CS 70 Discrete Mathematics and Probability Theory
Fall 2026 Hug, Sabin

# DIS 2

## Modular Arithmetic Intro I

Note 5

**Modular arithmetic**: working number "mod $m$": restrict to only $\{0, 1, \ldots, m-1\}$; other numbers are *congruent* 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 the 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 Buzzer Tournament

Note 5

A and B are partners in a buzzer-style quiz tournament. There are 20 questions in each round of the tournament, and only one of the partners (whoever comes up with an answer sooner) can hit the buzzer to answer each question. A and B have completed some number of rounds and have now solved the 7th question of the current round. While the parts below may be answered with algebra, try answering them using modular arithmetic relationships.

(a) Is it possible for A and B to have answered the same number of questions over the entirety of the tournament so far?

(b) Is it possible for B to have answered twice as many questions as A over the entirety of the tournament so far?

(c) A and B have now completed the 8th question of the current round. Is it possible for A and B to have answered the same number of questions over the entirety of the tournament so far?

**Solution:**

Let $x$ be the number of questions A has answered so far in the tournament and $y$ be the number of questions B has answered so far in the tournament. Since each round has 20 questions and they have just solved the 7th question of the current round,

$$x + y \equiv 7 \pmod{20}.$$

(a) No. If A and B have answered the same number of questions, then $x = y$. We have that

$$2y \equiv 7 \pmod{20}.$$

For this equation to have a solution, we'd need $\gcd(2,20) = 2$ to divide 7. Since 7 is odd, 2 does not divide 7, so no solution exists. Thus, A and B cannot possibly have answered the same number of questions so far in the tournament.

(b) Yes. If B has answered twice as many questions as A, then $y = 2x$. We have that

$$3x \equiv 7 \pmod{20}.$$

Since $\gcd(3,20) = 1$, we know that 3 has a unique multiplicative inverse mod 20, guaranteeing us a unique solution. We find the multiplicative inverse of $3 \pmod{20}$:

$$3 \cdot 7 = 21 \equiv 1 \pmod{20},$$

so $3^{-1} \equiv 7 \pmod{20}$. Multiplying both sides by $3^{-1}$:

$$x \equiv 7 \cdot 7 = 49 \equiv 9 \pmod{20}.$$

Hence, $x = 9, y = 18$ is a solution (indeed $9 + 18 = 27 \equiv 7 \pmod{20}$). Thus, B could have answered twice as many questions as A.

(c) Yes. If A and B have answered the same number of questions, then $x = y$. Since they've now completed the 8th question of the current round, $x + y \equiv 8 \pmod{20}$, so

$$2y \equiv 8 \pmod{20}.$$

We can rewrite this equivalence as an equation:

$$2y = 8 + 20k$$

for some arbitrary integer $k$. Since all terms are divisible by 2, we can simplify the equation by factoring and canceling out 2 from both sides:

$$y = 4 + 10k.$$

Returning to the modular form $y \equiv 4 \pmod{10}$, we find that $y = 4$ is a solution. Thus, A and B could have answered the same number of questions.

## 2 Modular Inverses

Note 5

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. For each of your answers, write Yes or No, and briefly explain your answer.

(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 5 have an inverse modulo 10?

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

**Solution:**

(a) Yes, because $3 \cdot 5 = 15 \equiv 1 \pmod{14}$.

(b) No, because $3 \cdot 5 = 15 \equiv 5 \pmod{10}$.

(c) Yes, because $(3 + 14n) \cdot 5 = 15 + 14 \cdot 5n \equiv 15 \equiv 1 \pmod{14}$.

(d) No. $\gcd(5, 10) = 5 \neq 1$, so 5 does not have an inverse modulo 10.

(e) No. We have $xa \equiv x'a \equiv 1 \pmod{m}$. So

$$xa - x'a = a(x - x') \equiv 0 \pmod{m}.$$

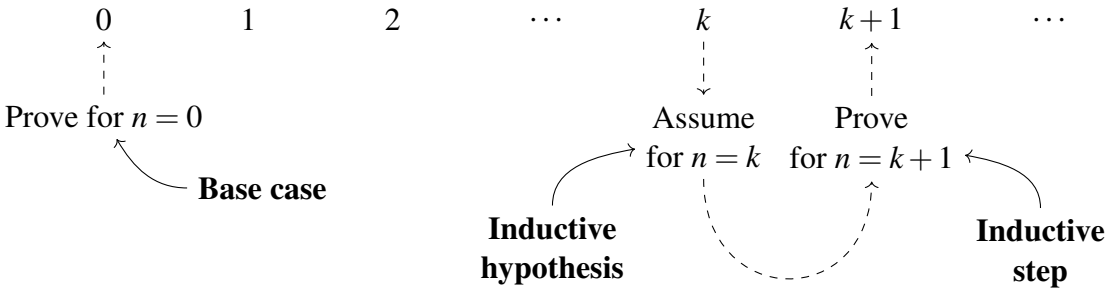
Multiply both sides by $x$, we get

$$xa(x-x') \equiv x \cdot 0 \pmod{m}$$
$$\implies x - x' \equiv 0 \pmod{m}$$
$$\implies x \equiv x' \pmod{m}$$

# Induction Intro

Note 4

Another key proof technique is induction. The general steps for induction are the following: base case, inductive hypothesis, inductive step.




Important point: *do not say* "Assume the claim holds for all $n$, ..." as the inductive hypothesis. The $k$ is arbitrary but is *fixed*.

**Strong induction**: assume for all $n \leq k$ instead of just $n = k$; use this when we need more than $n = k$ to prove the IS. Note that strong induction works whenever weak induction works.

**Strengthening the IH**: sometimes we can't prove with just the IH as is; proving something stronger can actually be easier. This is because a stronger IH gives us more to work with when trying to prove the IS.

# 3 Invalid Induction

Note 4

All of the induction proofs below are incorrect. For each proof, explain clearly the logical error. Simply saying that the claim or the induction hypothesis is false is *not* a valid explanation of what is wrong with the proof.

(a) **Claim:** For all positive numbers $n \in \mathbb{R}$, $n^2 \geq n$.

*Proof.* The proof will be by induction on $n$.
*Base Case:* $1^2 \geq 1$. It is true for $n = 1$.
*Inductive Hypothesis:* Assume that $n^2 \geq n$.
*Inductive Step:* We must prove that $(n+1)^2 \geq n+1$. Starting from the left hand side,

$$\begin{aligned}(n+1)^2 &= n^2 + 2n + 1 \\ &\geq n + 1.\end{aligned}$$

Therefore, the statement is true. □

(b) **Claim:** For all nonnegative integers $n$, $2n = 0$.

*Proof.* We will prove by strong induction on $n$.
*Base Case:* $2 \times 0 = 0$. It is true for $n = 0$.
*Inductive Hypothesis:* Assume that $2k = 0$ for all $0 \leq k \leq n$.
*Inductive Step:* We must show that $2(n+1) = 0$. Write $n+1 = a+b$ where $0 < a, b \leq n$. From the inductive hypothesis, we know $2a = 0$ and $2b = 0$, therefore,

$$2(n+1) = 2(a+b) = 2a + 2b = 0 + 0 = 0.$$

The statement is true. □

(c) **Claim:** In a group of $n$ horses, all horses are the same color.

*Proof.* The proof will be by induction on $n$.
*Base Case:* $n = 1$; There is only one horse, so there is only one color.
*Inductive Hypothesis (I.H):* Assume that $k$ horses are the same color.
*Inductive Step:* We must prove that $k+1$ horses are the same color. Consider a group of k+1 horses and two arbitrary horses A and B in the group.

- Consider the group with horse A excluded. By the I.H., the remaining k horses, including B, are the same color.
- Consider the group with horse B excluded. By the I.H., the remaining k horses, including A, are the same color.

Since the remaining k horses overlap between the two scenarios, A and B must also be the same color. Thus, we have shown that when k horses are the same color, k + 1 horses are also the same color.

□

**Solution:**

(a) Note that $n$ is a real number. The proof is incorrect because it does not consider $0 < n < 1$, for which the claim is false. Also, by the way it is set up, it can only cover integers for $n \geq 1$.

(b) The proof is incorrect because when $n = 0$, we cannot write $n+1 = 1 = a+b$ where $0 < a, b \leq n = 0$.

(c) The proof is incorrect because it fails when $k+1 = 2$. Here, A and B make up the entire group, so excluding either will leave the one other horse behind ($k = 1$). While the base case ensures that each horse is its own color, there is no overlap between the remaining horses, so we cannot say that A and B are the same color.

# 4 Weak is Strong

Note 4

In this problem, we will prove that weak induction and strong induction are equivalent.

(a) State the principles of weak induction and strong induction for an arbitrary predicate $P(n)$ on $\mathbb{N}$. What two implications must you prove to establish that these principles are equivalent?

(b) Prove that weak induction is equivalent to strong induction.

**Solution:**

(a) The Principle of Weak Induction can be written as:

$$\big[P(0) \wedge \forall n \in \mathbb{N}\,\big(P(n) \implies P(n+1)\big)\big] \implies \forall n \in \mathbb{N} P(n).$$

The Principle of Strong Induction can be written as:

$$[P(0) \wedge \forall n \in \mathbb{N}\,([P(0) \wedge P(1) \wedge \cdots \wedge P(n)] \implies P(n+1))] \implies \forall n \in \mathbb{N} P(n).$$

To show that these are equivalent, we need to show that each induction principle implies the other:

Weak Induction $\implies$ Strong Induction and Strong Induction $\implies$ Weak Induction.

(b) (i) *Weak Induction $\implies$ Strong Induction:* Assume the principle of weak induction holds. Let $P$ be a predicate such that $P(0)$ holds and, for every $n \in \mathbb{N}$,

$$(P(0) \wedge P(1) \wedge \cdots \wedge P(n)) \implies P(n+1).$$

Define $Q(n) = P(0) \wedge P(1) \wedge \cdots \wedge P(n)$. We will prove $Q(n)$ for all $n \in \mathbb{N}$ by weak induction.

*Base Case:* $Q(0) = P(0)$ holds by assumption.

*Inductive Hypothesis:* Assume $Q(k)$ holds.

*Inductive Step:* If $Q(k)$ holds, then $P(0), \ldots, P(k)$ are all true, so $P(k+1)$ is true by assumption. Thus $Q(k+1)$ is true.

By weak induction, $Q(n)$ holds for all $n \in \mathbb{N}$, so $P(n)$ holds for all $n \in \mathbb{N}$.

(ii) *Strong Induction* $\implies$ *Weak Induction:* Assume the principle of strong induction holds. Let $P$ be a predicate such that $P(0)$ holds and $P(n) \implies P(n+1)$ for every $n \in \mathbb{N}$. We will prove $P(n)$ for all $n \in \mathbb{N}$ by strong induction.

*Base Case:* $P(0)$ holds by assumption.

*Inductive Hypothesis:* Assume $P(0), P(1), \ldots, P(k)$ all hold.

*Inductive Step:* Since $P(k)$ holds, $P(k+1)$ is true by our assumption.

By strong induction, $P(n)$ holds for all $n \in \mathbb{N}$.

# 5 A Coin Game

Note 4

Your "friend" Stanley Ford suggests you play the following game with him. You each start with a single stack of $n$ coins. On each of your turns, you select one of your stacks of coins (that has at least two coins) and split it into two stacks, each with at least one coin. Your score for that turn is the product of the sizes of the two resulting stacks (for example, if you split a stack of 5 coins into a stack of 3 coins and a stack of 2 coins, your score would be $3 \cdot 2 = 6$). You continue taking turns until all your stacks have only one coin in them. Stan then plays the same game with his stack of $n$ coins, and whoever ends up with the largest total score over all their turns wins.

Prove that no matter how you choose to split the stacks, your total score will always be $\frac{n(n-1)}{2}$. (This means that you and Stan will end up with the same score no matter what happens, so the game is rather pointless.)

**Solution:**

We can prove this by strong induction on $n$.

**Base Case**: If $n = 1$, you start with a stack of one coin, so the game immediately terminates. Your total score is zero–and indeed, $\frac{n(n-1)}{2} = \frac{1 \cdot 0}{2} = 0$.

**Inductive Step**: Suppose that if you start with $i$ coins (for $i$ between 1 and $n$ inclusive), your score will be $\frac{i(i-1)}{2}$ no matter what strategy you employ. Now suppose you start with $n+1$ coins. In your first move, you must split your stack into two smaller stacks. Call the sizes of these stacks $s_1$ and $s_2$ (so $s_1 + s_2 = n+1$ and $s_1, s_2 \geq 1$). Your end score comes from three sources: the points you get from making this first split, the points you get from future splits involving coins from stack 1, and the points you get from future splits involving coins from stack 2. From the rules of the game, we know you get $s_1 s_2$ points from the first split. From the inductive hypothesis (which we can apply because $s_1$ and $s_2$ are between 1 and $n$), we know that the total number of points you get from future splits of stack 1 is $\frac{s_1(s_1-1)}{2}$ and similarly that the total number of points you get from future splits of stack 2 is $\frac{s_2(s_2-1)}{2}$, regardless of what strategy you employ in splitting them. Thus, the total number of points we score is

$$\begin{aligned} s_1 s_2 + \frac{s_1(s_1-1)}{2} + \frac{s_2(s_2-1)}{2} &= \frac{s_1(s_1-1) + 2s_1 s_2 + s_2(s_2-1)}{2} \\ &= \frac{\big(s_1(s_1-1) + s_1 s_2\big) + \big(s_2(s_2-1) + s_1 s_2\big)}{2} \\ &= \frac{s_1(s_1+s_2-1) + s_2(s_1+s_2-1)}{2} \\ &= \frac{(s_1+s_2)(s_1+s_2-1)}{2} \end{aligned}$$

Since $s_1 + s_2 = n+1$, this works out to $\frac{(n+1)(n+1-1)}{2}$, which is what we wanted to show your total number of points came out to. This completes our proof by induction.