Plan for the rest of the course

- Today: Questions about homework? Then one example of solving a congruence and then a quick tour of cardinality and infinite sets

- Tuesday: Review
  - I’ll try to post a review sheet for the final by sometime this weekend.

- May 7: Final exam, on Gradescope like the last exam (24-hour window to take the exam)
  - Office hours and review sessions: Let me know what times work for you.
\[ \gcd(a, b) = ax + by \quad \text{w/os using Euclidean Alg.} \]

Let \( X = \{ ax + by : a, b \in \mathbb{Z} \} \neq \emptyset \quad a, 1 + b, 0 \leq X \)

By well-ordering, \( X \) has a least element, say \( d \leq \gcd(a, b) \)

1. \( d \) is a common divisor of \( a, b \):

   \[ a = qd + r \quad 0 \leq r < d \]

   \[ a - qd = r = a - q(ax + by) = a(1 - qx_0) - qy_0 \]

   If \( r > 0 \), this says \( r \in X \) but \( r < d \) and \( d \) is the smallest thing in \( X \). Then \( r = 0 \) and \( a = qd \) so \( a/d \). Same sort of argument shows \( d/b \).

2. \( d \) is bigger than any other common divisor: Let \( c/d \) and \( c/b \)

   \[ a = q_1 c + r_1 \quad 0 \leq r_1 < c \]

   \[ a = q_2 b + r_2 \quad 0 \leq r_2 < b \]

   Then \( d = ax_0 + by_0 = c(q_1 x_0 + q_2 y_0) = c(jx_0 + ky_0) \). So \( c/d \). But \( d > 0 \)

   so \( c \leq d \).
$3x^2 - y^2 = -2$ (Diophantine)

\[
\begin{align*}
\text{a) if there is a solution, then that solution must solve } & 3x^2 - y^2 \equiv -2 \pmod{3} \\
\text{A solution is a pair of integers } (x_0, y_0) \text{ such that } & \\
& 3x_0^2 - y_0^2 = -2 \\
& (3x_0^2 - y_0^2) - (-2) = 0 \quad 0 \text{ is divisible by } 3 \\
& \text{so } 3x_0^2 - y_0^2 \equiv -2 \pmod{3}
\end{align*}
\]
An Application

From last time: Suppose we want to solve the equation \([a]x = [c]\) in \(\mathbb{Z}_n\).
So we want an integer \(x\) such that \(ax \equiv b \pmod{n}\), or
\[
ax - nk = c,
\]
for some integer \(k\).

This is a Diophantine equation of the type we’ve been discussing; it has solutions if and only if \(\gcd(a, n) \mid c\), and, if that holds, we can find a/all solutions easily.

Example: Solve the equation \([3]x = [4]\) in \(\mathbb{Z}_{20}\)

\[
3x - 20k = 4
\]

\[
x = 28
\]
\[
[x] = [8] = [28] \text{ in } \mathbb{Z}_{20}
\]
\[
[3][8] = [4] \text{ in } \mathbb{Z}_{20}
\]

Write \(\gcd(3, 20)\) as a lin. comb. of 3, 20

\[
7 \cdot 3 + (-1)20 = 1
\]
\[
4(7 \cdot 3) + (-1)20 = 4
\]
\[
(28)3 - 4 \cdot 20 = 4
\]
$[5][x] = [4]$ in $\mathbb{Z}_{20}$

$5x - 20k = 4$

no solution

no $[x]$ so $[5][x] = [4]$ in $\mathbb{Z}_{20}$

$\gcd(5, 20) = 5 \nmid 4$

$[5][x] = [4]$ in $\mathbb{Z}_{29}$

$\gcd(5, 29) = 1$
Cardinality

“Counting” a set \( X \) (for finite \( X \), at least) means placing \( X \) in one-to-one correspondence (bijection) with some subset of \( \mathbb{N} \) of the form \( \{1, 2, \ldots, n\} \). (The book calls this set \( \mathbb{N}_n \), other books call it \( \mathbb{N}_0 \) or \( n \), etc.)

It turns out that it actually takes a fair amount of work to prove that, given \( X \), you can only do that for one value of \( n \).

**Definition**

Two sets \( A \) and \( B \) are said to be **bijectively equivalent** if and only if there exists a bijective function \( f : A \rightarrow B \). We write \( A \approx B \) to denote that the two sets are bijectively equivalent.

This is reflexive, symmetric, and transitive (why?), but we want it to apply to the collection of all sets (which isn’t a set, due to Russell’s Paradox), so we don’t say it’s an equivalence relation.
### Finite sets

**Definition**

We say a set $X$ is **finite** if and only if $X = \emptyset$ or there is an $n \in \mathbb{N}$ such that $X \approx \mathbb{N}_n$. A set that is not finite is **infinite**.

**Theorem**

*If there is an injective function $f : \mathbb{N}_m \rightarrow \mathbb{N}_n$ then $m \leq n$.***

We prove this using induction on $n$. For the induction step, we assume we have an injection $f : \mathbb{N}_m \rightarrow \mathbb{N}_{k+1}$. We have to consider 2 cases, depending on whether $k+1$ is in the image of $f$; if it is, we have to cook up a new function from $\mathbb{N}_{m-1}$ to $\mathbb{N}_k$ from $f$ so that we can apply induction. Using this theorem, we can prove that if $X \approx \mathbb{N}_m$ and $X \approx \mathbb{N}_n$, then $m = n$.

**Definition**

If $X$ is a finite set, the **cardinality** of $X$, $|X|$, is 0 if $X$ is empty and the unique $n$ such that $X \approx \mathbb{N}_n$ otherwise.
Subsets

We can then prove that

**Theorem**

Let $B$ be a finite set and suppose $A \subseteq B$. Then $|A| \leq |B|$ and $|A| = |B|$ if and only if $A = B$.

and things like

**Theorem**

Suppose $A_1, A_2$ are finite sets and $A_1 \cap A_2 = \emptyset$. Then

$$|A_1 \cup A_2| = |A_1| + |A_2|.$$
Infinite sets

An infinite set can’t be bijectively equivalent to a proper subset of itself, but an infinite set can! $f(x) = \mathbb{R}^x$

Example: Consider $f: \mathbb{R} \to \mathbb{R}_{>0}$. We can use calculus to show this is a bijection. But the codomain is a proper subset of the domain.

**Definition**

A set $X$ is **countably infinite** if $X \approx \mathbb{N}$. It is **countable** if it is finite or countably infinite. A set that is not countable is **uncountable**.

Some authors use the term **denumerable** instead of countably infinite.

Some more examples:

1. $\mathbb{N} \approx \{2n \mid n \in \mathbb{N}\}$
2. $\mathbb{N} \approx \{2n - 1 \mid n \in \mathbb{N}\}$
3. $\mathbb{N} \approx \mathbb{Z}$.
Another example

**Theorem**

*The set \( \mathbb{N} \times \mathbb{N} \) is countable.*

**Proof.**

Define \( f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \) by \( f(m, n) = 2^{m-1}(2n - 1) \). To see this is surjective, recall that every natural number can be written as a product of primes, and so can be factored as a power of 2 (possibly the 0th power) times an odd number. Since \( m - 1 \) runs over the set of nonnegative integers as \( m \) runs over \( \mathbb{N} \) and \( 2n - 1 \) runs over all the odd natural numbers as \( n \) runs over \( \mathbb{N} \), we see that \( f \) is surjective. The factorization into primes is, moreover, unique (up to the order of the factors), which implies that \( f \) is injective. Thus, \( f \) is a bijection.

This implies that \( \mathbb{Z} \times \mathbb{Z} \) is countable.
There are several ways to prove \( \mathbb{Q} \) is countable from the fact that \( \mathbb{Z} \times \mathbb{Z} \) is countable, but it takes some work. I give one proof in the notes on cardinality that I’ll post on the course web site.

Cantor proved that \( \mathbb{R} \) is uncountable by showing that \([0,1]\) is uncountable. The standard way to do this uses a technique that’s now called a diagonalization argument. It goes something like this:
Every real number in \([0,1]\) has a decimal representation \(0.a_1a_2a_3\ldots\) with \(0 \leq a_i \leq 9\). To make the representation unique, we drop ones that end with infinitely many 0s and use the ones that end with infinitely many 9s.

\[
.2006\ldots = .1999\ldots
\]

agree to just use the ones that end with infinitely many 9s.
Cantor's diagonalization argument

If \([0,1]\) is countable, there's a bijection \(f: \mathbb{N} \rightarrow [0,1]\) and we can give all the decimal representations in an infinite list:

\[
\begin{align*}
f(1) &= 0.a_1,1a_1,2a_1,3a_1,4\ldots \\
f(2) &= 0.a_2,1a_2,2a_2,3a_2,4\ldots \\
f(3) &= 0.a_3,1a_3,2a_3,3a_3,4\ldots \\
f(4) &= 0.a_4,1a_4,2a_4,3a_4,4\ldots \\
\vdots
\end{align*}
\]

But let

\[
x_i = \begin{cases} 
1 & \text{if } a_{i,i} \neq 1, \text{ and} \\
2 & \text{if } a_{i,i} = 1.
\end{cases}
\]

The \(x = 0.x_1x_2\ldots\) isn't on the list!

Consider \(x = 0.x_1x_2x_3\ldots\) where

This makes sure that \(x\) differs from \(f(i)\) at least in the \(i\)th decimal place

\(x \neq f(i)\) so \(x \notin \text{Im}(f)\)

So \(x \notin [0,1]\)
Another theorem of Cantor

Theorem (Cantor, 1891)

For any set $X$, $X \not\approx \mathcal{P}(X)$.

So we have infinitely many “sizes” of infinite sets:

- $|\mathbb{N}| = \aleph_0$
- $|\mathcal{P}(\mathbb{N})| = 1\mathbb{R} \leq \mathcal{C}$
- $|\mathcal{P}(\mathcal{P}(\mathbb{N}))|$
- \ldots

(It turns out that $\mathcal{P}(\mathbb{N}) \approx \mathbb{R}$.)

For details and more results, you can read Chapter 9 and the notes on cardinality on the course web page. But this stuff won’t be on the final.
Example (Illustration) due to George Gamow

Alpher, Bethe, Gamow

Hilbert Hotel

Hotel with countably infinite number of rooms, numbered by \( \mathbb{N} = 1, 2, 3, \ldots \)

Hotel is full, new guest arrives: move person in room \( n \) to room \( n+1 \) (for all \( n \)). Now room 1 is free.

\[ \underline{k \text{ guests arrive: move person in room } n \text{ to room } n+k} \]

\[ \underline{\text{Countably infinitely many guests arrive. Move person in room } n \text{ to room } 2n. \text{ All odd-numbered rooms are free.}} \]