Name: ______________________________

Midterm 1

Math 2710 – Spring 2014

Professor Hohn

Instructions: Turn off and put away your cell phone. No calculators or electronic devices are allowed. Show all of your work! No credit will be given for unsupported answers or illegible solutions.

Question	1	2	3	4	5	6	Total
Definitions	4	4	4	4	4	4	24
Score:							

Question	1	2	3	4	5	6	Total
Proofs	6	6	6	6	6	6	36
Score:							

Total score:

1. (4 points) What does it mean for an integer a to divide an integer b?

> **Solution:** An integer a divides an integer b if there exists an integer q such that $b = a \cdot q$.

2. Let $a, b, c \in \mathbb{Z}$. Prove or find a counterexample for each of the following statements.

   (a) (3 points) If $a \mid b$ or $a \mid c$, then $a \mid bc$.

   > **Solution:** Since $a \mid b$, by definition $b = a \cdot q$. Multiplying both sides by c, we have $bc = a \cdot qc$. Then, $a \mid bc$.

   (b) (3 points) If $a \mid bc$, then $b \mid a$ or $c \mid a$.

   > **Solution:** Counterexample: Let $a = 2$, $b = 4$, and $c = 8$. Then, $2 \mid 4 \cdot 8$, but $4 \nmid 2$ and $8 \nmid 2$.

3. (4 points) What is the definition of the greatest common divisor of two integers a and b?

Solution: The greatest common divisor of two integers a and b, not both zero, is the largest positive integer dividing both a and b.

4. (6 points) Let a and b be integers. Show that if $\gcd(a, b) = 1$, then $\gcd(a, a + b) = 1$.

Solution: Let $d = \gcd(a, b)$. By definition, $d \mid a$ and $d \mid b$. Hence, $d \mid (a + b)$. Therefore, d is a common divisor of a and $a + b$, and $d \mid \gcd(a, a + b)$.

Let $\hat{d} = \gcd(a, a + b)$. By definition, $\hat{d} \mid a$ and $\hat{d} \mid (a + b)$. Hence, $\hat{d} \mid ((a + b) - a)$, and $\hat{d} \mid b$. $\hat{d}$ is a common divisor of a and b, so $\hat{d} \mid \gcd(a, b)$. Since $\gcd(a, b) \mid \gcd(a, a + b)$ and $\gcd(a, a + b) \mid \gcd(a, b)$, $\gcd(a, a + b) = \gcd(a, b) = 1$.

5. (4 points) Define the least common multiple of two integers.

Solution: The least common multiple of two positive integers a and b is the smallest positive integer that is divisible by both a and b.

6. (6 points) Prove that if a and b are nonzero integers, then

$$\operatorname{lcm}(a,b) = \frac{|ab|}{\gcd(a,b)}\,.$$

Solution: Let $|a| = p_1^{a_1} \dots p_n^{a_n}$ and $|b| = p_1^{b_1} \dots p_n^{b_n}$ be prime factorizations of the integers $|a|$ and $|b|$. It is always true that $a_i + b_i = \max\{a_i, b_i\} + \min\{a_i, b_i\}$. Let $d_i = \min\{a_i, b_i\}$ and $e_i = \max\{a_i, b_i\}$. Then,

$$\begin{aligned} |a \cdot b| &= p_1^{a_1} \dots p_n^{a_n} \cdot p_1^{b_1} \dots p_n^{b_n} \\ &= p_1^{a_1+b_1} \dots p_n^{a_n+b_n} \\ &= p_1^{d_1+e_1} \dots p_n^{d_n+e_n} \\ &= p_1^{d_1} \dots p_n^{d_n} \cdot p_1^{e_1} \dots p_n^{e_n} \\ &= \gcd(a,b) \cdot \operatorname{lcm}(a,b) \end{aligned}$$

since we know that $p_1^{d_1} \dots p_n^{d_n} = \gcd(a,b)$ and $p_1^{e_1} \dots p_n^{e_n} = \operatorname{lcm}(a,b)$. Since $\gcd(a,b) \mid a \cdot b$, we can write

$$\frac{|a \cdot b|}{\gcd(a,b)} = \operatorname{lcm}(a,b)$$

7. (4 points) Define the union of two sets S and T.

Solution: The union of the sets S and T is the set $S \cup T$ where

$$S \cup T = \{x \mid x \in S \text{ or } x \in T\}.$$

8. (6 points) Let S and T be sets. Prove $S \cup T = T \iff S \subseteq T$.

Solution: ($\Longrightarrow$) Suppose $S \cup T = T$. Let $x \in S$. Then, $x \in S \cup T$ and since $S \cup T = T$, $x \in T$. Therefore, $S \subseteq T$.

($\Longleftarrow$) Suppose $S \subseteq T$. Let $x \in S \cup T$. Then, $x \in S$ or $x \in T$. If $x \in S$, $x \in T$ since $S \subseteq T$. Hence, $S \cup T \subseteq T$.

Let $x \in T$. Then, $x \in S \cup T$ and $T \subseteq S \cup T$. Therefore, $S \cup T = T$.

9. (4 points) Define a linear Diophantine equation.

Solution: An equation of the form

$$ax + by = c \quad \text{for integers } x, y$$

where a, b, c are given integers.

10. (6 points) Show that the Diophantine equation $ax^2+by^2 = c$ does not have any integer solutions unless $\gcd(a, b) \mid c$. If $\gcd(a, b) \mid c$, does the equation always have an integer solution?

Solution: Let $d = \gcd(a, b)$. By definition, $d \mid a$ and $d \mid b$. Then, $d \mid (ax^2 + by^2)$ for integers x, y. If $ax^2 + by^2 = c$, then $d \mid c$.

If $\gcd(a, b) \mid c$, the equation $ax^2 + by^2 = c$ does not always have an integer solution. For example, let $a = 1$, $b = 1$, and $c = 3$. The $\gcd(a, b) = 1$ and $1 \mid 3$. However, $x^2 + y^2 = 3$ does not have any integer solutions.

11. (4 points) Define what it means for an integer to be prime.

> **Solution:** An integer $p > 1$ is called prime if its only divisors are 1 and p.

12. (6 points) Let m be an integer greater than 1. Suppose that for all $a, b \in \mathbb{Z}$

$$m \mid ab \implies m \mid a \text{ or } m \mid b\,.$$

Show m is prime.

> **Solution:** Suppose m is not prime. Then, there exists $p, q \in \mathbb{Z}$ such that $m = pq$ where $p < m$ and $q < m$. Since $m = pq$, $m \mid pq$ and so (by assumption) $m \mid p$ or $m \mid q$. But this cannot happen since $p < m$ and $q < m$. Hence, m must be prime.