Introduction to Proof (part 4): Cardinality and Countability (by Evan Dummit, 2022, v. 2.00)

Contents

4 Cardinality and Countability

Our goal in this chapter is to discuss the notions of cardinality and countability of sets, which use functions to formalize the idea of measuring the number of elements in a set. We begin by discussing bijections (functions that are both one-to-one and onto) and then use them to define an equivalence relation on sets whose equivalence classes correspond to the different possible sizes of sets. We then study infinite sets and establish a surprising distinction between different sizes of infinite sets: that of countable and uncountable sets. We close with a discussion of the pigeonhole principle, which allows us to exploit properties of cardinality in a variety of useful ways.

4.1 Bijections and Cardinality

- In the previous chapter, we discussed bijections, functions that are both one-to-one and onto, and saw that they provide a one-to-one correspondence between the elements of the domain with the elements of the target.
- We now use one-to-one correspondences to discuss cardinality more formally

4.1.1 Cardinality

- Notice that the process of counting the elements of a finite set A is the same as labeling the elements of a set with the positive integers $1, 2, 3, \dots, n$.
  - ◦ By our interpretation of a bijection as a relabeling, this is the same as giving a bijection between A and the set $\{1, 2, 3, \dots, n\}$.
  - ◦ We can use this idea to give a formal definition of the cardinality of a finite set:
- Definition: If A is a set and n is a nonnegative integer, we say the cardinality of A is n (written $\#A = n$) if there exists a bijection between A and the set $\{1, 2, 3, \dots, n\}$. If there exists an integer n such that the cardinality of A is n, we say A is a finite set, and otherwise we say A is an infinite set.
  - ◦ We take the usual convention that if $n = 0$ the set written as $\{1, 2, 3, \dots, n\}$ means the empty set, and so the cardinality of $\emptyset$ is 0.
  - ◦ We must verify that this definition is well-posed, in the sense that for any finite set A, there is a unique positive integer n for which there exists a bijection between A and $\{1, 2, 3, \dots, n\}$.

  - If there were bijections between A and $\{1, 2, 3, \ldots, n\}$, and also between A and $\{1, 2, 3, \ldots, m\}$, then since one-to-one correspondence is an equivalence relation, this would give a bijection between $\{1, 2, 3, \ldots, n\}$ and $\{1, 2, 3, \ldots, m\}$.
  - However, such a bijection cannot exist unless $m = n$, as is straightforward to verify using induction. For completeness: without loss of generality assume $n \leq m$, and induct on n. The base case $n = 0$ follows by observing that the only function from the empty set is the empty function (with image the empty set) so necessarily $m = 0$ also.
  - For the inductive step, assume that having a bijection from $\{1, 2, 3, \ldots, n\}$ to $\{1, 2, 3, \ldots, m\}$ for $m = k$ implies $n = k$, and suppose we have a bijection from $\{1, 2, 3, \ldots, n\}$ to $\{1, 2, 3, \ldots, m\}$ where $m = k + 1$. If we have a bijection $f : \{1, 2, \ldots, k + 1\} \to \{1, 2, \ldots, n\}$, then let $g = f|_{\{1,2,\ldots k\}}$ be the restriction of f to $\{1, 2, \ldots, k\}$ and observe that the image of g is the set $\{1, 2, \ldots, n\}$ with one element removed. So then g is a bijection between $\{1, 2, \ldots, k\}$ and its image, which (by relabeling) is in turn in bijection with the set $\{1, 2, \ldots, n - 1\}$. Hence by the inductive hypothesis, we see $k = n - 1$, and so $m = k + 1 = n$ as claimed.

- We have various other basic properties of cardinality:

- Proposition (Properties of Cardinality): Suppose A and B are sets.

  1. If A is finite and $B \subseteq A$, then B is finite, and $\#B \leq \#A$ with equality if and only if $B = A$.
     - Proof: Induction on $n = \#A$. The base case $n = 0$ is trivial, since in that case $A = B = \emptyset$ so $\#A = \#B = 0$, and we have equality.
     - For the inductive step, suppose $\#A = n$ with $n \geq 1$. If $B = A$ the result is trivial so suppose B is a proper subset of A.
     - Since $\#A = n$ there exists a bijection $f : A \to \{1, 2, \ldots, n\}$. Then the set $f(B) = \{f(b) : b \in B\}$ is a proper subset of $\{1, 2, \ldots, n\}$ since B is a proper subset of A and f is a bijection. Restricting f to $f|_B$ yields a bijection of B with this proper subset, which must have cardinality k for some $k < n$. Then by relabeling the elements of this subset as $\{1, 2, \ldots, k\}$ we see that $\#B = k < n = \#A$, as required.
  2. If A and B are finite and disjoint, then $\#(A \cup B) = \#A + \#B$.
     - Proof: Suppose $\#A = n$ and $\#B = m$ and let $f : A \to \{1, 2, \ldots, n\}$ and $g : B \to \{1, 2, \ldots, m\}$ be bijections. Then the function $h : \{1, 2, \ldots, m+n\} \to A \cup B$ with $h(k) = \begin{cases} f(k) & \text{for } 1 \leq k \leq m \\ g(k - n) & \text{for } m + 1 \leq k \leq m + n \end{cases}$ is also a bijection, so $\#(A \cup B) = m + n = \#A + \#B$.
  3. If A is finite, then for any B we have $\#(A \backslash B) = \#A - \#(A \cap B)$.
     - Proof: By (1) we see that $A \backslash B$ and $A \cap B$ are finite since they are both subsets of A. Since they are also disjoint and have union A, by (2) we have $\#A = \#(A \backslash B) + \#(A \cap B)$ which yields the desired result immediately.
  4. If A and B are finite, then $\#(A \cup B) = \#A + \#B - \#(A \cap B)$.
     - Proof: Let $C = A \backslash B$ and observe that $C \cup B = A \cup B$ and that C and B are disjoint. Then by (2) and (3) we have $\#(A \cup B) = \#(C \cup B) = \#C + \#B = \#A + \#B - \#(A \cap B)$ as claimed.
     - Remark: This result generalizes inductively to larger unions, yielding a general statement that is known as the inclusion-exclusion formula. For example, for three sets one obtains $\#(A \cup B \cup C) = \#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C)$.
  5. If A and B are finite, then $\#(A \times B) = \#A \cdot \#B$.
     - Proof: Suppose $\#A = n$ and $\#B = m$ and let $f : \{1, 2, \ldots, n\} \to A$ and $g : \{1, 2, \ldots, m\} \to B$ be bijections. Then the function $h : \{1, 2, \ldots, mn\} \to A \times B$ defined by taking $h(a + n(b - 1)) = (f(a), g(b))$ for $1 \leq a \leq n$ and $1 \leq b \leq m$ is also a bijection, so $\#(A \times B) = mn = \#A \cdot \#B$ as claimed.
     - Remark: This result generalizes inductively to larger Cartesian products. For example, for three sets one obtains $\#(A \times B \times C) = \#A \cdot \#B \cdot \#C$.

6. If A is infinite and $A \subseteq B$, then B is infinite. In particular, $A \cup C$ is infinite precisely when A or C is infinite.
   - Proof: Suppose $A \subseteq B$. By (1), if B is finite, then A is finite, so taking the contrapositive yields that if A is infinite, then B is infinite.
   - For the second part, if A or C is infinite, then since each is a subset of the union $A \cup C$, the union is infinite. Otherwise, if both A and C are finite, then by (4) so is $A \cup C$.
7. If A is infinite and B is nonempty, then $A \times B$ is infinite.
   - We remark that $A \times \emptyset = \emptyset$, so the hypothesis that B be nonempty is needed here for $A \times B$ to be infinite.
   - Proof: Suppose A is infinite and $x \in B$. Then $A \times B$ contains the subset $A \times \{x\}$, which is in bijection with the infinite set A hence is also infinite. Then by (6), we see $A \times B$ is infinite.

- By employing these results in various ways we can solve simple counting problems.
- Two fundamental counting principles are as follows:
  - ("Addition Principle") When choosing among n disjoint options labeled 1 through n, if option i has a_i possible outcomes for each $1 \le i \le n$, then the total number of possible outcomes is $a_1 + a_2 + \cdots + a_n$.
  - To illustrate the addition principle, if a restaurant offers 5 main courses with chicken, 6 main courses with beef, and 12 vegetarian main courses, then (presuming no course is counted twice) the total possible number of main courses is $5 + 6 + 12 = 23$.
  - The addition principle can be justified using our results about cardinalities of unions of disjoint sets: if A_i corresponds to the set of outcomes of option i, then the union $A_1 \cup A_2 \cup \cdots \cup A_n$ corresponds to a single choice of one outcome from one of the A_i. Then because all of the different options are disjoint, the number of such choices is $\#(A_1 \cup A_2 \cup \cdots \cup A_n) = \#A_1 + \#A_2 + \cdots + \#A_n$ by repeatedly applying (2).
  - ("Multiplication Principle") When making a sequence of n independent choices, if step i has b_i possible outcomes for each $1 \le i \le n$, then the total number of possible collections of choices is $b_1 \cdot b_2 \cdot \cdots \cdot b_n$.
  - To illustrate the multiplication principle, if a fair coin is tossed (2 possible outcomes) and then a fair 6-sided die is rolled (6 possible outcomes), the total number of possible results of flipping a coin and then rolling a die is $2 \cdot 6 = 12$.
  - The multiplication principle follows from our results about cardinalities of Cartesian products: if B_i corresponds to the set of outcomes of choice i, then the elements of the Cartesian product $B_1 \times B_2 \times \cdots \times B_n$ correspond to ordered n-tuples of outcomes, one for each choice. The number of such n-tuples is $\#(B_1 \times B_2 \times \cdots \times B_n) = \#B_1 \cdot \#B_2 \cdot \cdots \cdot \#B_n$ by repeatedly applying (5).
- By employing these principles appropriately, we can solve a variety of basic counting problems.
- Example: Determine the number of possible outcomes from rolling a 6-sided die 5 times in a row.
  - Each individual roll has 6 possible outcomes. Thus, by the multiplication principle, the number of possible sequences of 5 rolls is $6^5 = \boxed{7776}$.
- Example: Determine the number of subsets of the set $\{1, 2, \ldots, n\}$.
  - We may characterize a subset S of $\{1, 2, \ldots, n\}$ by listing, for each $k \in \{1, 2, \ldots, n\}$, whether $k \in S$ or $k \notin S$.
  - By the multiplication principle, the number of possible ways of making this sequence of n choices is $\boxed{2^n}$.
- Example: If $\#A = n$ and $\#B = m$, find the total number of functions $f : A \to B$.
  - If $A = \{a_1, a_2, \ldots, a_n\}$, then such a function is completely determined by the values $f(a_1)$, $f(a_2)$, ... , $f(a_n)$.
  - Since $\#B = m$, there are m possible choices for each of the n values $f(a_1)$, $f(a_2)$, ... , $f(a_n)$.
  - Since all such choices are allowed, the total number of functions is therefore $\boxed{m^n}$.

- Example: Find the number of positive integer divisors of 90000.
  - Note that $90000 = 2^4 3^2 5^4$, so any positive integer divisor must have the form $2^a 3^b 5^c$ where $a \in \{0,1,2,3,4\}$, $b \in \{0,1,2\}$, and $c \in \{0,1,2,3,4\}$.
  - On the other hand, every such integer is a divisor, and so since there are 5 choices for a, 3 for b, and 5 for c, there are $5 \cdot 3 \cdot 5 = \boxed{75}$ divisors in total.
  - Remark: In the same way, one may see that $n = 2^{n_2} 3^{n_3} 5^{n_5} \cdots$ has a total of $(n_2+1)(n_3+1)(n_5+1)\cdots$ positive integer divisors.

4.1.2 Countable and Uncountable Sets

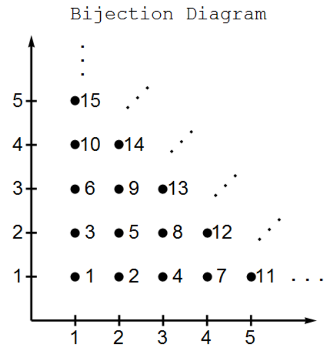
- Because we have defined cardinality in terms of bijections, and the property of being in a one-to-one correspondence is an equivalence relation on sets, we see that there is a bijection between two finite sets if and only if they have the same cardinality.
  - This gives us an alternative way to view cardinalities, namely, as representing the equivalence classes of sets under the relation of being in one-to-one correspondence.
  - For example, one equivalence class contains the sets $\{1,2\}$, $\{1,5\}$, $\{22,\pi\}$, $\{A,B\}$, $\{\star, \text{potato}\}$, ... , since any pair of these sets is in one-to-one correspondence with one another. This equivalence class may be thought of as being the collection of all sets of cardinality 2.
  - The advantage of this approach to cardinality is that it also extends to infinite sets:
- Definition: We say two sets are equinumerous (or equipollent) if there exists a bijection between them.
  - Example: The sets $\{1,2,3\}$ and $\{a,b,Q\}$ are equinumerous because there exists a bijection between them, namely, the function $f = \{(1,a),\ (2,b),\ (3,Q)\}$.
  - Example: The sets $\mathbb{Z}$ and $2\mathbb{Z}$ (the even integers) are equinumerous because there exists a bijection between them, namely, the function $f : \mathbb{Z} \to 2\mathbb{Z}$ given by $f(n) = 2n$ (it is easy to see that f is one-to-one and onto).
  - We think of two equinumerous sets as having the same cardinality: from our observations above, this interpretation agrees with the definition of cardinality for finite sets.
  - It is somewhat strange to think of the set of even integers as having the same cardinality as the set of all integers, because the set of even integers is a proper subset of the set of all integers (indeed, in some sense[1] only "half" of all integers are even). But this is the type of statement we must accept if we are to give any sensible definition for the cardinality of an infinite set that behaves well under set operations.
  - Example: The sets $\mathbb{Z}$ and $\mathbb{Z}_{>0}$ (the positive integers) are equinumerous, because the function $f : \mathbb{Z} \to \mathbb{Z}_{>0}$ given by $f(n) = \begin{cases} 2n+2 & \text{if } n \geq 0 \\ -2n+1 & \text{if } n < 0 \end{cases}$ is a bijection, since it maps the nonnegative integers to the even positive integers and it maps the negative integers to the odd positive integers.
  - Example: The sets $\mathbb{Z}_{>0}$ (the positive integers) and the set S of perfect squares are equinumerous, because the function $f : \mathbb{Z}_{>0} \to S$ given by $f(n) = (n-1)^2$ is a bijection.
- As we have noted above, counting elements of a set is the same as assigning positive integer labels to the elements of the set, which is in turn the same as creating a bijection with a subset of the positive integers.
- Definition: If S is a set, we say S is countable if there exists a bijection between S and a subset of the positive integers, and we say S is countably infinite if S is countable and infinite. If S is not countable, we say S is uncountable.

[1] One may make precise the idea that half of all integers are even by noting that if E is the set of even integers, then the limit $\lim_{N\to\infty} \dfrac{\#[E \cap \{-N,\dots,N\}]}{\#[\{-N,\dots,N\}]}$ is equal to $\dfrac{1}{2}$. Equivalently, the proportion of the integers in $\{-N,-N+1,\dots,N-1,N\}$ that are even approaches $1/2$ as $N \to \infty$). In general, if S is a subset of the integers, its "natural density" is defined as the limit $\lim_{N\to\infty} \dfrac{\#[S \cap \{-N,\dots,N\}]}{\#[\{-N,\dots,N\}]}$, if the limit exists; note that there do exist sets whose natural density is undefined, such as the set of integers with leading digit 1 (in base 10).

  - By definition, any finite set is countable since it can be put in bijection with the set $\{1, 2, 3, \dots, n\}$ where n is its cardinality.

- Proposition (Properties of Countability): The following are true:

  1. If S is a countably infinite subset of the positive integers, there exists a bijection between S and $\mathbb{Z}_{>0}$.
     - Intuitively, we can just define the bijection by mapping 1 to the smallest element of S, 2 to the second smallest, and so forth.
     - Proof: By the well ordering axiom, since S is nonempty it has a smallest element a_1.
     - Since S is infinite, $S \backslash \{a_1\}$ is also infinite hence nonempty, so it has a smallest element $a_2 > a_1$.
     - By a trivial induction, we may continue this process for each positive integer $n \geq 1$ to construct $a_n > a_{n-1} > \cdots > a_1$ where $S \backslash \{a_1, \dots, a_n\}$ is infinite and has all elements greater than a_n. Since the a_i are all distinct positive integers in increasing order, we also see that $a_n \geq n$ for each n.
     - Setting $f(n) = a_n$ then yields a one-to-one function $f : \mathbb{Z}_{>0} \to S$. But f is also onto, since any $k \in S$ will be the smallest element of $S \backslash \{1, 2, \dots, k-1\}$ hence necessarily is among the values $f(1), \dots, f(k)$.
  2. More generally, any subset of a countable set is countable.
     - Proof: Suppose A is countable and $B \subseteq A$. Then by definition there is a bijection $f : A \to Z$ with a subset Z of the positive integers.
     - The restriction $f|_B$ is a then bijection from B to $\text{im}(f|_B) \subseteq Z$, which is also a subset of the positive integers.
     - Hence there is a bijection from B to a subset of the positive integers, so B is countable.
  3. A nonempty set S is countable if and only if there exists an onto function $f : \mathbb{Z}_{>0} \to S$.
     - The utility of this result is that it provides an easier way to establish countability, since onto maps are less restrictive and thus easier to construct than bijections.
     - Proof: Suppose S is nonempty. If there exists an onto function $f : \mathbb{Z}_{>0} \to S$, let n_x be the smallest positive integer such that $f(n_x) = x$. (Note that this integer necessarily exists by applying the well-ordering axiom to the set of integers f maps to x which is nonempty since f is onto.)
     - Then for $A = \{n_x : x \in S\}$, we see that $f|_A$ is a bijection (since it is onto and also one-to-one) with the subset A of $\mathbb{Z}_{>0}$ with S, so S is countable.
     - Conversely, suppose S is countable and nonempty, so that there exists a bijection $g : A \to S$ where A is a subset of the positive integers. Let $x \in S$ (here is where we are using the fact that S is nonempty), and then define $f : \mathbb{Z}_{>0} \to S$ via $f(n) = \begin{cases} g(n) & \text{if } n \in A \\ x & \text{if } n \notin A \end{cases}$.
     - Clearly f is onto since it contains the image of g (which is A), so there exists an onto function $f : \mathbb{Z}_{>0} \to S$ as claimed.
  4. The Cartesian product of two countable sets is countable.
     - Proof: Since the product map of two bijections is a bijection on the respective Cartesian products, and a subset of a countable set is countable by (2) above, it is enough to prove that the Cartesian product $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ is countable.
     - We give an explicit bijection $f : \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ by labeling the points in "diagonal stripes" as shown in the diagram below:



   - More explicitly, the bijection is given by $f(a,b) = \dfrac{(a+b)(a+b-1)}{2} - a + 1$ for positive integers a and b.
   - It is a straightforward induction on b to see that this labeling is correct on all of the points with $a = 1$: then increasing a by 1 and decreasing b by 1 decreases f by exactly 1 (since $a + b$ is not changed), so the labeling is also correct on all of the diagonal stripes.
   - Thus, $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ is countable, hence so is the Cartesian product of any two countable sets.

5. The union of two countable sets is countable.
   - Proof: Suppose A and B are countable. If either A or B is empty then the union is just the other of the two sets, so the result is trivial.
   - Now assume both sets are nonempty. Then by (3) there exist onto functions $f_A : \mathbb{Z}_{>0} \to A$ and $f_B : \mathbb{Z}_{>0} \to B$.
   - Now define the function $f : \mathbb{Z}_{>0} \to A \cup B$ via $f(n) = \begin{cases} f_A(\frac{n+1}{2}) & \text{if } n \text{ is odd} \\ f_B(\frac{n}{2}) & \text{if } n \text{ is even} \end{cases}$.
   - Then f is onto, since its image contains each value $f_A(k) = f(2k)$ and $f_B(k) = f(2k-1)$ for each positive integer k. Hence by (3) again we see that $A \cup B$ is countable.

6. More generally, a countable union of countable sets is countable: if I is a countable indexing set and S_i is a countable set for each $i \in I$, then $\bigcup_{i \in I} S_i$ is countable.
   - Proof: If any S_i is empty we may simply discard it without affecting the union, so suppose each S_i is nonempty. Additionally, if I is finite, then an easy induction using (5) shows that $\bigcup_{i \in I} S_i$ is countable.
   - So assume that I is infinite. Then by (1) there is a bijection $f : \mathbb{Z}_{>0} \to I$ and the positive integers, so by setting $T_j = S_{f(j)}$ for each positive integer j, we are reduced to showing that $\bigcup_{j=1}^{\infty} T_j$ is countable.
   - By (3), for each $j \geq 1$ there exists an onto function $f_j : \mathbb{Z}_{>0} \to T_j$. Now define the function $g : \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \to \bigcup_{j=1}^{\infty} T_j$ via $g(a,b) = f_a(b)$. Then g is onto, since its image contains $\mathrm{im}(f_j) = T_j$ for each j.
   - Finally, since $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ is countable by (5), composing a bijection $h : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ with g yields an onto map $h \circ g : \mathbb{Z}_{>0} \to \bigcup_{j=1}^{\infty} T_j$, so by (3) we see that $\bigcup_{j=1}^{\infty} T_j$ is countable.

7. (Cantor) The set of rational numbers $\mathbb{Q}$ is countable.
   - Proof 1: For $\mathbb{Q}$, associate the rational number a/b in lowest terms with $b > 0$ to the ordered pair (a,b) in the Cartesian product $\mathbb{Z} \times \mathbb{Z}$. This yields a bijection between $\mathbb{Q}$ and a subset of $\mathbb{Z} \times \mathbb{Z}$.
   - Then since $\mathbb{Z} \times \mathbb{Z}$ is countable by (4) above, and any subset of a countable set is countable by (2) above, we conclude $\mathbb{Q}$ is countable, as claimed.
   - Proof 2: By definition $\mathbb{Q}$ is the union of the countable sets $S_n = \dfrac{1}{n}\mathbb{Z} = \{\dots, -\dfrac{2}{n}, -\dfrac{1}{n}, 0, \dfrac{1}{n}, \dfrac{2}{n}, \dfrac{3}{n}, \dots\}$ for integers $n \geq 1$. By (6), a countable union of countable sets is countable, so $\mathbb{Q}$ is countable.
   - Remark: It is also possible to show that $\mathbb{Z} \times \mathbb{Z}$ is countable directly by labeling the points in "spirals" outward from the origin. The countability of $\mathbb{Q}$ can also be established using this method, where we label the points (a,b) in spirals, where a/b is a rational number in lowest terms.
   - Remark: Another way to show that $\mathbb{Q}$ is countable is first to observe that the rational numbers between 0 and 1 are countable, by simply listing them first in order of increasing denominators and then in order of increasing numerators, skipping terms already listed: $\left\{\dfrac{0}{1}, \dfrac{1}{1}, \dfrac{1}{2}, \dfrac{1}{3}, \dfrac{2}{3}, \dfrac{1}{4}, \dfrac{3}{4}, \dfrac{1}{5}, \dfrac{2}{5}, \dfrac{3}{5}, \dfrac{4}{5}, \dfrac{1}{6}, \dfrac{5}{6}, \dots\right\}$. Then we can obtain any rational number merely by including reciprocals and negatives (and negative reciprocals) after each term in the list above: $\left\{\dfrac{0}{1}, \dfrac{1}{1}, -\dfrac{1}{1}, \dfrac{1}{2}, -\dfrac{1}{2}, \dfrac{2}{1}, -\dfrac{2}{1}, \dfrac{1}{3}, -\dfrac{1}{3}, \dfrac{3}{1}, -\dfrac{3}{1}, \dots\right\}$.

- So far we have only given examples of sets that are countable. However, not every set is countable:

- Theorem (Cardinality of Power Set): If S is any set, finite or infinite, then there does not exist a bijection between S and its power set $\mathcal{P}(S)$. In particular, the power set $\mathcal{P}(\mathbb{Z}_{>0})$ is uncountable.
   - Proof: Suppose $f : S \to \mathcal{P}(S)$ is any function. We will show that f cannot be onto, so in particular, f cannot be a bijection.

- Let $A = \{a \in S : a \notin f(a)\}$ be the collection of elements of S that are not an element of their image under f. We claim that A is not in the image of f.
- For any $s \in S$, either $s \in A$ or $s \notin A$.
- If $s \in A$, then by definition of A, $s \notin f(s)$. Hence $f(s) \neq A$ because s is an element of A but not $f(s)$.
- If $s \notin A$, then by definition of A, $s \in f(s)$. Hence $f(s) \neq A$, because s is an element of $f(s)$ but not A.
- In either case, $f(s) \neq A$. Since this holds for every $s \in S$, we conclude $A \notin \text{im}(f)$. Hence f is not onto, so (in particular) is not a bijection.
- Remark: Compare this argument to our analysis of Russell's paradox, in which we established that there is no set of all sets. It uses the same technique of considering sets whose (image) does not contain itself.

- It is also true that the set $\mathbb{R}$ of real numbers is uncountable, as first established by Cantor in 1874:

- Theorem (Uncountability of $\mathbb{R}$): The set $\mathbb{R}$ of real numbers is uncountable. In fact, the set of real numbers in the interval $[0, 1]$ is uncountable.

  - In this proof we will use a few basic facts about decimal expansions of real numbers; in particular, recall that every real number has a decimal expansion, and some real numbers have two decimal representations, such as $1.000\cdots = 0.999\ldots$. More specifically, the real numbers with two decimal expansions are the ones of the form $n/10^k$ where n and k are integers: one representation ends in an infinite string of 0s while the other ends in an infinite string of 9s.
  - Proof: By way of contradiction suppose that the set of real numbers in $[0, 1]$ is countable. Then we may list the elements as $r_1, r_2, r_3, \ldots$.
  - Arrange the decimal expansions of these real numbers in an array as follows:

$$\begin{array}{rcl} r_1 & = & 0.d_{1,1}d_{2,1}d_{3,1}d_{4,1}\ldots \\ r_2 & = & 0.d_{1,2}d_{2,2}d_{3,2}d_{4,2}\ldots \\ r_3 & = & 0.d_{1,3}d_{2,3}d_{3,3}d_{4,3}\ldots \\ r_4 & = & 0.d_{1,4}d_{2,4}d_{3,3}d_{4,4}\ldots \\ \vdots & \vdots & \vdots \end{array}$$

  - Now we construct a real number in $[0, 1]$ that cannot be equal to any of the numbers r_1, r_2, r_3, r_4 using the "diagonal" digits $d_{i,i}$: if $d_{i,i} = 1$, set $e_i = 2$, and if $d_{i,i} = 2$, set $e_i = 1$.
  - We claim the real number $\alpha = 0.e_1e_2e_3e_4\ldots$ cannot be equal to any of the numbers r_i.
  - To see this, first observe that for any i, the ith decimal digit of α differs from the ith decimal digit of r_i. Then because α cannot have two decimal representations and its representation cannot be equal to any decimal expansion of any r_i, we conclude that $\alpha \in [0, 1]$ is a real number not equal to any r_i.
  - This is a contradiction, and therefore the set of real numbers in $[0, 1]$ is countable.
  - Then $\mathbb{R}$ must be uncountable also, since otherwise $[0, 1]$ would be a subset of a countable set and thus countable itself.
  - Remark: This type of argument, first given by Cantor, is known as a diagonalization argument.

4.1.3 Infinite Cardinalities

- We now discuss some other results about infinite sets. We have seen above that there are at least two different "sizes" of infinite sets (namely, countably infinite and uncountably infinite) but in fact there are more:

- Proposition (Infinite Cardinals): There exists an infinite sequence of infinite sets $S_1, S_2, S_3, \ldots$, no two of which are equinumerous.

  - Another way to interpret this result is that there are infinitely many different infinite cardinalities, or more informally, there are infinitely many different infinities.
  - Proof: As we have shown, there does not exist an onto map from a set to its power set.

- Hence if we take $S_1 = \mathbb{Z}_{>0}$, and define $S_n = \mathcal{P}(S_{n-1})$ for each $n \geq 2$, then any map from S_i to S_j with $i < j$ cannot be onto, since an appropriate restriction would necessarily yield an onto map from S_i to $S_{i+1} = \mathcal{P}(S_i)$.
- This means in particular that no two of the infinite sets $S_1, S_2, S_3, \dots$ are equinumerous, as required.

- By definition, two sets have the same cardinality if there is a one-to-one correspondence between them. But it is also natural to want to compare sets of different cardinalities, which we may do using one-to-one functions:

- Definition: If A and B are sets, we say A is dominated by B, written $A \precsim B$, if there exists a one-to-one function $f : A \to B$.

  - The motivation for this definition is the observation that if $f : A \to B$ is one-to-one, then f is a bijection from A to $\mathrm{im}(f) \subseteq B$, and so A is in bijection with a subset of B. This is a reasonable way to capture the idea that B has "at least as many" elements as A.
  - Example: $\{1,2,3\} \precsim \{a,p,q,s\}$ because there exists a one-to-one function $f : \{1,2,3\} \to \{a,p,q,s\}$, such as $f = \{(1,a),(2,p),(3,s)\}$.
  - Example: $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \precsim \mathbb{Z}$ because there exists a one-to-one function $f : \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \to \mathbb{Z}$, namely the explicit map we constructed that gives a bijection of $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ with $\mathbb{Z}_{>0}$.

- Note that we have used the symbol $\precsim$, which suggests that this relation should behave like a partial ordering.

  - Reflexivity follows immediately, because the identity function from A to itself is one-to-one, so $A \precsim A$.
  - Transitivity is also straightforward: if $A \precsim B$ and $B \precsim C$, then there exist one-to-one functions $f : B \to C$ and $g : A \to B$. Then it is straightforward to check that $f \circ g : A \to C$ is also one-to-one, whence $A \precsim C$.
  - However, this relation is not antisymmetric: there are examples of sets A and B with $A \precsim B$ and $B \precsim A$ but with $A \neq B$. For example, $\{1,2\} \precsim \{a,b\}$ and $\{a,b\} \precsim \{1,2\}$, and also $\mathbb{Z} \precsim \mathbb{Q}$ and $\mathbb{Q} \precsim \mathbb{Z}$.
  - However, these examples do suggest that if $A \precsim B$ and $B \precsim A$, then A and B are equinumerous, in which case the relation $\precsim$ is antisymmetric when viewed on cardinalities (i.e., on equivalence classes of equinumerous sets). This turns out to be true, but not so easy to prove:

- Theorem (Cantor-Schröder-Bernstein): Suppose A and B are sets such that there exists an injection from A to B and an injection from B to A. Then there exists a bijection between A and B.

  - The proof of this theorem is somewhat involved, but the overall idea is to consider the one-to-one maps $f : A \to B$ and $g : B \to A$. If f is onto then we are done.
  - Otherwise, we glue together part of f with part of the surjective map $g^{-1} : \mathrm{im}(g) \to B$ to create a one-to-one map $h : A \to B$ that also takes on the values in B that were missing from $\mathrm{im}(f)$. Rather than motivating the construction further, we simply give the proof.
  - Proof: Suppose $f : A \to B$ and $g : B \to A$ are one-to-one. Then g has an inverse function $g^{-1} : \mathrm{im}(g) \to B$ whose image is B.
  - Now define a sequence of sets $A_1, A_2, A_3, \dots$ recursively: take $A_1 = A \backslash \mathrm{im}(g)$, and for each $n \geq 2$, take $A_n = g(f(A_{n-1})) = \{g(f(a)) : a \in A_{n-1}\}$.
  - Also define $X = \bigcup_{n \geq 1} A_n$ and $Y = A \backslash X$, and finally define $h : A \to B$ via $h(a) = \begin{cases} f(a) & \text{if } a \in X \\ g^{-1}(a) & \text{if } a \in Y \end{cases}$.
  - Observe that h is well-defined because X and Y are disjoint by definition, and also that if $a \in Y$ (so that $a \notin X$) then by definition $a \notin A_1$, so $a \in \mathrm{im}(g)$ and thus $g^{-1}(a)$ makes sense.
  - To show that h is one-to-one, suppose $h(a_1) = h(a_2)$.
  - If $a_1, a_2 \in X$ then we would have $f(a_1) = f(a_2)$, but since f is one-to-one, we see $a_1 = a_2$. Likewise, if $a_1, a_2 \in Y$ then we would have $g^{-1}(a_1) = g^{-1}(a_2)$, and then applying g yields $a_1 = a_2$.
  - For the remaining case assume without loss of generality that $a_1 \in X$ and $a_2 \in Y$. Then we would have $f(a_1) = g^{-1}(a_2)$, implying $g(f(a_1)) = a_2$, but this would mean $a_2 \in g(f(X)) = X$, which is a contradiction. Hence this case cannot occur, and so $a_1 = a_2$ in all cases, meaning that h is one-to-one.
  - To show that h is onto, let $b \in B$: then $g(b) \in A$.

- If $g(b) \in Y$, then $h(g(b)) = g^{-1}(g(b)) = b$, so $b \in \text{im}(h)$.
- If $g(b) \in X$, then by definition of X as a union we have $g(b) \in A_n$ for some n.
- In particular since $g(b) \in \text{im}(g)$ we have $n \neq 1$. This means $g(b) \in g(f(A_{n-1}))$, meaning that for some $a \in A_{n-1}$ we have $g(b) = g(f(a))$.
- But then since g is one-to-one this implies $b = f(a) = h(a)$ since $a \in A_{n-1} \subseteq X$, and so we also have $b \in \text{im}(h)$ in this case.
- Hence $b \in \text{im}(h)$ in either cases, so h is onto. Thus, h is a bijection as required.

- The Cantor-Schröder-Bernstein theorem shows that the relation $\precsim$ is a partial ordering on cardinalities.
  - A natural followup question is whether this relation is actually a *total* ordering on cardinalities.
  - Equivalently, we are asking whether any two sets are always comparable under $\precsim$, which is to say, given any two sets, does there necessarily exist an injection from one the other?
  - It turns out that the answer relies on a foundational axiom of set theory known as the axiom of choice, which (in one formulation) states that the Cartesian product of an arbitrary collection of nonempty sets is nonempty.
  - If the axiom of choice is accepted, it can be shown that $\precsim$ is a total ordering on sets: in fact, it is actually true that the axiom of choice is *equivalent* to the statement that $\precsim$ is a total ordering on sets.
- In this formulation (the Cartesian product of an arbitrary collection of nonempty sets is nonempty), the axiom of choice seems like a natural assumption to make, and it is generally accepted by most mathematicians in practical work.
  - There exist many other equivalent formulations of the axiom of choice, some of which seem fairly natural, and others which are less so.
  - Another statement equivalent to the axiom of choice is called Zorn's lemma, which states that every nonempty partially-ordered set having the property that any totally ordered subset has an upper bound (an element greater than or equal to every element of the subset) has a maximal element (an element such that no element is greater than it).
  - A third equivalent to the axiom of choice (familiar to students who have studied linear algebra) is the statement that every vector space has a basis.
  - A fourth equivalent to the axiom of choice is called the well-ordering principle, which states that every set admits a well-ordering (a total ordering in which every nonempty subset has a smallest element).
  - This fact was one of our axioms [N3] for the definition of the integers. However, it is much less intuitive to ask what a well-ordering on the set $\mathbb{R}$ would look like: the usual total ordering $\leq$ is not a well-ordering, because there are many sets, like the open interval $(0, 1)$ or even $\mathbb{R}$ itself, that have no smallest element under $\leq$.
  - It has also been proven that the axiom of choice is independent of the standard Zermelo-Fraenkel axioms of set theory, in the sense that the axioms are consistent provided the axiom of choice is accepted if and only if the axioms are consistent provided the axiom of choice is rejected.

4.2 The Pigeonhole Principle

- We now establish several related facts about cardinality and finite sets that all fall under the umbrella of the so-called "pigeonhole principle". These results are very intuitively natural, but we can give formal proofs using the language we have developed about functions and sets.

4.2.1 Statements of the Pigeonhole Principle

- Proposition (Pigeonhole Principle): Suppose $m > n$. Then there exists no one-to-one function $f : \{1, 2, \dots, m\} \to \{1, 2, \dots, n\}$. More generally, if A and B are finite sets and $\#A > \#B$, then there exists no one-to-one function $f : A \to B$.

- We often phrase this more intuitively as follows: suppose we have m pigeons and we place each pigeon into one of n holes. If $m > n$, then there must be at least one hole that has more than one pigeon. (This particular formulation is the reason for the name "pigeonhole principle".)
- Proof: For the first statement, we show the result by contradiction.
- If f is one-to-one, then f is a bijection between $\{1, 2, \dots, m\}$ and $\text{im}(f)$, and so $\#\text{im}(f) = m$.
- But since $\text{im}(f)$ is a subset of the target set $\{1, 2, \dots, n\}$, we also have $\#\text{im}(f) \le n$, and so $m \le n$.
- This contradicts the assumption that $m > n$, so there cannot exist any such function f.
- The second statement follows simply by replacing $\{1, 2, \dots, m\}$ with the set A and $\{1, 2, \dots, n\}$ with the set B.

- Here are some other formulations of the pigeonhole principle.

- Proposition (Pigeonhole, Set Version): If S is a finite set with $\#S = m$, and $S = S_1 \cup S_2 \cup \dots \cup S_n$ for some $m > n$, then $\#S_i > 1$ for at least one value of i.
  - Proof: Work by contradiction: if $\#S_i \le 1$ for all i, then $\#S = \#(S_1 \cup S_2 \cup \dots \cup S_n) \le \#S_1 + \#S_2 + \dots + \#S_n \le n$, with the latter inequality following by induction using $\#(A \cup B) \le \#A + \#B$.
  - But this is a contradiction since $m > n$. Hence $\#S_i > 1$ for at least one value of i.
  - Alternatively, we could deduce this formulation from the one we gave above by writing $S_i = \{x \in S : f(x) = i\}$, and then observing that $\#S_i > 1$ for some i is equivalent to saying that $f(x_1) = i = f(x_2)$ for two unequal values $x_1, x_2 \in S$, which in turn is the same as saying that f is not one-to-one.

- Proposition (Pigeonhole, Onto Version): If A and B are finite sets and $\#A < \#B$, then there exists no onto function $g : A \to B$.
  - Intuitively, if we have more holes than pigeons, then at least one hole must not have a pigeon in it.
  - Proof: Suppose there did exist an onto function $g : A \to B$. For each $b \in B$, let $S_b = \{x \in A : g(x) = b\}$.
  - Then the sets S_b have union A by the assumption that g is onto, so by the set version of the pigeonhole principle above, at least one set, say g_c has cardinality larger than 1.
  - But this contradicts the assumption that g is a function, because then g would not be well-defined on the element c.

- We can also strengthen the pigeonhole principle as follows:

- Proposition (Average-Value Pigeonhole): If S is a finite set with $\#S = m$, and $S = S_1 \cup S_2 \cup \dots \cup S_n$, then $\#S_i \ge m/n$ for at least one value of i. If S is infinite and $S = S_1 \cup S_2 \cup \dots \cup S_n$, then at least one of the S_i must also be infinite.
  - The intuitive version is that if we place m pigeons into n holes, there must be (at least) one hole that has at least the average number m/n of pigeons in it.
  - Proof: If $\#S = m$ and $\#S_i < m/n$ for all i, then $\#S = \#(S_1 \cup S_2 \cup \dots \cup S_n) \le \#S_1 + \#S_2 + \dots + \#S_n < n \cdot m/n = m$, which contradicts the statement $\#S = m$.
  - The infinite version follows in the same way: if all of the S_i are finite, then by definition there exists a finite number N for which $\#S_i \le N$ (namely, the maximum of all of the cardinalities).
  - Then we would have $\#S \le \#S_1 + \dots + \#S_n = n \cdot N$ which is finite, contradicting the assumption that S is infinite.

- By using the idea of the pigeonhole principle's proof we can establish the following very useful result about functions on finite sets of the same cardinality:

- Proposition (Maps on Same-Cardinality Sets): Suppose A and B are finite sets with of the same cardinality. Then a function $f : A \to B$ is one-to-one if and only if it is onto, if and only if it is a bijection.
  - Proof: Suppose $f : A \to B$ is one-to-one and $\#A = \#B$. Then f is a bijection of A with $\text{im}(f)$, so $\#\text{im}(f) = \#A$. But since $\#B = \#A$ and B is finite, the only possibility is to have $\text{im}(f) = B$. Hence f is onto, as claimed.

- Conversely, suppose $f : A \to B$ is onto. If we take $S_b = \{a \in A : f(a) = b\}$ for each $b \in B$, then the S_b are disjoint, $A = \cup_{b \in B} S_b$, and $\#S_b \geq 1$ for each $b \in B$ (since f is onto).
- Then we can write $\#A = \#B \leq \#S_1 + \cdots + \#S_{\#B} \leq \#A$, meaning that we must have equality everywhere. This means $\#S_b = 1$ for each $b \in B$, and so f is one-to-one.
- Hence f is one-to-one if and only if f is onto. This means either condition is equivalent to both, which is to say, either condition is equivalent to saying f is a bijection.

4.2.2 Examples of the Pigeonhole Principle

- Here are some problems that can be solved by using pigeonhole arguments:
- Example: A sock drawer contains 10 pairs of (identical) white socks, 8 pairs of blue socks, 3 pairs of black socks, and 1 pair of purple socks. What is the least number of socks that need to be taken out (without looking at them) in order to guarantee a matching pair?
  - If we think of the holes as the sock colors and the pigeons as the socks being drawn, the pigeonhole principle says that if we have more pigeons than holes, then at least two pigeons are in the same hole.
  - So if we draw 5 socks, we are guaranteed to have a matching pair since there are only 4 possible colors.
- Example: Show that if 25 people are sitting in a room, then at least 3 of them must share the same birth month (e.g., October).
  - If the holes are the 12 birth months and the pigeons are the 25 people, then by the average-value pigeonhole principle, at least one month has at least $25/12$ people corresponding to it.
  - Since $25/12 > 2$, there must be at least 3 people sharing the same birth month.
- Example: Show that if 51 elements from the set $\{1, 2, 3, \dots, 100\}$ are chosen, then at least one pair of the elements must sum to 101.
  - Observe that there are 50 pairs of elements summing to 101 are $\{1, 100\}$, $\{2, 99\}$, $\{3, 98\}$, ... , $\{50, 51\}$.
  - Thus, if we view the holes as the 50 pairs and the pigeons as the 51 elements being selected, then at least one hole must have 2 pigeons, which is to say, both elements of the pair are chosen.
  - But this means we obtain at least one pair of elements summing to 101, as claimed.
- Example: If a is any integer and m is a modulus, show that there must exist positive integers $p < q$ such that $a^p \equiv a^q \pmod{m}$.
  - Here, we want to look at the values $\{a^1, a^2, a^3, a^4, \dots\}$ modulo m.
  - Since there are only m residue classes modulo m and there are infinitely many different powers $a^1, a^2, a^3, a^4, \dots$, by the infinite version of the pigeonhole principle, some residue class contains infinitely many powers.
  - In particular it has at least 2 powers a^p and a^q, so that $a^p \equiv a^q \pmod{m}$.
- Example: Show that if any five lattice points in the plane (i.e., points whose coordinates are both integers) are chosen, then at least one of the line segments joining one pair of these points has a lattice midpoint.
  - Since the midpoint of (a, b) and (c, d) is $(\frac{a+c}{2}, \frac{b+d}{2})$, the midpoint is a lattice point precisely when $a + c$ and $b + d$ are both even.
  - This is the same as saying that the midpoint is a lattice point precisely when the ordered pairs of residue classes $(\overline{a}, \overline{c})$ and $(\overline{b}, \overline{d})$ modulo 2 are equal.
  - Since there are only $2 \cdot 2 = 4$ possible ordered pairs of residue classes modulo 2, then if we have 5 such ordered pairs, by the pigeonhole principle some two of them must land in the same class. Then the midpoint of that segment is a lattice point, as required.
- Example: Show that if any 51 elements from the set $\{1, 2, 3, \dots, 100\}$ are chosen, then at least one of them must divide another one.

- The idea is to find a way of partitioning the set into subsets that are totally ordered under divisibility: then if two elements are chosen in the same subset, one of them must divide the other.
- One way to do this is to start with an odd integer and repeatedly double it: this gives the 50 sets $\{1, 2, 4, 8, \dots, 64\}$, $\{3, 6, 12, \dots, 96\}$, $\{5, 10, 20, \dots, 80\}$, ... , $\{99\}$.
- Hence by the pigeonhole principle, if we select 51 elements from $\{1, 2, 3, \dots, 100\}$, at least two of them must land in the same of these 50 subsets, and then one of them will divide the other, as claimed.

- Example: Assume (somewhat contrary to reality) that friendship is a symmetric relation, and also that it is irreflexive, so that no one is friends with themself. Show that in any finite collection of people, there must be some pair that have the same number of friends.
  - If there are n people, then each person can have between 0 and $n - 1$ friends, inclusive. This does not allow for applying the pigeonhole principle, since there are n possible numbers of friends and n people.
  - However, it is not actually possible to have both a person with 0 friends and a person with $n - 1$ friends: the person with 0 friends would be friends with nobody, while the person with $n - 1$ friends would be friends with everyone else.
  - Thus, in fact, there are at most $n - 1$ possible numbers of friends for any actual collection of n people. Thus by the pigeonhole principle, there are 2 people with the same number of friends.

- Example: In a group of 6 people, each pair of people is either acquainted or strangers. Show that either there are 3 mutual acquaintances or 3 mutual strangers in the group.
  - Choose any person A and consider their relation to the 5 remaining people in the group.
  - Since each of these 5 people is either an acquaintance or a stranger to A, by the pigeonhole principle, there must be at least 3 people who fall into the same category.
  - If these 3 are all acquantances, then consider their relation to one another: if any pair are acquaintances, then this pair and A form 3 mutual acquaintances. Otherwise, all three are strangers to one another, so they form a set of 3 mutual strangers.
  - The same logic applies if all 3 are strangers: either some pair of them are strangers in which case they and A are 3 mutual strangers, or all 3 are acquainted with one another, so they form a set of 3 mutual acquaintances.
  - Thus in all cases, there are either 3 mutual acquaintances or 3 mutual strangers in the group.
  - Remark: A group of 5 people need not have 3 mutual acquaintances or mutual strangers: if the five people are arranged in a circle and each person is acquainted with the two people next to them (but not the other two) then this arrangement has no set of 3 mutual acquaintances or 3 mutual strangers.

- This type of problem above falls into the area of combinatorial graph theory called Ramsey theory, which (broadly speaking) studies how large a set must be before a particular type of structure must necessarily exist. Here is another result of this type:

- Example: Suppose m and n are positive integers. Show that any sequence of $mn + 1$ distinct real numbers must contain either a strictly increasing subsequence of $m + 1$ numbers or a strictly decreasing subsequence of $n + 1$ numbers.
  - For each integer in the sequence, label it with the ordered pair (a_i, b_i) where a_i is the length of the longest possible increasing subsequence starting with it, and b_i is the length of the longest possible decreasing subsequence ending with it. Note in particular each ordered pair has positive integer entries.
  - If there is no increasing subsequence of length $m + 1$ or longer, all of the first coordinates of the pairs are at most m, and if there is no decreasing subsequence of length $n + 1$ or longer, all of the second coordinates of the pairs are at most n.
  - Therefore there are only mn possible ordered pairs, so since there are $mn + 1$ numbers in the list, by the pigeonhole principle, two elements x_i and x_j with $i < j$ must be labeled with the same ordered pair.
  - But this is a contradiction: if $x_i < x_j$ then appending x_i to the longest increasing sequence starting at x_j gives a longer one for x_i, and if $x_i > x_j$ appending x_j to the longest decreasing sequence ending at x_i gives a longer one for x_j.

- ○ Remark: This result is known as the Erdős-Szekeres theorem. The numbers given are sharp, in the sense that there exists a list of mn numbers with no increasing sequence of length $m+1$ nor decreasing sequence of length $n+1$: one such list consists of the m runs of n decreasing integers $\{n, n-1, n-2, \dots, 1\}$, $\{2n, 2n-1, 2n-2, \dots, n+1\}$, $\{3n, 3n-1, \dots, 2n+1\}$, ... , $\{mn, mn-1, \dots, m(n-1)+1\}$.

- Example: Suppose α is an irrational real number. Show that there exists infinitely many rational numbers p/q such that $|\alpha - p/q| < 1/q^2$.
  - ○ First we recall a basic fact about the real numbers: for any real number x, there exists a unique integer n such that $n \le x < n+1$. (This n is simply the greatest integer less than or equal to x.) As such, for any real number x, we may write $x = n + \{x\}$ where $0 \le \{x\} < 1$. We call this quantity $\{x\}$ the fractional part of x.
  - ○ Now choose any positive integer m, and consider the $m+1$ multiples of α given by 0α, 1α, 2α, ... , $m\alpha$, take each of their fractional parts $\{0\alpha\}$, $\{1\alpha\}$, $\{2\alpha\}$, $\{m\alpha\}$. All of these fractional parts lie in the interval $[0, 1)$.
  - ○ Thus, applying the pigeonhole principle to the k intervals $[0, 1/m$, $[1/m, 2/m)$, ... , $[(m-1)/m, 1)$ and the $k+1$ fractional parts shows that at least one of the intervals must contain two fractional parts.
  - ○ Suppose specifically that one of these intervals contains both $\{q_1\alpha\}$ and $\{q_2\alpha\}$ where $q_1 < q_2$. Then the distance between $\{q_1\alpha\}$ and $\{q_2\alpha\}$ is less than $1/m$, since both of these numbers lie in an interval of length $1/m$, and one of the endpoints is excluded.
  - ○ So this means $-1/m < \{q_2\alpha\} - \{q_1\alpha\} < 1/m$. Writing $q_1\alpha = p_1 + \{q_1\alpha\}$ and $q_2\alpha = p_2 + \{q_2\alpha\}$ then yields $-1/m < (q_2\alpha - p_2) - (q_1\alpha - p_1) < 1/m$, which upon setting $p = p_2 - p_1$ and $q = q_2 - q_1$ is equivalent to $-1/m < q\alpha - p < 1/m$, so that $|q\alpha - p| < 1/m$ and thus $|\alpha - p/q| < 1/(mq)$.
  - ○ But now m is at least as large as $q = q_2 - q_1$, so in fact we have $|\alpha - p/q| < 1/(mq) \le 1/q^2$: this means p/q is one rational number satisfying the requirement. But since m can be arbitrarily as large, and $|\alpha - p/q|$ cannot be zero since α is irrational, there must be infinitely many such p/q.
  - ○ Remark: This result is known as Dirichlet's approximation theorem, and was the first recorded use of the pigeonhole principle in mathematics. The idea is that any irrational number has many good rational approximations, where we measure "good" in terms of how close the approximation is relative to the size of the denominator. The closeness of the rational approximations is much better than that obtained by using a decimal approximation: if we just take p/q to be the decimal expansion of α out to n decimal places, then q will (typically) be 10^n while the error could be as large as $10^{-n} \approx 1/q$.

- One real-world implication of the pigeonhole principle is the following:

- Example: Show that a lossless data compression algorithm (i.e., a function on data sets that does not lose information) cannot guarantee compression for all input data sets (i.e., cannot guarantee that the output of the function has smaller size than the input).
  - ○ Suppose that each file is represented as a string of bits, and that the compression algorithm transforms every file into an output file that has fewer bits.
  - ○ If we let A_N be the set of all files with at most N bits (note that A_N is finite, and in fact $A_N = 2^{N+1} - 1$ if we include the empty file), then if the compression algorithm never increases the size of an input file, it is a function $f : A_N \to A_N$.
  - ○ The statement that the compression algorithm is lossless means that the original data set can always be recovered from its output, which is simply saying that f is one-to-one.
  - ○ But now by our result on same-cardinality sets, this means that $f : A_N \to A_N$ is one-to-one, hence it is a bijection. Since this holds for every N, by an easy induction this means that f must map the files with exactly N bits to themselves, meaning that f cannot actually compress any file.
  - ○ Remark: Another way of phrasing this result is that if a lossless data compression algorithm shortens any one file, then it must lengthen another one.

Well, you're at the end of my handout. Hope it was helpful.