Direct Knowledge | Tutorials

The Mathematical Induction Equivalence

The Definitive Beginner's Guide

David A. Smith, Direct Knowledge, USA [*†‡]

Thursday, February 9, 2023

Abstract. *In this tutorial, we'll take a close look at the principle of mathematical induction and see how it works. We'll also work through plenty of examples so that you can get a better understanding of this vital principle. Toward the end, we prove the mathematical induction equivalence, investigate sequences, and provide several exercises. The prerequisites for this tutorial are knowledge of the properties of addition and multiplication and a basic understanding of summation notation and prime numbers. If you are learning how to write mathematical proofs this tutorial is for you.*

Table of contents

[*] email: david@directknowledge.com

1 The Principle of Mathematical Induction

Mathematical induction can be challenging, especially for beginners. That's why I made this tutorial – so you can become skilled. So let's start learning about mathematical induction.

The idea behind mathematical induction (or just **induction**) is simple: we prove that the statement holds for the first element in a well-ordered set (this is called the **base case**), and then we prove that if the statement holds for any given element in the set, it must also hold for the next element in the set (this is called the **inductive step**). By showing these two steps, the base case and the inductive step, it follows by mathematical induction that the statement holds for all elements in the set. This process can be used to prove statements involving natural numbers and is basically used throughout mathematics.

1.1 First Examples

The most basic form of mathematical induction is called **natural induction**. This type of induction can be used to prove statements involving the natural numbers

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

To use natural induction, we first need to prove the statement for the first natural number, which is 0. This is called the base case.

On the other hand, we also use mathematical induction to prove statements involving the natural numbers

$$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}.$$

In using this method, the base case is at 1. Now whichever of these two methods you wish to use, the next step is the same.

Next, we assume that the statement is true for some number k. This is called the **induction hypothesis**. Finally, we must prove that the statement is also true for the next number, $k + 1$. This is called the induction step.

If we can successfully complete these two steps (base case and inductive step), then we have written a mathematical proof based on the principle of mathematical induction. The Principle of Mathematical Induction is the following statement.

> **Principle Mathematical Induction**. If P is **a subset** of the natural numbers with the properties:
>
> - $0 \in P$, and
> - for all $k \in \mathbb{N}$, $k \in P$ implies $k+1 \in P$,
>
> then P is **the set** of the natural numbers.

The advantage of mathematical induction is that it gives us a procedure to change the **is a subset** in the hypothesis to **is the set** in the conclusion.

Before better understanding the foundations of mathematical induction, let's work through some examples and see how it works.

Example 1.1. Prove that for all natural numbers n,

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}. \tag{1}$$

Solution. Let P be the set of natural numbers for which (1) is true. When $n = 0$ the LHS[1] of (1) is 0 and the RHS of (1) is also 0. In other words, since $0 = 0 = 0(1)/2$ we see that $0 \in P$. Now the induction hypothesis is: assume $k \in P$. Then we find,

$$\begin{aligned} \sum_{i=0}^{k+1} i &= \sum_{i=0}^{k} i + (k+1) && (2) \\ &= \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}. && (3) \end{aligned}$$

Notice that the **induction hypothesis** is used in moving from steps (2) to (3). So we have shown that $k+1 \in P$. By mathematical induction $P = \mathbb{N}$ as desired. □

In the next example, I leave out the reference to the set P.

Example 1.2. Prove that for all natural numbers n,

$$\sum_{i=0}^{n} i^2 = \frac{n(2n+1)(n+1)}{6}. \tag{4}$$

Proof. For $n = 0$, we consider the LHS and the RHS as follows,

$$0 = \sum_{i=0}^{0} i^2 = \frac{0(2(0)+1)(0+1)}{6} = 0 \tag{5}$$

[1] LHS is shorthand for left hand side, similarly for RHS

and so the base case holds. Assume that (4) is true for some natural number k, we need to show that

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(2k+2)(k+2)}{6} \tag{6}$$

holds. We have

$$\begin{aligned}\sum_{i=1}^{k+1} i^2 &= (k+1)^2 + \sum_{i=1}^{k} i^2 && (7)\\ &= (k+1)^2 + \frac{k(2k+1)(k+1)}{6} && (8)\\ &= \frac{(k+1)(2k+2)(k+2)}{6}. && (9)\end{aligned}$$

Therefore, by mathematical induction (4) holds for all natural numbers n. □

In any proof by induction, we must not forget to show that 0 is in P. Even if we show that the truth of k in P implies that $k+1$ is in P, if 0 is not in P, then we cannot conclude that P is the set of natural numbers. For example, let P be the set of all natural numbers that satisfy:

$$n + (n+1) = 2n. \tag{10}$$

Suppose k satisfies, (10). Using this we have

$$\begin{aligned}(k+1) + (k+2) &= k + (k+1) + 2\\ &= 2k + 2\\ &= 2(k+1)\end{aligned}$$

and thus $k+1$ also satisfies (10). So, if 1 satisfies (10) then, it would follow that (10) is true for all natural numbers n. However, 0 does not satisfy (10). In fact, obviously, (10) is false for all natural numbers n. We conclude that the basis step is a **necessary** part of any proof by mathematical induction.

Now that we have established that a base case is required when using mathematical induction. It is now natural to ask: does the base case need to start at the first natural number 0.

1.2 The Principle of Strong Induction

The principle of strong (mathematical) induction is also a method of proof and is frequently useful in the theory of numbers. This principle can also be used to prove statements about arays, sequences, and many other structures. Familiarity with this type of argument is essential to subsequent work.

Theorem 1.1 (Principle of Strong Induction). *A set of positive integers that contains the integer 1, and that has the property: for every positive integer* n, *if the set contains* $1, 2, \ldots, n$, *then it also contains the integer* $n + 1$*; must be the set of all positive integers.*

Proof. Let P be the set with the stated properties and let S be the set consisting of all positive integers not in P. Assuming that S is nonempty, we can choose n to be the least integer in S by the Well-Ordering Principle. Since 1 is in P and n is not in P, we know that $n > 1$. Further, notice that none of the integers $1, 2, 3, \ldots, n-1$ lies in S, so that in fact, they are in P. Then by the second property, $n = (n-1) + 1$ is in P, which contradicts n is not in P. Thus, S is empty and P must be the set of all positive integers. □

Example 1.3. Show that any amount of postage more than 1-cent can be formed just using 2-cent and 3-cent stamps.

Solution. Notice that 2-cent and 3-cent stamps can be formed using 2-cent and 3-cent stamps, so the base case is obvious. Let k be a natural number with $k \geq 1$. For an induction hypothesis (strong), assume that any amount of postage up to k-cents can be formed using 2-cent and 3-cent stamps. Then using $k + 1 = k - 1 + 2$, and the fact that 2 is a 2-cent stamp and $k - 1$ can be formed using 2-cent and 3-cent stamps, we see that $k + 1$ can be formed using 2-cent and 3-cent stamps. Hence by strong induction, any amount can be formed using 2-cent and 3-cent stamps. □

Recall that the assumption that the statement is true for some number $n = k$ is referred to as the induction hypothesis. Sometimes the role that 0 plays in the principle of mathematical induction will be replaced by some other natural number, say a, in such instances mathematical induction establishes the statement for all natural numbers $n \geq a$.

Let a be a natural number. Consider the set defined by

$$\mathbb{N}_a = \{k \in \mathbb{N} : k \geq a\}. \tag{11}$$

In other words,

$$\mathbb{N}_a = \{a, a+1, a+2, a+3, \ldots\}. \tag{12}$$

Using this set notation we can formalize variations of mathematical induction as follows.

Notice that whenever $a = 0$, we have the Principle of Mathematical Induction as stated previously.

Theorem 1.2 (General Form of Mathematical Induction)**.** *Let a be a fixed natural number. The following statements are logically equivalent.*

1. *If $a \in P \subseteq \mathbb{N}_a$ and for all $k \in \mathbb{N}_a$, $k \in P$ implies $k+1 \in P$, then $P = \mathbb{N}_a$.*
2. *If $a \in P \subseteq \mathbb{N}_a$ and for all $k \in \mathbb{N}_a$, $a, a+1, \ldots, a+k \in P$ implies $a+k+1 \in P$, then $P = \mathbb{N}_a$.*

Proof. (1) ⇒ (2): Let S be a set of natural numbers with $a \in S$ and the property, for all natural numbers k, $a, a+1, \ldots, a+k \in S$ implies $a+k+1 \in S$. Let P be the set of natural numbers for which $a, a+1, \ldots, a+n \in S$ is true. Notice $a \in P$ since $a \in S$. Assume $k \in P$. Then $a, a+1, \ldots, a+k \in S$. Thus $a, a+1, \ldots, a+k, a+k+1 \in S$ meaning $a+k+1 \in P$. Hence, $P = \mathbb{N}_a$. By definition of P, $S = \mathbb{N}_a$ as desired.

(2) ⇒ (0): Assume, for a contradiction, there exists a nonempty subset S of $\mathbb{N}_a$ with no least element. Let P be the set of natural numbers for which $n \notin S$ is true. Because a is the least element of all elements in $\mathbb{N}_a$, $a \notin S$ and so $a \in P$. Assume $a, a+1, \ldots, a+k \in P$. If $a+k+1 \in S$ then $a+k+1$ is the least element of S. However, S has no least element and thus $a+k+1 \notin S$. Thus, $a+k+1 \in P$ and so $P = \mathbb{N}_a$. This contradiction shows S can not exist. □

1.3 Ordering the Natural Numbers

Now we are looking for orderings on the natural numbers. Afterwards, we'll explain the connection between mathematical induction and these orderings.

Recall a relation R is a set of ordered pairs. In this tutorial we'll restrict our attention to relations on the set of natural numbers.

- A relation R is reflexive on $\mathbb{N}$ whenever aRa, for all a in $\mathbb{N}$.
- A relation R is antisymmetric on $\mathbb{N}$ whenever aRb and bRa implies $a = b$, for all a, b in $\mathbb{N}$.
- A relation R is transitive on $\mathbb{N}$ whenever aRb and bRc implies aRc, for all a, b, c in $\mathbb{N}$.

We call a relation R a **partial ordering** whenever it is **reflexive**, **antisymmetric**, and **transitive**.

Here are the orderings we'll be interested in first.

Definition 1.1. Let $\mathbb{N}$ be the set of natural numbers.

1. The relation $\leq$ is defined on $\mathbb{N}$ by $a \leq b$ if and only if there exists a natural number c such that $b = a + c$. If $a \leq b$ we say a is **less than or equal to** b or we say b is **greater than or equal to** a.
2. The relation $|$ is defined on $\mathbb{N}$ by $a|b$ if and only if $a \neq 0$ and there exists a natural number c such that $b = ac$. If $a|b$ we say that a **divides** b or we say that a is a **factor** of b.
3. Let c be a natural number. The relation $\xrightarrow{*}_c$ is defined on $\mathbb{N}$ by $a \xrightarrow{*}_c b$ if and only if there exists a natural number m such that $a = b + mc$ and $a \leq b$. If $a \xrightarrow{*}_c b$ we say that a **reduces to** b **modulo** c.

Lemma 1.1. *The relations $\leq$ and $|$ are partial orderings on $\mathbb{N}$. Moreover, for any natural number c the relation $\xrightarrow{*}_c$ is a partial ordering on $\mathbb{N}$.*

Proof. Firstly, we'll show that $\leq$ is an ordering. If a is a natural number, then $a+0 = a$ and so $a \leq a$ by definition of $\leq$. In other words $\leq$ is reflexive. Notice the ordering is antisymmetric also. To see this suppose that $a \leq b$ and $b \leq a$. Then there exists natural numbers n and m such that $a + n = b$ and $b + m = a$. From this we see that

$$b = a + n = (b + m) + n = b + (m + n) \tag{13}$$

which yields that $n = m = 0$, and hence $a = b$ as needed. To show that $\leq$ is transitive assume that $a \leq b$ and $b \leq c$ where a, b, c are natural numbers. Then there exists natural numbers n and m such that $a + n = b$ and $b + m = c$. From this we see that

$$c = b + m = (a + n) + m = a + (n + m) \tag{14}$$

which yields that $a \leq c$. Secondly, we'll show that $|$ is an ordering. First, notice that $|$

is reflexive because if a is a natural number then $a|a$ since $a = 1(a)$. To show that $|$ is antisymmetric, suppose $a|b$ and $b|a$. Then there exists natural numbers m and n such that $b = ma$ and $a = nb$ and so we have

$$b = ma = m(nb) = (mn)b. \tag{15}$$

Thus, $nm = 1$ and so in particular $n = 1$. Whence, $a = b$ as desired. To show that $|$ is transitive, suppose $a|b$ and $b|c$. Then there exists natural numbers m and n such that $b = ma$ and $c = nb$ and so we find

$$c = nb = n(ma) = (nm)a. \tag{16}$$

Since nm is a natural number, we see that $a|c$ as desired. □

Notice the similarities between (13) and (15) and also between (14) and (16).

Before looking at these orderings in more detail, let's see more examples of mathematical induction.

Example 1.4. Show that $n! > n$ is true for for all natrural numbers n with $n \geq 3$.

Solution. So our base case is $n = 3$. Let's prove that $n! > n$ for all $n \geq 3$. Since $3! = 1 \cdot 2 \cdot 3 = 6 > 3$ we see that the base case holds. Now assume that for some positive natural numbers k greater than 3, that $k! > k$. Then we see that

$$(k+1)! = k!(k+1) > k(k+1) > k+1$$

Therefore, by mathematical induction, $n! > n$ for all $n \geq 3$. □

Example 1.5. Prove that $2^{n-1} > n$ for all natural numbers $n \geq 3$.

Solution. Since $4 = 2^{3-1} = 2^2 = 4 > 3$ the statement is true for $n = 3$. Assume that the result is true for a natural number n, we need to show that $2^{(n+1)-1} > n+1$ holds. Starting from $2^{n-1} > n$ we multiply by 2 to obtain $2^n > 2n$. But $2n = n + n > n + 1$ since $n \geq 3$. Therefore by mathematical induction, $2^{(n+1)-1} > 2n > n+1$ for all natural numbers $n \geq 3$ as desired. □

Example 1.6. Show that $0 \leq n$ for all natural numbers n.

Solution. Let $P = \{n \in \mathbb{N} \mid 0 \leq n\}$. Notice that $0 \in P$ because $\leq$ is reflexive. Asssume that $k \in P$. By transivivity and that $0 \leq k \leq k+1$ it follows that $0 \leq k+1$. By mathematical induction $P = \mathbb{N}$ as needed. □

Example 1.7. Prove that $n \leq 2^n$ for all natural numbers n.

Solution. Let P be the set of all natural numbers for which $n \leq 2^n$ is true. Since $0 \leq 1 = 2^0$ is true, $0 \in P$. Assume $k \in P$ and $k > 0$. Then $k \leq 2^k$ is true and since

$$k + 1 \leq k + k = 2k \leq (2)2^k = 2^{k+1} \tag{17}$$

it follows $k + 1 \in P$. Thus, for all $k \in P$, $k \in P$ implies $k + 1 \in P$ is true and so by mathematical induction $P = \mathbb{N}$ as desired. □

Example 1.8. Let a and b be natural numbers. Prove that $a|b$ if and only if $a^n|b^n$ for all natural numbers n.

Solution. We will use mathematical induction. Since $a|b$ certainly implies $a|b$, the case for $k = 1$ is trivial. Assume that $a^k|b^k$ holds for some natural number $k > 1$. Then there exists a natural number m such that $b^k = ma^k$. Then

$$b^{k+1} = bb^k = b\left(ma^k\right) = (bm)a^k = (m'am)a^k = Ma^{k+1} \tag{18}$$

where m' and M are natural numbers. Whence, $a^{k+1}|b^{k+1}$ as desired. □

The strict part of a relation R is the relation R minus the ordered pairs (a, a) for any a. In set notation we can write the strict part R^s of a relation R as follows

$$R^s = \{(a, b) \mid aRb \text{ and } a \neq b\}.$$

So for example, $2 < 3$ and $3 < 45$ where $<$ is the notation for the strict part of $\leq$. From Example 1.6 we can see that $0 < n$ for all nonzero natural numbers n.

Lemma 1.2 (Trichotomy)**.** *For any natural numbers a and b, exactly one of the following is true:*

$$a < b, \quad a = b, \quad \text{or} \quad b < a. \tag{19}$$

Proof. We will first show that at most one can be true and then show that at least one must be true.

(1): Assume that $a = b$. Then neither $a < b$ nor $b < a$ can hold by definition of the strict part. Assume that $a \neq b$. If $a < b$ and $b < a$, then $a \leq b$ and $b \leq a$ by definition of the strict part. By antisymmetry of $\leq$, we see that $a = b$, contrary to the case assumption. All cases considered at most one can be true from (19).

(2): Consider the set

$$P = \{a \in \mathbb{N} \mid \text{ for all } b \in \mathbb{N}, a < b, a = b, \text{ or } b < a\}$$

we will show by induction that $P = \mathbb{N}$. Notice that $0 \in P$ since either $b = 0$ or otherwise $0 < b$ holds as seen above. Assume that $k \in P$. The induction hypothesis is that one of the following must hold

$$k < b, \quad k = b, \quad \text{or} \quad b < k \tag{20}$$

for all natural numbers b. Let c be a natural number. If $c = k$, then $c < k + 1$ as wanted. On the other hand, if $c \neq k$, then either $k < c$ or $c < k$ (by induction hypothesis). In the case $k < c$, then either $c = k + 1$ or $k + 1 < c$. In the case $c < k$, then $c < k + 1$ by transitivity. All cases considered we have shown that

$$k + 1 < c, \quad k + 1 = c, \quad \text{or} \quad c < k + 1 \tag{21}$$

for all natural numbers c. Hence $k + 1 \in P$ as needed. □

A partial ordering that satisfies the **trichotomy property**, namely, exactly one of the following must hold: $a < b$, $a = b$, or $b < a$ is called a **total ordering**. So notice that from Lemma 1.2 we can say $\leq$ is an example of a partial ordering that is also a total ordering.

Example 1.9. Show that the divisibility relation is not a total ordering on $\mathbb{N}$.

Solution. Consider 3 and 7. Notice that none of these are true: $3|7$, $7|3$, nor $3 = 7$. In fact, we can say the same for any two distinct primes. □

In Lemma 1.3 we see that the less than relation $\leq$ is an extension of the divisibility relation. We also see that both relations are compatabile with the operations in which they were originally defined.

Lemma 1.3. *Let a and b be natural numbers.*

1. *If $a|b$, then $a \leq b$.*
2. *For all natural numbers c, $a \leq b$ if and only if $a + c \leq b + c$.*
3. *For all nonzero natural numbers c, $a|b$ if and only if $ac|bc$.*

Proof. (1): Suppose $a|b$. Then there exists a natural number c such that $b = ac$. If

$c = 1$, then $a \leq b$ is immediate. Otherwise, there exists a natural number d such that $c = 1 + d$. Hence $b = a(1 + d) = a + ad$ where ad is a natural number. Thus $a \leq b$.

(2): Suppose $a \leq b$. Then there exists an natural number n such that $b = a + n$. By substitution we find,

$$b + c = (a + n) + c = (a + c) + n.$$

So $a + c \leq b + c$ as needed.

Conversely, suppose that $a + c \leq b + c$. If $a = b$, then $a \leq b$ as needed. Assume that $a \neq b$, By Lemma 1.2 we have $a < b$ or $b < a$. If $b < a$, then $b \leq a$ and by the first part $b + c \leq a + c$. Hence by antisymmetry, $a + c = b + c$ and so $a = b$ contrary to case assumption. Therefore, $a < b$ which yields $a \leq b$ in this case as well.

(3): Suppose $a|b$. Then there exists a natural number n such that $b = an$. By substitution we find,

$$bc = (an)c = (ac)n.$$

Since $c \neq 0$, it follows that $ac \neq 0$, and so $ac|bc$ as needed.

Conversely, suppose that $ac|bc$. If $a = 0$, then $ac = 0$ contrary to $ac \neq 0$ by definition of divisibility. Hence $a \neq 0$. Further there exists a natural number d such that $bc = acd$. Case $b < ad$: There exists a natural number $e > 0$ such that $ad = b + e$ so that $bc = (b + e)c = bc + ec$. This yields $bc < bc$ and so this case can not happen. Case $ad < b$: There exists a natural number $f > 0$ such that $b = ad + f$ so that $bc = acd + fc = bc + fc$. This yields $bc < bc$ and so this case can not happen either. By Lemma 1.2 we find that $b = ad$ and so $a|b$ as needed. □

We say a natural number n is a **linear combination** of a and b if there exists natural numbers x and y such that $n = ax + by$. For example, 7 is a linear combination of 3 and 2 since $7 = 2(2) + 1(3)$. Notice that by Lemma 1.4 we can say that that if an natural number divides to other natural numbers, then it divides any linear combination of these two natural numbers.

Lemma 1.4 (Linear Combinations). *Let a, b, and c be natural numbers. If $c|a$ and $c|b$, then $c|(xa + yb)$ for any natural numbers x and y.*

Proof. Suppose $c|a$ and $c|b$. Then there exists natural numbers m and n such that

$a = mc$ and $b = nc$. Assume x and y are arbitrary natural numbers. We have

$$xa + yb = x(mc) + y(nc) = c(xm + yn)$$

Since $xm + yn \in \mathbb{N}$ we see that $c|(xa + yb)$ as desired. □

1.4 The Well-Ordering Principle

The Well-Ordering Principle is an important statement concerning the ordering on the natural numbers and can be used to prove mathematical statements. The Well-Ordering Principle is the following statement.

> **Well-Ordering Principle**. Every nonempty set of natural numbers has a least element.

In other words, no matter how a subset of natural numbers is defined, as long as it is nonempty, the Well-Ordering Principle guarantees us, that it must have a least element.

One of the most important statements in number theory is the Well-Ordering Principle. This principle states that every non-empty set of natural numbers contains a smallest element. In other words, there is no infinite sequence of natural numbers in which each number is smaller than the one before it. The Well-Ordering Principle is often used to prove results by contradiction. This makes it a very powerful tool for mathematical reasoning. Now it's time to show that strong induction implies the Well-Ordering Principle.

Theorem 1.3. $SFI \Rightarrow WOP$

Proof. Assume, for a contradiction, there exists a nonempty set of natural numbers S with no least element. Let P be the set of natural numbers for which $n \notin S$ is true. Because 0 is the least element of all natural numbers, $0 \notin S$ and so $0 \in P$. Assume $0, 1, \ldots, k \in P$. If $k + 1 \in S$ then $k + 1$ is the least element of S. However, S has no least element and thus $k + 1 \notin S$. Thus, $k + 1 \in P$ and so by Strong Induction, $P = \mathbb{N}$. This contradiction shows S can not exist. Therefore, $S = \mathbb{N}$. □

Notice that only $SFI \Rightarrow WOP$ was proven above. The converse statement, namely $WOP \Rightarrow SFI$ is left for the reader as an exercise.

Okay, so we have proven that $WOP \Rightarrow PMI \Rightarrow SFI \Rightarrow WOP$. This means, logically speaking that, $WOP \Leftrightarrow PMI \Leftrightarrow SFI$, and so all three theorems above are proven.

Lemma 1.5 (Division Algorithm)**.** *If a and b are nonzero natural numbers, then there are unique positive natural numbers q and r such that*

$$a = bq + r \qquad \textit{and} \qquad 0 \leq r < b.$$

Proof. First we prove existence. Let b be an arbitrary natural number greater than 0 and let S be the set of multiples of b that are greater than a, namely,

$$S = \{bi \mid i \in \mathbb{N} \text{ and } bi > a\}.$$

Notice S is nonempty since $ab > a$. By the Well-Ordering Axiom, S must contain a least element, say bk. Since $k \neq 0$, there exists a natural number q such that $k = q+1$. Notice $bq \leq a$ since bk is the least multiple of b greater than a. Thus there exists a natural number r such that $a = bq + r$. Notice $0 \leq r$. Assume, $r \geq b$. Then there exists a natural number $m \geq 0$ such that $b + m = r$. By substitution, $a = b(q+1) + m$ and so $bk = b(q+1) \leq a$. This contradiction shows $r < b$ as needed.

Now we prove uniqueness. Suppose

$$a = bq_1 + r_1, \quad a = bq_2 + r_2, \quad 0 \leq r_1 < b, \quad 0 \leq r_2 < b.$$

If $q_1 = q_2$ then $r_1 = r_2$. Assume $q_1 < q_2$. Then $q_2 = q_1 + n$ for some natural number $n > 0$. This implies

$$r_1 = a - bq_1 = bq_2 + r_2 - bq_1 = bn + r_2 \geq bn \geq b$$

which is contrary to $r_1 < b$. Thus $q_1 < q_2$ cannot happen. Similarly, $q_2 < q_1$ cannot happen either, and thus $q_1 = q_2$ as desired. □

Lemma 1.6 (Bezout's Identity)**.** *Let a and b be natural numbers, not both zero. Then $(a, b) = am + bn$ for some natural numbers m and n.*

Proof. Assume a and b are natural numbers and w.l.o.g. assume $a \neq 0$. Consider the set

$$S = \{ax + by \mid ax + by > 0, \, x \text{ and } y \text{ are natural numbers}\}.$$

Since S is nonempty, because $|a|$ is in S, the Well-Ordering Axiom yields a least positive natural number d such that $d = am + bn$ for some natural numbers m and n. The idea is to show that $d = (a, b)$. To do this we use the Division Algorithm obtaining q and r such that $a = qd + r$ where $0 \leq r < d$. If $r > 0$, then r is in S because

$$r = a - qd = a - q(am + bn) = a(1 - qm) + b(-qn).$$

But we can not have r is in S because $r < d$ and d is the least in S. Therefore $r = 0$ and so $d|a$. Using the same argument with a replaced by b, it is shown that $d|b$. To show $d = (a, b)$ it remains to show that d is greater than any other common divisor of a and b; and so let c be a common divisor of a and b. Then, $c \mid am + bn$ that is $c \mid d$ and so $d \geq c$. □

Recall a natural number greater than 1 is called **prime** whenever it has no divisors other than 1 or itself.

Lemma 1.7 (Prime Characterization)**.** *Let p be natural number greater than 1. Then p is a prime if and only if*

$$p|nm \implies p|n \text{ or } p|m \tag{22}$$

for all natural numbers n and m.

Proof. Assume that p is a prime number and that n, m are natural numbers. Suppose that $p|nm$. Then there exists a natural number k such that $nm = pk$. Assume further that p does not divide n. In particular, $p \neq n$ and so either $p < n$ or $n < p$ by Lemma 1.2.

Conversely, suppose (22) holds for all natural numbers n and m. To show that p is prime assume that $d|p$. Then $p = dt$ for some natural number t. In particular, notice that $p|dt$ because $dt = p(1)$. Hence, by (22) we have $p|d$ or $p|t$. Case $p|d$: there exists a natural number s such that $d = ps$ and so $p = dt = pst$. In this case, $s = 1$ and so $d = p$. Case $p|t$: there exists a natural number t such that $t = pk$ for some natural number k and so $p = dt = dpk = p(dk)$, and so $d = 1$. Therefore, the only divisors of p are 1 and p, and so p is prime. □

Lemma 1.8. *Prove if p is a prime number, a_1, $a_2, \ldots, a_n$ are natural numbers, and $p \,| a_1 a_2 \cdots a_n$, then $p \,| a_i$ for some $1 \leq i \leq n$.*

Proof. The statement is clearly true when $n = 1$ and $n = 2$ follows from Lemma 1.7. Assume the statement is true for $n = k$, and suppose $p \,| a_1 a_2 \cdots a_k a_{k+1}$. Then by Lemma 1.7, $p \,| a_1 a_2 \cdots a_k$ or $p \,| a_{k+1}$. If $p \,| a_{k+1}$, the statement is proven. If not, then by the induction hypothesis there is some $0 \leq i \leq k$ such that $p|a_i$. Therefore, there is some $0 \leq i \leq k + 1$ such that $p|a_i$ as desired. □

Lemma 1.9. *Every natural number greater than 1 is a product of primes.*

Proof. Consider the set S consisting of all positive natural numbers greater than 1 that are not a product of primes. Assume for a contradiction that S is not empty, then by the Well-Ordering Principle there is a least element, say m. Because m has no prime divisors and m divides m, we see that m is not prime. Thus, $m = ab$ where $1 < a < m$ and $1 < b < m$. Since m is the least element in S, a and b are products of primes; and thus so is m. This contradiction shows that S is empty and so every natural number greater than 1 is a product of primes. □

The **Fundamental Theorem of Arithmetic**, also called the **unique factorization theorem** or the unique-prime-factorization theorem, states that every natural number greater than 1 is either is prime itself or is the product of prime numbers, and that, although the order of the primes in the second case is arbitrary, the primes themselves are not.

Lemma 1.10 (Fundamental Theorem of Arithmetic)**.** *Every natural number greater than 1 can be written uniquely in the form*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \tag{23}$$

where $p_1 < p_2 < \cdots < p_k$ are prime numbers and $e_1, e_2, \ldots, e_k$ are natural numbers.

Proof. Every natural number has a prime factorization by Lemma 1.9. Thus existence is proven. Now we prove uniqueness. If there is an natural number greater than 1 for which the factorization is not unique, then by the Well-Ordering Principle there exists a smallest such natural number, say m. Assume that m has two prime factorizations say

$$m = {p_1}^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \qquad \text{and} \qquad m = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}, \tag{24}$$

where

$$p_1 < p_2 < \cdots < p_s \qquad q_1 < q_2 < \cdots < q_t \tag{25}$$

and the α_i and β_j are all positive for $0 \leq i \leq s$ and $0 \leq j \leq t$. By Lemma 1.8,

$$q_1 \mid p_{i^\star} \text{ for some } 1 \leq i^\star \leq s \quad \text{and} \quad p_1 \mid q_{j^\star} \text{ for some } 1 \leq j^\star \leq t. \tag{26}$$

Since all the numbers p_i and q_j are prime, we must have $q_1 = p_{i^\star}$ and $p_1 = q_{j^\star}$. Then $i^\star = j^\star = 1$ since

$$q_1 \leq q_{j^\star} = p_1 \leq p_{i^\star} = q_1. \tag{27}$$

Let u be the natural number defined as

$$u = \frac{m}{p_1} = \frac{m}{q_1} = {p_1}^{\alpha_1 - 1}{p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s} = {q_1}^{\beta_1 - 1}{q_2}^{\beta_2} \cdots {q_t}^{\beta_t}. \tag{28}$$

If $u = 1$, then $m = p_1$ has a unique factorization contrary to hypothesis. If $u > 1$, then $u < m$ and u has two factorizations. Both cases reveal that m can not exist as desired. □

Mathematical induction is a technique used to prove that a certain property holds for all natural numbers. The Well-Ordering Principle states that every non-empty set of natural numbers contains a smallest element. We will now prove that the Well-Ordering Principle implies mathematical induction.

Theorem 1.4. *$WOP \Rightarrow PMI$*

Proof. Let P be a subset of natural numbers with $0 \in P$ and the property, for all natural numbers k, $k \in P$ implies $k + 1 \in P$. Assume, for a contradiction, there exists a nonempty set S containing the natural numbers not in P. By WOP, S has a least natural number, s. Since $0 \in P$, $s \neq 0$. Thus there exists a natural number t such that $t + 1 = s$. Notice $t \notin S$ since $t < s$. Thus $t \in P$ and so $s = t + 1 \in P$. This contradiction shows S cannot exist, meaning $P = \mathbb{N}$ as desired. □

As an exercise for the reader, you should try proving that $PMI \Rightarrow WOP$. After trying that, read on.

As discussed above, there are several variations of mathematical induction. Now we would like to show that these are equivalent also. Recall we use the notation

$$N_a = \{k \in \mathbb{N} : k \geq a\} \tag{29}$$

where a is a natural number.