## Problem Set 7

## Discrete Mathematics

Due on the 27th of March, 2024

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

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

3. Let X, Y, Z be sets and consider  $f: X \to Y$  and  $g: Y \to Z$ . We define (15 pts) 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  $x \in X$ .

(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 nonempty sets and let  $f: X \to Y$ .

(a) If f is injective, show there exists  $g: Y \to X$  where  $g \circ f = id_X$ .

(b) If *f* is surjective, show there exists  $g: Y \to X$  where  $f \circ g = id_Y$ .

(c) If f is a bijection, then show that there exists a *unique* function  $g: Y \to X$  such that  $g \circ f = id_X$  and  $f \circ g = id_Y$ .

5. *Euler's totient function* is the function  $\varphi_e : \mathbb{N} \to \mathbb{N}$  that counts how (30 pts) many positive integers are *coprime* with each  $n \in \mathbb{N}$ , defined below.

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

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

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

These are called *monomorphisms*.

These are called *epimorphisms*.

These are called isomorphisms.

Hint: count the multiples of p.