Writing Portfolio 4

David Jackson

Math 3120

Southern Utah University

Fall 2024

Proof Count: 24

Theorem 28.12. *Let $m, n \in Z$. If $n \equiv 1 \pmod 2$ and $m \equiv 3 \pmod 4$, then $n^2 + m \equiv 0 \pmod 4$.*

Proof. We can express $n \equiv 1 \pmod 2$ as $1 \equiv 2k + n$ and $m \equiv 3 \pmod 4$ as $3 \equiv 4l + m$ where $k, l \in \mathbb{Z}$ so we have

$$\begin{aligned}
&n^2 + m \equiv (1 - 2k)^2 + 3 - 4l \\
&n^2 + m \equiv 1 - 4k + 4k^2 + 3 - 4l \\
&n^2 + m \equiv 4k^2 - 4k - 4l + 4 \\
&n^2 + m \equiv 4(k^2 - k - l + 1) \quad \text{This implies that} \\
&n^2 + m \equiv (k^2 - k - l + 1) \pmod 4 + 0 \quad \text{Since 0 is the remainder term we have} \\
&n^2 + m \equiv 0 \pmod 4
\end{aligned}$$

□

Theorem 29.2. *There exists $n \in \mathbb{Z}$ such that $n^5 - n$ is even, but n is not even.*

Proof. Consider $n = 3$ we have $3^5 - 3 = 240 = 2(120)$ therefore n is odd but $n^5 - n$ is even. □

Theorem 29.3. *There exists a natural number n, such that the integer $n^2 + 17n + 17$ is not prime.*

Proof. Suppose $n = 1$ then $1^2 + 17(1) + 17 = 35 = 5(7)$ thus n is a natural number but $n^2 + 17n + 17$ is not prime □

Theorem 29.10. *If $a, b \in \mathbb{N}$, then $a + b \geq ab$.*

Proof. Let $a = b = 1$ than $2 \geq 1$ hence a, b is a natural number where $a + b \geq ab$ □

Theorem 29.11. *If $a, b, c \in N$ and $ab, bc,$ and ac all have the same parity, then $a, b,$ and c all have the same parity.*

Proof. Let ab, bc, and ac all have the same parity, and suppose that a, b, and c all have the same. For the sake of contradiction also assume that a is odd, b is even, and c is even, without loss of generality then ab is even bc is even ac is even a contradiction of our assumption that b, b, and c all have the same parity therefore the theorem is not true to begin with. □

Theorem 29.26. *The equation $x^2 = 2^x$ has three real solutions.*

Proof. Rewrite $x^2 = 2^x$ as $f(x) = x^2 - 2^x$, assume that f is continuous for all $x \in \mathbb{R}$ and consider the points $x = \{-1, 1, 3, 5\}$ then we have

$$\begin{aligned}
f(-1) &= (-1)^2 - 2^{-1} = 1 - \frac{1}{2} = \frac{1}{2} > 0 \\
f(1) &= (1)^2 - 2^1 = 1 - 2 = -1 < 0 \\
f(3) &= 3^2 - 2^3 = 9 - 8 = 1 > 0 \\
f(5) &= 5^2 - 2^5 = 25 - 32 = -7 < 0
\end{aligned}$$

Then by the Immediate Value Theorem, $f(x) = 0$ has at least three solutions in the interval $I = [-1, 5]$ if f is continuous on I. □

Theorem 29.41. *If A is uncountable, then $|A| \neq |\mathbb{R}|$.*

Proof. Let $A = \mathcal{P}(\mathbb{R})$ then $|\mathcal{P}(\mathbb{R})| > |\mathbb{R}|$ by Cantor's theorem thus A is uncountable but $|A| \neq |\mathbb{R}|$. □

Theorem 30.11. *Given $f : A \to B$, let $Y, Z \subseteq B$. Then $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$*

Proof. Let $x \in f^{-1}(Y \cup Z)$. By definition of the preimage, this means: $f(x) \in Y \cup Z$. This implies that $f(x) \in Y$ or $f(x) \in Z$ and $x \in f^{-1}(Y)$ or $x \in f{-}1(Z)$. Thus $x \in f^{-1}(Y) \cup f^{-1}(Z)$. Therefore $f^{-1}(Y \cup Z) \subseteq f^{-1}(Y) \cup f^{-1}(Z)$.
Let $x \in f^{-1}(Y) \cup f^{-1}(Z)$ then $x \in f^{-1}(Y)$ or $x \in f^{-1}(Z)$. This implies that if $x \in f^{-1}(Y)$, then $f(x) \in Y$. If $x \in f^{-1}(Z)$, then $f(x) \in Z$. Thus $f(x) \in Y \cup Z$, which means $x \in f^{-1}(Y \cup Z)$. Therefore: $f^{-1}(Y) \cup f^{-1}(Z) \subseteq f^{-1}(Y \cup Z)$.
Thus $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$. □

Theorem 31.1. *Give an example of a function $f : \mathbb{Z} \to \mathbb{Z}$ so that f is not injective and is not surjective. Explain why f is not one-to-one and why f is not onto.*

Proof. Let $f(x) = x^2$ then for integers $x = \{2, -2\}$ we have $f(2) = f(-2) = 4$ there for f is not injective. Consider the integer $\{-1\}$ such that $\{-1\}$ is this the codomain then there exists an integer x in the domain such that $f(x) = -1$ but $f(x) = x^2 \geq 0$ for all $\mathbb{Z}$ thus f is not surjective □

Theorem 32.4. *Let $f : A \to B$ and $g : B \to C$ be functions. If $g \circ f$ is injective and f is surjective, then g is likewise injective.*

Proof. Suppose $g(b_1) = g(b_2)$ for some $b_1, b_2 \in B$ than $b_1 = b_2$. Since f is surjective that is $\forall b \in B$ there exsits $a \in A$ such that $f(a) = b$. Consider $(g \circ f)(a_1)$ and $(g \circ f)(a_2)$

$$\begin{aligned}
&(g \circ f)(a_1) = g(f(a_1)) = g(b_1) \\
&(g \circ f)(a_2) = g(f(a_2)) = g(b_2) \quad \text{Since } g(b_1) = g(b_2)\text{, we have} \\
&(g \circ f)(a_1) = (g \circ f)(a_2) \quad \text{This implies that} \\
&a_1 = a_2 \quad \text{Since } g \circ f \text{ is injective and since } a_1 = a_2\text{, we have} \\
&f(a_1) = f(a_2) \qquad \text{Thus} \\
&b_1 = b_2
\end{aligned}$$

therefore $g(b_1) = g(b_2)$ implies $b_1 = b_2$. Thus, g is injective. □

Theorem 33.10. *Let A and B be sets. The function $f : A \times B \to B \times A$ defined as $f(a, b) = (b, a)$ is bijective.*

Proof. f is injective if $f(x_1) = f(x_2)$ then $x_1 = x_2$. Let$(a_1, b_1), (a_2, b_2) \in A \times B$ such that:

$$\begin{aligned}
&f(a_1, b_1) = f(a_2, b_2) \quad \text{Then from the definition of } f \text{ we have} \\
&(b_1, a_1) = (b_2, a_2) \\
&b_1 = b_2 \quad \text{and} \quad a_1 = a_2 \quad \text{By the equality of ordered pairs} \\
&(a_1, b_1) = (a_2, b_2)
\end{aligned}$$

Therefore, f is injective.

f is surjective if for every $(b, a) \in B \times A$, there exists $(a', b') \in A \times B$ such that: $f(a', b') = (b, a)$ Let $(b, a) \in B \times A$. Choose $(a', b') = (a, b) \in A \times B$. Then $f(a', b') = f(a, b) = (b, a)$. Thus, for every$(b, a) \in B \times A$, there exists$(a', b') \in A \times B$ such that$f(a', b') = (b, a)$. Therefore,f is surjective. Since f is both injective and surjective, it is bijective. □

Theorem 34.13. *If* $|A| = \infty$*, then* $|A \times A| = |A|$*.*

Proof. To show that $|A| = |A \times A|$, construct a bijection and apply the Cantor-Schroeder-Bernstein theorem.

Part 1: Injective function from A to $A \times A$. Define the function $f : A \to A \times A$ by $f(a) = (a, b)$. For any $a, b \in A$, if $f(a) = f(b)$, then $(a, a) = (b, b)$, which implies $a = b$. Hence, f is injective.

Part 2: Injective function from $A \times A$ to A. Since A is infinite, we can select a fixed projection. Define $g : A \times A \to A$ by the rule $g(a, b) = a$. Then $\forall a, b \in (A \times A)$ if $g(a_1, b_1) = g(a_2, b_2)$ then $a_1 = a_2$. but no conclusion about b_1 and b_2 is needed because the function depends only on the first coordinate. Therefore, g is injective.

Then by the Cantor-Schroeder-Bernstein theorem. We have shown that there exist injective functions $f : A \to A \times A$ and $g : A \times A \to A$. Therefore there exists a bijection between A and $A \times A$. Thus, $|A| = |A \times A|$. □

Theorem 35.4. *Let* $f : A \to B$ *be a function. If* B *is countable and* f *is injective, then* A *is likewise countable.*

Proof. Case 1: B is finite. Let $|B| = n$ for some $n \in \mathbb{N}$. Since f is injective, each element of A maps to a unique element of B. Hence, A can have at most n elements, making A finite and therefore countable.

Case 2: B is countably infinite. Since B is countably infinite, there exists a bijection between B and $\mathbb{N}$. Let $g : B \to \mathbb{N}$ be a bijection. Define a composition function $h : A \to \mathbb{N}$ by $h(a) = g(f(a))$. Since f is injective and g is a bijection, h is injective. Therefore, A can have at most $\mathbb{N}$ elements, making A countably infinite. Therefore, A is countable. □

Theorem 36.7. *Suppose that* A *is countable and* B *is uncountable. Then* $B \setminus A$ *is uncountable.*

Proof. Assume, for the sake of contradiction, that $B \setminus A$ is countable. If $B \setminus A$ is countable, then there are two possibilities: $B \setminus A$ is finite, and $B \setminus A$ is countably infinite.

Case 1: If $B \setminus A$ is finite, then we can write $B \setminus A = \{b_1, b_2, \ldots, b_n\}$ for some finite n. Now, since A is countable, we can write $A = \{a_1, a_2, a_3, \ldots\}$. The set B can be expressed as $B = (A \cup \{b_1, b_2, \ldots, b_n\})$. Since the union of a countable set and a finite set is countable, B would be countable. This contradicts our assumption that B is uncountable. Therefore, $B \setminus A$ cannot be finite.

Case 2: If $B \setminus A$ is countably infinite, then we can write $B \setminus A = \{c_1, c_2, c_3, \ldots\}$. Combining this with the countable set A, we can write B as $B = (A \cup \{c_1, c_2, c_3, \ldots\})$. The union of two countable sets is countable, implying that B is countable. This contradicts our assumption that B is uncountable. Therefore, $B \setminus A$ cannot be countably infinite.
Therefore, $B \setminus A$ is uncountable. □

Theorem 28.1. *If* $a, b \in Z$*, then* $(a + b)^3 \equiv a^3 + b^3 \pmod{3}$.

Proof. We can expand $(a+b)^3$ as

$(a+b)^3 \equiv (a+b)(a+b)(a+b)$

$(a+b)^3 \equiv (a^2+2ab+b^2)(a+b)$

$(a+b)^3 \equiv a^3+a^2b+2a^2b+2ab^2+b^2a+b^3$

$(a+b)^3 \equiv a^3+3a^2b+3ab^2+b^3$ Note that the terms $3a^2b+3ab^2$ each have a factor of 3 therefore

$3a^2b \equiv 0 \pmod 3$ and $3ab^2 \equiv 0 \pmod 3$ Therefore we have

$(a+b)^3 \equiv a^3+0+0+b^3 \pmod 3$

Thus $(a+b)^3 \equiv a^3+b^3 \pmod 3$. □

Theorem 29.42. *Not every infinite set is a subset of a countably infinite set.*

Proof. Consider Hilbert's Hotel the set of rooms in the hotel is a countably infinite set namely $\mathbb{N}$, if every infinite set is a subset of the set of rooms then the hotel will never fill up. Imagine that an infinite bus shows up that can hold an infinite number of people but these people have names that are ordered by irrational numbers. Suppose for the sake of contradiction that you could assign everyone on the bus to a room but how do you know you gave every person on the bus a room. Since their names are ordered by irrational numbers we can form a list indexed by the natural numbers for everyone on the bus but then consider taking the diagonal of their irrational names and adding one to every number for example 1 goes to 2 and 3 goes to 4 if 9 then just go down to 8. This person is guaranteed to not be on the list since they differ from everyone else on the list across the diagonal. Suppose that this person was on our list when we took the diagonal we would have hit them somewhere along the way and changed one of the numbers making a number that is different from that person forming a new number that is assigned to a new person that wasn't on the list before. Therefore by Cantor's diagonal argument, the set of irrational numbers cannot for a bijection with the set of rooms, that is $|\mathbb{N}| < |\mathbb{R} \setminus \mathbb{Q}|$. Since $|\mathbb{R} \setminus \mathbb{Q}|$ is strictly greater than $|\mathbb{N}|$ implies that $\mathbb{R} \setminus \mathbb{Q} \not\subset \mathbb{N}$ contradiction of the assumption that every infinite set is a subset of a countably infinite set. □

Theorem 34.32. *The set of even integers and the set of odd integers have the same cardinality.*

Proof. Let the set $E = \{2n | n \in \mathbb{Z}\}$ and $O = \{2k+1 | k \in \mathbb{Z}\}$ be given. Let the functions $f : \mathbb{Z} \to E$ by the rule $f(x) = 2x$ and $g : \mathbb{Z} \to O$ by the rule $g(y) = 2y+1$ be given.

Lemma 1: All non-constant linear functions are bijective.
Proof. Let the function $f : \mathbb{R} \to \mathbb{R}$ by the rule $f(x) = ax+b$. Then assume that $f(x_1) = f(x_2)$ we have $ax_1 + b = ax_2 + b$ which implies that $x_1 = x_2$. Thus f is an injective function.
Let $\forall y \in \mathbb{R}$ then there exists $x \in \mathbb{R}$ such that $f(x) = y$ so we have.

$$ax+b=y$$
$$ax=y-b$$
$$x=\frac{y-b}{a}$$

$a \neq 0$ since f is a non-constant then $\exists x \in \mathbb{R}$ for every $y \in \mathbb{R}$. Thus, f(x) is subjective.
Therefore f is a bijection.
Since the functions $f(x) = 2x$ and $g(y) = 2y+1$ are non-constant linear functions they are both bijective. Thus $|E| = |\mathbb{Z}|$ and $|\mathbb{Z}| = |O|$ then by transitivity we have $|E| = |O|$. □

Theorem 36.1. *The set of irrational numbers is uncountable.*

Proof. In Theorem 29.42 we Show that $\mathbb{R}\backslash\mathbb{Q}$ is an uncountable set by Cantor's diagonalization argument therefore $\mathbb{R}$ must be an uncountable set since $\mathbb{R} \setminus \mathbb{Q} \subset \mathbb{R}$. □

Theorem 36.2. *The set of complex numbers C is uncountable.*

Proof. Since we have shown that $\mathbb{R}$ is an uncountable set in Theorem 36.1 and since $\mathbb{R} \subset \mathbb{C}$ by comparison it must be true that $\mathbb{C}$ is uncountable. □

Theorem 29.34. *If R is an equivalence relation on an infinite set A, then R has infinitely many equivalence classes.*

Proof. This is not true considering the counterexample where $A = \mathbb{N}$, and define an equivalence relation R on A as:

$$a \sim b \implies a \equiv b \pmod 3$$

This equivalence relation partitions A into three equivalence classes

$$C_1 = \{n \in \mathbb{N} | n \equiv 0 \pmod 3\}$$
$$C_2 = \{n \in \mathbb{N} | n \equiv 1 \pmod 3\}$$
$$C_3 = \{n \in \mathbb{N} | n \equiv 2 \pmod 3\}$$

Thus A is infinite, but there are only three equivalence classes. □

Theorem 30.2. *Define $f : \mathbb{Z}_8 \to \mathbb{Z}_4$ by $f(a) = a \pmod 4$. Then f is a well-defined function.*

Proof. The set $\mathbb{Z}_8$ canby expressed in the form

$$[r]_8 = \{r \equiv a \pmod 8 \mid a \in \mathbb{Z}\} = \{a = 8k + r \mid a \in \{Z\}$$

The function $f(a)$ maps a to its equivalence class in $\mathbb{Z}_4$, which is

$$[l]_4 = \{l \equiv m \pmod 4\} = \{m = 4c + l \mid m \in \mathbb{Z}\}.$$

If $a \equiv b \pmod 8$, then

$$a \equiv 8k + b \quad \text{for some } k \in \mathbb{Z} \text{ then take } \pmod 4$$
$$a \equiv b + 8k \equiv b \pmod 4 \quad (\text{since } 8 \equiv 0 \pmod 4)$$

This implies that $f(a) = b \pmod 4$ thus f is well-defined because it maps each equivalence class in $\mathbb{Z}_8$ to a unique equivalence class in $\mathbb{Z}_4$. □

Theorem 33.4. *The function $f : R \to R$ defined by $f(x) = \pi x - e$ is bijective.*

Proof. Since the function f is a non-constant linear function it must be a bijection by lemma 1 from theorem 34.32. □

Theorem 35.3. *Let X be a partition on a set A. If A is countable, then X is likewise countable.*

Proof. Let the function $f : A \to X$ be given.
Then assume that $\forall a_1, a_2 \in A$. This means that a_1 and a_2 belong to the same equivalence class. Since the partition splits A into non-empty subsets, in such a way that every element is included in exactly one subset, it follows that if $f(a_1) = f(a_2)$, then $a_1 = a_2$ thus the function is injective.
Also, every partition defines an equivalence relation. Then for all equivalence class $A_i \in X$ there exists $a_i \in A$ such that $f(a_i) = A_i$, Since, every equivalence class in X has a preimage in A, thus the function is surjective.
Therefore the function f is a bijection and $|A| = |X|$ thus if A is countable, then X is countable. □