The Euler ϕ-function

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

- Use Euler's Theorem to find the least nonnegative residue modulo a composite
- Use Euler's Theorem to find the multiplicative inverse of an integer modulo m
- Prove $\phi(4)\phi(5) = \phi(20)$ using an outline that mirrors the proof that $\phi(m)\phi(n) = \phi(mn)$ when $(m, n) = 1$.

We will also find a formula for $\phi(n)$ in general. The following exercise will outline the general proof:

In-class Problem 1 Let us prove that $\phi(20) = \phi(4)\phi(5)$. First, note that $\phi(4) = \boxed{2}$ and $\phi(5) = \boxed{4}$, so we will prove $\phi(20) = \boxed{8}$.

(a) A number a is relatively prime to 20 if and only if a is relatively prime to $\boxed{4}$ and $\boxed{5}$. The first blank should be smaller than second blank for the automatic grading to work.

Hint: *The number in each blank should be relevant to what we are trying to show.*

(b) We can partition the positive integers less that or equal to 20 into

$$\begin{aligned} 1 \equiv \boxed{5} \equiv \boxed{9} \equiv \boxed{13} \equiv \boxed{17} &\pmod 4 \\ 2 \equiv \boxed{6} \equiv \boxed{10} \equiv \boxed{14} \equiv \boxed{18} &\pmod 4 \\ 3 \equiv \boxed{7} \equiv \boxed{11} \equiv \boxed{15} \equiv \boxed{19} &\pmod 4 \\ 4 \equiv \boxed{8} \equiv \boxed{12} \equiv \boxed{16} \equiv \boxed{20} &\pmod 4 \end{aligned}$$

For any b in the range $1, 2, 3, 4$, define s_b to be the number of integers a in the range $1, 2, \ldots, 20$ such that $a \equiv b \pmod 4$ and $\gcd(a, 20) = 1$. Thus, $s_1 = \boxed{4}$, $s_2 = \boxed{0}$, $s_3 = \boxed{4}$, and $s_4 = \boxed{0}$.

We can see that when $(b, 4) = 1$, $s_b = \phi(\boxed{4})$ and when $(b, 4) > 1$, $s_b = \boxed{0}$.

(c) $\phi(20) = s_1 + s_2 + s_3 + s_4$. Why?

Free Response: Every positive integers less that or equal to 20 is counted by exactly one s_b.

(d) We have seen that $\phi(20) = s_1 + s_2 + s_3 + s_4$, that when $(b, 4) = 1$, $s_b = \boxed{\phi(5)}$, This blank is asking for a function, not a number. and that when $(b, 4) > 1$, $s_b = \boxed{0}$. To finish the "proof" we show that there are $\phi(\boxed{4})$ integers b where $(b, 4) = 1$. Thus, we can say that $\phi(20) = \boxed{\phi(4)\phi(5)}$.

In-class Problem 2 Repeat the same proof for m and n where $(m, n) = 1$.

Solution: Let m and m be relatively prime positive integers. A number a is relatively prime to mn if and only if a is relatively prime to $\boxed{m}$ and $\boxed{n}$.

Learning outcomes:

Author(s): Claire Merriman

We can partition the positive integers less that or equal to mn into

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

For any b in the range $1, 2, 3, \ldots, m$, define s_b to be the number of integers a in the range $1, 2, \ldots, mn$ such that $a \equiv b \pmod{m}$ and $\gcd(a, mn) = 1$. Thus, when $(b, m) = 1$, $s_b = \phi(\boxed{m})$ and when $(b, m) > 1$, $s_b = \boxed{0}$.

Free Response: Since every positive integers less that or equal to mn is counted by exactly one s_b, $\phi(mn) = s_1 + s_2 + \cdots + s_m$.

We have seen that $\phi(mn) = s_1 + s_2 + \cdots + s_m$, that when $(b, m) = 1$, $s_b = \boxed{\phi(n)}$, This blank is asking for a function, not a value. and that when $(b, m) > 1$, $s_b = \boxed{0}$. Since there are $\phi(\boxed{m})$ integers b where $(b, m) = 1$. Thus, we can say that $\phi(mn) = \boxed{\phi(m)\phi(n)}$.