Lecture 4D:
Discrete Math Review

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Everyone should've received an email confirming their exam format
- If you're taking the exam in-person show up to Pimentel 1 at 5:50 pm
  - Exam begins at 6 pm
- If you're taking the exam online you should have received a Zoom Link
  - Follow the online proctoring instructions shared on Piazza
  - Exam begins at 6 pm
  - Working past your allotted time (8pm for regular test takers) will be considered academic misconduct
- Answer sheet will be available tomorrow morning. Remote test takers are responsible for printing it out before the exam.

Lecture 1A: Introduction, Proposition Logic

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Course Overview

Course Webpage: www.eecs70.org

Explains policies, calendar for OH, HW, midterm dates, schedule, etc

Course Format

Lecture → Mon-Thu 12:30-2p Dwinelle 155 (and live Zoom/recorded)

Discussion → Mon-Thu. Will cover content from that day's lecture.

Office Hours → See eecs70.org/calendar for location and times. Submit tickets on oh.eecs70.org

Course Overview (cont.)

Software "Media Gallery"

bCourses → Lecture RecordMyS

Gradescope → HWs and Vitamins

Piazza → Questions, Communications, Everything else!

Email: cs70-staff@berkeley.edu → Personal questions, extenuating circumstances, etc

Top Bar Attendance Form → Attendance Credit

Weekly Post

On Piazza. It is required reading every week.

Course Overview (cont.)

Check you are enrolled in these services

bCourses, Piazza, Gradescope. Please email cs70-staff@berkeley.edu if not enrolled.

DSP

You should have received an email from Nikki Suzani. Please email us if you have not.

Incomplete

If you are finishing an incomplete this semester please email us with the conditions of your incomplete.

Assignments

Homework → released weekly on Saturday morning

Due every Thursday. No penalty grace period until Friday 11:59 pm. Graded on accuracy.

Material from last WTh and this MTue

Vitamins → released weekly on Saturday morning

Due every Thursday. No penalty grace period until Friday 11:59 pm Graded on accuracy. Instant feedback on your answers.

Material from this week's MTuWTh lecture

Discussion Attendance

1 point for each discussion. 13 needed for full credit

Exams

Midterm 7/15 Time 6-8p, Final 8/12 Time 6-9p.

We will drop lowest two scores

No alternates

Discussion Attendance	**5%**
Vitamin	**5%**
Homework	**20%**
Midterm	**30%**
Final	**40%**

Website

https://www.eecs70.org/

Lecture | Discussions | Calendar | Policies | Resources | Staff | Attendance | Piazza | Queue

Discrete Mathematics and Probability Theory

CS70 at UC Berkeley, Summer 2022
Jingjia Chen, Michael Psenka, and Tarang Srivastava

Lecture: MTuWTh 12:30 pm - 1:59 pm, Dwinelle 155
Jump to current week

Week	Date	Lecture	Resources	Notes	Discussion	Homework
1	Mon 6/20	*Juneteenth*			Disc 1A, solutions	HW 1, solutions
	Tue 6/21	Introduction, Propositional Logic		Note 0 Note 1	Disc 1B, solutions	
	Wed 6/22	Proofs		Note 2	Disc 1C, solutions	
	Thu 6/23	Induction		Note 3		

Instructors

Tarang: First third of the course

Michael: Secord third of the course

Jingjia: Last third of the course

Tarang Srivastava (he/him)

tarang.sriv@ • website

Hi! I'm a fourth year Math and CS double major. I have been a TA for 5 semesters and Head TA for 3, I'm very excited to be teaching yall this semester!

Michael Psenka (he/him)

psenka@ • website

I'm a 2nd year PhD student in BAIR–I currently work on representation learning in computer vision and robotics. I did my undergrad in math, and I continue to enjoy bringing my math nerdiness into my CS research. Outside of work, I play piano (& attempt at music production), Smash, chess, and snowboard.

Jingjia Chen (she/her)

jingjia.chen@

Collaboration

We highly encourage collaboration! So, let's define what that means. (Professor Sinclair)

Discussing approaches to problems is encouraged!

As long as you reach a good understanding of the final solution

You should not allow concerns for cheating to get in the way of discussing problems with your peers

How we recommend collaborating…

- Post on Piazza and read the relevant homework threads
- Come to OH. It's okay to just chill there even if you have no questions

Cases of Academic Misconduct will be dealt with by the course staff and Center for Student Conduct

Why CS70?

Programming + Microprocessors → Superpower

What are your computers doing?

- Logic and Proofs!
- Ex: Induction = Recursion

What can computers do?

- Work with discrete objects
- Discrete Math → immense applications

Computers learn and interact with the world?

- Probability → Ex: machine learning, data analysis, robotics,

Our goal: ***teach you to think more critically and powerfully…and to deal clearly with uncertainty itself.***

Tips for CS70

READ THE NOTES! READ THE NOTES! READ THE NOTES!

- Reading mathematical text is not the same as reading regular non-fiction.
- Read non-linearly. Jump around. Keep a pencil in hand. Work out examples.
- We will hold specific OH this week to give some tips on how to best read the notes. This is a skill we hope you pickup in this class.
- Reading the notes takes time. Allocate 1-2 hours for each note
- There is a myth that you need “mathematical maturity” to do well in this course.
- Give yourself plenty of time to think about homework problems.

Announcements!

- Join Piazza. Read the Welcome Post
- Discussions start today, signup link is on Piazza Do it today
- Office Hours start today, see course calendar on website
- **HW 1** and **Vitamin 1** have been released, due Thu (grace period Friday)

Propositions: Statements that are true or false

Statement	Is it a proposition?	true/false?
Square root of 2 is irrational	Yes, proposition	true
2 + 2 = 4	Yes, prop.	true
2 + 2 = 3	Yes, prop.	false
Tom Hanks is in Forrest Gump	Yes, prop	true
Tom Hanks is a good actor (fuzzy words)	No its not prop	—
2 + 2	No	—
2 + x = 5 (Free variable)	No	—
Any even > 2 is a sum of 2 primes	Yes, prop	false

Using variables to denote propositions

P = “I am Oski” Q = “I am Carol Christ”

Operation	Symbol	Meaning	Example
Conjunction	$P \wedge Q$	P AND Q must both be true	I am oski and I am carol christ
Disjunction	$P \vee Q$	P OR Q is true	I am oski or I am carol christ
Negation	$\neg P$	not P	I am not OSKI

Truth Tables

A way to systematically record what an operation on propositions is doing.

P	Q	P ∧ Q (AND)	P ∨ Q (OR)	¬P ∨ Q ★	¬P	P ∨ ¬P
T	T	T	T	T	F	T
T	F	F	T	F	F	T
F	T	F	T	T	T	T
F	F	F	F	T	T	T

Law of the excluded middle: P is true or ¬P is true (but not both)

A proposition that is always true tautology $(P \vee \neg P)$

A proposition that is always false contradiction $(P \wedge \neg P)$

Implications

if you stand in the rain, then you will get wet
P ⇒ Q

If P, then Q

P implies Q

P = "You like CS70"

Q = "You like probability"

P	Q	P ⇒ Q
T	T	T
T	F	F
F	T	T
F	F	T

- if you like 70, then you like prob.
- You like CS70 only if you like prob.
- The fact that you like probability is a necessary condition for you to like CS70

Vacuously true

if pigs can fly, then everyone in 70 will get an A

Converse, Inverse and Contrapositive

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	Converse $Q \Rightarrow P$	Inverse $\neg P \Rightarrow \neg Q$	Contrapositive $\neg Q \Rightarrow \neg P$	$P \Leftrightarrow Q$
T	T	F	F	T	T	T	T	T
T	F	F	T	F	T	T	F	F
F	T	T	F	T	F	F	T	F
F	F	T	T	T	T	T	T	T

Converse: if you like prof., then you like 70

Inverse:

Contrapositive

$P \Rightarrow Q \wedge Q \Rightarrow P \equiv P \Leftrightarrow Q$

P if and only if Q

P iff Q

Logical Equivalence

Propositional formula is an expression made up of propositional variables combined with logical operators.

Two propositional formulas are **logically equivalent** if they have the same truth table.

Example:

P	Q	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	$\neg P \vee Q$
T	T	T	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Contraposition is logically equivalent to the implication

$$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P \equiv \neg P \vee Q$$

DeMorgan's Law

$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$

$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$

P	Q	$P \wedge Q$	$\neg(P \wedge Q)$	$\equiv$	$\neg P \vee \neg Q$
T	T	T	F		F
T	F	F	T		T
F	T	F	T		T
F	F	F	T		T

1) $P \wedge (Q \vee R) \equiv ?$

2) $P \wedge (Q \wedge R) \equiv$

3) $(P \wedge Q) \vee (R \wedge S) \equiv ?$

Predicates and Quantifiers

Predicates: Statements with free variables. Ex: Q(x) = "2x is even"

Predicates by themselves are **not** propositions. Adding a quantifier and a universe allows us to state multiple propositions at once.

Example:

for all natural numbers n, $n^2 + n + 41$ is prime

quantifier — universe

$(\forall n \in \mathbb{N})(n^2 + n + 41 \text{ is prime})$

$0^2 + 0 + 41$ is prime

$1^2 + 1 + 41$ is prime

$2^2 + 2 + 41$ is prime

⋮

From Note 0:

$\mathbb{N} = 0, 1, 2, 3 \ldots$

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

$\mathbb{Z}^+ = 1, 2, 3, 4 \ldots$

$\mathbb{Q}$: p/q for $p, q \in \mathbb{Z}$

$\mathbb{R}$: Real numbers

$S = \{\heartsuit, \triangle, \square\}$

“For All” and “Exists”

$\forall$ “For all” means for all the values in the universe P(x) is true

$\exists$ “Exists” means there is at least one value x in the universe for which P(x) is true

Practice "Every nonzero rational number can be multiplied by some rational number to get 1"

"get mad"

$$(\forall q \in \mathbb{Q} \setminus \{0\})(\exists x \in \mathbb{Q})(q \cdot x = 1)$$

$\forall q \in \mathbb{Q}$ such that $q \neq 0$

Logical Equivalence with Quantifiers

$P(x, y)$

$\mathbb{N}$

$\exists x \, \exists y \; P(x, y) \equiv \exists y \, \exists x \; P(x, y)$

$\exists x \in S > y$

the number multiples of x are 1 more than y to that function

$\forall x \, \exists y \; P(x, y) \not\equiv \exists x \, \forall y \; P(x, y)$

there is always a bigger number

such a x that all the numbers are greater than it

$y > x$

$P(x, y) = y > x$

Universe $= \mathbb{Z}$

DeMorgan's Law for Quantifiers

$$\neg(\forall x \in S)\, P(x) \equiv (\exists x \in S)\, \neg P(x)$$

Example:

$P(x)$ $x^2 > 10$

$S = \{1, 2, 3, 4\}$

Review

Lecture 1B: Proofs

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Join Piazza. Read the Welcome Post
- Lecture is posted under “Media Gallery” in bCourses
- Evelyn’s 6-7 pm discussion is now hybrid
- Signup and attend discussion
- **HW 1** and **Vitamin 1** have been released, due Thu (grace period Friday)

Should be up around 4pm
Linked on website

What is a proof?

$P \Rightarrow K \Rightarrow S \Rightarrow ? \Rightarrow \ldots \Rightarrow Q$

A **proof** is a finite list of statements, each of which is logically implied by the previous statement, to establish the truth of some proposition.

The power here is that using *finite* statements, we can guarantee the truth of a statement with *infinitely* many cases.

Do it during lecture

Advice: When writing proofs, imagine a very skeptical friend is reading over your proof who questions every statement you make.

Since you're learning, try to be more formal in your proof writing

How to prove things?

Structure	How to generally prove it
$P \wedge Q$	Prove P and prove Q
$(P \Rightarrow Q)$	Assume P is true, then show the Q follow (also true)
$P \iff Q$ (P iff Q)	Prove $P \Rightarrow Q$ and prove $Q \Rightarrow P$
$(\exists x \in S)\ P(x)$	Provide some $x \in S$ and prove $P(x)$
$(\forall x \in S)\ P(x)$	Let x be arbitrary in S and prove $P(x)$

You can also replace the proposition to be proved with something logically equivalent that has a different structure.
Example: $P \Rightarrow Q$, $\neg P \vee Q$ $\neg Q \Rightarrow \neg P$ Contrapositive

Direct Proof (Example 1)

Theorem: For every natural number there is a natural number greater than it

Proof:

$$\forall n \in \mathbb{N}, \exists m \in \mathbb{N}(m > n)$$

Let n be an arbitrary natural number.
Observe that $n+1$ is also a natural number.
Since, $n+1 > n$ we have found a natural number greater than n. Since, n was arbitrary the statement holds $\forall n \in \mathbb{N}$.

Goal: $P \Rightarrow Q$
Method: Assume P
⋮ steps
Conclude Q

things we assumed
1) $n+1$ is natural
2) $n+1 > n$

Direct Proof (Example 2)

$a \mid b$ if no remainder

Definition: For $a, b \in \mathbb{Z}$ we say $a|b$ iff $\exists q \in Z$ such that $b = aq$ (iff $\Leftrightarrow$ $P \Rightarrow Q$)

Theorem: For any $a, b, c \in \mathbb{Z}$ if $a|b$ and $a|c$ then $a|(b-c)$

Proof:

Let $a, b, c \in \mathbb{Z}$ be arbitrary and assume $a|b$ and $a|c$. So, by definition $b = aq_1$ and $c = aq_2$ for some $q_1, q_2 \in \mathbb{Z}$. Then, $b - c = aq_1 - aq_2 = a(q_1 - q_2)$. Since $q_1 - q_2 \in \mathbb{Z}$ it follows by definition that $a|(b-c)$

Lesson: Use your definitions!

Scratch work

$a|b$ $a|c$

$b = aq_1$ $c = aq_2$

$b - c = aq_1 - aq_2$

$= a(q_1 - q_2)$

$q_1 - q_2 \in \mathbb{Z}$

$b - c = aq_3$

$a|(b-c)$

Proof by Contraposition

Definition: $n \in \mathbb{Z}$ is even if $\exists k \in \mathbb{Z}$ such that $n = 2k$
Definition: $n \in \mathbb{Z}$ is odd if $\exists k \in \mathbb{Z}$ such that $n = 2k + 1$
Theorem: For every $n \in \mathbb{Z}$ if n^2 is even, then so is n. (P) (Q)
Proof:
Let n be an integer. We will proceed by contraposition and show that if n is odd then n^2 is odd. By definition, $n = 2k+1$ for $k \in \mathbb{Z}$
then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
Since, $2k^2 + 2k \in \mathbb{Z}$ by definition n^2 is odd. □

Useful

$\forall x\, P(x) \Rightarrow \forall y\, P(y)$

$\neg(\forall y\, P(y)) \Rightarrow \neg(\forall x\, P(x))$

$\exists y\, \neg P(y) \Rightarrow \exists x\, \neg P(x)$

Let's try directly

$n^2 = 2k$ $\quad n = \sqrt{2k}$??

Contrapositive

Goal: $P \Rightarrow Q$
Method: prove $\neg Q \Rightarrow \neg P$

Contrapose:

if n is odd, then n^2 is odd

$n = 2k+1$

$n^2 = 4k^2 + 4k + 1$

$n^2 = 2(2k^2 + 2k) + 1$

$2k^2 + 2k \in \mathbb{Z}$

Proof by Cases (Example 1)

Theorem: For all $n \in \mathbb{N}$, $3|(n^3 - n)$

Proof:

Let $n \in \mathbb{N}$

Case 1: $n = 3k$ $\quad k \in \mathbb{N}$

$n^3 - n = (n)(n-1)(n+1)$

$= 3k(3k-1)(3k+1)$

$\in \mathbb{N}$ thus $3|n^3-n$

Case 2: $n = 3k-1$

$n^3 - n = (3k-1)(3k-1-1)(3k-1+1)$

$\hookrightarrow 3|n^3-n$

Case 3: $n = 3k+1$

$n^3 - n = (3k+1)(3k+1-1)(3k+1+1)$

$\hookrightarrow 3|n^3-n$

Goal: P

Method: $R_1 \vee \ldots \vee R_n$ true

Show $R_1 \Rightarrow P$

⋮

Show $R_n \Rightarrow P$

Scratch Work

$n^3 - n = 3q$

$n(n^2-1) = 3q$

$n(n-1)(n+1) = 3q$

$2^3 - 2 = 8 - 2 = 6$

$3^3 - 3 = 27 - 3 = 24$

$2(2-1)(2+1) = 6 = 3(2)$

$3(3-1)(3+1) = 24 = 3(8)$

$4(4-1)(4+1) = \ldots$

$5(5-1)(5+1) = \ldots$

$6(6-1)(6+1) \ldots$

$7(7-1)(7+1)$

Proof by Cases (Example 2)

$r \in \mathbb{Q}$ iff $r = \frac{p}{q}$

Definition: A real number r is **rational** if there are $p, q \in \mathbb{Z}$ such that $q \neq 0$ and $r = \frac{p}{q}$. Otherwise, r is **irrational**.

Theorem: There exist irrational x and y such that x^y is rational.

Proof:

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Then, we are done, $x = y = \sqrt{2}$

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

Since 2 is rational for $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ we've found an example that satisfies the claim.

Assumed $\sqrt{2}$ is irrational

Proof by Contradiction

A ***proof by contradiction*** proves a proposition "P" by first assuming "*not* P" is true. That is, the opposite of *P* is true.

Then, it follows logical steps to arrive at a contradiction by proving both some proposition "R" and "*not* R".

Why does this work?

Goal: P

Method: Assume ¬P

R is true

¬R is true

¬P ⇒ R ∧ ¬R ≡ F

P	¬P	F	¬P ⇒ F
T	F	F	T
F	T	F	F

¬P ⇒ F ≡ P

⇓

T ⇒ P

T	P	T ⇒ P
T	T	T

always true

what we're going here.

this from proof

Proof by Contradiction (Example 1)

Definition: A real number r is **rational** if there are $p, q \in \mathbb{Z}$ such that $q \neq 0$ and $r = \frac{p}{q}$. Otherwise, r is **irrational**.

Theorem: $\sqrt{2}$ is irrational

Proof:

Assume for contradiction that $\sqrt{2}$ is rational. Then, by definition $\sqrt{2} = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$. p, q share no common factors. $2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2$. So, by def. p^2 is even. From an earlier thm, if p^2 is even, then p is even. So, $p = 2k$ for some $k \in \mathbb{Z}$ $(2k)^2 = 4k^2 = 2q^2 \Rightarrow q^2 = 2k^2$. q^2 is then even, so q is even. This is a contradiction since p and q share a common factor of 2. Thus, $\sqrt{2}$ must be irrational.

$q = 2j$ $j \in \mathbb{Z}$

$\frac{1}{2}$

$\frac{p}{q} = \sqrt{2}$

Proof by Contradiction (Example 2)

NOT COVERED DURING LECTURE

Theorem: There's infinite prime numbers

Proof:

Every non-prime number has a prime divisor (ask students)

Assume for contradiction there are finite prime numbers. That is $p_1, p_2, \ldots, p_n$ are all the prime numbers. Let $q = p_1 \cdot p_2 \cdot \ldots \cdot p_n$

Consider $q+1$. Clearly $q+1 > p_n$, where p_n is the largest prime number. So $q+1$ is not prime, thus it has a prime divisor. That is, there exists some prime $x \mid q+1$. Since x is prime, $x \in \{p_1, \ldots, p_n\}$ and $x \mid q$. By previous Lemma 1, if $x \mid q$ and $x \mid q+1$, then $x \mid (q+1-q)$. That is, $x \mid 1$ but only ± 1 and $x \neq 1$. This is a contradiction, so there must be infinitely many prime numbers.

Incorrect Proof

Theorem: $1 = 2$

Proof: For $x = y$ we have

$$x^2 - xy = x^2 - yz$$

$$x(x-y) = (x-y)(x+y)$$

Divide by zero since $x = 0$

$$x = x + y$$

$$x = 2x$$

$$1 = 2$$

Summary

NOT COVERED DURING LECTURE

Proof Technique	General Procedure
Direct Proof	Goal : $P \Rightarrow Q$ Method: Assume P : steps Conclude Q
Proof by contraposition	Goal : $P \Rightarrow Q$ Method : prove $\neg Q \Rightarrow \neg P$
Proof by contradiction	Goal : P Method: Assume $\neg P$: Prove R : Prove $\neg R$
Proof by cases	Goal : P Method : Show $R_1 \vee \ldots \vee R_n$ is true Show $R_1 \Rightarrow P$: Show $R_n \Rightarrow P$

Few notes about what we did today

Write full proofs in your homework like we did today, but on discussion you can just write an outline/sketch of the proof.

No one gets the complete proof immediately, there's a lot of scratch work and thinking before you can write the proof.

Remember! Every step in your proof must be justified and follow from previous steps.

Usually how things go:

1. Think about problem
2. Do some scratch work
3. Come up with solution
4. Try to write a proof
5. Realize solution is wrong

FAQ

How do I get started?

Think about the definitions that may be relevant. Maybe a theorem or lemma that was in the notes.

I'm stuck?

Try doing a bit of scratch work to see if you missed some pattern. Read over what you currently have in the proof. Try proving an easier statement or an intermediary statement.

Is my proof correct?

Question every statement. Does it follow from a definition or previous statement?

Review

Lecture 1C: Induction

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

~4pm lecture will be up

- Lecture is posted under “Media Gallery” in bCourses
- **HW 1** and **Vitamin 1** have been released, due **Today** (grace period Friday)

question q

What is induction?

Goal in induction is to prove some statement for all natural numbers

$$(\forall n \in \mathbb{N}), P(n)$$

Principle of Induction

- Base Case: **Prove P(0)**
- Inductive Hypothesis: **Assume P(n)**
- Inductive Step: **Prove P(n) ⇒ P(n+1)**

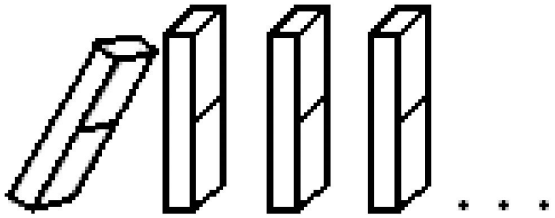
these get combined

Direct Proof $P \Rightarrow Q$

Assume P → Q

Visual Analogy

Prove all the dominos fall down



- $P(0)$ = "First domino falls"
- $P(k) \Rightarrow P(k+1)$ "kth domino falls implies that $k+1$st domino falls"

Even if you had infinite dominos lined up, this method would prove all of them will fall down (More on this Week 4).

Simple Induction (Example 1)

Base Case
Inductive Hypothesis
Inductive Step

Theorem: For all natural numbers n, $0 + 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$

Proof:

Base Case: $n = 0$ $\quad 0 = \frac{0(0+1)}{2} = 0$ ✓

Ind. Hyp.: Assume for some $n = k \geq 0$ it is true that $0 + 1 + \ldots + k = \frac{k(k+1)}{2}$

Ind. Step: Prove that for $n = k+1$ the claim holds

$$1 + 2 + \ldots + (k+1) = \frac{(k+1)(k+2)}{2}$$

$$\left[1 + 2 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1)\right] = \frac{k^2+k+2k+2}{2} = \frac{(k+1)(k+2)}{2}$$

The second equality holds from the inductive hypothesis. Thus, the theorem holds by induction.

Simple Induction (Example 2)

Theorem: For all $n \in \mathbb{N}$, $3|(n^3 - n)$

Proof:

We induct on the variable n

Base Case: $n=0$ $\quad 3 | 0^3 - 0$. This is trivially true.

Ind. Hyp: For $n=k$ assume $3|k^3-k$ i.e. $\exists q$ s.t. $k^3-k = 3q$

Ind. Step.: We wish to show that for $n=k+1$ $\quad 3|(k+1)^3-(k+1)$

$(k+1)^3-(k+1) = 3p \qquad p \in \mathbb{N}$

$k^3 + 3k^2 + 3k + 1 - (k+1) = 3p$

$k^3 - k + 3k^2 + 3k = 3p$

$3q + 3k^2 + 3k$ From the Ind. hyp.

$3(q + k^2 + k) = 3p$ by def. it follows that $(k+1)^3-(k+1)$ is divisible by 3 $\square$

$q + k^2 + k \in \mathbb{N}$

$p = q + k^2 + k$

Simple Induction (Example 3)

Theorem: Any map formed by dividing the plain into regions by drawing *straight* lines can be properly colored with two colors

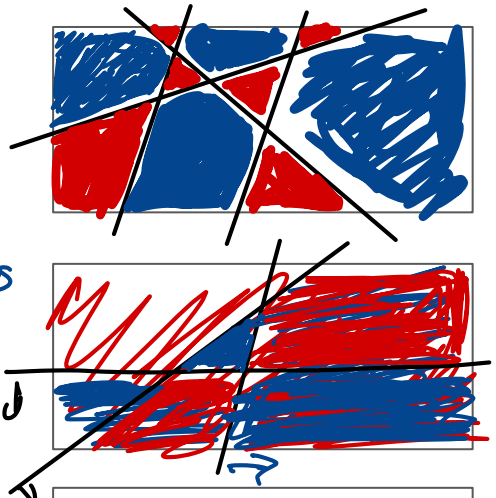
Proof: We will induct on the number of lines. Let n # of lines

Base Case: $n = 0$ Color the whole plain one colon

Ind Hyp: For $n = k$ lines assume it is two colorable

Ind Step: Consider an arbitrary map with $k+1$ lines. Then, remove one line from the map. By Ind. hyp. this new map with k lines is two colorable. Then, add back the line that was removed and flip all the colors on one side of the line.

By construction all the regions adjacent to the line that was added have different colors. Then, the region that was not flipped is correctly colored by hyp. That was flipped, is also two colored by hypothesis since we just changed the labellings.



Improving Induction Hypothesis (Example 1)

"strengthen"

Theorem: The sum of the first n odd numbers is a perfect square

Improved: The sum of the first n odd numbers is n^2

Proof:

Base Case $n = 1 = 1^2$ ✓

Ind Hyp: Assume $\underbrace{1 + 3 + 5 + \cdots + (2k-1)}_{\text{first } k \text{ odds}} = k^2$

Ind Step: Wish to show

$$\underbrace{1 + 3 + 5 + \cdots + (2k-1)}_{k^2} + (2k+1) = (k+1)^2$$

$k^2 + 2k + 1$ by hyp.

$(k+1)^2$ = ✓ □

$1 = 1^2$

$1 + 5 = 2^2$

$1 + 3 + 5 = 3^2$

$1 + 3 + 5 + 7 = 4^2$

$\vdots$

$n = k$

$1 + 3 + \cdots + (2k-1) = k^2$

$k^2 + 2k + 1 = (k+1)^2$

Improving Induction Hypothesis (Example 2)

notes :

Theorem: For all $n \geq 1$, $\sum_{i=1}^{n} \frac{1}{i^2} \leq 2$

Improved:

Proof:

What is Strong Induction?

Goal: ∀n P(n)

Principle of Strong Induction

- Base Case: **Prove P(0)**
- Inductive Hypothesis: **Assume P(0) and P(1) and ... and P(n)**
- Inductive Step: **Prove P(0) and ... and P(n) ⇒ P(n+1)**

$P(0) \wedge P(1) \wedge \ldots \wedge P(n) \Rightarrow P(n+1)$

Strong induction is implied by weak induction

Strong Induction (Example 1)

prime factorization

Theorem: Every natural number greater than 1 can be written as a product of one or more primes

Proof:

Base Case: $n = 2$. 2 is prime so it's prime factorization is just 2

Ind. Hyp: Assume claim holds for all $1 < n \leq k$

Ind. Step: let $n = k+1$

Case 1: $k+1$ is prime. We are done

Case 2: $k+1$ is composite. Therefore, $\exists a, b \in \mathbb{N}$, $k+1 = a \cdot b$

Since $k+1 > 1 \Rightarrow 1 < a, b < k+1$. Then, by the ind. hyp. a and b can be written as a product of primes. Thus, $k+1$ can be written as a product of a and b's primes.

□

Strong Induction with Multiple Base Cases (Example 2)

Theorem: For every natural number $n \geq 12$, it holds that $n = 4x + 5y$ for some $x, y \in \mathbb{N}$

Proof:

Base Cases $n = 12$

$12 = 4(3) + 5(0)$

$13 = 4(2) + 5(1)$

$14 = 4(1) + 5(2)$

$15 = 4(0) + 5(3)$

$12 = 4(3) + 5(0)$ $x = 3, y = 0$ ✓

Ind Hyp: Assume claim holds for all $12 \leq n \leq k$

Ind Step: $n = k+1 \geq 16$. Then, $(k+1) - 4 \geq 12$

By the Ind. Hyp. $(k+1) - 4 = 4x' + 5y'$ for some $x', y' \in \mathbb{N}$

$k+1 = 4x' + 5y' + 4 = 4(x'+1) + 5y'$. So, then we can set $x = x'+1$ and $y = y'$

$k+1 = 4x + 5y$

□

CHT

$n = 12$ ✓

$k = 4x + 5y$

$4(x+1) + 5(y+1)$

$k+1 = 4x' + 5y'$

$16 = 12 + 4$

$4x + 5y$

$4(x+1) + 5y$

$4x + 5y + 4$

$4(x+1) + 5y$

Why ever use weak induction?

Weak Induction ⇒ Strong Induction

If you wanted to you could always use strong induction

It is nicer to only use weak induction if strong induction is not needed.

Lits easier for the reader

Leasier to catch mistakes

Well-Ordering Principle

$S \subseteq \mathbb{N}$ and $S \neq \{\}$

$\exists u \in S$ s.t. $\forall m \in S \quad u \leq m$

The Well-Ordering Principle states that for any non-empty subset of the natural numbers there will be a least element.

Theorem: Every natural number greater than 1 can be written as a product of one or more primes (has a prime factorization)

Proof using WOP:

Let S be the set of natural numbers that cannot be written as a product of primes. Assume for contradiction that S is not empty. By WOP, S has a least element n.

Clearly, n is not prime! (otw it would not be in S) So, we can write $n = a \cdot b$ $a, b \in \mathbb{N}$.

It follows that a or b doesn't have a prime factorization.

Without loss of generality (WLOG) say a can't be written as a product of primes. Notice, since $n > 1$ $1 < a < n$. This is a contradiction because then $a \in S$, but we said n is the least element!

Thus, S is empty and theorem holds. □

Summary

- Simple Induction
  - P(0) and show P(n) ⇒ P(n+1)
- Multiple Base Cases
  - You may need multiple base cases to prove a statement
- Improve the Inductive Hypothesis
  - Sometimes proving a “stronger” statement is easier
- Strong Induction
  - P(0) and show P(0) and … and P(n) ⇒ P(n+1)
- Well Ordering Principle
  - For any subset of the naturals there is a least element

Review

Lecture 2A: Graph Theory I

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post
- Tarang's OH 4-6p in Woz Lounge (Zoom also–same link as lecture)
  - First 30 minutes for conceptual question
  - Last 90 minutes for reading Note 5 together and question about the note
  - Will not prioritize HW questions. Use regular OH for that.
- **HW 2** and **Vitamin 2** have been released, due **Thu** (grace period Fri)
- We are adding a bit more OH support, but also work on the HW early
- Throughout this lecture **definitions** will be underlined

Undirected Simple Graph Definitions

An undirected simple **graph** $G = (V, E)$ is defined by

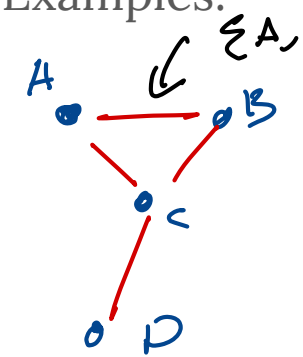
1. A set V of **vertices**. Sometimes we may call it a **node**.
2. A set E of **edges**

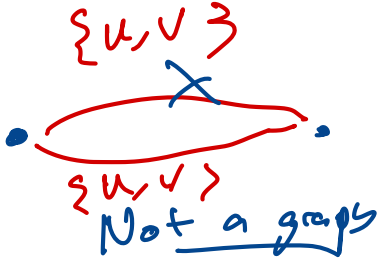
Where edges in E are of the form $\{u, v\}$ for u, v *in* V and $u \neq v$.

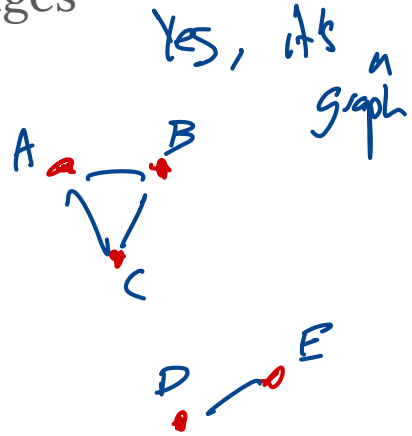
A graph being **simple** here means no parallel edges

A graph being **undirected** means there's no direction to the edges

Examples:



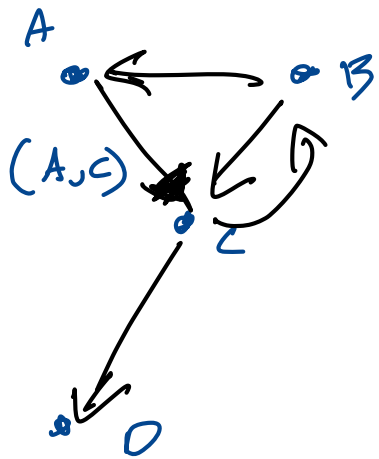




Directed Graph Definitions

Edges in a **directed graph** are defined as (u, v). That is, the order of the vertices matters. Therefore, $(u, v) \neq (v, u)$.

Examples:

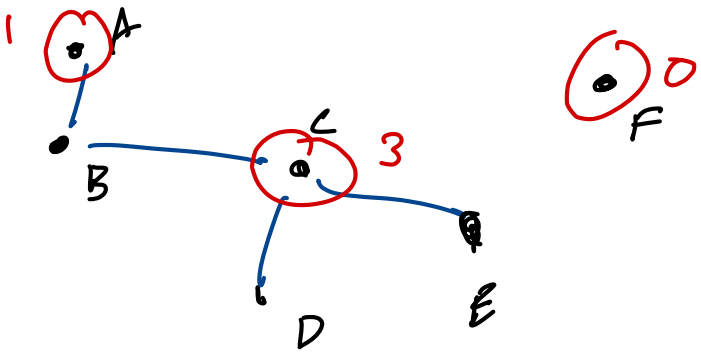


Edge and Degree Definitions

Given an edge $e = \{u, v\}$ we say

- e is **incident** to u and v
- u and v *are* **neighbors**
- u and v *are* **adjacent**
- The **degree** of a vertex v is the number of incident edges
  - $deg(v) = |\{v \text{ in } V \mid \{u, v\} \text{ in } E\}|$

Examples:



Summary Questions I

How many nodes in this graph? 11

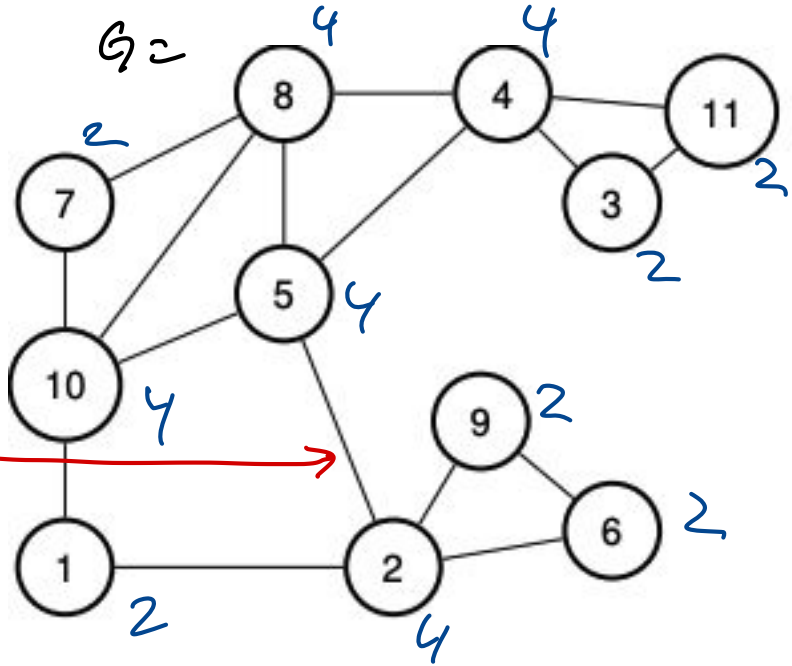
How many edges? 16

Which vertex has the max degree? 5, 8, 2, 10, 4

Which vertex has the min degree? 6, 11, 3, 9, 7, 1

Which vertices is this edge incident on? 2 and 5

What is the sum of the degrees? 32



Handshake Lemma

$A = \{1, 2, 3\}$ $\quad |A| = 3$

$|\cdot|$ ↑ size

"cardinality"

Lemma: The sum of the degree of all the vertices is equal to $2|E|$

Proof: Proceed by induction on $|E| = m$

Base Case: $m = 0$. A graph has no edges if all the vertices are isolated (i.e. no neighbors) thus each vertex is degree 0

$0 + \dots + 0 = 2(0)$ ✓

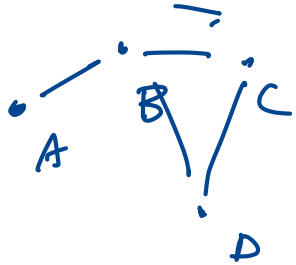
Ind Hyp: Assume claim holds for $m = k$ edges, .. sum of degrees is $2k$

Ind Step: Consider an arbitrary graph G with $k+1$ edges. Remove any edge from G. The new graph has k edges, and by the inductive hypothesis sum of degrees is $2k$. Then adding back the edge we add 1 degree to each incident vertex. thus sum of degrees is now $2k+2 = 2(k+1)$ as desired

↑ # edges

□

Path, Cycles, Walks and Tours



Deals with Vertices (though may imply things about edges):

Path: A sequence of vertices in G, generally with no repeated vertices.

Cycle: A path in G where the only repeated vertex is the first one and last one.

Deals with Edges (though may imply things about vertices):

Walk: Is a sequence of edges with possible repeated vertex or edges.

Tour: A walk that starts and ends at the same vertex.

Eulerian walk: A walk where each edge is visited exactly once.

Eulerian tour: An Eulerian walk that starts and ends at the same vertex

Summary Questions II

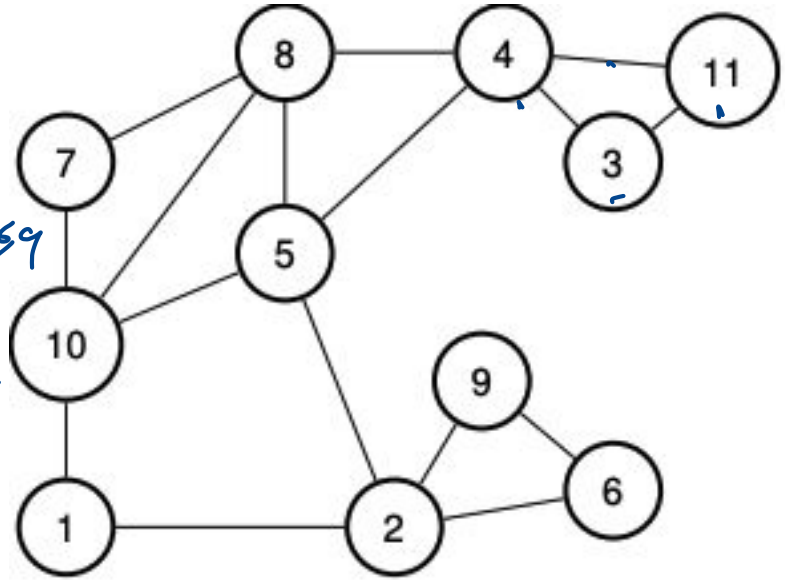
Give an example of length 3 cycle? 4, 3, 11, 4

Give an example of a path from 2 to 8? 2, 5, 8

Give the longest simple path? 4, 3, 4, 5, 8, 7, 10, 1, 2, 5, 9

How many connected components are there? 1

Give an example of length 4 tour? 7 → 10 → 5 → 8 → 7

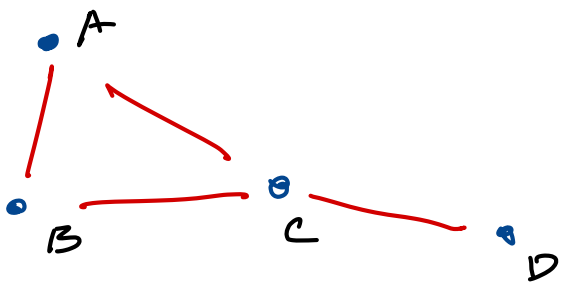


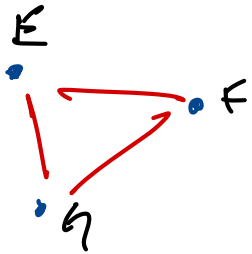
Connectivity

A graph G is said to be **connected** if there exists a path between any two vertices.

$V_1 = \{A, B, C, D\}$
$V_2 = \{E, F, G\}$
$V_3 = \{H\}$

Examples:





Any graph always consists of a collections of **connected components.** A connected component is a set of vertices in the graph that are connected.

see CS170 SCC

Eulerian Tours

Eulerian walk: A walk where each edge is visited exactly once.

Eulerian tour: An Eulerian walk that starts and ends at the same vertex

Theorem: A undirected graph G has an Eulerian ~~tour~~ walks iff G is even degree, and connected.

every vertex has even degree

Proof: *in the notes*

except two vertices that are odd

Summary Questions III

Is there an Eulerian Tour and if so provide a tour?

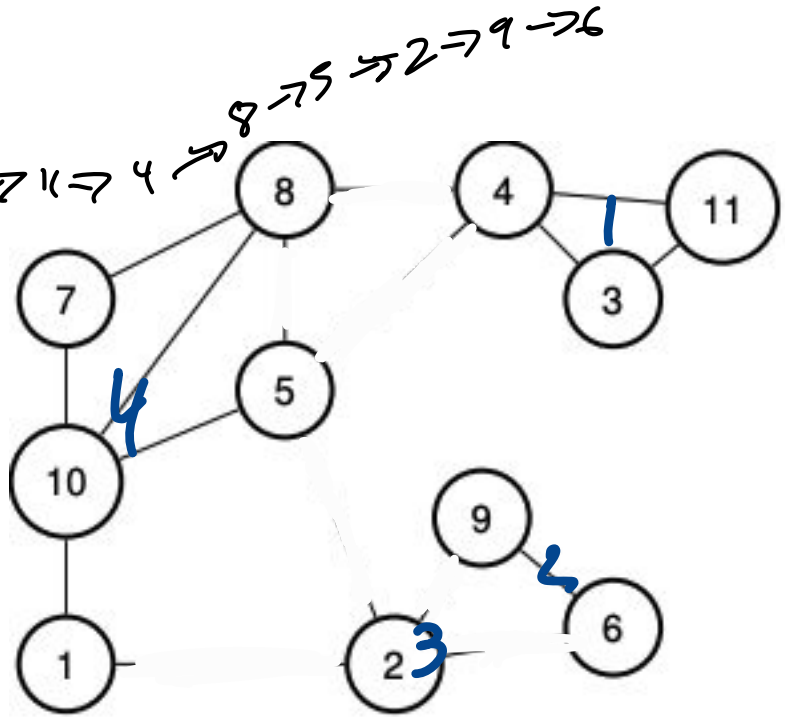
6 → 2 → 1 → 10 → 7 → 8 → 10 → 5 → 4 → 3 → 11 → 4 → 8 → 5 → 2 → 9 → 6

Why? every vertex has even degree & connected

How many connected components now? 1

Connected components now? 1

What about now? 4



Graph Proof

False Claim: If every vertex in an undirected graph has degree at least 1, then the graph is connected.

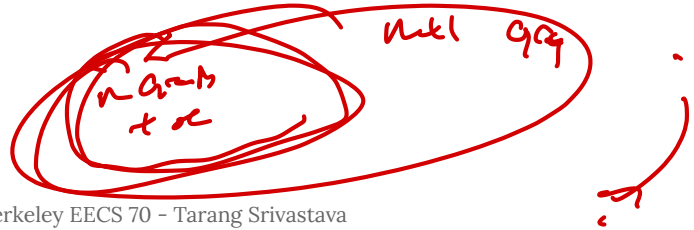
Proof: We use induction on the number of vertices $n \geq 1$

Base Case: There is only one graph with a single vertex and it has degree 0. Thus, vacuously true.

Inductive Hypothesis: Assume the claim is true for ~~some~~ $n \geq 1$

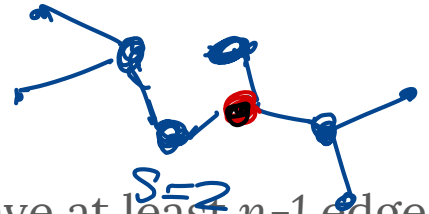
Inductive Step: We prove the claim is also true for $n + 1$. Consider an undirected graph with n vertices and each has degree greater than 1. By the inductive hypothesis, this graph is connected. Now add one more vertex x to obtain a graph with $(n + 1)$ vertices.

Since, the previous graph was connected, and x is connected to some node y then there's a path between x and any other vertex through y, since by definition there's a path from y to any other vertex. Thus, the graph is connected.



Minimum Edges for Connectivity

P(n) ⇒ P(n+1)



Theorem: Any connected graph with n vertices must have at least $n-1$ edges

Induction on vertices $n = |V|$

Base Case: $n=1$ 0 edges $0 \le (1)-1$

Ind Hyp: Assume claim holds for $1 \le n \le k$

Ind Step: Consider a connected graph G with $n = k+1$ vertices. Remove an arbitrary vertex v. Removing v suppose creates S connected components. By strong induction each connected component has $k_1 - 1$ edges, $k_2 - 1$ edges ... $k_S - 1$ edges. Adding back v we get to add back S edges

$$k_1 + k_2 + \dots + k_S - 1 - 1 - 1 \dots - 1$$

$$|E| \ge k - S$$

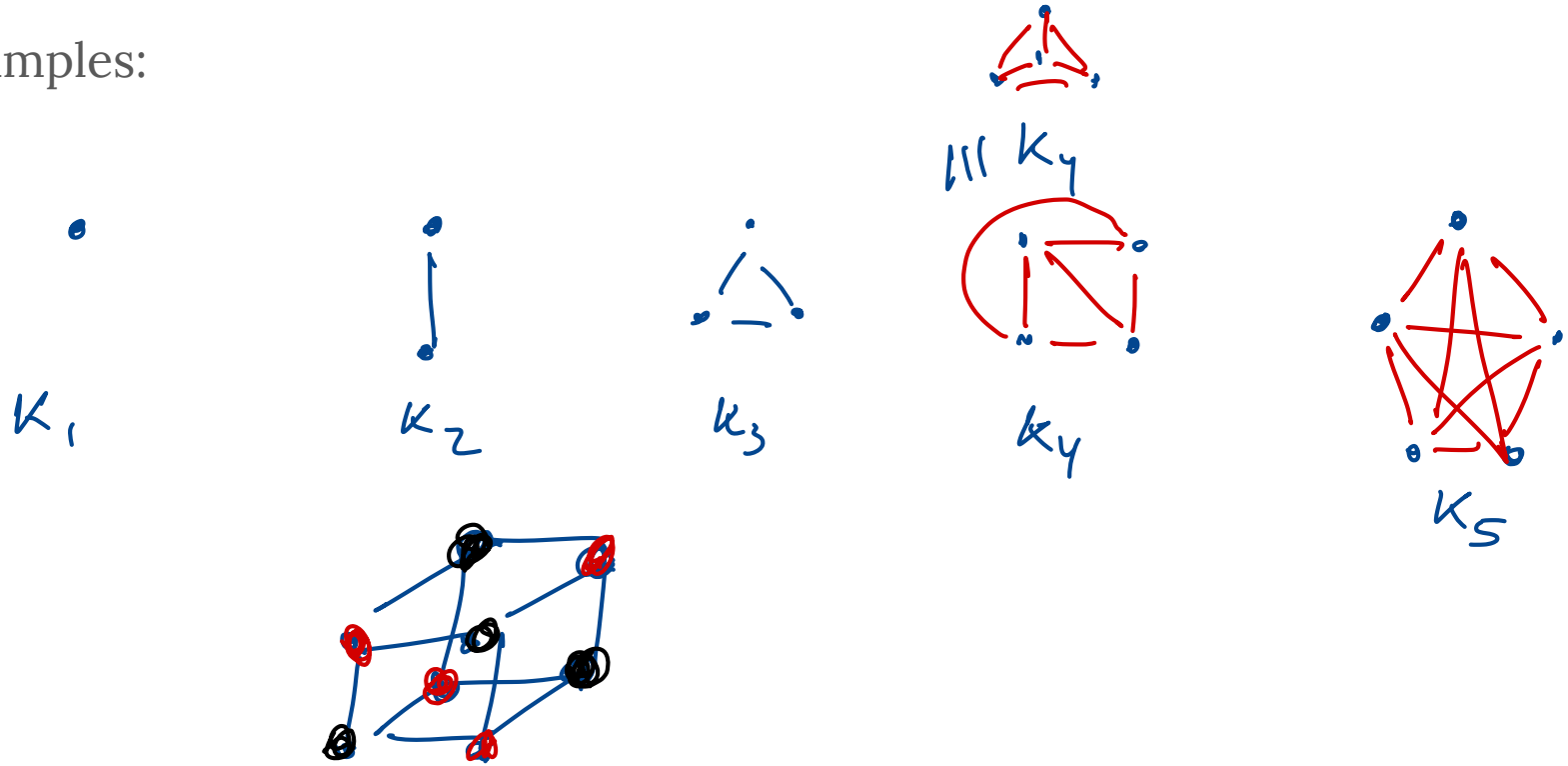
$$(k+1) - 1$$

$$|E| \ge k \quad \text{as desired}$$

Complete Graphs

A graph G is **complete** if it contains the maximum number of edges possible.

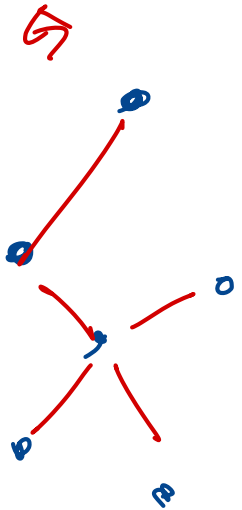
Examples:



Trees

The following definitions are all equivalent to show that a graph G is a **tree**.

1. G is connected and contains no cycles
2. G is connected and has n-1 edges (where $n = |V|$)
3. G is connected, and the remove of any single edge disconnects G
4. G has no cycles, and the addition of any single edge creates a cycle



Tree Definitions are Equivalent

Theorem: For a connected graph G it contains no cycles iff it has n-1 edges.
Proof:

Tree Definitions are Equivalent (cont.)

Theorem: For a connected graph G it contains no cycles iff it has n-1 edges.

Bipartite Graphs

A graph G is **bipartite** if the vertices can be split in two groups (L or R) and edges only go between groups.

Examples:

Review

Lecture 2B: Graph Theory II

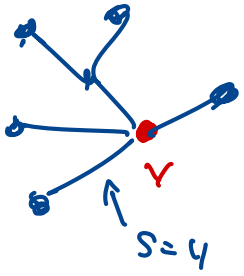
UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post required recording
- We have caught academic misconduct cases
- **HW 2** and **Vitamin 2** have been released, due **Thu** (grace period Fri)
- Throughout this lecture **definitions** will be underlined

- OH was yday

Minimum Edges for Connectivity



Theorem: Any connected graph with n vertices must have at least $n-1$ edges

Proceed by strong induction on $n = |V|$

Base Case: $n = 1$ $\quad (1) - 1 = 0$ ✓

Ind Hyp: Assume claim holds $1 \le n \le k$

Ind Step: Consider an arbitrary graph G with $n = k+1 = |V|$ $\quad G = (V, E)$

Then remove any vertex v, call the resulting graph $G' = (V', E')$

Removing v creates at most $\deg v$ connected components; let $S \le \deg v$

Denote k_i to be the number of vertices in the ith connected component

$|E_1|$ edges in 1st connected component $+ |E_2| + \dots + |E_S| \ge (k_1 - 1) + \dots + (k_S - 1)$ (follows from ind. hyp.)

$|E'| = |E_1| + \dots + |E_S| \ge (k_1 + \dots + k_S) - S$

$|E| = |E'| + \deg v \ge k - S + S$

$|E| \ge k$ as desired

we add back

$|E| = |E'| + S$

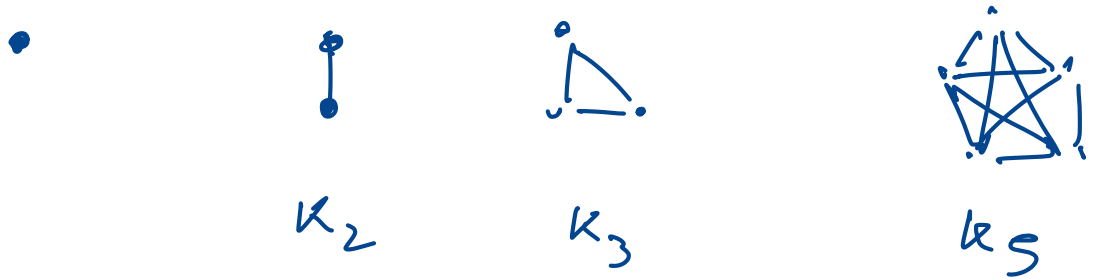
vertices $(k+1) - 1 = k$

Complete Graphs

A graph G is **complete** if it contains the maximum number of edges possible.

Correction: K is for mathematician Kazimierz Kuratowski

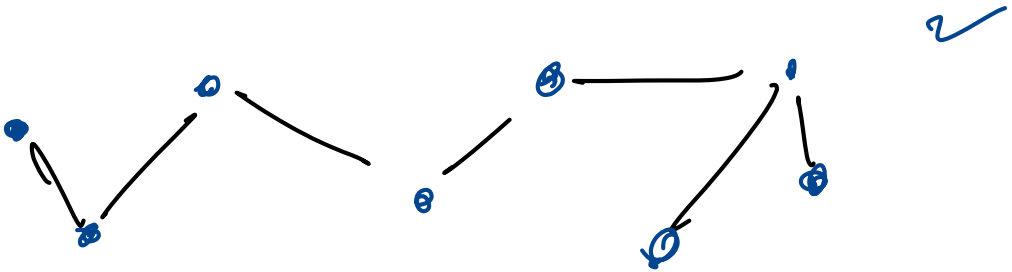
Examples:



Trees

The following definitions are all equivalent to show that a graph G is a **tree**.

1. G is connected and contains no cycles
2. G is connected and has n-1 edges (where $n = |V|$)
3. G is connected, and the remove of any single edge disconnects G
4. G has no cycles, and the addition of any single edge creates a cycle



Tree Definitions are Equivalent

Theorem: For a connected graph G it contains no cycles iff it has n-1 edges.

Proof:

$\Rightarrow$ if no cycles, then $n-1$ edges. Proceed by induction on # of vertices

Base case: $n=1$ has no edges ✓

Ind. Hyp: Assume the claim for all $1 \le n \le k$

Ind. Step: Consider a graph with $k+1$ vertices. Remove any arbitrary vertex v.

Case 1: G' is disconnected. Apply ind. hyp to each connected component (similar proof as before)

Case 2: G' is connected, then G' has $k-1$ edges by ind. hyp. We add back v. v can only be incident on one edge otherwise then G' is connected, G would've had a cycle. Thus adding back 1 edge there k edges for $k+1$ vertices ☐

Tree Definitions are Equivalent (cont.)

Theorem: For a connected graph G it contains no cycles iff it has n-1 edges.

$\Leftarrow$ if $n-1$ edges, then no cycles

Assume for contradiction G is connected and has $n-1$ edges but also contains a cycle. Then removing an edge from the cycle in G does not disconnect G. Now G' has n vertices but only $n-2$ edges. Which we proved earlier is not possible!

G has no cycles.

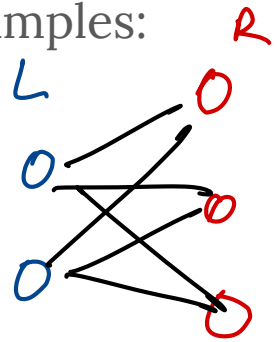
Bipartite Graphs

A graph G is **bipartite** if the vertices can be split in two groups (L or R) and edges only go between groups.

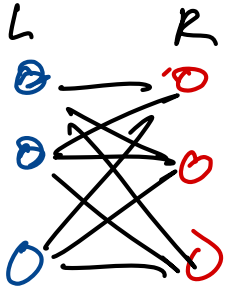
two adjacent vertices don't have the same color
We use at most 2 colors

G is bipartite iff G is two colorable

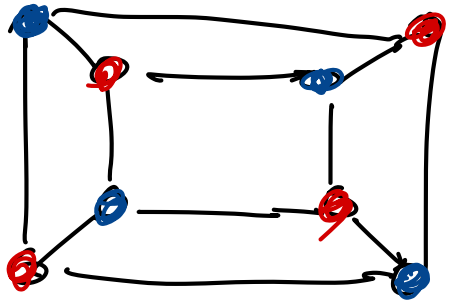
Examples:



$K_{2,3}$



$K_{3,3}$

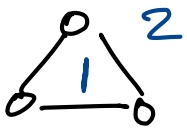


$K_{3,2}$

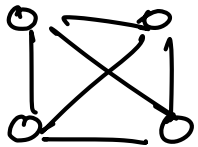
Planar Graphs

A graph is called **planar** if it can be drawn in the plane without any edges crossing.

Examples:

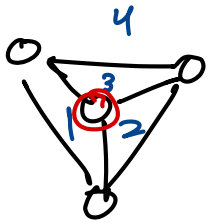


Yes



Yes

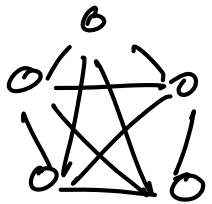
≡



yes

K_5

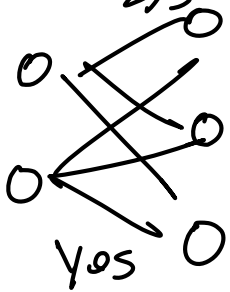
Complete graph



No

Bipartite

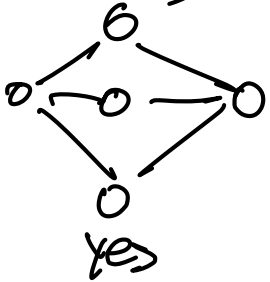
$K_{2,3} \equiv K_{3,2}$



Yes

≡

$K_{2,3}$



yes

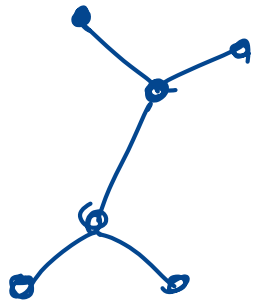
K_{33}

non planar

Euler's Formula: $v - e + f = 2$

Theorem: If G is a connected planar graph, then $v - e + f = 2$.

Proof: Proceed by induction on e



Base Case: $e=0$. $f=1$. $v=1$ $= 1-0+1=2$ ✓

Ind. Hyp: Assume claim holds for $e=k$

Ind. Step: Consider an arbitrary graph G with $e=k+1$

Case 1: G is a tree. Then $f=1$, $v=e+1$

$(e+1) - e + 1 = 2$ ✓

Case 2: G is not a tree, then G has a cycle. Remove an edge from the cycle. G is still connected and plane. This apply ind. hyp.

$v - e' + f' = 2$

Adding back the edge creates 1 face

$v - (e'+1) + (f'+1) = v - e + f = 2$ ✓

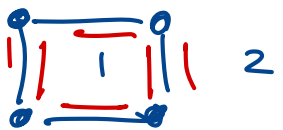
Euler's Formula Corollary: $e \leq 3v - 6$

Corollary: For a connected planar graph with $v \geq 3$, we have $e \leq 3v - 6$

Proof:

Define a side to be the "side" of an edge towards a face.

Ex:



face 1 has 4 sides

face 2 has 4 sides

1 has 4 sides

Let s_i := number of sides for i^{th} face

$$\sum_{i=1}^{f} s_i = 2e$$

Each face has 3 sides at least

$$2e = \sum_{i=1}^{f} s_i \geq \sum_{i=1}^{f} 3 \Rightarrow$$

$$2e \geq 3f$$

$$2e \geq 3(2+e-v) \Rightarrow e \leq 3v-6 \checkmark$$

$$2e \geq 6 + 3e - 3v$$

K_5 is non-planar

Proof:

Assume for contradiction K_5 is planar

$V = 5$

$e = \binom{5}{2} = 5 \cdot 4 \cdot \frac{1}{2} = 10$

$e \leq 3v - 6$

$10 \leq 3(5) - 6$

$16 \nleq 9$ ↯

$K_{3,3}$ is non-planar

this is on the HW

Proof:

Assume for contradiction

$v = 6$

$e = 9$

$9 \leq 3v - 6$

$9 \leq 3(6) - 6$

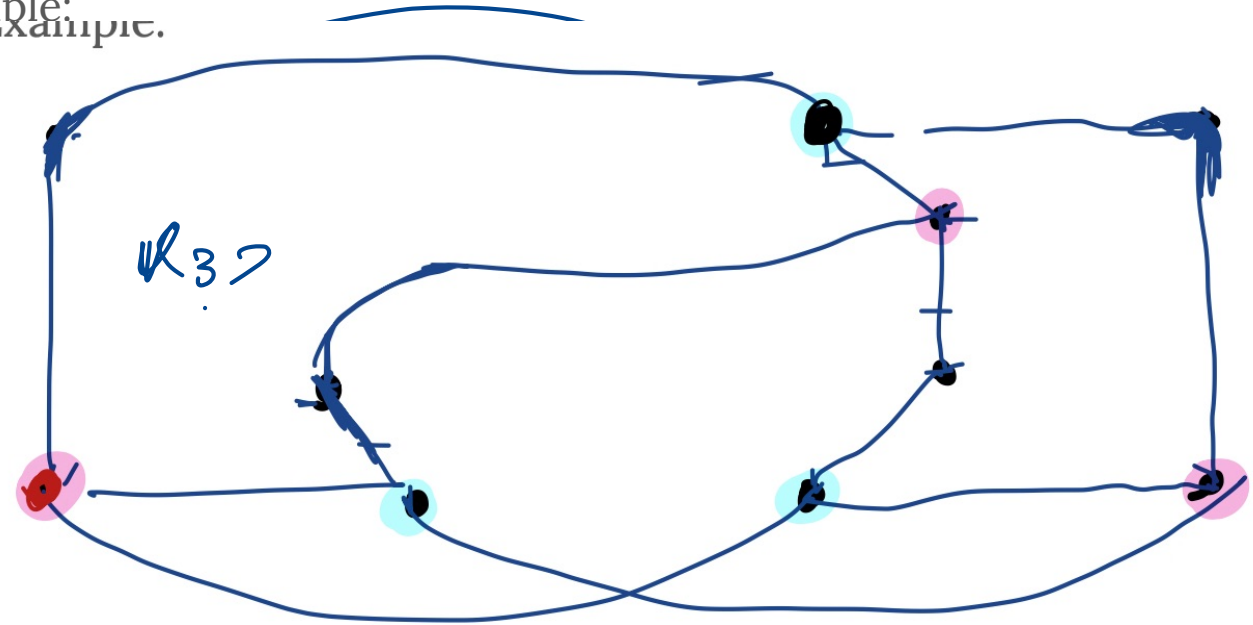
$9 \leq 12$???

Hint: Can you get a stronger inequality than $e \leq 3v - 6$ because $K_{3,3}$ is bipartite

Kuratowski's Theorem

Theorem: A graph is **non-planar** iff it contains K_5 or $K_{3,3}$

Example:



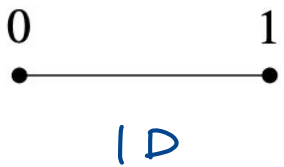
4D hypercube

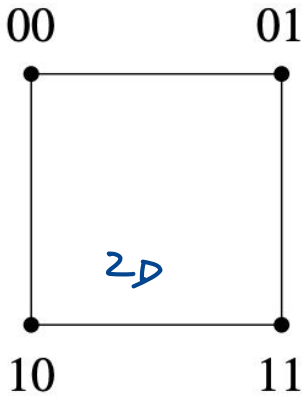
non-planar

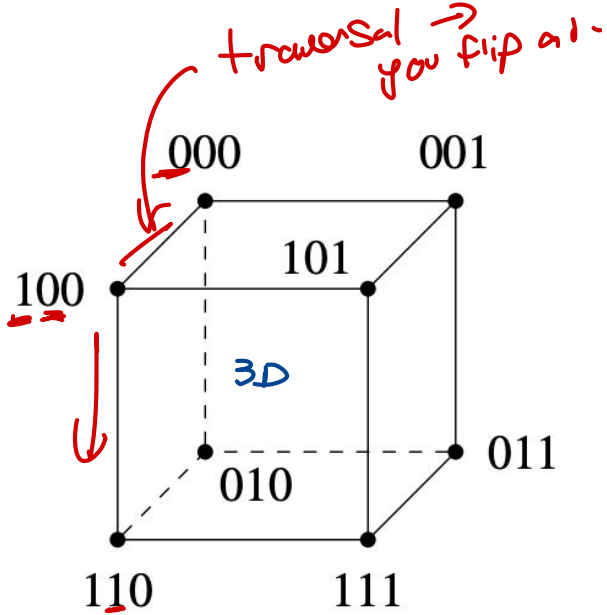
Hypercubes

The vertex set of a n-dimensional **hypercube** $G=(V, E)$ is given by $V = \{0, 1\}^n$ i.e. the vertices are n-bit strings.

n dim ⇒ 2^n vertices







Prove every hypercube is bipartite

Number of Edges in Hypercubes

Lemma: The total number of edges in an n-dimensional hypercube is $n2^{n-1}$

Proof:

$$\sum_v \deg(v) = \sum_v n = 2^n \cdot n = 2|E|$$

$$|E| = \frac{2^n \cdot n}{2}$$

$$= n2^{n-1}$$

Review

Lecture 2C:
Modular Arithmetic I

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post
- We have caught people for Academic Misconduct on HW1
- **HW 2** and **Vitamin 2** have been released, due **Thu** (grace period Fri)
- No lecture, OH, or Discussions on July 4th

Hopefully Review (Divides)

Def: We say $b|a$ if there exists some integer k such that $a = bk$

$b, a \in \mathbb{Z}$

$\frac{a}{b} = k \in \mathbb{Z}$

$b | 0$

$0 = b \cdot 0$

Example: 17, 51

$17 | 51$?

$k = 3$

$51 = 17 \cdot 3$

$a \quad b \quad k$

Hopefully Review (GCD)

Def: The greatest common divisor (GCD) of integers a and b is the greatest integer d such that $d|a$ and $d|b$

Examples:

gcd(4, 2) = 2 — 2|2 ✓ 2|4

gcd(12, 16) = 4 — 4|12 4|16

gcd(51, 17) = 17 ↦ since 17 is prime, gcd will be 17 or 1

gcd(15, 16) = 1 ↦ share no divisors, 15 and 16 are coprime

gcd(7, 96) = 1 ⟼ since 7 is prime, gcd will be 7 or 1

m = max(a,b)

O(m)

```
for i in range(m):
    i | a ?
    i | b ?
```

Hopefully Review (Division Algorithm)

Thm: For any two integers a, b. There are unique integers q, r with $0 \le r < b$ such that $a = qb + r$

4th Grade stuff

$a \div b = q + r$

q: quotient

r: remainder

$17 \div 5 = 3$ remainder 2

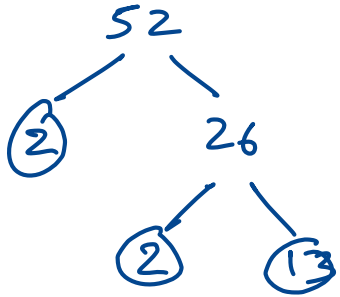
a b q r

$a \mid b$ iff $r = 0$ in the division algorithm

Hopefully Review (Fundamental Theorem of Arithmetic)

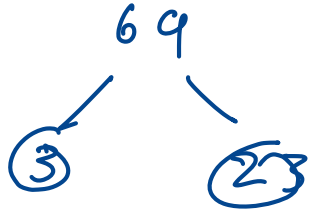
Thm: Every integer ≥2 can be **uniquely** expressed as a product of primes. (prime factorization)

We proved this using induction and well ordering principle Lecture 1C



$52 = 2 \cdot 2 \cdot 13$

∴ this set of primes is unique



$69 = 3 \cdot 23$

Mod as an *Operation*

You can think of mod as just an operation (i.e. what you're used to in 61A)

Python

"%"

$x \pmod{y}$

Example:

$13 \bmod 5 = 3$

$17 \bmod 2 = 1$

$17 \bmod 10 = 7$

Euclid's (GCD) Algorithm

Fact:

Thm: Let $x \geq y \geq 0$. Then, $\gcd(x, y) = \gcd(y, x \pmod y)$

Consider example $x = 10$, $y = 32$

$\gcd(10, 32) = \gcd(32, 10 \pmod{32})$

$= \gcd(32, 10)$

$= \gcd(10, 32 \bmod 10) = \gcd(10, 2)$

$= \gcd(2, 10 \bmod 2) = \gcd(2, 0) = 2 = a$

$\gcd(a, 0)$

$O(\log n)$ ≈

Mod as an *Operation* (cont.)

Math 113
114

You can think of mod as just an operation (i.e. what you're used to in 61A)

$x \pmod{y}$

Example:

$13 \mod 5 = 3$

$17 \mod 2 = 1$

$17 \mod 10 = 7$

$-17 \mod 10 \equiv -7 \equiv 3 \equiv 13$

equivalence

both 10

$0, \ldots, 9$

$-17 \xrightarrow{+10} -7 \xrightarrow{+10} 3 \xrightarrow{+10} 13$

$\mod m$

$m > 0$

$\{0, 1, \ldots, m-1\}$

$42 \div 5$

$(\mod 10)\ -17 = 10 \cdot (-2) + 3$

$3 = 3$

Mod as a *Clock*

(mod 12)

You can think of adding in mod as just going around a clock.

We will say all the numbers at the same step of the clock are part of the same **equivalence class**. (ex: ..., -11, 1, 13, 25, 37, ...)

$1 + 0 = 1$

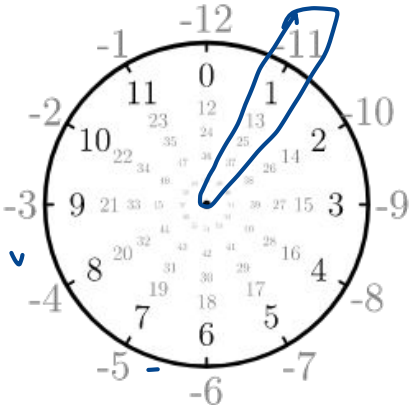
$1 + 12 = 13$

$1 + 12 + 12 = 25$

$1 \equiv 13 \equiv 25 \equiv \ldots \pmod{12}$

$1 \equiv -11 \equiv -23 \equiv -35 \pmod{12}$

(residue) equivalence class



How many equivalence classes?

12

Mod as *Space*

Math 110
Math 113

addition ✓
subtraction ✓
multiplication ✓
division ✓ next slide

You can consider doing ALL your arithmetic in a given mod *space*.

Let's come up with some rules:

Thm: if $a \equiv c \pmod m$ and $b \equiv d \pmod m$

$a+b \equiv c+d \pmod m$

$a \cdot b \equiv c \cdot d \pmod m$

Addition:

$3+8 \equiv 11 \equiv 1 \pmod 5$

$3+3 \equiv 6 \equiv 1$

$3+(-2) \equiv 1$

Sub:

$3-2 \equiv$

$3+(-2) \equiv$

$3+3 \equiv 1 \pmod 5$

Mul:

$2 \cdot 7 \equiv 14 \equiv 4 \pmod 5$

$2 \cdot 2 \equiv 4 \pmod 5$

CRT

Inverses (Modular Division)

We can redefine division in regular math, to just being multiplying by inverse.
The inverse of a is such a number a^{-1} such that $aa^{-1} = 1$
In (mod m) the inverse of a only exists if a and m are **coprime** (i.e. gcd(a, m) = 1).

$5^{-1} \equiv ?$ (mod 17)

$5 \cdot 5^{-1} \equiv 1$ (mod 17)

$5 \cdot 7 \equiv 35 \equiv 1$ (mod 17)

Example Solving an Equation

$5x + 3 \equiv 7$ (mod 17)

$5x \equiv 7 - 3$

$5^{-1} 5x \equiv 4 \cdot 5^{-1}$ (mod 17)

$x \equiv 4 \cdot 7 \equiv 28 \equiv 11$ (mod 17)

$5(11) + 3 = 58 \equiv 7$ (mod 17) ✓

Algebra 1 0

$35 = 17 \cdot 2 + 1$

$5 \div 2 = 5 \cdot \frac{1}{2}$

2's inverse is $\frac{1}{2}$

$2 \cdot \frac{1}{2} = 1$

5th Grade

$5 \div \frac{2}{3}$

$5 \cdot \frac{3}{2}$

$\frac{2}{3} \cdot \frac{3}{2} = 1$

just a symbol

prove that the inverse is unique

Sometimes we say **relatively prime** same thing as coprime.

Let's Bridge Algebraic Form with Modular Form

$a \equiv b \pmod{m}$ iff there exists some integer q such that $a = mq + b$ ← remainder

$a = mq + b \pmod{m}$

$a \equiv 0 \cdot q + b$

$a \equiv b \pmod{m}$

(GCD Algorithm): Let $x \geq y \geq 0$. Then, $\gcd(x, y) = \gcd(y, x \pmod{y})$ ⇐ common divisors; $x \pmod{y}$ = r

Proof. Suppose d is an arbitrary divisor of both x and y. ($d \mid x$ and $d \mid y$).

By the division algorithm, we can write $x = qy + r$.

Notice, $x \equiv r \pmod{y}$. Since, $d \mid y$ we know $d \mid qy$.

Then from lecture 1B, we know $d \mid x - qy$. $x - qy = r$

So, $d \mid r$. Thus, x, y and $x \pmod{y}$ share the same divisors

Since was arbitrary. Namely they have the same GCD.

Also show that divisors of y and r are divisors of x and y.

Extended Euclid's Algorithm: How to find inverses

Find the **inverse of x in (mod y)** by finding a, b such that $1 = ax + by$

Example 2: $x = 7, y = 32$

$\gcd(x,y) = 1$

$\gcd(x,1) = ax + by$

$1 = ax + by$

Solving for a, b gives you the inverse?

$7^{-1} \pmod{32}$

Alt. method from in the notes: Goal find a, b

$7(1) + 32(0) = 7$ ①

$7(0) + 32(1) = 32$ ②

×5

$7(5) + 32(0) = 35$ ⑥

$7(5) + 32(-1) = 3$ ④

×11

$7(55) + 32(-11) = 33$ ⑤

$7(55) + 32(-12) = 1$

$x \quad a \quad y \quad b$

$7^{-1} \pmod{32}$

$55 \equiv 23 \pmod{32}$

$\gcd(x,y)\ 7^{-1} \equiv 23$

$7 \cdot 23 = 161 \equiv 1 \pmod{32}$

$1 = ax + by \pmod{y}$

$1 \equiv ax \pmod{y}$

a ↔ inverse of x

$1 = ax + by \pmod{x}$

$1 \equiv by$

$y^{-1} \equiv b \pmod{x}$

$32^{-1} \pmod{7}$

$4^{-1} \pmod{7}$

$-12 \pmod{7}$

$4 \cdot 2 = 8 \equiv 1 \pmod{7}$

Repeated Squaring

How to find $x^y \pmod m$ for large exponents.
Example: $4^{42} \pmod 7$

$4^0 = 1 \pmod 7$

$4^1 = 4$

$4^2 = (4^1)^2 = 4^2 = 16 = 2$

$(4^2)^2 = 4^4 = 2^2 = 4$

$(4)^8 = 16 = 2$

$(4)^{16} = 4$

$(4)^{32} = 2$

$4^{42} = 4^{32} \cdot 4^8 \cdot 4^2$

$\equiv 2 \cdot 2 \cdot 2$

$\equiv 8 \pmod 7$

$\equiv 1$

$xa \equiv x'a \pmod m$

Review

Lecture 2D:
Modular Arithmetic II

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post
- **HW 2** and **Vitamin 2** have been released, due **Today** (grace period Fri)
- No lecture, OH, or Discussions on July 4th

Repeated Squaring

How to find $x^y \pmod m$ for large exponents.

Example: $4^{42} \pmod 7$

$4^0 \equiv 1 \pmod 7$

$4^1 \equiv 4$

$4^2 \equiv 16 \equiv 2$

$4^4 \equiv (4^2)^2 \equiv (2)^2 \equiv 4$

$4^8 \equiv (4^4)^2 \equiv (4)^2 \equiv 16 \equiv 2$

$4^{16} \equiv (4^8)^2 \equiv 2^2 \equiv 4$

$4^{32} \equiv (4^{16})^2 \equiv (4)^2 \equiv 16 \equiv 2$

$4^{42} \equiv 4^{32} \cdot 4^8 \cdot 4^2 \equiv 4^{32+8+2}$

$\equiv 2 \cdot 2 \cdot 2 \equiv 8 \equiv 1 \pmod 7$

Recap

- Division Algorithm a, b $a = bq + r$ (quotient, remainder)
- Greatest Common Divisor (GCD) Definition
- GCD Algorithm: Application and Proof $gcd(x, y) = gcd(y, x \bmod y)$
- Every number has a unique prime factorization ex: $52 = 13 \cdot 2 \cdot 2$
- Mod as a *Space*: Defined Addition, Subtraction, Multiplication and Division
- Definition of Coprime $gcd(x, y) = 1$
- Definition of Inverse and division via multiplying inverse
- Extended Euclid's Algorithm to find inverse $ax + by = 1$
- Repeated Squaring

$ax + by = gcd(x, y)$

Bijections

$f: A \to B$

$f(x) = 2x$

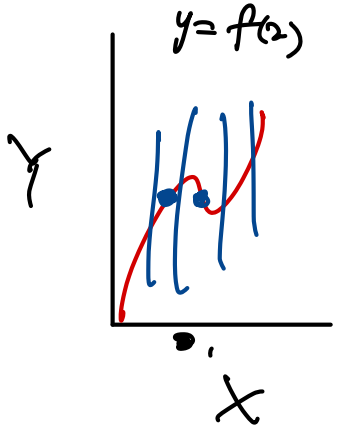
$\mathbb{R} \to \mathbb{R}$

A *bijection* is a function for which every $b \in B$ has a unique *pre-image* $a \in A$ such that $f(a) = b$. Note that this consists of two conditions:

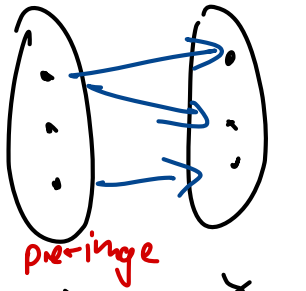
1. f is *onto*: every $b \in B$ has a pre-image $a \in A$. "surjective"
2. f is *one-to-one*: for all $a, a' \in A$, if $f(a) = f(a')$ then $a = a'$. "injective"

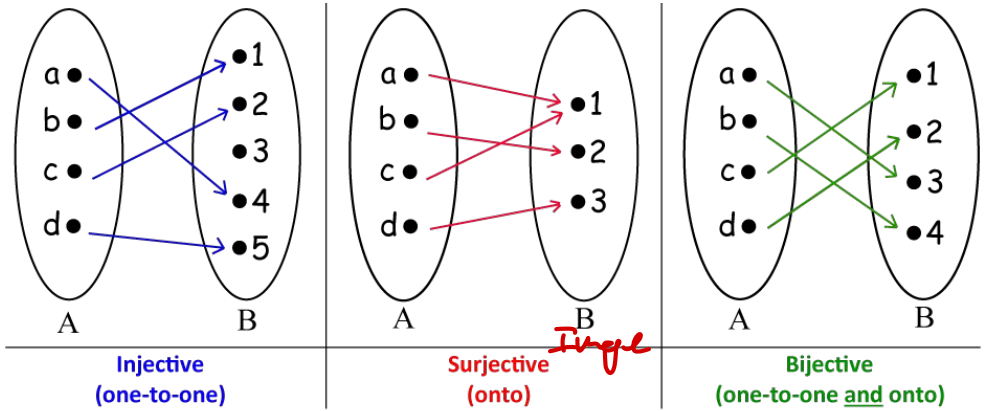
Contrapositive.

If $a \neq a'$, then $f(a) \neq f(a')$



NOT A FUNCTION



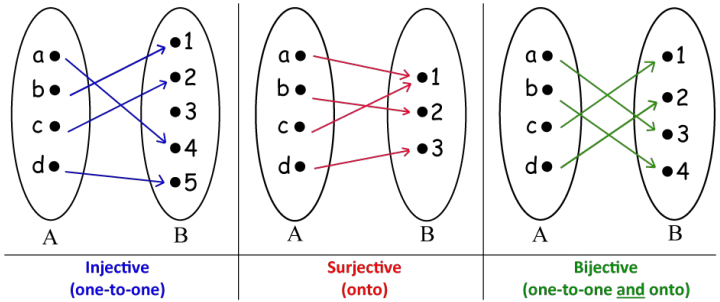


Bijections Examples

g is an inverse of f if
$g(f(x)) = x \quad \forall x$

A *bijection* is a function for which every $b \in B$ has a unique *pre-image* $a \in A$ such that $f(a) = b$. Note that this consists of two conditions:

1. f is *onto*: every $b \in B$ has a pre-image $a \in A$.
2. f is *one-to-one*: for all $a, a' \in A$, if $f(a) = f(a')$ then $a = a'$.



$f: A \to B$ and f is injective

$|A| \leq |B|$

. . . .

f is surjective

$|A| \geq |B|$

f is bijective

$|A| = |B|$

$f(x) = x^2$ $\quad f: \mathbb{R} \to \mathbb{R}$ neither

$f(x) = x^2$ $\quad f: \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$ surjective

$f(x) = 2x$ $\quad f: \mathbb{N} \to \mathbb{N}$ injective

$f(x) = 2x$ $\quad f: \mathbb{R} \to \mathbb{R}$ bijective

inverse $\frac{1}{2}x$

$f(x) = x^3 - x$ $\quad f: \mathbb{R} \to \mathbb{R}$ surjective

$f(0) = 0$

$f(1) = 0$

A Useful Lemma

$f(x) = ax \pmod m$ $\quad$ a and m are coprime

$f : \{0, 1, \dots, m-1\} \to \{0, 1, \dots, m-1\}$

Claim: $f(x) = ax \pmod m$ where a and m are coprime is a bijection.

Restated: The sequence $1a, 2a, 3a, \dots, (m-1)a$ is a reordering of the numbers $\{1, 2, \dots, m-1\}$.

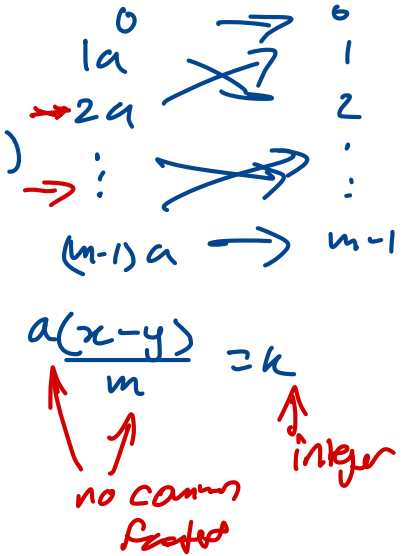
Proof:

Assume for contradiction that f is not a bijection.

Then, $\exists x, y$ s.t. $x \neq y \pmod m$ $ax \equiv ay \pmod m \Rightarrow ax - ay \equiv 0 \pmod m$

$\Rightarrow \exists k \in \mathbb{Z}$ $ax - ay = km$. Since a and m are coprime they share no factors and thus $m \mid (x-y)$

This is a contradiction since $x, y \in \{0, 1, \dots, m-1\}$ so $x - y < m$. Thus, f is a bijection.



Existence of an Inverse

Goal:
$\exists x \in \text{mod } m$
$ax \equiv 1 \pmod m$

Thm: if a and m are coprime, then a has an inverse in $mod\ m$

Proof:

Consider the sequence from before $1a, 2a, \ldots, (m-1)a$

We know this sequence is a bijection to $\{1, 2, \ldots, m-1\}$

if a and m are coprime. $\exists$ some ya in the sequence that maps to 1

Thus, $ya \equiv 1 \pmod m$, y is then the inverse of $a \pmod m$.

A Necessary Lemma

the existence of an inverse

Lemma: ~~x~~ a and m being coprime is a <u>necessary</u> condition for ~~$f(x) = ax \pmod m$ to be a bijection.~~

Proof: if $\gcd(a, m) > 1$ then a does not have an inverse $\pmod m$

Prove directly. Let $d = \gcd(a, m)$ and a has an inverse $\pmod m$

$ay \equiv 1 \pmod m \Rightarrow ay = mk + 1 \quad k \in \mathbb{Z}$. Since, $d \mid a$ and $d \mid m$

inverse we also know $d \mid ay$ and $d \mid mk \Rightarrow d \mid ay - mk$ Lec. 1B

$ay - mk = 1$ thus $d \mid 1$, So, d must be equal to 1. Thus, a and m are coprime.

Inverse is Unique (From Discussion 2C Q3E)

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

Suppose x and x' are inverses of a mod m

Then,

$$ax \equiv ax' \equiv 1 \pmod{m}$$

$$xax \equiv xax'$$

since $xa \equiv 1$

$$x \equiv x'$$

□

What makes prime numbers so special?

52 → 2 · 2 · 13

1. Building blocks of all numbers ← all numbers have a prime factorization
2. Given a prime p any number that's not a multiple of p is coprime to p

   i.e. $\gcd(x, p) = 1$ for all x that is not a multiple of p.

   Thus, the inverse always exists in modulo p

Working in mod p guarantees that division ~~almost~~ always

0, p, 2p, 3p

$0 \equiv p \equiv 2p \equiv \ldots \pmod{p}$

You can't divide by zero!

Galois Field

"GF(p)"

mod p

Fermat's Little Theorem Examples

Thm: For any prime p and any a in $\{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$.

Examples: $4^6 \pmod 7$, $4^{42} \pmod 7$

7 is prime

$4^{7-1} \equiv 4^6 \equiv 1 \pmod 7$

$4^{42} \equiv (4^6)^7 \pmod 7$ by FLT

$4^6 \equiv 1$

$\equiv 1^7$

$\equiv 1$

$4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4$

16 1 1

$2 \cdot 2 \cdot 2 \equiv 8 \equiv 1 \pmod 7$

Fermat's Little Theorem Proof

Thm: For any prime p and any a in $\{1, 2, \ldots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$.

Proof:

$1a, 2a, 3a, \ldots, (p-1)a$ is a reordering of $1, 2, 3, \ldots, p-1$

$1a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)$

$1 \cdot 2 \cdot 3 \cdots (p-1) \cdot \underbrace{a \cdot a \cdots a}_{(p-1)} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)$

$1 \cdot 2 \cdot 3 \cdots (p-1) \cdot a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1)$

$a^{p-1} \equiv 1 \pmod{p}$

Chinese Remainder Theorem (CRT) Example

Find a x in mod 30 such that it satisfies the following equations

$x \equiv 1 \pmod 2, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5$

$x = 11$

idea: $x = a + b + c$

$a \equiv 1 \pmod 2$ ✓ $\quad b \equiv 0 \pmod 2$ ✓ $\quad c \equiv 0 \pmod 2$ ✓

$a \equiv 0 \pmod 3$ ✓ $\quad b \equiv 2 \pmod 3$ ✓ $\quad c \equiv 0 \pmod 3$ ✓

$a \equiv 0 \pmod 5$ ✓ $\quad b \equiv 0 \pmod 5$ ✓ $\quad c \equiv 3 \pmod 5$ ✓

Guess: $a = 3 \cdot 5 = 15$ ✓

$b = 2 \cdot 5 = 10$

$b = 2 \cdot 2 \cdot 5 = 20$ ✓

$c = 2 \cdot 3 = 6$

$c = 2 \cdot 3 \cdot 3 = 18$ ✓

$x = 15 + 20 + 18$

$53 \mod 30 \Rightarrow$ **$23 \pmod{30}$** $= x$

Chinese Remainder Theorem

Chinese Remainder Theorem: Let $n_1, n_2, \ldots, n_k$ be positive integers that are coprime to each other. Then, for any sequence of integers a_i there is a unique integer x between 0 and $N = \prod_{i=1}^{k} n_i$ that satisfies the congruences:

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \equiv \vdots \\ x \equiv a_i \pmod{n_i} \\ \vdots \equiv \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

product

Given $n_1, n_2, \ldots, n_k$ that are coprime to each other. $N = n_1 n_2 \cdots n_k$

$\exists$ a unique solution $x \in \{0, 1, \ldots, N-1\}$ that satisfies all the equations.

$$\gcd(x, y) = ax + by$$

Review

Lecture 3A: RSA

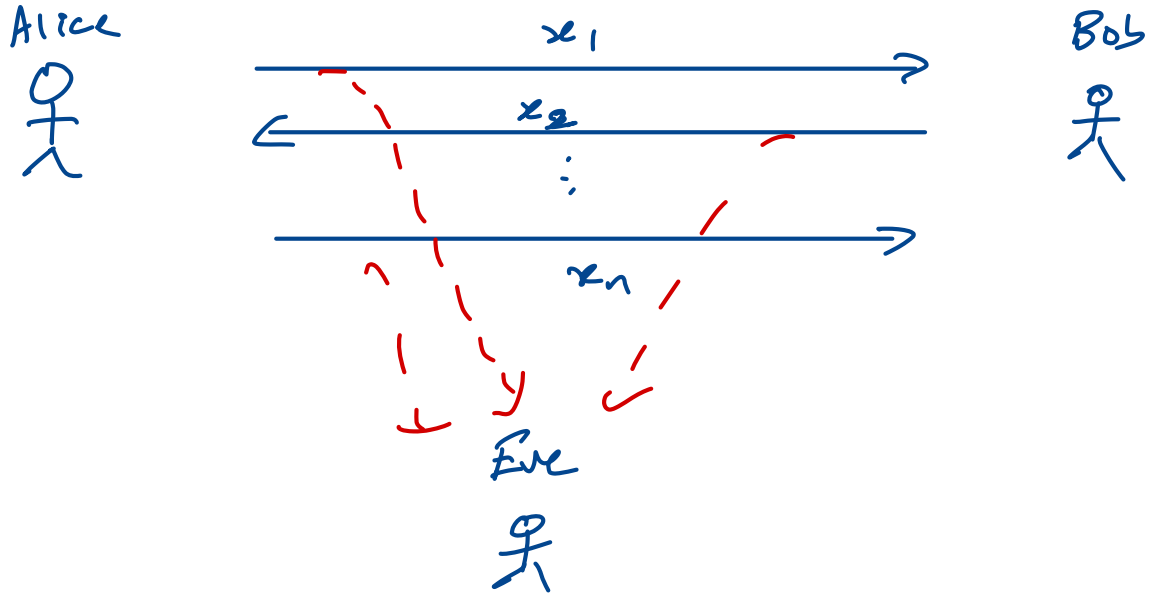
UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post
- **HW 3** and **Vitamin 3** have been released, due **Thursday** (grace period Fri)
- HW 3 covers last Wednesday, Thursday and Today's lecture
- Any topic that's out of scope in this lecture will be in Orange.
  - You are not responsible for these topics, they're just here to give context
  - These topics will be covered in CS170 and CS161
- In this lecture, we will use small prime numbers as examples but in implementation we use large prime numbers (256 bits $\approx 10^{77}$ or more).

Alice and Bob

Alice and Bob wish to send messages to each other **privately**.
Eve is able to intercept and read the messages.
How can Alice and Bob **encrypt** their messages, so even if Eve intercepts them she cannot understand them (i.e. **decrypt**).



Using a Codebook

"too few squares"
"repeat letters"

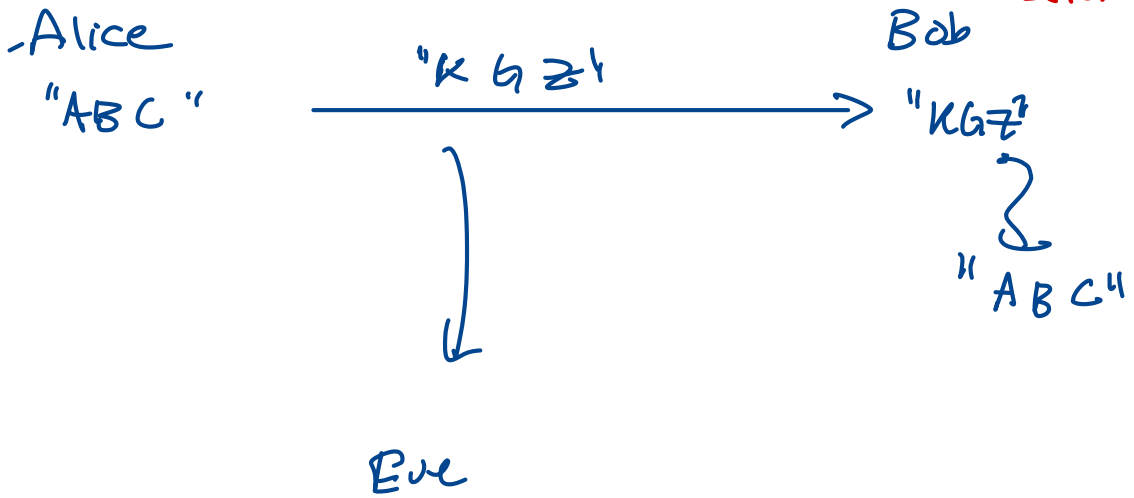
How can Alice and Bob **encrypt** their messages, so even if Eve intercepts them she cannot understand them (i.e. **decrypt**).

Problem: "Bob and Alice have to agree on a codebook before"

Carol → Osk:

Codebook

A → K
B → G
C → Z
D → F
⋮
Z → B



Public Key Cryptography

Not like a codebook!

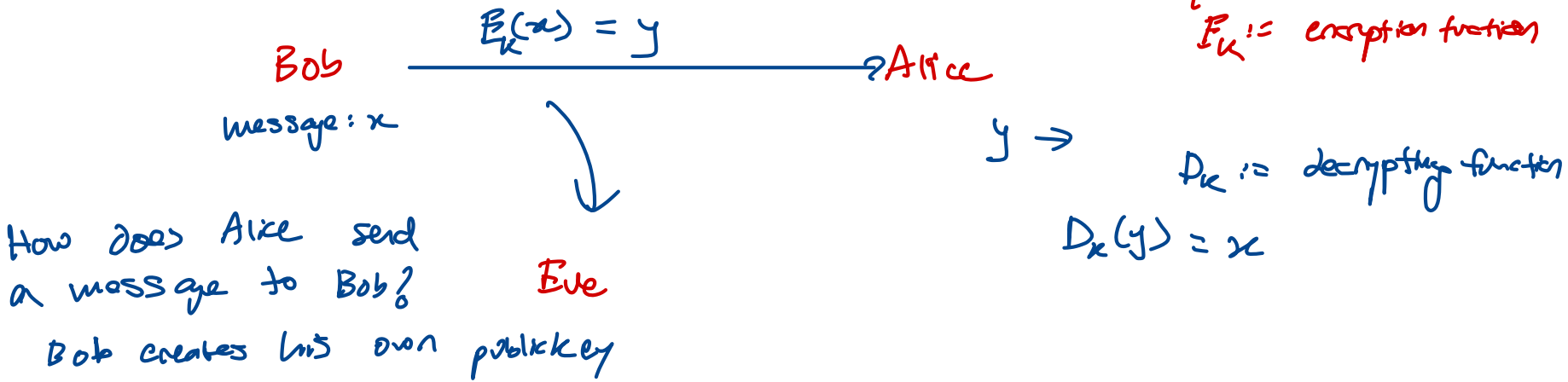
Alice generates

Alice generates a **Public Key** (K), and a corresponding **Private Key** (k).
The public key K is known to everyone (including Eve), the private key k is known only to Alice.

Alice publishes this

Anyone can encode their message using the public key, and send it to Alice.
Only Alice knows the private key, so only she can decrypt the messages sent to her.

Everyone knows
E_K := encryption function



RSA

Alice does the follow

Setting up a Public Key

Pick two large primes p and q. Let $N = pq$

Choose an e that is coprime to the product $(p-1)(q-1)$ $\gcd(e,(p-1)(q-1)) = 1$

Compute the private key $d = e^{-1} \pmod{(p-1)(q-1)}$.

Announce to the world the public key: $K = (N, e)$ → both to make a public key

Bob sends message

Encrypting Messages

Let x be your message. $E(.)$ is the encryption function. Send $E(x) = x^e \pmod{N}$.

Alice receives a message

public key

Decrypting Messages

Let y be the encrypted message. $D(.)$ is the decryption function. $D(y) = y^d \pmod{N}$.

private key

Why does this work?

Decrypting an encrypted message returns original message. $D(E(x)) = x = (x^e)^d \pmod{N}$

$D(E(x)) = D(x^e) = (x^e)^d = 1 \pmod{N}$

Can ppl figure out p,q from N?

Summary Questions

People

Alice, Bob, Eve

Alice has a public key (N,e)

Bob is sending a message x

Pick two large primes p and q. Let $N = pq$
Choose an e that is coprime to the product $(p-1)(q-1)$
Compute private key $k = d = e^{-1} \pmod{(p-1)(q-1)}$.
Announce to the world: $K = (N, e)$
Encryption: $E(x) = x^e \pmod{N}$.
Decryption: $D(y) = y^d \pmod{N}$.

RSA

	N	e	p and q	d	Private Key	Public Key	Encryption Function	Decryption Function	x message	y
Who knows	everyone	everyone	Alice	Alice	Alice	Everyone	Everyone	Alice	Bob (After Alice)	Everyone
Definition	$N = p \cdot q$	randomly choose e coprime to $(p-1)(q-1)$	Choose 2 large primes	$d = e^{-1} \pmod{((p-1)(q-1))}$	$K = (d, N)$	$K = (N, e)$	$E(x) = x^e \pmod{N}$	$D(y) = y^d \pmod{N}$	Bob just has a message	$y = E(x)$

RSA Example

Pick two large primes p and q. Let $N = pq$
Choose an e that is coprime to the product $(p-1)(q-1)$
Compute private key $k = d = e^{-1} \pmod{(p-1)(q-1)}$.
Announce to the world: $K = (N, e)$
Encryption: $E(x) = x^e \pmod{N}$.
Decryption: $D(y) = y^d \pmod{N}$.

$7(0) + 60(1) = 60$
$7(1) + 60(0) = 7$
$7(-8) + 60(1) = 4$
$7(9) + 60(-1) = 3$
$7(-17) + 60(2) = 1$

$7^{-1} \equiv -17 \equiv 43 \pmod{60}$

Alice Setting Up Public Key

$p = 7, q = 11 \quad N = 7 \cdot 11 = 77$

e coprime to $(7-1)(11-1) = 60$

$e = 7 \quad d = 43$

Public key $K = (N, e) = \boxed{(77, 7)}$

Bob Encrypting Message

$x = 2$: message

$E(x) = E(2) = 2^7 \bmod 77$

$2^7 = 128 \equiv 51 \bmod 77$

$y = 51$

51 →

Alice Decrypting Message

$y = 51 \quad D(y) = D(51) = 51^{43} \bmod 77$

↓ repeated squaring

$D(y) = 2 = x$ ☺

MAIN SLIDE

Why does encryption/decryption work?

Thm: For every x in {0, 1, ..., N-1}, $(x^e)^d \equiv x \pmod{N}$. (i.e. D(E(x)) = x)

Proof:

Notice that $d \equiv e^{-1} \pmod{(p-1)(q-1)}$. So, $ed \equiv 1 \pmod{(p-1)(q-1)}$

$ed = k(p-1)(q-1) + 1$, $k \in \mathbb{Z}$. $D(E(x)) = x$

We want to show that $x^{ed} \equiv x \pmod{N} \Rightarrow x^{ed} - x \equiv 0 \pmod{N}$

$x^{k(p-1)(q-1)+1} - x \equiv 0 \pmod{N}$. Since, p and q are prime and $N = p \cdot q$. If we show that $x^{k(p-1)(q-1)+1} - x \equiv 0 \pmod{p}$ and $\equiv 0 \pmod{q}$ then it is $\equiv 0 \pmod{N}$.

We wish to show $x^{k(p-1)(q-1)+1} - x \equiv 0 \pmod{p}$:

Case 1: x is a multiple of p, then p divides both the terms

Case 2: x is not a multiple, so $x \in \{1, 2, ..., p-1\} \pmod{p}$

So by FLT $(x^{p-1})^{k(q-1)} x - x \equiv 0 \pmod{p}$

(FLT: $x^{p-1} \equiv 1 \pmod{p}$)

$1^{k(q-1)} \cdot x - x \equiv x - x \equiv 0 \pmod{p}$

You can apply the identical argument to q. Thus, we are done.

FLT

$a \in \{1, 2, ..., p-1\}$

$a^{p-1} \equiv 1 \pmod{p}$

By CRT this uniquely determines x exists

Why can't Eve reconstruct the Private Key?

Idea: $d = e^{-1} \pmod{(p-1)(q-1)}$, but Eve knows e so why can't she just find the inverse?

Eve doesn't know (p-1) or (q-1) or even (p-1)·(q-1)

Eve only knows N

Why can't Eve then figure out p and q?

Eve knows N so why can't she figure out p and q using that?

We showed that every number has a prime factorization.
That is, given a natural number n there exist a unique set of primes such that n is equal to their product.

NP-HARD (CS170)

Finding this unique set of primes is **hard**.

What does it mean for a problem to be hard?
In this class, we will say that if the best solution is as good as guess-and-check it is hard.
To find the prime factorization you would have to try every factor for that number.

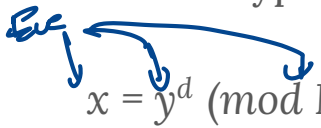
P vs. NP (CS170)

Is there a faster algorithm to find the factorization?
Unsolved Problem. It is possible with Quantum Computer.

Shors Algorithm

Why can't Eve just take the log?

Eve knows the public key (N, e). Eve then encrypts some message $y = x^e \ (mod\ N)$.
Then, the decryption is



So, why can't Eve just do log_y on both sides to **leak *d*** the private key?

This is called the discrete-log problem and it is **hard**. There is no known efficient solution for this problem.
Examples:

How easy is it to find large primes?

Theorem 7.3: **[Prime Number Theorem]** Let $\pi(n)$ denote the number of primes that are less than or equal to n. Then for all $n \geq 17$, we have $\pi(n) \geq \frac{n}{\ln n}$. (And in fact, $\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1$.)

If we want a 512-bit prime number

Theorem says there is roughly 1 prime number every 355 numbers.

For 1024-bit numbers there's a prime every 710.

Just try random numbers and you will eventually find a prime number

You can efficiently check if a number is prime using the Miller-Rabin test. (CS170)

$O(\sqrt{n})$ CS61A

↓

$O(\log n)$ CS170

Can Even find a match using the encryption function?

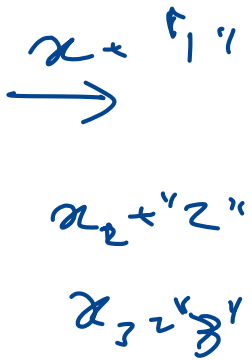
If Bob encrypts some message $y = x^e \ (mod\ N)$. Then, could Eve just plug in x' into the encryption function to find a match?

No! For 256-bit prime numbers that is 2^{256} it would take you 37 times the age of the universe to arrive at a guess for a $x' = x$.

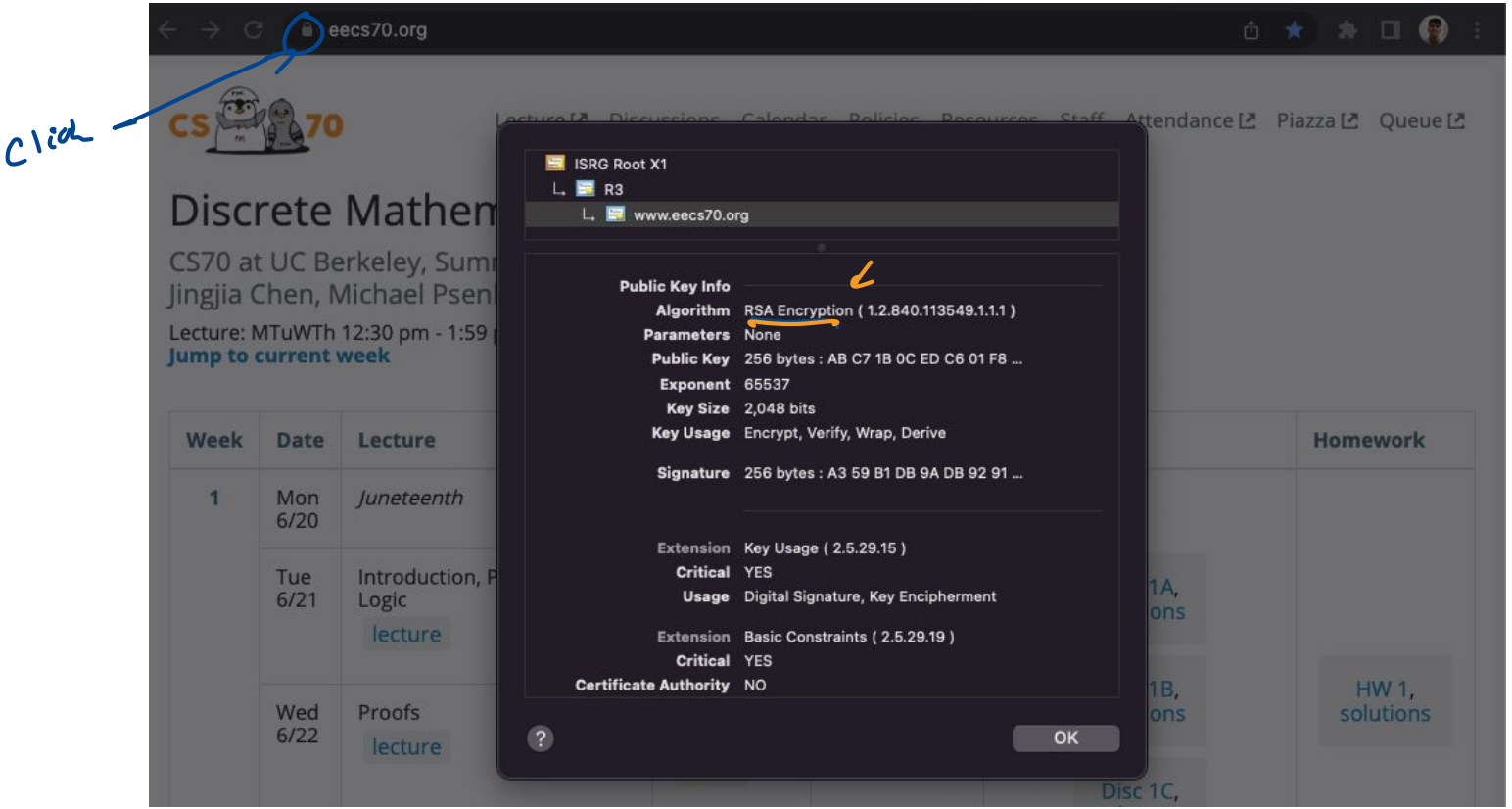
In Practice Sending Same Message Twice

Notice that since all the numbers are fixed, if you send the same message twice it will be encrypted the same way.

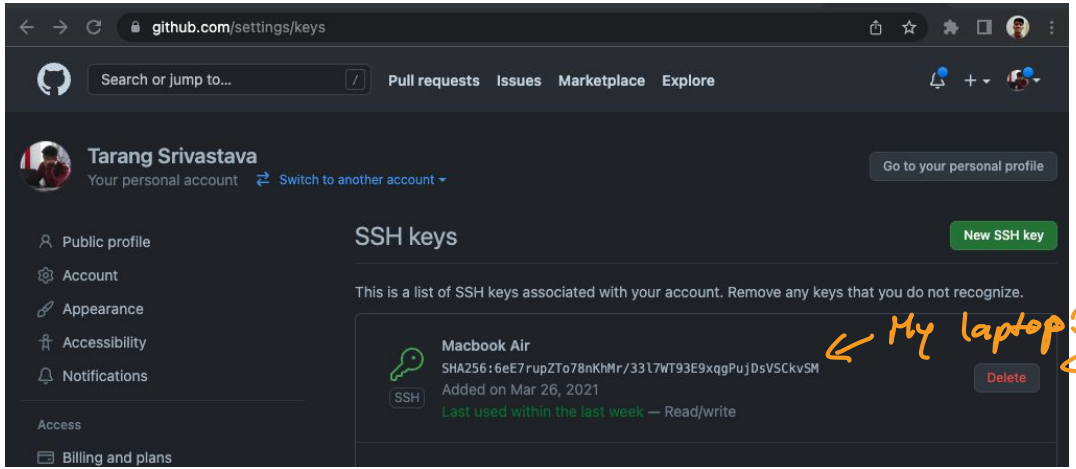
In practice, usually append a counter to the message so each message is unique.



You use some derivation of RSA every day



You use some derivation of RSA every day



We designed iMessage to use end-to-end encryption, so there's no way for Apple to decrypt the content of your conversations when they are in transit between devices. Attachments you send over iMessage (such as photos or videos) are encrypted so that no one but the sender and receiver(s) can access them. These encrypted attachments may be uploaded to Apple. To

A little story to end...

In 1977, Rivest, Shamir and Adleman publish the RSA algorithm you learned today.

Later that year, the British Intelligence Agency (GCHQ) declassify that they had developed the exact algorithm secretly in 1973.

Why do all this?

- Your company will ask you to make sure their data is secure
- You will want to make sure that your data is secure
- Most importantly, you have a **moral** responsibility to do so

Review

Lecture 3B: Polynomials, Secret Sharing

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post
- **HW 3** and **Vitamin 3** have been released, due **Thursday** (grace period Fri)
- HW 3 covers last Wednesday, Thursday and Yesterday's lecture.
- In this lecture, we will use small prime numbers as examples but in implementation we use large prime numbers (256 bits $\approx 10^{77}$ or more).

Finite Fields

Recall, that we talked about mod as a space.

When operating in a mod p where p is prime, we are working in a **finite field**.
A finite field is just a space of numbers, where we can define addition, subtraction, multiplication and division for all numbers in that space.

math 113/114

We will call this finite field a "Galois Field," denoted $GF(p)$

mod p

GF(p)

Polynomials in GF(p)

A **polynomial** in GF(p)

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

is specified by **coefficients** $a_d, \ldots, a_0$
$f(x)$ **contains** point (a, b) if $b = f(a)$

Polynomials over reals: $a_d, \ldots, a_0 \in \Re$, use $x \in \Re$
Polynomials in GF(p) have $a_d, \ldots, a_0 \in \{0, \ldots, p\text{-}1\}$, use $x \in \{0, \ldots, p\text{-}1\}$

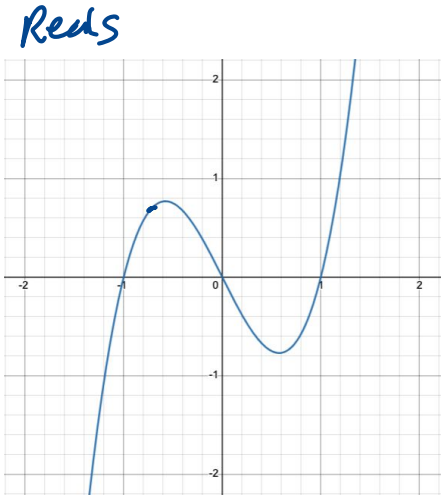
Example: $f(x) = 2x^3 - 2x = 2x^3 + 0x^2 + (-2)x + 0$

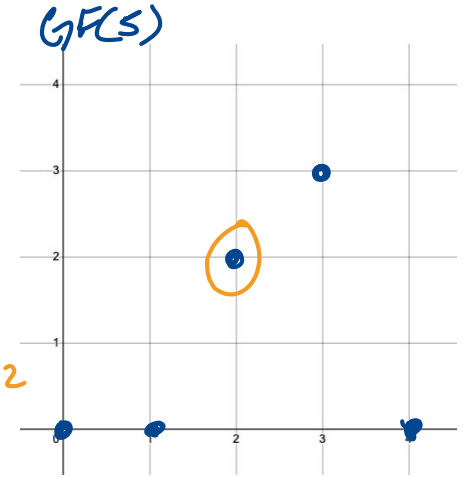
$a_3 = 2$
$a_2 = 0$
$a_1 = -2$
$a_0 = 0$

$f(2) = 2(2)^3 - 2(2)$
$= 2 \cdot 8 - 4$
$= 2$

Contains? $f(x)$

$(1, 2)$? No $f(1) \neq 2$
$(2, 2)$? Yes





Polynomials in $GF(p)$

A **polynomial** in $GF(p)$

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

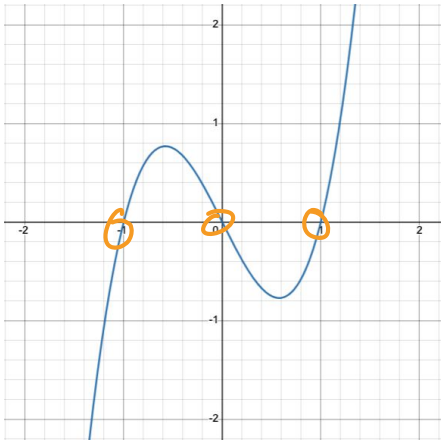
is specified by **coefficients** $a_d, \ldots, a_0$

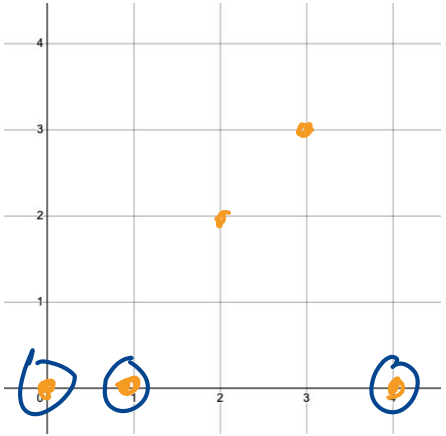
$f(x)$ **contains** point (a, b) if $b = f(a)$

The **degree** of a polynomial is the highest exponent in the polynomial

We say that a is a **root** (or **zero)** of a polynomial if $f(a) = 0$

Example: $f(x) = 2x^3 - 2x$





Degree $d \Rightarrow$ at most d roots

Property 1:

A non-zero polynomial of degree d has at most d roots

FLT $a^{p-1} \equiv 1 \mod p$

$a \in \{1, \ldots, p-1\}$

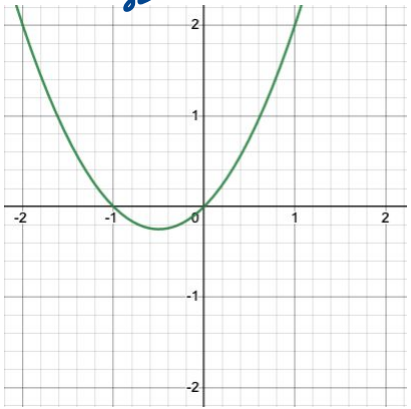
GF(5)

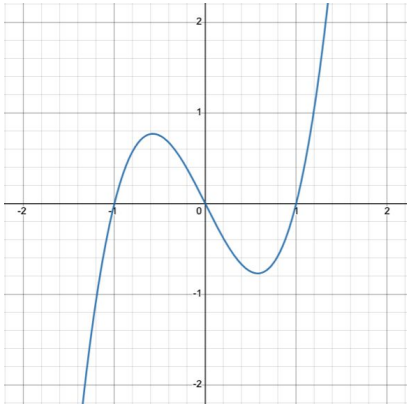
$f(x) = x^4$

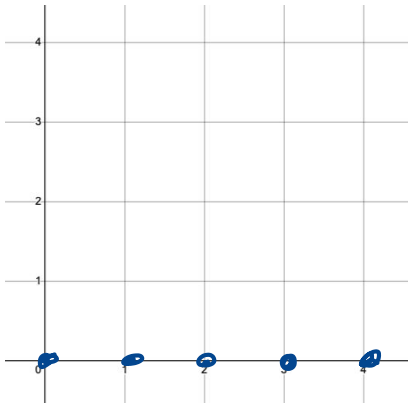
$f(x) = 0$

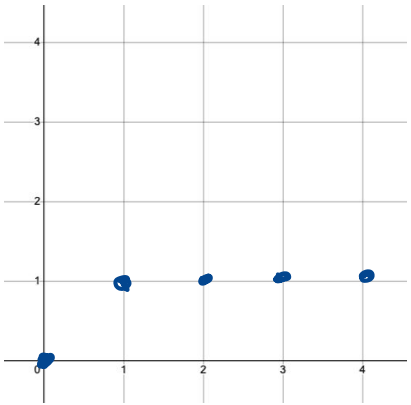
$x^2 + x$

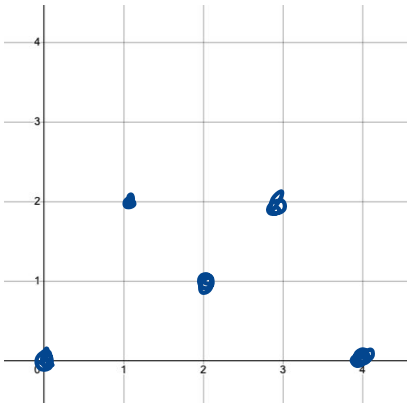
$2x^3 - 2x$

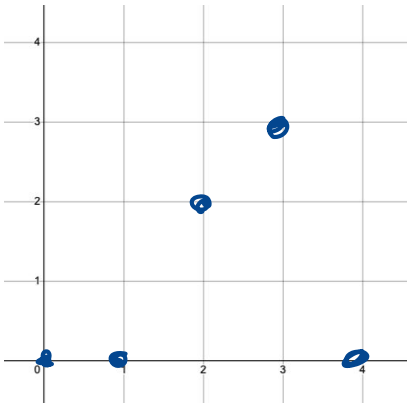












d+1 points ⇒ unique degree d polynomial

We say a **point** is a x, y pair where $y = f(x)$

Property 2:

Given d+1 pairs: (x_1, y_1), …, (x_{d+1}, y_{d+1}) with all the x_i distinct, there is a unique polynomial $f(x)$ of degree (at most) d such that $f(x_i) = y_i$ for $1 \le i \le d+1$

There is a unique degree d polynomial that goes through a given set of d+1 points

Key idea

Example:

Given 3 points ⟶ Degree 2 polynomial

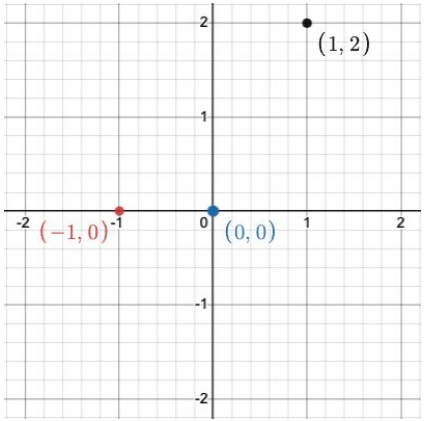
Points

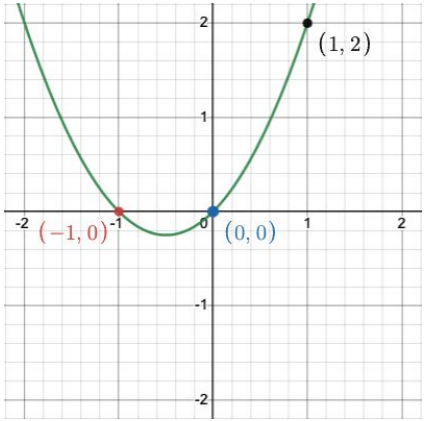
(−1, 0)

(0, 0)

(1, 2)

⟶ $x^2 + x$





Implication of Properties on a Line

Slope ↓ $\Rightarrow y = mx + b$ ← y-intercept

Suppose we have some linear polynomial

$$f(x) = a_1 x^1 + a_0$$

Property 1 says that if the line isn't just $f(x) = 0$ (x-axis) then it has at most 1 root.
Property 2 says two points define a line.

How to find a line that goes through a given two points:
Example: (1, 2) and (3, 4)

$y = mx + b$

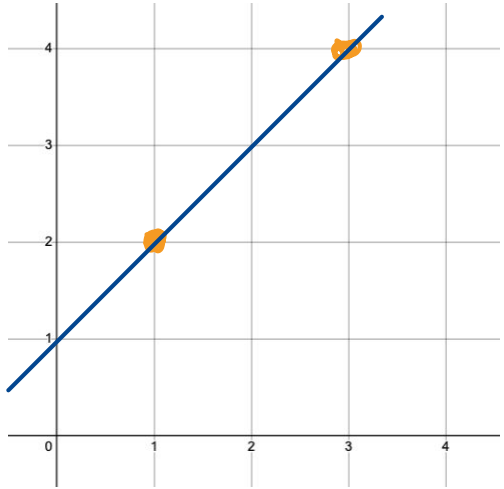
$m = \frac{y-2}{3-1} = \frac{2}{2} = 1$

y-intercept

$2 = (1)(1) + b$

$2 = 1 + b \qquad b = 1$

$f(x) = 1 \cdot x + 1$



Polynomial Equivalence

$a^{p-1} \equiv 1 \pmod{p}$

We state that two polynomials f and g are equivalent if for all x in GF(p), $f(x) = g(x)$

You can also show two polynomials are equivalent if they have the exact same coefficients.

$f(x) = 2x^2 + 2$

$g(x) = 2x^2 + 2$

Examples in GF(7):

$f_1(x) = x + 1$

$f_2(x) = 8x + 1$ $\quad 8 \equiv 1 \pmod 7$

$f_3(x) = x + 8$ $\quad 8 \equiv 1 \pmod 7$

$f_4(x) = x^7 + 1$

by FLT ✓

$x^6 \cdot x + 1$

$x + 1$

$f_3(0) = 1$

$f_4(0) = 1$ ✓

Polynomials from Points via Interpolation

Find the degree two polynomial in GF(5) that contains (1, 2); (2, 4); (3, 0)

mod 5

y_1 y_2 y_3

$$p(x) = y_1 \cdot \Delta_1(x) + y_2 \cdot \Delta_2 x + y_3 \cdot \Delta_3(x)$$

$$\Delta_i(x) = \begin{cases} 0 & \text{if } x \neq i \\ 1 & \text{if } x = i \end{cases}$$

$$\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = 3(x-2)(x-3) = 3x^2 - 15x + 18 = 3x^2 + 3$$

$$\Delta_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)} = 4(x-1)(x-3) = 4x^2 + 4x + 2$$

$$\Delta_3(x) = \frac{(x-1)(x-2)}{(3-1)(3-2)} = 3(x-1)(x-2) = 3x^2 - 9x + 6 = 3x^2 + x + 1$$

$$p(x) = 2(3x^2+3) + 4(4x^2+4x+2) + 0(3x^2+x+1)$$

$$\equiv 2x^2 + x + 4$$

p(x) contains these points

x	$2x^2+x+4$
1	$2(1)^2+1+4 \equiv 7 \equiv 2$ ✓
2	$2(2)^2+2+4 \equiv 4$ ✓
3	$2(3)^2+3+4 \equiv 0$ ✓

Polynomials from Points via Gaussian Elimination

Find the degree two polynomial in GF(5) that contains (1, 2); (2, 4); (3, 0)

$f(x) = a_2x^2 + a_1x + a_0$

input	
1	$2 = a_2(1)^2 + a_1(1) + a_0$
2	$4 = a_2(2)^2 + a_1(2) + a_0$
3	$0 = a_2(3)^2 + a_1(3) + a_0$

$$2 = a_2 + a_1 + a_0$$
$$4 = 4a_2 + 2a_1 + a_0$$
$$0 = 9a_2 + 3a_1 + a_0$$

Why you need $d+1$ points for degree d

$d+1$ unknown coefficients

Proving Property 2

Property 2: Given d+1 pairs: (x_1, y_1), …, (x_{d+1}, y_{d+1}) with all the x_i distinct, there is a unique polynomial $f(x)$ of degree (at most) d such that $f(x_i) = y_i$ for $1 \le i \le d+1$

"d+1 points, define a unique degree d polynomial"

1. We showed the existence of a polynomial via interpolation
2. We need to show uniqueness

Proof for uniqueness:

Assume for contradiction that given some d+1 points there exist two degree d polynomials that contain the same d+1 points, call them $p(x)$ and $q(x)$. Since, $p(x) \neq q(x)$ $p(x) - q(x) \neq 0$. Notice that $p(x) - q(x)$ is then a degree d polynomial at most. But $p(x) - q(x) = 0$ for the d+1 points that p and q share. This is a contradiction since by Property 1 $p(x) - q(x)$ can have d roots at most.

* $p(x) - q(x) \neq 0$ means it is not always zero.

Long Division

It is possible to divide polynomials. That is dividing $p(x)$ by $q(x)$ results in

$$p(x) = q'(x)\, q(x) + r(x)$$

Example: $p(x) = x^3+x^2-1$ and $q(x) = x - 1$

quotient ↑ remainder ↑

$\frac{p(x)}{q(x)}$

$$
\begin{array}{r|l}
 & x^2 + 2x + 2 \\
\hline
x-1 & x^3+x^2+0\cdot x-1 \\
 & -(x^3-x^2)\ \downarrow\quad\downarrow \\
\hline
 & 0+2x^2+0\cdot x-1 \\
 & -(2x^2-2x\ \downarrow) \\
\hline
 & 0+2x-1 \\
 & -(2x-2) \\
\hline
 & 1
\end{array}
$$

$q'(x) = x^2+2x+2$

$r(x) = 1$

Proving Property 1

Property 1: A non-zero polynomial of degree d has at most d roots
We will prove this by proving these two other claims.

Claim 1: If a is a root of a polynomial $p(x)$ with degree $d \geq 1$, then $p(x) = (x-a)q(x)$ for a polynomial $q(x)$ with degree $d - 1$

Claim 2: A polynomial $p(x)$ of degree d with distinct roots $a_1, \ldots, a_d$ can be written as $p(x) = c(x-a_1)\ldots(x-a_d)$ where c is just a number.

Proving Property 1 with Claim 1

Property 1: A non-zero polynomial of degree d has at most d roots

Claim 1: If a is a root of a polynomial $p(x)$ with degree $d \geq 1$, then $p(x) = (x-a)q(x)$ for a polynomial $q(x)$ with degree $d - 1$

deg $d-1$ $(d-1)$

deg d

$p(x) = (x-a)q(x) + r(x)$

if a is a root

$p(a) = 0 = (a-a)q(a) + r(a)$ ($a-a = 0$, $q(a)$ → 0)

$r(a) = 0$

Proving Property 1 with Claim 2

Property 1: A non-zero polynomial of degree d has at most d roots

Claim 2: A polynomial $p(x)$ of degree d with distinct roots $a_1, \ldots, a_d$ can be written as $p(x) = c(x-a_1)\ldots(x-a_d)$ where c is just a number.

$x^2 - 2x + 1 = (x-1)(x-1)$

By induction on degree

Ind. Step:

$p(x) = (x - r_1)\, q(x)$ and by Claim 1 $q(x)$ has degree $d-1$

So apply Ind. Hyp.

Secret Sharing

There is a code that can be used to launch nuclear weapons.
We don't want this code to be accessed unless k of the total n military generals agree.

How do we solve this?

1284

Secret Sharing (cont.)

There is a secret code that can be used to launch nuclear weapons.
We don't want this code to be accessed unless k of the total n military generals agree.

How do we solve this?

1. Construct a degree k-1 polynomial. Call it $p(x)$.
2. Encode the secret code as $p(0)$ = "*secret code*"
3. Give each general a point that $p(x)$ contains.
    a. i.e. General #1 gets $(1, p(1))$. General #2 gets $(2, p(2))$. So on…
4. When any k general agree. They can share their points and they will have k points to reconstruct a degree k-1 polynomial. Then, they just plug in $p(0)$ to find the secret.

Example of Secret Sharing

1 2 3 4 5 6 7

Tarang wants to set up a system that if any 3 of Michael, Jingjia, Nikki, Christine, Jet, Colby or Korinna agree then the midterm solutions will be released immediately.
Suppose the secret code to the solutions is "6".

What degree polynomial does Tarang need to construct? 2

How many points do we need to generate? 7 (not including secret)

$p(x) = x^2 + 2x + 6$ $\quad p(0) = 6$ ✓ $\quad GF(7)$

Michael = $(1, p(1)) = (1, 1^2 + 2(1) + 6) = (1, 2)$

Jingjia = $(2, p(2))$ $\quad (2, 0)$

Nikki = $(3, p(3))$ $\quad (3, 0)$

Christine = $(4, p(4))$ $\quad (4, 2)$

Example of Secret Sharing (cont.)

GF(7)

Suppose Jingjia, Nikki and Christine agree to release the solutions before the midterm. How would they do it?

Jingjia (2, 0)

Christine (4, 2)

Nikki (3, 0)

$$p(x) = \cancel{\Delta_2 \cdot 0}^{0} + \Delta_4 \cdot 2 + \cancel{\Delta_3 \cdot 0}^{0}$$

$$\Delta_4 = \frac{(x-2)(x-3)}{(4-2)(4-3)}$$

$$\Delta_4 = 4(x-2)(x-3)$$

$$p(x) = 2 \cdot 4(x-2)(x-3)$$

$$= x^2 + 2x + 6$$

$$p(0) = 6$$ (!!)

Counting Polynomials

Assume for all these questions we're working in $GF(p)$

How many unique degree at most k polynomials are there?

How many exactly degree k polynomials are there?

If we wish to find a degree 5 polynomial and we know only 3 points how many options do we have for the polynomials that currently go through our 3 points?

Review

Lecture 3C: Error Correction

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post
- **HW 3** and **Vitamin 3** have been released, due **Today** (grace period Fri)
- Tarang's Last Lecture, Michael will begin starting next week
- Midterm is 7/15 (6-8p)
- Midterm Scope
  - Notes: 1-11
  - HW: 1-4
  - Lectures: 1A-4B
  - Discussions: 1A-4B
  - Topics: Up to and including countability. (Computability will not be on the midterm)
- Midterm format will be different from previous semesters. More proofs.

Review

Property 1: A non-zero polynomial of degree d has at most d roots
Property 2: Any $d+1$ points define a unique degree d polynomial] main idea secret sharing

Claim 2: A polynomial of degree d with roots $a_1, \ldots, a_k$ can be written as $p(x) = c(x-a_1)\ldots(x-a_k)$.

$x^2 - 2x + 1$
$(x-1)(x-1)$

From Discussion 3B:
if f and g are degree x and degree y then

- $f + g$ is at most degree $max(x, y)$
- $f \bullet g$ is at most degree $x + y$
- f / g is at most degree $x - y$

Review (cont.)

Secret Sharing:

Problem: We need any k out of n people to agree to unlock some code.

Solution:

1. Create a degree k-1 polynomial $p(x)$
2. Encode the secret in the polynomial ($p(0)$ = "*secret*").
3. Give a point that the polynomial contains to each person (generate n points)
4. Any k points can be used to reconstruct the degree k-1 polynomial $p(x)$

$n > k$

Review of Gaussian Elimination

Why do d+1 points define a degree d polynomial uniquely?

A degree d polynomial has $d + 1$ coefficients:

$d+1$ coefficients

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

So, we need $d + 1$ equations to solve for $d + 1$ unknowns.
We get $d + 1$ equations by plugging in the $d + 1$ points.

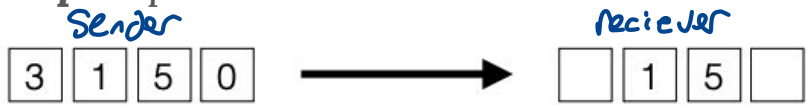
degree 3: $a_3 x^3 + a_2 x^2 + a_1 x + a_0$

$a_3(0)^3 + a_2(0)^2 + a_1 \cdot 0 + a_0 = 1$

x	$p(x)$
0	1

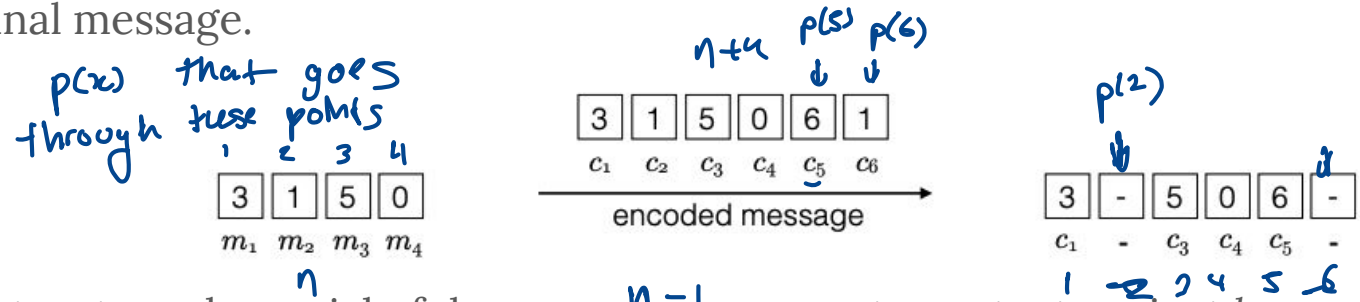
Erasure Errors

Send some message across an **unreliable** channel.
The channel randomly **drops** k packets.



How can we **recover** our original message? Polynomials!

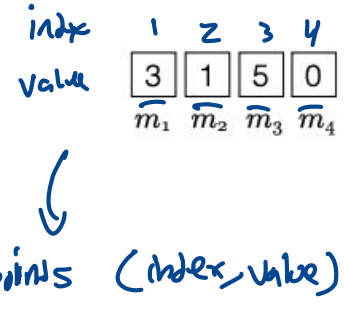
We want to encode our message into a polynomial, and then generate k extra packets. Then with any n received packets we can reconstruct the polynomial and get the original message.



Construct a polynomial of degree $n-1$ to protect against k erasures.

Bob sends message with erasure protection

Bob wants to send the message "3 1 5 0" to Alice.
Bob knows that at most 2 packets will drop when sending the message to Alice.
n := *message length* (4) k := *maximum erasures* (2)
Message "3 1 5 0" become points "(1, 3)" "(2, 1)" "(3, 5)" "(4, 0)"
Find a degree 3 polynomial that goes through these points in GF(7)



1) interpolation 2) Gaussian Elimination

$p(x) = ax^3 + bx^2 + cx + d$

$3 = a(1)^3 + b(1)^2 + c(1) + d$

$1 = a(2)^3 + b(2)^2 + c(2) + d$ ⟹

$a + b + c + d = 3$
$a + 4b + 2c + d = 1$
$6a + 2b + 3c + d = 5$ ⟹
$a + 2b + 4c + d = 0$

$a = 1$
$b = 4$
$c = 0$
$d = 5$

$p(x) = x^3 + 4x^2 + 5$

What are the extra points Bob generates?

$p(5) = 5^3 + 4(5)^2 + 5 = 6$ (5, 6)
$p(6) = 6^3 + 4(6)^2 + 5 = 1$ (6, 1)

Bob Sends | 3 | 1 | 5 | 0 | 6 | 1 |

Alice receives message with erasure errors

GF(7)

Alice receives the points (1, 3); (3, 5); (4, 0); (5, 6). How can Alice reconstruct the polynomial?

$p(x) = ax^3 + bx^2 + cx + d$

$3 = a + b + c + d$

$5 = 8a + 2b + 3c + d$

$0 = a + 2b + 4c + d$

$6 = 6a + 4b + 5c + d$

$\Rightarrow$ $a = 1$, $b = 4$, $c = 0$, $d = 5$

$p(x) = x^3 + 4x^2 + 5$

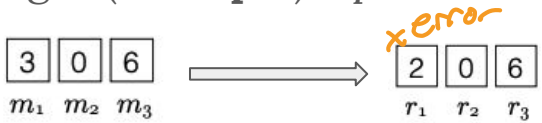
$p(2) = 1$

3 1 5 0

What if you drop less than k packets?

General Errors

Send some message across a **noisy** channel.
The channel randomly changes (**corrupts**) k packets



How can we **recover** our original message?

$e(x) = (x-1)$ indicates error at index 1

This is much harder that Erasure Errors because...

1. locate where the error occurs
2. recover the correct value

Erasure Errors: Send $n + k$ packets to protect against k erasures
General Errors: Send $n + 2k$ packets to protect against k **corruptions**.

Solution: Berlekamp-Welch

Message: $m_1, \ldots, m_n$ (length = n)

Sender:

1. Form degree n-1 polynomial $p(x)$ where $p(i) = m_i$
2. Send $p(1), \ldots, p(n + 2k)$

Same as erasure

Receiver:

1. Receive $r_1, \ldots, r_{n+2k}$ could be corrupted
2. Solve $n + 2k$ equations, $q(i) = e(i)\, r_i$ to find $q(x) = e(x)p(x)$ and $e(x)$
3. Compute $p(x) = q(x)/e(x)$
4. Compute $p(1), \ldots, p(n)$ to get original message

Here r_i are the received points possibly with errors.
$p(x)$ is the original polynomial the sender used, receiver doesn't know yet
$e(x)$ is an error locator polynomial. $e(x) = (x-e_1)\ldots(x-e_k)$ where e_i is the index where the error occurs
$e(x) = 0$ when you plug in a x value where error occurs. Receiver doesn't know $e(x)$ yet.
$q(x) = e(x)p(x)$. So, we find $q(x)$ and $e(x)$ to get $p(x)$.

Berlekamp-Welch (cont.)

$q(1) = e(1)p(1) = e(1) \cdot r_1$

$q(2) = e(2)p(2) = e(2)\, r_2$

$\vdots$

$q(n+2k) = e(n+2k)\,p(n+2k) = e(n+2k)\, r_{n+2k}$

Receiver:

1. Receive $r_1, \ldots, r_{n+2k}$
2. Solve $n + 2k$ equations, $q(i) = e(i)p(i) = e(i)\, r_i$ to find $q(x) = e(x)p(x)$ and $e(x)$ is error locator polynomial. $e(i) = 0$ when there is an error in index i
3. Compute $p(x) = q(x)/e(x)$
4. Compute $p(1), \ldots, p(n)$ to get original message

$\deg p(x) = n-1$

$\deg e(x) = k$

$e(x) = (x-e_1)\cdot(x-e_2)\cdots(x-e_k)$ (leading coefficient will be 1)

$= x^k + \ldots$

$q(x) = p(x) \cdot e(x)$

Case 1: $p(i) = r_i$

$e(i)p(i) = e(i)\, r_i$

Case 2: $p(i) \neq r_i$

$e(i)p(i) = e(i)\, r_i$

$e(i) = 0$

$0 \cdot p(i) = 0 \cdot r_i$

$0 = 0$ ✓

What is the degree of $q(x)$? $n+k-1$ How many unknowns? $n+k$ (coefficients)

What is the degree of $e(x)$? k How many unknowns? ~~$k+1$~~ k

We have $n+2k$ unknowns in total and $n+2k$ equations

Bob sends message with corruption protection

Bob wants to send the message "3 0 6" to Alice.

Bob knows that at most 1 packet will be **corrupted** when sending the message to Alice.

n := message length (3) *k := maximum corruptions* (1)

$n+2k = 5$

Find a degree 2 polynomial that goes through these points in GF(7)

$p(x) = x^2 + x + 1$ ← from points (1,3) (2,0) (3,6)

$p(4) = 0$

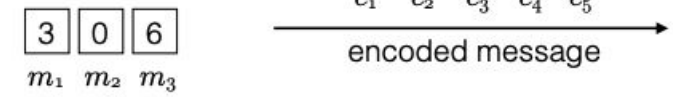
$p(5) = 3$

What are the extra points Bob generates?

(4,0)

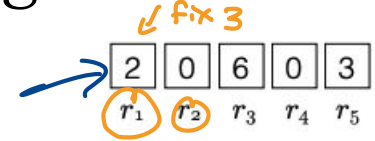
(5,3)

extra



Alice receives message with corruption errors

GF(7)



How can Alice find where the error is and fix it?

$q(x) = p(x)e(x)$

$\deg q = 3$

$\deg e = 1$

$q(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$e(x) = x + b_0$

i	$q(i) = p(i)e(i) =$	$r_i e(i)$
1	$a_3(1)^3 + a_2(1)^2 + a_1(1) + a_0 =$	$2(1 + b_0)$
2	$a_3(2)^3 + a_2(2)^2 + a_1(2) + a_0 =$	$0(2 + b_0)$
3		
$n+2k$		

$a_3 + a_2 + a_1 + a_0 - 2b_0 = 2$

$a_3 + a_2 + a_1 + a_0 + 5b_0 = 2$

$a_3 + 4a_2 + 2a_1 + a_0 = 0$

$6a_3 + 2a_2 + 3a_1 + a_0 + b_0 = 4$

$a_3 + 2a_2 + 4a_1 + a_0 = 0$

$6a_3 + 4a_2 + 5a_1 + a_0 + 4b_0 = 1$

$a_3 = 1$, $a_2 = 0$, $a_1 = 0$, $a_0 = 6$

$q(x) = (1)x^3 + (0)x^2 + (0)x + 6$

$= x^3 + 6$

$b_0 = 6 \rightarrow e(x) = x + 6$

error at index 1

$= (x - 1)$

$p(x) = \frac{q(x)}{e(x)}$

$$x-1 \;\big|\; x^3 + 0 + 0 + 6 \qquad \text{quotient } x^2 + x + 1$$

$p(x) = x^2 + x + 1$

correct value = $p(1)$

3 ✓

Alice receives same message with NO corruption errors

Will Alice still get the same correct answer?

Q(x) and E(x) are the same

$p(x)$ is unique from Berlekamp-Welch

Thm: Any solution to Berlekamp-Welch will result in the same final $p(x)$

Proof:

Assume there's another solution $Q'(x)$ and $E'(x)$ they satisfy

$$Q'(i) = r_i E'(i) \qquad 1 \le i \le n+2k$$

$$Q'(i) - r_i E(i) = r_i E'(i) - r_i E(i) = r_i E'(i) - Q(i)$$

$$\frac{Q'(i) - E(i)}{E'(i) - E(i)} = \frac{E'(i) \cdot Q(i)}{E'(i) E(i)} \qquad 1 \le i \le n+2k$$

$$\frac{Q'(i)}{E'(i)} = \frac{Q(i)}{E(i)} = P(i)$$

$p(x)$ is unique from Berlekamp-Welch

Thm: Any solution to Berlekamp-Welch will result in the same final $p(x)$

Proof:

Review Counting

Review Countability

Review

Review

Review