International Journal of Pure and Applied Mathematics

Volume 44 No. 3 2008, 347-362

RANDOMIZED COMPOSITENESS TESTING WITH CHEBYSHEV POLYNOMIALS

David P. Jacobs[1] §, Mohamed O. Rayes[2], Vilmar Trevisan[3]

[1]School of Computing
Clemson University
Clemson, SC 29634-0974, USA
e-mail: dpj@cs.clemson.edu

[2]Department of Computer Science and Engineering
Southern Methodist University
Dallas, TX 75275-0122, USA
e-mail: mrayes@engr.smu.edu

[3]Instituto de Matemática, UFRGS
Porto Alegre, 91509-900, BRAZIL
e-mail: trevisan@mat.ufrgs.br

Abstract: We consider a simple, fast randomized compositeness test. Let $U_n(x)$ denote the degree-n Chebyshev polynomial of the second kind. Rankin showed that if p is an odd prime, then exactly $\frac{p-1}{2}$ of the numbers $a \in \mathbb{Z}/p\mathbb{Z} - \{1, -1\}$, satisfy $U_{\frac{p-1}{2}}(a) \equiv 0 \bmod p$, and the remaining $\frac{p-3}{2}$ numbers satisfy $U_{\frac{p-3}{2}}(a) \equiv 0 \bmod p$. Moreover, these are precisely the numbers a for which $\left(\frac{a^2-1}{p}\right) = -1$ and $\left(\frac{a^2-1}{p}\right) = 1$ respectively. We show that when n is an odd composite, at least half of the members $a \in \mathbb{Z}/n\mathbb{Z}$ are witnesses, unless $n = pq$ where p and q are twin primes, in which case there must be at least $\frac{3}{8}n$ witnesses. However, these ratios occur only for a rare set of numbers, and in practice the expected ratio of witnesses is very high. In one experiment involving a million large composite numbers, all but two composites were recognized with the first randomly chosen a, the other two requiring only an additional guess.

AMS Subject Classification: 11Y11, 68W20
Key Words: primality, randomized algorithms, Chebyshev polynomial

Received: January 1, 2008

§Correspondence author

1. Introduction

The recent discovery of the deterministic polynomial-time AKS algorithm for recognizing primes was an exciting milestone in mathematics [1]. Yet, randomized testing algorithms continue to be important because they are fast and sometimes simple to implement.

We refer the reader to [3] for a good overview of various computational methods for recognizing primes and composites. A powerful result is the so-called Random Quadratic Frobenius Test [5]. If n is composite, not a square, and not divisible by any prime less than 50,000, then n is a strong Frobenius pseudoprime with probability at most $\frac{1}{7710}$.

In this paper we present some preliminary work involving randomized compositeness testing using Chebyshev polynomials. While the error bound of our algorithm is not as strong as some other methods, our approach is simple and mathematically interesting. In practice, compositeness testing is sometimes done with a blend of methods [9]. Thus our goal is to offer one more computational tool.

Recall that the *Chebyshev polynomials of the first kind*, denoted $T_n(x)$, can be defined recursively by setting $T_0(x) = 1$ and $T_1(x) = x$, and

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x).$$

The *Chebyshev polynomials of the second kind*, denoted $U_n(x)$, can be similarly defined by $U_0(x) = 1$, $U_1(x) = 2x$, and the recurrence relation

$$U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x). \tag{1}$$

Both the $T_n(x)$ and $U_n(x)$ are sequences of integer polynomials. In this paper, we will show how a fast random compositeness test can be achieved by evaluating the $U_n(x)$ over $\mathbb{Z}/n\mathbb{Z}$. To this end, we make use of a result in [10], where $\left(\frac{a}{p}\right)$ denotes the Jacobi symbol.

Theorem 1. (Rankin) *If p is an odd prime, then for each $a \in \mathbb{Z}/p\mathbb{Z} - \{1, -1\}$, exactly one of the following holds:*

1. $U_{\frac{p-1}{2}}(a) \equiv 0 \bmod p$ *and* $\left(\frac{a^2-1}{p}\right) = -1$
2. $U_{\frac{p-3}{2}}(a) \equiv 0 \bmod p$ *and* $\left(\frac{a^2-1}{p}\right) = 1$

Letting $I_n = \mathbb{Z}/n\mathbb{Z} - \{1, -1\}$, if n is an odd composite integer, we say that a number $a \in I_n$ is a *witness* for n if

1. $U_{\frac{n-1}{2}}(a) \not\equiv 0 \bmod n$ and $U_{\frac{n-3}{2}}(a) \not\equiv 0 \bmod n$ or

2. $U_{\frac{n-1}{2}}(a) \equiv 0 \bmod n$ and $\left(\frac{a^2-1}{n}\right) \neq -1$ or

3. $U_{\frac{n-3}{2}}(a) \equiv 0 \bmod n$ and $\left(\frac{a^2-1}{n}\right) \neq 1$.

Theorem 1 implies that discovering a witness proves that n is composite. Our algorithm, shown in Figure 1, is typical of many randomized compositeness tests. Given an odd n we choose a random $a \in I_n$ and compute $\left(\frac{a^2-1}{n}\right)$, $U_{\frac{n-1}{2}}(a)$ and $U_{\frac{n-3}{2}}(a)$. If it is a witness, then we halt and report with certainty that n is *composite*. Otherwise we repeat the process up to, say, k times. If n survives the test, then we report that it *fails*.

Our main result is that when n is an odd composite, at least half of the members in $\mathbb{Z}/n\mathbb{Z}$ are witnesses, unless $n = pq$ where p and q are twin primes, in which case there must be at least $\frac{3}{8}n$ witnesses. That is,

Theorem 2. *The algorithm of Figure 1 fails with probability less than* $(\frac{1}{2})^k$*, unless* n *is the product of two twin primes in which case its error is bounded by* $(\frac{5}{8})^k$*.*

The theoretical probability of error can be reduced by recognizing the twin prime possibility through a preprocessing step: One can efficiently determine if n is a product of two consecutive odd integers by solving $4k^2 - 1 = n$.

We do not know of cases where the ratio achieves $\frac{3}{8}$, but there does exist a rare set of composites whose ratio of witnesses is about $\frac{1}{2}$. So in the worst case, our ratio of witnesses is not as favorable as that of Miller-Rabin test in which there are at least $\frac{3}{4}$ witnesses [3]. However, in practice our test does well, and one experiment involving over 35,000 Carmichael numbers found that the percentage of witnesses was about 87%.

In Section 2 we report some experimental evidence suggesting that in practice our method works well. In Section 3 we give the framework which motivates this paper. The following three sections constitute the bulk of this paper and are devoted to proving that when n is an odd composite, there are many witnesses. The cases when n is divisible by a square, n is a squarefree product of at least three primes, and n a product of two distinct primes are handled with different arguments in Sections 4, 5, and 6, respectively. In Section 7 we summarize our analysis in Theorem 2, and in Section 8 we identify certain rare numbers which give our algorithm worst-case behavior. In Section 9 we explain how the algorithm can be implemented efficiently using fast exponentiation of a certain 2×2 matrix over $\mathbb{Z}/n\mathbb{Z}$.

Input: An odd integer $n \geq 3$

Output: *composite, fail*

1 **for** $i = 1$ **to** k
2 $a \leftarrow$ random number in $\{0, 2, 3 \ldots n-2\}$
3 **if** $U_{\frac{n-1}{2}}(a) \equiv 0 \bmod n$ and $\left(\frac{a^2-1}{n}\right) \neq -1$ **then return** *composite*
4 **else if** $U_{\frac{n-3}{2}}(a) \equiv 0 \bmod n$ and $\left(\frac{a^2-1}{n}\right) \neq 1$ **then return** *composite*
5 **else return** *composite*
6 **end**

7 **return** *fail*

Figure 1: Randomized compositeness test

2. Experiments

Here we describe some experiments which suggest that the expected behavior of our algorithm is very good, and that the worst-case behavior is achieved only for a thin set of numbers. Our algorithm is easy to implement. We did so in about 30 lines of *Maple*, using standard modular arithmetic operations and ordinary matrix multiplication.

In one experiment, we tested a million consecutive composite numbers, beginning with $2 \cdot 10^{10} + 1$. Except for two of the composites, a witness was found with a single guess. The other two composites each required only one additional guess.

In a second experiment, we constructed $14,400$ composite numbers $n > 10^{100}$, each a product of two large primes. For each such n we generated one hundred random a, and counted how many of them were witnesses, giving a score $s(n)$. All but six of the n received a perfect score $s(n) = 100$. Those six composities not receiving perfect scores had scores ranging from 70 to 78. All six of these composites were a product of twin primes, confirming that such numbers behave differently.

In a third experiment, using a file made available from R. Pinch, we ran our test on all 35,585 Carmichael numbers less than 10^{18}, having three prime factors. The worst score was 72 and the average score was 87.5.

3. Background

A connection between Chebyshev polynomials and prime numbers has long been known. For a polynomial $f(x) \in \mathbb{Z}[x]$, we will let $\phi_n(f)$ denote the image of the polynomial in $(\mathbb{Z}/n\mathbb{Z})[x]$ under the usual mapping. Consider the following theorem:

Theorem 3. *An odd integer $p > 1$ is prime if and only if $\phi_p(T_p(x)) = x^p$.*

The "only if" part of Theorem 3 was published in 1954 by Bang [2], and also appears in Rivlin's book [12, p. 232]. The "if" part of Theorem 3 is proven in [7]. An immediate consequence, using Fermat's Little Theorem, is:

Corollary 4. *For odd primes p, $T_p(a) \equiv a \bmod p$ for all integers a.*

A composite number n such that for all integers a,

$$T_n(a) \equiv a \bmod n,$$

is called a *Chebyshev number* in [7]. They are analogous to Carmichael numbers, but more rare. In fact, there is only one Chebyshev number less than 10^{10}, namely $7,056,721$. Nevertheless, the existence of Chebyshev numbers prevents a randomized compositeness test based on evaluating $T_n(x)$ alone. In [7] it was shown that

Theorem 5. *A composite integer n is Chebyshev if and only if n is odd, squarefree, and every prime divisor p of n satisfies one of the following:*

$$p-1 \mid n+1 \quad \textit{and} \quad p+1 \mid n-1 \tag{2}$$
$$p-1 \mid n-1 \quad \textit{and} \quad p+1 \mid n+1 \tag{3}$$
$$p-1 \mid n-1 \quad \textit{and} \quad p+1 \mid n-1 \tag{4}$$
$$p-1 \mid n+1 \quad \textit{and} \quad p+1 \mid n+1 \tag{5}$$

There are four basic divisibility conditions that appear in pairs in Theorem 5, which are important in this paper.

Lemma 6. *For any odd integer $n \geq 3$, the factorization in $\mathbb{Z}[x]$ holds:*

$$T_n(x) - x = -2(1-x^2)U_{\frac{n-1}{2}}(x)U_{\frac{n-3}{2}}(x)\,. \tag{6}$$

Proof. Let $x = \cos(\theta)$. The Chebyshev polynomials may be represented as

$$T_n(\cos\theta) = \cos(n\theta) \quad \text{and} \quad U_n(x) = \frac{\cos[(n+1)\theta]}{\sin(\theta)}.$$

Using well-known trigonometric identities we have

$$T_n(x) - x = \cos(n\theta) - \cos(\theta) = -2\sin\left(\frac{(n+1)\theta}{2}\right)\sin\left(\frac{(n-1)\theta}{2}\right)$$
$$= -2\left(1-\cos^2(\theta)\right)\frac{\sin\left(\frac{(n+1)\theta}{2}\right)}{\sin(\theta)}\frac{\sin\left(\frac{(n-1)\theta}{2}\right)}{\sin(\theta)}$$
$$= -2\left(1-x^2\right)U_{\frac{n-1}{2}}(x)U_{\frac{n-3}{2}}(x). \quad \square$$

Lemma 7. *If p is an odd prime divisor of n, then the roots of $T_n(x) - x$ in $\mathbb{Z}/p\mathbb{Z}$ are simple.*

Proof. Using a well-known composition property [12, Example 1.1.6], and then Theorem 3, we have

$$T_n(x) = T_p(T_{\frac{n}{p}}(x)) \equiv T_{\frac{n}{p}}(x)^p \bmod p,$$

and so the derivative of $T_n(x) - x$, in $\mathbb{Z}/p\mathbb{Z}$, is -1, and therefore nonzero. □

It follows that if n is odd, for any a, we must have $U_{\frac{n-1}{2}}(a) \not\equiv 0 \bmod n$ or $U_{\frac{n-3}{2}}(a) \not\equiv 0 \bmod n$. When both are nonzero, a is a witness, even though the product $U_{\frac{n-1}{2}}(a)U_{\frac{n-3}{2}}(a)$ may be zero in $\mathbb{Z}/n\mathbb{Z}$.

The following lemma describes a profound property of the greatest common divisor of two Chebyshev polynomials of the second kind.

Lemma 8. *For any two nonnegative integers m and n,*

$$\gcd(U_m(x), U_n(x)) = U_{g-1}(x),$$

where $g = \gcd(m+1, n+1)$.

Proof. This identity appears as Theorem 4 in [11], and as equation (5.33) in [12]. □

4. Divisible by a Square

In this section we show that if n is an odd composite containing a square factor, then the majority (at least two thirds) of numbers are witnesses.

Lemma 9. *Let $f(x)$ be a polynomial over Z, and for $n \geq 2$, let $N(n)$ denote the number of solutions of $f(x) \equiv 0 \bmod n$. Then $N(n) = \prod_{i=1}^{k} N(p_i^{e_i})$, where $n = p_1^{e_1} \ldots p_k^{e_k}$ is the canonical factorization of n.*

Proof. This is Theorem 2.18 in [8]. □

Lemma 10. *If a polynomial f has no repeated roots in $\mathbb{Z}/p\mathbb{Z}$, then there are at most p solutions to $f(x) \equiv 0 \bmod p^k$.*

Proof. This is a well known property. □

Lemma 11. *Let $n \geq 3$ be an odd composite integer divisible by $p_1^{e_1}, p_2^{e_2}, \ldots, p_j^{e_j}$ where the p_i are primes and $e_i \geq 2$. Then at most*

$$\frac{n}{p_1^{e_1-1} p_2^{e_2-1} \ldots p_j^{e_j-1}}$$

of the numbers in $\mathbb{Z}/n\mathbb{Z}$ are roots of $T_n(x) - x$.

Proof. Without loss of generality, assume $n = p_1^{e_1} \ldots p_k^{e_k}$, and assume that the first j prime powers are greater than one. Let $f = T_n(x) - x$. By Lemma 7, f has no repeated roots in $\mathbb{Z}/p_i\mathbb{Z}$, and so by Lemma 9 and Lemma 10 the number of roots of f is at most

$$\prod_{i=1}^{k} p_i = \frac{p_1^{e_1} \ldots p_k^{e_k}}{p_1^{e_1-1} \ldots p_j^{e_j-1}} = \frac{n}{p_1^{e_1-1} \ldots p_j^{e_j-1}}. \qquad \square$$

Lemma 12. *Let $n \geq 3$ be an odd composite integer which is not square-free. Then at most $\frac{1}{3}$ of the members of $\mathbb{Z}/n\mathbb{Z}$ are roots of $T_n(x) - x$.*

Proof. This follows from Lemma 11 since there must be some prime $p \geq 3$ and $e \geq 2$ for which $p^e \mid n$. □

Note that when n is odd and not prime, there must exist witnesses. If n contains a square factor then by Lemma 12, there exist numbers a which are not roots of $T_n(x) - x$. If n is square free, the quadratic factor in (6) has exactly two roots over each prime field $\mathbb{Z}/p\mathbb{Z}$. Thus if n has k prime factors, the quadratic factor, by Lemma 9, has 2^k roots in $\mathbb{Z}/n\mathbb{Z}$. Since n is a composite, $k \geq 2$ and so at least four numbers in $\mathbb{Z}/n\mathbb{Z}$ are roots. By Lemma 7, these cannot also be roots of $U_{\frac{n-1}{2}}(x)$ or $U_{\frac{n-3}{2}}(x)$. Hence there must exist at least two witnesses in I_n.

5. Square-free Case

From Lemma 12, we see that odd composite integers that are not square-free have an abundance of witnesses. In fact, the witnesses can be found without even having to examine the factors of $T_n(x) - x$. Therefore we now restrict our attention to odd square-free composites $n = p_1 p_2 \ldots p_k$. For each prime p_i, let α_i be the *ratio* of numbers in $\mathbb{Z}/p_i\mathbb{Z}$ that are roots of $U_{\frac{n-1}{2}}(x)$ and let β_i be the ratio of numbers in $\mathbb{Z}/p_i\mathbb{Z}$ that are roots of $U_{\frac{n-3}{2}}(x)$. Note that since $1, -1$ are not roots of either Chebyshev, $0 \leq \alpha_i, \beta_i \leq \frac{p_i-2}{p_i}$. Then in $\mathbb{Z}/p_i\mathbb{Z}$, $U_{\frac{n-1}{2}}(a)$ has

$\alpha_i p_i$ roots and $U_{\frac{n-3}{2}}(a)$ has $\beta_i p_i$ roots. So by Lemma 7, $U_{\frac{n-1}{2}}(x)U_{\frac{n-3}{2}}(x)$ has $(\alpha_i + \beta_i)p_i$ roots in $\mathbb{Z}/p_i\mathbb{Z}$. By Lemma 9, the total number of roots in $\mathbb{Z}/n\mathbb{Z}$ is

$$\prod_{i=1}^{k}(\alpha_i + \beta_i)p_i = n\prod_{i=1}^{k}(\alpha_i + \beta_i),$$

which is also the number of roots in I_n since there are no repeated roots. It is helpful to define

$$\rho(n) = \prod_{i=1}^{k}(\alpha_i + \beta_i), \tag{7}$$

the ratio of numbers in $\mathbb{Z}/n\mathbb{Z}$ that are roots of either $U_{\frac{n-1}{2}}(x)$ or $U_{\frac{n-3}{2}}(x)$.

Recall that the resultant of two polynomials $f(x)$ and $g(x)$ over Z, denoted $\mathrm{res}(f(x), g(x))$, is the determinant of their Sylvester matrix and is zero if and only if they share a common factor of positive degree. Therefore if one factors out their greatest common divisor, the resultant must be nonzero. The following lemma says that with Chebyshev polynomials of the second kind, the resultant is, to within a sign, a power of two.

Lemma 13. *For any m and n, $res(\frac{U_m}{h}, \frac{U_n}{h}) = \pm 2^i$ for some i, where $h = \gcd(U_m, U_n)$.*

Proof. This may be proven by induction on $\max\{m, n\}$. □

Lemma 14. *Let $a(x), b(x) \in \mathbb{Z}[x]$, and let p be a prime not dividing the leading coefficients of $a(x)$ and $b(x)$. Let $c(x) = \gcd(a(x), b(x))$. If $p \nmid res(\frac{a(x)}{c(x)}, \frac{b(x)}{c(x)})$, then in $(\mathbb{Z}/p\mathbb{Z})[x]$, $\gcd(\phi_p(a), \phi_p(b)) = \phi_p(c)$.*

Proof. This is Lemma 4.2.2.b in [13]. □

Lemma 15. *Let n and m be nonnegative integers, and p an odd prime. Let*

$$\begin{aligned} d(x) &= \gcd\left(U_n(x), U_m(x)\right) \in \mathbb{Z}[x] \\ d_p(x) &= \gcd\left(\phi_p(U_n(x)), \phi_p(U_m(x))\right) \in (\mathbb{Z}/p\mathbb{Z})[x] \end{aligned}$$

Then

(a) $d_p(x) = \phi_p(d)$;

(b) $\deg(d) = \deg(d_p)$.

Proof. It is easy to show, using equation (1), that the leading coefficient of each $U_n(x)$ is a power of two. By Lemma 13, $\mathrm{res}(\frac{U_m}{h}, \frac{U_n}{h})$ is also a power

of two, to within a sign. Since p is odd, part (a) follows by Lemma 14. It is easy to show that p does not divide the leading coefficient of $d(x)$, and so $\deg(d) = \deg(\phi_p(d))$, and so (b) follows from (a). □

Lemma 16. *Let n be a positive odd integer and let p be a prime divisor of n.*

$$p-1 \mid n-1 \iff U_{\frac{p-3}{2}}(x) \mid U_{\frac{n-3}{2}}(x)\,, \tag{8}$$

$$p+1 \mid n-1 \iff U_{\frac{p-1}{2}}(x) \mid U_{\frac{n-3}{2}}(x)\,, \tag{9}$$

$$p-1 \mid n+1 \iff U_{\frac{p-3}{2}}(x) \mid U_{\frac{n-1}{2}}(x)\,, \tag{10}$$

$$p+1 \mid n+1 \iff U_{\frac{p-1}{2}}(x) \mid U_{\frac{n-1}{2}}(x)\,. \tag{11}$$

Proof. We will prove relation (10), and the other arguments are similar. If $p-1 \mid n+1$, then since both $p-1$ and $n+1$ are even we must have $\frac{p-1}{2} \mid \frac{n+1}{2}$. Thus $\frac{p-1}{2} = \gcd(\frac{p-1}{2}, \frac{n+1}{2})$. By Lemma 8 it follows that $U_{\frac{p-3}{2}}(x) = \gcd(U_{\frac{p-3}{2}}(x), U_{\frac{n-1}{2}}(x))$. Conversely, $U_{\frac{p-3}{2}}(x) = \gcd(U_{\frac{p-3}{2}}(x), U_{\frac{n-1}{2}}(x))$ implies by Lemma 8 that $\frac{p-1}{2} = \gcd(\frac{p-1}{2}, \frac{n+1}{2})$, which implies $p-1 \mid n+1$. □

We are interested in the number of roots that the polynomials $U_{\frac{n-1}{2}}(x)$ and $U_{\frac{n-3}{2}}(x)$ have in $\mathbb{Z}/p\mathbb{Z}$ for each prime divisor p of n. We define the following polynomials in $(\mathbb{Z}/p\mathbb{Z})[x]$,

$$\begin{aligned} g_{rr} &= \gcd(\phi_p(U_{\frac{p-3}{2}}), \phi_p(U_{\frac{n-3}{2}}))\,, \\ g_{lr} &= \gcd(\phi_p(U_{\frac{p-1}{2}}), \phi_p(U_{\frac{n-3}{2}}))\,, \\ g_{rl} &= \gcd(\phi_p(U_{\frac{p-3}{2}}), \phi_p(U_{\frac{n-1}{2}}))\,, \\ g_{ll} &= \gcd(\phi_p(U_{\frac{p-1}{2}}), \phi_p(U_{\frac{n-1}{2}})) \end{aligned}$$

and let $d_{rr}, d_{lr}, d_{rl}, d_{ll}$ denote, respectively, their degrees. Consider a root a for $U_{\frac{n-1}{2}}(x)$ in $\mathbb{Z}/p\mathbb{Z}$. This is also a root of either $U_{\frac{p-1}{2}}(x)$ or $U_{\frac{p-3}{2}}(x)$ since the polynomial $U_{\frac{p-1}{2}}(x)U_{\frac{p-3}{2}}(x)$ factors completely in $\mathbb{Z}/p\mathbb{Z}$. Therefore the number of roots of $U_{\frac{n-1}{2}}(x)$ mod p is exactly $d_{rl} + d_{ll}$, and the number of roots of $U_{\frac{n-3}{2}}(x)$ mod p is exactly $d_{rr} + d_{lr}$. Now consider the following polynomials in $\mathbb{Z}[x]$:

$$h_{rr} = \gcd(U_{\frac{p-3}{2}}, U_{\frac{n-1}{2}})\,, \tag{12}$$

$$h_{lr} = \gcd(U_{\frac{p-1}{2}}, U_{\frac{n-3}{2}})\,, \tag{13}$$

$$h_{rl} = \gcd(U_{\frac{p-3}{2}}, U_{\frac{n-3}{2}})\,, \tag{14}$$

$$h_{ll} = \gcd(U_{\frac{p-1}{2}}, U_{\frac{n-1}{2}})\,. \tag{15}$$

By Lemma 15, their degrees are exactly $d_{rr}, d_{lr}, d_{rl}, d_{ll}$. It now follows that

Lemma 17. *Let n be an odd composite with prime divisor p, and let $d_{rr}, d_{lr}, d_{rl}, d_{ll}$ denote the degrees of the polynomials in (12)–(15). Then modulo p,*

1. *$U_{\frac{n-1}{2}}(x)$ has $d_{rl} + d_{ll}$ roots;*
2. *$U_{\frac{n-3}{2}}(x)$ has $d_{rr} + d_{lr}$ roots.*

Lemma 18. *Let $0 < k < m$, $d(x) = \gcd(U_k(x), U_m(x))$, and assume $U_k(x) \nmid U_m(x)$. Then*

(a) $\deg(d) < \frac{k}{2}$;

(b) if k is even, then $\deg(d) < \frac{k}{3}$.

Proof. By Lemma 8, $d(x) = U_{g-1}(x)$ where $g = \gcd(m+1, k+1)$. If $U_k(x) \nmid U_m(x)$, then $U_{g-1}(x) \neq U_k(x)$, and hence $g \neq k+1$. But since $g \mid k+1$, $g \leq \frac{k+1}{2}$ and so $g - 1 < \frac{k}{2}$, establishing *(a)*. If k is even then $k+1$ is odd and so $g \leq \frac{k+1}{3}$, establishing *(b)*. □

Lemma 19. *Let n be an odd composite with prime divisor p. Then*

$$p - 1 \nmid n - 1 \implies d_{rr} < \frac{p}{4}, \tag{16}$$

$$p + 1 \nmid n - 1 \implies d_{lr} < \frac{p}{4}, \tag{17}$$

$$p - 1 \nmid n + 1 \implies d_{rl} < \frac{p}{4}, \tag{18}$$

$$p + 1 \nmid n + 1 \implies d_{ll} < \frac{p}{4}. \tag{19}$$

If $\frac{p-3}{2}$ is even, then the bound in (16) and (18) may be replaced by $\frac{p}{6}$. If $\frac{p-1}{2}$ is even, then the bound in (17) and (19) may be also replaced by $\frac{p}{6}$.

Proof. This follows from Lemma 16 and Lemma 18. □

Lemma 20. *Let n be a squarefree composite which is the product of at least three primes, and assume that for some a and a', we have $U_{\frac{n-1}{2}}(a) \equiv 0 \bmod n$ and $U_{\frac{n-3}{2}}(a') \equiv 0 \bmod n$. Then $\rho(n) \leq \frac{7}{16}$.*

Proof. Let p be a prime divisor of n. Since $U_{\frac{n-1}{2}}(x)$ has a root, at least one of conditions (8) and (9) must fail, for otherwise $U_{\frac{n-3}{2}}(x)$ would contain all $p-2$ of the roots in $\mathbb{Z}/p\mathbb{Z}$, and $U_{\frac{n-1}{2}}(x)$ could not have a root in $\mathbb{Z}/n\mathbb{Z}$.

Thus, by Lemma 19 either (16) or (17) holds, so the number of roots, modulo p, of $U_{\frac{n-3}{2}}(x)$ is $d_{rr} + d_{lr} < \frac{3}{4}p$. That is, $\beta_p < \frac{3}{4}$. A similar argument shows that since $U_{\frac{n-3}{2}}(x)$ has a root, we must have $\alpha_p < \frac{3}{4}$. Since these numbers are between 0 and $\frac{3}{4}$, we have

$$\rho = \prod_{i=1}^{k} \alpha_i + \prod_{i=1}^{k} \beta_i \leq \alpha_1\alpha_2\alpha_3 + \beta_1\beta_2\beta_3.$$

It is sufficient to obtain a bound on the real valued function $\rho = \alpha_1\alpha_2\alpha_3 + \beta_1\beta_2\beta_3$, with constraints

$$0 \leq \alpha_i, \beta_i < \frac{3}{4} \qquad \text{and} \qquad \alpha_i + \beta_i \leq 1.$$

But since the values are nonnegative, ρ is bounded by

$$\rho_1 = \alpha_1\alpha_2\alpha_3 + (1-\alpha_1)(1-\alpha_2)(1-\alpha_3).$$

So we seek a bound on ρ_1, on the region defined by $\frac{1}{4} \leq \alpha_1, \alpha_2, \alpha_3 \leq \frac{3}{4}$. Since

$$\nabla\rho_1 = (\alpha_2 + \alpha 3 - 1, \alpha_1 + \alpha_3 - 1, \alpha_1 + \alpha_2 - 1)$$

there is only one point on the interior, namely $\alpha_1 = \alpha_2 = \alpha_3 = .5$, where the gradient is zero, and this happens to be a minimum. The maximum must be achieved on the border. It is straightforward to check that ρ_1 has a maximum value of $\frac{7}{16}$, when either $\alpha_1 = \alpha_2 = \alpha_3 = \frac{3}{4}$ or $\alpha_1 = \alpha_2 = \alpha_3 = \frac{1}{4}$. □

Lemma 21. *Let n be any odd squarefree integer. Then for less than half the $a \in \mathbb{Z}/n\mathbb{Z}$, we have $\left(\frac{a^2-1}{n}\right) = 1$, and for less than half the $a \in \mathbb{Z}/n\mathbb{Z}$, we have $\left(\frac{a^2-1}{n}\right) = -1$.*

Proof. The proof is by induction on the number of prime factors in $n = p_1 \dots p_k$. For $k = 1$, this is Theorem 1. Assume $k > 1$, and that the result holds for fewer than k factors. Define $S_n^+ = \{a \in \mathbb{Z}/n\mathbb{Z} | \left(\frac{a^2-1}{n}\right) = 1\}$ and $S_n^- = \{a \in \mathbb{Z}/n\mathbb{Z} | \left(\frac{a^2-1}{n}\right) = -1\}$. It is well-known that if $\gcd(l, m) = 1$ and $n = l * m$ then the function $a \longmapsto (a \bmod l, a \bmod m)$ is a bijection between Z_n and $Z_l \times Z_m$. Using this identification and well-known relations for the Jacobi, one can show, where $l = p_1 \dots p_{k-1}$, that

$$S_n^+ = (S_l^+ \times S_{p_k}^+) \cup (S_l^- \times S_{p_k}^-), \quad S_n^- = (S_l^+ \times S_{p_k}^-) \cup (S_l^- \times S_{p_k}^+).$$

Therefore, we see that

$$|S_n^+| = |S_l^+ \times S_{p_k}^+| + |S_l^- \times S_{p_k}^-| = |S_l^+| \times |S_{p_k}^+| + |S_l^-| \times |S_{p_k}^-|.$$

Using the induction hypothesis, it follows that $|S_n^+| < \frac{lp_k}{4} + \frac{lp_k}{4} = \frac{n}{2}$. A similar argument shows $|S_n^-| < \frac{n}{2}$. □

Lemma 22. *Let n be an odd squarefree composite and assume that for*

all a $U_{\frac{n-1}{2}}(a) \not\equiv 0 \bmod n$*, or for all a* $U_{\frac{n-3}{2}}(a) \not\equiv 0 \bmod n$*. Then at least half of the numbers* $a \in \mathbb{Z}/n\mathbb{Z}$ *are witnesses.*

Proof. Without loss of generality, assume that for all a $U_{\frac{n-1}{2}}(a) \not\equiv 0 \bmod n$. If $U_{\frac{n-3}{2}}(a)$ has fewer than $\frac{n}{2}$ roots we are done. Otherwise, assume $U_{\frac{n-3}{2}}(a)$ has $r > \frac{n}{2}$ roots. By Lemma 21, fewer than $\frac{n}{2}$ of these roots a can have $\left(\frac{a^2-1}{n}\right) = 1$, and so the rest must be witnesses. □

6. Product of Two Primes

Here we obtain a bound on $\rho(n)$, when n is the product of two distinct primes. There are two cases, depending on whether or not the primes are twin. The following can be easily verified.

Lemma 23. *If* p *is a divisor of* n *then*

$$p-1 \mid \frac{n}{p} - 1 \Longleftrightarrow p-1 \mid n-1\,, \tag{20}$$

$$p+1 \mid \frac{n}{p} + 1 \Longleftrightarrow p+1 \mid n-1\,, \tag{21}$$

$$p-1 \mid \frac{n}{p} + 1 \Longleftrightarrow p-1 \mid n+1\,, \tag{22}$$

$$p+1 \mid \frac{n}{p} - 1 \Longleftrightarrow p+1 \mid n+1\,. \tag{23}$$

Lemma 24. *Let* $n = pq$ *for odd primes* p *and* q*, where* $p < q$*. Then*

(a) $q-1 \nmid n-1$*;*

(b) $q-1 \nmid n+1$*, if* $q \neq p+2$*;*

(c) $q+1 \nmid n+1$*;*

(d) $q+1 \nmid n-1$*;*

(e) $p-1 \nmid n+1$ *if* $q = p+2$ *and* $p \neq 3, 5$*;*

Proof. To see *(a)*, suppose $q-1 \mid n-1$. Then by (20), we must have $q-1 \mid \frac{n}{q} - 1$. But this is impossible since $\frac{n}{q} - 1 = p - 1 < q - 1$. In a similar way, relation (23) proves *(c)*, and relation (21) proves *(d)*. Relation (22) proves *(b)*, provided $\frac{n}{q} + 1 = p + 1 < q - 1$. To see *(e)*, note that $n + 1 = pq + 1 = (p-1)(q+1) + (q-p+2)$. This remainder is exactly four if p and q are twin primes, and is strictly less than $p-1$ provided $p > 5$. □

Lemma 25. *Let $n = pq$, $p < q$, where p and q are any odd non-twin primes. Then $\rho(n) \leq \frac{5}{12}$.*

Proof. By Lemma 24, none of the four divisibility conditions can occur for q. Therefore, by Lemma 17 and Lemma 19, $U_{\frac{n-1}{2}}(x)$ gets at most $\frac{q}{4}$ roots from each of $U_{\frac{q-3}{2}}(x)$, and $U_{\frac{q-1}{2}}(x)$, as does $U_{\frac{n-3}{2}}(x)$. However, as exactly one of the indices $\frac{q-1}{2}$ and $\frac{q-3}{2}$, is even, Lemma 19 implies that the corresponding polynomial can contribute only $\frac{q}{6}$ of the roots to each of $U_{\frac{n-1}{2}}(x)$ and $U_{\frac{n-3}{2}}(x)$. Thus $\alpha_q, \beta_q \leq \frac{1}{4}+\frac{1}{6} = \frac{5}{12}$. But $\rho(n) = \alpha_p\alpha_q+\beta_p\beta_q \leq \frac{5}{12}\alpha_p+\frac{5}{12}(1-\alpha_p) = \frac{5}{12}$. □

Lemma 26. *Let $n = pq$, where p and q are twin primes. Then $\rho(n) \leq \frac{5}{8}$.*

Proof. One can verify the result when $n = 3 \cdot 5$ and $n = 5 \cdot 7$, so assume $5 < p < q$. Using Lemma 24, we see that $q-1 \nmid n-1$, $q+1 \nmid n+1$, $q+1 \nmid n-1$, and $p-1 \nmid n+1$. Using reasoning similar to that used in the previous lemma, we must have $\alpha_q, \alpha_p \leq .75$ and $\beta_q \leq .5$. We consider the function

$$\alpha_p\alpha_q + \beta_p\beta_q$$

subject to

$$\begin{aligned} 0 &\leq \alpha_p, \alpha_q \leq .75\,, \qquad 0 \leq \beta_q \leq .5\,, \\ 0 &\leq \beta_p \leq 1-\alpha_p\,, \qquad 0 \leq \beta_q \leq 1-\alpha_q\,. \end{aligned}$$

Using an argument similar to that used in Lemma 20, it can be shown that this function achieves a maximum when $\alpha_p = \alpha_q = \frac{3}{4}$ and $\beta_p = \beta_q = \frac{1}{4}$. Hence $\rho(n) \leq \frac{5}{8}$. □

7. Proof of Main Theorem

Consider our algorithm in Figure 1. After selecting a random a, we first determine if a is a root of either polynomial. If the algorithm returns in lines 3, 4 or 5, then the result is certain because a is a witness. If the algorithm returns *fail* in line 7, it is because no witness was found. We consider the probability of this happening, when n is composite. Let $\omega(n)$ denote the ratio of nonwitnesses in $\mathbb{Z}/n\mathbb{Z}$. There are five cases.

(a) *n has a square factor:* By Lemma 12, $\omega(n) \leq \frac{1}{3}$.

(b) *n is a product of two non-twin primes:* By Lemma 25, $\omega(n) \leq \frac{5}{12}$.

(c) *n is a square free product of at least three primes with roots in both factors:* By Lemma 20, $\omega(n) \leq \frac{7}{16}$.

(d) *n is the product of two twin primes:* By Lemma 26, $\omega(n) \leq \frac{5}{8}$.

(e) *n has roots in only one factor:* By Lemma 22 $\omega(n) \leq \frac{1}{2}$.

If ω is the ratio of nonwitnesses in $\mathbb{Z}/n\mathbb{Z}$ then $\omega(\frac{n}{n-2})$ is the ratio of witnesses over I_n, which we approximate with ω for large n. Given this simplification, Theorem 2 follows.

8. Behavior with Chebyshev Numbers

Consider the first Chebyshev number, $7056721 = 7 \cdot 47 \cdot\ 89 \cdot 241$. One of its prime factors, $p = 47$, satisfies condition (2), which is equivalent to conditions (21) and (22), or (9) and (10). Therefore $\alpha_p = \frac{23}{47}$ and $\beta_p = \frac{22}{47}$. The other three prime factors ($p = 7, 89, 241$) each satisfy condition (4), which is equivalent to conditions (20) and (21), or (8) and (9). Hence for these three primes p, $\alpha_p = 0$ and $\beta_p = \frac{5}{7}, \frac{87}{89}, \frac{239}{241}$, respectively. Therefore $\rho(n) = \frac{5}{7} \cdot \frac{22}{47} \cdot \frac{87}{89} \cdot \frac{239}{241} \approx .32$, and *all roots* are zeros of $U_{\frac{n-3}{2}}(x)$.

Most of the arguments have involved bounding the number of roots that an odd composite can have. However, there exist certain composite numbers having a large number of roots, in only one of the Chebyshev factors. Let us say that a composite number n is *right Chebyshev* if for each prime divisor p, both conditions (8) and (9) hold. A right Chebyshev number will have $\prod_{p|n}(p-2)$ roots of $U_{\frac{n-3}{2}}(x)$. It can easily shown that the rigid Carmichael numbers of order two [6] are right Chebyshev numbers. One example constructed by Howe is:

$31 \cdot 37 \cdot 101 \cdot 103 \cdot 109 \cdot 199 \cdot 419 \cdot 449 \cdot 521 \cdot 571 \cdot 911 \cdot 2089 \cdot 2551 \cdot 5851 \cdot 11969$

Here, $\rho(n) = \prod_{p|n} \frac{p-2}{p} \approx .809$.

Similarly, we will call n a *left Chebyshev* number if for each prime divisor p, both conditions (10) and (11) hold. A left Chebyshev number will have exactly $\prod_{p|n}(p-2)$ roots in I_n, all roots of $U_{\frac{n-1}{2}}(x)$. For example,

$$n = 43 \cdot 109 \cdot 199 \cdot 233 \cdot 349 \cdot 449 \cdot 521 \cdot 571 \cdot 701 \cdot 3191 \cdot 5851$$

is left Chebyshev number, and one finds $\rho(n) \approx .899$. Since left and right Chebyshev numbers can have more than 50% roots, the existence of witnesses depends heavily on roots having the wrong Jacobi.

9. Fast Evaluation

Since the calculation of the Jacobi $\left(\frac{a^2-1}{n}\right)$ can be done in $O(\log^2 n)$ time [3, p. 98], the running time of our algorithm is dominated by the evaluation of the polynomials $U_{\frac{n-1}{2}}(a)$ and $U_{\frac{n-3}{2}}(a)$ modulo n. We adapt a fast matrix exponentiation method of Fee and Monagan [4] as follows. The recurrence relation (1) may be written as

$$\begin{bmatrix} U_k(x) \\ U_{k+1}(x) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2\,x \end{bmatrix} \begin{bmatrix} U_{k-1}(x) \\ U_k(x) \end{bmatrix},$$

which can be repeated to yield

$$\begin{bmatrix} U_k(x) \\ U_{k+1}(x) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2\,x \end{bmatrix}^k \begin{bmatrix} U_0(x) \\ U_1(x) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2\,x \end{bmatrix}^k \begin{bmatrix} 1 \\ 2x \end{bmatrix}.$$

Thus we compute in $\mathbb{Z}/n\mathbb{Z}$ for each a,

$$\begin{bmatrix} U_{\frac{n-3}{2}}(a) \\ U_{\frac{n-1}{2}}(a) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 2\,a \end{bmatrix}^{\frac{n-3}{2}} \begin{bmatrix} 1 \\ 2a \end{bmatrix}. \tag{24}$$

We can compute (24) using $O(\log(n))$ matrix multiplications in $\mathbb{Z}/n\mathbb{Z}$. Classical matrix multiplication would require eight integer multiplications, four integer additions, and four integer remainder operations (or alternatively, seven multiplications, eighteen additions, and four remainder operations using the Strassen formulas).

As shown in [4], this can be slightly improved, as follows, so that only *five* multiplications, *three* additions, and *two* remainder operations are used. The characteristic polynomial of the matrix A being multiplied in (24) is $\lambda^2-2a\lambda+1$. By the Cayley-Hamilton Theorem, A satisfies this polynomial, and so rather than power the matrix in (24), we can compute $\lambda^{\frac{n-3}{2}}$ modulo this polynomial, obtaining a linear polynomial $f(\lambda) = b_1\lambda + b_0$. Then $A^{\frac{n-3}{2}}$ can be found with $f(A)$. Each basic step involves multiplying two linear polynomials, taking the remainder modulo the quadratic, and then reducing the coefficients modulo n.

Acknowledgements

This research was supported by CNPq Grant 478290/04-7, FAPERGS Grant 06/1001.7, and the Brazilian Fulbright Commission.

References

[1] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P, *Annals of Mathematics*, **160** (2004), 781-793.

[2] T. Bang, Congruence properties of Tchebycheff polynomials, *Mathematica Scandinavica*, **2** (1954), 327-333.

[3] R. Crandall, C. Pomerance, *Prime Numbers, a Computational Perspective*, Second Edition, Springer, New York (2005).

[4] G.J. Fee, M.B. Monagan, Cryptography using Chebyshev polynomials, *Preprint*.

[5] J. Grantham, A probable prime test with high confidence, *J. Number Theory*, **72** (1998), 32-47.

[6] E.W. Howe, Higher order Carmichael numbers, *Math. Comp.*, **69** (2000), 1711-1719.

[7] D.P. Jacobs, M.O. Rayes, Vilmar Trevisan, Characterization of Chebyshev numbers, *Preprint*.

[8] I. Niven, H.S. Zuckerman, *An Introduction to the Theory of Numbers*, Fourth Edition, John Wiley and Sons, New York (1980).

[9] R.G.E. Pinch, Some primality testing algorithms, *AMS Notices*, **40**, No. 9 (1993), 1203-1210.

[10] R.A. Rankin, Chebyshev polynomials and the modular group of level p, *Mathematica Scandinavica*, **2** (1954), 315-326.

[11] M.O. Rayes, V. Trevisan, P.S. Wang, Factorization properties of Chebyshev polynomials, *Computers and Mathematics with Applications*, **50** (2005), 1231-1240.

[12] T.J. Rivlin, *The Chebyshev Polynomials – From Approximation Theory to Algebra and Number Theory*, Second Edition, Pure and Applied Mathematics, Jonh Wiley and Sons, New York (1990).

[13] F. Winkler, *Polynomial Algorithms in Computer Algebra*, Springer-Verlag (1996).