Week 3: Induction and Representations of Natural Numbers

Michael Zhou

2023-01-07

Use induction to prove:

- Statements in number theory
- Statements in new domains
- Properties about sequences
- Counting combinatorial objects

1 The principle of induction

Definition 3.1. The principle of **induction** can be used to prove statements of the form $\forall n \in \mathbb{N}, P(n)$, and *only* applies to statements of this type — universal quantifiers over natural numbers.

The most bjasic form, **simple** induction, has two steps:[1]

- The **base case** is the proof that the statement holds for the first natural number, 0.
- The **inductive step** is a proof that for all $n \in \mathbb{N}$, if $P(n)$ is True, then $P(n+1)$ is also True:

$$\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$$

[1] These steps are called **conjunctions**, and may be presented in either order.

Once these two steps are proven, then by the principle of induction, we can conlcude that $\forall n \in \mathbb{N}, P(n)$.

Example 3.1. Prove that for any $m, x, y, n \in \mathbb{N}$ such that $n \geq 1$ if $x \equiv y \bmod m$, then $x^n \equiv y^n \bmod m$.

This is a question from PS1, and we could prove that $x^2 \equiv y^2 \bmod m$ and $x^3 \equiv y^3 \bmod m$ and so on by the same pattern of $ac \equiv bd \bmod n$. But to make it mathematically rigourous for all n and m, we need to use induction.

How does this work? It is essentially the domino effect that we've examined in PS1. By knowing $P(0)$ is True, we know that $P(0) \Rightarrow P(1)$ through the base case, then we know $P(1) \Rightarrow P(2)$ by the inductive step, and so on.

By showing that as long as it is True for n, it is also True for the number right after n, then we can conclude that it is True for every n.

2 Examples from number theory

Example 3.2. Prove that for every natural number n, $7 \mid 8^n - 1$.

Translation. $\forall n \in \mathbb{N}, 7 \mid 8^n - 1$[2]

Discussion. Definite the predicate $P(n)$ as "$7 \mid 8^n - 1$", then by the divisibility predicate, $7 \cdot y = 8^n - 1$. Then we know exactly how to use induction in this proof.

[2] The translation and discussion section will start merging into one soon.

Proof. Let $P(n)$ be $7 \cdot y = 8^n - 1$.

$$\exists y \in \mathbb{Z}, 7 \cdot y = 8^n - 1$$

We want to prove that for all $n \in \mathbb{N}$ that $P(n)$ holds.

Base case: Let $n = 0$, we want to prove $P(0)$ holds True.
We know that $7 \cdot 0 = 8^0 - 1$ holds True.

Inductive step: Let $k \in \mathbb{N}$, and assume that $P(n)$ is True, we want to prove $P(n+1)$. In other words,

$$7 \mid 8^{k+1} - 1 \text{ or } \exists y \in \mathbb{Z}, 8^{k+1} - 1 = 7y_k$$

How do we prove this? Well we want to use previously proved definitions, so extracting $8^k - 1$ from the equation could work.

$$\begin{aligned} 8^{k+1} - 1 &= 8^{k+1} - 8 + 7 \\ &= 8(8^k - 1) + 7 \end{aligned}$$

Next we can use the **induction hypothesis**, which is $7y_k = 8^k - 1$.

$$\begin{aligned} 8^{k+1} - 1 &= 8(8^k - 1) + 7 \\ &= 8(7y_k) + 7 \\ &= 56y_k + 7 \\ &= 7(8y_k + 1) \end{aligned}$$

We can let $8y_k + 1 = y_{k+1}$, and thus the proof is complete.

Example 3.3. Prove that for every natural number $n, n(n^2 + 5)$ is divisible by 6.

Proof. Let $P(n)$ be the statement that $\exists n \in \mathbb{N}, 6 \mid n(n^2 + 5)$.

Base case: Prove $P(0)$ is True. We know this is True since $6 \mid 0(0^2+5) = 6 \mid 0$, and anything divides 0.

Inductive step: Let $k \in \mathbb{N}$, and assume $P(k)$ is True. We want to prove $P(k+1)$ holds, such that $6 \mid (k+1)((k+1)^2 + 5)$. We are looking to isolate a $k(k^2 + 5)$ term to apply the induction hypothesis.

$$\begin{aligned} (k+1)((k+1)^2 + 5) &= (k+1)(k^2 + 2k + 6) \\ &= (k+1)((k^2 + 5) + (2k + 1)) \\ &= k(k^2 + 5) + k(2k + 1) + (k^2 + 5) + (2k + 1) \\ &= k(k^2 + 5) + 3k^2 + 3k + 6 \\ &= k(k^2 + 5) + 3k(k + 1) + 6 \end{aligned}$$

For the first term $k(k^2+5)$, we know that is divisible by 6 due to the induction hypothesis.

The second term is tricky, but we know that $k(k+1)$ has two consecutive natural numbers, meaning one of them is even, so the entire term is even. What does this imply? It means that $k(k+1)$ has a factor of 2. Adding in the coefficient of 3, it means that the second term has a factor of 6 for certain.

The third term is obviously divisible by 6.

Using the divisibility of linear combinations, since each term is divisible by 6, the entire sum is also divisible by 6. Thus, the proof is complete.

Finally let's go back to Example 3.1 to prove it using induction.

Example 3.4. Prove that for any $m, x, y \in \mathbb{N}$ and for any $n \in \mathbb{N}$ that if $x \equiv y(\mod m)$ we have $x^n \equiv y^n(\mod m)$.

Translation.[3]

$$\forall m, x, y \in \mathbb{N}, \forall n \in \mathbb{N}, x \equiv y(\mod m) \Rightarrow \forall n \in \mathbb{N}, x^n \equiv y^n(\mod m)$$

[3] Note that we separated the variables m, x, y and n, we will discuss this in the next section.

Base case: Prove $P(0)$ is True. We have $x^0 \equiv y^0(\mod m)$, which is trivially True.

Inductive step: Let $k \in \mathbb{N}$. Assuming $P(n)$ is True, prove $P(n+1)$ is True. We have $x^{k+1} \equiv y^{k+1}(\mod m)$.

From the previous example, we know that

$$x^k \equiv y^k(\mod m) \wedge x \equiv y(\mod m) \Rightarrow x \cdot x^k \equiv y \cdot y^k(\mod m)$$

Since we assumed the left side is True, we also know the right side is True due to the implication. Thus, the proof is complete.

Why did we exclude the n from the first quantification?

Changing the order of quantifiers can change the proof that we could write:

- Another way we could've written this is

  $$\forall n \in \mathbb{N}, \forall m, x, y \in \mathbb{N}, x \equiv y(\mod m) \Rightarrow x^n \equiv y^n(\mod m)$$

  Then we can define $P(n)$ to exclude the $\forall n \in \mathbb{N}$ portion.

- By convention, it would not make sense if we partitioned the the $\forall n \in \mathbb{N}$ and the conditions to define it as $P(n)$, so it would be best if we wrote it the same way as we planned to define it

Example 3.5. Prove that for all natural numbers n greater than or equal to 3, $2n+1 \leq 2^n$.

Translation. $\forall n \in \mathbb{N}, n \geq 3 \Rightarrow 2n+1 \leq 2^n$. We can assume the hypothesis is True and prove the conclusion.

Proof. Let $n \in \mathbb{N}$, and let $2n+1 \leq 2^n$ be $P(n)$. We can assume that $P(n)$ is True. WTS $P(0)$ is True, and $P(n+1)$ is True through induction.

Base case. $P(0)$ is $2^0 + 1 \leq 2^0$, which is $2 \leq 1$, thus it is True.

Inductive step. Let $k \in \mathbb{N}$, and $k = n$. We assume $P(k) : 2k + 1 \leq 2^k$. WTS $P(k+1)$ is True: $2(k+1) + 1 \leq 2^{k+1}$.

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

Example 3.6. Prove that for all $n \in \mathbb{N}$, if $n \geq 1$. then $2^{2^n} - 1$ is divisible by at least n distinct primes.

Proof. Let $k \in \mathbb{N}$, then $P(k)$ is $n \geq 1 \implies (Prime(k) \mid 2^{2^k} - 1)$.

Base case. $P(1)$ is $2^{2^1} - 1 = 3$, which is divisible by 3, thus it is True.

Inductive step. We assume $P(k)$ to be True. WTS $P(k+1)$ is True: $2^{2^{k+1}} - 1$.

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

We know the left term is True since that is $P(k)$, and the right term is an odd number. The difference between the two numbers is 2, so the gcd must be either 1 or 2, but it cannot be 2 since the right term is odd. Thus the right term introduces a new prime number since the gcd is 1, and proves $P(k+1)$.

3 Combinatorics

Definition 3.2. **Combinatorics** is an area concerned with counting objects and analyzing patterns. A **pattern** is a sequence of numbers that we often want to derive a closed-form expression for a_k (the k^{th} number in the sequence) or for $\sum_{i=0}^{k} a_i$ (the sum of the first $k+1$ numbers in the sequence).

Example 3.7. Consider the following sequence:

$$0, 1, 1, 2, 3, 5, 8, \ldots$$

Does it look familiar? The *Fibonacci sequence* is a famous pattern of combinatronics: for all $k \geq 2$, $a_k = a_{k-1} + a_{k-2}$.

Example 3.8. Another example is the *arithmetic sequence*. Suppose we start with \$20, and we gained \$200 every month. How much money would we have in k months?

$$a_0 = 20, a_1 = 220, a_2 = 420, \ldots$$

We get the sequence of $a_k = 20 + 200k$.[4]

[4] This is also $y = mx + b$.

Example 3.9. Suppose we started with \$10, and our money doubled every month. How much would we have in k months?

$$a_0 = 10, a_1 = 20, a_2 = 40, \ldots$$

We get a *geometric sequence* of $a_k = 10 \cdot 2^k$.

Example 3.10. Suppose we wanted to add all $n \in \mathbb{N}$ up to and including k, it would give rise to the following:

$$a_k = 0 + 1 + \ldots + k$$

We can express this infinite sequence as a closed form expression $a_n = n \cdot \frac{(n+1)}{2}$.

3.1 Proofs of closed form expressions

Definition 3.3. In general, a **sequence** is an ordered list of numbers such that $f : \mathbb{N} \to \mathbb{R}$ where $a(0) = f(0)$ and so on.

Definition 3.4. A sequence is **closed form** or **explicit** when there is a fixed number of elementary operations. We can often use induction to prove that an explicit formula computes the terms in a sequence.

For example, the Fibonacci sequence also has an explicit formula called Binet's formula:

$$a_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$$

Example 3.11. Use induction to prove the first n positive integers is equal to $n \cdot \frac{(n-1)}{2}$

Translation.

$$\forall n \in \mathbb{N}, \sum_{j=1}^{n} j = n \cdot \frac{(n+1)}{2}$$

Proof. Let $P(n)$ be $\sum_{j=1}^{n} j = n \cdot \frac{(n+1)}{2}$.

Base case. Let $n = 0$, then the left is an empty sum, and the right is $0 \cdot \frac{0-1}{2} = 0$. Thus the base case is True.

Inductive step. Let $k \in \mathbb{N}$ and assume that $P(k)$ is True: $\sum_{j=1}^{k} j = k \cdot \frac{(k+1)}{2}$. WTS that $P(k+1)$ is True: $\sum_{j=1}^{k+1} j = \frac{(k+1)(k+2)}{2}$.

$$\begin{aligned}
\sum_{j=1}^{k} j &= k \cdot \frac{(k+1)}{2} \\
\sum_{j=1}^{k+1} j &= k \cdot \frac{(k+1)}{2} + (k+1) \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{k(k+1) + 2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

Since we know that the sum we are expressing is $a_k = 1 + 2 + \ldots k$, to add the k^{th} term is just adding $(k+1)$ to the sum.

■

3.2 Strengthening the hypothesis

Example 3.12. Prove that the sum of the first n odd numbers is a perfect square.

Translation.

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N}, \sum_{i=0}^{n-1}(2i+1) = x^2$$

Discussion. To prove the inductive step, we can assume that $P(k)$ is True. But we run into an issue:

$$\sum_{i=0}^{k}(2i+1) = x^2$$
$$\sum_{i=0}^{(k+1)-1}(2i+1) = x^2 + (2k+1)$$

How can we prove that the $2k+1$ term adds into the right term to make it a perfect square? We can explore examples to learn more: $1^2 = 1$, $2^2 = 3+1$, $3^3 = 5+3+1$. We can conjecture that the sum of the first n odd numbers is equal to n^2. So, we can make our hypothesis even stronger:

$$\forall n \in \mathbb{N}, \sum_{i=1}^{n-1}(2i+1) = n^2$$

Proof. Let $P(n)$ be the predicate $\sum_{i=1}^{n-1}(2i+1) = n^2$, we will prove that for all $n \in \mathbb{N}, P(n)$ by induction on n.

Base case. Let $n = 0$, then the left is an empty sum and the right is 0, thus this is True.

Inductive step. Let $k \in \mathbb{N}$, we will assume that $P(k)$ is True: $\sum_{i=1}^{k-1}(2i+1) = k^2$. WTS that $P(k+1)$ is True: $\sum_{i=1}^{k}(2i+1) = (k+1)^2$.

$$\sum_{i=1}^{k-1}(2i+1) = k^2$$
$$\sum_{i=1}^{(k+1)-1}(2i+1) = k^2 + (2k+1)$$
$$\sum_{i=1}^{k}(2i+1) = k^2 + 2k + 1$$
$$= (k+1)^2$$

■

3.3 Going beyond numbers

Example 3.13. Prove that for every finite set S, $\mid \mathcal{P}(s) \mid = 2^{|S|}$.[5]. In other words, a power set of S will have $2^{|S|}$ number of subsets.[6]

Translation. We can perform induction on a variable representing the size of a set, since the size of a finite set is always a natural number. We can then define a predicate for $n \in \mathbb{N}$:

$$P(n) : \text{Every set } S \text{ of size } n \text{ satisfies } \mid \mathcal{P}(S) \mid = 2^n$$

[5] Recall that $\mathcal{P}$ denotes a power set — the set of all subsets of S

[6] $\mid P(n) \mid$ is the size of a set.

Then, our original statement would just be $\forall n \in \mathbb{N}, P(n)$, which means we can use induction.

Proof. **Base case.** Let $n = 0$. The only subset of an empty set is itself, $\mathcal{P}(S) = \{\emptyset\}$, which is size 1, and $2^0 = 1$.

Inductive step. Let $k \in \mathbb{N}$, and assume that $P(k)$ is True. WTS $P(k+1)$ is True. Let S be a set with size $k+1$, and let $s_1, \ldots, s_{k+1}$ be elements of the set, we wanrt to prove that the number of subsets in S is 2^{k+1}.

We know that subsets of S that do not contain the last element of s_{k+1} have the size 2^{k+1} according to our assumption.

Now consider subsets *only* including the last element — this is also 2^{k+1} since you simply add s_{k+1} to 2^k subsets.

Thus, $2^k + 2^k = 2^{k+1}$, and concludes the proof.

■

Example 3.14. Prove that for all $n, m \in \mathbb{N}$, and for all sets A and B of size n and m, respectively, $\mid A \times B \mid = n \cdot m$.

Translation. We can follow the above example, and perform induction on a variable representing the size of a set, and we only need to perform induction on one of them, as they are both natural numbers. We define a predicate for $n \in \mathbb{N}$:

$$P(n) : \text{Every set } A, B \text{ of size } n, m \text{ satisfies } \mid A \times B \mid = n \cdot m$$

Then our statement is $\forall n, m \in \mathbb{N}, P(n)$. We will prove for n.

Proof. **Base case.** Let $n = 0$, then A must be an empty set, and the Cartesian product would be an empty set, which is size 0. Thus, $0 = 0 \cdot m$.

Inductive step. Let $k \in \mathbb{N}$ and assume that $P(k)$ holds. WTS $P(k+1)$ is True. We can define $A \times B$ of size k and m respectively as the set S_k:

$$S_k = \{k_0 m_0, k_0 m_1, \ldots, k_0 m_{m-1}, \ldots k_{k-1} m_0, \ldots k_{k-1} m_{m-1}\}$$

And let $S_{(k+1)}$ be the set of $A \times B$ for only $k+1$ terms and m:

$$S_{(k+1)} = \{k_k m_0, \ldots, k_k m_{m-1}\}$$

We can express $\mid S_k \mid$ as $k \cdot m$ since we assumed $P(k)$ to be True, and thus we can express $\mid S_{(k+1)} \mid$ as m since there is only one term of $k+1$.

$$\begin{aligned} \mid A \times B \mid &= k \cdot m \\ &= \mid S_k \mid \\ &= \mid S_k \mid + \mid S_{(k+1)} \mid \\ &= k \cdot m + m \\ &= m(k+1) \end{aligned}$$

The proof for m is the same, thus $P(k+1)$ is proven for both $k = n$ and $k = m$.

■

4 Strong induction

Definition 3.5. **Strong induction** is a technique that assumes the first n terms are all True: $P(0), P(1), \ldots, P(n)$. This is in contrast to *simple induction*, which was the previously taught method of assuming only $P(n)$. These are equivalent. Formally, we want to prove that

$$\forall n \in \mathbb{N}, n \geq k \Rightarrow P(n)$$

where k is some natural number. We first prove the base case $P(k)$, then prove that for any fixed but arbitrary $n \geq k$, $P(j)$ for all j where $k \leq j \leq n$ implies $P(n+1)$

Example 3.15. Prove that for every integer $n \geq 2$, it can be expressed as a product of one or more prime numbers,[7]

[7] Sound familiar? This is the prime factorization theorem.

Proof. Let $P(n)$ be the statement that n can be expressed as a product of one or more prime numbers.

Base case. Let $n = 2$. 2 can be expressed as itself, which is prime, thus $P(2)$ is True.

Inductive step. Let n be an integer, $n \geq 2$. And assume that for every integer j, $2 \leq j \leq n$, that j can be expressed as a product of one or more prime numbers. WTS $P(n+1)$. There are two cases: either integer $n+1$ is a prime number, or it is not. If it is a prime number, then it is a product of itself, so this case is complete.

When it is a not a prime number, it is $n + 1 = a \cdot b$, where a, b are positive integers that are both not $n + 1$ or 1. Since $2 \leq a \leq n$, and $2 \leq b \leq n$, both a and b can be written as a product of prime numbers by the induction hypothesis, thus the proof is complete.

■

We would not have been able to show this with simple induction, since all we would know is that $P(n)$ can be factorized into primes.