Cheatsheet - Modular Arithmetic

Fabio Lama – fabio.lama@pm.me

1. Intro

Modulo is a math operation that finds the remainder when one number is divided by another. Two numbers are *congruent* modulo a given number if they give the same remainder when divided by that number.

If we divide 5 by 3, the remainder is 2. Hence:

$$5 \equiv 2 \mod 3$$

2. Congruence

We say that "a is *congruent* to b modulo n", denoted by:

$$a \equiv b \mod n$$

if n is a divisor of $a - b$, or equivalently, if $n \mid (a - b)$. Similarly, we write:

$$a \not\equiv b \mod n$$

if a is not congruent (or incongruent) to b modulo n, or equivalently, if $n \nmid (a - b)$.

For example:

$$5 \equiv 2 \mod 3$$

$$5 \equiv 5 \mod 3$$

$$5 \equiv 8 \mod 3$$

and negative numbers:

$$5 \equiv 2 \mod 3$$

$$5 \equiv -1 \mod 3$$

$$5 \equiv -4 \mod 3$$

3. Multiplicative Inverse

The modular multiplicative inverse of an integer a modulo n is an integer b such that:

$$ab \equiv 1 \mod n$$

and:

$$a^{n-2} = a^{-1} \mod n$$

Last updated 2022-07-16 17:46:41 UTC