Modular Arithmetic

Mckinley Xie

August 30, 2021

Modular arithmetic was recently removed from the IB curriculum for some reason. That makes me sad. So I'm just going to teach it here!

§1 Introduction

Modular arithmetic is a system of arithmetic when we consider all numbers after they're divided by some fixed number (known as the *modulus*).

An example of a modular system is a clock; 5 hours from 9:00 is 2:00, because 2 is the remainder of $9 + 5 = 14$ when divided by 12.

We'll take a moment to introduce the notation:

Theorem 1.1

We define $a \equiv b \pmod{n}$ (read "a is congrent to b mod n") for integers a, b and positive integer n if $a + kn = b$ for some integer $k \in \mathbb{Z}$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, where $a, b, c, d \in \mathbb{Z}$, then:

1. $a + c \equiv b + d \pmod{n}$
2. $ac \equiv bd \pmod{n}$

(Note that, $\frac{a}{c}$ is not necessarily congruent to $\frac{b}{d}$.)

For example, $2 \equiv 12 \equiv 22 \equiv \cdots \pmod{10}$, and $7 \equiv 18 \equiv 29 \equiv \cdots \pmod{11}$.

Exercise 1.2. Find $25 \mod 6$.

Exercise 1.3. Find the first 3 positive integers congruent to 5 modulo 7.

§2 Sources (and helpful links)

https://brilliant.org/wiki/modular-arithmetic/