Modular Arithmetic Background

1 Introduction

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 $a \equiv a \pmod{p}$.

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