Modular Arithmetic Background

1 Introduction

1.1 Modular Congruence and its Properties

To begin the background information, we start by defining modular congruence. We say that two numbers a and b are congruent modulo n, or that their equivalence classes are equal, if their difference is divisible by n:

$$a \equiv b \pmod{n} \iff n | a - b.$$

Recall that $a|b$ means that there is some integer c so that $ac = b$.

Modular congruence is an equivalence relation. This means it is:

- Reflexive: Every element of $\mathbb{Z}_n$ is equivalent to itself.

  Proof. Let $a \in \mathbb{Z}_n$. Then observe that $0 = 0n = (a - a)n$. So $n|a - a$ and $a \equiv a \pmod{n}$. □

- Symmetric: If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

  Proof. Suppose $a \equiv b \pmod{n}$. Then there exists some $k \in \mathbb{Z}$ so that $nk = a - b$. Then $n(-k) = b - a$. So $n|b - a$ and $b \equiv a \pmod{n}$. □

- Transitive: If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

  Proof. Suppose $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then we must have some $k, l \in \mathbb{Z}$ so that $kn = a - b$ and $ln = b - c$. Adding the second equality from the first, we get:

  $$\begin{aligned} kn - ln &= a - b + b - c \\ n(k - l) &= a - c. \end{aligned}$$

  And so we see that $a \equiv c \pmod{n}$. □

The consequence of this is that each element of $\mathbb{Z}_n$ is in exactly one equivalence class. In other words, $[a]_n = [b]_n$, or $[a]_n \cap [b]_n = \emptyset$.

1.2 Modular Arithmetic

In order to do anything useful or interesting with modular arithmetic, we must be able to add and subtract within our expressions. We define these as follows:

- If $a + b = c$, then $a + b \equiv c \pmod{n}$.
- If $ab = c$, then $ab \equiv c \pmod{n}$.

Thanks to these convenient definitions, we inherit convenient properties from the integers:

- $a + 0 \equiv a \pmod{n}$, equivalently: $a - a \equiv 0 \pmod{n}$

  Proof. $a = a + 0$, so $a \equiv a + 0 \pmod{n}$. □

- $1a \equiv a \pmod{n}$.

  Proof. $a = 1a$, so $a \equiv 1a \pmod{n}$. □

  It's important to note that we may not always have a multiplicative inverse, and when we do have one, it may not be unique.

1.3 Inverses

In the same way that we can find additive inverses, $a - a \equiv 0 \pmod{n}$, we seek to find multiplicative ones, so that $aa^{-1} \equiv 1 \pmod{n}$.

It turns out that a^{-1} exists if and only if $\gcd(a, n) = 1$. That is, a and n have no common factors.

Proof. $\implies$: Suppose a is invertible. Then $aa^{-1} \equiv 1 \pmod{n}$, and $n | aa^{-1} - 1$. For some $k \in \mathbb{Z}$, write $nk = aa^{-1} - 1$. Rewriting this we get $1 = aa^{-1} + nk$. We know that 1 is a common divisor of a, n, but we still must show that it is the greatest. Suppose we have another common divisor, d of both a and n.

□