Worksheet 6 Solution

March 16, 2020

Question 1

a. $P(123) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow n \leq 123)$

b. $isCD(x, y, d)$: $\exists x, y, d \in \mathbb{Z},\ d \mid x \wedge d \mid y$

   $isGCD(x, y, d)$: $\exists x, y, d \in \mathbb{Z},\ (x = 0 \wedge y = 0 \wedge d = 0) \vee ((x \neq 0 \vee y \neq 0) \wedge isCD(x, y, d) \wedge \forall e \in \mathbb{Z},\ e > d \Rightarrow \neg isCD(x, y, e))$

c. Statement: $\forall x \in \mathbb{Z}^+, IsGCD(x, 0, x)$

   For the value x, because we know $x \mid x$, and $\forall n \in \mathbb{Z}^+$ and $\forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n$, x is the biggest divisor of x

   For the value 0, because we know anything that divides 0 is 0, and $\exists k \in \mathbb{Z},\ 0 = k \times 0$, k can be chosen to be x.

   Then, it follows from the definition of GCD that the statement $IsGCD(x, 0, x)$ is true.

d. $\forall a, b \in \mathbb{Z}, (a \neq 0 \vee b \neq 0) \Rightarrow \exists p, q \in \mathbb{Z},\ gcd(a, b) = ap + qb \wedge \forall m \in \mathbb{Z}, m < gcd(a, b) \wedge m \neq ap + qb$

Question 2

a. Let $n \in \mathbb{Z}$. Assume $\exists l \in \mathbb{Z},\ n = 2l$.

Then,

$$
\begin{align}
n^2 - 3n &= (2l)^2 = 3(2l) \tag{1}\\
&= 4l^2 - 6l \tag{2}\\
&= 2(2l^2 - 3l) \tag{3}
\end{align}
$$

Since $2l^2 - 3l \in \mathbb{Z}$, it follows from the definition of even number that $n^2 - 3n$ is even

b. Let $n \in \mathbb{Z}$. Assume $\exists l \in \mathbb{Z},\ n = 2l - 1$.

Then,

$$
\begin{align}
n^2 - 3n &= (2l - 1)^2 = 3(2l - 1) \tag{1}\\
&= 4l^2 - 4l + 1 - 6l - 3 \tag{2}\\
&= 4l^2 - 10l - 2 \tag{3}\\
&= 2(2l^2 - 5l - 1) \tag{4}
\end{align}
$$

Since $2l^2 - 5l - 1 \in \mathbb{Z}$, it follows from the definition of even number that $n^2 - 3n$ is even

Question 3

a. $\forall a, b \in \mathbb{N}, Prime(b) \Rightarrow 1 \geq gcd(a, b) \lor gcd(a, b) \geq b$

b. **Case 1 ($b \mid a$):**

Let $a, b \in \mathbb{N}$, and assume $Prime(b)$. Also assume $b \mid a$.

Since b is a prime number, other than 1, b is the only number that divides b.

Since $b \mid a$, $\exists k \in \mathbb{Z}, a = kb$.

Then, it follows that $gcd(a, b) = b$, and contraposition of the statement is true for the case $b \mid a$.

Case 2 ($b \nmid a$):

Let $a, b \in \mathbb{N}$, and assume $Prime(b)$. Also assume $b \nmid a$.

Since b is a prime number, other than 1, b is the only number that divides b.

Since $b \nmid a$, but $1 \mid a$, $gcd(a, b) = 1$.

Then, it follows from contraposition of the statement that it is true for the case $b \nmid a$.