Homework 6

MATH 301
October 8, 2020

Kevin Evans
ID: 11571810

---

1. **Proposition.** *Let n be an integer. Then n is odd if and only if $3n + 6$ is odd.*

   Proof. Suppose n is an odd integer. Then n can be represented as

   $$n = 2k + 1$$

   for some $k \in \mathbb{Z}$. Then the expression $3n + 6$ can be written as

   $$\begin{aligned} 3n + 6 &= 3\,(2k + 1) + 6 \\ &= 6k + 9 = 2k' + 1 \end{aligned}$$

   where $k' = 3k + 4$ and $k' \in \mathbb{Z}$. Therefore, if n is odd, then $3n + 6$ is also odd. Next, we will show the converse is also true. Suppose $3n + 6$ is odd, then

   $$3n + 6 \equiv 1 \pmod 2$$

   And since $6 \equiv 0 \pmod 2$, we can subtract this out and

   $$3n \equiv 1 \pmod 2$$

   For an even n, the expression becomes $2(3j) \equiv 0 \pmod 2$ for $j \in \mathbb{Z}$. For an odd $n = 2j' + 1$, it equals $2(3j' + 1) \equiv 1 \pmod 2$ for $j' \in \mathbb{Z}$. Therefore, the converse is only true for odd n. ■

2. **Proposition.** *Let $n \in \mathbb{Z}$, then*

   $$n^2 \equiv 0 \pmod 4 \text{ or } n^2 \equiv 1 \pmod 4$$

   Proof. Suppose n is an integer. By the division algorithm, n can be expressed as

   $$n = 2q + r$$

   where $q, r \in \mathbb{Z}$ and $0 \le r < 2$, or $r \in \{0, 1\}$. If we square n, then

   $$n^2 = \begin{cases} 4q^2 & r = 0 \\ 4(q^2 + q) + 1 & r = 1 \end{cases}$$

   Since $q^2, (q^2 + q) \in \mathbb{Z}$, n^2 will either have a remainder of 0 or 1 when divided by 4. Therefore, it holds true that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

   ■

3. **Proposition.** *If $a, b \in \mathbb{Z}$ and $a^2 + b^2$ is a perfect square, then a and b are not both odd.*

   Proof. Here, we will show the contrapositive. Suppose $a, b \in \mathbb{Z}$ and both a and b are odd, then using the previous problem,

$$a^2 \equiv 1 \pmod 4$$
$$b^2 \equiv 1 \pmod 4$$

   Then, $\left(a^2 + b^2\right) \equiv 2 \pmod 4$. However, this sum cannot be a perfect square, as we have shown in Problem 2: any integer n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$. ■

4. **Proposition.** *Suppose the division algorithm applied to a and b yields $a = qb + r$, then*

$$\gcd(a, b) = \gcd(r, b)$$

   Proof. Suppose $a, b, q, r \in \mathbb{Z}$ and $a = qb + r$, where $0 \leq r < b$. Then let d be a divisor of a and b. Then it must hold true that d also divides r,

$$a = dx_1$$
$$b = dx_2$$
$$r = d(x_1 - x_2 q)$$

   where $x_i \in \mathbb{Z}$. Since the set of divisors are equal between a, b and r, b, then there is one greatest common divisor and $\gcd(a, b) = \gcd(r, b)$. ■