

Worksheet 6 Review 2

Hyungmo Gu

April 13, 2020

Question 1

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

Correct Solution:

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

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

$$IsGCD(x, y, d) : \forall n \in \mathbb{N}, IsCD(x, y, n) \Rightarrow \exists d \in \mathbb{N}, IsCD(x, y, d) \wedge n \leq d$$

Correct Solution:

$$IsCD(x, y, d) : d \mid x \wedge d \mid y, \text{ where } x, y, d \in \mathbb{Z}$$

$$IsGCD(x, y, d) : (x = 0 \wedge y = 0 \Rightarrow d = 0) \wedge (x \neq 0 \wedge y \neq 0 \Rightarrow IsCD(x, y, d) \wedge (\forall d_1 \in \mathbb{Z}, IsCD(x, y, d_1) \Rightarrow d_1 \leq d)), \text{ where } x, y, d \in \mathbb{Z}$$

Notes:

- Realized the definition of $IsGCD$ extends from previous question
- Noticed professor defines if...else conditions in a predicate logic the following way

$$(\text{case 1} \Rightarrow \text{statement 1}) \wedge (\text{case 2} \Rightarrow \text{statement 2})$$

- Hm... I feel puzzled about \wedge operator used in between cases (i.e. $(x = 0 \wedge y = 0 \Rightarrow d = 0) \wedge (x \neq 0 \wedge y \neq 0 \Rightarrow IsCD(x, y, d) \wedge (\forall d_1 \in \mathbb{Z}, IsCD(x, y, d_1) \Rightarrow d_1 \leq d))$). At glimpse, I felt \vee is more appropriate since if this case is not true, then we want other case should be true.

c. **Statement:** $IsCD(x, 0, x) \wedge (\forall d_1 \in \mathbb{Z}, IsCD(x, 0, d_1) \Rightarrow d_1 \leq x)$

Proof. Let $x \in \mathbb{Z}^+$

We need to prove x is a common divisor to both 0 and x , and we need to prove all common divisors d_1 of 0 and x is less than or equal to x .

First, we need to show there is $k_1 \in \mathbb{Z}$ such that $x = k_1 \cdot x$ and we need to show $k_2 \in \mathbb{Z}$ such that $0 = k_2 \cdot x$.

Let $k_1 = 1$ and $k_2 = 0$.

Then, we can calculate that

$$x = 1 \cdot x = k_1 \cdot x \quad (1)$$

$$0 = 0 \cdot x = k_2 \cdot x \quad (2)$$

Now, we need to show all integers d_1 that is a common divisor to both 0 and x is less than equal to x .

Let $d_1 \in \mathbb{Z}$ and assume $d_1 \mid x$ and $d_1 \mid 0$.

We need to show $d_1 \leq x$.

The hint tells us

$$\forall n \in \mathbb{Z}^+, \forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n \quad (3)$$

Because we know from assumption that $d_1 \mid x$, by using the hint, we can conclude

$$d_1 \leq x \quad (4)$$

□

Pseudoproof:

Let $x \in \mathbb{Z}^+$

We need to prove x is a common divisor to both 0 and x , and we need to prove all common divisors d_1 of 0 and x is less than or equal to x .

1. Show $IsCD(x, 0, x)$

We need to show there is $k_1 \in \mathbb{Z}$ such that $x = k_1 \cdot x$ and we need to show $k_2 \in \mathbb{Z}$ such that $0 = k_2 \cdot x$.

Let $k_1 = 1$ and $k_2 = 0$.

- Show $x = k_1 \cdot x$ and $0 = k_2 \cdot 0$

Then, we can calculate that

$$x = 1 \cdot x = k_1 \cdot x \quad (5)$$

$$0 = 0 \cdot x = k_2 \cdot x \quad (6)$$

2. Show $\forall d_1 \in \mathbb{Z}, IsCD(x, 0, d_1) \Rightarrow d_1 \leq x$

Let $d_1 \in \mathbb{Z}$ and assume $d_1 \mid x$ and $d_1 \mid 0$.

We need to show $d_1 \leq x$.

1. Use fact ' $\forall n \in \mathbb{Z}^+, \forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n$ ' to show $d_1 \leq x$.

The hint tells us

$$\forall n \in \mathbb{Z}^+, \forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n \quad (7)$$

Because we know from assumption that $d_1 \mid x$, by using the hint, we can conclude

$$d_1 \leq x \quad (8)$$

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

Question 2

a. *Proof.* Assume $Even(n)$. That is $\exists k \in \mathbb{Z}, n = 2k$.

We need to show there is an integer k_1 such that $n^2 - 3n = 2k_1$.

Let $k_1 = (2k^2 - 3k)$.

The assumption tells us $n = 2k$.

Then, by using this fact, we can write

$$n^2 - 3n = (2k)^2 - 3(2k) \tag{1}$$

$$= 4k^2 - 6k \tag{2}$$

$$= 2(2k^2 - 3k) \tag{3}$$

$$= 2k_1 \tag{4}$$

□

Pseudoproof:

Assume $Even(n)$. That is $\exists k \in \mathbb{Z}, n = 2k$.

We need to show there is an integer k_1 such that $n^2 - 3n = 2k_1$.

Let $k_1 = (2k^2 - 3k)$.

- Show $n^2 - 3n = 2k_1$ by using assumption.

The assumption tells us $n = 2k$.

Then, by using this fact, we can write

$$n^2 - 3n = (2k)^2 - 3(2k) \tag{5}$$

$$= 4k^2 - 6k \tag{6}$$

$$= 2(2k^2 - 3k) \tag{7}$$

$$= 2k_1 \tag{8}$$

- b. *Proof.* In this case, assume $Odd(n)$. That is $\exists k \in \mathbb{Z}, n = 2k - 1$.

We need to show there is an integer k_1 such that $n^2 - 3n = 2k_1$.

Let $k_1 = (2k^2 - 5k + 2)$.

The assumption tells us $n = 2k - 1$.

Then, by using this fact, we can write

$$n^2 - 3n = (2k - 1)^2 - 3(2k - 1) \quad (1)$$

$$= 4k^2 - 4k + 1 - 6k + 3 \quad (2)$$

$$= 4k^2 - 10k + 4 \quad (3)$$

$$= 2(2k^2 - 5k + 2) \quad (4)$$

$$= 2k_1 \quad (5)$$

□

Pseudoproof:

Assume $Odd(n)$. That is $\exists k \in \mathbb{Z}, n = 2k - 1$.

We need to show there is an integer k_1 such that $n^2 - 3n = 2k_1$.

Let $k_1 = (2k^2 - 5k + 2)$.

- Show $n^2 - 3n = 2k_1$ by using assumption.

The assumption tells us $n = 2k - 1$.

Then, by using this fact, we can write

$$n^2 - 3n = (2k - 1)^2 - 3(2k - 1) \quad (6)$$

$$= 4k^2 - 4k + 1 - 6k + 3 \quad (7)$$

$$= 4k^2 - 10k + 4 \quad (8)$$

$$= 2(2k^2 - 5k + 2) \quad (9)$$

$$= 2k_1 \quad (10)$$

Notes:

- Noticed professor uses predicate logic when expanding definition in assumption.

Assume that n is odd, i.e. $\exists k \in \mathbb{Z}, n = 2k - 1$.

Question 3

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

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

Proof. Let $a, b \in \mathbb{N}$. Assume $\text{Prime}(b)$. That is, $p > 1 \wedge (\forall d \in \mathbb{N}, d \mid p \Rightarrow d = 1 \vee d = p)$.

We will prove $1 \geq \gcd(a, b)$ or $\gcd(a, b) \geq b$ using proof by cases.

Case 1 ($b \mid a$):

In this case, assume b divides a . That is, $\exists k \in \mathbb{Z}, a = kb$.

We need to prove $b \geq \gcd(a, b)$.

First, we need to show b is the greatest common divisor to both a and b . That is, $\text{IsCD}(a, b, b) \wedge (\forall d_1 \in \mathbb{Z}, \text{IsCD}(a, b, d_1) \Rightarrow d_1 \leq b)$

Starting with showing $\text{IsCD}(a, b, b)$, the assumption tells us $b \mid a$, and we know $b \mid b$.

Then, it follows from these facts that b is a common divisor to both a and b .

Next for showing $(\forall d_1 \in \mathbb{Z}, \text{IsCD}(a, b, d_1) \Rightarrow d_1 \leq b)$, the definition of prime number tells us b has two non-negative divisors 1 and b .

Because we know $1 \mid a$ and $b \mid a$, we can conclude 1 and b are the only non-negative common divisor to both a and b .

Since $1 < b$, $b = b$ and all other common divisors are less than 0, we can conclude all common divisors to both a and b are less than or equal to b .

Now, we need to show $b \leq \gcd(a, b)$.

The hint from question 1.c tells us

$$\forall n \in \mathbb{Z}^+, \forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n \quad (1)$$

Since we know b divides b , by using this fact, we can write

$$b \leq b \quad (2)$$

Because we know $b = \gcd(a, b)$, we can conclude

$$b \leq \gcd(a, b) \tag{3}$$

Case 2 ($b \nmid a$):

In this case, assume b doesn't divide a .

We need to prove $1 \geq \gcd(a, b)$.

First, we need to show 1 is the greatest common divisor to both a and b .

The assumption tells us b is a prime number, and so, from definition, we know b has two non-negative divisors 1 and b .

Because we know $b \nmid a$ from assumption and $1 \mid a$, we can conclude 1 is the only non-negative common divisor to both a and b .

Because we know all common divisors to both a and b are less than or equal to 1, we can conclude $\gcd(a, b) = 1$.

Now, we need to show $1 \geq \gcd(a, b)$.

The hint from question 1.c tells us

$$\forall n \in \mathbb{Z}^+, \forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n \tag{4}$$

Since we know 1 divides 1, by using this fact, we can write

$$1 \geq 1 \tag{5}$$

Because we know $1 = \gcd(a, b)$, we can conclude

$$1 \geq \gcd(a, b) \tag{6}$$

□

Pseudoproof:

Let $a, b \in \mathbb{N}$. Assume $Prime(b)$. That is, $p > 1 \wedge (\forall d \in \mathbb{N}, d \mid p \Rightarrow d = 1 \vee d = p)$.

We will prove $1 \geq gcd(a, b)$ or $gcd(a, b) \geq b$ using proof by cases.

Case 1 ($b \mid a$):

In this case, assume b divides a . That is, $\exists k \in \mathbb{Z}, a = kb$.

We need to prove $gcd(a, b) \geq b$.

1. Show $IsGCD(a, b, b)$, i.e. $IsCD(a, b, b) \wedge (\forall d_1 \in \mathbb{Z}, IsCD(a, b, d_1) \Rightarrow d_1 \leq b)$

First, we need to show b is the greatest common divisor to both a and b . That is, $IsCD(a, b, b) \wedge (\forall d_1 \in \mathbb{Z}, IsCD(a, b, d_1) \Rightarrow d_1 \leq b)$

- Show $IsCD(a, b, b)$

Starting with showing $IsCD(a, b, b)$, the assumption tells us $b \mid a$, and we know $b \mid b$.

Then, it follows from these facts that b is a common divisor to both a and b .

- Show $\forall d_1 \in \mathbb{Z}, IsCD(a, b, d_1) \Rightarrow d_1 \leq b$

Next for showing $(\forall d_1 \in \mathbb{Z}, IsCD(a, b, d_1) \Rightarrow d_1 \leq b)$, the definition of prime number tells us b has two non-negative divisors 1 and b .

Because we know $1 \mid a$ and $b \mid a$, we can conclude 1 and b are the only non-negative common divisor to both a and b .

Since $1 < b$, $b = b$ and all other common divisors are less than 0, we can conclude all common divisors to both a and b are less than or equal to b .

2. Show $b \leq gcd(a, b)$ by using the fact $b \mid b$ and $\forall n \in \mathbb{Z}^+, \forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n$.

Now, we need to show $b \leq \gcd(a, b)$.

The hint from question 1.c tells us

$$\forall n \in \mathbb{Z}^+, \forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n \quad (7)$$

Since we know b divides b , by using this fact, we can write

$$b \leq b \quad (8)$$

Because we know $b = \gcd(a, b)$, we can conclude

$$b \leq \gcd(a, b) \quad (9)$$

Case 2 ($b \nmid a$):

In this case, assume b doesn't divide a .

We need to prove $1 \geq \gcd(a, b)$.

1. Show $IsGCD(a, b, 1)$

First, we need to show 1 is the greatest common divisor to both a and b .

- Find all possible common divisors to both a and b .

The assumption tells us b is a prime number, and so, from definition, we know b has two non-negative divisors 1 and b .

- Show 1 is the only common divisor to a and b .

Because we know $b \nmid a$ from assumption and $1 \mid a$, we can conclude 1 is the only non-negative common divisor to both a and b .

- Conclude $\gcd(a, b) = 1$.

Because we know all common divisors to both a and b are less than or equal to 1, we can conclude $\gcd(a, b) = 1$.

2. Show $\gcd(a, b) \leq 1$ by using the fact $\forall n \in \mathbb{Z}^+, \forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n$.

Now, we need to show $1 \geq \gcd(a, b)$.

The hint from question 1.c tells us

$$\forall n \in \mathbb{Z}^+, \forall d \in \mathbb{Z}, d \mid n \Rightarrow d \leq n \quad (10)$$

Since we know 1 divides 1, by using this fact, we can write

$$1 \geq 1 \quad (11)$$

Because we know $1 = \gcd(a, b)$, we can conclude

$$1 \geq \gcd(a, b) \quad (12)$$

Notes:

- $\text{Prime}(p) : p > 1 \wedge (\forall d \in \mathbb{N}, d \mid p \Rightarrow d = 1 \vee d = p)$
- I struggled so much with this problem (4+ hours).
- I struggled when trying to make the logic to flow in nested ‘shows’ in a ‘show’ (see case 1). Some of the thoughts I had are ‘should I use or here? Next? Finally? So?’ what phrases do I need to use when proving statements with \wedge operators? Should I use sub-headers like ‘part 1’ or ‘part 2’? But I am already using ‘case 1’ and ‘case 2’ up here.
- I re-read and re-read the paragraphs.
- The whole process feels like trying to write an essay with disconnected thoughts like when I was in ESL. I am trying to make it flow, but I don’t know how to make them connect and flow.
- What strategies are available to improve the flow of logics in nested shows?
- I tried to bundle up phrases and logics, because I felt like I was losing control.