Homework 2 Solutions

1. Determine whether the following statements are logically equivalent, using truth tables.

   (a) $(\sim P) \lor Q$ and $P \Rightarrow Q$.

   \[
   \begin{array}{c|c|c|c|c}
   P & Q & (\sim P) & (\sim P) \lor Q & P \Rightarrow Q \\
   T & T & F & T & T \\
   T & F & F & F & T \\
   F & T & T & T & T \\
   F & F & T & T & T \\
   \end{array}
   \]

   These are logically equivalent.

   (b) $P \Leftrightarrow Q$ and $(\sim P) \Leftrightarrow (\sim Q)$.

   \[
   \begin{array}{c|c|c|c|c|c|c}
   P & Q & \sim P & \sim Q & P \Leftrightarrow Q & (\sim P) \Leftrightarrow (\sim Q) \\
   T & T & F & F & T & T \\
   T & F & F & T & F & F \\
   F & T & T & F & F & F \\
   F & F & T & T & T & T \\
   \end{array}
   \]

   These are logically equivalent.

   (c) $P \Rightarrow (Q \lor R)$ and $P \Rightarrow (\sim Q \Rightarrow R)$.

   \[
   \begin{array}{c|c|c|c|c|c|c|c|c|c}
   P & Q & R & Q \lor R & (\sim Q) \Rightarrow R & P \Rightarrow (Q \lor R) & P \Rightarrow (\sim Q) \Rightarrow R \\
   T & T & T & T & T & T & T \\
   T & T & F & T & T & T & T \\
   T & F & T & T & T & T & T \\
   F & T & T & T & T & T & T \\
   T & F & F & F & F & F & F \\
   F & T & F & T & T & T & T \\
   F & F & T & T & T & T & T \\
   F & F & F & F & T & T & T \\
   \end{array}
   \]

   These are logically equivalent.

   (d) $(P \lor Q) \Rightarrow R$ and $(P \Rightarrow R) \land (Q \Rightarrow R)$.

   \[
   \begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c}
   P & Q & R & P \lor Q & P \Rightarrow R & Q \Rightarrow R & (P \lor Q) \Rightarrow R & (P \Rightarrow R) \land (Q \Rightarrow R) \\
   T & T & T & T & T & T & T & T \\
   T & T & F & T & F & F & F & F \\
   T & F & T & T & T & T & T & T \\
   F & T & T & T & T & T & T & T \\
   T & F & F & T & F & F & F & F \\
   F & T & F & T & F & F & F & F \\
   F & F & T & T & T & T & T & T \\
   F & F & F & T & T & T & T & T \\
   \end{array}
   \]

   These are logically equivalent.
2. Prove that if \( n \in \mathbb{Z} \) and \( n^2 + 4n + 5 \) is odd, then \( n \) is even.

**Proof:** (Proof by contrapositive) Assume that \( n \) is odd. Then we see that \( n = 2k + 1 \) for some \( k \in \mathbb{Z} \). Thus, \( n^2 + 4n + 5 = (2k + 1)^2 + 4(2k + 1) + 5 = 2(2k^2 + 6k + 3) \). Since \( (2k^2 + 6k + 3) \in \mathbb{Z} \), we see that \( n^2 + 4n + 5 \) is even.

\( \square \)

3. Prove that if \( n, m \in \mathbb{Z} \) and \( n^2 + m^2 \) is even, then \( n, m \) have the same parity.

**Proof:** (Proof by contrapositive) Assume \( n, m \) have opposite parities. The we have two cases; either \( n \) is even and \( m \) is odd, or \( m \) is even and \( n \) is odd. Since the statement and the cases are symmetric with respect to \( n \) and \( m \), WLOG we can assume \( n \) is even and \( m \) is odd. In this case, we can write \( n = 2a \) and \( m = 2b + 1 \) for some \( a, b \in \mathbb{Z} \). Hence, \( n^2 + m^2 = (2a)^2 + (2b + 1)^2 = 4a^2 + 4b^2 + 4b + 1 = 2(2a^2 + 2b^2 + 2b) + 1 \). Since \( (2a^2 + 2b^2 + 2b) \in \mathbb{Z} \), we see that \( n^2 + m^2 \) is odd.

\( \square \)

4. Prove that if \( n \) is an even integer than \( n = 4k \) or \( n = 4k + 2 \) for some integer \( k \).

**Proof:** Assume \( n \) is an even integer. Then we see \( n = 2a \) for some \( a \in \mathbb{Z} \). Since \( a \in \mathbb{Z} \) we see that \( a \) is either even or odd.

**Case 1:** \( a \) is even: In this case, we see that \( a = 2m \) for some \( m \in \mathbb{Z} \). Thus, \( n = 2a = 2(2m) = 4m \) for some integer \( m \).

**Case 2:** \( a \) is odd: In this case, we see that \( a = 2t + 1 \) for some \( t \in \mathbb{Z} \). Thus, \( n = 2a = 2(2t + 1) = 4t + 2 \) for some integer \( t \).

Therefore, if \( n \) is an even integer than \( n = 4k \) or \( n = 4k + 2 \) for some integer \( k \).

\( \square \)

5. Let \( a \in \mathbb{Z} \). Prove that \( 3 \mid 5a \) if and only if \( 3 \mid a \).

**Proof:** This is a biconditional statement. Hence, we need to prove both implications:

\[ (3 \mid 5a) \implies (3 \mid a) \text{ and } (3 \mid 5a) \implies (3 \mid a) \]

Proof of \( (3 \mid a) \implies (3 \mid 5a) \): Assume that \( 3 \mid a \). Then we see that \( a = 3k \) for some \( k \in \mathbb{Z} \). Hence, \( 5a = 5(3k) = 3(5k) \). Since \( 5k \in \mathbb{Z} \), we get \( 3 \mid 5a \).

Proof of \( (3 \mid 5a) \implies (3 \mid a) \): Assume that \( 3 \mid 5a \). This implies \( 5a = 3m \) for some \( m \in \mathbb{Z} \). Therefore we see that by adding \( a \) to both sides, we get \( 6a = 3m + a \). Thus, \( a = 6a - 3m = 3(2a - m) \). Since \( (2a - m) \in \mathbb{Z} \), we see \( 3 \mid a \).

\( \square \)
6. Use the logical equivalences given in class to negate the following sentences

(a) 8 is even and 5 is prime.
This statement can be written as \( P \land Q \) for
P: “8 is even”, and
Q: “5 is prime”. Then its negation is
\[ \sim(P \land Q) \equiv (\sim P) \lor (\sim Q). \]
Then, we can write the negation as:
“8 is not even or 5 is not prime”.

(b) If \( n \) is a multiple of 4 and 5, then it is a multiple of 10.
This statement can be written as \( (P \land Q) \implies R \) for
P: “\( n \) is a multiple of 4”,
Q: “\( n \) is a multiple of 5”, and
R: “\( n \) is a multiple of 10”. Then its negation is
\[ \sim((P \land Q) \implies R) \equiv \sim((P \land Q) \lor R) \equiv (P \land Q) \land \sim R. \]
Then, we can write the negation as:
“\( n \) is a multiple of 4 and 5, but it is not a multiple of 10”.

(c) \( 3 \leq x \leq 6 \).
This open sentence can be written as \( P \land Q \) for
P: “\( x \geq 3 \)”, and
Q: “\( x \leq 6 \)”. Then its negation is
\[ \sim(P \land Q) \equiv (\sim P) \lor (\sim Q). \]
Then, we can write the negation as:
“\( x < 3 \) or \( x > 6 \)”.

(d) A real number \( x \) is less than \(-2\) or greater than \(2\) if its square is greater than \(4\).
This statement can be written as \( R \implies (P \lor Q) \) for
P: “\( x \) is less than \(-2\)”,
Q: “\( x \) greater than 2”, and
R: “\( x^2 \) is greater than \(4\)”. Then its negation is
\[ \sim(R \implies (Q \lor P)) \equiv \sim((\sim R) \lor (Q \land P)) \equiv R \land ((\sim Q) \land (\sim P)). \]
Then, we can write the negation as:
“The square of a real number \( x \) is greater than 4 and \( x \) is greater than or equal to \(-2\), and less than or equal to \(2\)”.

(e) If a function \( f \) is differentiable everywhere then whenever \( x \in \mathbb{R} \) is a local maximum of \( f \) we have \( f'(x) = 0 \).
This statement can be written as \( P \implies (Q \implies R) \) for
P: “\( f \) is differentiable everywhere”,
Q: “\( x \) is a local maximum of \( f \)”, and
R: “\( f'(x) = 0 \)”. Then its negation is
\[ \sim(P \implies (Q \implies R)) \equiv \sim((\sim P) \lor (\sim Q) \lor (\sim R)) \equiv P \land (Q \land (\sim R)). \]
Then, we can write the negation as:
“A function \( f \) is differentiable everywhere and \( x \in \mathbb{R} \) is a local maximum of \( f \), but \( f'(x) \neq 0 \).”

7. Assume \( a, b \in \mathbb{Z} \). Prove that if \( ax + by = 1 \) for some \( x, y \in \mathbb{Z} \), then \( \gcd(a, b) = 1 \).

**Proof:** (Proof by contrapositive) Let \( a, b \in \mathbb{Z} \). Assume that \( \gcd(a, b) \neq 1 \). Then we have two cases:

- either \( \gcd(a, b) \) doesn’t exist, or \( \gcd(a, b) = m \neq 1 \).

We see that if \( \gcd(a, b) \) doesn’t exist, that means that \( a = b = 0 \), in which case there are no integers \( x, y \) such that \( ax + by \neq 0 \).

If \( \gcd(a, b) = m \neq 1 \), then we see that \( m \) is a common divisor of both \( a \) and \( b \). Thus, \( a = ms \) and \( b = mt \) for some \( s, t \in \mathbb{Z} \). Therefore, for any \( x, y \in \mathbb{Z} \), we have \( ax + by = msx + mty = m(sx + ty) \).
Since \((sx + ty) \in \mathbb{Z}\), we see that \(m \mid (ax + by)\), and therefore \(m \leq |ax + by|\). Since \(m > 1\), we get that \(ax + by \neq 1\) whenever \(x, y \in \mathbb{Z}\).

8. Without using the triangle inequality, prove that if \(x \in \mathbb{R}\), then \(|x + 4| + |x - 3| \geq 7\).

**Proof:** We see that the statement involves the expressions \(|x + 4|\) and \(|x - 3|\). Thus, we need to understand when the expressions \((x + 4)\) and \((x - 3)\) change signs. To do that, we need to consider three cases: \(x < -4\), \(-4 \leq x \leq 3\), and \(x > 3\).

**Case 1:** \(x < -4\): In this case, we see that \(|x + 4| = -x - 4\) and \(|x - 3| = 3 - x\). Therefore, \(|x + 4| + |x - 3| = (-x - 4) + (3 - x) = -2x - 1\). Moreover, since \(x < 4\), we see \(-2x - 1 \geq 7\) which implies \(|x + 4| + |x - 3| \geq 7\).

**Case 2:** \(-4 \leq x \leq 3\): In this case, we see that \(|x + 4| = x + 4\) and \(|x - 3| = 3 - x\). Therefore, \(|x + 4| + |x - 3| = (x + 4) + (3 - x) = 7\). Hence, \(|x + 4| + |x - 3| \geq 7\).

**Case 3:** \(x > 3\): In this case, we see that \(|x + 4| = x + 4\) and \(|x - 3| = x - 3\). Therefore, \(|x + 4| + |x - 3| = (x + 4) + (x - 3) = 2x + 1\). Moreover, since \(x > 3\), we see \(2x + 1 \geq 7\) which implies \(|x + 4| + |x - 3| \geq 7\).

Therefore if \(x \in \mathbb{R}\), then \(|x + 4| + |x - 3| \geq 7\).

9. Let \(m \in \mathbb{Z}\). Prove that if \(5 \nmid m\), then \(m^2 \equiv 1 \pmod{5}\) or \(m^2 \equiv -1 \pmod{5}\).

**Proof:** Assume that \(5 \nmid m\). By the Division Algorithm, there are four cases for \(m\): \(m = 5k + 1\), \(m = 5k + 2\), \(m = 5k + 3\), or \(m = 5k + 4\) for some \(k \in \mathbb{Z}\).

**Case 1:** \(m = 5k + 1\) for some \(k \in \mathbb{Z}\). In this case, we have \(m^2 = 25k^2 + 10k + 1\). Thus, we see \(m^2 - 1 = 5(5k^2 + 2k)\). Since \((5k^2 + 2k) \in \mathbb{Z}\), we see \(5 \mid (m^2 - 1)\), that is \(m^2 \equiv 1 \pmod{5}\).

**Case 2:** \(m = 5k + 2\) for some \(k \in \mathbb{Z}\). In this case, we have \(m^2 = 25k^2 + 20k + 4\). Thus, we see \(m^2 + 1 = 5(5k^2 + 2k + 1)\). Since \((5k^2 + 2k + 1) \in \mathbb{Z}\), we see \(5 \mid (m^2 + 1)\), that is \(m^2 \equiv -1 \pmod{5}\).

**Case 3:** \(m = 5k + 3\) for some \(k \in \mathbb{Z}\). In this case, we have \(m^2 = 25k^2 + 30k + 9\). Thus, we see \(m^2 + 1 = 5(5k^2 + 2k + 2)\). Since \((5k^2 + 2k + 2) \in \mathbb{Z}\), we see \(5 \mid (m^2 + 1)\), that is \(m^2 \equiv -1 \pmod{5}\).

**Case 4:** \(m = 5k + 4\) for some \(k \in \mathbb{Z}\). In this case, we have \(m^2 = 25k^2 + 40k + 16\). Thus, we see \(m^2 - 1 = 5(5k^2 + 2k + 3)\). Since \((5k^2 + 2k + 3) \in \mathbb{Z}\), we see \(5 \mid (m^2 - 1)\), that is \(m^2 \equiv 1 \pmod{5}\).

Therefore, if \(5 \nmid m\), then \(m^2 \equiv 1 \pmod{5}\) or \(m^2 \equiv -1 \pmod{5}\).

10. **Bézout’s identity:** Let \(a, b \in \mathbb{Z}\) such that \(\gcd(a, b) = 1\). Then there exists \(x, y \in \mathbb{Z}\) such that \(ax + by = 1\).

For example, for \(a = 5\) and \(b = 7\) we can take \(x = 10\) and \(b = -7\).

Using Bézout’s identity, show that for \(a \in \mathbb{Z}\) and \(p\) prime, if \(a \not\equiv 0 \pmod{p}\) then \(ak \equiv 1 \pmod{p}\) for some \(k \in \mathbb{Z}\).

**Proof:** Let \(a \in \mathbb{Z}\) and \(p\) be prime. Assume that \(a \not\equiv 0 \pmod{p}\). Then we see that, since \(p\) is prime, \(\gcd(a, p)\) is either 1 or \(p\). Moreover, since \(a \not\equiv 0 \pmod{p}\), we see that \(p \nmid a\). Hence, \(\gcd(a, p) = 1\). Thus, using the Bézout’s identity, we know that there exist \(x, y \in \mathbb{Z}\) such that \(ax + py = 1\). This implies, \(ax - 1 = py\). Hence, since \(y \in \mathbb{Z}\), we see \(p \mid (ax - 1)\).

Therefore \(ax \equiv 1 \pmod{p}\) for \(x \in \mathbb{Z}\) as chosen above.