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,

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

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,

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

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

b. **Case1 ($b \mid a$):**

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

Then,

$$\begin{aligned} gcd(a,b) &= pa + qb \qquad (1)\\ &= p(kb) + qb \qquad (2)\\ &= b(pk + q) \qquad (3) \end{aligned}$$

by the property in question 1.d.

Then,

$$\begin{aligned} gcd(a, b) &= p(kb) + qb && (4) \\ &= b(pk + q) && (5) \end{aligned}$$

by the fact that $b \mid a$, and by the definition of divisibility $\exists k \in \mathbb{Z},\ a = kb$.

Then,

$$\begin{aligned} gcd(a, b) &= b(pk + q) && (6) \\ &\geq b && (7) \end{aligned}$$

by the fact that b is prime, and b is the smallest common divisor to both a and b.

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