6. Mathematical Induction

Definition 6.1 (The Principle of Mathematical Induction)**.** For a fixed integer m, Let $S = i \in \mathbb{Z} : i \leq m$. For each $n \in S$, given a statement $X(n)$, if the following is true:

- $X(m)$ is true, and
- Given $X(k)$ is true, then $X(k+1)$ is true,

then for all $n \in S$, $X(n)$ is true by induction.

Definition 6.2 (The Strong Principle of Mathematical Induction)**.** For a fixed integer m, Let $S = i \in \mathbb{Z} : i \leq m$. For each $n \in S$, given a statement $X(n)$, if the following is true:

- $X(m)$ is true, and
- Given $X(i)$ is true for all $m \leq i \leq k$, then $X(k+1)$ is true,

then for all $n \in S$, $X(n)$ is true by strong induction.

Theorem 6.3. *For all $n \in \mathbb{N}$, the number 3^n is odd.*

Proof. For the base case $n = 1$, we have that $3^1 = 3 = 2 \cdot 1 + 1$ is odd. Now assume that 3^n is odd. Then $3^{n+1} = 3 \cdot 3^n$ is the product of the odd numbers 3 and 3^n, so 3^{n+1} is odd. That is,

$$n = 1 \implies 3^n \text{ is odd, and}$$
$$3^n \text{ is odd} \implies 3^{n+1} \text{ is odd,}$$

so 3^n is odd for all $n \in \mathbb{N}$ by induction. □

Theorem 6.4. *For all $n \in \mathbb{N}$,* $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Theorem 6.5. *For all $n \in \mathbb{N}$,* $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

7. The Integers mod n

Remark 7.1. For this whole section, fix a positive integer n called the *modulus*.

Definition 7.2. Two integers a and b are *congruent*, written $a \equiv b \pmod{n}$, if $n \mid (b - a)$.

Definition 7.3. Let $x \in \mathbb{Z}$. The *congruence class* of $x \pmod{n}$, written $[x]$, is

$$[x] = \{y \in \mathbb{Z} \mid y \equiv x \pmod{n}\}.$$

Definition 7.4. The integers mod n, written $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/(n)$ or $\mathbb{Z}_n$, is the ring whose elements are congruence classes mod n with the rules $[x] + [y] = [x + y], [x] \cdot [y] = [x \cdot y], 0 = [0]$, and $1 = [1]$.

Theorem 7.5. *Let $x \in \mathbb{Z}$. Then $5x - 11$ is even $\iff$ x is odd.*

Proof.
$$\begin{aligned} 5x - 11 \text{ is even} &\iff 2 \mid 5x - 11 \iff 5x - 11 \equiv 0 \pmod{2} \\ &\iff 5x \equiv 11 \pmod{2} \\ &\iff x \equiv 1 \pmod{2} \iff x \text{ is odd.} \end{aligned}$$
□

8. Functions

Definition 8.1. For this whole section, we consider a function $f : A \to B$. The set A is called the **domain** of f, and B is called the **codomain**.

Definition 8.2. If $a \in A$, then $b = f(a)$ is called the **image** of a under f.

Definition 8.3. If $b \in B$, then the **preimage** $f^{-1}(b)$ is the set of all $a \in A$ for which $f(a) = b$.

Remark 8.4. The **image** of f is the set of all elements in B created by mapping elements from A.

Definition 8.5. A function $f : A \to B$ is **injective** if $f(a) = f(b)$ in B implies $a = b$ in A.

Remark 8.6. A function is **injective** or **one-to-one** if for two sets A and B, each unique element of A maps to a unique element of B.

Definition 8.7. A function $f : A \to B$ is **surjective** if for all $r \in B$, there exists an $x \in A$ such that $f(x) = r$.

Remark 8.8. A function is **surjective** or **onto** if for two sets A and B, each element of B is the image of an element of A.

Definition 8.9. A function $f : A \to B$ is **bijective** if it is both injective and surjective.

Theorem 8.10. *For any bijection $f : A \to B$, there exists an inverse bijection $g : B \to A$.*

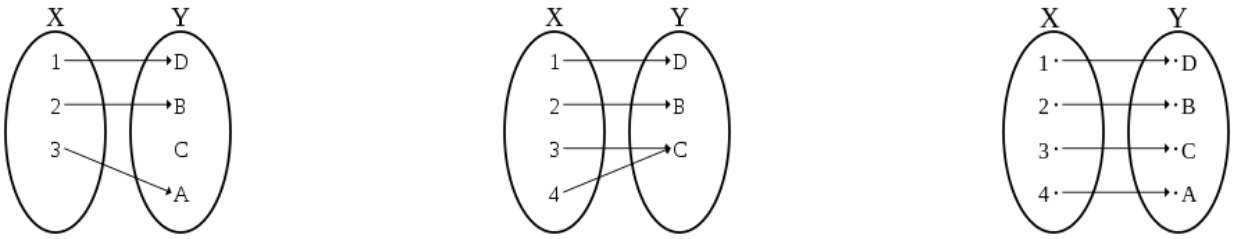

FIGURE 1. Injection, surjection, bijection.

Definition 8.11. If $D \subseteq A$, then f is **strictly increasing on** D if for all $a < b \in D$, $f(a) < f(b)$.

Remark 8.12. We say f is **strictly increasing** if f is strictly increasing on $D = A$.

Definition 8.13. If $D \subseteq A$, then f is **strictly decreasing on** D if for all $a < b \in D$, $f(a) > f(b)$.

Remark 8.14. We say f is **strictly decreasing** if f is strictly decreasing on $D = A$.

Theorem 8.15. *Any strictly increasing or strictly decreasing function is an injective mapping.*

Theorem 8.16. *If A and B are finite sets with $|A| = |B| = n$, then there are $n!$ bijective functions from A to B.*

Theorem 8.17. *Let A and B be finite nonempty sets such that $|A| = |B|$ and let f be a function from A to B. Then f is one-to-one if and only if f is onto.*

9. SETS

Definition 9.1. A set S is **countably infinite** or **denumerable** if there is a bijection $\mathbb{N} \to S$.

Theorem 9.2 (Cantor)**.** *$\mathbb{Z}$ is denumerable. $\mathbb{Q}$ is denumerable.*

Theorem 9.3. *Every infinite subset of a denumerable set is denumerable.*

Theorem 9.4. *If A and B are denumerable sets, then $A \times B$ is denumerable.*

Theorem 9.5. *If A and B are denumerable sets, then $A \cup B$ is denumerable.*

Definition 9.6. An infinite set S is **uncountable** if it is not denumerable.

Theorem 9.7 (Cantor)**.** *$\mathbb{R}$ is uncountable.*

Theorem 9.8. *Let A and B be sets such that $A \subseteq B$. If A is uncountable, then B is uncountable.*

Theorem 9.9 (Cantor-Schröder-Bernstein)**.** *Let A and B be sets. If there exists an injection from $A \to B$ and an injection from $B \to A$, then there exists a bijection $A \to B$.*

10. Exam 2

Remark 10.1. Welcome back, mathematician. Unless otherwise stated, you may freely refer to any definition or theorem in the previous sections either by name or by number. If you do, it is your responsibility to make it clear exactly how you are using it. You may use any given hint without proving it. You may assume elementary arithmetic facts. In proving true theorems, you may assume any previous true theorem even if you have not proved it.

Remark 10.2. The following theorems are true. Prove them.

Theorem 10.3. *The Blibonacci*[*] *numbers are defined by the recurrence*

$$B_1 = 2, B_2 = 4, \text{ and } B_{n+1} = B_n + 2B_{n-1} \text{ for } n > 1.$$

For all $n \in \mathbb{N}$*, we have that* $B_n = 2^n$.

[*]Not a real person.

Theorem 10.4. *The number* 7070707 *is not prime.*

Theorem 10.5. *The number* 56797 *is not prime.*

Remark 10.6. In binary, $56797 = 1101\ 1101\ 1101\ 1101_2$.

Theorem 10.7. *There are six different numbers* $n_1, ..., n_6 \in \mathbb{Z}$ *for which* $8 \mid 5n_i - 1$.

Theorem 10.8. *Exactly one of the following two functions is bijective:*

$$g : \mathbb{Z}_5 \to \mathbb{Z}_5, \qquad [x] \mapsto [2x - 1],$$
$$h : \mathbb{Z}_6 \to \mathbb{Z}_6, \qquad [x] \mapsto [2x - 1].$$

Theorem 10.9. *Define* $m : [0, 2) \to [0, 2)$ *by*

$$m(x) = \begin{cases} x + 1, & 0 \leq x < 1, \\ x - 1, & 1 \leq x < 2. \end{cases}$$

Then m *is not strictly increasing, and* m *is not strictly decreasing.*

Theorem 10.10. *There is a function $p : [0, 4] \to [0, 4]$ with the following properties:*

- *p is surjective,*
- *$p(0) = 1$, and*
- *$p^{-1}(0) = \{2, 3\}$.*

Remark 10.11. A good picture of p suffices, but all properties must be clear from the picture.

Theorem 10.12. *If p is any function satisfying the above conditions, then p is not injective.*