**Basic Info**

- **AM 106 / 206**: (Advanced) Applied Algebra
- **Lecturer**: Madhu Sudan
  
  madhu@cs.harvard.edu
- **TF**: Jaroslaw (Jarek) Blasiok
  
  jblasiok@g.harvard.edu
- **Website**: [http://madhu.seas.harvard.edu/Courses/Fall2016](http://madhu.seas.harvard.edu/Courses/Fall2016)

  (make sure you go over "Announcement" for the course. Important details.)

  (make sure you see calendar to mark quiz dates.)

- Sign Up for course on Piazza
What is this course about

Applied Algebra

will elaborate shortly
(a la Math. 122, 123)

? 

1. More algorithmic/constructive

Algebra:

\[ 3x^5 + 2x^2 - 27 = 0 \]

has at most 5 real solutions.

Algorithmic Question:

- Find them?
- Are there 5? or 3? or 1?
Motivated by (few) applications:
- Crystallography \(\equiv\) Group Theory
- Cryptography \(\equiv\) Number Theory
- Error Correcting \(\equiv\) Fields, Rings, Codes, Polynomials

\[
\text{Algebra} = ?
\]

Study of Sets, with binary operations:
- Integers \(\text{Addition}\)
- Integers \(\text{Multiplication}\)
- Integers \(\text{Add & Multi}\)
- Reals
- Matrices
- Polynomials
- Vectors \(\text{Add}\)
Binary Shings
Permutation
Symmetric g
Crystal

Properties of Operations

Commutativity?
Identity?
Inverse?
Factorization? Unique?

\[ x \oplus y = 1 \text{ if } x + y = 0 \text{ o.w.} \]

Power of abstraction

\[ \exists \text{ bits } x_1, x_2, x_3, x_4 \text{ s.t.} \]

\[ x_1 \oplus x_2 \oplus x_3 = 1 \]

\[ x_2 \oplus x_3 \oplus x_4 = 0 \]

\[ x_1 \oplus x_4 = 0 \]
\[ x_1 \oplus x_2 \oplus x_3 = 1 \]

\[ (x_2 \oplus x_3 \oplus x_4 = 0) \ominus \]

\[ x_1 \ominus x_4 = 1 \oplus 0 = 1 \]

\[ 1 = x_1 \ominus x_4 = 0 \]

\[ 0 \neq 1 ! \]

\[ \text{[same procedure as solving linear system over rationals!]} \]

Abstraction! Will allow us to say what conditions an operation/procedure/algorithm needs.
Aside: Modular Arithmetic

- \( a, m \in \mathbb{N} = \{0, 1, 2, ... \} \)

\( a \mod m = \) remainder when dividing \( a \) by \( m \).

- \( \oplus = + \mod 2 \)

- Modular "Twenty Question with a liar"

\[
\begin{align*}
X \mod 2 & = 1 \quad \text{for} \quad 0 \leq x \leq 10^5 \\
X \mod 3 & = 2 \\
5 & = 4 \\
7 & = 1 \\
11 & = 5 \\
13 & = 2 \\
17 & = 14 \\
19 & = 9 \\
23 & = 10 \\
29 & = 8 \\
31 & = 22
\end{align*}
\]
37  29
41  24
43  34

err... 3 of these ↑ numbers wrong

What is X?

Might see algorithm for this (in last lecture)
Aside: Adminstrivia

- Grading:
  - Weekly Psets - 50% 
    (for late psets ..., see announcements)

- PSET10 out now. Due Friday
  - Does not count (scores delayed)

- PSET 1 - 10: Out Wednesdays
  - Due Tuesday 12am
  - 10% + 10%  = 20%

- 2 quizes, 1 final

- Participation 5%

- AM206: All the above + two essays + 1 presentation
Course Schedule

- Preliminaries: Integers, Induction, Algorithm, O(n) notation, [3 lectures]

- Groups: Sets with one operation ("Multiplication")
  - Integer, Matrices, Permutations, [9 lectures]

- Rings/Fields: Sets with two operations
  - Polynomials, Factorization, codes, ... [9 lectures]
Today: Induction

- Important proof method in discrete math.

- Notation \( \mathbb{N} = \{0, 1, 2, \ldots \} \)
  \( \mathbb{Z} = \{ \ldots -2, -1, 0, 1, 2, \ldots \} \)

- Well-Ordering Principle

  \( \forall S \subseteq \mathbb{N} \exists \text{ minimal element} \)

  - Not true for \( \mathbb{Z} \)
  - Not true for \( \mathbb{R}^{>0} \) — positive reals

- Standard Induction

  \( 0 \in S \quad \text{and} \quad n \in S \implies n+1 \in S \)
Strong Induction

\[ 0 \in S \implies \mathbb{N} \subseteq S \]
\[ \{0, \ldots, n\} \subseteq S \implies n+1 \in S \]

Above are 3 equivalent ways of thinking of induction.

How to use induction

**Lemma:** \( \forall n \in \mathbb{N} \quad 1 + 2 + \ldots + n = \frac{n(n+1)}{2} \)

**Proof:**

Base Case: 

Inductive Step:
Home work

1. Submit PS0
2. Contact staff if taking AM206
3. Sign up on Piazza
4. Read "Announcement" fully.