Cyclotomic Polynomials

Brett Porter

May 15, 2015

Abstract

If n is a positive integer, then the n^{th} cyclotomic polynomial is defined as the unique monic polynomial having exactly the primitive n^{th} roots of unity as its zeros. In this paper we start off by examining some of the properties of cyclotomic polynomials; specifically focusing on their irreducibility and how they relate to primes. After that we explore some applications of these polynomials, including proofs of Wedderburn's Theorem, and when a regular n-gon is constructible with a straightedge and compass.

1 Introduction

Cyclotomic polynomials are an important type of polynomial that appears frequently throughout algebra. They are of particular importance because for any positive integer n, the irreducible factors of $x^n - 1$ over the rationals (and integers) are cyclotomic polynomials. Furthermore, the minimal polynomial of any n^{th} root of unity over the rationals is a cyclotomic polynomial. Records indicate that certain cyclotomic polynomials were studied as early as Euler, but perhaps their most famous use is due to Gauss. Cyclotomic polynomials appear in his *Disquisitiones Arithmeticae*, where they play a role in the proof of when a regular n-gon is constructible with a straightedge and compass (a result we will examine in more depth later).

We will start off by developing some concepts behind where the cyclotomic polynomials come from, taking a look at the n^{th} roots of unity, and then moving on to a formal definition of the n^{th} cyclotomic polynomial. From here we will explore the polynomials themselves; first looking at general properties such as their degree and how they relate to each other. The next section will be dedicated to proving that the cyclotomic polynomials are irreducible over the integers. After that we will explore how cyclotomic polynomials relate to prime numbers; starting with a discussion of the Bunyakovsky Conjecture, and then examining results that may be useful in proving or disproving a special case of this. The rest of the paper will explore the applications of cyclotomic polynomials and how they can be used in various proofs. We will focus on two main results; Wedderburn's Theorem, and when a regular n-gon is constructible with a straightedge and compass. Except where explicitly noted, the notation and terminology throughout this paper mimics [5].

2 Preliminaries and Definitions

Before we can formally define a cyclotomic polynomial we must first introduce some concepts.

Definition 2.1 (n^{th} Root of Unity). *Let n be a positive integer. A complex number ω is an n^{th} root of unity if $\omega^n = 1$.*

It is a well known result that there are n distinct n^{th} roots of unity, which are given by

$$e^{\frac{2\pi i}{n}}, e^{\frac{2\pi i}{n}2}, \dots, e^{\frac{2\pi i}{n}n} = \{e^{\frac{2\pi i}{n}k} : 1 \leq k \leq n\}.$$

Note that any complex number of the form $e^{\frac{2\pi i}{n}k}$, where $k \in \mathbb{Z}$, will be an n^{th} roots of unity. From here on out when we talk about an n^{th} root of unity, $e^{\frac{2\pi i}{n}k}$, we will assume that $1 \leq k \leq n$.

Theorem 2.2. *Suppose n is a positive integer, then the n^{th} roots of unity form a group under multiplication.*

Proof. Suppose $e^{\frac{2\pi i}{n}k}$ and $e^{\frac{2\pi i}{n}j}$ are any n^{th} root of unity. It can be shown from the division algorithm that there exist $q, r \in \mathbb{Z}$ such that $1 \leq r \leq n$, and $j + k = n \cdot q + r$. It follows that

$$e^{\frac{2\pi i}{n}j} e^{\frac{2\pi i}{n}k} = e^{\frac{2\pi i}{n}(n \cdot q + r)} = e^{2\pi i q} e^{\frac{2\pi i}{n}r} = e^{\frac{2\pi i}{n}r}.$$

Note that $e^{\frac{2\pi i}{n}r}$ is an n^{th} root of unity, and so the n^{th} roots of unity are closed under multiplication.

Because this multiplication is the same multiplication defined on $\mathbb{C}$, it is associative. Note that $1^n = 1$, so 1 is an n^{th} root of unity. If ω is any other n^{th} root of unity, then $1 \cdot \omega = \omega \cdot 1 = \omega$. Hence 1 is the identity for this set. Suppose $e^{\frac{2\pi i}{n}k}$ is any n^{th} root of unity, then $e^{\frac{2\pi i}{n}(n-k)}$ is an n^{th} root of unity. Note that $e^{\frac{2\pi i}{n}k} e^{\frac{2\pi i}{n}(n-k)} = e^{2\pi i} = 1$. Therefore every n^{th} root of unity has a multiplicative inverse that is also an n^{th} root of unity, and so the n^{th} roots of unity form a group under multiplication. □

The main reason why we are interested in the n^{th} roots of unity as a group is because of the following result; which allows us to derive properties of the n^{th} roots of unity by looking at a more familiar group. For our purposes, we will say that $\mathbb{Z}_n = \{1, 2, \dots, n\}$.

Lemma 2.3. *The function ψ from $\mathbb{Z}_n$ to the n^{th} roots of unity given by $\psi(k) = e^{\frac{2\pi i}{n}k}$ is a group isomorphism.*

Proof. Suppose $e^{\frac{2\pi i}{n}k}$ is an n^{th} root of unity; then $k \in \mathbb{Z}_n$, and $\psi(k) = e^{\frac{2\pi i}{n}k}$. Hence ψ is onto. Suppose $j, k \in \mathbb{Z}_n$ and $\psi(k) = \psi(j)$. In this case, $e^{\frac{2\pi i}{n}k} = e^{\frac{2\pi i}{n}j}$, which happens only if $j = k$. Therefore ψ is one-to-one.

Again suppose that $j, k \in \mathbb{Z}_n$. Say that $j + k \equiv r \pmod{n}$, then it follows that $j + k = n \cdot q + r$ for some $q \in \mathbb{Z}$. Hence,

$$\psi(j+k) = \psi(r) = e^{\frac{2\pi i}{n}r} = e^{\frac{2\pi i}{n}(n\cdot q+r)} = e^{\frac{2\pi i}{n}j}e^{\frac{2\pi i}{n}k} = \psi(j)\psi(k).$$

Thus ψ is operation preserving, and so it is an isomorphism. □

Definition 2.4 (Primitive n^{th} Root of Unity)**.** *A primitive n^{th} root of unity is an n^{th} root of unity whose order is n.*

It is worth noting that if ω is a primitive n^{th} root of unity; then $\langle\omega\rangle$ contains n distinct elements, and so ω is a generator of the group of n^{th} roots of unity.

Theorem 2.5. *If n is a positive integer, then the primitive n^{th} roots of unity are*

$$\{e^{\frac{2\pi i}{n}k} : 1 \leq k \leq n, \gcd(k,n) = 1\}.$$

Proof. By [5, Corollary 4 to Theorem 4.2], an element k of $\mathbb{Z}_n$ has order n if and only if $\gcd(n,k) = 1$. It follows from Lemma 2.3 that an n^{th} root of unity, $e^{\frac{2\pi i}{n}k}$, has order n if and only if $\gcd(n,k) = 1$. □

We have now developed enough background to give a formal definition, and derive a more convenient formula for, the n^{th} cyclotomic polynomial.

Definition 2.6 (n^{th} Cyclotomic Polynomial)**.** *For any positive integer n the n^{th} cyclotomic polynomial, $\Phi_n(x)$, is given by*

$$\Phi_n(x) = (x-\omega_1)(x-\omega_2)\ldots(x-\omega_s),$$

where ω_1, ω_2,…, ω_s are the primitive n^{th} roots of unity.

It follows from Theorem 2.5 that we can write the n^{th} cyclotomic polynomial as

$$\Phi_n(x) = \prod_{\substack{1\leq k\leq n \\ gcd(n,k)=1}} (x - e^{\frac{2i\pi k}{n}}). \tag{1}$$

Definition 2.7 (Möbius Function)**.** *Suppose n is a positive integer with prime factorization $\prod_{k=1}^{r} p_k^{f_k}$. The function $\mu : \mathbb{N} \to \mathbb{N}$ given by*

$$\mu(n) = \begin{cases} (-1)^r & \text{if } f_k = 1 \text{ for all } k, \\ 0 & \text{if } f_k > 1 \text{ for some } k. \end{cases}$$

is called the Möbius function.

It is worth noting that $\mu(n) = 0$ if and only if n is divisible by a perfect square. Hence, we will say that $\mu(n) = 0$ if n is not square free. It is also worth noting that μ is a multiplicative function.

The Möbius function is of concern to us because we can express the n^{th} cyclotomic polynomials as

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}. \tag{2}$$

A proof of this can be found in [1].

3 General Properties

Now that we have a formal definition and two formulas for the cyclotomic polynomials, we will explore some of their simpler properties. Notice that some results are easier to prove with Equation (1), while other are easier to prove with Equation (2); demonstrating the usefulness of both formulas.

Theorem 3.1. *If n is a positive integer, then $\Phi_n(x)$ is monic and its degree is $\phi(n)$, where ϕ is the Euler phi function.*

Proof. Since $\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ gcd(n,k)=1}} (x - e^{\frac{2i\pi k}{n}})$, when written as a product of linear factors every x term in $\Phi_n(x)$ has a coefficient of 1. It follows that when these linear factors are multiplied out, the x term with the largest exponent will have a coefficient of 1. Furthermore, it is apparent from this formula that the degree of $\Phi_n(x)$ will be the number of integers, k, such that $1 \leq k \leq n$ and $\gcd(k, n) = 1$. By definition this is $\phi(n)$. □

These next few results give us ways to relate different cyclotomic polynomials.

Theorem 3.2. *Let n be a positive integer and $\prod_{k=1}^{r} p_k^{f_k}$ be the prime factorization of n. If $m = \prod_{k=1}^{r} p_k^{g_k}$ where for all k, $1 \leq g_k \leq f_k$, then $\Phi_n(x) = \Phi_m(x^{n/m})$.*

Proof. Suppose $d \mid n$ but $d \nmid m$, then d is not square free, and so $\mu(d) = 0$. This means that $(x^{n/d}-1)^{\mu(d)} = (x^{n/d}-1)^0 = 1$, and therefore,

$$\begin{aligned}
\Phi_n(x) &= \prod_{d|n}(x^d-1)^{\mu(n/d)} \\
&= \prod_{d|n}(x^{n/d}-1)^{\mu(d)} \\
&= \prod_{d|m}(x^{n/d}-1)^{\mu(d)} \\
&= \prod_{d|m}((x^{n/m})^{m/d}-1)^{\mu(d)} \\
&= \prod_{d|m}((x^{n/m})^{d}-1)^{\mu(m/d)} \\
&= \Phi_m(x^{(m/n)}).
\end{aligned}$$

□

Corollary 3.3. *Let p be a prime and m a positive integer. If p divides m, then $\Phi_{pm}(x) = \Phi_m(x^p)$.*

Proof. Let $\prod_{k=1}^{r} p_k^{f_k}$ be the prime factorization of m, and assume without a loss of generality that $p = p_1$. It follows that the prime factorization of pm will be $p_1^{f_1+1}\prod_{k=2}^{r} p_k^{f_k}$. Therefore, by Theorem 3.2,

$$\begin{aligned}
\Phi_{pm}(x) &= \Phi_m(x^{pm/m}) \\
&= \Phi_m(x^p).
\end{aligned}$$

□

Corollary 3.4. *If p is prime and k is a positive integer, then $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}})$.*

Proof. This follows immediately from Theorem 3.2. □

Theorem 3.5. *Let p be a prime and m be a positive integer. If p does not divide m, then $\Phi_{pm}(x)\Phi_m(x) = \Phi_m(x^p)$.*

Proof. Say that $d \mid pm$ and $p \nmid d$. Since p is prime; this means that $\gcd(d,p) = 1$. Hence, by Euclid's Lemma, $d \mid m$. Now suppose $d \mid m$; then since $p \nmid m$, $p \nmid d$. Also since $m \mid pm$, $d \mid pm$. It follows that $d \mid pm$ and $d \nmid p$ if and only if $d \mid m$.

Now since p is prime its only divisors are 1 and p. Since p is not a divisor of m, this means that $\gcd(p,m) = 1$. It follows that if d is a divisor of m, then $\gcd(\frac{m}{d},p) = 1$. Because μ is a multiplicative function, this means that $\mu(\frac{mp}{d}) = \mu(\frac{m}{d})\mu(p) = -\mu(\frac{m}{d})$.

Suppose that $p \mid d$ and $d \mid pm$. It follows that $\frac{d}{p} \mid m$, so $d = pn$ for some integer n where $n \mid m$. Now suppose that $n \mid m$, then $pn \mid pm$, and if we let $d = pn$ then $p \mid d$ and $d \mid pm$. Thus $d \mid pm$ and $p \mid d$ if and only if $n \mid m$ where $n = \frac{d}{p}$.

Using this we can now write

$$\begin{aligned}
\Phi_{pm}(x)\Phi_m(x) &= \prod_{d|pm} (x^d - 1)^{\mu(pm/d)} \Phi_m(x) \\
&= \prod_{\substack{d|pm \\ p|d}} (x^d - 1)^{\mu(pm/d)} \prod_{\substack{d|pm \\ p\nmid d}} (x^d - 1)^{\mu(pm/d)} \Phi_m(x) \\
&= \prod_{n|m} (x^{pn} - 1)^{\mu(pm/pn)} \prod_{d|m} (x^d - 1)^{\mu(pm/d)} \Phi_m(x) \\
&= \Phi_m(x^p) \prod_{d|m} (x^d - 1)^{-\mu(m/d)} \Phi_m(x) \\
&= \Phi_m(x^p)(\Phi_m(x))^{-1}\Phi_m(x) \\
&= \Phi_m(x^p).
\end{aligned}$$

□

Lemma 3.6. *If n is odd, then ω is a primitive n^{th} root of unity if and only if $(-\omega)$ is a primitive $2n^{th}$ root of unity.*

Proof. Suppose n is odd and that ω is a primitive n^{th} root of unity. Let G be the group of $2n^{\text{th}}$ roots of unity, and note that set of n^{th} roots of unity will be a subgroup of G. Also note that because n is odd, -1 is not an n^{th} root of unity. Now ω is an n^{th} root of unity, and thus since ω has order n, $\langle\omega\rangle$ will be the set of n^{th} roots of unity. This means that $(-1) \notin \langle\omega\rangle$, but because $2n$ is even, $(-1) \in G$. Since G is closed, $(-\omega) \in G$, and so $(-\omega)$ has order k, where by [5, Corollar 2 to Theorem 7.1], $k \mid 2n$. We now have that $1 = (-\omega)^k = (-1)^k\omega^k$, which means that $(-1)^k = \omega^k$. Because $(-1) \notin \langle\omega\rangle$, k cannot be odd. This means that $k = 2j$ for some $j \in \mathbb{Z}$. Now $(-1)^{2j}\omega^{2j} = (-\omega)^{2j} = 1$, so $\omega^{2j} = (-1)^{2j} = 1$. Hence, $\omega^j = \pm 1$, but we know $\omega^j \neq -1$, so $\omega^j = 1$. Thus by [5, Theorem 4.1], $n \mid j$, and since $2j = k \mid 2n$, $j \mid n$. This means that $j = n$, and so $(-\omega)$ has order $k = 2n$; meaning that $(-\omega)$ is a primitive $2n^{\text{th}}$ root of unity.

Now suppose ω is a primitive $2n^{th}$ root of unity, so $\omega^{2n} = 1$ and for all $m < 2n$, $\omega^m \neq 1$. Because $\omega^{2n} = 1$, $\omega^n = \pm 1$. If $\omega^n = 1$ then this contradicts that ω is a primitive $2n^{\text{th}}$ root of unity. Thus $\omega^n = -1$. It follows that $(-\omega)^n = (-1)^n\omega^n = 1$, and so $(-\omega)$ is an n^{th} root of unity. Now suppose there exists an $m < n$ such that $(-\omega)^m = 1$. It follows that $2m < n$, and $\omega^{2m} = (-1)^{2m}\omega^{2m} = 1$, which contradicts that ω is a primitive root of order $2m$. Hence there does not exist an integer $m < n$ such that $(-\omega)^m = 1$, and so $(-\omega)$ is a primitive n^{th} root of unity. □

Lemma 3.7. *If* $\prod_{k=1}^{r} p_k^{f_k}$ *is the prime factorization of* n*, then*

$$\phi(n) = \prod_{k=1}^{r} p_k^{f_k - 1}(p_k - 1).$$

Proof. See [4, Theorem 5.22]. □

Theorem 3.8. *If* n *is an odd integer greater than 1, then* $\Phi_{2n}(x) = \Phi_n(-x)$*.*

Proof. Let n be odd and ω_1, ω_2,..., ω_s be the primitive n^{th} roots of unity. By Lemma 3.6, $-\omega_1$, $-\omega_2$,..., $-\omega_s$ are the primitive $2n^{\text{th}}$ roots of unity. Hence, by definition, $\Phi_n(x) = \prod_{k=1}^{s}(x - \omega_k)$ and $\Phi_{2n}(x) = \prod_{k=1}^{s}(x + \omega_k)$.

Note that the degree of $\Phi_n(x)$ will be s, and so by Theorem 3.1, $s = \phi(n)$. Because n is odd, there will be an odd prime, p, such that $p \mid n$. Therefore $p - 1$ will be even. By Lemma 3.7 $(p-1) \mid \phi(n)$, so $\phi(n)$, and hence s, will be even.

It follows that

$$\begin{aligned}
\Phi_n(-x) &= \prod_{k=1}^{s}(-x - \omega_k) \\
&= \prod_{k=1}^{s}(-1)(x + \omega_k) \\
&= (-1)^s \prod_{k=1}^{s}(x + \omega_k) \\
&= \prod_{k=1}^{s}(x + \omega_k) \\
&= \Phi_{2n}(x).
\end{aligned}$$

□

While the next two results are interesting in their own right, they are of particular importance because of their use in the proofs of later theorems.

Theorem 3.9. *Let* n *be a positive integer, then*

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

Proof. Suppose that ω is a root of $\Phi_d(x)$, where $d \mid n$. It follows that ω is a d^{th} root of unity. Let q be the integer such that $n = d \cdot q$; then

$$\omega^n = (\omega^d)^q = 1^q = 1.$$

It follows that ω is a root of $x^n - 1$.

Now suppose that ω is a root of $x^n - 1$. It follows that ω is an n^{th} root of unity. Say that the order of ω is d, and note that ω will be a primitive d^{th} root of unity. Therefore, ω is a root of $\Phi_d(x)$. Since the n^{th} root of unity form a group of n elements, by [5, Corollary 2 to Theorem 7.1], $d \mid n$, and so ω is a root of $\Phi_d(x)$ for some d that divides n.

We have now shown that $x^n - 1$ and $\prod_{d|n} \Phi_d(x)$ share all their roots. Note that $\prod_{d|n} \Phi_d(x)$ is a product of a collection of monic polynomials, and so it will be monic. Hence, $x^n - 1$ and $\prod_{d|n} \Phi_d(x)$ are both monic; which means that they must be equal. □

Theorem 3.10. *Let n be a positive integer, then the coefficients of $\Phi_n(x)$ are integers, i.e. $\Phi_n(x) \in \mathbb{Z}[x]$.*

Proof. See [1, Corollary 3]. □

4 Irreducibility of the Cyclotomic Polynomials Over the Integers

We will now show that for all positive integers n, $\Phi_n(x)$ is irreducible over $\mathbb{Z}$. Before we can prove this though we need a few results.

4.1 Lemmas and Interesting Results

Theorem 4.1. *A polynomial $f(x)$ over a field F has a multiple zero in some extension field of F if and only if $f(x)$ and its derivative, $f'(x)$, have a common factor of positive degree in $F[x]$.*

Proof. See [5, Theorem 20.5]. □

Lemma 4.2. *Let $g(x)$ and $h(x)$ belong to $\mathbb{Z}[x]$, and let $h(x)$ be monic. If $h(x)$ divides $g(x)$ in $\mathbb{Q}[x]$, then $h(x)$ divides $g(x)$ in $\mathbb{Z}[x]$.*

Proof. We will prove this by induction on the degree of $g(x)$. Let $\deg g(x) = m$ and $\deg h(x) = n$, and say that a is the leading coefficient of $g(x)$. Assume that $m = n$, then $g(x) = a \cdot h(x)$, and since a is an integer, this means that $h(x)$ divides $g(x)$ in $\mathbb{Z}[x]$.

Now assume that $m > n$ and for all q such that $n \le q < m$, if $l(x) \in \mathbb{Z}[x]$ is a polynomial of degree q that is divisible by $h(x)$ in $\mathbb{Q}[x]$, then $h(x)$ divides $l(x)$ in $\mathbb{Z}[x]$. Let $k(x) = g(x) - ax^{m-n}h(x)$ and note that $h(x)$ divides $k(x)$ in $\mathbb{Q}[x]$, $\deg k(x) < m$, and $k(x)$ has integer coefficients. If $k(x) = 0$, then $g(x) = ax^{m-n}h(x)$, so $h(x)$ divides $g(x)$ in $\mathbb{Z}[x]$. If $k(x) \neq 0$ then since $h(x)$ divides $k(x)$, $\deg k(x) \ge n$. It follows from the induction hypothesis that $h(x)$ divides $k(x)$ in $\mathbb{Z}[x]$, and thus $h(x)$ divides $k(x) + ax^{m-n}h(x) = g(x)$ in $\mathbb{Z}[x]$. □

Lemma 4.3. *If $g(x) \in \mathbb{Z}_p[x]$ where p is prime, then $(g(x))^p = g(x^p)$.*

Proof. Consider the function $\psi : \mathbb{Z}_p[x] \to \mathbb{Z}_p[x]$ given by $\psi(f(x)) = (f(x))^p$. Suppose $f(x), h(x) \in \mathbb{Z}_p[x]$. Note that $\psi(f(x)h(x)) = (f(x)h(x))^p = (f(x))^p(h(x))^p$. Now, by [4, Theorem 3.17], if p is prime and $0 < j < p$, then p divides $\binom{p}{j}$. Because $\mathbb{Z}_p[x]$ has characteristic p, it follows from the binomial theorem that

$$\begin{aligned} \psi(f(x)+h(x)) &= (f(x)+h(x))^p \\ &= \sum_{j=0}^{p} \binom{p}{j} (f(x))^p(h(x))^p \\ &= (f(x))^p + (g(x))^p + \sum_{j=1}^{p-1} \binom{p}{j} (f(x))^p(h(x))^p \\ &= \psi(f(x)) + \psi(h(x)) + \sum_{j=1}^{p-1} 0 \cdot (f(x))^p(h(x))^p \\ &= \psi(f(x)) + \psi(h(x)). \end{aligned}$$

Therefore ψ is operation preserving, and hence a homomorphism.

Suppose $a \in \mathbb{Z}_p[x]$ and a is a constant polynomial. If $a \neq 0$, then $\gcd(a,p) = 1$, and so by Fermat's Little Theorem, $a^p \equiv a \pmod{p}$. Also $0^p = 0$, and therefore if a is a constant polynomial in $\mathbb{Z}_p[x]$, then $\psi(a) = a^p = a$.

If $g(x) \in \mathbb{Z}_p[x]$, then we may write $g(x) = \sum_{j=0}^{n} a_j x^j$. It follows that

$$\begin{aligned} (g(x))^p &= \psi(g(x)) \\ &= \psi(\sum_{j=0}^{n} a_j x^j) \\ &= \sum_{j=0}^{n} \psi(a_j)\psi(x^j) \\ &= \sum_{j=0}^{n} a_j x^{pj} \\ &= g(x^p). \end{aligned}$$

□

4.2 The Proof

Theorem 4.4. *The cyclotomic polynomials $\Phi_n(x)$ are irreducible over $\mathbb{Z}$.*

Proof. Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible factor of $\Phi_n(x)$. We will show that every zero of $\Phi_n(x)$ is a zero of $f(x)$.

Since $\Phi_n(x)$ divides $x^n - 1$ in $\mathbb{Z}[x]$, there exists a polynomial $g(x) \in \mathbb{Z}[x]$ such that $x^n - 1 = f(x)g(x)$. Let ω be a primitive n^{th} root of unity that is a zero of $f(x)$. Let p be a prime that does not divide n; then $\gcd(p,n) = 1$, and so by [1, Lemma 3], ω^p is also a primitive n^{th} root of unity. It follows that $0 = (\omega^p)^n - 1 = f(\omega^p)g(\omega^p)$, and so ω^p is a zero of either $f(x)$ or $g(x)$. Suppose $f(\omega^p) \neq 0$, then $g(\omega^p) = 0$, so ω is a zero of $g(x^p)$. Because $f(x)$ is monic, irreducible, and has ω as a zero, by definition $f(x)$ is the minimal polynomial for ω over $\mathbb{Q}$. Therefore, by [5, Theorem 21.3], $f(x)$ divides $g(x^p)$ in $\mathbb{Q}[x]$, and so because $f(x)$ is monic, by Lemma 4.2, $f(x)$ divides $g(x^p)$ in $\mathbb{Z}[x]$. Say that $g(x^p) = f(x)h(x)$ where $h(x) \in \mathbb{Z}[x]$. Let $\bar{g}(x)$, $\bar{f}(x)$, and $\bar{h}(x)$ be the polynomials in $\mathbb{Z}_p[x]$ formed by reducing the coefficients of $g(x)$, $f(x)$, and $h(x)$ modulo p respectively; then $\bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$. Now by Lemma 4.3, $(\bar{g}(x))^p = \bar{g}(x^p) = \bar{f}(x)\bar{h}(x)$. Since by [5, Corollary to Theorem 18.3], $\mathbb{Z}_p[x]$ is a unique factorization domain, $\bar{f}(x)$ and $\bar{g}(x)$ share a common irreducible factor, call it $k(x)$. Thus for some $m_1(x), m_2(x) \in \mathbb{Z}_p[x]$, $\bar{f}(x) = k(x)m_1(x)$ and $\bar{g}(x) = k(x)m_2(x)$. It follows that in $\mathbb{Z}_p[x]$,

$$x^n - 1 = \bar{f}(x)\bar{g}(x) = (k(x))^2 m_1(x)m_2(x).$$

Hence $x^n - 1$ has a multiple zero in some extension field of $\mathbb{Z}_p$, and so by Theorem 4.1, $x^n - 1$ and its derivative, nx^{n-1}, must have a common factor of positive degree. Note that every factor of nx^{n-1} will be of the form cx^q, where $c \mid n$ and $0 \leq q \leq n-1$. Also note that any element of this form with positive degree cannot divide $x^n - 1$, which means that $x^n - 1$ and nx^{n-1} cannot share a common factor. Thus we have reached a contradiction, and so $f(\omega^p) = 0$. Therefore, if ω is any primitive n^{th} root of unity that is a zero of $f(x)$ and p is any prime that does not divide n, then ω^p is a zero of $f(x)$.

Still assuming that ω is a primitive n^{th} root of unity that is also a zero of $f(x)$, let ξ be any other primitive n^{th} root of unity. Because ω generates the group of n^{th} roots of unity, there exists an integer k such that $\omega^k = \xi$. Now by [1, Lemma 3], $\gcd(k, n) = 1$. It follows that $k = p_1 p_2 \dots p_r$ where for all i, p_i is a prime that does not divide n. Therefore ω, ω^{p_1}, $(\omega^{p_1})^{p_2}$, $(\omega^{p_1 p_2})^{p_3}$, $\dots$, $(\omega^{p_1 p_2 \cdots p_{r-1}})^{p_r} = \omega^k$ are all zeros of $f(x)$ that are primitive n^{th} roots of unity, in particular ξ is a zero of $f(x)$. Hence every primitive n^{th} root of unity is a zero of $f(x)$, and so $f(x)$ and $\Phi_n(x)$ share all their zeros. Since by Theorem 3.1, $\Phi_n(x)$ is monic, this means that $\Phi_n(x) = f(x)$, and so $\Phi_n(x)$ is irreducible over the integers. □

Corollary 4.5. *The cyclotomic polynomials $\Phi_n(x)$ are irreducible over $\mathbb{Q}$.*

Proof. By [5, Theorem 17.2], if a polynomial with integer coefficients is reducible over $\mathbb{Q}$ then it is reducible over $\mathbb{Z}$. The result follows from the contrapositive of this. □

5 Cyclotomic Polynomials and Primes

5.1 Unsolved Questions and Conjectures

A well known unanswered question about cyclotomic polynomials is if n is a fixed positive integer, then is $\Phi_n(m)$ prime for an infinite number of integer inputs

m? It is worth noting that this question is a special case of the Bunyakovsky Conjecture, an unproved result which states as follows:

Bunyakovsky Conjecture. *Suppose f is a polynomial of one variable with positive degree and integer coefficients. If*

1. *the leading coefficient of f is positive;*
2. *f is irreducible over the integers;*
3. *as n runs over the positive integers, the numbers $f(n)$ are relatively prime (i.e. the only integer that divides $f(n)$ for all $n \in \mathbb{N}$ is 1)*

then the polynomial $f(x)$ is prime for infinitely many positive integers m.

We have already seen that every cyclotomic polynomials satisfies the first two conditions; it is left to the reader to verify that they also satisfy the third. It follows that if the Bunyakovsky Conjecture is true then for all positive integers n, $\Phi_n(m)$ is prime for an infinite number of integer inputs m.

5.2 Relations Between Cyclotomic Polynomials and Primes

We will now explore some of the relationships between cyclotomic polynomials and prime numbers. The main focus of this subsection is results that may be useful in proving whether or not Φ_n assumes an infinite number of prime values over the integers.

Theorem 5.1. *If p is a prime and k is any positive integer, then $\Phi_{p^k}(1) = p$.*

Proof. For any prime p,

$$\begin{aligned}\Phi_p(x) &= \prod_{d|p}(x^d - 1)^{\mu(p/d)} \\ &= \frac{x^p - 1}{x - 1} \\ &= \sum_{k=0}^{p-1} x^k.\end{aligned}$$

Therefore $\Phi_p(1) = \sum_{k=0}^{p-1} 1^k = p$, and so by Corollary 3.4, $\Phi_{p^k}(1) = \Phi_p(1^{p^{k-1}}) = \Phi_p(1) = p$. □

Lemma 5.2. *Let p be a prime. Suppose that the polynomial $x^n - 1$ has a root of multiplicity greater than 1 modulo p, so there exists an integer b and a polynomial $f(x) \in \mathbb{Z}[x]$ such that*

$$x^n - 1 \equiv (x - b)^2 f(x) \pmod{p}.$$

Then p divides n.

Proof. See [1, Lemma 6]. □

Theorem 5.3. *Suppose n is a positive integer, d is a proper divisor of n, and b is any integer. If p is a common prime divisor of $\Phi_n(b)$ and $\Phi_d(b)$, then p divides n.*

Proof. By Theorem 3.9,

$$x^n - 1 = \prod_{t|n} \Phi_t(x),$$

so $x^n - 1$ is divisible by $\Phi_n(x)\Phi_d(x)$. Since $\Phi_n(b)$ and $\Phi_d(b)$ are both divisible by p, $\Phi_n(b) \equiv 0 \equiv \Phi_d(b) \pmod{p}$, so b is a root of both $\Phi_n(x)$ and $\Phi_d(x)$ in $\mathbb{Z}_p[x]$. Because $\mathbb{Z}_p$ is a field, by [5, Corollay 2 to Theorem 16.2], $x - b$ is a factor of both $\Phi_n(x)$ and $\Phi_d(x)$ in $\mathbb{Z}_p[x]$, and so $(x - b)^2$ is a factor of $x^n - 1$ in $\mathbb{Z}_p[x]$. It follows from Lemma 5.2 that p divides n. □

Theorem 5.4. *Let n be a positive integer and let b be any integer. If p is a prime that divides $\Phi_n(b)$, then either p divides n or $p \equiv 1 \pmod{n}$.*

Proof. Let p be a prime divisor of $\Phi_n(b)$. By Theorem 3.9, $\Phi_n(b) \mid b^n - 1$, and so $p \mid b^n - 1$. Therefore, since $\gcd(b^n - 1, b) = 1$, $p \nmid b$. It follows that $b \pmod{p}$ is an element of U_p (the group of units modulo p). Let k be the order of b in U_p. Since $p \mid b^n - 1$, $b^n \equiv 1 \pmod{p}$, which by [5, Theorem 4.1] means that $k \mid n$.

If $k = n$, then since U_p has $p - 1$ elements, by [5, Corollary 2 to Theorem 7.1], $n \mid p - 1$. In this case $p - 1 \equiv 0 \pmod{n}$, and so $p \equiv 1 \pmod{n}$.

If $k < n$, then since

$$0 \equiv b^k - 1 = \prod_{d|k} \Phi_d(b) \pmod{p},$$

there exists a divisor d of k such that $p \mid \Phi_d(b)$. Since $k \mid n$, this means that d is a proper divisor of n. It follows from Theorem 5.3 that $p \mid n$. □

Lemma 5.5. *If b is an integer and m and n are positive integers, then*

$$\gcd(b^m - 1, b^n - 1) = |b^{\gcd(m,n)} - 1|.$$

Proof. See [1, Lemma 7]. □

Theorem 5.6. *Let n and m be positive integers. Suppose that*

$$\gcd(\Phi_n(b), \Phi_m(b)) > 1$$

for some integer b; then $\frac{n}{m} = p^k$ for some prime p and integer k.

Proof. Suppose the p is a common prime divisor of $\Phi_m(b)$ and $\Phi_n(b)$. Let $m = p^\alpha M$ and $n = p^\beta N$ where $\alpha, \beta \geq 0$ are integers and M, N are positive integers not divisible by p. Note that since $p \mid \Phi_m(b)$ and $\Phi_m(b) \mid b^m - 1$, $p \nmid b$.

We will now show that $p \mid \Phi_M(b)$. If $\alpha = 0$, then $\Phi_m(b) = \Phi_M(b)$, so $p \mid \Phi_M(b)$. If $\alpha \geq 1$ then by Corollary 3.3 and Theorem 3.5,

$$\begin{aligned} 0 &\equiv \Phi_m(b) \\ &= \Phi_{p^{\alpha-1}pM}(b) \\ &= \Phi_{pM}(b^{p^{\alpha-1}}) \\ &= \frac{\Phi_M(b^{p^\alpha})}{\Phi_M(b^{p^{\alpha-1}})} \pmod{p}. \end{aligned}$$

Multiplying both sides of this congruence by $\Phi_M(b^{p^{\alpha-1}})$ gives us $\Phi_M(b^{p^\alpha}) \equiv 0 \pmod{p}$. Now since $p \nmid b$, $\gcd(p, b) = 1$, so $b \pmod{p} \in U_p$. By Lemma 5.5, $p - 1 \mid p^\alpha - 1$, so $p^\alpha - 1 = c(p - 1)$ for some integer c. Since U_p has $p - 1$ elements, by [5, Corollary 5 to Theorem 7.1],

$$b^{p^\alpha} = b^{p^\alpha - 1} b = (b^{p-1})^c b \equiv 1^c b = b \pmod{p}.$$

It follows that

$$0 \equiv \Phi_M(b^{p^\alpha}) \equiv \Phi_M(b) \pmod{p},$$

so $p \mid \Phi_M(b)$. Similarly $p \mid \Phi_N(b)$.

If we show that $M = N$, we will have that

$$\frac{n}{m} = \frac{p^\beta N}{p^\alpha M} = p^{\beta - \alpha},$$

which proves the theorem. Suppose that $M > N$. Let $t = \gcd(M, N)$ and note that $t < M$. Now since $\Phi_M(b) \mid b^M - 1$ and $\Phi_N(b) \mid b^N - 1$, and because p divides both $\Phi_M(b)$ and $\Phi_N(b)$, p is a common divisor of both $b^M - 1$ and $b^N - 1$. Therefore $p \mid \gcd(b^M - 1, b^N - 1)$. By Lemma 5.5, $\gcd(b^M - 1, b^N - 1) = |b^t - 1|$, so $p \mid b^t - 1$. Hence

$$0 \equiv b^t - 1 = \prod_{d \mid t} \Phi_d(b) \pmod{p},$$

so there exists a divisor d of t such that $p \mid \Phi_d(b)$. Since $t \mid M$ and $t < M$, d is a proper divisor of M, and because $p \mid \Phi_M(b)$, by Theorem 5.3, $p \mid M$, which is a contradiction since we assumed that $p \nmid M$. Thus $M \leq N$. A similar proof gives us $N \leq M$, which means that $M = N$. □

6 Wedderburn's Theorem

In this section we will look at an interesting application of the cyclotomic polynomials, but first some background. A *division ring* is a ring with unity in which every nonzero element a has a multiplicative inverse, i.e. an element x such that $ax = xa = 1$ (we will use 1 to denote the multiplicative identity of a ring). If R is a ring then we use R^* to denote the nonzero elements of R; note that if R is a division ring then R^* is a group under multiplication. For an element g of a group G, $I(g)$ denotes the *centralizer* of g, which is the set of all element of G that commute with g.

Lemma 6.1. *If* $0 < r < n$ *and* r *divides* n*, then* $\Phi_n(x)$ *divides* $\dfrac{x^n - 1}{x^r - 1}$ *in* $\mathbb{Z}[x]$.

Proof. By Theorem 3.9, for all positive integers m, $x^m - 1 = \prod_{d|m} \Phi_d(x)$. Therefore

$$\begin{aligned} \frac{x^n - 1}{x^r - 1} &= \frac{\prod_{d|n} \Phi_d(x)}{\prod_{d|r} \Phi_d(x)} \\ &= \prod_{\substack{d|n \\ d\nmid r}} \Phi_d(x). \end{aligned}$$

Because $r < n$, n divides n but not r, and so $\Phi_n(x)$ divides $\dfrac{x^n - 1}{x^r - 1}$. □

Lemma 6.2. *Let* G *be a group and suppose* a *is an element of* G*, then* a *is in a conjugacy class with one element if and only if* a *is in the center of* G.

Proof. Suppose a is in a conjugacy class with only itself; then for all g in G, $g^{-1}ag = a$, so $ag = ga$. By definition a commutes with every element of G, so a is in the center of G.

Now suppose a is in the center of G, then $I(a) = G$, and so by [6, Lemma 13.7], the conjugacy class containing a has

$$\begin{aligned} \frac{|G|}{|I(a)|} &= \frac{|G|}{|G|} \\ &= 1 \end{aligned}$$

element. □

Lemma 6.3. *If* $b > 1$ *and* n *and* r *are positive integers such that* $b^r - 1$ *divides* $b^n - 1$*, then* r *divides* n.

Proof. If $b^r - 1$ divides $b^n - 1$ then $\gcd(b^r - 1, b^n - 1) = b^r - 1$. By Lemma 5.5, $\gcd(b^r - 1, b^n - 1) = b^{\gcd(r,n)} - 1$. Thus $r = \gcd(r, n)$, and so r divides n. □

Now we have all the information we need to prove the main result of this section.

Theorem 6.4 (Wedderburn's Theorem)**.** *A finite division ring is a field.*

Proof. Let D be a finite division ring and let

$$K = \{a \in D : ax = xa \text{ for all } x \in D\}$$

be the center of D. Note that K is closed under subtraction and multiplication (meaning it will be a ring), every nonzero element in K will also have its inverse in K, and K is commutative, making it a finite field. Thus because every finite field has prime power order, $|K| = q$ where $q = p^m$ for some prime p and non-negative integer m. Also note that D is a vector space over K, say of dimension n, so $|D| = q^n$. Assume that $n > 1$. Now for all $a \in D^*$, $I(a) \cup \{0\}$ is a division ring, and $K \subseteq I(a) \cup \{0\}$. Therefore $I(a) \cup \{0\}$ is a vector space over K, so for some integer r, $|I(a) \cup \{0\}| = q^r$, and thus $|I(a)| = q^r - 1$. Note that for all $a \in D^*$, $a \cdot 1 = a = 1 \cdot a$, so $1 \in I(a)$. Thus $|I(a) \cup \{0\}| \geq 2$, so $q^r \geq 2$. It follows that $r > 0$, since if $r = 0$ then $q^r = 1 \ngeq 2$. Also, by [5, Theorem 3.6], $I(a)$ is a subgroup of D^*, so by Lagrange's Theorem $q^r - 1$ divides $q^n - 1$, and therefore by Lemma 6.3, r divides n.

Let $C_1, C_2, \ldots, C_s$ be the conjugacy classes of D^*; then the class equation is

$$|D^*| = \sum_{j=1}^{s} |C_j|.$$

Note that the center of D^* will be the same as the center of D without the element 0, and thus the center of D^* has $q - 1$ elements. By Lemma 6.2 there are exactly $q - 1$ conjugacy classes of D^* with one element; assume without a loss of generality that these classes are $C_1, C_2, \ldots, C_{q-1}$. The class equation then becomes

$$|D^*| = (q - 1) + \sum_{j=q}^{s} |C_j|.$$

For all j such that $q \leq j \leq s$, let a_j be an element of C_j, then there exists an integer r_j such that $0 < r_j < n$, r_j divides n, and $|I(a_j)| = q^{r_j} - 1$. Therefore by [6, Lemma 13.7], for all $j \geq q$, $|C_j| = \dfrac{q^n - 1}{q^{r_j} - 1}$, and so the class equation becomes

$$q^n - 1 = (q - 1) + \sum_{j=q}^{s} \frac{q^n - 1}{q^{r_j} - 1},$$

or, in another form

$$(q^n - 1) - \sum_{j=q}^{s} \frac{q^n - 1}{q^{r_j} - 1} = q - 1.$$

By Lemma 6.1, for all j such that $q \leq j \leq s$, $\Phi_n(q)$ divides $\dfrac{q^n - 1}{q^{r_j} - 1}$, and thus because $\Phi_n(q)$ divides $q^n - 1$, $\Phi_n(q)$ divides $(q^n - 1) - \displaystyle\sum_{j=q}^{s} \frac{q^n - 1}{q^{r_j} - 1} = q - 1$. On the other hand recall that

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ gcd(n,k)=1}} (x - e^{\frac{2i\pi k}{n}}),$$

and so (using the reverse triangle inequality),

$$\begin{aligned}
|\Phi_n(q)| &= \prod_{\substack{1\leq k\leq n\\ gcd(n,k)=1}} |q - e^{\frac{2i\pi k}{n}}| \\
&\geq \prod_{\substack{1\leq k\leq n\\ gcd(n,k)=1}} ||q| - |e^{\frac{2i\pi}{n}}|^k| \\
&= \prod_{\substack{1\leq k\leq n\\ gcd(n,k)=1}} (q-1) \\
&> q-1
\end{aligned}$$

when $n > 2$. When $n = 2$, $\Phi_n(q) = q + 1$, which is greater than $q - 1$. Thus $\Phi_n(q)$ cannot divide $q - 1$, and so we have a contradiction, meaning that it is impossible that $n > 1$. Therefore D is a vector space over K of degree 1, which means that $D = K$, and hence D is commutative. Since D is a commutative ring with unity where every element is a unit, by definition it is a field. □

7 Constructible Regular N-Gons

Another application of cyclotomic polynomials that we will explore is when a regular n-gon (in $\mathbb{R}^2$) is constructible with a straightedge and compass (from here on out we will assume that n-gon means regular n-gon). Before we do this though we need to solidify exactly what we mean by constructible. Suppose that A is a subset of $\mathbb{R}^2$. We say that a line is *constructible from A* if it passes through two distinct points that are either constructible from or in A. We say that a circle is *constructible from A* if its center is a point that is constructible from or in A and some other point that is constructible from or in A lies on the circle. A point in $\mathbb{R}^2$ is *constructible from A* if it is a point shared by two distinct lines, two distinct circles, or a line and a circle constructible from A. An n-gon is *constructible from a set A* if all the points at its vertices are constructible from A.

We say that an object (line, circle, point, or n-gon) is *constructible* if it is constructible from the set $A = \{(0, 0), (1, 0)\}$. It is worth noting that it can be shown that every point in $\mathbb{Q}^2$ is constructible.

From here on out we will identify the point $(a, b) \in \mathbb{R}^2$ with the complex number $a + bi$. Finally, recall that a *Fermat prime* is any prime number of the form $2^{2^j} + 1$, where j is a nonnegative integer.

Theorem 7.1. *The set of constructible complex numbers form a subfield of* $\mathbb{C}$.

Proof. See [8, Section 7.7; Theorem 3]. □

Theorem 7.2. *Suppose ω is a complex number with minimal polynomial $f(x)$ over $\mathbb{Q}$. If F is the splitting field for $f(x)$ over $\mathbb{Q}$, then ω is constructible if and only if $[F : \mathbb{Q}] = 2^l$, where l is a nonnegative integer.*

Proof. See [7, Theorem 9.1]. □

Theorem 7.3. *Suppose n is a positive integer. Let F be the spitting field for $\Phi_n(x)$ over $\mathbb{Q}$, then $[F:\mathbb{Q}] = \phi(n)$.*

Proof. Let $\omega = e^{\frac{2\pi i}{n}}$, and note that ω is a zero of $\Phi_n(x)$. It follows that F contains ω, so $\mathbb{Q}(\omega) \subseteq F$. Let ξ be any zero of $\Phi_n(x)$, then ξ is a primitive n^{th} root of unity. Hence, by Theorem 2.5, $\xi = \omega^k$ for some k such that $1 \leq k \leq n$ and $\gcd(k,n) = 1$. It follows that $\xi \in \mathbb{Q}(\omega)$. Therefore all the zeros of $\Phi_n(x)$ are contained in $\mathbb{Q}(\omega)$, and so $\Phi_n(x)$ splits in $\mathbb{Q}(\omega)$. Because by definition $\Phi_n(x)$ cannot split in any proper subfield of F, this means that $\mathbb{Q}(\omega) = F$. By Theorem 3.1, $\deg \Phi_n(x) = \phi(n)$, and so by [5, Theorem 20.3], $\{1, \omega, \omega^2, \ldots, \omega^{\phi(n)-1}\}$ is a basis for $\mathbb{Q}(\omega)$ over $\mathbb{Q}$. By definition this means that $[F:\mathbb{Q}] = [\mathbb{Q}(\omega):\mathbb{Q}] = \phi(n)$. □

Lemma 7.4. *If $2^n + 1$ is prime for some positive integer n, then $n = 2^k$ for some nonnegative integer k (i.e. $2^n + 1$ is a Fermat prime).*

Proof. We will prove this by the contrapositive. Suppose that $n \neq 2^k$ for any integer k. It follows that n must have an odd factor $r > 1$, and so $n = t \cdot r$ for some $t \in \mathbb{N}$. One can see by routine verification that

$$(2^t + 1)(\sum_{j=0}^{r-1} (-1)^j 2^{(r-1-j)t}) = 2^n + 1.$$

Since $0 < t < n$ we have that $2 < 2^t + 1 < 2^n + 1$. Therefore $2^n + 1$ has a nontrivial factor, making it composite. □

Theorem 7.5. *Suppose n is a positive integer, then $\phi(n)$ is a power of 2 if and only if n has the form $2^k p_1 p_2 \ldots p_r$, where $k \geq 0$ and the p_j's are distinct Fermat primes.*

Proof. By [4, Theorem 5.21], ϕ is a multiplicative function. Thus if $\prod_{j=1}^{r} p_j^{f_j}$ is the prime factorization of n, then $\phi(n) = \prod_{j=1}^{r} \phi(p_j^{f_j})$. Hence $\phi(n)$ is a power of 2 if and only if for all primes p and positive integers f such that $p^f \parallel n$, $\phi(p^f)$ is a power of 2.

Suppose $k \geq 1$, then by Lemma 3.7, $\phi(2^k) = 2^{k-1}$, which is clearly a power of 2.

Now Suppose p is an odd prime and $\phi(p^f) = 2^m$ for some $f, m \in \mathbb{N}$. Again by Lemma 3.7, $\phi(p^f) = p^{f-1}(p-1)$. This means that if $f > 1$, then $p \mid \phi(p^f)$, which would contradict that $\phi(p^f)$ is a power of 2. Hence $f = 1$, and so

$$p - 1 = \phi(p) = \phi(p^f) = 2^m.$$

Therefore $p = 2^m + 1$, which by Lemma 7.4 means that p is a Fermat prime. If we suppose that p is a Fermat prime, then $p = 2^{2^j} + 1$ for some $j \in \mathbb{N}$. In this case, $\phi(p) = 2^{2^j}$, which is a power of 2. Thus if $f \in \mathbb{N}$ and p is an odd prime, then $\phi(p^f)$ is a power of 2 if and only if $f = 1$ and p is a Fermat prime.

Therefore, $\phi(n)$ is a power of 2 if and only if for all primes p and $f \in \mathbb{N}$ such that $p^f \parallel n$, either $p = 2$, or p is a Fermat prime and $f = 1$. □

Theorem 7.6. *It is possible to construct the regular n-gon with a straightedge and compass if and only if n has the form $2^k p_1 p_2 \ldots p_r$, where $k \geq 0$ and the p_j's are distinct Fermat primes.*

Proof. Note that if an n-gon is constructible, then the point in the center of the n-gon is constructible. Hence we may assume that the n-gon we are trying to construct is centered at the origin. Also note that if we are able to construct an n-gon then we can construct an n-gon where every point has distance 1 from the origin. Thus we may assume that the vertices of the n-gon we are trying to construct are located on the unit circle. It follows that we may assume that the vertices of the n-gon will be located at the n^{th} roots of unity.

Now if an n-gon is constructible, then the point $e^{\frac{2\pi i}{n}}$ must be constructible. Furthermore, if $e^{\frac{2\pi i}{n}}$ is constructible, then since every n^{th} root of unity is a power of $e^{\frac{2\pi i}{n}}$, by Theorem 7.1 every n^{th} root of unity will be constructible. Hence, an n-gon is constructible if and only if the point $e^{\frac{2\pi i}{n}}$ is constructible.

Notice that $e^{\frac{2\pi i}{n}}$ is a zero of $\Phi_n(x)$, and thus because $\Phi_n(x)$ is irreducible over $\mathbb{Q}$ and monic, it is the minimal polynomial for $e^{\frac{2\pi i}{n}}$ over $\mathbb{Q}$. It follows from Theorems 7.2 and 7.3 that $e^{\frac{2\pi i}{n}}$ is constructible if and only if $\phi(n) = 2^l$, where l is a nonnegative integer. By Theorem 7.5, this happens if and only if n has the form $2^k p_1 p_2 \ldots p_r$, where $k \geq 0$ and the p_j's are distinct Fermat primes. □

8 Acknowledgments

The author would like to thank Dr. Patrick Keef for his support and guidance on this project, along with suggesting the topic in the first place. He would also like to acknowledge Austin Sloane for editing this work and ensuring its quality.

References

[1] Yimin Ge, *Elementary Properties of Cyclotomic Polynomials*, http://www.yimin-ge.com/doc/cyclotomic_polynomials.pdf

[2] Yves Gallot, *Cyclotomic Polynomials and Prime Numbers*, http://yves.gallot.pagesperso-orange.fr/papers/cyclotomic.pdf

[3] Pantelis A. Damianou, *On Prime Values of Cyclotomic Polynomials*, http://arxiv.org/pdf/1101.1152.pdf

[4] Robbins, Neville. *Beginning Number Theory.* 2nd ed. Sudbury, Mass.: Jones and Bartlett, 2006. Print.

[5] Gallian, Joseph A. *Contemporary Abstract Algebra.* 7th ed. Belmont, CA: Brooks/Cole, Cengage Learning, 2010. Print.

[6] Stewart, Ian. *Galois Theory*. 2nd ed. London: Chapman and Hall, 1989. Print.

[7] Kuh, Devin. “Constructible Regular N-gons.”(2013). Web. 4 May 2015. https://www.whitman.edu/Documents/Academics/Mathematics/Kuh.pdf.

[8] Goldstein, Larry Joel. *Abstract Algebra; a First Course*. Englewood Cliffs: Prentice-Hall, 1973. Print.

[9] Warner, Seth. *Modern Algebra I*. Englewood Cliffs: Prentice-Hall, 1965. Print.