Abstract

While I was studying music composition in Amsterdam during the winter and spring of 2009, I took interest in relating prime numbers to musical intervals. For my final composition project, I decided to compose a chamber piece that would be based heavily on prime numbers. Within the first week of writing I found a surprising and almost disturbing relationship between pitch intervals and prime numbers: I thought that I had stumbled upon a simple way to generate every prime number. I tried to assign each prime number to a pitch, but the method I used resulted in only 4 distinct tones being assigned. If there are infinitely many primes, how can they all be represented with only 4 tones? Since mathematicians have been trying to accomplish prime number prediction for thousands of years, I was very skeptical of the pattern I found. This paper will explain the pattern while including a discussion of special forms of prime numbers, including a proof of a special case of Dirichlet’s theorem.
1 Musical Introduction

Before going into the details of the pattern, we will study some basic knowledge of music theory. In the Western classical music system, there exist 12 unique tones. In ascending order they are C, C♯, D, D♯, E, F, F♯, G, G♯, A, A♯, and B. After B, we repeat the cycle starting again with C, except this C is one octave higher than the previous. Every pitch in every octave is represented by one of these twelve tones. The interval between any two adjacent tones is called one semi-tone. For example, between C and F there are 5 semi-tones (C to C♯, C♯ to D, D to D♯, D♯ to E, and E to F). Between F and C, there are 7 semi-tones.

Let us select C as our starting pitch and make a list of the pitches that are higher than C by a semi-tone difference equal to the first 17 prime numbers.
C + 2 = D
3 = D♯
5 = F
7 = G
11 = B
13 = C♯
17 = F
19 = G
23 = B
29 = F
31 = G
37 = C♯
41 = F
43 = G
47 = B
53 = F
59 = B

Notice that after C + 3, there appears to be only 4 tones that correspond to prime number pitch intervals. They are F, G, B and C♯. Remember that the cycle of tones repeats every 12 tones, thus any prime greater than 12 can be reduced by subtracting some multiple of 12. For example, adding 13 is equivalent to adding 1 since 13 − 12(1) = 1, and adding 53 is equivalent to adding 5 since 53 − 12(4) = 5. Now it is more clear why tones are being repeated, but there are other intriguing questions to be answered. Why are only 4 tones repeated? Will the other 8 tones ever appear? Why do D and D♯ only appear once? Can we predict the pitch of the next prime interval or any given prime interval? Notice that if our starting pitch is different from C, the
tones corresponding to prime intervals will change. Given a starting pitch $S$, can we come up with a method of showing precisely which tones (with respect to $S$) might correspond to a prime interval and precisely which tones will never correspond to a prime interval? Let us formulate some conjectures to motivate a more detailed analysis of the patterns we are noticing.

**Conjecture 1.1.** Let $S$ denote a starting tone and $N = \{4, 6, 8, 9, 10, 12\}$. Then the tones $S + n$ for $n \in N$ (in any octave) will never correspond to a prime interval.

To make this clearer, let $S = G$. Then the tones $G + n = B, C^\#,$ $D^\#, E,$ $F$ and $G$ (respectively, in any octave) will never correspond to a prime interval. Earlier we noted that a pitch that is greater than 12 semi-tones away from the starting pitch can be reduced by subtracting some multiple of 12. This reduced form is the same as the remainder of $(the\ semi-tone\ difference\ between\ S\ and\ S + n)/12$.

**Conjecture 1.2.** Let $S$ denote a starting tone. Then the tones $S + 2$ and $S + 3$ correspond to a prime interval only once: within the first octave above $S$.

The proof of this conjecture, which will come later, will explain why D and $D^\#$ appeared only once in the first example of prime intervals.

**Conjecture 1.3.** Let $S$ denote a starting tone and $R = \{1, 5, 7, 11\}$. Then, for any $r \in R$, the tones $S + r$ (in any octave) are the only four tones that may repeatedly correspond to prime intervals. Furthermore, these four tones will correspond to prime intervals with infinitely many repetitions (limited only by the spectrum of audible frequencies).

Notice how we have added the modifier *in any octave* to two of the conjectures above. That is because every octave is a cycle of 12 semi-tones. We can
let $S = 0$ and add $12k$ semi-tones to $S$ for some $k \in \mathbb{N}$ to get any octave trans-
position of $S$. Then the tones $S + r$ are equal to the tones $S + 12k + r = 12k + r$.

Using number theory, we can relate this cycle to something called the theory of congruences. Before we do so, let us first try to compile the musical conjectures into one mathematical conjecture.

**Conjecture 1.4.** There are infinitely many prime numbers of the form $12k + r$, for some $k \in \mathbb{N}$ and $r \in R = \{1, 5, 7, 11\}$. For any positive integer $n \leq 12$ with $n \notin R$, $12k + n$ is never prime; the only exception is when $k = 0$ and $n = 2$ or $n = 3$.

To make this statement more precise and easier to understand, we will introduce congruences and some other important background information from elementary number theory.

## 2 Elementary Number Theory

As a note to the reader, please be aware that all letter variables correspond to an arbitrary positive integer unless specified otherwise.

**Theorem 2.1. Division Algorithm.** Given integers $a$ and $b$, with $b > 0$, there exists unique integers $q$ and $r$ such that

$$a = qb + r \quad \text{for } 0 \leq r < b$$

We call $q$ the quotient and $r$ the remainder in the division of $a$ by $b$.

The proof of this theorem can be found in most number theory textbooks. We will omit the proof and immediately continue on the topic of division.

**Definition 2.2.** An integer $b$ is said to be divisible by an integer $a \neq 0$ if there exists some integer $c$ such that $b = ac$. To denote divisibility, we write $a|b$, read as $a$ divides $b$. If $a$ does not divide $b$, we write $a \nmid b$. 
Theorem 2.3. Properties of Division. Let $a, b, c \in \mathbb{Z}$, nonzero as needed. We have,

(a) $a|0, 1|a, a|a$

(b) $a|1$ if and only if $a = \pm 1$

(c) if $a|b$ and $b|c$, then $a|c$

(d) if $a|b$ and $b \neq 0$ then $|a| \leq |b|$

(e) if $a|b$ and $a|c$ then $a|b - c$

Proof. Let $a \neq 0$ be an arbitrary integer.

(a) We must produce an integer $c$ such that $0 = ac$. Let $c = 0$. Clearly, $0 = a \cdot 0$. Also, it is clear that $a = 1 \cdot a$ and $a = a \cdot 1$.

(b) Assume that $a|1$. Then $1 = ac$. The product of two integers is equal to $1$ only when the two integers are $1 \cdot 1$ or $(-1) \cdot (-1)$. Therefore $a = \pm 1$. Now assume that $a = \pm 1$. If $a = 1$ then $a|1$ is obvious. If $a = -1$, we let $c = -1$ and it is clear that $1 = ac = (-1)(-1)$. Therefore $a|1$.

(c) Assume that $a|b$ and $b|c$ for $b, c \in \mathbb{Z}$, $b \neq 0$. Then $b = ad$ for some integer $d \in \mathbb{Z}$, and $c = be$ for some $e \in \mathbb{Z}$. Since $b = ad$, it follows that $c = a(de)$ with $de \in \mathbb{Z}$. Therefore $a|c$.

(d) Assume $a|b$ and $b \neq 0$. Then there exists an integer $c$ such that $b = ac$; also $b \neq 0$ implies that $c \neq 0$. We may take the absolute values to obtain $|b| = |ac| = |a||c|$. Since $c \neq 0$, it follows that $|c| \geq 1$. Thus $|b| = |a||c| \geq |a|$.

(e) Assume $a|b$ and $a|c$. Then $b = ak_1$ and $c = ak_2$ for some $k_1, k_2 \in \mathbb{Z}$. Therefore $b - c = ak_1 - ak_2 = a(k_1 - k_2)$. Since $(k_1 - k_2) \in \mathbb{Z}$, this shows that $a|b - c$.

We have all seen and heard of prime numbers, but a precise definition will prove useful later in the paper.
**Definition 2.4.** Let $p$ be an integer greater than 1. If the only positive divisors of $p$ are itself and 1, i.e., if $k|p$ then $k = p$ or $k = 1$ for a positive integer $k$, then $p$ is said to be a **prime** number. An integer $r > 1$ is called a **composite** number if it is not prime.

We now have the necessary background to define the congruence notation.

**Definition 2.5. Theory of Congruences.** Let $n$ be a fixed positive integer. Two integers $a$ and $b$ are congruent modulo $n$, written as

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

if $n$ divides the difference $a - b$, i.e., $a - b = kn$ for some $k \in \mathbb{Z}$.

We can take the reductions we made earlier and rewrite them using congruences modulo 12.

**Example 2.6.** We have $13 \equiv 1 \pmod{12}$, since $13 - 1 = 12(1)$. Also, $53 \equiv 5 \pmod{12}$, since $53 - 5 = 12(4)$.

Before we try to prove the conjectures posed in Section 1, there are two related definitions we must understand.

**Definition 2.7.** Let $a$ and $b$ be integers with $a$ or $b \neq 0$. The **greatest common divisor** of $a$ and $b$, denoted by $\text{gcd} (a, b)$, is the positive integer $d$ such that $d|a$ and $d|b$, and if $c|a$ and $c|b$, then $c \leq d$.

**Definition 2.8.** Two integers $a$ and $b$ are said to be **relatively prime** if $\text{gcd} (a, b) = 1$.

**Example 2.9.** The $\text{gcd} (15, 24) = 3$, and $\text{gcd} (13, 24) = 1$. Then 24 and 15 are not relatively prime, but 24 and 13 are relatively prime.
Calling upon these previous definitions, we will state the contrapositive of a theorem often referred to as Euclid’s lemma. The result will prove useful in the Section 6. For a proof of the theorem, please see [1].

**Theorem 2.10.** Let the \( \gcd(a, b) = 1 \) for integers \( a \) and \( b \). If \( a \nmid c \) for some integer \( c \), then \( a \nmid bc \).

**Example 2.11.** Let \( a = 11 \) and \( b = 4 \) and note that \( \gcd(11, 4) = 1 \). By Theorem 2.10, since \( 11 \nmid 25 \), \( 11 \nmid 4(25) \).

Now that we have a some basic background in number theory, let us take another look at the conjectures posed in the first section. Let us begin with Conjecture 1.1. What are the similarities between the numbers of the set \( n \in \mathbb{N} = \{4, 6, 8, 9, 10, 12\} \)? The most apparent commonality is that they are all composite numbers. Secondly, of the six numbers, none is relatively prime to 12. Let \( t \) equal the semi-tone difference between \( S \) and whatever note is obtained by \( S + n \). We will now refer to \( S \) as a positive integer rather than a specific pitch. Applying the definition of division, Conjecture 1.1 states that for \( t = 12S + n \), \( t \) can never be prime.

**Proof.** (Conjecture 1.1).

Note that for \( t = 12S + n \), the \( \gcd(12, n) > 1 \). Let \( d = \gcd(12, n) \) for some integer \( d \geq 2 \). Then \( t = d[(12/d)S + (n/d)] \) where \( 12/d \) and \( n/d \) must be integers since \( d \) is a divisor of both 12 and \( n \). If \( d = 12 \), then \( t \) is divisible by every factor of 12. This proves that \( 12S + n \) has an integer factor other than 1 and itself, i.e., \( 12S + n \) is never prime.

\[ \square \]

From this proof it follows that if \( \gcd(12, r) = d > 1 \) for \( t = 12S + r \), then \( t \) is not prime. However, in Conjecture 1.3 we acknowledged that 2 and 3
correspond to a prime interval once. This is because 2 and 3 are prime numbers to begin with. Once we go beyond the first octave above the starting pitch, any $t$ having a remainder of 2 or 3 upon division by 12 will not be prime since 2 and 3 are factors of both 12 and 2 or 3.

The only claim left to prove is the first statement within Conjecture 1.4. In congruence notation, this conjecture states that there are infinitely many primes $p$ of the form $p \equiv 1 \text{ or } 5 \text{ or } 7 \text{ or } 11 \pmod{12}$. We were able to prove that numbers of the form $t = 12k + n$ are never prime, but how does one prove numbers of a special form are frequently prime? We will study a useful method for proving the existence of an infinitude of primes in the following section. This method will aid us in proving that special forms of numbers contain infinitely many prime numbers. Also, we will take a look at one example of prime numbers in a special form keeping in mind that our goal is to prove the first statement within Conjecture 1.4.

3 An Infinitude of Prime Numbers

Before we begin any proofs or examples, we must understand an all important theorem that will be utilized within every following theorem.

**Theorem 3.1. Fundamental Theorem of Arithmetic.** Every positive integer $n \geq 2$ can be expressed as a product of prime numbers. Furthermore, this representation is unique, apart from the order in which the primes occur.

**Proof.** Omitted. This proof can be found in any elementary number theory textbook.

Let us take a look at some numerical examples of 3.1.

**Example 3.2.** Consider the following prime factorizations:
30 = 2 \cdot 3 \cdot 5
15 = 3 \cdot 5
64 = 2^6
41 = 41

There exists a very effective method for proving the existence of an infinitude of primes. Around 300 BCE, Euclid proved the existence of an infinitude of primes by first assuming that there is a finite number of primes. Next, he constructed a number based on the product of all primes plus a remainder. Upon studying the prime factorization of this number, he arrived at a contradiction within the proof. From this contradiction, the only conclusion is that there must be an infinitude of primes. This method motivates the proof of every theorem involving primes of a special form throughout Section 4. Let us begin our study of primes with Euclid’s famous theorem:

**Theorem 3.3.** There is an infinite number of primes.

**Proof.** To arrive at a contradiction, assume that there is a finite number of primes. Let \( p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_n \) be the complete listing of the primes in ascending order. By our assumption, \( p_n \) is the largest and last prime in existence. Consider the positive integer

\[
N = p_1p_2p_3 \ldots p_n + 1
\]

Since \( N \geq 2 \), we call upon Theorem 3.1 to conclude that \( N \) must have some prime factorization. Let \( p \) be a prime factor of \( N \), i.e., \( p|N \). We have listed all of the prime numbers \( (p_1, \ldots, p_n) \), therefore \( p \) must equal one of the listed primes. Thus \( p|p_1p_2p_3 \ldots p_n \). Since \( p|p_1p_2p_3 \ldots p_n + 1 \) and \( p|p_1p_2p_3 \ldots p_n \), by Theorem 2.3, \( p|1 \). Then \( p = \pm 1 \). But \( p \) is prime by assumption, hence \( p \geq 2 \). This contradiction forces us to conclude that there is not a finite number of primes, i.e., there is an infinite number of primes.
Using Euclid’s method as a guide, let us move on to our first special form of prime numbers: $4k + 3$. Before we start our proof, we will need to examine a small lemma.

**Lemma 3.4.** The product of two or more integers of the form $4k+1$ is also of the form $4k + 1$.

**Proof.** We will prove the result for the product of two integers of the form $4k+1$. The general result for more than two integers follows easily by induction. Consider the integers $a = 4n + 1$ and $b = 4m + 1$. We multiply to obtain

$$ab = (4n + 1)(4m + 1) = 16nm + 4m + 4n + 1 = 4(4nm + m + n) + 1$$

We let $k = 4nm + m + n$ to see that $ab$ is of the form $4k + 1$. \qed

Now we may prove the following theorem.

**Theorem 3.5.** There is an infinite number of primes of the form $4k + 3$.

**Proof.** To arrive at a contradiction, assume that there is a finite number of primes of the form $4k + 3$, call them $p_1, p_2, p_3, \ldots, p_s$. Consider the positive integer

$$(*) \quad N = 4p_1p_2p_3\ldots p_s - 1 = 4(p_1p_2\ldots p_s - 1) + 3$$

and let $N = q_1q_2\ldots q_r$ be its prime factorization. Note that $4p_1p_2p_3\ldots p_s$ is even, thus $N$ is odd. Because $N$ is odd, $q_i \neq 2$ for every prime $q_i$ in the factorization of $N$. Then each $q_i$ is either of form $4k + 1$ or $4k + 3$. By Lemma 3.4, $N$ may be of the form $4k + 1$ if every $q_i$ is of the same form. But, by $(*)$, $N$ is of the form $4k + 3$. Therefore there exists at least one $q_i$, call it $q$, such that $q = 4k + 3$. Then $q$ must equal one of the primes $p_i$ of the form $4k + 3$,
and so \( q | 4p_1p_2p_3 \ldots p_s \). Since \( q | 4p_1p_2p_3 \ldots p_s - 1 \) as well, it follows by Theorem 2.3 that \( q | 1 \). But \( q \geq 3 \) by assumption. This contradiction to Theorem 2.3 (b) forces us to conclude that there is an infinite number of primes of the form 
\[ 4k + 3. \]

To continue our study of special forms of prime numbers we must introduce some more background from number theory. Notice that our construction of \( N \) in the last two proofs depended on which form of prime numbers we were examining. The following examples of special forms of prime numbers have less obvious constructions of \( N \). These examples will also require a deeper understanding of congruences and something called quadratic residues. We will explore the required background and study five examples of special forms of prime numbers in the next section.

### 4 Special Forms of Primes

In this section, the background from number theory will rely heavily on a sound understanding of congruences. The following theorem states some basic properties of congruences.

**Theorem 4.1.** Let \( n \geq 2 \) be fixed and \( a, b, c, d \) be arbitrary integers. The following properties hold:

(a) For any \( a \), \( a \equiv a \pmod{n} \)

(b) If \( a \equiv b \pmod{n} \), then \( b \equiv a \pmod{n} \)

(c) If \( a \equiv b \pmod{n} \) and \( b \equiv c \pmod{n} \), then \( a \equiv c \pmod{n} \).

(d) If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \), then \( a + c \equiv b + d \pmod{n} \) and 
\[ ac \equiv bd \pmod{n} \]
(e) If $a \equiv b \pmod{n}$, then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$

(f) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any $k \in \mathbb{N}$

Notice the power of congruencies allows us to generalize the result from Lemma 3.4.

**Corollary 4.2.** If $a \equiv 1 \pmod{n}$ and $b \equiv 1 \pmod{n}$, then $ab \equiv 1 \pmod{n}$. In particular, the result in Lemma 3.4 holds.

**Definition 4.3.** Let $p$ be an odd prime with $\gcd(a, p) = 1$. If the quadratic congruence

$$x^2 \equiv a \pmod{p}$$

has a solution, then $a$ is said to be a *quadratic residue* of $p$. If there is no solution, $a$ is called a *quadratic nonresidue* of $p$.

**Example 4.4.** Let $p = 13$. Before finding the quadratic residues of $p$, let us try to minimize the number of steps we will need to perform. Notice that the quadratic residues are congruent to the perfect squares modulo $p$. To determine the quadratic residues, we need only determine the congruencies of perfect squares modulo $p$. Next, notice that $x$ is being squared. Since $(-x) \equiv (p-x) \pmod{p}$, by Theorem 4.1 we have $(x)^2 = (-x)^2 \equiv (p-x)^2 \pmod{p}$.

For modulo 13, we have the following:

$$1^2 \equiv 12^2 \equiv 1 \pmod{13}$$
$$2^2 \equiv 11^2 \equiv 4$$
$$3^2 \equiv 10^2 \equiv 9$$
$$4^2 \equiv 9^2 \equiv 16 \equiv 3$$
$$5^2 \equiv 8^2 \equiv 25 \equiv 12$$
$$6^2 \equiv 7^2 \equiv 36 \equiv 10$$
Then the values of $a$ for which solutions to $x^2 \equiv a \pmod{13}$ exist, i.e., the quadratic residues of 13, are $a \in A$ where $A = \{1, 3, 4, 9, 10, 12\}$. Then the quadratic nonresidues of 13 are all integers $b < 13$ such that $b \not\in A$.

We can see that if $p$ is very large, say $p = 997$, it would take a long time to find the quadratic residues using the same method as above. Euler recognized this issue and came up with a formula for quadratic residue verification.

**Theorem 4.5. Euler’s Criterion.** Let $p$ be an odd prime with the gcd $(a, p) = 1$. Then $a$ is a quadratic residue of $p$ if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

In order to avoid introducing excess background from number theory, the proof of this theorem is omitted. Instead, we will show how the theorem above applies when $p = 13$ using the quadratic residues found earlier. For $p = 13$, $a^{(p-1)/2} = a^6$. Then $a$ is a quadratic residue of 13 if and only if $a^6 \equiv 1 \pmod{13}$.

\[
\begin{align*}
1^6 &\equiv 1 \pmod{13} \\
3^6 &\equiv 27^2 \equiv 1 \pmod{13} \\
4^6 &\equiv 16^3 \equiv 3^3 \equiv 1 \pmod{13} \\
9^6 &\equiv 81^3 \equiv 3^3 \equiv 1 \pmod{13} \\
10^6 &\equiv 100^3 \equiv 9^3 \equiv 27^2 \equiv 1 \pmod{13} \\
12^6 &\equiv (-1)^6 \equiv 1 \pmod{13}
\end{align*}
\]

An integer $a$ is a quadratic nonresidue of 13 if and only if $a^6 \equiv -1 \pmod{13}$.

\[
\begin{align*}
2^6 &\equiv 64 \equiv -1 \pmod{13} \\
5^6 &\equiv (-1)^3 \equiv -1 \pmod{13} \\
6^6 &\equiv 10^3 \equiv -1 \pmod{13} \\
7^6 &\equiv 10^3 \equiv -1 \pmod{13} \\
8^6 &\equiv 64^3 \equiv (-1)^3 \equiv -1 \pmod{13} \\
11^6 &\equiv 4^3 \equiv 64 \equiv -1 \pmod{13}
\end{align*}
\]
Quadratic residues are vital to our study of prime numbers. They are used so often that a short-hand notation was developed by Adrien Marie Legendre in the late 18th century.

**Definition 4.6.** Let $p$ be an odd prime with $\gcd(a, p) = 1$. The Legendre symbol $(a/p)$ is defined as

$$(a/p) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue of } p \\
-1 & \text{if } a \text{ is a quadratic nonresidue of } p
\end{cases}$$

**Example 4.7.** Going back to 13 again, we can now apply the Legendre symbol:

$$(1/13) = 1$$
$$(3/13) = 1$$
$$(5/13) = -1$$

**Theorem 4.8. Properties of the Legendre symbol.** Let $p$ be an odd prime and let the integers $a$ and $b$ be relatively prime to $p$. The following properties hold:

(a) If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$

(b) $(a^2/p) = 1$

(c) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$

(d) $(ab/p) = (a/p)(b/p)$

(e) $(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$

We will again omit the proof of theorem, which is not difficult. The properties above allow for an important corollary which will establish a theorem concerning our second special form of prime numbers.
Corollary 4.9. If \( p \) is an odd prime, then \((-1/p) = 1\) if \( p \equiv 1 \pmod{4} \), and \((-1/p) = -1\) if \( p \equiv -1 \pmod{4} \).

Proof. Let \( p \) be an odd prime and assume \( p \equiv 1 \pmod{4} \). Then \( p = 4k + 1 \) for some \( k \in \mathbb{Z} \). By Theorem 4.8 (e),

\[
(-1/p) = (-1)^{(p-1)/2} = (-1)^{4k/2} = (-1)^{2k} = (-1)^{2k} = 1^k = 1.
\]

Now we assume \( p \equiv -1 \pmod{4} \). Then \( p = 4k + 3 \) for some \( k \in \mathbb{Z} \). We have,

\[
(-1/p) = (-1)^{(p-1)/2} = (-1)^{(4k+2)/2} = (-1)^{2k+1} = (-1)^{2k}(-1) = -1.
\]

\[\square\]

We will call upon this corollary during the proof of our next theorem.

Theorem 4.10. There is an infinite number of primes \( p \) of the form \( p = 4k+1 \).

Proof. Suppose for contradiction that there is a finite number of primes of the form \( p = 4k + 1 \), call them \( p_1, p_2, \ldots, p_n \). Consider the positive integer

\[
N = (2p_1p_2\ldots p_n)^2 + 1
\]

and note that \( N \) is odd because \((2p_1p_2\ldots p_n)^2\) is even. Since \( N \) is odd, there exists some odd prime \( q \) in the prime factorization of \( N \). Then \( N \equiv 0 \pmod{q} \) and so \((2p_1p_2\ldots p_n)^2 = N - 1 \equiv -1 \pmod{q}\). Thus \(-1\) is a quadratic residue of \( q \). In Legendre symbol notation, \((-1/q) = 1\). By Corollary 4, since \((-1/q) = 1\), we know \( q \) is of the form \( 4k + 1 \). Then \( q \) must be equal to one of the primes \( p_1, p_2, \ldots, p_n \). Consequently, \( q | (2p_1p_2\ldots p_n)^2 \) By Theorem 2.3 (e), since \( q | N \) and \( q | (2p_1p_2\ldots p_n)^2 \), we have \( q | 1 \). But, since \( q \geq 5 \), this is a contradiction. This contradiction forces us to conclude that there are infinitely many primes of the form \( 4k + 1 \).

\[\square\]
What are all of the possible congruencies of prime numbers modulo 4? We have seen that there are infinitely many primes congruent to 1 (mod 4) and 3 (mod 4). There are only two other possibilities; they are primes congruent to 0 (mod 4) or 2 (mod 4). However, no prime is congruent to 0 (mod 4) because this implies the prime is divisible by 4. The only prime congruent to 2 (mod 4) is 2. Any integer whose absolute value is greater than 2 and is of the form $4k + 2 = 2(2k + 1)$ clearly has a factor of 2. Thus any prime number is either congruent to 1 (mod 4) or 3 (mod 4), except for the special case when $p = 2$.

Now that we have seen all of the possible congruencies of prime numbers modulo 4, we will move on to some examples of primes modulo 8, modulo 6, and modulo 12. The next special form for study will be $8k - 1$, but we will first state a useful lemma similar to the corollary used for $p = 4k + 1$.

**Lemma 4.11.** Let $p$ be an odd prime. If $(2/p) = 1$, then $p \equiv 1$ or $-1$ (mod 8).

**Theorem 4.12.** There are infinitely many primes of the form $8k - 1$.

**Proof.** Suppose for contradiction that there are finitely many primes of the form $8k - 1$, call them $p_1, p_2, \ldots, p_n$ where $p_n$ is the largest such prime. Consider the positive integer

$$N = (4p_1p_2 \ldots p_n)^2 - 2 = 16p_1^2p_2^2 \ldots p_n^2 - 2.$$ 

Note the following two properties of $N$:

1. $N \equiv 0 - 2 \equiv 6$ (mod 8)
2. $N = 2q_1q_2 \ldots q_r$, with odd primes $q_i$.

By (2), $N$ has at least one odd prime divisor. In addition, every odd prime divisor $q$ of $N$ satisfies $(4p_1p_2 \ldots p_n)^2 - 2 \equiv 0$ (mod $q$). It follows that $(4p_1p_2 \ldots p_n)^2 \equiv 2$ (mod $q$), and so $(2/q) = 1$. By Lemma 4.11, since $(2/q) = 1$, we have $q \equiv \pm 1$ (mod 8).
Suppose \( q_i \equiv 1 \) (mod 8) for every odd prime divisor \( q_i \). By Corollary 4.2, \( q_1 \cdots q_r \equiv 1 \) (mod 8) so that \( N = 2q_1 \cdots q_r \equiv 2 \) (mod 8). However, by (1) above, \( N \equiv 6 \neq 2 \) (mod 8). Therefore, there exists at least one odd prime divisor \( q \) such that \( q \equiv -1 \) (mod 8). Then \( q \) is of form \( 8k - 1 \), that is, \( q = p_j \) for some \( j \). Thus \( q \mid (4p_1p_2 \cdots p_n)^2 \). Since \( q \mid N \) and \( q \mid (4p_1p_2 \cdots p_n)^2 \), it follows that \( q \mid 2 \). But \( q > 2 \) since \( q \) is an odd prime. With this contradiction, our only possible conclusion is that there are infinitely many primes of the form \( 8k - 1 \).

Continuing with special forms of primes modulo 8, let us have look at primes of the form \( 8k + 3 \). Before processing the proof, we will need to state another lemma.

**Lemma 4.13.** Let \( p \) be an odd prime. If \((−2/p) = 1\), then \( p \equiv 1 \) or \( 3 \) (mod 8).

**Theorem 4.14.** There are infinitely many primes of the form \( 8k + 3 \).

**Proof.** Suppose for contradiction that there is a finite number of primes of the form \( 8k + 3 \). Call these primes \( p_1, p_2, \ldots, p_n \) and consider the positive integer

\[
N = (2p_1p_2 \cdots p_n)^2 + 2 = 2(2p_1^2p_2^2 \cdots p_n^2 + 1).
\]

From this, we see that

1. Since \( p_i \equiv 3 \) (mod 8), we have \( p_i^2 \equiv 1 \) (mod 8). Consequently, \( N \equiv 2(2(1)^n + 1) \equiv 6 \) (mod 8).

2. \( N \) is even and has a prime factorization \( N = 2q_1q_2 \cdots q_r \) for odd primes \( q_i \).

As a consequence of (2), we have \( N \equiv 0 \) (mod \( q_i \)). Thus \( (2p_1p_2 \cdots p_n)^2 \equiv -2 \) (mod \( q_i \)), that is, \((−2/q_i) = 1\). By Lemma 4.13, for each \( i \) we have \( q_i \equiv 1 \) or \( 3 \) (mod 8).
We will show there exists some \( q_i \equiv 3 \pmod{8} \). Suppose every \( q_i \) is congruent to 1 (mod 8). Then, from the factorization of \( N \) in (2), we have \( N \equiv 2(1^r) \equiv 2 \pmod{8} \). This contradicts that \( N \equiv 6 \pmod{8} \) from (1). Therefore, not every \( q_i \equiv 1 \pmod{8} \). So there exists some \( q_i \equiv 3 \pmod{8} \); call it \( q \). But then \( q \) is equal to some \( p_i \) on the complete and finite list of primes congruent to 3 (mod 8). Therefore \( q | (2p_1p_2 \ldots p_n)^2 \). Since \( q | (2p_1p_2 \ldots p_n)^2 \) and \( q | N \), it follows that \( q | 2 \). However, \( q \) is an odd prime, thus \( q \geq 3 \). This contradiction forces us to conclude that there are infinitely many primes of the form \( 8k + 3 \).

\[ \square \]

**Lemma 4.15.** Let \( p > 3 \) be an odd prime. If \((-3/p) = 1\), then \( p \equiv 1 \pmod{6} \).

**Theorem 4.16.** There is an infinite number of primes of the form \( 6k + 1 \).

**Proof.** Assume for contradiction that there is a finite number of primes of the form \( 6k + 1 \), call them \( p_1, p_2, \ldots, p_n \). Consider the integer

\[ N = (2p_1p_2 \ldots p_n)^2 + 3. \]

Since \( N \) is odd, there exists at least one odd prime divisor \( q \) of \( N \). For every odd prime divisor \( q \) of \( N \), \((2p_1p_2 \ldots p_n)^2 \equiv -3 \pmod{q} \). Note \( q \neq 3 \) because \( N = (2p_1p_2 \ldots p_n)^2 + 3 \equiv (2 \cdot 1 \cdots 1)^2 \equiv 4 \equiv 1 \pmod{3} \). Then by Lemma 4.15, since \((-3/q) = 1 \) and \( q > 3 \), we know that \( q \equiv 1 \pmod{6} \), i.e., \( q \) is of the form \( 6k + 1 \). Thus \( q \) is equal to one of the \( p_i \). Therefore \( q | (2p_1p_2 \ldots p_n)^2 \). Since \( q | (2p_1p_2 \ldots p_n)^2 \) and \( q | N \), it follows that \( q | 2 \). But this contradicts that \( q > 3 \). This contradiction leads to the conclusion that there is an infinite number of primes of the form \( 6k + 1 \).

\[ \square \]

Now we move on to our last example, primes of the form \( 12k - 1 \), or equivalently, \( 12k + 11 \). This example relates back to our musical introduction. If
there are infinitely many primes \( p = 12k + 11 \), then there are infinitely many primes intervals with pitch \( 12S + 11 \).

**Lemma 4.17.** Let \( p > 3 \) be an odd prime. If \( (3/p) = 1 \), then \( p \equiv \pm 1 \pmod{12} \).

**Theorem 4.18.** There are infinitely many primes of the form \( 12k - 1 \).

**Proof.** Assume for contradiction that there are finitely many prime numbers of the form \( 12k - 1 \), call them \( p_1, p_2, \ldots, p_n \). Consider the integer

\[
N = (6p_1 p_2 \ldots p_n)^2 - 3 = 3(12p_1^2 p_2^2 \ldots p_n^2 - 1)
\]

Note that

1. Since \( 12p_1^2 p_2^2 \ldots p_n^2 - 1 \) is odd and is not divisible by 3, we have the prime factorization \( N = 3q_1 \ldots q_r \) where \( q_i > 3 \) are odd primes.

2. \( N = 3(12p_1^2 p_2^2 \ldots p_n^2 - 1) \equiv 3(0 - 1) \equiv -3 \equiv 9 \pmod{12} \).

Thus, for each of these \( q_i \), we have \( (6p_1 p_2 \ldots p_n) \equiv 3 \pmod{q_i} \), that is, \( (3/q_i) = 1 \). Hence, by Lemma 4.17, \( q_i \equiv \pm 1 \pmod{12} \).

We now show that not all of the \( q_i \) are congruent to 1 (mod 12). Suppose this were the case. Then from the prime factorization of \( N \) in (1), we have \( N \equiv 3 \cdot 1 \cdots 1 \equiv 3 \pmod{12} \). But, by (2), \( N \equiv 9 \neq 3 \pmod{12} \). Hence, at least one of the \( q_i \) is congruent to \(-1\) (mod 12), call it \( q \). Then \( q \) is equal to one of the \( p_1, p_2, \ldots, p_n \). Therefore \( q \mid (6p_1 p_2 \ldots p_n)^2 \). Since \( q \mid (6p_1 p_2 \ldots p_n)^2 \) and \( q \mid N \), it follows that \( q \mid 3 \). But we know \( q > 3 \). This contradiction forces us to conclude that there are infinitely many primes of the form \( 12k - 1 \). \qed

This proof concludes our study of specific examples of special primes. One might notice that there seems to be an endless number of special forms of primes numbers for which there are infinitely many primes. We saw primes congruent to modulo 4, 6, 8 and 12; but with a little more investigation, we
might make a conjecture about primes modulo 5, 14 or more generally, modulo \( n \). This curiosity motivated a very powerful theorem that will be the focus of the remainder of this paper.

5 Dirichlet’s Theorem

Theorem 5.1. Dirichlet’s Theorem. If \( a \) and \( b \) are relatively prime positive integers, then the arithmetic progression

\[
a, a + b, a + 2b, a + 3b, \ldots
\]

contains infinitely many primes.

Take a moment to this theorem to special forms of prime numbers we have studied thus far. Let \( a = 3 \) and \( b = 8 \) in the following arithmetic progression:

\[
3, 3 + 8, 3 + 2(8), 3 + 3(8), \ldots
\]

Notice that this progression is precisely all integers of the form \( 8k+3 \). Dirichlet’s theorem proves Theorem 4.14 very quickly. In fact, Dirichlet’s theorem is very powerful; not only does it prove the result from Theorem 4.14 and all other special forms in Section 4, it also proves that there are infinitely many primes of the general form \( p = nk + r \), as long as \( n \) and \( r \) are relatively prime positive integers.

However, there are no known elementary proofs of Dirichlet’s theorem. We must also note that Dirichlet’s theorem does not state that every entry is prime. In fact, there are also infinitely many composite numbers contained in any given Dirichlet arithmetic progression.

Theorem 5.2. If \( a \) and \( b \) are relatively prime positive integers, then the arithmetic progression
contains infinitely many composite numbers.

Proof. Let us assume, for now, that $a > 1$. We will refer to any entry in the progression by the coefficient of $b$, e.g., the $j^{th}$ entry is $a + jb$. Consider every entry that is a multiple of $a$, e.g., the $ka^{th}$ entry is $a + ka(b)$ for some $k \in \mathbb{N}$. Since $a > 1$, there exists a nontrivial factorization of every entry that is a multiple of $a$ as follows:

$$a + ka(b) = a(1 + bk).$$

Since the series is infinite, and there are infinitely many $k \in \mathbb{N}$, it follows that the progression contains infinitely many composites.

Now let us assume that $a = 1$. The progression is as follows:

$$1, 1 + b, 1 + 2b, \ldots$$

Consider the composite number $(b + 1)^2 = 1 + 2b + b^2 = 1 + (2 + b)b$. This number is clearly the $(2+b)^{th}$ entry of the progression. Let us also consider the integer $(b + 1)^3 = 1 + (b^2 + 3b + 3)b$, and note that this composite number is the $(b^2 + 3b + 3)^{th}$ entry in the progression. Recall the general binomial expansion for

$$(b + 1)^n = b^n + k_{n-1}b^{n-1} + \cdots + k_2b^2 + k_1b + 1$$

where $n, k_i \in \mathbb{N}$. Notice that every term has a factor of $b$, except for the constant term 1. Then we may write

$$(b + 1)^n = 1 + (b^{n-1} + k_{n-1}b^{n-2} + \cdots + k_2b + k_1)b$$

to see that $(b + 1)^n$ is the $(b^{n-1} + k_{n-1}b^{n-2} + \cdots + k_2b + k_1)^{th}$ entry in the arithmetic progression. Furthermore, it is clear that $(b + 1)^n$ is a composite
number for every \( n > 1 \). Therefore the progression \( 1, 1 + b, 1 + 2b, \ldots \) contains infinitely many composite numbers.

Not only do composites appear infinitely many times in a Dirichlet progression, but we can prove something intriguing about how often they appear. We claim that any Dirichlet progression contains an infinite string of consecutive composite numbers. Let us state this claim precisely in the following theorem.

**Theorem 5.3.** For any \( a, b, k \in \mathbb{N} \) with \( \gcd (a, b) = 1 \), the arithmetic progression

\[
  a, a + b, a + 2b, a + 3b, \ldots
\]

contains \( k \) consecutive composite numbers.

**Proof.** Let \( a, b, k \) be chosen as in the hypothesis. Then let \( n = (a + b) \cdot (a + 2b) \cdot \cdots (a + kb) \). Consider the \( k \) consecutive terms

\[
a + (n + 1)b, a + (n + 2)b, \ldots, a + (n + k)b
\]

in the arithmetic progression. Note that, for each \( j \) with \( 1 \leq j \leq k \), we have

\[
  (x) \quad a + (n + j)b = a + bn + jb = bn + (a + jb).
\]

Further,

\[
bn = b \cdot (a + b) \cdot (a + 2b) \cdots (a + jb) \cdots (a + kb).
\]

Thus, \( (a + jb) \mid bn \). But, as \( (a + jb) \mid (a + jb) \), it follows that \( a + jb \) divides the sum \( bn + (a + jb) \), which, by (x), is \( a + (n + j)b \). Consequently, \( a + (n + j)b \) is composite for each \( 1 \leq j \leq k \), showing the result.
Now that we have studied Dirichlet arithmetic progressions and composite numbers, let us come back to primes of special forms. Since Dirichlet’s theorem is too difficult to prove here, we will study the case in which \( a = 1 \). We will prove not only the corresponding statement of Dirichlet’s theorem when \( a = 1 \), but discuss the size of the smallest prime in the arithmetic progression.

6 The Least Prime in Certain Arithmetic Progressions

In this section we will follow closely the work in [4]. As we did in Theorem 5.2, let us consider the Dirichlet progression when \( a = 1 \). We have

\[
1, 1 + n, 1 + 2n, 1 + 3n, \ldots
\]

We wish to study the primes contained in this progression. In terms of congruences, we will be studying primes that are congruent to 1 (mod \( n \)). In proving there are infinitely many primes of this form, we will use a different approach than we used in the five examples from Section 4. This new approach requires some additional background not yet introduced.

Firstly, we will define and introduce some examples of an important number-theoretic function called Euler’s phi function.

**Definition 6.1.** For \( n \geq 1 \), define \( \phi(n) \) as the number of positive integers not exceeding \( n \) that are relatively prime to \( n \).

**Example 6.2.** Let us find \( \phi(n) \) for \( 2 \leq n \leq 8 \).
\( \phi(2) = 1 \)
\( \phi(3) = 2 \) since 1 and 2 are relatively prime to 3
\( \phi(4) = 2 \) since 1 and 3 are relatively prime to 4
\( \phi(5) = 4 \) since 1, 2, 3 and 4 are relatively prime to 5
\( \phi(6) = 2 \) since 1 and 5 are relatively prime to 6
\( \phi(7) = 6 \) since 1, 2, 3, 4, 5 and 6 are relatively prime to 7
\( \phi(8) = 4 \) since 1, 3, 5 and 7 are relatively prime to 8

Notice that for any prime \( p \), every positive integer less than \( p \) is relatively prime to \( p \). Then for any prime \( p \), \( \phi(p) = p - 1 \). There are some other useful methods for computing \( \phi(n) \) when \( n \) is prime or a power of a prime. The next two theorems will state these methods, followed by a way to compute \( \phi(n) \) for any integer \( n \). For proofs of the following theorems, please see [1].

**Theorem 6.3.** If \( p \) is a prime and \( k \geq 1 \), then
\[
\phi(p^k) = p^k - p^{k-1}
\]

**Theorem 6.4.** The function \( \phi \) is a multiplicative function. Equivalently, for positive integers \( m \) and \( n \) with \( \gcd(m, n) = 1 \), \( \phi(mn) = \phi(m)\phi(n) \).

**Corollary 6.5.** If \( n > 1 \) has a prime factorization such that \( n = p_1^{k_1}p_2^{k_2} \ldots p_r^{k_r} \), then
\[
\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \ldots (p_r^{k_r} - p_r^{k_r-1})
\]

Let us take a look at some examples:

**Examples 6.6.** We have
\[
\begin{align*}
\phi(8) & = 2^3 - 2^2 = 4 \\
\phi(25) & = 5^2 - 5^1 = 20 \\
\phi(36) & = \phi(3^2)\phi(2^2) = (9 - 3)(4 - 2) = 12 \\
\phi(45) & = \phi(3^2)\phi(5) = (6)(4) = 24
\end{align*}
\]
Euler’s phi function has some important applications to congruencies. The following two theorems and definition have to do with special congruencies; in particular, when exponentiated integers are congruent to 1 (mod \( n \)). We will call upon these theorems in our work with [4]. Please refer to [1] for proofs of the following two theorems.

**Theorem 6.7. Euler’s Theorem.** If \( n \geq 1 \) and \( \gcd(a, n) = 1 \), then \( a^{\phi(n)} \equiv 1 \pmod{n} \).

Observe that for \( a = 2 \) and \( n = 7 \), we have \( \phi(7) = 6 \). Hence, \( 2^6 \equiv 8^2 \equiv 1^2 \equiv 1 \pmod{7} \). However, one might notice that 6 is not the smallest power for which \( 2^r \equiv 1 \pmod{7} \). By our first string of congruencies, \( 1 \equiv 8 \equiv 2^3 \pmod{7} \). Thus 3 is the smallest integer \( k \) for which \( 2^k \equiv 1 \pmod{7} \). We focus on the smallest power of \( a \) that is congruent to 1 (mod \( n \)) in the following definition.

**Definition 6.8.** Let \( n > 1 \) and \( \gcd(a, n) = 1 \). The order of \( a \) modulo \( n \) is the smallest positive integer \( k \) such that \( a^k \equiv 1 \pmod{n} \).

**Theorem 6.9.** Let the integer \( a \) have order \( k \) modulo \( n \). Then \( a^h \equiv 1 \pmod{n} \) if and only if \( k|\phi(n) \); and further; \( k|\phi(n) \).

Next, in anticipation of defining cyclotomic polynomials, we must have a basic understanding of complex numbers. Recall that a complex number \( z = (x, y) \) is an ordered pair of real numbers, where \( x = \text{Real component of } z \), denoted \( x = \text{Re}(z) \), and \( y = \text{Imaginary component of } z \), denoted \( y = \text{Im}(z) \). The ordered pair notation comes from a geometrical representation of \( z \), where the real numbers correspond to points on the \( x \)-axis and the imaginary numbers correspond to points on the \( y \)-axis. The algebraic representation is \( z = x + yi \) where \( i = \sqrt{-1} \).

Most arithmetic operations that apply to the real numbers also apply to the complex numbers. For a more detailed listing of the specific properties of
complex numbers, please see [2]. We will state some useful background and basic properties of complex numbers.

**Definition 6.10.** Two complex numbers \( z_1 \) and \( z_2 \) are collinear if \( z_1 = k z_2 \) for some non-zero real scalar \( k \).

Geometrically, in the complex plane the collinear vectors from the origin to the corresponding ordered pairs of \( z_1 \) and \( z_2 \) have the same slope.

**Definition 6.11.** We define the *modulus* of a complex number \( z = (x, y) \), written \( |z| \), as

\[
|z| = \sqrt{x^2 + y^2}
\]

Geometrically, \( |z| \) is the distance from the origin to the point \( (x, y) \).

The following proposition states two important properties of complex numbers that we will use in an upcoming proof.

**Proposition 6.12.** For \( z_1, z_2 \in \mathbb{C} \), we have

(1) \( |z_1 z_2| = |z_1||z_2| \).

(2) \( |z_1 - z_2| \geq ||z_1| - |z_2|| \). Further, this inequality is strict unless \( z_1 \) and \( z_2 \) are collinear.

Before we define cyclotomic polynomials, we need to introduce some terminology and definitions that will arise. Recall that if a polynomial has \( n \) as the highest exponent of all variables with non-zero coefficients, then we say this polynomial is of *degree* \( n \). We call a polynomial *monic* if the leading coefficient (the term with degree \( n \)) is 1. A polynomial is said to be irreducible if its non-zero coefficients are all relatively prime.

**Definition 6.13.** The \( n^{th} \) roots of unity are all of the complex numbers \( z \), such that \( z^n = 1 \), or equivalently, \( z^n - 1 = 0 \).
To make our discussion of roots of unity much simpler, we will introduce some basics about the polar coordinate system. Recall that a polar coordinate has two dimensions: \((r, \theta)\), where \(r\) is the radius (the distance from the origin) and \(0 \leq \theta < 2\pi\) is the angle from the horizontal axis going in the counter clockwise direction. One can imagine a polar coordinate system superimposed onto the complex coordinate system. Using this idea, we can convert complex coordinates into polar coordinates.

Notice that the radius of a polar coordinate is equal to the distance between the origin and the corresponding complex coordinate pair. Thus, for some \(z = (x, y)\), \(|z| = |re^{i\theta}| = |r||e^{i\theta}|\). We will need a better understanding of \(e^{i\theta}\) to compute \(|r||e^{i\theta}|\).

To find \(\theta\) for some complex coordinate pair, we can set up a right triangle between Re\((z)\), Im\((z)\) and the modulus of \(z\). Using trigonometry, when \(|z| = 1\) it follows that, the Im\((z) = \sin \theta\), and Re\((z) = \cos \theta\). Therefore \(z = \cos \theta + i\sin \theta\). By Euler’s famous formula (see below), we have \(\cos \theta + i\sin \theta = e^{i\theta}\). This powerful formula allows us to represent complex numbers easily in polar form.

Here is the statement of Euler’s formula:

**Theorem 6.14. Euler’s Formula.** Let \(z = x + yi\) be a complex number and let \(0 \leq \theta < 2\pi\). Then \(z = re^{i\theta}\) where \(\cos \theta = x\), \(\sin \theta = y\) and \(r = |z|\).

Now we may finish our computation of \(|e^{i\theta}|\):

\[
|z| = |re^{i\theta}| = |r||e^{i\theta}| = |r| \cdot 1 \text{ since } |e^{i\theta}| = \sqrt{\cos^2 \theta + \sin^2 \theta} = 1.
\]

Thus, \(|z| = |r|\). Note that \(r\) is always positive.

For \(n^{th}\) roots of unity, by Proposition 6.12 (1), we have \(|z^n| = |z|^n = 1\). Notice that \(|z|\) is a real number. Therefore, \(|z| = 1\) for all roots of unity.

**Example 6.15.** Consider the complex number \(z = \frac{-1}{2} + \frac{i\sqrt{3}}{2}\). Let us compute
the modulus:

$$|z| = \sqrt{\left(\frac{-1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2} = \sqrt{\frac{1}{4} + \frac{3}{4}} = 1$$

As is, $z$ looks somewhat intimidating. However, we convert $z$ into polar form by using $\cos \theta = \text{Re}(z) = -\frac{1}{2}$. Thus $\theta = 2\pi/3$, and so the polar form is $re^{i\theta} = e^{2\pi i/3}$.

**Theorem 6.16. Fundamental Theorem of Algebra.** Every non-constant single-variable polynomial with complex coefficients has at least one complex root. Consequently, every non-zero single-variable polynomial with complex coefficients has exactly as many complex roots as its degree, as long as all multiplicities of roots are counted.

Note that monic polynomials factor over the complex numbers as

$$(z - r_1)(z - r_2)\cdots(z - r_n)$$

where each $r_i$ is a root of the monic polynomial. Theorem 6.16 allows us to easily factor polynomials whose roots are the $n^{th}$ roots of unity. The theorem also allows us to conclude that $X^n - 1 = 0$ has precisely $n$ roots over the complex numbers.

Remember that $z$ is an $n^{th}$ root of unity if $z^n = 1$. Converting $z$ into polar form yields $z^n = (e^{i\theta})^n = e^{i\theta n} = 1$. We must find values of $\theta$ for which $e^{i\theta n} = 1$. Using Euler’s formula again, we must find $\theta$ values for which $e^{i\theta n} = \cos n\theta + i\sin n\theta = 1$. Since there is no imaginary component to the number 1, we know $\sin n\theta = 0$. Therefore $n$ must satisfy $\cos n\theta = 1$. These two previous equations are satisfied only when $n\theta$ is any multiple of $2\pi$. However, due to the periodicity of sine and cosine, we need to ensure that $a/n \leq 1$ so that $2\pi a/n$ does not exceed $2\pi$. Thus we have determined that the $n^{th}$ roots of unity are
precisely equal the values $e^{2\pi ia/n}$ for integers $0 \leq a \leq n - 1$. Notice that when $a = 0$, $e^{2\pi ia/n} = e^0 = 1$. Therefore 1 is always an $n^{th}$ root of unity.

Now let us see some examples for fixed values of $n$.

**Example 6.17.** The $n^{th}$ roots of unity for $1 \leq n \leq 5$:

1. $z^1 - 1 = (z - e^0) = (z - 1) = 0$
2. $z^2 - 1 = (z - e^0)(z - e^{2\pi i}) = (z - 1)(z + 1) = 0$
3. $z^3 - 1 = (z - e^0)(z - e^{2\pi i/3})(z - e^{4\pi i/3}) = (z - 1)(z - e^{2\pi i/3})(z - e^{4\pi i/3})$
   \[= (z - 1)(z^2 + z + 1)\]
4. $z^4 - 1 = (z - e^0)(z - e^{2\pi i/4})(z - e^{4\pi i/4})(z - e^{6\pi i/4})$
   \[= (z - 1)(z - e^{2\pi i/4})(z + 1)(z + e^{2\pi i/4})\]
   \[= (z - 1)(z - i)(z + 1)(z + i)\]
5. $z^5 - 1 = (z - e^0)(z - e^{2\pi i/5})(z - e^{4\pi i/5})(z - e^{6\pi i/5})(z - e^{8\pi i/5})$
   \[= (z - 1)(z - e^{2\pi i/5})(z - e^{4\pi i/5})(z - e^{6\pi i/5})(z - e^{8\pi i/5})\]
   \[= (z - 1)(z^4 + z^3 + z^2 + z + 1)\]

**Definition 6.18.** An $n^{th}$ root of unity is **primitive** if $z^k \neq 1$ for $k = \{1, 2, 3, \ldots, n - 1\}$.

Notice that for $z^4 - 1 = 0$, $-1$ is a root. However, $-1$ is not a primitive $4^{th}$ root of unity since $(-1)^4 = (-1)^2 = 1$. We have $(-1)$ is primitive for $n = 2$ only. Earlier we noted that all of the $n^{th}$ roots of unity are of the form $e^{2\pi ia/n}$ for any integer $a$. We will show that these roots are primitive unless gcd $(a, n) > 1$.

**Proposition 6.19.** Let $e^{2\pi ia/n}$ be an arbitrary $n^{th}$ root of unity. Then $e^{2\pi ia/n}$ is primitive if and only if gcd $(a, n) = 1$.

**Proof.** ⇒ Assume $e^{2\pi ia/n}$ is a primitive $n^{th}$ root of unity. By definition, $(e^{2\pi ia/n})^n = 1$ and $(e^{2\pi ia/n})^m \neq 1$ for all integers $m < n$. Assume for contradiction that
\[ \gcd(a, n) = g \geq 2 \] for some integer \( g \). Then \( a = gx \) and \( n = gy \) for some \( x, y \in \mathbb{N} \). Recall that \( e^{2\pi i (a/n)} = 1 \) if and only if \( (a/n) \) is an integer. But \( (a/n) = (gx/gy) = (x/y) \). Thus \( (x/y) \) is an integer equal to the integer \( (a/n) \). Since \( (x/y) \) is an integer, \( e^{2\pi i (x/y)} = 1 \). Clearly \( (x/y) < (a/n) \). This contradicts that \( e^{2\pi ia/n} \) is primitive, therefore \( \gcd(a, n) = 1 \) must hold.

\[ \iff \] Assume \( \gcd(a, n) = 1 \) and let \( e^{2\pi ia/n} \) be an arbitrary \( n^{th} \) root of unity. By Theorem 2.10, since \( \gcd(a, n) = 1 \) i.e., \( n \nmid a \), it follows that \( n \nmid am \) for any \( m < n \). Hence, \( (am/n) \) is not an integer. Thus, we have \( (e^{2\pi ia/n})^m = (e^{2\pi i(am/n)}) \neq 1 \) for all \( m < n \). But \( (e^{2\pi ia/n})^n = 1 \); and so, by definition, \( e^{2\pi ia/n} \) is a primitive \( n^{th} \) root of unity.

Using Theorem 6.16, let us take a deeper look at the polynomial \( x^n - 1 \). This polynomial has exactly \( n \) roots over the complex numbers and we have determined that all roots are of the form \( e^{2\pi ia/n} \), where \( 0 \leq a \leq n - 1 \). Then we can factor the polynomial as follows:

\[
x^n - 1 = (x - 1)(x - e^{2\pi ia_1/n})(x - e^{2\pi ia_2/n}) \cdots (x - e^{2\pi ia_{n-1}/n}) = \prod_{a=0}^{n-1} (x - e^{2\pi ia/n}).
\]

Notice that this product includes both the primitive roots of \( n \) and the non-primitive roots of \( n \). Using Proposition 6.19 to classify roots, we can separate the overall product into the product of primitive roots, i.e., \( \gcd(a, n) = 1 \), and non-primitive roots, i.e., \( \gcd(a, n) > 1 \). We have,

\[
x^n - 1 = \prod_{\substack{a=0 \atop \gcd(a, n)=1}}^{n-1} (x - e^{2\pi ia/n}) \cdot \prod_{\substack{a=0 \atop \gcd(a, n)>1}}^{n-1} (x - e^{2\pi ia/n}).
\]

The primitive roots are of great importance. We give the polynomial that includes only the product of primitive roots a special name in the following definition.
Definition 6.20. Let \( \Phi_n(x) \) denote the \( n \)th cyclotomic polynomial. We have

\[
\Phi_n(x) = \prod_{\substack{a=0 \\ \gcd(a,n)=1}}^{n-1} (x - e^{2\pi ia/n})
\]

is the polynomial of degree \( \phi(n) \) whose roots are the \( n \)th primitive roots of unity.

Notice that we claim \( \Phi_n(x) \) is of degree \( \phi(n) \). This is evident because the product is taken over all \( a < n \) such that \( a \) is relatively prime to \( n \). Thus the number of terms included in the product is equal to the number of integers less than \( n \) and relatively prime to \( n \). By definition, this number is \( \phi(n) \). Then \( \phi(n) \) is the highest exponent of any variable term in \( \Phi_n(x) \) with non-zero coefficients.

For more on cyclotomic polynomials, see [3].

In addition to this, there are some other important attributes of \( \Phi_n(x) \) and its binomial expansion. We collect these attributes in the following proposition.

Proposition 6.21. The polynomial \( \Phi_n(x) \) is monic, irreducible and has all integer coefficients.

Here are some examples of cyclotomic polynomials:

Example 6.22. Note that cyclotomic polynomials are the factors of \( x^n - 1 \) that contain primitive roots. We have,

(a) \( \Phi_2(z) = z + 1 \)

(b) \( \Phi_3(z) = (z - e^{2\pi i/3})(z - e^{4\pi i/3}) = z^2 + z + 1 \)

(c) \( \Phi_4(z) = (z - e^{2\pi i/4})(z - e^{6\pi i/4}) = z^2 + 1 \)

(d) \( \Phi_5(z) = (z - e^{2\pi i/5})(z - e^{4\pi i/5})(z - e^{6\pi i/5})(z - e^{8\pi i/5}) = z^4 + z^3 + z^2 + z + 1 \)

Earlier, after we stated Theorem 6.16, we noted that monic polynomials factor over the complex numbers as \((z-r_1)(z-r_2)\cdots(z-r_n)\). Notice that \( \Phi_n(x) \)
expressed as the product of its factors is of the same form: 
\((x - e^{2\pi i a_1/n})(x - e^{2\pi i a_2/n}) \cdots (x - e^{2\pi i a_{n-1}/n})\), where \(\gcd(a_i, n) = 1\). Hence, \(\Phi_n(x)\) is monic. We will accept the statements, \(\Phi_n(x)\) is irreducible and has integer coefficients, without proof.

With this background on cyclotomic polynomials, we will now state and prove a theorem from [4]. This theorem is the culmination of our study of prime numbers within this thesis paper. First, we will state a two-part lemma, followed by the statement of the theorem. We will then prove the theorem for the case \(n = 2\), followed by the case \(n \geq 3\). Following the proof of the theorem, we will prove the statements of the lemma.

**Lemma 6.23.** For the cyclotomic polynomial \(\Phi_n(b)\) with \(b \in \mathbb{N}\),

1. Let the prime factorization of \(\Phi_n(b) = q_1q_2 \cdots q_r\). For every \(q_i\), either \(q_i | n\) or \(q_i \equiv 1 \pmod{n}\).

2. If \(n > 2\), the \(q_i^2 \nmid n\).

**Theorem 6.24.** There are infinitely many primes congruent to 1 \(\pmod{n}\). The least such prime lies below \((3^n - 1)/2\).

\(\square\)

Proof when \(n = 2\). Primes congruent to 1 \(\pmod{2}\) are of the form \(2k + 1\). Since 2 is the only even prime, all other primes are of the form \(2k + 1\). Thus, by Theorem 3.3, there are infinitely many primes congruent to 1 \(\pmod{2}\). Notice that \((3^2 - 1)/2 = 4\). The least prime of the form \(2k + 1\) is 3, and 3 < 4. Therefore, Theorem 6.24 holds for \(n = 2\).

\(\square\)

Proof when \(n \geq 3\). This will require some understanding about the relative size of cyclotomic polynomials through the use of certain inequalities. We will
prove the following string of inequalities which will aid us later:

\((*) \quad |\Phi_n(3)| = \prod_{\substack{a=0 \atop \gcd(a,n)=1}}^{n-1} |(3 - e^{2\pi ia/n})| > 2^\phi(n) \geq 2\sum_{q|n} q^{-1} \geq \prod q\)

Note that \(\Phi_n(3)\) is an integer whose modulus is

\[ |\Phi_n(3)| = \prod_{\substack{a=0 \atop \gcd(a,n)=1}}^{n-1} (3 - e^{2\pi ia/n}) = \prod_{\substack{a=0 \atop \gcd(a,n)=1}}^{n-1} |(3 - e^{2\pi ia/n})| \]

with the last equality following by Proposition 6.12 (1). By Proposition 6.12 (2),

\[ |(3 - e^{2\pi ia_j/n})| \geq |3| - |e^{2\pi ia_j/n}| = |3 - 1| = 2. \]

However, the only cases in which \(|3| - |e^{2\pi ia_j/n}| = 2\) are when 1 or -1 are primitive roots. But this is impossible for \(n \geq 3\), since \(\gcd(0, n) \neq 1\), i.e., 1 is never a primitive root, and -1 is primitive for \(n = 2\) only. Therefore, when \(n \geq 3\), roots that are collinear with 3 are not primitive \(n^{th}\) roots of unity. Therefore, \(|(3 - e^{2\pi ia_j/n})| > 2\). Also, the product \(|\Phi_n(3)|\) contains exactly \(\phi(n)\) terms by definition. From this and the lower bound 2, it follows that

\[ \prod_{\substack{a=0 \atop \gcd(a,n)=1}}^{n-1} |(3 - e^{2\pi ia/n})| > 2^\phi(n). \]

Now, continuing the inequalities from \((*)\), we will now show that \(2^\phi(n) \geq \prod q\), i.e., the product over the distinct primes dividing \(n\). We first note that for some integer \(k > 0\) and prime \(q\),

\[ \phi(q^k) = q^k - q^{k-1} = q^{k-1}(q - 1) \geq q - 1. \]

We know that \(n\) has a prime factorization \(n = q_1^{k_1} q_2^{k_2} \cdots q_r^{k_r}\). Therefore

\[ (***) \quad \phi(n) = \phi(q_1^{k_1}) \cdot \phi(q_2^{k_2}) \cdots \phi(q_r^{k_r}) \geq \prod_{q|n} q - 1. \]
Next, we show that $ab \geq a + b$ for two integers $a \geq b \geq 2$. We have

\[
\begin{align*}
    a & \geq b \\
    a(b - 1) & \geq b, \text{ since } b - 1 \geq 1 \\
    ab - a & \geq b \\
    ab & \geq a + b.
\end{align*}
\]

The general result for any number of integers follows easily by induction.

We apply the result to the product of the terms in (**) and obtain the following inequality,

\[
\phi(n) \geq \prod_{q | n} q - 1 \geq \sum_{q | n} q - 1.
\]

Hence, $2^{\phi(n)} \geq 2\sum_{q | n} q^{-1}$.

**Note:** We recognize that $q - 1$ might equal 1, i.e., $q$ might equal 2. In this case, the above argument might not be valid. However, separate arguments show that the ultimate inequality in which we are interested, namely (**), still hold.

To show $2\sum_{q | n} q^{-1} \geq \prod_{q | n} q$, i.e., the final equality in (**), we will prove that $2^{q^{-1}} \geq q$ by induction. Note that for $q = 2$, $2^{(2^{-1})} = 2 \geq 2$. Now we assume that $2^{k^{-1}} \geq k$ holds for an arbitrary prime $k$. We must show that $2^{k} \geq k + 1$. Notice that $2k = k + k \geq k + 1$. Also, from our induction hypothesis, $2^{(2^{-1})} = 2^{k} \geq 2(k)$. From the previous two inequalities, it follows that $2^{k} \geq 2k \geq k + 1$, as desired. Hence,

\[
2\sum_{q | n} q^{-1} = 2^{q_{1}^{-1}} \cdot 2^{q_{2}^{-1}} \cdots 2^{q_{r}^{-1}} \geq q_{1}q_{2} \cdots q_{r} = \prod_{q | n} q.
\]

Therefore, by this final equality,

\[
(*) \quad |\Phi_{n}(3)| > \prod_{q | n} q.
\]

35
Now we will use the ultimate inequality to prove Theorem 6.24 for \( n \geq 3 \).

By Lemma 6.23 (2), since \( n > 2 \), for any prime divisor \( p \) of \( \Phi_n(3) \), \( p^2 \nmid n \). But, by \((*)\), it follows that \( \Phi_n(3) \) has some prime factor that does not divide \( n \).

By Lemma 6.23 (1) there exists some prime divisor \( p \) of \( \Phi_n(3) \) such that \( p \equiv 1 \pmod{n} \). Notice that \((3−1)\) is not included in the product defining \( \Phi_n(3) \) since \( 1 \) is not a primitive root. Then, \( \Phi_n(3) \mid \frac{3^n - 1}{3 - 1} \). Since \( p \mid \Phi_n(3) \), it follows that \( p \mid \frac{3^n - 1}{2} \). Therefore, there exists some prime congruent to 1 (mod \( n \)) below \((3^n - 1)/2 \). This proves the latter half of Theorem 6.24.

Note that for \( x > 3 \), the argument, \( |\Phi_n(x)| > \prod_{q \mid n} q \), still holds. Let us denote this generalized version by \((*)\). We will now use \((*)\) to prove there are infinitely many primes congruent to 1 (mod \( n \)). As we did in our prime proofs throughout Section 4, suppose there are finitely many primes congruent to 1 (mod \( n \)), and call them \( p_1, p_2, \ldots, p_r \). Consider the cyclotomic polynomial \( \Phi_n(b) = \Phi_n(p_1 \ldots p_r) \) with its prime factorization equal to \( q_1 q_2 \ldots q_t \). By \((*)\), we have \( \Phi_n(b) = q_1 q_2 \ldots q_t > \prod_{q \mid n} q \). By this inequality and Lemma 6.23 (2), since \( q^2 \nmid n \), there exists at least one \( q_i \) in the prime factorization of \( \Phi_n(b) \) such that \( q_i \nmid n \). By Lemma 6.23 (1), \( q_i \equiv 1 \pmod{n} \). Thus \( q_i \) is equal to one of the \( p_i \) in \( p_1, \ldots, p_r \). Therefore, \( q_i \mid (p_1 \ldots p_r)^n \). We have \( q_i \mid \Phi_n(b) \) and \( \Phi_n(b) \mid (b)^n - 1 \). Hence, \( q_i \mid (p_1 \ldots p_r)^n - 1 \). By Theorem 2.3, since \( q_i \mid (p_1 \ldots p_r)^n \) and \( q_i \mid (p_1 \ldots p_r)^n - 1 \), it follows that \( q_i \mid 1 \), which is impossible. Thus there are infinitely many primes congruent to 1 (mod \( n \)).

So, for the special \( a = 1 \) case of Dirichlet’s theorem, we have provided an elementary proof. In terminology from Section 4, we have proved that there exist infinitely many primes of the form \( nk + 1 \) for any \( n \geq 2 \).
Now we will prove the statements of Lemma 6.23.

**Proof of Lemma 6.23 (1).** Let \( p \) be a prime factor of \( \Phi_n(b) \). Thus \( p|\Phi_n(b) \), and so \( p|(b^n - 1) \). Hence, \( b^n \equiv 1 \pmod{p} \). By Theorem 6.9, the order of \( b \pmod{p} \) divides both \( n \) and \( \phi(p) \). Since \( p \) is prime, it follows that the order of \( b \pmod{p} \) divides \( \phi(p) = p - 1 \). If the order is exactly \( n \), then \( n|p - 1 \). Thus \( p \equiv 1 \pmod{n} \) as desired.

Now suppose the order is not exactly \( n \). Then there exists some \( q \) in the prime factorization of \( n \) such that \( n/q \) is a divisor of the order of \( b \pmod{p} \), i.e., \( p|b^{(n/q)} - 1 \). We claim that the \( \left( \frac{n}{q} \right)^{th} \) roots of unity

(a) are \( n^{th} \) roots of unity, but

(b) are not primitive \( n^{th} \) roots of unity.

First, we prove (a). Let \( a \) be an \( \left( \frac{n}{q} \right)^{th} \) root of unity, i.e., \( a^{\frac{n}{q}} = 1 \). Note that

\[
\begin{align*}
a^{\frac{n}{q}} &= 1 \\
(a^{\frac{n}{q}})^q &= (1)^q \\
a^n &= 1.
\end{align*}
\]

Therefore, \( a \) is an \( n^{th} \) root of unity.

Now we prove (b). Let \( a^{\frac{n}{q}} = 1 \). We just showed that \( a \) is also an \( n^{th} \) root of unity. By definition, since \( \frac{n}{q} < n \) and \( a^{\frac{n}{q}} = 1 \), \( a \) is not a primitive \( n^{th} \) root of unity.

Thus, we have shown that \((b^{\frac{n}{q}} - 1)\) is some factor of \( b^n - 1 \). We wish to show that \( \Phi_n(b) \) divides \( \frac{b^n - 1}{b^{\frac{n}{q}} - 1} \) in the integers. In general, we have \( x^n - 1 = (x^{\frac{n}{q}} - 1)(\Phi_n(x))(Q(x)) \) where \( Q(x) \) is the polynomial quotient:

\[
\frac{x^n - 1}{\Phi_n(x)}.
\]

Notice that \( Q(x) \) contains the \( n^{th} \) roots of unity that are not primitive \( n^{th} \) roots and are not \( \left( \frac{n}{q} \right)^{th} \) roots of unity. To show \( \Phi_n(x) \) divides \( \frac{x^n - 1}{x^{\frac{n}{q}} - 1} \), for which we
will then evaluate at \( b \), we must prove \( Q(x) \) has integer coefficients. To do this, we will state one definition and one lemma.

**Definition 6.25.** Let \( f = a_0 + a_1X + \cdots + a_nX \), \( a_i \in \mathbb{Z} \) be a non-zero polynomial. We say \( f \) is **primitive** if \( a_0, a_1, \ldots, a_n \) are relatively prime.

**Lemma 6.26.** Let \( f \) be a primitive polynomial in \( \mathbb{Z}[X] \) and let \( g \) be any polynomial in \( \mathbb{Z}[X] \). Suppose \( f \) divides \( g \) in \( \mathbb{Q}[X] \) such that \( g = fq \) with \( q \in \mathbb{Q}[X] \). Then \( q \in \mathbb{Z}[X] \), and hence \( f \) divides \( g \) in \( \mathbb{Z}[X] \).

Since \( \Phi_n(x) \) is irreducible with integer coefficients, it is primitive. Note that \( (x^n - 1)/(x^q - 1) \) is a polynomial in \( \mathbb{Z}[X] \). By Lemma 6.26, since \( \Phi_n(x) \) divides \( (x^n - 1)/(x^q - 1) \) in \( \mathbb{Q}[X] \), \( Q(x) \) is in \( \mathbb{Z}[X] \). Thus, by Lemma 6.26, \( Q(x) \) has integer coefficients. Then \( \Phi_n(b) \) divides \( (x^n - 1)/(x^n/q - 1) \) in \( \mathbb{Z}[X] \). Notice that \( (x^n - 1)/(x^n/q - 1) = 1 + x^n/q + x^{2n/q} + \ldots + x^{n(q-1)/q} \). Hence, \( \Phi_n(b) \) divides \( (b^n - 1)/(b^n/q - 1) = 1 + b^n/q + b^{2n/q} + \ldots + b^{n(q-1)/q} \). Notice that there are \( q \) terms in the final equality. By assumption, \( b^n/q \equiv 1 \pmod{p} \). We have,

\[
(b^n - 1)/(b^n/q - 1) = 1 + b^n/q + (b^n/q)^2 + \ldots + (b^n/q)^{q-1} \equiv q \pmod{p}
\]
since there are \( q \) terms congruent to 1 (mod \( p \)). We have \( p|\Phi_n(b) \) and \( \Phi_n(b)|(b^n - 1)/(b^n/q - 1) \). But \( q \) and \( p \) are both prime. The only conclusion is that \( (b^n - 1)/(b^n/q - 1) \equiv q \equiv 0 \pmod{p} \). Therefore \( q = p \) is a divisor of \( n \).

\[\square\]

**Proof of Lemma 6.23 (2).** Let \( q \) be a prime divisor of \( n \) > 2, and \( q|\Phi_n(b) \). We know that \( \Phi_n(b)|\frac{b^n - 1}{b^q - 1} \) and \( \frac{b^n - 1}{b^q - 1} = 1 + b^{(n/q)} + (b^{(n/q)})^2 + \ldots + (b^{(n/q)})^{q-1} \). Then, to prove \( q^2 \nmid \Phi_n(b) \), it is sufficient to show that

\[
q^2 \nmid 1 + b^{(n/q)} + (b^{(n/q)})^2 + \ldots + (b^{(n/q)})^{q-1}.
\]

We will study each individual term of this expansion. Since \( b^{n/q} \equiv 1 \pmod{q} \), it follows that \( b^{n/q} = 1 + cq \) for some integer \( c \). Using the binomial theorem, it
follows that for $2 \geq j \geq q - 1$

$$(x) \quad b^{nj/q} = (b^{n/q})^j = (1 + cq)^j = 1 + cjq + \cdots + c^j q^j.$$  

Notice that 1 and $cj q$ are the only terms in this sum that are not divisible by $q^2$. Therefore $b^{nj/q} \equiv 1 + cj q + 0 + \cdots + 0 \equiv 1 + cj q \pmod{q^2}$ by $(x)$. Then,

$$\frac{b^n - 1}{b^{nj/q} - 1} = 1 + b^{n/q} + b^{2n/q} + \cdots + b^{n(q-1)/q}$$

is congruent to $1 + (1 + cq) + (1 + 2cq) + \cdots + (1 + (q - 2)cq) + (1 + (q - 1)cq)$ (mod $q^2$). Observe that the number 1 is added $q$ times. Thus this sum has

$$\frac{b^n - 1}{b^{nj/q} - 1} \equiv q + cq + 2cq + \cdots + (q - 1)cq$$

$$\equiv q + cq(q) + \cdots + cq(q)$$

$$(xx) \quad \equiv q + cq \frac{q(q - 1)}{2} \pmod{q^2}.$$  

If $q$ is odd, then $(xx)$ is congruent to $q$ (mod $q^2$) since $cqq \frac{q(q - 1)}{2} = cqq \frac{q(q - 1)}{2}$, where $\frac{q - 1}{2}$ is an integer. It follows that $q^2 \nmid \frac{b^n - 1}{b^{nj/q} - 1}$, i.e.,

$$q^2 \nmid 1 + b^{n/q} + (b^{n/q})^2 + \cdots + (b^{n/q})^{q-1}.$$  

If $q = 2$, then $q^2 = 4$, and so $(xx)$ becomes congruent to $2(1 + c)$ (mod 4).

If $c$ is even, we let $2k = c$, then $2(1 + c) \equiv 2(1 + 2k) \equiv 2 + 4k \equiv 2 \neq 0$ (mod 4), and we are done. If $c$ is odd, we have $1 + b^{n/2} \equiv 2 + 2c$. We let $c = 2k + 1$ to see that $b^{n/2} \equiv 2c + 1 \equiv 4k + 3 \equiv 3$ (mod 4). Then $b$ is odd.

We claim that if $(n/2 = 2k)$ is even, then $b^{n/2} \equiv 3$ (mod 4). Note that any odd integer $b$ is either congruent to 1 or 3 (mod 4). However, if $b \equiv 1$ (mod 4), then $b^{n/2} \equiv 1$ (mod 4). Hence, $b \equiv 3$ (mod 4). We have $b^{2k} \equiv 3^{2k} \equiv (3^2)^k \equiv 1^k \equiv 3$ (mod 4). Therefore, $n/2$ is odd.

Next we show that $n/2$ cannot be odd. Earlier, we noted that $n/q$ roots of unity are not primitive $n^{th}$ roots of unity. Hence, $\Phi_n(b)\mid b^n - 1$. Also, since
If $n$ is even, $(b + 1)$ is an $n^{th}$ root of unity, but is not primitive since $n > 2$ is assumed. Therefore, $\Phi_n(b) \mid \frac{b^n - 1}{(b^{n/2} - 1)(b + 1)}$, where

$$
\frac{b^n - 1}{(b^{n/2} - 1)(b + 1)} = 1 + b^2 - b^3 + b^4 - b^5 + \cdots - b^{n/2 - 2} + b^{n/2 - 1} = \sum_{a=0}^{n/2 - 1} (-b)^a.
$$

Since $b$ is odd, every term in the sum is odd. Also, since $n/2$ is odd, the sum has an odd number of terms. Therefore $\sum_{a=0}^{n/2 - 1} (-b)^a$ is odd. But if this sum is odd, then $q \nmid \sum_{a=0}^{n/2 - 1} (-b)^a$ since $q = 2$. This contradicts that $\Phi_n(b) \mid \sum_{a=0}^{n/2 - 1} (-b)^a$. Therefore, this last case in which $c$ is odd cannot arise.

□

This concludes our proof of Lemma 6.23, and thus concludes our study of [4].

7 Conclusion

Now that we have a deeper understanding of special forms of prime numbers, let us take another look at the conjectures posed in Section 1. For a 12-tone musical system, we were able to prove in Section 4 that there are infinitely many prime intervals that correspond to $12S - 1$, for some starting pitch $S$. With Theorem 6.24, we may conclude that there are infinitely many prime intervals that correspond to $12S + 1$. It seems that for $12S + 5$ and $12S + 7$, we cannot find a more elementary method than to call upon Dirichlet's theorem. Using the method from Section 4 for $12S + 5$ and $12S + 7$ leads to difficulties constructing a proper $N$ or finding an appropriate lemma. However, with Theorem 6.24, we can go one big step further and conclude that in an $n$-tone system, the tones $nS + 1$ correspond to prime intervals infinitely many times, with the spectrum of audible sound permitting.
The connection between number theory and music theory is very strong. It was surprising that even abstract algebra played its part here too. As composers continue to ponder special intervals and rhythms and all things music, we will continue to stumble upon interesting and almost disturbing connections between math and music.

References


