MATH 301: Spring 2023 **Instructor: Nicholas Vlamis**

Wednesday 3/1/2023 Exam 1 110 minutes

Name: Solutions

Instructions.

1. ***Read each problem carefully.*** Make sure you understand what the problem is asking.
2. Proofs can be informal: use of logical symbols and incomplete sentences **are** permitted. However, make sure all statements and logical steps are clear and correct.
3. You are allowed to use notes handwritten by you on the front and back of one 8.5" x 11" sheet of paper. You must turn in your note sheet with the exam.
4. No devices other than a writing utensil may be used.

Question	Points	Score
1	5	
2	8	
3	5	
4	8	
5	8	
6	8	
7	8	
Total:	50	

1. [5 points] (a) Use the Euclidean algorithm to compute $\gcd(34, 114)$.

$114 = 3 \cdot 34 + 12$

$34 = 2 \cdot 12 + 10$

$12 = 1 \cdot 10 + 2$

$10 = 5 \cdot 2$

$\Rightarrow \gcd(34, 114) = 2$

(b) Write $\gcd(34, 114)$ as a linear combination of 34 and 114.

$2 = 12 - 10$

$= 12 - (34 - 2 \cdot 12)$

$= 3 \cdot 12 - 34$

$= 3(114 - 3 \cdot 34) - 34$

$= 3 \cdot 114 - 10 \cdot 34$

2. [8 points] For each of following pairs of sets and binary operations, give **one reason** why the pair is **not** a group.

(a) the natural numbers with addition, $(\mathbb{N}, +)$

No identity element: $x+y > x \quad \forall\, x, y \in \mathbb{N}$

or, No inverses

(b) the integers with substraction, $(\mathbb{Z}, -)$

Subtraction is not associative

$3 - 4 \neq 4 - 3$

(c) the rational numbers with multiplication, $(\mathbb{Q}, \cdot)$

0 does not have an inverse

$0 \cdot x \neq 1 \quad \forall\, x \in \mathbb{Q}$

(d) the equivalence classes of integers modulo 15 with multiplication modulo 15, $(\mathbb{Z}_{15}, \cdot)$

Same as above

(meant to ask about $\mathbb{Z}_{15}^{\times}$)

3. [5 points] Recall that $U(10)$ is the group of units of $\mathbb{Z}_{10}$, with the group operation being multiplication modulo 10.

   (a) List the elements of $U(10)$.

   1, 3, 7, 9

   (b) Construct the Cayley table for $U(10)$.

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

4. [8 points] Let $n \in \mathbb{N}$ such that $n \geq 2$. Prove that n and $n-1$ are relatively prime.

Let $d = \gcd(n, n-1)$.

Then $d \mid n$ and $d \mid n-1$

$\Rightarrow d \mid (n-(n-1)) \Rightarrow d \mid 1$

$\Rightarrow d = 1$. $\square$

5. [8 points] Let $n \in \mathbb{N}$ such that $3 \mid (n^2+n+1)$. Find the remainder of n divided by 3. Justify your answer.

By division algorithm, $n = 3q + r$ w/ $r \in \{0, 1, 2\}$.

Case 1 $r = 0 \Rightarrow n^2+n+1 = 3(3q^2+q)+1$

$\Rightarrow 3 \nmid n^2+n+1$

Case 2 $r = 1 \Rightarrow n^2+n+1 = (9q^2+6q+1)+(3q+1)+1$

$= 3(3q^2+3q+1)$

$\Rightarrow 3 \mid n^2+n+1$

Case 3 $r = 2 \Rightarrow n$

6. [8 points] Let G be a group. Prove that if $a^2 = e$ for every $a \in G$, then G is abelian.

7. 8 points (a) Use induction to prove that $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1)$ for any $x \in \mathbb{R}$ and any $p \in \mathbb{N}$.

(b) Let $p \in \mathbb{N}$. Prove that if $2^p - 1$ is prime, then p is prime. (Hint: use part (a) and recall that $(b^n)^m = b^{nm}$.)