manuscript. Whenever material was needed to fill the Academy's journal, the printers would help 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, while 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

The present 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 as follows:

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 which 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 $\phi(1) = 1$, since $\gcd(1, 1) = 1$. While if $n > 1$, 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, ..., n which are not relatively

prime to n, namely, d and n itself. As a result, $\phi(n) \leq n - 2$. This proves: for $n > 1$,

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

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

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

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 which are 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 which 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 are 1, 2, 4, 5, 7, 8. To give a second illustration, there are 8 integers which are less than 16 and relatively prime to it, to wit, 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: Suppose first 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, let $\gcd(a, b) = 1 = \gcd(a, c)$ and assume that $\gcd(a, bc) = d_1 > 1$. Then d_1 must have a prime divisor p. Since $d_1 \mid bc$, 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 $p \mid a$) $\gcd(a, b) \geq p$, 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 $\phi(mn) = \phi(m)\phi(n)$, whenever m and n have no common factor. Since $\phi(1) = 1$, 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:

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

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

Before embarking on the details, it is worth commenting on the tactics to be adopted: Since $\gcd(qm + r, m) = \gcd(r, m)$, 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 which are relatively prime to n; for then there would be altogether $\phi(m)\phi(n)$ numbers in the table which 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, were

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

with $0 \leq k < j < n$, it would follow that $km \equiv jm \pmod{n}$. Since $\gcd(m, n) = 1$, 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, ..., $n-1$, 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 which 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 can now prove

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*

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

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 $r = i$. Since

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

the definition of multiplicative function gives

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

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

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

and this serves to complete the induction step, as well as 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

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