Contributions to Discrete Mathematics

Volume 2, Number 2, Pages 219–236
ISSN 1715-0868

PSEUDOPOWERS AND PRIMALITY PROVING

PEDRO BERRIZBEITIA, SIGUNA MÜLLER, AND HUGH C. WILLIAMS

Dedicated to John Selfridge on the occasion of his 80th birthday.

Abstract. The so-called pseudosquares can be employed in very powerful machinery for the primality testing of integers N. In fact, assuming reasonable heuristics (which have been confirmed for numbers to 2^{80}) they can be used to provide a deterministic primality test in time $O(\log N)^{3+o(1)}$, which some believe to be best possible. In the 1980s D.H. Lehmer posed a question tantamount to whether this could be extended to pseudo r^{th} powers. Very recently this was accomplished for $r = 3$, which naturally leads to the question of whether anything can be achieved for $r > 3$. In this paper we show how these earlier results can be extended to all prime values of r.

1. Introduction

Throughout this paper we will use the symbol N to denote an odd positive integer. In 1957, Robinson [15] introduced the idea of using Euler's criterion to prove primality for certain integers. He noted that if $(b, N) = 1$, the condition

$$b^{(N-1)/2} \equiv \left(\frac{b}{N}\right) \pmod{N}, \tag{1.1}$$

where $\left(\frac{\cdot}{N}\right)$ is the Jacobi symbol, could be used in testing N for primality, particularly when $\left(\frac{b}{N}\right) = -1$. Since 1978 it has been customary to call an integer N satisfying (1.1) a base b Euler probable prime. Two decades after [15], Solovay and Strassen [16] used the condition (1.1) in their probabilistic test for establishing the primality of N, and about this same time Rabin [13, 14] made use of a property that can not be satisfied by a prime. This was introduced by Miller [12] and used to produce a conditional primality test. This property, denoted by Rabin as $W(b)$, is as follows:

(1) $b^{N-1} \not\equiv 1 \pmod{N}$, or
(2) $1 < (b^m - 1, N) < N$ for some $m = (N-1)/2^k \in \mathbb{Z}$.

Received by the editors August 10, 2006, and in revised form October 5, 2007.

Research of the second author is partially supported under APART (Austrian Programme for Advanced Research and Technology) by the Austrian Academy of Sciences.

Research of the third author is supported by NSERC of Canada.

Clearly, if N is a prime, then N cannot satisfy $W(b)$ for any b ($1 \leq b \leq N-1$). Rabin showed that if N is composite and

$$S = \{1 \leq b \leq N-1 \,:\, N \text{ satisfies } W(b)\},$$

then $|S| \geq \frac{3}{4}(N-1)$, a better result than that yielded by the Solovay-Strassen technique.

As reported in [17], Selfridge showed that N does not satisfy $W(b)$ if and only if N is a strong base b probable prime. We call N a strong base b probable prime if $2^s \mid\mid N-1$ and either

$$a^t \equiv 1 \pmod{N} \quad (t = (N-1)/2^s)$$

or

$$a^{t2^k} \equiv -1 \pmod{N}$$

for some k ($0 \leq k < s$). Thus for a randomly selected base b, we expect the probability that a composite N is a strong base b probable prime to be less than $1/4$. The resulting primality test is given without attribution by Knuth [9, p. 379] as algorithm P. It is still the standard test used by the cryptographic community (using at least 50 randomly selected bases) to certify the primality of large integers (see, for example, FIPS 182-2, 2001). It is often referred to as the Miller-Rabin test, but in view of Selfridge's contribution, it should really be called the Miller-Rabin-Selfridge test. For further information concerning these developments the reader is referred to [18, Chapter 15].

As mentioned in [17], Selfridge also proved the following theorem involving Euler and strong base b probable primes.

Theorem A. *If N is a strong base b probable prime, then N is an Euler base b probable prime.*

Define F_x to be the least positive non-square integer such that the Jacobi symbol $\left(\frac{q}{F_x}\right) = 1$ for all primes $q \leq x$. Selfridge and Weinberger [17] prove the following primality test.

Theorem B. *Suppose that N is not a prime power, i.e. $N \neq p^a$ for some prime p and $a \geq 2$, and suppose that all prime divisors of N exceed B. If $N/B < F_x$, and for each prime $q \leq x$ we have*

$$q^{(N-1)/2} \equiv \pm 1 \pmod{N}$$

and for at least one prime $q' \leq x$ we have

$$q'^{(N-1)/2} \equiv -1 \pmod{N},$$

then N is a prime.

Later, this theorem was modified by Lukes, Patterson and Williams [10]. In order to state their result (Theorem C), we require the definition of a pseudosquare $M_{2,x}$.

If $S_{2,x}$ is the set of all odd primes $q \leq x$, then the pseudosquare $M_{2,x}$ is defined to be the smallest positive integer M, that is not a perfect square, satisfying:

(1) $M \equiv 1 \pmod 8$ and
(2) $M^{(q-1)/2} \equiv 1 \pmod q$ for all $q \in S_{2,x}$.

Conditions (1) and (2) are used to compute $M_{2,x}$ via sieving machines. Wooding and Williams [20] have computed them by making use of a new numerical sieving device (CASSIE) which implements the ideas of Bernstein in [2]. So far, $M_{2,x}$ has been computed for all $x < 367$.

Quadratic reciprocity implies that the following is an alternative definition for $M_{2,x}$: $M_{2,x}$ is the smallest non-square positive integer M such that $1 = \left(\frac{-1}{M}\right) = \left(\frac{2}{M}\right) = \left(\frac{q}{M}\right)$ for all odd primes $q \leq x$.

Note that $1 = \left(\frac{-1}{M}\right) = \left(\frac{2}{M}\right)$ is equivalent to condition (1), and quadratic reciprocity implies that $1 = \left(\frac{q}{M}\right)$, for all odd prime $q \leq x$, is equivalent to condition (2).

Theorem C. *If*

(1) *all prime divisors of N exceed B,*
(2) *$N/B < M_{2,x}$ for some x,*
(3) *$q^{(N-1)/2} \equiv \pm 1 \pmod N$ for all primes $q \leq x$,*
(4) *$2^{(N-1)/2} \equiv -1 \pmod N$ when $N \equiv 5 \pmod 8$, and*
(5) *$q'^{(N-1)/2} \equiv -1 \pmod N$ for a prime $q' \leq x$ when $N \equiv 1 \pmod 8$,*

then N is a prime or prime power.

Condition (5) is needed here in order to make use of the factor bound B in the case when $N \equiv 1 \pmod 8$, but as we expect that it will always be satisfied, this does not usually pose any problem. However, we can not prove that this condition must hold if N is a prime, $N < BM_{2,x}$ and $B > 1$. If we put $B = 1$, then the following alternative theorem can be proved.

Theorem 1.1. *Let $N < M_{2,x}$ be a positive integer that is neither a prime nor a perfect power. Then there is a prime $q \leq x$ such that*

$$\left(\frac{q}{N}\right) \not\equiv q^{(N-1)/2} \pmod N. \tag{1.2}$$

In other words, N fails to be an Euler probable prime with respect to (w.r.t.) some prime $q \leq x$.

The application of the theorem to testing primality of numbers less than $M_{2,x}$ is evident, and the complexity will depend on how rapidly these pseudosquares grow. Heuristic arguments suggest that $M_{2,x} \approx 2^{\pi(x)}$, where $\pi(x)$ is the number of primes up to x. This suggests that the theory of pseudosquares might lead to a primality test of complexity $O(\log n)^3$, a fact that has been confirmed by the data obtained up to now (see [20]).

From Theorem A, it follows that the theorem above can be replaced by the following result, which is better from a computational point of view, since the calculation of the Legendre symbols is avoided.

Corollary 1.2. *Let $N < M_{2,x}$ be a positive integer that is neither a prime nor a prime power. Then N fails to be a strong probable prime w.r.t. some prime $q \leq x$.*

Proof of Theorem 1.1. Assume that the conclusion of the theorem is false. By the reasoning employed in the proof of Theorem 16.2.6 of [18], it can be shown that if $2^s \mid\mid N-1$, then $2^s \mid\mid P-1$, where P is any prime divisor of N when $s \leq 2$. If $s > 2$, then since N is not a perfect square, there must exist some prime $q \leq x$ such that $\left(\frac{N}{q}\right) = -1$. This can then be used to show that $2^s \mid\mid P-1$.

If $N - 1 = 2^s t_N$ and $P - 1 = 2^s t_P$, then for any prime $q \leq x$ we have

$$q^{(N-1)/2} \equiv \left(\frac{q}{N}\right) \pmod{N} \text{ and } q^{(P-1)/2} \equiv \left(\frac{q}{P}\right) \pmod{P}.$$

Hence,

$$\left(\frac{q}{N}\right)^{t_P} \equiv q^{2^{s-1} t_N t_P} \equiv \left(\frac{q}{P}\right)^{t_N} \pmod{P}.$$

Since $t_P \equiv t_N \equiv 1 \pmod 2$, we have

$$\left(\frac{q}{N}\right) \equiv \left(\frac{q}{P}\right) \pmod{P},$$

and since $P > 2$, we must have $\left(\frac{q}{N}\right) = \left(\frac{q}{P}\right)$. Thus, there must exist two distinct prime divisors P, Q of N such that $\left(\frac{q}{PQ}\right) = 1$ for all $q \leq x$. The proof now follows by using the reasoning employed in the latter part of the proof of Theorem 16.2.6 of [18]. □

The purpose of this paper is to provide a generalization of Theorem 1.1. In the course of this, we will extend the definition of Euler and strong probably primes, and prove a version of a generalization of Theorem A. Some idea of how we intend to proceed is given in the next section.

2. Pseudocubes

To simplify our exposition we will use the following notation in the sequel. For any integer M denote by $\nu_r(M)$ the largest power of r that divides M. We also denote $S_{r,x}$ the set of primes q up to x such that $q \equiv 1 \pmod r$.

The extension of the pseudosquare theory to the pseudocube theory is described in [3]. Following the scheme presented above for pseudosquares, we describe briefly the main elements of the theory for pseudocubes.

Definition 2.1. *The pseudocube $M_{3,x}$ is the least positive M satisfying the following properties:*

1. *M is not a cube of an integer;*
2. *$\nu_3(M^2 - 1) \geq 2$;*
3. *$M^{(q-1)/3} \equiv 1 \pmod q$ for all primes $q \in S_{3,x}$;*
4. *$(M, q) = 1$ if $q \not\equiv 1 \pmod 3$ and $q \leq x$.*

Definition 2.2 (Alternative definition)**.** *The pseudocube $M_{3,x}$ is the least positive M satisfying the following properties:*

(1) *M is not a cube of an integer;*
(2) *$\nu_3(M^2-1) \geq 2$;*
(3) *$1 = \left(\frac{\zeta_3}{M}\right)_3 = \left(\frac{1-\zeta_3}{M}\right)_3 = \left(\frac{\pi_q}{M}\right)_3$, for all odd primes $q \in S_{3,x}$, where $\left(\frac{\cdot}{M}\right)_3$ denotes the cubic power residue symbol, ζ_3 is a cubic root of unity, and π_q is a prime in the Eisenstein ring $\mathbb{Z}[\zeta_3]$ lying over q;*
(4) *$(M,q) = 1$ if $q \not\equiv 1 \pmod 3$ and $q \leq x$.*

Note that in the alternative definition, condition (3) is analogous to the criterion obtained previously for $M_{2,x}$. We replace the square root -1 by the cube root ζ_3. The equivalence follows from the supplementary laws (see [7, Ex. 19, p. 135])

$$\left(\frac{\zeta_3}{\gamma}\right)_3 = \zeta_3^{m+n}, \quad \left(\frac{1-\zeta_3}{\gamma}\right)_3 = \zeta_3^{2n},$$

for any $\gamma = -1 + 3m + 3n\zeta_3$ that is primary (one of $\pm\gamma$ satisfies this condition), and the fact that $\left(\frac{-1}{M_{3,x}}\right)_3 = 1$.

Definition 2.3. *N is an Eisenstein probable prime w.r.t. the prime base q if*

$$\left(\frac{\pi_q}{\overline{\pi}_q}\right)^{(N^*-1)/3} \equiv \left(\frac{\pi_q}{N}\right)_3 \pmod N, \tag{2.1}$$

where $N^* = N$ if $N \equiv 1 \pmod 3$ and $N^* = -N$ if $N \equiv -1 \pmod 3$.

Theorem 2.4. *Let $N < M_{3,x}^{2/3}$ be a positive integer that is neither a prime nor a prime power. Then there is a prime $q \leq x$ such that N fails to be an Eisenstein probably prime w.r.t. some prime $q \in S_{3,x}$.*

As in the pseudosquare theory, there is also a notion of strong-Eisenstein probable primes, and hence a corollary to the main pseudocube theorem that avoids the calculation of the cubic power residue symbols.

What we achieve in this paper is a generalization of the scheme for any odd prime r. The computable definition for the pseudo r^{th} power $M_{r,x}$ is the following.

Definition 2.5. *The pseduo r^{th}-power $M_{r,x}$ is the least positive M satisfying the following properties:*

(1) *M is not an r^{th}-power of an integer;*
(2) *$\nu_r(M^{r-1}-1) \geq 2$;*
(3) *$M^{(q-1)/r} \equiv 1 \pmod q$ for all $q \in S_{3,x}$;*
(4) *$(M,q) = 1$ if $q \not\equiv 1 \pmod r$ and $q \leq x$.*

The paper is organized as follows. In Section 3, we present the preliminaries of characters, Gaussian sums and Jacobi sums in cyclotomic rings,

necessary in order to obtain the notion of cyclotomic probably primes, also defined in that section. Subsequently, we present equivalent definitions of the notion of probable primes, and show that the notions of Euler probable primes and Eisenstein probable primes are obtained when we set $r = 2$ or $r = 3$, respectively. In Section 4, we define what we call r-probable primes, which require a simpler underlying ring than cyclotomic probable primes. We also define Euler and strong versions in analogy to the classical cases. In Section 5, we fix a prime r and prove the main theorem for the pseudo r^{th} powers $M_{r,x}$. We next observe some problems with the speed of the test associated with this result, and present a faster alternative. In Section 6, we study heuristically the growth of $M_{r,x}$ and analyze the effectiveness of the test.

3. Background

3.1. **Characters, Gauss sums and Jacobi sums.** We give a short summary of some known results (cf. [7]). A (Dirichlet) character χ modulo q is a group homomorphism from $(\mathbb{Z}/q\mathbb{Z})^*$ to $\mathbb{C}^*$ for some integer q. This can be naturally extended to a multiplicative map from $\mathbb{Z}/q\mathbb{Z}$ to $\mathbb{C}$ by setting $\chi(x) = 0$ if $(x, q) \neq 1$, and it can clearly be lifted to a map from $\mathbb{Z}$ to $\mathbb{C}$. The set of characters modulo q forms a group that is known to be (non-canonically) isomorphic to $(\mathbb{Z}/q\mathbb{Z})^*$. The unit element of this group is the character χ_0 such that $\chi_0(x) = 1$ if $(x, q) = 1$ and 0 otherwise. The order of a character χ is the smallest positive m such that $\chi(a)^m = 1$ for all integers coprime to q.

We recall a few well-known facts.

Proposition 3.1. *Let q be a prime, $\chi \neq \chi_0$ be a character modulo q of order r, and let $a \in \mathbb{Z}$ coprime to q. Then*

(1) *$\chi(a)$ is an r^{th} root of unity;*
(2) *$\chi(1) = 1$ and $\chi(-1) = (-1)^{(q-1)/r}$;*
(3) *$\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$;*
(4) *$\chi(a) = 1$ iff $a^{(q-1)/r} \equiv 1 \pmod{q}$.*

In the sequel we will use the symbols q and r to represent primes such that $r \mid q-1$. We will also use χ to represent an arbitrary but fixed character modulo q of order r.

Definition 3.2. *Let χ, χ_1 and χ_2 be characters modulo q.*

(1) *The Gauss sum $\tau(\chi)$ is defined by*

$$\tau(\chi) = \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^*} \chi(x)\zeta_q^x,$$

where, as usual, $\zeta_q = e^{2\pi i/q}$.

(2) *The Jacobi sum* $j(\chi_1, \chi_2)$ *is defined by*

$$j(\chi_1, \chi_2) = \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^*} \chi_1(x)\chi_2(1-x).$$

It is clear that if χ is of order r (and hence $r \mid q-1$), then

$$\tau(\chi) \in \mathbb{Z}[\zeta_r, \zeta_q],$$

while for any χ_1, χ_2 of order dividing r,

$$j(\chi_1, \chi_2) \in \mathbb{Z}[\zeta_r].$$

This will, in general, be a much simpler ring that $\mathbb{Z}[\zeta_r, \zeta_q]$, and this observation will be important in the test.

We also note that, since $\overline{\chi(-1)} = \chi(-1)$,

$$\overline{\tau(\chi)} = \sum_x \overline{\chi}(x)\zeta^{-x} = \sum_x \overline{\chi}(-x)\zeta^x = \chi(-1)\tau(\overline{\chi}).$$

Furthermore, we have the following well-known facts.

Proposition 3.3. *Let* χ, χ_1 *and* χ_2 *be characters modulo a prime* q *such that* $\chi \neq \chi_0$ *and* $\chi_1\chi_2 \neq \chi_0$. *Then*

(1)
$$\tau(\chi)\tau(\chi^{-1}) = \chi(-1)q \text{ and } |\tau(\chi)| = \sqrt{q};$$

(2)
$$j(\chi_1, \chi_2) = \frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)};$$

(3) *if* χ_1 *and* χ_2 *are not equal to* χ_0, *then*
$$|j(\chi_1, \chi_2)| = \sqrt{q}.$$

From Proposition 8.3.3 of [7] we know the following.

Proposition 3.4. *Suppose that* χ *is a character of prime order* r *modulo* $q \equiv 1 \pmod{r}$. *Then*

$$\tau(\chi)^r = q\chi(-1)\prod_{i=1}^{r-2} j(\chi, \chi^i),$$

where the product of Jacobi sums is defined to be 1 when $r = 2$.

Definition 3.5. *We define* $T(\chi) = \tau(\chi)^r$.

Proposition 3.4 and the remarks preceding Definition 3.2 give an important and simple fact which will be of practical relevance for what follows.

Corollary 3.6. $T(\chi) \in \mathbb{Z}[\zeta_r]$.

3.2. **Cyclotomic Probable Primes.** Our algorithm for testing the primality of N will be based on a simplification of the condition underlying the APR test [1, 6, 8].

Let $K = \mathbb{Q}(\zeta_r)$ be the r^{th} cyclotomic field. It is known that K is Galois over $\mathbb{Q}$ with group G given by

$$G = \mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_a \,:\, (a,r) = 1, \text{where } \sigma_a(\zeta_r) = \zeta_r^a\}.$$

The group ring $\mathbb{Z}[G]$ is the set of formal expressions $\sum_{\sigma\in G} a(\sigma)\sigma$, where $a(\sigma) \in \mathbb{Z}$. With addition and multiplication defined in a suitable way (see e.g. [5, Definition 9.1.3]) one obtains a ring structure on $\mathbb{Z}[G]$. For $\gamma \in \mathbb{Z}[G]$ and $x \in K$, we denote by x^γ the action of the element γ of $\mathbb{Z}[G]$ on the element x of K. By definition, $x^{\sum a(\sigma)\sigma} = \prod_{\sigma\in G} \sigma(x)^{a(\sigma)}$.

Remark: Throughout we will use mod N ($N \in \mathbb{Z}$) to denote mod $N\mathcal{R}$, where $\mathcal{R}$ is an appropriate ring. Here, for $\alpha_1, \alpha_2 \in \mathcal{R}$, the congruence $\alpha_1 \equiv \alpha_2 \pmod{N\mathcal{R}}$ means that $\alpha_1 - \alpha_2 = N\gamma$ for some $\gamma \in \mathcal{R}$.

Now let χ be a character of prime order r modulo a prime q. We assume that N is coprime to r and q. Propositions 9.1.7 and 9.1.8 of [5] imply the following.

Proposition 3.8. *If N is prime then*

$$\tau(\chi)^N \equiv \tau(\chi^N)\chi(N)^{-N} \pmod{N}. \tag{3.1}$$

If (3.1) *holds for any odd integer N, then for an arbitrary $\beta \in \mathbb{Z}[G]$,*

$$\tau(\chi)^{\beta(N-\sigma_N)} \equiv \chi(N)^{-\beta N} \pmod{N}, \tag{3.2}$$

$$\tau(\chi)^{N^{r-1}-1} \equiv \chi(N) \pmod{N}. \tag{3.3}$$

For (3.1)–(3.3), $\mathcal{R} = \mathbb{Z}[\zeta_r, \zeta_q]$.

Definition 3.9. *We say that N is an r^{th} cyclotomic probable prime w.r.t. the prime $q \equiv 1 \pmod{r}$ if $(N, rq) = 1$ and N satisfies* (3.1)*. We call N an r^{th} cyclotomic probable prime w.r.t. a set S of primes $q \equiv 1 \pmod{r}$ if it is such w.r.t. all $q \in S$.*

Proposition 3.10. *Suppose that N is a cyclotomic probable prime w.r.t. q.*

- *If $r = 2$, then N is an Euler probable prime w.r.t. q.*
- *If $r = 3$, then N is an Eisenstein probable prime w.r.t. q.*

Proof. Let $r = 2$. Then χ is given by $\chi(x) = \left(\frac{x}{q}\right)$. If we put $\tilde{q} = (-1)^{(q-1)/2}q$, then $T(\chi) = \tilde{q}$, so (3.1) amounts to

$$\tilde{q}^{(N-1)/2} \equiv \left(\frac{N}{q}\right) \pmod{N}.$$

This, of course, is the same as Euler's condition by the quadratic reciprocity law.

For $r = 3$, let χ be the cubic residue character on $\mathbb{Z}[\zeta_3]$, and π a prime in $\mathbb{Z}[\zeta_3]$ lying over q. Then, $T(\chi) = q\pi$.

Let $N \equiv 1 \pmod 3$. Here (3.1) becomes $\tau(\chi)^{N-1} \equiv \chi(N)^{-N} \pmod N$. On the right, we get $\chi(N)^{-N} \equiv (N/\pi)_3^{-1} \equiv (\pi/N)_3^2 \pmod N$ via cubic reciprocity, and by appealing to Definition 3.5 on the left we get

$$T(\chi)^{(N-1)/3} \equiv \left(\frac{\pi}{N}\right)_3^{-1} \pmod N.$$

Raising this congruence to the power $\beta = 1 - \sigma_{-1}$ leads to the required statement (2.1),

$$\left(\frac{T(\chi)}{\overline{T}(\chi)}\right)^{(N-1)/3} \equiv \left(\frac{\pi}{\overline{\pi}}\right)^{(N-1)/3} \equiv \left(\frac{\pi}{N}\right)_3 \pmod N.$$

For $N \equiv -1 \pmod 3$, (3.1) reduced to

$$\tau(\chi)^N \equiv \overline{\tau(\chi)} \left(\frac{\pi}{N}\right)_3 \pmod N,$$

since $\tau(\chi^{-1}) = \overline{\tau(\chi)}$. Hence,

$$\tau(\chi)^{N+1} = T(\chi)^{(N+1)/3} \equiv q \left(\frac{\pi}{N}\right)_3 \pmod N.$$

After raising this to the power $\beta = 1 - \sigma_{-1}$,

$$\left(\frac{\pi}{\overline{\pi}}\right)^{(N+1)/3} \equiv \left(\frac{\pi}{N}\right)_3^{-1} \pmod N;$$

taking the inverse on both sides, we get the required statement (2.1). □

4. r-PROBABLE PRIMES

The difficulty with using (3.1) to define probable primes is that the underlying ring $\mathcal{R}$ is $\mathbb{Z}[\zeta_r, \zeta_q]$. In this section we define what we call r-probable primes which only require the underlying ring to be $\mathbb{Z}[\zeta_r]$.

By (3.3) we see that since $r \mid N^{r-1} - 1$, we must have

$$T(\chi)^{(N^{r-1}-1)/r} \equiv \chi(N) \pmod N \tag{4.1}$$

when N is prime. This weaker condition, rather than (3.1), will be what we use to generalize an Euler probable prime. For a method of evaluating $T(\chi)$ see [18, Section 11.1].

Definition 4.1. *We say that N is an Euler r-probable prime w.r.t. the prime $q \equiv 1 \pmod r$ if $(N, qr) = 1$ and N satisfies* (4.1).

Note that an Euler 2-probable prime w.r.t. q is an Euler probable prime w.r.t. q by Proposition 3.10.

We will now develop the notion of a strong r-probable prime. Before we do so, we will need some preliminary observations. We let f be the least positive integer such that

$$N^f \equiv 1 \pmod r.$$

Clearly, $f \mid r - 1$. It is easy to prove from (3.1) that

$$T(\chi)^{(N^f-1)/r} \equiv \chi(N)^{-f} \pmod N \tag{4.2}$$

when N is a prime. Notice that

(4.3)
$$\frac{N^{r-1}-1}{r} = \frac{N^f-1}{r}\left(N^{(g-1)f} + N^{(g-2)f} + \cdots + 1\right) \equiv g\frac{N^f-1}{r} \pmod{r},$$

where $g = (r-1)/f$. Thus, if (4.2) holds for any N, then (4.1) must also hold for that same N. Hence, instead of using the exponent $(N^{r-1}-1)/r$ on the left hand side of (4.1), we use the (perhaps) smaller exponent $(N^f-1)/r$ in our definition of a strong r-probable prime.

Now suppose that the value on the right of (4.2) equals 1 and that $r^2 \mid (N^f-1)$. We now consider $T(\chi)^{(N^f-1)/r^2}$ modulo each ideal $\mathcal{N} \subseteq \mathbb{Z}[\zeta_r]$ lying over N. Unfortunately, this value may or may not be the same modulo each of these ideals, and hence could be difficult to evaluate modulo n. The following idea of [8] gets around this problem.

Let N be any rational prime and let $s = \nu_r(N^f-1)$ and $t_N = (N^f-1)/r^s$. We define $\omega(\chi)$ to be the least integer $i \in \{0,1,\ldots,s-1\}$ such that

$$T(\chi)^{r^i t_N} \equiv \zeta^j \pmod{N}$$

for some $j \in \{0,1,\ldots,r-1\}$, where $\zeta = \zeta_r$. By definition of $\omega(\chi)$ we see that when $\omega(\chi) \geq 1$ and

$$T(\chi)^{r^{\omega(\chi)} t_N} \equiv 1 \pmod{N},$$

the element $T(\chi)^{r^{\omega(\chi)-1} t_N} - \zeta^l$ of $\mathbb{Z}[\zeta]$ has, for all $l \in \{0,1,\ldots,r-1\}$, when expressed in terms of the basis $\{1,\zeta,\ldots,\zeta^{r-2}\}$ of $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$, a coefficient which is not divisible by N and is therefore coprime with N. This observation inspires the following.

Definition 4.2. *Let s and t_N be as defined above. We say that N is a strong r-probable prime w.r.t. q if*

(1) *there exists $\omega = \omega(\chi)$, the least integer $i \in \{0,1,\ldots,s-1\}$ such that*

$$T(\chi)^{r^i t_N} \equiv \zeta^j \pmod{N}$$

for some $j \in \{0,1,\ldots,r-1\}$, where $\zeta = \zeta_r$, and

(2) *if $\omega(\chi) \geq 1$ and $T(\chi)^{r^{\omega(\chi)} t_N} \equiv 1 \pmod{N}$, then for each $l \in \{0,1,\ldots,s-1\}$ the element $T(\chi)^{r^{\omega(\chi)-1} t_N} - \zeta_l$ of $\mathbb{Z}[\zeta]$ has, when expressed in terms of the basis $\{1,\zeta,\ldots,\zeta^{r-2}\}$ of $\mathbb{Z}[\zeta]$ over $\mathbb{Z}$, a coefficient that is coprime with N.*

For the case $\omega(\chi) \geq 1$, each $T(\chi)^{r^{\omega(\chi)-1} t_N} - \zeta^l$ has a coefficient not equivalent to $0 \pmod{N}$, so by a gcd-calculation we can check the second condition of the definition, or else find a non-trivial divisor of N.

Note that in order to test condition (2), we only require the value of $T(\chi)^{r^{\omega(\chi)-1} t_N} \pmod{N}$. Also, by the observations in the proof of Proposition 3.10, we see that a strong 2-probable prime w.r.t q is a strong probable prime w.r.t. q.

Remark: When $r = 3$, we use $\lambda = T(\chi)/\overline{T(\chi)} = T(\chi)^{1-\sigma_{-1}}$ instead of $T(\chi)$ in our definition of a strong cubic pseudoprime [3]. In this case, if we use λ instead of $T(\chi)$, we can easily show that $\omega(\chi) = 0$. This follows by noting that if N is a prime, then it either remains a prime or it is the product of two primes ν and $\overline{\nu}$ in $\mathbb{Z}[\zeta_3]$. In the first case it is clear that $\omega(\chi) = 0$; in the second case we define i in a manner analogous to that above using λ instead of $T(\chi)$. If

$$\lambda^{3^i t_N^*} \equiv 1 \pmod{N}$$

and $i \geq 1$, then

$$\lambda^{3^{i-1} t_N^*} \equiv \zeta_3^k \pmod{\nu}$$

for some $k \in \{0, 1, 2\}$, $t_N^* = (N^* - 1)/3^s$, $s = \nu_3(N^* - 1)$, where $N^* = \pm N$ such that $3 \mid N^* - 1$. After conjugating,

$$\overline{\lambda}^{3^{i-1} t_N^*} \equiv \zeta_3^{2k} \pmod{\overline{\nu}}.$$

Since $\overline{\lambda} = 1/\lambda$, we get

$$\lambda^{3^{i-1} t_N^*} \equiv \zeta_3^k \pmod{\overline{\nu}}$$

and

$$\lambda^{3^{i-1} t_N^*} \equiv \zeta_3^k \pmod{N}.$$

This contradicts the minimality of i. Hence we must have $\omega(\chi) = 0$ in this case. Unfortunately, when $r > 3$ there does not appear to be any element $\rho \in \mathbb{Z}[G]$ such that we can get a similar result for $T(\chi)^\rho$.

Proposition 4.4. *If P is any prime divisor of N and N is a strong r-probable prime w.r.t. q then $r^{\omega(\chi)+1} \mid P^{r-1} - 1$.*

Proof. Consider the conditions in Definition 4.2, where we write $\tau(\chi)^r$ in place of $T(\chi)$, and $\omega(\chi)'$ in place of $\omega(\chi)$. Then [8, Proposition 5.3] asserts that $r^{\omega(\chi)'} \mid P^{r-1} - 1$, which is the desired result, since $T(\chi) = \tau(\chi)^r$ implies that $\omega(\chi) = \omega(\chi)' + 1$. □

We now require a simple lemma.

Lemma 4.5. *If for some fixed $i \geq 1$ we have $r^i \mid m_1^{r-1} - 1$ and $r^i \mid m_2^{r-1} - 1$, then $r^i \mid (m_1 m_2)^{r-1} - 1$. If we write $e_m(i) = (m^{r-1} - 1)/r^i$, then*

$$e_{m_1 m_2}(i) \equiv e_{m_1}(i) + e_{m_2}(i) \pmod{r^i}.$$

Proof. By definition, $m_j^{r-1} = e_{m_j}(i) r^i + 1$ for $j = 1, 2$. Thus,

$$(m_1 m_2)^{r-1} \equiv (e_{m_1}(i) + e_{m_2}(i)) r^i + 1 \pmod{r^{2i}},$$

from which the result immediately follows. □

Observer that $e_m(i) \equiv 0 \pmod{r}$ for any $i \geq 1$ implies $\nu_r(m^{r-1} - 1) \geq 2$.

Definition 4.6. *For $M > 1$, let $s = \nu_r(M^{r-1} - 1)$ and $a_M = (M^{r-1} - 1)/r^s$. (Note that $(r, a_M) = 1$ and $a_M = e_M(s)$.)*

By Proposition 4.4 there is a fixed $\omega = \omega(\chi)$ so that for any $P \mid N$ we can write $P^{r-1} - 1 = r^{\omega+1}k_P$ for some integer $k_P = e_P(\omega + 1)$. By multiplicativity, this also defines a unique integer $k_N = e_N(\omega + 1)$ via

$$N^{r-1} - 1 = r^{\omega+1}k_N.$$

Note that $k_N = r^{s-\omega-1}a_N$. By Lemma 4.5,

$$\sum_{P|N} k_P \equiv k_N \pmod{r}. \tag{4.4}$$

Theorem 4.7. *If N is a strong r-probable prime w.r.t. q, then N is an Euler r-probable prime w.r.t. q.*

Proof. It suffices to show that if N is a strong r-probable prime w.r.t. q, then

$$T(\chi)^{r^{s-1}a_N} \equiv \chi(N) \pmod{N}.$$

By hypothesis,

$$T(\chi)^{r^{\omega}t_N} \equiv \zeta^j \pmod{N}, \tag{4.5}$$

where $t_N = (N^f - 1)/r^s$, as above. Since $P \mid N$, this also hold modulo P. On the other hand, since P is a prime, (4.1) implies

$$T(\chi)^{r^{\omega}k_P} \equiv \chi(P) \pmod{P}. \tag{4.6}$$

Raising the former equation to the power k_P, and the latter to the power t_N, it follows that $\chi(P)^{t_N} \equiv \zeta^{jk_P} \pmod{P}$. Note that on both sides we have roots of unity. It is well known (cf. [18, Lemma 17.2.3]) that since $(r, P) = 1$ this implies

$$\chi(P)^{t_N} = \zeta^{jk_P}.$$

Multiplying over all primes P dividing N, we obtain

$$\chi(N)^{t_N} = \zeta^{j\sum_{P|N} k_P} = \zeta^{jk_N}, \tag{4.7}$$

where we have used (4.4). By appealing to (4.5) we get

$$\chi(N)^{t_N} \equiv T(\chi)^{r^{\omega}k_N t_N} \pmod{N}.$$

Since $(t_N, r) = 1$, it follows that $\chi(N) \equiv T(\chi)^{r^{\omega}k_N} = T(\chi)^{r^{s-1}a_N} \pmod{N}$, as desired. □

5. Pseudopowers and r-probable primes

5.1. **Definition and Fundamental Properties.** In the following, let r be an *odd* prime. As above, let $\chi = \chi_q$ be a fixed character modulo q of order r. We first give an equivalent formulation of Definition 2.5.

Definition 5.1. *The pseudo r^{th} power $M_{r,x}$ w.r.t. the set $S_{r,x}$ is the least positive integer M satisfying the following properties.*

1. *M is not an r^{th} power of an integer;*
2. *$\nu_r(M^{r-1} - 1) \geq 2$;*
3. *$\chi_q(M) = 1$ for all $q \in S_{r,x}$;*

(4) $(M, q) = 1$ *if* $q \not\equiv 1 \pmod{r}$ *and* $q \leq x$.

Lemma 5.2. *If N is an Euler r-probable prime w.r.t. each $q \in S_{r,x}$ and does not satisfy condition (2) or (3) of Definition 5.1, then*

$$\nu_r(P^{r-1} - 1) \geq \nu_r(N^{r-1} - 1),$$

for all prime divisors P of N.

Proof. This can be deduced from [5, Corollary 9.1.15, Proposition 9.1.17]. For the sake of completeness we include a proof. If N does not satisfy condition (2), then $\nu_r(M^{r-1} - 1) = 1$, and hence the conclusion is trivial. Otherwise, for some $q \in S_{r,x}$,

$$T(\chi_q)^{(N^{r-1}-1)/r} \equiv \chi_q(N) \not\equiv 1 \pmod{P}.$$

Let $s = \nu_r(N^{r-1} - 1)$ and $\mathcal{P}$ be a prime ideal in $\mathbb{Z}[\zeta_r]$ lying over P. Then $T(\chi_q)^{(N^{r-1}-1)/r^s}$ has order r^s in $(\mathbb{Z}[\zeta_r]/\mathcal{P})^*$, so that $r^s \mid P^{r-1} - 1$. □

5.2. **The Main Theorem.** We can now sharpen the inequality in Lemma 5.2 to obtain equality.

Proposition 5.3. *Let $N < M_{r,x}$ be an Euler r-probable prime w.r.t. all primes in $S_{r,x}$. Assume N is not a perfect power and let P and Q be any prime divisors of N. Then, with a_M as defined in Definition 4.6,*

(1) $\nu_r(N^{r-1} - 1) = \nu_r(P^{r-1} - 1)$;
(2) $\chi_q(P)^{a_N} = \chi_q(N)^{a_P}$ *for all* $q \in S_{r,x}$;
(3) $\chi_q(P)^{a_Q} = \chi_q(Q)^{a_P}$ *for all* $q \in S_{r,x}$.

Proof. Since $N < M_{r,x}$ it must violate either condition (2) or (3) (for some $q \in S_{r,x}$) of Definition 5.1. Hence, from Lemma 5.2, we get $\nu_r(P^{r-1} - 1) \geq \nu_r(N^{r-1} - 1)$ for any prime P dividing N. It remains to show equality.

By our hypothesis, and since P is a prime, we obtain

$$\tau(\chi_q)^{N^{r-1}-1} \equiv \chi_q(N) \pmod{N},$$
$$\tau(\chi_q)^{P^{r-1}-1} \equiv \chi_q(P) \pmod{P}.$$

Since P divides N, both equalities hold modulo P.

Let $s = \nu_r(N^{r-1} - 1)$. Then $b_P = (P^{r-1} - 1)/r^s \in \mathbb{Z}$ by Lemma 5.2. Observe that

$$\frac{N^{r-1} - 1}{P^{r-1} - 1} = \frac{a_N}{b_P}.$$

Using the above two congruences, we get

$$\chi_q(N)^{b_P} = \chi_q(P)^{a_N}. \tag{5.1}$$

If $\nu_r(P^{r-1} - 1) = 1$, then necessarily $\nu_r(N^{r-1} - 1) = 1$, and the first assertion of the proposition trivially holds (note also that $b_P = a_P$ in this case). Otherwise, $\nu_r(P^{r-1} - 1) \geq 2$. Since by hypothesis $P < M_{r,x}$, this yields $\chi_q(P) \neq 1$ for some $q \in S_{r,x}$.

It follows that since $r \nmid a_N$ we have $\chi_q(P)^{a_N} \neq 1$ and hence, by (5.1), $\chi_q(N)^{b_P} \neq 1$. This shows $r \nmid b_P$. Therefore, $b_P = a_P$, which proves the first assertion of the proposition.

The second assertion follows automatically. This, applied to P and Q gives

$$\chi_q(P)^{a_N} = \chi_q(N)^{a_P},$$
$$\chi_q(Q)^{a_N} = \chi_q(N)^{a_Q},$$

that, when raised to the appropriate powers a_Q and a_P, respectively, proves the third assertion (since $r \nmid a_N$). □

We now obtain the main result that generalizes both Theorem 1.1 and the main result of [3].

Theorem 5.4. *If $N < M_{r,x}^{2/r}$, and N is not a prime or a perfect power, then N fails to be an Euler r-probable prime w.r.t. $S_{r,x}$.*

Proof. N must have at least two distinct prime divisors P and Q. Without loss of generality we may assume $Q < \sqrt{N}$. Suppose to the contrary that N is an Euler r-probable prime w.r.t. $S_{r,x}$.

If q is arbitrarily selected from $S_{r,x}$, then by Proposition 5.3, $\chi_q(P)^{a_Q} = \chi_q(Q)^{a_P}$. Let $t \equiv a_P a_Q^{-1} \pmod r$. Note that $1 \leq t < r$ and

$$\chi_q(P) = \chi_q(Q^t).$$

Put $M = PQ^{r-t}$. We obtain the following.

(1) $M = PQQ^{r-t-1} < N(\sqrt{N})^{r-2} = N^{r/2} < (M_{r,x}^{2/r})^{r/2} = M_{r,x}$.
(2) $\chi_q(PQ^{r-t}) = \chi_q(P)\chi_q(Q)^{r-t} = \chi_q(Q)^t\chi_q(Q)^{r-t} = \chi_q(Q)^r = 1$.
(3) If $\nu_r(N^{r-1}-1) = i$, then $\nu_r(P^{r-1}-1) = i$ for all $P \mid N$ by Proposition 5.3. By Lemma 4.5, $e_M(i) = e_{PQ^{r-t}}(i) \equiv e_P(i) + e_{Q^{r-t}}(i) \equiv e_P(i) + (r-t)e_Q(i) \pmod r$. Therefore, $e_M(i) \equiv e_P(i) - te_Q(i) \equiv 0 \pmod r$, since $t \equiv a_P a_Q^{-1} \equiv e_P(i)(e_Q(i))^{-1} \pmod r$. This shows that $\nu_r(M^{r-1}-1) \geq 2$ since $i \geq 1$.

However, since $M < M_{r,x}$ and M is not an r^{th} power, we cannot have $\nu_r(M^{r-1}-1) \geq 2$ and $\chi_q(M) = 1$ for all $q \in S_{r,x}$. □

5.3. **A More Practical Version.** The formulation of our testing condition via Definition 4.1 or Definition 4.2, may require very large exponents such as $(N^{r-1}-1)/r$ or $(N^f-1)/r$, respectively. In particular, testing (4.2) requires the computation of $T(\chi)^{(N^f-1)/r}$, which is feasible only for $f = 1$ or 2. For larger values of f we can do better than computing (4.2) by using the following proposition (variants of our presentation have been used in [1, 6, 5, 4, 11]).

Recall that the condition given in Definitions 4.1 and 4.2 are both consequences of condition (3.1), which, as stated above, is highly impractical since $\tau(\chi) \in \mathbb{Z}[\zeta_r, \zeta_q]$.

Proposition 5.5. *If $(N, qr) = 1$, the following three statements are equivalent.*

(1) *Condition* (3.1)*, i.e.,*
$$\tau(\chi)^N \equiv \tau(\chi^N)\chi(N)^{-N} \pmod{N}.$$
(2) *Let $s < r$ be defined via $N \equiv s \pmod{r}$. If we let $J(s,\chi) = \tau(\chi)^s/\tau(\chi^s)$, then*
$$J(s,\chi)T(\chi)^{(N-s)/r} \equiv \chi(N)^{-s} \pmod{N}.$$
In particular, $J(s,\chi) = \prod_{i=1}^{s-1} j(\chi,\chi^i) \in \mathbb{Z}[\zeta_r]$.
(3) *Let $1 \le s \le r/2$ be such that $N \equiv \pm s \pmod{r}$. If $N \equiv s \pmod{r}$, let $N^* = N$ and $\epsilon(N^*) = 0$. Alternatively, if $N \equiv -s \pmod{r}$, let $N^* = -N$ and $\epsilon(N^*) = 1$. For $J(s,\chi)$ as before, we have*
$$q^{\epsilon(N^*)}J(s,\chi)T(\chi)^{(N^*-s)/r} \equiv \chi(-1)\chi(N^*)^{-s} \pmod{N}.$$

Proof. Recall that
$$J(s,\chi) = \frac{\tau(\chi)^s}{\tau(\chi^s)} = \prod_{i=1}^{s-1} j(\chi,\chi^i) \in \mathbb{Z}[\zeta_r]$$
by inductive application of fact (2) of Proposition 3.3 [7, Proposition 8.3.3]. Then the first equivalence follows immediately from the definition of s, t and $T(\chi)$.

For the second equivalence, we need only consider the case when $N \equiv -s \pmod{r}$, where $N^* = -N < 0$. Here, Proposition 3.3 asserts that
$$\tau(\chi)^{-1} = \chi(-1)\tau(\chi^{-1})/q,$$
which holds for any $\chi \neq \chi_0$, and hence also for χ^s. Substituted into the previous result, this establishes the claim. □

Note that the appropriate ring in (1) is $\mathbb{Z}[\zeta_q, \zeta_r]$, but the ring in (2) and (3) is just $\mathbb{Z}[\zeta_r]$.

From Proposition 5.5, we now deduce the following consequence (namely (5.2)), that we use as the testing condition in practice. If we apply $\beta = 1 - \sigma_{-1} \in \mathbb{Z}[G]$ to both sides of the formula in (3), we get

$$\left(\frac{\overline{T}(\chi)}{T(\chi)}\right)^{(N^*-s)/r} \equiv \chi(N^*)^{2s} \prod_{i=1}^{s-1} \frac{j(\chi,\chi^i)}{\overline{j}(\chi,\chi^i)} \pmod{N}. \tag{5.2}$$

For $r = 3$ formula (5.2) becomes very simple, as the product on the right disappears because $s = 1$. In fact, (5.2) reduces immediately to the notion of an Eisenstein probable prime (see (2.1)).

Note that the most time consuming part of (5.2) is the computation on the left. Also, the right hand side involves computations of $s-1$ different Jacobi sums, and the multiplication of $2s$ of these. Recall that χ is a character modulo q for some prime $q \equiv 1 \pmod{r}$, hence q may be rather large. In that case, working out the right hand side may involve quite some computational

effort. There are some more efficient ways for doing this such that the right hand side will require the computation of only one Jacobi sum (see [4, 5]).

6. Growth-Rate Estimate

In [3], it was shown that it seems there is some advantage to using pseudocubes instead of pseudosquares for testing primality. Generally, an exact comparison is difficult, mainly because the actual rate of growth of pseudosquares, pseudocubes, or pseudo r^{th} powers is not known. However, in comparing the relative growth rates, it becomes clear that the test based on the pseudocubes is 'better' than the test based on pseudosquares, only if

$$M_{3,q_n}^{2/3} > L_{p_n}, \tag{6.1}$$

where p_n denotes the n^{th} prime, q_n the n^{th} prime congruent to 1 (mod 3), and $L_{p_n} = M_{2,p_n}$ (see [3]). In fact, it is shown in [3] that this inequality holds for sufficiently large n by appealing to a reasonable heuristic.

Here, we show the somewhat surprising result, that there is no advantage in replacing the pseudocubes by pseudo r^{th} powers, for $r > 3$.

Recall that the test for the pseudosquares involves all primes less than or equal to p, where p is the smallest prime p_n such that $N < L_{p_n}$. The r^{th} cyclotomic test only requires the primes $q \equiv 1 \pmod{r}$, $q \leq p$. On the other hand, the p in this case is the smallest prime q_n such that $N < M_{r,q_n}^{2/r}$. By Theorem 5.4, the above argument generalizes to the following. The test based on the pseudo r^{th} powers is 'better' than the test based on the pseudosquares, only if

$$M_{r,q_n}^{2/r} > L_{p_n}. \tag{6.2}$$

In [10] it is conjectured that the pseudosquares L_{p_n} should have a growth rate of the form

$$L_{p_n} \approx c_1 2^n \log p_n. \tag{6.3}$$

This estimate was derived from the conjecture that the solutions of

$$x \equiv 1 \pmod{8}, \ \left(\frac{x}{p_i}\right) = 1 \quad (i = 1, 2, \ldots, n) \tag{6.4}$$

are equidistributed in the region $0 < x < 8p_2p_3 \cdots p_n$.

Appealing to part (4) of Proposition 4 and Definition 5.1, we can make the analogous heuristic assumption that the solutions of

$$x^{r-1} \equiv 1 \pmod{r^2}, \ x^{(q_i-1)/r} \equiv 1 \pmod{q_i} \quad (i = 1, 2, \ldots, n) \tag{6.5}$$

are equidistributed in the region $0 < x < rq_1q_2 \cdots q_n$. We would therefore expect that

$$M_{r,q_n} \approx r^2 \prod_{i=1}^{n} \frac{q_i}{S},$$

where S is the number of solutions of (6.5). Since

$$S = (r-1)\prod_{i=1}^{n}\frac{q_i-1}{r},$$

we get

$$M_{r,q_n} \approx r^{n+1}\prod_{i=1}^{n}\frac{q_i}{q_i-1}.$$

Now, Mertens' Theorem for arithmetic progressions states that

$$\prod_{p_i \le q_n p_i \equiv 1 \pmod r}\left(1-\frac{1}{p_i}\right) \approx c(\log q_n)^{-1/(r-1)},$$

where the constant c (which depends only on r) and the error term can be made explicit (see [19]). From this, we get

$$M_{r,q_n} \approx c_2 r^n (\log_n)^{r-1} \tag{6.6}$$

for a constant c_2 which only depends on r. To compare their relative growth rates, we get from (6.3) and (6.6),

$$\frac{(M_{r,q_n})^{2/r}}{L_{p_n}} \approx \frac{c_2^{2/r} r^{2n/r}(\log q_n)^{2(r-1)/r}}{c_1 2^n \log p_n}.$$

However, the dominating term here becomes $(r^{2/r}/2)^n$, and $r^{2/r} < 2$ for any $r > 3$ (but $r^{2/r} > 2$ for $r = 3$). This suggests the following.

Conjecture. *Under the same heuristic estimates* (6.4) *and* (6.5) *for the pseudosquares and the pseudo* r^{th} *powers, we have* $M_{r,q_n}^{2/r} > L_{p_n}$ *for sufficiently large* n *only for* $r = 3$.

References

1. L. M. Adleman, C. Pomerance, and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), no. 1, 173–206.
2. D. J. Bernstein, *Doubly focused enumeration of locally square polynomial values*, pp. 69–76, Fields Institute Communications, AMS, Providence, Rhode Island, 1996.
3. P. Berrizbeitia, S. Müller, and H. C. Williams, *Pseudocubes and primality testing*, LNCS, vol. 3076, pp. 102–116, Springer, Berlin, 2004.
4. W. Bosma and M.-P. van der Hulst, *Primality proving with cyclotomy*, Ph.D. thesis, Universiteit van Amsterdam, 1990.
5. H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.
6. H. Cohen and H. W. Lenstra Jr., *Primality testing and Jacobi sums*, Math. Comp. **42** (1984), no. 165, 297–330.
7. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2 ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.
8. H. W. Lenstra Jr., *Primality testing algorithms (after Adleman, Rumely and Williams)*, LNCS, vol. 901, pp. 243–257, springer, Belin, 1981.
9. D. E. Knuth, *The art of computer programming. Vol. 2: Seminumerical algorithms*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, ON, 1969.

10. R. F. Lukes, C. D. Patterson, and H. C. Williams, *Some results on pseudosquares*, Math. Comp. **65** (1996), no. 213, 361–372, S25-S27.
11. P. Mihailescu, *Cyclotomy primiality proving—recent developments*, Algorithmic number theory: ANTS-III (J. P. Buhler, ed.), LNCS, vol. 1423, Springer, Berlin, 1998, pp. 95–110.
12. G. L. Miller, *Riemann's hypothesis and tests for primality*, Seventh Annual ACN Symposium of Theory of Computing (Albuquerque, NM, 1975), ACM, New York, 1975, pp. 234–239.
13. M. O. Rabin, *Probabilistic algorithms*, Algorithms and complexity (Proc. Sympos., Carnegie-Mellon Univ., Pittsburgh, PA, 1976), Academic Press, New York, 1975, pp. 21–39.
14. ———, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138.
15. R. M. Robinson, *The converse of Fermat's theorem*, Amer. Math. Monthly **64** (1957), 703–710.
16. R. Solovary and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), no. 1, 84–85.
17. H. C. Williams, *Primality testing on a computer*, Ars Combin. **5** (1978), 127–185.
18. ———, *Édouard Lucas and primality testing*, John Wiley & Sons Inc., New York, 1998.
19. K. S. Williams, *Mertens' theorem for arithmetic progressions*, J. Number Theory **6** (1974), 353–359.
20. K. Wooding and H. C. Williams, *Doubly-focused enumeration of pseudosquares and pseudocubes*, Proceedings of ANTS-VII (2006), LNCS 4076, Springer-Verlag, 2006, to appear, pp. 208–221.

Departamento de matematicas P. y A., Universidad Simón Bolívar,
Apartado 89000, Caracas 1080-A, Venezuela
E-mail address: pedrob@usb.ve

Department of Mathematics, University of Wyoming,
1000 E. University Avenue, Laramie, Wyoming 82070, USA
E-mail address: smuller@uwyo.edu

Centre for Applied Cryptographic Research, University of Calgary,
2500 University Drive NW, Calgary, Alberta T2N 1N4, Canada
E-mail address: williams@math.ucalgary.ca