Number Theory
Fall 2023

A Totient Identity

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. If $a \equiv b \pmod{n}$, then $a = b + nk$ for some $k \in \mathbb{Z}$, so that

$$(a, n) = (b + kn, n) = (b, n)$$

by the bi-periodicity of the GCD. It follows that the function $x \mapsto (x, n)$ is constant on any given congruence class $a + n\mathbb{Z}$ so that the set

$$\{a + n\mathbb{Z} \mid (a, n) = d\}$$

is well-defined for any positive $d|n$, and we have a partition (disjoint union)

$$\mathbb{Z}/n\mathbb{Z} = \coprod_{d|n} \{a + n\mathbb{Z} \mid (a, n) = d\} \tag{1}$$

of $\mathbb{Z}/n\mathbb{Z}$. We can count the size of each "part" using the φ-function as follows.

If $a \in \mathbb{Z}$ and $(a, n) = d$, then $(a/d, n/d) = 1$ and $\frac{1}{d}(a + n\mathbb{Z}) = \frac{a}{d} + \frac{n}{d}\mathbb{Z} \in \mathbb{Z}/\frac{n}{d}\mathbb{Z}$. We therefore have a map

$$\begin{array}{rcl} \{a + n\mathbb{Z} \mid (a, n) = d\} & \to & (\mathbb{Z}/\frac{n}{d}\mathbb{Z})^\times \\ a + n\mathbb{Z} & \mapsto & \frac{a}{d} + \frac{n}{d}\mathbb{Z}, \end{array}$$

which is clearly a bijection (multiplication by d is its inverse). It follows at once that

$$\varphi(n/d) = \left|\{a + n\mathbb{Z} \mid (a, n) = d\}\right|.$$

Applying this to the partition (1) we find that

$$n = |\mathbb{Z}/n\mathbb{Z}| = \left|\coprod_{d|n} \{a + n\mathbb{Z} \mid (a, n) = d\}\right| = \sum_{d|n} \left|\{a + n\mathbb{Z} \mid (a, n) = d\}\right| = \sum_{d|n} \varphi(n/d).$$

Since n/d runs through the positive divisors of n as d does, we finally conclude that

$$\varphi(n) = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d). \tag{2}$$

More carefully, the map $d \mapsto n/d$ is an involution (self-inverse function) on the set of positive divisors of n. Therefore the images n/d permute the set of divisors of n, and we obtain (2). This identity will be an essential ingredient in our proof of the existence of "primitive roots" modulo primes.