Section 2.4

Problem 3

Claim: For \( a, b, c \in \mathbb{Z} \) and \( d \in \mathbb{Z} - \{0\} \), if \( a \) and \( b \) are divisible by \( d \), and \( c \) is not divisible by \( d \), then the equation

\[ ax + by = c \]

has no integral solution for \( x \) and \( y \).

Proof:

Let \( a, b, c \in \mathbb{Z} \) and let \( d \in \mathbb{Z} - \{0\} \). Suppose that \( a \) and \( b \) are divisible by \( d \) and \( c \) is not divisible by \( d \).

Suppose by way of contradiction that there exist \( x_0, y_0 \in \mathbb{Z} \) such that

\[ ax_0 + by_0 = c. \]

Since \( a \) and \( b \) are divisible by \( d \), we know that there exist integers \( j \) and \( k \) such that \( a = kd \) and \( b = jd \). Substituting these expressions into our equation, we get

\[ (kd)x_0 + (jd)y_0 = c. \]

Substituting these expressions into our equation, we get

\[ d(kx_0 + y_0) = c, \]

so that \( c \) is divisible by \( d \). But this contradicts our assumption that \( c \) is not divisible by \( d \). Since the assumption that the integral solutions \( x_0, y_0 \) exist leads to a contradiction, there cannot be any integral solutions to the equation. \[\Box\]

Problem 4a

Claim: If \( x \in \mathbb{Z} \) and \( x^2 \) is even, then \( x \) is even.

Proof:

Let \( x \in \mathbb{Z} \). Suppose by way of contradiction that \( x^2 \) is even and \( x \) is odd. Since \( x \) is odd, we know there exists \( k \in \mathbb{Z} \) such that \( x = 2k + 1 \). Then

\[ x^2 = \]

\[ = (2k + 1)^2 \]

\[ = 4k^2 + 4k + 1 \]

\[ = 2(2k^2 + 2k) + 1, \]
so that $x^2$ is odd. But this contradicts our assumption that $x^2$ is even. Since the assumption that $x$ is odd led to a contradiction, $x$ must be even. 

Problem 4c

Claim: If $a, b, c \in \mathbb{Z}$ and $a \nmid bc$, then $a$ does not divide either $b$ or $c$.

Proof:

Let $a, b, c \in \mathbb{Z}$. Suppose by way of contradiction that $a \nmid bc$ and $a$ divides $b$ or $a$ divides $c$. \footnote{This claim is an example of the difficulties of English. The intended meaning is clearly “$a$ does not divide $b$ \textbf{and} $a$ does not divide $c$,” but in shortening the expression English uses “or”. The negation of the claim is properly “$a$ divides $b$ \textbf{or} $a$ divides $c$.”} We have two cases: $a$ divides $b$ and $a$ divides $c$.

If $a$ divides $b$, then there exists $k \in \mathbb{Z}$ such that $b = ak$. Then $bc = (ak)c = a(kc)$, so that $bc$ is divisible by $a$. But this contradicts our hypothesis that $a$ does not divide $bc$. Since the assumption that $a$ divides $b$ leads to a contradiction, it cannot be true and thus $a$ must divide $c$.

However, if we suppose that $a$ divides $c$ we reach a similar contradiction. Since assuming that $a$ divides $b$ or $a$ divides $c$ led to a contradiction, it cannot be true and thus its negation, $a$ does not divide $b$ and $a$ does not divide $c$, must be true.

Problem 5c

Statement: If $\text{GCD}(a, b) = x$ and $\text{GCD}(a, c) = y$, then $\text{GCD}(a, bc) = xy$.

Analysis:

This statement is false. For example, let $a = 12$, $b = 2$, and $c = 4$. Then $\text{GCD}(a, b) = 2$ and $\text{GCD}(a, c) = 4$, but $\text{GCD}(a, bc) = \text{GCD}(2, 8) = 2 \neq 2 \cdot 4$.

The trouble comes from the fact that $x \mid a$ and $y \mid a$ do not necessarily imply $xy \mid a$. This statement is only true when $x$ and $y$ are relatively prime (that is, when $\text{GCD}(x, y) = 1$). If we change the statement to “If $\text{GCD}(a, b) = x$ and $\text{GCD}(a, c) = y$ and $\text{GCD}(x, y) = 1$, then $\text{GCD}(a, bc) = xy$,” it will be true.

Problem 6

Question: If $x$ is a prime number and $y \in \mathbb{Z}$, what are the possibilities for $\text{GCD}(x, y)$?

Answer:

If $x$ is prime and $y \in \mathbb{Z}$, there are only two possibilities for $\text{GCD}(x, y)$: $\text{GCD}(x, y) = x$ (when $y$ is a multiple of $x$) and $\text{GCD}(x, y) = 1$ (when $y$ is not a multiple of $x$).

Problem 7a

Claim: If $x$ and $y$ are both nonzero integers, then there is at least one positive integer which is a multiple of both $x$ and $y$.

Proof:
Let \( x, y \in \mathbb{Z} - \{0\} \). We claim that \(|xy|\) is the desired integer.

Clearly \(|xy|\) is nonnegative; it is also nonzero since \( x \) and \( y \) are nonzero. So \(|xy|\) is a positive integer. To show that \(|xy|\) is a multiple of \( x \), note that \(|xy| = \pm xy = x(\pm y)\). Similarly \(|xy|\) is a multiple of \( y \). Hence \(|xy|\) is our desired integer. ■

**Problem 7b**

**Question:** Why do we require that both \( x \) and \( y \) be nonzero in the general definition of LCM?

**Answer:** The least common multiple of two numbers is defined to be the least positive number which is a multiple of both numbers. If we don’t make the stipulation that the LCM be positive, there would be either no LCM (if we allow it to be positive, negative, or zero) or every pair of numbers would have the same LCM (if we only allow it to be nonnegative) - namely zero.

If \( x \) or \( y \) were zero, then the LCM would be undefined because there is no positive number which is a multiple of zero (since every multiple of zero is zero).

**Problem 7c**

(i) **Question:** If \( \text{GCD}(x, y) = 1 \), what conclusion can you draw about \( \text{LCM}(x, y) \)?

**Answer:**

If \( \text{GCD}(x, y) = 1 \), then \( \text{LCM}(x, y) = |xy| \).

(ii) **Question:** If \( x \) is a prime number, what are the possibilities for \( \text{LCM}(x, y) \)?

**Answer:**

If \( x \) is prime, then either \( \text{LCM}(x, y) = |xy| \) (if \( y \) is not a multiple of \( x \)) or \( \text{LCM}(x, y) = |y| \) (if \( y \) is a multiple of \( x \)).

(iii) **Question:** What general equation can you write relating \( x, y, \text{GCD}(x, y) \), and \( \text{LCM}(x, y) \)?

**Answer:**

\( \text{GCD}(x, y) \cdot \text{LCM}(x, y) = |xy| \).

**Problem 8**

(a) **Statement:** \( x < y \).

**Negation:** \( x \geq y \).

(b) **Statement:** \( z \) is composite.

**Negation:** \( z \) is prime or \( z = 1 \).

(c) **Statement:** \( t \in A \cup B \).

**Negation:** \( t \in A' \cap B' \).
Problem 9

(b) The theorem is true and the proof is correct.

(c) The theorem is false since any two power sets will always have a nonempty intersection, regardless of whether $A$ and $B$ intersect. The proof fails by misunderstanding the meaning of “disjoint”: $A$ and $B$ are disjoint means that $A \cap B = \emptyset$. The proof seems to understand the opposite. The correct contradiction hypothesis should be “Suppose $\mathcal{P}(A) \cap \mathcal{P}(B) \neq \emptyset$ and $A \cap B = \emptyset$.”

(d) The theorem is true and the proof is correct.

(e) The theorem is true. However, the proof shows only that if $d$ divides $a$ and $b$, then $d^2$ divides $a^2$ and $b^2$. It remains to be shown that if $d$ is the greatest common divisor of the integers then its square is the greatest common divisor of their squares.