One of the chief virtues of primitive roots lies in our next theorem.

THEOREM 8-4. *Let* $\gcd(a, n) = 1$ *and let* $a_1, a_2, \ldots, a_{\phi(n)}$ *be the positive integers less than n and relatively prime to n. If a is a primitive root of n, then*

$$a, a^2, \ldots, a^{\phi(n)}$$

are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$, *in some order.*

Proof: Since a is relatively prime to n, the same holds for all the powers of a; hence, each a^k is congruent modulo n to some one of the a_i. The $\phi(n)$ numbers in the set $\{a, a^2, \ldots, a^{\phi(n)}\}$ are incongruent by the corollary to Theorem 8-2, hence these powers must represent (not necessarily in order of appearance) the integers $a_1, a_2, \ldots, a_{\phi(n)}$.

One consequence of what has just been proved is that, in those cases in which a primitive root exists, we can now state exactly how many there are.

COROLLARY. *If n has a primitive root, then it has exactly* $\phi(\phi(n))$ *of them.*

Proof: Suppose that a is a primitive root of n. By the theorem, any other primitive root of n is found among the members of the set $\{a, a^2, \ldots, a^{\phi(n)}\}$. But the number of powers a^k, $1 \leq k \leq \phi(n)$, which have order $\phi(n)$ is equal to the number of integers k for which $\gcd(k, \phi(n)) = 1$; there are $\phi(\phi(n))$ such integers, hence $\phi(\phi(n))$ primitive roots of n.

Theorem 8-4 can be illustrated by taking $a = 2$ and $n = 9$. Since $\phi(9) = 6$, the first six powers of 2 must be congruent modulo 9, in some order, to the positive integers less than 9 and relatively prime to it. Now the integers less than and relatively prime to 9 are 1, 2, 4, 5, 7, 8 and we see that

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 7,\ 2^5 \equiv 5,\ 2^6 \equiv 1 \pmod{9}.$$

By virtue of the corollary, there are exactly $\phi(\phi(9)) = \phi(6) = 2$ primitive roots of 9, these being the integers 2 and 5.

PROBLEMS 8.1

1. Find the order of the integers 2, 3, and 5: (a) modulo 17, (b) modulo 19, and (c) modulo 23.

2. Establish each of the statements below:
(a) If a has order hk modulo n, then a^h has order k modulo n.
(b) If a has order $2k$ modulo the odd prime p, then $a^k \equiv -1 \pmod{p}$.
(c) If a has order $n-1$ modulo n, then n is a prime.

3. Prove that $\phi(2^n - 1)$ is a multiple of n for any $n > 1$. [*Hint:* The integer 2 has order n modulo $2^n - 1$.]

4. Assume that the order of a modulo n is h and the order of b modulo n is k. Show that the order of ab modulo n divides hk; in particular, if $\gcd(h, k) = 1$, then ab has order hk.

5. Given that a has order 3 modulo p, where p is an odd prime, show that $a+1$ must have order 6 modulo p. [*Hint:* Because $a^2+a+1 \equiv 0 \pmod{p}$, it follows that $(a+1)^2 \equiv a \pmod{p}$ and $(a+1)^3 \equiv -1 \pmod{p}$.]

6. Verify the following assertions:
(a) The odd prime divisors of the integer $n^2 + 1$ are of the form $4k + 1$. [*Hint:* $n^2 \equiv -1 \pmod{p}$, where p is an odd prime, implies that $4 \mid \phi(p)$ by Theorem 8-1.]
(b) The odd prime divisors of the integer $n^4 + 1$ are of the form $8k + 1$.
(c) The odd prime divisors of the integer $n^2 + n + 1$ which are different from 3 are of the form $6k + 1$.

7. Establish that there are infinitely many primes of each of the forms $4k + 1$, $6k + 1$, and $8k + 1$. [*Hint:* Assume that there are only finitely many primes of the form $4k + 1$; call them $p_1, p_2, \ldots, p_r$. Consider the integer $(2p_1 p_2 \cdots p_r)^2 + 1$ and apply the previous problem.]

8. (a) Prove that 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. [*Hint:* Since $a^p \equiv 1 \pmod{q}$, the order of a modulo q is either 1 or p; in the latter case, $p \mid \phi(q)$.]
(b) Use part (a) to show that if p is an odd prime, then the prime divisors of $2^p - 1$ are of the form $2kp + 1$.
(c) Find the smallest prime divisor of the integers $2^{17} - 1$ and $2^{29} - 1$.

9. Prove that there are infinitely many primes of the form $2kp + 1$, where p is an odd prime. [*Hint:* Assume that there are finitely many primes of the form $2kp + 1$, call them $q_1, q_2, \ldots, q_r$, and consider the integer $(q_1 q_2 \cdots q_r)^p - 1$.]

10. (a) Verify that 2 is a primitive root of 19, but not of 17.
(b) Show that 15 has no primitive root by calculating the orders of 2, 4, 7, 8, 11, 13, and 14 modulo 15.

11. Let r be a primitive root of the integer n. Prove that r^k is a primitive root of n if and only if $\gcd(k, \phi(n)) = 1$.

12. (a) Find two primitive roots of 10.
    (b) Use the information that 3 is a primitive root of 17 to obtain the eight primitive roots of 17.

8.2 PRIMITIVE ROOTS FOR PRIMES

Since primitive roots play a crucial role in many theoretical investigations, a problem exerting a natural appeal is that of describing all integers which possess primitive roots. We shall, over the course of the next few pages, prove the existence of primitive roots for all primes. Before doing this, let us turn aside briefly to establish a theorem dealing with the number of solutions of a polynomial congruence.

THEOREM 8-5 (Lagrange). *If p is a prime and*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \qquad a_n \not\equiv 0 \pmod{p}$$

is a polynomial of degree $n \geq 1$ with integral coefficients, then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n incongruent solutions modulo p.

Proof: We proceed by induction on n, the degree of $f(x)$. If $n = 1$, then our polynomial is of the form

$$f(x) = a_1 x + a_0.$$

Since $\gcd(a_1, p) = 1$, we know by Theorem 4-7 that the congruence $a_1 x \equiv -a_0 \pmod{p}$ has a unique solution modulo p. Thus, the theorem holds for $n = 1$.

Now assume inductively that the theorem is true for polynomials of degree $k - 1$ and consider the case in which $f(x)$ has degree k. Either $f(x) \equiv 0 \pmod{p}$ has no solutions (and we are finished) or it has at least one solution, call it a. If $f(x)$ is divided by $x - a$, the result is

$$f(x) = (x - a)q(x) + r,$$

in which $q(x)$ is a polynomial of degree $k-1$ with integral coefficients and r is an integer. Substituting $x = a$, we obtain

$$0 \equiv f(a) = (a-a)q(a) + r = r \pmod{p}$$

and so $f(x) \equiv (x-a)q(x) \pmod{p}$.

If b is another one of the incongruent solutions of $f(x) \equiv 0 \pmod{p}$, then

$$0 \equiv f(b) = (b-a)q(b) \pmod{p}.$$

Since $b - a \not\equiv 0 \pmod{p}$, this implies that $q(b) \equiv 0 \pmod{p}$; in other words, any solution of $f(x) \equiv 0 \pmod{p}$ which is different from a must satisfy $q(x) \equiv 0 \pmod{p}$. By our induction assumption, the latter congruence can possess at most $k-1$ incongruent solutions and so $f(x) \equiv 0 \pmod{p}$ will have no more than k incongruent solutions. This completes the induction step and the proof.

From this theorem, we can pass easily to

Corollary. *If p is a prime number and $d \mid p-1$, then the congruence*

$$x^d - 1 \equiv 0 \pmod{p}$$

has exactly d solutions.

Proof: Since $d \mid p-1$, we have $p-1 = dk$ for some k. Then

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

where the polynomial $f(x) = x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1$ has integral coefficients and is of degree $d(k-1) = p-1-d$. By Lagrange's Theorem, the congruence $f(x) \equiv 0 \pmod{p}$ has at most $p-1-d$ solutions. We also know from Fermat's Theorem that $x^{p-1} - 1 \equiv 0 \pmod{p}$ has precisely $p-1$ incongruent solutions; namely, the integers $1, 2, \ldots, p-1$.

Now any solution $x = a$ of $x^{p-1} - 1 \equiv 0 \pmod{p}$ that is not a solution of $f(x) \equiv 0 \pmod{p}$ must satisfy $x^d - 1 \equiv 0 \pmod{p}$. For

$$0 \equiv a^{p-1} - 1 = (a^d - 1)f(a) \pmod{p},$$

with $p \nmid f(a)$, implies that $p \mid a^d - 1$. It follows that $x^d - 1 \equiv 0 \pmod{p}$ must have at least

$$p - 1 - (p-1-d) = d$$