Math 110A Homework 1

Brendan Connelly

Monday, January 20, 2025

1 Textbook 1.2

Question 12: Suppose that $(a, b) = 1$ and $(a, c) = 1$. Are any of the following statements false?

i. $(ab, a) = 1$

ii. $(b, c) = 1$

iii. $(ab, c) = 1$

For (i), this statement is false. $(ab, a) = |a|$. We can show this by corollary 1.3. $|a|$ trivially divides a and $|a|$ divides ab, with a factor of $\pm b$. Furthermore, if $c \mid |a|$, then, $c \mid a$ trivially and, with just another factor of b, $c \mid ab$. Thus, by corollary 1.3, $(ab, a) = |a|$.

For (ii), this statement is false. We can choose a counterexample. $(a = 2, b = 3) = 1$ and $(2, c = 9) = 1$. However, $(3, 9) = 3$ as $3 = 3 \times 1$ and $9 = 3 \times 3$.

For (iii), this statement is also false. We can choose a counterexample. $(a = 2, b = 3) = 1$ and $(2, c = 9) = 1$. However, $(2 \times 3, 9) = 3$.

$\implies$ $\boxed{\text{None of the statements are true.}}$

Question 24: Let $a, b, c \in \mathbb{Z}$. Prove that the equation $ax + by = c$ has integer solutions if and only if $(a, b) \mid c$

$(\implies)$ Assume $ax + by = c$ has integer solutions. Let $d = (a, b)$. Since, $d \mid a$ and $d \mid b$ by the definition of the greatest common divisor, we have that there exists an $a', b' \in \mathbb{Z}$ such that $da' = a$ and $db' = b$. Thus, $d(a' + b') = c$ so $d \mid c$.

$(\impliedby)$ This direction directly follows from Bezout's Identity. Assume $d = (a, b) \mid c$. Then, there exist $x_0, y_0 \in Z$ such that $ax_0 + by_0 = d$. However, since $d \mid c$, there exists a $k \in \mathbb{Z}$ such that $kd = c$. Therefore, $ax_0k + by_0k = kd = c$. Therefore, for $x = kx_0$ and $y = ky_0$, we are done. □

---

2 Textbook 1.3

Question 16: Prove that $(a, b) = 1$ if and only if there is no prime p such that $p \mid a$ and $p \mid b$

$(\implies)$ Assume $(a, b) = 1$. Assume for contradiction that there existed a prime $p \geq 2$ such that $p \mid a$ and $p \mid b$. Then, $(a, b) \geq p \geq 1$.

$(\Longleftarrow)$ Assume there is no prime p such that $p \mid a$ and $p \mid b$. Assume for contradiction, $(a, b) = d > 1$. Then, $d = q_1 \times \cdots \times q_n$ for q_i prime by the Fundamental Theorem of Arithmetic. Then, take q_1. $q_1 \mid d$. Thus by the transitivity of divisibility, $q_1 \mid a$ and $q_1 \mid b$. Thus, we are done by contradiction and $(a, b) = 1$. $\square$

Question 32: (Euclid) Prove that there are infinitely many primes

Suppose for contradiction there exist only finitely many primes $p_1, \ldots, p_n$. Then, consider $d = p_1 \times \cdots \times p_n + 1$. Each of $p_i \nmid d$. Then, either d is prime, which is a contradiction. Otherwise, d cannot be broken into a product of primes as it is divisible by none of them. This contradicts the Fundamental Theorem of Arithmetic. Therefore, there exist infinitely many primes. $\square$

---

3 Textbook 2.1

Question 14:

i. Prove or disprove: If $ab \equiv 0 \pmod{n}$, then $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$.

ii. Do part (a) when n is prime

For (i), this statement is false. Consider a counterexample. $2 \times 3 \equiv \pmod{6}$. However, $2 \not\equiv 0 \pmod{6}$ and $3 \not\equiv 0 \pmod{6}$.

For (ii), this statement becomes true where n is prime. $n \mid ab$ implies that $nm = ab$ for some $m \in \mathbb{Z}$. Then, we can consider two cases. Either the $(n, a) = 1$ or $(n, a) = n$ because n is prime, meaning its only divisors are $\pm 1, \pm n$. If $(n, a) = n$, we are done because then $n \mid a \implies a \equiv 0 \pmod{n}$. If $(n, a) = 1$, by theorem 1.4, $n \mid b \implies b \equiv 0 \pmod{n}$. Thus, we have shown that $ab \equiv 0 \pmod{p}$, then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$ for prime p. $\square$

Question 22:

i. Give an example to show that the following statement is false: If $ab \equiv ac \pmod{n}$ and $a \not\equiv 0 \pmod{n}$, then $b \equiv c \pmod{n}$.

ii. Prove that the statement is true whenever $(a, n) = 1$

For (i), we can consider the case when $a \equiv 2 \pmod{4}$, $b \equiv 3 \pmod{4}$, $c \equiv 1 \pmod{4}$. Then, we have that $ab \equiv 2 \pmod{4}$ and $ac \equiv 2 \pmod{4}$. However, $3 \not\equiv 1 \pmod{4}$, proving this statement is false.

For (ii), we have that $n \mid ab - ac$. Thus, $n \mid a(b - c)$. By theorem 1.4 again, because $(n, a) = 1$, we have that $n \mid b - c$. Thus, by definition, $b \equiv c \pmod{n}$. $\square$