Euler's phi function

Definition 16. Euler's phi function $\phi(n)$ denotes the number of integers in $\{1, 2, ..., n\}$ that are relatively prime to n.

In other words, $\phi(n)$ counts how many residues are invertible modulo n.

Example 17. Compute $\phi(n)$ for $n = 1, 2, ..., 8$.

Solution. $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$.

Observation. $\phi(n) = n - 1$ if and only if n is a prime.
This is true because $\phi(n) = n - 1$ if and only if n is coprime to all of $\{1, 2, ..., n-1\}$.

Observation. If p is a prime, then $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.

This is true because, if p is a prime, then $n = p^k$ is coprime to all $\{1, 2, ..., p^k\}$ except $p, 2p, 3p, ..., p^k$ (the multiples of p, of which there are $p^k / p = p^{k-1}$ many).

If the prime factorization of n is $n = p_1^{k_1} \cdots p_r^{k_r}$, then $\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$.

Why is this true?

- We observed above that the formula is true if $n = p^k$ is a prime power.
- On the other hand, for composite n, say $n = ab$, we have: $\boxed{\phi(ab) = \phi(a)\phi(b) \text{ if } \gcd(a, b) = 1}$
  This is a consequence of the Chinese remainder theorem. (Review if necessary! We'll use it later but will only review it briefly then.)

The above formula follows from combining these two observations. Can you fill in the details?

Example 18. Compute $\phi(35)$.

Solution. $\phi(35) = \phi(5 \cdot 7) = \phi(5)\phi(7) = 4 \cdot 6 = 24$

Example 19. Compute $\phi(100)$.

Solution. $\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) = (2^2 - 2^1) \cdot (5^2 - 5^1) = 40$

[Alternatively: $\phi(100) = \phi(2^2 \cdot 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$]

Example 20. Compute $\phi(1000)$.

Solution. $\phi(1000) = \phi(2^3) \cdot \phi(5^3) = (8 - 4)(125 - 25) = 400$

[Alternatively: $\phi(1000) = \phi(2^3 \cdot 5^3) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400$.]

Armin Straub
straub@southalabama.edu