Pure Math Topics

Nathaniel Green

February 14, 2025

The goal of this text is to summarize fundamental ideas in pure math. These ideas are used all throughout pure math and can even be found outside of pure math. Efforts have been made to offer both technical and intuitive explanations for most topics. This document may be updated to include better examples or new ideas.

Contents

1 Sets

A set is a collection of items. Neither order nor multiplicity matter in sets. Below lie several examples of sets.

Example.

$$A = \{1, 2, 3, 4, 5, 6\} \quad B = \{\text{cat},\ \text{dog},\ \text{mouse}\} \quad C = \{15, -75,\ \text{cat}, 15\} = \{\text{cat}, 15, -75\}$$

Several common sets which are deserving of their own symbols are listed below.

1. The set of *natural numbers*, $\mathbb{N} := \{1, 2, 3, 4, \ldots\}$ (sometimes $\mathbb{N}$ will include 0, but this is not normally the case).

2. The set of *integers*, $\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

3. The set of *rational numbers*, $\mathbb{Q} := \left\{\frac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \neq 0\right\}$.

4. The set of *real numbers*, $\mathbb{R}$ (rational numbers and all other numbers such as π, $\sqrt{2}$, $-\sqrt[3]{11}$).

5. The set of *complex numbers*, $\mathbb{C} := \{a + bi : a, b \in \mathbb{R}\}$ where $i := \sqrt{-1}$.

As seen above, sets can be defined in different ways. If it is clear from context, dots can be used, as in the definition of natural numbers and integers. The explicit statement of a set via the enumeration of its elements (including the use of dots) is referred to as *set roster notation*. The other way sets are written is through *set builder notation*. The format for set builder notation follows two typical patterns:

$$A = \{x \in X : x \text{ satisfies property } P\},$$

$$B = \{E(x) : x \in X\}.$$

Set A is read as "the set containing all elements x coming from the set X, such that x satisfies the property P." An example of this notation is seen in the set of even integers,

$$2\mathbb{Z} = \{x \in \mathbb{Z} : x \text{ is even}\}.$$

Set B is read as "the set of elements $E(x)$ (where $E(x)$ is some expression in terms of x), such that x is contained in X." This notation is sometimes referred to as set runner notation (the set of $E(x)$ where x runs through all the elements of X). The even integers can also be expressed in this pattern,

$$2\mathbb{Z} = \{2x : x \in \mathbb{Z}\}.$$

The pattern of set A can be thought of as a filter, whereas the pattern of set B is more like a generator.

If each element of a set A is contained in a set B, then we say A is a subset of B, written $A \subseteq B$ (or $B \supseteq A$). If $A \subseteq B$ but $A \neq B$, meaning B contains an element not in A, we say A is a proper subset of B and write $A \subset B$ (some authors will use $\subset$ to mean subset, and $\subsetneq$ to mean proper subset).

Example.

$$2\mathbb{Z} \subseteq \mathbb{Z} \qquad \mathbb{R} \subset \mathbb{C} \qquad \{-13, 15, 22, 1, 9\} \subseteq \{-13, 7, 91, 15, 22, 1, 9, 100\}$$

It is common to want to show one set is a subset of another. Say we want to show A is a subset of B. This is done by 'choosing' an arbitrary element of the set A and showing it is contained in B. The idea is, if the element of A was chosen arbitrarily, and then shown to be in B, the specifics of any given element of A aren't what guarantees them to be in B, the simple containment in A guarentees containment in B.

Example. Show that $\mathbb{R}$ is a subset of $\mathbb{C}$.

Proof. The complex numbers are defined to be $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$. Let $x \in \mathbb{R}$ and note,

$x = x + 0i$ and since x and 0 are in $\mathbb{R}$ we have $x = x + 0i \in \mathbb{C}$. Since an arbitrary element of $\mathbb{R}$ is in $\mathbb{C}$, we know $\mathbb{R} \subseteq \mathbb{C}$. $\square$

There are a variety of operations that can be performed on sets. Let A and B be nonempty sets. Below lie several operations,

1. *Set union*, $A \cup B \coloneqq \{x : x \in A \text{ or } x \in B\}$;
2. *Set intersection*, $A \cap B \coloneqq \{x : x \in A \text{ and } x \in B\}$;
3. *Set difference*, $A \backslash B \coloneqq \{x \in A : x \notin B\}$ (sometimes the notation $A - B$ is used);
4. *Set complement*, suppose $B \subseteq A$ then $\overline{B} \coloneqq \{x \in A : x \notin B\}$ (sometimes the notation B^c is used);
5. *Cartesian product*, $A \times B \coloneqq \{(a, b) : a \in A \text{ and } b \in B\}$.
6. *Power set*, the power set of A, denoted $\mathcal{P}(A) \coloneqq \{X : X \subseteq A\}$ is the set of all subsets of A.
7. *Cardinality*, the cardinality of a finite set A is the number of elements in the set, denoted by $|A|$. The cardinality of infinite sets will be touched on more in Section 5.

Although the definitions of set difference and set complement look the same, they are different. Performing a set complement on a set B requires B is a subset of some other set. Sometimes this will be stated explicitly, sometimes it comes from context. For example, $\overline{(1, 100)} = (-\infty, 1] \cup [100, \infty)$. Although it wasn't explicitly stated that the context of $(1, 100)$ was the real number line, it is an implicit assumption when talking about intervals. On the other hand, set difference makes no requirement of any inclusion relationship between the two sets. In fact, if $A \backslash B = A$ then we know A and B share no elements.

A common technique to show two sets A and B are equal is to show both $A \subseteq B$ and $B \subseteq A$.

2 Functions

Definition 2.1. A *function* $f : A \to B$ is defined to be a subset of $A \times B$ with the property that for all $a \in A$ there exists some $b \in B$ such that $(a, b) \in f$, and if $(a, b), (a, b') \in f$ then $b = b'$. Additionally, if $(a, b) \in f$ then we write $f(a) = b$.

This definition may seem clunky, but it captures the idea that every input is mapped to one and only one output.

Definition 2.2. A function $f : A \to B$ is said to be *injective* (or *one-to-one*) if $f(a) = f(a')$ implies $a = a'$.

This definition means no two distinct inputs map to the same output.

Definition 2.3. A function $f : A \to B$ is *surjective* (or *onto*) if for all $b \in B$ there exists an $a \in A$ such that $f(a) = b$.

This definition means every element of the codomain is mapped to by some element in the domain. If f is surjective we say f maps A **onto** B, otherwise we say f maps A **into** B.

Definition 2.4. A function $f : A \to B$ is a *bijection* (or a *one-to-one correspondence*) if f is both injective and surjective.

Example. Below lie examples of functions with each of these properties.

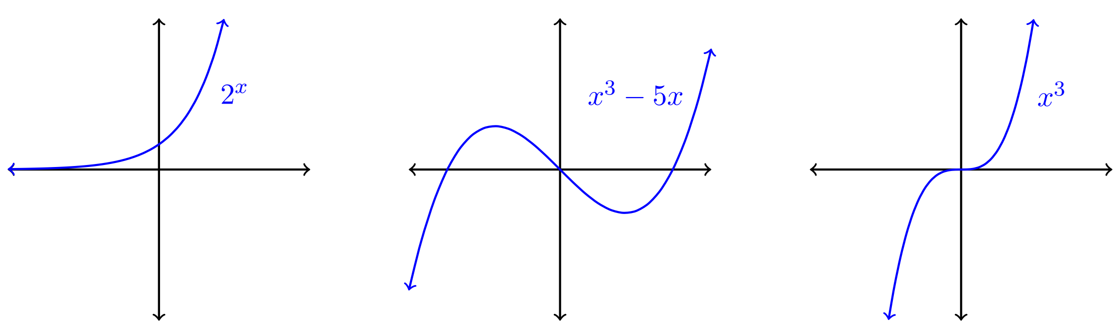

Figure 1: Injective, surjective, and bijective functions

3 Modular Arithmetic

Modular arithmetic is constantly used in daily life without people realizing it. Suppose it is 7:00 am, and you are asked what time it will be in 5 hours. Assuming you don't use military time, you would respond 2:00 pm without much thought. Now, if you were instead asked what time of the day it will be in 22 hours, after a moment of thought you would respond 5:00 am. This is modular arithmetic.

Definition 3.1. For $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ we say $a \mod n = r$ if $a = qn + r$ for some $q \in \mathbb{Z}$ and $0 \leq r < n$. We say two numbers a, b are *congruent* mod n if $a \mod n = b \mod n$, and we write $a \equiv b \pmod{n}$.

Example. Below lie several examples of modular arithmetic.

$$\begin{aligned} 5 &\mod 2 = 1 & 7 &\mod 5 = 2 & 19 &\mod 5 = 4 \\ 93 &\mod 17 = 8 & 15 &\mod 6 = 3 & -19 &\mod 5 = 1 \\ 5 &\mod 21 = 5 & 7 &\mod 1 = 0 & 125 &\mod 5 = 0 \end{aligned}$$

4 Logic

"Pure mathematics is, in its way, the poetry of logical ideas." - Emmy Noether

Logic is the most important part of math. Without logic, there is no math. Logic is the study of valid arguments, which are the core of math. Math is sometimes jocularly referred to as applied logic.

In logic there are statements, which have truth values, and relations between them. Below lie several important logic operators. Let p and q be statements,

1. *Not*, denoted $\neg p$, evaluates to true if p is false;

2. *And*, denoted $p \wedge q$, evaluates to true if p is true and q is true;

3. *Or*, denoted $p \vee q$, evaluates to true if at least one of p and q is true;

4. *Implies*, denoted $p \implies q$, evaluates to true so long as p is not true while q is false;

5. *Double implication*, denoted $p \iff q$, evaluates to true if both p and q have the same truth value (also referred to as equivalence).

Figure 2 features truth tables for each of the logical operators described above.

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

p	q	$p \implies q$
T	T	T
T	F	F
F	T	T
F	F	T

p	q	$p \iff q$
T	T	T
T	F	F
F	T	F
F	F	T

Figure 2: Truth tables for logical operators

There are several logical equivalences that are important to know. We use $\equiv$ to mean two logical statements have the same truth values.

1. *Contrapositive*, the contrapositive of the statement $p \implies q$ is $\neg q \implies \neg p$ and we have

$$(p \implies q) \equiv (\neg q \implies \neg p).$$

2. *De Morgan's Laws*, there are two De Morgan's Laws, the first states

$$\neg(p \vee q) \equiv \neg p \wedge \neg q,$$

   and the second states

$$\neg(p \wedge q) \equiv \neg p \vee \neg q.$$

3. *Negation of Implication*, the negation of the implication is $p \wedge \neg q$ and thus

$$\neg(p \implies q) \equiv p \wedge \neg q.$$

4. *Double Implication*, the double implication $p \iff q$ is the same as two implication, in symbols,

$$p \iff q \equiv (p \implies q) \wedge (q \implies p).$$

   The reverse implication $q \implies p$ is called the *converse* of $p \implies q$.

5. *Implication as a Disjunction*, the implication $p \implies q$ can be rewritten using an or statement, in symbols,

$$p \implies q \equiv \neg p \vee q.$$

5 Infinity

Infinity is a fascinating concept in mathematics. Much of our mathematical understanding of infinity can be attributed to Georg Cantor, who was pivotal in the development of set theory, which laid the groundwork for the rigorous study of infinity. One of Cantor's discoveries was that not all infinite sets have the 'same' number of elements; in other words, not all infinities are the same size.

Two sets A and B are said to have the same cardinality if there is a bijection f from A onto B.

Example. The sets $\mathbb{N}$ and $\mathbb{Z}$ have the same cardinality since the function $f : \mathbb{N} \to \mathbb{Z}$ defined by $f(n) \coloneqq (-1)^n \lfloor n/2 \rfloor$ is a bijection from $\mathbb{N}$ onto $\mathbb{Z}$.

Example. There is no bijection from $\mathbb{N}$ onto $\mathbb{R}$, so the set of real numbers is said to have more elements than the set of natural numbers.

Definition 5.1. If a set A is finite, or has the same cardinality as the natural numbers $\mathbb{N}$, then A is said to be *countable* (or *countably infinite* in the infinite case). If A is infinite and does not have the same cardinality as the natural numbers, then A is said to be *uncountable* (or *uncountably infinite*).

Figure 3 displays a bijection between $\mathbb{N}$ and $\mathbb{Z}$. Because a bijection between $\mathbb{N}$ and $\mathbb{Z}$ exists, we say that $\mathbb{Z}$ is a countable set. Another example of a countably infinite set is $\mathbb{Q}$.

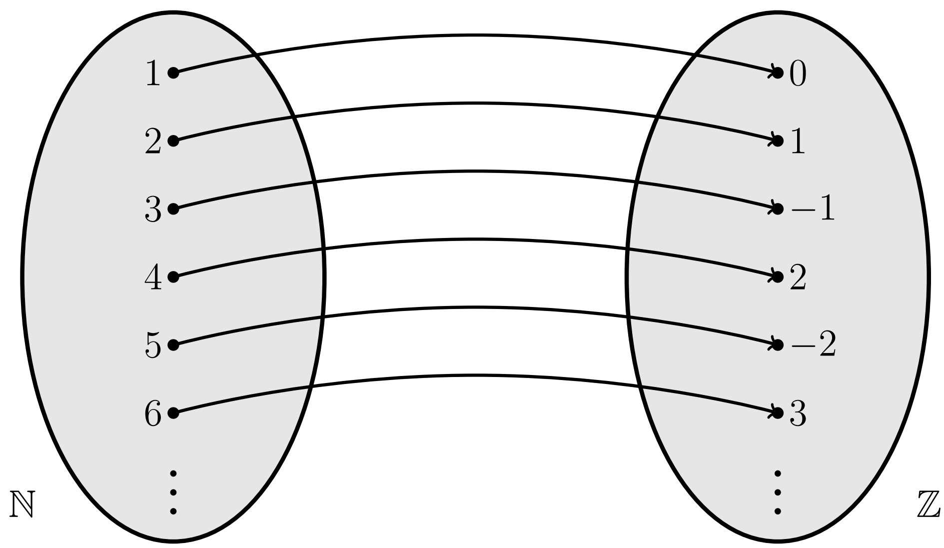

Figure 3: Bijection from $\mathbb{N}$ onto $\mathbb{Z}$

A theorem from Georg Cantor states that there is never a bijection between a set A and its powerset $\mathcal{P}(A)$. This means there is an infinite tower of sets with different infinite cardinalities $\aleph_0, \aleph_1, \aleph_2, \ldots$, such that $\aleph_\alpha < \aleph_{\alpha+1}$.

6 Relations

Definition 6.1. A *relation* R between two sets X and Y is a subset of the cartesian product $X \times Y$. We say that $x \in X$ is related to $y \in Y$, denoted xRy, if $(x, y) \in R$.

Definition 6.2. A relation $\sim$ on A is called an *equivalence relation* if the following properties hold:

(i) Reflexive, $a \sim a$ for all $a \in A$;

(ii) Symmetric, if $a \sim b$ then $b \sim a$ for all $a, b \in A$;

(iii) Transitive, if $a \sim b$ and $b \sim c$ then $a \sim c$, for all $a, b, c \in A$.

Example. Define the relation $\sim$ on $\mathbb{Z}$ by $a \sim b$ if $a \equiv b \pmod{n}$. We will show $\sim$ is an equivalence relation.

Proof. For $a \in \mathbb{Z}$ clearly $a \mod n = a \mod n$. Thus $\sim$ is reflexive. Now let $a, b \in \mathbb{Z}$ and suppose $a \sim b$. We have $a \mod n = b \mod n$ and since $b \mod n = a \mod n$ we have $b \sim a$ and thus $\sim$ is symmetric. Now suppose for some $a, b, c \in \mathbb{Z}$ we have $a \sim b$ and $b \sim c$. We have $a \mod n = b \mod n = c \mod n$ and thus $a \equiv c \pmod{n}$ so $a \sim c$ and $\sim$ is transitive. Therefore, $\sim$ defines an equivalence relation on $\mathbb{Z}$. $\square$

Definition 6.3. Let $\sim$ be an equivalence relation on a set A. For an element $a \in A$ we define the *equivalence class* of a to be the set $[a]_\sim := \{x \in A : a \sim x\}$. The set of equivalence classes is denoted by $[A]_\sim := \{[a]_\sim : a \in A\}$.

Example. Let $\sim_5$ be the equivalence relation on $\mathbb{Z}$ defined by $a \sim_5 b$ if $a \mod 5 = b \mod 5$. Then, the set of equivalence classes is

$$[\mathbb{Z}]_{\sim_5} := \{[a]_{\sim_5} : a \in \mathbb{Z}\} = \{[0]_{\sim_5}, [1]_{\sim_5}, [2]_{\sim_5}, [3]_{\sim_5}, [4]_{\sim_5}\}.$$

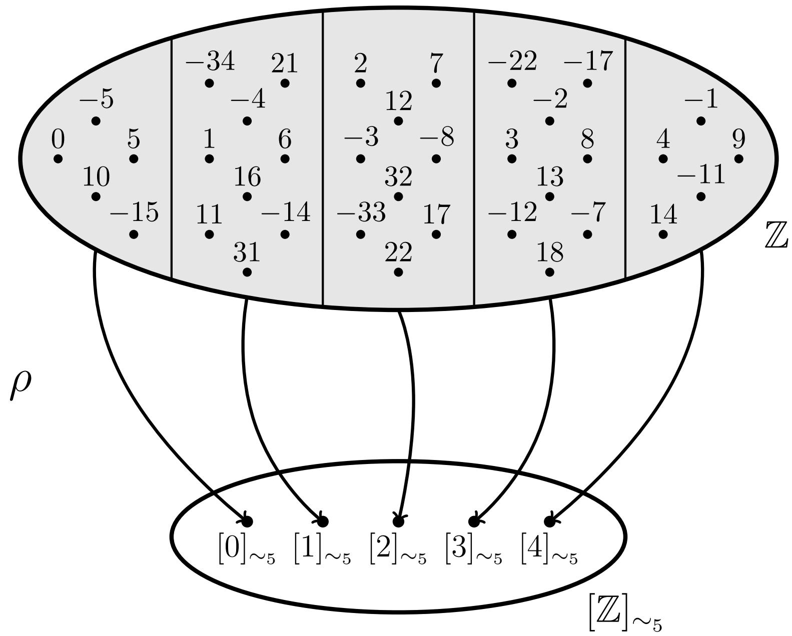

Figure 4: The map $\rho : \mathbb{Z} \to [\mathbb{Z}]_{\sim_5}$

Note, $[1]_{\sim_5} = [6]_{\sim_5} = [11]_{\sim_5} = \cdots = [5n+1]_{\sim_5}$ for $n \in \mathbb{Z}$. Further, we can view the entire set as such,

$$
\begin{aligned}
&[0]_{\sim_5} = [5]_{\sim_5} = [10]_{\sim_5} = \cdots = [5n]_{\sim_5}, && \forall n \in \mathbb{Z};\\
&[1]_{\sim_5} = [6]_{\sim_5} = [11]_{\sim_5} = \cdots = [5n+1]_{\sim_5}, && \forall n \in \mathbb{Z};\\
&[2]_{\sim_5} = [7]_{\sim_5} = [12]_{\sim_5} = \cdots = [5n+2]_{\sim_5}, && \forall n \in \mathbb{Z};\\
&[3]_{\sim_5} = [8]_{\sim_5} = [13]_{\sim_5} = \cdots = [5n+3]_{\sim_5}, && \forall n \in \mathbb{Z};\\
&[4]_{\sim_5} = [9]_{\sim_5} = [14]_{\sim_5} = \cdots = [5n+4]_{\sim_5}, && \forall n \in \mathbb{Z}.
\end{aligned}
$$

Figure 4 displays the map $\rho : \mathbb{Z} \to [\mathbb{Z}]_{\sim_5}$ defined by $a \mapsto [a]_{\sim_5}$. The image of this function $\rho(\mathbb{Z})$ is equal to the set of all equivalence classes of $\mathbb{Z}$ on the relation $\sim_5$.

7 Proof Strategies

There are several common proof strategies that are important to add to your mathematical toolbox.

7.1 Direct Proof

Direct proof is a very common, but very bare bones proof technique. Below lies a direct proof.

Example. Show that if n is odd then n^2 is odd.

Proof. Let $n \in \mathbb{Z}$ be an odd number. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. So, $(2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + k) + 1$ and since $(2k + 1)^2$ is equal to 2 times an integer plus 1, $(2k + 1)^2$ is odd. $\square$

In this proof, we wanted to prove a statement $p \implies q$. We did so by showing if we assume p to be true, then the conclusion q must be true.

7.2 Proof by Contradiction

Suppose you want to prove a statement. If we assume the statement is false and show that assumption leads to a contradiction, it means the statement cannot be false. Therefore the statement is true. We often want to show an implication $p \implies q$ is true. The negation of the statement $p \implies q$ is $\neg(p \implies q) \equiv p \wedge \neg q$. Thus, for a proof by contradiction we would show the assumption $p \wedge \neg q$ is a contradiction.

Below lies a classic example of a proof by contradiction.

Example. Show that $\sqrt{2}$ is irrational.

Proof. We want to show $\sqrt{2}$ is irrational, that is, there do not exist integers p and q such that $\frac{p}{q} = \sqrt{2}$. To start off our proof we will assume there do exist integers p and q such that

$\frac{p}{q} = \sqrt{2}$. We can also assume this fraction is reduced as much as possible, so that p and q share no common factors. We then have $\left(\frac{p}{q}\right)^2 = 2 \implies p^2 = 2q^2$. Because p^2 equals 2 times an integer, we know p^2 is even. If p^2 is even, then p is even and since p and q share no common factors q is odd. We can then write p as $p = 2k$ for some integer k. We then have $p^2 = (2k)^2 = 4k^2 = 2q^2 \implies q^2 = 2k^2$, and since q^2 is equal to 2 times an integer, we know q^2 is even. This implies q is even. This though is a contradiction, because we already showed q is odd, and since an integer cannot be both even and odd, we know our assumption must have been false. Therefore, there do not exist integers p and q such that $\frac{p}{q} = \sqrt{2}$, hence $\sqrt{2}$ is irrational. $\square$

7.3 Induction

Suppose you want to prove a statement $P(n)$ for each $n \in \mathbb{N}$. Generally, the best tool to do this is a proof by induction. A proof by induction involves showing that if $P(n)$ is true, then $P(n+1)$ is true, referred to as the *inductive case*, and then showing that $P(1)$ is true, referred to as the *base case*. If the inductive case holds, and $P(1)$ is true, then $P(2)$ is true, and $P(3)$ is true, so on and so forth. One way to imagine this idea is like a line of dominos. The inductive step is analagous to saying if the n'th domino falls, then it will knock over the $(n+1)$'th domino, then proceeding to push over the first domino via the base case. This causes every domino to fall.

Below lies the classic example of a proof by induction.

Example. Show that $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

Proof. We will show $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$ through induction. Note, $\frac{1(1+1)}{2} = \frac{2}{2} = 1$, thus the base case holds. Now suppose our proposition holds for some $k \in \mathbb{N}$.

Then we have

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

and the inductive case holds. Therefore, $1+2+3+\cdots+n=\frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$. $\square$

7.4 Proof by Cases

Another common proof technique is a proof by cases. This proof technique involves breaking the problem down into multiple cases, and showing each case leads to the desired conclusion. Below lies an example of a proof by cases.

Example. Show that the product of two consecutive natural numbers is even.

Proof. Let $n \in \mathbb{N}$. We will show $n(n+1)$ is even. Note, either n is even or n is odd.

Case 1: Suppose n is even. Then, there exists some $k \in \mathbb{N}$ such that $n = 2k$. Thus, $2k(2k+1) = 2(2k^2+k)$ and since $n(n+1)$ can be written as the product of 2 and an integer, we know $n(n+1)$ is even.

Case 2: Suppose n is odd. Then, $n = 2k-1$ for some $k \in \mathbb{N}$. Thus, $(2k-1)(2k-1+1) = 2k(2k-1) = 2(2k^2-k)$ and since $n(n+1)$ can be written as the product of 2 and an integer, we know $n(n+1)$ is even.

In either case we see $n(n+1)$ is even, therefore the product of two consecutive natural numbers is even. $\square$

Question: Can you combine the result of the proof by induction example and a proof by contradiction to show this result?

Hint: Assume the sum of two consecutive natural numbers if odd, then use the fact that the sum of $1 + 2 + \cdots + n$ is $\frac{n(n+1)}{2}$.

This section went over several proof techniques. Other proof techniques exist, such as proof by contraposition or the principal of strong mathematical induction. Logic is your best friend when doing proofs. If you are struggling to prove a statement p, it is often worth considering trying to prove one of the statements logically equivalent to p.