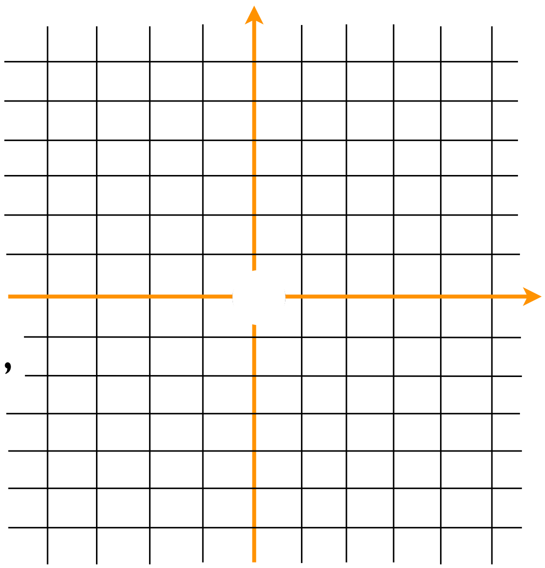
- Given two sets A , B , how do we decide which is the larger? We could either count the number of things in each and compare results, or simply pair up the terms (a , b) with $a \in$ A and $b \in$ B and see which set runs out first! Attempting to create such a *1-1* correspondence between A and B is really trying to construct a *1-1* function from A onto (a subset) of B or the other way around. On the other hand, trying to *count* the number of elements in a set S is really building a *1-1* function from S into $\mathbb{N}_{>0}$. We'll denote the *size* (or *cardinality*) of the set S by |S|.

- Defining the size for finite sets is easy, but amusing things happen when we start working with infinite sets. For example, which is the larger of $\mathbb{Z}$ and $2\mathbb{Z}$, where the latter is just the integer multiples of 2? Since $2\mathbb{Z} \subseteq \mathbb{Z}$ and $2\mathbb{Z} \neq \mathbb{Z}$ it's obvious that $|2\mathbb{Z}| \leq |\mathbb{Z}|$, where we're inclined to treat the inequality as strict. However, consider the function $f : \mathbb{Z} \longrightarrow 2\mathbb{Z}$ given by $f(n) = 2n$. It's easy to show that f is *1-1*, which means that $|\mathbb{Z}| \leq |2\mathbb{Z}|$ and hence $|2\mathbb{Z}| = |\mathbb{Z}|$. Similarly, we can show that $|\mathbb{Z}| = |\mathbb{N}|$. This ability for a set to be in *1-1* correspondence with a *proper* subset of itself could be taken as a defining property of infinite sets.

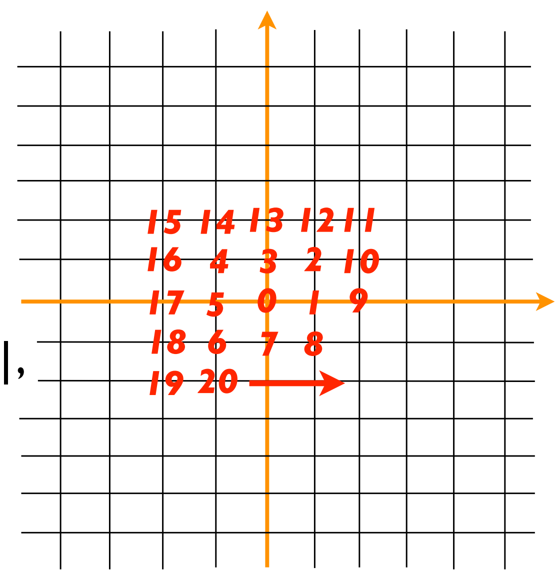
- Let's compare the sizes of $\mathbb{Z}$ and $\mathbb{Z}^2$. The function $f : \mathbb{Z} \longrightarrow \mathbb{Z}^2$ given by $f(n) = (n , 0)$ is *1-1* (check this), so $|\mathbb{Z}| \leq |\mathbb{Z}^2|$. Consider the function $g : \mathbb{Z}^2 \longrightarrow \mathbb{N}$ as described in the picture. This is also *1-1*, so $|\mathbb{Z}^2| \leq |\mathbb{N}| \leq |\mathbb{Z}|$, and hence $|\mathbb{Z}^2| = |\mathbb{Z}|$. Notice that since $\mathbb{Z} \subseteq Q \subseteq \mathbb{Z}^2$ (by the construction of Q), we have $|\mathbb{Z}| \leq |Q| \leq |\mathbb{Z}^2|$, and hence $|Q| = |\mathbb{Z}|$. We say that a set S is *countable* if it has the same size as $\mathbb{N}$, and write $|S| = \aleph_0$ (using the Hebrew letter *aleph*).



- Given two sets A , B , how do we decide which is the larger? We could either count the number of things in each and compare results, or simply pair up the terms (a , b) with $a \in$ A and $b \in$ B and see which set runs out first! Attempting to create such a *1-1* correspondence between A and B is really trying to construct a *1-1* function from A onto (a subset) of B or the other way around. On the other hand, trying to *count* the number of elements in a set S is really building a *1-1* function from S into $\mathbb{N}_{>0}$. We'll denote the *size* (or *cardinality*) of the set S by |S|.

- Defining the size for finite sets is easy, but amusing things happen when we start working with infinite sets. For example, which is the larger of $\mathbb{Z}$ and $2\mathbb{Z}$, where the latter is just the integer multiples of 2? Since $2\mathbb{Z} \subseteq \mathbb{Z}$ and $2\mathbb{Z} \neq \mathbb{Z}$ it's obvious that $|2\mathbb{Z}| \leq |\mathbb{Z}|$, where we're inclined to treat the inequality as strict. However, consider the function $\mathrm{f} : \mathbb{Z} \longrightarrow 2\mathbb{Z}$ given by $\mathrm{f}(n) = 2n$. It's easy to show that f is *1-1*, which means that $|\mathbb{Z}| \leq |2\mathbb{Z}|$ and hence $|2\mathbb{Z}| = |\mathbb{Z}|$. Similarly, we can show that $|\mathbb{Z}| = |\mathbb{N}|$. This ability for a set to be in *1-1* correspondence with a *proper* subset of itself could be taken as a defining property of infinite sets.

- Let's compare the sizes of $\mathbb{Z}$ and $\mathbb{Z}^2$. The function $\mathrm{f} : \mathbb{Z} \longrightarrow \mathbb{Z}^2$ given by $\mathrm{f}(n) = (n , 0)$ is *1-1* (check this), so $|\mathbb{Z}| \leq |\mathbb{Z}^2|$. Consider the function $\mathrm{g} : \mathbb{Z}^2 \longrightarrow \mathbb{N}$ as described in the picture. This is also *1-1*, so $|\mathbb{Z}^2| \leq |\mathbb{N}| \leq |\mathbb{Z}|$, and hence $|\mathbb{Z}^2| = |\mathbb{Z}|$. Notice that since $\mathbb{Z} \subseteq \mathrm{Q} \subseteq \mathbb{Z}^2$ (by the construction of Q), we have $|\mathbb{Z}| \leq |\mathrm{Q}| \leq |\mathbb{Z}^2|$, and hence $|\mathrm{Q}| = |\mathbb{Z}|$. We say that a set S is *countable* if it has the same size as $\mathbb{N}$, and write $|\mathrm{S}| = \aleph_0$ (using the Hebrew letter *aleph*).



- It might be natural to assume that none of this is surprising, and that it's simply enough to say that things are 'infinite', and that all infinities are the same. However, there's a pretty argument due to Cantor which shows that $\mathbb{R}$, the set of real numbers, is actually strictly larger than Q.

- The argument proceeds by contradiction, starting by supposing $\mathbb{R}$ to be countable.

  - It will be enough to consider the subset* $[0\,,1] \subseteq \mathbb{R}$; since if $\mathbb{R}$ is countable then every subset of $\mathbb{R}$ must be countable, consequently there would be an explicit one-to-one function from $[0\,,1]$ to $\mathbb{N}$. Looking at this list, where we have written each number in $[0\,,1]$ as an infinite decimal, we will now exhibit a number which fails to be in that supposedly complete list.

$$
\begin{array}{lcll}
\alpha_1 & = & 0\cdot a_{11}a_{12}a_{13}a_{14}a_{15}a_{16}\,\ldots\ldots & \mathbf{1} \\
\alpha_2 & = & 0\cdot a_{21}a_{22}a_{23}a_{24}a_{25}a_{26}\,\ldots\ldots & \mathbf{2} \\
\alpha_3 & = & 0\cdot a_{31}a_{32}a_{33}a_{34}a_{35}a_{36}\,\ldots\ldots & \mathbf{3} \\
\alpha_4 & = & 0\cdot a_{41}a_{42}a_{43}a_{44}a_{45}a_{46}\,\ldots\ldots & \mathbf{4} \\
\alpha_5 & = & 0\cdot a_{51}a_{52}a_{53}a_{54}a_{55}a_{56}\,\ldots\ldots & \mathbf{5} \\
\alpha_6 & = & 0\cdot a_{61}a_{62}a_{63}a_{64}a_{65}a_{66}\,\ldots\ldots & \mathbf{6} \\
\downarrow & & \downarrow & \downarrow
\end{array}
$$

  - Consider the number $\beta = 0\cdot b_1\, b_2\, b_3\, b_4\, b_5\, b_6\, \ldots.$ where the value of the *r*-th decimal place is given by $b_r = a_{rr}$ (mod 5) so that, for example, if $a_{rr} = 8$ then $b_r = 3$. Clearly $\beta \neq \alpha_1$ since it's about as wrong as possible in the first decimal place. Similarly, $\beta \neq \alpha_2$ since it fails to match at the second decimal place. Indeed, β fails to equal *any* of the α_r, always failing in the 'diagonal position', which means that β fails to be in the supposedly complete list of reals in $[0\,,1]$. Since this argument can be repeated for any purported *counting* of $[0\,,1]$, this proves that $[1\,,0]$, and hence also $\mathbb{R}$, is uncountable.

- Another version of this proof applies nicely to sets and their power sets. Claim $|A| \lneqq |\mathscr{P}(A)|$.

  - Consider $f : A \longrightarrow \mathscr{P}(A)$ given by $f(a) = \{a\}$. Clearly this is 1-1, so $|A| \leq |\mathscr{P}(A)|$. To prove the inequality strict, suppose false, i.e., suppose $\exists$ surjection $g : A \longrightarrow \mathscr{P}(A)$. Let's define $B = \{\, a \in A \mid a \notin g(a) \,\}$, then certainly $B \subseteq A$, so $B \in \mathscr{P}(A)$, so since g is onto, $\exists\, a' \in A$ with $g(a') = B$. If $a' \in B$, then $a' \notin g(a') = B$ ... oops! But if $a' \notin B$, then $a' \in g(a') = B$ ... oops again!! So our original supposition is untenable, and hence the inequality must be strict.

- This *uncountable* set has size $\aleph_1$, the notation for which probably hints to you that this is the start of a sequence of distinct infinite sizes!!!!

* The notation $(a\,,b) = \{\, x \in \mathbb{R} \mid a < x < b \,\}$ and $[a\,,b] = \{\, x \in \mathbb{R} \mid a \leq x \leq b \,\}$ for *open* and (respectively) *closed intervals* is standard, with obvious meanings for $[a\,,b)$ and $(a\,,b]$.

- It might be natural to assume that none of this is surprising, and that it's simply enough to say that things are 'infinite', and that all infinities are the same. However, there's a pretty argument due to Cantor which shows that $\mathbb{R}$, the set of real numbers, is actually strictly larger than Q.

- The argument proceeds by contradiction, starting by supposing $\mathbb{R}$ to be countable.

  - It will be enough to consider the subset* $[0\,,\,1] \subseteq \mathbb{R}$; since if $\mathbb{R}$ is countable then every subset of $\mathbb{R}$ must be countable, consequently there would be an explicit one-to-one function from $[0\,,\,1]$ to $\mathbb{N}$. Looking at this list, where we have written each number in $[0\,,\,1]$ as an infinite decimal, we will now exhibit a number which fails to be in that supposedly complete list.

$$
\begin{array}{lcll}
\alpha_1 & = & 0\cdot \underline{a_{11}}\,a_{12}\,a_{13}\,a_{14}\,a_{15}\,a_{16}\,\cdots\cdots & \mathbf{1} \\
\alpha_2 & = & 0\cdot a_{21}\,\underline{a_{22}}\,a_{23}\,a_{24}\,a_{25}\,a_{26}\,\cdots\cdots & \mathbf{2} \\
\alpha_3 & = & 0\cdot a_{31}\,a_{32}\,\underline{a_{33}}\,a_{34}\,a_{35}\,a_{36}\,\cdots\cdots & \mathbf{3} \\
\alpha_4 & = & 0\cdot a_{41}\,a_{42}\,a_{43}\,\underline{a_{44}}\,a_{45}\,a_{46}\,\cdots\cdots & \mathbf{4} \\
\alpha_5 & = & 0\cdot a_{51}\,a_{52}\,a_{53}\,a_{54}\,\underline{a_{55}}\,a_{56}\,\cdots\cdots & \mathbf{5} \\
\alpha_6 & = & 0\cdot a_{61}\,a_{62}\,a_{63}\,a_{64}\,a_{65}\,\underline{a_{66}}\,\cdots\cdots & \mathbf{6} \\
\downarrow & & \downarrow \qquad\qquad\qquad\qquad - & \downarrow
\end{array}
$$

  - Consider the number $\beta = 0\cdot b_1\, b_2\, b_3\, b_4\, b_5\, b_6\, \ldots$ where the value of the r-th decimal place is given by $b_r = a_{rr}$ (mod 5) so that, for example, if $a_{rr} = 8$ then $b_r = 3$. Clearly $\beta \neq \alpha_1$ since it's about as wrong as possible in the first decimal place. Similarly, $\beta \neq \alpha_2$ since it fails to match at the second decimal place. Indeed, β fails to equal *any* of the α_r, always failing in the 'diagonal position', which means that β fails to be in the supposedly complete list of reals in $[0\,,\,1]$. Since this argument can be repeated for any purported *counting* of $[0\,,\,1]$, this proves that $[1\,,\,0]$, and hence also $\mathbb{R}$, is uncountable.

- Another version of this proof applies nicely to sets and their power sets. Claim $|A| \lneqq |\mathscr{P}(A)|$.

  - Consider $f : A \longrightarrow \mathscr{P}(A)$ given by $f(a) = \{a\}$. Clearly this is 1-1, so $|A| \leq |\mathscr{P}(A)|$. To prove the inequality strict, suppose false, i.e., suppose $\exists$ surjection $g : A \longrightarrow \mathscr{P}(A)$. Let's define $B = \{ a \in A \mid a \notin g(a) \}$, then certainly $B \subseteq A$, so $B \in \mathscr{P}(A)$, so since g is onto, $\exists\, a' \in A$ with $g(a') = B$. If $a' \in B$, then $a' \notin g(a') = B$ ... oops! But if $a' \notin B$, then $a' \in g(a') = B$ ... oops again!! So our original supposition is untenable, and hence the inequality must be strict.

- This *uncountable* set has size $\aleph_1$, the notation for which probably hints to you that this is the start of a sequence of distinct infinite sizes!!!!

---

* The notation $(a\,,b) = \{ x \in \mathbb{R} \mid a < x < b \}$ and $[a\,,b] = \{ x \in \mathbb{R} \mid a \leq x \leq b \}$ for *open* and (respectively) *closed intervals* is standard, with obvious meanings for $[a\,,b)$ and $(a\,,\,b]$.