Math 251W: Foundations of Advanced Mathematics

Portfolio Assignment 3: §2.1-3

Name: August Bergquist

Problem 2.2.6

proposition: Let a, b, c, m, and n be integers. If $a|b$ and $a|c$ then $a|(bm + cn)$.

$\boxed{\text{proof}}$ (Direct Proof)

By definition of divides, there exists an integer q such that $b = qa$.

Similarly, because $a|c$, there exists some integer r such that $c = ra$.

By substitution, $(bm + cn) = (aqm + arm)$.

By the distributive property, $(bm + cn) = a(qm + rn)$.

Because $(qm + rn)$ is also an integer by the closure properties of integers over addition and multiplication. To generalize this, there exists some integer x such that $ax = (bm + cn)$.

Thus, by definition of divides, $a|(bm + cn)$.
■

Problem 2.2.8

proposition: If a and b are integers and $a|b$, then $a^n|b^n$.

$\boxed{\text{proof}}$ (Direct Proof)

By definition of divides, there exists some integer q such that $aq = b$.

By substitution, $b^n = (aq)^n$.
By the commutative property of multiplication, $b^n = a^n q^n$. Because of the closure property of integers over multiplication, q^n is an integer $x = q^n$, which means there exists an integer such that $b^n = xa^n$. Thus, by definition of divides, if b and a are integers such that $a|b$, then $a^n|b^n$. ■

Problem 2.3.5

proposition: Let a, b, and c be integers. If there exists an integer d such that $d|a$ and $d|b$ but $d \nmid c$, then $ax + by = c$ has no integer solutions for x and y.

$\boxed{\text{proof}}$ (Contradiction)

Suppose by way of contradiction that if there exists an integer d such that $d|a$, $d|b$, and $d \nmid c$, then $ax + by = c$ has an integer solution for x and y. In other words, there exists integers x and y such that $ax + by = c$.

By definition of divides, there exists integers n and m such that $a = dn$ and $b = dm$.

By substitution, $dnx + dmy = c$. Using the commutative property, $d(nx + my) = c$. By the closure properties of integers over multiplication and addition, $d(nx + my)$ is an integer. Furthermore, by definition of of divides, $d|c$. This is a contradiction, as we have already stated that $d| \not c$. Thus, if there exists an integer d such that $d|a$ and $d|b$ but $d \not| c$, then $ax + by = c$ has no integer solutions for x and y. ■

Problem 2.3.6

proposition: If $c \geq 2$ is a composite integer, then there exists a positive integer $b \geq 2$ such that $b|c$ and $b \leq \sqrt{c}$.

$\boxed{\text{proof}}$ (Contrapositive)

The contrapositive of this statement is the following statement. For each integer $c \geq 2$ there exists a positive integer $b \geq 2$ such that if $b \not| c$ and $b > \sqrt{c}$ then c is not composite.

By definition of divides, $b \not| c$ means there does not exist an integer q such that $c = bq$.

Because there is currently no definition of square roots to work with, let us define $\sqrt{c} = b$ to mean $bb = c$ for all positive integers b and c. Thus, the statement $b > \sqrt{c}$ implies $bb > c$. If c is less than b^2, and there is no integer such that $c = bq$, then the only numbers that divide c are 1 and c.

By definition of a prime number, a prime number is a number that is not composite. By definition, c is prime if and only if the only numbers that divide c are 1 and c.

Using this definition, we can say that c is prime, and therefore not composite.

Thus, for each integer $c \geq 2$ there exists a positive integer $b \geq 2$ such that if $b \not| c$ and $b > \sqrt{c}$ then c is not composite. The contrapositive is true, thus the statement is also true.

Thus, If $c \geq 2$ is a composite integer, then there exists a positive integer $b \geq 2$ such that $b|c$ and $b \leq \sqrt{c}$. ■

Problem 2.3.8

proposition: Let $q \geq 2$ be a positive integer. If for all integers a and b, whenever $q|ab$, $q|a$ or $q|b$, then q is prime.

$\boxed{\text{proof}}$ (Contrapositive)

The contrapositive of this statement is: "if q is composite, then there exists integers a and b such that $q|ab$ and $q \not| a$ and $q \not| b$.

Suppose q is composite. Then by definition there exists integers other than q and 1 that divide q.
Furthermore, for every integer q there exists a prime number p such that $p|q$. By the Axioms Page, every integer can be uniquely expressed, up to an ordering of the factors and multiplications by ± 1, as a product of primes. Because q is a positive integer, there must be more than one prime numbers, greater than one, that are factors of q. Thus, we can say that there exists at least two prime numbers p and s such that $q = ps$.

p and s are prime numbers, and q is composite, so $p \neq q$, therefore the only numbers that divide p and s are themselves and 1. Because of this, $q \not| p$ and $q \not| s$.

Thus there exists two integers, a and b such that if q is composite, then $q|ab$ and $q \not| a$ and $q \not| b$. The contrapositive of the propasition is true, therefore the contrapositive is true. Thus if for all integers a and b, whenever $q|ab$, $q|a$ or $q|b$, then q is prime.

■