Another example: Suppose we want to prove $2^n \geq n^2 \quad \forall \ n \geq 4$

This is actually pretty easy to prove by induction (exercise – do it) but just for fun we will prove it using PMCE.

Proof: Let $m$ be the minimal counter-example

Observe that $2^4 \geq 4^2$, so 4 is not a counter-example. Thus $m \geq 5$

$\Rightarrow m - 1 \geq 4$

(Rationale for this: we are going to use 3 pieces of information:
- $m - 1 \geq 4$
- $m - 1$ is not a counter-example
- $m$ is a counter-example
to get a contradiction)

Since $m - 1$ is not a counter-example and $m - 1 \geq 4$, we know $2^{(m-1)} \geq (m - 1)^2$

$\Rightarrow 2^m \geq 2(m - 1)^2$

Since $m$ is a counter-example, we know $2^m < m^2$

Combining these we get $m^2 > 2(m - 1)^2$

Expanding the RHS gives $m^2 > 2m^2 - 2m + 1$

Simplifying gives $-1 > m(m - 2)$

But $m$ and $m - 2$ are both positive, so $m(m - 2) \geq 1 \therefore$

Therefore the claim is true.
A Note on Writing Proofs

A lot of people are taught in school to write proofs that look like this example:

Prove that \((a + b)^2 = (a - b)^2 + 4ab\)

Proof:
\[
(a + b)^2 = (a - b)^2 + 4ab \\
= a^2 + 2ab + b^2 = a^2 - 2ab + b^2 + 4ab \\
= a^2 + 2ab + b^2 = a^2 + 2ab + b^2
\]

QED

In other words, the proof begins by stating the equation to be proved, and then manipulates the left side and the right side until they are identical.

This has a big problem! In a proper mathematical proof, when we state an equation (other than as an assumption or a hypothetical case) we are asserting that it is true.

So the proof above actually starts by asserting that \((a + b)^2 = (a - b)^2 + 4ab\) is a true statement ... which is the very thing we are trying to prove. This is known as begging the question\(^1\) and it effectively invalidates the proof.

I do understand that the above method of writing a proof is considered acceptable in many schools ... but it is not acceptable in CISC-203. So how should we write out the proof of this simple equality? We start with the left side and manipulate it until it is identical to the desired right side. See the next page for a demonstration.

---

\(^1\) Note: many people use the phrase “begging the question” to mean “inviting the question”. For example, they might say “Winslow fell and broke his leg, which begs the question ‘Why was he sitting on a flagpole?’” This is incorrect usage. “Begging the question” means “assuming the truth of what you are trying to prove”.

Prove that \((a + b)^2 = (a - b)^2 + 4ab\)

Proof: 
\[
(a + b)^2 = a^2 + b^2 + 2ab \\
= a^2 - 2ab + b^2 + 2ab + 2ab \\
= (a - b)^2 + 4ab
\]

QED

When people see a properly written proof, even one as trivial as this, they often wonder “how did anyone come up with subtracting 2ab and then adding in another 2ab to make up for it?”

The answer is that the thought process may well have followed a path similar to the manner in which the first proof above was written (manipulating both sides until we reach identical expressions). There’s nothing wrong with that as a way of **appoaching and solving** the problem ... but when it comes to **writing down** the proof it has to flow in a simple top-to-bottom sequence.
Permutations

We reviewed the idea of function composition.

Let \( f : A \to B \) and \( g : B \to C \) be functions (ie. \( f \) is a function from set \( A \) to set \( B \), and \( g \) is a function from set \( B \) to set \( C \)) then we write the composition of \( g \) and \( f \) as \( g \circ f \). \( g \circ f \) is a function from \( A \) to \( C \) (in notation \( g \circ f : A \to C \)) such that \( \forall a \in A \), \( (g \circ f)(a) = g(f(a)) \)

In plain English, when we see \( g \circ f \) we just have to remember that it means, “apply \( f \), then apply \( g \) to the result of that”. The key thing to remember is that the first function we apply is the last one listed.

Example (having nothing to do with permutations): let \( f : \mathbb{N} \to \mathbb{N} \) be defined by \( f(x) = x + 3 \) and let \( g : \mathbb{N} \to \mathbb{N} \) be defined by \( g(x) = 2x \)

Consider \( g \circ f (5) \). We know this is equivalent to \( g(f(5)) \). Since \( f(5) = 5 + 3 = 8 \), our answer is \( g(8) \), which is 16. But now consider \( f \circ g(5) \) ... this equals \( f(g(5)) \), which is \( f(10) \)... so the answer is 13. This demonstrates that \( g \circ f \) and \( f \circ g \) are not the same.

End of example.

Note that when \( g \circ f \) is well-defined, \( f \circ g \) may not be defined at all. To compose two functions, the “target set” of the first one we apply must match the “input set” of the second one we apply.

Now on to permutations. We’ve seen the word “permutation” before, in the context of counting the number of different linear arrangements of \( n \) distinct objects. For the next couple of classes we are going to define the concept of a permutation precisely, using our established understanding of relations and functions. We’ll discuss the rudiments of a system of mathematics in which permutations are the fundamental objects. The idea of creating meaningful mathematical systems for things that are not numbers is of fundamental importance in discrete mathematics.

Definition: A permutation is a bijection from a set to itself.

For example, let the set \( A = \{a, \text{red, 3, } \alpha\} \) One permutation of \( A \) is the bijection defined by the ordered pairs \( \{ (a,3), (\text{red,a}), (3, \alpha), (\alpha, \text{red}) \} \) --- make sure that you agree that this is a bijection.

When we are studying permutations the objects in the set don’t usually matter – what really
matters is the size of the set. For this reason, when we talk about permutations the set \( A \) is usually just \{1, 2, 3, ..., n\} for some value of \( n \).

We use \( S_n \) to represent the set of all permutations of the set \{1, 2, 3, ..., n\}

One of the first questions we can ask is, what is \( |S_n| \)? It is easy to answer: The number of ways to create an ordered pair \((1, x)\) (where \( x \) represents an element of \{1, 2, ..., n\}) is \( n \). For each of those there are \( n-1 \) ways to create an ordered pair \((2, y)\) ... and so on. The result is \( n! \)

Consider the permutation of \{1,2,3,4\} defined by \{(1,4), (2,1), (3,3) (4,2)\} Notice that under this function, 3 maps to itself. This is perfectly fine. In fact, there is a permutation that changes nothing: \( f(x) = x \) for all \( x \). For \{1,2,3,4\} the ordered pairs for this permutation are \{((1,1), (2,2), (3,3), (4,4))\}. This is called the **identity permutation**, and we represent it with the Greek letter \( \iota \) which looks like this: \( \iota \). It’s basically \( i \) without the dot.

In fact we almost always use Greek letters to name permutations: \( \pi \) (pi), \( \sigma \) (sigma), and \( \tau \) (tau) are among the favourites.

Permutations can be represented in a variety of ways. So far we have just listed the ordered pairs, but we can also use an \( n \)-by-\( n \) matrix, a diagram that shows the mapping of the set onto itself, or a 2-by-\( n \) matrix. For example, the permutation \{(1,4), (2,1), (3,3) (4,2)\} can also be represented as

\[
\begin{bmatrix}
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0
\end{bmatrix}
\]

in which each row corresponds to the first element in one of the ordered pairs, and each column corresponds to the second element. A “1” in the matrix indicates that the elements represented by the row and the column form an ordered pair. For example, there is a “1” in the second row and first column, so we know \((2,1)\) is one of the ordered pairs in the permutation.
We can also draw a diagram to represent the permutation.

![Permutation Diagram]

The 2-by-n matrix representation of this permutation looks like this:

\[
\begin{bmatrix}
1 & 2 & 3 & 4 \\
4 & 1 & 3 & 2
\end{bmatrix}
\]

in which each column represents one of the ordered pairs in the permutation.

It’s important to understand that each of these representations contains exactly the same information (they define the same permutation) and that if we are given any one of them we can construct all the others.

If we look at the 2-by-n matrix representation for different members of \( S_n \) such as

\[
\begin{bmatrix}
1 & 2 & 3 & 4 \\
4 & 1 & 3 & 2
\end{bmatrix} \quad \text{and} \quad \begin{bmatrix}
1 & 2 & 3 & 4 \\
2 & 3 & 4 & 1
\end{bmatrix} \quad \text{and} \quad \begin{bmatrix}
1 & 2 & 3 & 4 \\
3 & 4 & 1 & 2
\end{bmatrix}
\]

we can see that the first line is always the same. So we can leave it out! We represent those permutations by

\[
\begin{bmatrix}
4 & 1 & 3 & 2 \\
2 & 3 & 4 & 1 \\
3 & 4 & 1 & 2
\end{bmatrix}
\]
I will call this the **standard notation** for a permutation of \{1, \ldots, n\} because it is used very widely ... but as we will see, there is another notation that is often more useful in practice.

Remember that a permutation is a function, so we can use it as one ... the “input” is a position, and the “output” is the value that occupies that position. So if \(\pi = [4 \ 1 \ 3 \ 2]\), we can say \(\pi(1) = 4, \pi(4) = 2\) etc.

Composing permutations is just like composing other functions. If \(\pi\) and \(\sigma\) are permutations of \{1, \ldots, n\} we can write \(\pi \circ \sigma\) to represent the result of applying \(\sigma\) (as a function) and then applying \(\pi\)

For example, let \(\pi = [4 \ 1 \ 3 \ 2]\) and \(\sigma = [2 \ 3 \ 4 \ 1]\) ... what is \(\pi \circ \sigma\) ?

We can work it out: \(\pi \circ \sigma(x) = \pi(\sigma(x))\) so we get

\[
\begin{align*}
\pi \circ \sigma(1) &= \pi(\sigma(1)) = \pi(2) &= 1 \\
\pi \circ \sigma(2) &= \pi(\sigma(2)) = \pi(3) &= 3 \\
\pi \circ \sigma(3) &= \pi(\sigma(3)) = \pi(4) &= 2 \\
\pi \circ \sigma(4) &= \pi(\sigma(4)) = \pi(1) &= 4
\end{align*}
\]

and look ... the result is a permutation! Exercise: Try to prove that the composition of two permutations will always be a permutation.\(^2\)

We can create a diagram to visualize the composition of permutations. Using the same two permutations \(\pi\) and \(\sigma\) as in the previous example we get the figure on the next page:

---

\(^2\) Hint: prove a broader statement: the composition of two bijections will always be a bijection. The result for permutations follows automatically since every permutation is a bijection.
This diagram illustrates $\pi \circ \sigma$. To see this, try starting at position $x$ in the first column (for example, 3) and follow the arrows to the last column (starting with 3, we end up on 2) ... and find that this corresponds exactly to $\pi \circ \sigma(x)$.

We can also just think of the operation of a permutation as “turns $x$ into $y$”, so we can interpret $\pi \circ \sigma(3) = 2$ as “$\sigma$ turns 3 into 4, then $\pi$ turns 4 into 2”