Problem Set 05: Advanced Proofs

Blingblong

CS/MATH 113 Discrete Mathematics
Habib University
Spring 2025

In this problem set you may be using needing the following definitions and theoremstyle

Definition 1. *An integer $p > 1$ is called a prime number, or simply a prime, iff $\forall x \in \mathbb{Z}^+,\ x|p \implies x = 1$ or $x = p$. In other words an integer $p > 1$ is prime, if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is termed composite.*

Definition 2. *A real number $r \in \mathbb{R}$ is called rational, if there exists $p, q \in \mathbb{Z}$, such that $r = \frac{p}{q}$ where $q \neq 0$. A real number that is not rational is called irrational.*

Definition 3 (Divisor and GCD)**.** *Let $a, b \in \mathbb{Z}$, $a \neq 0$ is said to divide b or b is divisible by a (denoted as $a \mid b$), if there exists an integer k such that $b = ak$. If no such k exists then we say a doesn't divide b (denoted by $a \nmid b$).*

For integers a and b, d is the greatest common divisor of a and b (denoted as $\gcd(a, b) = d$), if $d \mid a$ and $d \mid b$ and $\forall c \in \mathbb{Z},\ c \mid a$ and $c \mid b \implies c \leq d$.

Definition 4 (Multiple and LCM)**.** *For integers a and b, a positive integer m is the least common multiple of a and b (denoted as $\operatorname{lcm}(a, b) = m$), if $a \mid m$ and $b \mid m$ and $\forall c \in \mathbb{Z}^+,\ a \mid c$ and $b \mid c \implies m \leq c$.*

Theorem 1 (Division algorithm)**.** *If $a, b \in \mathbb{Z}$, where $b > 0$, then there exists unique $q, r \in \mathbb{Z}$, $a = bq + r$ where, $0 \leq r < b$*

Theorem 2 (Bezout's Lemma)**.** *For any integers a and b there exist integers s and t such that $gcd(a, b) = as + bt$*

Corollary 1 (Corollary of Bezout's Lemma)**.** *If a and b are relatively prime then $as + bt = 1$*

Theorem 3 (Fundamental Theorem of Arithmetic)**.** *Every integer $N > 1$ has a prime factorization, meaning either N is itself prime or can be written as a product of prime numbers.*

Problems

1. Prove or disprove the following claim: $x \in \mathbb{Z}$. If $7x + 9$ is even, then x is odd.
2. Prove or disprove the following claim: there exists irrational numbers a and b such that a^b is rational.
3. Prove or disprove the following claim: if n is an integer and n^2 is divisible by 4, then n is divisible by 4.
4. Prove or disprove the following claim: if a is a positive integer and $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ must be an integer.
5. Prove Euclid's Lemma: if p is a prime number that divides ab then p divides a or p divides b.
6. Show that $\sqrt{p}$ is irrational for any prime number p.
7. Show that for all positive integers a and b show that $\gcd(a, b)\mathrm{lcm}(a, b) = ab$.