A SURVEY OF PRIMALITY TESTS

STEFAN LANCE

Abstract. In this paper, we show how modular arithmetic and Euler's totient function are applied to elementary number theory. In particular, we use only arithmetic methods to prove many facts that are fundamental to the study of prime numbers. These proofs lead us to examine the theorems governing several simple primality tests.

Contents

1. Introduction

The goal of this paper is to provide proofs of several theorems and lemmas essential to introductory number theory and to expose some basic primality tests. The paper will therefore establish a basis for further exploring number theory.

We first review properties of modular arithmetic and the fundamental theorem of arithmetic and use them to explore elementary properties of prime numbers. This naturally requires the investigation of Euler's totient (or phi) function and related topics, such as reduced residue systems and order. We finish by using these results to prove the theorems behind some basic primality tests.

This paper relies upon and provides detailed explanations of arithmetic rather than analytic methods, so we assume relatively little.

Remark 1.1. For the sake of reducing redundancy, we do not consider negative integers in the following proofs. Adjusting these proofs to apply to the negative integers is trivial and not significant for the results we prove.

Date: August 27, 2014.

2. Modular Arithmetic and The Fundamental Theorem of Arithmetic

We begin by reviewing some notation and the basic properties of modular arithmetic on $\mathbb{N}$.

Definition 2.1. We define *natural numbers* to be nonnegative integers and denote the set of natural numbers by $\mathbb{N}$.

Notation 2.2. If a and b are integers and a divides b, then we use the notation $a|b$.

This is equivalent to saying that when b is divided by a, the remainder is 0, and it implies that $|a| \leq |b|$.

Definition 2.3. Two integers a and b are said to be *congruent modulo a positive integer* n if $n|(a-b)$. If this is the case, then we write

$$a \equiv b \pmod{n}.$$

We say that n is the *modulus* and that b is a *remainder* or *residue* of $a \pmod{n}$. If b is the smallest nonnegative integer such that this is true, then we say that b is the *least nonnegative residue* of $a \pmod{n}$. If b is positive, then we say that b is the *least positive residue* of $a \pmod{n}$.

Remark 2.4. Congruence $\pmod{n}$ on the integers is an equivalence relation. Below, we provide several of the properties modular congruence is equipped with, and their proofs are left as exercises for the reader.

Let $a, b, c, d, n \in \mathbb{N}$ such that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then we have the following.

(1) Reflexivity: $a \equiv a \pmod{n}$.
(2) Symmetry: $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$.
(3) Transitivity: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
(4) $a + b \equiv c + d \pmod{n}$.
(5) $a - b \equiv c - d \pmod{n}$.
(6) $ab \equiv cd \pmod{n}$.
(7) If $a \equiv b \pmod{n}$, then $ka \equiv kb \pmod{n}$ for any $k \in \mathbb{Z}$.
(8) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any $k \in \mathbb{N}$.

We can express these properties in slightly different ways, and doing so is often useful. For example, a slight variation of statement (4) is that if $n|a$ and $n|b$, then $n|(a+b)$. We will use these derivations liberally and will not derive all of them.

Along with modular arithmetic, the concept of the greatest common divisor (gcd) is crucial to number theory.

Definition 2.5. Let a and b be positive integers. We call d the *greatest common divisor* of a and b if d is the largest positive integer satisfying $d|a$ and $d|b$.

Now we examine the fundamental theorem of arithmetic, which will allow us to write each positive integer $n > 1$ as the product of primes less than or equal to n.

Theorem 2.6 (Fundamental Theorem of Arithmetic)**.** *Each positive integer greater than* 1 *can be uniquely written as the product of primes, up to their arrangement.*

Proof. The integer 2 is the first positive prime, and it can be written as the product 2^1. Now suppose that we can write the first n positive integers as products of primes, and consider the integer $n+1$. If $n+1$ is prime, then it can be written as $(n+1)^1$. If $n+1$ is not prime, then it must be composite. By the definition of a composite number, $n+1$ can be written as the product of two positive integers a and b such that $a, b < n+1$. By assumption, a and b can be written as the products of primes; that is, we may write $a = \prod_{i=1}^{k} p_i^{c_i}$ and $b = \prod_{j=1}^{l} q_j^{d_j}$, where each p_i, q_j is prime. Since $n+1 = ab$, we have

$$n+1 = \prod_{i=1}^{k} p_i^{c_i} \cdot \prod_{j=1}^{l} q_j^{d_j},$$

and $n+1$ can thus be written as the product of primes less than or equal to it.

Now we shall prove that each positive integer greater than 1 has a unique prime factorization. Let $a \in \mathbb{N}$ and suppose it has two distinct prime factorizations $a = p_1 \cdots p_n$ and $a = q_1 \cdots q_m$. Clearly $p_1 | a = q_1 \cdots q_m$, and since p_1 is prime, there must exist some $j \leq m$ such that $p_1 | q_j$. But q_j is also prime, so we necessarily have $p_1 = q_j$. This process can be repeated to find that for all $p_i | a$, there exists a q_j satisfying $q_j = p_i$. Hence $n \leq m$. Now we repeat the process but by considering all of the q_j to deduce that for all $q_j | a$, there exists a p_i satisfying $p_i = q_j$, and thus $m \leq n$. This means $m = n$ and the prime factorizations $p_1 \cdots p_n$ and $q_1 \cdots q_m$ contain the same primes and are simply rearrangements of one another. Therefore, each positive integer greater than 1 has a unique prime factorization up to the ordering of the primes. □

Equipped with these properties and definitions, we can now prove the division theorem and Bézout's identity. The division theorem tells us how two positive integers are related when we divide one by the other, and Bézout's identity reveals a powerful relationship between two integers and their gcd. We will make extensive use of both theorems throughout this paper.

Theorem 2.7 (Division Theorem)**.** *Let $a, b \in \mathbb{N}$ such that $b \neq 0$. There exist $q, r \in \mathbb{N}$ such that $a = bq + r$ and $0 \leq r < b$.*

Proof. Consider $\frac{a}{b} \in \mathbb{Q}$. There exists a nonnegative integer q such that $q \leq \frac{a}{b} < q+1$. Multiplication yields $bq \leq a < b(q+1)$, so there exists an integer r such that $bq + r = a$, where r is at least 0 and always less than b, since $bq + b = b(q+1) > a$. In other words, $0 \leq r < b$. □

Theorem 2.8 (Bézout's Identity)**.** *Let a, b, d be positive integers such that $d = \gcd(a, b)$. We can write d as a $\mathbb{Z}-$linear combination of a and b, that is, as an expression of the form $ma + nb$, where $m, n \in \mathbb{Z}$. In fact, d is the smallest positive integer that is a $\mathbb{Z}-$linear combination of a and b.*

Proof. Let x be the smallest positive integer that can be written as a $\mathbb{Z}-$linear combination of a and b, that is, such that $x = ma + nb$ for some $m, n \in \mathbb{Z}$. Let $d \in \mathbb{N}$ such that $d = \gcd(a, b)$. Since $d | a$ and $d | b$, it follows that $d | ma$ and $d | nb$, and thus $d | (ma + nb)$. By substitution, $d | x$, so $d \leq x$.

Now suppose $x > d$. Since $d = \gcd(a, b)$, either $x \nmid a$ or $x \nmid b$, so suppose without loss of generality $x \nmid a$. We can use the division theorem to rewrite a as $a = qx + r$,

where $q, r \in \mathbb{N}$ such that $0 \leq r < x$. Indeed, since we assume $x \nmid a$, we have $0 < r < x$. Hence $r = a - xq$, and by substitution, we have

$$r = a - (ma + nb)q = (1 - m)a + (-nq)b.$$

But this means r is a positive integer that is a $\mathbb{Z}-$linear combination of a and b less than x, which contradicts our definition of x. Therefore, $x = d$; that is,

$$\gcd(a, b) = \min\{k \in \mathbb{N} \mid k = ma + nb, \text{ where } m, n \in \mathbb{Z}\}.$$

□

We now temporarily set aside these two theorems to explore the basic properties of prime numbers, although we will find them useful in later proofs.

3. Applications of The Fundamental Theorem of Arithmetic

We can perform many interesting exercises with the fundamental theorem of arithmetic, including the following.

Exercise 3.1. Let a, b, and c be positive integers satisfying $\gcd(a, b) = 1$ and $c|ab$. Then there exist unique positive integers d and e such that $c = de$, $d|a$, and $e|b$. Also, $\gcd(d, e) = 1$.

Proof. By the fundamental theorem of arithmetic, we can write a and b as products of powers of primes up to the greatest prime factor of a and b. That is, we can write $a = \prod_{i=1}^{k} p_i^{a_i}$ and $b = \prod_{i=1}^{k} p_i^{b_i}$. Since a and b are coprime, it is necessarily the case that for all $i \in \mathbb{N}$ satisfying $1 \leq i \leq k$, either $a_i = 0$ or $b_i = 0$. Otherwise, a and b would share a common factor p_i, so we would have $\gcd(a, b) > 1$. Observe that

$$ab = \prod_{i=1}^{k} p_i^{a_i} \cdot \prod_{i=1}^{k} p_i^{b_i} = \prod_{i=1}^{k} p_i^{a_i + b_i}.$$

Since $c|ab$, we know $c \leq ab$, so c must be factorizable into powers of the p_i for all i. By the fundamental theorem of arithmetic, we therefore have $c = \prod_{i=1}^{k} p_i^{c_i}$, where each $c_i \leq a_i + b_i$, since $c < ab$. But remember that $a_i + b_i$ is just a_i when $b_i = 0$ and b_i when $a_i = 0$. Now define $d, e \in \mathbb{N}$ such that

$$d = \prod_{\substack{i=1 \\ b_i = 0}}^{k} p_i^{d_i} \quad \text{and} \quad e = \prod_{\substack{i=1 \\ a_i = 0}}^{k} p_i^{d_i}.$$

It follows that $c = de$, $d|a$, and $e|b$. Furthermore, d and e are products of primes from disjoint sets, so $d \neq e$ are unique and $\gcd(d, e) = 1$. □

Note that the fundamental theorem is not necessary to prove the above theorem, but we use it anyway to demonstrate how it can be used.

We can also study the infinitude of primes in $\mathbb{N}$ with the fundamental theorem of arithmetic.

Theorem 3.2 (Euclid's Theorem)**.** *There exist infinitely many primes in* $\mathbb{N}$.

Proof. Suppose there are finitely many primes $p_1, \ldots, p_n$, where $p_1 < \ldots < p_n$. Let $q, r \in \mathbb{N}$ such that

$$q = \prod_{i=1}^{n} p_i \quad \text{and} \quad r = q + 1.$$

Since p_n is the largest prime by assumption, r must be composite, and by the fundamental theorem of arithmetic, it must have a prime factorization including at least one of the primes p_a satisfying $1 \leq a \leq n$; that is, $p_a | r$. We also know $p_a | q$ by the definition of q. Therefore, $p_a | 1$. But this is a contradiction, since 1 is not prime and $p_a > 1$. Therefore, there are infinitely many primes. □

What is even more fascinating is that there are infinitely many primes of different forms. Some basic, well-known ones are $4k + 1$, $3k + 2$, $8k + 7$, and $6k + 5$, where $k \in \mathbb{N}$. The methods used to prove that infinitely many primes of these forms exist differ from form to form, and they are not relevant to our later discussions, so we will examine only one such proof.

Exercise 3.3. There are infinitely many primes of the form $4k + 3$, where $k \in \mathbb{N}$.

Proof. Let $p_1 = 3$ and consider the primes $p_1, \ldots, p_n$, where $n \in \mathbb{N}$. Define q as

$$q = 4(p_1 \cdots p_n) - 1.$$

The integer q is of the form $4k+3$, because all integers of the form $4k-1$ are equal to $4(k-1)+3$. Suppose there exists p_k such that $1 \leq k \leq n$ and $p_k | q$. We know $p_k | 4(p_1 \cdots p_n) = q + 1$, so there exist $m, n \in \mathbb{N}$ such that $mp_k | q$ and $np_k | q + 1$. Subtraction yields $(m - n)p_k = 1$, which implies $p_k | 1$, which is a contradiction. Hence q has no prime factors less than or equal to p_n.

Note that if $\alpha, \beta \in \mathbb{N}$ such that α, β are of the form $4k+1$, then $\alpha\beta$ is also of the form $4k+1$. This can be extended by induction for any number of positive integers of the form $4k + 1$. Since q is of the form $4k + 3$, it follows that it must have at least one prime factor of the form $4k + 3$. We can repeat this procedure for any such q (for instance, $q_2 = 4(p_1 \cdots p_r) - 1$, where p_r is the first prime greater than q) to obtain that there always exists a larger prime of the form $4k + 3$, and hence that there are infinitely many such primes. □

Dirichlet proved a general theorem about the infinitude of certain forms of primes:

Theorem 3.4 (Dirichlet's Theorem)**.** *If a and b are positive integers such that $\gcd(a, b) = 1$, then there are infinitely many primes of the form $ak + b$, where $k \in \mathbb{N}$.*

We will not prove this theorem in this paper.

4. Euler's Totient Function

We now come to one of the most useful functions we will use to study number theory.

Definition 4.1 (Euler's Totient Function)**.** The *totient function* $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ is defined as

$$\varphi(n) \coloneqq \#\{x \in \mathbb{N} \colon 1 \leq x \leq n \text{ and } \gcd(x, n) = 1\},$$

and it yields the number of positive integers less than and coprime to n.

Remark 4.2. It is simple to verify that $\varphi(x) \geq 2$ for all positive integers $x \neq 1$, and that p is prime if and only if $\varphi(p) = p - 1$.

In this section, we will derive some properties of φ, and we will heavily rely on Euler's totient function and these properties throughout the rest of this paper. It is useful to have a formula to calculate $\varphi(n)$ for any $n \in \mathbb{N}$, and we will derive such a formula, and introduce several other concepts in number theory, in the following proofs.

Lemma 4.3. *If p and a are positive integers and p is prime, then $\varphi(p^a) = p^a(1-\frac{1}{p})$.*

Proof. Since p is prime, the only positive integers that are not coprime with p^a are the multiples of p, so we must count the number of multiples of p. We have $p, 2p, \ldots, p^{a-1}p$, since $p^{a-1}p = p^a$. Hence there are p^{a-1} positive integers that are not coprime with p^a, so we must subtract p^{a-1} from p^a to obtain the value of φ:

$$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1) = p^a(1 - \frac{1}{p}).$$

□

Definition 4.4. Let a and n be positive integers. If there exists a positive integer a^{-1} satisfying

$$a(a^{-1}) \equiv 1 \pmod{n},$$

then we call a^{-1} a *modular multiplicative inverse*, or simply a *modular inverse*, of $a \pmod{n}$. If a has a modular inverse, then we say that it is *invertible* $\pmod{n}$.

modular inverses are powerful, and they will help us derive a formula for $\varphi(n)$ and pursue other topics.

Theorem 4.5. *A modular inverse of a positive integer $a \pmod{n}$ exists if and only if $\gcd(a, n) = 1$.*

Proof. Suppose $x = a^{-1}$ exists. Then $ax \equiv 1 \pmod{n}$, so there exist $j, k \in \mathbb{Z}$ such that $jn = kax - 1$. Thus 1 is a $\mathbb{Z}-$linear combination of a and n, and it follows that $\gcd(a, n) = 1$, by Bézout's identity.

Now suppose $\gcd(a, n) = 1$. Then there exist $j, k \in \mathbb{Z}$ such that $ja + kn = 1$, and hence $ja + kn \equiv 1 \pmod{n}$. As $kn \equiv 0 \pmod{n}$, we are left with $ja \equiv 1 \pmod{n}$, so $j = a^{-1}$ exists. The proof is thus complete. □

We often wish to find solutions to *linear congruences*, that is, equations of the form $ax \equiv b \pmod{n}$, where a, b, n are known and x is unknown. From this, we naturally desire to solve *systems of linear congruences*, which comprise multiple congruences and potentially multiple unknown variables. The Chinese remainder theorem provides a method for solving certain systems of linear congruences of a certain form, and it thus serves as yet another powerful tool.

Theorem 4.6 (Chinese Remainder Theorem)**.** *Let $n_1, \ldots, n_r$ be positive integers such that the $n_1, \ldots, n_r$ are pairwise coprime; that is, $\gcd(n_i, n_j) = 1$ for all $i, j \in \mathbb{N}$ between 1 and r such that $i \neq j$. Then there exists exactly one solution x modulo $\prod_{i=1}^{r} n_i$ to the system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ &\vdots \\ x &\equiv a_r \pmod{n_r}. \end{aligned}$$

Proof. For all j such that $1 \leq j \leq r$, define $k_j \in \mathbb{N}$ as

$$k_j = \frac{1}{n_j} \prod_{i=1}^{r} n_i.$$

Since all n_i are coprime, $\gcd(k_j, n_j) = 1$ for all j. Therefore, each k_j has a modular inverse $\pmod{n_j}$, which we respectively denote ${k_j}^{-1}$. Define x as

$$x = \sum_{i=1}^{r} a_i k_i {k_i}^{-1}$$

and fix some positive integer s such that $s \leq r$. We have

$$x \equiv a_s k_s {k_s}^{-1} \pmod{n_s},$$

because all $a_t k_t {k_t}^{-1}$ are divisible by n_s except when $t = s$, by the definition of k_j. By the definition of k_s^{-1}, we know $k_s {k_s}^{-1} \equiv 1 \pmod{n_s}$; thus $x \equiv a_s \pmod{n_s}$. This is true for all $s \leq r$, so x satisfies all of the linear congruences and is thus a solution.

Now we must show x is unique modulo $n_1 \cdots n_r$. Suppose a positive integer z satisfies the linear congruences; that is, let $z \equiv a_t \pmod{n_t}$ for all $t \leq r$. For any $t \leq r$, we have both $z \equiv a_t \pmod{n_t}$ and $x \equiv a_t \pmod{n_t}$. Hence, by the symmetric and transitive properties of congruence relations, $z \equiv x \pmod{n_t}$ for all $t \leq r$, and since all n_s are coprime, we have $z \equiv x \pmod{n_1 \cdots n_r}$. Therefore, x is a unique solution modulo $n_1 \cdots n_r$. □

With the Chinese remainder theorem, we can prove the following arithmetic property of the totient function.

Lemma 4.7. *The totient function is multiplicative for coprime positive integers. That is, if m and n are positive integers and $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. Let

$$A \coloneqq \{a \in \mathbb{N} \colon a \leq mn \text{ and } \gcd(a, mn) = 1\}$$

and

$$B \coloneqq \{(b, c) \in \mathbb{N}^2 \colon b \leq m, c \leq n, \gcd(b, m) = 1, \text{ and } \gcd(c, n) = 1\}.$$

It follows from the definition of φ that $\#(A) = \varphi(mn)$ and $\#(B) = \varphi(m)\varphi(n)$. We will show that there exists a bijection between A and B.

Define $f : A \longrightarrow B$ by $f(a) = (a \pmod{m}, a \pmod{n})$.

If $f(a_1) = f(a_2)$, then

$$(a_1 \pmod{m}, a_1 \pmod{n}) = (a_2 \pmod{m}, a_2 \pmod{n}),$$

so $a_1 \equiv a_2 \pmod{m}$ and $a_1 \equiv a_2 \pmod{n}$. By the Chinese remainder theorem, $a_1 \equiv a_2 \pmod{mn}$. Hence $a_1 = a_2$. This is true for all such a_1 and a_2, so f is injective.

Now let $(b, c) \in B$. We wish to find an $a \in A$ satisfying $f(a) = bc$. In other words, we wish to find an $a \in \{1, \ldots, mn\}$ coprime with mn such that $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$. We showed in the Chinese remainder theorem that such an a exists, since this is simply a system of linear congruences. Since $\gcd(m, n) = 1$, this is true for all $(b, c) \in B$, so f is surjective.

Since f is surjective and injective, it is bijective, so $\#(A) = \#(B)$; that is,

$$\varphi(mn) = \varphi(m)\varphi(n).$$

□

Note that we can extend this multiplicative property to any number of coprime positive integers $a_1, \ldots, a_k$ by induction. That is, if $a_1, \ldots, a_k$ are all pairwise coprime, then

$$\varphi(\prod_{i=1}^{k} a_i) = \prod_{i=1}^{k} \varphi(a_i).$$

We use this property in the following proof, which gives us a general formula for $\varphi(n)$.

Theorem 4.8. *Let n be a positive integer greater than 1 and $n = \prod_{i=1}^{k} p_i^{c_i}$ be its prime power factorization. Then*

$$\varphi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

Proof. All of the primes in the prime power factorization of n are coprime with one another. Since n is the product of its prime factors raised to powers, we have

$$\varphi(n) = \varphi(\prod_{i=1}^{k} p_i^{c_i}),$$

by substitution. By Lemma 4.7, this is equivalent to

$$\prod_{i=1}^{k} \varphi(p_i^{c_i}),$$

which, by Lemma 4.3, is equal to

$$\prod_{i=1}^{k} p_i^{c_i}(1 - \frac{1}{p_i}).$$

Finally, since $n = \prod_{i=1}^{k} p_i^{c_i}$, the above is equal to

$$n \prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

The proof is thus complete.

□

5. Reduced Residue Systems, Euler's Totient Theorem, and Order

Now we introduce reduced residue systems and prove some of their properties.

Definition 5.1. Let n be a positive integer. A *reduced residue system modulo n* is a set of positive integers

$$S_n \coloneqq \{r_1, \ldots, r_{\varphi(n)}\}$$

satisfying the following conditions.

(1) for each $i \in \mathbb{N}$ such that $1 \leq i \leq \varphi(n)$, we have $\gcd(r_i, n) = 1$;
(2) for each $i, j \in \mathbb{N}$ such that $1 \leq i \leq \varphi(n)$, $1 \leq j \leq \varphi(n)$, and $i \neq j$, we have $r_i \not\equiv r_j \pmod{n}$.

Remark 5.2. All of the r_i are the distinct residues $\pmod{n}$ and there are exactly $\varphi(n)$ of them; That is, $\#(S_n) = \varphi(n)$. This follows from the definition of $\varphi(n)$ and the fact that $\gcd(r_i, n) = 1$ for all $r_i \in S_n$.

Also note that a reduced residue system need not contain only least positive residues. For example, one reduced residue system modulo 12 is $\{1, 5, 7, 11\}$, but $\{13, 17, 19, 23\}$ and $\{5, 25, 35, 55\}$ are as well.

Lemma 5.3. *Let n be a positive integer and S_n be a reduced residue system modulo n and let $a \in \mathbb{N}$ such that $a \in S_n$. Then a^{-1} modulo n exists, and a positive residue a^{-1} modulo n is in S_n. That is, for any $a \in S_n$, the modular inverse of a (or a positive residue of the inverse, modulo n) is also in S_n.*

Proof. Let S_n be a reduced residue system $\pmod{n}$ and let $a \in S_n$. Then a^{-1} exists and a positive residue a^{-1} is in S_n, by Theorem 4.5.

□

Lemma 5.4. *Let n be a positive integer. If $S_n = \{r_1, \ldots, r_{\varphi(n)}\}$ is a reduced residue system modulo n and a is a positive integer such that $\gcd(a, n) = 1$, then the set $aS_n = \{ar_1, \ldots, ar_{\varphi(n)}\}$ is a reduced residue system modulo n.*

Proof. Fix $i \leq \varphi(n)$. Since $\gcd(r_i, n) = 1$ and $\gcd(a, n) = 1$, it follows that $\gcd(ar_i, n) = 1$. This is true for all i, so the first criterion is satisfied.

Now suppose that $ar_i \equiv ar_j \pmod{n}$ for some i and j. Since $\gcd(a, n) = 1$, we know by Theorem 4.5 that a has an inverse $a^{-1} \pmod{n}$, so we have $aa^{-1} \equiv 1 \pmod{n}$. By multiplication, we have $a^{-1}ar_i \equiv a^{-1}ar_j \pmod{n}$ and thus $r_i \equiv r_j \pmod{n}$. Since S_n is a reduced residue system, this is only possible if $i = j$. Therefore $ar_i \equiv ar_j \pmod{n}$ only if $i = j$, so the elements of aS_n must be distinct $\pmod{n}$. The two criteria of Definition 5.1 are satisfied, so aS_n is a reduced residue system modulo n. □

With these properties of reduced residue systems, we can prove the following result, which involves Euler's totient function.

Theorem 5.5 (Euler's Totient Theorem)**.** *Let a and n be positive integers such that $\gcd(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof. Let $S = \{r_1, \ldots, r_{\varphi(n)}\}$ be a reduced residue system modulo n. Since $\gcd(a, n) = 1$, it follows from the previous lemma that the set $aS = \{ar_1, \ldots, ar_{\varphi(n)}\}$ is also a reduced residue system modulo n. It follows from the definition of reduced residue systems that the sets S and aS have the same elements modulo n; that is, their least positive residues when divided by n are equal. Therefore, the product of

all of the residues in S must equal the product of all of the residues in aS, modulo n:

$$r_1 \cdots r_{\varphi(n)} \equiv (ar_1) \cdots (ar_{\varphi(n)}) \pmod{n}.$$

All of the r_i have the property that $\gcd(r_i, n) = 1$. Hence they are invertible modulo n, so we can multiply this congruence by the product of the inverses of the residues to obtain

$$r_1{}^{-1} r_1 \cdots r_{\varphi(n)}{}^{-1} r_{\varphi(n)} \equiv (ar_1{}^{-1} r_1) \cdots (ar_{\varphi(n)}{}^{-1} r_{\varphi(n)}) \pmod{n}.$$

Since $r_i{}^{-1} r_i \equiv 1 \pmod{n}$ for all i, and since there are $\varphi(n)$ residues and thus $\varphi(n)$ instances of a, this simplifies to

$$1 \equiv a^{\varphi(n)} \pmod{n},$$

as required. □

We now use Euler's totient theorem to prove Fermat's little theorem, which is used in the probabilistic Fermat primality test and to help prove theorems used in other primality tests.

Corollary 5.6 (Fermat's Little Theorem)**.** *Let a and p be positive integers such that p is prime and $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$. If $p \mid a$, then $a^p \equiv a \pmod{p}$.*

Proof. We first consider a prime p such that $p \nmid a$. Since $p \nmid a$, we know $\gcd(p, a) = 1$, so we can apply Euler's totient theorem. Since p is prime, we know $\varphi(p) = p - 1$, so we simply have $a^{p-1} \equiv 1 \pmod{n}$, as required.

If $p \mid a$, then $a^n \equiv 0 \pmod{p}$ for all positive integers n and $a \equiv 0 \pmod{p}$ Therefore, $a^p \equiv 0 \pmod{p}$. □

Indeed, Euler's totient theorem and Fermat's little theorem are very similar: Euler's is a more general statement of Fermat's.

Now we discuss modular order, which we will use when proving primality test theorems in the next section.

Definition 5.7. Let a and n be positive integers satisfying $\gcd(a, n) = 1$. The *multiplicative order*, or simply the *order*, of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. We denote the order as $\operatorname{ord}_n a$.

Theorem 5.8. *Let a and n be positive integers. If $\gcd(a, n) = 1$, then $\operatorname{ord}_n a$ exists.*

Proof. The powers of a modulo n are limited to at most n positive integers. Since $\mathbb{N}$ is infinite, we know by the pigeonhole principle that there exist positive integers b and c such that $c > b$ and $a^b \equiv a^c \pmod{n}$. Since $\gcd(a, n) = 1$, we know a has a multiplicative inverse, a^{-1}. We can therefore multiply $a^b \equiv a^c \pmod{n}$ by a^{-b} to obtain $a^{c-b} \equiv 1 \pmod{n}$. If there is no positive integer less than $c - b$ satisfying the definition of ord, then $c - b = \operatorname{ord}_n a$. □

Definition 5.9. Let a and n be positive integers such that $\gcd(a, n) = 1$. We call a a *primitive root modulo n* if $\operatorname{ord}_n a = \varphi(n)$.

We will not discuss primitive roots in this paper, although they can be helpful to keep in mind while working through the following proofs.

Exercise 5.10. Let a and n be positive integers such that $\gcd(a, n) = 1$. Then $a^m \equiv 1 \pmod{n}$ if and only if $\operatorname{ord}_n a | m$.

Proof. Suppose $\operatorname{ord}_n a | m$. Then there exists $c \in \mathbb{N}$ such that $c \cdot \operatorname{ord}_n a = m$. Since $a^{\operatorname{ord}_n a} \equiv 1 \pmod{n}$, it follows that $a^{c \cdot \operatorname{ord}_n a} \equiv 1 \pmod{n}$; that is, $a^m \equiv 1 \pmod{n}$.

Now suppose $a^m \equiv 1 \pmod{n}$. We wish to divide m by $\operatorname{ord}_n a$ and show that the residue is 0, so we apply the division algorithm to find that there exist $q, r \in \mathbb{N}$ such that $m = q \cdot \operatorname{ord}_n a + r$. By substitution,

$$a^{q \cdot \operatorname{ord}_n a} a^r \equiv 1 \pmod{n}.$$

Since $\operatorname{ord}_n a | q \cdot \operatorname{ord}_n a$, we know $a^{q \cdot \operatorname{ord}_n a} \equiv 1 \pmod{n}$, as shown in the first direction. Therefore $a^r \equiv 1 \pmod{n}$. Since $0 \leq r < \operatorname{ord}_n a$ by the division algorithm and $\operatorname{ord}_n a$ is defined as being the smallest positive integer e such that $a^e \equiv 1 \pmod{n}$, it follows that $r = 0$. Therefore $m = q \cdot \operatorname{ord}_n a$, so $\operatorname{ord}_n a | m$. □

We finish this section with an exercise which will help us prove theorems used in primality tests.

Exercise 5.11. Let x and p be positive integers such that p is prime. Then $x^2 \equiv 1 \pmod{p}$ if and only if $x \equiv \pm 1 \pmod{p}$.

Proof. Suppose $x \equiv \pm 1 \pmod{p}$. Squaring both sides yields $x^2 \equiv 1 \pmod{p}$. Now suppose that $x^2 \equiv 1 \pmod{p}$. This implies that $p | (x-1)(x+1)$. Since p is prime, either $p | x-1$ or $p | x+1$. If $p | x-1$, then $x \equiv 1 \pmod{p}$, and if $p | x+1$, then $x \equiv -1 \pmod{p}$. Hence $x \equiv \pm 1 \pmod{p}$. □

6. Primality Tests

We now prove some theorems that are used in historically significant primality tests. We first examine the Rabin-Miller theorem, which is used in the probabilistic Rabin-Miller primality test.

Theorem 6.1 (Rabin-Miller Theorem)**.** *Let p be an odd prime and let a be a positive integer such that $\gcd(a, p) = 1$. Factor $p - 1$ as $p - 1 = 2^e q$ for some odd $q \in \mathbb{N}$. Then either*

(1) $a^q \equiv 1 \pmod{p}$; or

(2) there exists $i \in \{0, \ldots, e-1\}$ such that $a^{2^i q} \equiv -1 \pmod{p}$.

Proof. Since $p - 1 = 2^e q$, we know

$$a^{p-1} = a^{2^e q} = a^{2 \cdot 2^{e-1} q} = (a^{2^{e-1} q})^2.$$

Since $\gcd(a, p) = 1$, we know $p \nmid a$, so we can apply Fermat's little theorem to obtain

$$a^{p-1} = (a^{2^{e-1} q})^2 \equiv 1 \pmod{p}.$$

By Exercise 5.11, we have

$$a^{2^{e-1} q} \equiv \pm 1 \pmod{p}.$$

If $a^{2^{e-1} q} \equiv -1 \pmod{p}$, then we fulfill the second condition and are done. Otherwise, if $a^{2^{e-1} q} \equiv 1 \pmod{p}$, then we can apply the process we applied above to obtain

$$a^{2^{e-2} q} \equiv \pm 1 \pmod{p}.$$

If we never obtain a congruence with -1 by repeating this process, then we eventually come to $a^{2^0 q} \equiv 1 \pmod{p}$ and thus $a^q \equiv 1 \pmod{p}$, fulfilling the first condition. □

Next we prove Wilson's theorem, which is itself a primality test.

Theorem 6.2 (Wilson's Theorem)**.** *A positive integer p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.*

Proof. If $p = 2$, then we have $(2-1)! = 1 \equiv -1 \pmod{2}$.

Now suppose p is prime and $p > 2$; then p is odd. Because p is prime, we know that for all $a \in \mathbb{N}$ such that $1 \leq a \leq p-1$, we have $\gcd(a, p) = 1$. Hence $S_p = \{1, \ldots, p-1\}$ is a reduced residue system of p. By Lemma 5.3, each residue $a \in S_p$ has an inverse modulo p that is also in S_p. We first desire to find all of the $a \in S_p$ such that $a \equiv a^{-1} \pmod{p}$. If $a \equiv a^{-1} \pmod{p}$, then $a^2 \equiv 1 \pmod{p}$. It follows from Exercise 5.11 that $a \equiv \pm 1 \pmod{p}$. This means that if $a \equiv 1 \pmod{p}$, then a is in the same congruence class as 1, and if $a \equiv -1 \pmod{p}$, then a is in the same congruence class as $p-1$. Hence, the only two values of a that are their own inverses modulo p are 1 and $p-1$. Now we evaluate $(p-1)!$ modulo p, substituting based on the above results:

$$\begin{aligned}(p-1)! &\equiv 1 \cdot 2 \cdots (p-2) \cdot (p-1) \pmod{p} \\ &\equiv 2 \cdots (p-2) \cdot (p-1) \pmod{p} \\ &\equiv -(2 \cdots (p-2)) \pmod{p}.\end{aligned}$$

As shown above, each least positive residue modulo p is in S_p and has an inverse in S_p. For each pair of a residue a and its inverse a^{-1}, we have $aa^{-1} \equiv 1 \pmod{p}$. We can therefore simplify the above congruence to yield

$$(p-1)! \equiv -1 \pmod{p}.$$

Now suppose that $(p-1)! \equiv -1 \pmod{p}$ and assume that p is composite. Then there exist $a, b \in \mathbb{N}$ such that $1 < a$, $b < p$, and $p = ab$. It follows that $a|(p-1)!$ and $a|p$. Therefore, there exist $c, d \in \mathbb{N}$ such that $ac = (p-1)!$ and $ad = p$. By substitution into $(p-1)! \equiv -1 \pmod{p}$, we have $ac \equiv -1 \pmod{ad}$, which implies $a|1$ and thus contradicts the inequality $1 < a < p$. We can form an identical contradiction with b, so p is not composite; therefore, p is prime. □

Note that Wilson's theorem is not helpful if p is sufficiently large, because for a large enough p, calculating $(p-1)!$ would be expensive.

There is also a primality test for integers of the form $2p+1$, where p is prime. It relies upon modular order.

Theorem 6.3. *Let p and n be positive integers. Suppose p is prime and let $n = 2p+1$. If*

$$2^{n-1} \equiv 1 \pmod{n} \quad \text{and} \quad 3 \nmid n,$$

then n is prime.

Proof. Let $q \in \mathbb{N}$ be prime and suppose $q|n$. The positive integer $n = 2p+1$ is odd, so q must also be odd. By substitution, $2^{n-1} = 4^p \equiv 1 \pmod{n}$. We thus know that there exists α such that $4^p - 1 = \alpha n$. Since $q|n$, there exists β such that $\beta q = n$, so we have $4^p - 1 = (\alpha\beta)q$. Therefore,

$$2^{n-1} = 4^p \equiv 1 \pmod{q}.$$

It follows that $\operatorname{ord}_q 4|p$, and since p is prime, $\operatorname{ord}_q 4$ is either 1 or p. If $\operatorname{ord}_q 4 = 1$, then $4^1 \equiv 1 \pmod{q}$, and this implies $q = 3$. Since $q|n$ by assumption, we would thus have $3|n$, which would contradict our hypothesis. Thus we deduce $\operatorname{ord}_q 4 = p$. By Euler's totient theorem, since $\operatorname{ord}_q 4|\varphi(q)$ and q is prime, we have $p|q-1$, by substitution.

Since $p|q-1$, we know $p \leq q-1$ and thus $q \geq p+1$. Since $n = 2p+1$, we know $\frac{n}{2} = p + \frac{1}{2}$, so $p+1 > \frac{n}{2}$. Since $p \geq 2$, we know $n \geq 5$, so it follows that $\frac{n}{2} > \sqrt{n}$. We thus have the inequality

$$q \geq p+1 > \frac{n}{2} > \sqrt{n},$$

which is true for every prime factor q of n. But this implies $q = n$ and n is prime, because composite numbers have at least two factors k_1 and k_2 satisfying $k_1 \leq \sqrt{n} \leq k_2$. □

The Lucas primality test theorem can also be proven using the concept of modular order.

Theorem 6.4 (Lucas Primality Test)**.** *Let a and n be positive integers. Suppose $a^{n-1} \equiv 1 \pmod{n}$ and that for all primes $q \in \mathbb{N}$ such that $q \mid n-1$, we have $a^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$. Then n is prime.*

Proof. Let $r = \operatorname{ord}_n a$. By the first part of our hypothesis, and by Exercise 5.10, it follows that $r|n-1$. Hence there exists $k \in \mathbb{N}$ such that $kr = n-1$. Assume $k > 1$, which implies $n-1 > r$. Now let $q \in \mathbb{N}$ be prime and suppose $q|k$. Since $kr = n-1$ and $q|k$, there exists $\alpha \in \mathbb{N}$ such that $\alpha q = k$, and thus $(\alpha r)q = n-1$. Hence $q|n-1$, fulfilling the second part of our hypothesis.

Now consider $a^{\frac{n-1}{q}}$. Since $kr = n-1$, we know $a^{\frac{n-1}{q}} = (a^r)^{\frac{k}{q}}$. Since $r = \operatorname{ord}_n a$, we know $a^r \equiv 1 \pmod{n}$ by definition, so we have $(a^r)^{\frac{k}{q}} \equiv 1^{\frac{k}{q}} = 1 \pmod{n}$. Therefore, $a^{\frac{n-1}{q}} \equiv 1 \pmod{n}$, but this contradicts the second part of our hypothesis, so we now know $k = 1$ and thus $n-1 = r = \operatorname{ord}_n a$.

Since $a^{n-1} \equiv 1 \pmod{n}$, there exists β such that $\beta n = a^{n-1} - 1$ and therefore

$$1 = a^{n-1} - \beta n = (a^{n-2})a + (-\beta)n.$$

Hence 1 is a $\mathbb{Z}-$linear combination of a and n, so by Bézout's identity, we know $\gcd(a, n) = 1$. We can thus use Theorem 5.5 and the definition of ord to deduce $\operatorname{ord}_n a|\varphi(n)$, so $\operatorname{ord}_n a = n-1 \leq \varphi(n)$. But by the definition of $\varphi(n)$, we know $\varphi(n) \leq n-1$. Hence we have $n-1 \leq \varphi(n) \leq n-1$, so $\varphi(n) = n-1$. By Remark 4.2, it follows that n is prime. □

The Pocklington criterion is itself a primality test, but it is also used in the more general Pocklington-Lehmer primality test.

Theorem 6.5 (Pocklington Criterion)**.** *Let n be a positive integer such that $n-1 = FR$, where F and R are positive integers and $\gcd(F, R) = 1$. Suppose that there exists $a \in \mathbb{N}$ such that*

$$a^{n-1} \equiv 1 \pmod{n} \quad \text{and} \quad \gcd(a^{\frac{n-1}{q}} - 1, n) = 1$$

for all primes $q|F$. Then for each prime $p \in \mathbb{N}$ such that $p|n$, we have $p \equiv 1 \pmod{F}$. Furthermore, if $F \geq \sqrt{n}$, then n is prime.

Proof. Let p be a prime dividing n. By our hypothesis, $a^{n-1} \equiv 1 \pmod{p}$, since $p|n$. Now let q be a prime such that $q|F$ and q^α is the largest power of q dividing F, and suppose that $a^{\frac{n-1}{q}} \equiv 1 \pmod{p}$. This implies $p|a^{\frac{n-1}{q}} - 1$. But since $p|n$, this would mean $\gcd(a^{\frac{n-1}{q}} - 1, n) > 1$, contradicting our hypothesis. Therefore $a^{\frac{n-1}{q}} \not\equiv 1 \pmod{p}$.

Now let $r = \operatorname{ord}_p a$. By the above results and the definition of ord, we know $r|n-1$ and $r \nmid \frac{n-1}{q}$. Since $n - 1 = FR$ and $q^\alpha|F$, we can write $n - 1 = q^\alpha t$ for some $t \in \mathbb{N}$, and thus $r|q^\alpha t$ and $r \nmid \frac{q^\alpha t}{q} = q^{\alpha-1}t$. From these, we can deduce $q^\alpha|r$. This is true for all prime factors q of F, so it follows that $F|r$. Since p is prime, $\varphi(p) = p - 1$, and by the definition of ord and by Euler's totient theorem, we know $r|p-1$. Therefore, $F|p-1$. Thus $p \equiv 1 \pmod{F}$, as required. This is true for all prime factors p of n.

We lastly show that if $F \geq \sqrt{n}$, then n is prime. Suppose $F \geq \sqrt{n}$. If n were composite, then it would have at least one prime factor p satisfying $p \leq \sqrt{n}$. However, we just showed that for all prime factors p of n, we have $p \equiv 1 \pmod{F}$. This implies that there exists γ such that $\gamma F = p - 1$ and thus $\gamma F + 1 = p$. The smallest positive value p could have (when $\gamma = 1$) is thus $F + 1$, which is strictly greater than $\sqrt{n}$, since we assumed $F \geq \sqrt{n}$. Therefore, all prime factors p of n are greater than $\sqrt{n}$, so n must be prime. □

We finish by proving a specific case of the Pocklington criterion, which is given by Proth.

Corollary 6.6 (Proth's Theorem)**.** *Let n, k, and m be positive integers such that k is odd, $m \geq 2$, and $k < 2^m$. Define n as $n = k \cdot 2^m + 1$ and suppose that there exists a positive integer a such that $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. Then n is prime.*

Proof. Let $F = 2^m$ and $R = k$; then we have $n - 1 = FR$ and $\gcd(F, R) = 1$ since F is even and R is odd. Since we are given $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$, we have $a^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}$, and we can square the congruence to obtain $a^{n-1} \equiv 1 \pmod{n}$. Hence $\gcd(a^{\frac{n-1}{q}}, n) = 1$ for $q = 2$, the only prime q such that $q|F$. Since $k < 2^m$, we know $R < F$, and since $n = FR + 1$, it follows that $F \geq \sqrt{n}$. Hence the requirements of the Pocklington criterion are met, so n is prime. □

There are, of course, many other primality tests we could discuss, several of which are related to and build on the ones we have proven here (such as Pépin's test, which is an alteration of Proth's test). The background and methods provided in this paper are hopefully sufficient to further study primality tests, as well as number theory in general.

Acknowledgments. I thank my mentors, Zhiyuan Ding and Quoc Ho, for continuously supporting my efforts and for suggesting several introductory number theory books, which I used and found invaluable. I also thank Peter May, director of the REU program, and everyone else who made the REU possible, for supporting my exploration of mathematics this summer.

References

[1] Peter Giblin. Primes and Programming. Cambridge University Press. 1993.
[2] G. H. Hardy and E. M. Wright. An Introduction to the Theory of Numbers (Fifth Edition). Oxford University Press. 1979.
[3] Firas Kraïem. Primality Testing, Part 1: Compositeness Tests, Fermat and Rabin-Miller. Firas Kraïem. 2013.
http://blog.fkraiem.org/2013/04/08/primality-testing-part-1-compositeness-tests-fermat-and-rabin-miller/
[4] Benjamin Lynn. Number Theory – The Chinese Remainder Theorem. Applied Cryptography Group. Stanford University.
http://crypto.stanford.edu/pbc/notes/numbertheory/crt.html
[5] Victor Shoup. A Computational Introduction to Number Theory and Algebra (Version 1). Cambridge University Press. 2005.
[6] Eric W. Weisstein. Congruence. MathWorld – A Wolfram Web Resource.
http://mathworld.wolfram.com/Congruence.html
[7] Euler's Phi Function and the Chinese Remainder Theorem. The Oxford Math Center. Oxford College of Emory University.
http://www.oxfordmathcenter.com/drupal7/node/172