# Problem 1 (12 points)

In the following statements, \( \mathbb{P} \) is the set of primes, \( \mathbb{N} \) is the set of natural numbers, and \( \mathbb{Z} \) is the set of integers. Which of these statements are true and which are false?

<table>
<thead>
<tr>
<th>True</th>
<th>False</th>
</tr>
</thead>
</table>
| ✓    | □     | The statement form \( pq \lor \overline{p} \lor p\overline{q} \) is a tautology.  
  Simplifies to \( \overline{p} \lor pq \lor p\overline{q} \equiv \overline{p} \lor p(q \lor \overline{q}) \equiv \overline{p} \lor p \equiv T \) |
| □    | ✓     | The statement forms \( \sim(p \lor (q \land r)) \) and \( \overline{p} \lor \overline{q} \lor \overline{r} \)
  are logically equivalent.  
  Consider, for example, the case \( p = T, q = T, r = F \). |
| ✓    | □     | \( \forall n \in \mathbb{Z}, \) if \( 3n + 2 \) is even then \( n + 5 \) is odd.  
  \( 3n + 2 \) is even if and only if \( n \) is even, in which case \( n + 5 \) is odd. |
| □    | ✓     | \( \exists m \in \mathbb{N}, \forall n \in \mathbb{Z}, \) if \( n \geq m \) then \( (n^2 - n + 17) \in \mathbb{P} \).  
  \( n^2 - n + 17 \) cannot be a prime whenever \( n \) is a multiple of 17. |
| □    | ✓     | The last decimal digit of the number \( 42^7 \) is 7.  
  Since 42 is even, so is \( 42^7 \). Hence its last digit is one of 0, 2, 4, 6 or 8. |
| ✓    | □     | The number \( 10110100101100_2 \), expressed in binary, is divisible by 4.  
  \( a_k2^k + \cdots + a_22^2 + a_12^1 + a_0 \) is divisible by 4 when \( a_1 = a_0 = 0 \). |
Problem 2 (18 points)

a. The numbers \( x = 210_3 \) and \( y = 112_3 \) are expressed in the ternary (base-3) number system. Compute their sum \( a = x + y \) and product \( b = xy \) using ternary arithmetic. Show all stages of your ternary computation and express its results in the ternary number system.

**Answer:** Here are the ternary computations:

\[
\begin{array}{c}
210 \\
\hline
+ 112 \\
\hline
1022
\end{array}
\]

\[
\begin{array}{c}
210 \\
1120 \\
210 \\
101220
\end{array}
\]

Indeed, \( 210_3 = 2 \cdot 3^2 + 3 = 57 \) and \( 112_3 = 3^2 + 3 + 2 = 32 \). It can be easily verified that \( 57 + 32 = 89 \) and \( 57 \times 32 = 1824 \). In turn, \( 89 = 1022_3 \) and \( 1824 = 101220_3 \).

\[
a = 1022_3 \quad b = 101220_3
\]

b. In this problem, \( n \) is an arbitrary integer with \( n \geq 2 \). What is \( (n - 1)^2(n + 1) \) modulo \( n \)?

**Answer:** Using the rules of modular arithmetic, we can first reduce the terms in the product as follows: \( n + 1 \equiv 1 \mod n \) and \( n - 1 \equiv -1 \mod n \). Therefore:

\[
(n - 1)^2(n + 1) \equiv (-1)^2 \cdot 1 \equiv 1 \mod n
\]

\[
(n - 1)^2(n + 1) = 1 \mod n
\]

c. Let \( m = 2^{11} \cdot 3^5 \cdot 5^9 \cdot 11^2 \) and \( n = 3^7 \cdot 5^3 \cdot 7^2 \). Let \( d \) be the largest integer such that \( d|m \) and \( d|n \). What is the prime factorization of \( d \)?

**Answer:** Clearly, \( d = \gcd(m, n) \) and the prime factorization of \( \gcd(m, n) \) can be computed as follows:

\[
d = \gcd(m, n) = 2^{\min\{11,0\}} \cdot 3^{\min\{5,7\}} \cdot 5^{\min\{9,3\}} \cdot 7^{\min\{0,2\}} \cdot 11^{\min\{2,0\}} = 3^5 \cdot 5^3
\]

\[
d = 3^5 \cdot 5^3
\]
Problem 3 (30 points)

a. Since the Boolean function \( f(p, q, r) \) takes the value 1 if and only if at least two of the three variables are 1, the truth table is given by:

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>r</th>
<th>( f(p, q, r) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

b. To express the function \( f(p, q, r) \) in disjunctive normal form (DNF), we can simply read off the corresponding minterms from the truth table, and obtain:

\[
f(p, q, r) = \bar{p}qr \lor p\bar{q}r \lor pq\bar{r} \lor pqr
\]

(1)

c. To express the function \( f(p, q, r) \) in conjunctive normal form (CNF), we can start with the disjunctive normal form for \( \sim f(p, q, r) \), namely \( \sim f(p, q, r) = \bar{p}\bar{q}\bar{r} \lor \bar{p}q\bar{r} \lor \bar{p}qr \lor p\bar{q}r \), and then use De Morgan rules of negation to obtain:

\[
f(p, q, r) = (p \lor q \lor \bar{r})(p \lor q \lor \bar{r})(p \lor \bar{q} \lor \bar{r})(\bar{p} \lor q \lor r)
\]

Alternatively, we can simply read off the corresponding \textit{maxterms} for the zeors of \( f(p, q, r) \) from the truth table to arrive at the same result.

d. To design a logic circuit that implements \( f(p, q, r) \), one could simplify the DNF in (1). Alternatively, one can recognize that \( f(p, q, r) \) is precisely the Boolean function that produces the carry in the binary addition of \( p, q, \) and \( r \), since the carry is produced if and only if at least two of the three variables are 1. Thus a logic circuit implementing \( f(p, q, r) \) is the same as the one that implements carry in a full-adder. That circuit was designed in class, as follows:

![Logic circuit diagram]

Problem 4 (20 points)

a. Using the specified domains and predicates, the assertion that a sequence \( \{a_n\}_{n=1}^{\infty} \) converges to zero can be expressed as follows:

\[
S : \forall \epsilon \in \mathbb{R}^+, \exists m \in \mathbb{N}^+, \forall n \in \mathbb{N}^+, \quad P(n, m) \rightarrow Q(a_n, \epsilon)
\]
b. The contrapositive, the converse, the inverse, and the negation of the statement \( S \) from part (a) are given by:

**Contrapositive:** \( \forall \epsilon \in \mathbb{R}^+, \exists m \in \mathbb{N}^+, \forall n \in \mathbb{N}^+, \quad \sim P(n, m) \lor Q(a_n, \epsilon) \)

**Converse:** \( \forall \epsilon \in \mathbb{R}^+, \exists m \in \mathbb{N}^+, \forall n \in \mathbb{N}^+, \quad \sim Q(a_n, \epsilon) \lor P(n, m) \)

**Inverse:** \( \forall \epsilon \in \mathbb{R}^+, \exists m \in \mathbb{N}^+, \forall n \in \mathbb{N}^+, \quad \sim Q(a_n, \epsilon) \lor P(n, m) \)

**Negation:** \( \exists \epsilon \in \mathbb{R}^+, \forall m \in \mathbb{N}^+, \exists n \in \mathbb{N}^+, \quad \sim Q(a_n, \epsilon) \land P(n, m) \)

To obtain these expressions we used the equivalences \( \tilde{q} \rightarrow \tilde{p} \equiv q \lor \tilde{p}, \ q \rightarrow \tilde{p} \equiv \tilde{q} \lor p, \) and \( \tilde{p} \rightarrow \tilde{q} \equiv p \lor \tilde{q}, \) for the contrapositive, the converse, and the inverse, respectively. We have also used the rules of negation in predicate and propositional logic. Note that the contrapositive is equivalent to \( S, \) while converse and inverse are precisely the same statement.

**Problem 5 (20 points)**

a. If \( n \) is a positive even integer, then \( n = 2t \) for some \( t \in \mathbb{Z}^+ \) and therefore \( n^2 = (2t)^2 = 4t^2. \) It follows that \( n^2 \) is divisible by 4.

\[
\begin{array}{c}
\text{n}^2 \equiv 0 \text{ mod 4}
\end{array}
\]

b. If \( n \) is a positive odd integer, then \( n = 2t + 1 \) for some \( t \in \mathbb{N} \) and therefore \( n^2 = (2t + 1)^2 = 4t^2 + 4t + 1. \) It follows that \( n^2 \equiv 1 \text{ mod 4} \)

\[
\begin{array}{c}
\text{n}^2 \equiv 1 \text{ mod 4}
\end{array}
\]

c. Let \( m = 4k + 3, \) where \( k \) is a positive integer. Then \( m \equiv 3 \text{ mod 4} \). We will show by contradiction that there do not exist \( a, b \in \mathbb{Z} \) such that \( m = a^2 + b^2. \) Assume, to the contrary, that such \( a, b \in \mathbb{Z} \) do exist. Then evaluating \( m = a^2 + b^2 \) modulo 4, based upon the results of parts (a) and (b) above, we obtain either \( 0 + 0 = 0 \) or \( 0 + 1 = 1 \) or \( 1 + 1 = 2. \) This contradicts the fact that \( m \equiv 3 \text{ mod 4} \). Therefore \( a, b \in \mathbb{Z} \) such that \( m = a^2 + b^2 \) do not exist.

**Extra credit Problem 6 (30 points)**

We will prove that \( p = 3 \) is the unique prime \( p, \) such that \( p + 2 \) and \( p + 4 \) are also primes. Obviously, \( 3, 3 + 2 = 5, \) and \( 3 + 4 = 7 \) are all primes. To show that there are no other primes \( p \) that have this property, let us consider the residues of \( p, p + 2, \) and \( p + 4 \) modulo 3.

Since \( 0 = 0 \text{ (mod 3)}, \ 2 = 2 \text{ (mod 3)}, \) and \( 4 = 1 \text{ (mod 3)} \) are all different, it follows that \( p, p + 2, \) \( p + 3 \) belong to different residue classes modulo 3. As there are only three residue classes modulo 3, namely \( \mathbb{Z}_0, \mathbb{Z}_1, \mathbb{Z}_2, \) it follows that (exactly) one of the numbers \( p, p + 2, p + 3 \) belongs to \( \mathbb{Z}_0, \) and thus is divisible by 3. This number cannot be prime, unless it is 3 itself!