Problem Set 7

Discrete Mathematics

Due on the 25th of March, 2024

All basic arithmetic and algebraic facts about $\mathbb{N}$ and $\mathbb{Z}$ are now yours to use.

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

(15 pts) 2. Show that $\forall X \forall Y \Big(|X| \leqslant |Y| \Rightarrow \exists Z(Z \subseteq Y \wedge |X| = |Z|)\Big)$.

(15 pts) 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 $(g \circ f)(x) := g(f(x))$ for all $x \in X$.

Since the codomain of f and the domain of g are the same, they are *compatible*, and their composition is sensibly defined.

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

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

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

(30 pts) 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 $g \circ f = \mathrm{id}_X$.

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

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

(30 pts) 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.

$$\varphi_e(n) := \Big|\big\{z \in \mathbb{N} \;\big|\; 1 \leqslant z \leqslant n \wedge \gcd(z, n) = 1\big\}\Big|$$

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

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

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

Hint: count the multiples of p.