CS 70 Discrete Mathematics and Probability Theory
Summer 2025 Tate

DIS 1C

Modular Arithmetic Intro I

Note 6

Modular arithmetic: working number "mod m": restrict to only $\{0, 1, \ldots, m-1\}$; other numbers are *equivalent* to some number in this set.

Think of a clock; "13-o'clock" is the same as "1-o'clock"; $2m$ is the same as m, which is the same as 0. We can go the other way too; 0 is the same as $-m$, etc.

Saying $a \equiv b \pmod{m}$ means:

- a, b have same remainder when divided by m
- $a = b + km$ for some integer k
- $m \mid (a-b)$

Operations: Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Addition/subtraction: $a \pm c \equiv b \pm d \pmod{m}$

Multiplication: $ac \equiv bd \pmod{m}$

Exponentiation: $a^k \equiv b^k \pmod{m}$. You *cannot* apply the mod to the exponent.

There is no division; there are multiplicative inverses though: $x^{-1} \equiv a \pmod{m}$ means $ax \equiv 1 \pmod{m}$.

1 Party Tricks

Note 6

You are at a party celebrating your completion of the CS 70 midterm. Show off your modular arithmetic skills and impress your friends by quickly figuring out the last digit(s) of each of the following numbers:

(a) Find the last digit of 11^{3142}.

(b) Find the last digit of 9^{9999}.

(c) Find the last digit of 3^{641}.

2 Modular Potpourri

Note 6

Prove or disprove the following statements:

(a) There exists some $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{16}$ and $x \equiv 4 \pmod{6}$.

(b) $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{12}$.

(c) $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{6}$.

3 Modular Inverses

Note 6

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod{m}$, then we say x is an **inverse of** a **modulo** m.

Now, we will investigate the existence and uniqueness of inverses.

(a) Is 3 an inverse of 5 modulo 14?

(b) Is 3 an inverse of 5 modulo 10?

(c) For all $n \in \mathbb{N}$, is $3 + 14n$ an inverse of 5 modulo 14?

(d) Does 4 have an inverse modulo 8?

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod{m}$?

4 Wilson's Theorem

Note 6

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

(a) Prove that $(p-1)! \equiv -1 \pmod{p}$ if p is prime. As a hint, consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

(b) Prove that $(p-1)! \equiv -1 \pmod{p}$ only if p is prime. As a hint, if p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?