MAT 319 & 320 Fall 2021, Lecture 2, Thursday, Aug 26, 2021

1. Questions from last time?
2. **Lemma:** $1 + 2 + 4 + \cdots + 2^n < 2^{n+1}$ for $n = 1, 2, 3 \ldots.$
Proof: Base case $n = 1$, $1 + 2 = 3 < 4$.
Assume true for n, prove for $n + 1$:

$$(1 + \cdots + 2^n) + 2^{n+1} < 2^{n+1} + 2^{n+1} = 2 \cdot 2^{n+1} = 2^{n+2}.$$

3. Which color of paper there more of? Counting by bijections.
4. Definitions:
(a) empty set has zero elements
(b) A set S has n elements if there is a bijection from S to $\mathbb{N}_n$.
(c) A set is finite it is has n elements for some $n \in \mathbb{N}$.
(d) A set is infinite if it not finite.
5. **Theorem B.1:** Let $m, n \in \mathbb{N}$ with $m > n$. Then there does not exist a bijection h from $\mathbb{N}_n$ to $\mathbb{N}_m$.
Sketch: Induct on n, easy for $n = 1$, since h is constant. Assume $1 < n < m$. Let $h : \mathbb{N}_m \to \mathbb{N}_m$. If $n \notin h(\mathbb{N}_m)$, then h maps into $\mathbb{N}_{n-1}$ so is not a bijection by induction. Otherwise, there is a p than maps to n. Define $h_1(q) = h(q)$ for $q < p$ and $h_1(q) = h(q + 1)$ for $q > p$. This is a map $\mathbb{N}_{m-1}$ into $\mathbb{N}_{n-1}$ so is not a bijection by induction. Hence h was not a bijection.
6. **Theorem 1.3.2:** For a finite set S, the number of elements in S is a unique element of $\mathbb{N}$.
Proof: If S has bijections to both $\mathbb{N}_m$ and $\mathbb{N}_m$, then there is a bijection between $\mathbb{N}_m$ and $\mathbb{N}_m$. Hence $n < m$ and $m < n$ are both impossible by Thm B.1, so $m = n$.
7. **Theorem B.2:** If $n \in \mathbb{N}$ there is not a bijection from $\mathbb{N}$ to $\mathbb{N}_n$.
Proof: If there were such a map then restriction gives an injection from $\mathbb{N}_{n+1}$ into $\mathbb{N}_n$, a contradiction.
8. **Theorem 1.3.3:** $\mathbb{N}$ is an infinite set.
Proof: If $\mathbb{N}$ were finite there would be a bijection from $\mathbb{N}$ to $\mathbb{N}_n$. This contradicts Theorem B.2, so $\mathbb{N}$ is not finite.
9. This is an example of an "impossibility proof". Showing something can't happen.
10. **Defn:** denumerable = has bijection with $\mathbb{N}$. Aka "countably infinite".
countable = finite or denumerable.
11. **Theorem 1.3.8:** $\mathbb{N} \times \mathbb{N}$ is denumerable.
Sketch diagonal argument for constructing bijections. Details are checked in Appendix B of text.
We will give a different proof after giving some more results.
12. **Theorem B.3:** If $A \subset \mathbb{N}$ is infinite, then there is an increasing bijection from $\mathbb{N}$ to A.
Proof: We will define $\varphi : \mathbb{N} \to A$.

Since A is not empty, by the well ordering principle, it has a smallest element, that we call $\varphi(1)$. Note that $\varphi(1) \geq 1$.

Since A is infinite, $A_1 = A \setminus \{\varphi(1)\}$ is not empty, so it has a smallest element called $\varphi(2)$. Note that $\varphi(1) < \varphi(2)$, since $\varphi(1)$ was smallest element of A. Hence $\varphi(2) \geq 2$.

In general, suppose $\varphi(1) < \varphi(2) < \cdots < \varphi(k)$ have been defined. Since A is infinite, removing these from A leaves a non-empty set A_k, that has a smallest element, that we set to be $\varphi(k+1)$. Also $\varphi(k+1) > \varphi(k) \geq k$, so $\varphi(k+1) \geq k+1$.

By induction φ is defined on all of $\mathbb{N}$i and satisfies $\varphi(n) \geq n$ for all n.

To see φ is 1-1, suppose $n \neq m$. We may assume $n < m$. Then $\varphi(n) < \varphi(n+1) < \cdots < \varphi(m)$, so $\varphi(n) \neq \varphi(m)$.

To prove φ is surjective, we use a proof by contradiction. Assume φ is not onto. Then there is an element $p \in A$ not in the image of φ. In particular,

$$p \in A_p = A \setminus \{\phi(1), \ldots, \phi(p)\}.$$

But $\varphi(p+1) \geq p+1 > p$ and it was defined to be the **smallest** element of A_p. This is a contradiction, so φ must be onto. $\square$

13. **Theorem B.4:** If $A \subset \mathbb{N}$, then A is countable.

Proof: For finite sets this is the definition. For infinite sets, the previous result give a bijection from $\mathbb{N}$ to A.

14. **Theorem 1.3.9:** Suppose $T \subset S$.

(a) if S is countable, so is T

(b) if T is uncountable, so is S.

Proof:

(a) If S is finite, Theorem 1.3.5(a) says T is finite. If S is infinite, there is a bijection $\psi : S \to \mathbb{N}$. Theorem B.3 gives a bijection φ between $A = \psi(T)$ and $\mathbb{N}$. Composing these maps gives a bijection between T and $\mathbb{N}$.

(b) is contrapositive of (a), so is equivalent (true iff (a) is true).

15. **Theorem 1.3.10:** The following are equivalent (TFAE):

(a) S is countable.

(b) there is a surjection from $\mathbb{N}$ onto S.

(c) there is an injection from S into $\mathbb{N}$.

Proof:

(a) $\to$ (b) If S is denumerable, there is a bijection between S and $\mathbb{N}$. This is also a surjection. If S is finite there is a bijection from $\mathbb{N}_n = \{1, \ldots, n\}$ to S and a surjection $\psi(k) = \min(k, n)$ from $\mathbb{N}$ to $\mathbb{N}_n$.

(b) $\to$ (c) Suppose $\psi : \mathbb{N} \to S$ is onto. Then for every $x \in S$, the set $\psi^{-1}(x) \subset \mathbb{N}$. Let $\varphi(x)$ be the smallest element of this set. This gives a map $S \to \mathbb{N}$ and it is 1-1 because $x \neq y$ implies the sets $\psi^{-1}(x)$ and $\psi^{-1}(y)$ are disjoint (ψ can't take different values at the same point).

16. **Corollary:** If S is countable and $f : S \to T$ is onto then T is countable.

16. **Theorem 1.3.12:** If A_n is a countable set for each n, then $\cup_{n=1}\infty A_n$ is countable.

Proof: Let $A_n = \{a_1^n, a_2^n, \ldots\}$. then $(n, m) \to a_m^n$ is surjective from $\mathbb{N} \times \mathbb{N}$ to $\cup A_n$.

17. **Theorem 1.3.8:** $\mathbb{N} \times \mathbb{N}$ is countable.
Proof:

First show $A = \{(n, m) : n < m\}$ is countable. Define a map $f(n, m) = 2^n + 2^m$ from A to $\mathbb{N}$. We claim this is injective. Suppose $(n, m) \neq (p, q)$. If $m = q$, then we must have $n \neq q$

$$f(n, m) = 2^n + 2^m = 2^n + 2^q \neq 2^p + 2^q = f(p, q).$$

If $m \neq q$ then we may assume $m < q$ or $m + 1 \leq q$. Then

$$f(n, m) = 2^n + 2^m < 2^{m+1} \leq 2^q < 2^p + 2^q = f(p, q).$$

In both cases, $f(n, m) \neq f(p, q)$, so f is an injection from $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

The set $B = \{(n, m) : n > m\}$ is also countable since it is bijective to A by $(n, m) \to (m, n)$. Finally, $\{(n, m) : n = m\}$ is bijective to $\mathbb{N}$ by $n \to (n, n)$. Thus $\mathbb{N} \times \mathbb{N}$ is a union of three countable sets, hence is countable. $\square$

If you known that every integer has a unique factorization into primes, you can make an easier proof using the map $f(n, m) = 2^n \cdot 3^m$.

For a proof of unique factorization, see

https://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic

18. **Theorem 1.3.11:** The set $\mathbb{Q}$ of rational numbers is countable.

Proof: $(n, m) \to n/m$ is surjective from $\mathbb{N} \times \mathbb{N}$ to positive rationals. Negative rationals are bijective positives by $r \to -r$. All rationals are union of two countable sets plus the finite set $\{0\}$.

19. There are uncountable sets. Later we will prove $\mathbb{R}$ is uncountable. The subsets of $\mathbb{N}$ is an uncountable collections.

20. Define power set to be set of all subsets (including empty set). Power set of a finite set with n elements has 2^n elements. So a set and its power sets have different numbers of elements. Sometimes denoted 2^S. What about infinite sets?

21. **Theorem 1.3.13 (Cantor's theorem)**: If A is a set then there is no surjection from A to $\mathcal{P}(A)$, the set of all subsets of A.

Proof: Suppose φ is such a surjection. We will obtain a contradiction.

Let $D = \{a \in A : a \notin \phi(a)\}$. D is a subset of A, so $D = \phi(b)$ for some $b \in A$. Either $b \in D$ or $b \notin D$. If $b \in D$ then by definition of D, we have $b \notin D = \phi(b)$, a contradiction. Thus $b \notin D = \phi(b)$. By definition of D, we get $b \in D$, another contradiction.

Therefore there is no b so that $D = \phi(b)$. Hence there is no surjection from A to its power set.

22. There are uncountably many subsets of $\mathbb{N}$.

They each subset corresponds to a sequence of zeros and ones. These can be associated to real numbers via binary expansions. Later we will use this idea to show $\mathbb{R}$ is uncountable.

23. We say two infinite sets have the same cardinality if there is a bijection between them. Cantor's theorem implies there are an infinite number of different possible

infinite cardinalities. Most of mathematics only needs the first few infinities to deal with $\mathbb{N}$, $\mathbb{R}$,... The study of all cardinalities is part of mathematical logic.

The cardinality of $\mathbb{R}$ is sometimes denoted c or "the continuum". More about this later.

Some extra material, if there is time.

23. Theorem: If S is infinite, then there is an injection $f : \mathbb{N} \to S$.

Since S is infinite, it is non-empty so there is some $s_1 \in S$. Let $f(1) = s_1$. Assume we have defined f for $1, \ldots, n$. Since S is infinite $S \setminus \{f(1), \ldots, f(n)\}$ is not empty so there is a point s_{n+1} in this set. Let $f(n+1) = s_{n+1}$. By induction, the set of n's where f is defined is all of $\mathbb{N}$. f is injective because of $n < m$, then $f(m)$ was chosen not to be $f(1), \ldots, f(m-1)$, so is not $f(n)$. $\square$

24. Theorem: A set S is infinite if and only if there is an injection from S to a proper subset of itself.

Proof sketch: If S is finite, there is no such injection by Theorem 1.3.2. If S is infinite, then let $f : \mathbb{N} \to S$ be the injection above. Define a map from S to itself as follows. If $x = f(n)$ for some $n \geq 1$, let $h(x) = f(n+1)$. Otherwise $h(x) = x$. This is injective, but $f(1)$ is not in the image, so the map is not onto. The range (co-domain) is a proper subset of S.

25. Schröder–Bernstein theorem: if there exist injective functions $f : A \to B$ and $g : B \to A$ between the sets A and B, then there exists a bijective function $h : A \to B$.

See https://en.wikipedia.org/wiki/Schr der-Bernstein_theorem