Worksheet 7 Solution

March 17, 2020

Question 1

a. **Case 1 ($n \geq 1$):**

No more proof required. This is exactly what we want to show.

Case 2 ($\exists d \in \mathbb{N}, d \mid n \wedge d \neq 1 \wedge d \neq n$):

Let $a = d$ and $b = k$.

Because we know $\forall n \in \mathbb{Z}^+$, and $l \in \mathbb{Z}, l \mid n \Rightarrow l \leq n$, $a \leq n$.

Then $n \mid a$ is true only when $a = n$ and $b = 1$, by the fact that any lower value of a results in non-integer value.

Then it follows from the assumption $a \neq 1 \wedge a \neq n$ that $n \nmid a$.

The same logic holds for $n \nmid b$.

Lastly, since $n = ab$, and $\forall x \in \mathbb{Z},\ x \mid x$, $n \mid ab$.

Question 2

a. Let $n, m \in \mathbb{N}$. Assume $Prime(n)$, and $n \nmid m$.

Then,

$$gcd(n, m) = 1 \tag{1}$$

by fact 2 (i.e. $\forall n, p \in \mathbb{Z}, Prime(p) \wedge p \nmid n \Rightarrow gcd(p, n) = 1$).

Then $\exists r, s \in \mathbb{Z}$,

$$1 = gcd(n, m) = rn + sm \tag{2}$$

by fact 6 (i.e. $\forall n, m \in \mathbb{N}, \exists r, s \in \mathbb{Z}, rn + sm = gcd(n, m)$).

Then, it follows from above that the statement $\forall n, m \in \mathbb{N}$, $Prime(n) \wedge n \nmid m \Rightarrow (\exists r, s \in \mathbb{Z}, rn + sm = 1)$ is true.

b. Let $n, m \in \mathbb{N}$. Assume $Prime(n)$ and $(\exists r, s \in \mathbb{Z}, rn + sm = 1)$.

Then,

$$gcd(n, m) = 1 \tag{3}$$

by fact 6 (i.e. $\forall n, m \in \mathbb{N}$, $\exists r, s \in \mathbb{Z}$, $rn + sm = gcd(n, m)$).

Then, 1 is the maximum number that divides both n and m, by the definition of GCD.

It follows from the above that $n \mid m$ only when $n = 1$.

Since n is prime and $n > 1$, the above is not possible, and $n \nmid m$.

Question 3

a. Let $x \in \mathbb{Z}$.

Then,

$$x = x \tag{1}$$
$$x = (1)x \tag{2}$$

Then, it follows from the definition of divisibility that x divides x.

b. Let $x, y \in \mathbb{N}$. Assume $y \geq 1$ and $x \mid y$.

Then $\exists k \in \mathbb{Z}$,

$$y = kx \tag{1}$$

Then, because we know $y \geq 1$, and $x \geq 1$, we can conclude that $k \geq 1$.

Then it follows from the above that

$$1 \leq x \leq kx = y \tag{2}$$

c. Let $n, p \in \mathbb{Z}$. Assume $Prime(p)$ and $p \nmid n$.

Because we know from the definition of prime number, the common divisors available for p are 1 and p.

Also, because we know $\forall n \in \mathbb{Z}, n \mid n$, we can conclude that $1 \mid n$.

Since $p \nmid n$, but $1 \mid p$ and $1 \mid n$, $gcd(p, n) = 1$

d. Let $n, m \in \mathbb{N}$.

Case 1 ($n \neq 0, m = 0$):

Assume $n \neq 0$ and $m = 0$.

Since $n \mid n$ (by fact 1) and $n \mid m$, n is a common divisor, and

$$gcd(n, m) = n \tag{1}$$

by the definition of greatest common divisor.

Since, $n \in \mathbb{N}$ and $n \mid gcd(n, m)$ (by fact 1),

$$1 \leq gcd(n, m) \leq n \tag{2}$$

by fact 2.

Case 2 ($n = 0, m \neq 0$):

The inequality $gcd(n, m) \geq 1$ holds using the same logic as case 1.

Case 3 ($n \neq 0, m \neq 0$):

Let $n, m \in \mathbb{N}$. Assume $n \neq 0$ and $m \neq 0$.

Since 1 is the smallest divisor that exists in both n and m,

$$gcd(n, m) \geq 1 \tag{1}$$

e. Let $n, m \in \mathbb{N}$, and $d, r, s \in \mathbb{Z}$, and assume $d = gcd(n, m)$.

Then, $gcd(n, m)$ divides both n and m, by the definition of greatest common divisor.

Then, it follows from above that $gcd(n, m)$ divides $rn + sm$.