Section 10. Primitive Roots

Note. In the previous section, Section 9. Euler's Theorem and Function we saw:

Theorem 9.1. Euler's Theorem. Suppose that $m \geq 1$ and $(a, m) = 1$. Then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Here $\varphi(m)$ is *Euler's φ-function* which is, for m is a positive integer, the number of positive integers less than or equal to m and relatively prime to m.

Note. If $(a, m) = 1$ then there is positive integer t such that $a^t \equiv 1 \pmod{m}$; namely, $t = \varphi(m)$. Of course there are infinitely many choices for t, since we could take $t = k\varphi(m)$ where k is any positive integer: $a^{k\varphi(m)} \equiv (a^{\varphi(m)})^k \equiv 1^k \equiv 1 \pmod{m}$. We are particularly interested in the smallest value of t such that $a^t \equiv 1 \pmod{m}$.

Definition. If $(a, m) = 1$ then the *order* of a modulo m is the smallest positive integer t such that $a^t \equiv 1 \pmod{m}$.

Note. Of course $a = 1$ is of order 1 for all m. When $a = m - 1$ we have $a^2 \equiv (m-1)^2 \equiv m^2 - 2m + 1 \equiv 1 \pmod{m}$ so that $a = m - 1$ has order 2. For $m = 7$ we have $\varphi(m) = \varphi(7) = 6$, and with $a = 2$ we have $a^3 \equiv 2^3 \equiv 1 \pmod{7}$ so that the order of 2 modulo 7 is 3. So there are ample examples that the order of a modulo m can be less than $\varphi(m)$. We will see below that if a is of order t modulo m then $t \mid \varphi(m)$; see Theorem 10.2. The next result shows that the only exponents on a that produce a product of 1 modulo m are multiples of the order of a (from which Theorem 10.2 will easily follow).

Theorem 10.1. Suppose that $(a, m) = 1$ and a has order t modulo m. Then $a^n \equiv 1 \pmod{m}$ if and only if n is a multiple of t.

Note. From Theorem 10.1, we easily get the following.

Theorem 10.2. If $(a, m) = 1$ and a has order $t \pmod{m}$, then $t \mid \varphi(m)$.

Exercise 10.2. What order can an integer have modulo 9? Find an example of each.

Solution. Since 1, 2, 4, 5, 7, 8 are relatively prime to 9, then $\varphi(9) = 6$. Since the divisors of $\varphi(9) = 6$ are 1, 2, 3, and 6, the possible orders by Theorem 10.2 are also $\boxed{\text{1, 2, 3, and 6}}$. By the definition of "order," we see that we only consider elements a that are relatively prime with 9. Element $a = 1$ is of order 1 modulo 9. Element $a = 2$ is of order 6 modulo 9 since $2^6 = 64 \equiv 1 \pmod{9}$. Element $a = 4$ is of order 3 modulo 9 since $4^3 = 64 \equiv 1 \pmod{9}$. Element $a = 5$ is of order 6 modulo 9 since $5^6 = 15{,}625 \equiv 1 \pmod{9}$. Element $a = 7$ is of order 3 modulo 9 since $7^3 = 343 \equiv 1 \pmod{9}$. Element $a = 8$ is of order 2 modulo 9 since $8^2 = 64 \equiv 1 \pmod{9}$. So an element of $\boxed{\text{order 1 is } a = 1}$, an element of $\boxed{\text{order 2 is } a = 8}$, elements of $\boxed{\text{order 3 are } a = 4 \text{ and } a = 7}$, and elements of $\boxed{\text{order 6 are } a = 2 \text{ and } a = 5}$. $\square$

Note. We now explore odd prime divisors of powers of a, minus 1.

Theorem 10.3. If p and q are odd primes and $q \mid a^p - 1$, then either $q \mid a - 1$ or $q = 2kp + 1$ for some integer k.

Note. With $a = 2$ (so that $a - 1 = 1$) in Theorem 10.3, we cannot have $q \mid a - 1$. So if $q \mid 2^p - 1$ then we must have that $q = 2kp + 1$ for some k. This is summarized in the next corollary.

Corollary 10.A. Any prime divisor of $2^p - 1$ is of the form $2kp + 1$ for some integer k.

Note. We now return to a consideration of powers of a.

Theorem 10.4. If the order of a modulo m is t, then $a^r \equiv a^s \pmod{m}$ if and only if $r \equiv s \pmod{t}$.

Definition. For $(a, m) = 1$, if a is a least residue and the order of a modulo m is $\varphi(m)$, then a is a *primitive root* of m.

Note. The next theorem lets us use primitive roots to generate the $\varphi(m)$ positive integers less than m that are relatively prime to m.

Theorem 10.5. If g is a primitive root of m, then the least residues modulo m of $g, g^2, g^3, \ldots, g^{\varphi(m)}$ are a permutation of the $\varphi(m)$ positive integers less than m and relatively prime to it.

Note. To illustrate Theorem 10.5, with $m = 9$ and $a = 2$ we have that a is a primitive root of m since $\varphi(9) = 6$ and $2^1 \equiv 2 \pmod{9}$, $2^2 \equiv 4 \pmod{9}$, $2^3 \equiv 8 \pmod{9}$, $2^4 \equiv 7 \pmod{9}$, $2^5 \equiv 5 \pmod{9}$, and $2^6 \equiv 1 \pmod{9}$. Now $2^1 \equiv 2 \pmod{9}$, $2^2 \equiv 4 \pmod{9}$, $2^3 \equiv 8 \pmod{9}$, $2^4 \equiv 7 \pmod{9}$, $2^5 \equiv 5$, and $2^6 \equiv 1$ and these are the positive integers less than $m = 9$ that are relatively prime to $m = 9$.

Note. Not every integer has a primitive root. For example, with $m = 8$ we have $\varphi(8) = 4$, but the order of $a = 1$ is 1, $a = 3$ has order 2 since $3^2 \equiv 1 \pmod{8}$, $a = 5$ has order 2 since $5^2 \equiv 1 \pmod{8}$, and $a = 7$ has order 2 since $7^2 \equiv 1 \pmod{8}$; remember, we only consider those numbers less than $m = 8$ and relatively prime to $m = 8$. Our next goal is to show that each prime number has a primitive root (see Theorem 10.6). The proof requires three lemmas and the existence of a primitive root of a prime is given, though a technique of finding the primitive root is not part of the proof. Dudley comments (see page 77): "For these reasons, you do not lose too much if you take the result on faith."

Lemma 10.1. Suppose that a has order t modulo m. Then a^k has order t modulo m if and only if $(k, t) = 1$.

Corollary 10.B. Suppose that g is a primitive root of prime p. Then the least residue of g^k is a primitive root of p if and only if $(k, p-1) = 1$.

Note. The next result is reminiscent of the Fundamental Theorem of Algebra (that is, an n degree polynomial with complex coefficients has exactly n zeros, counting multiplicity). However, in considering a polynomial *equivalence* with an n-degree polynomial, we do not get exactly n zeros but instead *at most* n zeros.

Lemma 10.2. If f is a polynomial of degree n, then $f(x) \equiv 0 \pmod{p}$ has at most n solutions.

Note. Lemma 10.2 does not hold if the modulus is not prime. For example, the equation $x^2 + x \equiv 0 \pmod{6}$ has more than $n = 2$ solutions, namely 0, 2, 3, and 5. This is because there are "zero divisors" modulo 6. Namely, $2 \cdot 3 \equiv 0 \pmod{6}$, yet neither 2 nor 3 is $0 \pmod{6}$. For more on zero divisors, see my online notes for Introduction to Modern Algebra (MATH 4127/5127) on Section IV.19. Integral Domains; notice Definition 19.2.

Lemma 10.3. If $d \,|\, p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Note. With Lemmas 10.1 to 10.3, we now have the equipment to prove that every prime number has a primitive root. In fact, we can also quantify the number of primitive roots.

Theorem 10.6. Every prime p has $\varphi(p-1)$ primitive roots.

Note. In the proof of Theorem 10.6, we introduced function $\psi(t)$ as the number of integers $1, 2, \ldots, p-1$ that have order t mod p. We showed that $\psi(t) = \varphi(t)$ for each t a divisor of $p-1$. Therefore, we have also proved the following.

Corollary 10.C. If p is a prime and $t \mid (p-1)$, then the number of least residues modulo p with order t is $\varphi(t)$.

Note. We know by Theorem 10.6 that every prime has a primitive root. It is reasonable to consider other values of m for which a primitive root mod m exist. Such m are classified in the Primitive Root Theorem. A (lengthy) proof of it can be found in Amin Witno's *Theory of Numbers* online book; see his Chapter 5 Primitive Roots.

Theorem 10.A. The Primitive Root Theorem.
Suppose $m \geq 2$. Then primitive roots mod m exist if and only if m is 2 or 4 or of the form p^α or $2p^\alpha$ for some odd prime p and some $\alpha \geq 1$. In particular, primitive roots mod p exist for every prime number p.

Note. Even though the Primitive Root Theorem lets us classify which numbers have primitive roots, it does not tell us how to find the primitive roots. Dudley comments (page 80): "No method is known for predicting what will be the smallest positive primitive root of a given prime p, nor is there much known about the distribution of the $\varphi(p-1)$ primitive roots among the least residues modulo p."

Note. Recall that Wilson's Theorem (Theorem 6.2) states: Positive integer p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$. We can use primitive roots to easily prove one of the implications of Wilson's Theorem

Theorem 10.B. If p is an odd prime then $(p-1)! \equiv -1 \pmod{p}$.

Revised: 3/6/2022