Modular Arithmetic

Placeholder

June 29, 2020

Note: This handout is for people with little to no experience with modular arithmetic. If you are already familiar with modular arithmetic, feel free to do the problems at the bottom and the ones dispersed throughout.

Introduction

In essence, modular arithmetic is the addition, subtraction, multiplication and sometimes division of the remainders of numbers.

Two numbers are said to be congruent modulo n if their difference is evenly divisible by n. So a is congruent to b modulo n if $n|(a-b)$.
This congruence is written as

$$a \equiv b \pmod{n}.$$

Modular congruences are very similar to regular equations. For instance, you can add two congruences as if they were equations.
If we have $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$ This can be easily proven from the definition of modular congruences.

$$\begin{aligned} a \equiv b \pmod{n} \text{ and } c \equiv d \pmod{n} \\ &\implies n|(a-b) \text{ and } n|(c-d) \\ &\implies n|(a-b)+(c-d) \\ &\implies n|(a+c)-(b+d) \\ &\implies \boxed{a+c \equiv b+d \pmod{n}} \end{aligned}$$

Subtraction and multiplication follow similarly.