Chapter 5

Primitive Roots

The name primitive root applies to a number a whose powers can be used to represent a reduced residue system modulo n. Primitive roots are therefore generators in that sense, and their properties will be very instrumental in subsequent developments of the theory of congruences, especially where exponentiation is involved.

5.1 Orders and Primitive Roots

With $\gcd(a, n) = 1$, we know that the sequence $a \,\%\, n$, $a^2 \,\%\, n$, $a^3 \,\%\, n$, ... must eventually reach 1 and make a loop back to the first term. In fact, Euler's theorem says that the length of this periodicity is at most $\phi(n)$. We will define this length, for a given a, and ask whether it can sometimes equal $\phi(n)$.

Definition. Suppose a and $n > 0$ are relatively prime. The *order* of a modulo n is the smallest positive integer k such that $a^k \,\%\, n = 1$. We denote this quantity by $|a|_n$, or simply $|a|$ when there is no ambiguity. For example, $|2|_7 = 3$ because $x = 3$ is the smallest positive solution to the congruence $2^x \equiv 1 \pmod 7$.

Exercise 5.1. Find these orders.

a) $|3|_7$
b) $|3|_{10}$
c) $|5|_{12}$
d) $|7|_{24}$
e) $|4|_{25}$

Exercise 5.2. Suppose $|a| = 6$. Find $|a^k|$ for $k = 2, 3, 4, 5, 6$.

From now on we agree that the notation $|a|_n$ implicitly assumes the condition $\gcd(a, n) = 1$, for otherwise it makes no sense. In particular, by Euler's theorem, $|a|_n \leq \phi(n)$. It is also clear that the definition of order extends to residue classes, for we have $|a|_n = |b|_n$ whenever $a \equiv b \pmod{n}$.

EXERCISE 5.3. Investigate true or false.

a) $|-a| = |a|$
b) $|a^{-1}| = |a|$
c) If $|a|_n = |b|_n$ then $a \equiv b \pmod{n}$.
d) If $a^j \equiv a^k \pmod{n}$ then $j \equiv k \pmod{n}$.
e) If $\gcd(a, n) > 1$, then $a^x \equiv 1 \pmod{n}$ has no solution.

EXERCISE 5.4. Prove that if $|a|_n = n - 1$ then n is a prime.

Proposition 5.1. Fix a modulus $n > 0$. Then

1) $a^k \equiv 1 \pmod{n}$ if and only if $|a|_n \mid k$. In particular, $|a|_n \mid \phi(n)$.

2) $a^j \equiv a^k \pmod{n}$ if and only if $j \equiv k \pmod{|a|_n}$.

3) $|a| = |a^k| \gcd(k, |a|)$ for any $k \geq 1$. In particular, $|a^k| = |a|$ if and only if $\gcd(k, |a|) = 1$.

4) $|ab| = |a|\,|b|$ if $\gcd(|a|, |b|) = 1$.

Proof. 1) Let $j = \lfloor k/|a|_n \rfloor$ so that we may write $k = j|a|_n + k \,\%\, |a|_n$. Then $a^k = (a^{|a|_n})^j \cdot a^{k \,\%\, |a|_n} \equiv a^{k \,\%\, |a|_n} \pmod{n}$. But $k \,\%\, |a|_n < |a|_n$, hence the congruence $a^k \equiv 1 \pmod{n}$ can hold if and only if $k \,\%\, |a|_n = 0$.

2) The congruence $a^j \equiv a^k \pmod{n}$ is equivalent to $a^{j-k} \equiv 1 \pmod{n}$, and the result follows from (1).

3) The positive integer $|a^k|$ is the least x for which $a^{kx} \equiv 1 \pmod{n}$. This congruence is equivalent to $kx \equiv 0 \pmod{|a|}$ and to $x \equiv 0 \pmod{|a|/d}$, where $d = \gcd(k, |a|)$—according to (1) and Theorem 3.5, respectively. Hence, $|a^k| = |a|/d$ as claimed.

4) Suppose $\gcd(|a|, |b|) = 1$. The following congruence holds.

$$a^{|b|\,|ab|} = a^{|b|\,|ab|}(b^{|b|})^{|ab|} = (ab)^{|ab|\,|b|} \;\equiv\; 1 \pmod{n}$$

Then by (1) we have $|a| \mid |b|\,|ab|$ and in turn, by Euclid's lemma, $|a| \mid |ab|$. Now by symmetry $|b| \mid |ab|$, hence $|a|\,|b| \mid |ab|$ by Proposition 1.8(2). It is clear, however, that $|ab| \leq |a|\,|b|$, so it follows that $|ab| = |a|\,|b|$. ▽

EXERCISE 5.5. Show that $|2|_{F_n} = 2^{n+1}$ for the Fermat number $F_n = 2^{2^n} + 1$.

Primitive roots, described earlier, turn out to be exactly the integers whose orders equal $\phi(n)$. This distinguishing feature is now adopted as the formal definition of a primitive root, and we shall then demonstrate that the two descriptions are equivalent.

Definition. An integer g is called a *primitive root* modulo n if $|g|_n = \phi(n)$. For example, 3 is a primitive root modulo 7 because $|3|_7 = 6 = \phi(7)$.

EXERCISE 5.6. Is 13 a primitive root modulo 257?

As with order, the concept of primitive roots also extends to residue classes. Thus, g is a primitive root modulo n if and only if every integer in $[g]_n$ is too. Accordingly, we use the word *distinct* or *incongruent* primitive roots modulo n when we mean that they belong to different residue classes.

So, to search for a primitive root modulo n it suffices to look at a reduced residue system modulo n. For example, a reduced residue system modulo 8 is $\{1, 3, 5, 7\}$. None of these elements has order equals 4, where $\phi(8) = 4$. (See Exercise 3.1.) We conclude that primitive roots modulo 8 do not exist.

EXERCISE 5.7. Find all the primitive roots modulo n, if any.
a) $n = 6$
b) $n = 7$
c) $n = 9$
d) $n = 10$
e) $n = 12$

Proposition 5.2. The following statements are equivalent.

1) g is a primitive root modulo n.

2) $G = \{g, g^2, g^3, \ldots, g^{\phi(n)}\}$ is a reduced residue system modulo n.

3) $g^x \equiv c \pmod{n}$ has a solution whenever $\gcd(c, n) = 1$.

4) g^k is a primitive root modulo n whenever $\gcd(k, \phi(n)) = 1$.

Proof. Note that statements (1) and (4) are equivalent, as a special case of Proposition 5.1(3). We will complete the proof going (1) $\rightarrow$ (2) $\rightarrow$ (3) $\rightarrow$ (1).

It is clear that the exponents 1, 2, ... , $\phi(n)$ in G are all distinct modulo $\phi(n)$. So if $|g|_n = \phi(n)$ then, by Proposition 5.1(2), $g, g^2, \ldots, g^{\phi(n)}$ are all distinct modulo n, and G is a reduced residue system. As a consequence, the congruence $g^x \equiv c \pmod{n}$ finds a unique solution in $1 \leq x \leq \phi(n)$, provided that $\gcd(c, n) = 1$. More generally, if (3) holds then we can find a reduced residue system modulo n in the form $G' = \{g^{k_1}, g^{k_2}, \ldots, g^{k_{\phi(n)}}\}$. By Proposition 5.1(2), these exponents k_1, k_2, ... , $k_{\phi(n)}$ may be reduced mod $|g|_n$. But, as $|g|_n \leq \phi(n)$, the elements of G' would not be all distinct, unless $|g|_n = \phi(n)$. $\triangledown$

EXERCISE 5.8. If any exists, show that there are exactly $\phi(\phi(n))$ primitive roots modulo n.

EXERCISE 5.9. Find all the primitive roots modulo 37 among the numbers $2, 2^2, 2^3, \ldots, 2^{36}$, given that no two are congruent.

EXERCISE 5.10. Prove the following claims, where p denotes any odd prime.
a) If g is a primitive root modulo p then $g^{(p-1)/2} \equiv -1 \pmod{p}$.
b) The number 4 is not a primitive root modulo p.
c) The product of two primitive roots modulo p is not a primitive root.
d) If $p \,\%\, 4 = 1$, then g is a primitive root modulo p if and only if $-g$ is too.

5.2 The Existence of Primitive Roots

We have seen that primitive roots exist with some moduli, but not all of them. The main objective in this section is to prove that primitive roots exist for any prime modulus. For the general composite case, we will state the theorem but delay its proof to a later time.

Definition. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_rx^r$ be a polynomial with integer coefficients. We define the *degree* of $f(x)$ modulo n to be the largest exponent k for which $n \nmid a_k$. If no such k exists then we say that $f(x)$ is the *zero polynomial* modulo n, since then $f(c) \equiv 0 \pmod{n}$ for any integer c.

For example, the polynomial $14x^5 - 6x^2 + 35$ has degree 5 modulo 3, degree 0 modulo 2, and degree 2 modulo 7. For convenience, we will use the term *zero* of $f(x)$ modulo n, by which we mean a solution to the congruence $f(x) \equiv 0 \pmod{n}$.

Theorem 5.3. Every polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_kx^k$ of degree k, modulo a prime p, has at most k incongruent zeros.

Proof. The case $k = 0$ means that $f(c) \equiv a_0 \pmod{p}$ for all integers c, where $p \nmid a_0$. Accordingly, there cannot be a solution to $f(x) \equiv 0 \pmod{p}$.

By way of induction, assume that the theorem is true up to degree $k-1$, modulo p. Let $f(x) = a_0 + a_1x + \cdots + a_kx^k$ with $p \nmid a_k$. If $f(x)$ has less than k zeros, then there is nothing to prove. Else, let $r_1, r_2, \ldots, r_k$ be distinct zeros of $f(x)$ modulo p, and let

$$g(x) = f(x) - a_k(x - r_1)(x - r_2)\cdots(x - r_k)$$

Note that the degree of $g(x)$ modulo p is now less than k, and yet $g(x)$ claims all these k zeros of $f(x)$ as its own. By our induction hypothesis, this is impossible unless $g(x)$ is the zero polynomial modulo p. Thus,

$$f(x) \;\equiv\; a_k(x - r_1)(x - r_2)\cdots(x - r_k) \pmod{p}$$

and by Theorem 2.3, $f(x) \equiv 0 \pmod{p}$ if and only if $x \equiv r_i \pmod{p}$. This shows that $f(x)$ can have no more zeros other than these k. $\triangledown$

Corollary 5.4. If p is a prime number and $d \mid (p-1)$, then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions modulo p.

Proof. Let $p-1 = dk$ and $f(x) = (x^d)^{k-1} + (x^d)^{k-2} + \cdots + x^d + 1$. We have the following polynomial identity.

$$x^{p-1} - 1 = (x^d - 1)f(x)$$

By Fermat's little theorem, $x^{p-1} - 1$ has exactly $p - 1 = dk$ zeros modulo p, each of which must also be a zero of either $x^d - 1$ or $f(x)$, as p is prime. But, by Theorem 5.3, the latter two polynomials have no more than d and $dk - d$ zeros, respectively. The only way this can happen is when $x^d - 1$ has exactly d zeros, and $f(x)$ exactly $dk - d$, modulo p. $\triangledown$

At this point we are ready to present our goal of showing the existence of primitive roots modulo any prime. We even know their exact number.

Theorem 5.5. There are exactly $\phi(p-1)$ incongruent primitive roots modulo every prime p.

Proof. In view of Proposition 5.2(4), (see also Exercise 5.8) it suffices to show that at least one primitive root exists. Let $p - 1$ be factored into prime powers, written $p - 1 = \prod q_i^{e_i}$, with $e_i \geq 1$. By Corollary 5.4, for each $q^e = q_i^{e_i}$, there are exactly q^e zeros of $x^{q^e} - 1$ modulo p, all of which must have orders q^j modulo p, where $j \leq e$, according to Proposition 5.1(1). At least one of these zeros must have order q^e, because those with $j < e$ constitute the zeros of $x^{q^{e-1}} - 1$ modulo p—only q^{e-1} of them. (In fact, there will be $q^e - q^{e-1} = \phi(q^e)$ zeros of order q^e.) By Proposition 5.1(4), the product of integers of orders $q_i^{e_i}$ is of order $\prod q_i^{e_i} = p - 1$, i.e., a primitive root modulo p. $\triangledown$

EXERCISE 5.11. Count how many primitive roots modulo these primes.

a) $p = 11$
b) $p = 37$
c) $p = 89$
d) $p = 101$

EXERCISE 5.12. Show that there are exactly $\phi(d)$ incongruent integers of order d modulo p, whenever $d \mid (p-1)$.

The existence of primitive roots modulo a composite is dealt with by the following theorem, whose proof is set aside in Appendix C, as none of the subsequent results will be dependent upon it.

Theorem 5.6 (Primitive Root Theorem)**.** A primitive root modulo n exists if and only if $n = 1$, 2, 4, p^k, or $2p^k$, for any prime $p > 2$ and $k > 0$.

EXERCISE 5.13. Is there a primitive root modulo n? How many?

a) $n = 25$
b) $n = 50$
c) $n = 100$
d) $n = 1250$
e) $n = 19392$

EXERCISE 5.14. When we have primitive roots, prove that

$$\prod_{a \in G} a \equiv -1 \pmod{n}$$

where G is any reduced residue system modulo n. In particular, if n is a prime number, use this fact to prove again Wilson's theorem.

Concluding this section, the next result is actually the first step toward proving Theorem 5.6, but it is included here considering its usefulness in later chapters.

Proposition 5.7. Let g be a primitive root modulo a prime p. Then either g or $g + p$ is a primitive root modulo p^2.

Proof. Being in the same residue class, $g+p$ is another primitive root modulo p. Now if $g^{p-1} \equiv 1 \pmod{p^2}$ then, by the binomial theorem, (Theorem B.3)

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \not\equiv 1 \pmod{p^2}$$

Let $a = g$ or $g + p$, whichever gives $a^{p-1} \not\equiv 1 \pmod{p^2}$. Now the congruence $a^{|a|_{p^2}} \equiv 1 \pmod{p}$ implies that $|a|_{p^2}$ is a multiple of $p-1$. At the same time, $|a|_{p^2} \mid \phi(p^2) = p(p-1)$. The only way both claims can be true is when $|a|_{p^2} = p(p-1)$, and a is a primitive root modulo p^2. ▽

EXERCISE 5.15. Give an example of a primitive root modulo p which is not a primitive root modulo p^2.

Knowing exactly when a primitive root exists does not really help us in finding one. It remains open, for instance, to determine modulo which primes 2 is a primitive root.[1]

EXERCISE 5.16. Find three primes modulo which 2 is *not* a primitive root.

[1] There is a famous *Artin's conjecture,* which predicts that the number 2 is a primitive root modulo infinitely many primes, about one in every three. Up to 10,000, you can check this claim against the table of primes given in the unnumbered appendices.

5.3 Finding Discrete Logarithms

Suppose that, instead of computing $b = a^k \,\%\, n$, we are given b and asked to find the exponent k. In ordinary arithmetic, we would be computing the logarithm of b to the base a, that is, $k = \log_a b$. In modular arithmetic, however, this *discrete logarithm* problem is very difficult to solve, especially so when n is large.

For a relatively small modulus n, and with a known primitive root g, finding a discrete logarithm commonly involves a preconstructed table[2] of discrete logarithms base g, via a technique illustrated in the next example.

Example. Let us solve the congruence $5^x \equiv -1 \,(\mathrm{mod}\, 13)$. We choose $g = 2$, a primitive root modulo 13, and construct a reduced residue system modulo 13 represented by powers of 2. In general, this is made possible by Proposition 5.2(2). Next, we rewrite the congruence using only powers of 2. Here, $(2^9)^x \equiv 2^6 \,(\mathrm{mod}\, 13)$. This is equivalent, by Proposition 5.1(2), to the congruence $9x \equiv 6 \,(\mathrm{mod}\, 12)$. The linear congruence theorem takes it from here. We have $\gcd(9, 12) = 3$ and a particular solution $x_0 = 2$, hence the general solution given by the class $[2]_4$.

k	1	2	3	4	5	6	7	8	9	10	11	12
$2^k \,\%\, 13$	2	4	8	3	6	12	11	9	5	10	7	1

Table 5.1: Powers of 2, a primitive root, modulo 13.

EXERCISE 5.17. Solve the discrete logarithm problems, all modulo 13.

a) $6^x \equiv 9 \,(\mathrm{mod}\, 13)$
b) $9^x \equiv 6 \,(\mathrm{mod}\, 13)$
c) $10^x \equiv 3 \,(\mathrm{mod}\, 13)$
d) $11^x \equiv 7^x \,(\mathrm{mod}\, 13)$

EXERCISE 5.18. Use Table 5.1 to find all the solutions to $2^x \equiv x \,(\mathrm{mod}\, 13)$.

EXERCISE 5.19. Find a primitive root modulo 23 and use it, in a similar manner, to help solve the congruence $3^x \equiv 2 \,(\mathrm{mod}\, 23)$.

This technique of replacing the integer by its exponent, or *index*, with respect to a chosen primitive root, is named *index arithmetic*. With this method, we will be able to tackle some more root extraction problems. The next result along this line is somewhat a generalization of Theorem 4.9.

[2]In an analogous way, an extensive table of ordinary logarithms base 10 was made available in the old days before pocket calculators were invented.

Theorem 5.8. Suppose $\gcd(a, n) = 1$, and assume there exists a primitive root modulo n. Let $d = \gcd(k, \phi(n))$. Then the congruence $x^k \equiv a \pmod{n}$ has a solution if and only if $a^{\phi(n)/d} \equiv 1 \pmod{n}$, in which case there are exactly d distinct solutions modulo n.

Proof. Let g be a primitive root modulo n, and let $g^c \equiv a \pmod{n}$ for some $c \geq 0$. It suffices to seek a solution x in the reduced residue system $G = \{g, g^2, \ldots, g^{\phi(n)}\}$. By the substitution $x = g^y$, the three congruences

$$\begin{aligned} x^k &\equiv a \pmod{n} \\ g^{ky} &\equiv g^c \pmod{n} \\ ky &\equiv c \pmod{\phi(n)} \end{aligned}$$

can be shown equivalent one to another, and they have a solution if and only if $d \mid c$. In that case, by Theorem 3.5, the solution set is given by a unique y-value modulo $\phi(n)/d$, i.e., exactly d solutions for x in G.

To complete the proof, we will show that the condition $d \mid c$ is necessary and sufficient to have $a^{\phi(n)/d} \equiv g^{\phi(n)c/d} \equiv 1 \pmod{n}$. This last congruence, by Proposition 5.1(1), holds if and only if $|g|_n \mid \phi(n)c/d$—that is, if and only if c/d is an integer, since $|g|_n = \phi(n)$. ▽

Example. Consider the congruence $x^2 \equiv 3 \pmod{13}$. We have $\gcd(2, 12) = 2$, and we check that $3^{12/2} = 3^6 \equiv 1 \pmod{13}$, so we know a solution exists. Using Table 5.1, we obtain $2^{2y} \equiv 2^4 \pmod{13}$, and hence $2y \equiv 4 \pmod{12}$. The solution set for y is $[2]_6$, which gives two distinct solutions $x = 2^2$ and $x = 2^8$, corresponding to two residue classes $[4]_{13}$ and $[9]_{13}$, respectively.

Exercise 5.20. Solve each congruence, when possible.
a) $x^2 \equiv 10 \pmod{13}$
b) $x^9 \equiv 1 \pmod{13}$
c) $x^5 \equiv 3 \pmod{14}$
d) $x^4 \equiv 5 \pmod{17}$
e) $x^8 \equiv 16 \pmod{17}$

Exercise 5.21. Without solving it, count how many distinct solutions the congruence $x^{45} \equiv 53 \pmod{729}$ has, if any at all.

Corollary 5.9. Let p be a prime not dividing a, and let $d = \gcd(k, p-1)$. The congruence $x^k \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$, in which case it has exactly d incongruent solutions modulo p.

Proof. Primitive roots exist modulo any prime, so Theorem 5.8 applies. ▽

Exercise 5.22. For any odd prime p, prove that $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \,\%\, 4 = 1$. Similarly, show that $x^4 \equiv -1 \pmod{p}$ has a solution if and only if $p \,\%\, 8 = 1$.

5.4 Secret Key Exchange [Project 5]

For cryptological purposes, Alia and Bob need to establish a common secret key. However, the only available means of communication between them is the mobile phone, which they know is being tapped by the enemy. They resort to the *Diffie-Hellman key exchange* protocol [DH76] as follows.

Alia picks a large prime p, a primitive root g, and another number $m < p$. She gives to Bob, over the nonsecure line, the numbers p, g, and $a = g^m \,\%\, p$, but keeps m secret. In the next step, Bob selects a secret number $n < p$ and gives to Alia $b = g^n \,\%\, p$. They agree that their common secret key is $g^{mn} \,\%\, p$, which Alia obtains by computing $b^m \,\%\, p$ and Bob, independently, by $a^n \,\%\, p$. Both of them know the successive squaring algorithm.

If Cobra, the enemy, gathers this information—but not m and n for they are not transmitted across—then in order to capture the secret key, he will have to solve the congruence $g^x \equiv a \,(\mathrm{mod}\, p)$ from Alia's number, or alternately $g^x \equiv b \,(\mathrm{mod}\, p)$ from Bob's. But there is no efficient algorithm known for solving the discrete logarithm problem and, for large p, it is just not computationally feasible to do it by trial and error.

Project 5.4.1. For a small example, Alia sends to Bob the numbers $p = 8191$, $g = 3$, and $3^m \,\%\, 8191 = 8119$. Bob, in his turn, sends to Alia $3^n \,\%\, 8191 = 3731$.

a) Try your luck in finding m or n.
b) Could there be a way to find the secret key without knowing m or n?
c) Is it really necessary for g to be a primitive root modulo p?
d) What could go wrong if Cobra is aware of this protocol and he, with evil intent, is mediating the communication between Alia and Bob?

Project 5.4.2. The difficulty in solving the discrete logarithm problem can in fact be used to develop an algorithm for another public-key cryptosystem, by the name of *ElGamal encryption*. Write a paper on this subject.