The sharp-eyed reader will have noticed that, save for $\phi(1)$ and $\phi(2)$, the values of $\phi(n)$ in our examples are always even. This is no accident, as the next theorem shows.

THEOREM 7-4. *For $n > 2$, $\phi(n)$ is an even integer.*

Proof: First, assume that n is a power of 2, let us say $n = 2^k$, with $k \geq 2$. By Theorem 7-3,

$$\phi(n) = \phi(2^k) = 2^k(1 - \tfrac{1}{2}) = 2^{k-1},$$

an even integer. If n does not happen to be a power of 2, then it is divisible by an odd prime p; we may therefore write n as $n = p^k m$, where $k \geq 1$ and $\gcd(p^k, m) = 1$. Exploiting the multiplicative nature of the phi-function, one gets

$$\phi(n) = \phi(p^k)\phi(m) = p^{k-1}(p - 1)\phi(m),$$

which is again even since $2 \mid p - 1$.

We can establish Euclid's Theorem on the infinitude of primes in the following new way: As before, assume that there are only a finite number of primes. Call them $p_1, p_2, \ldots, p_r$ and consider the integer $n = p_1 p_2 \cdots p_r$. We argue that if $1 < a \leq n$, then $\gcd(a, n) \neq 1$. For, the Fundamental Theorem of Arithmetic tells us that a has a prime divisor q. Since $p_1, p_2, \ldots, p_r$ are the only primes, q must be one of these p_i, whence $q \mid n$; in other words, $\gcd(a, n) \geq q$. The implication of all this is that $\phi(n) = 1$, which is clearly impossible by Theorem 7-4.

PROBLEMS 7.2

1. Calculate $\phi(1001)$, $\phi(5040)$, and $\phi(36{,}000)$.
2. Verify that the equality $\phi(n) = \phi(n + 1) = \phi(n + 2)$ holds when $n = 5186$.
3. Show that the integers $m = 3^k \cdot 568$ and $n = 3^k \cdot 638$, where $k \geq 0$, satisfy simultaneously

$$\tau(m) = \tau(n),\ \sigma(m) = \sigma(n),\ \phi(m) = \phi(n).$$

4. Establish each of the assertions below:
   (a) If n is an odd integer, then $\phi(2n) = \phi(n)$.
   (b) If n is an even integer, then $\phi(2n) = 2\phi(n)$.
   (c) $\phi(3n) = 3\phi(n)$ if and only if $3 \mid n$.
   (d) $\phi(3n) = 2\phi(n)$ if and only if $3 \nmid n$.

(e) $\phi(n) = n/2$ if and only if $n = 2^k$ for some $k \geq 1$. [*Hint:* Write $n = 2^k N$, where N is odd, and use the condition $\phi(n) = n/2$ to show that $N = 1$.]

5. Prove that the equation $\phi(n) = \phi(n+2)$ is satisfied by $n = 2(2p-1)$ whenever p and $2p-1$ are both odd primes.

6. Show that there are infinitely many integers n for which $\phi(n)$ is a perfect square. [*Hint:* Consider the integers $n = 2^{k+1}$ for $k = 1, 2, \ldots$.]

7. Verify the following:

(a) For any positive integer n, $\frac{1}{2}\sqrt{n} \leq \phi(n) \leq n$. [*Hint:* Write $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$, so $\phi(n) = 2^{k_0 - 1} p_1^{k_1 - 1} \cdots p_r^{k_r - 1}(p_1 - 1) \cdots (p_r - 1)$. Now use the inequalities $p - 1 > \sqrt{p}$ and $k - \frac{1}{2} \geq k/2$ to obtain $\phi(n) \geq 2^{k_0 - 1} p_1^{k_1/2} \cdots p_r^{k_r/2}$.]

(b) If the integer $n > 1$ has r distinct prime factors, then $\phi(n) \geq n/2^r$.

(c) If $n > 1$ is a composite number, then $\phi(n) \leq n - \sqrt{n}$. [*Hint:* Let p be the smallest prime divisor of n, so that $p \leq \sqrt{n}$. Then $\phi(n) \leq n(1 - 1/p)$.]

8. Prove that if the integer n has r distinct odd prime factors, then $2^r \mid \phi(n)$.

9. Prove that:

(a) If n and $n+2$ are twin primes, then $\phi(n+2) = \phi(n) + 2$; this also holds for $n = 12$, 14, and 20.

(b) If p and $2p+1$ are both odd primes, then $n = 4p$ satisfies $\phi(n+2) = \phi(n) + 2$.

10. If every prime that divides n also divides m, establish that $\phi(nm) = n\phi(m)$; in particular, $\phi(n^2) = n\phi(n)$ for every positive integer n.

11. (a) If $\phi(n) \mid n - 1$, prove that n is a square-free integer. [*Hint:* Assume that n has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, where $k_1 \geq 2$. Then $p_1 \mid \phi(n)$, whence $p_1 \mid n - 1$, which leads to a contradiction.]

(b) Show that if $n = 2^k$ or $2^k 3^j$, with k and j positive integers, then $\phi(n) \mid n$.

12. If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, derive the inequalities

(a) $\sigma(n)\phi(n) \geq n^2(1 - 1/p_1^2)(1 - 1/p_2^2) \cdots (1 - 1/p_r^2)$, and

(b) $\tau(n)\phi(n) \geq n$. [*Hint:* Show that $\tau(n)\phi(n) \geq 2^r \cdot n(1/2)^r$.]

13. Assuming that $d \mid n$, prove that $\phi(d) \mid \phi(n)$. [*Hint:* Work with the prime factorizations of d and n.]

14. Obtain the following two generalizations of Theorem 7-2:

(a) For positive integers m and n,

$$\phi(m)\phi(n) = \phi(mn)\phi(d)/d,$$

where $d = \gcd(m, n)$.

(b) For positive integers m and n,

$$\phi(m)\phi(n) = \phi(\gcd(m, n))\phi(\operatorname{lcm}(m, n)).$$

15. Show that Goldbach's Conjecture implies that for each even integer $2n$ there exist integers n_1 and n_2 with $\phi(n_1) + \phi(n_2) = 2n$.

16. Given a positive integer k, show that
(a) there are at most a finite number of integers n for which $\phi(n) = k$;
(b) if the equation $\phi(n) = k$ has a unique solution, say $n = n_0$, then $4 \mid n_0$. [*Hint:* See Problem 4(a) and 4(b).]

A famous conjecture of Carmichael is that the number of solutions of $\phi(n) = k$ cannot be equal to one.

17. Find all solutions of $\phi(n) = 16$ and $\phi(n) = 24$. [*Hint:* If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ satisfies $\phi(n) = k$, then $n = [k/\Pi\,(p_i - 1)]\,\Pi p_i$. Thus the integers $d_i = p_i - 1$ can be determined by the conditions (1) $d_i \mid k$, (2) $d_i + 1$ is prime and (3) $k/\Pi\, d_i$ contains no prime factor not in $\Pi\, p_i$.]

18. (a) Prove that the equation $\phi(n) = 2p$, where p is a prime number and $2p + 1$ is composite, is not solvable.
(b) Prove that there is no solution to the equation $\phi(n) = 14$, and that 14 is the smallest (positive) even integer with this property.

19. If p is a prime and $k \geq 2$, show that $\phi(\phi(p^k)) = p^{k-2}\phi((p-1)^2)$.

7.3 EULER'S THEOREM

As remarked earlier, the first published proof of Fermat's Theorem (that $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$) was given by Euler in 1736. Somewhat later, in 1760, he succeeded in generalizing Fermat's Theorem from the case of a prime p to an arbitrary integer n. This landmark result states: if $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

For example, putting $n = 30$ and $a = 11$, we have

$$11^{\phi(30)} \equiv 11^8 \equiv (11^2)^4 \equiv (121)^4 \equiv 1^4 \equiv 1 \pmod{30}.$$

As a prelude to launching our proof of Euler's Generalization of Fermat's Theorem, we require a preliminary lemma.

LEMMA. *Let $n > 1$ and $\gcd(a, n) = 1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the positive integers less than n and relatively prime to n, then*

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

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

Proof: Observe that no two of the integers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n. For if $aa_i \equiv aa_j \pmod{n}$, with $1 \leq i <$

$j \leq \phi(n)$, then the cancellation law yields $a_i \equiv a_j \pmod{n}$, a contradiction. Furthermore, since $\gcd(a_i, n) = 1$ for all i and $\gcd(a, n) = 1$, the lemma on page 137 guarantees that each of the aa_i is relatively prime to n.

Fixing on a particular aa_i, there exists a unique integer b, where $0 \leq b < n$, for which $aa_i \equiv b \pmod{n}$. Because

$$\gcd(b, n) = \gcd(aa_i, n) = 1,$$

b must be one of the integers $a_1, a_2, \ldots, a_{\phi(n)}$. All told, this proves that the numbers $aa_1, aa_2, \ldots, aa_{\phi(n)}$ and the numbers $a_1, a_2, \ldots, a_{\phi(n)}$ are identical (modulo n) in a certain order.

THEOREM 7-5 (Euler). *If n is a positive integer and* $\gcd(a, n) = 1$ *then* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof: There is no harm in taking $n > 1$. Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n which are relatively prime to n. Since $\gcd(a, n) = 1$, it follows from the lemma that $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent, not necessarily in order of appearance, to $a_1, a_2, \ldots, a_{\phi(n)}$. Then

$$\begin{aligned} aa_1 &\equiv a_1' \pmod{n}, \\ aa_2 &\equiv a_2' \pmod{n}, \\ &\vdots \\ aa_{\phi(n)} &\equiv a_{\phi(n)}' \pmod{n}, \end{aligned}$$

where $a_1', a_2', \ldots, a_{\phi(n)}'$ are the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in some order. On taking the product of these $\phi(n)$ congruences, we get

$$\begin{aligned} (aa_1)(aa_2) \cdots (aa_{\phi(n)}) &\equiv a_1' a_2' \cdots a_{\phi(n)}' \pmod{n} \\ &\equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n} \end{aligned}$$

and so

$$a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}.$$

Since $\gcd(a_i, n) = 1$ for each i, the lemma preceding Theorem 7-2 implies that $\gcd(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$. Therefore we may divide both sides of the foregoing congruence by the common factor $a_1 a_2 \cdots a_{\phi(n)}$, leaving us with

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