Lecture 10: Countable and uncountable sets. Principles of counting.

October 14, 2026

Last time we asked whether the evens, $\mathbb{Z}$, $\mathbb{N} \times \mathbb{N}$, and $\mathcal{P}(\mathbb{N})$ are countable. We settled the first two; today we settle the other two.

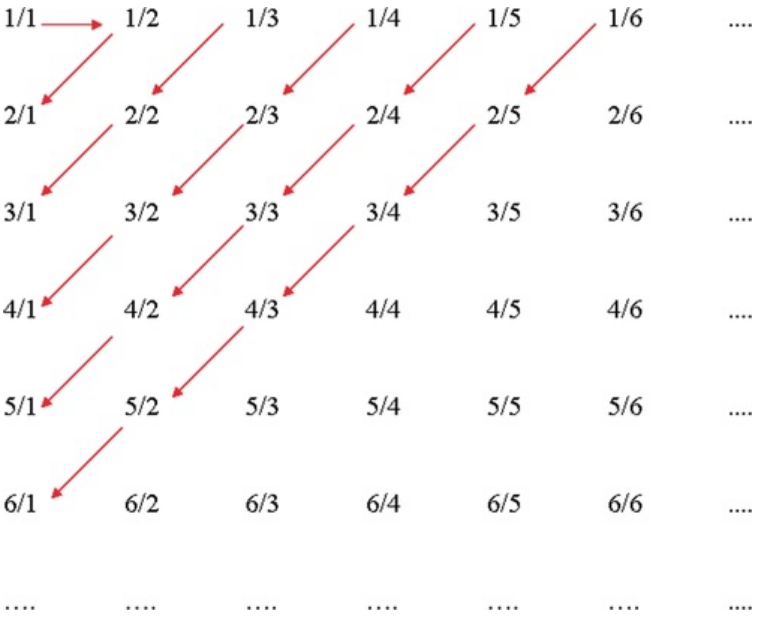
Definition 0.1. *Two sets A and B have the same* cardinality *if there is a bijection $A \to B$.*

This generalizes the notion of the "size" of a set to infinite-sized sets. A set is countably infinite if it has the same cardinality as $\mathbb{N}$.

Let $\{0,1\}^{\mathbb{N}}$ be the set of **infinite binary strings**, so that $0000000\ldots$ and $010101010\ldots$ are both elements of $\{0,1\}^{\mathbb{N}}$.

Theorem 0.2. *$\mathbb{N} \times \mathbb{N}$ is countable.*

Proof. We give a bijection $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, based on the idea of going in a "diagonal order":



Here the cell in row p and column q holds the pair (p, q), and we visit the cells in the order shown. We can write this down explicitly. The cells with $p + q = d + 1$ form the d-th anti-diagonal, for $d = 1, 2, 3, \ldots$; this anti-diagonal holds the d cells

$$(1, d), \quad (2, d-1), \quad \ldots, \quad (d, 1),$$

and the anti-diagonals before it contain $1+2+\cdots+(d-1)=\frac{(d-1)d}{2}$ cells in total. So given $n\in\mathbb{N}$, let d be the unique integer $d\geq 1$ with

$$\frac{(d-1)d}{2}<n\leq\frac{d(d+1)}{2},\qquad\text{and let}\qquad i=n-\frac{(d-1)d}{2},$$

so that the n-th cell is the i-th one along the d-th anti-diagonal. Define

$$f(n)=(i,\ d+1-i).$$

For instance $f(1)=(1,1)$, $f(2)=(1,2)$, $f(3)=(2,1)$, $f(4)=(1,3)$, $f(5)=(2,2)$, and so on.

Such a d exists and is unique because $\frac{(d-1)d}{2}$ is 0 at $d=1$ and strictly increases without bound, so every $n\in\mathbb{N}$ falls in exactly one of these blocks. Since $\frac{d(d+1)}{2}=\frac{(d-1)d}{2}+d$, each block contains d values of n, so $1\leq i\leq d$ and each n does name a cell on the d-th anti-diagonal. Conversely, the pair (p,q) lies on exactly one anti-diagonal, namely $d=p+q-1$, where it is the i-th cell for $i=p$. So $(p,q)=f(n)$ for exactly one n, namely

$$n=\frac{(p+q-2)(p+q-1)}{2}+p.$$

This is a two-sided inverse of f, so f is a bijection. □

Corollary 0.3. $\mathbb{Q}^+$ *is countable.*

Proof. The map $\mathbb{N}\times\mathbb{N}\to\mathbb{Q}^+$ via $(p,q)\mapsto p/q$ is a surjection, since every positive rational can be written as p/q for some $p,q\in\mathbb{N}$. Composing it with the bijection f above gives a surjection $\mathbb{N}\to\mathbb{Q}^+$, so $\mathbb{Q}^+$ is countable. □

Remark 0.4. This surjection is not injective: it hits each rational once for every way of writing it as a fraction, so 1/1 and 2/2 both get hit. That's fine for us — a surjection $\mathbb{N}\to\mathbb{Q}^+$ is enough. To get an actual bijection you can skip the cells where $\gcd(p,q)>1$, though then there's no longer a nice closed form.

So lots of sets turn out to be countable: the evens, $\mathbb{Z}$, $\mathbb{N}\times\mathbb{N}$, and now $\mathbb{Q}^+$. Is *every* infinite set countable?

Example 0.5. Is $\mathcal{P}(\mathbb{N})$ countable? Is $\{0,1\}^{\mathbb{N}}$ countable?

Theorem 0.6. $\{0,1\}^{\mathbb{N}}$ *is uncountable.*

Proof. Suppose for the sake of contradiction that it is countable. Then there is a surjection $f:\mathbb{N}\to\{0,1\}^{\mathbb{N}}$ from the naturals to the infinite binary strings. Write $f(n)_i$ for the i-th digit of the string $f(n)$, and picture the outputs listed in a table — say it begins

$$\begin{aligned}
f(1)&=\underline{1}\,1\,0\,0\,1\,0\,1\,1\,1\ldots\\
f(2)&=1\,\underline{0}\,0\,0\,1\,0\,0\,0\,1\ldots\\
f(3)&=0\,0\,\underline{0}\,0\,0\,0\,0\,0\,0\ldots\\
f(4)&=1\,0\,1\,\underline{0}\,1\,0\,1\,0\,1\ldots\\
&\ \ \vdots
\end{aligned}$$

We claim there is a string that is not the output of any $f(n)$. Take the one obtained by walking down the underlined diagonal and flipping each digit: define $\text{bad} \in \{0,1\}^{\mathbb{N}}$ by

$$\text{bad}_n = 1 - f(n)_n.$$

In the table above the diagonal digits are $1, 0, 0, 0, \ldots$, so $\text{bad} = 0111\ldots$.

Why can bad not be the output of any $f(n)$? Because it differs from $f(n)$ in the n-th digit, by construction: $\text{bad}_n = 1 - f(n)_n \neq f(n)_n$. Two strings that differ in a digit are not equal, so $\text{bad} \neq f(n)$ for every $n \in \mathbb{N}$, contradicting the surjectivity of f.

So there is no surjection $\mathbb{N} \to \{0,1\}^{\mathbb{N}}$, and in particular no bijection, since a bijection would be one. □

Example 0.7. Write a bijection between $\{0,1\}^{\mathbb{N}}$ and $\mathcal{P}(\mathbb{N})$.

Here is one: $f : \{0,1\}^{\mathbb{N}} \to \mathcal{P}(\mathbb{N})$ via

$$f(b_1 b_2 b_3 \ldots) = \{i : b_i = 1\}.$$

That is, we read a string as a record of which naturals are in the set, with $b_i = 1$ meaning i is in it. Its inverse sends a set S to the string whose i-th digit is 1 exactly when $i \in S$, so f is a bijection.

For example, $f(010010100000...) = \{2, 5, 7\}$ since those are the digits that are 1s.

Theorem 0.8. *There is no surjection $\mathbb{N} \to \mathcal{P}(\mathbb{N})$. In particular, $\mathcal{P}(\mathbb{N})$ is uncountable.*

Proof. Suppose $g : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ were a surjection. The bijection above, $f : \{0,1\}^{\mathbb{N}} \to \mathcal{P}(\mathbb{N})$ has an inverse $f^{-1} : \mathcal{P}(\mathbb{N}) \to \{0,1\}^{\mathbb{N}}$, which is itself a bijection and so a surjection. A composition of surjections is a surjection, so $f^{-1} \circ g : \mathbb{N} \to \{0,1\}^{\mathbb{N}}$ would be a surjection — contradicting the previous theorem. □

Theorem 0.9. *The real numbers are uncountable.*

We don't do the whole proof, but you can convert a real number's decimal representation into binary and then use that to biject to $\{0,1\}^{\mathbb{N}}$.

So, overall, our results for today are

$$|\mathbb{N}| = |\text{evens}| = |\mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| < |\mathcal{P}(\mathbb{N})| = |\{0,1\}^{\mathbb{N}}| = |\mathbb{R}|$$