## CSE 311: PRACTICE PROOF SOLUTIONS

### Definitions

*The following are definitions that will be useful in your proofs:*

**Def 1.1:** Let $a, b \in \mathbb{Z}$. Then **a divides b**, written $a|b$, if $\exists c \in \mathbb{Z}$ such that $b = ac$.

**Def 1.2:** We say an integer $x$ is **even** if $x = 2k$ for some $k \in \mathbb{Z}$. An integer $y$ is **odd** if $y = 2j + 1$ for some $j \in \mathbb{Z}$.

**Def 1.3:** Let $a, b \in \mathbb{Z}$, and $n \in \mathbb{N}$. Then $a \equiv b \pmod{n} \leftrightarrow n|(a - b)$.

**Def 1.4:** Let A and B be sets. Then $A \subseteq B \leftrightarrow \forall x(x \in A \rightarrow x \in B)$.

### Solutions

**1. Let $A = \{x \in \mathbb{Z} \colon 18|x\}$ and $B = \{x \in \mathbb{Z} \colon 6|x\}$. Prove that $A \subseteq B$.**

*Proof. (Direct Proof: want to show $\forall x(x \in A \rightarrow x \in B)$.)*

Let $x \in A$. Then by def. of $A$, $18|a$.
Thus $a = 18c$ for $c \in \mathbb{Z}$, by def. of integer division
$= 6(3c)$ by factoring, where $3c \in \mathbb{Z}$ since $c \in \mathbb{Z}$.
Therefore, by definition of integer division, $6|a$.
Thus $a \in B$ by def. of $B$.
We have shown $a \in A \rightarrow a \in B$, therefore $A \subseteq B$ by def. of a subset. □

**2. Show that if $x^2 - 6x + 5$ is even for $x \in \mathbb{Z}$, then $x$ is odd.**

*Proof. (By Contradiction: show that if we assume x is even, then we reach a contradiction.)*

Let $x^2 - 6x + 5$ be even, and suppose $x$ is also even.
Then by def. of even, $x = 2k$ for some $k \in \mathbb{Z}$.
$x^2 - 6x + 5 = (2k)^2 - 6(2k) + 5$ (by substitution)
$= 4k^2 - 12k + 5$ (after squaring and distributing)
$= 2(2k^2 - 6k + 2)+1$ (using distributive, associative laws)
Let $j = 2k^2 - 6k + 2$. Then $j \in \mathbb{Z}$ since $k \in \mathbb{Z}$.
Thus $x^2 - 6x + 5 = 2j + 1$ for $j \in \mathbb{Z}$, so $x^2 - 6x + 5$ is odd by definition.
However, this is a contradiction because by hypothesis, $x^2 + 6x + 5$ is even.
Therefore our assumption that $x$ is even must be false, hence $x$ is odd. □

**3. Prove that if $x \equiv 14 \pmod{25}$, then $x \equiv 4 \pmod{5}$.**

*Proof.* *(Direct proof: show $\forall x(x \equiv 14$ (mod 25) $\rightarrow x \equiv 4$ (mod 5)))*

Let $a \equiv 14$ (mod 25).

Then $25|(a-14)$ by definition of modular equivalence, and so $a = 25k + 14$ for $k \in \mathbb{Z}$ by applying the def. of integer division and rearranging by algebra.

We can apply distributive and associative properties to get

$$\begin{aligned} a &= 25k + 14 \\ &= 5(5k) + 10 + 4 \\ &= 5(5k+2) + 4 \end{aligned}$$

where $5k + 2 \in \mathbb{Z}$ because $k \in \mathbb{Z}$.

Therefore after rearranging and applying the def. of integer division again, we get $5|(a-4)$,

thus $a \equiv 4$(mod 5) by definition of modular equivalence. □

**4. Suppose $B \neq \emptyset$ and $A \times B \subseteq B \times C$. Prove $A \subseteq C$.**

*Proof.* *(Direct Proof: show $\forall x(x \in A \rightarrow x \in C)$)*

Let $a \in A$ and $B \neq \emptyset$, where $A \times B \subseteq B \times C$.

Since $B \neq \emptyset, \exists b \in B$. So $(a, b) \in A \times B$ by definition of the Cartesian product.

$A \times B \subseteq B \times C$, so $(a, b) \in B \times C$ by definition of subset.

Therefore $a \in B$ by definition of the Cartesian product, so $(x, a) \in A \times B$ for some $x \in A$ (note that $x$ could equal $a$ since we have just shown $A \subseteq B$).

Similarly, $A \times B \subseteq B \times C \rightarrow (x, a) \in B \times C$ by definition of subset, and thus $(x, a) \in B \times C \rightarrow a \in C$ by definition of Cartesian product.

Since we have shown that a generic $a \in A \rightarrow a \in C$, then we have that $A \subseteq C$ and we have reached our conclusion. □