# Counting – Part 2

CS70: Discrete Mathematics and Probability Theory

*UC Berkeley – Summer 2025*

Lecture 13

*Ref: Still Note 10*

# Today

Combinatorial Proofs
- Proving identities using counting
- Binomial Theorem
- Pascal's Triangle and Pascal's Rule

Brief Midterm Review

# Combinatorial Proofs: Counting for Proving Identities

**Theorem:** For all $n, k \in \mathbb{N}$, $\binom{n}{k} = \binom{n}{n-k}$.

*Proof?* In this case, the algebra is easy... but let's count instead.

**Counting Proof** (Sketch):

*Question:* Given the set of all $n$-bit strings, how many have $k$ zeros?

$$\binom{n}{k}$$

Given the set of all $n$-bit strings, how many have $n-k$ ones?

$$\binom{n}{n-k}$$

These are the same set! Length $n$: $k$ zeroes $\iff$ $(n-k)$ ones.

So

$$\binom{n}{k} = \binom{n}{n-k}.$$

□

*Another view:* # ways to *choose* $k$ from $n$ $=$ # ways to *exclude* $n-k$.

# Binomial Coefficients 1

*Question:* What is $(a+b)^n$? Algebra? Yes.
... But also combinatorics. Counting.

$$(a+b)^2 = (a+b)^1(a+b) = \underbrace{(a+b)}_{\text{all len-1 seq}}\ (a+b)$$

$$= \underbrace{(a+b)}_{\text{all len-1 seq}}\ a + \underbrace{(a+b)}_{\text{all len-1 seq}}\ b$$

$$= \underbrace{aa+ab+ba+bb}_{\text{all length-2 sequences}}$$

$$(a+b)^3 = (a+b)^2(a+b) = \underbrace{(aa+ab+ba+bb)}_{\text{all length-2 sequences}}(a+b)$$

$$= \underbrace{(aa+ab+ba+bb)}_{\text{all length-2 sequences}}a + \underbrace{(aa+ab+ba+bb)}_{\text{all length-2 sequences}}b$$

$$= \underbrace{aaa+aab+aba+abb+baa+bab+bba+bbb}_{\text{all length-3 sequences}}$$

# Binomial Coefficients 2

$$(a+b)^3 = \underbrace{aaa+aab+aba+abb+baa+bab+bba+bbb}_{\text{all length-3 sequences}}$$

How many terms have 3 $a$'s? Just one.

How many terms have 2 $a$'s? Three – and all are $a^2b$

How many terms have 1 $a$? Three – and all are $ab^2$

General for $(a+b)^n$

All length $n$ sequences of $a$'s and $b$'s

How many have exactly $k$ $a$'s? $\binom{n}{k}$ – and all are $a^k b^{n-k}$

So:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Great algebraic identity... proved by counting - a combinatorial proof

# Pascal's Triangle

*Construction:* Each entry in a triangle is sum of two above it.

$$
\begin{array}{ccccccc}
 & & & 0 & & & \\
 & & 1 & & 1 & & \\
 & 1 & & 2 & & 1 & \\
1 & & 3 & & 3 & & 1 \\
1 & 4 & & 6 & & 4 & 1 \\
 & & & \cdots & & &
\end{array}
$$

Looks like... combinations:

$$
\begin{array}{ccccccc}
 & & & \binom{0}{0} & & & \\
 & & \binom{1}{0} & & \binom{1}{1} & & \\
 & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3}
\end{array}
$$

Is this true (Pascal's rule)? $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

# Combinatorial Proof: Pascal's Rule

**Theorem:** For $n, k \in \mathbb{N}$, $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

**Proof:** How many size $k$ subsets of $\{1, \ldots, n+1\}$? $\binom{n+1}{k}$

How many size $k$ subsets with value $n+1$? *Remaining* $k-1$ *from* $\{1, \ldots, n\}$*:*

$$\binom{n}{k-1} \tag{1}$$

How many size $k$ subsets without value $n+1$? *All* $k$ *come from* $\{1, \ldots, n\}$*:*

$$\binom{n}{k} \tag{2}$$

Any subset of size $k$ is counted once, in either (1) or (2), so

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}. \qquad \square$$

**Sum Rule:** Size of union of disjoint sets of objects is sum of set size
Above: With and without value $n+1 \longrightarrow$ disjoint.

# Hockey Stick Identity

**Theorem:**

$$\binom{n}{k+1} = \binom{n-1}{k} + \binom{n-2}{k} + \cdots + \binom{k}{k}$$

In Pascal's Triangle

$$\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}$$

General Position

$$\begin{array}{ccccc}
 & \cdots & \binom{n-4}{k} & \cdots & \\
\cdots & & \binom{n-3}{k} & & \cdots \\
 & \cdots & \binom{n-2}{k} & \cdots & \\
\cdots & & \binom{n-1}{k} & & \cdots \\
 & \cdots & \binom{n}{k+1} & \cdots &
\end{array}$$

Can prove algebraically... but what does it mean for counting?

# Hockey Stick Identity: Combinatorial Proof

**Theorem:** $\binom{n}{k} = \binom{n-1}{k-1} + \cdots + \binom{k-1}{k-1}$.

**Proof:** Count subsets of $\{1, 2, \ldots, n\}$.

*First way of counting:* Subsets of $k$ items from $n$: $\binom{n}{k}$

*Second way of counting:* What is smallest item in subset?

How many subsets where the smallest item is 1?
Remaining $k-1$ from $2, \ldots, n$ ($n-1$ choices): $\binom{n-1}{k-1}$

How many subsets where the smallest item is 2?
Remaining $k-1$ from $3, \ldots, n$ ($n-2$ choices): $\binom{n-2}{k-1}$

How many subsets where the smallest item is 3?
Remaining $k-1$ from $4, \ldots, n$ ($n-3$ choices): $\binom{n-3}{k-1}$

...

Must leave at least $k-1$ for remaining elements
$\Rightarrow$ Pattern continues until $\binom{k-1}{k-1}$

*Conclusion:* $\binom{n}{k} = \binom{n-1}{k-1} + \cdots + \binom{k-1}{k-1}$. □

# Sum of Binomial Coefficients

**Theorem:** $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$ .

**Proof:** How many subsets of $\{1, \ldots, n\}$?

*First way of counting:* Sequence of $n$ choices to include or exclude:

Element $i$ is **in** or **not in** the subset: 2 choices

First rule of counting: $2 \times 2 \cdots \times 2 = 2^n$ subsets

*Second way of counting:* Count subsets of each size:

How many subsets of size $k$? $\binom{n}{k}$

Every subset has a specific size (size $k$ disjoint from size $k+1$)

Counting subsets of all sizes: $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$ subsets

*Conclusion:* $\binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{0} = 2^n$ □

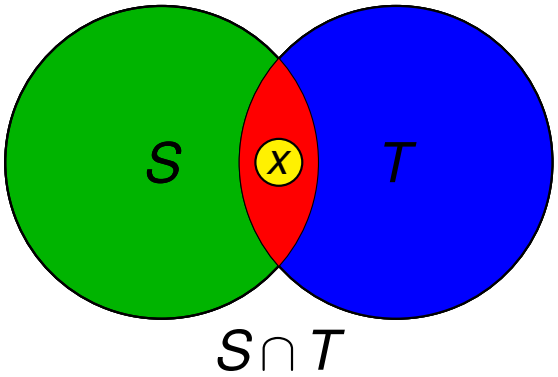
# Simple Inclusion/Exclusion: Two Sets

**Sum Rule:** For disjoint sets $S$ and $T$, $|S \cup T| = |S| + |T|$

Used to reason about all subsets
... adding number of subsets of size 1, 2, 3,...

Also reasoned about subsets that contained or didn't contain an element
... first element, smallest element, ...

**Inclusion/Exclusion Rule:** For any $S$ and $T$, $|S \cup T| = |S| + |T| - |S \cap T|$ .




Count in $S \implies |S|$

Count in $T \implies |T|$

Elements in $S \cap T$, like $x$, are counted twice

Remove double-counts $\implies -|S \cap T|$

$$|S \cup T| = |S| + |T| - |S \cap T|$$

# Simple Inclusion/Exclusion: Two Set Example

**Sum Rule:** For disjoint sets $S$ and $T$, $|S \cup T| = |S| + |T|$

Used to reason about all subsets
... adding number of subsets of size 1, 2, 3,...

Also reasoned about subsets that contained or didn't contain an element
... first element, smallest element, ...

**Inclusion/Exclusion Rule:** For any $S$ and $T$, $|S \cup T| = |S| + |T| - |S \cap T|$ .

**Example:** How many 10-digit numbers have 7 as their first or second digit?

$S$ = 10-digit numbers with 7 as first digit. $|S| = 10^9$

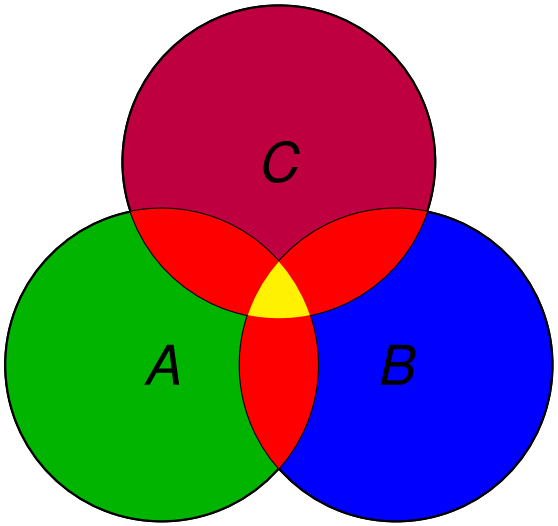
$T$ = 10-digit numbers with 7 as second digit. $|T| = 10^9$

$S \cap T$ = 10-digit numbers with 7 as first and second digit. $|S \cap T| = 10^8$

*Answer:* 10-digit numbers with 7 as first *or* second digit: $S \cup T$

$$|S \cup T| = |S| + |T| - |S \cap T| = 10^9 + 10^9 - 10^8 = 1,900,000,000$$

# Inclusion/Exclusion: Three Sets




All with duplications: $|A \cup B \cup C|$

$A$ and $C$ overlap overcounted, so subtract: $-|A \cap C|$

$A$ and $B$ overlap overcounted, so subtract: $-|A \cap B|$

$B$ and $C$ overlap overcounted, so subtract: $-|B \cap C|$

What about the yellow area?

- Added in 3 times (with $A$, $B$, and $C$)
- Subtracted out 3 times (each intersection)
- Too much!! Need to add back in: $+|A \cap B \cap C|$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

*Generalizing:* Add in all sets,
subtract out pairwise intersections,
add in 3-way intersections,
subtract out 4-way intersections,
...

# Inclusion/Exclusion: General

$$|A_1 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i,j} |A_i \cap A_j| + \sum_{i,j,k} |A_i \cap A_j \cap A_k| \cdots (-1)^n |A_1 \cap \cdots A_n|$$

*Proof Idea:* How many times is each element counted?

Element $a$ in $m$ sets: $a \in A_{i_1} \cap A_{i_2} \cdots \cap A_{i_m}$

For each $i \leq m$: Included in $\binom{m}{i}$ $i$-way intersections

Total counts for $a$: $\binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \binom{m}{4} + \cdots + (-1)^{m-1}\binom{m}{m}$

Binomial Theorem: $(x+y)^m = \binom{m}{0}x^m + \binom{m}{1}x^{m-1}y + \binom{m}{2}x^{m-2}y^2 + \cdots \binom{m}{m}y^m$

For $x = 1, y = -1$:

$(x+y)^m = (1-1)^m = 0$

$(x-y)^m = \binom{m}{0} - \binom{m}{1} + \binom{m}{2} - \binom{m}{3} + \binom{m}{4} + \cdots + (-1)^m\binom{m}{m}$

$\implies \quad \binom{m}{0} = \binom{m}{1} - \binom{m}{2} \cdots + (-1)^{m-1}\binom{m}{m}$

$\implies \quad 1 = \binom{m}{1} - \binom{m}{2} \cdots + (-1)^{m-1}\binom{m}{m}$

Each element counted exactly once!

# Lecture 12 Summary

Combinatorial Proofs: Identity from counting same set in two ways

- Basic combinations: $\binom{n}{k} = \binom{n}{n-k}$ ways to include $k$ = ways to exclude $n-k$
- Binomial Coefficients and Binomial Theorem
  - Expansion of monomial power is ways of choosing $a$ factors
- Pascal's Triangle and Pascal's Identity: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.
  - LHS: Count as number of subsets of $n+1$ items size $k$.
  - RHS: $\binom{n}{k-1}$ counts subsets of $n+1$ items with first item.
    - $\binom{n}{k}$ counts subsets of $n+1$ items without first item.
    - Disjoint – so add!
- Hockey Stick Identity
  - Count as subsets, and count as subsets with given smallest element

Inclusion/Exclusion: Two sets of objects

- Add number of each subtract intersection of sets
- Sum Rule: If intersection is empty, nothing to subtract!

Inclusion/Exclusion: General

- Alternate adding/subtracting: Add 1-way, subtract 2-way, add 3-way, ...

# Quick Midterm Review

The Course Until Now...

# Lecture 1 (Propositions and Predicates): Summary

Propositions are statements that are true or false.

Propositional forms use $\wedge, \vee, \neg$.

The meaning of a propositional form is given by its truth table.

Logical equivalence of forms means same truth tables.

Implication: $P \implies Q \equiv \neg P \vee Q$.

Contrapositive: $\neg Q \implies \neg P$ (equivalent to $P \implies Q$)

Converse: $Q \implies P$ (not equivalent)

Predicates: Statements with variables

Quantifiers: Universal $\forall x\ P(x)$ and existential $\exists y\ Q(y)$

Now can state theorems (provable propositions)! And disprove false ones!

De Morgan's Laws: "Flip and Distribute negation"

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

$\neg \forall x\ P(x) \iff \exists x\ \neg P(x)$.

# Concept Check: Propositions

True or False?

(A) $P \vee Q \equiv (\neg P \implies Q)$? True

A version of $R \implies S \equiv \neg R \vee S$.

(B) $\exists n \in N\,(\neg P(n)) \equiv \neg \forall n\, P(n)$? True

If its not always true, it must be false at some point.

(C) $\forall n \in N\,\big(Q(n) \vee P(n)\big) \equiv \big(\forall n \in N\, Q(n)\big) \vee \big(\forall n \in N\, P(n)\big)$? False

$Q(n)$ could be true on evens and $P(n)$ could be true on odds.
The left hand side is true, and the right is false.

# Lecture 2 (Proofs): Summary

By Example:
To Prove: $(\exists x)P(x)$. Give such an $x$ and show $P(x)$.

Direct Proof:
To Prove: $P \implies Q$. Assume $P$. reason forward, Prove $Q$.

By Contraposition:
To Prove: $P \implies Q$ Assume $\neg Q$. Prove $\neg P$.

By Contradiction:
To Prove: $P$ Assume $\neg P$. Prove False.

By Cases: informal.
Universal: show that statement holds in all cases.
Existence: used cases where one is true.
Either $\sqrt{2}$ and $\sqrt{2}$ worked.
or $\sqrt{2}$ and $\sqrt{2}^{\sqrt{2}}$ worked.

Careful when proving!
Don't assume the theorem. Divide by zero. Watch converse. ...

# Concept Check: Proofs

Which type of proof does each describe?

(A) Prove $P \implies Q$ using the equivalent $\neg Q \implies \neg P$? Contraposition
*Example:* "$n^2$ is odd $\implies$ $n$ is odd" $\equiv$ "$n$ is even $\implies$ $n^2$ is even"

(B) Prove $P \implies Q$ by assuming $P$ and proving $Q$? Direct Proof
*Example:* $a|b$ and $a|c \implies a|(b-c)$

(C) Prove $P$ by showing $\neg P \implies R \wedge \neg R$? Contradiction
*Example:* $\sqrt{2}$ is irrational – assume it is rational, reach a contradiction.

# Lecture 3 (Induction): Summary

Basic principle of induction – proving $\forall n \in \mathbb{N}$ by simple induction

- Prove $P(0)$ directly (base case)
- Prove that $P(k) \implies P(k+1)$ for all $k \geq 0$ (inductive step)

What if it doesn't work? (almost but not quite)

- Do we need to change the base case?
- Would a stronger theorem (so a stronger induction hypothesis) work?
- Would it help to "reach back" farther than just the previous step (just $P(k)$ isn't sufficient to prove $P(k+1)$)?
  - Strong induction lets you use all $P(0)$ through $P(k)$
  - Make sure "reaching back farther than the previous step" doesn't skip over the base case

# Concept Check: Induction

What are the three fundamental parts of an induction proof?

Base case

Induction hypothesis

Induction step

# Lecture 4 (Stable Matching): Summary

Analysis of cool algorithm with interesting goal: stability.

Stability seems like a good idea – is it possible?

- Two-set instance: Yes
- One-set instance: No

Can we *find* a stable matching?

- Yes! Propose and Reject algorithm
- Basic idea: Over time things get better for candidates, worse for jobs
- Eventually reaches a balance

... and we can (and did) prove it always finds a stable matching

Beyond stability – several stable solutions – which is better?
$\Rightarrow$ For jobs? For candidates?

# Concept Check: Stable Matching

What kind of matching does the propose and reject algorithm produce?

Job optimal

What if candidates propose to jobs?

Candidate optimal

True or False: All matchings are job optimal or candidate optimal.

False

# Lecture 5 (Graphs 1): Summary

Graphs:
- Definitions, basic properties (degree, path, cycle, tour, ...)
- Degree-sum formula (sum of degrees is $2|E|$)
- Connected: Path between every pair of nodes
- Connected Component: Maximal set of connected vertices

Euler tour and condition for existence (even degree vertices)
- Necessary: Existence of tour $\implies$ connected, even degree
- Sufficient: Recursive algorithm for finding an Eulerian tour

Trees:
- Definitions – *four* of them – all equivalent
- Equivalence of definitions
  - $\Rightarrow$ Two proved - others “left as an exercise for the reader”

# Concept Check: Basic Graphs

Are the following statements true or false?

(A) Removing a degree 1 vertex does change connectivity of graph. True
No path goes through a degree 1 vertex.

(B) A graph with two odd-degree vertices has an Eulerian tour. False
All vertices must have even degree to have an Eulerian tour.

(C) Adding an edge anywhere in a tree creates a cycle. True
This is in fact one of the four equivalent definitions of a tree.

# Lecture 6 (Graphs 2): Summary

Planar graphs and planar embeddings
- Euler's formula: $v + f = e + 2$.
  - Proof: removing an edge from a cycle removes a face (and keeps connected)
- Euler's formula consequence: $e \leq 3v - 6$
  - Use to show that $K_5$ is not planar
  - Modify slightly to show that $K_{3,3}$ is not planar

Coloring Planar Graphs
- Can color with 6 colors! Easy proof – just needs existence of deg $\leq 5$ vertex
- Can color with 5 colors! Argue about intersection of paths in the plane
- Can color with 4 colors! Proof.. well, it's possible

Graph connectivity
- Trees: few edges, but fragile (easily disconnected)
- Complete: very robust, but many, many edges
- Hypercube: very connected with modest edges
  - Beautiful structure – bits, bits, bits!

# Concept Check: Graphs 2

Does $v + f = e + 2$ apply to all planar graphs? No

It only applies to *connected* planar graphs.

Does adding an edge to a connected planar graph increase number of faces?

Yes

From Euler's formula: $v$ doesn't change, so $e$ increasing means $f$ must too

# Lecture 7 (Modular Arithmetic): Summary

Modular Arithmetic: $x \equiv y \pmod{N}$
- if $x - y = kN$ for some integer $k$
- .. or (equiv) if $x = y + kN$ for some integer $k$

For $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$:
- $ac \equiv bd \pmod{N}$ and $(a+c) \equiv (b+d) \pmod{N}$.

Division?
- Multiply by multiplicative inverse
- $a \pmod{N}$ has multiplicative inverse iff $\gcd(a, N) = 1$

Euclid's Algorithm:
- Based on fact that $gcd(x, y) = gcd(y, x \bmod y)$
- Very fast!
- Algorithm invented around 300 B.C. is still in use today! Cool.

# Concept Check: Modular Arithmetic

True or False: $\gcd(x, y) = \gcd(x, \lfloor \frac{y}{x} \rfloor)$? False

Use remainder instead of quotient: $\gcd(x, y) = \gcd(x, y \bmod x)$

For how many $a \in \{0, \ldots, 60\}$ does $ax \equiv 5 \pmod{61}$ have a unique solution?

60 – all but $a = 0$, where there is no solution

# Lecture 8 (Euclid, FLT, CRT): Summary

Extended Euclid: Find $a, b$ where $ax + by = gcd(x, y)$

Idea: compute $a, b$ recursively (euclid), or iteratively

Inverse: $ax + by \equiv ax \equiv gcd(x, y) \pmod{y}$

If $gcd(x, y) = 1$, we have $ax \equiv 1 \pmod{y}$

$\longrightarrow a \equiv x^{-1} \pmod{y}$

Fundamental Theorem of Arithmetic: Unique prime factorization of any $n$

Claim: if $p|n$ and $n = xy$, $p|x$ of $p|x$.

Proof relies on Extended Euclid GCD Theorem

Fundamental Theorem follows using induction + contradiction. Chinese

Remainder Theorem:

If $gcd(n, m) = 1$ then $x = a \pmod{n}$, $x = b \pmod{m}$ unique sol.

Proof: Find $u = 1 \pmod{n}$, $u = 0 \pmod{m}$,

and $v = 0 \pmod{n}$, $v = 1 \pmod{m}$.

Then: $x = au + bv = a \pmod{n}$

Fermat: For prime $p$, $a^{p-1} \equiv 1 \pmod{p}$

Proof Idea: $f(x) = a \cdot x \pmod{p}$ is bijection on $S = \{1, \ldots, p-1\}$.

Multiply domain elts and range elts – cancel and left with just $a^{p-1}$ in range

# Concept Check: FLT and CRT

What is $43^{61} \bmod 61$? 43

Using FLT, $a^{p-1} \equiv 1 \pmod{p}$, we have $43^{60} \cdot 43 \equiv 1 \cdot 43 \equiv 43 \pmod{43}$.

Is there a unique $x \in \{0, 1, \ldots, 76\}$ with $x \equiv 6 \pmod{7}$ and $x \equiv 6 \pmod{11}$?

Yes – this is the main point of the Chinese Remainder Theorem

What is $x$ in the previous question? 6

# Lecture 9 (RSA): Summary

Public-Key Cryptography
- Basic idea: Asymmetric power of parties and keys (public vs private)
- Used for confidentiality (encryption) and integrity (signatures)

Cool and historically important public-key scheme: RSA
- Works due to all the things we have been discussing!
  - *Modular arithmetic, Fermat's Little Theorem, Chinese Remainder Theorem, ...*
- Efficiency: Repeated squaring, small $e$, CRT for decryption

Some warnings/caveats:
- Understanding this math doesn't make you a cryptography expert
  - *Many real-world problems – modifications made*
  - *Always use a robust, well-tested cryptographic library*
- Modern threats to RSA (and related algorithms)
  - *Quantum computing*

# Concept Check: RSA

(A) Can 61 be a modulus used for RSA? No
61 is prime, and the RSA modulus must be the product of two primes

(B) In RSA, can 45 be the encryption exponent $e$ with modulus 77? No
The exponent must be relatively prime to $(p-1)(q-1)$ which is 60, and $\gcd(45,60) = 15$.

# Lecture 10 (Polynomials & Secret Sharing): Summary

Two points make a unique line
- Existence: Compute solution: $m, b$.
- Unique: Assume two solutions, show they are the same.

$d+1$ points make a unique degree $d$ polynomial.
- Existence: Lagrange interpolation
- Unique: Assume two solutions, show they are the same.

If you're careful about limiting degree $d$ or making $p$ large enough...
- Proofs work for polynomials over $GF(p)$ just like over $\mathbb{R}$
- And over $GF(p)$: values from a finite set – all likely

Secret Sharing:
- $k$ points on degree $k-1$ polynomial is all we need!
- Can hand out $n$ points on polynomial as shares.

# Concept Check: Polynomials and Secret Sharing

Which of the following is a good modulus for a secret sharing polynomial?

40, 53, 63, 99

53 – the modulus must be prime

If $P(x)$ has degree 10 and $Q(x)$ has degree 8, what is the maximum number of $x$ values where $P(x) = Q(x)$?

10 – $P(x) - Q(x)$ has degree 10, which has at most 10 roots

In the standard secret sharing scheme, the secret is $P(x)$ for what $x$?

$x = 0$

# Lecture 11 (Error Correcting Codes): Summary

Erasure codes: Communicate $n$ packets with $k$ erasures.

- How many packets to send? $n+k$
- How to encode? With polynomial $P(x)$.
  - ... of degree? $n-1$
- Recover? Reconstruct $P(x)$ with any $n$ points!

Error Correcting Codes (ECC): Communicate $n$ packets with $k$ errors.

- How many packets to send? $n+2k$
- How to encode? With polynomial $P(x)$.
  - ... of degree? $n-1$
- Recover?
  - Reconstruct error polynomial, $E(x)$, and $P(x)$! Nonlinear equations.
  - Reconstruct $E(x)$ and $Q(x) = E(x)P(x)$. Linear Equations.
- Polynomial division! $P(x) = Q(x)/E(x)$!

Reed-Solomon codes. Welsh-Berlekamp Decoding. Optimality. Perfection!

# Lecture 12 (Counting 1): Summary

**First rule:** $n_1 \times n_2 \times \cdots \times n_k$

$k$ Samples with replacement from $n$ items: $n^k$.

Sample without replacement: $\frac{n!}{(n-k)!}$

**Second rule: when order doesn't matter divide .. when possible**

Sample without replacement, no order: $\binom{n}{k} = \frac{n!}{(n-k)!k!}$. "$n$ choose $k$"

**One-to-one rule: equal in number if one-to-one correspondence**

Sample with replacement and order doesn't matter: $\binom{k+n-1}{n-1}$

Distribute $k$ samples (stars) over $n$ poss. ($n-1$ bars group poss..)

Distribute $k$ dollars to $n$ people.

# Midterm

That's "all"

Study - but get sleep

Don't get overly stressed

**YOU CAN DO THIS!**