CHAPTER 7

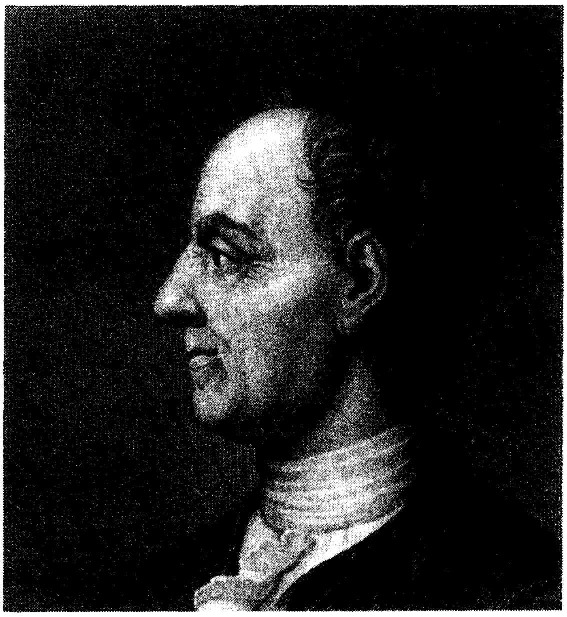
EULER'S GENERALIZATION OF FERMAT'S THEOREM

Euler calculated without apparent effort, just as men breathe, as eagles sustain themselves in the air.
ARAGO

7.1 LEONHARD EULER

The importance of Fermat's work resides not so much in any contribution to the mathematics of his own day, but rather in its animating effect on later generations of mathematicians. Perhaps the greatest disappointment of Fermat's career was his inability to interest others in his new number theory. A century was to pass before a first-class mathematician, Leonhard Euler (1707–1783), either understood or appreciated its significance. Many of the theorems announced without proof by Fermat yielded to Euler's skill, and it is likely that the arguments devised by Euler were not substantially different from those that Fermat said he possessed.

The key figure in 18th century mathematics, Euler was the son of a Lutheran pastor who lived in the vicinity of Basel, Switzerland. Euler's father earnestly wished him to enter the ministry and sent his son, at the age of 13, to the University of Basel to study theology. There the young Euler met Johann Bernoulli—then one of Europe's leading mathematicians—and befriended Bernoulli's two sons, Nicolaus and Daniel. Within a short time, Euler broke off the theological studies that had been selected for him to address himself exclusively to mathematics. He received his master's degree in 1723, and in 1727 at the age of 19, he won a prize from the Paris Academy of Sciences for a treatise on the most efficient arrangement of ship masts.



Leonhard Euler
(1707–1783)

(*Dover Publications, Inc.*)

Where the 17th century had been an age of great amateur mathematicians, the 18th century was almost exclusively an era of professionals—university professors and members of scientific academies. Many of the reigning monarchs delighted in regarding themselves as patrons of learning, and the academies served as the intellectual crown jewels of the royal courts. Although the motives of these rulers may not have been entirely philanthropic, the fact remains that the learned societies constituted important agencies for the promotion of science. They provided salaries for distinguished scholars, published journals of research papers on a regular basis, and offered monetary prizes for scientific discoveries. Euler was at different times associated with two of the newly formed academies, the Imperial Academy at St. Petersburg (1727–1741; 1766–1783) and the Royal Academy in Berlin (1741–1766). In 1725, Peter the Great founded the Academy of St. Petersburg and attracted a number of leading mathematicians to Russia, including Nicolaus and Daniel Bernoulli. On their recommendation, an appointment was secured for Euler. Because of his youth, he had recently been denied a professorship in physics at the University of Basel and was only too ready to accept the invitation of the Academy. In St. Petersburg, he soon came into contact with the versatile scholar Christian Goldbach (of the famous conjecture), a man who subsequently rose from professor of mathematics to Russian Minister of Foreign Affairs. Given his interests, it seems likely that Goldbach was the one who first drew Euler's attention to the work of Fermat on the theory of numbers.

Euler eventually tired of the political repression in Russia and accepted the call of Frederick the Great to become a member of the Berlin Academy. The story is told that, during a reception at Court, he was kindly received by the Queen Mother who inquired why so distinguished a scholar should be so timid and reticent; he replied, "Madame, it is because I have just come from a country where, when one speaks, one is hanged." However, flattered by the warmth of the Russian feeling toward him and unendurably offended by the contrasting coolness of Frederick and his court, Euler returned to St. Petersburg in 1766 to spend his remaining days. Within two or three years of his return, Euler became totally blind.

However, Euler did not permit blindness to retard his scientific work; aided by a phenomenal memory, his writings grew to such enormous proportions as to be virtually unmanageable. Without a doubt, Euler was the most prolific writer in the entire history of mathematics. He wrote or dictated over 700 books and papers in his lifetime, and left so much unpublished material that the St. Petersburg Academy did not finish printing all his manuscripts until 47 years after his death. The publication of Euler's collected works was begun by the Swiss Society of Natural Sciences in 1911 and it is estimated that more than 75 large volumes will ultimately be required for the completion of this monumental project. The best testament to the quality of these papers may be the fact that on 12 occasions they won the coveted biennial prize of the French Academy in Paris.

During his stay in Berlin, Euler acquired the habit of writing memoir after memoir, placing each when finished at the top of a pile of manuscripts. Whenever material was needed to fill the Academy's journal, the printers helped themselves to a few papers from the top of the stack. As the height of the pile increased more rapidly than the demands made upon it, memoirs at the bottom tended to remain in place a long time. This explains how it happened that various papers of Euler were published, when extensions and improvements of the material contained in them had previously appeared in print under his name. We might also add that the manner in which Euler made his work public contrasts sharply with the secrecy customary in Fermat's time.

7.2 EULER'S PHI-FUNCTION

This chapter deals with that part of the theory arising out of the result known as Euler's Generalization of Fermat's Theorem. In a nutshell, Euler extended Fermat's theorem, which concerns congruences with prime moduli, to arbitrary moduli. While doing so, he introduced an important number-theoretic function, described in Definition 7.1.

Definition 7.1. For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.

As an illustration of the definition, we find that $\phi(30) = 8$; for, among the positive integers that do not exceed 30, there are eight that are relatively prime to 30; specifically,

$$1, 7, 11, 13, 17, 19, 23, 29$$

Similarly, for the first few positive integers, the reader may check that

$$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4,$$
$$\phi(6) = 2, \phi(7) = 6, \ldots$$

Notice that $\phi(1) = 1$, because $\gcd(1, 1) = 1$. In the event $n > 1$, then $\gcd(n, n) = n \neq 1$, so that $\phi(n)$ can be characterized as the number of integers less than n and relatively prime to it. The function ϕ is usually called the *Euler* *phi-function* (sometimes, the *indicator* or *totient*) after its originator; the functional notation $\phi(n)$, however, is credited to Gauss.

If n is a prime number, then every integer less than n is relatively prime to it; whence, $\phi(n) = n - 1$. On the other hand, if $n > 1$ is composite, then n has a divisor d such that $1 < d < n$. It follows that there are at least two integers among $1, 2, 3, \ldots, n$ that are not relatively prime to n, namely, d and n itself. As a result, $\phi(n) \leq n - 2$. This proves that for $n > 1$,

$$\phi(n) = n - 1 \qquad \text{if and only if } n \text{ is prime}$$

The first item on the agenda is to derive a formula that will allow us to calculate the value of $\phi(n)$ directly from the prime-power factorization of n. A large step in this direction stems from Theorem 7.1.

Theorem 7.1. If p is a prime and $k > 0$, then

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

Proof. Clearly, $\gcd(n\,, p^k) = 1$ if and only if $p \nmid n$. There are p^{k-1} integers between 1 and p^k divisible by p, namely,

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

Thus, the set $\{1, 2, \ldots, p^k\}$ contains exactly $p^k - p^{k-1}$ integers that are relatively prime to p^k, and so by the definition of the phi-function, $\phi(p^k) = p^k - p^{k-1}$.

For an example, we have

$$\phi(9) = \phi(3^2) = 3^2 - 3 = 6$$

the six integers less than and relatively prime to 9 being 1, 2, 4, 5, 7, 8. To give a second illustration, there are 8 integers that are less than 16 and relatively prime to it; they are 1, 3, 5, 7, 9, 11, 13, 15. Theorem 7.1 yields the same count:

$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$$

We now know how to evaluate the phi-function for prime powers, and our aim is to obtain a formula for $\phi(n)$ based on the factorization of n as a product of primes. The missing link in the chain is obvious: Show that ϕ is a multiplicative function. We pave the way with an easy lemma.

Lemma. Given integers a, b, c, $\gcd(a\,, bc) = 1$ if and only if $\gcd(a\,, b) = 1$ and $\gcd(a\,, c) = 1$.

Proof. First suppose that $\gcd(a\,, bc) = 1$, and put $d = \gcd(a\,, b)$. Then $d \mid a$ and $d \mid b$, whence $d \mid a$ and $d \mid bc$. This implies that $\gcd(a\,, bc) \geq d$, which forces $d = 1$. Similar reasoning gives rise to the statement $\gcd(a\,, c) = 1$.

For the other direction, take $\gcd(a\,, b) = 1 = \gcd(a\,, c)$ and assume that $\gcd(a\,, bc) = d_1 > 1$. Then d_1 must have a prime divisor p. Because $d_1 \mid bc$, it follows that $p \mid bc$; in consequence, $p \mid b$ or $p \mid c$. If $p \mid b$, then (by virtue of the fact that $p \mid a$) we have $\gcd(a, b) \geq p$, a contradiction. In the same way, the condition $p \mid c$ leads to the equally false conclusion that $\gcd(a, c) \geq p$. Thus, $d_1 = 1$ and the lemma is proven.

Theorem 7.2. The function ϕ is a multiplicative function.

Proof. It is required to show that $\phi(mn) = \phi(m)\phi(n)$, wherever m and n have no common factor. Because $\phi(1) = 1$, the result obviously holds if either m or n equals 1. Thus, we may assume that $m > 1$ and $n > 1$. Arrange the integers from 1 to mn in m columns of n integers each, as follows:

$$\begin{array}{ccccc}
1 & 2 & \cdots & r & \cdots \; m \\
m+1 & m+2 & & m+r & 2m \\
2m+1 & 2m+2 & & 2m+r & 3m \\
\vdots & \vdots & & \vdots & \vdots \\
(n-1)m+1 & (n-1)m+2 & & (n-1)m+r & nm
\end{array}$$

We know that $\phi(mn)$ is equal to the number of entries in this array that are relatively prime to mn; by virtue of the lemma, this is the same as the number of integers that are relatively prime to both m and n.

Before embarking on the details, it is worth commenting on the tactics to be adopted: Because $\gcd(qm + r, m) = \gcd(r, m)$, the numbers in the rth column are relatively prime to m if and only if r itself is relatively prime to m. Therefore, only $\phi(m)$ columns contain integers relatively prime to m, and every entry in the column will be relatively prime to m. The problem is one of showing that in each of these $\phi(m)$ columns there are exactly $\phi(n)$ integers that are relatively prime to n; for then altogether there would be $\phi(m)\phi(n)$ numbers in the table that are relatively prime to both m and n.

Now the entries in the rth column (where it is assumed that $\gcd(r, m) = 1$) are

$$r, m + r, 2m + r, \ldots, (n - 1)m + r$$

There are n integers in this sequence and no two are congruent modulo n. Indeed, if

$$km + r \equiv jm + r \pmod{n}$$

with $0 \leq k < j < n$, it would follow that $km \equiv jm \pmod{n}$. Because $\gcd(m, n) = 1$, we could cancel m from both sides of this congruence to arrive at the contradiction that $k \equiv j \pmod{n}$. Thus, the numbers in the rth column are congruent modulo n to $0, 1, 2, \ldots, n - 1$, in some order. But if $s \equiv t \pmod{n}$, then $\gcd(s, n) = 1$ if and only if $\gcd(t, n) = 1$. The implication is that the rth column contains as many integers that are relatively prime to n as does the set $\{0, 1, 2, \ldots, n - 1\}$, namely, $\phi(n)$ integers. Therefore, the total number of entries in the array that are relatively prime to both m and n is $\phi(m)\phi(n)$. This completes the proof of the theorem.

With these preliminaries in hand, we now can prove Theorem 7.3.

Theorem 7.3. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then

$$\begin{aligned}\phi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_r^{k_r} - p_r^{k_r-1}\right)\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right)\end{aligned}$$

Proof. We intend to use induction on r, the number of distinct prime factors of n. By Theorem 7.1, the result is true for $r = 1$. Suppose that it holds for $r = i$. Because

$$\gcd\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}, p_{i+1}^{k_{i+1}}\right) = 1$$

the definition of multiplicative function gives

$$\begin{aligned}\phi\left(\left(p_1^{k_1} \cdots p_i^{k_i}\right) p_{i+1}^{k_{i+1}}\right) &= \phi\left(p_1^{k_1} \cdots p_i^{k_i}\right)\phi\left(p_{i+1}^{k_{i+1}}\right)\\ &= \phi\left(p_1^{k_1} \cdots p_i^{k_i}\right)\left(p_{i+1}^{k_{i+1}} - p_{i+1}^{k_{i+1}-1}\right)\end{aligned}$$

Invoking the induction assumption, the first factor on the right-hand side becomes

$$\phi\left(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i}\right) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_i^{k_i} - p_i^{k_i-1}\right)$$

and this serves to complete the induction step, and the proof.

Example 7.1. Let us calculate the value $\phi(360)$, for instance. The prime-power decomposition of 360 is $2^3 \cdot 3^2 \cdot 5$, and Theorem 7.3 tells us that

$$\begin{aligned}\phi(360) &= 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\\ &= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96\end{aligned}$$

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 that $n = 2^k$, with $k \geq 2$. By Theorem 7.3,

$$\phi(n) = \phi(2^k) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1}$$

an even integer. If n does not happen to be a power of 2, then it is divisible by an odd prime p; we therefore may 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, we obtain

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

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

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. Because $p_1, p_2, \ldots, p_r$ 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 clearly is 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

$$\tau(m) = \tau(n), \qquad \sigma(m) = \sigma(n), \text{ and } \qquad \phi(m) = \phi(n)$$

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 $n = 2^{2k+1}$ 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 the following:
   (a) If n and $n + 2$ are a pair of 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 following inequalities:
   (a) $\sigma(n)\phi(n) \geq n^2(1 - 1/p_1^2)(1 - 1/p_2^2) \cdots (1 - 1/p_r^2)$.
   (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, where $d = \gcd(m, n)$,

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

(b) For positive integers m and n,

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

15. Prove the following:

(a) There are infinitely many integers n for which $\phi(n) = n/3$.
[*Hint:* Consider $n = 2^k 3^j$, where k and j are positive integers.]

(b) There are no integers n for which $\phi(n) = n/4$.

16. Show that the Goldbach conjecture implies that for each even integer $2n$ there exist integers n_1 and n_2 with $\phi(n_1) + \phi(n_2) = 2n$.

17. Given a positive integer k, show the following:

(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 Problems 4(a) and 4(b).]
A famous conjecture of R. D. Carmichael (1906) is that there is no k for which the equation $\phi(n) = k$ has precisely one solution; it has been proved that any counterexample n must exceed $10^{10000000}$.

18. 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 Πp_i.]

19. (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.

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

21. Verify that $\phi(n)\sigma(n)$ is a perfect square when $n = 63457 = 23 \cdot 31 \cdot 89$.

7.3 EULER'S THEOREM

As remarked earlier, the first published proof of Fermat's theorem (namely 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 positive 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 $a_i \equiv a_j \pmod{n}$, and thus $a_i = a_j$, a contradiction. Furthermore, because $\gcd(a_i, n) = 1$ for all i and $\gcd(a, n) = 1$, the lemma preceding Theorem 7.2 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 $n \geq 1$ 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 that are relatively prime to n. Because $\gcd(a, n) = 1$, 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

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

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

$$\begin{aligned} (aa_1)(aa_2)\cdots(aa_{\phi(n)}) &\equiv a_1'a_2'\cdots a_{\phi(n)}' \pmod{n} \\ &\equiv a_1a_2\cdots a_{\phi(n)} \pmod{n} \end{aligned}$$

and so

$$a^{\phi(n)}(a_1a_2\cdots a_{\phi(n)}) \equiv a_1a_2\cdots a_{\phi(n)} \pmod{n}$$

Because $\gcd(a_i, n) = 1$ for each i, the lemma preceding Theorem 7.2 implies that $\gcd(a_1a_2\cdots a_{\phi(n)}, n) = 1$. Therefore, we may divide both sides of the foregoing congruence by the common factor $a_1a_2\cdots a_{\phi(n)}$, leaving us with

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

This proof can best be illustrated by carrying it out with some specific numbers. Let $n = 9$, for instance. The positive integers less than and relatively prime to 9 are

$$1, 2, 4, 5, 7, 8$$

These play the role of the integers $a_1, a_2, \ldots, a_{\phi(n)}$ in the proof of Theorem 7.5. If $a = -4$, then the integers aa_i are

$$-4, -8, -16, -20, -28, -32$$

where, modulo 9,

$$-4 \equiv 5 \quad -8 \equiv 1 \quad -16 \equiv 2 \quad -20 \equiv 7 \quad -28 \equiv 8 \quad -32 \equiv 4$$

When the above congruences are all multiplied together, we obtain

$$(-4)(-8)(-16)(-20)(-28)(-32) \equiv 5 \cdot 1 \cdot 2 \cdot 7 \cdot 8 \cdot 4 \pmod 9$$

which becomes

$$(1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8)(-4)^6 \equiv (1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8) \pmod 9$$

Being relatively prime to 9, the six integers 1, 2, 4, 5, 7, 8 may be canceled successively to give

$$(-4)^6 \equiv 1 \pmod 9$$

The validity of this last congruence is confirmed by the calculation

$$(-4)^6 \equiv 4^6 \equiv (64)^2 \equiv 1^2 \equiv 1 \pmod 9$$

Note that Theorem 7.5 does indeed generalize the one credited to Fermat, which we proved earlier. For if p is a prime, then $\phi(p) = p - 1$; hence, when $\gcd(a\,, p) = 1$, we get

$$a^{p-1} \equiv a^{\phi(p)} \equiv 1 \pmod p$$

and so we have the following corollary.

Corollary **Fermat.** If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$.

Example 7.2. Euler's theorem is helpful in reducing large powers modulo n. To cite a typical example, let us find the last two digits in the decimal representation of 3^{256}. This is equivalent to obtaining the smallest nonnegative integer to which 3^{256} is congruent modulo 100. Because $\gcd(3\,, 100) = 1$ and

$$\phi(100) = \phi(2^2 \cdot 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$$

Euler's theorem yields

$$3^{40} \equiv 1 \pmod{100}$$

By the Division Algorithm, $256 = 6 \cdot 40 + 16$; whence

$$3^{256} \equiv 3^{6 \cdot 40 + 16} \equiv (3^{40})^6 3^{16} \equiv 3^{16} \pmod{100}$$

and our problem reduces to one of evaluating 3^{16}, modulo 100. The method of successive squaring yields the congruences

$$3^2 \equiv 9 \pmod{100} \qquad 3^8 \equiv 61 \pmod{100}$$

$$3^4 \equiv 81 \pmod{100} \qquad 3^{16} \equiv 21 \pmod{100}$$

There is another path to Euler's theorem, one which requires the use of Fermat's theorem.

Second Proof of Euler's Theorem. To start, we argue by induction that if $p \nmid a$ (p a prime), then

$$a^{\phi(p^k)} \equiv 1 \pmod{p^k} \qquad k > 0 \tag{1}$$

When $k = 1$, this assertion reduces to the statement of Fermat's theorem. Assuming the truth of Eq. (1) for a fixed value of k, we wish to show that it is true with k replaced by $k + 1$.

Because Eq. (1) is assumed to hold, we may write

$$a^{\phi(p^k)} = 1 + qp^k$$

for some integer q. Also notice that

$$\phi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p\phi(p^k)$$

Using these facts, along with the binomial theorem, we obtain

$$\begin{aligned}
a^{\phi(p^{k+1})} &= a^{p\phi(p^k)} \\
&= (a^{\phi(p^k)})^p \\
&= (1 + qp^k)^p \\
&= 1 + \binom{p}{1}(qp^k) + \binom{p}{2}(qp^k)^2 + \cdots \\
&\quad + \binom{p}{p-1}(qp^k)^{p-1} + (qp^k)^p \\
&\equiv 1 + \binom{p}{1}(qp^k) \pmod{p^{k+1}}
\end{aligned}$$

But $p \mid \binom{p}{1}$, and so $p^{k+1} \mid \binom{p}{1}(qp^k)$. Thus, the last-written congruence becomes

$$a^{\phi(p^{k+1})} \equiv 1 \pmod{p^{k+1}}$$

completing the induction step.

Let $\gcd(a, n) = 1$ and n have the prime-power factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. In view of what already has been proven, each of the congruences

$$a^{\phi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}} \qquad i = 1, 2, \ldots, r \tag{2}$$

holds. Noting that $\phi(n)$ is divisible by $\phi(p_i^{k_i})$, we may raise both sides of Eq. (2) to the power $\phi(n)/\phi(p_i^{k_i})$ and arrive at

$$a^{\phi(n)} \equiv 1 \pmod{p_i^{k_i}} \qquad i = 1, 2, \ldots, r$$

Inasmuch as the moduli are relatively prime, this leads us to the relation

$$a^{\phi(n)} \equiv 1 \pmod{p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}}$$

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

The usefulness of Euler's theorem in number theory would be hard to exaggerate. It leads, for instance, to a different proof of the Chinese Remainder Theorem. In other words, we seek to establish that if $\gcd(n_i, n_j) = 1$ for $i \neq j$, then the system of linear congruences

$$x \equiv a_i \pmod{n_i} \qquad i = 1, 2, \ldots, r$$

admits a simultaneous solution. Let $n = n_1 n_2 \cdots n_r$, and put $N_i = n/n_i$ for $n = 1, 2, \ldots, r$. Then the integer

$$x = a_1 N_1^{\phi(n_1)} + a_2 N_2^{\phi(n_2)} + \cdots + a_r N_r^{\phi(n_r)}$$

fulfills our requirements. To see this, first note that $N_j \equiv 0 \pmod{n_i}$ whenever $i \neq j$; whence,

$$x \equiv a_i N_i^{\phi(n_i)} \pmod{n_i}$$

But because $\gcd(N_i, n_i) = 1$, we have

$$N_i^{\phi(n_i)} \equiv 1 \pmod{n_i}$$

and so $x \equiv a_i \pmod{n_i}$ for each i.

As a second application of Euler's theorem, let us show that if n is an odd integer that is not a multiple of 5, then n divides an integer all of whose digits are equal to 1 (for example, $7 \mid 111111$). Because $\gcd(n, 10) = 1$ and $\gcd(9, 10) = 1$, we have $\gcd(9n, 10) = 1$. Quoting Theorem 7.5, again,

$$10^{\phi(9n)} \equiv 1 \pmod{9n}$$

This says that $10^{\phi(9n)} - 1 = 9nk$ for some integer k or, what amounts to the same thing,

$$kn = \frac{10^{\phi(9n)} - 1}{9}$$

The right-hand side of this expression is an integer whose digits are all equal to 1, each digit of the numerator being clearly equal to 9.

PROBLEMS 7.3

1. Use Euler's theorem to establish the following:
   (a) For any integer a, $a^{37} \equiv a \pmod{1729}$.
   [*Hint:* $1729 = 7 \cdot 13 \cdot 19$.]
   (b) For any integer a, $a^{13} \equiv a \pmod{2730}$.
   [*Hint:* $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.]
   (c) For any odd integer a, $a^{33} \equiv a \pmod{4080}$.
   [*Hint:* $4080 = 15 \cdot 16 \cdot 17$.]
2. Use Euler's theorem to confirm that, for any integer $n \geq 0$,

$$51 \mid 10^{32n+9} - 7$$

3. Prove that $2^{15} - 2^3$ divides $a^{15} - a^3$ for any integer a.
   [*Hint:* $2^{15} - 2^3 = 5 \cdot 7 \cdot 8 \cdot 9 \cdot 13$.]
4. Show that if $\gcd(a, n) = \gcd(a - 1, n) = 1$, then

$$1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n}$$

[*Hint:* Recall that $a^{\phi(n)} - 1 = (a - 1)(a^{\phi(n)-1} + \cdots + a^2 + a + 1)$.]

5. If m and n are relatively prime positive integers, prove that

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$

6. Fill in any missing details in the following proof of Euler's theorem: Let p be a prime divisor of n and $\gcd(a\,,p) = 1$. By Fermat's theorem, $a^{p-1} \equiv 1 \pmod p$, so that $a^{p-1} = 1 + tp$ for some t. Therefore $a^{p(p-1)} = (1+tp)^p = 1 + \binom{p}{1}(tp) + \cdots + (tp)^p \equiv 1 \pmod{p^2}$ and, by induction, $a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}$, where $k = 1, 2, \ldots$. Raise both sides of this congruence to the $\phi(n)/p^{k-1}(p-1)$ power to get $a^{\phi(n)} \equiv 1 \pmod{p^k}$. Thus, $a^{\phi(n)} \equiv 1 \pmod n$.

7. Find the units digit of 3^{100} by means of Euler's theorem.

8. (a) If $\gcd(a\,,n) = 1$, show that the linear congruence $ax \equiv b \pmod n$ has the solution $x \equiv ba^{\phi(n)-1} \pmod n$.

(b) Use part (a) to solve the linear congruences $3x \equiv 5 \pmod{26}$, $13x \equiv 2 \pmod{40}$, and $10x \equiv 21 \pmod{49}$.

9. Use Euler's theorem to evaluate $2^{100000} \pmod{77}$.

10. For any integer a, show that a and a^{4n+1} have the same last digit.

11. For any prime p, establish each of the assertions below:

(a) $\tau(p!) = 2\tau((p-1)!)$.

(b) $\sigma(p!) = (p+1)\sigma((p-1)!)$.

(c) $\phi(p!) = (p-1)\phi((p-1)!)$.

12. Given $n \geq 1$, a set of $\phi(n)$ integers that are relatively prime to n and that are incongruent modulo n is called a *reduced set of residues modulo n* (that is, a reduced set of residues are those members of a complete set of residues modulo n that are relatively prime to n). Verify the following:

(a) The integers $-31, -16, -8, 13, 25, 80$ form a reduced set of residues modulo 9.

(b) The integers $3, 3^2, 3^3, 3^4, 3^5, 3^6$ form a reduced set of residues modulo 14.

(c) The integers $2, 2^2, 2^3, \ldots, 2^{18}$ form a reduced set of residues modulo 27.

13. If p is an odd prime, show that the integers

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}$$

form a reduced set of residues modulo p.

7.4 SOME PROPERTIES OF THE PHI-FUNCTION

The next theorem points out a curious feature of the phi-function; namely, that the sum of the values of $\phi(d)$, as d ranges over the positive divisors of n, is equal to n itself. This was first noticed by Gauss.

Theorem 7.6 **Gauss.** For each positive integer $n \geq 1$,

$$n = \sum_{d \mid n} \phi(d)$$

the sum being extended over all positive divisors of n.

Proof. The integers between 1 and n can be separated into classes as follows: If d is a positive divisor of n, we put the integer m in the class S_d provided that $\gcd(m\,,n) = d$. Stated in symbols,

$$S_d = \{m \mid \gcd(m\,,n) = d; 1 \leq m \leq n\}$$

Now $\gcd(m, n) = d$ if and only if $\gcd(m/d, n/d) = 1$. Thus, the number of integers in the class S_d is equal to the number of positive integers not exceeding n/d that are relatively prime to n/d; in other words, equal to $\phi(n/d)$. Because each of the n integers in the set $\{1, 2, \ldots, n\}$ lies in exactly one class S_d, we obtain the formula

$$n = \sum_{d \mid n} \phi\left(\frac{n}{d}\right)$$

But as d runs through all positive divisors of n, so does n/d; hence,

$$\sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d)$$

which proves the theorem.

Example 7.3. A simple numerical example of what we have just said is provided by $n = 10$. Here, the classes S_d are

$$\begin{aligned} S_1 &= \{1, 3, 7, 9\} \\ S_2 &= \{2, 4, 6, 8\} \\ S_5 &= \{5\} \\ S_{10} &= \{10\} \end{aligned}$$

These contain $\phi(10) = 4$, $\phi(5) = 4$, $\phi(2) = 1$, and $\phi(1) = 1$ integers, respectively. Therefore,

$$\begin{aligned} \sum_{d \mid 10} \phi(d) &= \phi(10) + \phi(5) + \phi(2) + \phi(1) \\ &= 4 + 4 + 1 + 1 = 10 \end{aligned}$$

It is instructive to give a second proof of Theorem 7.6, this one depending on the fact that ϕ is multiplicative. The details are as follows. If $n = 1$, then clearly

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

Assuming that $n > 1$, let us consider the number-theoretic function

$$F(n) = \sum_{d \mid n} \phi(d)$$

Because ϕ is known to be a multiplicative function, Theorem 6.4 asserts that F is also multiplicative. Hence, if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of n, then

$$F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r})$$

For each value of i,

$$\begin{aligned}F(p_i^{k_i}) &= \sum_{d \mid p_i^{k_i}} \phi(d)\\ &= \phi(1) + \phi(p_i) + \phi(p_i^2) + \phi(p_i^3) + \cdots + \phi(p_i^{k_i})\\ &= 1 + (p_i - 1) + (p_i^2 - p_i) + (p_i^3 - p_i^2) + \cdots + (p_i^{k_i} - p_i^{k_i-1})\\ &= p_i^{k_i}\end{aligned}$$

because the terms in the foregoing expression cancel each other, save for the term $p_i^{k_i}$. Knowing this, we end up with

$$F(n) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = n$$

and so

$$n = \sum_{d \mid n} \phi(d)$$

as desired.

We should mention in passing that there is another interesting identity that involves the phi-function.

Theorem 7.7. For $n > 1$, the sum of the positive integers less than n and relatively prime to n is $\frac{1}{2}n\phi(n)$.

Proof. Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. Now because $\gcd(a\,, n) = 1$ if and only if $\gcd(n - a\,, n) = 1$, the numbers $n - a_1$, $n - a_2, \ldots, n - a_{\phi(n)}$ are equal in some order to $a_1, a_2, \ldots, a_{\phi(n)}$. Thus,

$$\begin{aligned}a_1 + a_2 + \cdots + a_{\phi(n)} &= (n - a_1) + (n - a_2) + \cdots + (n - a_{\phi(n)})\\ &= \phi(n)n - (a_1 + a_2 + \cdots + a_{\phi(n)})\end{aligned}$$

Hence,

$$2(a_1 + a_2 + \cdots + a_{\phi(n)}) = \phi(n)n$$

leading to the stated conclusion.

Example 7.4. Consider the case where $n = 30$. The $\phi(30) = 8$ integers that are less than 30 and relatively prime to it are

$$1, 7, 11, 13, 17, 19, 23, 29$$

In this setting, we find that the desired sum is

$$1 + 7 + 11 + 13 + 17 + 19 + 23 + 29 = 120 = \frac{1}{2} \cdot 30 \cdot 8$$

Also note the pairings

$$1 + 29 = 30 \qquad 7 + 23 = 30 \qquad 11 + 19 = 30 \qquad 13 + 17 = 30$$

This is a good point at which to give an application of the Möbius inversion formula.

Theorem 7.8. For any positive integer n,

$$\phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d}$$

Proof. The proof is deceptively simple. If we apply the inversion formula to

$$F(n) = n = \sum_{d \mid n} \phi(d)$$

the result is

$$\begin{aligned} \phi(n) &= \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) \\ &= \sum_{d \mid n} \mu(d) \frac{n}{d} \end{aligned}$$

Let us again illustrate the situation where $n = 10$. As easily can be seen,

$$\begin{aligned} 10 \sum_{d \mid 10} \frac{\mu(d)}{d} &= 10\left[\mu(1) + \frac{\mu(2)}{2} + \frac{\mu(5)}{5} + \frac{\mu(10)}{10}\right] \\ &= 10\left[1 + \frac{(-1)}{2} + \frac{(-1)}{5} + \frac{(-1)^2}{10}\right] \\ &= 10\left[1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{10}\right] = 10 \cdot \frac{2}{5} = 4 = \phi(10) \end{aligned}$$

Starting with Theorem 7.8, it is an easy matter to determine the value of the phi-function for any positive integer n. Suppose that the prime-power decomposition of n is $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, and consider the product

$$P = \prod_{p_i \mid n} \left(\mu(1) + \frac{\mu(p_i)}{p_i} + \cdots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}} \right)$$

Multiplying this out, we obtain a sum of terms of the form

$$\frac{\mu(1)\mu(p_1^{a_1})\mu(p_2^{a_2}) \cdots \mu(p_r^{a_r})}{p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}} \qquad 0 \leq a_i \leq k_i$$

or, because μ is known to be multiplicative,

$$\frac{\mu(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r})}{p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}} = \frac{\mu(d)}{d}$$

where the summation is over the set of divisors $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ of n. Hence, $P = \sum_{d \mid n} \mu(d)/d$. It follows from Theorem 7.8 that

$$\phi(n) = n \sum_{d \mid n} \frac{\mu(d)}{d} = n \prod_{p_i \mid n} \left(\mu(1) + \frac{\mu(p_i)}{p_i} + \cdots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}} \right)$$

But $\mu(p_i^{a_i}) = 0$ whenever $a_i \geq 2$. As a result, the last-written equation reduces to

$$\phi(n) = n \prod_{p_i \mid n} \left(\mu(1) + \frac{\mu(p_i)}{p_i} \right) = n \prod_{p_i \mid n} \left(1 - \frac{1}{p_i} \right)$$

which agrees with the formula established earlier by different reasoning. What is significant about this argument is that no assumption is made concerning the multiplicative character of the phi-function, only of μ.

PROBLEMS 7.4

1. For a positive integer n, prove that

$$\sum_{d \mid n} (-1)^{n/d} \phi(d) = \begin{cases} 0 & \text{if } n \text{ is even} \\ -n & \text{if } n \text{ is odd} \end{cases}$$

[*Hint:* If $n = 2^k N$, where N is odd, then

$$\sum_{d \mid n} (-1)^{n/d} \phi(d) = \sum_{d \mid 2^{k-1} N} \phi(d) - \sum_{d \mid N} \phi(2^k d).]$$

2. Confirm that $\sum_{d \mid 36} \phi(d) = 36$ and $\sum_{d \mid 36} (-1)^{36/d} \phi(d) = 0$.

3. For a positive integer n, prove that $\sum_{d \mid n} \mu^2(d)/\phi(d) = n/\phi(n)$.
[*Hint:* Both sides of the equation are multiplicative functions.]

4. Use Problem 4(c), Section 6.2, to prove $n \sum_{d \mid n} \mu(d)/d = \phi(n)$.

5. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, establish each of the following:

(a) $\displaystyle\sum_{d \mid n} \mu(d)\phi(d) = (2 - p_1)(2 - p_2) \cdots (2 - p_r)$.

(b) $\displaystyle\sum_{d \mid n} d\phi(d) = \left(\frac{p_1^{2k_1+1} + 1}{p_1 + 1} \right) \left(\frac{p_2^{2k_2+1} + 1}{p_2 + 1} \right) \cdots \left(\frac{p_r^{2k_r+1} + 1}{p_r + 1} \right)$.

(c) $\displaystyle\sum_{d \mid n} \frac{\phi(d)}{d} = \left(1 + \frac{k_1(p_1 - 1)}{p_1} \right) \left(1 + \frac{k_2(p_2 - 1)}{p_2} \right) \cdots \left(1 + \frac{k_r(p_r - 1)}{p_r} \right)$.

[*Hint:* For part (a), use Problem 3, Section 6.2.]

6. Verify the formula $\sum_{d=1}^{n} \phi(d)[n/d] = n(n+1)/2$ for any positive integer n.
[*Hint:* This is a direct application of Theorems 6.11 and 7.6.]

7. If n is a square-free integer, prove that $\sum_{d \mid n} \sigma(d^{k-1})\phi(d) = n^k$ for all integers $k \geq 2$.

8. For a square-free integer $n > 1$, show that $\tau(n^2) = n$ if and only if $n = 3$.

9. Prove that $3 \mid \sigma(3n + 2)$ and $4 \mid \sigma(4n + 3)$ for any positive integer n.