Lecture 21 — Cardinalities

Table of contents

Learning goals . . . 1
Worked: why is $|\mathbb{Z}| = |\mathbb{Z}^+| = |\mathbb{Q}|$? . . . 2
How do we measure the size of infinite sets? . . . 2
Finite sets, and the definition . . . 3
Proving that $|\mathbb{Z}^+| = |\mathbb{Q}^+|$ . . . 3
Worked: prove that $|\mathbb{Z}| = |S|$ . . . 4
Hilbert's Hotel . . . 6
Worked: prove that $|\mathbb{Z}^+| = |\mathbb{Z} \times \mathbb{Z}|$ . . . 8
Proving that $|\mathbb{Z}^+| = |\mathbb{Q}|$ . . . 8
Infinite subsets of $\mathbb{Z}^+$ . . . 10
See also . . . 12

Pre-work: Video 027 (Cardinalities). The reference notes are cardinality[1] for what "the same size" means and how to prove it, and countable-and-uncountable-sets[2] for the listing arguments that start here and finish in 2026-09-15-countable-and-uncountable-sets[3]. Every tool used is a bijection, so one-to-one-and-onto-functions[4] is the prerequisite.

Learning goals

- Understand cardinalities of finite and infinite sets.
- Learn how to prove properties concerning cardinalities of sets.

The picture to keep in mind is two columns of dots, each dot joined to a partner in the other column, both columns going on without end. It is a pairing that never runs out, and that is the whole idea.

[1] courses/math1061/cardinality.pdf
[2] courses/math1061/countable-and-uncountable-sets.pdf
[3] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf
[4] courses/math1061/one-to-one-and-onto-functions.pdf

Worked: why is $|\mathbb{Z}| = |\mathbb{Z}^+| = |\mathbb{Q}|$?

If cardinality is a measure of how large a set is, then why is $|\mathbb{Z}| = |\mathbb{Z}^+| = |\mathbb{Q}|$, when clearly $|\mathbb{Q}| > |\mathbb{Z}| > |\mathbb{Z}^+|$?

$|\mathbb{Q}| > |\mathbb{Z}| > |\mathbb{Z}^+|$ is false. The *clearly* is the mistake. Put $1, 2, 3, 4, 5$ over $\{a, b, c, d, e\}$ and join each number to one letter. That is what counting a finite set *is*: pairing its elements off with $1, 2, \ldots, n$. Cardinality keeps the pairing and drops the requirement that it stop.

The "clearly" comes from containment. $\mathbb{Z}^+ \subset \mathbb{Z} \subset \mathbb{Q}$, each a proper subset of the next, and for finite sets a proper subset is always smaller. For infinite sets that inference fails, and the proofs below show it. Every example below is infinite.

How do we measure the size of infinite sets?

$\mathbb{Z}^+$: the positive integers $1, 2, 3, \ldots$

$2\mathbb{Z}^+$: the even positive integers $2, 4, 6, \ldots$

There are two ways to set the two sets side by side. The first is as a subset: $2\mathbb{Z}^+ \subset \mathbb{Z}^+$, the even entries in the row $1, 2, 3, \ldots$. That is **not how to think of it**. The second is as a pairing: $\mathbb{Z}^+$ sits over $2\mathbb{Z}^+$, with each n joined to $2n$.

To measure the size of infinite sets, **think with functions**:

$$|2\mathbb{Z}^+| = |\mathbb{Z}^+|, \qquad f : \mathbb{Z}^+ \to 2\mathbb{Z}^+,\ f(x) = 2x,\ f \text{ is a bijection.}$$

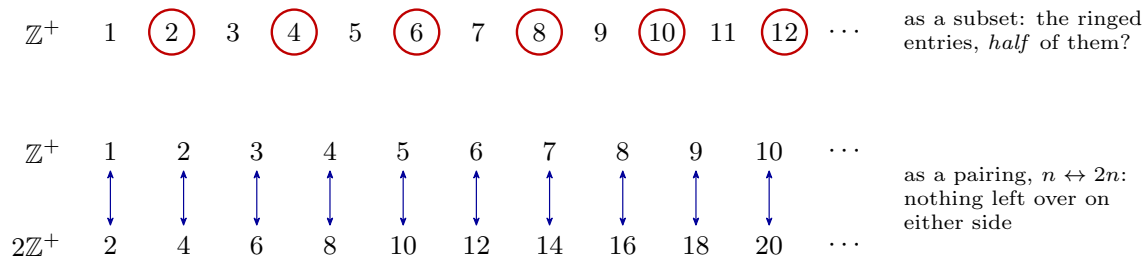


Figure 1: Two ways of setting the even positive integers beside the positive integers. Top: as a subset, $2\mathbb{Z}^+$ is every second entry, which makes it look like half of $\mathbb{Z}^+$. Bottom: as a pairing, $n \leftrightarrow 2n$ matches every positive integer with exactly one even number and every even number with exactly one positive integer, with nothing left over on either side. Cardinality is defined by the pairing, so $|2\mathbb{Z}^+| = |\mathbb{Z}^+|$ even though $2\mathbb{Z}^+$ is a proper subset.

Both halves of "bijection" are quick. One-to-one: $2x_1 = 2x_2$ gives $x_1 = x_2$. Onto: an even positive integer y is $2k$ for some $k \in \mathbb{Z}^+$, and $f(k) = y$.

Finite sets, and the definition

Four facts hold for **finite** sets. Each one is drawn, with the reason it works, in cardinality[5].

1. If A has more elements than B, then there is no one-to-one (injective) function $f : A \to B$. With five elements in A and four in B, the fifth element of A has nowhere new to land.
2. If A has fewer elements than B, then there is no onto (surjective) function $f : A \to B$. Some element of B is left that nothing reaches.
3. If A and B have the same number of elements, then **any** function $f : A \to B$ is one-to-one if and only if it is onto.
4. When A and B have the same number of elements there can be functions from A to B that are **neither** one-to-one **nor** onto.

The definition:

> Any two **finite** sets have the same number of elements if and only if there is a bijection between them.
>
> Any two sets have the same **cardinality** if and only if there is a bijection between them.
>
> If the sets A and B have the same cardinality, then we write $|A| = |B|$.

Any two sets means finite or infinite. The first sentence is a fact about counting. The second is a **definition**: "same size" is *defined* to mean "there is a bijection", so that the word makes sense for infinite sets too.

Fact 3 is the one that does **not** survive into the infinite case. $f : \mathbb{Z}^+ \to \mathbb{Z}^+$, $f(n) = 2n$, is one-to-one but not onto (nothing maps to 1), between two sets of the same cardinality. For infinite sets one-to-one and onto come apart, which is why every proof below checks them separately.

Proving that $|\mathbb{Z}^+| = |\mathbb{Q}^+|$

> A **positive** rational number has the form $\frac{a}{b}$ where $a, b \in \mathbb{Z}^+$.

[5] courses/math1061/cardinality.pdf

Define $f : \mathbb{Z}^+ \to \mathbb{Q}^+$ in three stages. First, display the elements of $\mathbb{Q}^+$ in a grid: row a, column b holds $\frac{a}{b}$. Next, run a path that snakes through the grid diagonal by diagonal. It meets some numbers more than once: $\frac{1}{1}$ and $\frac{2}{2}$ are the same number. Last, number the fractions the path counts, in the order it meets them. Some of the values: $f(1) = \frac{1}{1}$, $f(2) = \frac{1}{2}$, $f(3) = \frac{2}{1}$, $f(4) = \frac{3}{1}$, $f(5) = \frac{1}{3}$, $f(6) = \frac{1}{4}$, $f(10) = \frac{5}{1}$, $f(11) = \frac{1}{5}$, $f(12) = \frac{1}{6}$, $f(17) = \frac{6}{1}$, $f(18) = \frac{7}{1}$, $f(19) = \frac{5}{3}$. The path runs through $\frac{2}{2}$ without counting it.

Worked questions on f.

(a) What is $f(12)$? What is $f(18)$? — $f(12) = \frac{1}{6}$, $f(18) = \frac{7}{1}$.

(b) Why is this function both one-to-one and onto? **Onto:** any positive rational in lowest terms, $\frac{a}{b}$, sits in row a, column b, on the diagonal $a + b$. There are only finitely many cells on the diagonals before it, so the path gets there after finitely many steps and gives it a number. **One-to-one:** the path counts a cell only if its fraction is in lowest terms, and each positive rational has exactly one lowest-terms name, so two different positive integers never land on the same rational.

(c) What is $f^{-1}(\frac{5}{3})$? — $f^{-1}(\frac{5}{3}) = 19$. The notation makes sense here only because f is a bijection (inverse-functions[6]). To answer it, count along the path until $\frac{5}{3}$ comes up.

Worked: prove that $|\mathbb{Z}| = |S|$

> Let $S = \{n \in \mathbb{Z} \text{ such that } n \bmod 3 = 1\}$. Prove that $|\mathbb{Z}| = |S|$.

The template below is the one the rest of the course uses. It has three steps, and the proof has the same three parts in the same order.

> **One way to show $|X| = |Y|$ for sets X and Y:**
>
> - Define a **function** $f : X \to Y$ and **explain why it is a function** (each element of X has a unique image in Y)
> - Show f is one-to-one (injective)
> - Show f is onto (surjective)

First list the two sets and pair them up. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ goes over $S = \{\dots, -5, -2, 1, 4, 7, 10, \dots\}$, with $-1 \leftrightarrow -2$, $0 \leftrightarrow 1$, $1 \leftrightarrow 4$, $2 \leftrightarrow 7$, $3 \leftrightarrow 10$. Then define $f : \mathbb{Z} \to S$ by $f(n) = 3n + 1$.

It is a function into S. For any $n \in \mathbb{Z}$, $3n + 1 \equiv 1 \pmod 3$ so $f(n) \in S$, and $3n + 1$ is unique so f is a function.

One-to-one. Suppose $f(n_1) = f(n_2)$. Then

$$3n_1 + 1 = 3n_2 + 1, \qquad 3n_1 = 3n_2, \qquad n_1 = n_2.$$

[6] courses/math1061/inverse-functions.pdf

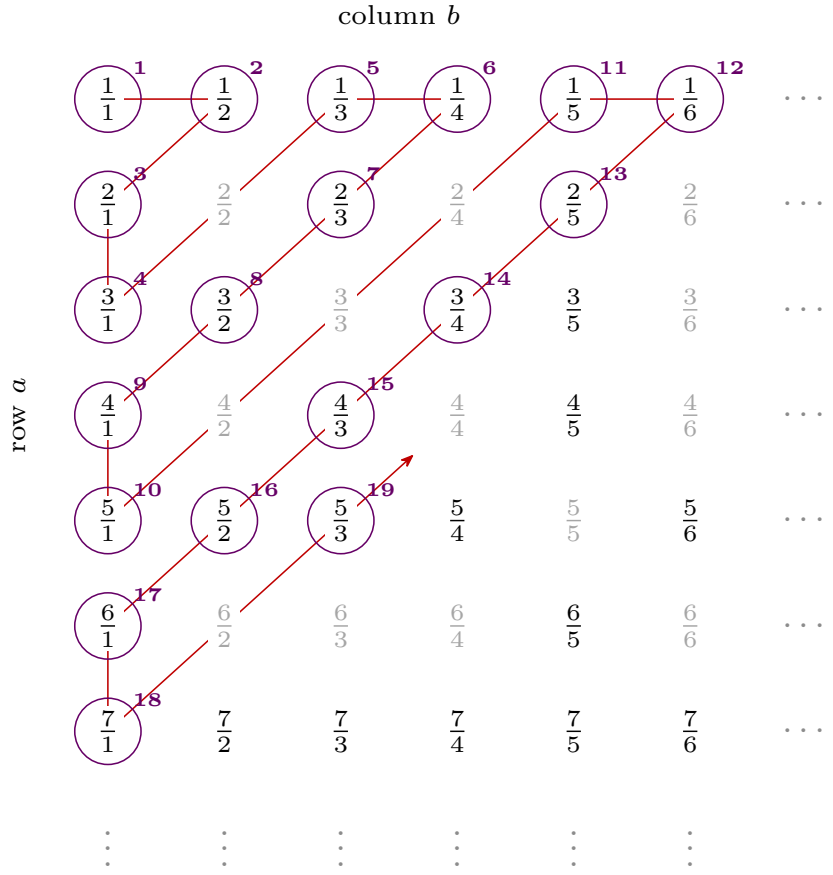


Figure 2: Listing the positive rationals. Row a, column b holds $\frac{a}{b}$, so every positive rational appears somewhere — infinitely often, under all its names. The path walks the anti-diagonals one after another, snaking back and forth. A fraction met in lowest terms gets the next positive integer (ringed, number above). Any other name for a rational already counted, such as $\frac{2}{2}$ or $\frac{4}{2}$, is stepped over (grey). Every diagonal is finite, so the walk reaches every cell after finitely many steps, which makes f onto; skipping the repeats makes it one-to-one.

$\therefore f$ is injective.

Onto. Let $y \in S$. Take $\frac{y-1}{3} \in \mathbb{Z}$, which is an integer because $y-1$ is divisible by 3 (by definition of S). Also

$$f\left(\frac{y-1}{3}\right) = 3\left(\frac{y-1}{3}\right) + 1 = (y-1) + 1 = y. \qquad \therefore f \text{ is onto.}$$

We have f is a bijection, so $|\mathbb{Z}| = |S|$.

The **rough work** does the solving that the onto step then runs forwards: want $y = 3x + 1$, so $\frac{y-1}{3} = x$. This is the same *solve backwards, run forwards* move as in one-to-one-and-onto-functions[7]. And the **domain check** again carries the real content. $\frac{y-1}{3}$ is an integer only because $y \in S$. For an arbitrary integer y it would not be, and f would not be onto $\mathbb{Z}$.

Two details about S. The members include negatives, -2 and -5, because mod here is the remainder from the quotient-remainder theorem, which is never negative: $-2 = 3 \cdot (-1) + 1$ (modular-arithmetic[8]). And the first bullet of the template is not a formality. It is where you check that f lands *in* S, not just in $\mathbb{Z}$.

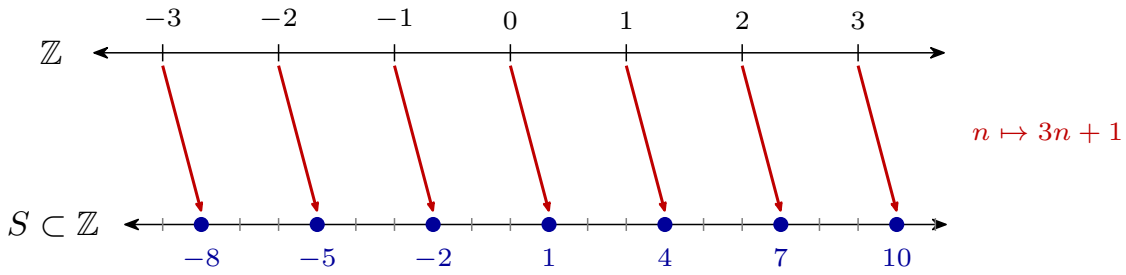


Figure 3: The bijection $f(n) = 3n + 1$ from $\mathbb{Z}$ to $S = n \in \mathbb{Z} : n \bmod 3 = 1$. On the lower line the members of S are only every third integer (the dots), yet each integer n above is sent to exactly one dot, and each dot y is hit from exactly one integer, namely $\frac{y-1}{3}$. Spreading a set out does not change its cardinality.

Hilbert's Hotel

> Suppose that you manage a hotel with infinitely* many rooms, numbered 1, 2, 3, etc. All rooms are occupied, when a new guest arrives and asks for a room. What do you do?
>
> *Here "infinite" means having the same cardinality as $\mathbb{Z}^+$.

[7] courses/math1061/one-to-one-and-onto-functions.pdf
[8] courses/math1061/modular-arithmetic.pdf

The question comes in three versions, by who arrives. The answers:

Arrivals	Move the existing guests	Put the new guests
one new guest	each person in room x goes to room $x+1$	in room 1
an infinite* busload	each room x goes to room $2x$	into the odd rooms
infinitely* many infinite* busloads	each room x goes to room 2^x	1st extra bus to all 3^x, 2nd to all 5^x, … continue for all primes

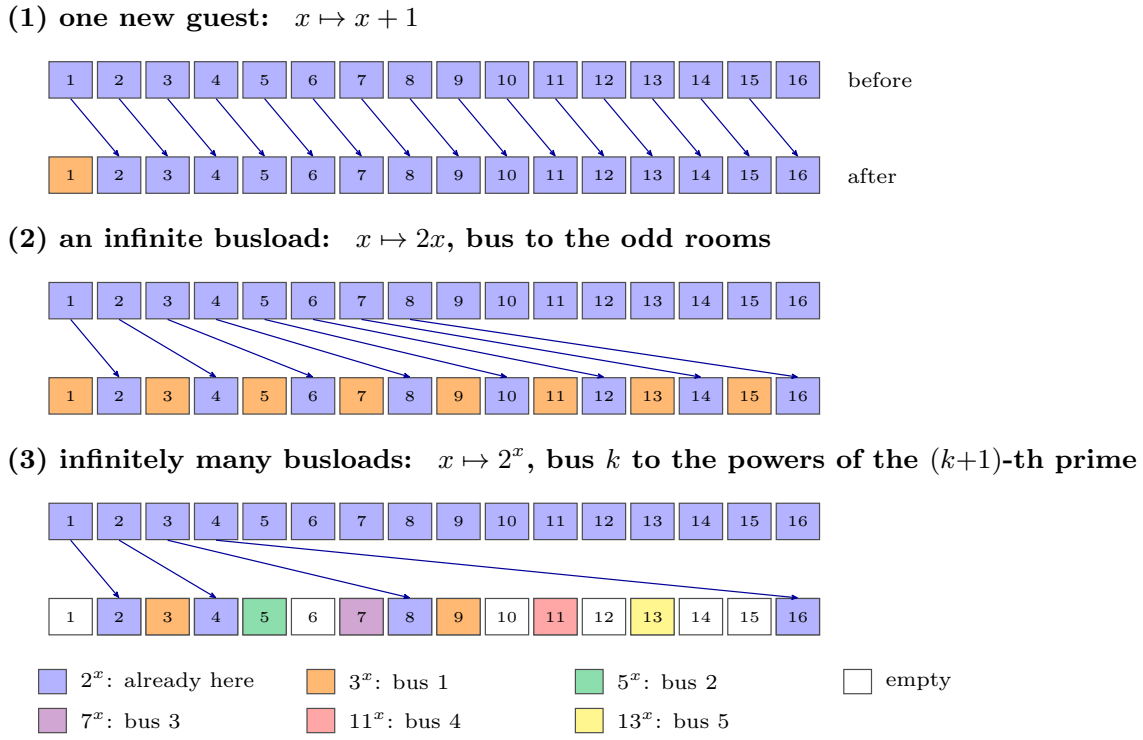


Figure 4: Hilbert's Hotel, rooms 1 to 16 of infinitely many. In each panel the top row is the full hotel before the move and the bottom row is after it: blue for the guests already there, other colours for arrivals, white for an empty room. (1) $x \mapsto x+1$ frees room 1. (2) $x \mapsto 2x$ frees every odd room, one for each passenger on the bus. (3) $x \mapsto 2^x$, with the k-th bus sent to the powers of the next prime — 3, 5, 7, 11, 13, … — gives everyone a room of their own, because a prime power is a power of only one prime. Rooms such as 1, 6 and 10 stay empty, and that is allowed: the new assignment only has to be one-to-one.

Each answer is a one-to-one function from guests to rooms, and each says something about cardinality.

- **One guest.** $x \mapsto x + 1$ is a bijection from $\mathbb{Z}^+$ to $\mathbb{Z}^+ - \{1\}$. Removing one element from $\mathbb{Z}^+$ does not make it smaller.
- **One bus.** $x \mapsto 2x$ is a bijection onto the even rooms, and the odd rooms are a second copy of $\mathbb{Z}^+$. $\mathbb{Z}^+$ splits into two parts each the same size as itself.
- **Infinitely many buses.** Nobody collides, because a room number p^x with p prime determines both p and x — unique factorisation again (divisibility-and-factorisation[9]). This assignment is *not* onto (room 1, room 6 and every other room that is not a prime power stays empty), and a hotel does not need it to be. Everyone needs a room, and no two guests may share one. That is an injection into $\mathbb{Z}^+$, which is exactly what $|X| \leq |\mathbb{Z}^+|$ means in the next lecture (cardinality[10]).

Worked: prove that $|\mathbb{Z}^+| = |\mathbb{Z} \times \mathbb{Z}|$

> Prove that $|\mathbb{Z}^+| = |\mathbb{Z} \times \mathbb{Z}|$. Draw a picture to illustrate a bijection.

Take $\mathbb{Z}^+$ as the list $1, 2, 3, ...$ and $\mathbb{Z} \times \mathbb{Z}$ as the points of a lattice. Walk a square spiral out from the origin: $(0, 0)$ to $(1, 0)$, up to $(1, 1)$, left to $(-1, 1)$, down to $(-1, -1)$, right to $(2, -1)$, up to $(2, 2)$, left to $(-2, 2)$, down to $(-2, -2)$, right to $(3, -2)$, up to $(3, 3)$, and on. Then:

$$f : \mathbb{Z}^+ \to \mathbb{Z} \times \mathbb{Z}, \qquad f(x) \text{ is "position } x\text{" along this spiral.}$$

Rows would not work in place of the spiral. Listing $\mathbb{Z} \times \mathbb{Z}$ row by row never gets past the first row, because the first row is already infinite. A listing has to reach every element after *finitely many* steps, so it must visit the pairs in finite batches that together cover everything. The spiral's rings are those batches, as the anti-diagonals were for the $\mathbb{Q}^+$ grid.

Proving that $|\mathbb{Z}^+| = |\mathbb{Q}|$

> Since each rational number can be written as $\frac{a}{b}$ where $(a, b) \in \mathbb{Z} \times \mathbb{Z}$, there is a bijection f from $\mathbb{Q}$ to a proper subset A of $\mathbb{Z} \times \mathbb{Z}$.

For $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$, use the same spiral but use only ordered pairs that give each rational number exactly once:

- Take $\gcd(a, b) = 1$.
- Decide whether the minus sign goes in the numerator (a) or the denominator (b).

[9] courses/math1061/divisibility-and-factorisation.pdf
[10] courses/math1061/cardinality.pdf

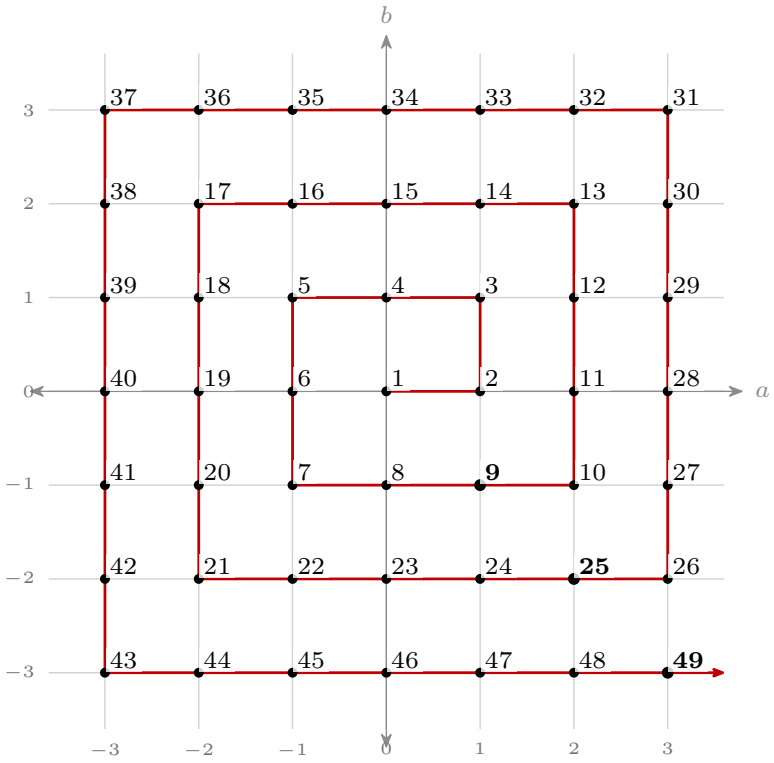


Figure 5: The spiral that lists $\mathbb{Z} \times \mathbb{Z}$: the number beside each lattice point is its position on the path, so the point marked n is $f(n)$. The path starts at $f(1) = (0, 0)$ and winds anticlockwise outwards. It never visits a point twice, so f is one-to-one. Each square ring is finite and is finished before the next begins — ring k closes at step $(2k + 1)^2$, the bold 9, 25 and 49 — so every lattice point is reached after finitely many steps, and f is onto.

- Leave out the whole horizontal axis, where $b = 0$, including $(0, 0)$. A pair with $b = 0$ is not a fraction at all.

For example, f sends $\frac{1}{2}$ to $(1, 2)$ and, with the minus sign in the denominator, $-\frac{4}{3}$ to $(4, -3)$. Either choice of sign works if it is made once and kept. Next, represent the rational numbers as blue spots in the spiral, and label them in the order the spiral meets them: $g(1), g(2), g(3), ...$ Then:

> $g : \mathbb{Z}^+ \to \mathbb{Q}$ is a bijection. **So** $|\mathbb{Z}^+| = |\mathbb{Q}|$**.**

Strictly, $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$ is a bijection onto A; as a function into all of $\mathbb{Z} \times \mathbb{Z}$ it is one-to-one but not onto, since A is a proper subset. That is enough, because g only ever walks through A.

The running total:

> Now we have seen that $|\mathbb{Z}^+| = |2\mathbb{Z}| = |\mathbb{Z}| = |\mathbb{Q}^+| = |\mathbb{Q}| = |\mathbb{Z} \times \mathbb{Z}|$.

Two of these links are not proved above. What was proved is $|2\mathbb{Z}^+| = |\mathbb{Z}^+|$, not $|2\mathbb{Z}| = |\mathbb{Z}|$, though $n \mapsto 2n$ works just as well from $\mathbb{Z}$ to the even integers $2\mathbb{Z}$. And $|\mathbb{Z}| = |\mathbb{Z}^+|$ is the listing $0, 1, -1, 2, -2, 3, -3, ...$, drawn in countable-and-uncountable-sets[11]. Equality of cardinality chains like this because bijections compose and invert (composition-of-functions[12], inverse-functions[13]).

Infinite subsets of $\mathbb{Z}^+$

> **Every infinite subset of $\mathbb{Z}^+$ has the same cardinality as $\mathbb{Z}^+$.**

The proof opens by listing the subset in increasing order:

> **Proof.** Let $A = \{a_1, a_2, a_3, ...\}$ be an infinite subset of $\mathbb{Z}^+$ such that $a_1 < a_2 < a_3 < \cdots$, that is, let a_1 be the least element of A, let a_2 be the least element of $A - \{a_1\}$, let a_3 be the least element of $A - \{a_1, a_2\}$, …and so on…

From there it goes by the $|X| = |Y|$ template, with one more tool:

> **The Well-Ordering Principle for the integers:** If S is a non-empty set of integers all of which are greater than some fixed integer, then S has a least element.

[11] courses/math1061/countable-and-uncountable-sets.pdf
[12] courses/math1061/composition-of-functions.pdf
[13] courses/math1061/inverse-functions.pdf

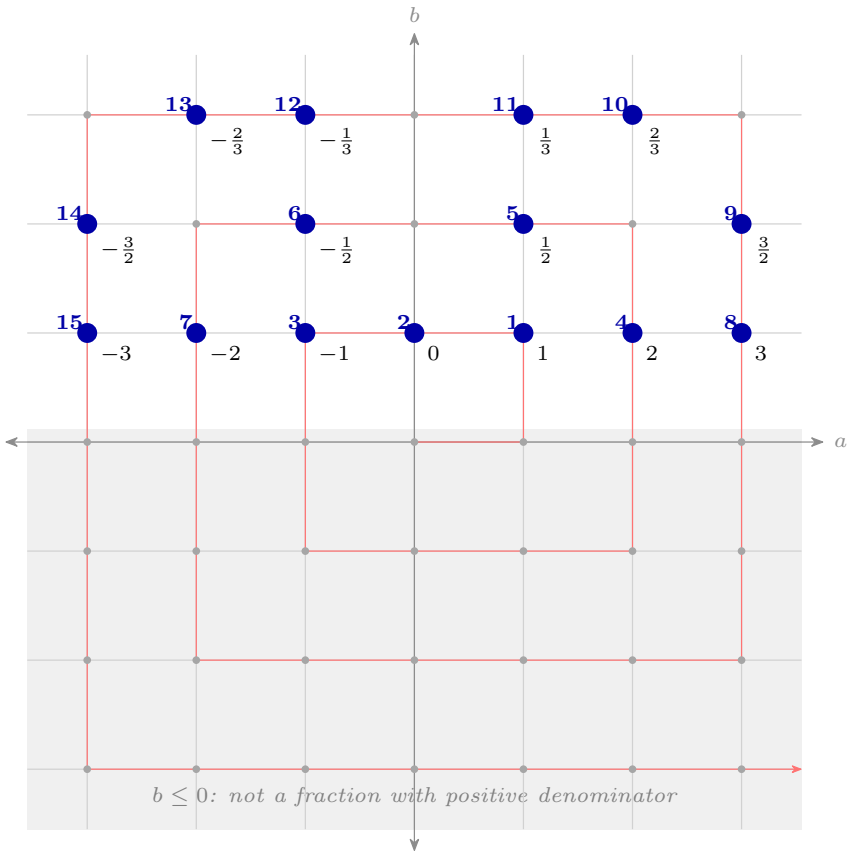


Figure 6: Listing $\mathbb{Q}$ with the same spiral. Write each rational in lowest terms with a positive denominator, $\frac{a}{b}$ with $b \geq 1$ and $\gcd(a, b) = 1$, and plot it at (a, b). Those points are the blue spots, and each rational owns exactly one. Walk the spiral and count only the blue spots: $g(1) = 1$, $g(2) = 0$, $g(3) = -1$, $g(4) = 2$, $g(5) = \frac{1}{2}$, and so on (index in blue, value beside it). Every rational is reached (onto) and none twice (one-to-one), so $g : \mathbb{Z}^+ \to \mathbb{Q}$ is a bijection. Points with $b \leq 0$ are never used, and neither is a point like $(2, 2)$ whose fraction is already spotted at $(1, 1)$.

The function to define is $f : \mathbb{Z}^+ \to A$. The finished proof is at the start of 2026-09-15-countable-and-uncountable-sets[14].

The well-ordering principle (strong-induction-and-the-well-ordering-principle[15]) is what makes each "let a_i be the least element" legitimate. $A - \{a_1, \ldots, a_{i-1}\}$ is a set of positive integers, all greater than 0. It is non-empty because A is infinite and only finitely many elements have been removed. So it has a least element.

See also

- cardinality[16] — the definition, the finite-set facts, the $|X| = |Y|$ template, comparing sizes
- countable-and-uncountable-sets[17] — listing arguments for $\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q}$, and what cannot be listed
- one-to-one-and-onto-functions[18] · inverse-functions[19] — bijections, which every argument here is built from
- 2026-09-08-composition-of-functions[20] — Lecture 20 · 2026-09-15-countable-and-uncountable-sets[21] — Lecture 22
- practice-problems[22] — §27, with full worked solutions

[14] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf
[15] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[16] courses/math1061/cardinality.pdf
[17] courses/math1061/countable-and-uncountable-sets.pdf
[18] courses/math1061/one-to-one-and-onto-functions.pdf
[19] courses/math1061/inverse-functions.pdf
[20] courses/math1061/2026-09-08-composition-of-functions.pdf
[21] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf
[22] courses/math1061/practice-problems.pdf