Appendix A More Proofs using Contradiction, Construction and Induction

A.1 More Proofs using Contradiction

We have the following examples.

Example 1. *Let $p \in \mathbb{N}$ be prime. Show that $\sqrt{p}$ is irrational.*

Proof. To the contrary, suppose that $\sqrt{p}$ is rational. Then we can write $\sqrt{p} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ such that $b \neq 0$, and we can assume $\gcd(a, b) = 1$. Then

$$\begin{aligned} \sqrt{p} &= \frac{a}{b} \\ p &= \frac{a^2}{b^2} \\ pb^2 &= a^2 \end{aligned}$$

Hence, we have that $p \mid a$. It follows that $a = pc$, for some $c \in \mathbb{Z}$. Then

$$pb^2 = (pc)^2 = p^2c^2,$$

so $b^2 = pc^2$, and hence we have that $p \mid b$. But then $p \mid \gcd(a, b)$, which contradicts that $\gcd(a, b) = 1$. Therefore, $\sqrt{p}$ cannot be rational. □

Example 2. *Show that there are infinitely many primes in $\mathbb{N}$ and that the set of primes is countable.*

Proof. Let X be the set of primes. Note that since $X \subseteq \mathbb{N}$, we know that X is either finite or countable. To the contrary, suppose there are only finitely many primes in $\mathbb{N}$, and let t denote the number of primes. We know there is at least one prime, namely 2, so $t \geq 1$. So let $p_1, p_2 \ldots, p_t$ be all the primes in $\mathbb{N}$. Now, consider $m = p_1p_2 \cdots p_t + 1$. Since $m \in \mathbb{Z}$ with $m > 1$, we know that there exists some prime $q \in \mathbb{N}$ such that $q \mid m$ by the Fundamental Theorem of Arithmetic. Hence, there exists some $m' \in \mathbb{Z}$ such that $m = qm'$, and therefore, $1 = qm' - p_1p_2 \cdots p_t$. Since we assumed that there are only finitely many primes, we must have that $q = p_j$ for some $j \in \mathbb{Z}$ with $1 \leq j \leq t$. Then $1 = p_jm' - p_1 \cdots p_t$, so $p_j \mid 1$, which is a contradiction since $q = p_j$ is prime. Therefore, there cannot be finitely many primes. The result follows. □

A.2 More Proofs by Construction

Given $a, b, c \in \mathbb{Z}$, we can use Euclid's algorithm to find all $x, y \in \mathbb{Z}$ such that $ax + by = c$. Before we continue to prove the general theorem in Example 4, let us consider a specific example in Example 3.

Example 3. *Construct all $x, y \in \mathbb{Z}$ such that $6x + 8y = 2$.*

Proof. First note that for $x, y \in \mathbb{Z}$, we have that $6x + 8y = 2$ if and only if we have $3x+4y = 1$. Since $\gcd(3, 4) = 1$, we know that there exist $s, t \in \mathbb{Z}$ such that $3s+4t = 1$ by Euclid's algorithm. Setting $s = -1$ and $t = 1$, we have $3 \cdot (-1) + 4 \cdot 1 = 1$. Now, suppose we also have $x, y \in \mathbb{Z}$ such that $3x + 4y = 1$. Hence,

$$3s + 4t = 3x + 4y$$
$$3(s - x) = 4(y - t).$$

Then $3 \mid 4(y-t)$, and since $\gcd(3, 4) = 1$, it follows that $3 \mid y-t$. Thus, there exists some $k \in \mathbb{Z}$ such that $y - t = 3k$, or equivalently, $y = t + 3k$. Similarly, we have that $4 \mid s - x$, so there exists some $k' \in \mathbb{Z}$ such that $x = s - 4k'$. Then

$$3s + 4t = 3x + 4y = 3(s - 4k') + 4(t + 3k),$$

so $0 = -12k'+12k$, or equivalently, $k' = k$. Hence, we have shown that if $s, t, x, y \in \mathbb{Z}$ such that $3s + 4t = 1 = 3x + 4y$, then there exists $k \in \mathbb{Z}$ such that $x = s - 4k$ and $y = t + 3k$.

On the other hand, suppose that $3s + 4t = 1$. Take any $k \in \mathbb{Z}$ and set $x = s - 4k$ and $y = t + 3k$. Then

$$3x + 4y = 3s + 4t = 1.$$

So $3x + 4y = 1$ if and only if $x = -1 - 4k$ and $y = 1 + 3k$ for some $k \in \mathbb{Z}$. It follows that $6x + 8y = 2$ if and only if $x = -1 - 4k$ and $y = 1 + 3k$ for some $k \in \mathbb{Z}$. □

More generally, we have the following examples.

Example 4. *Fix $a, b, c \in \mathbb{Z}$ such that $a, b \neq 0$ and let $d = \gcd(a, b)$. Take $a', b' \in \mathbb{Z}$ such that $a = da'$ and $b = db'$. Show that*

(i) if $d \nmid c$, there do not exist $x, y \in \mathbb{Z}$ such that $ax + by = c$.

(ii) if $d \mid c$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$.

(iii) $ax + by = c$ if and only if there exists $k \in \mathbb{Z}$ such that $x = s - b'k$ and $y = t + a'k$.

Proof.

(i) The contrapositive of the statement 'if $d \nmid c$, then there do not exist $s, t \in \mathbb{Z}$ such that $ax+by = c$' is given by 'if $\exists x, y \in \mathbb{Z}$ such that $ax+by = c$ then $d|c$'. So suppose that $x, y \in \mathbb{Z}$ are such that $ax + by = c$. Thus

$$c = da'x + db'y = d(a'x + b'y),$$

so $d|c$ since $a'x + b'y \in \mathbb{Z}$. The result follows by contrapositive.

(ii) Let $d \mid c$. Then there exists $c' \in \mathbb{Z}$ such that $c = dc'$. By Eulcid's algorithm, we know $\exists s', t' \in \mathbb{Z}$ such that $as' + bt' = d$. Set $s = s'c'$, $t = t'c'$. Then

$$as + bt = (as' + bt')c' = dc' = c.$$

(iii) ($\Rightarrow$) Let $ax+by = c$. Since $as+bt = c = ax+by$, we have $a(s-x) = b(y-t)$. Hence $a'(s - x) = b'(y - t)$ [where, as above, $d = \gcd(a, b)$ and $a = da'$, $b = db'$ for some $a', b' \in \mathbb{Z}$ with $\gcd(a', b') = 1$]. Hence $a'|b'(y-t)$, and since $\gcd(a', b') = 1$, we have $a'|(y-t)$. Similarly, $b'|a'(s-x)$, $\gcd(a', b') = 1$, so $b'|(s-x)$. Therefore

$\exists k, k' \in \mathbb{Z}$ such that $y - t = a'k$ and $s - x = b'k'$, or equivalently, $y = t + ak$ and $x = s - bk'$. Using that $a's + b't = a'x + b'y$, we get

$$a's + b't = a'(s - b'k') + b'(t + a'k),$$

so $0 = -a'b'k' + a'b'k$. Since $a'b' \neq 0$, this means $k' = k$, and thus $x = s - b'k$, $y = t + a'k$.

($\Leftarrow$) Suppose there exists $k \in \mathbb{Z}$ such that $x = s - b'k$ and $y = t + a'k$. Since $s, t \in \mathbb{Z}$ and $a = a'd$, $b = b'd$, $c = c'd$ and $d \neq 0$, we have $a's + b't = c'$. Then

$$a'x + b'y = a'(s - b'k) + b'(t + a'k) = a's + b't = c',$$

and hence $ax + by = c$.

Summarising, $ax + by = c$ if and only if there exists $k \in \mathbb{Z}$ such that $x = s - b'k$ and $y = t + a'k$.

□

Example 5. *Fix $a, b, n \in \mathbb{Z}$ such that $n \geq 1$. Show that there exists some $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$ if and only if $\gcd(a, n) \mid b$.*

Proof.

($\Rightarrow$) Suppose first that $x \in \mathbb{Z}$ such that $as \equiv b \pmod{n}$. Thus $ax - b = nk$ for some $k \in \mathbb{Z}$. Hence $ax - nk = b$. Let $d = \gcd(a, n)$, and take $a', n' \in \mathbb{Z}$ such that $a = a'd$, $n = n'd$. Thus $b = a'dx - n'dk = d(a'x - n'k)$; since $a'x - n'k \in \mathbb{Z}$, we have that $d \mid b$.

($\Leftarrow$) Now suppose that $d \mid b$ where $d = \gcd(a, n)$. Thus by the preceding exercise, $\exists x, y \in \mathbb{Z}$ such that $ax + ny = b$. Hence $n|(ax - b)$, and thus $ax \equiv b \pmod{n}$.

Summarising, we have that there exists some $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$ if and only if $\gcd(a, n) \mid b$. □

Example 6. *Suppose $n \in \mathbb{N}$. Show that $\gcd(n, n + 1) = 1$.*

Proof. Let $d = \gcd(n, n + 1)$. Thus $n = dx$ and $n + 1 = dy$ for some $x, y \in \mathbb{Z}$. Thus $dx+1 = n+1 = dy$, so $1 = dy-dx = d(y-x)$. Since $y-x \in \mathbb{Z}$, this means $d|1$. But the only integers that divide 1 are ± 1; since $\gcd(n, n+1) \geq 1$, we must have $\gcd(n, n+1) = 1$. □

A.3 More Proofs by Induction

We have the following examples.

Example 7. *Suppose $m \in \mathbb{N}$ such that $m \geq 2$, and let $A_1, A_2, \ldots, A_m$ be non-empty, finite sets. Show that*

(i) if $A_1, \ldots, A_m$ are pairwise disjoint, that is for $i, j \in \mathbb{N}$ with $i, j \leq m$ and $i \neq j$ we have $A_i \cap A_j = \emptyset$, we have that

$$| A_1 \cup A_2 \cup \cdots \cup A_m | = | A_1 | + | A_2 | + \cdots + | A_m | .$$

(ii) $| A_1 \times A_2 \times \cdots \times A_m | = | A_1 | \, | A_2 | \cdots | A_m |$.

Proof.

(i) Let $P(m)$ be the following statement: if $A_1, \ldots, A_m$ are pairwise disjoint, then $| A_1 \cup A_2 \cup \cdots \cup A_m | = | A_1 | + | A_2 | + \cdots + | A_m |$.

We will prove by induction that $P(m)$ holds for all $m \geq 2$.

(I) Let $|A_1| = s$, $|A_2| = t$. Thus we know there exist bijections $f : \{1, 2, \ldots, s\} \to A_1$ and $g : \{1, 2, \ldots, t\} \to A_2$. Define $h : \{1, 2, \ldots, s+t\} \to A_1 \cup A_2$ by

$$h(i) = \begin{cases} f(i) & \text{if } i \leq s, \\ g(i-s) & \text{if } s < i. \end{cases}$$

We claim h is bijective. To see h is surjective, take $x \in A_1 \cup A_2$. [So $x \in A_1$ or $x \in A_2$.] If $x \in A_1$ then there is some $i \in \{1, 2, \ldots, s\}$ such that $x = f(i) = h(i)$. If $x \in A_2$ then there is some $j \in \{1, 2, \ldots, t\}$ such that $x = g(j) = h(j+s)$. Hence h is surjective. To see h is injective, suppose $i, j \in \{1, 2, \ldots, s+t\}$ such that $h(i) = h(j)$. Let $x = h(i)$. If $i, j \leq s$ then $x, y \in A_1$, and $f(i) = h(i) = x = h(j) = f(j)$, and since f is injective, we have $i = j$. If $i, j > s$ then $x, y \in A_2$, then $g(i-s) = h(i-s) = x = h(j-s) = g(j-s)$, and since g is injective we have $i = j$. If $i \leq s$ and $j > s$, then $x \in A_1 \cap A_2$ (since $h(i) = f(i) \in A_1$ and $h(j) = g(j-s) \in A_2$); but this is impossible since $A_1 \cap A_2 = \emptyset$. Similarly, if $i > s$ and $j \leq s$, $x \in A_1 \cap A_2$, which is impossible. So if $h(i) = h(j)$ for some $i, j \in \{1, 2, \ldots, s+t\}$ then $i = j$, and hence h is injective. Since h is both surjective and injective, h is bijective.

(II) Suppose $k \in \mathbb{Z}$ with $k \geq 2$, and suppose $|A_1 \cup \cdots \cup A_k| = |A_1| + \cdots + |A_k|$. Set $A = A_1 \cup \cdots \cup A_k$. Then by the base case, $|A \cup A_{k+1}| = |A| + |A_{k+1}|$. By the induction hypothesis, $|A| = |A_1| + \cdots + |A_k|$. Hence $|A_1 \cup \cdots \cup A_k \cup A_{k+1}| = |A_1| + \cdots + |A_k| + |A_{k+1}|$. So if $P(k)$ holds, then $P(k+1)$ holds.

By the Principle of Mathematical Induction, $P(m)$ holds for all $m \geq 2$.

(ii) Let $P(m)$ be the following statement.

$$| A_1 \times A_2 \times \cdots \times A_m | = | A_1 | \, | A_2 | \cdots | A_m |.$$

We will show that $P(m)$ is a true statement, for all $m \in \mathbb{N}$ with $m \geq 2$, by giving a proof by induction.

(I) First, let us consider $m = 2$. So suppose that $| A_1 | = s$, $| A_2 | = t$, for some $s, t \in \mathbb{N}$. Then there exist bijections $f : \{1, 2, \ldots, s\} \to A_1$ and $g : \{1, 2, \ldots, t\} \to A_2$. For $i, j \in \mathbb{N}$ with $i \leq s$ and $j \leq t$, set $a_i = f(i)$ and set $b_j = g(j)$. Note that since f and g are bijections, we have that $a_1, a_2, \ldots, a_s$ are distinct and $b_1, b_2, \ldots, b_t$ are distinct.
Now, define $h : \{1, 2, \ldots, st\} \to A_1 \times A_2$ as follows. Take $n \in \{1, 2, \ldots, st\}$. Hence, by the division algorithm for $\mathbb{Z}$, there exist unique $q, r \in \mathbb{Z}$ such that $n = tq + r$ where $1 \leq r \leq t$. Note that since $n \geq 1$, we must have $q \geq 0$, for if $q < 0$ then $q \leq -1$ and $n \leq -t + r \leq 0$. Further, we have that $q < s$ since otherwise $st + 1 \leq n = tq + r \leq st$. Hence, $a_{q+1} \in A_1$ and $b_r \in A_2$. We define

$$h(n) = (a_{q+1}, b_r) \text{ where } q, r \in \mathbb{Z} \text{ such that } n = tq + r \text{ with } 1 \leq r \leq t.$$

Since the conditions on q and r determine them uniquely, we have that h is well-defined.

We need to show that h is bijective. Suppose first that $m, n \in \{1, 2, \ldots, st\}$ such that $h(m) = h(n)$. Take the unique $q, r, q', r' \in \mathbb{Z}$ such that $n = tq + r$, $m = tq' + r'$ where $1 \leq r \leq t$, $1 \leq r' \leq t$. Then

$$(a_{q'+1}, b_{r'}) = f(m) = f(n) = (a_{q+1}, b_r).$$

Hence, we have $a_{q'+1} = a_{q+1}$ and $b_{r'} = b_r$. Then $q'+1 = q+1$ since $a_1, a_2, \ldots, a_s$ are distinct, and $r' = r$ since $b_1, b_2, \ldots, b_t$ are distinct. It follows that $m = tq'+r' = tq+r = n$, showing that h is injective. Now, take an arbitrary element $(a_i, b_j) \in A_1 \times A_2$. Then $1 \leq i \leq s$ and $1 \leq j \leq t$, so $1 \leq t(i-1) + j \leq st$. Hence, with $n = t(i-1) + j$, we have that $h(n) = (a_i, b_j)$, showing that h is surjective. Therefore, h is bijective. It follows that $| A_1 \times A_2 | = st = | A_1 | \, | A_2 |$, so $P(2)$ is a true statement.

(II) Now assume that $P(k)$ is true for some integer $k \geq 2$, that is

$$| A_1 \times A_2 \times \cdots \times A_k | = | A_1 | \, | A_2 | \cdots | A_k | .$$

Set $A = A_1 \times A_2 \times \cdots \times A_k$. Then

$$| A_1 \times \cdots \times A_k \times A_{k+1} | = | A \times A_{k+1} |,$$

and by the above argument, we know that $| A \times A_{k+1} | = | A | \cdot | A_{k+1} |$. Then

$$| A_1 \times A_2 \times \cdots \times A_k \times A_{k+1} | = | A | \cdot | A_{k+1} | = | A_1 | \, | A_2 | \cdots | A_k | \cdot | A_{k+1} |,$$

showing that if $P(k)$ is true then $P(k+1)$ is true.

By the Principle of Mathematical Induction, it follows that $P(m)$ is true for all natural numbers $m \geq 2$.

□

Example 8. *Show that the union of countably many non-empty and pairwise disjoint finite sets is countable.*

Proof. [This solution is very similar to the proof in the notes that a countable union of countable sets is countable.]

For each $k \in \mathbb{N}$, enumerate the elements of A_k as $a_{k1}, a_{k2}, \ldots, a_{kn_k}$ [where $n_k = |A_k|$, and hence for $i \neq j$, we have $a_{ki} \neq a_{kj}$]. Define $f : \bigcup_{k=1}^{\infty} A_k \to \mathbb{N} \times \mathbb{N}$ by $f(x) = (i, j)$ where $i \in \mathbb{N}$ such that $x \in A_i$ and $j \in \mathbb{N}$ such that $x = a_{ij}$. Since $A_1, A_2, A_3, \ldots$ are pairwise disjoint, for any $x \in \bigcup_{k=1}^{\infty} A_k$, there is a unique $i \in \mathbb{N}$ such that $x \in A_i$, and then there is a unique $j \in \mathbb{N}$ with $j \leq n_i$ such that $x = a_{ij}$; hence this definition for f is unambiguous and thus defines a function. We claim that f is injective. Suppose $x, x' \in \bigcup_{k=1}^{\infty} A_k$ such that $f(x) = f(x')$. Take $i, j \in \mathbb{N}$ such that $f(x) = (i, j)$; thus $x = a_{ij}$. Since $f(x') = f(x) = (i, j)$, we also have $x' = a_{ij}$. Hence $x = x'$ and so f is injective. Since $\mathbb{N} \times \mathbb{N}$ is countable, this means $\bigcup_{k=1}^{\infty} A_k$ is finite or countable. We claim that $\bigcup_{k=1}^{\infty} A_k$ is infinite, and hence countable: Let $B = \{a_{k1} : \ k \in \mathbb{N} \}$. We know the A_k are pairwise disjoint, so for $j, k \in \mathbb{N}$, we have $a_{j1} \neq a_{k1}$; hence B is an infinite set. Since $B \subseteq \bigcup_{k=1}^{\infty} A_k$, we must have that $\bigcup_{k=1}^{\infty} A_k$ is infinite, and thus countable. □

Example 9. *Let A and B be non-empty finite sets such that $\mid A \mid = \mid B \mid$. Show that*

(i) if $f : A \to B$ is injective, we have that f is bijective.

(ii) if $f : A \to B$ is surjective, we have that f is bijective.

Proof. Let $n \in \mathbb{N}$ such that $n = \mid A \mid$. Then $\mid B \mid = n$, and there are bijections $g : \{1, 2, \ldots, n\} \to A$ and $h : \{1, 2, \ldots, n\} \to B$. For $i \in \{1, 2, \ldots, n\}$, set $a_i = g(i)$ and $b_i = h(i)$. Since g is injective, we have that $a_1, \ldots, a_n$ are distinct and $b_1, \ldots, b_n$ are distinct.

(i) Suppose that $f : A \to B$ is injective. Then $f(a_1), \ldots, f(a_n)$ are distinct, so $\mid f[A] \mid = \mid A \mid = n$. Since $f[A] \subseteq B$ and $\mid f[A] \mid = \mid B \mid = n \leq \infty$, we must have that $f[A] = B$. Hence, f is surjective and therefore bijective.

(ii) Suppose that $f : A \to B$ is surjective. To the contrary, suppose that f is not bijective. Then f is not injective. Hence, there exist $i, j \in \{1, 2, \ldots, n\}$ such that $a_i \neq a_j$ but $f(a_i) = f(a_j)$. Since $a_i \neq a_j$, we have that $i \neq j$. Then

$$f[A] = \{a_k : k \in \mathbb{Z},\ 1 \leq k \leq n,\ k \neq j\}.$$

So $\mid f[A] \mid < n$. But since f is surjective, we know that $f[A] = B$ and hence $\mid f[A] \mid = \mid B \mid = n$, which is a contradiction. Therefore, we must have that f is injective and hence bijective.

□

Example 10. *Finally, we offer a 'party trick' based on the theory presented in these notes.*

Take $x \in \mathbb{N}$. We write x as a decimal expansion given by

$$a_m a_{m-1} \cdots a_1 a_0$$

where $a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ for $0 \leq i \leq m$. Then

$$x = \sum_{i=0}^{m} a_i 10^i.$$

We know $10 \equiv 1 \ (mod\ 9)$. The using induction, one shows that, for all $i \in \mathbb{N}$, we have $10^i \equiv 1 \ (mod\ 9)$. Next, using induction again, one shows that

$$\sum_{i=0}^{m} a_i 10^i \equiv \sum_{i=0}^{m} a_i \ (mod\ 9).$$

Recall that x is divisible by 9 if and only if $x \equiv 0 \ (mod\ 9)$, so x is divisible by 9 if and only if the digits of x sum to a number divisible by 9.

One can devise a similar party trick to test for divisibility by 11. In this case, one uses that for $i \in \mathbb{Z}$, $i \geq 0$, $10^i \equiv 1 \ (mod\ 11)$ when i is even, and $10^i \equiv -1 \ (mod\ 11)$ when i is odd. So what is the party trick???

We have the following definition.

Definition. For $n \in \mathbb{N}$, we define $n!$ to be the product of all the positive integers less than or equal to n; for later convenience, we define $0!$ to be 1. (So $1! = 1$, $2! = 2 \cdot 1$, $3! = 3 \cdot 2 \cdot 1$, etc.) We read $n!$ as "n factorial". For $n, k \in \mathbb{Z}$ with $0 \leq k \leq n$, we define

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

We read $\binom{n}{k}$ as "n k", and we call $\binom{n}{k}$ a binomial coefficient (the reason for this will be made clear shortly).

Example 11. *Suppose $n, k \in \mathbb{Z}$ with $0 < k \leq n$. Show that*

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n_1}{k}.$$

Proof. We know

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k_1)!}.$$

Also, $k! = (k-1)! \cdot k$, and $(n+1)! = n! \cdot (n+1)$. Thus

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n! \cdot k + n! \cdot (n-k+1)}{k!(n-k+1)!} \\
&= \frac{n! \cdot (n+1)}{k!(n-k+1)!} \\
&= \frac{(n+1)!}{k!(n+1-k)!} \\
&= \binom{n+1}{k}.
\end{aligned}$$

□

Example 12. *(The Binomial Theorem) For $a, b \in \mathbb{C}$ and $n \in \mathbb{N}$, show that*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Proof. Let $P(n)$ be the following statement: $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.
We will prove by induction that $P(n)$ holds for all $n \in \mathbb{N}$.

(I) Since $\binom{1}{0} = 1 = \binom{1}{1}$, we have

$$(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^k b^{1-k}.$$

Therefore, $P(1)$ holds.

(II) Let $m \in \mathbb{N}$ and suppose that $P(k)$ holds. Then

$$(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^k b^{m-k}.$$

Thus

$$\begin{aligned}
(a+b)^{m+1} &= a\cdot\sum_{k=0}^{m}\binom{m}{k}a^k b^{m-k} + b\cdot\sum_{k=0}^{m}\binom{m}{k}a^k b^{m-k}\\
&= \sum_{k=0}^{m}\binom{m}{k}a^{k+1}b^{m-k} + \sum_{k=0}^{m}\binom{m}{k}a^k b^{m+1-k}\\
&= \sum_{j=1}^{m+1}\binom{m}{j-1}a^j b^{m-j+1} + \sum_{k=0}^{m}\binom{m}{k}a^k b^{m+1-k}\\
&= a^{m+1} + \sum_{j=1}^{m}\binom{m}{j-1}a^j b^{m-j+1}\\
&\quad + \sum_{k=1}^{m}\binom{m}{k}a^k b^{m-k} + b^{m+1}\\
&= a^{m+1} + \sum_{k=1}^{m}\left(\binom{m}{k-1} + \binom{m}{k}\right)a^k b^{m-k+1} + b^{m+1}\\
&= \sum_{k=0}^{m+1}\binom{m+1}{k}a^k b^{m+1-k}.
\end{aligned}$$

Hence, if $P(k)$ holds, then $P(k+1)$ holds.

By the Principle of Mathematical induction, $P(n)$ holds for all $n \in \mathbb{N}$. □

Example 13. *Use induction to prove the following identities.*

(a) For $n \in \mathbb{N}$, $\sum_{i=1}^{n} i(i+2) = \frac{n(n+1)(2n+7)}{6}$.

(b) For $n \in \mathbb{N}$, $\sum_{i=1}^{n}(-1)^i i^2 = \frac{(-1)^n n(n+1)}{2}$.

Proof.

(i) [Scratch work: We long divide $2k^3+15k^2+31k+18$ by $k+1$ to deduce

$$2k^3+15k^2+31k+18 = (k+1)(2k^2+13k+18),$$

and then we long divide $2k^2+13k+18$ by $k+2$ to deduce that $2k^2+13k+18 = (k+2)(2k+9)$.]

Let $P(n)$ be the proposition that

$$\sum_{i=1}^{n} i(i+2) = \frac{n(n+1)(2n+7)}{6}.$$

(I) $1(1+2) = 3 = \frac{1(1+1)(2\cdot 1+7)}{6}$, so $P(1)$ holds.

(II) Suppose that $k \in \mathbb{N}$ and that $P(k)$ holds. Thus

$$\begin{aligned}
\sum_{i=1}^{k+1} i(i+2) &= (k+1)(k+2) + \sum_{i=1}^{k} i(i+2) \\
&= (k+1)(k+2) + \frac{k(k+1)(2k+7)}{6} \\
&= \frac{6(k^2+4k+3) + k(k+1)(2k+7)}{6} \\
&= \frac{6k^2+24k+18) + (2k^3+9k^2+7k)}{6} \\
&= \frac{2k^3+15k^2+31k+18}{6} \\
&= \frac{(k+1)(2k^2+13k+18)}{6} \\
&= \frac{(k+1)(k+2)(2k+9)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+7)}{6}.
\end{aligned}$$

Thus $P(k)$ implies that $P(k+1)$.

Hence by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{N}$.

(ii) Let $P(n)$ be the proposition that

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

(I) $(-1)^1 \cdot 1^2 = 1 = \frac{(-1)^1 \cdot 1 \cdot (1+1)}{2}$. Thus $P(1)$ holds.

(II) Suppose that $k \in \mathbb{N}$ and that $P(k)$ holds. Using this, we have

$$\begin{aligned}
\sum_{i=1}^{k+1} (-1)^i i^2 &= (-1)^{k+1}(k+1)^2 + \sum_{i=1}^{n} (-1)^i i^2 \\
&= (-1)^{k+1}(k+1)^2 + \frac{(-1)^k k(k+1)}{2} \\
&= \frac{(-1)^{k+1}(2k^2+4k+2) + (-1)^k(k^2+k)}{2} \\
&= \frac{(-1)^{k+1}(2k^2+4k+2-k^2-k)}{2} \\
&= \frac{(-1)^{k+1}(k^2+3k+2)}{2} \\
&= \frac{(-1)^{k+1}(k+1)(k+2)}{2}.
\end{aligned}$$

Thus $P(k)$ implies that $P(k+1)$.

Hence by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{N}$.

□

Example 14. *Find a formula for*

$$S(n) = \sum_{i=1}^{n} \frac{1}{i(i+1)},$$

and use induction to prove your formula.

Proof. We have $S(1) = \frac{1}{2}$, $S(2) = \frac{2}{3}$, $S(3) = \frac{3}{4}$, $S(4) = \frac{4}{5}$. So we conjecture/claim that for $n \in \mathbb{N}$, $S(n) = \frac{n}{n+1}$. [Now we attempt to prove this using induction.]

For $n \in \mathbb{N}$, let $P(n)$ be the proposition that $S(n) = \frac{n}{n+1}$.

(I) $S(1) = \frac{1}{2}$, so $P(1)$ holds.

(II) Suppose $k \in \mathbb{N}$ and $P(k)$ holds. Then

$$\begin{aligned} S(k+1) &= S(k) + \frac{1}{(k+1)(k+2)} \\ &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k(k+2)+1}{(k+1)(k+2)} \\ &= \frac{k^2+2k+1}{(k+1)(k+2)} \\ &= \frac{(k+1)^2}{(k+1)(k+1)} \\ &= \frac{k+1}{k+2}. \end{aligned}$$

Thus $P(k)$ implies $P(k+1)$.

Hence by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{N}$. □