FROBENIUS PSEUDOPRIMES

JON GRANTHAM

July 16, 1998

ABSTRACT. The proliferation of probable prime tests in recent years has produced a plethora of definitions with the word "pseudoprime" in them. Examples include pseudoprimes, Euler pseudoprimes, strong pseudoprimes, Lucas pseudoprimes, strong Lucas pseudoprimes, extra strong Lucas pseudoprimes and Perrin pseudoprimes. Though these tests represent a wealth of ideas, they exist as a hodge-podge of definitions rather than as examples of a more general theory. It is the goal of this paper to present a way of viewing many of these tests as special cases of a general principle, as well as to re-formulate them in the context of finite fields.

One aim of the reformulation is to enable the creations of stronger tests; another is to aid in proving results about large classes of pseudoprimes.

§1 INTRODUCTION

Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \bmod p$ for p an odd prime; thus we have an easy way to prove that many numbers are composite. For example, since $2^{90} \equiv 64 \bmod 91$, we prove that 91 is composite. The technique of repeated squaring can be used to perform the required exponentiation very rapidly.

This test is not foolproof. In particular, $2^{340} \equiv 1 \bmod 341$. Composites which fool the test with $a = 2$ are called pseudoprimes, and in general, composites n with $a^{n-1} \equiv 1 \bmod n$ are pseudoprimes to the base a.

The existence of such numbers provides incentive to create other tests which are similarly fast, but which may have fewer, or at least different, "pseudoprimes." Two of these tests are more elaborate versions of the test described above and create the notions of Euler pseudoprime and strong pseudoprime.

Most other tests, however, involve recurrence sequences. One reason that pseudoprimes based on recurrence sequences have attracted interest is that the pseudoprimes for these sequence are often different from ordinary pseudoprimes. In fact, nobody has claimed the \$620 offered for a Lucas pseudoprime with parameters $(1, -1)$ (see §2 for a definition of this term), congruent to 2 or 3 mod 5, that is also a pseudoprime to the base 2 [22, 14].

Furthermore, some tests based on higher order recurrence sequences seem to have few pseudoprimes. Adams and Shanks [2] introduced such a test based on a third order recurrence sequence known as Perrin's sequence.

A problem with tests based on recurrence sequences is that analysis of the tests can be difficult. For example, the concepts of Lucas and Lehmer pseudoprimes have

1991 *Mathematics Subject Classification.* 11Y11.

Typeset by $\mathcal{A}_\mathcal{M}\mathcal{S}$-TEX

been analyzed separately in the literature. In §2, we show that they are equivalent definitions.

Instead of recurrence sequences, the language used in this paper is that of finite fields. In particular, when n is a prime, $f(x) \in \mathbb{Z}[x]$, and n does not divide $\operatorname{disc}(f)$, the residue ring $\mathbb{Z}[x]/(n, f(x))$ is a product of finite fields of characteristic n. When n is composite, this ring is not equal to such a product. For a given composite n, this fact is often easy to discover, thus providing a quick proof of the compositeness of n. Using properties of finite fields, we establish the definition of Frobenius probable prime, which is a generalization, and sometimes a strengthening, of many existing definitions.

We introduce the concept of Frobenius pseudoprimes, not to inflict a new and different notion of pseudoprimality on the mathematical world, but to show that many existing pseudoprimality tests can be generalized and described in terms of finite fields. In fact, we show that some specific instances of the Frobenius pseudoprime test are equivalent to other pseudoprimality tests, and stronger than many of them.

In [11], we use the structure given by the introduction of finite fields to show that the probability of error in declaring a number "prime" using a certain Frobenius test is less than $\frac{1}{7710}$. In 1980, Monier [19] and Rabin [23] proved that the Strong Probable Prime Test has probability of error at most $\frac{1}{4}$. Although the test introduced in [11] has asymptotic running time three times that of the Strong Probable Prime Test, the proven bound on the error is much smaller than the $\frac{1}{64}$ achieved through three Strong Probable Prime Tests.

Perhaps the primary benefit of this approach is that instead of having to prove ten different theorems about ten different types of pseudoprimes, one can prove one theorem about Frobenius pseudoprimes and apply it to each type of pseudoprime.

In [12], the techniques of [3] are used to prove that for any monic, squarefree polynomial, there are infinitely many Frobenius pseudoprimes. In particular, this theorem answers a 1982 conjecture of Adams and Shanks [2] that there are infinitely many Perrin pseudoprimes. It also proves the infinitude of the types of pseudoprimes defined by Gurak [13] and Szekeres [27].

We should note that the idea of primality testing in finite fields is not entirely new. Lenstra's Galois Theory Test [17] is a method of proving primality using finite fields. In [10], I describe the relation between the two ideas. The combination of finite fields and pseudoprimes also exists implicitly in some other works, such as [27]. The goal here, however, is different. I am trying to provide a clear theoretical framework in which various existing probable prime tests can be generalized and analyzed.

§2 A Wealth of Pseudoprimes

For the purposes of this paper, the following test for primality will be considered foolproof. If an integer is denoted by the letter p, then p is prime. If q is a prime power, we let $\mathbb{F}_q$ denote a finite field with q elements.

We begin by reviewing many of the existing notions of pseudoprimality. Each of these definitions of "pseudoprime" characterizes composite numbers with a certain property. In each of these cases, it can be proven that all prime numbers (with a finite, known set of exceptions) have this property.

This paper does not pretend to be an exhaustive treatment of all notions of pseudoprimality. For example, nothing is said about elliptic pseudoprimes [8].

Fermat's Little Theorem tells us that if p is prime, then $a^{p-1} \equiv 1 \bmod p$, if $p \nmid a$. The original notion of a pseudoprime (sometimes called a Fermat pseudoprime) involves counterexamples to the converse of this theorem.

Definition. *A* **pseudoprime** *to the base a is a composite number n such $a^{n-1} \equiv 1 \bmod n$.*

Definition. *A number n which is a pseudoprime to all bases a with $(a,n) = 1$ is a* **Carmichael number***.*

We also know that if p is an odd prime, then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \bmod p$, where $\left(\frac{a}{p}\right)$ is the Jacobi symbol. The converse of this theorem leads to the definition of Euler pseudoprime, due to Raphael Robinson [24].

Definition. *An* **Euler pseudoprime** *to the base a is an odd composite number n with $(a,n) = 1$ such that $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n$.*

An Euler pseudoprime to the base a is also a pseudoprime to the base a.

If $n \equiv 1 \bmod 4$, we can also look at $a^{(n-1)/2^k}$ for $k > 1$, and doing so gives us the definition of strong pseudoprime [22], due independently to R. Dubois and John Selfridge.

Definition. *A* **strong pseudoprime** *to the base a is an odd composite $n = 2^r s + 1$ with s odd such that either $a^s \equiv 1 \bmod n$, or $a^{2^t s} \equiv -1$ for some integer t, with $r > t \geq 0$.*

A strong pseudoprime to the base a is also an Euler pseudoprime to the base a [19, 22].

It is possible to define notions of pseudoprimality based on congruence properties of recurrence sequences. The simplest of these are based on the Lucas sequences $U_n(P,Q)$, where P and Q are integers, $U_0 = 0$, $U_1 = 1$ and $U_n = PU_{n-1} - QU_{n-2}$. (When $P = 1$ and $Q = -1$, this is the Fibonacci sequence.)

We recall the fact that we can express U_n in terms of roots of the polynomial $f(x) = x^2 - Px + Q$. If α and β are roots of $f(x)$ in a commutative ring (with identity), with $\alpha - \beta$ invertible, then $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. By induction on n, this equality holds even if there are more than two distinct roots of $f(x)$.

Theorem 2.1. *Let $U_n = U_n(P,Q)$ and $\Delta = P^2 - 4Q$. If $p \nmid 2Q\Delta$, then $U_{p - \left(\frac{\Delta}{p}\right)} \equiv 0 \bmod p$.*

Proof. Since $p \nmid \Delta$, $x^2 - Px + Q$ has distinct roots, α and β, in $\bar{\mathbb{F}}_p$.

If $\left(\frac{\Delta}{p}\right) = 1$, then $f(x)$ factors mod p, and α and β are in $\mathbb{F}_p$. Thus $\alpha^{p-1} \equiv \beta^{p-1} \equiv 1 \bmod p$. So $U_{p-1} \equiv (1-1)/(\alpha - \beta) = 0 \bmod p$.

If $\left(\frac{\Delta}{p}\right) = -1$, then $f(x)$ does not factor, and the roots of $f(x)$ lie in $\mathbb{F}_{p^2}$. The Frobenius automorphism permutes the roots of $f(x)$, so $\alpha^p \equiv \beta$ and $\beta^p \equiv \alpha$. Thus $U_{p+1} \equiv (\alpha\beta - \beta\alpha)/(\alpha - \beta) = 0 \bmod p$.

Definition. *Let $U_n = U_n(P,Q)$ and $\Delta = P^2 - 4Q$. A* **Lucas pseudoprime** *with parameters (P,Q) is a composite n with $(n, 2Q\Delta) = 1$ such that $U_{n - \left(\frac{\Delta}{n}\right)} \equiv 0 \bmod n$.*

Baillie and Wagstaff [7] gave a version of this test that is analogous to the strong pseudoprime test. We first define the sequence $V_n(P,Q)$ to be the sequence with

$V_0 = 2$, $V_1 = b$, and $V_n = PV_{n-1} - QV_{n-2}$. Note that $V_n = \alpha^n + \beta^n$, where α and β are distinct roots of $x^2 - Px + Q$.

Theorem 2.2. *Let $U_n = U_n(P,Q)$ and $\Delta = P^2 - 4Q$. Let p be a prime not dividing $2Q\Delta$. Write $p = 2^r s + \left(\frac{\Delta}{p}\right)$, where s is odd. Then either $U_s \equiv 0$ or $V_{2^t s} \equiv 0 \bmod p$ for some t, $0 \le t < r$.*

Proof. As above, since $p \nmid \Delta$, $x^2 - Px + Q$ has distinct roots in $\bar{\mathbb{F}}_p$. If $\left(\frac{\Delta}{p}\right) = 1$, the roots α and β are elements of $\mathbb{F}_p$. If $\left(\frac{\Delta}{p}\right) = -1$, they are elements of $\mathbb{F}_{p^2}$. Their product is $\alpha\beta = Q \ne 0$, so $\beta \ne 0$.

We have that $U_{2^r s} = (\alpha^{2^r s} - \beta^{2^r s})/(\alpha - \beta) \equiv 0 \bmod p$. Thus $(\alpha/\beta)^{2^r s} \equiv 1 \bmod p$. Taking square roots, we have that either $(\alpha/\beta)^{2^t s} \equiv -1$ for some t with $0 \le t < r$, or $(\alpha/\beta)^s \equiv 1$.

In the first case, we can conclude $V_{2^t s} \equiv 0 \bmod p$, while in the second case we have that $U_s \equiv 0 \bmod p$.

Definition. *Let $U_n = U_n(P,Q)$, $V_n = V_n(P,Q)$, and $\Delta = P^2 - 4Q$. A* **strong Lucas pseudoprime** *with parameters (P,Q) is a composite $n = 2^r s + \left(\frac{\Delta}{n}\right)$, where s is odd and $(n, 2Q\Delta) = 1$ such that either $U_s \equiv 0 \bmod n$ or $V_{2^t s} \equiv 0 \bmod n$ for some t, $0 \le t < r$.*

Any strong Lucas pseudoprime is also a Lucas pseudoprime with the same parameters.

Jones and Mo [18] have recently given another test that relies on the sequences $U_n(b,1)$ and $V_n(b,1)$.

Theorem 2.3. *Let $U_n = U_n(b,1)$, $V_n = V_n(b,1)$, and $\Delta = b^2 - 4$. Let p be a prime not dividing 2Δ. Write $p = 2^r s + \left(\frac{\Delta}{p}\right)$, where s is odd. Then either $U_s \equiv 0 \bmod p$ and $V_s \equiv \pm 2 \bmod p$, or $V_{2^t s} \equiv 0 \bmod p$, for some t, $0 \le t < r - 1$.*

Proof. By Theorem 2.2, it suffices to show that $V_{2^{r-1} s} \not\equiv 0$, and that if $U_s \equiv 0$, then $V_s \equiv \pm 2$.

Note that $V_n = \alpha^n + \alpha^{-n}$, where α is a root of $x^2 - bx + 1$. So $V_{2^{r-1} s} \equiv 0 \bmod p$ implies $\alpha^{2^r s} \equiv -1$. If $\left(\frac{\Delta}{p}\right) = 1$, then $\alpha \in \mathbb{F}_p$, and we have a contradiction. If $\left(\frac{\Delta}{p}\right) = -1$, then $\alpha^p \equiv \alpha^{-1}$. So $\alpha^{p+1} \equiv 1 \not\equiv -1$, and we also have a contradiction.

If $U_s \equiv 0 \bmod p$, then $\alpha^s \equiv \alpha^{-s} \bmod p$, and thus $\alpha^{2s} \equiv 1$. We must have $\alpha^s \equiv \pm 1$, and thus $V_s \equiv \pm 2$.

Definition. *Let $U_n = U_n(b,1)$, $V_n = V_n(b,1)$, and $\Delta = b^2 - 4$. An* **extra strong Lucas pseudoprime** *to the base b is a composite $n = 2^r s + \left(\frac{\Delta}{n}\right)$, where s is odd and $(n, 2\Delta) = 1$, such that either $U_s \equiv 0 \bmod n$ and $V_s \equiv \pm 2 \bmod n$, or $V_{2^t s} \equiv 0 \bmod n$ for some t with $0 \le t < r - 1$.*

Any extra strong Lucas pseudoprime base b is a strong Lucas pseudoprime with parameters $(b, 1)$.

The definition of Lehmer pseudoprime, due to Rotkiewicz [25], is related to that of Lucas pseudoprime.

The Lehmer sequence with parameters (L,Q) is defined by $\bar{U}_0 = 0$, $\bar{U}_1 = 1$, $\bar{U}_k = L\bar{U}_{k-1} - Q\bar{U}_{k-2}$ for k odd, and $\bar{U}_k = \bar{U}_{k-1} - Q\bar{U}_{k-2}$ for k even. It is easy to see by induction that $\bar{U}_k = (\alpha^k - \beta^k)/(\alpha^2 - \beta^2)$ for k even, and $\bar{U}_k = (\alpha^k - \beta^k)/(\alpha - \beta)$ for k odd, where α and β are roots of $x^2 - \sqrt{L}x + Q$.

Definition. *Let $D = L - 4Q$ and $\epsilon(n) = \left(\frac{LD}{n}\right)$. A* **Lehmer pseudoprime** *with parameters (L, Q) is a composite n with $(2LD, n) = 1$ and $\bar{U}_{n-\epsilon(n)} \equiv 0$ mod n.*

Lehmer pseudoprimes can be analyzed by the same means as Lucas pseudoprimes, because of the following new result.

Theorem 2.4. *An integer n is a Lehmer pseudoprime with parameters (L, Q) if and only if it is a Lucas pseudoprime with parameters (L, LQ).*

Proof. Let $D = L - 4Q$ be the discriminant of the Lehmer sequence. The characteristic polynomial of the Lucas sequence is $f(x) = x^2 - Lx + LQ$, which has discriminant $L^2 - 4LQ = LD$. So $\epsilon(n) = \left(\frac{L^2-4LQ}{n}\right)$. The roots of $f(x)$ are $\alpha = \frac{L+\sqrt{L^2-4LQ}}{2}$ and $\beta = \frac{L-\sqrt{L^2-4LQ}}{2}$. The characteristic polynomial of the Lehmer sequence is $g(x) = x^2 - \sqrt{L}x + Q$. Its roots are $\alpha' = \alpha/\sqrt{L}$ and $\beta' = \beta/\sqrt{L}$.

Thus $L^{(n-\epsilon(n))/2}\bar{U}_{n-\epsilon(n)} = U_{n-\epsilon(n)}$, and we conclude that $\bar{U}_{n-\epsilon(n)} \equiv 0 \bmod n$ if and only if $U_{n-\epsilon(n)} \equiv 0 \bmod n$. This proves the theorem.

Rotkiewicz [26] has also given a definition of strong Lehmer pseudoprime.

Definition. *Let $\bar{U}_k$ be as in the definition of Lehmer pseudoprime. Let $\bar{V}_n$ satisfy $\bar{V}_0 = 2$, $\bar{V}_1 = 1$, $\bar{V}_k = L\bar{V}_{k-1} - Q\bar{V}_{k-2}$ for k even, and $\bar{V}_k = \bar{V}_{k-1} - Q\bar{V}_{k-2}$ for k odd. Let $\epsilon(n)$ be as above. An odd composite number $n = 2^r s + \epsilon(n)$ is a* **strong Lehmer pseudoprime** *with parameters (L, Q) if $(n, DQ) = 1$ and either $\bar{U}_s \equiv 0 \bmod n$ or $\bar{V}_{2^t s} \equiv 0$ for some t with $0 \le t < r$.*

Theorem 2.5. *An integer n is a strong Lehmer pseudoprime with parameters (L, Q) if and only if it is a strong Lucas pseudoprime with parameters (L, LQ).*

Proof. The technique of proof is exactly the same as for Theorem 2.4.

In a series of papers in the 1980s ([2], [16] and [1]), Adams, Shanks and coauthors proposed and analyzed a pseudoprime test based on a third order recurrence sequence known as Perrin's sequence, and on generalizations of this sequence. A good exposition of the test is given in [5].

We consider sequences $A_n = A_n(r, s)$ defined by the following relations: $A_{-1} = s$, $A_0 = 3$, $A_1 = r$, and $A_n = rA_{n-1} - sA_{n-2} + A_{n-3}$. Let $f(x) = x^3 - rx^2 + sx - 1$ be the associated polynomial and Δ its discriminant. Perrin's sequence is $A_n(0, -1)$.

Definition. *The* **signature mod** *m of an integer n with respect to the sequence $A_k(r, s)$ is the 6-tuple $(A_{-n-1}, A_{-n}, A_{-n+1}, A_{n-1}, A_n, A_{n+1}) \bmod m$.*

Definitions. *An integer n is said to have an* **S-signature** *if its signature mod n is congruent to $(A_{-2}, A_{-1}, A_0, A_0, A_1, A_2)$.*

An integer n is said to have a **Q-signature** *if its signature mod n is congruent to (A, s, B, B, r, C), where for some integer a with $f(a) \equiv 0 \bmod n$, $A \equiv a^{-2} + 2a$, $B \equiv -ra^2 + (r^2 - s)a$, and $C \equiv a^2 + 2a^{-1}$.*

An integer n is said to have an **I-signature** *if its signature mod n is congruent to (r, s, D', D, r, s), where $D' + D \equiv rs - 3$ mod n and $(D' - D)^2 \equiv \Delta$.*

Definition. *A* **Perrin pseudoprime** *with parameters (r, s) is an odd composite n and either*

1) $\left(\frac{\Delta}{n}\right) = 1$ and n has an S-signature or an I-signature, or

2) $\left(\frac{\Delta}{n}\right) = -1$ *and* n *has a Q-signature.*

In the past, the term Perrin pseudoprime has referred only to pseudoprimes with respect to Perrin's original sequence, but we feel it is useful to have a convenient name for composites having an acceptable signature for other such sequences.

Also, we have omitted a portion of the test involving quadratic forms. If n has an I-signature, it is possible to construct a quadratic form representing n. A prime with an I-signature can only be represented by forms lying in a certain subgroup of the class group of quadratic forms with discriminant Δ. The only examples found where this portion of the test has exposed composites involve pseudoprimes very small compared to the discriminant of the associated polynomials. In fact, the polynomials were cleverly constructed specifically to have pseudoprimes which would be exposed in this way. In particular, there are no known examples where the quadratic form exposes a composite for the test using Perrin's sequence. The test does not apply to integers with Q-signatures or S-signatures. The interested reader should consult [2] for details.

Generalizations to higher order recurrence sequences have been given by Gurak [13]. His basic definition is shown below to be subsumed in the definition of Frobenius pseudoprimes. Later in his paper, he gives ideas as to how his test could be made stronger. He does not, however, give exact definitions of other notions of pseudoprimality.

A nice variation on these tests is given by Szekeres [27].

Definition. *Let* $f(x)$ *be an irreducible polynomial in* $\mathbb{Z}[x]$ *and* $\beta_1, \ldots, \beta_k$ *be its roots. A* **pseudoprime (in the sense of Szekeres)** *is a composite* n *such that for every symmetric polynomial* $S(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$, $S(\beta_1^n, \ldots, \beta_k^n) \equiv S(\beta_1, \ldots, \beta_k) \bmod n$.

Szekeres does not test signatures and notes, "Signatures can be tested without much additional effort but they don't seem to add significantly to the efficiency of primality testing through higher order Lucas sequences ... " He also does not use knowledge gained from Jacobi symbols in his test.

Atkin has proposed a specific test based on arithmetic modulo polynomials; it shares some similarities with the test described in Section 3. He describes it fully in [6].

§3 Frobenius Pseudoprimes

In this section, We will be introducing the definition of Frobenius pseudoprime. This definition does not in and of itself solve any open questions in the subject. We do, however, aim to provide a clearer way of thinking about the definitions given in the previous section. Some open questions are solved in [11] and [12].

We first prove some elementary facts about polynomials over finite fields. In particular, we exploit the following fact. Given a polynomial $f(x)$ of degree d, we can factor it as $\prod_1^d F_i(x)$, where each $F_i(x)$ is the product of the irreducible polynomials of degree i dividing $f(x)$.

Theorem 3.1. *Let* p *be an odd prime, and let* $f(x)$ *be a monic polynomial in* $\mathbb{F}_p[x]$ *of degree* d *with discriminant* Δ. *Assume* $p \nmid f(0)\Delta$.

1) Let $f_0(x) = f(x)$. *For* $1 \le i \le d$, *define* $F_i(x) = \gcd(x^{p^i} - x, f_{i-1}(x))$ *in* $\mathbb{F}_p[x]$ *and* $f_i(x) = f_{i-1}(x)/F_i(x)$. *Then* $f_d(x) = 1$, *and for each* i, $1 \le i \le d$, $i \mid \deg(F_i)$.

2) For $2 \le i \le d$, $F_i(x) | F_i(x^p)$.

3) Let $S = \sum_{2|i} \deg(F_i(x))/i$. Then $(-1)^S = \left(\frac{\Delta}{p}\right)$. That is, if $\left(\frac{\Delta}{p}\right) = 1$, then S is an even integer, and if $\left(\frac{\Delta}{p}\right) = -1$, then S is an odd integer.

Proof. 1) The polynomial $x^{p^i} - x$ is the product of all irreducible polynomials in $\mathbb{F}_p[x]$ with degree dividing i. Inductively, we see that

$$F_i(x) = \gcd\left(\prod_{j|i}(x^{p^j} - x)^{\mu(i/j)}, f(x)\right),$$

where μ is the Mobius function. Thus $F_i(x)$ is the product of all irreducible factors of $f(x)$ of degree exactly i, and $f_i(x)$ is the product of the irreducible polynomials dividing $f(x)$ with degree greater than i.

Since $\Delta \neq 0$, $f(x)$ is squarefree, and since $f(x)$ is equal to the product of its irreducible factors, $f(x) = \prod_{1 \le i \le d} F_i(x)$, so $f_d(x) = f(x)/(\prod_{1 \le i \le d} F_i(x)) = 1$.

2) In fact, for any nonzero polynomial $g(x) \in \mathbb{F}_p[x]$, we have $g(x)|g(x^p)$ since $g(x^p) = g(x)^p$.

3) The degree of $F_i(x)$ is i times the number of irreducible factors of f of degree i. So S is equal to the number of irreducible factors of f of even degree.

If $f(x)$ is irreducible mod p, then $d = \deg(f)$ is the least power with $\alpha^{p^d} = \alpha$, and the map $\alpha \mapsto \alpha^p$ has order equal to d. Thus, that map is a generator of the Galois group of f over $\mathbb{F}_p$.

For all polynomials, the Galois group acts transitively on the roots of each irreducible factor of f over $\mathbb{F}_p$. Thus, S gives the number of cycles of even length in the Frobenius automorphism. Cycles of even length are odd (and vice versa), so the parity of S determines whether the automorphism is odd or even. Since the discriminant is the product of the square of the differences of the roots of $f(x)$, this parity is also determined by $\left(\frac{\Delta}{p}\right)$. For a more detailed proof of this fact, see [15].

As an example, let $f(x) = x^4 + 12x + 1$. (It is irreducible over $\mathbb{Q}$.) Let $p = 89$. We have $x^{89} - x \equiv 59x^3 + 51x^2 + 20x + 86 \bmod (89, f(x))$, so

$$F_1(x) = \gcd(f(x), 59x^3 + 51x^2 + 20x + 86) = x + 78,$$

and $f_1(x) = x^3 + 11x^2 + 32x + 8$.

Since $x^{89^2} - x \equiv 64x^2 + 86x + 19 \bmod (89, f_1(x))$, and

$$F_2(x) = \gcd(f_1(x), 64x^2 + 86x + 19) = 1,$$

we have $f_2(x) = f_1(x) = x^3 + 11x^2 + 32x + 8$.

Next, $x^{89^3} - x \equiv 0 \bmod (89, f_2(x))$, so $F_3(x) = f_2(x)$ and $f_3(x) = 1$.

Thus $F_4(x) = f_4(x) = 1$.

Note that $x^{89} \equiv 25x^2+x+59 \bmod (89, F_3(x))$. We verify that $F_3(25x^2+x+59) \equiv 0 \bmod (89, F_3(x))$.

Finally, the discriminant of $f(x)$ is -559616. $\left(\frac{-559616}{89}\right) = 1$, which agrees with the fact that $S = 0$.

We would like to define any composite with satisfies the consequences of this theorem to be a type of pseudoprime, but we may run into a problem when we take the gcd of two polynomials modulo a composite, since we are working over a ring that is not a domain.

With this in mind, we consider the following definition.

Definition. *Let $f(x), g_1(x), g_2(x)$ be monic polynomials over a commutative ring (with identity). We say that polynomial $f(x)$ is the* **greatest common monic divisor (gcmd)** *of $g_1(x)$ and $g_2(x)$ if the ideal generated by $g_1(x)$ and $g_2(x)$ is equal to the ideal generated by $f(x)$. We write $f(x) = \operatorname{gcmd}(g_1(x), g_2(x))$. (Note that $\operatorname{gcmd}(g_1(x), g_2(x))$ does not necessarily exist.)*

Clearly if $\operatorname{gcmd}(g_1(x), g_2(x))$ exists, it is a common monic divisor of $g_1(x)$ and $g_2(x)$ of greatest degree. Further, it is not hard to show that the gcmd is unique. The gcmd has the following additional property.

Proposition 3.2. *Let $p|n$ and $g_1(x), g_2(x)$ be monic polynomials in $\mathbb{Z}[x]$. If $f(x) = \operatorname{gcmd}(g_1(x), g_2(x))$ in $(\mathbb{Z}/n\mathbb{Z}[x])$, then $f(x) \equiv \gcd(g_1(x), g_2(x)) \bmod p$, where the* gcd *is taken in $(\mathbb{Z}/p\mathbb{Z})[x]$.*

Proof. For $i = 1, 2$, we have that $g_i(x) \equiv k_i(x)f(x) \bmod n$, for some $k_i(x) \in \mathbb{Z}[x]$. Thus $f(x)|g_i(x)$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.

We have that $f(x) \equiv g_1(x)h_1(x) + g_2(x)h_2(x) \bmod n$ for some $h_1(x), h_2(x) \in \mathbb{Z}[x]$. Thus $f(x) \equiv g_1(x)h_1(x) + g_2(x)h_2(x) \bmod p$, and by the definition of gcd, $f(x) = \gcd(g_1(x), g_2(x))$ in $(\mathbb{Z}/p\mathbb{Z})[x]$.

Corollary 3.3. *If $\operatorname{gcmd}(g_1(x), g_2(x))$ exists in $(\mathbb{Z}/n\mathbb{Z})[x]$, then for all p dividing n, $\gcd(g_1(x), g_2(x))$ has the same degree.*

Proof. Since the leading coefficient of the gcmd is 1, that coefficient is the leading coefficient of all the gcds, by Proposition 3.2. Thus, they all have the same degree.

Proposition 3.4. *Assume, for each $p|n$, $\gcd(f(x), g(x)) = 1$ in $\mathbb{F}_p[x]$. Then $\operatorname{gcmd}(f(x), g(x)) = 1$ in $(\mathbb{Z}/n\mathbb{Z})[x]$.*

Proof. By the Chinese Remainder Theorem, it suffices to prove that the gcmd of $f(x)$ and $g(x)$ is 1 in $(\mathbb{Z}/p^j\mathbb{Z})[x]$ for any integer $j \geq 1$. We proceed by induction. We know that there exist polynomials $a_1(x)$, $b_1(x)$, and $k_1(x)$ such that $f(x)a_1(x)+g(x)b_1(x) = 1+pk_1(x)$. Assume that there exist polynomials $a_j(x)$, $b_j(x)$ and $k_j(x)$ with $f(x)a_j(x)+g(x)b_j(x) = 1+p^jk_j(x)$. Multiplying by $pk_1(x)$, $pf(x)a_j(x)k_1(x)+pg(x)b_j(x)k_1(x) = pk_1(x) + p^{j+1}k_1(x)k_j(x)$.

Substituting for $pk_1(x)$, $pf(x)a_j(x)k_1(x) + pg(x)b_j(x)k_1(x) = -1 + f(x)a_1(x) + g(x)b_2(x) + p^{j+1}k_1(x)k_j(x)$. Rearranging, $f(x)[a_1(x) - pa_j(x)k_1(x)] + g(x)[b_1(x) - pb_j(x)k_1(x)] = 1 + p^{j+1}[-k_1(x)k_j(x)]$.

Thus we have shown that $\operatorname{gcmd}(f(x), g(x)) = 1$ in $(\mathbb{Z}/p^{j+1}\mathbb{Z})[x]$, and the Proposition is proven.

The concept of gcmd would not be useful in the context of this paper if it were difficult to calculate. We have the following result, which aids us in testing primality.

Proposition 3.5. *The Euclidean algorithm will either find the* gcmd *of two monic polynomials in $(\mathbb{Z}/n\mathbb{Z})[x]$ or find a proper factor of n.*

Proof. The Euclidean algorithm will only fail to finish if one of the divisions fails due to the leading coefficient of a non-zero remainder being non-invertible. This coefficient will have a gcd with n that is a nontrivial factor of n.

If the Euclidean algorithm terminates (i.e., one of the remainders is zero), we have inductively that the last non-zero remainder is a divisor of the two polynomials and can be written as a linear combination of the two. The proof is the same as the proof of correctness of the Euclidean algorithm over $\mathbb{F}_p[x]$. Since the leading coefficient of the last non-zero remainder is invertible, this remainder can be made monic by division, and we find the gcmd.

Definition. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree d with discriminant Δ. An odd integer $n > 1$ is said to pass the* **Frobenius probable prime test** *with respect to $f(x)$ if $(n, f(0)\Delta) = 1$, and it is declared to be a probable prime by the following algorithm. (Such an integer will be called a* **Frobenius probable prime** *with respect to $f(x)$.) All computations are done in $(\mathbb{Z}/n\mathbb{Z})[x]$.*

Factorization Step *Let $f_0(x) = f(x) \bmod n$. For $1 \le i \le d$, let $F_i(x) = \operatorname{gcmd}(x^{n^i} - x, f_{i-1}(x))$ and $f_i(x) = f_{i-1}(x)/F_i(x)$. If any of the* gcmd*s fail to exist, declare n to be composite and stop. If $f_d(x) \ne 1$, declare n to be composite and stop.*

Frobenius Step *For $2 \le i \le d$, compute $F_i(x^n) \bmod F_i(x)$. If it is nonzero for some i, declare n to be composite and stop.*

Jacobi Step *Let $S = \sum_{2|i} \deg(F_i(x))/i$.*

If $(-1)^S \ne \left(\frac{\Delta}{n}\right)$, declare n to be composite and stop.

If n is not declared to be composite by one of these three steps, declare n to be a Frobenius probable prime and stop.

The Factorization Step produces a "distinct degree" factorization when n is prime. It may be of some interest to apply algorithms that factor the polynomials completely, thus developing definitions for Berlekamp and Cantor-Zassenhaus probable primes. The Cantor-Zassenhaus algorithm shares ideas with the "strong" Frobenius probable prime test of Section 5. Berlekamp's algorithm has two forms; one deterministic and one probabilistic. The deterministic version has running time proportional to n, so it is too slow to be used in primality testing. The probabilistic version is fast, but since it is significantly more complicated than most existing probable prime tests, we omit consideration of it here.

Corollary 3.6. *Every odd prime p is a Frobenius probable prime with respect to any monic polynomial $f(x)$ such that p does not divide $f(0)\Delta$.*

Proof. Immediate from Theorem 3.1.

Definition. *Let $f(x) \in \mathbb{Z}[x]$. A* **Frobenius pseudoprime** *with respect to a monic polynomial $f(x)$ is a composite which is a Frobenius probable prime with respect to $f(x)$.*

§4 The Relation of Frobenius Pseudoprimes to Other Pseudoprimes

Theorem 4.1. *An odd integer n is a pseudoprime to the base a if and only if it is a Frobenius pseudoprime with respect to the polynomial $f(x) = x - a$.*

Proof. First, assume n is an pseudoprime to the base a. Thus, $a^{n-1} \equiv 1 \bmod n$. Since $\Delta = 1$, $(n, f(0)\Delta) = (n, a) = 1$. Because $(x-a)|(x^n - a^n)$ and $a^n - a = 0$ in $(\mathbb{Z}/n\mathbb{Z})[x]$, we have $(x-a)|((x^n - a^n) + (a^n - a) + (a - x))$ or $(x-a)|(x^n - x)$. Therefore, $F_1(x) = x - a$, and $f_1(x) = 1$, so n passes the Factorization Step. Since $d = 1$, The Frobenius Step is vacuous. Note that $S = 0$ and $\left(\frac{\Delta}{n}\right) = \left(\frac{1}{n}\right) = 1$, so n passes the Jacobi Step. Therefore n is a Frobenius pseudoprime.

Now, assume n is a Frobenius pseudoprime with respect to $x - a$. In order to have $f_1(x) = 1$, we must have $F_1(x) = x - a$. So by the Factorization Step,

$(x-a)|(x^n-x)$. Since $(x-a)|(x^n-a^n)$, $(x-a)$ divides a^n-a. Since the latter is a constant and $x-a$ is monic, a^n-a must be 0 in $(\mathbb{Z}/n\mathbb{Z})[x]$. So $a^n \equiv a \bmod n$. Since $(n, f(0)\Delta) = (n,a) = 1$, we have $a^{n-1} \equiv 1 \bmod n$. Thus n is a pseudoprime to the base a.

In fact, a more general result can be proven: a Frobenius pseudoprime with respect to $f(x)$ is a pseudoprime to the base $f(0)$. The idea for the proof can be found in [13], Corollary 1. We first need to prove a lemma about polynomials mod p^k.

Lemma 4.2. *Let $g(y)$ be a polynomial in $\mathbb{Z}[y]$, irreducible mod p. Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ with $p \nmid \operatorname{disc}(f)$. If $f(x)$ has d roots in $(\mathbb{Z}[y]/(p, g(y)))[x]$, then it has d roots in $(\mathbb{Z}[y]/(p^k, g(y)))[x]$ for k a positive integer.*

Proof. By Hensel's Lemma, a root mod p lifts to exactly one root mod p^k, since the discriminant of f is non-zero mod p. Hensel's Lemma applies to any finite field of characteristic p.

Theorem 4.3. *Let $f(x)$ be a monic, squarefree polynomial in $\mathbb{Z}[x]$. If an odd integer n is a Frobenius pseudoprime with respect to $f(x)$, then it is a pseudoprime to the base $f(0)$.*

Proof. It suffices to prove $f(0)^n \equiv f(0) \bmod p^k$ for every prime power $p^k|n$.

Let d be the degree of $f(x)$. There exists an extension field of $\mathbb{F}_p$, $\mathbb{F}_p[y]/(g(y))$, in which $f(x)$ splits completely. The d roots must be distinct, since n is coprime to the discriminant of $f(x)$. Thus there are d distinct roots of $f(x)$ in $\mathbb{Z}[y]/(p^k, g(y))$, by Lemma 4.2.

Call the roots $y_1, y_2, \ldots, y_d$. Consider the map $y_i \mapsto y_i^n$. By the Frobenius Step, this map sends each root to another root. By the Factorization Step, $(y_i^n)^{n^{d-1}} = y_i$, so the map is invertible. Therefore, it permutes the roots. Thus $\prod_{i=1}^d y_i = \prod_{i=1}^d y_i^n$. But $\prod_{i=1}^d y_i \equiv (-1)^d f(0) \bmod p$, so $(-1)^d f(0) \equiv ((-1)^d f(0))^n \bmod p^k$. Simplifying, we see that $f(0)^n \equiv f(0) \bmod p^k$ for each $p^k|n$. Thus n is a pseudoprime to the base $f(0)$.

Theorem 4.3 can be used, in conjunction with results about the distribution of pseudoprimes base a, to give an upper bound on the number of Frobenius pseudoprimes with respect to a given polynomial $f(x)$.

Corollary 4.4. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial with nonzero discriminant. If $|f(0)| \neq 1$, then the number of Frobenius pseudoprimes with respect to $f(x)$ up to y is less than $y^{1-\log\log\log y/2\log\log y}$, for y sufficiently large, where "sufficiently large" depends only on $|f(0)|$.*

Proof. Immediate from Theorem 4.3 and [21].

When $|f(0)| = 1$, it is possible that all integers are Frobenius pseudoprimes with respect to $f(x)$, such as if $f(x) = x-1$. In fact, we conjecture that for every monic, squarefree polynomial $f(x)$, not the product of cyclotomic polynomials, the bound of Corollary 4.4 holds. For quadratic polynomials, the conjecture follows from [9].

Theorem 4.5. *If a, b are integers, $f(x) = (x-a)(x-b)$, and n is a Frobenius pseudoprime with respect to $f(x)$, then n is a pseudoprime to both bases a and b.*

Proof. Since $f(x)$ factors, its discriminant must be a square, so $\left(\frac{\Delta}{n}\right) = 1$. Therefore $F_2(x) = 1$ and $F_1(x) = f(x)$ by the Jacobi Step. Since $f(x)|(x^n - x)$, we have

$(x-a)|(x^n-x)$. Therefore, as in the proof of Theorem 4.1, we conclude n is a pseudoprime to the base a and, similarly, base b.

Theorem 4.6. *If $f(x), g(x) \in \mathbb{Z}[x]$ with $(n, \operatorname{disc}(fg)) = 1$ and n is a Frobenius pseudoprime with respect to $f(x)$ and $g(x)$, then it is a Frobenius pseudoprime with respect to $f(x)g(x)$.*

Proof. Let $h(x) = f(x)g(x)$. Let $f_i(x), g_i(x), h_i(x)$ and $F_i(x), G_i(x), H_i(x)$ be the polynomials produced in the Factorization Steps for $f(x), g(x), h(x)$, respectively. If a polynomial is not defined in that step (e.g., $f_{d+1}(x)$, if $f(x)$ has degree d), define it to be 1.

We will show by induction on i that $h_i(x) = f_i(x)g_i(x)$ and $H_i(x) = F_i(x)G_i(x)$.

We have that $h_0(x) = h(x) = f(x)g(x) = f_0(x)g_0(x)$. Assume that $h_{k-1}(x) = f_{k-1}(x)g_{k-1}(x)$. By definition, we have $H_k(x) = \operatorname{gcmd}(x^{n^k} - x, h_{k-1}(x))$, should this gcmd exist. Since $F_k(x)|f_{k-1}(x)$, $G_k(x)|g_{k-1}(x)$, $F_k(x)G_k(x)|h_{k-1}(x)$.

Because $\gcd(\operatorname{disc}(fg), n) = 1$, we have that $\gcd(F_k(x), G_k(x)) = 1$ in $\mathbb{F}_p[x]$ for each $p|n$. By Proposition 3.4, $\operatorname{gcmd}(F_k(x), G_k(x)) = 1$ in $(\mathbb{Z}/n\mathbb{Z})[x]$. Therefore $F_k(x)A_1(x) + G_k(x)A_2(x) \equiv 1 \bmod n$ for some $A_1(x)$ and $A_2(x)$ in $\mathbb{Z}[x]$. Also, $x^{n^k} - x \equiv B_1(x)F_k(x) \equiv B_2(x)G_k(x)$, for some $B_1(x)$ and $B_2(x)$ in $\mathbb{Z}[x]$, by the definitions of $F_k(x)$ and $G_k(x)$. Thus $F_k(x)B_1(x) \equiv G_k(x)B_2(x) \bmod n$. Multiplying by $A_1(x)$ gives $F_k(x)A_1(x)B_1(x) \equiv G_k(x)A_1(x)B_2(x)$. If we substitute for $F_k(x)A_1(x)$, we get $(1 - G_k(x)A_2(x))B_1(x) \equiv G_k(x)A_1(x)B_2(x)$, or $B_1(x) \equiv G_k(x)[A_2(x)B_1(x) + A_1(x)B_2(x)]$. Hence $G_k(x)|B_1(x)$, and $F_k(x)G_k(x)|x^{n^k} - x$. Thus $F_k(x)G_k(x)|H_k(x)$.

We have, by the definitions of $F_k(x)$ and $G_k(x)$, that $F_k(x) \equiv r_1(x)(x^{n^k} - x) + s_1(x)f_{k-1}(x)$ and $G_k(x) \equiv r_2(x)(x^{n^k} - x) + s_2(x)g_{k-1}(x)$, for some polynomials $r_1(x)$, $r_2(x)$, $s_1(x)$, and $s_2(x)$. Multiplying these two congruences together, $F_k(x)G_k(x) \equiv r_3(x)(x^{n^k} - x) + s_1(x)s_2(x)h_{k-1}(x)$, where $r_3(x) = r_1(x)r_2(x)(x^{n^k} - x) + r_1(x)s_2(x)g_{k-1}(x) + r_2(x)s_1(x)f_{k-1}(x)$. Therefore, $H_k(x) = F_k(x)G_k(x)$. Now $h_k(x) = h_{k-1}(x)/H_{k-1}(x)$, so by the inductive hypothesis,

$$h_k(x) = f_{k-1}(x)g_{k-1}(x)/(F_{k-1}(x)G_{k-1}(x)) = f_k(x)g_k(x).$$

Each of the gcmds in the Factorization Step exists, and $h_{\deg(fg)}(x) = 1$. Thus n passes the Factorization Step.

Since $H_i(x) = F_i(x)G_i(x)$, and n passes the Frobenius Step for $f(x)$ and $g(x)$, $H_i(x)|H_i(x^n)$. Thus n passes the Frobenius Step for $h(x)$.

Let S_f and S_g be the values of S computed in the Jacobi Step for $f(x)$ and $g(x)$, respectively. Then $S = S_f + S_g$. So it suffices to show that $\left(\frac{\operatorname{disc}(fg)}{n}\right) = \left(\frac{\operatorname{disc}(f)}{n}\right)\left(\frac{\operatorname{disc}(g)}{n}\right)$. To show this equality, it suffices to show that $\operatorname{disc}(fg) = \operatorname{disc}(f)\operatorname{disc}(g)\ell^2$, where $\ell \in \mathbb{Z}$.

Let $\alpha_1, \ldots, \alpha_j$ be the roots of $f(x)$ and $\alpha_{j+1}, \ldots, \alpha_d$ be the roots of $g(x)$, all in $\bar{\mathbb{Q}}$. Then $\operatorname{disc}(fg) = \prod_{i<i'}(\alpha_i - \alpha_{i'})^2 = \operatorname{disc}(f)\operatorname{disc}(g)\prod_{i\le j<i'}(\alpha_i - \alpha_{i'})^2$. Let $\ell = \prod_{i\le j<i'}(\alpha_i - \alpha_{i'})$.

We will show that $\ell \in \mathbb{Z}$, by showing $\sigma(\ell) = \ell$ for all $\sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Any such σ must map each α_i with $i \le j$ to some $\alpha_{\bar{i}}$ with $\bar{i} \le j$, and similarly for $i > j$. Thus σ must only rearrange terms in the product, and $\sigma(\ell) = \ell$. Thus

$\left(\frac{\operatorname{disc}(fg)}{n}\right) = \left(\frac{\operatorname{disc}(f)}{n}\right)\left(\frac{\operatorname{disc}(g)}{n}\right)$, n passes the Jacobi Step, and n is a Frobenius pseudoprime with respect to $f(x)g(x)$.

The converse to Theorem 4.6 is true for the product of two linear polynomials, as Theorems 4.1 and 4.5 show. It is not, however, true in general. If $f(x) = (x-1341)(x-513)(x-545)$, then 1537 is a Frobenius pseudoprime with respect to $f(x)$, but it is not a pseudoprime to any of the bases 1341, 513, or 545. This example appears in [2] and indicates the possible usefulness of the quadratic forms test contained therein. The examples produced in that paper, however, all involve polynomials with relatively large discriminant compared to the pseudoprimes.

Corollary 4.7. *If n is a Carmichael number, $f(x) \in \mathbb{Z}[x]$ is monic, $f(x)$ factors into linear factors mod n and $(n, f(0)\Delta) = 1$, then n is a Frobenius pseudoprime with respect to $f(x)$.*

Proof. Apply Theorem 4.1 and Theorem 4.6.

Lemma 4.8. *Let m, n be positive integers, and let $f(x), g(x), r(x) \in \mathbb{Z}[x]$. If $f(r(x)) \equiv 0 \bmod (n, f(x))$ and $x^m \equiv g(x) \bmod (n, f(x))$, then $r(x)^m \equiv g(r(x)) \bmod (n, f(x))$.*

Proof. $x^m \equiv g(x) + f(x)h(x) \bmod n$, for some $h(x) \in \mathbb{Z}[x]$. Since x is an indeterminate, $r(x)^m \equiv g(r(x)) + f(r(x))h(r(x)) \bmod n$. Because $f(r(x)) \equiv 0 \bmod (n, f(x))$, $r(x)^m \equiv g(r(x)) \bmod (n, f(x))$.

Theorem 4.9. *If $f(x) = x^2 - Px + Q \in \mathbb{Z}[x]$, and n is a Frobenius pseudoprime with respect to $f(x)$, then n is a Lucas pseudoprime with parameters (P, Q).*

Proof. Note that $S = 0$ or 1.

If $\left(\frac{\Delta}{n}\right) = 1$, then we must have $S = 0$, so $x^n \equiv x \bmod (n, f(x))$. Since Q is invertible mod n, x is invertible mod $(n, f(x))$. Thus $x^{n-1} \equiv 1$. By Lemma 4.8, $(P-x)^{n-1} \equiv 1$, since $f(P-x) \equiv 0 \bmod (n, f(x))$.

The two roots of $f(x)$ in $\mathbb{Z}[x]/(f(x))$ are x and $P - x$, and $(x-(P-x))^2 \equiv P^2 - 4Q \bmod f(x)$. Since n is coprime to the discriminant $P^2 - 4Q$, the difference of the two roots is invertible. Thus $U_{n-1} \equiv \frac{x^{n-1}-(P-x)^{n-1}}{x-(P-x)} \equiv \frac{1-1}{2x-P} = 0 \bmod (n, f(x))$.

If $\left(\frac{\Delta}{n}\right) = -1$, then we must have $S = 1$, so $x^n \not\equiv x \bmod (n, f(x))$. We cannot have $x^n \equiv x \bmod (p^k, f(x))$ for $p^k | n$, since then $x^n - x \equiv 0 \bmod (p^k, f(x))$, and the gcmd in the Factorization Step would not exist. Because $p \nmid \Delta$, there are only 2 roots to $f(x) \bmod (p^k, f(x))$, by Lemma 4.2. Since they are known to be x and $P - x$, we must have $x^n \equiv P - x \bmod (p^k, f(x))$ for each prime power $p^k | n$, by the Frobenius Step. Since $f(x)$ is monic, the congruence must hold mod $(n, f(x))$ by the Chinese Remainder Theorem. By Lemma 4.8, $(P-x)^n \equiv x \bmod (n, f(x))$, so $U_{n+1} \equiv \frac{x^{n+1}-(P-x)^{n+1}}{2x-P} \equiv \frac{x(P-x)-(P-x)x}{2x-P} = 0$.

Note that the Frobenius test is in fact stronger than the Lucas test. For example, 323 is the first Lucas pseudoprime with respect to the Fibonacci sequence. If we compute $x^{323} - x \bmod (323, x^2 - x - 1)$, we get -1. So $F_1(x) = 1$. If we compute $x^{323^2} - x \bmod (323, x^2-x-1)$, we get 0. So $F_2(x) = x^2 - x - 1$ and $f_2(x) = 1$. So 323 passes the Factorization Step. Note that it also passes the Jacobi Step, since $\left(\frac{5}{323}\right) = -1$. But it fails the Frobenius Step, because $x^{323} \equiv x - 1 \bmod (323, x^2 - x - 1)$, and $F_2(x-1) = -2x + 2$. The first Frobenius pseudoprime with respect to the Fibonacci polynomial $x^2 - x - 1$ is 5777.

Theorem 4.10. *If $f(x) = x^3 - rx^2 + sx - 1$, then any Frobenius pseudoprime n with respect to $f(x)$ is also a Perrin pseudoprime. In particular, if $F_1(x) = f(x)$, then n has an S-signature, if $F_3(x) = f(x)$, then n has an I-signature, and if $\deg(F_1) = 1$ and $\deg(F_2) = 2$, n has a Q-signature.*

Proof. The idea behind this proof is that relationships between nth powers of the roots determine the signature, and the necessary relationships are guaranteed to hold because n passes the Frobenius Probable Prime Test.

To this end, we use Lemma 2 of [2]. Let K be the splitting field of $f(x)$. Let α_1, α_2 and α_3 be the three roots of $f(x)$ in K. Lemma 2 says that n has a Q- signature if for each prime power $p^k | n$, and for each prime ideal $\mathfrak{p}$ of K with $\mathfrak{p}|p$, $\alpha_1^n \equiv \alpha_1$, $\alpha_2^n \equiv \alpha_3$, and $\alpha_3^n \equiv \alpha_2 \bmod \mathfrak{p}^k$ (or some other permutation of the roots of order 2.)

If $\deg(F_1) = 1$ and $\deg(F_2) = 2$, then we must have $f(x) \equiv F_1(x)F_2(x) \bmod p^k$. So $f(\alpha) = 0 \equiv F_1(\alpha)F_2(\alpha)$. Because the discriminant of $f(x)$ is not divisible by p, we know that $F_1(x)$ has exactly one root mod p^k, by Lemma 4.2. Therefore, one of the roots (say α_1) is a root of $F_1(x)$ and the other two are roots of $F_2(x)$.

For α_1, we have $x^n \equiv x \bmod (p^k, F_1(x))$. But we must have $F_1(x) \equiv x - \alpha_1 \bmod p^k$, so $\alpha_1^n \equiv \alpha_1 \bmod p^k$, and hence for every prime ideal power dividing p^k.

We have $x^n \not\equiv x \bmod (p^k, F_2(x))$, but $F_2(x^n) \equiv 0$. Since there are only two roots of $F_2(x)$, we must have $\alpha_2^n \equiv \alpha_3 \bmod p^k$, and similarly $\alpha_3^n \equiv \alpha_2$.

The proofs of the S and I cases are similar.

Theorem 4.11. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, squarefree polynomial. Let $\beta_1, \ldots, \beta_d$ be its roots, and let $V_k = \beta_1^k + \cdots + \beta_d^k$. If n is a Frobenius pseudoprime with respect to $f(x)$, then n is a pseudoprime with respect to V, in the sense of* [13], *Section 4.*

Proof. The theorem follows directly from Theorem 2 of [13].

Theorem 4.12. *Let $f(x)$ be a monic, squarefree polynomial. If n is a Frobenius pseudoprime with respect to $f(x)$, then n is a pseudoprime in the sense of Szekeres.*

Proof. It suffices to show that the map $x \mapsto x^n$ permutes the roots of $f(x)$. This fact follows from the Frobenius Step.

Having presented the definition of Frobenius pseudoprime as a generalization of other definitions of pseudoprime, we would like to use the above theorems to produce a theorem that holds for all of these types of pseudoprimes.

Conjecture 4.13. *For any monic, squarefree polynomial $f(x) \in \mathbb{Z}[x]$, there are infinitely many Frobenius pseudoprimes with respect to $f(x)$. In fact, for any $\epsilon > 0$, there exists a T (depending on $f(x)$ and ϵ) such that if $t > T$, there are at least $t^{1-\epsilon}$ Frobenius pseudoprimes less than t.*

It is straightforward to prove the first assertion for many polynomials (those which split into linear and quadratic factors over $\mathbb{Z}$). The proof uses Corollary 4.7 and an extension of results in [3] and [4]. It is possible to prove this statement for all polynomials, but the proof requires results about L-functions over number fields. The proof is given in [12]. The second assertion seems considerably more difficult to prove; for a discussion of impediments, see [3].

§5 Strong Frobenius Pseudoprimes

We can strengthen the test developed in the previous section by using the identity $x^{n^i-1} - 1 = (x^s - 1)\prod_{j=1}^{r}(x^{2^{j-1}s} + 1)$ (where $n^i - 1 = 2^r s$) to further factor $F_i(x)$.

Theorem 5.1. *Let $f(x)$, d, Δ, p, and $F_i(x)$ be as in Theorem 3.1. Let $p^i - 1 = 2^r s$ with s odd. Let $F_{i,0}(x) = \gcd(F_i(x), x^s - 1)$. For $1 \le j \le r$, let $F_{i,j}(x) = \gcd(F_i(x), x^{2^{j-1}s} + 1)$. Then $\prod_{j=0}^{r} F_{i,j}(x) = F_i(x)$ and for each j, the degree of $F_{i,j}(x)$ is divisible by i.*

Proof. We have the identity $x^{p^i-1} - 1 = (x^s - 1)\prod_{j=1}^{r}(x^{2^{j-1}s} + 1)$. The result follows since the factors in the product are pairwise coprime, and since $f(0) \neq 0$.

Definition. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree d with discriminant Δ. An odd integer n with $(n, f(0)\Delta) = 1$ is said to pass the* **strong Frobenius probable prime test** *with respect to $f(x)$ if it is a Frobenius probable prime and is declared to be a probable prime by the following additional step. (Such an integer will be called a* **strong Frobenius probable prime** *with respect to $f(x)$.)*

Square Root Step *For each $1 \le i \le d$, let $n^i - 1 = 2^r s$ with r odd. Let $F_{i,0}(x) = \mathrm{gcmd}(F_i(x), x^s - 1)$. Let $F_{i,j}(x) = \mathrm{gcmd}(F_i(x), x^{2^{j-1}s} + 1)$. Then if $F_i(x) \neq \prod_{j=0}^{r} F_{i,j}(x)$, if for some j, the degree of $F_{i,j}(x)$ is not a multiple of i, or if one of the* gcmd*s fails to exist, declare n to be composite and terminate.*

If n is not declared to be composite by the Frobenius probable prime test or the Square Root Step, declare n to be a strong Frobenius probable prime.

Corollary 5.2. *Every odd prime p is a strong Frobenius probable prime with respect to any monic polynomial $f(x)$ such that p does not divide $f(0)\Delta$.*

Definition. *A* **strong Frobenius pseudoprime** *with respect to a monic polynomial $f(x) \in \mathbb{Z}[x]$ is a composite strong Frobenius probable prime with respect to $f(x)$.*

Clearly every strong Frobenius pseudoprime with respect to $f(x)$ is a Frobenius pseudoprime with respect to $f(x)$.

Theorem 5.3. *A number n with $(n, 2a) = 1$ is a strong Frobenius pseudoprime with respect to $x - a$ if and only if n is a strong pseudoprime to the base a.*

Proof. From Theorem 3.1 it suffices to show that a pseudoprime to the base a is strong if and only if it passes the Square Root Step with respect to $x - a$.

In order to pass the Square Root Step, we need to have $x - a | x^{2^{r-j}s} + 1$ for some $1 \le j \le r$ or $x - a | x^s - 1$. The first statement is equivalent to $a^{2^{r-j}s} \equiv -1 \bmod n$ and the second is equivalent to $a^s \equiv 1 \bmod n$. These are exactly the conditions for strong pseudoprimality. So n passes the Square Root Step if and only if it is a strong pseudoprime to the base a.

Corollary 5.4. *Every strong Frobenius pseudoprime with respect to $x - a$ is an Euler pseudoprime to the base a.*

The situation with strong Lucas pseudoprimes is a bit more complicated, as the polynomial needs to be changed.

Theorem 5.5. *Let $f(x) = x^2 - Px + Q$. Let n be a integer with $(n, 2\Delta Q) = 1$. Let Q' be an integer with $Q' \equiv Q^{-1} \bmod n$. If n is a strong Frobenius pseudoprime with respect to $X^2 + (2 + b^2c')X + 1$, then n is a strong Lucas pseudoprime with parameters (P, Q).*

Proof. Let $U_k = U_k(P, Q)$ and $V_k = V_k(P, Q)$. Note that $U_k \equiv 0 \bmod n$ if and only if $x^k - (P - x)^k \equiv 0 \bmod (n, x^2 - Px + Q)$ if and only if $\left(\frac{P-x}{x}\right)^k \equiv 1$. Similarly,

$V_k \equiv 0$ if and only if $\left(\frac{P-x}{x}\right)^k \equiv -1$. Let $X = -Q'Px + Q'P^2 - 1$. Then $X \equiv (P-x)/x \bmod (n, x^2 - Px + Q)$ and $X^2 + (2 - P^2Q')X + 1 = (PQ')^2(x^2 - Px + Q)$. So, by a change of variables, we see that $U_k \equiv 0 \bmod n$ if and only if $X^k \equiv 1 \bmod (n, X^2 + (2 - P^2Q')X + 1)$. The same statement holds for V_k, with 1 replaced by -1. So $U_k \equiv 0 \bmod n$ if and only if $X^2 + (2 - P^2Q')X + 1$ divides $X^k - 1$. Using this statement, the fact that n is a strong Lucas pseudoprime with parameters (P, Q) follows immediately from the Square Root Step.

If we insist on keeping the same polynomial, a weaker result can be proven.

Theorem 5.6. *Every strong Frobenius pseudoprime n with respect to $f(x) = x^2 - Px + Q$ such that $\left(\frac{P^2-4Q}{n}\right) = -1$ is a strong Lucas pseudoprime with parameters (P, Q).*

Proof. Let $U_k = U_k(P, Q)$ and $V_k = V_k(P, Q)$. Write $n + 1 = 2^R S$ and $n^2 - 1 = 2^r s$ with s and S odd. Note that $2^r s = (n-1)2^R S$, so $R < r$ and $S|s$.

Observe that the only ways to pass the Square Root Step are if $f(x)|x^s - 1$ or $f(x)|x^{2^{r-j}s} + 1$ for some j such that $r \geq j > 0$.

This means that either $f(x)|x^{2^{r-R}s} - 1$ or $f(x)|x^{2^{r-j}s} + 1$ for some j such that $R \geq j > 0$.

In the first case, we observe $2^{r-R}s = (n-1)S = nS - S$. So $x^{nS-S} \equiv 1 \bmod (n, f(x))$, or $x^{nS} \equiv x^S$. But we know that $x^n \equiv (P - x)$, so $(P-x)^S \equiv x^S$. Thus $U_S \equiv (x^S - (P-x)^S)/(x - (P-x)) \equiv 0 \bmod (n, f(x))$ and thus mod n.

In the second case, we use the formula $2^{r-j}s = (n-1)2^{R-j}S = n2^{R-j}S - 2^{R-j}S$. But $x^{2^{r-j}s} \equiv -1 \bmod (n, f(x))$, so $x^{2^{R-j}S} \equiv -x^{n2^{R-j}S}$. This gives us that $x^{2^{R-j}S} \equiv -(P-x)^{2^{R-j}S}$.

Since $V_m \equiv x^m + (P-x)^m$, $V_{2^{R-j}S} \equiv 0 \bmod n$. We conclude that n is a strong Lucas pseudoprime.

Theorem 5.6 would not be true without the restriction that $\left(\frac{b^2+4c}{n}\right) = -1$. For example, 294409 is a strong Frobenius pseudoprime with respect to $x^2 - 1185x + 56437$, but it is not a strong Lucas pseudoprime with parameters $(1185, 56437)$.

Theorem 5.7. *If n is a strong Frobenius pseudoprime with respect to $x^2 - bx + 1$, then n is an extra strong Lucas pseudoprime to the base b.*

Proof. Let $U_k = U_k(b, 1)$ and $V_k = V_k(b, 1)$. Assume that $\left(\frac{b^2+4}{n}\right) = -1$. Let R, r, S, s be as in the proof of Theorem 5.6. Observe that $x^{n+1} \equiv x(b-x) \equiv 1$.

If $f(x)|x^{2^{r-j}s} + 1$ for some j such that $r \geq j > 0$, then we have that $V_{2^{R-j}s} \equiv 0$, as in Theorem 5.6.

If $V_{2^{r-1}s} \equiv 0$, we have that $V_{\frac{n+1}{2}} \equiv 0$, so $x^{\frac{n+1}{2}} + (b-x)^{\frac{n+1}{2}} \equiv 0$. Since $(b-x) \equiv x^{-1}$, we deduce $x^{n+1} \equiv -1$, a contradiction. This establishes that $j > 1$, as the definition of extra strong Lucas pseudoprime requires.

If $f(x)|x^s - 1$, this means that $x^s \equiv 1 \bmod (n, f(x))$. $s = S(n-1)/2^{r-R}$. So $\gcd(\frac{s}{S}, n+1) = 1$. Therefore $x^S \equiv 1$, and $V_S \equiv x^S + (b-x)^S \equiv 1 + 1 = 2$, and $U_S \equiv 0$ as above.

Similarly, if $f(x)|x^s + 1$, we have $V_S \equiv -2$ and $U_S \equiv 0$.

The only remaining case is $f(x)|x^{2^{r-j}s} + 1$ for some j such that $r > j \geq R + 1$. $r > R + 1$ only if $n \equiv 1 \bmod 4$. Then $R = 1$, and $j \leq r - 1$. So $2^{r-j}s = (n+1)\frac{n-1}{2^j}$, and $x^{2^{r-j}s} \equiv x^{(n+1)\frac{n-1}{2^j}} \equiv 1$. This contradicts the assumption that $f(x)|x^{2^{r-j}s} + 1$.

The proof for the case where the Jacobi symbol is 1 is similar.

§6 Carmichael-Frobenius Numbers

A Carmichael number is to be a number which is a (Fermat) pseudoprime to every base. With that in mind, we make the following definition.

Definition. *Let K be a number field and n an odd composite with $(n, \operatorname{disc}(K)) = 1$. If, for each polynomial $f(x) \in \mathbb{Z}[x]$ with all its roots in K and $(n, f(0)\operatorname{disc}(f)) = 1$, n is a Frobenius pseudoprime with respect to $f(x)$, then n is a* **Carmichael-Frobenius number** *with respect to K.*

Note that n is a Carmichael number if and only if it is a Carmichael-Frobenius number with respect to $\mathbb{Q}$. Also, if n is a Carmichael-Frobenius number with respect to K, then it is also a Carmichael-Frobenius number with respect to any subfield of K. In particular, a Carmichael-Frobenius number with respect to K is also a Carmichael number.

Proposition 6.1. *Let n be a Carmichael number, and let K be a number field with $(n, \operatorname{disc}(K)) = 1$. If every prime $p|n$ splits completely in K, then n is a Carmichael-Frobenius number with respect to K.*

Proof. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with all of its roots in K such that $\gcd(n, f(0)\operatorname{disc}(f)) = 1$. For each $p|n$, $f(x)$ must split into linear factors mod p, since p splits completely in K. Since n is a Carmichael number, it is squarefree, so $f(x)$ splits into linear factors mod n. The Proposition follows from Corollary 4.7.

These Carmichael-Frobenius numbers have $F_1(x) = f(x)$ in the Factorization Step for each $f(x)$ with all of its roots in K. In [12], we will show that there are infinitely many of them for each number field K. Other types of Carmichael-Frobenius numbers are harder to come by. The methods of [20] can be used to give heuristics suggesting that there are infinitely many Carmichael-Frobenius numbers with respect to K with $F_2(x) = f(x)$ for each irreducible $f(x)$ with all of its roots in K. We also have the following Proposition, which is similar to Proposition 6 of [13].

Proposition 6.2. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree k with splitting field K. Let n be a Carmichael-Frobenius number with respect to K. If $F_k(x) = f(x)$ in the Factorization Step of the Frobenius Probable Prime Test with respect to $f(x)$, then n has at least $k+2$ prime factors.*

Proof. Let p be a prime factor of n, and let $f_p(x)$ be an irreducible factor of $f(x)$ of maximal degree in $\mathbb{F}_p[x]$. Let $A_p = \mathbb{F}_p[x]/(f_p(x))$. We have that $A_p = \mathbb{F}_{p^r}$ for some $r \geq 1$.

We will show that $r = k$. Since x^n is a root of $f(x)$ in $\mathbb{Z}[x]/(n, f(x))$, it is a root in A_p, and we must have $x^n = x^{p^t}$ in A_p, for some $t > 0$. We thus have $x^{n^r} \equiv x^{p^{tr}} \equiv x$ in A_p. Thus $f_p(x)|\gcd(f(x), x^{n^r} - x)$ in $\mathbb{F}_p[x]$. Since all gcmds were computable, $f_p(x)|F_{r'}(x)$, for some $r' \leq r$. But since $F_k(x) = f(x)$, we must have $r' = k$, and thus $r = k$.

Let α be a root of $f(x)$ in K. Then for some $g_p(x) \in \mathbb{Z}[x]$, $g_p(\alpha)$ has order $p^k - 1$ in A_p^*. By the Chinese Remainder Theorem, there is a monic polynomial $g(x) \in \mathbb{Z}[x]$ such that $g(x) \equiv g_p(x) \bmod p$ for each $p|n$. Let $h(x)$ be the minimal polynomial of

$g(\alpha)$ over $\mathbb{Q}$. Then $h(x)$ has all of its roots in K. Since $h(x)$, considered mod p, is the minimal polynomial for $g_p(\alpha)$, we have $p \nmid h(0)\,\mathrm{disc}(h)$ for each $p|n$, and thus $\gcd(n, h(0)\,\mathrm{disc}(h)) = 1$.

Thus $h(x^n) = 0$ in A_p. But the roots of $h(x)$ in A_p are $x^p, x^{p^2}, \ldots, x^{p^{k-1}}, x^{p^k}$. Then $n \equiv p^t \bmod (p^k-1)$, for some $1 \le t \le r$. This congruence gives $p^k-1|n-p^t$, for some $1 \le t \le k$. Therefore, $p^k-1|\frac{n}{p}-p^{t-1}$. Since n is a Carmichael number, it is not a prime power, and $n > p^t$, which implies $\frac{n}{p}-p^{t-1} > 0$. So $p^k-1 \le \frac{n}{p}-p^{t-1} \le \frac{n}{p}-1$; thus $p^k \le \frac{n}{p}$. Since $n \ne p^{k+1}$, $p^k < \frac{n}{p}$. Thus we have for all $p|n$, $p^k < \frac{n}{p}$, or $p^{k+1} < n$. If n has less than or equal to $k+1$ prime factors, we have $n^{k+1} < n^{k+1}$, by taking the product over all prime factors. The contradiction gives the proposition.

§7 Implementation Issues

Performing the Frobenius test as stated on quadratic polynomials would seem to require computing x^{n^2}. As the theorem below shows, there is an equivalent version of the test that merely requires computing x^n.

Theorem 7.1. *Let $f(x) = x^2 - bx - c$. Let $\Delta = b^2 + 4c$. Let n be an integer with $(n, 2f(0)\Delta) = 1$. If $\left(\frac{\Delta}{n}\right) = 1$ and $x^n \equiv x \bmod (n, f(x))$, then n is a Frobenius probable prime with respect to $f(x)$. If $\left(\frac{\Delta}{n}\right) = -1$ and $x^n \equiv b - x \bmod (n, f(x))$, then n is a Frobenius probable prime with respect to $f(x)$.*

Proof. If $\left(\frac{\Delta}{n}\right) = 1$, then the fact that $f(x)$ divides $x^n - x$ verifies both the Factorization Step and the Jacobi Step. The Frobenius Step is trivial.

Suppose $\left(\frac{\Delta}{n}\right) = -1$, and $x^n \equiv b - x \bmod (n, f(x))$. By Lemma 4.8, $(b-x)^n \equiv x \bmod (n, f(x))$, and so $x^{n^2} \equiv x \bmod (n, f(x)))$. Note that $4f(b/2) = -\Delta$ is coprime to n, so $x^n - x \equiv b - 2x$ has gcmd 1 with $f(x)$ in $(\mathbb{Z}/n\mathbb{Z})[x]$. Thus $F_1(x) = 1$ and $F_2(x) = f(x)$, so n passes the Factorization and Jacobi steps. Since $f(b-x) \equiv f(x) \equiv 0 \bmod (n, f(x))$, it passes the Frobenius Step.

We will leave a proof of the running time and an description of how to speed the strong test to [11].

Note that Lemma 4.8 can also be used to speed up the test with any degree polynomial.

Also, when computing $\mathrm{gcmd}(x^n - x, f(x))$, the first step should be to compute $x^n \bmod f(x)$. Then the Euclidean algorithm can be applied to two polynomials whose degree is at most that of $f(x)$.

Although the Square Root Step is listed as a separate step, in practice it would be integrated into the Factorization Step. A description of how to do this in the quadratic case is given in [11].

§8 A Challenge

Pomerance, Selfridge and Wagstaff offer \$620 for a number 2 or 3 mod 5 that is a pseudoprime to the base 2 and also a Lucas pseudoprime with respect to the Fibonacci sequence or a proof that none exists [22, 14].

In this spirit, I have offered \$6.20 for a Frobenius pseudoprime with respect to x^2+5x+5 that is congruent to 2 or 3 mod 5. This polynomial is used instead of the Fibonacci polynomial because $x^{2(p+1)} \equiv 1 \bmod (p, x^2 - x - 1)$, if p is 2 or 3 mod 5. With $x^2 + 5x + 5$, there is no similar guarantee x will have small order mod p.

The lower monetary figure is a reflection of my financial status at the time of the offer, not of any lower confidence level. Heuristics [20] suggest that an example should exist for the PSW test, and these heuristics can be modified to suggest that it should also be possible to find one for the above Frobenius test. I believe that the two problems are equally challenging. A justification for my belief is that an n that passes my challenge must be a pseudoprime to the base 5 (by Theorem 4.3) as well as a Lucas pseudoprime with parameters $(-5, -5)$ (by Theorem 4.9).

References

1. W. W. Adams, *Characterizing pseudoprimes for third-order linear recurrence sequences*, Math. Comp. **48** (1987), 1–15.
2. W. W. Adams and D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), 255–300.
3. W. R. Alford, Andrew Granville and Carl Pomerance, *There are infinitely many Carmichael numbers*, Annals of Mathematics **140** (1994), 703–722.
4. W. R. Alford, Andrew Granville, and Carl Pomerance, *On the difficulty of finding reliable witnesses*, Algorithmic Number Theory (L. M. Adleman and M.-D. Huang, eds.), Lecture Notes in Comput. Sci., Springer-Verlag, New York, 1994, pp. 1–16.
5. S. Arno, *A note on Perrin pseudoprimes*, Math. Comp. **56** (1991), 371–376.
6. A. O. L. Atkin, *Intelligent Primality Test Offer*, Computational Perspectives on Number Theory (D. A. Buell and J. T. Teitelbaum, eds.), Proceedings of a Conferece in Honor of A. O. L. Atkin, International Press, 1998, pp. 1–11.
7. R. Baillie and S. S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), 1391-1417.
8. D. M. Gordon, *Pseudoprimes on elliptic curves*, Théorie des nombres (J. M. DeKoninck and C. Levesque, eds.), de Gruyter, Berlin, 1989, pp. 290–305.
9. D. M. Gordon and C. Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), 825–838.
10. J. Grantham, *Frobenius Pseudoprimes*, dissertation (1997), University of Georgia.
11. J. Grantham, *A Probable Prime Test With High Confidence*, to appear, J. Number Theory (1998).
12. J. Grantham, *There Are Infinitely Many Perrin Pseudoprimes.*
13. S. Gurak, *Pseudoprimes for higher-order linear recurrence sequences*, Math. Comp. **55** (1990), 783–813.
14. R. K. Guy, *Unsolved Problems in Number Theory*, Second Edition, Springer-Verlag, New York, 1994, p. 28.
15. N. Jacobson, *Basic Algebra I*, Second Edition, W.H. Freeman, New York, 1985, p. 258.
16. G. C. Kurtz, D. Shanks, and H. C. Williams, *Fast primality tests for numbers less than* $50 \cdot 10^9$, Math. Comp. **46** (1986), 691–701.
17. H. W. Lenstra, Jr., *Primality testing*, Computational Methods in Number Theory (H. W. Lenstra, Jr. and R. Tijdeman, eds.), Part I, vol. 154, Math. Centre Tract, Amsterdam, 1982, pp. 55–77.
18. Z. Mo and J. P. Jones, *A new primality test using Lucas sequences*, preprint.
19. L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoretical Computer Science **12** (1980), 97-108.
20. C. Pomerance, *Are there counter-examples to the Baillie – PSW primality test?*, Dopo Le Parole aangeboden aan Dr. A. K. Lenstra (H. W. Lenstra, Jr., J. K. Lenstra and P. Van Emde Boas, eds.), Amsterdam, 1984.
21. C. Pomerance, *On the distribution of pseudoprimes*, Math. Comp. **37** (1981), 587–593.
22. C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003-1026.
23. M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), 128–138.
24. R. M. Robinson, *The converse of Fermat's theorem*, Amer. Math. Monthly **64** (1957), 703–710.
25. A. Rotkiewicz, *On the pseudoprimes of the form* $ax+b$ *with respect to the sequence of Lehmer*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. **20** (1972), 349–354.

26. A. Rotkiewicz, *On Euler Lehmer pseudoprimes and Strong Lehmer pseudoprimes with parameters L, Q in arithmetic progressions*, Math. Comp. **39** (1982), 239–247.
27. G. Szekeres, *Higher order pseudoprimes in primality testing*, Combinatorics, Paul Erdős is eighty, Bolyai Soc. Math. Stud., vol. 2, János Bolyai Math Soc., Budapest, 1996, pp. 451–458.

INSTITUTE FOR DEFENSE ANALYSES, CENTER FOR COMPUTING SCIENCES, 17100 SCIENCE DRIVE, BOWIE, MD 20715