

The ϕ -function and a preview of primitive roots

Learning Objectives. By the end of class, students will be able to:

- Prove that $\phi(m)\phi(n) = \phi(mn)$ when $(m, n) = 1$.

Reading None

Turn In Paper 2

Quiz (10 min)

The Euler ϕ -function (20 min)

We will use ?? as an outline to prove

Theorem 1 (Theorem 3.2). Let m and n be positive integers where $(m, n) = 1$. Then $\phi(mn) = \phi(m)\phi(n)$.

maybe works?

Proof First, we note that an integer a is relatively prime to mn if and only if it is relatively prime to m and n , since m and n (together) have the same prime divisors as mn .

We can partition the positive integers less than mn into

$$\begin{array}{ccccccc} 0 & \equiv m & \equiv 2m & \equiv \cdots \equiv (n-1)m & \pmod{m} \\ 1 & \equiv m+1 & \equiv 2m+1 & \equiv \cdots \equiv (n-1)m+1 & \pmod{m} \\ 2 & \equiv m+2 & \equiv 2m+2 & \equiv \cdots \equiv (n-1)m+2 & \pmod{m} \\ \vdots & \vdots & \vdots & \vdots & \\ m-1 & \equiv 2m-1 & \equiv 3m-1 & \equiv \cdots \equiv nm-1 & \pmod{m} \end{array}$$

For any b in the range $0, 1, 2, \dots, m-1$, define s_b to be the number of integers a in the range $0, 1, 2, \dots, mn-1$ such that $a \equiv b \pmod{m}$ and $\gcd(a, mn) = 1$. For each equivalence class b , $\gcd(b, m) \mid km + b$ by linear combination. Thus, $s_b = 0$ if $(b, m) > 1$. If $\gcd(b, m) = 1$, the arithmetic progression, $\{b, m+b, 2m+b, \dots, (n-1)m+b\}$ contains n elements. By ??, the arithmetic progression is a ?? modulo n , so $\phi(n)$ elements are relatively prime to n and thus mn .

Thus, can see that when $(b, m) = 1$, $s_b = \phi(n)$ and when $(b, m) > 1$, $s_b = 0$.

Since all of the positive integers less than or equal to mn is in exactly one of the congruence classes above and the s_i count how many integers in each congruence class are relatively prime to mn , $\phi(mn) = s_0 + s_1 + \cdots + s_{m-1}$.

Since $\phi(m)$ of the $s_i = \phi(n)$ and the rest are 0, $\phi(mn) = s_0 + s_1 + \cdots + s_{m-1} = \phi(m)\phi(n)$. ■

In-class Problem 1 Complete the proof of ?? by proving that, if m, n , and i are positive integers with $(m, n) = (m, i) = 1$, then the integers $i, m+i, 2m+i, \dots, (n-1)m+i$ form a complete system of residues modulo n .

Learning outcomes:
Author(s): Claire Merriman