**Homework 3**

**Oliver Kis**

**15576333**

**02 February 2024**

The University of British Columbia

Electrical and Computer Engineering

Math 220 - Mathematical Proofs

Instructor: Bennett Michael

## Solutions

For Homework 3, Problem 3, 4, 5, 6, a part of 7, and a part of 8 are worth marks.

**Problem 3.** (2 *Points*) Let $a \in \mathbb{Z}$. Prove the following statement:

$$\text{if } 5 \mid 2a, \text{ then } 5 \mid a.$$

Proof: Let $a \in \mathbb{Z}$. Using divisibility rules and implication rules, if the hypothesis and conclusion are both true, then the implication is true.

$$\text{if } 2a = 5k \text{ where } k \in \mathbb{Z}$$
$$a = \tfrac{5k}{2}$$
$$\text{Where } a \in \mathbb{Z}, \text{ this means } k = 2m$$
$$a = \tfrac{5*2m}{2} = 5m$$

**Problem 4.** (5 *Points*)

1. (1 *Points*) Prove the following statement. For every $a \in \mathbb{R}$,

$$\text{if } a \geq 4, \text{ then } -a^2/4 + a \leq 0.$$

Proof: Let $a \in \mathbb{R}$. Solve via contrapositive.

$$\text{if } -\frac{a^2}{4} + a > 0 \text{ then } a < 4$$
$$-\frac{a^2}{4} > -a \longrightarrow \frac{a^2}{4} < a$$
$$a^2 < 4a = a < 4$$

2. (4 *Points*) Let $a \in \mathbb{R}$. Prove the following statement:

$$(\text{for every } x \in \mathbb{R}, \text{ we have } x^2 + ax + a > 0) \text{ if and only if } (0 < a < 4).$$

Proof: Let $a \in \mathbb{R}$. Biconditionally solve this problem.

$$\forall\ x \in \mathbb{R},\ x^2 + ax + a > 0 \Longleftrightarrow 0 < a < 4$$

$$(\Longleftarrow): \text{ Completeteting the square first} \rightarrow (x + \tfrac{a}{2})^2 + \tfrac{4a-a^2}{4} > 0$$
$$\text{Since } 0 < a < 4 \therefore 4a - a^2 > 0, \text{ thus } \tfrac{4a-a^2}{4} > 0$$
$$(x + \tfrac{a}{2})^2 \geq 0 \text{ since } ()^2 \text{ is always positive}$$
$$\text{Hence, } (x + \tfrac{a}{2})^2 + \tfrac{4a-a^2}{4} > 0 \text{ when } 0 < a < 4$$

$$(\Longrightarrow): \text{ Utilizing the contrapositive from part one to solve this.}$$
$$4a - a^2 = -\tfrac{a^2}{4} + a \longrightarrow -\tfrac{a^2}{4} + a > 0 \text{ from earlier proof.}$$
$$\therefore 4a - a^2 > 0 \text{ and reworking } a < 4.$$
$$\text{Thus, our range for } a \text{ is } 0 < a < 4 \text{ for } \tfrac{4a-a^2}{4}$$
$$\text{Additionally, } (x + \tfrac{a}{2})^2 \geq 0 \text{ since } ()^2 \text{ is always positive, but it can be zero}$$
$$\text{Finally, if } (x + \tfrac{a}{2})^2 \text{ is zero} \longrightarrow 0 + \tfrac{4a-a^2}{4} > 0, \text{ this implies to get } > 0, \text{ we need } 0 < a < 4$$

With both implications being solved, the biconditional statement is true.

**Problem 5.** (2 *Points*) 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: This is solved by proof by cases. Let $m \in \mathbb{Z}$. When $5 \nmid m$, there are 4 cases.

$$1) \text{ Case } 1: \; m \equiv 1(mod 5) \longrightarrow m = 5k + 1 \text{ for some } k \in \mathbb{Z}$$
$$m^2 = (5k+1)^2 \longrightarrow m^2 = 25k^2 + 10k + 1 \longrightarrow m^2 = 5(5k^2 + 2k) + 1$$
$$\therefore m^2 \equiv 1(mod 5), \text{ which holds our first statement true}$$

$$2) \text{ Case } 2: \; m \equiv 2(mod 5) \longrightarrow m^2 = (5k+2)^2 \longrightarrow m^2 = 5(5k^2 + 4k) + 4$$
$$\therefore m^2 \equiv 4(mod 5) \text{ which is equivalent to } m^2 \equiv -1(mod 5)$$

$$3) \text{ Case } 3: \; m \equiv 3(mod 5) \text{ achieves the same as Case 2}$$
$$m^2 \equiv 9(mod 5) = m^2 \equiv -1(mod 5)$$

$$4) \text{ Case } 4: \; m \equiv 4(mod 5) \text{ achieved the same as Case 1}$$
$$m^2 \equiv 16(mod 5) = m^2 \equiv 1(mod 5)$$

Thus, we proved that $5 \nmid m$, then $m^2 \equiv 1 \pmod 5$ or $m^2 \equiv -1. \pmod 5$

**Problem 6.** (2 *Points*) For $a \in \mathbb{Z}$, prove:

$$3 \nmid a \Longrightarrow (\text{there exists } b \in \mathbb{Z} \text{ such that } ab \equiv 1 mod 3$$

Proof: Let $a, b \in \mathbb{Z}$. This is solved by two cases

$$1) \text{ Case } 1: \; a = 3k + 1 \Longrightarrow \exists\, b \in \mathbb{Z} \; s.t. \; ab = 3k + 1$$
$$\text{Using simple numbers, when } b = 1 \longrightarrow a = 3k + 1 \Longrightarrow a \equiv 1(\text{mod} 3).$$

$$2) \text{ Case } 2: \; a = 3k + 2 \Longrightarrow \exists\, b \in \mathbb{Z} \; s.t. \; ab = 3k + 1$$
$$\text{When } b = 2,\; a = 3k + 2 \longrightarrow 2a = 2(3k+2) = 6k + 4 = 6k + 3 + 1 = 3(2k+1) + 1$$
$$\therefore \text{ when } b = 2, ab \equiv 1(\text{mod} 3)$$

**Problem 7.** (2 *Points*) Prove that the product of 5 consecutive integers is a multiple of 5.

Proof: Pure logic solves this question. Since we utilize 5 consecutive integers, this indicates at one point there is a multiple of 5 in the product. This means the product will be divisible by 5.

$a, b, c, d, e \in \mathbb{Z}$. We know with consecutive numbers that
$a = a, b = a + 1, c = a + 2, d = a + 3$, and $e = a + 4$.
Testing a value such as $a = 1$ or $a = 2$, this stands true.
Since we know our hypothesis is true, it also stands that
$a = a + 1, b = a + 2, c = a + 3, d = a + 4$, and $e = a + 5$
$e = a + 5$ has a remainder of 5, thus as long as one part of the product is divisble by 5, all of it is.

**Problem 8.** (2 *Points*) We recall that given $a, b \in \mathbb{Z}$ such that $ab \neq 0$, we define the gcd of $a$ and $b$ to be the greatest integer that divides both $a$ and $b$. We denote this by $gcd(a, b)$

Let $a, b \in \mathbb{Z}$ such that $ab \neq 0$. We suppose that there exists $u, v, \in \mathbb{Z}$ such that

$$1 = au + bv$$

Prove that $\gcd(a, b) \equiv 1$.

Proof: Let $a, b \in \mathbb{Z}$. We also know neither $a$ or $b$ can be 0. Researching Bézout's identity and greatest common divisor, we know that $c \in \mathbb{Z}$ divides $gcd(a, b)$. We also know that $c$ also divides $au$ and $bv$. Through linearity, we know when added, $au + bv = 1$. This also states that 1 is divisible by $c$. If you divide 1, you can only divide by 1 or -1. But gcd is always going to assume a positive value. $\therefore gcd(a, b) \equiv 1$. Additionally, that means $a, b$ are primes.