Some Methods of Primality Testing

by
Jesse Krauel

A project submitted to the Department of
Mathematical Sciences in conformity with the requirements
for Math 4301 (Honours Seminar)

Lakehead University
Thunder Bay, Ontario, Canada

Abstract

Given an integer, how can we decide whether it is prime or composite? In this paper, we explore different answers to this question. Beginning with some basic properties of primes, we then describe Eratosthenes' method of sieving out the composites from a finite, ordered list of positive integers. We give quick tests to determine if the numbers 2, 3, 5 or 11 are divisors of a given integer and discuss the classical method of trial division, as well as testing integers via Wilson's Theorem and Fermat's Little Theorem. More recent results, including Lucas' converse of Fermat's Little Theorem, the Miller-Rabin test and the Agrawal-Kayal-Saxena (AKS) test are also presented.

To my parents,
for never having doubted my dreams.

Acknowledgements

I would like to thank both of my supervisors, Dr. Adam Van Tuyl and Dr. Jennifer Biermann, for their guidance throughout the preparation of this paper. During our weekly seminar, Dr. Greg Lee also provided valuable input.

Contents

CHAPTER 1

Introduction

Among the set of integers are those elements which are reducible through multiplication and those which are not. This distinction among the positive integers is our main focus. We ask how we can decide whether or not a given integer $n > 1$ is reducible through multiplication. Let us define what it is we mean by the term "reducible".

DEFINITION 1.1. Let m, n be integers with $m \neq 0$. If $n = km$ for some integer k, we say that m *is a divisor of* n or m *divides* n and write $m \mid n$. Similarly, we say that m *does not divide* n and write $m \nmid n$ if $n \neq km$ for any integer k

Notice that we can always write $n = (\pm 1)(\pm n)$, regardless of the choice of n. So the integers $\pm 1, \pm n$ are always divisors of n and we refer to them as the *trivial divisors* of n. Some integers have only trivial divisors, while others have more. The integers with only trivial divisors are of special interest and deserve a name.

DEFINITION 1.2. An integer $n > 1$ is *prime* if its only divisors are ± 1 and $\pm n$, that is, if it has only trivial divisors.

EXAMPLE 1.3. By our definition, the integers 0 and 1 cannot be prime, but the integer 2 is prime as it only has trivial divisors.

A consequence of Example 1.3 is that any integer multiple $2n$ of 2 which is greater than 2 cannot be prime since then $2n$ will possesses $\pm 2 \neq \pm 1,\ \pm 2n$ as divisors. Of course, this result holds for any integer multiple np of a prime p, with $n > 1$. We have a name for these multiple values as well.

DEFINITION 1.4. An integer $n > 1$ is *composite* if it is not prime. This means that $n = ab$ for two integers a, b with $1 < a < n$ and $1 < b < n$, and we call any a, b with this property *nontrivial divisors* of n.

The goal of this paper is to look at the problem of how to determine if an integer is prime or composite. The problem of primality testing is of interest in itself. Perhaps Gauss said it best in his *Disquisitiones Arithmeticae* of 1801[**4**]:

> The problem of distinguishing prime numbers from composite numbers, and of resolving the latter into their prime [divisors] is known to be one of the most important and useful in arithmetic. ... Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.

In this paper, we concern ourselves with the properties of primes which allow us to derive methods to check if a given integer is prime. We provide theorems from which we can derive tests for primality or compositeness. Some tests will be stronger than others, and some will be more practical. Those tests which allow us to decide with absolute certainty whether an integer is prime or composite are referred to as deterministic tests.

Our paper is structured as follows. In Chapter 2, we recall some basic properties of primes and introduce some naive primality tests. Chapter 3 focuses on some classical theorems regarding primes. Specifically, we will optimize the method known as trial division and explore both Fermat's Little Theorem and Wilson's Theorem. Chapter 4 handles some more recent results: Lucas' converse of Fermat's Little Theorem, the Miller-Rabin test and the Agrawal-Kayal-Saxena (AKS) test. Chapter 5 contains our conclusions. Throughout this paper, we use log for base 2 logarithms and ln for natural logarithms.

CHAPTER 2

Preliminaries

In this chapter, we will recall some properties of primes and divisibility from a course in abstract algebra. We will begin with the theorems which outline the importance of the primes among the set of integers. Then we will describe a method to find all the primes less than or equal to a given integer. In the final section, we will develop some tests to determine whether specific numbers are divisors of a given integer.

1. Properties of Primes

Primes are the essential building blocks of the positive integers with respect to multiplication. It is for this reason that primes are so important, as the following theorem justifies.

THEOREM 2.1. *Let $p > 1$ be an integer. Then p is prime if and only if p has the property that whenever $p \mid ab$, then $p \mid a$ or $p \mid b$.*

The proof of this theorem is omitted since it requires several prior theorems. A proof can be found in [**5**].

EXAMPLE 2.2. Composites do not have this desirable property. For example, we have $4 \mid 12 = 2 \cdot 6$ but $4 \nmid 2$ and $4 \nmid 6$.

Given a composite integer $n > 1$, we can factor n as a product of primes. For example,

$$30 = 6 \cdot 5 = 2 \cdot 3 \cdot 5 \quad \text{and}$$

$$148 = 4 \cdot 39 = 2^2 \cdot 3 \cdot 13.$$

THEOREM 2.3. *Every integer $n > 1$ is either prime or a product of primes.*

PROOF. Let $P(n)$ be the statement "n is prime or a product of primes" and note that $P(2)$ is true since 2 is prime. By induction, assume $P(m)$ is true for all m with $2 \leq m < n$.

The integer n is either prime or composite. If n is prime, then the statement $P(n)$ is true. If n is composite, then $n = ab$ for some positive integers a, b with $1 < a < n$ and $1 < b < n$. Since both $a < n$ and $b < n$ we have that both $P(a)$ and $P(b)$ hold true. This means that both a and b are prime or products of primes. Then $n = ab$ is a product of primes and the statement $P(n)$ is true. □

For composite n, we can ask if their prime factorization is unique. The Fundamental Theorem of Arithmetic settles this question.

THEOREM 2.4 (The Fundamental Theorem of Arithmetic). *Every integer $n > 1$ is either prime or a product of primes. This factorization is unique up to the arrangement of its divisors.*

Again, the proof of this theorem is omitted due to its length, and can be found in [**5**]. At this point, it is natural to ask whether there are only finitely many primes. As one can imagine, the situation would be rather uninteresting if this were the case. Indeed, we have the following theorem, which was established by Euclid, though the proof given below is due to Kummer [**8**].

THEOREM 2.5. *There are infinitely many primes.*

PROOF. Suppose that there are only finitely many primes, say $p_1, p_2, \ldots, p_r$, and set $N = p_1 p_2 \cdots p_r$. Then we necessarily have $N > 2$ since 2 is among the finite number of primes. By the Theorem 2.3, the integer $N - 1$ is a product of primes, so it must have a prime divisor p_i in common with N. Then p_i divides both N and $N-1$, thus p_i divides the difference $N-(N-1) = 1$, which is a contradiction since no prime divides the integer 1. □

Now that we are guaranteed an infinitude of primes, we can inquire about the distribution of the primes among the positive integers. This question is answered by the much celebrated Prime Number Theorem.

THEOREM 2.6 (The Prime Number Theorem). *If n is a large positive integer, then the number $\pi(n)$ of primes less than or equal to n is approximately $n/\ln n$. More precisely,*

$$\lim_{n\to\infty} \left(\frac{\pi(n)}{n/\ln n} \right) = 1.$$

The proof of this theorem is beyond the scope of this paper, but the curious reader can find citations for proofs in [**5**], [**8**].

We could seek a formula for primes, though it can be shown, as in [**8**], that no polynomial in a single variable can evaluate to a prime for each value of its input. However, in 1970, Matijasevič constructed a polynomial, affectionately known as the unbelievable polynomial, in several variables with integer coefficients which evaluates to a prime whenever one substitutes in integer values for the variables and obtains a positive value. Moreover, every prime will be such a value of the polynomial. At present, using this polynomial for the purpose of primality testing is out of reach [**4**]. For now, we turn our attention to a method for finding all the primes less than or equal to a given integer $n > 1$.

2. Sieve of Eratosthenes

In primality testing, it is often useful to have a list of the smaller primes. Such a list can be generated using a sieving method developed over two thousand years ago by the Greek scholar Eratosthenes. The method is as follows [**5**], [**6**].

Given an integer $n > 1$, list the integers from 2 to n in increasing order. The first member for the list is the prime 2. Strike out all multiples of 2 greater than 2. The next remaining member of the list which is greater than 2 is the prime 3. Strike out all multiples of 3 greater than 3. Continue in this way until there are no more members of the list to strike out.

The following theorem allows us to pinpoint the integer at which we may stop striking out multiples and be guaranteed that the resulting list contains only primes.

THEOREM 2.7. *Let $n > 1$ be an integer. If n has no prime divisor less than or equal to $\sqrt{n}$, then n is prime.*

PROOF. Suppose n is composite and each prime divisor p_i of n satisfies $p_i > \sqrt{n}$. Since n is composite, we know that $n = p_1 p_2 \cdots p_k$ is a product of at least two primes. But then

$$n = p_1 p_2 \cdots p_k > \sqrt{n}\sqrt{n} p_3 \cdots p_k = n p_3 \cdots p_k \geq n$$

which shows that $n > n$, a contradiction. So n must be prime. □

The contrapositive of this theorem states that if n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$. Consequently, when using the Sieve of Eratosthenes to find all the primes less than a given integer $n > 1$ we may stop striking out multiples once we reach a prime greater than $\sqrt{n}$. To illustrate the steps involved in implementing the Sieve of Eratosthenes, consider the following example.

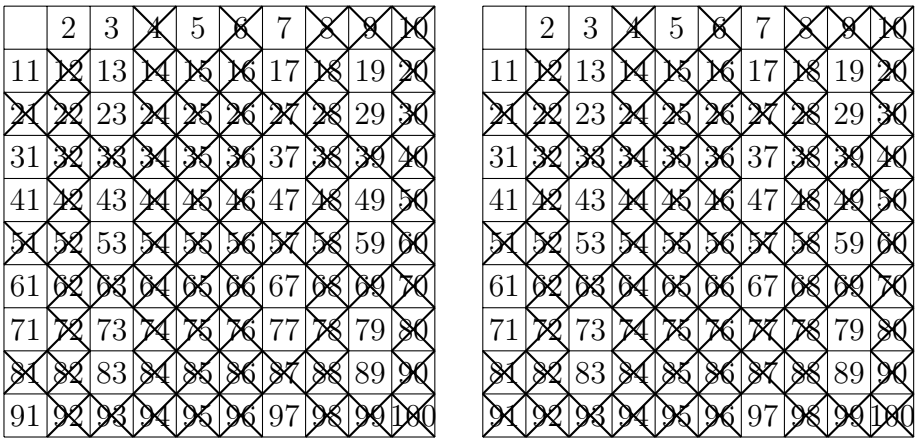
EXAMPLE 2.8. To find all the primes less than or equal to 100, we list the integers from 2 to 100 in increasing order. Calculating $\sqrt{100} = 10$, we may stop striking out multiples once we reach a prime greater than 10. We begin striking out multiples below.

	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

(a) Striking out the multiples of 2.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

(b) Striking out the multiples of 3.



(c) Striking out the multiples of 5. (d) Striking out the multiples of 7.

FIGURE 1. Finding all the primes less than or equal to 100.

After we strike out the multiples of 7, we see that the next prime in the list is 11. Since 11 is greater than $\sqrt{100}$, at this step the resulting list contains only the primes less than 100.

3. Some Divisibility Results

Due to our base ten arithmetic, it can be quick and easy to determine if certain numbers are divisors of a given integer. In this section, we verify that if the final digit of an integer $n > 1$ is one of 0, 2, 4, 6 or 8, then n is a multiple of 2, and that if the final digit of n is either 0 or 5, then n is a multiple of 5. We also give quick tests to determine if the numbers 3 and 11 are divisors of a given integer.

We have already noted that every multiple of 2 greater than 2 is by definition composite. These even integers are easily distinguished from the odd integers by checking their final digit, as are the multiples of 5. Let the digit representation of an integer $n > 1$ be $d_1 d_2 \dots d_{k-1} d_k$ with $0 \leq d_i \leq 9$ for $i = 1, \dots, k$. Then

$$n = \sum_{1 \leq i \leq k} 10^{k-i} d_i \tag{3.1}$$

and it is clear from (3.1) that n is divisible by 2 (or 5) when the final digit d_k is divisible by 2 (5, respectively). Therefore, we can immediately decide whether 2 or 5 are divisors of a given integer $n > 1$ by checking the final digit of n: Except for the integers 0, 2 and 5, if the final digit of n is one of 0, 2, 4, 5, 6 or 8, then n is composite.

There are also quick tests to determine if the numbers 3 and 11 are divisors of a given integer $n > 1$. In order to discuss these tests, we first need to recall the concept of congruence modulo n.

DEFINITION 2.9. Let a, b, n be integers with $n > 0$. We say that a is *congruent* to b modulo n and write $a \equiv b \pmod{n}$ if n divides $a - b$. If n does not divide $a - b$, then a is *not congruent* to b modulo n and we write $a \not\equiv b \pmod{n}$.

We require the following rules for addition and multiplication modulo n. The proofs of these rules are derived in [**5**].

LEMMA 2.10. *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then*

(1) $a + c \equiv b + d \pmod{n}$
(2) $ac \equiv bd \pmod{n}$

This lemma enables us to derive the theorems governing the divisibility of an integer $n > 1$ by the divisors 3 and 11. We begin with the theorem for 3 below [**6**].

THEOREM 2.11. *If the sum of the digits of an integer* $n > 1$ *is a multiple of 3, then* n *is divisible by 3.*

PROOF. Let n be written in the form (3.1) and assume that $\sum_{1 \le i \le k} d_i = 3m$ for some integer m. Since $10 \equiv 1 \pmod{3}$, we have $10^k \equiv 1 \pmod{3}$ for all $k \ge 1$ by the previous theorem and so

$$\begin{aligned} n &\equiv d_1 + d_2 + \cdots + d_k \pmod{3} \\ &\equiv 3m \pmod{3} \\ &\equiv 0 \pmod{3}, \end{aligned}$$

which shows that n is divisible by 3. □

Testing for 3 as a divisor using the previous theorem works well for integers with relatively few digits. However, if n has many digits, then it is easier to check for 3 as a divisor by actually dividing n by 3 and checking whether the remainder term is zero. The following example shows that the process of summing the digits can be applied iteratively.

EXAMPLE 2.12. We can quickly decide whether the integer $n = 17865843$ is divisible by 2, 3 or 5. Notice that the final digit of n is neither 5 nor an even number, so n does not have 2 or 5 as divisors. To test whether 3 is a divisor of n, we sum the digits of n:

$$1 + 7 + 8 + 6 + 5 + 8 + 4 + 3 = 42.$$

If it is not clear that 42 is a multiple of 3, we can sum the digits of 42 to find that

$$4 + 2 = 6 = 2 \cdot 3$$

so that 42 is a multiple of 3, and therefore n is also a multiple of 3.

There is a similar test for determining whether 11 is a divisor of a given integer [**6**].

THEOREM 2.13. *If the alternating sum* $\sum_{1 \le i \le k} (-1)^{k-i} d_i$ *of the digits of an integer* $n > 1$ *is a multiple of 11, then* n *is divisible by 11.*

PROOF. Let n be written in the form (3.1) and assume that $\sum_{1\leq i\leq k}(-1)^{k-i}d_i = 11m$ for some integer m. Now for an integer $k > 0$, we can use the binomial theorem to expand and write

$$\begin{aligned}10^k &= (11-1)^k \\ &= 11^k + \binom{k}{1}(11)^{k-1}(-1) + \cdots + \binom{k}{k-1}(11)(-1)^{k-1} + (-1)^k \\ &= 11q + (-1)^k\end{aligned}$$

for some integer q. So n can be rewritten, for some integers r, q_i $(1 \leq i \leq k-1)$, as

$$\begin{aligned}n &= \big(11q_1 + (-1)^{k-1}\big)d_1 + \big(11q_2 + (-1)^{k-2}\big)d_2 + \cdots + \big(11q_{k-1} + (-1)\big)d_{k-1} + d_k \\ &= 11\sum_{1\leq i\leq k} q_i d_i + \sum_{1\leq i\leq k}(-1)^{k-i}d_i \\ &\equiv 11(r+m) \pmod{11} \\ &\equiv 0 \pmod{11},\end{aligned}$$

which shows that n is divisible by 11. □

As was the case with the test for 3, using the previous theorem to test for 11 as a divisor works well for integers with relatively few digits. For an integer with many digits, it is easer to test for 11 as a divisor by dividing the integer by 11 and checking whether the remainder term is zero. We can also apply this test iteratively, though this is usually not necessary since the size of the sum is controlled by the subtraction present in the alternating sum.

EXAMPLE 2.14. We can decide whether 11 is a divisor of the integer $n = 8132619$ by taking a "right-to-left" alternating sum as is done below.

$$8 - 1 + 3 - 2 + 6 - 1 + 9 = 22 = 2 \cdot 11$$

Since the alternating sum of the digits of n is a multiple of 11, we conclude that n is divisible by 11.

There are also simple tests to determine if specific composites such as 4, 9 or 10 are divisors of an integer $n > 1$. These tests could have been derived alongside the tests for 2, 3, 5 and 11. However, only tests for prime divisors are necessary for the purpose of primality testing since a composite divisor will always have a smaller prime divisor.

The advantage of the tests developed in this section is the ease with which we can employ them. Compared to the tests we will derive in the following chapters, these tests have the disadvantage of being weak: These tests only conclude whether a specific number is a divisor of a given integer, not whether an integer is definitely composite.

CHAPTER 3

Classical Methods

In this chapter, we will provide two theorems which completely characterize the primes and one property which holds for all primes. We will derive deterministic primality tests from the first two theorems, though these tests will not be practical to employ for integers with many digits. The property which holds for all primes will lead to a test which is easy to employ, though it will have the disadvantage that it will apply not only to all primes, but to some troublesome composites as well.

1. Trial Division

The definition of a prime already provides a way to determine whether a given integer $n > 1$ is prime. We could systematically or randomly divide n by its potential positive nontrivial divisors, the integers from 2 to $n - 1$. If for some division the remainder term is zero, then n has a nontrivial divisor and is therefore composite. Otherwise, n is prime.

In performing trial divisions as mentioned above, we would be doing more work than is necessary. As we noted at the end of the previous section, we only need to check for prime divisors. Even in performing trial divisions by only the primes less than n, we would still be doing more work than is necessary. Theorem 2.7 asserts that if n is composite, then n must have a prime divisor less than or equal to $\sqrt{n}$. Notice that Theorem 2.7 can be strengthened to an "if and only if" statement:

THEOREM 3.1. *Let $p > 1$ be an integer. Then p has no prime divisor less than or equal to $\sqrt{p}$ if and only if p is prime.*

PROOF. The first implication is just Theorem 2.7, so assume p is prime. Then the only prime divisor of p is itself. Indeed, we have $p > \sqrt{p}$ since $p > 1$. So p has no prime divisor less than or equal to $\sqrt{p}$. □

Thus, to make a conclusive decision regarding the primality of n, we only need to perform trial divisions by the primes less than or equal to $\sqrt{n}$. If any one of these primes divides n, then n is composite. Otherwise, n is prime.

The amount of work required by this test can be costly. First, we require a complete list of primes less than or equal to $\sqrt{n}$. Generating such a list can be done using the Sieve of Eratosthenes. If n has many digits, however, then acquiring such a list is a formidable task. Second, once we have obtained the required list of primes, we need to do trial divisions by the primes in the list, of which there may be a great many. To illustrate

what is meant by "a great many", notice that we can use the Prime Number Theorem to approximate the number of primes less than or equal to $\sqrt{n}$ [**5**]:

$$\pi(\sqrt{n}) \doteq \frac{\sqrt{n}}{\ln \sqrt{n}}$$

If n has more than 10 digits, then $n > 10^{10}$ and there are more than roughly $\dfrac{10^5}{\ln 10^5} \doteq 8686$ primes which require trial division in order to declare n prime. However, when n has very few digits, this method works well, as we see in the following example.

EXAMPLE 3.2. We can determine whether $n = 9701$ is prime using the primes less than 100 found in Figure 2.8 since $\sqrt{n} \leq 100$. Performing trial divisions systematically or randomly, we find that division by 89 yields a zero remainder and therefore n is composite.

The most desirable property of this method of primality testing is its conclusive nature. Given enough time, we can always use the method of trial division to make a conclusive decision regarding the primality of a given integer $n > 1$. The next method of primality testing we derive shares this desirable property.

2. Wilson's Theorem

The result described in this section first appeared without proof in Waring's *Meditationes Algebraicae* of 1770. It was attributed to one of his former students, John Wilson, who conjectured it based on numerical computations. The result was stated as follows [**3**].

$$\text{"For a prime } p, \quad \frac{1 \cdot 2 \cdots (p-1) + 1}{p} \quad \text{is an integer."}$$

Later that year, Lagrange published a proof of both the statement above and its converse, establishing the complete characterization of the primes now known as Wilson's Theorem [**3**]. In order to prove Wilson's Theorem, we first need to recall some concepts from abstract algebra. A full treatment of the subject can be found in [**5**]. Here, we state only the essentials needed to prove Wilson's Theorem. First, we recall the definition of a field.

DEFINITION 3.3. A *field* is a nonempty set F equipped with two operations (written as addition and multiplication) that satisfy the following axioms. For all $a, b, c \in F$:

(1) If $a, b \in F$, then $a + b \in F$. [closure for addition]
(2) $a + (b + c) = (a + b) + c$. [associative addition]
(3) $a + b = b + a$. [commutative addition]
(4) There is an element 0_F in F such that $a + 0_F = a = 0_F + a$ for every $a \in F$. [additive identity or zero element]
(5) For each $a \in F$, the equation $a + x = 0_F$ has a solution in F. [additive inverse]
(6) If $a \in F$ and $b \in F$, then $ab \in F$. [closure for multiplication]
(7) $a(bc) = (ab)c$. [associative multiplication]

(8) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$. [distributive laws]
(9) $ab = ba$. [commutative multiplication]
(10) There is an element $1_F \neq 0_F$ in F such that $a1_F = a = 1_F a$ for every $a \in F$. [multiplicative identity]
(11) For each $a \neq 0_F$ in F, the equation $ax = 1_F$ has a solution in F. [multiplicative inverse]

REMARK 3.4. Where F is a field, one can show that whenever $a, b \in F$ and $ab = 0_F$, then $a = 0_F$ or $b = 0_F$. This property is known as the zero product rule. It is also possible to show that the multiplicative inverse of an $a \neq 0_F$ in F is unique. These facts are derived in [**5**] and are necessary to prove Wilson's Theorem.

EXAMPLE 3.5. The set $\mathbb{R}$ of real numbers is a familiar example of a field when equipped with the usual addition and multiplication. When p is prime, the set $\mathbb{Z}_p$ of remainders modulo p also constitutes a field under the usual addition and multiplication.

LEMMA 3.6. *Let p be a prime. If $x^2 \equiv 1 \pmod{p}$, then $x \equiv \pm 1 \pmod{p}$.*

PROOF. We rearrange the necessary congruence by using Lemma 2.10 and factoring:

$$\begin{aligned} x^2 &\equiv 1 \pmod{p} \\ x^2 - 1 &\equiv 0 \pmod{p} \\ (x-1)(x+1) &\equiv 0 \pmod{p}. \end{aligned}$$

Then since p is prime, the zero product rule holds so either

$$\begin{aligned} x - 1 &\equiv 0 \pmod{p} \qquad \text{or} \qquad x + 1 \equiv 0 \pmod{p} \\ x &\equiv 1 \pmod{p} \qquad\qquad x \equiv -1 \pmod{p}, \end{aligned}$$

as desired. □

THEOREM 3.7 (Wilson's Theorem). *An integer $p > 1$ is prime if and only if*

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

PROOF. First note that if $p = 2$ or $p = 3$, then the congruence is satisfied since

$$(2-1)! = 1 \equiv -1 \pmod{2} \qquad \text{and} \qquad (3-1)! = 2 \equiv -1 \pmod{3},$$

so assume $p > 3$ is prime. Then the $p - 1$ nonzero elements of $\mathbb{Z}_p$ each have a unique multiplicative inverse. The previous lemma shows that 1 and $-1 = p - 1$ are their own inverses. So there are $p - 3$ elements of $\mathbb{Z}_p$ with distinct inverses. Since p is odd, $p - 3$ is even and since products in $\mathbb{Z}_p$ are commutative and associative, we can pair off the $p - 3$ elements in inverses in the product

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

Then multiplication by $(p-1)$ yields

$$\begin{aligned}(p-1)! &\equiv p-1 \pmod{p} \\ &\equiv -1 \pmod{p},\end{aligned}$$

which proves the first implication.

Conversely, suppose n is composite. Then n has a divisor a with $1 < a < n$. Since $(n-1)! \equiv -1 \pmod{n}$, we have that $n \mid (n-1)!+1$ and thus $a \mid (n-1)!+1$. We also have that $a \mid (n-1)!$ since $1 < a < n$. Thus, a also divides the difference $(n-1)!+1-(n-1)! = 1$, a contradiction since $a > 1$. So $(n-1)! \not\equiv -1 \pmod{n}$. □

Wilson's Theorem asserts that we can conclusively determine whether an integer $n > 1$ is prime by testing only one congruence, namely

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

If this congruence holds, then n is prime. Otherwise, n is composite. Wilson's Theorem works well as a primality test for small n, as is seen in the following example.

Example 3.8. Wilson's Theorem is capable of proving that 13 is prime by computing

$$12! = 479001600 \equiv 12 \equiv -1 \pmod{13}.$$

We can also use Wilson's Theorem to quickly demonstrate that 14 is composite since

$$13! = 6227020800 \equiv 0 \not\equiv -1 \pmod{14}.$$

Though Wilson's Theorem enjoys the same conclusive nature as the method of trial division, it is not practical as a primality test when n is large since the factorial in the necessary computation grows too rapidly. For example, an integer n with only three digits yields more than a hundred digits in the integer $(n-1)!$ [**9**].

3. Fermat's Little Theorem

In this section, we develop a result which first appeared in a letter written by Fermat in 1640. It was stated without proof, though it is speculated that Fermat's proof relied on the binomial theorem [**10**]. In modern language, the result was stated as follows.

"For a prime p and any integer a relatively prime to p, $\dfrac{a^{p-1}-1}{p}$ is an integer."

This result is now known as Fermat's Little Theorem (named as such to distinguish it from Fermat's Last or "Great" Theorem). Nearly one hundred years after Fermat stated this theorem, Euler published the first proof in *Proceedings* of the St. Petersburg Academy in 1736 [**7**]. We give Euler's proof below, as found in [**10**], after stating Fermat's Little Theorem in terms of congruence.

THEOREM 3.9 (Fermat's Little Theorem). *Let p be a prime and a any integer with $(a, p) = 1$. Then*

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

PROOF. We begin by listing the $p-1$ distinct nonzero elements of $\mathbb{Z}_p$:

$$1, 2, 3, \ldots, p-2, p-1. \tag{3.1}$$

By multiplying each member of (3.1) by some fixed nonzero $a \in \mathbb{Z}_p$ we obtain a new list:

$$1a, 2a, 3a, \ldots, (p-2)a, (p-1)a. \tag{3.2}$$

Since $\mathbb{Z}_p$ is closed under multiplication, each member of (3.2) is in $\mathbb{Z}_p$. Moreover, each member of (3.2) is distinct. To see this, suppose that $ma \equiv na \pmod{p}$ for any two multiples of a. Then multiplication by the inverse of a shows that $m \equiv n \pmod{p}$, so we have two lists of the $p-1$ distinct nonzero elements of $\mathbb{Z}_p$. This means that (3.2) is just a reordering of (3.1). Since products in $\mathbb{Z}_p$ are commutative and associative, we may form the product of the elements in each list and obtain the congruence

$$1a \cdot 2a \cdot 3a \cdots (p-2)a \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1) \pmod{p}$$
$$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod{p}.$$

Finally, multiplication by the inverse of $(p-1)!$ yields the desired result. □

We can use the contrapositive of Fermat's Little Theorem to test not for primality, but instead for compositeness. Letting $n > 2$ be odd, if we can find a base a relatively prime to n for which $a^{n-1} \not\equiv 1 \pmod{n}$, then n is necessarily composite.

In order to employ the contrapositive of Fermat's Little Theorem to test for compositenes, we require quick ways to compute greatest common divisors and expressions of the form x^y modulo n, where x, y, n are positive integers. The former can be computed using the Euclidean Algorithm, as discussed in [**5**], [**6**]. Expressions of the form x^y modulo n can be computed using the method of repeated squaring, as described below.

EXAMPLE 3.10. To compute 14^{42} modulo 87, we begin by squaring the congruence

$$14^1 \equiv 14 \pmod{87},$$

reducing the right-hand side modulo 87 and doubling the exponent of the left-hand side to obtain the congruence

$$14^2 \equiv 22 \pmod{87}.$$

We repeat this process until the exponent of the left-hand side is the largest power of 2 which can be subtracted from the original exponent:

$$14^1 \equiv 14 \pmod{87} \qquad 14^8 \equiv 52 \pmod{87}$$
$$14^2 \equiv 22 \pmod{87} \qquad 14^{16} \equiv 7 \pmod{87}$$
$$14^4 \equiv 49 \pmod{87} \qquad 14^{32} \equiv 49 \pmod{87}.$$

Then writing the original exponent 42 as a greedy sum of powers of 2,

$$42 = 32 + 8 + 2,$$

we find that $14^{42} = 14^{32} \cdot 14^8 \cdot 14^2 \equiv 49 \cdot 52 \cdot 22 \equiv 28 \pmod{87}$.

From now on, any expression of the form x^y modulo n in this paper has been computed using the method of repeated squaring and any greatest common divisor has been computer using the Euclidean Algorithm. We can now begin to test numbers for compositeness using the contrapositive of Fermat's Little Theorem:

EXAMPLE 3.11. Consider $n = 5461$. Choosing the base $a = 680$ at random, we find that $(a, n) = 1$. Now we compute

$$680^{5460} \equiv 1162 \not\equiv 1 \pmod{5461},$$

which shows that n is composite. In fact, $n = 43 \cdot 127$.

Notice that if we had chosen the base $a = 16$, we would have again had $(a, n) = 1$, but we would have computed

$$16^{5460} \equiv 1 \pmod{5461}$$

and we would not have been able to make a conclusive decision regarding the compositeness of n.

Unfortunately, our example outlines the fact that there are composites n which can satisfy Fermat's Little Theorem for a particular base a with $(a, n) = 1$. This leads us to the following definition.

DEFINITION 3.12. Let a and n be integers with $(a, n) = 1$. Then n is a *pseudoprime* to the base a if n is composite, yet we still have $a^{n-1} \equiv 1 \pmod{n}$.

The existence of pseudoprimes means that the converse of Fermat's Little Theorem does not hold true. One would hope that for a particular base a, there are only finitely many pseudoprimes. This is not the case. As shown in [**6**], there are infinitely many pseudoprimes to the base 2. The base 2 is not the only base troubled by pseudoprimes; each base has infinitely many pseudoprimes associated to it [**10**]. Worse yet, there are composites which are pseudoprimes to *every* possible base. These troublesome composites were studied by Carmichael and are named for him.

DEFINITION 3.13. Let a and n be integers. Then n is a *Carmichael number* if n is composite and $a^{n-1} \equiv 1 \pmod{n}$ for all a with $(a, n) = 1$.

In 1912, Carmichael conjectured that there are infinitely many Carmichael numbers. Eighty years later, Alford, Granville and Pomerance proved Carmichael's conjecture [**6**]. Though Carmichael numbers appear less frequently than primes, their infinitude still provides an infinite amount of trouble in testing for compositeness using Fermat's Little Theorem [**6**].

CHAPTER 4

Modern Methods

More elaborate tests for primality have been developed in the last two centuries. In this chapter, we will discuss three of these tests. The methods will vary greatly, though each is based on Fermat's Little Theorem.

1. Lucas' Converse of Fermat's Little Theorem

In the previous section, we saw that the converse of Fermat's Little Theorem does not hold true. However, Lucas showed in a work published in 1876 that an additional condition can be placed on the converse of Fermat's Little Theorem so that it does hold true [**11**]. In order to discuss Lucas' work, we first need to define Euler's totient function and derive its relevant properties.

DEFINITION 4.1. Let n be a positive integer. *Euler's totient function* $\phi(n)$ is defined to be the number of positive integers less than or equal to n which are relatively prime to n.

EXAMPLE 4.2. The first several values of Euler's totient function are given below [**11**].

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16

Observe that when n is prime, $\phi(n) = n - 1$ and that when $\phi(n) = n - 1$, n is prime. This fact will be of use later in this section and is proved below.

THEOREM 4.3. *Let $n > 1$ be an integer. Then n is prime if and only if $\phi(n) = n - 1$.*

PROOF. Suppose n is prime. Then all the integers $1, 2, \ldots, n-1$ are relatively prime to n and therefore $\phi(n) = n-1$. Now suppose n is composite. Then n has a divisor a with $1 < a < n$, that is, there is an integer a among the integers $2, \ldots, n-1$ with $(a, n) > 1$. Hence, $\phi(n) \leq n - 2$ [**11**]. □

Using the totient function, Euler was able to generalize Fermat's Little Theorem [**10**].

THEOREM 4.4 (Euler-Fermat Theorem). *If n is a positive integer and $(a, n) = 1$, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

PROOF. As in the proof of Fermat's Little Theorem, the positive integers $a_1, a_2, \ldots, a_{\phi(n)}$ less than or equal to n which are relatively prime to n each have a unique multiplicative inverse modulo n. For the same reasons as in the proof of Fermat's Little Theorem, we can list these integers and multiply each member of the list by a fixed a with $(a, n) = 1$

to obtain a permutation of the original list. Taking the product of the members of each list, we have that

$$\begin{aligned}(a \cdot a_1)(a \cdot a_2) \cdots (a \cdot a_{\phi(n)}) &\equiv a_1 \cdot a_2 \cdots a_{\phi(n)} \pmod{n} \\ a_1 \cdot a_2 \cdots a_{\phi(n)} \cdot a^{\phi(n)} &\equiv a_1 \cdot a_2 \cdots a_{\phi(n)} \pmod{n}\end{aligned}$$

and multiplication by the inverses of $a_1, a_2, \ldots, a_{\phi(n)}$ yields the desired result. □

With the Euler-Fermat Theorem in hand, we can prove a theorem which is essential to the development of Lucas' converse of Fermat's Little Theorem. First, we require a definition.

Definition 4.5. Let n be a positive integer and a any integer with $(a, n) = 1$. The *order* of an element modulo n, denoted $\text{ord}_n(a)$, is the least positive integer k for which $a^k \equiv 1 \pmod{n}$.

Example 4.6. We find the $\text{ord}_{16}(3)$ as follows.

$$\begin{aligned}3^1 &\equiv 3 \pmod{16} \\ 3^2 &\equiv 9 \pmod{16} \\ 3^3 &\equiv 11 \pmod{16} \\ 3^4 &\equiv 1 \pmod{16}\end{aligned}$$

This shows that $k = 4$ is the least positive exponent for which $3^k \equiv 1 \pmod{16}$, and therefore $\text{ord}_{16}(3) = 4$. From this, it follows that

$$3^4 = 9^2 \equiv 1 \pmod{16}$$

and since $9^1 \not\equiv 1 \pmod{16}$, we can also conclude that $\text{ord}_{16}(9) = 2$. Notice that $\text{ord}_{16}(3)$ and $\text{ord}_{16}(9)$ both divide $\phi(16)$. The following theorem shows that this is no coincidence.

Theorem 4.7. *Let n be a positive integer and a any integer with $(a, n) = 1$. Then*

$$ord_n(a) \mid \phi(n).$$

Proof. Suppose $\text{ord}_n(a) = k$. Then $a^k \equiv 1 \pmod{n}$ and, by definition, k is the least positive exponent for which this congruence holds. By the Euler-Fermat Theorem, we also have that $a^{\phi(n)} \equiv 1 \pmod{n}$ and therefore $k \leq \phi(n)$. By the division algorithm, there exist q and r such that $\phi(n) = kq + r$ with $0 \leq r < k$. Then

$$\begin{aligned}a^{\phi(n)} &\equiv 1 \pmod{n} \\ a^{kq+r} &\equiv 1 \pmod{n} \\ (a^k)^q \cdot a^r &\equiv 1 \pmod{n} \\ a^r &\equiv 1 \pmod{n},\end{aligned}$$

but this contradicts the fact that k is the least positive exponent for which this congruence holds, unless $r = 0$. Thus, $r = 0$ and we have that $\text{ord}_n(a) \mid \phi(n)$. □

We are now equipped to prove Lucas' converse of Fermat's Little Theorem [**11**].

THEOREM 4.8. *Let n be a positive integer. If there is an integer a for which every prime divisor p_i of $n-1$ satisfies*

(1) $a^{n-1} \equiv 1 \pmod{n}$,
(2) $a^{(n-1)/p_i} \not\equiv 1 \pmod{n}$,

then n is prime.

PROOF. We show that n is prime by verifying that $\phi(n) = n-1$. By the previous theorem, our first hypothesis means that $\mathrm{ord}_n(a) \mid n-1$. Now suppose $\mathrm{ord}_n(a) \neq n-1$, then $n-1 = k \cdot \mathrm{ord}_n(a)$ for some integer $k > 1$. Let p_i be any prime divisor of $n-1$. Then

$$a^{(n-1)/p_i} = a^{k \cdot \mathrm{ord}_n(a)/p_i} = (a^{\mathrm{ord}_n(a)})^{k/p_i} \equiv 1 \pmod{n},$$

which contradicts our second hypothesis. Thus, $\mathrm{ord}_n(a) = n-1$. Now by definition, $\mathrm{ord}_n(a) \leq \phi(n)$ and $\phi(n) \leq n-1$, and since $\mathrm{ord}_n(a) = n-1$, this means that $\phi(n) = n-1$ and therefore n is prime. □

This theorem allows us to derive a test which is stronger than the test derived from Fermat's Little Theorem since it is capable of detecting both primes and composites. This new test is well-suited for application to n for which $n-1$ is easy to factor. The following example illustrates this.

EXAMPLE 4.9. Consider $n = 65537$. The prime factorization of $n-1$ is $65536 = 2^{16}$. Choosing the base $a = 44188$ and random, we find that $(a, n) = 1$. We then compute

$$44188^{65536} \equiv 1 \pmod{65537},$$

which gives evidence that n is prime. Continuing the test, we now compute

$$44188^{65536/2} = 44188^{32768} \equiv -1 \not\equiv 1 \pmod{65537},$$

and then by Lucas' converse of Fermat's Little Theorem, n is prime.

There is one notable drawback to this test: Finding the prime factorization of $n-1$ can be just as daunting factoring n itself [**11**]. For example, to test $n = 507199$, we begin to factor $n-1 = 2 \cdot 3 \cdot 84533$ and in order to proceed, we must determine if 84533 is prime.

2. The Miller-Rabin Test

In this section, we investigate the quadratic congruence

$$x^2 \equiv 1 \pmod{n}. \tag{2.1}$$

Our investigation will lead to a new method of compositeness testing known as the Miller-Rabin test. First, a definition will ease the language used.

DEFINITION 4.10. The number x is called a *square root* of 1 modulo n if x satisfies (2.1). We always have $x = \pm 1$ modulo n as solutions to (2.1), so we call these *trivial square roots* of 1 modulo n. We call any other solutions to (2.1) *nontrivial square roots* of 1 modulo n.

EXAMPLE 4.11. The following table shows the square roots x of 1 modulo n for different values of n:

n	7	8	9	10	11	12	13	14	15	16
x	± 1	$\pm 1, \pm 3$	± 1	± 1	± 1	$\pm 1, \pm 5$	± 1	± 1	$\pm 1, \pm 4$	$\pm 1, \pm 7$

THEOREM 4.12. *Let p be a prime. Then the congruence $x^2 \equiv 1 \pmod{p}$ is satisfied if and only if $x \equiv \pm 1 \pmod{p}$.*

PROOF. The proof that if $x^2 \equiv 1 \pmod{p}$, then $x \equiv \pm 1 \pmod{p}$ was given in Lemma 3.6. So assume $x \equiv \pm 1 \pmod{p}$, then squaring both sides of this congruence yields the desired result. □

Theorem 4.12 asserts that if we can find a nontrivial square root of 1 modulo n, then n is composite. The problem now is to derive a method of finding such a square root. Note that since the n to be tested is always odd, then $n - 1$ is even. We factor as many 2's as possible from $n - 1$ to write $n - 1 = 2^j d$, with d odd. Then for a base a with $(a, n) = 1$, we compute the sequence of squares

$$\{a^d, a^{2d}, a^{4d}, a^{8d}, \ldots, a^{2^{j-1}d}, a^{2^j d}\} \pmod{n},$$

where each term is reduced modulo n. Observe that the final term of this sequence is exactly a^{n-1} modulo n, so if this term is 1, then reading the sequence right-to-left can show a nontrivial square root of 1 modulo n [**11**].

THEOREM 4.13. *Let n be an odd prime. Then the sequence of squares previously defined has one of the following two forms, where a question mark "?" denotes a number different from ± 1:*

$$\{1, 1, \ldots, 1, \quad 1, \quad 1, \ldots, 1\},$$
$$\{?, ?, \ldots, ?, \quad -1, \quad 1, \ldots, 1\}.$$

PROOF. By Fermat's Little Theorem, the final term in the sequence, a^{n-1} modulo n, must be 1 since $(a, n) = 1$. Then by the previous theorem, the only square roots of 1 modulo n are ± 1 modulo n. Thus the sequence is either unanimously 1, or the first instance of a 1 is preceded by a -1. That is, the sequence must have one of the above two forms. □

The contrapositive of the above theorem affords a test for compositeness. Since the sequence of squares is constructed by squaring the preceding term, once we reach a term which is ± 1, all following terms must be 1. So if the sequence has one of the following three "bad" forms

$$\{?, \ldots, ?, 1, 1, \ldots, 1\},$$
$$\{?, \ldots, ?, ?, ?, \ldots, -1\},$$
$$\{?, \ldots, ?, ?, ?, \ldots, ?\},$$

then n is necessarily composite. Otherwise, n could be prime or composite.

EXAMPLE 4.14. Consider $n = 3057601$, then $n - 1 = 2^6 \cdot 47775$. Choosing the base $a = 99908$ at random, we then find that $(a, n) = 1$. Now we compute the sequence of squares

$$\{1193206, 2286397, 235899, 1, 1, 1, 1\}.$$

Since there is a term preceding a 1 different from ± 1, n is composite.

3. The AKS Test

In this section, we develop the core ideas of a recent primality test. The test was derived in 2002 and is based on a generalization of Fermat's Little Theorem to polynomial rings. To begin, we discuss binomial coefficients modulo a prime.

THEOREM 4.15. *Let p be a prime. If $0 < i < p$, then* $\binom{p}{i} \equiv 0 \pmod{p}$.

PROOF. For $0 < i < p$, each term in the denominator of the binomial coefficient

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

is strictly less than p and since p is prime, this means that the factor of p in the numerator cannot cancel. Hence, p divides $\binom{p}{i}$ and the theorem is proved [**4**]. □

This theorem is the key to proving the generalization of Fermat's Little Theorem to the polynomial case. The following definition will ease the language used in the proof.

DEFINITION 4.16. We write $p^k \,||\, n$ if $p^k \mid n$ and $p^{k+1} \nmid n$. That is, p^k is the largest power of p dividing n.

EXAMPLE 4.17. Let $n = 459$. Then $3^3 \,||\, 459$ since $3^3 = 27 \mid 459$ but $3^4 = 81 \nmid 459$.

THEOREM 4.18. *Let $n > 1$ be an integer and a any integer with $(a, n) = 1$. Then n is prime if and only if*

$$(x + a)^n \equiv x^n + a \pmod{n}. \tag{3.1}$$

PROOF. First note that

$$\begin{aligned}(x+a)^n - (x^n + a) &= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}x + \cdots + \binom{n}{n-1}ax^{n-1} + \binom{n}{n}x^n - x^n - a \\ &= a^n - a + \sum_{0<i<n} \binom{n}{i} a^{n-i}x^i.\end{aligned}$$

Suppose n is prime. Then each binomial coefficient in the sum is zero, so this case reduces to Fermat's Little Theorem.

Conversely, suppose n is composite. Then n has a prime divisor q, so let $q^k \mid\mid n$. We show that the coefficient $\binom{n}{q}a^{n-q}$ of x^q in $(x+a)^q$ is not divisible by n and therefore, doing a term-by-term comparison, the congruence (3.1) cannot hold. Since $(a,n)=1$, then $(a,q)=1$ and consequently

$$(a^{n-q}, q^k) = 1. \tag{3.2}$$

Now suppose $q^k \mid \binom{n}{q}$. Then there is an integer u such that $uq^k = \dfrac{n(n-1)\cdots(n-q+1)}{q!}$. Rearranging and pulling a factor of q from $q!$ into q^k yields

$$n = \frac{uq^{k+1}(q-1)!}{(n-1)(n-2)\cdots(n-q+1)} \tag{3.3}$$

and since the left-hand side is an integer, so is the right-hand side. Now we show that no factor of q in the numerator can cancel. Suppose a factor of q can cancel, then some term in the denominator $(n-1)(n-2)\cdots(n-q+1)$ must be divisible by q. Since q is prime, Theorem 2.1 guarantees that q must divide one of the terms in the product, that is, $q \mid (n-j)$ for some $0<j<q$. Then $n-j \equiv 0 \pmod{q}$ and since $n \equiv 0 \pmod{q}$, we must also have $j \equiv 0 \pmod{q}$, which contradicts the fact that $0<j<q$. Thus $q \nmid (n-j)$ and no factor of q can cancel. Then (3.3) implies that $q^{k+1} \mid n$, a contradiction. Hence, $q^k \nmid \binom{n}{q}$.

Finally, suppose $n \mid \binom{n}{q}a^{n-q}$. Then there is an integer v such that $vn = \binom{n}{q}a^{n-q}$. It follows that

$$\frac{vn}{q^k} = \frac{\binom{n}{q}a^{n-q}}{q^k}.$$

Since $q^k \mid n$, the left-hand side is an integer and then so is the right-hand side. We have shown that $q^k \nmid \binom{n}{q}$, so we must have $q^k \mid a^{n-q}$, contradicting (3.2). Therefore $n \nmid \binom{n}{q}a^{n-q}$ and hence the congruence (3.1) cannot hold. □

This theorem provides us with a deterministic primality test. Given an integer $n>1$, we can choose an a with $(a,n)=1$ and check if the polynomial congruence (3.1) is satisfied. Note that we can always choose $a=1$ since $(n,1)=1$ for any integer n.

Example 4.19. We use the previous theorem to verify that 7 is prime. We expand $(x+1)^7$ and reduce modulo 7 to find that

$$\begin{aligned}(x+1)^7 &= x^7 + \binom{7}{1}x^6 + \binom{7}{2}x^5 + \binom{7}{3}x^4 + \binom{7}{4}x^3 + \binom{7}{5}x^2 + \binom{7}{6}x + 1\\ &= x^7 + 7x^6 + 21x^5 + 35x^4 + 35x^3 + 21x^2 + 7x + 1\\ &\equiv x^7 + 1 \pmod{7}.\end{aligned}$$

Then since the congruence (3.1) is satisfied, 7 is prime.

We can also verify that 8 is composite. We expand $(x+1)^8$ and reduce modulo 8:

$$\begin{aligned}(x+1)^8 &= x^8 + \binom{8}{1}x^7 + \binom{8}{2}x^6 + \binom{8}{3}x^5 + \binom{8}{4}x^4 + \binom{8}{5}x^3 + \binom{8}{6}x^2 + \binom{8}{7}x + 1\\ &= x^8 + 8x^7 + 28x^6 + 56x^5 + 70x^4 + 56x^3 + 28x^2 + 8x + 1\\ &\equiv x^8 + 4x^6 + 6x^4 + 4x^2 + 1 \pmod 8\\ &\not\equiv x^8 + 1 \pmod 8.\end{aligned}$$

Since the congruence (3.1) is not satisfied, 8 is composite.

Unfortunately, testing numbers in this way is impractical. There are too many coefficients to compute when expanding $(x+a)^n$. We can eliminate some of the coefficients if we choose to reduce the polynomial $(x+a)^n$ modulo a convenient polynomial. Recall what it means to reduce one polynomial modulo another.

Definition 4.20. Let $f(x), g(x), h(x) \in \mathbb{Z}[x]$. We say that $f(x)$ is *congruent* to $g(x)$ modulo $h(x)$ and write $f(x) \equiv g(x) \pmod{h(x)}$ if $f(x) - g(x) = h(x)k(x)$ for some $k(x) \in \mathbb{Z}[x]$.

Similarly, we write $f(x) \not\equiv g(x) \pmod{h(x), n}$ to mean that $f(x) - g(x) \neq h(x)k(x)$ for any $k(x) \in \mathbb{Z}_n[x]$.

Choosing to reduce modulo $x^r - 1$, where $r > 1$ is an integer not exceeding n, will simplify the situation. This is due to the fact that if $x^r - 1 \equiv 0 \pmod{x^r - 1, n}$, then $x^r \equiv 1 \pmod{x^r - 1, n}$, meaning that we can replace any instance of x^r with 1 in the expansion of $(x+a)^n$. In other words, we replace any exponent $m \geq n$ with m modulo r.

Note that if the congruence $(x+a)^n \equiv x^n + a \pmod n$ holds, then the congruence $(x+a)^n \equiv x^n + a \pmod{x^r - 1, n}$ also holds. The only problem we encounter in reducing modulo $x^r - 1$ is that it is possible for two polynomials which are not congruent modulo n to leave the same remainder when further reduced modulo $x^r - 1$. This means that for some composite n, we could still obtain the congruence $(x+a)^n \equiv x^n + a \pmod{x^r - 1, n}$ when $(x+a)^n \not\equiv x^n + a \pmod n$.

Agrawal, Kayal and Saxena were able to provide additional restrictions which guarantee that the congruence $(x+a)^n \equiv x^n + a \pmod{x^r - 1, n}$ cannot hold for composite n. The algorithm derived is as follows and its proof of correctness can be found in [**1**], [**4**], [**11**].

Algorithm 4.21 (The AKS Test).

Input: integer $n > 1$.

1. If $n = a^b$ for $a \in \mathbb{N}$ and $b > 1$, output COMPOSITE.
2. Find the smallest r such that $\operatorname{ord}_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output COMPOSITE.
4. If $n \leq r$, output PRIME.
5. For $a = 1$ to $\lfloor \sqrt{\phi(r)} \log n \rfloor$ do
   if $(x+a)^n \neq x^n + a \pmod{x^r - 1, n}$, output COMPOSITE;
6. Output PRIME.

The main idea of the AKS test is that if n is composite, then the reduced polynomial congruence cannot hold for too many a's [**1**]. In order to implement the AKS algorithm, we require a quick method to detect perfect powers in step (1). Such a method is given below.

First, notice that we only need to check for prime exponents: If $b = pq$, where p is prime, then

$$n = a^{pq} = (a^q)^p.$$

The largest possible exponent we need to check for is the one for which the base a is 2. So we only need to check if $n = a^b$ for prime exponents b not exceeding $\log n$. Note that such a list can be obtained using the Sieve of Eratosthenes. Now for n to be a perfect power, the base $a = n^{1/b}$ must be an integer. Otherwise, n is not a perfect power.

Example 4.22. We can determine whether $n = 371293$ is a perfect power using the method described above. If $n = a^b$, then the largest possible exponent is $\log n \doteq 18.50$. Since we only need to check for prime exponents not exceeding $\log n$, the only exponents we need to check are 2, 3, 5, 7, 11, 13, and 17. Now we compute the necessary roots:

$$371293^{1/2} \doteq 609.34, \qquad 371293^{1/3} \doteq 71.87, \qquad 371293^{1/5} = 13.$$

Since the fifth root of n is the integer 13, we conclude that $n = 13^5$ is a perfect power.

With a method for detecting perfect powers in hand, we can begin to implement the AKS algorithm. The algorithm is easy to implement on a computer. On paper, however, there are many computations to do. For this reason, we only test very small values of n in this paper.

Example 4.23. Given $n = 5$, we first determine whether 5 is a perfect power. The only prime less than or equal to $\log 5 \doteq 2.32$ is 2, and computing

$$5^{1/2} \doteq 2.24,$$

we find that 5 is not a perfect power. Now we find the r in step (2). One can verify the following computations.

$$\begin{aligned} &\mathrm{ord}_2(5) = 1, && \mathrm{ord}_4(5) = 1, \\ &\mathrm{ord}_3(5) = 2, && \mathrm{ord}_5(5) > 6. \end{aligned}$$

So the smallest r for which $\mathrm{ord}_r(5) > \log^2 5 \doteq 5.39$ is $r = 5$. Then computing the necessary greatest common divisors in step (3), we find the following.

$$\begin{aligned} &(2,5) = 1, && (4,5) = 1, \\ &(3,5) = 1, && (5,5) = 5. \end{aligned}$$

None of these values are strictly between 1 and $n = 5$, so we continue to step (4). Since $n = 5 \leq 5 = r$, we conclude that 5 is prime.

EXAMPLE 4.24. Given $n = 15$, we first check whether 15 is a perfect power. The only primes less than or equal to $\log 15 \doteq 3.91$ are 2 and 3. Computing the roots

$$15^{1/2} \doteq 3.87 \qquad \text{and} \qquad 15^{1/3} \doteq 2.47,$$

we find that 15 is not a perfect power. Now we compute the following orders to complete step (2):

$$\text{ord}_2(15) = 1, \qquad \text{ord}_3(15) > 16.$$

The smallest r for which $\text{ord}_r(5) > \log^2 15 \doteq 15.26$ is $r = 3$. Then we compute the greatest common divisors in step (3) and find that

$$(2, 15) = 1, \qquad (3, 15) = 3.$$

Since $1 < (3, 15) < n = 5$, we conclude that 15 is composite.

EXAMPLE 4.25. For our final example, we test the integer $n = 31$. To see that 31 is not a perfect power, we note that $\log 31 \doteq 4.95$ and that neither of the necessary roots,

$$31^{1/2} \doteq 5.57 \qquad \text{and} \qquad 31^{1/3} \doteq 3.14,$$

are integers. To find the r is step 2, we compute $\text{ord}_r(31)$ for increasing values of r, beginning with $r = 2$. The first r for which $\text{ord}_r(31) > \log^2 31 \doteq 24.54$ is $r = 29$. Since $(a, 31) = 1$ for all $1 \leq a \leq r = 29$, we cannot conclude that 31 is composite in step (3), and since $n = 31 > 29 = r$, we cannot conclude in step (4) that 31 is prime.

Finally, we enter step (5) of the AKS algorithm. We find that $\phi(29) = 28$ either by inspection or by using the Euclidean algorithm to compute $(a, 29)$ for $a = 1$ to 28. Now we must check whether the polynomial congruence

$$(x + a)^n \equiv x^n + a \pmod{x^{29} - 1, 31}$$

is satisfied for $a = 1$ to $\lfloor \sqrt{\phi(29)} \log 31 \rfloor = 26$. After computing all 26 necessary congruences, we find that each congruence is satisfied. Therefore, 31 is prime.

CHAPTER 5

Conclusions

There are many ways to decide whether an integer is prime. In this paper, we have only covered a small number of methods. Some have been practical and some have been conclusive. Those tests which are practical have not been conclusive and those tests which are conclusive have not been practical [**4**]. The tests we have discussed here have ranged in complexity, from requiring only simple trial divisions to very involving computations, as in the AKS test.

Though some tests, such as trial division and Wilson's Theorem, cannot be improved upon, others can [**11**]. For example, Lucas' converse of Fermat's Little Theorem has several extensions past what we have developed here. In 1975, Brillhart, Lehmer and Selfridge proved that the base a discussed in Lucas' converse can be allowed to vary for each prime divisor of $n-1$, loosening the restrictions of the theorem and making the associated test much easier to implement. Better yet, Pocklington proved that $n-1$ need only be partially factored to make a probabilistic conclusion regarding the primality of n. The curious reader can find the derivation of these improvements in [**2**], [**11**].

The subject of primality testing has some surprising topics. Though all number-theoretical or algebraic, one might not suspect that the Fibonacci numbers or elliptic curves could have anything to do with primality testing. To see that theses topics (and more) can play in important role in the subject, we refer the reader to [**3**], [**7**], [**8**] and [**11**].

Bibliography

[1] Agrawal, Manindra, Neeraj Kayal, and Nitin Saxena. *PRIMES is in P*. Ann. of Math., 160:2 (2004) 781-793.

[2] Brillhart, John, D. H. Lehmer, and J. L. Selfridge. *New Primality Criteria and Factorizations of* $2^m \pm 1$. Math. Comp., 29 (1975) 620–647.

[3] Burton, David M. *Elementary Number Theory*. Boston: Allyn and Bacon, 1976.

[4] Granville, Andrew. *It is Easy to Determine Whether a Given Integer is Prime*. Bull. Amer. Math. Soc. (N.S.) 42 (2005), no. 1, 338.

[5] Hungerford, Thomas W. *Abstract Algebra, an Introduction*. 2nd ed. Toronto: Brooks Cole, 1996.

[6] Jones, Gareth A., and J. Mary Jones. *Elementary Number Theory*. London: Springer, 1998.

[7] Ore, Oystein. *Number Theory and its History*. Toronto: McGraw-Hill, 1948.

[8] Ribenboim, Paulo. *The New Book of Prime Number Records*. 3rd ed. New York: Springer-Verlag, 1996.

[9] Sierpiński, Waclaw. *A Selection of Problems in the Theory of Numbers*. Trans. A. Sharma. New York: PWN-Polish Scientific Publishers, 1964.

[10] Solomon, Richard. *Abstract Algebra*. Providence: Amer. Math. Soc., 2003.

[11] Yan, Song Y. *Primality Testing and Integer Factorization in Public-Key Cryptography*. 2nd ed. New York: Springer, 2009. *SpringerLink*.