Homework 3 Solutions

1.7 #17(a) was too easy, I meant to assign 17(c) . . .

1.7 #18: We’ll show separately that each set is contained in the other (frequently this is a good approach to proving that two sets are equal). First, to show that \((A - B) - C \subseteq (A - C) - (B - C)\), suppose \(x \in (A - B) - C\). Then \(x \in A - B\), so \(x \in A\), and we also have \(x \notin C\). This shows \(x \in A - C\). We also need to show \(x \notin B - C\). This follows because \(x \in A - B\) and therefore \(x \notin B\).

Second, to show that \((A - C) - (B - C) \subseteq (A - B) - C\), suppose \(x \in (A - C) - (B - C)\). We need to show \(x \in (A - B)\) and \(x \notin C\). Since \(x \in A - C\), we have \(x \in A\), and \(x \notin C\). We still need to show \(x \notin B\). But if \(x \in B\), then since \(x \notin C\), we would have \(x \in B - C\), contrary to the supposition that \(x \in (A - C) - (B - C)\).

This problem can also be solved using a membership table or a Venn diagram.

1.8 #12 (a) is one-to-one, (b) is not, for example \(f(-1) = f(1)\), (c) is one-to-one, (d) is not, for example \(f(1) = f(2)\).

Extra problem:
(A) If \(ab \equiv 0 \pmod{p}\), then \(p|ab\). Since \(p\) is prime, it follows that \(p|a\) or \(p|b\), so \(a \equiv 0\) or \(b \equiv 0 \pmod{p}\).

(B) If \(x^2 \equiv 1 \pmod{p}\), then using the algebra identity \(x^2 - 1 = (x + 1)(x - 1)\), we see that \((x + 1)(x - 1) \equiv 0 \pmod{p}\). By part (A), it follows that \(x + 1 \equiv 0\) or \(x - 1 \equiv 0 \pmod{p}\), so \(x \equiv \pm 1 \pmod{p}\).

(C) Consider the square of \(x^{(p+1)/2}\), which is \(x^{q+1} = x^{(p-1)/2+1}\). The key point is now to notice that \(x^{(p-1)/2} = x^{p-1} \equiv 1 \pmod{p}\), by Fermat’s theorem, and therefore \(x^{(p-1)/2} \equiv \pm 1 \pmod{p}\), by part (B). Since \(x^{q+1} = x^{(p-1)/2} \cdot x\), it follows that \(x^{q+1} \equiv \pm x \pmod{p}\).

(D) Since 103 is prime and 103 \(\equiv 3 \pmod{4}\), we can follow the recipe in part (C) to find a square root of 2 by computing \(2^{26} \pmod{102}\). This gives the answer \(38 \pmod{103}\). Of course \((-38)^2 = 38^2\), so \(-38 \equiv 65 \pmod{103}\) is another solution.