CMSC 250H - Homework 5, Writing Proofs, Induction, Recurrences

March 4, 2026

Homework 5 - Problem 2

Definition

g is a generator of $\{1, \ldots, n-1\}$ (the multiplicative group mod n), if there exists $k \in \mathbb{Z}$ such that

$$g^k = a$$

for all $a \in \{1, \ldots, n-1\}$

- $p = 521$
- $g = 3$ is a generator
- $g = 43$ is not a generator
- Should have seen more repeated secrets for 43 because 43^{ab} takes on less values mod 521

Problem 3 – a)

Proof.

Assume to the contrary that $10^{1/3}$ is rational. Then for $a, b \in$ we have that

$$10^{1/3} = \frac{a}{b}$$

with a, b sharing no common factors, for if they did, we could simply remove those to obtain new a and b. Cubing both sides we obtain:

$$10 = \frac{a^3}{b^3} \implies 10b^3 = a^3$$

Problem 3 – a) $10^{1/3}$ is irrational

Proof.

So 10 divides a, and $a = 10k$ for some $k \in$. Plugging back in for a, we obtain

$$10b^3 = (10k)^3 \implies 10b^3 = 10^3k^3 \implies b^3 = 10^2k$$

So 10 divides b. However, we assumed that a and b shared no common factors, a contradiction. Thus, $10^{1/3}$ must be irrational $\square$

Problem 3 – b) $10^{1/3}$ is irrational using UF

Proof.

Suppose by way of contradiction that $10^{1/3}$ is rational. Then, for $a, b \in$, we have

$$10^{1/3} = \frac{a}{b}$$

Let $p_1 p_2 \dots p_k$ denote the prime factors of either a or b, and let the unique prime factorizations of a, b be

$$a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$
$$b = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$$

Then, we have that

$$10(p_1^{b_1} p_2^{b_2} \dots p_k^{b_k})^3 = (p_1^{a_1} p_2^{a_2} \dots p_k^{a_k})^3$$

$$\implies 10 \cdot p_1^{3b_1} p_2^{3b_2} \dots p_k^{3b_k} = p_1^{3a_1} p_2^{3a_2} \dots p_k^{3a_k}$$

Problem 3 – bs)

Proof.

Since, $10 = 2 \cdot 5$, the exponent for $p_i = 2$ is

$$3a_i + 1$$

on the left hand side, and

$$3b_i$$

on the right hand side. Since these exponents need to match due to unique prime factorization, we need

$$3a_i + 1 = 3b_i$$

for some $a_i, b_i \in^+$. However, this can never be the case since the left is $1 \mod 3$ and the right is $0 \mod 3$. This contradiction proves no such a, b can exist, hence $10^{1/3}$ must be irrational. □

Problem 3 – c) $101^{1/4}$ is irrational

Proof.

Assume by way of contradiction that $101^{1/4}$ is rational. Then, there exists $a, b \in$, uniquely factored, such that

$$101^{1/4} = \frac{a}{b} \implies 101b^4 = a^4$$

Let $p_1 p_2 \dots p_k$ denote the prime factors of either a or b, and let the unique prime factorizations of a, b be

$$a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$
$$b = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$$

Problem 3 – c)

Proof.

Thus, substituting in, we obtain

$$101 \cdot p_1^{4b_1} p_2^{4b_2} \dots p_k^{4b_k} = p_1^{4a_1} p_2^{4a_2} \dots p_k^{4a_k}$$

Since 101, is prime, it must be that the exponent for $p_i = 101$ is odd on the left hand side, and even on the right. This contradicts unique prime factorization, thus $10^{1/4}$ must be irrational. □

Problem 4) $p^{1/3}$ is irrational using UF

Proof.

Suppose by way of contradiction contrary that $p^{1/3}$ is rational. Then there exists $a, b \in$ with $\gcd(a, b) = 1$, such that

$$p^{1/3} = \frac{a}{b} \implies pb^3 = a^3$$

Let $p_1 p_2 \dots p_k$ denote the prime factors of either a or b, and let the unique prime factorizations of a, b be

$$a = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$
$$b = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$$

Problem 4)

Proof.

Then, substituting, we obtain:

$$p \cdot p_1^{3b_1} p_2^{3b_2} \dots p_k^{3b_k} = p_1^{3a_1} p_2^{3a_2} \dots p_k^{3a_k}$$

Then, for $p_i = p$, its exponent on the left hand side is $3b_i + 1$. So, the only possible way the two sides are equivalent is if $3b_i + 1 = 3a_i$. However, there exist no such a_i and b_i satisfying the relation. This results in a contradiction, so $p^{1/3}$ must be irrational. □

What Does a Proof Look Like?

Definition

A proof is a series of statements, each of which follows logically from what has gone before.

Like a good story, a proof has three parts:

1. **Beginning:** Things we assume to be true, including definitions
2. **Middle:** Statements, each following logically from before
3. **End:** The thing we are trying to prove

"We're given the beginning and the end — we have to fill in the middle."

Key Rule: Beginning and End

Golden Rule

The proof should **end** with the thing you're trying to prove.
The proof should **not begin** with the thing you're trying to prove.

It is fine to *announce* what you will prove at the start — but then you must work from the beginning to reach that goal.

Think of it like a story that begins: *"This is a tale of how the hero saved the kingdom"* — the entire story still unfolds from the start.

Common Mistakes (1 & 2)

Mistake 1: Begin at the end, end at the beginning

Writing the steps in *reverse order*. All the right ideas — but completely backwards. The proof never actually arrives anywhere.

Mistake 2: Flying leaps

Jumping from one statement to another without:

- Justifying the leap
- Filling in intermediate steps
- Citing the theorem being used

Common Mistakes (3, 4 & 5)

Mistake 3: Wrong steps that reach a “right” end

Using illegal reasoning to get a correct-looking answer.
The conclusion is not actually proven — it’s an illusion.

Mistake 4: Handwaving

Stating a step in vague English prose instead of mathematical language. Right idea, wrong execution.

Mistake 5: Incorrect logic

- Negating a statement incorrectly
- Proving the *converse* instead of the statement itself

Common Mistakes (6 & 7)

Mistake 6: Incorrect assumption

Starting from a false premise, or using an unjustified assumption mid-proof. Everything after that point is invalid.

Mistake 7: Wrong or missing definitions

Getting a definition wrong (especially avoidable outside of tests).

Example error: Confusing $(g \circ f)(a) = g(f(a))$ with $g(a) \circ f(a)$.

Rule of thumb: Justify enough for your **peers** to understand each step.

Practicalities: How to Find a Proof

Work on rough paper first:

1. **Write out the beginning carefully** — definitions, assumptions, in precise mathematical language
2. **Write out the end carefully** — the exact statement to be proved
3. **Manipulate both ends** — try to make beginning and end look like each other (build the bridge from both sides)
4. **Take big leaps** to see what might work, then fill in smaller steps
5. **Look for familiar patterns** — can you adapt a method you've seen before?

Always **re-read** the proof afterwards

Problem 1

Statement

Prove that for every positive integer n,

$$21 \mid (4^{n+1} + 5^{2n-1}).$$

Problem 1 — Base Case

Base Case: $n = 1$

$$4^{1+1} + 5^{2(1)-1} = 4^2 + 5^1 = 16 + 5 = 21$$

Since $21 \mid 21$, the base case holds.

Problem 1 — Inductive Step

Inductive Hypothesis

Assume for some positive integer k: $\quad 21 \mid (4^{k+1} + 5^{2k-1})$.

Inductive Step: $n = k + 1$

$$\begin{aligned} 4^{k+2} + 5^{2k+1} &= 4 \cdot 4^{k+1} + 25 \cdot 5^{2k-1} \\ &= 4 \cdot 4^{k+1} + (21 + 4) \cdot 5^{2k-1} \\ &= 4(4^{k+1} + 5^{2k-1}) + 21 \cdot 5^{2k-1} \end{aligned}$$

By the inductive hypothesis, $21 \mid 4^{k+1} + 5^{2k-1}$, and $21 \mid 21 \cdot 5^{2k-1}$.

Therefore $21 \mid (4^{k+2} + 5^{2k+1})$. By PMI, the statement holds. ■

Problem 2

Statement

Prove that for every positive integer n,

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > 2(\sqrt{n+1} - 1).$$

Problem 2 — Base Case

Base Case: $n = 1$

$$2(\sqrt{1+1} - 1) = 2(\sqrt{2} - 1) \approx 0.828$$

Since $1 > 0.828$, the base case holds.

Problem 2 — Inductive Step (1/2)

Inductive Hypothesis

Assume for some $k \geq 1$:

$$\sum_{i=1}^{k} \frac{1}{\sqrt{i}} > 2(\sqrt{k+1} - 1).$$

Inductive Step: $n = k + 1$

$$\sum_{i=1}^{k+1} \frac{1}{\sqrt{i}} = \sum_{i=1}^{k} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{k+1}} > 2(\sqrt{k+1} - 1) + \frac{1}{\sqrt{k+1}}$$

It suffices to show:

$$2(\sqrt{k+1} - 1) + \frac{1}{\sqrt{k+1}} > 2(\sqrt{k+2} - 1).$$

Problem 2 — Inductive Step (2/2)

Completing the inequality

Rearranging, we need:

$$\frac{1}{\sqrt{k+1}} > 2(\sqrt{k+2} - \sqrt{k+1}).$$

Multiplying both sides by $(\sqrt{k+2} + \sqrt{k+1})$:

$$\frac{\sqrt{k+2} + \sqrt{k+1}}{\sqrt{k+1}} > 2(\sqrt{k+2} - \sqrt{k+1})(\sqrt{k+2} + \sqrt{k+1}) = 2$$

This simplifies to:

$$1 + \frac{\sqrt{k+2}}{\sqrt{k+1}} > 2 \implies \sqrt{k+2} > \sqrt{k+1}$$

which holds for all $k \geq 1$. By PMI, the statement holds. ■

Problem 3

Sequence

$$a_n = \begin{cases} 1 & n = 1 \\ 3 & n = 2 \\ a_{n-2} + 2a_{n-1} & n \geq 3 \end{cases}$$

Statement

Prove that a_n is odd for all integers $n \geq 1$.

Problem 3 — Solution

Base Cases

$a_1 = 1$ is odd. $a_2 = 3$ is odd. Base cases hold.

Inductive Hypothesis

Assume a_i is odd for all $1 \leq i \leq k$ (for some $k \geq 2$).

Inductive Step: $n = k + 1$

$$a_{k+1} = a_{k-1} + 2a_k$$

By the IH, $a_{k-1} = 2h + 1$ and $a_k = 2m + 1$ for some $h, m \in \mathbb{Z}$. So:

$$a_{k+1} = (2h + 1) + 2(2m + 1) = 2h + 4m + 3 = 2(h + 2m + 1) + 1$$

Thus a_{k+1} is odd. By PMI, the statement holds. ■

Problem 4

Sequence

$$a_n = \begin{cases} 1 & n = 1 \\ 2 & n = 2 \\ \sum_{i=1}^{n-1} (i-1)\, a_i & n \geq 3 \end{cases}$$

Statement

Prove that $a_n = (n-1)!$ for all integers $n \geq 3$.

Problem 4 — Base Case & Hypothesis

Base Case: $n = 3$

$$a_3 = (1-1)(1) + (2-1)(2) = 0 + 2 = 2 = (3-1)!\checkmark$$

Inductive Hypothesis

Assume for some $k \geq 3$: $\quad a_k = (k-1)!$

Problem 4 — Inductive Step

Inductive Step: $n = k + 1$

$$a_{k+1} = \sum_{i=1}^{k}(i-1)a_i = \sum_{i=1}^{k-1}(i-1)a_i + (k-1)a_k$$

Note that $\sum_{i=1}^{k-1}(i-1)a_i = a_k$. So:

$$a_{k+1} = a_k + (k-1)a_k = (k-1)! + (k-1)(k-1)!$$

$$= (k-1)!\,(1 + k - 1) = (k-1)! \cdot k = k!$$

By PMI, the statement holds. ■

Problem 5 — Setup

Sequence

$$a_n = \begin{cases} 1 & n = 1 \\ 2 & n = 2 \\ \dfrac{a_{n-1}}{a_{n-2}} & n \geq 3 \end{cases}$$

Problem 5(a)

Statement

Prove that for all positive integers n,

$$a_n = \begin{cases} 1 & \text{if } n \equiv 1, 4 \pmod 6 \\ 2 & \text{if } n \equiv 2, 3 \pmod 6 \\ \frac{1}{2} & \text{if } n \equiv 0, 5 \pmod 6 \end{cases}$$

Problem 5(a) — Base Cases & Hypothesis

Base Cases

$n = 1$: $a_1 = 1$ and $1 \equiv 1 \pmod 6$ ✓
$n = 2$: $a_2 = 2$ and $2 \equiv 2 \pmod 6$ ✓

Inductive Hypothesis

Assume for some $k \geq 2$ and all $1 \leq i \leq k$, a_i satisfies the formula above.

Problem 5(a) — Inductive Step

Inductive Step: $n = k + 1$, all cases for $a_{k+1} = a_k / a_{k-1}$

$k-1 \pmod 6$	$k \pmod 6$	a_{k-1}	a_k	a_{k+1}	
0	1	$\frac{1}{2}$	1	2	$(k+1 \equiv 2)$
1	2	1	2	2	$(k+1 \equiv 3)$
2	3	2	2	1	$(k+1 \equiv 4)$
3	4	2	1	$\frac{1}{2}$	$(k+1 \equiv 5)$
4	5	1	$\frac{1}{2}$	$\frac{1}{2}$	$(k+1 \equiv 0)$
5	0	$\frac{1}{2}$	$\frac{1}{2}$	1	$(k+1 \equiv 1)$

All cases hold. By PMI, the statement holds. ■

Problem 5(b)

Statement

Prove that for all nonnegative integers j,

$$\sum_{i=1}^{6} a_{j+i} = 7.$$

Problem 5(b) — Base Case & Hypothesis

Base Case: $j = 0$

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 = 1 + 2 + 2 + 1 + \tfrac{1}{2} + \tfrac{1}{2} = 7 \checkmark$$

Inductive Hypothesis

Assume for some $k \geq 0$: $\displaystyle\sum_{i=1}^{6} a_{k+i} = 7.$

Problem 5(b) — Inductive Step

Inductive Step: $j = k + 1$

$$\sum_{i=1}^{6} a_{k+1+i} = \left(\sum_{i=1}^{6} a_{k+i}\right) + a_{k+7} - a_{k+1} = 7 + a_{k+7} - a_{k+1}$$

Since a_n is periodic with period 6, $k + 7 \equiv k + 1 \pmod 6$, so $a_{k+7} = a_{k+1}$.

$$= 7 + a_{k+1} - a_{k+1} = 7$$

By PMI, the statement holds. ■

Problem 6 — Constructive Induction

Statement

Use Constructive Induction to find constants A, B, C such that

$$\sum_{i=1}^{n}(4i-3) = An^2 + Bn + C.$$

Problem 6 — Finding the Constants

Base Case: $n = 1$

$\sum_{i=1}^{1}(4i-3) = 1$, so $A + B + C = 1$.

Inductive Step

Assuming $\sum_{i=1}^{n}(4i-3) = An^2 + Bn + C$, for $n+1$:

$$An^2 + Bn + C + 4(n+1) - 3 = A(n+1)^2 + B(n+1) + C$$

$$4n + 1 = 2An + A + B$$

Matching coefficients: $4 = 2A \Rightarrow A = 2$, $1 = A + B \Rightarrow B = -1$.
From base case: $C = 1 - A - B = 0$.

Result

Problem 7 — Constructive Induction

Statement

Use Constructive Induction to find constants A, B, C, D such that

$$\sum_{i=1}^{n} i(i+2) = An^3 + Bn^2 + Cn + D.$$

Problem 7 — Finding the Constants

Base Case: $n = 1$

$1(3) = 3$, so $A + B + C + D = 3$.

Inductive Step

Assuming the formula for n, expanding for $n + 1$:

$$n^2 + 4n + 3 = 3An^2 + (3A + 2B)n + (A + B + C)$$

Matching coefficients:

$1 = 3A \Rightarrow A = \frac{1}{3}$, $\quad 4 = 3A+2B \Rightarrow B = \frac{3}{2}$, $\quad 3 = A+B+C \Rightarrow C =$

From base case: $D = 0$.

Result

$\sum_{i}^{n} i(i+2) = \frac{1}{3}n^3 + \frac{3}{2}n^2 + \frac{7}{6}n$ ■

Problem 8 — Constructive Induction

Sequence

$$a_n = \begin{cases} 1 & n = 1 \\ 4 & n = 2 \\ 9 & n = 3 \\ a_{n-1} - a_{n-2} + a_{n-3} + 2(2n-3) & n \geq 4 \end{cases}$$

Statement

Use Constructive Induction to find constants A, B, C such that $a_n = An^2 + Bn + C$.

Problem 8 — Finding the Constants (1/2)

Base Cases

$$\begin{aligned} n = 1: &\quad 1 = A + B + C \\ n = 2: &\quad 4 = 4A + 2B + C \\ n = 3: &\quad 9 = 9A + 3B + C \end{aligned}$$

Inductive Step — Coefficient Matching

Expanding $a_{n+1} = a_n - a_{n-1} + a_{n-2} + 2(2n-1)$ using the IH:

$$(4n - 2) = (4An) + (-2A + 2B)$$

Matching: $4 = 4A \Rightarrow A = 1, \quad -2 = -2A + 2B \Rightarrow B = 0.$

Problem 8 — Finding the Constants (2/2)

Solving for C

Substituting $A = 1$, $B = 0$ into the base cases:

$$1 = 1 + 0 + C \;\Rightarrow\; C = 0$$

All three base cases are consistent with $C = 0$.

Result

$$a_n = n^2 \qquad \blacksquare$$

Problem 9 — Constructive Induction

Statement

Use Constructive Induction to find a constant A such that

$$\sum_{i=1}^{n} \frac{1}{(i+2)(i+3)} \leq An$$

for all positive integers n.

Problem 9 — Finding the Constant

Base Case: $n = 1$

$\frac{1}{(3)(4)} = \frac{1}{12} \leq A(1)$, so we need $A \geq \frac{1}{12}$.

Inductive Step

Assuming $\sum_{i=1}^{n} \frac{1}{(i+2)(i+3)} \leq An$, for $n+1$:

$$An + \frac{1}{(n+3)(n+4)} \leq A(n+1) = An + A$$

We need $\frac{1}{(n+3)(n+4)} \leq A$.

The maximum of the left side occurs at $n = 1$: $\frac{1}{(4)(5)} = \frac{1}{20} < \frac{1}{12}$.