7 Mathematical Induction and the Fundamental Theorem of Arithmetic

7.1 The Principle of Mathematical Induction

Induction is applied when we have an infinite number of statements which are indexed by the natural numbers as, for example, with the following statement:

$$2n + 6 \text{ is even for all } n \in \mathbb{N}.$$

Here, it would not be sufficient to prove the statement for a sample of natural numbers, no matter how large the sample is. We have to prove it for *all* natural numbers! Hence, we first show that the statement is true for the smallest natural number. Then we assume a statement is true for some arbitrary natural number k and we proceed to show that the statement is true for its consecutive number, given by $k + 1$. That is, the truth of one statement implies the truth of the next statement. Since k was arbitrary and the statement is true for the smallest natural number and any two consecutive numbers, the statement is then true for all numbers. This is based on the Principle of Mathematical Induction:

Axiom 7.1 (The Principle of Mathematical Induction)**.** *Let $n_0 \in \mathbb{N}$ be given, and for each positive integer $n \geq n_0$, let $P(n)$ be a statement. If*

(I) $P(n_0)$ is true, and

(II) $P(k) \implies P(k+1)$ is true for all $k \in \mathbb{N}$ with $k \geq n_0$,

then $P(n)$ is true $\forall\ n \geq n_0$.

Example. *Show that, for every $n \in \mathbb{N}$, we have*

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof. For $n \in \mathbb{N}$, let $P(n)$ be the following statement.

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

We will show that $P(n)$ is a true statement, for all $n \in \mathbb{N}$ by giving a proof by induction.

First, let us consider $P(1)$. We have

$$1 = \frac{1(1+1)}{2}.$$

Hence, $P(1)$ is a true statement.

Now, suppose that $P(k)$ is true for some positive integer k, that is

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}.$$

Then

$$\begin{aligned} 1+2+3+\cdots+k+(k+1) &= \frac{k(k+1)}{2}+(k+1) \\ &= \frac{k(k+1)}{2}+\frac{2(k+1)}{2} \\ &= \frac{k^2+3k+2}{2} \\ &= \frac{(k+1)(k+2)}{2}, \end{aligned}$$

showing that if $P(k)$ is true then $P(k+1)$ is true. By the Principle of Mathematical Induction, it follows that $P(n)$ is true for all natural numbers n. □

As we saw in the above example, we often have that $n_0 = 1$. However, this does not always follow. As a matter of fact, the following example shows that setting $n_0 = 1$ may lead to false statements.

Example. *Show that* $n^2 \leq 2^{n-1}$ *for all* $n \in \mathbb{N}$ *such that* $n \geq 7$.
We first note that the above statement is certainly true for $n = 1$. *However, it is* ***not*** *true for* $n = 2, 3, 4, 5,$ *and* 6. *Therefore, setting* $n_0 = 1, 2, 3, 4, 5$ *or* 6 *would lead to false statements. Since it is given that* $n \geq 7$, *we must set* $n_0 = 7$.

Proof. Let $P(n)$ be the following statement:

$$n^2 \leq 2^{n-1}.$$

We will show that $P(n)$ is a true statement, for all natural numbers n such that $n \geq 7$, by giving a proof by induction.

First, let us consider $n = 7$. We have that $7^2 = 49 \leq 64 = 2^6$. Hence, $P(7)$ is a true statement.

Now, suppose that $P(k)$ is a true statement for some natural number $k \geq 7$, that is

$$k^2 \leq 2^{k-1}.$$

Then

$$\begin{aligned} (k+1)^2 &= k^2+2k+1 \\ &\leq k^2+2k+k, && \text{since } k \geq 7, \\ &= k^2+3\cdot k \\ &\leq k^2+k\cdot k, && \text{since } k \geq 7, \\ &= 2k^2 \\ &\leq 2\cdot 2^{k-1}, && \text{by assumption}, \\ &= 2^k \\ &= 2^{(k+1)-1}, \end{aligned}$$

showing that if $P(k)$ is true then $P(k+1)$ is true. By the Principle of Mathematical Induction, it follows that $P(n)$ is true for all natural numbers $n \geq 7$. □

We have the following proposition.

Proposition 7.2. *Let X be a set, and let $A, B_1, B_2, \ldots, B_n \subseteq X$ where $n \in \mathbb{N}$. Then we have the following results.*

(i) $A \cup (B_1 \cap B_2 \cap \cdots \cap B_n) = (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_n)$.

(ii) $A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)$.

(iii) For $n \geq 2$, $(B_1 \cap B_2 \cap \cdots \cap B_n)^c = B_1^c \cup B_2^c \cup \cdots \cup B_n^c$.

(iv) For $n \geq 2$, $(B_1 \cup B_2 \cup \cdots \cup B_n)^c = B_1^c \cap B_2^c \cap \cdots \cap B_n^c$.

Proof. We will prove (i) and leave (ii), (iii) and (iv) as Exercise 4.11.

Let $P(n)$ be the following statement:

$$A \cup (B_1 \cap B_2 \cap \cdots \cap B_n) = (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_n)$$

We will show that $P(n)$ is a true statement, for all $n \in \mathbb{N}$ by giving a proof by induction.

First note that $A \cup B_1 = A \cup B_1$. Hence, $P(1)$ is a true statement.

Now suppose that $P(k)$ is true for some $k \geq 1$, that is

$$A \cup (B_1 \cap B_2 \cap \cdots \cap B_k) = (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_k).$$

Let $C = B_1 \cap B_2 \cap \cdots \cap B_k$. Then

$$A \cup (B_1 \cap B_2 \cap \cdots \cap B_{k+1}) = A \cup (C \cap B_{k+1}).$$

We have that $A \cup (C \cap B_{k+1}) = (A \cup C) \cap (A \cup B_{k+1})$. Then by our induction hypothesis,

$$\begin{aligned} A \cup C &= A \cup (B_1 \cap B_2 \cap \cdots \cap B_k) \\ &= (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_k). \end{aligned}$$

Hence

$$\begin{aligned} &A \cup (B_1 \cap B_2 \cap \cdots \cap B_{k+1}) \\ &= A \cup (C \cap B_{k+1}) \\ &= (A \cup B_1) \cap (A \cup B_2) \cap \cdots \cap (A \cup B_k) \cap (A \cup B_{k+1}), \end{aligned}$$

showing that if $P(k)$ is true then $P(k+1)$ is true. By the Principle of Mathematical Induction, it follows that $P(n)$ is true for all natural numbers n. □

7.2 The Strong Principle of Mathematical Induction

Consider the following example:

Example. *Suppose that $x_1 = 3$ and $x_2 = 5$ and suppose that, for $n \geq 3$, we have that*

$$x_n = 3x_{n-1} - 2x_{n-2}.$$

Show that $x_n = 2^n + 1$, for all $n \in \mathbb{N}$.

For the above example, it is not sufficient to assume the statement is true for some natural number k. We must also have that the statement is true for $k-1$ and $k-2$ (since $x_k = 3x_{k-1} - 2x_{k-1}$). Therefore, we would assume that the statement is true for all integers i such that $2 \leq i \leq k$. This would be a case when we use the Strong Principle of Mathematical Induction:

Axiom 7.3 (The Strong Principle of Mathematical Induction)**.** *Let $n_0 \in \mathbb{N}$ be given. For each positive integer $n \geq n_0$, let $P(n)$ be a statement. If*

(I) $P(n_0)$ is true, and

(II) $(P(i),\ \forall\ i \in \mathbb{N}$ with $n_0 \leq i \leq k) \implies P(k+1)$ is true for all $k \in \mathbb{N}$,

then $P(n)$ is true $\forall\, n \geq n_0$.

Example. *Suppose that $x_1 = 3$ and $x_2 = 5$ and suppose that, for $n \geq 3$, we have*

$$x_n = 3x_{n-1} - 2x_{n-2}.$$

Show that $x_n = 2^n + 1$, for all $n \in \mathbb{N}$.

Proof. Let $P(n)$ be the following statement:

$$x_n = 2^n + 1.$$

We will show that $P(n)$ is a true statement, for all $n \in \mathbb{N}$, by giving a proof by induction. First, let us consider $n = 1$ and $n = 2$. We have the given initial conditions $x_1 = 3$ and $x_2 = 5$. Using the formula $x_n = 2^n + 1$, we have

$$x_1 = 2^1 + 1 = 3 \qquad \text{and} \qquad x_2 = 2^2 + 1 = 5,$$

as required. Therefore, $P(1)$ and $P(2)$ are true statements.

Let $k \in \mathbb{N}$ and suppose $P(i)$ is a true statement, for all $i \in \mathbb{N}$ such that $2 \leq i \leq k$. Then $P(k)$ and $P(k-1)$ are true statements. That is, we have

$$\begin{aligned} x_{k-1} &= 2^{k-1} + 1 \\ x_k &= 2^k + 1. \end{aligned}$$

Then

$$\begin{aligned} x_{k+1} &= 3x_k - 2x_{k-1} \\ &= 3(2^k + 1) - 2(2^{k-1} + 1) \\ &= 3 \cdot 2^k - 2 \cdot 2^{k-1} + 1 \\ &= 3 \cdot 2^k - 2^k + 1 \\ &= 2 \cdot 2^k + 1 \\ &= 2^{k+1} + 1, \end{aligned}$$

showing that if $P(i)$ is true, for $2 \leq i \leq k$, then $P(k+1)$ is true. By the Strong Principle of Mathematical Induction, it follows that $P(n)$ is true for all natural numbers n. □

7.3 The Fundamental Theorem of Arithmetic

As a further example of strong induction, we will prove the Fundamental Theorem of Arithmetic, which states that for $n \in \mathbb{Z}$ with $n > 1$, n can be written uniquely as a product of primes. But before we can prove the Fundamental Theorem of Arithmetic, we need to establish some other basic results.

Definition 7.4. *We say an integer $p > 1$ is **prime** if the only positive divisors of p are 1 and p.*

We have the following proposition.

Proposition 7.5. *Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ where $n \in \mathbb{N}$ with $n \geq 2$, and suppose that p is a prime such that $p \mid a_1 a_2 \cdots a_n$. Then $p \mid a_j$ for some $j \in \mathbb{Z}$ with $1 \leq j \leq n$.*

Proof. Let $P(n)$ be the following statement:

$$\text{If } p \mid a_1 a_2 \cdots a_n, \text{ then } p \mid a_j \text{ for some } 1 \leq i \leq n.$$

We will show that $P(n)$ is a true statement for all $n \geq 2$ by giving a proof by strong induction. First, consider $n = 2$ and suppose that

$$p \mid a_1 a_2.$$

If $p \mid a_1$ then we are done. So suppose $p \nmid a_1$. Then $\gcd(p, a_1) = 1$ since p is prime. It follows that $p \mid a_2$. Therefore, $P(2)$ is a true statement.

Now let $k \in \mathbb{N}$ such that $k \geq 2$, and suppose that $P(i)$ is a true statement for all $i \in \mathbb{N}$ with $2 \leq i \leq k$, that is

$$\text{if } p \mid a_1 \cdots a_i \text{ then } p | a_j \text{ for some } j \in \mathbb{N} \text{ with } 1 \leq j \leq i.$$

So suppose that $p \mid a_1 \cdots a_k a_{k+1}$ and set $t = a_1 a_2 \cdots a_k$. Then $p \mid t\ a_{k+1}$. If $p \mid t$ then our induction hypothesis tells us that $p \mid a_j$ for some $j \in \mathbb{N}$ with $1 \leq j \leq k$. If $p \nmid t$, then $\gcd(p, t) = 1$ since p is prime. Hence, $p \mid a_{k+1}$. Then $p \mid a_j$ for some $1 \leq j \leq k+1$. Hence, we have shown that if $P(i)$ is true, for $2 \leq i \leq k$ then $P(k+1)$ is true. By the Strong Principle of Mathematical Induction, it follows that $P(n)$ is true for all natural numbers n. □

We have the following theorem.

Theorem 7.6 (Fundamental Theorem of Arithmetic)**.** *Let $n \in \mathbb{N}$ such that $n > 1$. Then for every n, we can write*

$$n = p_1 p_2 \cdots p_r,$$

for some primes $p_1, p_2, \ldots, p_r$ with $p_1 \leq p_2 \leq \cdots \leq p_r$ and $r \in \mathbb{N}$. Further, if we also have

$$n = q_1 q_2 \cdots q_s,$$

for some primes $q_1, q_2, \ldots, q_s$ with $q_1 \leq q_2 \leq \cdots \leq q_s$ and $s \in \mathbb{N}$, then $r = s$ and $p_i = q_i$ for all $i \in \mathbb{N}$ with $1 \leq i \leq r$.

Proof.

(i) First, we will argue by strong induction that each integer $n > 1$ is a product of primes.

Let $P(n)$ be the following statement.

$$n = p_1 p_2 \cdots p_r \text{ for some primes } p_1, p_2, \ldots, p_r \text{ with } p_1 \leq p_2 \leq \cdots \leq p_r \text{ and } r \in \mathbb{N}$$

(I) First, consider $n = 2$. Since 2 is prime, we have that 2 is a product of a prime. Therefore, $P(2)$ is a true statement.
Now, let $k \in \mathbb{N}$ such that $k \geq 2$, and suppose that $P(i)$ is a true statement for all integers i with $2 \leq i \leq k$, that is

$$i = p_1 p_2 \cdots p_r \text{ for some primes } p_1, p_2, \ldots, p_r \text{ with } p_1 \leq p_2 \leq \cdots \leq p_r \text{ and } r \in \mathbb{N}$$

(II) Now, consider the integer $k+1$. If $k+1$ is prime, then we are done. So suppose that $k+1$ is not prime. Then 1 and $k+1$ are not the only positive integers dividing $k+1$. Hence, there exists some $a \in \mathbb{N}$ with $1 < a < k+1$ such that $a \mid k+1$. Hence, there exists some $b \in \mathbb{N}$ such that $ab = k+1$. Since $1 < a$, we have that $b < ab$, so $b < k+1$. Further, since $a < k+1$ and $ab = k+1$, we have $1 < b$. It follows that a and b are products of primes. Therefore, $k+1$ must be a product of primes.

Hence, we have shown that if $P(i)$ is true, for $2 \leq i \leq k$ then $P(k+1)$ is true. By the Strong Principle of Mathematical Induction, it follows that $P(n)$ is true for all natural numbers n.

(ii) Second, we want to show that for any integer $n > 1$, there is a unique prime factorisation for n.

Let $P(r)$ be the following statement.

$$\text{If } p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \text{ for some primes } p_1, p_2, \ldots, p_r \text{ and } q_1, q_2, \ldots, q_s \text{ such that } p_1 \leq p_2 \leq \cdots \leq p_r \text{ and } q_1 \leq q_2 \leq \cdots \leq q_s, \text{ then } r = s \text{ and } p_i = q_i \text{ for all } i \in \mathbb{N} \text{ with } 1 \leq i \leq r.$$

We will show that $P(r)$ is a true statement for all $r \geq 1$ by giving a proof by induction.

(I) So suppose first that $p_1 = q_1 \cdots q_s$ where p_1 is prime and $q_1 \leq \cdots \leq q_s$ are prime. Since p_1 is prime, we must have that $s = 1$ and $p_1 = q_1$. Hence, $P(1)$ is a true statement.

(II) Now, let $k \in \mathbb{N}$ suppose that $P(k)$ is a true statement, that is

$$\text{if } p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_s \text{ for some primes } p_1, p_2, \ldots, p_k \text{ and } q_1, q_2, \ldots, q_s \text{ such that } p_1 \leq p_2 \leq \cdots \leq p_k \text{ and } q_1 \leq q_2 \leq \cdots \leq q_s, \text{ then } k = s \text{ and } p_i = q_i \text{ for all } i \in \mathbb{N} \text{ with } 1 \leq i \leq k.$$

Now, suppose that $p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_t$ for some primes $p_1, p_2, \ldots, p_{k+1}$ and $q_1, q_2, \ldots, q_t$ such that $p_1 \leq p_2 \leq \cdots \leq p_i$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. Note that since $k \geq 1$, $p_1 p_2 \cdots p_{k+1}$ is not prime, and hence $t \geq 2$. Let p be the largest prime such that $p \mid p_1 p_2 \cdots p_{k+1}$. Then $p \mid p_i$ for some i with $1 \leq i \leq k+1$. Since p_i is prime, we must have $p = p_i$. Then $p = p_i \leq p_{k+1}$. Further, by our choice of p, we have that $p \geq p_{k+1}$. It follows that $p = p_{k+1}$.

A similar argument shows that $p = q_t$, and hence $p_{k+1} = q_t$. Then $p_1 \cdots p_k = q_1 \cdots q_{t-1}$. By the induction hypothesis, we have that $k = t - 1$ and $p_i = q_i$ for i with $1 \leq i \leq k$. Therefore, $k + 1 = t$ and $p_i = q_i$ for all i with $1 \leq i \leq k + 1$.

Hence, we have shown that if $P(k)$ is true then $P(k+1)$ is true. By the Principle of Mathematical Induction, it follows that $P(r)$ is true for all natural numbers r.

Setting $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, the result follows.

□

Example. *We will use the Fundamental Theorem of Arithmetic to find all primes p such that $5p + 9 = n^2$, for some $n \in \mathbb{N}$.*

First, we suppose we have a prime p such that $5p + 9 = n^2$ for some $n \in \mathbb{N}$. We want to find constraints on p. We have that

$$5p = (n + 3)(n - 3).$$

By the Fundamental Theorem of Arithmetic, the only positive factors of $5p$ are $1, 5, p$ and $5p$. Let us now consider all possible cases subject to these constraints.

(i) Suppose $n + 3 = 1$. Then $n - 3 = -5$, that is $5p = (n + 3)(n - 3) = -5$. But this implies that $p = -1$, which is not prime. It follows that $n + 3 \neq 1$.

(ii) Suppose $n + 3 = 5$. Then $n - 3 = -1$, so $5p = (n + 3)(n - 3) = -5$ and hence $p = -1$, which is a contradiction. Hence, $n + 3 \neq 5$.

(iii) Suppose $n + 3 = p$. Then $n - 3 = p - 6$, so $5p = p(p - 6)$. Hence $5 = p - 6$, so $p = 11$, which is prime.

(iv) Suppose $n + 3 = 5p$. Then $5p = (n + 3)(n - 3) = 5p(n - 3)$. Hence $n - 3 = 1$, and so $n = 4$. Then $5p = (n + 3)(n - 3) = 7$. But this is not possible since $5 \nmid 7$. Hence, $n + 3 \neq 5p$.

Summarising all of the above cases, we have that if p is a prime such that $5p + 9 = n^2$, for some $n \in \mathbb{N}$, then $p = 11$.

On the other hand, let $p = 11$. Then

$$5p + 9 = 55 + 9 = 64 = 8^2.$$

Summarising, we have that p is prime with $5p + 9 = n^2$, for some $n \in \mathbb{N}$, if and only if $p = 11$.

Example. *One can use induction and the Fundamental Theorem of Arithmetic to prove the following generalisation of the Chinese Remainder Theorem:*

Let $r \in \mathbb{N}$ with $r \geq 2$, and let $m_1, \ldots, m_r \in \mathbb{N}$ be pairwise relatively prime, that is $\gcd(m_i, m_j) = 1$ for $i, j \in \mathbb{Z}$ with $1 \leq i \leq r$, $1 \leq j \leq r$ and $i \neq j$. Then for any $a_1, \ldots, a_r \in \mathbb{Z}$, there exists some $x \in \mathbb{Z}$ such that

$$x \equiv a_i \ (mod\ m_i)$$

for all $i \in \mathbb{Z}$ with $1 \leq i \leq r$. Further, for $x' \in \mathbb{Z}$, we have

$$x' \equiv a_i \ (mod\ m_i)$$

for $i = 1, 2, \ldots, r$ if and only if

$$x' \equiv x \ (mod\ m_1 m_2 \cdots m_r).$$

We have the following corollaries.

Corollary 7.7. *For $x \in \mathbb{Q}_+$, $\exists!\, a, b \in \mathbb{N}$ with $\gcd(a,b) = 1$ such that $x = \frac{a}{b}$.*

Proof. Take $x \in \mathbb{Q}_+$. Then there exist $a, b \in \mathbb{Z}$ with $a, b \neq 0$ such that $x = \frac{a}{b}$. Since $x > 0$, we have that

$$x = |x| = \frac{|a|}{|b|},$$

so we have that x is a quotient of two elements of $\mathbb{N}$. So suppose that $a, b > 0$. Let $c = \gcd(a,b)$, and take $a', b' \in \mathbb{N}$ such that $a = ca'$ and $b = cb'$. Then $\gcd(a', b') = 1$ and $x = \frac{a'}{b'}$. It remains to show that a', b' are unique.

So suppose that there exist $c, d \in \mathbb{N}$ such that $x = \frac{a}{b} = \frac{c}{d}$ with $\gcd(a,b) = 1 = \gcd(c,d)$. Then $ad = bc$. Now, suppose $a = 1$. Then $d = bc$, so $c \mid d$. Since $\gcd(c,d) = 1$ and $c > 0$, this means that $c = 1$ and hence $a = c$ and $b = d$.

So suppose that $a > 1$. Then $a = p_1 \cdots p_r$ for some $r \in \mathbb{N}$ and primes $p_1, \ldots, p_r$. We will now prove by induction on r that $a = c$ and $b = d$.

Let $P(r)$ be the following statement.

$$\text{If } x = \tfrac{a}{b} = \tfrac{c}{d} \text{ with } \gcd(a,b) = \gcd(b,d) = 1 \text{ and } a = p_1 \cdots p_r \text{ for primes } p_1, \ldots, p_r, \text{ then } a = c \text{ and } b = d.$$

(I) First, suppose that $a = p_1$, where p_1 is prime. We have that $p_1 \mid bc$ and $\gcd(a,b) = 1$, so $\gcd(p_1, b) = 1$. Hence, $p_1 \mid c$. Then $c = p_1 c'$ for some $c' \in \mathbb{N}$. So $d = bc'$ and we have that $c' \mid d$. Since $\gcd(c,d) = 1$ and c' is a positive factor of d, we must have $c' = 1$ and hence $a = p_1 = c$ and $b = d$. Hence, $P(1)$ is a true statement.

(I) Now, let $k \in \mathbb{N}$ and suppose that $P(k)$ is a true statement, that is

$$\text{If } x = \tfrac{a}{b} = \tfrac{c}{d} \text{ with } \gcd(a,b) = \gcd(b,d) = 1 \text{ and } a = p_1 \cdots p_k \text{ for primes } p_1, \ldots, p_k, \text{ then } a = c \text{ and } b = d.$$

This means that whenever $p_1, \ldots, p_k$ are prime and $b', c', d' \in \mathbb{N}$ are such that $\gcd(p_1 \cdots p_k, b') = 1 = \gcd(c', d')$ with $p_1 \cdots p_k d' = b'c'$, we have $p_1 \cdots p_k = c'$.

Now, let $a = p_1 \cdots p_k p_{k+1}$ where $p_1, \ldots, p_k, p_{k+1}$ are prime. Then $p_{k+1} \mid c$, so $c = p_{k+1} c'$ for some $c' \in \mathbb{N}$. Therefore $p_1 \cdots p_k d = bc'$, so by the induction hypothesis, we have that $p_1 \cdots p_k = c'$. Hence $a = c$ and $b = d$.

Hence, we have shown that if $P(k)$ is true then $P(k+1)$ is true. By the Principle of Mathematical Induction, it follows that $P(r)$ is true for all natural numbers r. □

Corollary 7.8. *There are infinitely many prime numbers in $\mathbb{N}$.*

Euclid's Proof. To the contrary, suppose that there are only finitely many primes, say $p_1, p_2, \ldots, p_m$ for some $m \in \mathbb{N}$. Set $n = p_1 p_2 \cdots p_m + 1$. Clearly $m \geq 2$, as 2 and 3 are prime. Hence $n > 1$. By the Fundamental Theorem of Arithmetic, n can be factored as a product of primes. So we let q be some prime dividing n. Then $n = qk$ for some $k \in \mathbb{N}$. Since there are only finitely many primes, we must have that $q = p_j$ for some $j \in \mathbb{N}$, $1 \leq j \leq m$. Hence,

$$n = p_j k = p_1 p_2 \cdots p_m + 1,$$

so

$$1 = n - p_1 p_2 \cdots p_m = p_j \left(k - \frac{p_1 p_2 \cdots p_m}{p_j} \right).$$

Hence the prime p_j divides 1, which is a contradiction. The result follows. □