CMSC 250H - Homework 4, Induction

March 9, 2026

CMSC250H

Safe Primes

Definition:
A prime p is a safe prime if

$$\frac{p-1}{2}$$

is also prime.
Example:

- $p = 23$ is safe
- $(23-1)/2 = 11$ which is prime

Safe primes are important in cryptography (Diffie–Hellman groups).

Prime Number Theorem Conjecture

It is known that

$$\pi(n) \approx \frac{n}{\ln n}$$

where $\pi(n)$ is the number of primes $\leq n$.
From experimental data we estimate

$$\pi(n) \approx A\frac{n}{\ln n}$$

Observation from data: A is close to 1.
This matches the Prime Number Theorem.

Safe Prime Growth

From the experimental data we estimate a function $f(n)$ such that

$$\text{safe primes } \leq n \approx f(n)$$

Empirically, safe primes appear much less frequently than primes. Rough heuristic:

$$f(n) \approx \frac{n}{(\ln n)^2}$$

So safe primes are about a factor of $1/\ln n$ rarer than primes.

Generators of Safe Prime Groups

Let p be a safe prime.
We examine numbers $g \in \{1, \ldots, p\}$ and test if g is a generator of the multiplicative group mod p.
For each safe prime we record:

$$p \text{ — generators — fraction of generators}$$

This measures how common generators are.

Generator Conjecture

From experimental data we observe:

$$\text{generators} \approx \alpha p$$

For safe primes

$$\alpha \approx \frac{1}{2}$$

Reason:
For prime p, the number of generators is

$$\varphi(p-1)$$

When p is safe, $p-1 = 2q$ where q is prime, so

$$\varphi(2q) = q - 1 \approx \frac{p}{2}.$$

Fourth Powers Mod 16

We compute

$$0^4, 1^4, 2^4, \ldots, 15^4 \pmod{16}$$

Observation:

- Even numbers give $0 \pmod{16}$
- Odd numbers give $1 \pmod{16}$

So any fourth power mod 16 is either

$$0 \text{ or } 1.$$

Sums of 15 Fourth Powers

Each fourth power is 0 or 1 mod 16.
So the sum of 15 fourth powers can only be

$$0, 1, 2, \ldots, 15 \pmod{16}$$

but never $15 \pmod{16}$.
Thus numbers congruent to 15 mod 16 cannot be written as

$$x_1^4 + x_2^4 + \cdots + x_{15}^4.$$

Infinite Family of Counterexamples

Numbers of the form

$$16k + 15$$

are $15 \pmod{16}$.
Since these cannot be written as sums of 15 fourth powers, there are infinitely many such numbers.
Therefore:

There are infinitely many integers that are not sums of 15 fourth powers.

Ordered Sets with Successors and Predecessors

We construct a subset $D \subseteq \mathbb{R}$.
Example:

$$D = \{2^k : k \in \mathbb{Z}\} \cup \{-(2^k) : k \in \mathbb{Z}\}$$

Looks like:

$$\ldots, -4, -2, -1, -\tfrac{1}{2}, -\tfrac{1}{4}, \ldots$$

$$\ldots \tfrac{1}{4}, \tfrac{1}{2}, 1, 2, 4, \ldots$$

Never cross zero! Properties:

- Every element has a predecessor
- Every element has a successor
- There exist $x < y$ for which you can't reach y from a chain of succesors x (ex. 1 and $-\frac{1}{2}$)

Planar Graph Coloring

Known result:

Every planar graph is 4-colorable.

Definition:
A graph has crossing number c if removing c edges makes it planar.

Graphs With Crossing Number c

If removing c edges makes the graph planar:

1. Remove those c edges
2. Color the planar graph with 4 colors
3. Reinsert edges

Each removed edge may require an additional color.
Thus the graph can be colored with

$$f(c) = 4 + c$$

colors.

Conclusion

Key ideas from this homework:

- Experimental mathematics with primes
- Structure of safe primes and generators
- Modular arithmetic arguments
- Constructing ordered sets
- Graph coloring via planar reductions

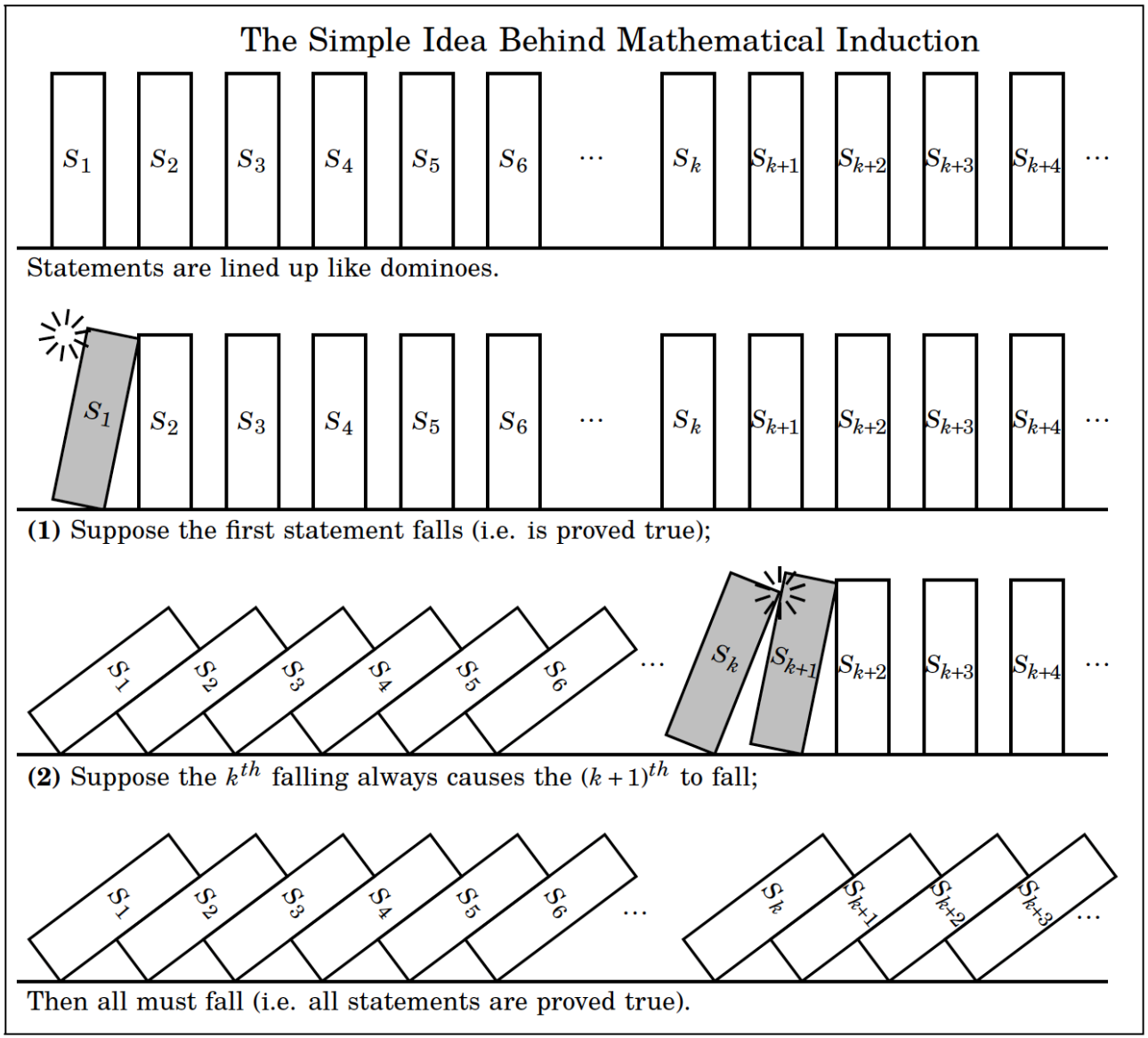
These techniques appear throughout number theory and combinatorics.

CMSC 250H - Homework 4, Induction

March 9, 2026

CMSC250H

Induction


The Simple Idea Behind Mathematical Induction
S_1 S_2 S_3 S_4 S_5 S_6 ⋯ S_k S_{k+1} S_{k+2} S_{k+3} S_{k+4} ⋯
Statements are lined up like dominoes.
S_1 S_2 S_3 S_4 S_5 S_6 ⋯ S_k S_{k+1} S_{k+2} S_{k+3} S_{k+4} ⋯
(1) Suppose the first statement falls (i.e. is proved true);
S_1 S_2 S_3 S_4 S_5 S_6 ⋯ S_k S_{k+1} S_{k+2} S_{k+3} S_{k+4} ⋯
(2) Suppose the k^{th} falling always causes the $(k+1)^{th}$ to fall;
S_1 S_2 S_3 S_4 S_5 S_6 ⋯ S_k S_{k+1} S_{k+2} S_{k+3} ⋯
Then all must fall (i.e. all statements are proved true).

Outline for Inductive Proof

Proposition

The statements $S_1, S_2, S_3 \ldots$ are all true.

1. Prove that the first statement S_1 is true (or several first statements depending on what you need).
2. Given any integer $k \geq 1$, prove that $S_1 \wedge S_2 \wedge S_3 \wedge \ldots \wedge S_k \implies S_{k+1}$ is true
3. It follows that S_n is true for all n

Example

Theorem

For all $n \in \mathbb{N}$

$$\sum_{i=0}^{n} i \cdot i! = (n+1)! - 1$$

Try it yourself!

Solution

Proof.

For $n = 0$, LHS:

$$0 \cdot 0! = 0 \cdot 1 = 0$$

RHS:

$$(0 + 1)! - 1 = 1 - 1 = 0$$

So the statement holds for $n = 0$
Assume it holds for all $0 \leq k < n$. We have

$$\sum_{i=0}^{n} i \cdot i! = \sum_{i=0}^{n-1} i \cdot i! + n \cdot n!$$

Solution

Proof.

By the Inductive Hypothesis

$$\sum_{i=0}^{n-1} i \cdot i! + n \cdot n! = (n-1+1)! - 1 + n \cdot n! = n! - 1 + n \cdot n!$$

Rearranging:

$$\begin{aligned} n! + n \cdot n! - 1 &= n!(n+1) - 1 \\ &= (n+1)! - 1 \end{aligned}$$

Thus, the statement holds for all n. □

Example

Theorem

If $n \in \mathbb{N}$, then 12 divides $n^4 - n^2$

How many base cases do we need for this one?

Intuition

Observe that

$$n^4 - n^2 = n^2(n-1)(n+1)$$

So $n^4 - n^2$ is a product of three consecutive integers $n-1, n, n+1$.
It is known that the product of 3 consecutive integers is divisible by 6.
We also have an extra factor of n:

1. If n is even, then its divisible by 12 immediately.
2. If n is odd, then, $n-1$ and $n+1$ are even, so $4 \cdot 3 = 12$, so it is also divisible by 12.

Idea: We need at least two multiples of 2, one multiple of 3

Solution

Proof.

1. $n = 1, \quad 1^4 - 1^2 = 0$
2. $n = 2, \quad 2^4 - 2^2 = 12$
3. $n = 3, \quad 3^4 - 3^2 = 72$
4. $n = 4, \quad 4^4 - 4^2 = 240$
5. $n = 5, \quad 5^4 - 5^2 = 600$
6. $n = 6, \quad 6^4 - 6^2 = 1260$

All of these are divisible by 12.
Now assume it holds for $6 \leq m \leq n$. For simplicity let $m = n - 5$ □

Solution

Proof.

Then,

$$\begin{aligned}(n+1)^4-(n+1)^2 &= (m+6)^4-(m+6)^2\\ &= m^4+24m^3+216m^2+864m^2+1296-(m^2+12m\\ &= (m^4-m^2)+24m^3+216m^2+852m+1260\\ &= 12(a+2m^3+18m^2+71m+105)\end{aligned}$$

with $m^4-m^2=12a$ by the Inductive Hypothesis. Thus, the statement holds for all n. □

Fibonacci Sequence

Definition

The Fibonacci Sequence is a recursive sequence defined by

$$F(n) = F(n-1) + F(n-2)$$

for $n \geq 2$ with $F(0) = 0$ and $F(1) = 1$

It actually has a closed form as well!

Solving Fibonacci by Guessing

Observe that the roots for the polynomial $x^2 - x - 1$ are

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \beta = \frac{1-\sqrt{5}}{2}$$

We also have that $\alpha^2 = 1 + \alpha$, $\beta^2 = 1 + \beta$ since they are roots.

Theorem

For all n, $\sqrt{5}F(n) = \alpha^n - \beta^n$

Solution

Proof.

Observe that for $n = 0, 1$

$$F(0) = 0 \implies \sqrt{5}F(0) = 0 = \alpha^0 - \beta^0$$

and

$$F(1) = 1 \implies \sqrt{5}F(1) = \sqrt{5} = \alpha - \beta$$

So it holds for $n = 0, 1$ □

Solution

Proof.

Then,

$$\begin{aligned}\sqrt{5}F(n) &= \sqrt{5}[F(n-1)+F(n-2)] \\ &= [\alpha^{n-1}-\beta^{n-1}+\alpha^{n-2}-\beta^{n-2}] \\ &= [\alpha^{n-2}(\alpha+1)-\beta^{n-2}(\beta+1)] \\ &= [\alpha^{n-2}\cdot\alpha^2-\beta^{n-2}\cdot\beta^2] \\ &= \alpha^n-\beta^n\end{aligned}$$

□

So, $\sqrt{5}F(n) = \alpha^n - \beta^n \implies F(n) = \frac{\alpha^n-\beta^n}{\sqrt{5}}$

Classic CS Problem

Suppose we have a $2^n \times 2^n$ board, and we want to tile them with L-shaped trominoes.

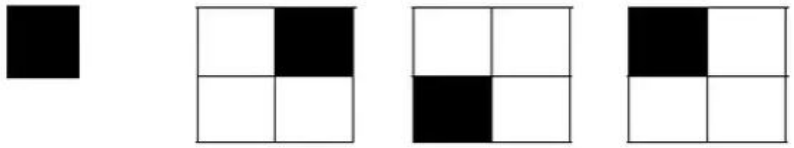


Figure: 2×2

Is it possible to tile the board and only leave one square uncovered?

Proof

Theorem

For all $n \geq 1 \in \mathbb{N}$, a $2^n \times 2^n$ board can be tiled with L-shaped trominoes with only one square remaining.

Proof.

I shall draw it on the board! □