Throughout this set of notes, $X$ and $Y$ are nonempty sets.

Relations are central to mathematics. Here is the basic definition:

A relation from a nonempty set $X$ to a nonempty set $Y$ is any subset of $X \times Y$.

For a relation $R \subseteq X \times Y$, if $(x, y) \in R$ we say that $x$ is related to $y$ through $R$.

Note: An alternative notation to $(x, y) \in R$ is $xRy$.

For any relation $R \subseteq X \times Y$, the domain is the set of $\{x | \exists y \in Y, (x, y) \in R\}$ and the range is the set $\{y | \exists x \in X, (x, y) \in R\}$.

A relation $R \subseteq X \times X$ is called a binary relation on $X$. Often we just say that $R$ is a relation $X$ (dropping the word “binary”).

Examples:

(1) Let $X, Y$ be arbitrary (nonempty) sets and $R = \emptyset$.

(2) Let $X = \{\text{security, certification, wisdom, happiness}\}$, $Y = \{\text{money, time}\}$, and $R = \{(\text{security, money}), (\text{certification, money}), (\text{certification, time}), (\text{wisdom, time})\}$.

(3) Let $X = \{2, 3, 5, 7\}$, $Y = \{4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21\}$, and $R = \{(2, 4), (2, 6), (2, 8), (2, 10), (2, 12), (2, 14), (2, 16), (2, 18), (2, 20), (3, 6), (3, 9), (3, 12), (3, 15), (3, 18), (3, 21), (5, 10), (5, 15), (5, 20), (7, 14), (7, 21)\}$.

(4) Let $X = Y = \{1, 2, 3, 4\}$ and $R = \{(x, y) | x < y\}$. In this case we have defined a binary relation by a condition. Can you list all the elements of $R$?

Two relations $R \subseteq X \times Y$ and $R' \subseteq X' \times Y'$ are equal if $X = X'$, $Y = Y'$, and $xRy$ iff $xR'y$.

Let $R$ be a relation from $X$ to $Y$. The inverse relation is found by reversing the pairs in relation: $R^{-1} = \{(y, x) | (x, y) \in R\}$. The inverse is a relation from $Y$ to $X$.

Note: Whenever it might be useful, one can always draw a relation by plotting curves/points in the $xy$-plane. The $x$-axis represents $X$ and the $y$-axis represents $Y$. 
Let’s solve the following counting problem:

How many binary relations are there on $X$ when $|X| = n \in \mathbb{N}$?

Since a binary relation on $X$ is any subset $R \subseteq X \times X$ we just count the number of subsets of $X \times X$. There are $n^2$ points in $X \times X$. Call them $p_1, p_2, \ldots, p_{n^2}$. Every relation corresponds uniquely to series of decisions to either include or exclude $p_i$ for $i = 1, 2, \ldots, n^2$. Thus by the multiplication principle, there are $2^{n^2}$ binary relations on an $n$-element set $X$.

Using this theory, let’s determine the number of binary relations on $X = \{1, 2, 3\}$. Well, this set has 3 elements so the number of relations is $2^9 = 512$. We wouldn’t want to write them all down!

A relation $R$ on $X$ is **reflexive** if $\forall x \in X, (x, x) \in R$.

A relation $R$ on $X$ is **symmetric** if $\forall x, y \in X, (x, y) \in R \Rightarrow (y, x) \in R$.

A relation $R$ on $X$ is **transitive** if $\forall x, y, z \in X, (x, y), (y, z) \in R \Rightarrow (x, z) \in R$.

A relation $R$ on $X$ is **antisymmetric** if $\forall x, y \in X, (x, y), (y, x) \in R \Rightarrow x = y$.

Can you write the definition of antisymmetric in a contrapositive form to the above?

Lets negate the definition of symmetric:

$$\neg(\forall x, y \in X, (x, y) \in R \Rightarrow (y, x) \in R) \equiv$$

$$\equiv \exists x, y \in X, \neg((x, y) \in R \rightarrow (y, x) \in R) \equiv \exists x, y \in X, ((x, y) \in R) \land ((y, x) \notin R).$$

So a relation $R$ on $X$ is not symmetric if there exists $x, y \in X$ such that $(x, y) \in R$ and $(y, x) \notin R$.

Lets negate the definition of antisymmetric:

$$\neg(\forall x, y \in X, (x, y), (y, x) \in R \Rightarrow x = y) \equiv$$

$$\equiv \exists x, y \in X, \neg((x, y), (y, x) \in R \Rightarrow x = y) \equiv \exists x, y \in X, ((x, y) \in R \land (y, x) \in R) \land x \neq y).$$

So a relation $R$ on $X$ is not antisymmetric if there exists distinct $x, y \in X$ such that $(x, y) \in R$ and $(y, x) \in R$.

VERY IMPORTANT: A relation can be neither symmetric nor antisymmetric, or one but not the other (either way), or both!
Let’s consider some relations on $X = \{1, 2, 3\}$:

Let $R_1 = \{(1, 1), (2, 2)\}$, $R_2 = \{(1, 1), (2, 2), (3, 3)\}$, $R_3 = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$, $R_4 = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$, $R_5 = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (3, 3)\}$, $R_6 = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3)\}$ and $R_7 = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$.

Let’s classify each relation in terms of whether or not they are reflexive, symmetric, transitive, and/or antisymmetric:

$R_1$: This relation is not reflexive (it’s missing $3, 3$). It’s symmetric (for any pair in $R_1$ the reverse pair is in $R_1$ – cause the reverse pair is the same pair). It’s transitive (the only way for $(x, y)$ and $(y, z)$ to be in this relation is for $x = y = z$, in which case $(x, z)$ is in relation). It’s antisymmetric (any $x, y$ where $(x, y), (y, x)$ are both in this relation forces $x = y$).

$R_2$: This relation is clearly reflexive. It’s symmetric (for any pair in $R_2$ the reverse pair is in $R_2$ – cause the reverse pair is the same pair). It’s transitive (the only way for $(x, y)$ and $(y, z)$ to be in this relation is for $x = y = z$, in which case $(x, z)$ is in relation). It’s antisymmetric (any $x, y$ where $(x, y), (y, x)$ are both in this relation forces $x = y$).

$R_3$: This relation is clearly reflexive. It’s not symmetric ($(1, 2)$ is in $R_3$, but the reverse pair $(2, 1)$ isn’t in $R_3$). It’s transitive (for any $x, y, z$ where $(x, y), (y, z)$ are in $R_3$, we have $(x, z)$ in $R_3$). It’s antisymmetric (any $x, y$ where $(x, y), (y, x)$ are both in this relation forces $x = y$).

$R_4$: This relation is clearly reflexive. It’s symmetric (for any pair in $R_4$ the reverse pair is in $R_4$). It’s transitive (for any $x, y, z$ where $(x, y), (y, z)$ are in $R_4$, we have $(x, z)$ in $R_4$). It’s not antisymmetric (we have that $(1, 2), (2, 1)$ are both in this relation, but $1 \neq 2$).

$R_5$: This relation is clearly reflexive. It’s not symmetric ($(1, 3)$ is in $R_5$, but the reverse pair $(3, 1)$ isn’t in $R_5$). It’s transitive (for any $x, y, z$ where $(x, y), (y, z)$ are in $R_5$, we have $(x, z)$ in $R_5$). It’s not antisymmetric (we have that $(1, 2), (2, 1)$ are both in this relation, but $1 \neq 2$).

$R_6$: This relation is not reflexive (it’s missing $(3, 3)$). It’s not symmetric ($(2, 3)$ is in $R_6$, but the reverse pair $(3, 2)$ isn’t in $R_6$). It’s not transitive ($(1, 2)$ and $(2, 3)$ are in $R_6$, but $(1, 3)$ isn’t in $R_6$). It’s not antisymmetric (we have that $(1, 2), (2, 1)$ are both in this relation, but $1 \neq 2$).

$R_7$: This relation is clearly reflexive. It’s symmetric (for any pair in $R_7$ the reverse pair is in $R_7$). It’s not transitive ($(1, 2)$ and $(2, 3)$ are in $R_7$, but $(1, 3)$ isn’t in $R_7$). It’s not antisymmetric (we have that $(1, 2), (2, 1)$ are both in this relation, but $1 \neq 2$).
Let’s classify the following relations given by conditions in terms of whether it is reflexive, symmetric, transitive, and/or antisymmetric:

(i) Let $R \subseteq \mathbb{R} \times \mathbb{R}$ be given by $(x, y) \in R$ if $y \leq x^2$.

$R$ is not reflexive: Consider that $(0.5, 0.5) \notin R$ as $0.5 > 0.25 = 0.5^2$.

$R$ is not symmetric: Consider that $(2, 1) \in R$, but $(1, 2) \notin R$.

$R$ is not transitive: Consider that $(2, 4), (4, 16) \in R$, but $(2, 16) \notin R$.

$R$ is not antisymmetric: Consider that $(-1, 0), (0, -1) \in R$, but $-1 \neq 0$.

(ii) Let $S \subseteq \mathbb{N} \times \mathbb{N}$ be given by $(m, n) \in S$ if $m$ divides $n$ (equivalently, $n$ is divisible by $m$).

$S$ is reflexive: For all $n \in \mathbb{N}$, $(n, n) \in S$ since $n = 1 \cdot n$, so $n$ divides $n$.

$S$ is not symmetric: Consider that $(2, 6) \in S$ since $6 = 3 \cdot 2$, but $(6, 2) \notin S$ as $2$ is not a multiple of $6$.

$S$ is transitive: Let $m, n, p \in \mathbb{N}$ and assume that $(m, n), (n, p) \in S$. Then $\exists j, k \in \mathbb{N}$ such that $n = jm$ and $p = kn$. Then since $p = (kj)m$ and $kj \in \mathbb{N}$ we have that $(m, p) \in S$.

$S$ is antisymmetric: Let $m, n \in \mathbb{N}$ and assume that $(m, n), (n, m) \in S$. Then $\exists j, k \in \mathbb{N}$ such that $n = jm$ and $m = kn$. Then $m = (kj)m$, which implies that $kj = 1$, and thus $j = k = 1$. Hence $m = n$.

(iii) Let $T \subseteq \mathbb{Z} \times \mathbb{Z}$ be given by $(k, j) \in T$ if $(k - j)$ is a multiple of $5$.

$T$ is reflexive: For all $k \in \mathbb{Z}$, $(k, k) \in T$ since $k - k = 0$ which is a multiple of $5$.

$T$ is symmetric: Let $k, j \in \mathbb{Z}$ and assume $(k, j) \in T$. Then $k - j = 5m$ for some $m \in \mathbb{Z}$. But then $j - k = 5(-m)$ is a multiple of $5$, and hence $(j, k) \in T$.

$T$ is transitive: Let $k, j, \ell \in \mathbb{Z}$ and assume $(k, j), (j, \ell) \in T$. Then $\exists m, n \in \mathbb{Z}$ such that $k - j = 5m$ and $j - \ell = 5n$. Adding these together yields $k - \ell = 5(m + n)$, which is a multiple of $5$, so $(k, \ell) \in T$.

$T$ is not antisymmetric: Consider that $(5, 0), (0, 5) \in T$, but $0 \neq 5$. 
Theorem: Let \( X \) be a nonempty set and \( R, S \subseteq X \times X \). If \( R \) and \( S \) are symmetric then \( R \cup S \) is symmetric.

Proof: Assume \( R, S \) are symmetric. Let \( x, y \in X \). Assume \((x, y) \in R \cup S\). Let’s proceed by cases:

Suppose \((x, y) \in R\). Then we have \((y, x) \in R\) since \( R \) is symmetric.

Now suppose \((x, y) \notin R\). Then \((x, y) \in S\). Then \((y, x) \in S\) since \( S \) is symmetric.

Hence \((y, x) \in R \cup S\) in either case □

The above theorem doesn’t hold with “symmetric” replaced by “antisymmetric.” Here is a counterexample:

Let \( X = \{1, 2\} \), \( R = \{(1, 2)\} \), and \( S = \{(2, 1)\} \). Then \( R, S \) are antisymmetric, but \( R \cup S \) isn’t

The above theorem also doesn’t hold with “symmetric” replaced by “transitive.” The same counterexample works.

The following two definitions are central to the study of relations:

Let \( X \) be a nonempty set.

If a relation \( R \subseteq X \times X \) is reflexive, symmetric, and transitive, then it is called an equivalence relation. Given an equivalence relation \( R \) we often just write \( a \sim_R b \) or just \( a \sim b \) instead of \((a, b) \in R\) or \( aRb \).

If a relation \( R \subseteq X \times X \) is reflexive, antisymmetric, and transitive, then it called a partial order under which \( X \) is a partially ordered set (POSET). Given a partial order \( R \) we often write \( a \leq b \) instead of \((a, b) \in R\) and \( a < b \) when \( a \leq b \) and \( a \neq b \).

Considering examples on the previous page, we have that the relation \((\text{ii})\) where naturals \( m, n \) are related (in that order) if \( m \) divides \( n \) is a partial order and the relation \((\text{iii})\) where integers \( i, j \) are related if 5 divides \((i - j)\) is an equivalence relation.

Let \( S \) be a finite set and \( X = \mathcal{P}(S) \) (the power set of \( X \)).

Consider the following two relations on \( X \):

(i) \( R \) given by \((A, B) \in R\) if \(|A| = |B|\).

This relation is obviously reflexive, symmetric, and transitive. So it is an equivalence relation.

(ii) \( R' \) given by \((A, B) \in R'\) if \( A \subseteq B \).

This relation is obviously reflexive, antisymmetric, and transitive. So it is a partial order.
Let $X$ be a nonempty set and $R \subseteq X \times X$.

Let $a \in X$. Define $[a] = \{x \in X | (a, x) \in R\}$. If $R$ is an equivalence relation it’s called the equivalence class of $a \in X$ (aka congruence class).

**Theorem:** Let $X$ be a nonempty set and $R \subseteq X \times X$. If $R$ is an equivalence relation $\sim$ on $X$ then the set of equivalence classes, $S = \{[a] | a \in X\}$, is a partition of $X$.

**Proof:** Suppose $R$ is an equivalence relation. Consider $S = \{[a] | a \in X\}$, which is nonempty by construction. Let $A \in S$. Then $A = [a]$ for some $a \in X$. Since $R$ is reflexive, $a \sim a$, and hence $a \in A$. So $A \neq \emptyset$. This also justifies that $\bigcup_{A \in S} A = X$.

It remains to show that the sets in $S$ are pairwise disjoint.

Suppose $A = [a]$ and $B = [b]$ where $a, b \in X$. Two cases arise. Either $a \sim b$ or $a \not\sim b$.

Let’s suppose $a \sim b$. In this case we have that $b \sim a$, since $R$ is symmetric. We want to show that $[a] = [b]$. Assume $x \in [a]$. Then $a \sim x$ and $x \sim a$ (using symmetry). Together with $b \sim a$ this yields $b \sim x$ as $\sim$ is transitive. Hence $x \in [b]$, which implies that $[a] \subseteq [b]$. A symmetric argument shows that $[b] \subseteq [a]$. Hence $[a] = [b]$.

Now let’s suppose $a \not\sim b$. (TYAC) Suppose $[a] \cap [b] \neq \emptyset$. Let $c \in [a] \cap [b]$. Then $a \sim c$ and $b \sim c$. Then $c \sim b$ by symmetry, and thusly $a \sim b$ by transitivity. This contradiction implies $[a] \cap [b] = \emptyset$. That completes the proof $\square$

**Theorem:** Let $X$ be a nonempty set. If $S$ is partition of $X$ then $R \subseteq X \times X$ given by $aRb$ if $a, b \in A$ for some $A \in S$ is an equivalence relation on $X$.

**Proof:** Assume $S$ is a partition of $X$ and let $R \subseteq X \times X$ be given by $aRb$ if $a, b \in A$ for some $A \in S$.

Suppose $x \in X$. Then $x \in A$ for some $A \in S$. Then $(x, x) \in R$. So $R$ is reflexive.

Suppose $x, y \in X$ and $(x, y) \in R$. Then $x, y$ both belong to $A$ for some $A \in S$. But then so do $y, x$. Hence $(y, x) \in R$, showing $R$ is symmetric.

Now suppose $x, y, z \in X$ and $(x, y), (y, z) \in R$. Then $x, y$ both belong to $A$ and $y, z$ both belong to $A'$ for some $A, A' \in S$. Since $y$ belongs to both $A = A'$. Hence $x, z$ both belong to $A$. So $(x, z) \in R$ showing $R$ to be transitive; thus $R$ is an equivalence relation $\square$

Let $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Let’s determine the equivalence classes in $X$ of the equivalence relation $a \sim b$ if $(a - b)$ is div. by 5:

Consider the following relation on \( \mathbb{Z} \times \mathbb{Z} \):

\[(a, b) R (c, d) \text{ if } b = d = 0 \lor (ad = bc \land b \neq 0 \land d \neq 0).\]

This relation is reflexive: Let \( a, b \in \mathbb{Z} \). If \( b = 0 \) then \((a, b) R (a, b)\). Suppose \( b \neq 0 \). Then \((a, b) R (a, b)\) since \( ab = ba \).

This relation is symmetric: Let \( a, b, c, d \in \mathbb{Z} \) and assume \((a, b) R (c, d)\). If \( b = 0 \) then \( d = 0 \) implying that \((c, d) R (a, b)\). Suppose \( b \neq 0 \). In this case we have \( d \neq 0 \) and \( ad = bc \). But then \( cb = da \) with \( d \neq 0 \) and \( b \neq 0 \) so \((c, d) R (a, b)\).

This relation is transitive: Let \( a, b, c, d, e, f \in \mathbb{Z} \) and assume \((a, b) R (c, d)\) and \((c, d) R (e, f)\). If \( b = 0 \) then \( d = 0 \) and \( f = 0 \) implying that \((a, b) R (e, f)\). Suppose \( b \neq 0 \). Then \( d \neq 0 \) and \( ad = bc \). Then \( f \neq 0 \) and \( cf = de \). Then \( adf = bcf = bde \) implies \( adf - bde = 0 \) which becomes \((af - be)d = 0 \). Since \( d \neq 0 \) we get \( af = be \) and hence \((a, b) R (e, f)\).

So this is an equivalence relation \( \sim \) on \( \mathbb{Z} \times \mathbb{Z} \) (formally giving us that for \( a, b, c, d \in \mathbb{Z} \), \( a/b = c/d \) in \( \mathbb{Q} \) if \( b \neq 0 \), \( d \neq 0 \) and \( (a, b) \sim (c, d) \)).

Consider the partial order \( R \) on \( X = \mathcal{P} \{1, 2, 3\} \) given by \((A, B) \in R\) if \( A \subseteq B \). We will write \( A \leq B \) for \((A, B) \in R \). Consider that we have the following in relation:

\[\emptyset \leq S \text{ for all } S \in X.\]

\[\{1\} \leq S \text{ for } S = \{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}.\]

\[\{2\} \leq S \text{ for } S = \{2\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}.\]

\[\{3\} \leq S \text{ for } S = \{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}.\]

\[\{1, 2\} \leq S \text{ for } S = \{1, 2\}, \{1, 2, 3\}.\]

\[\{1, 3\} \leq S \text{ for } S = \{1, 3\}, \{1, 2, 3\}.\]

\[\{2, 3\} \leq S \text{ for } S = \{2, 3\}, \{1, 2, 3\}.\]

And \(\{1, 2, 3\} \leq \{1, 2, 3\}\).

For any POSET we have a Hasse Diagram: All the elements of the set on which \( \leq \) is a partial order are points and lines segments join the points such that if there is an upward path from point \( p \) to point \( q \) then \( p \leq q \). Let’s draw this for the POSET above.

Let \( X \) be a POSET under \( \leq \). For any \( x, y \in X \) where \( x \leq y \) or \( y \leq x \) we say that \( x, y \) are comparable under the partial order. Notice that \( \{1, 2\} \) and \( \{1, 3\} \) are not comparable under the partial order in the POSET above. When two elements of a POSET are not in relation in either order, we say they are incomparable under the partial order.
If $X$ is a POSET under $\leq$ and every pair of elements $x, y \in X$ is comparable, we call $X$ a totally ordered set and $\leq$ a total order on $X$.

For example, the set $\mathbb{R}$ under the standard inequality partial order $x \leq y$ is a totally ordered set!

ELFY: Explain why the standard inequality $\leq$ is indeed a partial order on $\mathbb{R}$.

Suppose $X$ is a nonempty set that is a POSET under a partial order $\leq$.

An element $m \in X$ is a greatest element (aka a maximum) of $X$ if $\forall x \in X, x \leq m$.

An element $m \in X$ is maximal if $\forall x \in X$, if $m \leq x$ then $m = x$.

ELFY: Define minimum and minimal.

Consider the POSET $\{1, 2, 3, ..., 10\}$ under the partial order $x \leq y$ if $y$ is divisible by $x$ (ELFY: Show this is indeed a partial order). Clearly for $x \leq y$ it must be the case that $x$ is smaller or equal to $y$ (I know, confusing if you don’t understand that $\leq$ means something else here). It is also clear that 9 and 10 are not comparable. So there is no maximum (it could only be 10, but it’s not). However, we have maximal elements: 10, 9, 8, 7, and 6.

ELFY: Draw a Hasse diagram for this POSET.

**Theorem:** Let $X$ be a nonempty set that is a POSET under a partial order $\leq$. We can use the notation $(X, \leq)$ for this. The following hold:

(i) If $X$ has a maximum then it is unique.

(ii) If $X$ has a maximum then it is maximal.

(iii) If $\leq$ is a total order on $X$ then if $X$ has a maximal element it is a maximum (and hence unique).

**Proof:** Let’s start with (i). Suppose $a, b \in X$ are both maximum elements of $X$ under $\leq$. Since $a$ is a maximum, $b \leq a$. Since $b$ is a maximum $b \leq a$. Since $\leq$ is antisymmetric, $a = b$.

(ii) is pretty straightforward. Suppose $a \in X$ is a maximum (really, the maximum by part (i)). Let $x \in X$. Assume $a \leq x$. But then $x \leq a$ since $a$ is the maximum, and hence $a = x$ since $\leq$ is antisymmetric. So $a$ is maximal.

Now consider (iii). Assume $\leq$ is a total order. Suppose $a \in X$ be maximal. Thus for all $x \in X$ if $a \leq x$ then $a = x$. Let $x \in X$. Since $\leq$ is a total order either $a \leq x$ or $x \leq a$. The former implies $a = x$ since $a$ is maximal. Hence either way, $x \leq a$. So $a$ is the maximum.
Let $R_1$ be a relation from $Y$ to $Z$ and $R_2$ be a relation from $X$ to $Y$. The composition of $R_1$ and $R_2$ is $R_1 \circ R_2 = \{ (x, z) \in X \times Z \mid \exists y \in Y, ((x, y) \in R_2) \land ((y, z) \in R_1) \}$.

Example: Let $X = \{1, 2, 3, 4\}$ and consider the binary relation $R = \{ (1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4) \}$ and the binary relation $S = \{ (1, 2), (1, 4), (2, 1), (2, 3), (3, 2), (3, 4), (4, 1), (4, 3), (4, 4) \}$ (both are binary relations on $X$).

Then $R \circ S = \{ (1, 2), (1, 4), (2, 1), (2, 2), (2, 3), (2, 4), (3, 2), (3, 4), (4, 1), (4, 2), (4, 3), (4, 4) \}$.

This is not the same as $S \circ R = \{ (1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 3), (3, 2), (3, 4), (4, 1), (4, 3) \}$.

A matrix is a nice way to represent a relation $R$ between $X$ and $Y$. The rows of the matrix are labeled by the elements of $X$ in some arbitrary fixed order, and the columns of the matrix are labeled by the elements of $Y$ in some arbitrary fixed order. The entry in row $x$ and column $y$ is 1 if $xRy$ and 0 otherwise. This is called the matrix of the relation.

For example, let $X = \{a, b\}$, $Y = \{1, 2, 3\}$, and $R = \{ (a, 1), (a, 2), (b, 2), (b, 3) \}$. Using alphabetical and numerical order for the rows and columns respectively, the matrix of this relation is

$$
\begin{pmatrix}
1 & 1 & 0 \\
0 & 1 & 1
\end{pmatrix}
$$

Suppose $X = \{1, 2, 3\}$. Consider the following matrix:

$$
\begin{pmatrix}
1 & 1 & 0 \\
1 & 1 & 0 \\
0 & 0 & 1
\end{pmatrix}
$$

ELFY: Assuming the standard numerical order on $X$ for the rows/columns write the ordered pairs of the relation on $X$ that has this matrix. Is it an equivalence relation?

Note: The transpose of an $m \times n$ matrix $A$ is the $n \times m$ matrix found by swapping rows for columns (or vice versa). For example the transpose of $\begin{pmatrix}
1 & 1 & 0 \\
0 & 1 & 1
\end{pmatrix}$ is $\begin{pmatrix}
1 & 0 \\
1 & 1 \\
0 & 1
\end{pmatrix}$. The transpose of a matrix $A$ is denoted $A^T$ When a square $n \times n$ matrix equals it’s own transpose the matrix is called symmetric.
Theorem: Let $R_1$ be a relation from $Y$ to $Z$ and $R_2$ be a relation from $X$ to $Y$. Fix orderings of $X, Y, Z$. Let $A_1$ be the matrix of $R_1$ and $A_2$ be the matrix of $R_2$ (with respect to the fixed orderings). Then the matrix of $R_1 \circ R_2$ is found by replacing all nonzero entries in $A_2A_1$ by 1.

Proof: Recall the if $A$ is an $m \times n$ matrix and $B$ is an $n \times r$ matrix then $AB$ is an $m \times r$ matrix, and for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, r$ the $(i,j)$-entry of $AB$ is the dot product of row $i$ of $A$ with column $j$ of $B$ (both of which have $n$ components).

Let $x \in X$ and $z \in Z$. Consider row $x$ of $A_2$ and column $z$ of $A_1$. If 1 is found in some position $y$, of both row $x$ and column $z$, then the $(x, z)$ entry of $A_2A_1$ is non-zero. In that case, $(x, y) \in R_2$ and $(y, z) \in R_1$, so $(x, z) \in R_1 \circ R_2$. Otherwise, the $(x, z)$ entry is 0, and $\forall y \in Y, (x, y) \not\in R_2 \lor (y, z) \not\in R_1$. That completes the proof □

Consider $X = Y = Z = \{a, b\}$, $R_1 = \{(a, a), (a, b), (b, a)\}$ and $R_2 = \{(a, b), (b, a), (b, b)\}$.

Then $R_1 \circ R_2 = \{(a, a), (b, a), (b, b)\}$.

In matrices:

$$
\begin{pmatrix}
0 & 1 \\
1 & 1
\end{pmatrix}
\begin{pmatrix}
1 & 1 \\
1 & 0
\end{pmatrix} =
\begin{pmatrix}
1 & 0 \\
2 & 1
\end{pmatrix} \equiv
\begin{pmatrix}
1 & 0 \\
1 & 1
\end{pmatrix}
$$

Given an $n \times n$ matrix $A$ of a relation $R \subseteq X \times X$ where $X$ has $n$ elements (under some fixed ordering) how can we tell if the relation is reflexive, symmetric, antisymmetric, and/or transitive?

Reflexive: If all the main diagonal entries $a_{11}, a_{22}, \ldots, a_{nn}$ are all 1’s then $R$ is reflexive. If any of these main diagonal entries is not 1 then $R$ is not reflexive.

Symmetric: If the matrix is symmetric (equals its own transpose) then $R$ is symmetric. Otherwise, $R$ is not symmetric.

Antisymmetric: If $a_{ij} + a_{ji} = 2$ for some distinct pair $i, j \in \{1, 2, \ldots, n\}$ then $R$ is not antisymmetric. Otherwise, $R$ is antisymmetric.

Transitive: This is trickier. We will address this with a theorem (on the next page).
Theorem: A relation $R$ on a nonempty finite set $X$ is transitive if and only if the matrix $A$ of the relation satisfies the following condition:

If the $(i, j)$-entry of $A^2$ is non-zero then the $(i, j)$ entry of $A$ is non-zero.

Proof: Let’s fix an ordering $x_1, x_2, ..., x_n$ on $X$ and let $A$ be the matrix of a relation $R \subseteq X \times X$. Suppose $R$ is transitive on $X$. Assume the $(i, j)$-entry of $A^2$ is non-zero. Then there exists $x_k \in X$ such that $(x_i, x_k), (x_k, x_j) \in R$. But then $(x_i, x_j) \in R$ since $R$ is transitive, and thus the $(i, j)$-entry of $A$ is 1.

Now assume that if the $(i, j)$-entry of $A^2$ is non-zero then the $(i, j)$-entry of $A$ is non-zero. (TYAC) Suppose $R$ is not transitive. Then there exists $x_i, x_j, x_k \in X$ such that $(x_i, x_k), (x_k, x_j) \in R$, but $(x_i, x_j) \notin R$. Then the $(i, j)$-entry of $A$ is zero while the $(i, j)$-entry of $A^2$ is non-zero. That contradicts our assumption. So $R$ must be transitive □

Recall that we already know that there are $2^{n^2}$ relations on an $n$-element set $X$. Now let’s consider the following counting problems:

(1) How many symmetric relations are there on an $n$-element set $X$?

Well, this is equivalent to counting how many symmetric $n \times n$ matrices there are using only 1’s and 0’s. There are two choices for what to insert into every entry on or above the main diagonal (by symmetry, the entries $a_{ij}$ below the main diagonal must satisfy $a_{ij} = a_{ji}$).

So how many entries are there on or above the main diagonal? There are $(n^2 - n)/2$ entries above the main diagonal and $n$ on the main diagonal. Hence there are $n + (n^2 - n)/2 = (n^2 + n)/2$ entries on or above the main diagonal. So by the multiplication principle, the number of symmetric relations on an $n$-element set $X$ is $2^{(n^2+n)/2}$.

(2) How many reflexive relations are there on an $n$-element set $X$?

This is equivalent to counting how many $n \times n$ matrices have 1’s along the main diagonal. There are two choices for what to insert into every entry off the main diagonal and $n^2 - n$ such entries. So by the multiplication principle, the number of reflexive relations on an $n$-element set is $2^{n^2 - n}$.

(3) How many relations on an $n$-element set $X$ are symmetric and antisymmetric? What about symmetric, but not antisymmetric?

Well, the matrix a relation that is symmetric and antisymmetric must have all 0’s off the main diagonal. So there are two choices for what to insert into every main diagonal entry. So by the multiplication principle, there are $2^n$ relations that are both symmetric and antisymmetric. By subtraction, there are $2^{(n^2+n)/2} - 2^n$ relations on an $n$-element set that are symmetric, but not antisymmetric.

(4) How many relations on an $n$-element set $X$ are reflexive, symmetric, and antisymmetric?

Just one! The identity relation $\text{Id}$ which has the identity matrix $I_n$ as its matrix.
6.1-6.3 Functions

Let $X$ and $Y$ be non-empty sets. A function $f$, from $X$ to $Y$ (denoted $f : X \to Y$) is a subset of $X \times Y$ having the following property:

$$\forall x, \exists! y, (x, y) \in f.$$  

$X$ is the **domain** and $Y$ the **codomain**. The set $f(X) = \{ y \in Y | \exists x \in X, (x, y) \in f \} \subseteq Y$ is the range of $f$. For each $x \in X$, the image of $x$ is the unique $y$ such that $(x, y) \in f$. So the range is the set of images. Sometimes we say the image of $f$ for the range.

A function is a special kind of relation. It is a relation whose domain is $X$ and for each $x \in X$ there is exactly one $y \in Y$ such that $(x, y)$ is in the relation.

One can think of a function as a rule that assigns to each member of a set $X$ exactly one member a set $Y$. So a function is a set of ordered pairs where $(x, y)$ belongs to the function if the function assigns $x$ to $y$. We often use the shorthand notation $y = f(x)$ for $(x, y) \in f$. In this convention we write things like $f(x) = x^2 + 1$ as shorthand for the function \{(x, x^2 + 1) | x \in \mathbb{R}\}.

Let $f : X \to Y$ be a function and $S \subseteq Y$ be nonempty. The set $f^{-1}(S) = \{ x \in X | (x, y) \in f, \exists y \in S \}$ is called the **pre-image** of $S$. If $S = \{ y \}$ then we just say it’s the pre-image of $y$ and write $f^{-1}(y)$.

One can draw the arrow diagram of a function $f$: Draw two ovals, one for $X$ and one for $Y$ and label points within the ovals for each set’s elements. From each point $x$ in the $X$ oval, draw an arrow from $x$ to the unique $y$ that satisfies $(x, y) \in f$.

Each element in $X$ is represented by a point in a plane and an arrow points from $x_1$ to $x_2$ if $(x_1, x_2)$ is in the function.

Let’s solve the following counting problem:

How many functions are there from an $m$-element domain to an $n$-element codomain?

Well, there are $n$ choices for the image of each of the $m$ points in the domain. So by the multiplication principle, there are $n^m$ functions from an $m$-element domain to an $n$-element codomain.
Examples of functions:

(1) Let $X = Y = \{1, 2, 3, 4\}$ and $f = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$. Describe the range. What’s the pre-image of $\{2, 3\}$?

(2) Let $X = \{a, b, c\}$, $Y = \mathbb{R}$ and $g = \{(a, e), (b, \pi), (c, \sqrt{2})\}$. Describe the range. What’s the pre-image of $Q$?

(3) The real square root function: $h : [0, \infty) \to \mathbb{R}$ given by $h(x) = \sqrt{x}$ (non-negative number whose square is $x$). Describe the range. What’s the pre-image of 9?

(4) Consider the function $\ell : \mathbb{N} \to \mathbb{N}$ given by $\ell(n) = 2n - 1$. Describe the range. What’s the pre-image of 3?

(5) Any sequence of terms in a set $D$ is a function from the index set $\{n_0, n_1, \ldots\} \subseteq \mathbb{Z}$ to $D$. For example the sequence $a_n = n!$ for $n = 0, 1, 2, \ldots$ is equivalent to the function $\mu : \{0, 1, 2, \ldots\} \to \mathbb{N}$ where $\mu(n) = n!$.

ELFY: Consider the relation $R = \{(x, y) | x, y \in \mathbb{R}$ and $x = y^2\}$. Why is this not a function?

Modulus operator: If $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ then define $m \mod n$ to be the remainder when $m$ is divided by $n$.

For a fixed $n \in \mathbb{N}$, the modulus operator is a function $f_n : \mathbb{Z} \to \mathbb{Z}$ where $f(m) = m \mod n$.

Consider these calculations:

(1) $5 \mod 3 = 2$.

(2) $1991 \mod 5 = 1$.

(3) $-11 \mod 7 = 3$.

What day of the week will it be 365 days from Friday? Hint: $350 = 7(50)$.

Well, $365 \mod 7 = 1$. It will be a Saturday!

**Theorem:** Let $j, k \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $(j + k) \mod n = [(j \mod n) + (k \mod n)] \mod n$.

**Proof:** Assume the remainders of $j, k$ when divided by $n$ are $a, b$ respectively. So $\exists \ell, \ell' \in \mathbb{Z}$ such that $j = \ell n + a$ and $k = \ell' n + b$. Then $j + k = (\ell + \ell') n + (a + b)$ and hence the remainder of $j + k$ when divided by $n$ is the same as for $a + b$. Therefore $(j + k) \mod n = (a + b) \mod n = [(j \mod n) + (k \mod n)] \mod n \square$
Theorem: Let $j, k \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then $(jk) \mod n = [(j \mod n)(k \mod n)] \mod n$.

Proof: Assume the remainders of $j, k$ when divided by $n$ are $a, b$ respectively. So $\exists \ell, \ell' \in \mathbb{Z}$ such that $j = \ell n + a$ and $k = \ell' n + b$. Then $jk = (\ell n + a)(\ell' n + b) = (\ell \ell' n + \ell b + \ell' a)n + (ab)$ and hence the remainder of $jk$ when divided by $n$ is the same as for $ab$. Therefore $(jk) \mod n = (ab) \mod n = [(j \mod n)(k \mod n)] \mod n$ □

With these new tools we can make calculations easier! What day of the week will it be 20 years from Friday? Here we have to account for leap years, 5 of them. That gives us $20 \cdot 365 + 5$ days.

Then $(20 \cdot 365 + 5) \mod 7$ reduces to $(6 \cdot 1 + 5) \mod 7$ which equals 4. It will be a Tuesday!

Here are important “step” functions:

The floor (or greatest lower integer) function assigns to each real number the largest integer less than or equal to that number.

The ceiling (or least higher integer) function assigns to each real number the least integer greater than or equal to that number.

A function $f : X \to Y$ is one-to-one or 1-1 if for each $y \in Y$ there exists at most one $x \in X$ such that $y = f(x)$. The function $f$ is surjective or onto if for each $y \in Y$ there exists at least one $x \in X$ such that $y = f(x)$. The function $f$ is bijective or a bijection if it is 1 − 1 and onto.

In terms of pre-images, a function is 1 − 1 when the pre-image of each point in the codomain has at most 1 element, and onto when the pre-image of each point in the codomain has at least 1 element.

Note: Sometimes we say $f$ is a surjection (or surjective) or an injection (or injective) when it’s onto and 1 − 1 respectively.

Let $X$ be all OSU students and employees. Let $Y$ be the set of 9-digit strings. There is a function from $X$ to $Y$ which assigns to each person in $X$ an identification number in $Y$. Is this function 1 − 1?

It is! Each 9-digit string relates to at most one person in $X$. No two people in $X$ are assigned the same number (since any new ID number is always chosen outside the range of the existing ID numbers).

Is this function onto?

No, since the cardinality of $X$ is less than the number of possible 9-digit strings (1 billion).
To prove $f : X \to Y$ is $1 - 1$, let $x_1, x_2 \in X$ be arbitrary and prove $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.

To prove $f : X \to Y$ is not $1 - 1$, find $x_1, x_2 \in X$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.

To prove $f : X \to Y$ is onto, let $y \in Y$ be arbitrary and find $x \in X$ such that $y = f(x)$.

To prove $f : X \to Y$ is not onto, find $y \in Y$ such that for all $x \in X$, $y \neq f(x)$.

Examples:

(1) Let $X = Y = \{1, 2, 3\}$. Let $f = \{(1, 2), (2, 3), (3, 1)\}$. Is $f$ $1 - 1$? Onto? A bijection?

(2) Let $X = \{1, 2, 3\}$ and $Y = \{a, b\}$. Let $g = \{(1, a), (2, a), (3, b)\}$. Is $g$ $1 - 1$? Onto? A bijection?

(3) Let $h : \mathbb{N} \to \mathbb{N}$ be defined by $h(n) = n + 1$. Is $h$ $1 - 1$? Onto? A bijection?

(4) Let $k : \mathbb{N} \to \mathbb{N}$ be defined by $k(1) = k(2) = 1$ and for $n \geq 3$, $k(n) = n - 1$. Is $k$ $1 - 1$? Onto? A bijection?

(5) Let $X = \mathbb{R} - \{0\}$ and $Y = \mathbb{R}$. Let $r : X \to Y$ be defined by $r(x) = \frac{1}{x}$. Is $r$ $1 - 1$? Onto? A bijection? What if we delete $\{0\}$ from the codomain?

Consider the function $f : \mathbb{N} \to \mathbb{Q}$ given by $f(n) = \frac{n}{1 + n^2}$. Let’s determine if this function is $1 - 1$, onto, and/or a bijection.

Let $m, n \in \mathbb{N}$ and suppose $f(m) = f(n)$. Then $\frac{m}{1 + m^2} = \frac{n}{1 + n^2} \Rightarrow m + mn^2 = n + nm^2 \Rightarrow (m - n) = nm^2 - mn^2 = mn(m - n) \Rightarrow (m - n)(1 - mn) = 0 \Rightarrow m = n$ or $mn = 1$.

Suppose $mn = 1$. Since $m, n \in \mathbb{N}$ this means $m = 1 = n$. So either way $m = n$. Hence $f$ is $1 - 1$.

Consider that $\forall m \in \mathbb{N}$, $1 + m^2 > m$ so $\frac{m}{1 + m^2} < 1$. Hence $f$ is not onto as in particular $f^{-1}(1) = \emptyset$.

Here is a nice counting problem:

How many onto functions are there from a 5-element set to a 4-element set?

An onto function from a set with 5 elements to a set of 4 elements must assign exactly two of the 5 points to one of the four points. Then the remaining three points in the domain can be paired bijectively with the remaining three points in the codomain. Thus by the multiplication principle there are $C(5, 2)4! = 240$ such onto functions.
Theorem: Suppose $f$ is a bijection from $X$ to $Y$. Consider the inverse relation $g = \{(y, x) | (x, y) \in f\}$. We shall show $g$ is a bijection from $Y$ to $X$.

Proof: First lets show it is a function. Let $y \in Y$. Since $f$ is onto, there exists $x \in X$ such that $(x, y) \in f$. Then $(y, x) \in g$. Now let $x' \in X$. Suppose $(y, x') \in g$. Then $y = f(x')$. Since $f$ is an inverse, $y = f(x) = f(x')$ implies $x = x'$. So $g$ assigns to each $y \in Y$ exactly one $x \in X$ and therefore it is a function.

Now lets show $g$ is a bijection. Let $y, y' \in Y$ and suppose $(y, x), (y', x) \in g$. Then $(x, y), (x, y') \in f$. Since $f$ is a function, $y = y'$, which makes $g$ a 1-1 function. Now let $x \in X$. Since $f$ is a function there exists $y \in Y$ such that $(x, y) \in f$. Then $(y, x) \in g$, so $g$ is onto and therefore a bijection.

Such a function $g$ is called an inverse function. It swaps domain and range for bijections. It swaps $x$ and $y$. Notation: $g = f^{-1}$. Clearly $(f^{-1})^{-1} = f$:

$$(f^{-1})^{-1} = \{(x, y) | (y, x) \in f^{-1}\} = \{(x, y) | (x, y) \in f\}.$$

Careful: Context tells that this is either the inverse function notation or just the pre-image notation. For this notation to be the inverse function notation, the function MUST BE A BIJECTION. Otherwise, it’s just the pre-image notation, unless we specify that we are talking about the inverse relation of a non-bijection function (in which case this will be specified).

1. Let $a > 0$ and $a \neq 1$. Consider the bijection $f : \mathbb{R} \to (0, \infty)$ given by $f(x) = a^x$.

What is the inverse function? We call the logarithm base $a$ function and give it the following notation:

$$f^{-1}(x) = \log_a(x).$$

So $(x, a^x) \in f \Rightarrow (a^x, x) \in f^{-1} \Rightarrow \log_a(a^x) = x$.

Also, since $(f^{-1})^{-1} = f$, $(x, \log_a(x)) \in f^{-1} \Rightarrow (\log_a(x), x) \in f \Rightarrow a^{\log_a(x)} = x$.

2. Let $X = Y = \mathbb{R} - \{0\}$ and $g : X \to Y$ be given by $g(x) = \frac{1}{x}$. What is $g^{-1}(x)$?
Let $X, Y, Z$ be sets. Let $f : Y \to Z$ and $g : X \to Y$ be functions. The composition of $f$ with $g$, denoted $f \circ g$, is the function from $X$ to $Z$ defined by

$$(f \circ g)(x) = f(g(x)).$$

Note: This is the same as the composition of $f, g$ viewed purely as relations (a concept already defined).

First, let’s justify that this is a function: Let $x \in X$. Then $g(x) \in Y$ and $f(g(x)) \in Z$. Since $g(x)$ is the only member of $Y$ corresponding to $x$ and $f(g(x))$ is the only member of $Z$ corresponding to $g(x)$, $f(g(x))$ is the only element of $Z$ corresponding to $x$.

Let $X = Y = \{a, b, c\}$. Let $f = \{(a, a), (b, c), (c, b)\}$ and $g = \{(a, b), (b, c), (c, a)\}$. Then $f \circ g = \{(a, c), (b, b), (c, a)\}$.

Let $X = Y = \mathbb{R}$. Let $f(x) = 2x + 1$ and $g(x) = x^{\frac{1}{3}}$. Find rules for $f \circ g$ and $g \circ f$.

Let $f : Y \to Z$ and $g : X \to Y$ are functions. Suppose $g$ is one-to-one. Is $f \circ g$ one-to-one?

No: Suppose $g = \{(1, a), (2, b), (3, c)\}$ and $f = \{(a, \alpha), (b, \beta), (c, \beta)\}$.

What if $f \circ g$ is known to be $1 − 1$? Would $g$ be? What about $f$?

Well, it turns out that $g$ must indeed be $1 − 1$: Suppose $f \circ g$ is $1 − 1$. Consider $g(x) = g(x')$. Then since $f$ is a function $f(g(x)) = f(g(x'))$. Since $f \circ g$ is $1 − 1$ this implies that $x = x'$, and hence $g$ is $1 − 1$.

However, $f$ need not: Consider the function $f : \{0, 1\} \to \{0\}$ given by $f(0) = f(1) = 0$. Clearly $f$ is not $1 − 1$. Consider the function $g : \{0\} \to \{0, 1\}$ given by $g(0) = 0$. Then $f \circ g : \{0\} \to \{0\}$ clearly is $1 − 1$.

ELFY: Show that if $f \circ g$ is onto then $f$ must also be onto, but $g$ need not be.

Lemma: Let $X$ be a finite nonempty set and $n = |X|$. Let $Y$ be a nonempty set. Then for every function $f : X \to Y$, $|f(X)| \leq |X|$.

Proof: Let’s use induction on $n$. Suppose $n = 1$. Then $X = \{x\}$ and for any function $f : X \to Y$, by the definition of a function we get that $f = \{(x, y)\}$ for some $y \in Y$. Hence $f(X) = \{y\}$ and $|f(X)| \leq |X|$, so the base case holds. Let $n \in \mathbb{N}$. Assume for any $n$-element set $Z$ a function $f : Z \to Y$ satisfies $|f(Z)| \leq |Z|$. Let $X$ be an $(n + 1)$-element set and $f : X \to Y$. Let $x \in X$. Set $Z = X \setminus \{x\}$, which is an $n$-element set. Let $g : Z \to Y$ be given by $g(z) = f(z)$. By induction $|g(Z)| \leq |Z|$ and by construction $|Z| = |X| − 1$. By looking at the ranges of $f$ and $g$ we get that $f(X) = f(Z) \cup \{f(x)\} = g(Z) \cup \{f(x)\}$. Putting this all together, $|f(X)| = |g(Z) \cup \{f(x)\}| \leq |Z| + 1 = |X|$ □
**Theorem:** Let $X$ be a finite nonempty set and $n = |X|$. Let $Y$ be a finite set with $m = |Y|$. If $m < n$ then for every function $f : X \to Y$, $f$ is not $1-1$. Equivalently, if $f : X \to Y$ is $1-1$ then $m \geq n$.

**Proof:** Suppose $X = \{x_1, x_2, ..., x_n\}$ and $Y = \{y_1, y_2, ..., y_m\}$ where $m < n$. Assume $f$ is a function from $X$ to $Y$. Consider that $f(x_1), f(x_2), ..., f(x_n) \in \{y_1, y_2, ..., y_m\}$. By the pigeonhole principle, since $m < n$ there exists (at least one) $k \in \{1, 2, ..., m\}$ such that $y_k = f(x_i) = f(x_j)$ some pair of distinct $i, j \in \{1, 2, ..., n\}$. Thus $f$ is not $1-1$. □

**Theorem:** Let $X, X'$ be a finite nonempty sets with equal numbers of elements and $n = |X| = |X'|$. Then for any function $f : X \to X'$, $f$ is $1-1$ iff $f$ is onto.

**Proof:** Clearly the theorem is true when $n = 1$ as any function from a 1-element set to a 1-element set is both $1-1$ and onto.

Let $n \geq 2$ be an integer and let $f$ be a function from $X$ to $X'$ where both are $n$-element sets.

Assume $f$ is $1-1$. Set $R = f(X)$ (the range of $X$). The function $g : X \to R$ given by $g(x) = f(x)$ is $1-1$ since $f$ is $1-1$; $g$ is also onto by construction.

It suffices to show $R = X'$ (and thus $f$ would be onto). Suppose otherwise. Then the function $g : X \to R$ cannot be $1-1$ as $|R| < n = |X|$. This contradiction implies $R = X'$, and so $f$ is onto.

Now assume $f$ is not $1-1$. We want to show that $f$ is not onto. Suppose otherwise (that is, suppose $f$ is onto).

Since $f$ is not $1-1$ there exists a distinct pair $a, b \in X$ such that $f(a) = f(b)$. Consider the function $g : X \setminus \{a\} \to X'$ given by $g(x) = f(x)$. By construction this function would still be onto as $g(X \setminus \{a\}) = f(X) = X'$. Then since $g$ is a function $|X'| = |g(X \setminus \{a\})| \leq |X \setminus \{a\}| < |X'|$. This contradiction completes the proof. □

Suppose $g : X \to X'$ is a function that is not $1-1$ between finite nonempty sets $X, X'$.

Consider the following algorithm:

If $g$ is not $1-1$ then proceed to find a distinct pair $a_1, b_1 \in X$ such that $g(a_1) = g(b_1)$ and then construct $g_1 : X \setminus \{a_1\} \to X'$ by the rule $g_1(x) = g(x)$.

For $k = 1, 2, ..., n$ while $g_k$ is not $1-1$ find a distinct pair $a_{k+1}, b_{k+1} \in X \setminus \{a_1, a_2, ..., a_k\}$ such that $g_k(a_{k+1}) = g_k(b_{k+1})$ and then construct $g_{k+1} : X \setminus \{a_1, ..., a_{k+1}\} \to X'$ by the rule $g_{k+1}(x) = g_k(x)$.

At some point this recursive process terminates (since $|X|$ is finite). It terminates with a $1-1$ function $g_k$ from a domain of at least one element (any function from a 1-element set is $1-1$) to a codomain $X'$ of $n \geq 1$ elements. Restricting the codomain to $g_k(X)$ makes a bijection!
An set $X$ is countable if either $X$ is finite or there exists a bijection $f : X \to \mathbb{N}$ (equivalently, a bijection $g : \mathbb{N} \to X$). Otherwise, the set is uncountable (and necessarily infinite).

For an infinite set $X$ we may say that $X$ is countably infinite if countable or uncountably infinite if not countable.

Obviously the naturals are countable (just use the identity function).

**Theorem:** Any subset of a countable set $X$ is countable.

**Proof:** If $X$ is finite then clearly any subset of $X$ is finite and hence countable. So assume that $X$ is countably infinite. Let $S$ be a subset of $X$. If $S$ is finite then we are done. So assume $S$ is infinite. Since $X$ is countable, there is a bijection $f : \mathbb{N} \to X$ such that $X = \{f(1), f(2), \ldots\}$. Since $S$ is infinite the following process constructs a subsequence of $f(1), f(2), \ldots$ Let $s_1 = f(k_1)$ where $k_1$ satisfies being the minimum of the set $I = \{i \in \mathbb{N} | f(i) \in S\}$ (first term of the list $f(1), f(2), \ldots$ that is in $S$). Let $s_2 = f(k_2)$ where $k_2$ satisfies being the minimum of the set $I \setminus \{k_1\}$ (second term of the list $f(1), f(2), \ldots$ that is in $S$). Let $s_3 = f(k_3)$ where $k_3$ satisfies being the minimum of the set $I \setminus \{k_1, k_2\}$ (third term of the list $f(1), f(2), \ldots$ that is in $S$). Continuing in this way we get the infinite subsequence $s_1, s_2, \ldots$ and for distinct $i, j \in \mathbb{N}$ $s_i \neq s_j$ by construction. Then $g : \mathbb{N} \to S$ given by $g(n) = s_n$ is a bijection, implying that $S$ is countable $\square$

**Theorem:** Any infinite set has a subset that is countably infinite.

**Proof:** Let $X$ be an infinite set. Obviously there exists $x_1 \in X$. Let $n \in \mathbb{N}$. Suppose $x_1, x_2, \ldots, x_n$ are pairwise distinct elements of $X$. Since $X$ is infinite, there exists $x_{n+1} \in X$. By mathematical induction it follows that given $x_1, x_2, \ldots, x_n$ pairwise distinct elements of $X$ we can always find an $(n + 1)^{st}$ element distinct from the previous $n$. In this way we can construct a subset $\{x_1, x_2, \ldots\}$ that is obviously countably infinite $\square$

Let $X$ be a set. We know from a theorem on the previous page that if $X$ is a finite set then every $1 - 1$ function $f : X \to X$ is also onto. Call this statement $P$.

$P$ can be reformulated in an equivalent way: If there exists a $1 - 1$ function $f : X \to X$ that is not onto, then $X$ is an infinite set. Furthermore, if there is a $1 - 1$ function $f : X \to X$ that is not onto, then for $S = f(X) \subset X$, $g : X \to S$ given by $g(x) = f(x)$ is $1 - 1$ and onto.

Hence $P$ can be reformulated into another equivalent form:

If there is a bijection $f : X \to S$ where $S$ is a proper subset of $X$ then $X$ is infinite. Call this statement $Q$.

The converse also holds: Suppose $X$ is an infinite set. Let $S = \{x_1, x_2, \ldots\}$ be a countably infinite subset of $X$. 

Define \( f : X \to X \setminus \{x_1\} \) by the rule
\[
 f(x) = \begin{cases} 
 x & \text{if } x \in X \setminus S \\
 x_{i+1} & \text{if } x = x_i \in S 
\end{cases}
\]

Let’s show that \( f \) is 1 – 1: Suppose \( a, b \in X \) and \( f(a) = f(b) \). Then \( a, b \in S \) or \( a, b \in X \setminus S \) since \( f(S) = \{f(s) | s \in S\} \subseteq S \) and \( f(X \setminus S) = \{f(t) | t \in X \setminus S\} \subseteq X \setminus S \). If \( a, b \in S \) then \( a = x_i \) and \( b = x_j \) for some \( i, j \in \mathbb{N} \). Since \( f(a) = f(b) \) this implies \( x_{i+1} = x_{j+1} \) and hence \( i = j \) and \( a = b \). If \( a, b \in X \setminus S \) then \( f(a) = f(b) \) implies \( a = b \). So \( f \) is 1 – 1.

Let’s show that \( f \) is onto: Suppose \( x \in X \setminus \{x_1\} \). If \( x \in X \setminus S \) then \( f(x) = x \). If \( x \in S \) then \( x = x_j \) for some integer \( j \geq 2 \). Then \( f(x_{j-1}) = x \). So \( f \) is onto.

To summarize, we have just proven the following theorem: \( X \) is an infinite set iff there is a bijection from \( X \) to a proper subset of \( X \). \( \square \)

Let \( A = \{m \in \mathbb{Z} | \exists k \in \mathbb{Z}, m = 2k + 1\} \) and consider \( f : \mathbb{Z} \to A \) given by \( f(n) = 2n + 1 \).

ELFY: Show that this function is a bijection.

**Theorem:** \( \mathbb{Z} \) is countable.

**Proof:** Let \( f : \mathbb{Z} \to \mathbb{N} \) be given by
\[
 f(n) = \begin{cases} 
 2n + 1 & \text{if } n \geq 0 \\
 -2n & \text{if } n < 0 
\end{cases}
\]

\( f \) is onto: Let \( m \in \mathbb{N} \). Suppose \( m \) is even. Then \( \exists k \in \mathbb{N} \) such that \( m = 2k \). Then \( -k \in \mathbb{Z} \) and \( m = f(-k) \). Suppose \( m \) is odd. Then \( \exists k \in \mathbb{N}_0 \) such that \( m = 2k + 1 \). Then \( k \in \mathbb{Z} \) and \( m = f(k) \).

\( f \) is 1 – 1: Let \( a, b \in \mathbb{Z} \) and \( f(a) = f(b) \). We get that \( a, b \) aren’t both non-negative and aren’t both negative since in those cases \( f(a) = f(b) \) implies there is an integer that is both even and odd. Hence either \( a, b \) are both non-negative or both negative.

Suppose both are negative. Then \( f(a) = f(b) \) implies \( -2a = -2b \) and hence \( a = b \).

Suppose both are non-negative. Then \( f(a) = f(b) \) implies \( 2a + 1 = 2b + 1 \) and hence \( a = b \). \( \square \)
Lemma: The union of two countable sets is countable.

Proof: Let \( X, Y \) be countable sets. If both are finite then obviously \( X \cup Y \) is finite, and thus countable. Assume at least one is infinite. Without loss of generality assume it is \( X \) that is infinite and that \( X \cap Y = \emptyset \) (since we can replace \( X \) with \( X \setminus Y \) and \( Y \) with \( Y \setminus X \), and that preserves the union). Then \( X \) is countably infinite and so there exists a bijection \( f : \mathbb{N} \to X \). So \( X = \{ f(1), f(2), \ldots \} \). For convenience, let’s denote \( f(n) \) by \( x_n \).

Two cases arise: \( Y \) is finite or countably infinite.

Suppose \( Y = \{ y_1, y_2, \ldots, y_n \} \). Then define \( g : \mathbb{N} \to X \cup Y \) by the rule \( g(i) = \begin{cases} y_i & \text{if } i \leq n \\ x_{i-n} & \text{if } i > n \end{cases} \).

Clearly \( g \) is onto by construction: \( \forall z \in X \cup Y \) if \( z \in Y \) then \( g(i) = y_i = z \) for some \( i \in \{1, 2, \ldots, n\} \) and if \( z \in X \) then \( z = x_i \) for some \( i \in \mathbb{N} \) and hence \( g(i + n) = x_{(i+n)-n} = x_i = z \).

It also follows that \( g \) is 1–1: For any \( i, j \in \mathbb{N} \), \( g(i) = g(j) \) implies either \( g(i), g(j) \in Y \) or \( g(i), g(j) \in X \) since \( X \cap Y = \emptyset \). If the former is the case, then \( y_i = y_j \), implying \( i = j \). If the latter is the case, \( x_{i-n} = x_{j-n} \), implying \( i = j \). So \( g \) is a bijection as desired.

Now suppose \( Y = \{ y_1, y_2, \ldots \} \) is countably infinite (with a bijection \( h : \mathbb{N} \to Y \) given by \( h(k) = y_k \)). Then define \( g : \mathbb{N} \to X \cup Y \) by the rule \( g(i) = \begin{cases} \frac{x_i}{2} & \text{if } i \text{ is even} \\ \frac{y_i+1}{2} & \text{if } i \text{ is odd} \end{cases} \).

This function is onto since for \( x \in X \) we have \( x = x_j \) for some \( j \in \mathbb{N} \), hence \( g(2j) = x \), and for \( y \in Y \) we have \( y = y_k \) for some \( k \in \mathbb{N} \), hence \( g(2k-1) = y \). Let’s show it’s 1–1. Let \( i, j \in \mathbb{N} \) and assume \( g(i) = g(j) \). Since \( X \cap Y = \emptyset \), it must be the case that either \( i, j \) are both even or both odd. In the former case, \( g(i) = g(j) \) implies \( x_{i/2} = x_{j/2} \) and hence \( i = j \). In the latter case, \( g(i) = g(j) \) implies \( y_{(i+1)/2} = y_{(j+1)/2} \) and hence \( i = j \). So \( g \) is a bijection as desired.

The proof is complete \( \Box \)

Theorem: \( \mathbb{N} \times \mathbb{N} \) is countable.

Proof: Let \( A = \{ (m, n) \in \mathbb{N} \times \mathbb{N} | m \leq n \} \) and \( B = \{ (m, n) \in \mathbb{N} \times \mathbb{N} | m \geq n \} \). Clearly \( A \cup B = \mathbb{N} \times \mathbb{N} \). Also, there is an obvious bijection from \( A \) to \( B \) that maps \( (i, j) \in A \) to \( (j, i) \in B \).

So it suffices to show that \( A \) is countable. Let’s systematically list the element so \( A \):

\[(1, 1), (1, 2), (2, 2), (1, 3), (2, 3), (3, 3), \ldots \]

Let \( f : A \to \mathbb{N} \) be given by \( f(m, n) = \frac{(n-1)n}{2} + m \) (for convenience we write \( f(m, n) \) for \( f((m, n)) \)). For instance, \( f(1, 1) = 0 + 1 = 1 \), \( f(1, 2) = 1 + 1 = 2 \), \( f(2, 2) = 1 + 2 = 3 \), \( f(1, 3) = 3 + 1 = 4 \), \( f(1, 3) = 3 + 2 = 5 \), \( f(1, 3) = 3 + 3 = 6 \), etc...

So it only remains to show that \( f \) is a bijection.
Let’s show $f$ is onto: Let $k \in \mathbb{N}$. If $k = 1 + 2 + 3 + \cdots + m$ for some $m \in \mathbb{N}$ then $k = \left[1 + 2 + \cdots + (m - 1)\right] + m = \frac{(m - 1)m}{2} + m = f(m, m)$ and $(m, m) \in A$.

Suppose $k \neq 1 + 2 + 3 + \cdots + m$ for all $m \in \mathbb{N}$. Then $1 + 2 + \cdots + n - 1 < k < 1 + 2 + \cdots + n$ for some $n \in \mathbb{N}$. So $k = 1 + 2 + \cdots + (n - 1) + m$ where $m \in \{1, 2, \ldots, n - 1\}$. So $(m, n) \in A$ and $k = f(m, n)$. Hence $f$ is onto.

Let’s show that $f$ is $1 - 1$: Let $k \in \mathbb{N}$. Suppose $0 < m \leq n$ are integers and $k = f(m, n) = \frac{(n - 1)n}{2} + m$. Then $
\frac{(n - 1)n}{2} + 0 < \frac{(n - 1)n}{2} + m \leq \frac{(n - 1)n}{2} + n = \frac{n(n + 1)}{2}.$

So $n$ is the uniquely determined as the least integer satisfying $\frac{n(n + 1)}{2} \geq k$. Then $m$ is uniquely determined by $m = k - \frac{(n - 1)n}{2}$. Thus $k = f(m, n)$ for exactly one $(m, n) \in A$. So $f$ is $1 - 1$.

That completes the proof $\Box$

**Theorem:** $\mathbb{Q}$ is countable.

**Proof:** Let $\mathbb{Q}^+ = \{q \in \mathbb{Q} | q > 0\}$ and $\mathbb{Q}^- = \{q \in \mathbb{Q} | q < 0\}$. Let’s justify that it suffices to show that $\mathbb{Q}^+$ is countable: There is an obvious bijection from $\mathbb{Q}^+$ to $\mathbb{Q}^-$ given by mapping $q \in \mathbb{Q}^+$ to $-q \in \mathbb{Q}^-$. So if $\mathbb{Q}^+$ is countable then so is $\mathbb{Q}^-$. Then since the union of countable sets is countable, we would get that $\mathbb{Q}^* = \mathbb{Q}^+ \cup \mathbb{Q}^-$ is countable and hence $\mathbb{Q} = \mathbb{Q}^* \cup \{0\}$ is countable.

We systematically list all the symbols $\frac{a}{b}$ where $a, b \in \mathbb{Z}^+$ (this includes all the rationals with repetition):

\[1 \ 2 \ 1 \ 1 \ 2 \ 3 \ 4 \ 3 \ 2 \ 1 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \]
\[\frac{1}{1} \ \frac{1}{2} \ \frac{2}{2} \ \frac{3}{3} \ \frac{2}{1} \ \frac{1}{1} \ \frac{2}{3} \ \frac{3}{4} \ \frac{4}{5} \ \frac{5}{6} \ \frac{6}{2} \ \frac{3}{2} \ \frac{2}{1} \ \frac{1}{1} \ \cdots\]

How are we doing this? Imagine an infinite matrix with the symbol $\frac{i}{j}$ in row $i$, column $j$.

Run through this matrix by assigning 1 to the $(1, 1)$-entry, going down to assign 2 to the $(2, 1)$-entry, then diagonally up to assign 3 to the $(1, 2)$-entry, then to the right to assign 4 to the $(1, 3)$-entry, then diagonally down assigning 5 to the $(2, 2)$-entry and then 6 to the $(1, 3)$-entry, then down assigning 7, then diagonally up assigning 8, 9, 10, then right assigning 11, then diagonally down assigning 12, 13, 14, 15, then down assigning 16, etc...

This construction provides a bijection between the set of symbols $\frac{a}{b}$ such that $a, b \in \mathbb{Z}^+$ and $\mathbb{N}$. Since $\mathbb{Q}^+$ is a subset of this set of symbols (including only those in lowest terms) and a subset of a countable set is countable, we get that $\mathbb{Q}^+$ is countable, and hence that $\mathbb{Q}$ is countable $\Box$
Theorem: $\mathbb{R}$ is uncountable.

Proof: Let’s prove it by contradiction. Suppose the real numbers are countable, which means there is a correspondence with the natural numbers (we can list all the real numbers). This means we have a sequence $r_1, r_2, ...$ such that every real number appears exactly once. Tossing out all the reals not in the interval $(0, 1)$ would give a subsequence $r_{k_1}, r_{k_2}, ...$ where $k_1, k_2, ...$ is an increasing sequence of naturals such that every real in $(0, 1)$ appears exactly once. So if the reals are countable, then so is the interval $(0, 1)$.

In particular, that means that every decimal expansion of every real number in $(0, 1)$ can be put into an infinite matrix row by row, where the first column represents the tenths, the second column represents the hundredths, and so it goes:

\[
\begin{pmatrix}
  a_{11} & a_{12} & a_{13} & \cdots \\
  a_{21} & a_{22} & a_{23} & \cdots \\
  \vdots & \vdots & \vdots & \ddots
\end{pmatrix}
\]

But then consider the following decimal expansion of a real number in $(0, 1)$:

\[0.b_1b_2b_3\cdots\ 	ext{where for } i = 1, 2, 3... \text{ we have } b_i = a_{ii} + 1 \mod 10.\]

This represents a real number not found in any row of the matrix because in particular it does not match on the diagonal entry. This contradiction implies the reals are uncountable $\blacksquare$