Today.

Wrapup of Polynomials.

..and modular arithmetic.

Coutability and Uncountability.

Reed-Solomon code.

Problem: Communicate n packets $m_1,\ldots,m_n$
on noisy channel that corrupts $\le k$ packets.

Reed-Solomon Code:

1. Make a polynomial, $P(x)$ of degree $n-1$,
   that encodes message: coefficients, $p_0,\ldots,p_{n-1}$.

2. Send $P(1),\ldots,P(n+2k)$.

After noisy channel: Recieve values $R(1),\ldots,R(n+2k)$.

Properties:
(1) $P(i) = R(i)$ for at least $n+k$ points i,
(2) $P(x)$ is unique degree $n-1$ polynomial
that contains $\ge n+k$ received points.

Matrix view of encoding: modulo p.

$$\begin{bmatrix} P(1) \\ P(2) \\ P(3) \\ \vdots \\ P(n+2k) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1^2 & \cdot & 1 \\ 1 & 2 & 2^2 & \cdot & 2^{n-1} \\ 1 & 3 & 3^2 & \cdot & 3^{n-1} \\ \vdots & . & \vdots & \vdots & \\ 1 & (n+2k) & (n+2k)^2\cdot & (n+2k)^{n-1} & \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-1} \end{bmatrix} \pmod p$$

Berlekamp-Welsh Algorithm

$P(x)$: degree $n-1$ polynomial.
Send $P(1),\ldots,P(n+2k)$
Receive $R(1),\ldots,R(n+2k)$
At most k i's where $P(i) \neq R(i)$.

Idea:
$E(x)$ is error locator polynomial.
Root at each error point. Degree k.
$Q(x) = P(x)E(x)$ or degree $n+k-1$ polynomial.

Set up system corresponding to $Q(i) = R(i)E(i)$ where
$Q(x)$ is degree $n+k-1$ polynomial. Coefficients: $a_0,\ldots,a_{n+k-1}$
$E(x)$ is degree k polyonimal. Coefficients: $b_0,\ldots,b_{k-1},1$

Matrix equations: modulo p!

$$\begin{bmatrix} 1 & 1 & \cdot & 1 \\ 1 & 2 & \cdot & 2^{n+k-1} \\ 1 & 3 & \cdot & 3^{n+k-1} \\ \vdots & & \vdots & \vdots \\ \vdots & \cdot & \vdots & \vdots \\ 1 & (n+2k) & \cdot & (n+2k)^{n+k-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n+k-1} \end{bmatrix} = \begin{bmatrix} R(1) & \cdot & 0 \\ 0 & \cdot & 0 \\ \vdots & \vdots & \\ \vdots & \vdots & 0 \\ 0 & \cdot & R(n+2k) \end{bmatrix} \begin{bmatrix} 1 & \cdot & 1 \\ 1 & \cdot & 2^k \\ 1 & \cdot & 3^k \\ \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots \\ 1 & \cdot & (n+2k)^k \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ \vdots \\ b_{k-1} \\ 1 \end{bmatrix}$$

Solve. Then output $P(x) = Q(x)/E(x)$.

Berlekamp-Welsh algorithm decodes correctly when k errors!

Summary: polynomials.

Set of $d+1$ points determines degree d polynomial.

Encode secret using degree $k-1$ polynomial:
Can share with n people. Any k can recover!

Encode message using degree $n-1$ polynomail:
n packets of information.

Send $n+k$ packets (point values).
Can recover from k losses: Still have n points!

Send $n+2k$ packets (point values).
Can recover from k corruptionss.
Only one polynomial contains $n+k$
Efficiency.
Magic!!!!
Error Locator Polynomial.

Relations:
Linear code.
Almost any coding matrix works.
Vandermonde matrix (the one for Reed-Solomon)..
allows for efficiency. Magic of polynomials.
Other Algebraic-Geometric codes.

Wrapping up: RSA example with “easy” extended gcd.

Example: $p = 7$, $q = 11$.

$N = 77$.
$(p-1)(q-1) = 60$
Choose $e = 7$, since $\gcd(7,60) = 1$.
egcd(7,60).

$$
\begin{aligned}
7(0)+60(1) &= 60\\
7(1)+60(0) &= 7\\
7(-8)+60(1) &= 4\\
7(9)+60(-1) &= 3\\
7(-17)+60(2) &= 1
\end{aligned}
$$

Confirm: $-119+120 = 1$

$d = e^{-1} = -17 = 43 = \pmod{60}$

Farewell (for now) to modular arithmetic...

Modular arithmetic modulo a prime.

Add, subtract, commutative, associative, inverses!
Allow for solving linear systems, discussing polynomials...

Why not modular arithmetic all the time?

$4 > 3$? Yes!

$4 > 3 \pmod 7$? Yes...maybe?

$-3 > 3 \pmod 7$? Uh oh.. $-3 = 4 \pmod 7$.

Another problem.

4 is close to 3.
But can you get closer? Sure. 3.5. Closer. Sure? 3.25, 3.1, 3.000001. $\ldots$

For reals numbers we have the notion of limit, continuity, and derivative.......

....and Calculus.

For modular arithmetic...no Calculus. Sad face!

Next up: how big is infinity.

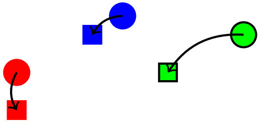
- Countable
- Countably infinite.
- Enumeration

How big are the reals or the integers?

Infinite!

Is one bigger or smaller?

Same size?



Same number?
Make a function f : Circles $\to$ Squares.
f(red circle) $=$ red square
f(blue circle) $=$ blue square
f(circle with black border) $=$ square with black border
One to one. Each circle mapped to different square.
One to One: For all $x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.
Onto. Each square mapped to from some circle .
Onto: For all $s \in R$, $\exists c \in D, s = f(c)$.

Isomorphism principle: If there is $f : D \to R$ that is one to one and onto, then, $|D| = |R|$.

Isomorphism principle.

Given a function, $f : D \to R$.
One to One:
For all $\forall x, y \in D$, $x \neq y \implies f(x) \neq f(y)$.
or
$\forall x, y \in D$, $f(x) = f(y) \implies x = y$.

Onto: For all $y \in R$, $\exists x \in D, y = f(x)$.

$f(\cdot)$ is a **bijection** if it is one to one and onto.

Isomorphism principle:
If there is a bijection $f : D \to R$ then $|D| = |R|$.

Countable.

How to count?

0, 1, 2, 3, ...

The Counting numbers.
The natural numbers! N

Definition: S is **countable** if there is a bijection between S and some subset of N.

If the subset of N is finite, S has finite **cardinality**.

If the subset of N is infinite, S is **countably infinite**.

Where's 0?

Which is bigger?
The positive integers, $\mathbb{Z}^+$, or the natural numbers, $\mathbb{N}$.

Natural numbers. $0, 1, 2, 3, \ldots$.

Positive integers. $1, 2, 3, \ldots$.

Where's 0?

More natural numbers!

Consider $f(z) = z - 1$.

For any two $z_1 \neq z_2 \implies z_1 - 1 \neq z_2 - 1 \implies f(z_1) \neq f(z_2)$.
One to one!

For any natural number n, for $z = n + 1$, $f(z) = (n+1) - 1 = n$.
Onto for $\mathbb{N}$

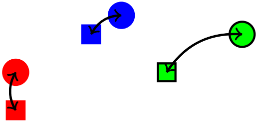
Bijection! $\implies |\mathbb{Z}^+| = |\mathbb{N}|$.

But.. but Where's zero? "Comes from 1."

A bijection is a bijection.

Notice that there is a bijection between N and Z^+ as well.
$f(n) = n+1$. $0 \to 1, 1 \to 2, \ldots$

Bijection from A to B $\implies$ a bijection from B to A.



Inverse function!

Can prove equivalence either way.
Bijection to or from natural numbers implies countably infinite.

More large sets.

E - Even natural numbers?

$f : N \to E$.

$f(n) \to 2n$.

Onto: $\forall e \in E$, $f(e/2) = e$. $e/2$ is natural since e is even
One-to-one: $\forall x, y \in N, x \neq y \implies 2x \neq 2y. \equiv f(x) \neq f(y)$

Evens are countably infinite.
Evens are same size as all natural numbers.

All integers?

What about Integers, Z?
Define $f : N \rightarrow Z$.

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ even} \\ -(n+1)/2 & \text{if n odd.} \end{cases}$$

One-to-one: For $x \neq y$
if x is even and y is odd,
then $f(x)$ is nonnegative and $f(y)$ is negative $\implies f(x) \neq f(y)$
if x is even and y is even,
then $x/2 \neq y/2 \implies f(x) \neq f(y)$
$\ldots.$

Onto: For any $z \in Z$,
if $z \geq 0$, $f(2z) = z$ and $2z \in N$.
if $z < 0$, $f(2|z| - 1) = z$ and $2|z| + 1 \in N$.

Integers and naturals have same size!

Listings..

$$f(n) = \begin{cases} n/2 & \text{if } n \text{ even} \\ -(n+1)/2 & \text{if n odd.} \end{cases}$$

Another View:

n	$f(n)$
0	0
1	-1
2	1
3	-2
4	2
$\dots$	$\dots$

Notice that: A listing “is” a bijection with a subset of natural numbers.
Function $\equiv$ “Position in list.”
If finite: bijection with $\{0, \dots, |S| - 1\}$
If infinite: bijection with N.

Enumerability $\equiv$ countability.

Enumerating (listing) a set implies that it is countable.

"Output element of S",
"Output next element of S"
$\ldots$
Any element x of S has *specific, finite* position in list.
$Z = \{0, 1, -1, 2, -2, \ldots..\}$
$Z = \{\{0, 1, 2, \ldots, \}$ and then $\{-1, -2, \ldots\}\}$

When do you get to -1? at infinity?

Need to be careful.

61A —- streams!

Countably infinite subsets.

Enumerating a set implies countable.
Corollary: Any subset T of a countable set S is countable.

Enumerate T as follows:
Get next element, x, of S,
output only if $x \in T$.

Implications:
Z^+ is countable.
It is infinite since the list goes on.
There is a bijection with the natural numbers.
So it is countably infinite.

All countably infinite sets have the same cardinality.

Enumeration example.

All binary strings.
$B = \{0,1\}^*$.

$B = \{\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, \ldots\}$.
ϕ is empty string.

For any string, it appears at some position in the list.
If n bits, it will appear before position 2^{n+1}.

Should be careful here.

$B = \{\phi; , 0, 00, 000, 0000, ...\}$
Never get to 1.

More fractions?

Enumerate the rational numbers in order...

$0, \ldots, 1/2, ..$

Where is $1/2$ in list?

After $1/3$, which is after $1/4$, which is after $1/5$...

A thing about fractions:
any two fractions has another fraction between it.

Can't even get to "next" fraction!

Can't list in "order".

Pairs of natural numbers.

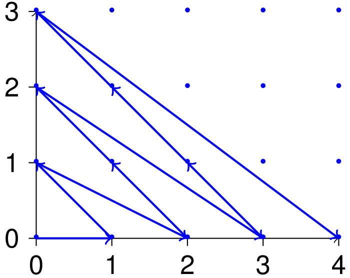
Consider pairs of natural numbers: $N \times N$
E.g.: $(1,2)$, $(100,30)$, etc.

For finite sets S_1 and S_2,
then $S_1 \times S_2$
has size $|S_1| \times |S_2|$.

So, $N \times N$ is countably infinite squared ???

Pairs of natural numbers.

Enumerate in list:
$(0,0),(1,0),(0,1),(2,0),(1,1),(0,2),\ldots\ldots$



The pair (a,b), is in first $(a+b+1)(a+b)/2$ elements of list!
(i.e., “triangle”).

Countably infinite.

Same size as the natural numbers!!

Rationals?

Positive rational number.
Lowest terms: a/b
$a, b \in N$
with $gcd(a, b) = 1$.

Infinite subset of $N \times N$.

Countably infinite!

All rational numbers?

Negative rationals are countable. (Same size as positive rationals.)

Put all rational numbers in a list.

First negative, then nonegative ??? No!

Repeatedly and alternatively take one from each list.
  Interleave Streams in 61A

The rationals are countably infinite.

Real numbers..

Real numbers are same size as integers?

The reals.

Are the set of reals countable?

Lets consider the reals $[0,1]$.

Each real has a decimal representation.
.500000000... $(1/2)$
.785398162... $\pi/4$
.367879441... $1/e$
.632120558... $1-1/e$
.345212312... Some real number

Diagonalization.

If countable, there a listing, L contains all reals. For example

0: .500000000...
1: .785398162...
2: .367879441...
3: .632120558...
4: .345212312...
$\vdots$

Construct “diagonal” number: $.77677\ldots$

Diagonal Number: Digit i is 7 if number i's ith digit is not 7
and 6 otherwise.

Diagonal number for a list differs from every number in list!
Diagonal number not in list.

Diagonal number is real.

Contradiction!

Subset $[0,1]$ is not countable!!

All reals?

Subset $[0,1]$ is not countable!!

What about all reals?
No.

Any subset of a countable set is countable.

If reals are countable then so is $[0,1]$.

Diagonalization.

1. Assume that a set S can be enumerated.
2. Consider an arbitrary list of all the elements of S.
3. Use the diagonal from the list to construct a new element t.
4. Show that t is different from all elements in the list
   $\Longrightarrow$ t is not in the list.
5. Show that t is in S.
6. Contradiction.

Another diagonalization.

The set of all subsets of N.

Example subsets of N: $\{0\}$, $\{0,\ldots,7\}$,
evens, odds, primes,

Assume is countable.

There is a listing, L, that contains all subsets of N.

Define a diagonal set, D:
If ith set in L does not contain i, $i \in D$.
otherwise $i \notin D$.

D is different from ith set in L for every i.
$\implies$ D is not in the listing.

D is a subset of N.

L does not contain all subsets of N.

Contradiction.

Theorem: The set of all subsets of N is not countable.
(The set of all subsets of S, is the **powerset** of N.)

Diagonalize Natural Number.

Natural numbers have a listing, L.

Make a diagonal number, D:
differ from ith element of L in ith digit.

Differs from all elements of listing.

D is a natural number... Not.

Any natural number has a finite number of digits.

"Construction" requires an infinite number of digits.

The Continuum hypothesis.

There is no set with cardinality between the naturals and the reals.

First of Hilbert's problems!

Cardinalities of uncountable sets?

Cardinality of $[0,1]$ smaller than all the reals?

$f : R^+ \rightarrow [0,1]$.

$$f(x) = \begin{cases} x + \frac{1}{2} & 0 \leq x \leq 1/2 \\ \frac{1}{4x} & x > 1/2 \end{cases}$$

One to one. $x \neq y$
If both in $[0,1/2]$, a shift $\implies f(x) \neq f(y)$.
If neither in $[0,1/2]$ a division $\implies f(x) \neq f(y)$.
If one is in $[0,1/2]$ and one isn't, different ranges $\implies f(x) \neq f(y)$.
Bijection!

$[0,1]$ is same cardinality as nonnegative reals!

Generalized Continuum hypothesis.

There is no infinite set whose cardinality is between the cardinality of an infinite set and its power set.

The powerset of a set is the set of all subsets.

Resolution of hypothesis?

Gödel. 1940.
Can't use math!
If math doesn't contain a contradiction.

This statement is a lie.

Is the statement above true?

The barber shaves every person who does not shave themselves.

Who shaves the barber?

Self reference.

More on...

...Tuesday..