Define \( F : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \) by
\[
f(mn) = m + n
\]
and \( g : \mathbb{Z} \rightarrow \mathbb{N} \) by
\[
g(n) = n^2 + 1
\]

Then:
\[
g \circ F(2, 3) = g(F(2, 3))
\]
\[
= g(1 + 3)
\]
\[
= g(4) = 4^2 + 1 = 17
\]

In general:
\[
g \circ F(mn) = g(F(mn))
\]
\[
= g(m + n)
\]
\[
= (m + n)^2 + 1
\]

Observe \( g \circ F : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{N} \).

The identity function:

Define \( \text{id}_A \) as a set. The identity function on \( A \), denoted \( \text{id}_A \), is defined by:
\[
\text{id}_A : A \rightarrow A
\]
\[
\text{id}_A (x) = x
\]
E.g. if \( A = \{(*)_0, \Delta \} \) then \( (dA: A\to A) \) is
\[
(dA = \{(*, *), (\square, \square), (\Delta, 0) \})
\]

**Defn:** a function \( F: A\to B \) is called **invertible** if there is a function \( g: B\to A \) such that \( g \circ F = \text{id}_A \) i.e. \( (\forall x \in A) \ g(F(x)) = x \) and \( F \circ g = \text{id}_B \) i.e. \( (\forall y \in B) \ F(g(y)) = y \)

When \( g \) exists, it is called the **inverse** of \( F \), and denoted \( F^{-1} \)

Ex: Consider \( f: \mathbb{R}\to \mathbb{R} \) defined by \( f(x) = 2x + 1 \).
Let \( g: \mathbb{R}\to \mathbb{R} \) be defined by \( g(x) = \frac{x-1}{2} \).
Observe: \((\forall x \in \mathbb{R}) \ g(f(x)) = g(2x+1) = \frac{(2x+1)-1}{2} = x\)

hence: \(g \circ f = \text{id}_\mathbb{R}\)

also: \((\forall x \in \mathbb{R}) \ f(g(x)) = f(\frac{x-1}{2}) = 2(\frac{x-1}{2}) + 1 = x\)

hence: \(f \circ g = \text{id}_\mathbb{R}\).

thus: \(f\) is invertible - it's inverse \(f^{-1} = g\).

Note: not all functions are invertible!

In fact:

**Theorem** a function \(f: A \to B\) is invertible \(\text{iff} f\) is a bijection

**Proof** (\(\Rightarrow\)) Suppose \(f\) is invertible and let \(g = f^{-1}\) be its inverse.

\(\Rightarrow f\) is a bijection
(Surjectivity): \[ \text{Fix } y \in B \]
- \[ y = g(y) \]
- \[ \text{Then: } f(x) = f(g(y)) = y \]

Since \( y \in B \) was arbitrary, \( f \) is surjective.

(Injectivity): \[ \text{Fix } x, y \in A \text{ and suppose } f(x) = f(y) \]
- \[ \text{Then } g(f(x)) = g(f(y)) \]
- \[ \text{Hence } x = y \quad (g \circ f = \text{id}_A) \]

Since \( x, y \in A \) were arbitrary, \( f \) is injective.

\( \Leftarrow \) Suppose now that \( f : A \rightarrow B \) is a bijection.

\[ \text{This implies } f \text{ is invertible.} \]

Define: \( g = \{(b, a) \in B \times A \mid (a, b) \in f^{-1}\} \)

Claim: \( g \) is a function from \( B \) to \( A \)
- \( 1 \) \( g \) is a function from \( B \) to \( A \)
- \( 2 \) \( g = f^{-1} \)
Proof: \( \forall b \in B \ \exists \text{unique } a \in A \text{ s.t. } (b, a) \in S \).

- So fix \( b \in B \).

**Existence:** Since \( f \) is surjective, \( \exists a \in A \text{ s.t. } f(a) = b \), i.e. \((a, b) \in S\).

- Hence \((b, a) \in S\), by definition of \( S \).

**Uniqueness:** Suppose there is a' \in A \text{ s.t. } (b, a') \in S as well.

- Then must be that \((a', b) \in S\).
- i.e. \( f(a') = b \).
- But then \( f(a') = f(a) \). Since \( f \) is injective, this implies \( a = a' \).

Hence \( S \) is proved.

2. \( \text{wts: } g = f^{-1} \) i.e. \( g \circ f = \text{id}_A \) \( f \circ g = \text{id}_B \).

- So fix \( a \in A \).
- Let \( b = f(a) \), so that \((a, b) \in S\).
- Then \((b, a) \in S\), i.e. \( g(b) = a \).

Hence \( g(f(a)) = g(b) = a \).

- Since \( a \) was arbitrary, \( g \circ f = \text{id}_A \).
We can sometimes use them to prove a given $f$ is a bijection.

**Example:**

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = 2x + 1$.

- **Pf:**
  - We checked down: if $g(x) = 2x + 1$ then $g^{-1}(x) = \frac{x - 1}{2}$.
  - Hence $g$ is a bijection.

Now, since $f$ is an arbitrary function, $f(g(x))$ is also a function of $x$.

Thus, if $g(b) = a$, then $f(a) = b$.

Hence $f$ is a bijection.

---

Note that fixing $a = g(b)$, we get $f(c) = b$. 

---

Since $b = f^{-1}(c)$, as claimed.
Infinity:
The concept of cardinality:
- We would say that \([*, 0, 0]_3\) has 3 elements, or is of size 3.
- Why? By counting it:
  \([*, 0, 0]_3\)
  1 2 3
- In doing so, we are implicitly defining a bijection between \([1, 2, 3]\) and \([*, 0, 0]_3\).

- We could've counted differently:
  \([*, 0, 0]_3\)
  2 3 1

- Generalizing this idea: We'll say two sets have the same size if there is a bijection between them.
We say that two sets $A$, $B$ have the same cardinality, and write $A \sim B$, iff there is a bijection $f : A \rightarrow B$.

Note: In set theory courses, one defines, for every set $A$, the cardinal number $|A|$. One then proves: $A \sim B$ (if $|A| = |B|$) (e.g. $|\mathbb{R} \times \mathbb{Q}| = |\mathbb{Z} \times \mathbb{Q}| = 3$).

- Defining cardinal $\#s$ beyond our scope: for $\#s$ $|A| = |B|$ just means $A \sim B$.

i.e. $f : A \rightarrow B$ a bijection.

Properties of $\sim$:
1. For any set $A$, $id_A : A \rightarrow A$ is a bijection (why?).
   - Hence $A \sim A$, i.e. $\sim$ is reflexive.
2. If $f : A \rightarrow B$ is a bijection, then $f^{-1} : B \rightarrow A$ is a bijection too (why?).
   - Hence if $A \sim B$ then $B \sim A$.
   - i.e. $\sim$ is symmetric.
3. On how you show: if \( f: A \rightarrow B \) and \( g: B \rightarrow C \) are bijections, then \( g \circ f: A \rightarrow C \) is a bijection.

- Hence if \( A \sim B \) and \( B \sim C \) then \( A \sim C \), i.e. \( \sim \) is transitive.
- \( \circ \circ \circ \circ \circ \) show \( \sim \) is an equiv. relation on sets.

So most interesting when the sets being compared are infinite.

Ex. 5: 1. \( \{1,2,3\} \sim \{\ast, 0, \Delta\} \) since \( f = \{ (1, \ast), (2, 0), (3, \Delta) \} \) is a bijection.

2. Let \( -N \) denote the set \( \{ -1, -2, -3, \ldots \} \)

Define \( f: N \rightarrow -N \) by:

\[
f(n) = -n
\]

- To check: \( f \) is a bijection.

- Hence \( N \sim -N \).

3. We showed before: \( f: \mathbb{Z} \rightarrow N \) defined by:

\[
f(n) = \begin{cases} 2n & n > 0 \\ 2n + 1 & n \leq 0 \end{cases}
\]

is a bijection, Hence \( \mathbb{Z} \sim \mathbb{N} \).