4

Primitive Roots and Quadratic Reciprocity

4.1 Primitive Roots

In this section the notion of primitive root is explored. Several examples are given that show how to find primitive roots, and we demonstrate their utility in solving congruence relations. Our main goal here is to classify which integers n have primitive roots.

Let n be a fixed positive integer. Let a be such that $\gcd(a, n) = 1$. By the Euler-Fermat Theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$. It is of interest to determine whether there is an $m < \phi(n)$ for which $a^m \equiv 1 \pmod{n}$. Definition 4.1 allows us to speak more precisely.

Definition 4.1: Let $\gcd(a, n) = 1$. The smallest positive integer m for which $a^m \equiv 1 \pmod{n}$ is the **order of a modulo n**, denoted $\text{ord}_n a$.

The next example is instructive and serves to demonstrate much of what will be proved in this section.

Example 4.1

(a) Let $n = 13$. One can readily verify that $\text{ord}_{13}1 = 1$, $\text{ord}_{13}12 = 2$, $\text{ord}_{13}3 = \text{ord}_{13}9 = 3$, $\text{ord}_{13}5 = \text{ord}_{13}8 = 4$, $\text{ord}_{13}4 = \text{ord}_{13}10 = 6$, and $\text{ord}_{13}2 = \text{ord}_{13}6 = \text{ord}_{13}7 = \text{ord}_{13}11 = 12$. Notice that $\phi(13) = 12$ and that $\text{ord}_{13}a \mid 12$ for all a. Furthermore, in this case for every $d \mid 12$ there is an a such that $\text{ord}_{13}a = d$.
(b) Let $n = 8$. Then $\text{ord}_8 1 = 1$ and $\text{ord}_8 3 = \text{ord}_8 5 = \text{ord}_8 7 = 2$. In this case, there is no a for which $\text{ord}_8 a = 4 = \phi(8)$.

Definition 4.2: Let $\gcd(g, n) = 1$. If $m = \phi(n)$ is the smallest integer for which $g^m \equiv 1 \pmod{n}$, then g is called a **primitive root modulo n**. Equivalently, g is a primitive root modulo n if $\text{ord}_n g = \phi(n)$.

Consequently, in Example 4.1, 2, 6, 7, and 11 are primitive roots modulo 13. On the other hand, there are no primitive roots modulo 8. Our next observation shows why primitive roots are considered so important.

Proposition 4.1: Let g be a primitive root modulo n. Then $g, g^2, \ldots, g^{\phi(n)}$ form a reduced residue system modulo n.

Proof: Since g is a primitive root modulo n, $\gcd(g, n) = 1$ and hence $\gcd(g^m, n) = 1$ for all $m \geq 1$. Suppose that $g^a \equiv g^b \pmod{n}$ with $a < b$. Then $n \mid (g^a - g^b)$. But $g^a - g^b = g^a(1 - g^{b-a})$. Hence $n \mid (1 - g^{b-a})$ by Corollary 2.1.1(b), so $g^{b-a} \equiv 1 \pmod{n}$. But since g is a primitive root, $b - a \geq \phi(n)$ and the result follows. ∎

Proposition 4.2 presents some of the basic results concerning the order of a modulo n. We will refer repeatedly to these results in our discussion of primality tests in Chapter 7.

Proposition 4.2: Let $\gcd(a, n) = 1$. Then

(a) $\text{ord}_n a$ divides $\phi(n)$.
(b) If $a^m \equiv 1 \pmod{n}$, then $\text{ord}_n a$ divides m.
(c) $\text{ord}_n(a^s) = \text{ord}_n a / \gcd(s, \text{ord}_n a)$.

Proof: Let $k = \text{ord}_n a$. Note that (b) implies (a) by the Euler-Fermat Theorem.

(b) By the division algorithm, $m = kq + r$ for some r satisfying $0 \leq r < k$. Thus

$$1 \equiv a^m = a^{kq+r} = (a^k)^q a^r \equiv 1^q a^r \equiv a^r \pmod{n}.$$

The minimality of k implies that $r = 0$. Hence $m = kq$ and $k \mid m$.

(c) Let $t = \gcd(s, k)$. By (b),

$(a^s)^u = a^{su} \equiv 1 \pmod{n}$ if and only if $k \mid su$. Thus

$(a^s)^u \equiv 1 \pmod{n}$ if and only if $\dfrac{k}{t} \,\Big|\, \dfrac{su}{t}$. But $\gcd(k/t, s/t) = 1$, so

$(a^s)^u \equiv 1 \pmod{n}$ if and only if $\dfrac{k}{t} \,\Big|\, u$.

Hence k/t is the least integer u for which $(a^s)^u \equiv 1 \pmod{n}$ by Proposition 1.3(e). That is, $\text{ord}_n(a^s) = \text{ord}_n a / \gcd(s, \text{ord}_n a)$. ∎

For example, refer to Example 4.1. If $n = 13$ and $a = 2$, then $\text{ord}_{13}2 = 12$. If $s = 3$, then Proposition 4.2(c) says that

$\text{ord}_{13}8 = \dfrac{\text{ord}_{13}2}{(3,\ \text{ord}_{13}2)} = 12/3 = 4$. Similarly, if $s = 4$, then

$$\text{ord}_{13}3 = \text{ord}_{13}16 = \frac{\text{ord}_{13}2}{(4,\ \text{ord}_{13}2)} = 12/4 = 3.$$

Corollary 4.2.1: Let p be prime and g be a primitive root modulo p. Then $g^i \equiv g^j \pmod p$ if and only if $i \equiv j \pmod{p-1}$.

Proof: Without loss of generality, suppose $i \geq j$. If $g^i \equiv g^j \pmod p$, then $g^{i-j} \equiv 1 \pmod p$. Proposition 4.2(b) implies that $(p-1) \mid (i-j)$, so $i \equiv j \pmod{p-1}$. On the other hand, if $i \equiv j \pmod{p-1}$, then $i = j + k(p-1)$ for some k. Then

$$g^i = g^j \cdot (g^{p-1})^k \equiv g^j \cdot 1^k \equiv g^j \pmod p. \blacksquare$$

Example 4.2

Solve the congruence $x^5 \equiv 7 \pmod{13}$.

Solution: We know that 2 is a primitive root modulo 13. The following table is useful.

Powers of 2 Modulo 13

a	0	1	2	3	4	5	6	7	8	9	10	11	12
2^a	1	2	4	8	3	6	12	11	9	5	10	7	1

We see from the table that $7 \equiv 2^{11} \pmod{13}$. We write $x^5 \equiv 2^{11} \pmod{13}$. If x is a solution, then $x \equiv 2^y$ for some y by Proposition 4.1. Hence $2^{5y} \equiv 2^{11} \pmod{13}$. By Corollary 4.2.1 it must be the case that $5y \equiv 11 \pmod{12}$. But $5^* \equiv 5 \pmod{12}$ and so $y \equiv 5^* \cdot 11 \equiv 55 \equiv 7 \pmod{12}$. Using the table again, $x = 2^7 \equiv 11 \pmod{13}$ is a solution.

The method used here is especially useful when the exponent or modulus is large.

Proposition 4.3: Let $a_1, a_2, \ldots, a_m$ be relatively prime to n. Let $\text{ord}_n a_i = k_i$ and suppose the k_i are pairwise relatively prime. Then

$$\text{ord}_n(a_1 a_2 \cdots a_m) = k_1 k_2 \cdots k_m. \blacksquare$$

Before proving Proposition 4.3, we first establish the following lemma.

Lemma 4.3.1: If $\gcd(a, n) = 1$, then $\text{ord}_n a = \text{ord}_n a^*$.

Proof: Let $k = \text{ord}_n a$ and $t = \text{ord}_n a^*$. Since $a^k \equiv 1 \pmod n$, it follows that

$$(a^*)^k = 1(a^*)^k \equiv a^k a^{*k} = (aa^*)^k \equiv 1^k \equiv 1 \pmod n.$$

By Proposition 4.2(b), $t \mid k$. Similarly, $(a^*)^t \equiv 1 \pmod n$ implies

$$a^t = 1(a^t) \equiv (a^*)^t a^t = (a^* a)^t \equiv 1^t \equiv 1 \pmod n.$$

Hence $k \mid t$. By Proposition 1.3(f), $k = t$. $\blacksquare$

Proof of Proposition 4.3: Certainly the proposition is trivially true when $m = 1$. Now assume that it is true for some m. Let $P = a_1 a_2 \cdots a_m$ and $Q = k_1 k_2 \cdots k_m$. We will demonstrate that the proposition holds for $m + 1$.

Let $\text{ord}_n a = k$ with $\gcd(k, Q) = 1$. We have $(Pa)^{Qk} = (P^Q)^k (a^k)^Q \equiv 1^k 1^Q \equiv 1 \pmod n$. By Proposition 4.2(b), $\text{ord}_n(Pa) \mid Qk$.

Let $\text{ord}_n(Pa) = t$. Then $1 \equiv (Pa)^t \equiv P^t a^t \pmod n$ and hence $a^t \equiv (P^t)^* \pmod n$. Lemma 4.3.1 implies that $\text{ord}_n a^t = \text{ord}_n P^t$.

Now Proposition 4.2(c) implies that $Q/\gcd(t, Q) = k/\gcd(t, k)$. Thus $Q \cdot \gcd(t, k) = k \cdot \gcd(t, Q)$. But $\gcd(k, Q) = 1$ and hence $k \mid \gcd(t, k)$ and $Q \mid \gcd(t, Q)$. Thus $k \mid t$ and $Q \mid t$. But then $Qk \mid t$ by Corollary 2.1.1(c). Combining this with the above, $\text{ord}_n(Pa) = Qk$ and the result follows by induction on m. $\blacksquare$

For a given prime p, finding a primitive root (mod p) requires some effort. As Gauss said, "Skillful mathematicians know how to reduce tedious calculations by a variety of devices, [but] experience is a better teacher than precept."

Example 4.3

Let us find a primitive root modulo 41. Here $\phi(41) = 40 = 2^3 \cdot 5$. We begin with the smallest candidate, 2. It must be the case that $\text{ord}_{41}2 \mid 40$ by Proposition 4.2(a). Successive doubling and reducing (mod 41) shows that the smallest exponent a for which $2^a \equiv -1 \pmod{41}$ is $a = 10$. It necessarily follows that $\text{ord}_{41}2 = 20$ since $(-1)^2 = 1$.

The next smallest candidate is 3. Since $a = 4$ is the smallest exponent for which $3^a \equiv -1 \pmod{41}$, $\text{ord}_{41}3 = 8$. But $\text{ord}_{41}2 = 20$ implies $\text{ord}_{41}16 = 5$ since $16 = 2^4$, so $a = 5$ is the smallest exponent for which $16^a \equiv 1 \pmod{41}$. Since $\gcd(5, 8) = 1$, we can apply Proposition 4.3, obtaining $\text{ord}_{41}48 = 40$. But $48 \equiv 7 \pmod{41}$, so 7 is a primitive root modulo 41.

We have been discussing $\text{ord}_n a$ for arbitrary n. Now we must specialize to the case where n is prime. Notice how Theorem 4.4 (proved by L. Poinsot, 1845) jibes with Example 4.1.

Theorem 4.4: Let p be prime and let $d \mid p - 1$. Then there exist $\phi(d)$ integers a modulo p for which $\text{ord}_p a = d$.

Proof: If $d = 1$, then $\phi(1) = 1$ and $a = 1$ is the only integer of order 1. So assume $d > 1$. Let $d = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$ be its canonical prime factorization. The crux of the matter is to demonstrate the existence of any integer a for which $\text{ord}_p a = d$. Counting the number of such a will then be an easy matter. To construct an integer a with $\text{ord}_p a = d$ it suffices to find integers $b_1, \ldots, b_t$ such that $\text{ord}_p b_i = p_i^{a_i}$ for all $i = 1, \ldots, t$; for then if $a = \prod_{i=1}^t b_i$, then $\text{ord}_p a = d$ by Proposition 4.3.

In order for b_i to be such that $\text{ord}_p b_i = p_i^{a_i}$, it must be the case that b_i is a solution to

$$x^{p_i^{a_i}} - 1 \equiv 0 \pmod p. \tag{4.1}$$

Furthermore, b_i must not be a solution to

$$x^{p_i^{a_i - 1}} - 1 \equiv 0 \pmod p. \tag{4.2}$$

In fact, these two conditions characterize those b_i for which $\text{ord}_p b_i = p_i^{a_i}$. To see this, notice that since b_i satisfies (4.1) it follows that $\text{ord}_p b_i | p_i^{a_i}$ by Proposition 4.2(b). But then $\text{ord}_p b_i = p_i^r$ for some $r \le a_i$. If $r \le a_i - 1$, then b_i would satisfy (4.2) by Proposition 4.2(b). Hence those b_i that satisfy (4.1) but do not satisfy (4.2) are precisely the b_i with $\text{ord}_p b_i = p_i^{a_i}$.

But by Corollary 2.19.1, there are $p_i^{a_i}$ solutions mod p to (4.1) and $p_i^{a_i-1}$ solutions mod p to (4.2). Further, all solutions of (4.2) are solutions of (4.1) since $p_i^{a_i-1} \mid p_i^{a_i}$. Thus there are exactly $p_i^{a_i} - p_i^{a_i-1} = \phi(p_i^{a_i})$ numbers $b_i \pmod p$ for which $\text{ord}_p b_i = p_i^{a_i}$.

Now apply Proposition 4.3 to obtain $\phi(d) = \prod_{i=1}^{t} \phi(p_i^{a_i})$ integers a modulo p with $\text{ord}_p a = d$. ∎

Corollary 4.4.1: If p is prime, then there are $\phi(\phi(p)) = \phi(p-1)$ primitive roots modulo p.

Proof: Let $d = p - 1$ in Proposition 4.4. ∎

For example, there are $\phi(18) = 6$ primitive roots (mod 19).

Our next three results answer the question, "For which values of n do there exist primitive roots modulo n?"

Proposition 4.5: If p is prime, then there are $(p-1)\phi(p-1)$ primitive roots modulo p^2.

Proof: If h is a primitive root (mod p^2), then h^k runs through a reduced residue system (mod p^2) by Proposition 4.1, and h^k is a primitive root if and only if $\gcd(k, p(p-1)) = 1$ by Proposition 4.2(c). But there are $\phi(p(p-1)) = (p-1)\phi(p-1)$ such k, so the result will follow once we establish the existence of any primitive root (mod p^2). In fact we will construct the primitive roots (mod p^2) fairly explicitly (given that we have found a primitive root modulo p).

By Corollary 4.4.1, it suffices to establish that if g is a primitive root (mod p), then $g + mp$ is a primitive root (mod p^2) for precisely $p - 1$ values of m (mod p). Now let $r = \text{ord}_{p^2}(g + mp)$. (Here r may be a function of m.) Since $(g+mp)^r \equiv 1 \pmod{p^2}$, it follows that $(g+mp)^r \equiv 1 \pmod p$. By the Binomial Theorem, $(g+mp)^r = g^r + p \cdot k$ for some integer k and hence $g^r \equiv 1 \pmod p$. But then $p - 1 \mid r$ by Proposition 4.2(b).

On the other hand, $r \mid \phi(p^2) = p(p-1)$ by Proposition 4.2(a). So either (i) $r = p-1$ or (ii) $r = p(p-1)$.

Now let $f(x) = x^{p-1} - 1$ and consider the congruence

$$f(x) \equiv 0 \pmod{p^2}. \tag{4.3}$$

In case (i), $g + mp$ is a solution of (4.3) lying above $g \pmod p$. But $f'(g) = (p-1)g^{p-2}$, so $f'(g) \not\equiv 0 \pmod p$. By Hensel's Lemma (nonsingular case) there is a unique $m \pmod p$ for which $x = g + mp$ satisfies (4.3).

So for all the other $p - 1$ values of $m \pmod p$, $h = g + mp$ does not satisfy (4.3) and hence case (ii) applies. But then $r = \text{ord}_{p^2}(g + mp) = \phi(p^2)$. Hence there are $(p-1)\phi(p-1)$ primitive roots modulo p^2. ∎

Proposition 4.6: If p is an odd prime and g is a primitive root modulo p^2, then g is a primitive root modulo p^a for all $a \ge 2$.

Proof: Let g be a primitive root modulo p^2 and let $r = \text{ord}_{p^a} g$ for some $a \ge 2$. Since $g^r \equiv 1 \pmod{p^a}$, it follows that $g^r \equiv 1 \pmod{p^2}$. Hence $\phi(p^2) = p(p-1) \mid r$ by Proposition 4.2(b). On the other hand, $r \mid \phi(p^a) = p^{a-1}(p-1)$ by Proposition 4.2(a). Thus $r = p^b(p-1)$ for some $b = 1, 2, \ldots, a-1$. It remains to show that in fact $b = a - 1$. It suffices to demonstrate that

$$g^s \not\equiv 1 \pmod{p^a} \quad \text{where} \quad s = p^{a-2}(p-1). \tag{4.4}$$

By Fermat's Little Theorem, $g^{p-1} \equiv 1 \pmod p$ and thus $g^{p-1} = 1 + cp$ where $p \nmid c$ (since g is a primitive root modulo p^2). The binomial theorem says $g^s = (1+cp)^{p^{a-2}(p-1)} = 1 + p^{a-1}c(p-1) + p^a k$ for some integer k. Hence $g^s \equiv 1 + p^{a-1}c(p-1) \pmod{p^a}$, so $g^s \not\equiv 1 \pmod{p^a}$ because $p \nmid c(p-1)$. Since a is arbitrary, this establishes (4.4) for all $a \ge 2$. ∎

Theorem 4.7 (Primitive Root Theorem): There exists a primitive root modulo n if and only if $n = 1, 2, 4, p^a$, or $2p^a$ for odd primes p. In addition, if n has a primitive root, then there are $\phi(\phi(n))$ primitive roots modulo n.

We begin by establishing a technical lemma. ∎

Lemma 4.7.1: If b is odd and $m \ge 3$, then $2m \mid b^r - 1$ where $r = 2^{m-2}$.

Proof: (Induction on m) Let $m = 3$. Then $r = 2$ and $b^2 - 1 = (b+1)(b-1)$. But b odd implies that either $b+1$ or $b-1$ is exactly divisible by 2 (being congruent to 2 mod 4) and the other must be divisible by 4. Hence $8 \mid b^2 - 1$.

Assume now that $2^m \mid b^r - 1$ where $r = 2^{m-2}$. But $b^{2r} - 1 = (b^r + 1)(b^r - 1)$. Since $b^r + 1$ is even, it follows that $2^{m+1} \mid b^{2r} - 1$. ∎

Proof of Theorem 4.7: The integers 1 and 2 have 1 as a primitive root and 3 is a primitive root (mod 4). As we saw in Example 4.1, there is no primitive root (mod 8). More generally, if $m \ge 3$ and b is odd, then $2^m \mid b^r - 1$ where $r = 2^{m-2}$ by Lemma 4.7.1. But $\phi(2^m) = 2^{m-1}$ and hence $b^{\phi(2^m)/2} \equiv 1 \pmod{2^m}$ for all odd b. So there are no primitive roots (mod 2^m) for $m \ge 3$.

Suppose p is an odd prime and g is a primitive root modulo p^a. We may assume that g is odd (if not, replace g by $g + p^a$). By Proposition 4.1, the integers $g, g^2, \ldots, g^{\phi(p^a)}$ form a reduced residue system (mod p^a). But they are all odd and $\phi(2p^a) = \phi(p^a)$. So $r = \phi(2p^a)$ is the smallest r for which $g^r \equiv 1 \pmod{2p^a}$. So all integers of the form $2p^a$ have primitive roots.

Now suppose that $n \ne p^a$ or $2p^a$ for any prime p. Then we can express n as $n = s \cdot t$ where $\gcd(s,t) = 1$ and $s > 2$ and $t > 2$. Let $c = \text{lcm}[\phi(s), \phi(t)]$. If $\gcd(b, n) = 1$, then $\gcd(b, s) = \gcd(b, t) = 1$. So $b^{\phi(s)} \equiv 1 \pmod s$ and $b^{\phi(t)} \equiv 1 \pmod t$. But $\phi(s) \mid c$ and $\phi(t) \mid c$. Hence $b^c \equiv 1 \pmod s$ and $b^c \equiv 1 \pmod t$. Since $\gcd(s,t) = 1$, $b^c \equiv 1 \pmod n$. Since $s > 2$ and $t > 2$, it must be the case that $\phi(s)$ and $\phi(t)$ are even. Hence $2 \mid \gcd(\phi(s), \phi(t))$. By Problem 10(a), Exercises 2.1, the product of two integers equals the product of their greatest common divisor and least common multiple.

Hence $c = \frac{\phi(s)\cdot\phi(t)}{\gcd(\phi(s),\phi(t))}$, so $c < \phi(s)\cdot\phi(t) = \phi(n)$. Therefore, there is no primitive root (mod n) in this case.

Hence the integers possessing primitive roots are precisely 1, 2, 4, p^a, and $2p^a$ for odd primes p.

To establish the latter assertion of the theorem, let g be a primitive root (mod n). By Proposition 4.1, $g, g^2, \ldots, g^{\phi(n)}$ form a reduced residue system (mod n). By Proposition 4.2(c), g^k is a primitive root if and only if $\gcd(k, \phi(n)) = 1$. But there are exactly $\phi(\phi(n))$ such k. ∎

The study of primitive roots has a long history. The term *primitive root* was coined by Euler in 1773 when he gave a defective proof that all primes have primitive roots. Such a claim was essentially given by Johann Lambert in 1769. The first correct proof was given by A. M. Legendre in 1785 based on Lagrange's Theorem (Corollary 2.19.1), much as in our proof of Theorem 4.4.

Gauss launched an extensive study of primitive roots in the *Disquisitiones Arithmeticae* (1801), including two new proofs of the existence of primitive roots (mod p) as well as introducing the notion of $\text{ord}_n a$. Most of the theorems in this section are due to Gauss, including Proposition 4.2 and Theorem 4.7.

If $a = -1$, then a is not a primitive root (mod p) for any prime $p > 3$. Similarly, if $a = n^2$ for some integer n, then $a^{(p-1)/2} \equiv 1 \pmod{p}$ and so a is not a primitive root for any prime $p > 2$. The Artin Conjecture states that all other integers a are primitive roots for infinitely many primes. In 1967, Christopher Hooley proved the Artin Conjecture subject to the truth of another yet unproven conjecture, the generalized Riemann Hypothesis. Since then, others have shown that substantially weaker hypotheses besides the generalized Riemann Hypothesis would suffice. However, an unconditional proof of the Artin Conjecture has not yet been effected.

Building on the work of Rajiv Gupta and Ram Murty, the best result to date is an amazing theorem of Roger Heath-Brown (1986) that utilizes difficult sieve techniques from analytic number theory. A consequence of Heath-Brown's work is that there are at most two primes and at most three positive square-free integers that are exceptions to the Artin Conjecture. Despite this, interestingly, no particular value of a has been proven to be a primitive root for infinitely many primes. However, Heath-Brown's result has tantalizing corollaries such as the following: At least two of the integers 2, 3, 5 are primitive roots for infinitely many primes.

A great deal of research has been done concerning algorithms for finding a primitive root modulo p for a given prime p, including an excellent algorithm of Gauss (Article 73 of the *Disquisitiones*). An open question of Erdös asks whether every sufficiently large prime p has a primitive root $q < p$ that is also prime. Much work remains to be done.

Exercises 4.1

1. Prove the converse of Proposition 4.1.
2. *(a)* Find all primitive roots modulo 11.
   (b) Find all primitive roots modulo 17.
3. *(a)* Find the smallest primitive root modulo 41.
   (b) Find the smallest primitive root modulo 47.
4. Let $p = 43$. For each $d \mid p-1$, determine how many integers a (mod p) have $\text{ord}_p a = d$.

5. *(a)* Verify Proposition 4.2 for $a = 7, n = 40, m = 20, s = 2$.
   (b) Verify Proposition 4.2 for $a = 3, n = 121, m = 20, s = 10$.
6. *(a)* Let g be a primitive root (mod p). Let $\gcd(a, p) = 1$ and $a \equiv g^s \pmod{p}$. Show that $\text{ord}_p a = \frac{p-1}{\gcd(s, p-1)}$.
   (b) Use the formula in (a) to compute $\text{ord}_{13} a$ for $a = 3$, 6, and 8.
7. *(a)* Verify Theorem 4.4 for all $d \mid p-1$ with $p = 17$.
   (b) Verify Theorem 4.4 for all $d \mid p-1$ with $p = 23$.
8. Determine how many primitive roots the following primes have:
   (a) $p = 29$ *(b)* $p = 73$ *(c)* $p = 107$ *(d)* $p = 337$ *(e)* $p = 9973$
9. Determine which of the following integers n have primitive roots. For those that do, determine how many distinct primitive roots (mod n) there are.
   (a) $n = 143$ *(b)* $n = 250$ *(c)* $n = 729$ *(d)* $n = 1372$
   (e) $n = 2662$ *(f)* $n = 11979$ *(g)* $n = 117649$ *(h)* $n = 156250$
10. *(a)* Solve $x^5 \equiv 6 \pmod{13}$.
    (b) Solve $x^4 \equiv 9 \pmod{13}$.
11. *(a)* Solve $x^6 \equiv -2 \pmod{17}$.
    (b) Solve $x^4 \equiv 4 \pmod{17}$.
12. *(a)* Solve $x^4 \equiv 5 \pmod{19}$.
    (b) Solve $x^3 \equiv 11 \pmod{19}$.
13. Solve $x^{17} \equiv 7 \pmod{29}$. [*Note:* 2 is a primitive root modulo 29.]
14. If $\text{ord}_n a = 12$, $\text{ord}_n b = 5$, and $\text{ord}_n c = 91$ where a, b, and c are pairwise relatively prime, then what is $\text{ord}_n abc$?
15. *(a)* Determine all primitive roots modulo p^2 where $p = 5$.
    (b) Determine all primitive roots modulo p^2 where $p = 7$. (Compare with Problem 27.)
16. Use Proposition 4.5 to determine how many primitive roots there are (mod p^2) for
    (a) $p = 5$ *(b)* $p = 11$ *(c)* $p = 73$ *(d)* $p = 1201$
17. What is the maximal order of a (mod 32)? How many a (mod 32) obtain this maximal order?
18. Where did we use the fact that p is odd in the proof of Proposition 4.6?
19. Use Proposition 4.1 to prove Wilson's Theorem.
20. Make use of the fact that $x \equiv x^{25} \pmod{13}$ to solve the congruence $x^5 \equiv 7 \pmod{13}$ in Example 4.2 more quickly.
21. If p is prime and $p \nmid a$, let g be a primitive root (mod p). Then there exists an i such that $a \equiv g^i \pmod{p}$ with $1 \le i \le p-1$. Following Gauss, call i the *index* of a with respect to g modulo p and write $i = \text{ind}\, a$. Show the following:
    (a) $\text{ind}\, ab \equiv \text{ind}\, a + \text{ind}\, b \pmod{p-1}$ for $p \nmid ab$.
    (b) $\text{ind}\, a^r \equiv r \cdot \text{ind}\, a \pmod{p-1}$ for $p \nmid a$.
22. Use Proposition 4.6 to show that 2 is a primitive root mod 5^n for all $n \ge 1$.
23. Let p be prime with $p \nmid a$ and set $A = \prod_{i=1}^{\text{ord}_p a} a^i$. Show that $A \equiv 1 \pmod{p}$ when $\text{ord}_p a$ is odd and $A \equiv -1 \pmod{p}$ when $\text{ord}_p a$ is even.
24. Prove the following generalization of Wilson's Theorem (Gauss, *Disquisitiones*, Art. 78): For any natural number n, the product of all the integers in a reduced residue system (mod n) is congruent to either $+1$ or -1 (mod n).
25. Let p be prime and $d \mid p-1$. Let g be a primitive root (mod p).
    (a) Show that if $a = g^{r(p-1)/d}$ where r is relatively prime to d, then $\text{ord}_p a = d$.
    (b) Explain how this leads to a constructive proof of Theorem 4.4.