$\gcd(a, p) = 1$. 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, since $(-1)^2 = 1$, -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. Since $2^5 \equiv 1 \pmod{31}$, the integer 2 is clearly ruled out. We need not search too far, since 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 which 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 that

(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 $2, 3, \ldots, p - 1$.

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 $p = 17$, 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
   (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 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 that
   (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 5-3 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 by Theorem 8-4 $(p-1)! \equiv r^{1+2+\cdots+(p-1)} \pmod{p}$.]

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 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 sum is congruent modulo p to $1 + r^n + r^{2n} + \cdots + r^{(p-2)n} = \dfrac{r^{(p-1)n} - 1}{r^n - 1}$.]

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 of 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 which are relatively prime to 2^k are precisely the odd integers; also, $\phi(2^k) = 2^{k-1}$. 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. *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 $d = \gcd(\phi(m), \phi(n))$.

Since $\phi(m)$ 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 equation 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 which 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*

(1) *n is divisible by two odd primes, or*

(2) *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 they restrict 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 shall 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.