PSTAT 8 Sample Midterm Answer

Haosheng Zhou

Feb, 2023

Problem 3

Theorem 1. *If* $a \equiv b\ (mod\ n)$*, then* $\gcd(a, n) = \gcd(b, n)$.

Proof. Use direct proof.

Since $a \equiv b\ (mod\ n)$, by definition

$$\exists q_a \in \mathbb{Z}, r_a \in \{0, 1, ..., n-1\}, a = q_a \cdot n + r_a \tag{1}$$
$$\exists q_b \in \mathbb{Z}, r_b \in \{0, 1, ..., n-1\}, b = q_b \cdot n + r_b \tag{2}$$
$$r_a = r_b \tag{3}$$

by Euclidean algorithm, $\gcd(a, n) = \gcd(n, r_a), \gcd(n, r_b) = \gcd(b, n)$. Since $r_a = r_b$, we have $\gcd(n, r_a) = \gcd(n, r_b)$, that's why $\gcd(a, n) = \gcd(b, n)$. $\square$

Problem 4

Theorem 2. *If* $A - B \neq \emptyset$*, then* $A \not\subset B$.

Proof. Prove by contradiction.

Assume $A \subset B$, then since $A - B \neq \emptyset$, we can always take any element in $A - B$ to find $\forall x \in A - B$, $x \in A$ and $x \notin B$. Since $x \in A, A \subset B$, we know $x \in B$.

This gives a contradiction since $x \notin B$ and $x \in B$. So the statement is proved. $\square$

Problem 5

Theorem 3. $\sqrt{5}$ *is irrational.*

Proof. Prove by contradiction.

Assume $\sqrt{5}$ is rational so $\exists p, q \in \mathbb{Z}, \gcd(p, q) = 1, \sqrt{5} = \frac{p}{q}$. So now $p^2 = 5q^2, 5|p^2$.

Let's make an observation here that $5|p^2$ always implies that $5|p$ (will be proved later).

By using this observation, we conclude that $5|p$ so $\exists k \in \mathbb{Z}, p = 5k$. Plug back to find $p^2 = (5k)^2 = 25k^2 = 5q^2$ so $q^2 = 5k^2, 5|q^2$. Use the observation once more to see $5|q$ so $\gcd(p, q) \geq 5$ since 5 is the common divisor of p, q.

This is a contradiction with $\gcd(p, q) = 1$, so the statement is proved assuming that the observation is true.

At last, let's prove that our observation above is correct. Divide p by 5 so $\exists q \in \mathbb{Z}, r \in \mathbb{Z}, r \in \{0, 1, 2, 3, 4\}$ such that $p = 5q + r$, so $p^2 = (5q + r)^2 = 25q^2 + 10qr + r^2 = 5(5q^2 + 2qr) + r^2$. Since $5|p^2$ and $5|5(5q^2 + 2qr)$, we know that $5|r^2$. Since $1^2, ..., 4^2$ are all not multiple of 5, we conclude that $r = 0$ and $5|p$. The observation is proved.

$\square$

Remark. *Notice the fact that for positive integer p and any* ***prime*** *integer a,* $a|p^2$ *always implies* $a|p$*. This is a very useful observation one shall bear in mind since it can be applied to prove that* $\sqrt{a}$, $\sqrt[3]{a}$ *are irrational for prime integer a.*

Problem 6

Theorem 4. *For positive integer a, b, $a = \gcd(a, b)$ if and only if $a|b$.*

Proof. Use direct proof for both directions.

If $a = \gcd(a, b)$, a must be the common divisor of a, b so $a|b$, proved.

If $a|b$, a is a common divisor of a, b so by the definition of greatest common divisor, $\gcd(a, b) \geq a$. On the other hand, notice that any positive divisor of a cannot exceed a so the common divisor of a, b must not exceed a, so $\gcd(a, b) \leq a$. As a result, $\gcd(a, b) = a$, proved.

□

Problem 7

Theorem 5. *For set A, B, C, D, $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.*

Proof. Use direct proof. To prove that two sets are the same, just need to show they are subsets of each other.

First prove that $(A \times B) \cap (C \times D) \subset (A \cap C) \times (B \cap D)$.

$\forall x \in (A \times B) \cap (C \times D)$, we know $x \in A \times B$ and $x \in C \times D$ so x must be an ordered pair $x = (x_1, x_2)$. As a result, $x_1 \in A$ and $x_2 \in B$ and $x_1 \in C$ and $x_2 \in D$. So $x_1 \in A \cap C$ and $x_2 \in B \cap D$, so $x = (x_1, x_2) \in (A \cap C) \times (B \cap D)$ and it's proved.

Next prove that $(A \cap C) \times (B \cap D) \subset (A \times B) \cap (C \times D)$.

$\forall x \in (A \cap C) \times (B \cap D)$, we know x must be an ordered pair $x = (x_1, x_2)$ such that $x_1 \in A \cap C$ and $x_2 \in B \cap D$, so $x_1 \in A$ and $x_1 \in C$ and $x_2 \in B$ and $x_2 \in D$. So $(x_1, x_2) \in A \times B$ and $(x_1, x_2) \in C \times D$ so $x = (x_1, x_2) \in (A \times B) \cap (C \times D)$, proved.

□