Homework 3 Solutions

via Gradescope

- Failure to submit homework correctly will result in zeroes.
- Handwritten homework is OK. You do not have to type up your work.
- Problems assigned from the textbook are from the 5^{th} edition.
- No late homework accepted. Lateness due to technical issues will not be excused.

1. (12 points) Section 4.3 #32, 33, 36.

Solution: #32.

Proof. Let $c \in \mathbb{R}$. Suppose $p \in \mathbb{Q}[x]$ such that $p(c) = 0$. Since $p \in \mathbb{Q}[x]$,

$$p(x) = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i = \frac{a_n}{b_n} x^n + \frac{a_{n-1}}{b_{n-1}} x^{n-1} + \cdots + \frac{a_2}{b_2} x^2 + \frac{a_1}{b_1} x + \frac{a_0}{b_0}$$

and $a_n \neq 0$ for some $n \in \mathbb{Z}^+ \cup \{0\}$, $a_i \in \mathbb{Z}$, and $b_i \in \mathbb{Z} - \{0\}$, for all $i \in \{0, \ldots, n\}$. Define

$$\begin{aligned} q(x) &= p(x) \prod_{j=0}^{n} b_j = p(x) b_0 b_1 \cdots b_n \\ &= \left(\sum_{i=0}^{n} \frac{a_i}{b_i} x^i \right) \left(\prod_{j=0}^{n} b_j \right) = \sum_{i=0}^{n} \left(a_i \left(\prod_{\substack{j=0 \\ j \neq i}}^{n} b_j \right) x^i \right). \end{aligned}$$

so $q \in \mathbb{Z}[x]$.

$$q(c) = p(c) \prod_{i=0}^{n} b_i = 0 \prod_{i=0}^{n} b_i = 0$$

such that $c \in \mathbb{R}$ is the root of a polynomial with integer coefficients. □

#33.

(a) $(x - r)(x - s) = x^2 + (r + s)x + rs$.
If both r and s are odd, then $r + s$ is even (property 2) and rs is odd (property 3).
If both r and s are even, then $r + s$ is even (property 2) and rs is even (property 1).
If one is even and the other is odd, then $r + s$ is odd (property 5) and rs is even (property 4).

(b) Since -1253 is odd, it follows that r and s must have different parity. However, if r and s have different parity, then rs must be even. Hence rs cannot equal 255.

#36. Cannot start a universal proof with explicit rationals $r = 1/4$ and $s = 1/2$.

2. (12 points) Section 4.4 $\#28, 29, 30, 37$.

Solution: #28. This is false. Choose $a = 25$, $b = 5$, and $c = 5$. Then $a \mid bc$ however $a \mid b$ and $a \mid c$ are both false.

#29. This is true.

Proof. Let a and b be any integers that satisfy $a \mid b$. By the definition of divisibility $b = ka$ for some integer k. Therefore $b^2 = (ka)^2 = k^2a^2$. Set $t = k^2$. Then $b^2 = ta^2$. Since t is an integer, it follows that $a^2 \mid b^2$. $\square$

#30. This is false. Choose $a = -25$ and $n = 5$. Then $a \mid n^2$ and $a \leq n$. However $a \mid n$ is false.

#37. No solution provided.

3. (6 points) Section 4.4 $\#45, 48$.

Remark. We should all know the decimal representation of a non-negative integer.

Solution: #45.

Proof. Let n be any integer whose decimal representation ends in 5. Then

$$n = \sum_{l=0}^{k} d_l 10^l$$

where the decimal digits $d_l \in \{0, 1, \ldots, 9\}$, $d_k \neq 0$, and $d_0 = 5$. Notice that $10^l = 2^l 5^l$ for $l = 1, 2, \ldots k$. Therefore

$$n = 5 + \sum_{l=1}^{k} d_l 10^l = 5\left(1 + \sum_{l=1}^{k} d_l 2^l 5^{l-1}\right)$$

Since

$$t = 1 + \sum_{l=1}^{k} d_l 2^l 5^{l-1}$$

is an integer, we have $n = 5t$. It follows that 5 divides n. $\square$

#48.

Proof. Let n be any integer where the sum of its digits are divisible by 3. Then

$$n = \sum_{l=0}^{k} d_l 10^l$$

where 3 divides $d_0 + d_1 + \cdots + d_k$, the decimal digits $d_l \in \{0, 1, \ldots, 9\}$, and $d_k \neq 0$. Note that 3 divides $10^l - 1$ for $l = 1, 2, \ldots k$. Therefore

$$\begin{aligned} n = \sum_{l=0}^{k} d_l 10^l &= d_0 + \sum_{l=1}^{k} d_l (10^l - 1 + 1) \\ &= d_0 + \sum_{l=1}^{k} d_l (10^l - 1) + \sum_{l=1}^{k} d_l \\ &= \sum_{l=1}^{k} d_l (10^l - 1) + \sum_{l=0}^{k} d_l \end{aligned}$$

Set

$$\begin{aligned} t &= \sum_{l=1}^{k} d_l (10^l - 1) \\ s &= \sum_{l=0}^{k} d_l \end{aligned}$$

Notice that 3 divides t since 3 divides $10^l - 1$ for $l = 1, 2, \ldots, k$. 3 also divides s, since s is the sum of the digits in n. Therefore 3 divides $t + s$, that is 3 divides n. □

4. (6 points) Section 4.5 #17, 21.

Solution: #17.

Proof. Let $n \in \mathbb{Z}$.

Case 1: Assume that n is an even integer. Then $n = 2k$ for some integer k. Therefore $n^2 - n + 3 = 4k^2 - 2k + 3 = 4k^2 - 2k + 2 + 1 = 2(2k^2 - k + 1) + 1$. Set $t = 2k^2 - k + 1$. Since t is an integer and $n^2 - n + 3 = 2t + 1$, it follows $n^2 - n + 3$ is odd.

Case 2: Assume that n is an odd integer. Then $n = 2m + 1$ for some integer m. Therefore $n^2 - n + 3 = 4m^2 + 4m + 1 - 2m - 1 + 3 = 4m^2 + 2m + 3 = 4m^2 + 2m + 2 + 1 = 2(2m^2 + m + 1) + 1$. Set $t = 2m^2 + m + 1$. Since t is an integer and $n^2 - n + 3 = 2t + 1$, it follows $n^2 - n + 3$ is odd. □

#21.

Proof. Let $b \in \mathbb{Z}$. Suppose $b \bmod 12 = 5$. Then, via Quotient-Remainder theorem, $b = 12q + 5$ for some unique $q \in \mathbb{Z}$ such that

$$\begin{aligned} b &= 12q + 5 \\ 8b &= 8(12q) + 40 = 12(8q) + 36 + 4 \\ &= 12(8q + 3) + 4. \end{aligned}$$

Thus $8b \bmod 12 = 4$ since $0 \leq 4 < 12$. □

5. (9 points) Section 4.5 $\#25, 31(a), 33$.

Solution: #25.

Proof. Let a and b be any integers that satisfy $a \bmod 7 = 5$ and $b \bmod 7 = 6$. Then $a = 7q + 5$ and $b = 7k + 6$ where q and k are integers. We multiply ab and obtain

$$\begin{aligned} ab &= 49qk + 42q + 35k + 30 \\ &= 49qk + 42q + 35k + 28 + 2 \\ &= 7(7qk + 6q + 5k + 4) + 2 \end{aligned}$$

Set $t = 7qk + 6q + 5k + 4$. Then $ab = 7t + 2$ and, by the uniqueness in the Quotient-Remainder Theorem, it follows that $ab \bmod 7 = 2$. □

#31(a).

Proof. Let m and n be any integers.

Case 1: m and n are both odd. Then, by property 2, it follows that $m+n$ and $m-n$ are even.

Case 2: m and n are both even. Then, by property 1, it follows that $m+n$ and $m-n$ are both even.

Case 3: m and n have different parity. Then, by properties 5 and 6, it follows that $m+n$ and $m-n$ are odd.

Therefore $m+n$ and $m-n$ are either both even or both odd. □

#33.

Proof. Let a, b, and c be any integers such that $a-b$ is even and $b-c$ is even. Since $a-c = (a-b)+(b-c)$ it follows that $a-c$ is the sum of two even integers. Then, by property 1, it follows that $a-c$ is even. □

6. (9 points) Section 4.5 $\#38, 42, 47$.

Solution: #38.

Proof. Let $m \in \mathbb{Z}$. $m = 5q$, $m = 5q+1$, $m = 5q+2$, $m = 5q+3$, or $m = 5q+4$ for some $q \in \mathbb{Z}$ via Quotient-Remainder Theorem.

Case 1: Suppose $m = 5q$. Then $m^2 = 25q^2 = 5t$ for some $t := 5q \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products. $m^2 = 5t + r$ for some $t \in \mathbb{Z}$ and r equals 0, 1, or 4 via generalization.

Case 2: Suppose $m = 5q+1$. Then $m^2 = 25q^2 + 10q + 1 = 5(5q^2 + 2q) + 1 = 5t + 1$ for some $t := 5q^2 + 2q \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products and sums. $m^2 = 5t + r$ for some $t \in \mathbb{Z}$ and r equals 0, 1, or 4 via generalization.

Case 3: Suppose $m = 5q+2$. Then $m^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4 = 5t + 4$ for some $t := 5q^2 + 4q \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products and sums. $m^2 = 5t + r$ for some $t \in \mathbb{Z}$ and r equals 0, 1, or 4 via generalization.

Case 4: Suppose $m = 5q+3$. Then $m^2 = 25q^2 + 30q + 9 = 25q^2 + 30q + 5 + 4 = 5(5q^2+6q+1)+4 = 5t+4$ for some $t := 5q^2+6q+1 \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products and sums. $m^2 = 5t + r$ for some $t \in \mathbb{Z}$ and r equals 0, 1, or 4 via generalization.

Case 5: Suppose $m = 5q+4$. Then $m^2 = 25q^2 + 40q + 16 = 25q^2 + 40q + 15 + 1 = 5(5q^2+8q+3)+1 = 5t+1$ for some $t := 5q^2+8q+3 \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products and sums. $m^2 = 5t + r$ for some $t \in \mathbb{Z}$ and r equals 0, 1, or 4 via generalization.

Therefore $m^2 = 5t + r$ for some $t \in \mathbb{Z}$ and r equals 0, 1, or 4 via generalization. $\square$

#42. This is a biconditional. This will require us to prove the following two conditional statements

1. For all real numbers r and $c \geq 0$, if $-c \leq r \leq c$, then $|r| \leq c$.
2. For all real numbers r and $c \geq 0$, if $|r| \leq c$, then $-c \leq r \leq c$.

Proof of 1. Let r be any real number and c be any non-negative real number which satisfies $-c \leq r \leq c$.

Case 1: Assume that r is non-negative. Then $r = |r|$. Therefore $-c \leq |r| \leq c$. Therefore $|r| \leq c$ via specialization.

Case 2: Assume that $r < 0$. Then $-r = |r|$. Since $-c \leq r \leq c$ we multiply by -1 and obtain $-c \leq -r \leq c$. Therefore $-c \leq |r| \leq c$, that is $|r| \leq c$. $\square$

Proof of 2. Let r be any real number and c be any non-negative real number which satisfies $|r| \leq c$. So $-|r| \geq -c$.

$r \geq 0$ or $r < 0$.

Case 1: Suppose $r \geq 0$. So $-r \leq 0$.

$$c \geq |r| = r \geq 0 \geq -r = -|r| \geq -c$$

Thus $-c \leq r \leq c$.

Case 2: Suppose $r < 0$. So $-r > 0$.

$$c \geq |r| = -r > 0 > r = -(-r) = -|r| \geq -c$$

Thus $-c \leq r \leq c$. □

#47. Can you prove the following theorem?

Theorem. *For any $d \in \mathbb{Z}^+$ and $m, n \in \mathbb{Z}$, m mod $d = n$ mod d implies $d \mid (m - n)$.*

Perhaps surprisingly, the converse of the theorem above is also true, which is the object of this question:

Theorem. *For any $d \in \mathbb{Z}^+$ and $m, n \in \mathbb{Z}$, $d \mid (m - n)$ implies m mod $d = n$ mod d.*

Proof. Let $d \in \mathbb{Z}^+$ and $m, n \in \mathbb{Z}$. Via the Quotient-Remainder Theorem, there exist unique $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that $m = dq_1 + r_1$, $n = dq_2 + r_2$, $0 \leq r_1 < d$, and $0 \leq r_2 < d$, i.e. m mod $d = r_1$ and n mod $d = r_2$. Suppose $d \mid (m - n)$. Then there exists $k \in \mathbb{Z}$ such that $m - n = dk + 0 = d(q_1 - q_2) + (r_1 - r_2)$ so $k = q_1 - q_2$ and $0 = r_1 - r_2$ component-wise. Thus $r_1 = r_2$ and m mod $d = n$ mod d. □