8. Given $n \geq 1$, a set of $\phi(n)$ integers which are relatively prime to n and which 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 which are relatively prime to n).
   Verify that
   (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.

9. 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* $n \geq 1$,

$$n = \sum_{d|n} \phi(d),$$

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 which are relatively prime to n/d; in other words,

equal to $\phi(n/d)$. Since each of the n integers in the set $\{1, 2, \ldots, n\}$ lies in exactly one class S_d, we obtain the formula

$$n = \sum_{d|n} \phi(n/d).$$

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

$$\sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$$

and the theorem follows.

Example 7-3

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

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

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

$$\sum_{d|10} \phi(d) = \phi(10) + \phi(5) + \phi(2) + \phi(1) = 4 + 4 + 1 + 1 = 10.$$

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

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

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

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

Since 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,

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

since 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 which 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 $\frac{1}{2}n\phi(n)$; in symbols,*

$$\tfrac{1}{2}n\phi(n) = \sum_{\substack{\gcd(k,n)=1 \\ 1 \le k < n}} k.$$

Proof: Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. Now, since $\gcd(a, n) = 1$ if and only if $\gcd(n - a, n) = 1$, we have

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

Hence,

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

leading to the stated conclusion.

Example 7-4

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

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