Intro to Proofs: HW04

Aamod Varma

September 15, 2024

7.4

Proof. Forward case
We show if $a^2 + 4a + 5$ is odd then a is even.
Assume the contrary that a is odd. Then we can write a as

$$a = 2n + 1 \text{ for any } n \in Z.$$

Then we can write, $a^2 + 4a = 5 = 4n^2 + 4n + 1 + 8n + 4 + 1 = 4n^2 + 12n + 6$

$$= 2(2n^2 + 12n + 6) = 2m \text{ where } m = 2n^2 + 12n + 6.$$

So we got $a^2 + 4a + 5 = 2m$ which shows that it is even. By contrapositive
proof we can say that a is even.
Reverse case
We show if a is even then $a^2 + 4a + 5$ is odd.
If a is even we can write $a = 2n$ for some $n \in Z$
So $a^2 + 4a = 5 = 4n^2 + 8a + 5 = 2(2n^2 + 4a + 2) + 1 = 2m + 1$
Where $m = 2n^2 + 4a + 2$
So $a^2 + 4a + 5 = 2m + 1$ which means it is odd.

$\square$

7.10

Proof. Let's assume the contrary that, $a^3 \not\equiv a \bmod 3$
This means that $a^3 - a$ is not divisible by 3.
But
$$a^3 - a = a(a+1)(a-1).$$

Or in other words it is the product of three consequtive integers.
So
$$a(a+1)(a-1) \neq 3k.$$

However we know that the product of any three consecutive intgers should
be divisible by three. So our assumption contradicts this fact. Hence by
proof by contradiction it has to be true that $a^3 \equiv a \bmod 3$ $\square$

7.16

Proof. We know that if ab is odd then both a and b must be odd.
So we can write $a = 2n + 1$ and $b = 2m + 1$ for any $m, n \in Z$
So,

$$a^2 + b^2 = (2n+1)^2 + (2m+1)^2 = 4(m^2 + n^2) + 4(m+n) + 2 = 2(2m^2 + 2n^2 + 2m + 2n + 1) = 2k.$$

Which means that $a^2 + b^2$ can be written as a multiple of 2 which implies
that it is even.

$\square$

7.17

Proof. We have to identify a number between 90 and 100 that has no factors other than 1 and itself. we see that 97 is between 90 and 100 and has no other factors other that 1 and 97. Hence it is a prime number $\qquad\square$

7.33

Proof. Let the GCD be d which means that $d|2n+1$ and $d|4n^2+1$

We can write $4n^2 + 1 = (2n+1)(2n-1) + 2$

So,

$$d|(2n+1)(2n-1) + 2.$$

So, $k_1 d = (2n+1)(2n-1) + 2$

As $d|2n+1$ we can say, $k_0 d = 2n+1$

Putting this above we get

$$k_1 d = k_0 d(2n-1) + 2.$$

$$d(k_1 - k_0(2n-1)) = 2.$$

As $k_1 - k_0(2n-1)$ is an integer this means that $d|2$

So we have $d|2n+1$ and $d|2$.

And the only number that d could be is 1.

$\qquad\square$

7.35

Proof. Forward direction

Given $a = gcd(a,b)$ which means that a is the greater divisor of both a, b.

If a divides b then we know $a|b$

Reverse direction We know $a|b$ this means that a divides b. We also know that a divides a.

This means that a is a divisor for both a and b.

Now we need to show that a is the greatest common divisor.

Assume there exists another divisor $a_0 > a$ that divides b.

Now for $a_0|a$ we need $a = ka_0$ where k is an integer. However we knwo that $|a_0| > |a|$ so a_0 cannot divide a number a smaller (in terms of absolute value) than it.

Hence our assumptino is wrong that there exists a greater divisior $a_0 > a$ which means that a is the greater common divisor that divides both a and b.

$\qquad\square$

8.2

Forward direction

Let $x \in \{6n : n \in \mathbb{Z}\}$. This means that x is divisible by 6.

If x is divisible by 6 meaning $x = 6k$ for some $k \in \mathbb{Z}$. We can write $x = 2(3k) = 2n$ taking $3k = n$ which means that $x \in \{2n : n \in \mathbb{Z}\}$. At the same time we can write $x = 3(2k) = 3n$ taking $2k = n$ which means that $x \in \{3n : n \in \mathbb{Z}\}$.

As $x = 2n$ and $x = 3n$ we can write $x \in \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$ which implies that $\{6n : n \in \mathbb{Z}\} \subseteq \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$

Reverse direction

If $x \in \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$ then we know that $x \in \{2n : n \in \mathbb{Z}\}$ and $x \in \{3n : n \in \mathbb{Z}\}$

If $x \in \{2n : n \in \mathbb{Z}\}$ then we know that for some $n \in \mathbb{Z}$ we can write

$$x = 2n.$$

Now if $x \in \{3n : n \in \mathbb{Z}\}$ we know that 3 dividies x. Or in other words

$$3 | 2n.$$

For thsi to be the case we need $3|n$ which means we can write $n = 3k$ for $k \in \mathbb{Z}$

So $x = 2n = 6k \Rightarrow x \in \{6n : n \in \mathbb{Z}\}$

This shows that,

$$\{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\} \subseteq \{6n : n \in \mathbb{Z}\}.$$

So in conclusion we can say that

$$\{6n : n \in \mathbb{Z}\} = \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}.$$

8.12

Proof. First we show that

$$A - (B \cap C) \subseteq (A - B) \cup (A - C).$$

If $x \in A - (B \cap C)$ then we can say that, x is in A but not in B and C. So this means that x is in A but not in B or x is in A but not in C. We can write this as $x \in (A - B)$ or $x \in (A - C)$ which is

$$x \in (A - B) \cup (A - C).$$

which implies that $A - (B \cap C) \subseteq (A - B) \cup (A - C)$

Now we show that

$$(A - B) \cup (A - C) \subseteq A - (B \cap C)$$

If $x \in (A - B) \cup (A - C)$ then we know $x \in (A - B)$ or $x \in (A - C)$. We can write this as x is in A and not in B or x is in A and not in C. In both cases x is definitely not in $B \cap C$. So we can rewrite this as x is in A but not in $B \cap C$, or,

$$x \in A - (B \cap C).$$

Which gives us,

$$(A - B) \cup (A - C) \subseteq A - (B \cap C).$$

Now we can say that

$$(A - B) \cup (A - C) = A - (B \cap C).$$

$\square$

8.22

Proof. Consider $y \in \bigcap_{x \in R} [3 - x^2, 5 + x^2]$

So we need y such that $3 - x^2 \leq y \leq 5 + x^2$ for all $x \in R$. Now as $|x^2| \geq 0$ we can say that $3 - x^2 \leq 3$ and $5 \leq 5 + x^2$. Which is the case when x goes to 0.

So the lower bound of y is 3 as the maximum value of $3 - x^2$ is 3 when $x = 0$ and the upper bound of y is 5 as the min value of $5 + x^2$ is 5 when $x = 0$. So we can say for sure that

$$3 \leq y \leq 5 \text{ or } y \in [3, 5].$$

Now consider $y \in [3, 5]$. So we know $3 \leq y \leq 5$. If $3 \leq y$ then it is also true that for any $x \in R, 3 - x^2 \leq y$ as $3 - x^2 \leq 3, \forall x \in R$. Similarly it is true that $y \leq 5 + x^2, \forall x \in R$. Now we get,

$$3 - x^2 \leq y \leq 5 + x^2, \forall x \in R.$$

Which is equivalent to saying,

$$y \in \bigcap_{x \in R} [3 - x^2, 5 + x^2].$$

So we showed that

$$\bigcap_{x \in R} [3 - x^2, 5 + x^2] = [3, 5].$$

$\square$