110A HW1

Warren Kim

Winter 2024

Question 1

Let a and b be integers, such that $b \neq 0$. Show that there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$, where $0 \leq r < |b|$.

Response

Existence Define a set $S = \{a - bx : x \in \mathbb{Z}\} \cap \mathbb{Z}_{\geq 0}$. There are two cases:

Case (i): If $b > 0$, we showed in class that there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ where $0 \leq r < b$.

Case (ii): If $b < 0$, consider $b' = -b$. Then, $b' > 0$. From *Case (i)*, there exist $q', r \in \mathbb{Z}$ such that $a = b'q' + r$, where $0 \leq r < b'$. Then, we have $a = b'q' + r = -bq' + r = b(-q') + r$. Letting $q = -q'$, we get $a = bq + r$. So, there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ where $0 \leq r < b'$.

In either case, there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ where $0 \leq r < |b|$.

Uniqueness Suppose we have $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that $a = bq_1 + r_1 = bq_2 + r_2$ where $0 \leq r_1, r_2 < |b|$. Then, we have $bq_1 + r_1 = bq_2 + r_2$. Subtracting $bq_2 + r_2$ from both sides, we get

$$(bq_1 + r_1) - (bq_2 + r_2) = 0$$

or

$$b(q_1 - q_2) + (r_1 - r_2) = 0$$

Subtracting $r_1 - r_2$ from both sides, we get

$$b(q_1 - q_2) = r_2 - r_1$$

Since $0 \leq r_1, r_2 < |b|$, we have that $-|b| < r_2 - r_1 < |b|$. The possible values for $r_2 - r_1$ are $0b, b, 2b, \ldots$, but since $-|b| < r_2 - r_1 < |b|$, we have that $r_2 - r_1 = 0$. Then, $b(q_1 - q_2) = 0$ and since $b \neq 0$, $q_1 - q_2 = 0$. This implies $r_1 = r_2$ and $q_1 = q_2$. Therefore, $q_1, r_1 \in \mathbb{Z}$ are unique.

Question 2

If $b|a$ and $a \neq 0$, show that $|b| \leq |a|$. Hint: recall that $|xy| = |x||y|$.

Response

Proof: Suppose $b|a$ and $a \neq 0$. Then, there exists some $c \in \mathbb{Z}$ such that $a = bc$. Since $a \neq 0$, c is necessarily nonzero. Applying the absolute value to the equation, we get $|a| = |b||c| = |bc|$. Then, since $c \neq 0$, we have that $|b| \leq |bc|$. But $|bc| = |a|$ so $|b| \leq |a|$. $\square$

Question 3

Let $a, b, c \in \mathbb{Z}$ such that $(a, b) = 1$. Suppose $a|c$ and $b|c$. Show that $ab|c$.

Response

Proof: Let $a, b, c \in \mathbb{Z}$ such that $(a, b) = 1$. Suppose $a|c$ and $b|c$. Then there exist some $n, m \in \mathbb{Z}$ such that $c = an$ and $c = bm$. Then we have the following:

$$\begin{aligned}
1 &= ax + by \\
c &= (ax + by)c \\
&= acx + bcy \\
&= a(bm)x + b(an)y \\
&= abmx + abny \\
c &= ab(mx + ny)
\end{aligned}$$

Setting $q = mx + ny$, we get $c = (ab)q$, so $ab|c$. $\square$

Question 4

Show the backwards direction of Theorem 1.5:
Let $p \in \mathbb{Z}$ such that $p \neq 0, \pm 1$. Show that the second statement implies the first.

1. p is prime
2. If $p|bc$ where $b, c \in \mathbb{Z}$, then $p|b$ or $p|c$.

[Hint: contrapositive/contradiction are valid ways to prove this.]

Response

Proof: To prove the reverse implication, suppose the contrapositive: "If p is not prime, then there exists some $b, c \in \mathbb{Z}$ such that $p|bc$ but $p \nmid b$ and $p \nmid c$." Suppose $p \in \mathbb{Z}$ such that $p \neq 0, \pm 1$ is not prime; i.e. p is composite. Then, p can be written as $q_1 q_2 \cdots q_n$ where $n \geq 2$ and each q_i is a unique prime. Choose $b = q_1$ and $c = q_2 \cdots q_n$. Then $p|bc$ because $bc = p$ and $p|p$, but $p \nmid b$ and $p \nmid c$ because $p > b$ and $p > c$. $\square$

Question 5

If p is prime and $p|a_1 \cdots a_n$, show that there must be at least one a_i such that $p|a_i$.

Response

Proof: Suppose p is prime and $p|a_1 \cdots a_n$. To show that there must be at least one a_i such that $p|a_i$, we proceed by induction on n. If $n = 2$, $p|a_1 \cdot a_2$, by Theorem 1.5, either $p|a_1$ or $p|a_2$. Assume the inductive hypothesis holds for all natural numbers up to n. At $n = n + 1$, we have $p|a_1 \cdots a_n \cdot a_{n+1}$. By associativity of the integers, rewrite the statement as $p|(a_1 \cdots a_n) \cdot (a_{n+1})$. Then, either $p|(a_1 \cdots a_n)$ or $p|a_{n+1}$. $\square$

Question 6

Suppose $a, b, c \in \mathbb{Z}$, such that $(a, c) = (b, c) = 1$. Show that $(ab, c) = 1$.

Response

Proof: Suppose $a, b, c \in \mathbb{Z}$, such that $(a, c) = (b, c) = 1$. Then, we can rewrite the gcd as $ax + cy = 1$ and $bn + cm = 1$ respectively. Then, we have

$$\begin{aligned}
1 &= ax + cy \\
&= (ax + cy) \cdot 1 \\
&= (ax + cy)(bn + cm) \\
&= abxn + acxm + bcny + ccym \\
1 &= ab(xn) + c(axm + bny + cym)
\end{aligned}$$

Setting $p = xn$ and $q = axm + bny + cym$, we get $(ab)p + cq = 1$. To show $(ab, c) = 1$, let $d = (ab, c)$. Then, $d|(ab)$ and $d|c$ by definition. This implies that $d|(abp + cq)$, but $abp + cq = 1$, so $d = 1$. Therefore, $(ab, c) = 1$. $\square$

Question 7

Let $p > 3$ be prime. Prove that p^2+2 is not prime. [hint: If you divide p by 3, what are the possible remainders?]

Response

Proof: Let $p > 3$ be prime. If $p \equiv 0 \pmod 3$, p would be divisible by 3 and therefore p would not be prime. There are two remaining cases:

Case (i): If $p \equiv 1 \pmod 3$, we can rewrite this as $p = 3n + 1$ for some $n \in \mathbb{N}$. Then, we can write $p^2 + 2 = (3n + 1)^2 + 2 = 9n^2 + 6n + 1 + 2 = 3(3n^2 + 2n + 1)$.

Case (ii): If $p \equiv 2 \pmod 3$, we can rewrite this as $p = 3n + 2$ for some $n \in \mathbb{N}$. Then, we can write $p^2 + 2 = (3n + 2)^2 + 2 = 9n^2 + 12n + 4 + 2 = 3(3n^2 + 4n + 2)$

In either case, $p^2 + 2$ is divisible by 3 and therefore is not prime. $\square$

Question 8

Let p be prime. Show that if $p|a^5$, then $p|a$.

Response

Proof: Let p be prime and suppose $p|a^5$. Rewrite a^5 as $a \cdot a \cdot a \cdot a \cdot a$. Then, $p|a^5$ is equivalent to writing $p|(a \cdot a \cdot a \cdot a \cdot a)$. By Corollary 1.2 (proven in **Question 5**), since p divides the product a^5, p must divide a, so $p|a$. $\square$