this is only possible if n is a product of only Q primes. Moreover, from Section 5, in order for n to have an acceptable Q signature, it must be a product of an odd number of Q primes. Thus we will construct an $n = p_1p_2p_3$ where p_1, p_2, p_3 are all Q primes and n has a Q signature.

As is evident from Theorem 1, in order to construct suitable composites for suitable recurrences we must place severe divisibility requirements on the periods of the primes. To do this, we first find an appropriate type of prime p for any (say Perrin) recurrence and then reduce the period of p by changing the recurrence appropriately. The following lemma isolates this technique (greater generality in the lemma is easily given, but is not necessary here).

LEMMA 5. *Let $A_f(n)$ be the sequence corresponding to the cubic polynomial f. Let $p \nmid 2d$ be a prime with a T signature, where $T = Q$ or I. Let $u \mid W_f(p)$ be a positive integer such that $W_f(p) \nmid u(p-1)$ ($W_f(p) =$ period* mod *p with respect to f). Set*

$$g(X) = X^3 - A_f(u)X^2 + A_f(-u)X - 1.$$

Then for g, p is also a T prime, and

$$W_g(p) = W_f(p)/u.$$

Proof. As always, α, β, γ are the roots of f. (If $T = Q$, assume α corresponds to the rational root.) Then from Corollary 9 of [1], we have $W_f(p) = \operatorname{ord}_p \beta = \operatorname{ord}_p \gamma$ and $\operatorname{ord}_p \alpha \mid W_f(p)$. (Here ord_p denotes the multiplicative order in I_K/pI_K.) Now $g(X)$ has roots α^u, β^u, γ^u. We note that $\operatorname{ord}_p \beta^u = \operatorname{ord}_p \gamma^u = W_f(p)/u$ and $\operatorname{ord}_p \alpha^u \mid W_f(p)/u$ since

$$\operatorname{ord}_p \alpha^u = \frac{\operatorname{ord}_p \alpha}{\gcd(\operatorname{ord}_p \alpha, u)}.$$

Thus from Theorem 8 of [1] we see $W_g(p) = W_f(p)/u$. Now p is an S prime for g if and only if $W_g(p) \mid p - 1$, which we have assumed is not the case. Moreover, it is impossible for a Q prime for f to become an I prime for g, or vice versa, because, for example, f generates a degree 2 ($T = Q$) or degree 3 ($T = I$) extension of $\mathbf{Z}/p\mathbf{Z}$ which cannot contain an extension of the other degree. □

The integer $n = p_1 p_2 p_3$ has a Q signature where p_1, p_2, p_3 are Q primes if and only if

$$p_1 p_2 \equiv 1 \pmod{W(p_3)}, \quad p_1 p_3 \equiv 1 \pmod{W(p_2)} \quad \text{and} \quad p_2 p_3 \equiv 1 \pmod{W(p_1)} \tag{5}$$

(Theorem 1). Let f_0 be the Perrin polynomial, $f_0(X) = X^3 - X - 1$. We first choose two Q primes for Perrin, $p_1 = 7$, $p_2 = 11$. We have $W_{f_0}(p_1) = 48$ and $W_{f_0}(p_2) = 120$. We want to solve the congruences (5) for p_3. To facilitate this, we choose polynomials f_1, f_2 such that $W_{f_1}(p_1)$ and $W_{f_2}(p_2)$ are relatively prime. By Lemma 5 we see that for

$$f_1(X) \equiv X^3 - A_{f_0}(3)X^2 + A_{f_0}(-3)X - 1 \equiv X^3 - 3X^2 + 2X - 1 \pmod 7,$$

$p_1 = 7$ is a Q prime and $W_{f_1}(p_1) = 16$. Also for

$$f_2(X) \equiv X^3 - A_{f_0}(8)X^2 + A_{f_0}(-8)X - 1 \equiv X^3 - 10X + 5X - 1 \pmod{11},$$

we have $p_2 = 11$ is a Q prime and $W_{f_2}(p_2) = 15$. Now the congruences (5) become

$$7 \cdot 11 \equiv 1 \pmod{W(p_3)}, \quad 7p_3 \equiv 1 \pmod{15} \quad \text{and} \quad 11p_3 \equiv 1 \pmod{16}. \tag{6}$$

In particular, $W(p_3) \mid 76 = 4 \cdot 19$. Of course, $W(p_3) \mid p_3^2 - 1$. We need to get a Q prime, not an S prime, so we cannot have $W(p_3) \mid p_3 - 1$. So we find a prime p_3 so that $p_3 \equiv -1 \pmod{19}$ (19, not 76, to be sure this congruence is compatible with the second two congruences of (6)). By the CRT we solve this congruence and the second two congruences in (6) to get $p_3 \equiv 4483 \pmod{15 \cdot 16 \cdot 19}$. Now 4483 is prime, so set $p_3 = 4483$. We need a recurrence such that p_3 is a Q prime; there is a 50-50 chance that this occurs, so one is readily found. Indeed, 4483 is a Q prime for Perrin. We know $W_{f_0}(p_3) \mid 4483^2 - 1 = (2 \cdot 3^3 \cdot 83)(2^2 \cdot 19 \cdot 59)$. We again drop the period by Lemma 5. We find that for $u = 3^3 \cdot 83 \cdot 59$ we have for

$$f_3(X) = X^3 - A_{f_0}(u)X^2 + A_{f_0}(-u)X - 1 = X^3 - 1670X^2 + 1670X - 1,$$

$p_3 = 4483$ is a Q prime and $W_{f_3}(p_3) = 38$. We now have all the conditions (5) satisfied for the polynomial $f(X) = X^3 - rX^2 + sX - 1$ where r, s satisfy

$$r \equiv 3 \pmod 7, \quad r \equiv 10 \pmod{11}, \quad r \equiv 1670 \pmod{4483},$$
$$s \equiv 2 \pmod 7, \quad s \equiv 5 \pmod{11}, \quad s \equiv 1670 \pmod{4483},$$

which give for $n = 7 \cdot 11 \cdot 4483 = 345191$

$$r \equiv 10636 \pmod{n} \quad \text{and} \quad s \equiv 113745 \pmod{n}.$$

In the definition of a Q signature the root of the polynomial is given by $a_1 \equiv 6 \pmod 7$ for f_1, $a_2 \equiv 4 \pmod{11}$ for f_2, and $a_3 \equiv 1 \pmod{4483}$ for f_3. By the CRT we get $a \equiv 174838 \pmod n$ for the root of f. Computing, we get the signature of $n = 345191$ for

$$f(X) = X^3 - 10636X^2 + 113745X - 1$$

is

$$-121038 \quad 113745 \quad 248182 \quad 248182 \quad 10636 \quad -26895,$$

which is a Q signature corresponding to the root $a = 174838$. We note that

$$W(n) = \operatorname{lcm}(W(p_1), W(p_2), W(p_3)) = 16 \cdot 15 \cdot 19 = 4560.$$

As usual, we have had to drop the period substantially from the maximum $n^2 - 1 = 11.9 \times 10^{10}$.

Next, we briefly show how to find an acceptable I composite. We will construct $n = pq$ to have an I signature where p is an S prime and q is an I prime. In Section 5 we noted that this configuration for n guarantees that n has an acceptable I signature. From Theorem 1 we see we must have

$$p \equiv 1 \text{ or } q \pmod{W(q)} \tag{7}$$

and

$$f(X) \equiv (X - a)(X - a^q)(X - a^{q^2}) \pmod p, \tag{8}$$

where $a^{q^2+q+1} \equiv 1 \pmod p$. In order to guarantee the last condition, we need $q^2 + q + 1$ and $p - 1$ to have nontrivial common factors; this is trivial with the condition $p \equiv 1 \pmod{W(q)}$, since $W(q) \mid q^2 + q + 1$, but is also possible for $p \equiv q \pmod{W(q)}$. In order to guarantee p is unramified, it suffices to get $a^3 \not\equiv 1 \pmod p$.

We first note $q = 3$ is an I prime for Perrin with $W(3) = 13$. To make it easier, we find a prime $p \equiv 1 \pmod{W(3)}$ and choose $p = 53$. We choose $a \not\equiv 1 \pmod{53}$ so that $a^{13} \equiv 1 \pmod{53}$. We see $a \equiv 44 \pmod{53}$ works. Then $a^3 \equiv 13 \pmod{53}$ and $a^9 \equiv 24 \pmod{53}$. So define

$$f_1(X) \equiv (X - 44)(X - 13)(X - 24) \equiv X^3 - 28X^2 + 32X - 1 \pmod{53}.$$

So $\bmod 159 = 3 \cdot 53$ solve $r \equiv 0 \pmod 3$, $r \equiv 28 \pmod{53}$ and $s \equiv -1 \pmod 3$, $s \equiv 32 \pmod{53}$ to obtain

$$f(X) \equiv X^3 - 81X^2 + 32X - 1 \pmod{159},$$

for which $n = 159$ has an acceptable I signature. Indeed the signature of 159 for f is

$$81 \quad 32 \quad 67 \quad -22 \quad 81 \quad 32,$$

where $(67 - (-22))^2 \equiv d \pmod{159}$ and $67 + (-22) \equiv 81 \cdot 32 - 3 \pmod{159}$. We note that $W(n) = \operatorname{lcm}(W(3), W(53)) = 13$.

It was suggested that it might be harder to construct such composites for Abelian cubic polynomials. Of course, for such polynomials only S and I primes are possible. As a final example we construct an Abelian cubic with an acceptable I composite n. Again we will have $n = pq$, where p is an S prime and q is an I prime.

We obtain Abelian cubics by considering Shanks' class of *simplest cubics* (see [9]):

$$f(X) = X^3 - tX^2 - (t+3)X - 1, \tag{9}$$

which are known to be Abelian. Where before we had two degrees of freedom r, s, here we have just one. As a result, the polynomial we construct has very large coefficients.

As in the last example, we need to find two primes p, q and a polynomial $f(X)$ satisfying conditions (7) and (8) for which q is an I prime. Now, however, the polynomial $f(X)$ has the shape given in (9). This requires that we have the congruences

$$a^{q^2+q+1} \equiv 1 \pmod{p}, \tag{10}$$

$$a + a^q + a^{q^2} \equiv t \pmod{p}, \tag{11}$$

$$a^{-1} + a^{-q} + a^{-q^2} \equiv -t - 3 \pmod{p}. \tag{12}$$

Defining t by (11) we see that (11) and (12) may be replaced by

$$a + a^q + a^{q^2} + a^{-1} + a^{-q} + a^{-q^2} \equiv -3 \pmod{p}. \tag{13}$$

Our conditions now become (7), (10), and (13) and q is an I prime (we also want to ensure $f(X)$ is not ramified at p).

Our search procedure will now be described. Condition (13) is the one to concentrate on, as it is the most difficult to achieve. Indeed, we will achieve it without condition (7). Afterwards, condition (7) will be obtained by reducing the period as in Lemma 5. This latter is done after we have the simplest cubic we desire. Then defining g as in Lemma 5 we have that if f has roots α, β, γ, then g has roots α^u, β^u, γ^u and thus, even though g is no longer a simplest cubic, it is nevertheless Abelian.

We search for an integer $w (3 \nmid w)$ and a prime p such that $p \equiv 1 \pmod{w}$ (we will reduce the period to w) and such that there are integers q_0 and a satisfying $q_0^2 + q_0 + 1 \equiv 0 \pmod{w}$, $a^w \equiv 1 \pmod{p}$ and (13) is true for $q = q_0$. Given these, we first find a prime $q \equiv q_0 \pmod{w}$. Then find t_0 such that for the simplest cubic corresponding to t_0, q is an I prime with $w \mid W(q)$ (easy to do since there is a 50-50 chance that q is an I prime and $w \mid q^2 + q + 1$). Define $t_1 \equiv a + a^q + a^{q^2} \equiv a + a^{q_0} + a^{q_0^2} \pmod{p}$. Define $t \equiv t_0 \pmod{q}$ and $t \equiv t_1 \pmod{p}$. This t gives the desired simplest cubic. Set $u = W(q)/w$ and define g as in Lemma 5. Since $W(q) \nmid u(q-1)$ (i.e., $w \nmid q - 1$ since $w \mid q^2 + q + 1$) we see q is an I prime for g. Also p is an S prime for g of the desired shape, which is readily checked to be unramified. Hence the polynomial g gives the desired Abelian polynomial.

To find w, p we proceed as follows. Since $3 \nmid w$ and we need $q_0^2 + q_0 + 1 \equiv 0 \pmod{w}$, we search through w's all of whose prime factors are $\equiv 1 \pmod{6}$. For all such w, such q_0 exist. Given such a q_0, w we set, for integers ν,

$$\eta_\nu = \zeta_w^\nu + \zeta_w^{\nu q_0} + \zeta_w^{\nu q_0^2} + \zeta_w^{-\nu} + \zeta_w^{-\nu q_0} + \zeta_w^{-\nu q_0^2}$$

$$= 2\left(\cos\frac{2\pi\nu}{w} + \cos\frac{2\pi\nu q_0}{w} + \cos\frac{2\pi\nu q_0^2}{w}\right),$$

where $\zeta_w = \exp(2\pi i/w)$. We note that if $\nu \equiv \pm\mu,\ \pm q_0\mu,\ \pm q_0^2\mu$, then $\eta_\nu = \eta_\mu$. So define

$$F_w(X) = \prod(X - \eta_\nu),$$

where the product is over all ν such that $\gcd(\nu, w) = 1$ and where we avoid the obvious duplications in η_ν above. It is readily seen that $F_w(X)$ has integer coefficients. For each such w we compute $F_w(-3)$. Suppose p is a prime and $p \mid F_w(-3)$. Then in the field $\mathbf{Q}(\eta_1)$ we see p splits completely, and thus there is an integer $a \equiv \zeta_w \pmod{\mathfrak{p}}$ where $\mathfrak{p}$ lies over p. For this a, (13) is true for $q = q_0$. We would be done if $p \equiv 1 \pmod w$. We note that F_w should be irreducible over $\mathbf{Q}$ of degree $\phi(w)/6$ and so the degree of p in $\mathbf{Q}(\zeta_w)$ divides 6, i.e., $p^6 \equiv 1 \pmod w$. So the chance of $p \equiv 1 \pmod w$ seems reasonably good.

In performing the actual computations, $w = 91$ is the first time there is a $p \mid F_w(-3)$ with $p \equiv 1 \pmod w$. Indeed, $F_{91}(-3) = 2549 \equiv 1 \pmod{91}$. Then $q = q_0 = 107$ is a prime such that $q^2 + q + 1 \equiv 0 \pmod{91}$. For $t_0 = -1$ we have 107 is an I prime with period $q^2 + q + 1 = 91 \cdot 127$. Also for $a = 1933$ we have (13) for $q = 107$. Define

$$t_1 \equiv 1933 + 1933^{107} + 1933^{107^2} \equiv 2127 \pmod{2549}.$$

Define $t \equiv -1 \pmod{107}$, $t \equiv 2127 \pmod{2549}$ and set $t = 14872$. Finally, we reduce the period by setting $u = W(107)/91 = 127$ and define g as in Lemma 5. The polynomial g is Abelian and has $n = 107 \cdot 2549 = 272743$ with an I signature. We note that for g the coefficient $r \approx 14871^{127} \approx 7.7 \times 10^{529}$. The example is not small! But the period $W_g(p) = W_g(q) = 91$ is small.

7. Conclusions and Questions. The results of this paper clear up completely the question left open in [1] concerning the construction of pseudoprimes of various types when the recurrent sequence is not specified in advance. In [11], p-adic techniques are used to consider these questions from a different viewpoint. But other questions are still open and very important.

First we note that the techniques of this paper still do not allow us to construct a cubic polynomial for which there are an infinite number of pseudoprimes. In [8], Rotkiewicz shows the analogous result for many second-degree recurrent sequences, and this is a well-known result for the first-degree case (see [10]). Looking at the methods used in [8], we see they depend on the existence of two primitive prime divisors of certain related sequences. It is not at all clear what should replace these sequences in the cubic case.

The next question I would like to discuss is the one most emphasized in [1]. Namely, for the Perrin sequence ($r = 0$, $s = -1$), do there exist any composites with acceptable Q or I signatures? No examples are known. Let us see what this means. The problem has already been met a little in the construction of an Abelian example in the last section. There, reducing the degree of freedom from two (finding r, s) to one (finding t), complicated matters considerably. Of course, now we have no degrees of freedom.

Let us consider what should be one of the easier cases in more detail. Let us try to construct a composite $n = pq$, where p is an S prime, q is a Q prime, and n has a Q signature. As above (from Theorem 1), we need to determine a Perrin Q prime q

and S prime p satisfying conditions (3) and (4) for rational integers a, b, c, with a, b, c distinct. Comparing coefficients for $f(X) = X^3 - X - 1$ and eliminating the a, c we see that we need (3) and

$$b^{q^2-1} \equiv 1 \pmod{p}, \quad b^{-q-1} + b + b^q \equiv 0 \pmod{p}, \quad b^{-q} + b^{-1} + b^{q+1} \equiv -1 \pmod{p}, \tag{14}$$

for some integer b with b, b^q, and b^{-q-1} distinct. It is manifestly very difficult to find an integer b and primes p, q satisfying (3) and (14). No case is known.

We note that (14) is equivalent to finding an integer b such that $b^{q^2-1} \equiv 1 \pmod{p}$ and b is a zero of $f(X) = X^3 - X - 1$ and $g(X) = X^{2q+1} + X^{q+2} + 1$. Set $R_q =$ Resultant of f and g.

A formula for R_q can be given in terms of $A(n)$ for n near q and $2q$, so R_q can be computed in $O(\log q)$ steps. We note that for the first few q primes, $R_5 = 5^2$, $R_7 = 7^2$, $R_{11} = 2^3 \cdot 11^2$, $R_{17} = 17^2 \cdot 59$, and $R_{19} = 19^2 \cdot 173$. It is not hard to show that for Q primes q, $q^2 \mid R_q$ and to give congruence conditions for the S or I primes dividing R_q. Moreover, if for an S prime p, $p^2 \mid R_q$ then it can be shown that we are more than likely to obtain (14). In these examples the S primes p divide only to the first power, and indeed neither (3) nor $b^{q^2-1} \equiv 1 \pmod{p}$ are satisfied (indeed it can be shown that (14) implies $p^2 \mid R_q$). An example *might* be constructed by examining the R_q more closely, but it is still seen to be very unlikely for any given value of q.

We note in passing that similar statements can be made if q is an I prime with the same resultant R_q. Here one can show $q^3 \mid R_q$ and for an S prime p to work we need $p^3 \mid R_q$. We note $R_{31} = 31^3 \cdot 1669$ for the S prime 1669 and $R_{29} = 29^3 \cdot 3^3 \cdot 5^2$. More investigation is necessary here.

One final avenue of exploration will be discussed. In [12] it is shown that there is a probability of at least $1/2$ that the Euler Test for primality detects a composite. In [6] Rabin shows that there is a probability of at least $3/4$ that Gary Miller's so-called strong primality test will detect a composite (see also [5] and [10]). Rabin's test may be verified in the following way: For simplicity, let n be a *square-free* composite integer and let $R(n)$ be the number of integers a such that $1 \leqslant a \leqslant n$ and $\gcd(a, n) = 1$ and n is a strong pseudoprime a. For an odd integer m write $m - 1 = 2^{k_m} u_m$ where $2 \nmid u_m$. Say there are t primes p dividing n. Then

$$R(n) = \frac{2^{tK} + 2^t - 2}{2^t - 1} \prod_{p \mid n} \gcd(u_n, u_p), \tag{15}$$

where $K = \min k_p(p \mid n)$. This is easily proved (see [7]). A simple analysis shows that

$$R(n)/\phi(n) \leqslant \tfrac{1}{4}, \tag{16}$$

yielding Rabin's result ($\phi(n)$ is the Euler Phi Function). Moreover, the extreme cases are easily given.

The test under consideration in this paper is manifestly much stronger than the strong pseudoprimality test, and so an analogous result to Rabin's (and Solovay and Strassen's) should yield a better result than (16). The analogue to (15) can be derived, but because of the existence of S, Q, I primes, each with their own peculiarities, the formula is much more complicated. Given an integer n, we let the

r, s in $f(X) = X^3 - rX^2 + sX - 1$ range independently through a complete residue system modulo n for n^2 different values of r, s. Let $N(n)$ denote the number of these r, s such that n is unramified and has a signature. Again, for simplicity, assume n is square free. For a prime $p \mid n$ write $n = mp$. Then

(17)

$$N(n) = \prod_{p \mid n} \frac{\gcd(m-1, p-1)^2 + \gcd(m-p, p-1) + \gcd(m-p^2, p^2+p+1)}{6}$$

$$+ \prod_{p \mid n} \frac{\gcd(m^2-1, p-1) + \gcd(m-1, p^2-1) - 2\gcd(m-1, p-1)}{2}$$

$$+ \prod_{p \mid n} \frac{\gcd(m^2+m+1, p-1) + \gcd(m-1, p^2+p+1) + \gcd(m-p, p^2+p+1) - 3\varepsilon(p)}{3},$$

where

$$\varepsilon(p) = \begin{cases} 3 & \text{if } 3 \mid \gcd(m-1, p-1), \\ 1 & \text{otherwise.} \end{cases}$$

This result is derivable from Theorem 1. The first term counts the number of S signatures, the second the number of Q signatures, and the third the number of I signatures. As opposed to Rabin's simpler formula (15), from which (16) is readily derived, the various gcd's to bound in (17) seem much less tractable. It would be hoped that $N(n)/n^2$ can be shown to be quite small, allowing an improvement in the Rabin test—even allowing for the added computational complexity of the current test (at least for n large).

The following is a table of a few Carmichael numbers and $N(n)/n^2$. These numbers tend to maximize the contributions due to S signatures.

n	$N(n)/n^2$	n	$N(n)/n^2$
$561 = 3 \cdot 11 \cdot 17$	1/31.65	$7045248121 = 821 \cdot 1231 \cdot 6971$	1/215.53
$1729 = 7 \cdot 13 \cdot 19$	1/28.64	$2000436751 = 487 \cdot 1531 \cdot 2683$	1/215.33
$2465 = 5 \cdot 17 \cdot 29$	1/92.53		
$8911 = 7 \cdot 19 \cdot 67$	1/104.12		

We note that for Carmichael numbers $n = p_1 p_2 p_3$, $N(n)/n^2 \geqslant 1/6^3 = 1/216$.

Finally, we note that for Lucas-Lehmer sequences the analogue of (16) could also be asked. These primality tests are discussed in [2], where a version of the strong primality test is given. A formula analogous to (15) can be derived for this strong Lucas-Lehmer test, but again deriving a result similar to (16) seems difficult.

Department of Mathematics
University of Maryland
College Park, Maryland 20742

Technion
Israel Institute of Technology
Haifa, Israel

1. W. W. ADAMS & D. SHANKS, "Strong primality tests that are not sufficient," *Math. Comp.*, v. 39, 1982, pp. 255–300.

2. R. BAILLIE & S. S. WAGSTAFF, "Lucas pseudoprimes," *Math. Comp.*, v. 35, 1980, pp. 1391–1417.

3. G. KURTZ, D. SHANKS & H. C. WILLIAMS, "Fast primality tests for numbers less than $50 \cdot 10^9$," *Math. Comp.*, v. 46, 1986, pp. 691–701.

4. H. W. LENSTRA, "On the calculation of regulators and class numbers of quadratic fields," *J. Arith.*, 1980 (J. V. Armitage, ed.), Cambridge Univ. Press, 1982, pp. 123–150.

5. G. L. MILLER, "Riemann's hypothesis and tests for primality," *J. Comput. System Sci.*, v. 13, 1976, pp. 300–317.

→ M. O. RABIN, "Probabilistic algorithm for testing primality," *J. Number Theory*, v. 12, 1980, pp. 128–138.

7. K. ROSEN, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, Mass., 1984.

8. A. ROTKIEWICZ, "On the pseudoprimes with respect to the Lucas sequences," *Bull. Acad. Polon. Sci.*, v. 21, 1973, pp. 793–797.

9. D. SHANKS, "The simplest cubic fields," *Math. Comp.*, v. 28, 1974, pp. 1137–1152.

10. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, Chelsea, New York, 1978.

11. D. SHANKS & W. W. ADAMS, "Strong primality tests II. Algebraic identification of the *P*-adic limits and their implications." (In preparation.)

→ R. SOLOVAY & V. STRASSEN, "A fast Monte-Carlo test for primality," *SIAM J. Comput.*, v. 6, 1977, pp. 84–85.