Math N55– Midterm 1
Discrete Mathematics

Instructor: Max Hlavacek

July 12, 2019

Name: ______________________________

Student ID number: ______________________________

In this exam, you are allowed writing utensils and one 8.5x11 notesheet. No calculators are allowed. Please write your name and id number at the top of each page in the space provided.

This exam contains 7 pages (including this cover page) and 5 questions. The total number of points is 50.
Good luck!

Distribution of Marks

Question	Points	Score
1	10	
2	10	
3	10	
4	10	
5	10	
Total:	50	

1. Mark each of the following True or False. No explanation required. To ease the grading process, please clearly write T for true and F for false on the provided line.

   (a) (2 points) F If $gcd(a, m) \neq 1$, then the congruence $ax \equiv b(\text{mod } m)$ has no solutions.

   (b) (2 points) T Let A and B be finite sets. Then $|A \times B| = |B \times A|$

   (c) (2 points) F The statement $\forall x(16x = y)$ is a proposition.

   (d) (2 points) F The statement $\exists y \forall x(x + y = 0)$ is true, where the domain is real numbers.

   (e) (2 points) T The sum of two rational numbers is a rational number.

2. (10 points) Give an example of each of the following, or explain why an example does not exist.

(a) A surjective function from the set $\{1, 2, 3\}$ to the set $\{1, 2, 3, 4, 5\}$.

There are a few different ways to

This does not exist. Since the domain has size 3, the range can have size at most 3. Since the size of the codomain is 5, the size of range and codomain cannot be equal. So no onto function exists.

(b) A surjective function from the set of odd integers to the set of integers.

This does exist. $f(n) = \frac{n-1}{2}$. (there are a few dif answers).

~~Every odd integer can be uniquely expressed as 2n+~~

(c) A bijective function from the positive real numbers to the prime numbers.

Impossible since the two sets have different cardinalities.

The positive real numbers are uncountably infinit.

The prime numbers are countably infinit.

3. (10 points) Prove that if an integer n is a perfect square, then the remainder when n is divided by 4 is either 0 or 1.

~~One possible proof is: Since n is a perf~~

~~We have two cases~~

~~Case 1: n is odd. So n can be expressed as n = 2k+1 for some k ∈ ℤ.~~

~~So~~

Note: There are a few different proofs:

First, since n is a perfect square, we can write $n = k^2$ for some integer k.

Case 1: k is odd, so we can write $k = 2m+1$ for some $m \in \mathbb{Z}$. So

$$n = k^2 = (2m+1)^2 = 4m^2 + 4m + 1 \equiv 1 \pmod 4.$$

Case 2: k is even, so we can write $k = 2m$ for some $m \in \mathbb{Z}$.

So $n = k^2 = (2m)^2 = 4m^2 \equiv 0 \pmod 4$.

So n is either congruent to 0 or 1 mod 4.

4. (10 points) Prove that if a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$. For this problem, you are not allowed to assume the existence and uniqueness of prime factorizations.

We use Bezout's lemma:

since $\gcd(a,b)=1$, $\exists\ s,t \in \mathbb{Z}$ s.t.

$as + bt = 1$. Multiplying both sides

by c we get

$$\underbrace{acs}_{a \text{ divides this}} + \underbrace{bct}_{a \text{ divides this since } a|bc} = c$$

Since a divides the left hand side, it has to divide the right hand side.

So $a|c$ as desired.

5. (a) (5 points) Write the number $(10010)_2$ in base 4.

$$(10010)_2 = 2^4 + 2^1 = 18.$$

$$18 = 4^2 + 2 = 4^2 + 0(4) + 2(4^0) = (102)_4.$$

(b) (5 points) What is the inverse of 19 modulo 44?

We first do the Euclidean algorithm:

$$44 = \underline{19} \cdot 2 + \underline{6}$$

$$19 = \underline{6} \cdot 3 + 1.$$

We now do this backwards:

$$1 = 19 - 6 \cdot 3 = 19 - (44 - 19 \cdot 2)3 = 19 \cdot \underline{7} - 44 \cdot 3.$$

So the inverse of 19 mod 44 is 7.

This page is intentionally left blank to accommodate work that wouldn't fit elsewhere and/or scratch work.