Math N55– Practice Midterm 1
Discrete Mathematics

Instructor: Max Hlavacek

July 9, 2019

Name: Max :)

Student Number: 123456789.

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

Distribution of Marks

Question	Points	Score
1	10	Good
2	10	Luck
3	10	You
4	10	Got
5	10	This
Total:	50	!! :)

1. Mark each of the following True or False. No explanation required.
   (a) (2 points) The compound proposition $(p \to q) \wedge (q \to r) \to (p \to r)$ is a tautology.
   (b) (2 points) If x and y are irrational numbers, then $x + y$ is irrational.
   (c) (2 points) For every integer n there is a unique integer m such that $0 \leq m \leq 5$ and $m \equiv n($ mod 5)
   (d) (2 points) The set of prime numbers is countably infinite.
   (e) (2 points) If A and B are sets such that $A \subset \mathbb{Z}$ and $B \subset \mathbb{Z}$, then $A \times B = B \times A$.

(a). True
(b) False
(c) False
(d) True.
(e) False.

2. Prove that the following statements are false, i.e. prove their negations.

(a) (5 points)

$$\forall a, b \in \mathbb{Z}^+, \exists k \in \mathbb{Z}^+ (a + bk \text{ is prime}).$$

(b) (5 points)

$$\exists a, b \in \mathbb{Z}^+, \forall k \in \mathbb{Z}^+ (a + bk \text{ is prime}).$$

(a). First, let's write the negation down:

$\neg(\forall a,b \in \mathbb{Z}^+, \exists k \in \mathbb{Z}^+ (a+bk \text{ is prime})) =$

$\exists a,b \in \mathbb{Z}^+, \forall k \in \mathbb{Z}^+ (a+bk \text{ is not prime})$.

So we just have to show that there is a pair (a,b) s.t. $a+bk$ is never prime, regardless of k.

$a=2$ and $b=2$ works, since then $a+bk$ will always be divisible by 2.

(b). Similarly to above, we can rewrite the negation as

$\forall a,b \in \mathbb{Z}^+, \exists k \in \mathbb{Z}^+ (a+bk \text{ is not prime})$.

So we need to show that for all pairs a,b, there is a k s.t. $a+bk$ is not prime.

One way to show this is using the following 2 cases:

Case 1: $a \neq 1$. Then let $k = a$. Then $a + bk = a + ba = a(b+1)$ which is composite.

Case 2: $a = 1$. Then let $k = b+2$. Then $a + bk = 1 + b(b+2) = b^2 + 2b + 1 = (b+1)^2$ which is composite.

This is in my opinion is the hardest problem on the practice exam. Don't panic if you couldn't figure this one out.

3. (10 points) Prive that if an integer n is the sum of two squares, then $n \not\equiv 3 (\mod 4)$. Here, square means square of an integer.

You can use the fact that every perfect square is either congruent to 0 or 1 (mod 4).

So the sum of two squares is either congruent to,

0+0, 0+1, 1+0 or 1+1 mod 4.

None of these gives us 3 (mod 4)

4. (10 points) Prove that if a and m are positive integers such that $\gcd(a, m) \neq 1$ then a does not have an inverse modulo m.

A lot of you proved this by contradiction on the HW. I will give a slightly different (but basically the same) version using contrapositive:

We will prove this by contrapositive: Assume a has an inverse modulo m. Thus, there exists an integer s such that $as \equiv 1 \bmod m$. By definition, this means $m \mid as-1$. By the definition of divisibility, this means $\exists\, t \in \mathbb{Z}$ such that $mt = as - 1$. This rearranges to $as - mt = 1$. Let $d = \gcd(a, m)$. Since $d \mid a$ and $d \mid m$, $d \mid as - mt$. So since $as - mt = 1$, $d \mid 1$. The only divisor of 1 is 1, so $d = 1$. Thus, we have shown $\gcd(a, m) = 1$.

So by contrapositive the original statement holds.

5. (a) (5 points) Find the remainder when 2^{55} is divided by the prime number 53.

   (b) (5 points) Use the Euclidean Algorithm to find the greatest common divisor of 270 and 63.

(a). By FLT, $2^{52} \equiv 1 \bmod 53$. ($a=2$ and $p=53$.)

So $2^{55} \equiv 2^{52} 2^3 \equiv 1 \cdot 2^3 \equiv 8 \bmod 53$.

So $2^{55} \bmod 53 = 8$

(b). $270 = 4 \cdot 63 + 18$

$63 = 3 \cdot 18 + 9$

$18 = 2 \cdot 9 + 0$

So gcd is 9.