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?

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?

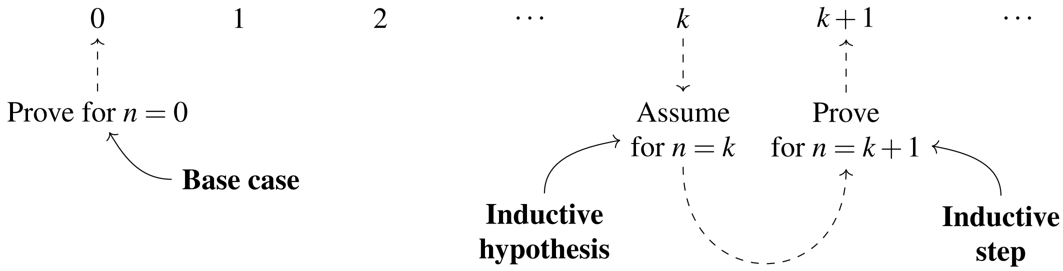
(d) Does 5 have an inverse modulo 10?

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

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. □

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.

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.)