Existence of Primitive Roots Modulo a Prime Via Cyclotomic Polynomials

RoKuluro96

July 6, 2020

This text will introduce interesting relations between elementary number theory and algebra. In particular, we explore surface level connections between cyclotomic polynomials and primitive roots which are both interesting and useful when dealing with divisibility problems of certain exponential expressions. Everything presented in the earlier section of the text will lead up to a proof of the existence of primitive roots modulo a prime. The interested reader is then encouraged to take this knowledge further to learn about more in-depth topics such as Gauss' famous theory on the constructibility of regular polygons. Enjoy!

We'll begin by introducing a few definitions. These objects will be the key players throughout our discussion.

Definition 1 (Primitive Roots)**.** Let n be a positive integer. Define a **primitive root** mod n to be an integer g, $1 \leq g < n$, such that $\operatorname{ord}_n g = \phi(n)$ where $\phi(n)$ denotes the Euler Totient Function. In particular, we observe that when $n = p$ for odd prime p, $\operatorname{ord}_p g = p - 1$.

In particular, we will be examining the existence of these primitive roots when n is a prime number.

Definition 2 (Primitive Roots of Unity)**.** Let n be a positive integer and let $\omega_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$. For some integers k where $1 \leq k < n$, we define the **primitive nth roots of unity** as the values ω_n^k such that $(\omega_n^k)^n = 1$ and $(\omega_n^k)^j \neq 1$ for all integers j where $1 \leq j < n$. In other words, the "order" of ω_n^k is n. That is, n is the first power that returns ω_n^k to 1.

Proposition 1. If $\omega_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$, then the primitive nth roots of unity are precisely the values ω_n^k, such that $\gcd(n, k) = 1$ for integers k where $1 \leq k < n$.

Proof. Let $g = \gcd(n, k)$. By the definition of primitive roots of unity, we have that $(\omega_n^k)^n = 1$ and $(\omega_n^k)^j \neq 1$ for integers j such that $1 \leq j < n$. Now consider what happens when $g > 1$. If $g > 1$, we have that

$$nk > \operatorname{lcm}(n, k)$$

or

$$\frac{\operatorname{lcm}(n, k)}{k} < n.$$

Now let

$$d = \frac{\operatorname{lcm}(n,k)}{k}.$$

Obviously, d must be an integer. Raising ω_n^k to the dth power, we get the value $\omega_n^{\operatorname{lcm}(n,k)}$. Noting that $\operatorname{lcm}(n,k)$ is a multiple of n, it's easy to see that

$$\begin{aligned}\omega_n^{\operatorname{lcm}(n,k)} &= \omega_n^{n\cdot\operatorname{lcm}(n,k)/n} \\ &= (\omega_n^n)^{\operatorname{lcm}(n,k)/n} = 1^{\operatorname{lcm}(n,k)/n} = 1\end{aligned}$$

Thus, d is an integer less than n such that $(\omega_n^k)^d = 1$. This contradicts the definition, so $g = 1$.

Now we show that this is sufficient. Letting $g = 1$, we have $d = n$ implying that $(\omega_n^k)^n = 1$. However, we also require that $(\omega_n^k)^j \neq 1$ for all integers j where $1 \leq j < n$. This is actually easy to see by noting that $\omega_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$. We have

$$(\omega_n^k)^j = \cos\left(\frac{2\pi kj}{n}\right) + i\sin\left(\frac{2\pi kj}{n}\right).$$

Since $g = 1$ and $j < n$, the fraction kj/n can never be an integer, so the argument of $(\omega_n^k)^j$ cannot be a multiple of 2π. Therefore, $(\omega_n^k)^j \neq 1$, and we're done. □

This is a lot to grapple with at first, but think of primitive roots of unity as the complex number version of primitive roots modulo primes. Note how similar the two are to each other. They both deal with the concept of taking numbers to different powers and seeing when they return to 1. To be more precise, they both look at numbers which "take the longest" to return to 1.

Definition 3 (Cyclotomic Polynomials)**.** Given any positive integers n, we define the nth **cyclotomic polynomial** $\Phi_n(X)$ as

$$\Phi_n(X) = \prod_{\substack{\gcd(k,n)=1 \\ 1\leq k\leq n}} (X - \omega_n^k).$$

In other words, they are polynomials whose roots are precisely all the primitive nth roots of unity.

The way we think about the roots of these polynomials becomes key when we start thinking about them in Z_p. In particular these polynomials have a tight relationship with the polynomial $X^n - 1$.

Proposition 2 (Divisors of $X^n - 1$)**.** For any positive integer n, we have that

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Proof. Note that

$$X^n - 1 = \prod_{1 \le k \le n} (X - \omega_n^k),$$

and let ω_n^k be one of its roots. If we let $s = \gcd(n, k)$, note that because $\omega_n = \omega_{n/s}^{1/s}$, we have $\omega_n^k = \omega_{n/s}^{k/s}$. By definition, this then must mean that ω_n^k is a root of $\Phi_{n/s}(X) = 0$. It then follows that all the roots in $X^n - 1 = 0$ are also roots of the product on the right. Now to show that there are no extraneous factors on the right hand side, note that $\Phi_n(X)$ is always monic and that the roots of cyclotomic factors are precisely the primitive roots of unity. Therefore it suffices to show that no double roots exist among these roots of unity. By definition, $\Phi_n(X)$ only has unique roots and all primitive roots of unity have a single order, so we're done. □

As a nice exercise, we can use this relation to compute the first couple of cyclotomic polynomials. We have $\Phi_1(X) = X-1$, $\Phi_2(X) = X+1$, $\Phi_3(X) = X^2+X+1$, $\Phi_4(X) = X^2+1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, etc.

Corollary 1 (Sum of ϕ)**.** For all positive integers n, we have that

$$n = \sum_{d|n} \phi(d).$$

Proof. Consider the degree of each polynomial in the theorem above. $X^n - 1$ has a degree of n and $\prod_{d|n} \Phi_d(X)$ has a degree of $\sum_{d|n} \phi(d)$. Since they are the same polynomial, they must have the same degree, so the result follows. □

The corollary by itself seems quite surprising, but because of the proposition above, this is something that naturally follows. The idea behind it is that each integer from 1 to n can be categorized into disjoint sets depending on its gcd with n.

Proposition 3 (Cyclotomic Polynomials as Integer Polynomials)**.** All cyclotomic polynomials are integer polynomials. That is, every coefficient of $\Phi_n(X)$ is an integer for all positive integers n.

Proof. We prove the statement via induction on n. For the base case, it's easy to see that $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$.

We then assume that for all positive integers k less than n, $\Phi_k(X) \in \mathbb{Z}[X]$ and let

$$P(X) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X).$$

By the inductive hypothesis, $P(X)$ is a monic, integer polynomial. Now consider the polynomial $X^n - 1$. Since $\deg P(X) = n - \phi(n) < n = \deg(X^n - 1)$, by the division algorithm, we see that there must exist a unique pair of integer polynomials $Q(x)$ and $R(X)$ with $\deg R(X) < \deg P(X)$ such that

$$X^n - 1 = P(X) \cdot Q(X) + R(X).$$

By proposition 2, we then see that all of the roots of $P(X)$ are also the roots of $X^n - 1$. This means that $R(X)$ must either share the same roots as $P(X)$ or be equal to the zero polynomial. In the former case, we see that $\deg R(X) = n - \phi(n) \not< \deg P(X)$, which is a contradiction. Therefore, $R(X)$ must be the zero polynomial further implying that $Q(X)$ is precisely equal to $\Phi_n(X)$. Since $Q(X)$ is an integer polynomial, we're done. □

Although this seems trivial, this is actually an important result that allows us to work with cyclotomic polynomials modulo primes.

Now that the base knowledge has been built, we can then explore more interesting results. The following theorem turns out to be very useful because it reveals an important connection between the idea of orders and these polynomials.

Theorem 1 (Primes Dividing Cyclotomic Polynomials)**.** Let p be a prime and let a be some positive integer. For all positive integers n, either $p \mid n$ or

$$\Phi_n(a) \equiv 0 \pmod{p}$$

if and only if $\operatorname{ord}_p a = n$.

Proof. We first show that if $\Phi_n(a) \equiv 0 \pmod{p}$, then $\operatorname{ord}_p a = n$. After that we prove the converse.

Let $m = \operatorname{ord}_p a$. Because we're given that

$$\Phi_n(a) \equiv 0 \pmod{p},$$

and $\Phi_n(X)$ is a divisor of $X^n - 1$, we quickly see that

$$a^n - 1 \equiv 0 \pmod{p}.$$

From this, we either have that $m = n$ or $m < n$. Note that we can't have $m > n$ since that will contradict the definition of an order.

In the first case where $m = n$, we have $\operatorname{ord}_p a = m = n$, which gets us the first result. Otherwise, we have $m < n$, so m divides n by orders. Now because $m = \operatorname{ord}_p a < n$, we see that

$$0 \equiv a^m - 1 = \prod_{d \mid m} \Phi(a) \pmod{p}.$$

Thus, we note there must exist some divisor d of m such that

$$\Phi_d(a) \equiv 0 \pmod{p}.$$

Now because both $\Phi_d(X)$ and $\Phi_n(X)$ are divisors of $X^n - 1$ and a is a root of both polynomials, a must be a double root of $X^n - 1 \equiv 0 \pmod{p}$. Therefore, taking the derivative of this congruence, we see that a is a root of

$$nX^{n-1} \equiv 0 \pmod{p}.$$

And since a cannot be a multiple of p, it's impossible for a to be a root of $X^{n-1} \equiv 0 \pmod{p}$. Therefore, p must divide n. Note that these are the edge cases in the theorem.

We now proceed to prove the converse. Since we're given that $\operatorname{ord}_p a = n$, we have $a^n - 1 \equiv 0 \pmod{p}$. This means that there exists some divisor d of n such that

$$\Phi_d(a) \equiv 0 \pmod{p}.$$

Now note that we can't actually have $d = k < n$, since from the derivations above,

$$\Phi_k(a) \equiv 0 \pmod{p} \Rightarrow \operatorname{ord}_p a = k,$$

which is a contradiction. Thus, $d = n$ and we're done. □

On the surface, this seems like a highly unmotivated theorem, but you will soon see its breadth in the upcoming proof of the existence of primitive roots. A nice way to remember this theorem is to think about what the roots of cyclotomic polynomials mod p reveal about the relations between a, n, and p. Another interesting thing to note is that this theorem is actually a generalization of Fermat's Christmas Theorem in the case when one of the two squares is equal to 1. (Do you see why?)

Now before we delve into the proof of the existence of primitive roots, we present another useful theorem. It does not have anything to do with cyclotomic polynomials per say, but it gives us a general understanding of how integer polynomials work in Z_p.

Theorem 2 (Lagrange)**.** Let p be a prime number. Given an integer polynomial $f(x)$ such that $f(x) \equiv 0 \pmod{p}$, then either there are at most $\deg f$ roots modulo p or all the coefficients are multiples of p.

Proof. We prove the statement by induction on the degree of f. Let $f(x)$ be a polynomial with degree n and assume that the conclusion holds for all positive integers less than n. We show that $f(x)$ has at most n roots modulo p.

The base case is simple in that we can either always solve for linear equations mod p or the coefficients are multiples of p.

For the inductive step, consider the roots of $f(x)$. If $f(x)$ has no roots mod p, then obviously our statement holds, so we can assume that there exists some root a of the congruence. Using the division algorithm, we can write this as

$$f(x) = g(x) \cdot (x - a) + r \equiv 0 \pmod{p},$$

where $g(x)$ is a polynomial with degree $n - 1$ and r is some integer constant. Letting $x = a$, we note that

$$f(a) = r \equiv 0 \pmod{p},$$

so r must be a multiple of p. Thus, we note that

$$f(x) \equiv g(x) \cdot (x - a) \equiv 0 \pmod{p}.$$

The only way this can happen is if either $g(x) \equiv 0$ or $x - a \equiv 0$, so using our hypothesis, either the coefficients of $g(x)$ are all multiples of p meaning all the coefficients of $f(x)$ are multiples of p, or the number of roots of $f(x)$ is at most $\deg g + 1 = (n - 1) + 1 = n$. □

With that out of the way, we are finally ready to present and prove the following theorem.

Theorem 3 (The Existence of Primitive Roots)**.** There exists $\phi(p-1)$ primitive roots modulo any prime p.

Proof. Since p is relatively prime to $p-1$, note by Theorem 1 that

$$\Phi_{p-1}(a) \equiv 0 \pmod p$$

if and only if $\operatorname{ord}_p a = p-1$. It then follows that the values a are all the primitive roots mod p by definition. Therefore, it suffices to show these roots actually exist when $\Phi_{p-1}(X) \equiv 0$.

To begin, consider the degree of the polynomial $\Phi_{p-1}(X)$. By definition, since we have

$$\Phi_{p-1}(X) = \prod_{\substack{\gcd(k,p-1)=1 \\ 1\le k\le p-1}} (X - \omega_{p-1}^k),$$

where $\omega_{p-1} = \cos\left(\frac{2\pi}{p-1}\right) + i\sin\left(\frac{2\pi}{p-1}\right)$, its degree is simply $\phi(p-1)$. We then claim the following.

Claim. The number of roots modulo p of

$$\Phi_{p-1}(X) \equiv 0 \pmod p$$

is exactly $\phi(p-1)$.

It turns out that Lagrange's Theorem helps us prove just that. Noting that all cyclotomic polynomials are monic, integer polynomials, we can apply Lagrange's Theorem to see that

$$\Phi_d(X) \equiv 0 \pmod p$$

has at most $\phi(d)$ roots modulo p for each divisor $d \mid p-1$. This alone certainly does not assert our claim, so now consider the factorization of the polynomial $X^{p-1}-1$. We can write this as

$$X^{p-1} - 1 = \prod_{d|p-1} \Phi_d(X).$$

Taking modulo p, we see by Fermat's Little Theorem that

$$\prod_{d|p-1} \Phi_d(X) \equiv 0 \pmod p$$

has roots for all $X = a$, $a \in \{1, 2, \cdots, p-1\}$. In other words, this congruence has *exactly* $p-1$ roots. And since

$$\sum_{d|p-1} \phi(d) = p-1,$$

it turns out that each cyclotomic factor must have the maximum number of roots, which is precisely $\phi(d)$.

Thus, to find a primitive root modulo some prime p, it suffices to choose one of the $\phi(p-1)$ roots of $\Phi_{p-1}(X) \equiv 0 \pmod p$. □

Now the neat part about this proof is that we never specified a way to generate each primitive root. Nonetheless, we were able to not only show that they existed, but were able to show exactly *how many* there were.

A constructive proof of this theorem does exists however; the first of which was discovered by Gauss in his *Disquisitiones Arithmeticae* in 1801, which delves more deeply into the subject.

To get back on topic though, primitive roots give us interesting properties to think about.

Corollary 2 (Unique Representation of Primitive Roots)**.** Let p be a prime number. Given some primitive root g mod p, the set $\{g^1, g^2, \cdots, g^{p-1}\}$ is some permutation of the set $\{1, 2, \cdots, p-1\}$ mod p. In other words, each power of g uniquely represents a value in Z_p.

Proof. Let i and j be positive integers such that $1 \leq i < j \leq p-1$ and assume

$$g^j \equiv g^i \pmod{p}.$$

Since g is relatively prime to p, dividing both sides by g^i, we see that

$$g^{j-i} \equiv 1 \pmod{p}.$$

However, this is impossible since $p-1$ is the order of g by definition and $j-i < p-1-i < p-1$. Therefore, each power of g must uniquely represent a value in Z_p. □

The reason why this is so nice can be demonstrated by the following problem.

Problem 1 (Classic)**.** Let n be a positive integer and $p > n+1$ is a prime. Prove that p divides

$$1^n + 2^n + \cdots + (p-1)^n.$$

Proof. Let S be the given sum. Since p is a prime, note that there exists some primitive root $g \in \{1, 2, \cdots, p-1\}$. Now because each integer in $\{1, 2, \cdots, p-1\}$ can be rewritten as unique powers of g modulo p, we can write

$$\begin{aligned} S &\equiv (g^0)^n + (g^1)^n + \cdots + (g^{p-2})^n \\ &= (g^n)^0 + (g^n)^1 + \cdots + (g^n)^{p-2} \\ &= \frac{(g^n)^{p-1} - 1}{g^n - 1} \pmod{p}. \end{aligned}$$

Thus, we see that for some integer k,

$$S = kp + \frac{(g^n)^{p-1} - 1}{g^n - 1}$$

which becomes

$$S(g^n - 1) = kp(g^n - 1) + (g^n)^{p-1} - 1.$$

By Fermat's Little Theorem, we see that this further simplifies to

$$S(g^n - 1) \equiv 0 \pmod{p}.$$

This implies that either S or $g^n - 1$ are divisible by p. We can then eliminate the latter choice by noting that $p - 1 > n$ and noting that $\operatorname{ord}_p g = p - 1$. □

Here is a list of a few more propositions, theorems, and problems I recommend thinking about that will get you familiar with the subject more. Many of these can be solved with only the content discussed above, but most of these require additional knowledge. If you can't solve many of these problems, don't feel discouraged; they're meant to be fun teasers with the purpose of sparking your interest. Otherwise, these facts are famous enough that their proofs can be found elsewhere.

Proposition 4. Let p be an odd prime. Given that g is a primitive root mod p, we have

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Theorem 4 (Primitive Roots Modulo Non-Primes)**.** Let n be a positive integer. Primitive roots exist modulo n if and only if $n \in \{2, 4, p^k, 2p^k\}$ for all odd primes p and positive integers k.

Theorem 5 ($n^2 + 1$)**.** Let p be an odd prime. There exists positive integers n such that $n^2 + 1 \equiv 0 \pmod{p}$ if and only if $p \equiv 1 \pmod{4}$. Stated differently, there cannot exist n satisfying $n^2 + 1 \equiv 0 \pmod{p}$ if and only if $p \equiv 3 \pmod{4}$

Problem 2. Let p be an odd prime and let g be a primitive root modulo p. Prove that for each divisor of $p - 1$, there exists a value $a \in \{1, 2, \cdots, p - 1\}$ such that the order of a mod p is that divisor.

Proposition 5 (Cyclotomic Polynomials as Minimal Polynomials)**.** The cyclotomic polynomial $\Phi_n(X)$ is a minimal polynomial for all positive integers n.

Problem 3 (Coefficients of Cyclotomic Polynomials)**.** Is it always the case that the coefficients of cyclotomic polynomials are -1, 0, or 1? If so, can you prove it is? If not, is there a counterexample?

Theorem 6 (Migotti)**.** Let n be a positive integer. All the coefficients of the cyclotomic polynomial $\Phi_n(X)$ will be in the set $\{-1, 0, 1\}$ if n has at most 2 distinct odd prime factors.

Theorem 7 (Dirichlet)**.** There are infinitely many primes p, such that $p \equiv 1 \pmod{n}$ for any positive integer n.

Problem 4 (Gauss)**.** Given a length of 1, prove that the value $\cos \frac{2\pi}{17}$ can be constructed with a compass and straight-edge.

References

[1] Evan Chen. *Orders Modulo a Prime* (2015). `https://web.evanchen.cc/handouts/ORPR/ORPR.pdf`

[2] Lawrence Sun. *Cyclotomic Polynomials in Olympiad Number Theory* (2013).

[3] Alexander Gorodnik. *Polynomial Congruences Modulo Primes* (2017). `https://people.maths.bris.ac.uk/~mazag/nt/lecture6.pdf`