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

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. Therefore, we have the inequality $-bc \leq b \leq bc$. This is equivalent to $|b| \leq |bc|$. 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

Let $a, b, c \in \mathbb{Z}$ such that $(a, b) = 1$. Suppose $a|c$ and $b|c$. Then there exist some $x, y \in \mathbb{Z}$ such that $c = ax$ and $c = by$.

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

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

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 $bx' + cy' = 1$ respectively. Then, we have

$$\begin{aligned}
1 &= ax + cy \\
&= (ax + cy) \cdot 1 \\
&= (ax + cy)(bx' + cy') \\
&= abxx' + acxy' + bcx'y + c^2yy' \\
1 &= ab(xx') + c(axy' + bx'y + cyy')
\end{aligned}$$

Setting $n = xx'$ and $m = axy' + bx'y + cyy'$, we get $(ab)n + cm = 1$, so $(ab, c) = 1$. $\square$

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

Question 8

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

Response

Proof: Let p be prime and suppose that $p|a^5$. Rewrite $a^5 = a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5$ where $a_1 = a_2 = a_3 = a_4 = a_5 = a$. Then, $p|a^5$ is equivalent to writing $p|a_1 \cdot a_2 \cdot a_3 \cdot a_4 \cdot a_5$. By Corollary 1.2 (proven in **Question 5**), p must divide at least one a_i, but since $a_i = a$ for $i \in \{1, 2, 3, 4, 5\}$, $p|a$. $\square$