The Exponential Structure of Arithmetic mod $m$: Euler’s Theorem

One of the fundamental features of mod $m$ arithmetic is that it carries the structure of a **ring** (congruence classes can be added and multiplied; addition is commutative, associative, has additive identity 0 and additive inverses for every object; multiplication is commutative, associative, and has multiplicative identity 1). However, as we have seen, arithmetic modulo a prime is even more striking since it carries the structure of a **field** (in addition to all the properties of a ring, every nonzero element has a multiplicative inverse).

If $p$ is prime then every nonzero congruence class has a multiplicative inverse; if $m$ is composite, then in addition to the 0 congruence class, the congruence class of any divisor of $m$ will fail to be invertible mod $m$. Euler defined the function

$$\varphi(n) = \# \text{ of invertible congruence classes mod } n$$

$$= \# \text{ of integers between 1 and } n \text{ that are relatively prime to } n$$

which he called the **totient function**, but is also known today as **Euler’s } \varphi \text{ function**. Notice that we must always have that $\varphi(n) \leq n - 1$. But our remarks above can be restated to say that
**Proposition**  $p$ is prime iff $\varphi(p) = p - 1$.  //

**Proposition**  If $p$ is a prime number, then

$$\varphi(p^e) = p^{e-1}(p-1) = p^e \left(1 - \frac{1}{p}\right).$$

**Proof**  Since there are exactly $p^{e-1}$ multiples of $p$ between 1 and $p^e$, $\varphi(p^e) = p^e - p^{e-1}$.  //

To extend this computation to all integers, we prove a very important property of the function:

**Theorem**  If $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

**Proof**  Let $U_m = \{ a \mid 1 \leq a \leq n, (a, m) = 1 \}$ (the set of units mod $m$) so that $|U_m| = \varphi(m)$. Then we also have $|U_n| = \varphi(n)$ and $|U_{mn}| = \varphi(mn)$. Consider now the function $f: U_{mn} \rightarrow U_m \times U_n$ that maps $x \in U_{mn}$ to the ordered pair $(a, b)$ of standard residues of $x$ mod $m$ and mod $n$. (Since $x \in U_{mn}$, $x$ is relatively prime to $mn$, so it is also relatively prime to $m$ and to $n$, so $a \in U_m$ and $b \in U_n$. i.e., this function is well-defined.) But since $(m, n) = 1$, $f$ is one-to-one and onto by the CRT. So,

$$|U_{mn}| = |U_m \times U_n| = |U_m| \cdot |U_n|,$$

and the result follows directly.  //
Corollary If $n$ has prime factorization $n = \prod_{i=1}^{k} p_i^{e_i}$, then $\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$.

So, for instance,

$$\varphi(10800) = \varphi(2^4 \cdot 3^3 \cdot 5^2) = 10800 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 2880.$$ 

Euler used the totient function to prove a generalization of Fermat’s Little Theorem:

Euler’s Theorem If $(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$ 

Proof Consider the map from $U_m$ to $U_m$ that sends $x$ to the standard residue of $ax \mod m$. This map is one-to-one as $ax \equiv ay \pmod{m} \Rightarrow x \equiv y \pmod{m}$. But then, the function must also be onto, since domain and range have the same cardinality. If $U_m = \{x_1, x_2, \ldots, x_{\varphi(m)}\}$, then

$$ax_1 \cdot ax_2 \cdots ax_{\varphi(m)} \equiv x_1 \cdot x_2 \cdots x_{\varphi(m)} \pmod{m}$$

or more simply, $a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} x_i \equiv \prod_{i=1}^{\varphi(m)} x_i \pmod{m}$. By cancelling the invertible product, we deduce that $a^{\varphi(m)} \equiv 1 \pmod{m}$.