1. (5 points) Find integers $q$ and $r$ such that $-54 = 13q + r$ with $0 \leq r < 13$.

\[
\begin{align*}
q &= -5 \\
r &= 11
\end{align*}
\]

2. (12 points) (a) Use the Euclidean algorithm to compute the greatest common divisor of 3618 and 1139.

\[
\begin{align*}
3618 &= 3 \times 1139 + 201 \\
1139 &= 5 \times 201 + 134 \\
201 &= 1 \times 134 + 67 \\
134 &= 2 \times 67
\end{align*}
\]

\[
\text{gcd}(3618, 1139) = 67
\]

(b) Write this gcd as a linear combination of 3618 and 1139.

\[
3618 \cdot 6 + 1139 \cdot (-19) = 67
\]

3. (8 points) Prove that \( \frac{n^3 + 2n}{3} \) is an integer for all integers \( n \).

4. (5 points) What is the least residue of \( 776^{79} \) modulo 7?

\[
776 \equiv 6 \equiv -1 \quad (\text{mod } 7) \quad \Rightarrow \quad 776^{79} \equiv (-1)^{79} \equiv -1 \equiv 6 \quad (\text{mod } 7)
\]
5. (8 points) Use the definition of congruence to prove that if \( a \equiv 3 \pmod{4} \) and \( b \equiv 1 \pmod{4} \) then \( a^2 + 2ab \equiv 7 \pmod{8} \).

Suggestion: \( \color{red}a \equiv 3 \pmod{4} \) \( \Rightarrow \) \( a = 4k + 3 \) for some \( k, b \in \mathbb{Z} \)
and \( \color{red}b \equiv 1 \pmod{4} \) \( \Rightarrow \) \( b = 4m + 1 \) for some \( m, b \in \mathbb{Z} \).

\[
\begin{align*}
    a^2 + 2ab &= (4k + 3)^2 + 2(4k + 3)(4m + 1) \\
               &= 16k^2 + 24k + 9 + 8mk + 12k + 6m \\
               &= 16k^2 + 32k + 16m^2 + 24k + 6m \\
               &= 16k^2 + 32k + 16m^2 + 24k + 6m \\
               &= 7 + 3(1 + 4k + 3k + 4m + 2k^2) \\
               &= 7 + 3m
\end{align*}
\]

Hence, \( a^2 + 2ab \equiv 7 \pmod{8} \).

6. (12 points) Decide whether the following linear Diophantine equations have any solutions. If so, give the general solution; if not, say why there are no solutions. There is no need to go through the Euclidean algorithm to find obvious gcds or solutions.

(a) \( 21x - 35y = 77 \), \( x, y \in \mathbb{Z} \).

\( \gcd(21, 35) = \gcd(7, 35) = 7 \)

\( \frac{77}{7} = 11 \) \( \Rightarrow \) \( \) \text{Yes, solution.}

(b) \( 24x + 39y = 26 \), \( x, y \in \mathbb{Z} \).

\( \gcd(24, 39) = \gcd(3, 13) = 3 \)

\( \frac{26}{3} \) \( \text{No solution.} \)

7. (10 points) What values can \( 3a + 5, 5a + 7 \) take? When is it 4?

\( d | 3a + 5 \) \( \Rightarrow \) \( 5(3a + 5) - 3(5a + 7) = k \) \( \Rightarrow \) \( k = 2, 12, 14 \)

\( d | 5a + 7 \) \( \Rightarrow \) \( 3a + 5, 5a + 7 \) \( \text{check all possible a mod 4} \)

\( a \equiv 0 \pmod{4} \)
\( 5a + 7 \equiv 3 \not\equiv 0 \pmod{4} \)

\( a \equiv 1 \pmod{4} \)
\( 3a + 5 \equiv 2 \not\equiv 0 \pmod{4} \)
\( 5a + 7 \equiv 7 \not\equiv 0 \pmod{4} \)

\( a \equiv 2 \pmod{4} \)
\( 3a + 5 \equiv 3 \not\equiv 0 \pmod{4} \)
\( 5a + 7 \equiv 7 \not\equiv 0 \pmod{4} \)

\( a \equiv 3 \pmod{4} \)
\( 3a + 5 \equiv 1 \not\equiv 0 \pmod{4} \)
8. (8 points) Use the definition of divisibility to prove that if \( a, b, c \) and \( d \) are non-zero integers with \( a \mid b \) and \( b \mid c \) and \( c \mid d \) then \( a \mid 2c + d \).

\[
\text{Suppose } a \mid b, b \mid c \text{ and } c \mid d. \\
\text{So } b = an, \ c = bn = amn, \ d = c = amnl \text{ for some integers } n, m, l.
\]

Hence,
\[
2c + d = 2amnl + amnl = a(2mn + ml) = as
\]
where \( s = 2mn + ml \) is an integer, and \( a \mid 2c + d \).

9. (22 points) Circle True (T) or False (F).

- (a) If \((3a, 3b) = 3 \) then \( a \) and \( b \) must be relatively prime. (a) \( (3a, 3b) = 3(a, b) \)
- (b) If \( n^2 + 1 \) is not prime then \( n \) is odd.
- (c) If \( a \mid b \) then \( a^2 \mid b^2 \).
- (d) If \( a \mid b^2 \) then \( a \mid b \).
- (e) If \( d \mid a \) and \( d \mid b \) then \( d \mid (a, b) \).
- (f) Any even integer can be written as a linear combination of 10 and 21.
- (g) The smallest positive integer of the form \( 6x + 9y + 15z, \ x, y, z \in \mathbb{Z}, \) is 3.
- (h) For any integer \( b \) there exist unique integers \( q, r \) with \( b = 7q + r \) and \( 0 < r < 7 \). \( r = 0, 1, 2, \ldots, 6 \).
- (i) If \( a \) and \( b \) are both even then \([a, b] = ab/2 \).
- (j) \{5, 11, -3, -1, 2\} is a complete system of residues modulo 5.
- (k) \( 2^{26} + 1 \) is divisible by \( 2^{11} + 1 \).

10. (8 points) Suppose that \( a, b \) and \( c \) are positive integers with \( b \mid c \) and \( m = [a, c] \). Prove that \( [a, b] \leq m \).

\[
m = [a, c] \text{ is a positive integer which is a multiple of both } a \text{ and } c,
\]
so \( a \mid m \) and \( c \mid m \) (in fact the smallest but we don't use this fact!).

Since \( b \mid c \) and \( c \mid m \) we have \( b \mid m \) (\( c = bk, \ m = cl \Rightarrow m = b(kl) \)).

Thus \( a \mid m \) and \( b \mid m \) and \( m \) is a positive integer which is a common multiple of both \( a \) and \( b \). Since by definition \( \text{gcd}(a, b) \) is the least such common multiple we must have \([a, b] \leq m \).