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

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

Since r is a primitive root of p, $\gcd(r, p) = 1$ and so $p \nmid r^{p-2}$. The outcome of all this is that $(r')^{p-1} \not\equiv 1 \pmod{p^2}$, as desired.

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 $r + p$ 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 else $p(p-1) = \phi(p^2)$. The foregoing proof shows that if r has order $p - 1$ modulo p^2, then $r + p$ will be a primitive root of p^2.

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

LEMMA 2. *Let p be an odd prime and r be a primitive root of p such 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 $k + 1$. Since $\gcd(r, p^{k-1}) = \gcd(r, p^k) = 1$, 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-written equation to the pth power and expand to obtain

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

Since 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 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 $\phi(p^k) = p^{k-1}(p-1)$. Since $r^n \equiv 1 \pmod{p^k}$ implies that $r^n \equiv 1 \pmod{p}$, 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 picked. 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 so $\phi(p^k) \mid n$. 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. Since

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

these also serve as primitive roots for 5^2, 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 $2 \cdot 5^k$.

We summarize what has been accomplished in

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, while 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 $r^{pk} \equiv 1 \pmod{p^2}, \ldots, r^{p^{n-1}k} \equiv 1 \pmod{p^n}$, 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 3^7 and 3^{11} 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
$$\lambda(n) = \text{lcm}\,(\lambda(2^{k_0}), \phi(p_1^{k_1}), \ldots, \phi(p_r^{k_r}))$$
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, $2p^k$, $\lambda(n) | \frac{1}{2}\phi(n)$; hence, $a^{\phi(n)/2} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$.]
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. Let n be any integer which 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
$$a \equiv r^k \pmod{n}$$