

Items in this supplement are numbered N.1, N.2, and so on, and you are free to use the Theorems without proving them first. If you use a result from this document in your homework, you should cite it by number, e.g. “by N.3”. The Rules of the Game still apply. Read this supplement alongside Appendix A of the textbook.

The Principle of Mathematical Induction

Recall that the **natural numbers** are $\mathbb{N} = \{1, 2, 3, \dots\}$. A **proposition** is a sentence that is either true or false. For example, the sentence “ $7 \mid 21$ ” is a true proposition, while the sentence “ $2^4 \equiv 2 \pmod{3}$ ” is a false proposition. The classic example of a sentence which is not a proposition is the paradox “This sentence is false.” An **open sentence** is a sentence which contains variables, together with a set from which each variable may be chosen, that becomes a proposition once a particular element of that set has been chosen for each variable. You have already encountered open sentences over the natural numbers in your homework. Let $a, b, n \in \mathbb{Z}$ with $n > 0$, and assume that $a \equiv b \pmod{n}$. Then

$$P(k) : a^k \equiv b^k \pmod{n}$$

is an open sentence over the natural numbers. In Exercises 1.15 and 1.16, you proved that $P(1)$ implies $P(2)$ and $P(3)$, and in Exercise 1.17 you proved that for every $k \in \mathbb{N}$ with $k > 1$, $P(k-1)$ implies $P(k)$.

The textbook states the following axiom just before the Division Algorithm. An **axiom** is a statement we accept without proof.

Axiom (The Well-Ordering Axiom for the Natural Numbers). Let S be any non-empty set of natural numbers. Then S has a smallest element.

In our course, we never constructed the natural numbers, instead treating them as a familiar mathematical object. From this perspective, the Well-Ordering Axiom looks more like an obvious *theorem*. However, our “definition” $\mathbb{N} = \{1, 2, 3, \dots\}$ is not a precise mathematical definition at all, so there is no foundation from which to prove it. The axiom also fails for other familiar sets of numbers: neither $\mathbb{Z}$ nor the set of positive rationals has a smallest element.

Now, suppose we want to prove a proposition of the form $\forall n \in \mathbb{N}, P(n)$, where P is an open sentence over $\mathbb{N}$. Checking the cases one at a time will not do, since there are infinitely many natural numbers. Suppose instead that we know two things: that $P(1)$ is true, and that for every $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true. Applying the second fact with $k = 1$, we see that $P(1)$ implies $P(2)$, so $P(2)$ is true. Applying it again with $k = 2$, we see that $P(2)$ implies $P(3)$, so $P(3)$ is true. Then $P(3)$ implies $P(4)$, which implies $P(5)$, and so on. Our intuition tells us that we may conclude $P(n)$ is true for every n , and you may have written a proof of Theorem 1.18 using reasoning like this. Appendix A calls it the domino effect: if the first domino falls, and each domino knocks over the one after it, then every domino falls. In our class, the Principle of Mathematical Induction is a *theorem* which makes this precise. We will prove it in class as a consequence of the Well-Ordering Axiom.

N.1 Theorem (Principle of Mathematical Induction). Let $P(n)$ be an open sentence over $\mathbb{N}$. Suppose that

- (a) $P(1)$ is true; and
- (b) for every $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for every $n \in \mathbb{N}$.

Writing a Proof by Induction

Proof by induction is a technique for proving propositions of the form $\forall n \in \mathbb{N}, P(n)$, and it relies on invoking N.1. Hypothesis (a) of N.1 is called the **base case**, and hypothesis (b) is called the **inductive step**. In the inductive step, the assumption that $P(k)$ is true is called the **inductive hypothesis**. Notice that (b) does not claim that $P(k)$ is true. It claims only that *if* $P(k)$ is true, then so is $P(k+1)$.

A proof by induction has the following shape.

1. State the open sentence $P(n)$ clearly.
2. *Base case.* Show that $P(1)$ is true.
3. *Inductive step.* Let $k \in \mathbb{N}$ and suppose that $P(k)$ is true. Using this assumption, show that $P(k+1)$ is true.
4. *Conclusion.* By N.1, $P(n)$ is true for every $n \in \mathbb{N}$.

N.2 Exercise. For each of Theorems A.10 and A.18 in Appendix A, write down the open sentence $P(n)$, then state precisely the base case $P(1)$, the inductive hypothesis $P(k)$, and the statement $P(k+1)$ that you must prove in the inductive step. Which item in Appendix A is the inductive step?

Theorem 1.18 can be proved by induction. Here is an example of what such a proof looks like.

Theorem 1.18. Let a, b, k , and n be integers with $n > 0$ and $k > 0$. If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

Proof. Let $a, b, n \in \mathbb{Z}$ with $n > 0$, and assume that $a \equiv b \pmod{n}$. For each $k \in \mathbb{N}$ let

$$P(k) : a^k \equiv b^k \pmod{n}.$$

We will prove that $P(k)$ is true for all $k \in \mathbb{N}$ using the Principle of Mathematical Induction.

Base case. The proposition $P(1)$ says that $a^1 \equiv b^1 \pmod{n}$, which is true by hypothesis.

Inductive step. Let $k \in \mathbb{N}$ and suppose that $P(k)$ is true, so that $a^k \equiv b^k \pmod{n}$. Since we also have $a \equiv b \pmod{n}$, Theorem 1.14 applied to these two congruences gives

$$a \cdot a^k \equiv b \cdot b^k \pmod{n},$$

that is, $a^{k+1} \equiv b^{k+1} \pmod{n}$. So $P(k+1)$ is true.

Conclusion. By the Principle of Mathematical Induction, $P(k)$ is true for every $k \in \mathbb{N}$. □

Notice that the inductive step is exactly Exercise 1.17, which you have already proved (although it was stated there with $k-1$ and k in place of k and $k+1$). Exercises 1.15 and 1.16 were not used in the proof, even in the base case! The role of those two exercises was to let you discover the inductive step by carrying it out twice.

A correct proof by induction in this course will follow all of these steps explicitly. Many authors leave some of them implicit, which is mathematically correct and reads more gracefully, but is confusing for anyone not yet comfortable with the Principle of Mathematical Induction. Most authors would write the same proof more briefly. Here is one such version.

Proof. The case $k = 1$ is the hypothesis. If $a^k \equiv b^k \pmod{n}$, then since $a^{k+1} = a \cdot a^k$ and $b^{k+1} = b \cdot b^k$, Theorem 1.14 gives $a^{k+1} \equiv b^{k+1} \pmod{n}$. The result follows by induction. □

Other Starting Points

Some statements are true only from some point on. For instance, Theorem A.20 in Appendix A is about natural numbers $n > 3$, so its base case is $n = 4$. The next theorem generalizes the Principle of Mathematical Induction, allowing the base case to be any integer.

N.3 Theorem. Let $n_0 \in \mathbb{Z}$, and let $P(n)$ be an open sentence over $\{n \in \mathbb{Z} : n \geq n_0\}$. Suppose that

- (a) $P(n_0)$ is true; and
- (b) for every $k \in \mathbb{Z}$ with $k \geq n_0$, if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for every $n \in \mathbb{Z}$ with $n \geq n_0$.

Strong Induction

Strong induction is a theorem used to prove statements of the form $\forall n \geq n_0, P(n)$, where $n_0 \in \mathbb{Z}$ and $P(n)$ is an open sentence over $\{n \in \mathbb{Z} : n \geq n_0\}$. The adjective *strong* refers to the fact that the theorem apparently allows you to assume a much stronger inductive hypothesis.

N.4 Theorem. Let $n_0 \in \mathbb{Z}$, and let $P(n)$ be an open sentence over $\{n \in \mathbb{Z} : n \geq n_0\}$. Suppose that

- (a) $P(n_0)$ is true; and
- (b) for every $k \in \mathbb{Z}$ with $k \geq n_0$, if $P(j)$ is true for every $j \in \mathbb{Z}$ with $n_0 \leq j \leq k$, then $P(k+1)$ is true.

Then $P(n)$ is true for every $n \in \mathbb{Z}$ with $n \geq n_0$.

The inductive hypothesis in (b) is the assumption that *all* of $P(n_0), P(n_0+1), \dots, P(k)$ are true, rather than just $P(k)$. Every proof by N.3 is already a proof by N.4, since one is always free to use only the case $P(k)$. Thus, Theorem N.4 implies Theorem N.3, and in particular Theorem N.1. Conversely, Theorem N.3 implies Theorem N.4: apply N.3 to the open sentence $Q(n)$: “ $P(j)$ is true for every $j \in \mathbb{Z}$ with $n_0 \leq j \leq n$.” So the stronger inductive hypothesis is only apparent, since strong induction is ordinary induction applied to $Q(n)$.

Theorem 2.1 was proved in class using the Well-Ordering Axiom. However, it can be also be proved by strong induction.

Theorem 2.1. If n is a natural number greater than 1, then there exists a prime p such that $p \mid n$.

Proof. For each integer $n \geq 2$ let

$$P(n) : \text{there exists a prime } p \text{ such that } p \mid n.$$

We will prove that $P(n)$ is true for all $n \geq 2$ using Theorem N.4 with $n_0 = 2$.

Base case. The base case is $P(2)$. Note that the only natural number less than 2 is 1, and any product of copies of 1 is equal to 1. Since $2 > 1$, 2 is not a product of natural numbers less than 2. Thus, 2 is prime. Since $2 \mid 2$, $P(2)$ is true.

Inductive step. Let $k \geq 2$ and suppose that $P(j)$ is true for every j with $2 \leq j \leq k$. If $k+1$ is prime, then $P(k+1)$ is true, since $k+1 \mid k+1$. Otherwise, $k+1$ is *composite*, meaning that it is a product of natural numbers less than $k+1$. So $k+1 = ab$ for some natural numbers a and b with $a < k+1$ and $b < k+1$. Note that $a > 1$: if $a = 1$, then $k+1 = b$, contradicting $b < k+1$. Thus $2 \leq a \leq k$, so by the inductive hypothesis, $P(a)$ is true, and there is a prime p with $p \mid a$. By Theorem 1.6, $p \mid ab$, that is, $p \mid k+1$. So $P(k+1)$ is true.

Conclusion. By Theorem N.4, $P(n)$ is true for every $n \geq 2$.

□

In the proof above, the inductive hypothesis was applied to a , which may be strictly less than k . For example, if $k + 1 = 12$, then we might have $a = 3$, and knowing only that $P(11)$ is true would not help. This is a good example of a proof where strong induction is the natural tool.

How do you know when to use strong induction? Ask what you need in order to prove $P(k + 1)$. If $P(k)$ is enough, ordinary induction will do. If you need an earlier case other than $P(k)$, or several earlier cases at once, use strong induction. Factoring is one typical situation, since the factors of $k + 1$ can be any size. The Fibonacci numbers are another, since each term depends on the two before it.

Example. The **Fibonacci numbers** are defined by $F_1 = 1$, $F_2 = 1$, and

$$F_{n+2} = F_{n+1} + F_n \quad \text{for } n \geq 1.$$

Then for every $n \in \mathbb{N}$, $F_n \leq \varphi^{n-1}$, where $\varphi = \frac{1+\sqrt{5}}{2}$ is the golden ratio.

Proof. For each $n \in \mathbb{N}$ let

$$P(n) : F_n \leq \varphi^{n-1}.$$

We will prove that $P(n)$ is true for all $n \in \mathbb{N}$ using Theorem N.4 with $n_0 = 1$.

Base case. Since $F_1 = 1 = \varphi^0$, $P(1)$ is true.

Inductive step. Let $k \geq 1$ and suppose that $P(j)$ is true for every j with $1 \leq j \leq k$. If $k = 1$, we must show that $P(1)$ implies $P(2)$. This holds because $P(2)$ is true, since $F_2 = 1 \leq \varphi = \varphi^1$. If $k \geq 2$, then by the inductive hypothesis, $F_k \leq \varphi^{k-1}$ and $F_{k-1} \leq \varphi^{k-2}$. Since $\varphi^2 = \varphi + 1$, we have

$$F_{k+1} = F_k + F_{k-1} \leq \varphi^{k-1} + \varphi^{k-2} = \varphi^{k-2}(\varphi + 1) = \varphi^{k-2}\varphi^2 = \varphi^k,$$

so $P(k + 1)$ is true.

Conclusion. By Theorem N.4, $P(n)$ is true for every $n \in \mathbb{N}$.

□

Notice that the inductive step required both $P(k)$ and $P(k - 1)$, so ordinary induction would not apply directly here. Why did we handle the case $k = 1$ separately? The recurrence relation $F_{k+1} = F_k + F_{k-1}$ only makes sense when $k + 1 \geq 3$, that is, when $k \geq 2$. Yet, the inductive step must be proved *for all* $k \geq 1$, including $k = 1$, so we must check this case directly. When $k = 1$, the statement to be proved is that $P(1)$ implies $P(2)$, and this holds because $P(2)$ is true on its own. The base case $P(1)$ is used when $k = 2$, since then $F_{k-1} = F_1$. Sometimes people will check $P(2)$ as a separate base case, which obscures the fact that it is part of the inductive step. Theorem N.4 only requires a single base case.