On cyclotomic primality tests

A Thesis Presented for

The Master of Science

Degree

The University of Tennessee, Knoxville

Thomas Francis Boucher

August 2011

I dedicate this work to my parents Anne and Tom for their continual guidance and unending encouragement.

Acknowledgments

I would like to foremost thank my adviser Luís Finotti, without whom this thesis could not have been written. The only thing more vast than his corrections and notes were his patience and optimism.

I would like to thank the members of my committee David Anderson and Charles Collins for graciously reviewing my thesis and serving on my board.

And I would like to thank all of my friends and family, especially my good friend Amanda Diegel.

Abstract

In 1980, L. Adleman, C. Pomerance, and R. Rumely invented the first cyclotomic primality test, and shortly after, in 1981, a simplified and more efficient version was presented by H.W. Lenstra for the Bourbaki Seminar. Later, in 2008, Rene Schoof presented an updated version of Lenstra's primality test. This thesis presents a detailed description of the cyclotomic primality test as described by Schoof, along with suggestions for implementation. The cornerstone of the test is a prime congruence relation similar to Fermat's "little theorem" that involves Gauss or Jacobi sums calculated over cyclotomic fields. The algorithm runs in very nearly polynomial time. This primality test is currently one of the most computationally efficient tests and is used by default for primality proving by the open source mathematics systems Sage and PARI/GP. It can quickly test numbers with thousands of decimal digits.

Contents

Chapter 1

Introduction

Since the time of Fermat, mathematicians have tried to find the most efficient methods for determining the primality of large numbers. Prior to Fermat, the methods of primality testing were derivations of factoring methods, like trial division and the sieve of Eratosthenes. These methods are computationally heavy and often rely on large tables of primes making them practical for only small numbers, 10^7 being a conservative upper bound. For practical implementations of these tests, see §8.1 of [4] and §3.1/3.2 of [7].

A groundbreaking advancement in primality testing came from Pierre de Fermat when he discovered his famous congruence on prime numbers, informally known as Fermat's little theorem.

Theorem 1.0.1. *Let p be a prime number and a a natural number. Then*

$$a^p \equiv a \pmod{p},$$

or, if $(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

This congruence is true for all prime numbers p, but is also true for some composite numbers. Otherwise put, all prime numbers satisfy this congruence, but numbers

satisfying this congruence are not necessarily prime. This is the cornerstone of the first efficient *compositeness tests* (not primality tests!). In general, a compositeness test only returns a verdict if it discovers the input n to be composite. If the test cannot find a witness to the compositeness of n, it returns no absolute verdict. A primality test is different because it returns an absolute verdict whether n is prime or composite. Thus compositeness tests are good for showing that a number is very likely prime, but primality tests are needed for guaranteeing a number is prime.

For example, a simple compositeness test might be trying k different values of a in Theorem 1.0.1. If the congruence fails for a single a, then n is declared composite, and if the congruence is true for all k values, then n is declared possibly prime. However, regardless of the size of k, this test can never guarantee the primality of n! Composite numbers exist that satisfy this congruence for every natural number. These numbers are known as *Carmichael numbers*.

To have a proper compositeness test that was not susceptible to the Carmichael number defect, a stronger version of Fermat's theorem was needed. In [18], R. Solovay and V. Strassen presented such a compositeness test. It utilized the following theorem.

Theorem 1.0.2. *Let n be an odd prime number, and let a be a natural number such that $a \not\equiv 0 \pmod{n}$. Then*

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \equiv \pm 1 \pmod{n},$$

where $\left(\frac{a}{n}\right)$ denotes the Legendre symbol, defined to be 1 if a is a quadratic residue modulo n, -1 if a is a quadratic nonresidue modulo n, and zero if $n \mid a$.

The test involved verifying the congruence for different base values a. If the congruence failed for a single a, then n would be declared composite. It was shown that for an odd composite number n, at most half of all $a \in \{1, 2, \ldots, n-1\}$ satisfied this congruence. Thus, if the congruence held for many values of a, the number tested n was declared very likely prime.

Shortly after this discovery, in [16], Michael Rabin described what has spawned the most efficient compositeness test, the Miller-Rabin test. The test was similar in form to the other tests we have seen. It relies on the following congruence.

Theorem 1.0.3. *Let n be an odd prime, and write $n-1$ as $2^s \cdot d$, where s and d are positive integers and d is odd. Then for $a \in (\mathbb{Z}/n\mathbb{Z})^*$, either*

$$a^d \equiv 1 \pmod{n}$$

or

$$a^{2^r \cdot d} \equiv -1 \pmod{n}$$

for some $0 \leq r \leq s-1$.

The test procedure was similar to the Solovay-Strassen test. Many different base values of a were verified, and the more values verified, the more likely it was that the number tested n was prime. However, the Miller-Rabin test was more efficient. It was shown that for an odd composite number n, at most one quarter of all $a \in (\mathbb{Z}/n\mathbb{Z})^*$ satisfied these congruences.

Although the Miller-Rabin test and its variants are very efficient at showing compositeness, it is sometimes necessary to know for certain the compositeness or primality of a number.

Efficient large number primality tests were known since the end of the 19^{th} century, but these tests relied on a constrained input. For example, to test the primality of a number n, the most common requirement was the known factorization or partial factorization of $n-1$ or $n+1$. In 1876, Éduardo Lucas proved the following theorem.

Theorem 1.0.4. *If a, n are integers with $n > 1$, and $a^{n-1} \equiv 1 \pmod{n}$, but $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for every prime q that divides $n-1$, then n is prime.*

For a complete proof, see [7] p. 173. This theorem was later adapted by Derrick Lehmer in [11] to create the Lucas-Lehmer primality test. While variants of the

test are still used to find the largest known Mersenne primes, primes of the form $2^p - 1$, they are not effective as general-purpose primality tests. However, it is worth noting, [3] described a very effective primality test that was a combination of the Lucas-Lehmer primality test and the cyclotomic primality test.

The cyclotomic primality test, first described by L. Adleman, C. Pomerance, and R. Rumley in [1], was the first modern general-purpose primality test. With an expected running time bounded by $(\log n)^{c \log\log\log n}$, where n is the number tested and c is an effectively computable constant, this was the first primality test that could routinely test numbers with thousands of decimal digits [15]. The invention of the cyclotomic primality test was a major breakthrough in computational number theory.

The test relied on a Fermat-like congruence that involved Jacobi sums calculated over cyclotomic fields. Like the compositeness tests before it, if the number tested n did not fulfill the congruence, it was declared composite. But unlike the compositeness tests, if n satisfied the congruence for all tested values, then it only took a few more steps to prove that n was prime. This primality test is now informally known as the APR primality test.

Two versions of the APR algorithm were originally presented, a completely deterministic version and a probabilistic version. The deterministic version was theoretically interesting, but the probabilistic version was simpler and more practical. One should not be confused, both versions were genuine primality tests (i.e., the probabilistic version is *not* a compositeness test!) and both had the same computational time complexity bound. The only difference was the variable running time of the probabilistic algorithm.

Shortly after the invention of the APR primality test, in [5], H. Cohen and H. W. Lenstra described an improved and simplified version of the cyclotomic primality test. Like the APR test, two versions of the test were presented, one utilizing Gauss sums and the other Jacobi sums. Both versions used a Fermat-like congruence to create a small list of possible divisors that could be manually checked for divisibility. The Gauss sum version of the test required calculations in a larger finite ring, whereas the

Jacobi sum version required calculations in a smaller finite ring, making the Jacobi sum test more practical. This primality test is now informally known as the APRCL primality test, and is currently the default primality proving test used by the open source mathematics software projects Sage and PARI/GP.

In [17], René Schoof presented an updated version of the APRCL primality test. Schoof's primality test is the topic of this thesis. Like Cohen and Lenstra, Schoof presented a Gauss sum and Jacobi sum version of the test. Schoof focused mostly on the Gauss sum test, and so this thesis will also focus on the Gauss sum version. We will describe the primality test from a theoretical and a practical viewpoint.

For the sake of completeness, it should be mentioned that the most commonly used alternative to the cyclotomic primality test is the elliptic curve primality (ECP) test. H.W. Lenstra first described using elliptic curves for prime factoring in 1985, and in 1986, S. Goldwasser and J. Killian extended this work to primality testing. The largest advantage of the ECP test was its ability to produce for n a quickly verifiable certificate of primality (or compositeness). Primality certificates allow the primality of n to be rapidly checked with limited resources. For further details, see [8].

Lastly, the most recent innovation to primality testing was the (truly) polynomial time AKS algorithm first described by M. Agrawal, N. Kayal, and N. Saxena in 2002. More efficient variants of the algorithm were quickly published by many others, most notably [14]. Although this variant boasted a time of $(\log n)^6 \cdot (2 + \log\log n)^c$, where c is an effectively computable real number, in practice, the AKS algorithm has yet to yield a computationally effective test.

Chapter 2

Background

2.1 Essentials in Algebra

Definition 2.1.1. An *algebraic number* is a complex number α that is a root of a polynomial

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0, \text{ where } a_i \in \mathbb{Q} \text{ and } a_0 \neq 0.$$

An *algebraic integer* is a complex number β that is a root of a polynomial

$$x^n + b_1x^{n-1} + b_2x^{n-2} + \cdots + b_n = 0, \text{ where } b_i \in \mathbb{Z}.$$

Definition 2.1.2. An *algebraic number field* is a finite field extension of the field of rationals, e.g., $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. (One can easily show that the elements of an algebraic extension are algebraic.)

Given an algebraic number field K, the algebraic integers contained in K form a commutative ring $\mathcal{O}_K$, called the *ring of integers in* K.

Proposition 2.1.3. *The group of units* $(\mathbb{Z}/p\mathbb{Z})^*$ *is cyclic and of order* $p-1$*, where* p *is a prime number.*

For a complete proof, see [10] p. 39-40.

Definition 2.1.4. Let $a, n \in \mathbb{Z}$. Then a is a *primitive root modulo* n if the residue class of a modulo n generates the group of units $(\mathbb{Z}/n\mathbb{Z})^*$.

Theorem 2.1.5 (Fundamental Theorem of Finitely-Generated Abelian Groups)**.** *Every finitely generated abelian group is a direct sum of cyclic groups of prime power orders and of a free abelian group.*

For a complete proof, see [2] p. 472-3.

Example 2.1.6. The finitely-generated abelian group $\mathbb{Z}/120\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z}$ can be written as the direct sum $\mathbb{Z}/2^2\mathbb{Z} \oplus \mathbb{Z}/2^3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3^2\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

2.2 Cyclotomic Fields

Definition 2.2.1. A complex number ζ is called an *n-th root of unity* if it satisfies the equation $\zeta^n - 1 = 0$ for some integer $n > 0$. If n is the least positive integer with this property, then ζ is called a *primitive n-th root of unity.* Throughout this thesis we denote $\zeta_n = \mathrm{e}^{2\pi \mathrm{i}/n}$.

Example 2.2.2. The 4-th roots of unity are the solutions to the equation $x^4 - 1 = 0$, namely 1, $\mathrm{e}^{2\pi\mathrm{i}/4} = \mathrm{i}$, $\mathrm{e}^{(2\pi\mathrm{i}/4)2} = -1$, $\mathrm{e}^{(2\pi\mathrm{i}/4)3} = -\mathrm{i}$. And among these $\mathrm{e}^{(2\pi\mathrm{i}/4)k}$, where $(4, k) = 1$, are the primitive 4-th roots of unity, namely i and $-\mathrm{i}$.

Proposition 2.2.3. *Suppose $\zeta = \zeta_n$. Then the set*

$$\langle \zeta \rangle = \{\zeta^j : j = 1, 2, \ldots, n\}$$

forms a cyclic multiplicative group of order n.

Proof. Since ζ is a primitive n-th root of unity, its order in the group of complex units $\mathbb{C}^*$ is n. Therefore, the cyclic subgroup $\langle \zeta \rangle$ is the same set as above and its order is n.

The group identity is $\zeta^n = 1$. And the inverse of ζ^a is $\zeta^{n-a} \in \langle \zeta \rangle$. □

Corollary 2.2.4. *Let p be a prime number. Then*

$$\langle \zeta_{p-1} \rangle \cong (\mathbb{Z}/p\mathbb{Z})^*.$$

Proof. This is a direct result of Propositions 2.1.3 and 2.2.3. □

Definition 2.2.5. Let n be a positive integer. Then the *n-th cyclotomic field* is the algebraic number field $\mathbb{Q}(\zeta_n)$. One has $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, where ϕ is Euler's totient function ([10], p. 195).

Remark 1. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois since $\mathbb{Q}(\zeta_n)$ is a splitting field of the polynomial $x^n - 1$. This leads to the Galois group

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

The generators of G are the elements σ_k such that k is a primitive root modulo n, and the order of G is equal to $\phi(n)$. Since $\sigma_a \circ \sigma_b = \sigma_{ab}$, we can conclude $G \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Example 2.2.6. Consider the case where $G = \mathrm{Gal}(\mathbb{Q}(\zeta_6)/\mathbb{Q}))$. Let $a \in \mathbb{Q}(\zeta_6)$ such that $a = \alpha\zeta_6 + \beta$, where $\alpha, \beta \in \mathbb{Q}$. Then $\mathrm{ord}(G) = \phi(6) = 2$, and we have

$$\sigma_1(a) = \alpha\sigma_1(\zeta_6) + \beta = \alpha\zeta_6 + \beta$$
$$\sigma_5(a) = \alpha\sigma_5(\zeta_6) + \beta = \alpha\zeta_6^5 + \beta = \alpha\zeta_6^{-1} + \beta.$$

Note that 5 is the only primitive root modulo 6, so $G = \langle \sigma_5 \rangle$.

Proposition 2.2.7. *Let K be equal to the n-th cyclotomic field. Then the ring of algebraic integers $\mathcal{O}_K$ is equal to $\mathbb{Z}[\zeta_n]$.*

Proof. For a complete proof, see Theorem 2.6 of [19]. For a simpler proof of only the prime case, see Proposition 13.2.10 of [10]. □

In this thesis, we will only be concerned with the cyclotomic fields $\mathbb{Q}(\zeta_q)$ and $\mathbb{Q}(\zeta_r)$, where q is a prime number and r is a power of a prime.

Definition 2.2.8. For the field extension $\mathbb{Q}(\zeta_q)/\mathbb{Q}$, write the Galois group G as

$$G = \{\sigma_i : i \in (\mathbb{Z}/q\mathbb{Z})^*, \text{ where } \sigma_i(\zeta_q) = \zeta_q^i\}.$$

Then *the group ring* $\mathbb{Z}[G]$ is the set

$$\mathbb{Z}[G] = \{\sum_{i=1}^{q-1} a_i\sigma_i : a_i \in \mathbb{Z}, \sigma_i \in G\}.$$

Let $\alpha, \beta \in \mathbb{Z}[G]$ with $\alpha = \sum_i \ a_i\sigma_i$ and $\beta = \sum_i \ b_i\sigma_i$. Addition and multiplication in the ring are defined to be

$$\alpha + \beta = \sum_{i=1}^{q-1} a_i\sigma_i + \sum_{i=1}^{q-1} b_i\sigma_i = \sum_{i=1}^{q-1}(a_i + b_i)\sigma_i,$$

and

$$\alpha \cdot \beta = \sum_{i=1}^{q-1}\sum_{j=1}^{q-1}(a_ib_j)(\sigma_i\sigma_j), \text{ where } \sigma_i\sigma_j \in G.$$

The group ring $\mathbb{Z}[G]$ acts on $\mathbb{Q}(\zeta_q)$, and we use exponential notation for these actions: Let $f \in \mathbb{Z}[G]$ such that $f = \sum_i a_i\sigma_i$, and let $x \in \mathbb{Q}(\zeta_q)$. Then

$$x^f = x^{\sum_i a_i\sigma_i} = \prod_{i=1}^{q-1} \sigma_i(x)^{a_i}.$$

Example 2.2.9. Let $\zeta_3 + 5 \in \mathbb{Q}(\zeta_3)$, and let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$. Let $f \in \mathbb{Z}[G]$ such that $f = 2\sigma_1 + \sigma_2$. Then

$$(\zeta_3 + 5)^f = \sigma_1(\zeta_3 + 5)^2\sigma_2(\zeta_3 + 5) = (\zeta_3 + 5)^2(\zeta_3^2 + 5) = \zeta_3^4 + 30\zeta_3^2 + 50\zeta_3 + 135.$$

2.3 Characters

Definition 2.3.1. Let k be a positive integer. A *Dirichlet character* χ *modulo* k is a group homomorphism from $(\mathbb{Z}/k\mathbb{Z})^*$ to $\mathbb{C}^*$, i.e., $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in$

$(\mathbb{Z}/k\mathbb{Z})^*$. We can lift this definition naturally to go from $(\mathbb{Z}/k\mathbb{Z})$ to $\mathbb{C}$ (or even $\mathbb{Z}$ to $\mathbb{C}$) by setting $\chi(a) = 0$ when $a \notin (\mathbb{Z}/k\mathbb{Z})^*$. The trivial character χ_0 is defined to be $\chi_0(a) = 1$ for all a such that $(a, k) = 1$ and 0 otherwise.

For the purposes of this thesis we are only interested in characters modulo a prime.

Proposition 2.3.2. *Let χ be a character modulo p where p is a prime, and let $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Then*

1. *$\chi(1) = 1$,*
2. *$\chi(a)$ is a $(p-1)$-st root of unity,*
3. *$\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$, the complex conjugate.*

Proof.

1. Since χ is a homomorphism, $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. And $\chi(1) \neq 0$ because $\chi(1) \in \mathbb{C}^*$. Thus $\chi(1) = 1$.
2. Recall that the $\text{ord}((\mathbb{Z}/p\mathbb{Z})^*) = \phi(p) = p - 1$. Thus we have $a^{p-1} = 1$. And this implies that $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$.
3. Observe that $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$, yielding the equation $\chi(a^{-1})\chi(a) = 1$. Right multiplying both sides by $\chi(a)^{-1}$ yields the equality $\chi(a^{-1}) = \chi(a)^{-1}$.

□

Proposition 2.3.3. *The set of characters χ modulo prime p which we denote by G_p forms a multiplicative group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$.*

Proof. Let g be a generator of the group $(\mathbb{Z}/p\mathbb{Z})^*$. It follows that every $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is equal to a power of g. And if $a = g^l$, then $\chi(a) = \chi(g^l) = \chi(g)^l$ for $\chi \in G_p$. Thus each χ in G_p is completely determined by its value $\chi(g)$.

We show next that G_p has a bijection onto $\langle \zeta_{p-1} \rangle$. By Proposition 2.3.2, all values of χ are $p-1$st roots of unity, so given $\lambda \in G_p$ we have that $\lambda(g) = \mathrm{e}^{2\pi \mathrm{i}(r/(p-1))}$ for some uniquely determined integer r, where $0 \leq r < (p-1)$.

Conversely, if $0 \leq r < (p-1)$, then define $\lambda(g^l) = \mathrm{e}^{2\pi \mathrm{i}(lr/(p-1))}$. It is easy to see that λ is in fact a well-defined character. By Proposition 2.2.3, there are exactly $(p-1)$ of these roots of unity, so there must be exactly $p-1$ characters on $(\mathbb{Z}/p\mathbb{Z})^*$.

To show that G_p is cyclic, let $\chi_1 \in G_p$ such that $\chi_1(g) = \zeta_{p-1}$. If $\lambda \in G_p$ as defined above, then $\chi_1(g^r) = \chi_1^r(g) = \lambda(g)$, which implies $\lambda = \chi_1^r$. And it follows that G_p is generated by χ_1.

Only one cyclic group of order $p-1$ exists (up to isomorphism). Therefore, by Proposition 2.1.3, $G_p \cong (\mathbb{Z}/p\mathbb{Z})^*$. □

Note 1. The trivial character χ_0 is the *unit element* of the group. The *order* of a character χ modulo p, denoted $\mathrm{ord}(\chi)$, is the order of χ when considered as an element of the group of characters, i.e., the smallest positive integer l such that $\chi^l = \chi_0$. We shall keep the notation of χ_0 for the identity and χ_1 for the generator of G_p.

Proposition 2.3.4. *Suppose χ is a character modulo prime p not equal to χ_0. Then*

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \chi(a) = 0.$$

Moreover, if $\chi = \chi_0$, then

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \chi(a) = p - 1.$$

Proof. To prove the first part of the proposition, we assume $\chi \neq \chi_0$; so then there must exist an $a \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $\chi(a) \neq 1$. Let $S = \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^*} \chi(b)$. Then

$$\chi(a)S = \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^*} \chi(a)\chi(b) = \sum_{b \in (\mathbb{Z}/p\mathbb{Z})^*} \chi(ab) = S.$$

The last equality holds because ab runs over all elements of $(\mathbb{Z}/p\mathbb{Z})^*$ as b does since $(\mathbb{Z}/p\mathbb{Z})^*$ is a multiplicative group. And since $\chi(a) \neq 1$, it must be that $S = 0$.

The second part of the proposition is a direct consequence of Proposition 2.1.3. □

Proposition 2.3.5. *Suppose a is an element in $\mathbb{Z}/p\mathbb{Z}$ such that $a \neq 1$, then*

$$\sum_{\chi \in G_p} \chi(a) = 0.$$

Moreover, if $a = 1$, then

$$\sum_{\chi \in G_p} \chi(a) = p - 1.$$

Proof. To prove the first part of the proposition, suppose $a \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $a \neq 1$. Let g be a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Since g is a generator, it follows that $a = g^l$, where $0 < l < (p-1)$ as $\mathrm{ord}((\mathbb{Z}/p\mathbb{Z})^*) = p - 1$. Thus $(p-1) \nmid l$, and so

$$\chi_1(a) = \chi_1(g^l) = \chi_1(g)^l = \zeta_{p-1}^l = \mathrm{e}^{2\pi \mathrm{i}(l/(p-1))} \neq 1.$$

Next, let $T = \sum_{\chi \in G_p} \chi(a)$. Then

$$\chi_1(a)T = \sum_{\chi} \chi_1(a)\chi(a) = \sum_{\chi} \chi_1\chi(a) = T.$$

The last equality holds because $\chi_1\chi$ runs over all characters of G_p as χ does. And since $\chi_1(a) \neq 1$, it must be that $T = 0$.

The second part of the proposition is a direct consequence of Proposition 2.3.3. □

Example 2.3.6. There are $\phi(5) = 4$ characters modulo 5. The group is wholly determined by $\chi(2)$ as $(\mathbb{Z}/5\mathbb{Z})^* = \langle 2 \rangle$.

Table 2.1: Characters modulo 5

	1	**2**	**3**	**4**
$\chi_0(n)$	1	1	1	1
$\chi_1(n)$	1	$\zeta_4 = \mathrm{i}$	$\zeta_4^3 = -\mathrm{i}$	$\zeta_4^2 = -1$
$\chi_2(n)$	1	$\zeta_4^2 = -1$	$\zeta_4^2 = -1$	1
$\chi_3(n)$	1	$\zeta_4^3 = -\mathrm{i}$	$\zeta_4 = \mathrm{i}$	$\zeta_4^2 = -1$

2.4 Gauss and Jacobi Sums

Definition 2.4.1. Let χ be the character modulo p. Then *the Gauss sum* $\tau(\chi)$ is defined by

$$\tau(\chi) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \chi(a)\zeta_p^a, \text{ where } \zeta_p = \mathrm{e}^{2\pi \mathrm{i}/p}.$$

Proposition 2.4.2. *Let χ be a nontrivial character modulo p, and let $\tau(\chi)$ be the corresponding Gauss sum. Then*

$$\tau(\chi)\overline{\tau(\chi)} = q,$$

where $\overline{\tau(\chi)}$ denotes the complex conjugate.

Proof. By Proposition 8.2.2 of [10], we have that $|\tau(\chi)| = \sqrt{p}$. It follows that

$$\tau(\chi)\overline{\tau(\chi)} = |\tau(\chi)|^2 = p.$$

□

Definition 2.4.3. Let χ and λ be the characters modulo p. Then the Jacobi sum $j(\chi, \lambda)$ is defined by

$$j(\chi, \lambda) = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \chi(a)\lambda(1-a).$$

2.5 p-adic Numbers

We present here only the most rudimentary introduction to p-adic numbers since that will suffice for this thesis. For a thorough introduction to this vast and fascinating subject, see [9].

Definition 2.5.1. For a nonzero integer n, the *p-adic valuation* is

$$v_p(n) = \max\{r : p^r \mid n\}, \text{ and } v_p(0) = \infty.$$

For $a/b \in \mathbb{Q}$, the *p-adic valuation* is

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

And for $m \in \mathbb{Q}$, the *p-adic norm* is

$$|m|_p = \begin{cases} p^{-v_p(m)}, & \text{if } m \neq 0 \\ 0, & \text{if } m = 0 \ . \end{cases}$$

Definition 2.5.2. The *p-adic numbers* $\mathbb{Q}_p$ are the completion of the rationals $\mathbb{Q}$ with respect to the p-adic norm (just as the reals $\mathbb{R}$ are the completion of $\mathbb{Q}$ with respect to the usual absolute value).

Remark 2. It should be noted that the p-adic norm and the p-adic valuation extend naturally to $\mathbb{Q}_p$.

Definition 2.5.3. The *p-adic integers* $\mathbb{Z}_p$ are the elements in the closed unit disc of $\mathbb{Q}_p$,

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}.$$

The p-adic integer x can be represented as the formal power series

$$x = \sum_{i=0}^{\infty} a_i p^i,$$

where $a_i \in \mathbb{Z}$. It is important to note that this representation is not unique.

The p-adic integers form a ring. Addition and multiplication in the ring are the same as for formal power series. If $x, y \in \mathbb{Z}_p$, then

$$x \cdot y = \left(\sum_{i=0}^{\infty} a_i p^i\right)\left(\sum_{i=0}^{\infty} b_i p^i\right) = \sum_{i=0}^{\infty} c_i p^i,$$

where $c_i = \sum_{j=0}^{i} a_j b_{i-j}$, and

$$x + y = \sum_{i=0}^{\infty} (a_i + b_i) p^i.$$

The zero element is $0 = 0 + 0 \cdot p + 0 \cdot p^2 + \cdots$, and the unit element is $1 = 1 + 0 \cdot p + 0 \cdot p^2 + \cdots$.

Remark 3. The units of $\mathbb{Z}_p$ are elements of the form $x = \sum_{i=0}^{\infty} a_i p^i$, where $a_0 \neq 0$. This is clear from the description of the unit element above. (One can show that the converse also holds.)

Furthermore, note that $\mathbb{Z}_p \cap \mathbb{Q} = \{\frac{a}{b} \in \mathbb{Q} : v_p(a) \geq v_p(b)\}$. Therefore, such fractions have representations as formal power series like above. For example,

$$\sum_{i=0}^{\infty} p^i = \frac{p^N - 1}{p - 1} + p^N \sum_{i=0}^{\infty} p^i = -\frac{1}{p-1}.$$

Definition 2.5.4. For $\mathbb{Z}_p$ we define the p-adic logarithm to be

$$\log(x+1) = \sum_{j=1}^{\infty} (-1)^{j+1} \frac{x^j}{j}$$

with a radius of convergence $|x|_P < 1$.

Similarly, we define can exponentiation for the p-adic numbers. Let $a, b \in \mathbb{Q}_p$ such that $a \equiv 1 \pmod{p}$ and $b = \sum_i b_i p^i$. Then

$$a^b = \lim_{N \to \infty} a^{\sum_{i=0}^{N} b_i p_i}.$$

(It can be shown that the limit exists in this case.)

Chapter 3

The Gauss Sum Test

3.1 Mathematical Underpinnings

In this section, we construct the propositions and theorem required for the cyclotomic primality test. We begin by explicitly constructing a character χ modulo prime q of order r, where r is relatively prime to q and $r \mid (q-1)$. This will be denoted as $\chi_{r,q}$ throughout. To construct $\chi_{r,q}$, begin by setting g to be a primitive root modulo q, so for all $a \in (\mathbb{Z}/q\mathbb{Z})^*$ we have $g^k = a$ for some $k \in (\mathbb{Z}/q\mathbb{Z})^*$. And define $\chi_{r,q}$ by $\chi_{r,q}(a) = \chi_{r,q}(g^k) = \zeta_r^k$, where ζ_r is a primitive r-th root of unity. This is well-defined as $r \mid (q-1)$, and one can easily show that $\chi_{r,q}$ is of order r.

Let $\chi = \chi_{r,q}$ and let $\tau(\chi)$ be the corresponding Gauss sum. Then we have

$$\tau(\chi) = \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \chi(a)\zeta_q^a = \sum_{k \in (\mathbb{Z}/q\mathbb{Z})^*} \chi(g^k)\zeta_q^{g^k} = \sum_{k \in (\mathbb{Z}/q\mathbb{Z})^*} \zeta_r^k \zeta_q^{g^k}.$$

It follows that $\tau(\chi)$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_r, \zeta_q)$.

We will next describe the Galois groups and group rings necessary for our calculations.

Let Δ be the Galois group of the extension $\mathbb{Q}(\zeta_r, \zeta_q)/\mathbb{Q}(\zeta_q)$. We know this extension is Galois because $\mathbb{Q}(\zeta_r, \zeta_q)$ is the splitting field of the polynomial $(x^r - 1)$

over $\mathbb{Q}(\zeta_q)$. We can write $\Delta = \{\sigma_i : i \in (\mathbb{Z}/r\mathbb{Z})^*\}$, where $\sigma_i \in \Delta$ is the isomorphism from $\mathbb{Q}(\zeta_r, \zeta_q)$ to itself that acts trivially on q-th roots of unity, while its action on r-th roots of unity is given by $\sigma_i(\zeta_r) = \zeta_r^i$. Let $\mathbb{Z}[\Delta]$ be the group ring of Δ over $\mathbb{Z}$ that acts on $\mathbb{Q}(\zeta_r, \zeta_q)^*$.

Similarly, let G be the Galois group of the extension $\mathbb{Q}(\zeta_r, \zeta_q)/\mathbb{Q}(\zeta_r)$. We can write $G = \{\rho_j : j \in (\mathbb{Z}/q\mathbb{Z})^*\}$, where $\rho_j \in G$ is the isomorphism from $\mathbb{Q}(\zeta_r, \zeta_q)$ to itself that acts trivially on r-th roots of unity, while its action on q-th roots of unity is given by $\rho_j(\zeta_q) = \zeta_q^j$. Let $\mathbb{Z}[G]$ be the group ring of G over $\mathbb{Z}$ that acts on $\mathbb{Q}(\zeta_r, \zeta_q)^*$.

We then have the following diagram

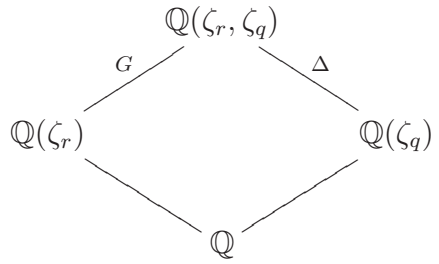

Figure 3.1: Cyclotomic field layout

It may still be a bit unclear what Gauss sums have to do with primality testing, but in the next proposition, we present a Fermat-like congruence that will be used to build our primality test. We first require one lemma.

Lemma 3.1.1. *Let $\chi = \chi_{r,q}$, let $\tau(\chi)$ be the corresponding Gauss sum, and let $\sigma_i \in \Delta$ (as defined as above). Then we have*

$$\tau(\chi)^{\sigma_i} = \tau(\chi^i), \text{ for } i \in (\mathbb{Z}/r\mathbb{Z})^*.$$

Proof. Let $a \in (\mathbb{Z}/q\mathbb{Z})^*$, and observe that $\sigma_i(x) = x^i$ for all $x \in \langle \zeta_r \rangle$. Then

$$\begin{aligned}
\tau(\chi)^{\sigma_i} &= \sigma_i \left(\sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \chi(a) \zeta_q^a \right) \\
&= \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \sigma_i \left(\chi(a) \right) \zeta_q^a \\
&= \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \chi^i(a) \zeta_q^a \\
&= \tau(\chi^i).
\end{aligned}$$

□

Now we can state the Fermat-like congruence that is necessary for the cyclotomic primality test.

Proposition 3.1.2. *Let q be a prime number, and let r be a positive integer relatively prime to q with $r \mid (q-1)$. Let $\chi = \chi_{r,q}$, and let $\tau(\chi)$ be the corresponding Gauss sum. Then, for every prime number p such that $(p, qr) = 1$, we have*

$$\tau(\chi)^{\sigma_p - p} = \chi^p(p), \text{ in the ring } \mathbb{Z}[\zeta_r, \zeta_q]/(p).$$

Proof. Since we are working modulo prime p, we can distribute the exponent p within the sum, and we have

$$\tau(\chi)^p \equiv \left(\sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \chi(a) \zeta_q^a \right)^p \equiv \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \chi^p(a) \zeta_q^{pa} \pmod{p}.$$

Then, as χ is a group homomorphism, we have

$$\chi^p(p) \tau(\chi)^p \equiv \chi^p(p) \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \chi^p(a) \zeta_q^{pa} \equiv \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \chi^p(pa) \zeta_q^{pa} \pmod{p}.$$

Next, we substitute $b = pa$, as p is a unit, and apply our lemma. This yields

$$\sum_{a\in(\mathbb{Z}/q\mathbb{Z})^*} \chi^p(pa)\zeta_q^{pa} \equiv \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^*} \chi^p(b)\zeta_q^{b} \equiv \tau(\chi^p) \equiv \tau(\chi)^{\sigma_p} \pmod{p}.$$

Recall that $\mathrm{ord}(\chi) = r$ implying $\chi \neq \chi_0$, and so by Proposition 2.4.2 we have $\tau(\chi)\overline{\tau(\chi)} = q$. And as $(q, p) = 1$, it follows that $\tau(\chi)$ is a unit in $\mathbb{Z}[\zeta_r, \zeta_q]/(p)$. Therefore,

$$\chi^p(p) \equiv \tau(\chi)^{\sigma_p} \cdot \tau(\chi)^{-p} \equiv \tau(\chi)^{\sigma_p - p} \pmod{p}.$$

□

Next, we present the main theorem of the thesis. Its two conditions form the majority of the primality test.

Theorem 3.1.3. *Let n be a natural number. Let q be a prime not diving n, let r be a power of a prime number l not dividing n with $r \mid (q-1)$ and $r \neq 1$, and let $\chi = \chi_{r,q}$. If*

1. *for every prime p dividing n there exists λ_p in the ring $\mathbb{Z}_l$ of l-adic integers such that*
$$p^{l-1} = n^{(l-1)\lambda_p}, \text{ in } \mathbb{Z}_l^*;$$

2. *the Gauss sum $\tau(\chi)$ satisfies*
$$\tau(\chi)^{\sigma_n - n} \in \langle\zeta_r\rangle, \text{ in the ring } \mathbb{Z}[\zeta_r, \zeta_q]/(n),$$

then we have

$$\chi(p) = \chi(n)^{\lambda_p}$$

for every prime divisor p of n.

Before we prove this theorem, we must first prove a few lemmas.

Lemma 3.1.4. *Let p be a prime. If $a \equiv b \pmod{p}$, then for all positive integer M we have $a^{p^M} \equiv b^{p^M} \pmod{p^M}$.*

Proof. We prove the lemma by induction on M. For $M = 1$, the lemma is a well known result which follows from the fact that

$$v_p\left(\binom{p}{i}\right) > 1, \text{ for } i \in \{1, \ldots, (p-1)\}.$$

Now assume that for some $M > 1$ we have that $a^{p^{M-1}} \equiv b^{p^{M-1}} \pmod{p^{M-1}}$, i.e., there exists c such that $a^{p^{M-1}} = b^{p^{M-1}} + p^{M-1}c$. Then,

$$a^{p^M} = b^{p^M} + p^M c b^{(p-1)p^{M-1}} + \sum_{i=2}^{p} \binom{p}{i} p^{(M-1)i} c^i b^{(p-i)p^{M-1}}.$$

But $(M-1)i \geq M$ for $i \geq 2$, and thus $a^{p^M} \equiv b^{p^M} \pmod{p^M}$. □

Lemma 3.1.5. *Let p be prime, and set $a \in \mathbb{Z}_p$ such that $a \equiv 1 \pmod{p}$. If $r \equiv s \pmod{p^M}$ in $\mathbb{Z}_p$, then*

$$a^r \equiv a^s \pmod{p^M}.$$

Proof. We have $a^r - a^s = a^s(a^{r-s} - 1)$. Then set $r - s = p^M t$, for some $t \in \mathbb{Z}_p$.

By the previous lemma, since $a \equiv 1 \pmod{p}$, then $a^{p^M} \equiv 1 \pmod{p^M}$. It follows that

$$a^{r-s} - 1 = (a^{p^M})^t - 1 \equiv (1)^t - 1 \equiv 0 \pmod{p^M}.$$

□

Observe that the ring $\mathbb{Z}[\zeta_r, \zeta_q]/(p)$ is finite. This follows since elements of the ring can be represented as

$$\sum_{i=1}^{q} \sum_{j=1}^{r} a_{i,j} \zeta_q^i \zeta_r^j, \text{ where } a \in \mathbb{Z}/p\mathbb{Z}.$$

Thus the group of units $H = (\mathbb{Z}[\zeta_r, \zeta_q]/(p))^*$ is a finitely generated abelian group. By Theorem 2.1.5, we can decompose H into a direct product of cyclic groups,

$$H \cong (\mathbb{Z}/l^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/l^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/l^{\alpha_k}\mathbb{Z}) \times \cdots, \text{ where } \alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$$

and where α_k is the largest power of the prime l in the decomposition. Set $M = \alpha_k$, and let A denote the group H modulo l^M-th powers, i.e., $A = H/H^{l^M} \cong \mathbb{Z}/l^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/l^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/l^{\alpha_k}\mathbb{Z}$. Note that this notation will be used in the proof of the theorem and following lemma.

Lemma 3.1.6. *Let p be a prime number such that $p \nmid r$, where r is a prime l-power such that $l \neq p$. Then the natural map $\langle \zeta_r \rangle \hookrightarrow A$ (as above) is injective.*

Proof. We first show that the natural map $\langle \zeta_r \rangle \hookrightarrow H$ is injective. Note that the natural map is simply reduction modulo p. It suffices to show that the kernel of this map is trivial. Suppose $\zeta_r^i = 1 + p\alpha$ where $\alpha \in \mathbb{Z}[\zeta_q, \zeta_r]$. Then we have

$$1 = (1 + p\alpha)^r = \sum_{i=0}^{r} \binom{r}{i} p^i \alpha^i = 1 + \sum_{i=1}^{r} \binom{r}{i} p^i \alpha^i,$$

which implies that $\sum_{i=1}^{r} \binom{r}{i} p^i \alpha^i = 0$.

Suppose that $\alpha \neq 0$, then we have

$$r + p \sum_{i=2}^{r} \binom{r}{i} p^{i-2} \alpha^{i-1} = 0,$$

which implies

$$\sum_{i=2}^{r} \binom{r}{i} p^{i-2} \alpha^{i-1} = -\frac{r}{p}.$$

But we know that the left-hand side of the equation above is an algebraic integer, whereas the right-hand side is clearly not. Therefore, by this contraction, $\alpha = 0$ and the map is injective.

In particular, the order of ζ_r in H is also r, and by the choice of M, we must have that $r \mid l^M$.

We next show that the natural map $\langle \zeta_r \rangle \hookrightarrow H/H^{l^M}$ (i.e., modulo l^M) is injective. If $\zeta_r^i = 1 \cdot \alpha^{l^M}$ for $\alpha \in H$, then $(\zeta_r^{l^M})^i = 1 = (\alpha^{l^M})^{l^M}$. Which implies that the order of α is a multiple of l. Furthermore, $\mathrm{ord}(\alpha) \mid l^M$ because of our selection of M. Therefore, as $r \mid l^M$, we have $\alpha^{l^M} = 1$ implying $\zeta_r^i = 1$ in H, and thus in $\mathbb{C}$. □

We can now prove the main theorem of the thesis.

Proof of Theorem 3.1.3. We may assume that $\chi \neq \chi_0$, the identity element, because $\mathrm{ord}(\chi) = r \neq 1$. By condition (2) of the theorem, we have that

$$\tau(\chi)^{\sigma_n - n} \equiv \hat{\eta} \pmod{n}, \text{ for some } \hat{\eta} \in \langle \zeta_r \rangle.$$

It follows that

$$\tau(\chi)^{\sigma_n} \tau(\chi)^{-n} \equiv \hat{\eta} \pmod{n}.$$

Multiplying through by $\tau(\chi)^n$ and applying σ_n^{-1} yields

$$\tau(\chi) \equiv \hat{\eta}^{\sigma_n^{-1}} \tau(\chi)^{\sigma_n^{-1} n} \pmod{n}.$$

Observe that $\hat{\eta}^{\sigma_n^{-1}} \in \langle \zeta_r \rangle$, so we may define $\eta \in \langle \zeta_r \rangle$ such that $\eta = \hat{\eta}^{\sigma_n^{-1}}$. It follows then that

$$\tau(\chi)^{\sigma_n^{-1} n} \equiv \eta \tau(\chi) \pmod{n}. \tag{3.1}$$

Note that $\eta^{\sigma_n^{-1} n} = \eta$, since for any $\zeta_r^i \in \langle \zeta_r \rangle$ we have $\sigma_n^{-1}(\zeta_r^i) = \zeta_r^{im}$, where $nm \equiv 1 \pmod{r}$. It follows that

$$(\zeta_r^i)^{\sigma_n^{-1} n} = \left(\zeta_r^{im}\right)^n = \zeta_r^i. \tag{3.2}$$

Therefore, for any integer $L \geq 0$, applying $\sigma_n^{-1} n$ to equation (3.1) $(l-1)L$ times yields

$$\tau(\chi)^{\sigma_n^{-1} n^{(l-1)L}} \equiv \eta^{(l-1)L} \tau(\chi) \pmod{n}. \tag{3.3}$$

For any prime divisor p of n, by Proposition 3.1.2, we have

$$\tau(\chi)^{\sigma_p} \equiv \chi^p(p)\tau(\chi)^p \pmod{p}.$$

Applying σ_p^{-1} yields

$$\tau(\chi) \equiv (\chi(p))^{\sigma_p^{-1}p}\,\tau(\chi)^{\sigma_p^{-1}p} \pmod{p}.$$

By equation (3.2), we have

$$\tau(\chi) \equiv \chi(p)\tau(\chi)^{\sigma_p^{-1}p} \pmod{p}.$$

And so

$$\tau(\chi)^{\sigma_p^{-1}p} \equiv \chi(p)^{-1}\tau(\chi) \pmod{p}.$$

If we apply $\sigma_p^{-1}p$ to the result $l-1$ times, we have

$$\tau(\chi)^{(\sigma_p^{-1}p)^{l-1}} \equiv \chi(p)^{1-l}\tau(\chi) \pmod{p}. \tag{3.4}$$

Next, let L be an integer between 0 and l^M such that $L \equiv \lambda_p \pmod{l^M}$. We can define L as such because we are working modulo l^M, i.e., we are truncating the formal power series expansion of λ_p at l^M.

Observe that $n^{(l-1)\lambda_p} \equiv n^{(l-1)L} \pmod{l^M}$. This is a direct consequence of Lemma 3.1.5, and so condition (1) tells us that

$$p^{l-1} \equiv n^{(l-1)L} \pmod{l^M}. \tag{3.5}$$

Next, we show that $(\sigma_n^{-1}n)^{(l-1)L} = (\sigma_p^{-1}p)^{l-1}$ in the ring $(\mathbb{Z}/l^M\mathbb{Z})[\Delta]$. Using equation (3.5), we have

$$(\sigma_n^{-1}n)^{(l-1)L} = (\sigma_n^{-1})^{(l-1)L}n^{(l-1)L} = \sigma_{n^{(l-1)L}}^{-1}n^{(l-1)L} \equiv \sigma_{n^{(l-1)L}}^{-1}p^{l-1} \pmod{l^M}.$$

Applying equation (3.5) again yields

$$\sigma_{n^{(l-1)L}}(\zeta_r) = \sigma_{p^{l-1}+l^M b}(\zeta_r) = \zeta_r^{p^{l-1}}\zeta_r^{l^M b} \text{ for } b \in \mathbb{Z}.$$

But observe that $\zeta_r^{l^M b} = 1$, since $r \mid l^M$ as we have seen. Hence, $\sigma_{n^{(l-1)L}}(\zeta_r) = \sigma_{p^{l-1}}(\zeta_r)$, and so $\sigma^{-1}_{n^{(l-1)L}} = \sigma^{-1}_{p^{l-1}}$. Therefore,

$$(\sigma_n^{-1}n)^{(l-1)L} \equiv (\sigma_p^{-1}p)^{l-1} \pmod{l^M}.$$

Taking the left-hand sides of equations (3.3) and (3.4), we have

$$\tau(\chi)^{(\sigma_n^{-1}n)^{(l-1)L}} = \tau(\chi)^{(\sigma_p^{-1}p)^{l-1}+l^M f} = \tau(\chi)^{(\sigma_p^{-1}p)^{l-1}}(\tau(\chi^f))^{l^M},$$

for $f \in \mathbb{Z}[\Delta]$. Therefore, $\tau(\chi)^{(\sigma_n^{-1}n)^{(l-1)L}} = \tau(\chi)^{(\sigma_p^{-1}p)^{l-1}}$, in the group A.

Also, since $p \mid n$ and the left-hand sides of equations (3.3) and (3.4) are equal in A, so are the right-hand sides, i.e.,

$$\eta^{(l-1)L}\tau(\chi) = \chi(p)^{1-l}\tau(\chi), \text{ in } A.$$

And since $\tau(\chi)$ is a unit, we have

$$\eta^{(l-1)L} = \chi(p)^{1-l}, \text{ in } A. \tag{3.6}$$

Recall that $((l-1), r) = 1$, and by Bézout's identity, there exists an $\alpha, \beta \in \mathbb{Z}$ such that $\alpha(l-1) + \beta r = 1$. And raising equation (3.6) to the power α yields

$$\eta^{\lambda_p} = \eta^L = \chi(p)^{-1}, \text{ in } A.$$

And since, by Lemma 3.1.6, the natural map $\langle\zeta_r\rangle \hookrightarrow A$ is injective, it follows that

$$\eta^{\lambda_p} = \eta^L = \chi(p)^{-1}, \text{ in } \mathbb{C}. \tag{3.7}$$

Multiplying the first condition of the theorem, we have that for any positive divisor d of n

$$d^{l-1} = n^{(l-1)\lambda_d}, \text{ in } \mathbb{Z}_l, \text{ where } \lambda_d \text{ is unique.}$$

From this computation, we have that if decomposing d into its prime divisors yields $d = p_1^{l_1} \cdots p_k^{l_k}$, then $\lambda_d = l_1\lambda_{p_1} + \cdots + l_k\lambda_{p_k}$. And from equation (3.7), we can then deduce that for all $d \mid n$,

$$\eta^{\lambda_d} = \chi(d)^{-1}.$$

As $\lambda_n = 1$, it follows that $\eta = \eta^{\lambda_n} = \chi(d)^{-1}$, and therefore,

$$\chi(p)^{-1} = \eta^{\lambda_p} = \chi(n)^{\lambda_p}, \text{ in } \mathbb{C}.$$

for all prime divisors p of n. □

The following proposition is not necessary for the cyclotomic primality test, but it does provide a simple method for checking condition (1) of Theorem 3.1.3. Since it is not a necessity and its proof is lengthy, we only state the proposition. For a complete proof, see Proposition 4.3 in [17].

Proposition 3.1.7. *Let $n > 1$ be an integer and let l be a prime number not dividing n. Then there exists a prime divisor p of n an exponent $\lambda_p \in \mathbb{Z}_l$ for which*

$$p^{l-1} = n^{(l-1)\lambda_p} \text{ in } \mathbb{Z}_l^*,$$

if there exists a prime q not dividing n for which the following holds.

1. *(If $l \neq 2$:) for some l-power $r > 1$ and $\chi_{q,r} = \chi$, the number $\tau(\chi)^{\sigma_n - n}$ is a generator of the cyclic subgroup $\langle \zeta_r \rangle$ of $(\mathbb{Z}[\zeta_r, \zeta_q]/(n))^*$.*

2. *(If $l = 2$ and $n \equiv 1 \pmod 4$:) for $\chi = \chi_{2,q}$ we have $\tau(\chi)^{\sigma_n - n} = -1$.*

3. *(If $l = 2$ and $n \equiv 3 \pmod 4$:) for some l-power $r \geq 4$ and $\chi = \chi_{r,q}$, the number $\tau(\chi)^{\sigma_n - n}$ is a generator of the cyclic subgroup $\langle \zeta_r \rangle$ of $(\mathbb{Z}[\zeta_r, \zeta_q]/(n))^*$. And also, $\tau(\chi_{2,q}^{r/2})^{\sigma_n - n} = -1$ in the ring $\mathbb{Z}[\zeta_q]/(n)$.*

3.2 The Algorithm

3.2.1 An Overview

To aid in conceptual understanding, we begin by giving a very broad overview of the algorithm. Suppose we have a positive integer n that we wish to prove is prime. We begin the algorithm by using n to calculate the positive integers R and s. These values are smaller than n and directly define the running time of the algorithm. Next, we submit n to a number of congruence tests similar in style to Fermat's "little theorem", with congruences that involve Gauss sums calculated in the ring $\mathbb{Z}[\zeta_r, \zeta_q]/(n)$, where prime q and prime power r are derived from R and s (see Proposition 3.1.2). If n fails any of the congruence tests, it is immediately declared to be composite. If n passes all of the congruence tests, it could still be composite, but information is then known about its possible divisors. And in the last step of the algorithm, if n is divisible by any of the candidate divisors, it is declared to be composite. Otherwise, n is declared to be prime.

3.2.2 A Detailed Description

Pre-compilation and Setup

We will now describe in detail the cyclotomic primality test based on Theorem 3.1.3 and Proposition 3.1.2. It will be described from both a theoretical and a practical perspective.

Suppose we have an integer n that we wish to prove is prime. In practice, before applying the cyclotomic test, we first apply to n a fast compositeness test, like the

probabilistic Miller-Rabin test. After passing this test, n is declared very likely prime, and we can begin the cyclotomic primality test to *prove* that n is prime.

The first step of the algorithm is to compute the integers R and s, where

$$s = \prod_{\substack{(q-1)|R \\ q \text{ prime}}} q \tag{3.8}$$

and $s > \sqrt{n}$.

It was shown by Pomerance in [1] that for every $n > e^e$ there exists positive integers R and s such that $R < (\log n)^{c \cdot \log\log\log n}$, where c is an effectively computable constant. From this the upper bound for the running time of the algorithm $O(\log n)^{c \cdot \log\log\log n}$ is derived, which is almost polynomial time since $\log\log\log n$ acts like a constant. Moreover, it was shown in [13] and further described in [6], that with slight modification to the algorithm, the condition on s could be loosened to $s > \sqrt[3]{n}$, greatly increasing the practical implementation of the test.

Ideally, R should be as small as possible while still satisfying the size condition on s. As we will see, larger values of R and s directly translate to larger rings for our computations and a greater number of calculations required.

The simplest method for generating the most efficient R and s values is the brute-force method, i.e., trying increasing values $R = 1, 2, 3, \ldots$ until a proper s is found. With the help of a computer and a sufficiently long list of primes in-hand, this is a trivial task. Slight modifications can be made to this method to improve practical performance, but typically in practice, a pre-compiled table of default R and s values is used. For example, default values like $R = 180$ and $s = 39921071190$ could be used for small values of n, i.e., $\log_{10} n \leq 20$. It is generally accepted that the product of the first few small prime powers makes for a good R, e.g., $180 = 2^2 \cdot 3^2 \cdot 5$.

After defining R and s, our next step is to construct the pairs q, r. For each prime q dividing s, we must calculate the prime powers r such that r exactly divides $q - 1$,

i.e., $r = l^k \mid (q-1)$ but $l^{k+1} \nmid (q-1)$. Thus we have $(r,q) = 1$ and $(r,R) = r$. There are at most $O(R)$ of these pairs.

Once the pairs are constructed, for each pair we make sure that $(n, qr) = 1$. Finding a single GCD greater than 1 would immediate indicate n was composite. For fast implementations of GCD, see Ch. 2 of [7] or §1.3. of [4].

For each pair q, r, we must find a primitive root modulo q (for a fast implementation, see §1.4 of [4]). Then define the character $\chi_{r,q}$ and calculate the corresponding Gauss sums in the ring $\mathbb{Z}[\zeta_r, \zeta_q]/(n)$. In practice, all of this data should be precomputed and stored in a table for small primes and prime powers.

The next two steps are the main part of the algorithm and are derived directly from the two conditions of Theorem 3.1.3. For each pair q, r, we must perform these two steps.

Step 1

Let l be the prime divisor of r. Then each l must satisfy condition (1) of Theorem 3.1.3. And although this condition cannot be checked directly, in practice it is quite easy.

Claim 1. If $l > 2$, then verifying that $n^{l-1} \not\equiv 1 \pmod{l^2}$ satisfies condition (1) of Theorem 3.1.3.

Proof. To satisfy condition (1), it suffices to show that $v_l(\lambda_p) \geq 0$.

By Theorem 1.0.1, we have that $p^{l-1} \equiv n^{l-1} \equiv 1 \pmod{l}$, and this implies that $0 < |p^{l-1} - 1|_l, |n^{l-1} - 1|_l < 1$. Therefore, we may apply the l-adic log to the equation $p^{l-1} = n^{(l-1)\lambda_p}$. Set $p^{l-1} - 1 = la$ and $n^{l-1} - 1 = lb$, for some $a, b \in \mathbb{Z}$. Then

$$\begin{aligned}\lambda_p &= \frac{\log(p^{l-1})}{\log(n^{l-1})} = \frac{\log(1+la)}{\log(1+lb)} = \frac{\sum_{j=1}^{\infty}(-1)^{j+1}\frac{(la)^j}{j}}{\sum_{j=1}^{\infty}(-1)^{j+1}\frac{(lb)^j}{j}} \\ &= \frac{(la)(1-(la)/2+(la)^3/3-\dots)}{(lb)(1-(lb)/2+(lb)^2/3-\dots)}.\end{aligned}$$

Thus, it suffices to show that

$$v_l\left(\frac{a}{b}\right) = v_l(a) - v_l(b) \geq 0.$$

Which implies

$$v_l(a) \geq v_l(b). \tag{3.9}$$

Equation (3.9) is automatically satisfied when $v_l(b) = 0$, which is satisfied by checking that $n^{l-1} \not\equiv 1 \pmod{l^2}$. □

If $l = 2$ or the above claim cannot be verified, then we resort to Proposition 3.1.7. The prime q defined in the proposition is not necessarily equal to the q from our q, r pair. For each l, its associated q should be tried first, but failing that, all other q's should be attempted until one is found to work. In practice, this happens very quickly. In the small chance that none of the q's satisfy this condition, then the condition is skipped and step 2 is tested for more primes $q \equiv 1 \pmod{l}$.

Step 2

Next, $\chi_{r,q}$ is tested against condition (2) of Theorem 3.1.3. All calculations are performed modulo n. If the character does not satisfy the condition, then n is composite.

Final Step

If all q, r pairs pass these two steps, then something is known about the possible divisors of n. To complete the algorithm, we set

$$a_k = (n^k \bmod s),$$

and then verify

$$a_k \nmid n, \text{ for } k = 1, \ldots, R-1. \tag{3.10}$$

Induction is the most efficient way to check this. Fast modular exponentiation is the simplest method (while still being efficient). For implementation, see §1.2 of [4]. If n satisfies equation (3.10), it is declared prime.

3.3 Proof of Correctness

If n is prime, then Proposition 3.1.2 implies that it passes all tests. Instead, assume n is composite, and let p be a prime divisor of n such that $p \leq \sqrt{n}$. For every prime divisor l that divides R, let λ_p be the l-adic integer from condition (1) of Theorem 3.1.3 and let r be the greatest prime power of l that divides R. Let $L_r \in \mathbb{Z}$ such that $L_r \equiv \lambda_p \pmod{r}$. (Note that an r' from the theorem is not necessarily the same as this r. But all r' values divide r, and so we still have that $\chi_{r',q}(p) = \chi_{r',q}(n)^{L_r}$.) Then, by the Chinese Remainder Theorem, we have a unique solution L in $\{0, \ldots, R-1\}$ of the system

$$x \equiv L_r \pmod{r}, \text{ for all divisors } r \text{ of } R \text{ as above.}$$

Then Theorem 3.1.3 implies that $\chi_{r,q}(p) = \chi_{r,q}(n)^L$ for all q, r pairs. Furthermore, we have

$$p \equiv n^L \pmod{s}, \text{ where } s \text{ is from equation (3.8).}$$

To see that this relation holds, assume $p \not\equiv n^L \pmod{q}$. Then let $(\mathbb{Z}/q\mathbb{Z})^* = \langle g \rangle$, and so we have $p = g^{t_1}$ and $n^L = g^{t_2}$, where $t_1 \not\equiv t_2 \pmod{q-1}$. Next, set $(q-1) = r_1 \cdots r_m$, where r_i is a power of a prime such that $(r_i, r_j) = 1$ if $i \neq j$, and so $t_1 \not\equiv t_2 \pmod{r_i}$ for some r_i. It then follows

$$\chi_{r_i,q}(p) = \chi_{r_i,q}(g^{t_1}) = \zeta_{r_i}^{t_1} \neq \zeta_{r_i}^{t_2} = \chi_{r_i,q}(g^{t_2}) = \chi_{r_i,q}(n^L),$$

which is a contradiction. Thus, since $p \equiv n^L \pmod{q}$ holds for all q, it must hold modulo s as well.

And since $0 < p < s$, it follows that p is *equal* to the smallest non-negative residue of n^k modulo s for some $k \in \{0, 1, \ldots, R-1\}$. But this was the final test of the algorithm, so by contradiction, n must be prime.

3.4 The Jacobi Sum Alternative

In practice, the best way to improve the performance of the Gauss sum test is to not use Gauss sums! The original APR algorithm used Jacobi sums, and most current implementations of the cyclotomic primality test use Jacobi sums. The only difference is in the second condition of Theorem 3.1.3. The Gauss sums are calculated in the finite ring $\mathbb{Z}[\zeta_r, \zeta_q]/(n)$ and require vectors of length $\phi(q)\phi(r)$ to be stored. These Gauss sums should in practice be exchanged for Jacobi sums calculated in the smaller finite ring $\mathbb{Z}[\zeta_r]/(n)$. This is significantly more efficient since $q > r$, and the difference between q and r can be large.

Bibliography

Bibliography

[1] L. Adleman, C. Pomerance, and R. Rumely. On distinguishing prime numbers from composite numbers. *Annals of Mathematics*, 117:173–206, 1983. 4, 27

[2] M. Artin. *Algebra*. Prentice Hall, 1991. 7

[3] W. Bosma and M. van der Hulst. *Primality proving with cyclotomy*. PhD thesis, Universiteit van Amsterdam, 1990. 4

[4] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993. 1, 28, 30

[5] H. Cohen and H. Lenstra. Primality Testing and Jacobi Sums. *Mathematics of Computation*, 42(165):297–330, 1984. 4

[6] D. Coppersmith, N. Howgrave-Graham, and S. V. Nagaraj. Divisors in Residue Classes, Constructively. *Mathematics of Computation*, 77(261):531–545, 2008. 27

[7] R. Crandall and C. Pomerance. *Prime Numbers, A Computational Perspective*. Springer, second edition, 2005. 1, 3, 28

[8] S Goldwasser and J Kilian. Almost all primes can be quickly certified. In *Proceedings of the eighteenth annual ACM symposium on Theory of computing*, STOC '86, pages 316–329, New York, NY, USA, 1986. ACM. 5

[9] F. Gouvêa. *p-adic Numbers, An Introduction*. Springer, second edition, 1997. 13

[10] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, second edition, 1990. 6, 8, 13

[11] D. H. Lehmer. An Extended Theory of Lucas' Functions. *Annals of Mathematics*, 31(3):419–448, 1930. 3

[12] H. W. Lenstra. *Primality testing algorithms [after Adleman, Rumely and Williams]*, volume 901 of *Lecture Notes in Mathematics*. Springer Berlin / Heidelberg, 1981.

[13] H. W. Lenstra. Divisors in Residue Classes. *Mathematics of Computation*, 42(165):331–340, 1984. 27

[14] H. W. Lenstra and C. Pomerance. Primality testing with Gaussian periods. Available at http://www.math.dartmouth.edu/~carlp/, 2011. 5

[15] P. Mihailescu. *Cyclotomy Primality Proving – Recent Developments*, volume 1423 of *Lecture Notes in Computer Science*. Springer, 1998. 4

[16] M. Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12:128–138, 1980. 3

[17] R. Schoof. Four primality testing algorithms. *Algorithmic Number Theory*, 44:101–126, 2008. 5, 25

[18] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 6:84–85, 1977. 2

[19] L. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag, 1982. 8

Vita

Thomas F. Boucher was born in Worcester, MA on October 17, 1982. After receiving his education at the Massachusetts Academy of Math and Science, in 2001, he enlisted in the U.S. Marine Corps. He served actively for five years, attained the rank of sergeant, and was honorably discharged. In 2006, he entered the University of Massachusetts at Amherst, and in 2009, he earned a Bachelor of Science degree in mathematics. Later that year, he entered the Master of Science program at the University of Tennessee studying mathematics.