Problem Set 7

Aaron Wang

March 25 2024

1. Let X be a set. Show that $(\forall Y \in \mathbb{P}(X))\ (|Y| \leq |X|)$.

   Proof. Let X and Y be arbitrary sets. Assume $Y \in \mathbb{P}(X)$. By definition of power sets, $Y \subseteq X$. Consider the function $f : Y \to X$ given by $f(a) := a$. Suppose $a_1, a_2 \in Y$ and assume $f(a_1) = f(a_2)$. Then, since $f(a_1) = a_1$ and $f(a_2) = a_2$, we know $a_1 = a_2$ by definition. This proves $(\forall x, y \in A)(f(x) = f(y) \implies x = y)$, meaning f is injective. Since f is injective, by Equinumerosity, $|Y| \leq |X|$. Thus, $(\forall Y \in \mathbb{P}(X))\ (|Y| \leq |X|)$. Q.E.D.

2. Show that $\forall X \forall Y(|X| \leq |Y| \implies \exists Z(Z \subseteq Y \wedge |X| = |Z|))$.

   Proof. Let X and Y be arbitrary sets. Assume $|X| \leq |Y|$. By Equinumerosity, we know that $\exists f(f : X \hookrightarrow Y)$. Let $Z := \{w | ((\exists a \in X)(w = f(a))) \wedge w \in y\}$. Additionally, let $g := f$ where $g : X \to Z$.

   $|X| = |Z|$
   g is injective because f is injective. Let $z \in Z$. By the definition of Z, there exists an $x \in X$ such that $f(x) = z$. Since $g = f$, there exists an $x \in X$ such that $g(x) = z$. Therefore, $(\forall z \in Z)(\exists x \in X)(g(x) = z)$. Consequently, g is surjective. Since g is injective and surjective, g is bijective, and by the definition of Equinumerosity, $|X| = |Z|$.

   $Z \subseteq Y$
   By definition of Z, Z only contains elements that are already contained in Y. Therefore, $\forall w(w \in Z \implies w \in Y)$. Thus, $Z \subset Y$.

   Thus, since X and Y are arbitrary sets, $\forall X \forall Y(|X| \leq |Y| \implies \exists Z(Z \subseteq Y \wedge |X| = |Z|))$. Q.E.D.

3. Let X, Y, Z be sets and consider $f : X \to Y$ and $g : Y \to Z$. We define the composition of f with g to be the function $g \circ f : X \to Z$ given by $(g \circ f)(x) \coloneqq g(f(x))$ for all $x \in X$.

   (a) Show that, if f and g are both injections, then $g \circ f$ is injective.

   Proof. Let $a, b \in X$. We know that $f(a) = f(b) \implies a = b$ because f is injective. Similarly, we know $g(f(a)) = g(f(b)) \implies f(a) = f(b)$ because g is injective. Thus, by hypothetical syllogism, we know that $g(f(a)) = g(f(b)) \implies a = b$ and since $(g \circ f)(x) \coloneqq g(f(x))$, we know $(g \circ f)(a) = (g \circ f)(b) \implies a = b$. As such, we know that $g \circ f$ is injective. Q.E.D.

   (b) Show that, if f and g are both surjections, then $g \circ f$ is surjective.

   Proof. Let $z \in Z$. Because g is surjective, we know that there is a $y \in Y$ such that $g(y) = z$. Similarly, since f is surjective, we know that there is an $x \in X$ such that $f(x) = y$. Because $f(x) = y$ and $g(y) = z$, we know that $g(f(x)) = z$ so by definition $g \circ f(x) = z$. As such, there exists an $x \in X$ such that $g \circ f(x) = z$. Since z was arbitrary, we know that $(\forall z \in Z)(\exists x \in X)(g \circ f(x) = z)$. Q.E.D.

   (c) Show that, if f and g are both bijections, then $g \circ f$ is bijective.

   Proof. To show that $f \circ g$ is bijective, we must show that it is injective and surjective. Note that f and g are both injective and surjective because they are bijective.

   Injective:
   Let $a, b \in X$. We know that $f(a) = f(b) \implies a = b$ because f is injective. Similarly, we know $g(f(a)) = g(f(b)) \implies f(a) = f(b)$ because g is injective. Thus, by hypothetical syllogism, we know that $g(f(a)) = g(f(b)) \implies a = b$ and since $(g \circ f)(x) \coloneqq g(f(x))$, we know $(g \circ f)(a) = (g \circ f)(b) \implies a = b$. As such, we know that $g \circ f$ is injective.

   Surjective:
   Let $z \in Z$. Because g is surjective, we know that there is a $y \in Y$ such that $g(y) = z$. Similarly, since f is surjective, we know that there is an $x \in X$ such that $f(x) = y$. Because $f(x) = y$ and $g(y) = z$, we know that $g(f(x)) = z$ so by definition $g \circ f(x) = z$. As such, there exists an $x \in X$ such that $g \circ f(x) = z$. Since z was arbitrary, we know that $(\forall z \in Z)(\exists x \in X)(g \circ f(x) = z)$.
   Therefore, $f \circ g$ is bijective. Q.E.D.

4. For this problem, let X and Y be arbitrary sets and let $f : X \to Y$.

(a) If f is injective, show there exists $g : Y \to X$ such that $g \circ f = \mathtt{id}_X$.

Proof. Let $x \in X$ and define $g : Y \to X$ where

$$g(y) = \begin{cases} a & \text{if } (\exists a \in X)(f(a) = y) \\ x & \text{otherwise} \end{cases}$$

Since f is injective, for any $a, b \in X$, if $f(b) = f(a)$, $b = a$. As such, for each input into g, if there is an a that satisfies the first predicate, there is only one output. Evidently, for any other input, there is only one output and that output is x. Thus, g is a well-defined function. Now, Let $c \in X$ and observe that $g \circ f(c) = \mathtt{id}_X(c)$.

$$\begin{aligned} g \circ f(c) &= g(f(c)) && \text{By definition of } g \circ f(x) \\ &= c && \text{By definition of } g(x) \\ &= \mathtt{id}_X(c) && \text{By definition of } \mathtt{id} \end{aligned}$$

Consequently, since c was arbitrary, $g \circ f = \mathtt{id}_X$. Q.E.D.

(b) If f is surjective, show there exists $g : Y \to X$ such that $f \circ g = \mathtt{id}_Y$.

Proof. Define $g : Y \to X$ where

$g(y) \coloneqq x$ where $x \in X$ such that $f(x) = y$; If there are multiple such x, pick one.

g is a well-defined function because for every input in Y, there exists a unique output in X. In other words, g is well-defined because $(\forall y \in Y)(\exists! x \in X)(g(y) = x)$.
Let $b \in Y$. Observe $f \circ g(b) = \mathtt{id}_Y(b)$.

$$\begin{aligned} f \circ g(b) &= f(g(b)) && \text{By def of } f \circ g(y) \\ &= b && \text{By def of } f(x) \\ &= \mathtt{id}_Y(b) && \text{By def of } \mathtt{id} \end{aligned}$$

Since b was arbitrary, $f \circ g = \mathtt{id}_Y$. Q.E.D.

(c) If f is a bijection, then show that there exists a function $g : Y \to X$ such that $g \circ f = \texttt{id}_X$ and $f \circ g = \texttt{id}_Y$.

Proof. Define $f : Y \to X$ where

$$g(y) \coloneqq x \text{ where } x \in X \text{ such that } f(x) = y$$

Because f is bijective, f is injective and subjective. Since f is injective, no two values in X map to the same value in Y, and since f is surjective f maps a value to every element of Y. Thus, g is a well-defined function.

Let $a \in X$. Observe $g \circ f(a) = \texttt{id}_X(a)$.

$$\begin{aligned} g \circ f(a) &= g(f(a)) && \text{By def of } g \circ f(x) \\ &= a && \text{By def of } g(y) \\ &= \texttt{id}_X(a) && \text{By def of } \texttt{id} \end{aligned}$$

Since a was arbitrary, $g \circ f = \texttt{id}_X$.

Let $b \in Y$. Observe $f \circ g(b) = \texttt{id}_Y(b)$.

$$\begin{aligned} f \circ g(b) &= f(g(b)) && \text{By def of } f \circ g(y) \\ &= b && \text{By def of } f(x) \\ &= \texttt{id}_Y(b) && \text{By def of } \texttt{id} \end{aligned}$$

Since b was arbitrary, $f \circ g = \texttt{id}_Y$.

Consequently, we have shown that there is a well-defined function $g : Y \to X$ such that $g \circ f = \texttt{id}_X$ and $f \circ g = \texttt{id}_Y$. Q.E.D.

5. Euler's totient function is the function $\varphi_e : \mathbb{N} \to \mathbb{N}$ that counts how many positive integers are *coprime* with each $n \in \mathbb{N}$, defined below.

$$\varphi_e(n) \coloneqq |\{z \in \mathbb{N} | 1 \leq z \leq n \land \gcd(z, n) = 1\}|$$

(a) If $p, k, m \in \mathbb{N}_+$ are *positive* naturals such that p is prime and $m \leq p^k$, then prove $\gcd(p^k, m) \neq 1 \iff p \mid m$.

Proof. Let $p, k, m \in \mathbb{N}_+$ such that p is prime and $m \leq p^k$. To show the biconditional, we must show that the conditional goes both ways.

$\gcd(p^k, m) \neq 1 \implies p \mid m$
Assume $\gcd(p^k, m) \neq 1$.
Theorem 5.7 says: $\gcd(a, b) = 1 \iff (\forall p \in \mathbb{N})(p \text{ is prime} \implies (p \nmid a \lor p \nmid b))$.
So we know: $\neg(\gcd(a, b) = 1) \iff \neg((\forall p \in \mathbb{N})(p \text{ is prime} \implies (p \nmid a \lor p \nmid b))$.
This is equivalent to: $\gcd(a, b) \neq 1 \iff (\exists p \in \mathbb{N})(p \text{ is prime} \land (p \mid a \land p \mid b))$.
Consequently, our assumption gives us $(\exists n \in \mathbb{N})(n \text{ is prime} \land (n \mid p^k \land n \mid m))$.
We can see that p is the only natural number that is prime and divides p^k.
Thus, p is the only natural number that satisfies "n is prime" and "$n \mid p^k$."
Consequently, since a value exists it must be p so we know $(p \text{ is prime} \land (p | p^k \land p | m))$.
Finally, with conjunction elimination, we get $p \mid m$.

$p \mid m \implies \gcd(p^k, m) \neq 1$
Assume $p | m$. Observe $p \cdot p^{k-1} = p^k$. When $k \in \mathbb{N}_+$, $p^{k-1} \in \mathbb{Z}$, so we know that $p | p^k$. Thus since $p | p^k \land p | m$, we can conclude that $p | \gcd(p^k, m)$. Towards a contradiction, assume that $\gcd(p^k, m) = 1$. Putting those two facts together implies that $p \mid 1$, so $p \leq 1$. However, $p > 1$ since p is prime. $\lightning$. Therefore, $\gcd(p^k, m) \neq 1$.

Since we have shown that $\gcd(p^k, m) \neq 1 \implies p \mid m$ and $p \mid m \implies \gcd(p^k, m) \neq 1$ by biconditional disintegration we know $\gcd(p^k, m) \neq 1 \iff p \mid m$. Q.E.D.

(b) If p is prime, then prove that $\varphi_e(p) = p - 1$.

Proof. Let p be a prime number.
By definition, $\varphi_e(p) = |\{z \in \mathbb{N} | 1 \leq z \leq p \land \gcd(z, p) = 1\}|$
Observe that since $p, z \in \mathbb{N}_+$, we can apply (a) so $\varphi_e(p) = |\{z \in \mathbb{N} | 1 \leq z \leq p \land p \nmid z\}|$
An equivalent way to express this is $\varphi_e(p) = |\{z \in \mathbb{N} | (1 \leq z < p \lor z = p) \land p \nmid z\}|$
Distributing the $\land$ we get $\varphi_e(p) = |\{z \in \mathbb{N} | (1 \leq z < p \land p \nmid z) \lor (z = p \land p \nmid z)\}|$
Contrapositive of Absolute Monotonicity of Divisibility says: $(1 \leq z < p) \implies p \nmid z$.
so $\varphi_e(p) = |\{z \in \mathbb{N} | (1 \leq z < p) \lor (z = p \land p \nmid z)\}|$ because $p \nmid z$ is implied by $(1 \leq z < p)$.
Further, $z = p \implies p | z$ because $p | p$ so $(z = p \land p \nmid z) \equiv \bot$ so $\varphi_e(p) = |\{z \in \mathbb{N} | (1 \leq z < p)\}|$
Thus, $\varphi_e(p) = |\{1, 2, ...p - 1\}|$.
By Lemma 6.2 we know that $|\{1, 2, ...p - 1\}| = p - 1$ so $\varphi_e(p) = p - 1$. Q.E.D.

(c) If p is prime and $k \in \mathbb{N}_+$, then prove that $\varphi_e(p^k) = p^k - p^{k-1}$.

Proof. Let p be a prime number and $k \in \mathbb{N}_+$. By definition, $\varphi_e(p^k) = |\{z \in \mathbb{N}|1 \leq z \leq p^k \wedge \gcd(z, p^k) = 1\}|$
Observe that since $p, z, k \in \mathbb{N}_+$, we can apply (a) so $\varphi_e(p) = |\{z \in \mathbb{N}|1 \leq z \leq p^k \wedge p \nmid z\}|$
By Theorem 6.4, we know $\varphi_e(p) = |\{z \in \mathbb{N}|1 \leq z \leq p^k\}| - |\{z \in \mathbb{N}|1 \leq z \leq p^k \wedge p \mid z\}|$.

i. $|\{z \in \mathbb{N}|1 \leq z \leq p\}| = p^k$
$|\{z \in \mathbb{N}|1 \leq z \leq p^k\}| = |\{1, 2, ...p^k\}|$. By Lemma 6.2 we know that $|\{1, 2, ...p^k\}| = p^k$.

ii. $|\{z \in \mathbb{N}|1 \leq z \leq p^k \wedge p \mid z\}| = p^{k-1}$
Define $A \coloneqq |\{z \in \mathbb{N}_+|z \leq p^{k-1}\}$
Define $B \coloneqq |\{z \in \mathbb{N}|1 \leq z \leq p^k \wedge p \mid z\}|$.
Observe $B = |\{z \in \mathbb{N}|1 \leq z \leq p^k \wedge (\exists c \in \mathbb{Z})(pc = z)\}|$
$B = |\{z \in \mathbb{N}|(\exists c \in \mathbb{Z})(1 \leq z \leq p^k \wedge p \cdot c = z)\}|$
$B = |\{z \in \mathbb{N}_+|(\exists c \in \mathbb{N}_+)(z \leq p^k \wedge p \cdot c = z)\}|$
$B = |\{z \in \mathbb{N}_+|(\exists c \in \mathbb{N}_+)(p \cdot c \leq p^k \wedge p \cdot c = z)\}|$
$B = |\{z \in \mathbb{N}_+|(\exists c \in \mathbb{N}_+)(c \leq p^{k-1} \wedge p \cdot c = z)\}|$
So we have $A = |\{z \in \mathbb{N}_+|z \leq p^{k-1}\}$
and $B = |\{z \in \mathbb{N}_+|(\exists c \in \mathbb{N}_+)(c \leq p^{k-1} \wedge p \cdot c = z)\}|$.
Let us define a function $f : A \to B$ where

$$f(a) = p \cdot a$$

A. f is injective
Let $a_1, a_2 \in A$. Assume $f(a_1) = f(a_2)$. By definition of f(a), we know that $p \cdot a_1 = p \cdot a_2$. Further by multiplicative cancellation, $a_1 = a_2$. Therefore, f is injective.

B. f is surjective
Let $b \in B$. By definition of B, $(\exists c \in \mathbb{N}_+)(c \leq p^{k-1} \wedge p \cdot c = z)$. Thus, $(\exists a \in A)(p \cdot a = b)$. Since b was arbitrary, we know that $(\forall b \in B)(\exists a \in A)(f(a) = b)$

Since f is both subjective and injective, f is bijective. We know that $|A| = p^{k-1}$ because $|\{z \in \mathbb{N}|1 \leq z \leq p^k\}| = |\{1, 2, ...p^{k-1}\}|$ and by Lemma 6.2 we know that $|\{1, 2, ...p^{k-1}\}| = p^{k-1}$. Further, since sets, with a bijective function between them have the same cardinality, $|A| = |B|$ so $|B| = p^{k-1}$.

Consequently, we have shown that $|\{z \in \mathbb{N}|1 \leq z \leq p\}| = p^k$ and $|\{z \in \mathbb{N}|1 \leq z \leq p^k \wedge p \mid z\}| = p^{k-1}$. From these two facts, we know that $\varphi_e(p) = p^k - p^{k-1}$. Q.E.D.