Sometimes we can interpret a transitive relation on a set as an ordering ... if the pair (a,b) is in the relation, then we can say “a comes before b”. For example, the relation might be “is a biological ancestor of” on a set of people or “must be compiled before” on a set of software modules. Some sets have natural orders, such as the set of integers or the set of real numbers. For these sets of numbers, the natural order is based on our understanding of “less than” and “less than or equal”. They have the property that for any two different numbers x and y, we know that either x < y or y < x ... in other words, either (x,y) or (y,x) is in the relation. For other sets and relations there may be some pairs that are not related. For example we can easily find two persons x and y where neither one is a biological ancestor of the other.

We will look at orderings in more detail later in the course. For now we will focus on **The Well-Ordering Principle**.

Suppose S is a set with a defined anti-symmetric relation R, and S contains an element x such that (x, y) ∈ R ∀y ∈ S. We say that x is a minimum (or least) element of S, with respect to R.

If S is a set with a defined relation R, and it is the case that every non-empty subset of S contains a least element with respect to R, then we say that S is well-ordered.

The Well-Ordering Principle states that the set of natural numbers \( \mathbb{N} = \{0, 1, 2, 3, \ldots\} \) is well-ordered with respect to \( \leq \).

We state this without proof ... it should be clear that in any non-empty subset of \( \mathbb{N} \) there is a least element.

---

1 *Anti-symmetry* is the relation property that nobody can ever remember. Basically, saying a relation R is anti-symmetric means that when a and b are different elements, we can’t have both (a,b) and (b,a) in R. When thinking about these well-ordered sets, you really can’t go wrong by just thinking about \( \leq \) for integers. If a and b are different integers, we can have a \( \leq \) b, or we can have b \( \leq \) a, but we can’t have both.
This may seem so obvious that you might wonder why we bother stating it and why we give it a fancy name. It’s important to state it because there are other useful sets of numbers for which well-ordering does not apply. For example, consider the set $S = \{1/2, 1/4, 1/8, \ldots\}$ This subset of $\mathbb{R}$ has no least element with respect to $\leq$, so $\mathbb{R}$ is not well-ordered with respect to $\leq$. However, it is easy to define a relation $\mathbb{R}^*$ for which $S$ is well-ordered. Think about how you would do this before you check out my answer in this footnote\(^2\).

That fact that $\mathbb{N}$ is well-ordered (and we usually don’t bother to state the “with respect to ...” part because we all know what the relation is ... it is just $\leq$) makes it possible to prove some properties of integers. Later in the course we may have the opportunity to similarly exploit well-ordering in other contexts.

The Well-Ordering Principle lies behind a specialized form of Proof by Contradiction, known as **Proof by Minimal Counter-example**. This name is a bit misleading because it seems to be self-contradictory ... if there is a counter-example, how can there be a proof? The full name of the proof technique should probably be **Proof by showing that there cannot exist a minimal counter-example**, but that’s just too long to be practical.

**PMCE** works like this. Suppose we want to prove some statement $P$ about all elements of some subset $S \subseteq \mathbb{N}$. We start by assuming that $P$ is not true for all elements of $S$ (standard PBC approach). This means that there must exist at least one counter-example in $S$. This means that the set of counter-examples is non-empty. This means that the set of counter-examples must contain a least element (by the Well-Ordering Principle). Let $x$ be this minimum counter-example. And from there, we construct a contradiction (the details of this bit depend on what the statement $P$ is). The contradiction shows that our assumption must be false, so $P$ is true for all elements of $S$.

\(^2\) Remember, even though $\leq$ is the most natural ordering to use on sets of numbers, there is nothing in the definition of well-ordering that requires us to use $\leq$. So for the set $S = \{1/2, 1/4, 1/8, \ldots\}$ we can observe that each element is of the form $1/2^k$ where $k$ is an integer. Then we can define $\mathbb{R}^* = \{(1/2^a, 1/2^b) \mid 1 \leq a \leq b\}$ ... you should satisfy yourself that $S$ is well-ordered with respect to $\mathbb{R}^*$.
Example of Proof by Minimal Counter-Example:

Claim: Every integer $\geq 2$ is either prime or can be written as the product of primes.

Proof by PMCE: Suppose the claim is not true. Then let $x$ be the smallest integer $\geq 2$ such that $x$ is neither prime nor the product of primes (This is a collapsed form of these steps:
  - Claim not true => there is a counter-example
  - => the set of counter-examples is non-empty
  - => the set of counter-examples has a least element
  Call the minimum counter-example $x$)

Since $x$ is not prime, $x$ must be composite.

  $\Rightarrow x = wz$ where $w$ and $z$ are integers and $1 < w < x$ and $1 < z < x$

Since $x$ is the minimum counter-example and $w$ and $z$ are both $< x$, $w$ and $z$ cannot be counter-examples (this is where we see the purpose of choosing $x$ to be the minimum counter-example). So $w$ and $z$ must both either be prime or the product of primes. Either way, we can write $x$ as the product of primes. But that contradicts our assertion that $x$ is not the product of primes. (That’s the contradiction symbol I use.)

Assuming that the claim is false led to a contradiction, so we conclude that the claim is true.
Another example:

Claim: Every integer $\geq 7$ can be written as $2a + 3b$ where $a$ and $b$ are positive integers

PMCE: Suppose the claim is not true. Let $k$ be the smallest integer such that $k \geq 7$ and $m$ cannot be written as $2a + 3b$ where $a$ and $b$ are positive integers. (i.e. $k$ is the minimum counter-example.)

In this proof we will begin by showing that $k$ cannot be 7 or 8

We see that $7 = 2*2 + 3*1$, so $k \neq 7$

We see that $8 = 2*1 + 3*2$, so $k \neq 8$

Thus $k \geq 9$

Since $k \geq 9$, $k-2 \geq 7$ .... so $7 \leq k-2 < k$

Since $k$ is the minimum counter-example, $k-2$ is not a counter-example.

Thus $k-2 = 2x + 3y$ for some positive integers $x$ and $y$

But that means $k = 2(x+1) + 3y$, so $k$ is not a counter-example at all \(\Box\)

Therefore the claim is true.

This proof may elicit a “where did that come from?” reaction ... it seems like there is no motivation for establishing that $k \geq 9$, and even less reason for looking at $k-2$. Let me try to fill in a bit of the thinking that goes on here.

We can start by looking at the thing we are trying to prove, and how we might attack it. Remember, in PMCE we are going to have two things to work with:

- the claim is false for the minimum counter-example $k$
- the claim is true for all members of the set that are $< k$

and from these we will create a contradiction.

We are trying to prove that every integer $\geq 7$ can be written as $2a + 3b$, and we know that we are going to be supposing the existence of a minimum counter-example $k$. We can guess that our contradiction is going to be that the (supposed) minimum counter-example $k$ is not a
counter-example at all (this is very often the contradiction that we reach). We will probably
do this by finding a way to write \( k \) as \( 2x + 3y \). We will also be using the knowledge that since
\( k \) is the minimum counter-example, all values \( < k \) in the set can be written as \( 2a + 3b \).

So we ask “How can we use the information that numbers \( < k \) can be written as \( 2a+3b \) to show
that \( k \) can be written in this way?” We might think about \( k-1 \) ... we know it can be written as
\( k-1 = 2a + 3b \) for some \( a \) and \( b \). This gives us \( k = 2a + 3b + 1 \) .... but that looks like a dead end.
There’s no easy way to get rid of the +1. So now we might try thinking about \( k-2 \). We know
\( k-2 = 2a + 3b \) for some \( a \) and \( b \). This gives us \( k = 2a + 3b + 2 \) .... which is great because we can
rewrite it as \( k = 2(a+1) + 3b \).

Now we are onto something. If we can be sure that \( k-2 \) can be written as \( k-2 = 2a + 3b \), then \( k 

But remember, we need \( k-2 \) to be a member of the set we are dealing with, and that set starts
at 7. So we need \( k-2 \geq 7 \) ..... which means \( k \geq 9 \). This means that our logic about relating \( k 
to \( k-2 \) can only be applied for values \( \geq 9 \). For the values in the set that are \( < 9 \) (ie 7 and 8) we
need to prove that they can be written as \( 2a + 3b \) in some other way. Fortunately, it is easy to
prove these facts directly: \( 7 = 2 \times 2 + 3 \times 1 \) and \( 8 = 2 \times 1 + 3 \times 2 \)

Now let’s revisit the proof and annotate it.

Claim : all integers \( \geq 7 \) can be written as \( 2a + 3b \) where \( a \) and \( b \) are positive integers.

PMCE: Assume \( k \) is the minimal counter-example  \( (\text{applying the well-ordering principle}) \)

\[
\begin{align*}
7 &= 2 \times 2 + 3 \times 1 \quad \text{and} \quad 8 = 2 \times 1 + 3 \times 2 \\
\Rightarrow k \geq 9 \\
\Rightarrow k - 2 \geq 7 \\
\Rightarrow k - 2 &= 2a + 3b \quad \text{for some} \ a \ \text{and} \ b \quad (\text{because} \ k \ \text{is the minimum counter-example}) \\
\Rightarrow k &= 2(a + 1) + 3b \\
\Rightarrow k \ \text{is not a counter-example} \\
\therefore \text{the claim is true}
\end{align*}
\]
PMCE is a form of Proof by Contradiction, but it is also very closely related to Proof by Induction. In both PMCE and PBI we use the assumption that the claim is true for small values to prove that it is also true for large values.

I often find that PMCE is easier than PBI because it actually gives us more to work with: we have the knowledge that the claim is true up to k-1 (which is what we have in PBI) and we also have the assumption that the claim is false for k (which is not usually part of PBI). Putting those things together to find a contradiction is often easier than constructing an inductive proof that the claim is true for k.

However, it is a matter of choice. Both proof techniques are valid – you should become comfortable with both. You will eventually find your own preference.

Exercises:

1. Use PMCE to prove that all integers $\geq 11$ can be written as $2a + 5b$ where $a$ and $b$ are positive integers

2. Use PMCE to prove that all integers $\geq 29$ can be written as $4a + 7b$ where $a$ and $b$ are positive integers.

3. Based on the proof we worked out above and the previous 2 exercises, what you think is the largest integer that cannot be written as $3a + 4b$ where $a$ and $b$ are positive integers? Prove that your answer is correct.