1. (12 points)
Let $U = \{n \in \mathbb{N} \mid n \leq 20\}$ be the universal set. Define subsets of $U$ as follows.

$$A = \{a \in U : a^2 \leq 16\}$$

$$B = \{b \in U : b \equiv 1 \pmod{3}\}$$

$$C = \{c \in U : 10 | c\}$$

In parts (a) - (f), determine the set by listing its elements between braces.

(a) $A$

$$A = \{1, 2, 3, 4\}$$

(b) $B$

$$B = \{1, 4, 7, 10, 13, 16, 19\}$$

(c) $C$

$$C = \{10, 20\}$$

(d) $A \cup B$

$$A \cup B = \{1, 2, 3, 4, 7, 10, 13, 16, 19\}$$

(e) $A \cap B$

$$A \cap B = \{1, 4\}$$

(f) $\overline{B}$

$$\overline{B} = \{2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17, 18, 20\}.$$
2. (4 points)

Let \( A = \{1, 2\} \) and \( B = \{\emptyset\} \). Determine the following sets by listing their elements between braces.

(a) \( A \times B \)

\[
A \times B = \{ (1, \emptyset), (2, \emptyset) \}
\]

(b) \( \mathcal{P}(A) \times \mathcal{P}(B) \)

\[
\mathcal{P}(A) = \{ \emptyset, \{1\}, \{2\}, A \}
\]

\[
\mathcal{P}(B) = \{ \emptyset, B \}
\]

\[
\mathcal{P}(A) \times \mathcal{P}(B) = \{ (\emptyset, \emptyset), (\emptyset, B), (\{1\}, \emptyset), (\{1\}, B), (\{2\}, \emptyset), (\{2\}, B), (A, \emptyset), (A, B) \}.
\]
3. (9 points)

Let \( n \in \mathbb{Z} \).

(a) State the definition of the phrase: \( n \) is even.

An integer \( n \) is even if \( n = 2k \) for some integer \( k \).

(b) Prove: If \( n \) is even, then \( n^3 \) is even.

Proof Assume that \( n \in \mathbb{Z} \) is even. Write \( n = 2k \), \( k \in \mathbb{Z} \).
Then \( n^3 = (2k)^3 = 8k^3 = 2(4k^3) \). Since \( 4k^3 \in \mathbb{Z} \), we know that \( n^3 \) is even. \( \Box \)

(c) Prove: If \( n^3 \) is even, then \( n \) is even.

Proof We prove the contrapositive.
Assume that \( n \) is odd. Then \( n = 2k+1 \), \( k \in \mathbb{Z} \).
So \( n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 \) (using Pascal's triangle)
\( = 2(4k^3 + 6k^2 + 3k) + 1 \).
Since \( 4k^3 + 6k^2 + 3k \in \mathbb{Z} \) we know that \( n^3 \) is odd. \( \Box \)
4. (6 points)

Let \( x \in \mathbb{R} \).

(a) State the definition of the phrase: \( x \) is a rational number.

A real number \( x \) is a **rational number** if there exist \( a, b \in \mathbb{Z} \) such that

\[
x = \frac{a}{b}.
\]

(b) Prove: \( \sqrt{2} \) is an irrational number.

Proof: Suppose, to the contrary, that \( 3 \sqrt{2} \) is a rational number. Let \( a, b \in \mathbb{Z} \) such that \( 3 \sqrt{2} = \frac{a}{b} \). Moreover, we assume that \( \frac{a}{b} \) is reduced; that is: \( a \) and \( b \) have no common factors other than \(-1\) and \(1\).

Now \( 2 = \frac{a^3}{b^3} \), so \( 2b^3 = a^3 \). Therefore \( a^3 \) is even.

By the previous problem, \( a \) is even. Write \( a = 2k \), \( k \in \mathbb{Z} \).

Then \( 2b^3 = (2k)^3 = 8k^3 \), so \( b^3 = 4k^3 = 2(2k^3) \). Hence \( b^3 \) is even, and it follows that \( b \) is even. We have reached a contradiction since we have proved that \( a \) and \( b \) have a common factor of 2, but this is contrary to our assumption. \( \Box \)
5. (6 points)
Let \(a, b \in \mathbb{Z}\), with \(a \neq 0\).

(a) State the definition of the phrase: \(a\) divides \(b\).

For integers \(a, b\) with \(a \neq 0\), \(a\) divides \(b\) means

\[ b = ak \text{ for some integer } k. \]

(b) Prove: If \(3 | ab\), then \(3 | a\) or \(3 | b\).

Proof: We start by rewriting the statement as:

If \(ab \equiv 0 \pmod{3}\), then \(a \equiv 0 \pmod{3}\) or \(b \equiv 0 \pmod{3}\).

We employ a proof by contrapositive.

Assume that \(a \not\equiv 0 \pmod{3}\) and \(b \not\equiv 0 \pmod{3}\). Then, without loss of generality, there are three cases.

Case 1 \(a \equiv 1 \pmod{3}, b \equiv 1 \pmod{3}\)

Then \(ab \equiv (1)(1) \equiv 1 \pmod{3}\), so \(ab \not\equiv 0 \pmod{3}\).

Case 2 \(a \equiv 1 \pmod{3}, b \equiv 2 \pmod{3}\).

Then \(ab \equiv (1)(2) \equiv 2 \pmod{3}\), so \(ab \not\equiv 0 \pmod{3}\).

Case 3 \(a \equiv 2 \pmod{3}, b \equiv 2 \pmod{3}\)

Then \(ab \equiv (2)(2) \equiv 4 \equiv 1 \pmod{3}\), so \(ab \not\equiv 0 \pmod{3}\). \[\square\]
6. (6 points)

Let \( a, b, m \in \mathbb{Z} \), with \( m \geq 2 \).

(a) State the definition of the phrase: \( a \) is congruent to \( b \) modulo \( m \).

For integers \( a, b, m \) with \( m \geq 2 \),

\( a \) is congruent to \( b \) modulo \( m \) means that

\[ m \mid a - b. \]

(b) Prove: For every integer \( n \), \( n^3 = 4n \mod 3 \).

**Proof**: We consider three cases. Let \( n \in \mathbb{Z} \).

**Case 1**: \( n \equiv 0 \mod 3 \)

Then \( n^3 \equiv 0^3 \equiv 0 \mod 3 \), and \( 4n = 4(0) \equiv 0 \mod 3 \),

so \( n^3 \equiv 4n \mod 3 \).

**Case 2**: \( n \equiv 1 \mod 3 \)

Then \( n^3 \equiv 1^3 \equiv 1 \mod 3 \), and \( 4n = 4(1) \equiv 4 \equiv 1 \mod 3 \),

so \( n^3 \equiv 4n \mod 3 \).

**Case 3**: \( n \equiv 2 \mod 3 \)

Then \( n^3 \equiv (2)^3 \equiv 8 \equiv 2 \mod 3 \), and \( 4n = 4(2) \equiv 8 \equiv 2 \mod 3 \),

so \( n^3 \equiv 4n \mod 3 \). \( \square \)
7. (7 points)

Choose one of the following. If you attempt both, clearly indicate which one you would like me to grade.

(a) Prove: For all sets A and B,
\[ B = (B - A) \cup (A \cap B). \]

(b) Prove: For every positive integer n,
\[ 1 + 5 + 9 + \cdots + (4n - 3) = 2n^2 - n. \]

Proof of (a)

Let \( b \in B \). Then either \( b \in A \) or \( b \notin A \).

If \( b \in A \), then \( b \in A \cap B \), so \( b \in (B - A) \cup (A \cap B) \).

If \( b \notin A \), then \( b \in B - A \), so \( b \in (B - A) \cup (A \cap B) \).

Hence \( B \subseteq (B - A) \cup (A \cap B) \).

Next, let \( c \in (B - A) \cup (A \cap B) \). So \( c \in B - A \) or \( c \in A \cap B \). In either case we know that \( c \in B \).

Hence \( (B - A) \cup (A \cap B) \subseteq B \). \( \Box \)

Proof of (b)

For the base step, observe that \( 4(1) - 3 = 1 \), and
\[ 1 = 2(1)^2 - 1. \]

For the inductive step assume that for some \( k \in \mathbb{N} \) that
\[ 1 + 5 + 9 + \cdots + (4k - 3) = 2k^2 - k. \]

Then
\[ 1 + 5 + \cdots + (4k - 3) + (4(k+1) - 3) = 2k^2 - k + 4k + 1, \quad \text{by assumption} \]
\[ = 2k^2 + 3k + 1 \]
\[ = 2(k+1)^2 - (k+1). \] \( \Box \)