INTRODUCTION TO PROOFS: HW4 SOLUTIONS

Your solutions should be organised to proceed logically, and should be written in complete sentences.

Note: In the solutions, remarks made in square brackets [such as these] are not necessary for a complete proof.

5.1. (b) Determine whether each of the following relations are reflexive, symmetric, transitive; justify your answers.

(i) Let $X = \{\ f : \mathbb{R} \to \mathbb{R}\ \}$. Define a relation $\sim$ on X by $f \sim g$ if $f(0) = g(0)$.

(iii) Let Z be the collection of all subsets of $\mathbb{Q}$. Define a relation on Z by $A \sim B$ if $A \subseteq B$.

Solution:

(b) (i) Take $f, g, h \in X$. $f \sim f$ since $f(0) = f(0)$. So $\sim$ is reflexive. Suppose $f \sim g$. So $f(0) = g(0)$, hence $g(0) = f(0)$, meaning $g \sim f$. Thus $\sim$ is symmetric. Suppose $f \sim g$ and $g \sim h$. Hence $f(0) = g(0)$ and $g(0) = h(0)$; so $f(0) = h(0)$, which implies $f \sim h$. Thus $\sim$ is transitive. [Hence $\sim$ is an equivalence relation.]

(iii) Take $A, B, C \in Z$. $A \subseteq A$, so $A \sim A$. We have $\{1\} \subseteq \{1, 2\}$, but $\{1, 2\} \not\subseteq \{1\}$, so $\{1\} \sim \{1, 2\}$ but $\neg[\{1, 2\} \subseteq \{1\}]$. Suppose $A \sim B$ and $B \sim C$. So $A \subseteq B$ and $B \subseteq C$. Then $A \subseteq C$, so $A \sim C$. Hence $\sim$ is reflexive and transitive, but not symmetric.

5.3. Let X be a set and $\sim$ a relation on X. Define

$$N = \{x \in X :\ \neg(x \sim x)\ \}.$$

Let

$$B = \{b \in X :\ (\forall n \in N)(b \sim n) \wedge (\forall n \notin N)[\neg(b \sim n)]\ \}.$$

Show that $B = \emptyset$. (Suggestion: Suppose there is some $b \in B$; show that $b \in N \implies b \notin N$, and $b \notin N \implies b \in N$. Then explain why it is impossible to have $b \in B$.)

Solution: For the sake of contradiction, suppose there is some $b \in B$. Since $B, N \subseteq X$, either $b \in N$ or $b \notin N$ [but not both].

Suppose first that $b \in N$. Then $\neg(b \sim b)$ [by the definition of N and the supposition that $b \in N$]. But then $\neg(\forall n \in N,\ b \sim n)$ [since $b \in N$ and $\neg(b \sim b)$], which means that $b \notin B$, contradicting the assumption that $b \in B$.

So suppose $b \notin N$. Then [by the definition of N] we must have $b \sim b$. But then $\neg(\forall n \notin N,\ \neg(b \sim n))$, contradicting the assumption that $b \in B$. Hence supposing that there is some $b \in B$ leads to a contradiction; thus $B = \emptyset$.

Either $b \in N$ or $b \notin N$, but we cannot have $b \in N$ and $b \notin N$. Hence there cannot be any $b \in B$, so $B = \emptyset$.

5.5. (b) Find $x \in \mathbb{Z}$ so that $0 \leq x < 7$ and $x \equiv 5^{10} \pmod 7$.
(c) Find $x \in \mathbb{Z}$ so that $0 \leq x < 11$ and $x \equiv 3^5 + 8^4 \pmod{11}$.

Solutions:

(b) $5^2 \equiv 4 \pmod 7$, so $5^3 \equiv 20 \equiv -1 \pmod 7$. Thus

$$t^10 \equiv (5^3)^3 \cdot 5 \equiv (-1)^3 \cdot 5 \equiv -5 \equiv 2 \pmod 7.$$

So we take $x = 2$.

(c) $3^2 \equiv -2 \pmod{11}$, so $3^4 \equiv (-2)^2 \equiv 4 \pmod{11}$ and hence $3^5 \equiv 12 \equiv 1 \pmod{11}$. We have $8 \equiv -3 \pmod{11}$, so $8^2 \equiv 9 \equiv -2 \pmod{11}$, and hence $8^4 \equiv 4 \pmod{11}$. Thus $3^5 + 8^4 \equiv 1 + 4 \equiv 5 \pmod{11}$. So we take $x = 5$.

6.2. (b) Suppose $a, b, c \in \mathbb{Z}$ so that $c \neq 0$, $c|ab$, and $\text{hcf}(b, c) = 1$. Show that $c|a$. (Suggestion: Use the fact that since $\text{hcf}(b, c) = 1$, $\exists s, t \in \mathbb{Z}$ so that $bs + ct = 1$, and that $a = 1 \cdot a$.)

Solution: (b) Since $\text{hcf}(b, c) = 1$, $\exists s, t \in \mathbb{Z}$ so that $bs + ct = 1$. Thus $abs + act = a$. Since $c|ab$, $\exists x \in \mathbb{Z}$ so that $ab = cx$. Hence

$$a = cxs + act = d(xs + at);$$

so $c|a$ [since $xs + at \in \mathbb{Z}$].

6.6. (a) Find $s, t \in \mathbb{Z}$ so that $11s + 13t = 1$.
(b) Find $x \in \mathbb{Z}$ so that $x \equiv 2 \pmod{11} \wedge x \equiv 3 \pmod{13}$. (Suggestion: Use the algorithm presented in the proof of the Chinese Remainder Theorem.)
(c) Find $x \in \mathbb{Z}$ so that $x \equiv 4 \pmod{11} \wedge x \equiv 7 \pmod{13}$.

Solutions:

(a) Using the Euclidean Algorithm, we have $13 = 11 \cdot 1 + 2$, $11 = 2 \cdot 5 + 1$. So

$$1 = 11 - 2 \cdot 5 = 11 - (13 - 11 \cdot 1) \cdot 5 = 11 \cdot 6 - 13 \cdot 5.$$

So we can take $s = 6$, $t = -5$.

(b) Following the proof in the Chinese Remainder Theorem, take

$$x = 11 \cdot 6 \cdot 3 - 13 \cdot 5 \cdot 2 = 68.$$

One checks that 68 is indeed a solution to the simultaneous congruences. [Note that for any $x' \in \mathbb{Z}$ with $x' \equiv x \pmod{11 \cdot 13}$, x' is also a solution to the simultaneous congruences.]

(c) Following the proof in the Chinese Remainder Theorem, take

$$x = 11 \cdot 6 \cdot 7 - 13 \cdot 5 \cdot 4 = 202.$$

One checks that 202 is indeed a solution to the simultaneous congruences. [Note that for any $x' \in \mathbb{Z}$ with $x' \equiv x \pmod{11 \cdot 13}$, x' is also a solution to the simultaneous congruences.]

6.7. Use induction to prove the following identities.
(b) $\sum_{i=0}^{n} \frac{1}{2^i} = 2 - \frac{1}{2^n}$ for $n \in \mathbb{Z}$ with $n \geq 0$.

Solution:

(b) [Base case:] Suppose $n = 0$. Then

$$\sum_{i=0}^{0} \frac{1}{2^i} = 1 = 2 - \frac{1}{2^0}.$$

Thus the identity holds for $n = 0$.

[Induction step:] Assume that $k \in \mathbb{Z}$ with $k \geq 0$ and $\sum_{i=0}^{k} \frac{1}{2^i} = 2 - \frac{1}{2^k}$. Thus

$$\begin{aligned}
\sum_{i=0}^{k+1} \frac{1}{2^i} &= \left(\sum_{i=0}^{k} \frac{1}{2^i} \right) + \frac{1}{2^{k+1}} \\
&= 2 - \frac{1}{2^k} + \frac{1}{2^{k+1}} \\
&= 2 - \frac{2}{2^{k+1}} + \frac{1}{2^{k+1}} \\
&= 2 - \frac{1}{2^{k+1}}.
\end{aligned}$$

Thus by the principle of mathematical induction, the identity holds for all $n \in \mathbb{Z}$ with $n \geq 0$.