Number Theory: Residue Classes

We recall that \( a \equiv b \pmod{m} \) means \( m \mid (a - b) \). As you may have noticed already, ANY integer \( a \) is congruent modulo \( m \) to one of the integers 0, 1, \ldots, \( m - 1 \). Why?

From Lemma 1 (the Division Lemma), we can write ANY integer \( a \) as \( a = qm + r \), where \( 0 \leq r < |m| \); that is, \( q \) and \( r \) are the quotient and remainder of the integer division of \( a \) by \( m \).

So, we have that \( a - r = qm \), i.e., \( a \equiv r \pmod{m} \), where \( 0 \leq r < |m| \).

We therefore have \( m \) distinct sets, denoted by \([0], [1], [2], \ldots, [m - 1]\), such that \([i]\) contains all integers \( a \) such that \( a \equiv i \pmod{m} \), i.e., whose remainder of the integer division by \( m \) is \( i \).
Number Theory: Residue Classes

For instance, let $m = 3$. Then, we have $[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$, $[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$, and $[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

It is clear that, for each $i \in \{0, 1, \ldots, m - 1\}$, we have $i \in [i]$ as $i \equiv i \pmod{m}$.

For any two integers $a$ and $b$ such that $a \in [i]$ and $b \in [i]$ for some $i \in \{0, 1, \ldots, m - 1\}$, we have that $a \equiv b \pmod{m}$. This is because $a \in [i]$ implies $a \equiv i \pmod{m}$ and $b \in [i]$ implies $b \equiv i \pmod{m}$. In turn, $b \equiv i \pmod{m}$ implies $i \equiv b \pmod{m}$. From Theorem 4, we can conclude that $a \equiv b \pmod{m}$.
Number Theory: Residue Classes

For any two integers $a$ and $b$ such that $a \in [i]$ and $b \in [j]$ for some $i, j \in \{0, 1, \ldots, m - 1\}$ with $i \neq j$, we have that $a \not\equiv b \pmod{m}$. Why?

So, each integer $a$ belongs to EXACTLY ONE $[i]$.

The sets $[0], [1], [2], \ldots, [m - 1]$ are called residue classes modulo $m$.

A set of elements, EXACTLY ONE from each residue class modulo $m$, is called a complete residue system modulo $m$.

For instance, $\{0, 1, 2\}$, $\{-6, 7, -1\}$, and $\{3, 4, 5\}$ are all complete residue systems modulo 3.
Suppose that $a$ is an integer prime to the integer $m$, i.e., $gcd(a, m) = 1$. If $a \in [i]$, for some $i \in \{0, 1, \ldots, m - 1\}$, what can we say about $gcd(b, m)$ if $b \in [i]$ and $b \neq a$?

Because $b \in [i]$, we have that $b \equiv a \pmod{m}$; that is, $m \mid (b - a)$. If $d = gcd(b, m)$, then we know that $d \mid m$. As a result, $d$ divides $(b - a)$. But, because $d$ also divides $b$, we have that $d \mid a$.

Now, we know that $d \mid a$ and $d \mid m$. Thus, $d$ must be 1 as $gcd(a, m) = 1$ by hypothesis.

So, if $a \in [i]$ and $gcd(a, m) = 1$, we must have that $gcd(b, m) = 1$ for all $b \in [i]$.
For instance, any integer $a$ in either $[1]$ or $[2]$ is such that $gcd(a, 3) = 1$.

How many residue classes $[i]$ modulo $m$ are there such that $gcd(i, m) = 1$? What if $m$ is composite? What if $m$ is prime?

If $n$ is a positive integer, the Euler $\phi$-function, $\phi(n)$, is defined to be the number of positive integers less than or equal to $n$ and relatively prime to $n$.

So, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$, $\phi(8) = 4$, $\phi(9) = 6$, and $\phi(10) = 4$.

What is the relationship between the value of $\phi$ at $m$, $\phi(m)$, and the number of residue classes $[i]$ modulo $m$ such that $gcd(i, m) = 1$, for $i \in \{0, 1, \ldots, m - 1\}$?
Consider the residue classes \([i]\) modulo \(m\) such that \(gcd(i, m) = 1\). We now know that there are \(\phi(m)\) of them. The set of elements, EXACTLY ONE from each of these residue classes, is called a **reduced residue system modulo** \(m\).

For instance, \(\{1, 2\}, \{7, -1\}\), and \(\{4, 5\}\) are all reduced residue systems modulo 3.

The concept of reduced residue systems plays a crucial role in the proof of the following important theorem:

**Theorem 8 (Euler’s Theorem).** Let \(a\) and \(m\) be any two integers. If \(gcd(a, m) = 1\) then

\[
 a^{\phi(m)} \equiv 1 \pmod{m}.
\]
Number Theory: Fermat’s Little Theorem

We now consider our very last “tool” needed to understand a public-key cryptosystem:

**Theorem 9 (Fermat’s Little Theorem).** If \( p \) is a prime then

\[ n^p \equiv n \pmod{p}. \]

Here is a very short proof:

If \( p \mid n \) then \( n^{p-1} \equiv 0 \equiv n \pmod{p} \). If \( p \notmid n \) then, since \( p \) is a prime, \( \gcd(p, n) = 1 \). By Theorem 8, we know that \( n^{p-1} \equiv 1 \pmod{p} \), as \( \phi(p) = p - 1 \).

Since \( n \equiv n \pmod{p} \), we can use congruence multiplication to conclude that \( n^p \equiv n \pmod{p} \).