

## Problem Set 7

### Discrete Mathematics

Due on the 27<sup>th</sup> 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  $\forall X \forall Y (|X| \leq |Y| \Rightarrow \exists Z (Z \subseteq Y \wedge |X| = |Z|))$ .
- (15 pts) 3. Let  $X, Y, Z$  be sets and consider  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$ . We define the *composition* of  $f$  with  $g$  to be the function  $g \circ f : X \rightarrow Z$  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  $f : X \rightarrow Y$ .
- (a) If  $f$  is injective, show there exists  $g : Y \rightarrow X$  where  $g \circ f = \text{id}_X$ .
- (b) If  $f$  is surjective, show there exists  $g : Y \rightarrow X$  where  $f \circ g = \text{id}_Y$ .
- (c) If  $f$  is a bijection, then show that there exists a *unique* function  $g : Y \rightarrow X$  such that  $g \circ f = \text{id}_X$  and  $f \circ g = \text{id}_Y$ .
- (30 pts) 5. *Euler's totient function* is the function  $\varphi_e : \mathbb{N} \rightarrow \mathbb{N}$  that counts how many positive integers are *coprime* with each  $n \in \mathbb{N}$ , defined below.

$$\varphi_e(n) := \left| \{z \in \mathbb{N} \mid 1 \leq z \leq n \wedge \gcd(z, n) = 1\} \right|$$

- (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  $p$ .