◆◇◆◇◆

A GENERALIZATION OF EULER'S Φ-FUNCTION

P. G. GARCIA
and
STEVE LIGH
University of Southwestern Louisiana, Lafayette, LA 70504
(Submitted November 1981)

Euler's ϕ-function, $\phi(n)$, denotes the number of positive integers less than n and relatively prime to it. There are many generalizations of this famous function; for example, see [1; 2; 3]. In this note, we extend the ϕ-function to an arithmetic progression

$$D(s, d, n) = \{s, s + d, \ldots, s + (n - 1)d\},$$

where $(s, d) = 1$. A formula will be established giving the number of elements in $D(s, d, n)$ that are relatively prime to n. Observe that $\phi(n)$ is the number of elements in the progression $D(1, 1, n)$ that are relatively prime to n.

Before we establish the formula, we begin with some preliminary remarks. Let

$$P(x, d, n) = \{x, x + d, \ldots, x + (n - 1)d\}$$

be an arbitrary progression of nonnegative integers. Note that if $(x, d) = 1$, then $P(x, d, n) = D(x, d, n)$.

Lemma 1

Let $P(x, d, n)$ be an arbitrary progression with $(d, n) = g$. Suppose that $n = gk$ and $d = gk_1$. Then no two elements in each of the g blocks of k consecutive elements are congruent (mod n). Furthermore, every block contains the same residues (mod n).

Proof: $x + rd \equiv x + td \pmod{n}$ if and only if $r \equiv t \pmod{k}$.

Definition: Let $\phi(s, d, n)$ denote the number of elements in the arithmetic progression $D(s, d, n)$ that are relatively prime to n.

Remark: $\phi(1, 1, n) = \phi(n) = \phi(s, 1, n)$.

Theorem 1

Suppose $(m, n) = 1$. Then

$$\phi(s, d, mn) = \phi(s, d, m)\phi(s, d, n).$$

Proof: Write the elements of $D(s, d, mn)$ as follows:

$$\begin{array}{lllll}
s & s+d & s+2d & \dots & s+(m-1)d \\
s+md & s+(m+1)d & s+(m+2)d & \dots & s+(2m-1)d \\
\vdots & & & & \\
s+(n-1)md & & & \dots & s+(nm-1)d.
\end{array}$$

Since the elements in the first row are elements of the progression $D(s, d, m)$, the number of elements in it that are relatively prime to m is $\phi(s, d, m)$. Let C_i denote the column headed by $s+id$. If $(s+id, m) > 1$, no element of C_i is relatively prime to m. If $(s+id, m) = 1$, every elements of C_i is prime to m. So to complete the proof, we need to show that $\phi(s, d, n)$ of the elements in each column of C_i are prime to n.

Let $(d, n) = g$. Since $(m, n) = 1$, it follows that $(md, n) = g$, and by Lemma 1, there are g blocks of k consecutive elements in which no two of them are congruent $\pmod{n}$. Thus, all we need to show is that each element in the first block of C_i is congruent modulo n to an element in the first block of $D(s, d, n)$. This would imply that there are $\phi(s, d, n)$ elements in C_i that are relatively prime to n.

Suppose $(s+id) + jmd$, $0 \leqslant j \leqslant k-1$, is an arbitrary element in the first block of C_i. Then there is an integer q such that

$$(i + jm) = qk + r, \quad 0 \leqslant r < k.$$

Thus

$$(s + id) + jmd \equiv s + rd \pmod{n},$$

where $s + rd$ is an element of $D(s, d, k)$.

Lemma 2

Let p be a prime and k a positive integer. Then

$$\phi(s, d, p^k) = \begin{cases} p^k\left(1 - \dfrac{1}{p}\right), & \text{if } p \nmid d, \\[2ex] p^k, & \text{if } p \mid d. \end{cases}$$

Proof: If $p \mid d$, then $(s, d) = 1$ implies that $(s + id, p^k) = 1$ and hence every element in $D(s, d, p^k)$ is relatively prime to p. If $p \nmid d$, then all p-consecutive elements in $D(s, d, p^k)$ form a complete residue system $\pmod{p}$. Thus, each has $(p - 1)$ elements relatively prime to p. Since there are p^{k-1} blocks of p-consecutive elements in $D(s, d, p^k)$, it follows that

$$\phi(s, d, p^k) = p^{k-1}(p - 1) = p^k\left(1 - \frac{1}{p}\right), \text{ if } p \nmid d.$$

Now combining Theorem 1 and Lemma 2, we have a formula for $\phi(s, d, n)$.

Theorem 2

Let $D(s, d, n)$ be an arithmetic progression with $n = p_1^{a_1} p_2^{a_2} \ldots p_j^{a_j}$. Then, for $n > 1$,

$$\phi(s, d, n) = \begin{cases} n, \text{ if } p_i \mid d \text{ for all } i, \\ n\Pi\left(1 - \frac{1}{p_i}\right) \text{ for all } p_i \nmid d. \end{cases}$$

Remark: $\phi(s, d, n)$ is independent of the first element in the progression $D(s, d, n)$.

The following corollaries are immediate.

Corollary 1

$$\phi(n) = \phi(1, 1, n) = n\Pi\left(1 - \frac{1}{p}\right).$$

Corollary 2

If $(n, d) = 1$, then $\phi(s, d, n) = \phi(n)$.

Corollary 3

Let a and b be any two positive integers. Then

$$\phi(ab) = \phi(a)\phi(s, a, b) = \phi(b)\phi(s, b, a).$$

Now we return to the arbitrary progression $P(x, d, n)$. Let $\Phi(x, d, n)$ denote the number of elements in $P(x, d, n)$ that are relatively prime to n. The proof of the following result is immediate.

Theorem 3

Suppose $P(x, d, n)$ is an arbitrary progression with $(x, d) = g$. Then

(i) If $(g, n) \neq 1$, then $\Phi(x, d, n) = 0$,

(ii) If $(g, n) = 1$, then $\Phi(x, d, n) = \Phi\left(\frac{x}{g}, \frac{d}{g}, n\right)$.

REFERENCES

1. H. L. Alder. "A Generalization of the Euler's ϕ-Function." *American Math. Monthly* 65 (1958):690-692.

2. Eckford Cohen. "Generalizations of the Euler ϕ-Function." *Scripta Math.* 23 (1957):157-161.

3. V. L. Klee, Jr. "A Generalization of Euler's ϕ-Function." *American Math. Monthly* 55 (1948):358-359.