CHAPTER 8

PRIMITIVE ROOTS AND INDICES

... mathematical proofs, like diamonds, are hard as well as clear, and will be touched with nothing but strict reasoning.
JOHN LOCKE

8.1 THE ORDER OF AN INTEGER MODULO *n*

In view of Euler's theorem, we know that $a^{\phi(n)} \equiv 1 \pmod{n}$, whenever $\gcd(a, n) = 1$. However, there are often powers of a smaller than $a^{\phi(n)}$ that are congruent to 1 modulo n. This prompts the following definition.

Definition 8.1. Let $n > 1$ and $\gcd(a, n) = 1$. The *order of a modulo n* (in older terminology: the *exponent to which a belongs modulo n*) is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Consider the successive powers of 2 modulo 7. For this modulus, we obtain the congruences

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1, \ldots$$

from which it follows that the integer 2 has order 3 modulo 7.

Observe that if two integers are congruent modulo n, then they have the same order modulo n. For if $a \equiv b \pmod{n}$ and $a^k \equiv 1 \pmod{n}$, Theorem 4.2 implies that $a^k \equiv b^k \pmod{n}$, whence $b^k \equiv 1 \pmod{n}$.

It should be emphasized that our definition of order modulo n concerns only integers a for which $\gcd(a, n) = 1$. Indeed, if $\gcd(a, n) > 1$, then we know from

Theorem 4.7 that the linear congruence $ax \equiv 1 \pmod{n}$ has no solution; hence, the relation

$$a^k \equiv 1 \pmod{n} \qquad k \geq 1$$

cannot hold, for this would imply that $x = a^{k-1}$ is a solution of $ax \equiv 1 \pmod{n}$. Thus, whenever there is reference to the order of a modulo n, it is to be assumed that $\gcd(a, n) = 1$, even if it is not explicitly stated.

In the example given previously, we have $2^k \equiv 1 \pmod{7}$ whenever k is a multiple of 3, where 3 is the order of 2 modulo 7. Our first theorem shows that this is typical of the general situation.

Theorem 8.1. Let the integer a have order k modulo n. Then $a^h \equiv 1 \pmod{n}$ if and only if $k \mid h$; in particular, $k \mid \phi(n)$.

Proof. Suppose that we begin with $k \mid h$, so that $h = jk$ for some integer j. Because $a^k \equiv 1 \pmod{n}$, Theorem 4.2 yields $(a^k)^j \equiv 1^j \pmod{n}$ or $a^h \equiv 1 \pmod{n}$.

Conversely, let h be any positive integer satisfying $a^h \equiv 1 \pmod{n}$. By the Division Algorithm, there exist q and r such that $h = qk + r$, where $0 \leq r < k$. Consequently,

$$a^h = a^{qk+r} = (a^k)^q a^r$$

By hypothesis, both $a^h \equiv 1 \pmod{n}$ and $a^k \equiv 1 \pmod{n}$, the implication of which is that $a^r \equiv 1 \pmod{n}$. Because $0 \leq r < k$, we end up with $r = 0$; otherwise, the choice of k as the smallest positive integer such that $a^k \equiv 1 \pmod{n}$ is contradicted. Hence, $h = qk$, and $k \mid h$.

Theorem 8.1 expedites the computation when we attempt to find the order of an integer a modulo n; instead of considering all powers of a, the exponents can be restricted to the divisors of $\phi(n)$. Let us obtain, by way of illustration, the order of 2 modulo 13. Because $\phi(13) = 12$, the order of 2 must be one of the integers 1, 2, 3, 4, 6, 12. From

$$2^1 \equiv 2 \qquad 2^2 \equiv 4 \qquad 2^3 \equiv 8 \qquad 2^4 \equiv 3 \qquad 2^6 \equiv 12 \qquad 2^{12} \equiv 1 \pmod{13}$$

it is seen that 2 has order 12 modulo 13.

For an arbitrarily selected divisor d of $\phi(n)$, it is not always true that there exists an integer a having order d modulo n. An example is $n = 12$. Here $\phi(12) = 4$, yet there is no integer that is of order 4 modulo 12; indeed, we find that

$$1^1 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$$

and therefore the only choice for orders is 1 or 2.

Here is another basic fact regarding the order of an integer.

Theorem 8.2. If the integer a has order k modulo n, then $a^i \equiv a^j \pmod{n}$ if and only if $i \equiv j \pmod{k}$.

Proof. First, suppose that $a^i \equiv a^j \pmod{n}$, where $i \geq j$. Because a is relatively prime to n, we may cancel a power of a to obtain $a^{i-j} \equiv 1 \pmod{n}$. According to

Theorem 8.1, this last congruence holds only if $k \mid i - j$, which is just another way of saying that $i \equiv j \pmod{k}$.

Conversely, let $i \equiv j \pmod{k}$. Then we have $i = j + qk$ for some integer q. By the definition of k, $a^k \equiv 1 \pmod{n}$, so that

$$a^i \equiv a^{j+qk} \equiv a^j (a^k)^q \equiv a^j \pmod{n}$$

which is the desired conclusion.

Corollary. If a has order k modulo n, then the integers $a, a^2, \ldots, a^k$ are incongruent modulo n.

Proof. If $a^i \equiv a^j \pmod{n}$ for $1 \leq i \leq j \leq k$, then the theorem ensures that $i \equiv j \pmod{k}$. But this is impossible unless $i = j$.

A fairly natural question presents itself: Is it possible to express the order of any integral power of a in terms of the order of a? The answer is contained in Theorem 8.3.

Theorem 8.3. If the integer a has order k modulo n and $h > 0$, then a^h has order $k/\gcd(h, k)$ modulo n.

Proof. Let $d = \gcd(h, k)$. Then we may write $h = h_1 d$ and $k = k_1 d$, with $\gcd(h_1, k_1) = 1$. Clearly,

$$(a^h)^{k_1} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} \equiv 1 \pmod{n}$$

If a^h is assumed to have order r modulo n, then Theorem 8.1 asserts that $r \mid k_1$. On the other hand, because a has order k modulo n, the congruence

$$a^{hr} \equiv (a^h)^r \equiv 1 \pmod{n}$$

indicates that $k \mid hr$; in other words, $k_1 d \mid h_1 dr$ or $k_1 \mid h_1 r$. But $\gcd(k_1, h_1) = 1$, and therefore $k_1 \mid r$. This divisibility relation, when combined with the one obtained earlier, gives

$$r = k_1 = \frac{k}{d} = \frac{k}{\gcd(h, k)}$$

proving the theorem.

The preceding theorem has a corollary for which the reader may supply a proof.

Corollary. Let a have order k modulo n. Then a^h also has order k if and only if $\gcd(h, k) = 1$.

Let us see how all this works in a specific instance.

Example 8.1. The following table exhibits the orders modulo 13 of the positive integers less than 13:

Integer	1	2	3	4	5	6	7	8	9	10	11	12
Order	1	12	3	6	4	12	12	4	3	6	12	2

We observe that the order of 2 modulo 13 is 12, whereas the orders of 2^2 and 2^3 are 6 and 4, respectively; it is easy to verify that

$$6 = \frac{12}{\gcd(2, 12)} \qquad \text{and} \qquad 4 = \frac{12}{\gcd(3, 12)}$$

in accordance with Theorem 8.3. The integers that also have order 12 modulo 13 are powers 2^k for which $\gcd(k, 12) = 1$; namely,

$$2^1 \equiv 2 \qquad 2^5 \equiv 6 \qquad 2^7 \equiv 11 \qquad 2^{11} \equiv 7 \pmod{13}$$

If an integer a has the largest order possible, then we call it a primitive root of n.

Definition 8.2. If $\gcd(a, n) = 1$ and a is of order $\phi(n)$ modulo n, then a is a *primitive root* of the integer n.

To put it another way, n has a as a primitive root if $a^{\phi(n)} \equiv 1 \pmod{n}$, but $a^k \not\equiv 1 \pmod{n}$ for all positive integers $k < \phi(n)$.

It is easy to see that 3 is a primitive root of 7, for

$$3^1 \equiv 3 \qquad 3^2 \equiv 2 \qquad 3^3 \equiv 6 \qquad 3^4 \equiv 4 \qquad 3^5 \equiv 5 \qquad 3^6 \equiv 1 \pmod{7}$$

More generally, we can prove that primitive roots exist for any prime modulus, which is a result of fundamental importance. Although it is possible for a primitive root of n to exist when n is not a prime (for instance, 2 is a primitive root of 9), there is no reason to expect that every integer n possesses a primitive root; indeed, the existence of primitive roots is more often the exception than the rule.

Example 8.2. Let us show that if $F_n = 2^{2^n} + 1, n > 1$, is a prime, then 2 is not a primitive root of F_n. (Clearly, 2 is a primitive root of $5 = F_1$.) From the factorization $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$, we have

$$2^{2^{n+1}} \equiv 1 \pmod{F_n}$$

which implies that the order of 2 modulo F_n does not exceed 2^{n+1}. But if F_n is assumed to be prime, then

$$\phi(F_n) = F_n - 1 = 2^{2^n}$$

and a straightforward induction argument confirms that $2^{2^n} > 2^{n+1}$, whenever $n > 1$. Thus, the order of 2 modulo F_n is smaller than $\phi(F_n)$; referring to Definition 8.2, we see that 2 cannot be a primitive root of F_n.

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. Because 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; thus, 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, $1 \leq k \leq \phi(n)$, that 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 $n = 9$. Because $\phi(9) = 6$, 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

$$2^1 \equiv 2 \qquad 2^2 \equiv 4 \qquad 2^3 \equiv 8 \qquad 2^4 \equiv 7 \qquad 2^5 \equiv 5 \qquad 2^6 \equiv 1 \pmod 9$$

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.
   (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:* From $a^2 + a + 1 \equiv 0 \pmod p$, 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 $n^2 + n + 1$ that 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 $(2p_1p_2 \cdots p_r)^2 + 1$ 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 else $q = 2kp + 1$ for some integer k.
   [*Hint:* Because $a^p \equiv 1 \pmod{q}$, 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 divisors 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 $(2q_1q_2 \cdots q_r)^p - 1$.]
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.
13. (a) Prove that if p and $q > 3$ are both odd primes and $q \mid R_p$, then $q = 2kp + 1$ for some integer k.
    (b) Find the smallest prime divisors of the repunits $R_5 = 11111$ and $R_7 = 1111111$.
14. (a) Let $p > 5$ be prime. If R_n is the smallest repunit for which $p \mid R_n$, establish that $n \mid p - 1$. For example, R_8 is the smallest repunit divisible by 73, and $8 \mid 72$.
    [*Hint:* The order of 10 modulo p is n.]
    (b) Find the smallest R_n divisible by 13.

8.2 PRIMITIVE ROOTS FOR PRIMES

Because primitive roots play a crucial role in many theoretical investigations, a problem exerting a natural appeal is that of describing all integers that 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 Lagrange's theorem, which deals with the number of solutions of a polynomial congruence.

Theorem 8.5 Lagrange. If p is a prime and

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \qquad a_n \not\equiv 0 \pmod{p}$$

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

$$f(x) = a_1x + a_0$$

Because $\gcd(a_1, p) = 1$, Theorem 4.7 asserts 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 the congruence $f(x) \equiv 0 \pmod{p}$ 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 therefore $f(x) \equiv (x - a)q(x) \pmod{p}$.

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

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

Because $b - a \not\equiv 0 \pmod{p}$, we may cancel to conclude that $q(b) \equiv 0 \pmod{p}$; in other words, any solution of $f(x) \equiv 0 \pmod{p}$ that 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 therefore $f(x) \equiv 0 \pmod{p}$ has no more than k incongruent solutions. This completes the induction step and the proof.

From this theorem, we can pass easily to the corollary.

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. Because $d \mid p - 1$, 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 $x \equiv a \pmod{p}$ 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

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

solutions. This last congruence can possess no more than d solutions (Lagrange's theorem enters again) and, hence, has exactly d solutions.

We take immediate advantage of this corollary to prove Wilson's theorem in a different way: Given a prime p, define the polynomial $f(x)$ by

$$\begin{aligned} f(x) &= (x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1) \\ &= a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_1 x + a_0 \end{aligned}$$

which is of degree $p-2$. Fermat's theorem implies that the $p-1$ integers $1, 2, \ldots, p-1$ are incongruent solutions of the congruence

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

But this contradicts Lagrange's theorem, unless

$$a_{p-2} \equiv a_{p-3} \equiv \cdots \equiv a_1 \equiv a_0 \equiv 0 \pmod{p}$$

It follows that, for any choice of the integer x,

$$(x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \pmod{p}$$

Now substitute $x = 0$ to obtain

$$(-1)(-2)\cdots(-(p-1)) + 1 \equiv 0 \pmod{p}$$

or $(-1)^{p-1}(p-1)! + 1 \equiv 0 \pmod{p}$. Either $p-1$ is even or $p = 2$, in which case $-1 \equiv 1 \pmod{p}$; at any rate, we get

$$(p-1)! \equiv -1 \pmod{p}$$

Lagrange's theorem has provided us with the entering wedge. We are now in a position to prove that, for any prime p, there exist integers with order corresponding to each divisor of $p-1$. We state this more precisely in Theorem 8.6.

Theorem 8.6. If p is a prime number and $d \mid p-1$, then there are exactly $\phi(d)$ incongruent integers having order d modulo p.

Proof. Let $d \mid p-1$ and $\psi(d)$ denote the number of integers k, $1 \le k \le p-1$, that have order d modulo p. Because each integer between 1 and $p-1$ has order d for some $d \mid p-1$,

$$p-1 = \sum_{d \mid p-1} \psi(d)$$

At the same time, Gauss' theorem tells us that

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

and therefore, putting these together,

$$\sum_{d \mid p-1} \psi(d) = \sum_{d \mid p-1} \phi(d) \tag{1}$$

Our aim is to show that $\psi(d) \le \phi(d)$ for each divisor d of $p-1$, because this, in conjunction with Eq. (1), would produce the equality $\psi(d) = \phi(d) \ne 0$ (otherwise, the first sum would be strictly smaller than the second).

Given an arbitrary divisor d of $p-1$, there are two possibilities: We either have $\psi(d) = 0$ or $\psi(d) > 0$. If $\psi(d) = 0$, then certainly $\psi(d) \le \phi(d)$. Suppose that

$\psi(d) > 0$, so that there exists an integer a of order d. Then the d integers $a, a^2, \ldots, a^d$ are incongruent modulo p and each of them satisfies the polynomial congruence

$$x^d - 1 \equiv 0 \pmod{p} \tag{2}$$

for, $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{p}$. By the corollary to Lagrange's theorem, there can be no other solutions of Eq. (2). It follows that any integer having order d modulo p must be congruent to one of $a, a^2, \ldots, a^d$. But only $\phi(d)$ of the just-mentioned powers have order d, namely those a^k for which the exponent k has the property $\gcd(k, d) = 1$. Hence, in the present situation, $\psi(d) = \phi(d)$, and the number of integers having order d modulo p is equal to $\phi(d)$. This establishes the result we set out to prove.

Taking $d = p - 1$ in Theorem 8.6, we arrive at the following corollary.

Corollary. If p is a prime, then there are exactly $\phi(p - 1)$ incongruent primitive roots of p.

An illustration is afforded by the prime $p = 13$. For this modulus, 1 has order 1; 12 has order 2; 3 and 9 have order 3; 5 and 8 have order 4; 4 and 10 have order 6; and four integers, namely 2, 6, 7, 11, have order 12. Thus,

$$\begin{aligned}\sum_{d \mid 12} \psi(d) &= \psi(1) + \psi(2) + \psi(3) + \psi(4) + \psi(6) + \psi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 = 12\end{aligned}$$

as it should. Also notice that

$$\begin{aligned}\psi(1) &= 1 = \phi(1) & \psi(4) &= 2 = \phi(4) \\ \psi(2) &= 1 = \phi(2) & \psi(6) &= 2 = \phi(6) \\ \psi(3) &= 2 = \phi(3) & \psi(12) &= 4 = \phi(12)\end{aligned}$$

Incidentally, there is a shorter and more elegant way of proving that $\psi(d) = \phi(d)$ for each $d \mid p - 1$. We simply subject the formula $d = \sum_{c \mid d} \psi(c)$ to Möbius inversion to deduce that

$$\psi(d) = \sum_{c \mid d} \mu(c) \frac{d}{c}$$

In light of Theorem 7.8, the right-hand side of the foregoing equation is equal to $\phi(d)$. Of course, the validity of this argument rests upon using the corollary to Theorem 8.5 to show that $d = \sum_{c \mid d} \psi(c)$.

We can use this last theorem to give another proof of the fact that if p is a prime of the form $4k + 1$, then the quadratic congruence $x^2 \equiv -1 \pmod{p}$ admits a solution. Because $4 \mid p - 1$, Theorem 8.6 tells us that there is an integer a having order 4 modulo p; in other words,

$$a^4 \equiv 1 \pmod{p}$$

or equivalently,

$$(a^2 - 1)(a^2 + 1) \equiv 0 \pmod{p}$$

Because p is a prime, it follows that either

$$a^2 - 1 \equiv 0 \pmod{p} \qquad \text{or} \qquad a^2 + 1 \equiv 0 \pmod{p}$$

If the first congruence held, then a would have order less than or equal to 2, a contradiction. Hence, $a^2 + 1 \equiv 0 \pmod{p}$, making the integer a a solution to the congruence $x^2 \equiv -1 \pmod{p}$.

Theorem 8.6, as proved, has an obvious drawback; although it does indeed imply the existence of primitive roots for a given prime p, the proof is nonconstructive. To find a primitive root, we usually must either proceed by brute force or fall back on the extensive tables that have been constructed. The accompanying table lists the smallest positive primitive root for each prime below 200.

Prime	Least positive primitive root	Prime	Least positive primitive root
2	1	89	3
3	2	97	5
5	2	101	2
7	3	103	5
11	2	107	2
13	2	109	6
17	3	113	3
19	2	127	3
23	5	131	2
29	2	137	3
31	3	139	2
37	2	149	2
41	6	151	6
43	3	157	5
47	5	163	2
53	2	167	5
59	2	173	2
61	2	179	2
67	2	181	2
71	7	191	19
73	5	193	5
79	3	197	2
83	2	199	3

If $\chi(p)$ designates the smallest positive primitive root of the prime p, then the table presented shows that $\chi(p) \leq 19$ for all $p < 200$. In fact, $\chi(p)$ becomes arbitrarily large as p increases without bound. The table suggests, although the answer is not yet known, that there exist an infinite number of primes p for which $\chi(p) = 2$.

In most cases $\chi(p)$ is quite small. Among the first 19862 odd primes up to 223051, $\chi(p) \leq 6$ holds for about 80% of these primes; $\chi(p) = 2$ takes place for 7429 primes or approximately 37% of the time, whereas $\chi(p) = 3$ happens for 4515 primes, or 23% of the time.

In his *Disquisitiones Arithmeticae*, Gauss conjectured that there are infinitely many primes having 10 as a primitive root. In 1927, Emil Artin generalized this unresolved question as follows: For a not equal to 1, -1, or a perfect square, do there exist infinitely many primes having a as a primitive root? Although there is little doubt that this latter conjecture is true, it has yet to be proved. Recent work has shown that there are infinitely many a's for which Artin's conjecture is true, and at most two primes for which it fails.

The restrictions in Artin's conjecture are justified as follows. Let a be a perfect square, say $a = x^2$, and let p be an odd prime with $\gcd(a, p) = 1$. If $p \nmid x$, then Fermat's theorem yields $x^{p-1} \equiv 1 \pmod{p}$, whence

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv 1 \pmod{p}$$

Thus, a cannot serve as a primitive root of p [if $p \mid x$, then $p \mid a$ and surely $a^{p-1} \not\equiv 1 \pmod{p}$]. Furthermore, because $(-1)^2 = 1$, -1 is not a primitive root of p whenever $p - 1 > 2$.

Example 8.3. Let us employ the various techniques of this section to find the $\phi(6) = 2$ integers having order 6 modulo 31. To start, we know that there are

$$\phi(\phi(31)) = \phi(30) = 8$$

primitive roots of 31. Obtaining one of them is a matter of trial and error. Because $2^5 \equiv 1 \pmod{31}$, the integer 2 is clearly ruled out. We need not search too far, because 3 turns out to be a primitive root of 31. Observe that in computing the integral powers of 3 it is not necessary to go beyond 3^{15}; for the order of 3 must divide $\phi(31) = 30$ and the calculation

$$3^{15} \equiv (27)^5 \equiv (-4)^5 \equiv (-64)(16) \equiv -2(16) \equiv -1 \not\equiv 1 \pmod{31}$$

shows that its order is greater than 15.

Because 3 is a primitive root of 31, any integer that is relatively prime to 31 is congruent modulo 31 to an integer of the form 3^k, where $1 \leq k \leq 30$. Theorem 8.3 asserts that the order of 3^k is $30/\gcd(k, 30)$; this will equal 6 if and only if $\gcd(k, 30) = 5$. The values of k for which the last equality holds are $k = 5$ and $k = 25$. Thus our problem is now reduced to evaluating 3^5 and 3^{25} modulo 31. A simple calculation gives

$$3^5 \equiv (27)9 \equiv (-4)9 \equiv -36 \equiv 26 \pmod{31}$$
$$3^{25} \equiv (3^5)^5 \equiv (26)^5 \equiv (-5)^5 \equiv (-125)(25) \equiv -1(25) \equiv 6 \pmod{31}$$

so that 6 and 26 are the only integers having order 6 modulo 31.

PROBLEMS 8.2

1. If p is an odd prime, prove the following:
   (a) The only incongruent solutions of $x^2 \equiv 1 \pmod{p}$ are 1 and $p - 1$.
   (b) The congruence $x^{p-2} + \cdots + x^2 + x + 1 \equiv 0 \pmod{p}$ has exactly $p - 2$ incongruent solutions, and they are the integers $2, 3, \ldots, p - 1$.
2. Verify that each of the congruences $x^2 \equiv 1 \pmod{15}$, $x^2 \equiv -1 \pmod{65}$, and $x^2 \equiv -2 \pmod{33}$ has four incongruent solutions; hence, Lagrange's theorem need not hold if the modulus is a composite number.

3. Determine all the primitive roots of the primes $p = 11$, 19, and 23, expressing each as a power of some one of the roots.
4. Given that 3 is a primitive root of 43, find the following:
   (a) All positive integers less than 43 having order 6 modulo 43.
   (b) All positive integers less than 43 having order 21 modulo 43.
5. Find all positive integers less than 61 having order 4 modulo 61.
6. Assuming that r is a primitive root of the odd prime p, establish the following facts:
   (a) The congruence $r^{(p-1)/2} \equiv -1 \pmod{p}$ holds.
   (b) If r' is any other primitive root of p, then rr' is not a primitive root of p.
   [*Hint:* By part (a), $(rr')^{(p-1)/2} \equiv 1 \pmod{p}$.]
   (c) If the integer r' is such that $rr' \equiv 1 \pmod{p}$, then r' is a primitive root of p.
7. For a prime $p > 3$, prove that the primitive roots of p occur in incongruent pairs r, r' where $rr' \equiv 1 \pmod{p}$.
   [*Hint:* If r is a primitive root of p, consider the integer $r' = r^{p-2}$.]
8. Let r be a primitive root of the odd prime p. Prove the following:
   (a) If $p \equiv 1 \pmod{4}$, then $-r$ is also a primitive root of p.
   (b) If $p \equiv 3 \pmod{4}$, then $-r$ has order $(p-1)/2$ modulo p.
9. Give a different proof of Theorem 5.5 by showing that if r is a primitive root of the prime $p \equiv 1 \pmod{4}$, then $r^{(p-1)/4}$ satisfies the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$.
10. Use the fact that each prime p has a primitive root to give a different proof of Wilson's theorem.
    [*Hint:* If p has a primitive root r, then Theorem 8.4 implies that $(p-1)! \equiv r^{1+2+\cdots+(p-1)} \pmod{p}$.]
11. If p is a prime, show that the product of the $\phi(p-1)$ primitive roots of p is congruent modulo p to $(-1)^{\phi(p-1)}$.
    [*Hint:* If r is a primitive root of p, then the integer r^k is a primitive root of p provided that $\gcd(k, p-1) = 1$; now use Theorem 7.7.]
12. For an odd prime p, verify that the sum

$$1^n + 2^n + 3^n + \cdots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{if } (p-1) \nmid n \\ -1 \pmod{p} & \text{if } (p-1) \mid n \end{cases}$$

    [*Hint:* If $(p-1) \nmid n$, and r is a primitive root of p, then the indicated sum is congruent modulo p to

$$1 + r^n + r^{2n} + \cdots + r^{(p-2)n} = \frac{r^{(p-1)n} - 1}{r^n - 1}.]$$

8.3 COMPOSITE NUMBERS HAVING PRIMITIVE ROOTS

We saw earlier that 2 is a primitive root of 9, so that composite numbers can also possess primitive roots. The next step in our program is to determine all composite numbers for which there exist primitive roots. Some information is available in the following two negative results.

Theorem 8.7. For $k \geq 3$, the integer 2^k has no primitive roots.

Proof. For reasons that will become clear later, we start by showing that if a is an odd integer, then for $k \geq 3$

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}$$

If $k = 3$, this congruence becomes $a^2 \equiv 1 \pmod 8$, which is certainly true (indeed, $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$). For $k > 3$, we proceed by induction on k. Assume that the asserted congruence holds for the integer k; that is, $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. This is equivalent to the equation

$$a^{2^{k-2}} = 1 + b2^k$$

where b is an integer. Squaring both sides, we obtain

$$\begin{aligned} a^{2^{k-1}} = (a^{2^{k-2}})^2 &= 1 + 2(b2^k) + (b2^k)^2 \\ &= 1 + 2^{k+1}(b + b^2 2^{k-1}) \\ &\equiv 1 \pmod{2^{k+1}} \end{aligned}$$

so that the asserted congruence holds for $k + 1$ and, hence, for all $k \geq 3$.

Now the integers that are relatively prime to 2^k are precisely the odd integers, so that $\phi(2^k) = 2^{k-1}$. By what was just proved, if a is an odd integer and $k \geq 3$,

$$a^{\phi(2^k)/2} \equiv 1 \pmod{2^k}$$

and, consequently, there are no primitive roots of 2^k.

Another theorem in this same spirit is Theorem 8.8.

Theorem 8.8. If $\gcd(m, n) = 1$, where $m > 2$ and $n > 2$, then the integer mn has no primitive roots.

Proof. Consider any integer a for which $\gcd(a, mn) = 1$; then $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$. Put $h = \operatorname{lcm}(\phi(m), \phi(n))$ and $d = \gcd(\phi(m), \phi(n))$.

Because $\phi(m)$ and $\phi(n)$ are both even (Theorem 7.4), surely $d \geq 2$. In consequence,

$$h = \frac{\phi(m)\phi(n)}{d} \leq \frac{\phi(mn)}{2}$$

Now Euler's theorem asserts that $a^{\phi(m)} \equiv 1 \pmod m$. Raising this congruence to the $\phi(n)/d$ power, we get

$$a^h = (a^{\phi(m)})^{\phi(n)/d} \equiv 1^{\phi(n)/d} \equiv 1 \pmod m$$

Similar reasoning leads to $a^h \equiv 1 \pmod n$. Together with the hypothesis $\gcd(m, n) = 1$, these congruences force the conclusion that

$$a^h \equiv 1 \pmod{mn}$$

The point we wish to make is that the order of any integer relatively prime to mn does not exceed $\phi(mn)/2$, whence there can be no primitive roots for mn.

Some special cases of Theorem 8.8 are of particular interest, and we list these below.

Corollary. The integer n fails to have a primitive root if either

(a) n is divisible by two odd primes, or
(b) n is of the form $n = 2^m p^k$, where p is an odd prime and $m \geq 2$.

The significant feature of this last series of results is that it restricts our search for primitive roots to the integers 2, 4, p^k, and $2p^k$, where p is an odd prime. In this section, we prove that each of the numbers just mentioned has a primitive root, the major task being the establishment of the existence of primitive roots for powers of an odd prime. The argument is somewhat long-winded, but otherwise routine; for the sake of clarity, it is broken down into several steps.

Lemma 1. If p is an odd prime, then there exists a primitive root r of p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$.

Proof. From Theorem 8.6, it is known that p has primitive roots. Choose any one, call it r. If $r^{p-1} \not\equiv 1 \pmod{p^2}$, then we are finished. In the contrary case, replace r by $r' = r + p$, which is also a primitive root of p. Then employing the binomial theorem,

$$(r')^{p-1} \equiv (r+p)^{p-1} \equiv r^{p-1} + (p-1)pr^{p-2} \pmod{p^2}$$

But we have assumed that $r^{p-1} \equiv 1 \pmod{p^2}$; hence,

$$(r')^{p-1} \equiv 1 - pr^{p-2} \pmod{p^2}$$

Because r is a primitive root of p, $\gcd(r, p) = 1$, and therefore $p \nmid r^{p-2}$. The outcome of all this is that $(r')^{p-1} \not\equiv 1 \pmod{p^2}$, which proves the lemma.

Corollary. If p is an odd prime, then p^2 has a primitive root; in fact, for a primitive root r of p, either r or $r + p$ (or both) is a primitive root of p^2.

Proof. The assertion is almost obvious: If r is a primitive root of p, then the order of r modulo p^2 is either $p - 1$ or $p(p-1) = \phi(p^2)$. The foregoing proof shows that if r has order $p - 1$ modulo p^2, then $r + p$ is a primitive root of p^2.

As an illustration of this corollary, we observe that 3 is a primitive root of 7; and that both 3 and 10 are primitive roots of 7^2. Also, 14 is a primitive root of 29, but not of 29^2.

To reach our goal, another somewhat technical lemma is needed.

Lemma 2. Let p be an odd prime and let r be a primitive root of p with the property that $r^{p-1} \not\equiv 1 \pmod{p^2}$. Then for each positive integer $k \geq 2$,

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$$

Proof. The proof proceeds by induction on k. By hypothesis, the assertion holds for $k = 2$. Let us assume that it is true for some $k \geq 2$ and show that it is true for $k + 1$. Because $\gcd(r, p^{k-1}) = \gcd(r, p^k) = 1$, Euler's theorem indicates that

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}$$

Hence, there exists an integer a satisfying

$$r^{p^{k-2}(p-1)} = 1 + ap^{k-1}$$

where $p \nmid a$ by our induction hypothesis. Raise both sides of this last equation to the pth power and expand to obtain

$$r^{p^{k-1}(p-1)} = (1 + ap^{k-1})^p \equiv 1 + ap^k \pmod{p^{k+1}}$$

Because the integer a is not divisible by p, we have

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}}$$

This completes the induction step, thereby proving the lemma.

The hard work, for the moment, is over. We now stitch the pieces together to prove that the powers of any odd prime have a primitive root.

Theorem 8.9. If p is an odd prime number and $k \geq 1$, then there exists a primitive root for p^k.

Proof. The two lemmas allow us to choose a primitive root r of p for which $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$; in fact, any integer r satisfying the condition $r^{p-1} \not\equiv 1 \pmod{p^2}$ will do. We argue that such an r serves as a primitive root for all powers of p.

Let n be the order of r modulo p^k. In compliance with Theorem 8.1, n must divide $\phi(p^k) = p^{k-1}(p-1)$. Because $r^n \equiv 1 \pmod{p^k}$ yields $r^n \equiv 1 \pmod{p}$, we also have $p - 1 \mid n$ (Theorem 8.1 serves again). Consequently, n assumes the form $n = p^m(p-1)$, where $0 \leq m \leq k-1$. If it happened that $n \neq p^{k-1}(p-1)$, then $p^{k-2}(p-1)$ would be divisible by n and we would arrive at

$$r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$$

contradicting the way in which r was initially chosen. Therefore, $n = p^{k-1}(p-1)$ and r is a primitive root for p^k.

This leaves only the case $2p^k$ for our consideration.

Corollary. There are primitive roots for $2p^k$, where p is an odd prime and $k \geq 1$.

Proof. Let r be a primitive root for p^k. There is no harm in assuming that r is an odd integer; for, if it is even, then $r + p^k$ is odd and is still a primitive root for p^k. Then $\gcd(r, 2p^k) = 1$. The order n of r modulo $2p^k$ must divide

$$\phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k)$$

But $r^n \equiv 1 \pmod{2p^k}$ implies that $r^n \equiv 1 \pmod{p^k}$, and therefore $\phi(p^k) \mid n$. Together these divisibility conditions force $n = \phi(2p^k)$, making r a primitive root of $2p^k$.

The prime 5 has $\phi(4) = 2$ primitive roots, namely, the integers 2 and 3. Because

$$2^{5-1} \equiv 16 \not\equiv 1 \pmod{25} \qquad \text{and} \qquad 3^{5-1} \equiv 6 \not\equiv 1 \pmod{25}$$

these also serve as primitive roots for 5^2 and, hence, for all higher powers of 5. The proof of the last corollary guarantees that 3 is a primitive root for all numbers of the form $2 \cdot 5^k$.

In Theorem 8.10 we summarize what has been accomplished.

Theorem 8.10. An integer $n > 1$ has a primitive root if and only if

$$n = 2, 4, p^k, \text{ or } 2p^k$$

where p is an odd prime.

Proof. By virtue of Theorems 8.7 and 8.8, the only positive integers with primitive roots are those mentioned in the statement of our theorem. It may be checked that 1 is a primitive root for 2, and 3 is a primitive root of 4. We have just finished proving that primitive roots exist for any power of an odd prime and for twice such a power.

This seems the opportune moment to mention that Euler gave an essentially correct (although incomplete) proof in 1773 of the existence of primitive roots for any prime p and listed all the primitive roots for $p \leq 37$. Legendre, using Lagrange's theorem, managed to repair the deficiency and showed (1785) that there are $\phi(d)$ integers of order d for each $d \mid (p-1)$. The greatest advances in this direction were made by Gauss when, in 1801, he published a proof that there exist primitive roots of n if and only if $n = 2, 4, p^k$, and $2p^k$, where p is an odd prime.

PROBLEMS 8.3

1. (a) Find the four primitive roots of 26 and the eight primitive roots of 25.
(b) Determine all the primitive roots of 3^2, 3^3, and 3^4.

2. For an odd prime p, establish the following facts:
(a) There are as many primitive roots of $2p^n$ as of p^n.
(b) Any primitive root r of p^n is also a primitive root of p.
[*Hint:* Let r have order k modulo p. Show that $r^{pk} \equiv 1 \pmod{p^2}, \ldots, r^{p^{n-1}k} \equiv 1 \pmod{p^n}$ and, hence, $\phi(p^n) \mid p^{n-1}k$.]
(c) A primitive root of p^2 is also a primitive root of p^n for $n \geq 2$.

3. If r is a primitive root of p^2, p being an odd prime, show that the solutions of the congruence $x^{p-1} \equiv 1 \pmod{p^2}$ are precisely the integers $r^p, r^{2p}, \ldots, r^{(p-1)p}$.

4. (a) Prove that 3 is a primitive root of all integers of the form 7^k and $2 \cdot 7^k$.
(b) Find a primitive root for any integer of the form 17^k.

5. Obtain all the primitive roots of 41 and 82.

6. (a) Prove that a primitive root r of p^k, where p is an odd prime, is a primitive root of $2p^k$ if and only if r is an odd integer.
(b) Confirm that 3, 3^3, 3^5, and 3^9 are primitive roots of $578 = 2 \cdot 17^2$, but that 3^4 and 3^{17} are not.

7. Assume that r is a primitive root of the odd prime p and $(r+tp)^{p-1} \not\equiv 1 \pmod{p^2}$. Show that $r + tp$ is a primitive root of p^k for each $k \geq 1$.

8. If $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, define the *universal exponent* $\lambda(n)$ of n by

$$\lambda(n) = \operatorname{lcm}(\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$$

where $\lambda(2) = 1$, $\lambda(2^2) = 2$, and $\lambda(2^k) = 2^{k-2}$ for $k \geq 3$. Prove the following statements concerning the universal exponent:
(a) For $n = 2, 4, p^k, 2p^k$, where p is an odd prime, $\lambda(n) = \phi(n)$.
(b) If $\gcd(a, 2^k) = 1$, then $a^{\lambda(2^k)} \equiv 1 \pmod{2^k}$.
[*Hint:* For $k \geq 3$, use induction on k and the fact that $\lambda(2^{k+1}) = 2\lambda(2^k)$.]
(c) If $\gcd(a, n) = 1$, then $a^{\lambda(n)} \equiv 1 \pmod{n}$.
[*Hint:* For each prime power p^k occurring in n, $a^{\lambda(n)} \equiv 1 \pmod{p^k}$.]

9. Verify that, for $5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, $\lambda(5040) = 12$ and $\phi(5040) = 1152$.

10. Use Problem 8 to show that if $n \neq 2, 4, p^k, 2p^k$, where p is an odd prime, then n has no primitive root.
[*Hint:* Except for the cases 2, 4, p^k, $2p^k$, we have $\lambda(n) \mid \frac{1}{2}\phi(n)$; hence, $\gcd(a, n) = 1$ implies that $a^{\phi(n)/2} \equiv 1 \pmod{n}$.]

11. (a) Prove that if $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has the solution $x \equiv ba^{\lambda(n)-1} \pmod{n}$.
(b) Use part (a) to solve the congruences $13x \equiv 2 \pmod{40}$ and $3x \equiv 13 \pmod{77}$.

8.4 THE THEORY OF INDICES

The remainder of the chapter is concerned with a new idea, the concept of index. This was introduced by Gauss in his *Disquisitiones Arithmeticae*.

Let n be any integer that admits a primitive root r. As we know, the first $\phi(n)$ powers of r,

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

are congruent modulo n, in some order, to those integers less than n and relatively prime to it. Hence, if a is an arbitrary integer relatively prime to n, then a can be expressed in the form

$$a \equiv r^k \pmod{n}$$

for a suitable choice of k, where $1 \leq k \leq \phi(n)$. This allows us to frame the following definition.

Definition 8.3. Let r be a primitive root of n. If $\gcd(a, n) = 1$, then the smallest positive integer k such that $a \equiv r^k \pmod{n}$ is called the *index of a relative to r.*

Customarily, we denote the index of a relative to r by $\operatorname{ind}_r a$ or, if no confusion is likely to occur, by $\operatorname{ind} a$. Clearly, $1 \leq \operatorname{ind}_r a \leq \phi(n)$ and

$$r^{\operatorname{ind}_r a} \equiv a \pmod{n}$$

The notation $\operatorname{ind}_r a$ is meaningless unless $\gcd(a, n) = 1$; in the future, this will be tacitly assumed.

For example, the integer 2 is a primitive root of 5 and

$$2^1 \equiv 2 \qquad 2^2 \equiv 4 \qquad 2^3 \equiv 3 \qquad 2^4 \equiv 1 \pmod{5}$$

It follows that

$$\operatorname{ind}_2 1 = 4 \qquad \operatorname{ind}_2 2 = 1 \qquad \operatorname{ind}_2 3 = 3 \qquad \operatorname{ind}_2 4 = 2$$

Observe that indices of integers that are congruent modulo n are equal. Thus, when setting up tables of values for $\operatorname{ind} a$, it suffices to consider only those integers a less than and relatively prime to the modulus n. To see this, let $a \equiv b \pmod{n}$, where a and b are taken to be relatively prime to n. Because $r^{\operatorname{ind} a} \equiv a \pmod{n}$ and $r^{\operatorname{ind} b} \equiv b \pmod{n}$, we have

$$r^{\operatorname{ind} a} \equiv r^{\operatorname{ind} b} \pmod{n}$$

Invoking Theorem 8.2, it may be concluded that ind $a \equiv$ ind $b \pmod{\phi(n)}$. But, because of the restrictions on the size of ind a and ind b, this is only possible when ind $a =$ ind b.

Indices obey rules that are reminiscent of those for logarithms, with the primitive root playing a role analogous to that of the base for the logarithm.

Theorem 8.11. If n has a primitive root r and ind a denotes the index of a relative to r, then the following properties hold:

(a) ind $(ab) \equiv$ ind $a +$ ind $b \pmod{\phi(n)}$.
(b) ind $a^k \equiv k$ ind $a \pmod{\phi(n)}$ for $k > 0$.
(c) ind $1 \equiv 0 \pmod{\phi(n)}$, ind $r \equiv 1 \pmod{\phi(n)}$.

Proof. By the definition of index, $r^{\text{ind}\, a} \equiv a \pmod{n}$ and $r^{\text{ind}\, b} \equiv b \pmod{n}$. Multiplying these congruences together, we obtain

$$r^{\text{ind}\, a + \text{ind}\, b} \equiv ab \pmod{n}$$

But $r^{\text{ind}(ab)} \equiv ab \pmod{n}$, so that

$$r^{\text{ind}\, a + \text{ind}\, b} \equiv r^{\text{ind}(ab)} \pmod{n}$$

It may very well happen that ind $a +$ ind b exceeds $\phi(n)$. This presents no problem, for Theorem 8.2 guarantees that the last equation holds if and only if the exponents are congruent modulo $\phi(n)$; that is,

$$\text{ind}\, a + \text{ind}\, b \equiv \text{ind}\, (ab) \pmod{\phi(n)}$$

which is property (a).

The proof of property (b) proceeds along much the same lines. For we have $r^{\text{ind}\, a^k} \equiv a^k \pmod{n}$, and by the laws of exponents, $r^{k\, \text{ind}\, a} = (r^{\text{ind}\, a})^k \equiv a^k \pmod{n}$; hence,

$$r^{\text{ind}\, a^k} \equiv r^{k\, \text{ind}\, a} \pmod{n}$$

As above, the implication is that ind $a^k \equiv k$ ind $a \pmod{\phi(n)}$. The two parts of property (c) should be fairly apparent.

The theory of indices can be used to solve certain types of congruences. For instance, consider the binomial congruence

$$x^k \equiv a \pmod{n} \qquad k \geq 2$$

where n is a positive integer having a primitive root and $\gcd(a, n) = 1$. By properties (a) and (b) of Theorem 8.11, this congruence is entirely equivalent to the linear congruence

$$k \text{ ind } x \equiv \text{ ind } a \pmod{\phi(n)}$$

in the unknown ind x. If $d = \gcd(k, \phi(n))$ and $d \nmid$ ind a, there is no solution. But, if $d \mid$ ind a, then there are exactly d values of ind x that will satisfy this last congruence; hence, there are d incongruent solutions of $x^k \equiv a \pmod{n}$.

The case in which $k = 2$ and $n = p$, with p an odd prime, is particularly important. Because $\gcd(2, p - 1) = 2$, the foregoing remarks imply that the quadratic

congruence $x^2 \equiv a \pmod{p}$ has a solution if and only if $2 \mid \operatorname{ind} a$; when this condition is fulfilled, there are exactly two solutions. If r is a primitive root of p, then $r^k (1 \leq k \leq p-1)$ runs modulo p through the integers $1, 2, \ldots, p-1$, in some order. The even powers of r produce the values of a for which the congruence $x^2 \equiv a \pmod{p}$ is solvable; there are precisely $(p-1)/2$ such choices for a.

Example 8.4. For an illustration of these ideas, let us solve the congruence

$$4x^9 \equiv 7 \pmod{13}$$

A table of indices can be constructed once a primitive root of 13 is fixed. Using the primitive root 2, we simply calculate the powers $2, 2^2, \ldots, 2^{12}$ modulo 13. Here,

$$\begin{array}{lll} 2^1 \equiv 2 & 2^5 \equiv 6 & 2^9 \equiv 5 \\ 2^2 \equiv 4 & 2^6 \equiv 12 & 2^{10} \equiv 10 \\ 2^3 \equiv 8 & 2^7 \equiv 11 & 2^{11} \equiv 7 \\ 2^4 \equiv 3 & 2^8 \equiv 9 & 2^{12} \equiv 1 \end{array}$$

all congruences being modulo 13; hence, our table is

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_2 a$	12	1	4	2	9	5	11	3	8	10	7	6

Taking indices, the congruence $4x^9 \equiv 7 \pmod{13}$ has a solution if and only if

$$\operatorname{ind}_2 4 + 9 \operatorname{ind}_2 x \equiv \operatorname{ind}_2 7 \pmod{12}$$

The table gives the values $\operatorname{ind}_2 4 = 2$ and $\operatorname{ind}_2 7 = 11$, so that the last congruence becomes $9 \operatorname{ind}_2 x \equiv 11 - 2 \equiv 9 \pmod{12}$ which, in turn, is equivalent to having $\operatorname{ind}_2 x \equiv 1 \pmod{4}$. It follows that

$$\operatorname{ind}_2 x = 1, 5, \text{ or } 9$$

Consulting the table of indices once again, we find that the original congruence $4x^9 \equiv 7 \pmod{13}$ possesses the three solutions

$$x \equiv 2, 5, \text{ and } 6 \pmod{13}$$

If a different primitive root is chosen, we obviously obtain a different value for the index of a; but, for purposes of solving the given congruence, it does not really matter which index table is available. The $\phi(\phi(13)) = 4$ primitive roots of 13 are obtained from the powers $2^k (1 \leq k \leq 12)$, where

$$\gcd(k, \phi(13)) = \gcd(k, 12) = 1$$

These are

$$2^1 \equiv 2 \qquad 2^5 \equiv 6 \qquad 2^7 \equiv 11 \qquad 2^{11} \equiv 7 \pmod{13}$$

The index table for, say, the primitive root 6 is displayed below:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_6 a$	12	5	8	10	9	1	7	3	4	2	11	6

Employing this table, the congruence $4x^9 \equiv 7 \pmod{13}$ is replaced by

$$\text{ind}_6\, 4 + 9\, \text{ind}_6\, x \equiv \text{ind}_6\, 7 \pmod{12}$$

or, rather,

$$9\, \text{ind}_6\, x \equiv 7 - 10 \equiv -3 \equiv 9 \pmod{12}$$

Thus, $\text{ind}_6\, x = 1, 5$, or 9, leading to the solutions

$$x \equiv 2, 5, \text{ and } 6 \pmod{13}$$

as before.

The following criterion for solvability is often useful.

Theorem 8.12. Let n be an integer possessing a primitive root and let $\gcd(a, n) = 1$. Then the congruence $x^k \equiv a \pmod{n}$ has a solution if and only if

$$a^{\phi(n)/d} \equiv 1 \pmod{n}$$

where $d = \gcd(k, \phi(n))$; if it has a solution, there are exactly d solutions modulo n.

Proof. Taking indices, the congruence $a^{\phi(n)/d} \equiv 1 \pmod{n}$ is equivalent to

$$\frac{\phi(n)}{d} \text{ ind } a \equiv 0 \pmod{\phi(n)}$$

which, in turn, holds if and only if $d \mid \text{ind } a$. But we have just seen that the latter is a necessary and sufficient condition for the congruence $x^k \equiv a \pmod{n}$ to be solvable.

Corollary. Let p be a prime and $\gcd(a, p) = 1$. Then the congruence $x^k \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$, where $d = \gcd(k, p - 1)$.

Example 8.5. Let us consider the congruence

$$x^3 \equiv 4 \pmod{13}$$

In this setting, $d = \gcd(3, \phi(13)) = \gcd(3, 12) = 3$, and therefore $\phi(13)/d = 4$. Because $4^4 \equiv 9 \not\equiv 1 \pmod{13}$, Theorem 8.12 asserts that the given congruence is not solvable.

On the other hand, the same theorem guarantees that

$$x^3 \equiv 5 \pmod{13}$$

possesses a solution (in fact, there are three incongruent solutions modulo 13); for, in this case, $5^4 \equiv 625 \equiv 1 \pmod{13}$. These solutions can be found by means of the index calculus as follows: The congruence $x^3 \equiv 5 \pmod{13}$ is equivalent to

$$3\, \text{ind}_2\, x \equiv 9 \pmod{12}$$

which becomes

$$\text{ind}_2\, x \equiv 3 \pmod{4}$$

This last congruence admits three incongruent solutions modulo 12, namely,

$$\text{ind}_2\, x = 3, 7, \text{ or } 11$$

The integers corresponding to these indices are, respectively, 8, 11, and 7, so that the solutions of the congruence $x^3 \equiv 5 \pmod{13}$ are

$$x \equiv 7, 8, \text{ and } 11 \pmod{13}$$

PROBLEMS 8.4

1. Find the index of 5 relative to each of the primitive roots of 13.
2. Using a table of indices for a primitive root of 11, solve the following congruences:
   (a) $7x^3 \equiv 3 \pmod{11}$.
   (b) $3x^4 \equiv 5 \pmod{11}$.
   (c) $x^8 \equiv 10 \pmod{11}$.
3. The following is a table of indices for the prime 17 relative to the primitive root 3:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3\, a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

   With the aid of this table, solve the following congruences:
   (a) $x^{12} \equiv 13 \pmod{17}$.
   (b) $8x^5 \equiv 10 \pmod{17}$.
   (c) $9x^8 \equiv 8 \pmod{17}$.
   (d) $7^x \equiv 7 \pmod{17}$.
4. Find the remainder when $3^{24} \cdot 5^{13}$ is divided by 17.
   [*Hint:* Use the theory of indices.]
5. If r and r' are both primitive roots of the odd prime p, show that for $\gcd(a, p) = 1$

$$\text{ind}_{r'}\, a \equiv (\text{ind}_r\, a)(\text{ind}_{r'}\, r) \pmod{p-1}$$

   This corresponds to the rule for changing the base of logarithms.
6. (a) Construct a table of indices for the prime 17 with respect to the primitive root 5.
   [*Hint:* By the previous problem, $\text{ind}_5\, a \equiv 13\, \text{ind}_3\, a \pmod{16}$.]
   (b) Solve the congruences in Problem 3, using the table in part (a).
7. If r is a primitive root of the odd prime p, verify that

$$\text{ind}_r\, (-1) = \text{ind}_r\, (p-1) = \frac{1}{2}(p-1)$$

8. (a) Determine the integers $a (1 \leq a \leq 12)$ such that the congruence $ax^4 \equiv b \pmod{13}$ has a solution for $b = 2$, 5, and 6.
   (b) Determine the integers $a (1 \leq a \leq p-1)$ such that the congruence $x^4 \equiv a \pmod{p}$ has a solution for $p = 7$, 11, and 13.
9. Employ the corollary to Theorem 8.12 to establish that if p is an odd prime, then
   (a) $x^2 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{4}$.
   (b) $x^4 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{8}$.
10. Given the congruence $x^3 \equiv a \pmod{p}$, where $p \geq 5$ is a prime and $\gcd(a, p) = 1$, prove the following:
   (a) If $p \equiv 1 \pmod{6}$, then the congruence has either no solutions or three incongruent solutions modulo p.
   (b) If $p \equiv 5 \pmod{6}$, then the congruence has a unique solution modulo p.
11. Show that the congruence $x^3 \equiv 3 \pmod{19}$ has no solutions, whereas $x^3 \equiv 11 \pmod{19}$ has three incongruent solutions.

12. Determine whether the two congruences $x^5 \equiv 13 \pmod{23}$ and $x^7 \equiv 15 \pmod{29}$ are solvable.

13. If p is a prime and $\gcd(k, p-1) = 1$, prove that the integers

$$1^k, 2^k, 3^k, \ldots, (p-1)^k$$

form a reduced set of residues modulo p.

14. Let r be a primitive root of the odd prime p, and let $d = \gcd(k, p-1)$. Prove that the values of a for which the congruence $x^k \equiv a \pmod{p}$ is solvable are $r^d, r^{2d}, \ldots, r^{[(p-1)/d]d}$.

15. If r is a primitive root of the odd prime p, show that

$$\operatorname{ind}_r (p-a) \equiv \operatorname{ind}_r a + \frac{(p-1)}{2} \pmod{p-1}$$

and, consequently, that only half of an index table need be calculated to complete the table.

16. (a) Let r be a primitive root of the odd prime p. Establish that the exponential congruence

$$a^x \equiv b \pmod{p}$$

has a solution if and only if $d \mid \operatorname{ind}_r b$, where the integer $d = \gcd(\operatorname{ind}_r a, p-1)$; in this case, there are d incongruent solutions modulo $p-1$.

(b) Solve the exponential congruences $4^x \equiv 13 \pmod{17}$ and $5^x \equiv 4 \pmod{19}$.

17. For which values of b is the exponential congruence $9^x \equiv b \pmod{13}$ solvable?