Worksheet 7 Solution

March 27, 2020

Question 1

1. Assume that $n \leq 1$.

   Then, it follows from the assumption that the statement holds for the case $n \leq 1$.

   > **Correct Solution:**
   >
   > Assume that $n \leq 1$.
   >
   > Then, the assumption satisfies the first part of the OR we want to prove.

   Notes:

   - the professor specifically states the assumption satisfies the first part of the OR we want to prove.

2. Assume $\exists k, d \in \mathbb{N},\ n = kd \wedge d \neq 1 \wedge d \neq n$.

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

   We will divide proof into parts and combine them together.

   Part 1 ($n \nmid a$):

Since $\frac{1}{k} \cdot n = d$, k must be 1 for n to divide d.

Then, because we know $d \neq n$, we can conclude that $n \nmid a$.

Part 2 ($n \nmid b$):

Since $\frac{1}{d} \cdot n = k$, d must be 1 for n to divide k.

Then, because we know $d \neq 1$, we can conclude $n \nmid b$.

Part 3 ($n \mid ab$):

Since $ab = n$ and $\forall n \in \mathbb{N}$, $n \mid n$, we can conclude that $n \mid ab$.

Then, it follows from the result of part 1, part 2 and part 3 that the second part of the OR is true.

<u>**Correct Solution:**</u>

Assume $\exists d \in \mathbb{N}$, $k \in \mathbb{Z}$, $n = dk \wedge d \neq 1 \wedge d \neq n$, and n ¿ 1.

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

We will prove this statement by dividing into cases and combining them together.

Case 1 ($n \mid ab$):

Because we know $n = ab$ and $n \mid n$ by fact 1 , we can conclude $n \mid ab$.

Case 2 ($n \nmid a$):

Because we know $d \geq 1$ from $d \in \mathbb{N}$ and $n > 1$ in assumption, we can conclude $k \geq 1$.

Then,

$$n = dk \tag{1}$$
$$n > d \tag{2}$$

where $' >'$ sign is due to the assumption $d \neq n$.

Then,

$$d < 1 \lor n \nmid d \tag{3}$$

by contrapositive of fact 2.

Since the first part of OR is not true, we can conclude $n \nmid a$.

Case 3 ($n \nmid b$):

Because we know $n = dk$, $d \geq 1$ from $d \in \mathbb{N}$ and $n > 1$ in assumption, we can conclude $k \geq 1$.

Then because we know $d \neq n \land d \neq 1$ and $n = dk$, we can conclude $k \neq n \land k \neq 1$.

Then,

$$n = dk \tag{4}$$
$$n > k \tag{5}$$

where $' >'$ sign is due to the fact $k \neq n \land k \neq 1$.

Then,

$$b < 1 \lor n \nmid y \tag{6}$$

by contrapositive of fact 2.

Since the first part of OR is not true, and we can conclude $n \nmid b$.

Notes:

- **Definition of Divisibility:** Let $a, d \in \mathbb{Z}$. There exists $k \in \mathbb{Z}$, $n = dk$
- **Contrapositive of Fact 2:** $\forall x, y \in \mathbb{N}$, $1 > x \lor x > y \Rightarrow y < 1 \lor x \nmid y$
- **Definition of Prime Number:** $Prime(p) : p > 1 \land (\forall d \in \mathbb{N},\ d \mid p \Rightarrow d = 1 \lor d = p)$, where $p \in \mathbb{N}$
- How can i create bridges or the connecting dots for proof? Should I examine from the start and the end thinking would this lead to conclusion?

Question 2

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

Then,

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

because $\mathbb{N}$ is a part of $\mathbb{Z}$, and $\forall n, p \in \mathbb{Z}$, $Prime(p) \land p \nmid n \Rightarrow gcd(p, n) = 1$ from fact 3.

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

$$\begin{aligned} rn + sm &= gcd(n, m) && (2) \\ &= 1 && (3) \end{aligned}$$

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

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.

Notes:

- Have I written the last line correctly?
- Can the line line '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.' be omitted?
- What is a good practice of writing conclusion to a proof?

b. Let $n, m \in \mathbb{N}$. Assume $Prime(n)$ (i.e. $n > 1 \wedge (\forall d \in \mathbb{N},\ d \mid n \Rightarrow d = 1 \vee d = n)$) and $\exists r, s \in \mathbb{Z},\ rn + sm = 1$.

Then,

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

by fact 5.

Then, since $(rn + sm) = 1$,

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

Because 1 is the highest possible common divisor to both n and m, and we know $n > 1$ from the definition of prime number, we can conclude $n \nmid m$.

Question 3