

# Worksheet 7 Review 2

Hyungmo Gu

April 17, 2020

## Question 1

- a. In this case assume that  $n \leq 1$ .

We want to show  $n \leq 1$ .

Since the assumption tells us  $n \leq 1$ , we can conclude this is true.

- b. *Proof.* Let  $a = d$  and  $b = k$ . Assume there exists  $d \in \mathbb{N}$  where  $(\exists k \in \mathbb{Z}, n = dk) \wedge d \neq 1 \wedge d \neq n$ . Assume  $n > 1$

We need to prove that  $n \nmid a$ ,  $n \nmid b$  and  $n \mid ab$ .

We will do so in parts.

### Part 1 (Proving $n \nmid a$ ):

We need to prove  $n \nmid a$ .

First, we need to show  $n \geq d$ .

The fact 2 tells us

$$\forall x, y \in \mathbb{N}, y \geq 1 \wedge x \mid y \Rightarrow 1 \leq x \leq y \quad (1)$$

and we know from headers that  $d \mid n$ ,  $n > 1$ , and  $n, d \in \mathbb{N}$ .

Then, by using these facts, we can write

$$1 \leq d \leq n \quad (2)$$

Second, we need to show  $n = d$ .

The definition of divisibility tells us for  $n$  to divide  $d$ , there must be some  $k_1 \in \mathbb{Z}$  such that  $d$  is equal to  $k_1 \cdot n$ .

Then, since we know  $n \geq d$ , by using these facts, we can conclude the definition of divisibility is satisfied only when  $k_1 = 1$ , or when  $n = d$ .

Finally, since we know from the header that  $n \neq d$ , we can conclude  $n \nmid d$ .

Then, since we know  $d = a$  from the header, we can conclude  $n \nmid a$ .

### **Part 2 (Proving $n \nmid b$ ):**

We need to prove  $n \nmid b$ .

First, we need to show  $k \mid n$ .

The assumption tells us  $n = kd$ .

Then, it follows from the definition of divisibility that  $k \mid d$ .

Second, we need to show  $k \geq 1$ .

The header tells us  $n > 1$   $d \geq 0$ , and we know from assumption that  $n = dk$ .

Since the facts tell us  $k \leq 0$  results in  $n \leq 0$  and this cannot happen, we can conclude  $k \geq 1$ .

Third, we need to show  $n \geq k$  using the fact  $k \geq 1$  and  $k \mid n$ .

The fact 2 tells us

$$\forall x, y \in \mathbb{N}, y \geq 1 \wedge x \mid y \Rightarrow 1 \leq x \leq y \quad (3)$$

Since we know  $k \mid n$ ,  $n > 1$  and  $k, n \in \mathbb{N}$ , we can conclude  $k \leq n$ .

Fourth, we need to show  $n = k$ .

The definition of divisibility tells us for  $n$  to divide  $k$ , there must be some  $k_1 \in \mathbb{Z}$  such that  $k$  is equal to  $k_1 \cdot n$ .

Then, using the fact  $n \geq k$ , we can conclude the definition of divisibility is satisfied only when  $k_1 = 1$ , or  $n = k$ .

Finally, since we know from the header that  $n \neq k$ , we can conclude  $n \nmid k$ .

Then, it follows from the fact  $k = b$ , we can conclude  $n \nmid b$ .

### **Part 3 (Proving $n \mid ab$ ):**

We need to prove  $n \mid ab$ .

The fact 1 tells us

$$\forall x \in \mathbb{Z}, x \mid x \tag{4}$$

Since we know  $n \in \mathbb{N}$ , we can conclude  $n \mid n$ .

Then, since we know  $n = dk$ ,  $d = a$  and  $k = b$ , we can conclude  $n \mid ab$ .

□

### **Pseudoproof:**

Let  $a = d$  and  $b = k$ . Assume there exists  $d \in \mathbb{N}$  where  $(\exists k \in \mathbb{Z}, n = dk) \wedge d \neq 1 \wedge d \neq n$ .  
Assume  $n > 1$

We need to prove that  $n \nmid a$ ,  $n \nmid b$  and  $n \mid ab$ .

We will do so in parts.

1. Show  $n \nmid a$ .

First, we need to show  $n \nmid a$ .

1. Show  $n \geq d$ .

The fact 2 tells us

$$\forall x, y \in \mathbb{N}, y \geq 1 \wedge x \mid y \Rightarrow 1 \leq x \leq y \quad (5)$$

and we know from headers that  $d \mid n$ ,  $n > 1$ , and  $n, d \in \mathbb{N}$ .

Then, by using these facts, we can write

$$1 \leq d \leq n \quad (6)$$

2. Show that for  $n$  to divide  $d$ ,  $n = d$ .

Now, the definition of divisibility tells us for  $n$  to divide  $d$ , there must be some  $k_1 \in \mathbb{Z}$  such that  $d$  is equal to  $k_1 \cdot n$ .

Then, since we know  $n \geq d$ , by using these facts, we can conclude the definition of divisibility is satisfied when  $k_1 = 1$ , or when  $n = d$ .

3. Conclude  $n \nmid a$ .

Then, since we know from header that  $n \neq d$ , we can conclude  $n \nmid d$ .

**Part 1 (Proving  $n \nmid a$ ):**

We need to prove  $n \nmid a$ .

First, we need to show  $n \geq d$ .

The fact 2 tells us

$$\forall x, y \in \mathbb{N}, y \geq 1 \wedge x \mid y \Rightarrow 1 \leq x \leq y \quad (7)$$

and we know from headers that  $d \mid n$ ,  $n > 1$ , and  $n, d \in \mathbb{N}$ .

Then, by using these facts, we can write

$$1 \leq d \leq n \quad (8)$$

Second, we need to show  $n = d$ .

The definition of divisibility tells us for  $n$  to divide  $d$ , there must be some  $k_1 \in \mathbb{Z}$  such that  $d$  is equal to  $k_1 \cdot n$ .

Then, since we know  $n \geq d$ , by using these facts, we can conclude the definition of divisibility is satisfied only when  $k_1 = 1$ , or when  $n = d$ .

Finally, since we know from the header that  $n \neq d$ , we can conclude  $n \nmid d$ .

Then, since we know  $d = a$  from the header, we can conclude  $n \nmid a$ .

2. Show  $n \nmid b$

- Show  $k \mid n$

First, we need to show  $k \mid n$ .

- State  $n = kd$ .

The assumption tells us  $n = kd$ .

- Show  $k \mid n$  by using the definition of divisibility

Then, it follows from the definition of divisibility that  $k \mid d$ .

First, we need to show  $k \mid n$ .

The assumption tells us  $n = kd$ .

Then, it follows from the definition of divisibility that  $k \mid d$ .

- Show  $k \geq 1$ .

Second, we need to show  $k \geq 1$ .

Second, we need to show  $k \geq 1$ .

The header tells us  $n > 1$   $d \geq 0$ , and we know from assumption that  $n = dk$ .

Since the facts tell us  $k \leq 0$  results in  $n \leq 0$  and this cannot happen, we can conclude  $k \geq 1$ .

- Show  $n \geq k$  using the fact  $k \mid n$  and  $k \geq 1$ .

Third, we need to show  $n \geq k$ .

Third, we need to show  $n \geq k$ .

The fact 2 tells us

$$\forall x, y \in \mathbb{N}, y \geq 1 \wedge x \mid y \Rightarrow 1 \leq x \leq y \quad (9)$$

Since we know  $k \mid n$ ,  $n > 1$  and  $k, n \in \mathbb{N}$ , we can conclude  $k \leq n$ .

- Show that for  $n$  to divide  $k$ ,  $n = k$ .

Fourth, we need to show  $n = k$ .

Fourth, we need to show  $n = k$ .

The definition of divisibility tells us for  $n$  to divide  $k$ , there must be some  $k_1 \in \mathbb{Z}$  such that  $k$  is equal to  $k_1 \cdot n$ .

Then, using the fact  $n \geq k$ , we can conclude the definition of divisibility is satisfied only when  $k_1 = 1$ , or  $n = k$ .

- Conclude  $n \nmid a$ .

Finally, since we know from the header that  $n \neq k$ , we can conclude  $n \nmid k$ .

It follows from the fact  $k = b$ , we can conclude  $n \nmid b$ .

**Part 2 (Proving  $n \nmid b$ ):**

We need to show  $n \nmid b$ .

First, we need to show  $k \mid n$ .

The assumption tells us  $n = kd$ .

Then, it follows from the definition of divisibility that  $k \mid d$ .

Second, we need to show  $k \geq 1$ .

The header tells us  $n > 1$   $d \geq 0$ , and we know from assumption that  $n = dk$ .

Since the facts tell us  $k \leq 0$  results in  $n \leq 0$  and this cannot happen, we can conclude  $k \geq 1$ .

Third, we need to show  $n \geq k$  using the fact  $k \geq 1$  and  $k \mid n$ .

The fact 2 tells us

$$\forall x, y \in \mathbb{N}, y \geq 1 \wedge x \mid y \Rightarrow 1 \leq x \leq y \quad (10)$$

Since we know  $k \mid n$ ,  $n > 1$  and  $k, n \in \mathbb{N}$ , we can conclude  $k \leq n$ .

Fourth, we need to show  $n = k$ .

The definition of divisibility tells us for  $n$  to divide  $k$ , there must be some  $k_1 \in \mathbb{Z}$  such that  $k$  is equal to  $k_1 \cdot n$ .

Then, using the fact  $n \geq k$ , we can conclude the definition of divisibility is satisfied only when  $k_1 = 1$ , or  $n = k$ .

Finally, since we know from the header that  $n \neq k$ , we can conclude  $n \nmid k$ .

Then, it follows from the fact  $k = b$ , we can conclude  $n \nmid b$ .

3. Show  $n \mid ab$

We need to show  $n \mid ab$ .

- State fact 1



The fact 1 tells us

$$\forall x \in \mathbb{Z}, x \mid x \quad (11)$$

- Show  $n \mid n$

Since we know  $n \in \mathbb{N}$ , we can conclude  $n \mid n$ .

- Show  $n \mid ab$  using the fact  $n = dk$  where  $a = d$  and  $b = k$ .

Then, since we know  $n = dk$ ,  $d = a$  and  $k = b$ , we can conclude  $n \mid ab$ .

### Part 3 (Proving $n \mid ab$ ):

We need to show  $n \mid ab$ .

The fact 1 tells us

$$\forall x \in \mathbb{Z}, x \mid x \quad (12)$$

Since we know  $n \in \mathbb{N}$ , we can conclude  $n \mid n$ .

Then, since we know  $n = dk$ ,  $d = a$  and  $k = b$ , we can conclude  $n \mid ab$ .

### Notes:

- Made some serious errors (i.e. show  $n = a$  or  $n = b$ ) :(.
- How can a proof be organized so it's structurally clear so moe 3 months from now can say I understand this proof? I used first, second and third to show steps involved but I still feel something is missing...
- Can I write a predicate logic for proving  $n \nmid b$  or  $n \nmid a$ ? (i.e.  $\dots \Rightarrow n \nmid b$ )?

## Question 2

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

We need to prove there are some integer numbers  $r$  and  $s$  such that  $rn + sm = 1$ .

First, we need to show  $\gcd(n, m) = 1$ .

The fact 3 tells us

$$\forall n, m \in \mathbb{Z}, \text{Prime}(n) \wedge n \nmid m \Rightarrow \gcd(n, m) = 1 \quad (1)$$

Because we know from assumption that  $n$  is prime and  $n \nmid m$ , we can write  $\gcd(n, m) = 1$ .

Finally, the fact 6 tells us

$$\forall n, m \in \mathbb{N}, \exists r, s \in \mathbb{Z}, rn + sm = \gcd(n, m) \quad (2)$$

Since  $\gcd(n, m) = 1$ , we can conclude

$$\gcd(n, m) = rn + sm = 1 \quad (3)$$

□

### Pseudoproof:

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

We need to prove  $\exists r, s \in \mathbb{Z}, rn + sm = 1$ .

1. Show  $\gcd(n, m) = 1$ , using fact 3

First, we need to show  $\gcd(n, m) = 1$ .

First, we need to show  $\gcd(n, m) = 1$ .

The fact 3 tells us

$$\forall n, m \in \mathbb{Z}, \text{Prime}(n) \wedge n \nmid m \Rightarrow \gcd(n, m) = 1 \quad (4)$$

Because we know from assumption that  $n$  is prime and  $n \nmid m$ , we can write  $\gcd(n, m) = 1$ .

2. Show  $rn + sm = \gcd(n, m) = 1$  using fact 6

Finally, the fact 6 tells us

$$\forall n, m \in \mathbb{N}, \exists r, s \in \mathbb{Z}, rn + sm = \gcd(n, m) \quad (5)$$

Since  $\gcd(n, m) = 1$ , we can conclude

$$\gcd(n, m) = rn + sm = 1 \quad (6)$$

### Notes:

- Noticed that professor doesn't put  $\exists$  symbols in 'we need to prove that...'.

Let  $n, m \in \mathbb{N}$ . Assume that  $n$  is prime and that  $n - m$ . We want to prove there exist  $r, s \in \mathbb{Z}$ ,  $rn + sm = 1$ .

- 형모야. 오늘도 사랑하는 내 여보 향해 화이팅 :)
- 오늘 켈거리에 구름이 많은데 날씨가 굉장히 밝구나.
- 오오오오오!!!!

- b. Contrapositive of Statement:  $\forall n, m \in \mathbb{N}, n \mid m \Rightarrow \neg \text{Prime}(n) \vee (\forall r, s \in \mathbb{Z}, rn + sm \neq 1)$

### Pseudoproof:

Let  $n, m \in \mathbb{N}$ . Assume  $n \mid m$  and assume there exists  $r, s \in \mathbb{Z}$ ,  $rn + sm = 1$ .

We need to show  $n$  is not prime. That is, there exists  $a, b \in \mathbb{N}$ ,  $n \mid a \wedge n \mid b \wedge n \mid ab$ .

## Question 3