CMSC 250
Discrete Structures

Modular Arithmetic

Modular Congruence

Definition

- **a mod n** represents the remainder when an integer **a** is divided by the positive integer **n**.
- **a** is congruent to **b** modulo **n** if **n** divides $a - b$.
- **a** congruent **b** is represented as, $a \equiv b \bmod n$ or $a \equiv_n b$.
- $a \equiv b \bmod n$ if $n|a - b$.

Modular Congruence

Example

- Is 17 congruent to 5 modulo 6?
- Is 24 congruent to 14 modulo 6?

Congruence Theorem

- Theorem: The integers a and b are congruent modulo n if and only if there is an integer k such that $a = b + kn$.
- Theorem: If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then

$$a + c \equiv b + d \pmod{n} \text{ and } ac \equiv bd \pmod{n}$$
$$a - c \equiv b - d \pmod{n} \text{ and } a^m \equiv b^m \pmod{n}$$

Example

$7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$

Equivalences

Theorem: $\forall$ a,b $\in \mathbb{N}$, the following are equivalent:

- $a \equiv_n b$
- $n|(a - b)$
- $(\exists k \in \mathbb{Z})[a = b + kn]$.

Quotient Remainder Theorem

Definition

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d$$

Example

- n = 54, d = 4
- n = -54, d = 4
- n = 54, d = 70

Quotient Remainder Theorem Representation

If we represent integers using the quotient remainder theorem, we observe

Modulus	Forms
2	$2q$, $2q + 1$
3	$3q$, $3q + 1$, $3q + 2$
4	$4q$, $4q + 1$, $4q + 2$, $4q + 3$
....	
k	kq, kq + 1, kq + 2 ... kq + (k-1)

Using quotient remainder theorem

- $\forall n, 2n^2 + 3n + 2$ is not divisible by 5.
- $(\forall n \in \mathbb{Z})[3 \not| n \rightarrow n^2 \equiv_3 1]$

Floor and Ceiling

Definition

- $\forall x \in \mathbb{R}, n \in \mathbb{Z}$

$$\lfloor x \rfloor = n \Leftrightarrow n \leq x < n + 1$$

- $\forall x \in \mathbb{R}, n \in \mathbb{Z}$

$$\lceil x \rceil = n \Leftrightarrow n - 1 < x \leq n$$

Proofs with Floor and Ceiling

- Theorem: $(\forall x \in \mathbb{R})(\forall y \in \mathbb{Z})[\lfloor x + y \rfloor = \lfloor x \rfloor + y]$
- Theorem: The floor of (n/2) is either
  a) n/2 when n is even, or
  b) (n-1)/2 when n is odd.

Sequences, Summations and Products

Practice finding an explicit formula

Figure out the formula for this sequence:

$$1, -\frac{1}{4}, \frac{1}{9}, -\frac{1}{16}, \frac{1}{25}, \ldots$$