

AM 106 Lecture 1

Basic Info

AM 106: Applied Algebra

Lecturer: MADHU SUDAN

madsu@cs.harvard.edu

TF: Richard Wang

richardmwang@college....

Website: <http://madsu.seas.harvard.edu/>

Courses/Fall2017

(make sure to read "Announcement".)

(make sure to scan calendar, mark important dates).

Sign up on piazza

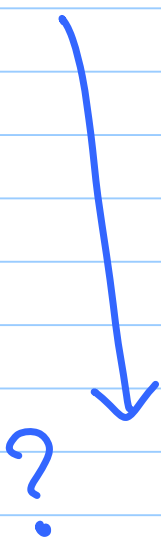
PSO out already!!

Submit by Friday...

(0 points...)

What is this Course about

Applied Algebra



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

(i) More algorithmic / constructive

Algebra:

$$- \quad 3x^5 + 2x^2 - 27 = 0$$

has at most 5 real solutions.

Algorithmic Question:

- find them?

- Are there 5? or 3? or 1?

② Motivated by (few) applications

- Crystallography \Leftarrow Group Theory

- Cryptography \Leftarrow Number Theory

- Error Correcting Codes \Leftarrow Fields, Rings, Polynomials



Algebra = ?

Study of Sets, with binary operations

Integers

Addition

Integers

Multiplication

Integers

Add & Mult

reals

matrices

Polynomials

vectors

Add

Binary Strings

bitwise XOR

Permutations

Composition

Symmetries of
Circuit

..

Properties of Operations

Commutativity?

Identity?

Inverse?

Factorization? Unique?

$$x \oplus y = 1 \text{ if } x \neq y \\ = 0 \text{ o.w.}$$

Power of abstraction

- \exists bits x_1, x_2, x_3, x_4 s.t.

$$x_1 \oplus x_2 \oplus x_3 = 1$$

$$x_2 \oplus x_3 \oplus x_4 = 0$$

$$x_1 \oplus x_4 = 0 \quad ?$$

$$\begin{array}{r}
 x_1 \oplus x_2 \oplus x_3 = 1 \\
 (x_2 \oplus x_3 \oplus x_4 = 0) \oplus \\
 \hline
 = x_1 \oplus x_4 = 1 \oplus 0 = 1
 \end{array}$$

$$1 = x_1 \oplus x_4 = 0$$

$$0 \neq 1 !$$

[Same procedure as solving linear system over rationals !]

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

Aside: Modular Arithmetic

- $a, m \in \mathbb{N} = \{0, 1, 2, \dots\}$

$a \bmod m =$ remainder when dividing a by m .

- $\oplus = + \bmod 2$

- Modular "Twenty Question with a liar"

$X \bmod 2 = 1$ $0 \leq X \leq 10^5$

$X \bmod 3 = 2$

$X \bmod 5 = 4$

$X \bmod 7 = 1$

$X \bmod 11 = 5$

$X \bmod 13 = 2$

$X \bmod 17 = 14$

$X \bmod 19 = 9$

$X \bmod 23 = 10$

$X \bmod 29 = 8$

$X \bmod 31 = 22$

37	29
41	24
43	34

err... 3 of these ↑ numbers wrong

What is X?

Might see algorithm for this (in last lecture)

Aside: Administrivia

- Grading:
 - Weekly Psets - 50%
(for late psets ... see announcement)
 - PSET0 out now. Due Friday
- Does not count (scores/delays)
 - PSET 1 - 10 : Out Wednesdays
Due Tuesday 12am
10% + 10% = 20%
 - 2 quizzes, 1 final
 - Participation 5%
- AM206 : All the above + two essays
+ 1 presentation.

Coarse Schedule

- Preliminaries: Integers, Induction, Algorithm, Oh. notation, [3 lectures]
- Groups: - Sets with one operation ("multiplication")
 - Integers, Matrices, Permutations. [9 lectures]
- Rings/Fields - Sets with two operations
 - Polynomials, Factorization... Codes ... [9 lectures]

TODAY: INDUCTION

• Important proof method in discrete math.

• Notation $\mathbb{N} = \{0, 1, 2, \dots\}$

$\mathbb{Z} = \{\dots -2, -1, 0, 1, 2, \dots\}$

• Well-Ordering Principle

$\forall S \subseteq \mathbb{N} \exists$ minimal element

- Not true for \mathbb{Z}

- Not true for $\mathbb{R}^{\geq 0}$ ← positive reals

• Standard Induction

$0 \in S$

& " $n \in S \Rightarrow n+1 \in S$ "

} $\Rightarrow \mathbb{N} \subseteq S$

• Strong Induction

$$\left. \begin{array}{l} 0 \in S \\ \& \{0, \dots, n\} \subseteq S \Rightarrow n+1 \in S \end{array} \right\} \Rightarrow \mathbb{N} \subseteq S$$

————— ∞ —————

Above ^{are} 3 equivalent ways of thinking of induction

————— ∞ —————

How to use induction

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

Proof:

Base Case: fill this in

Inductive Step: fill this in