MATH 301/601: Fall 2023 **Instructor: Nicholas Vlamis**

Wednesday 3/6/2024 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 one 8.5" x 11" sheet of notes, written on the front and back. Your sheet may only contain theorem statements and definitions. You must turn in your note sheet with the exam.
4. No devices other than a writing utensil may be used.
5. Feel free to use the back of any sheet. Just make it clear where I am meant to look for your solutions.

Question	Points	Score
1	6	
2	3	
3	4	
4	3	
5	6	
6	4	
7	8	
8	8	
9	8	
10	8	
Total:	50	

Part I: Computation and Understanding

1. [6 points] (a) Use the Euclidean algorithm to compute gcd(18, 120).

$120 = 6 \cdot 18 + 12$

$18 = 12 \cdot 1 + 6$ $\quad \gcd(18, 120) = 6$

$12 = 6 \cdot 2 + 0$

(b) Write gcd(18, 120) as a linear combination of 18 and 120.

$6 = 18 - 12$

$= 18 - (120 - 6 \cdot 18)$

$= 7 \cdot 18 + (-1) \cdot 120$

(c) Is 24 a linear combination of 18 and 120? If so, give the linear combination; if not, explain why not.

Yes, $\quad 24 = 4 \cdot 6 = 28 \cdot 18 + (-4) \cdot 120$

2. [3 points] Use the fact that $10^n \equiv (-1)^n \pmod{11}$ for each $n \in \mathbb{N}$ to show that 132539 is divisible by 11.

$132539 = 9 + 3 \cdot 10 + 5 \cdot 10^2 + 2 \cdot 10^3 + 3 \cdot 10^4 + 1 \cdot 10^5$

$\equiv 9 - 3 + 5 - 2 + 3 - 1 \mod 11$

$\equiv 11 \mod 11$

$\equiv 0 \mod 11$

$\Rightarrow 11 \mid 132539$

3. [4 points] Find infinitely many solutions to the equation $5x + 1 \equiv 15 \pmod{21}$. Justify your answer.

$5x+1 \equiv 15 \mod 21 \Rightarrow 5x \equiv 14 \mod 21$

If $x = 7$, then $5x = 5 \cdot 7 = 35 = 14 \mod 21$

$\Rightarrow x \in \{7 + 21k \mid k \in \mathbb{Z}\}$ is a solution to $5x+1 \equiv 15 \pmod{21}$

4. [3 points] Give an example of a function $f\colon \mathbb{N} \to \mathbb{N}$ that is surjective but not injective.

$$f(n) = \begin{cases} n-1 & \text{if } n \geq 2 \\ 1 & \text{if } n = 1 \end{cases}$$

$f(2) = f(1) = 1$, so f is not injective,

but it is surjective: given $k \in \mathbb{N}$, $f(k+1) = k$.

5. [6 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

$n + m > n, m \quad \forall\, n, m \in \mathbb{N}$

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

Not associative

$-2 = (0 - 1) - 1 \neq 0 - (1 - 1) = 0$

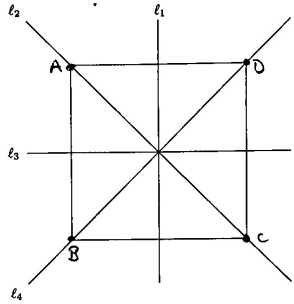
(c) the rational numbers with multiplication, $(\mathbb{Q}, \cdot)$

0 does not have an inverse

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

$\Rightarrow \nexists\, x \in \mathbb{Q}$ s.t. $x0 = 1$.

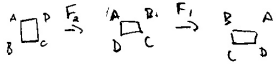
6. [4 points] This question asks you to work with the symmetries of a square S. For $\theta \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$, let R_θ denote the counter-clockwise rotation of angle θ about the center of S, and for $i \in \{1, 2, 3, 4\}$, let F_i be the symmetry of S given by reflection in the line ℓ_i, where ℓ_i is shown in the following figure:



The set $D_4 = \{R_0, R_{\frac{\pi}{2}}, R_\pi, R_{\frac{3\pi}{2}}, F_1, F_2, F_3, F_4\}$ is a group under composition.

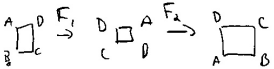
(a) Find the element of D_4 that is equal to $F_1 \circ F_2$.

$R_{3\pi/2}$



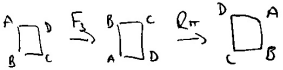
(b) Find the element of D_4 that is equal to $F_2 \circ F_1$.

$R_{\pi/2}$



(c) Find the element of D_4 that is equal to $R_\pi \circ F_3$.

F_1



(d) Find the element of D_4 that is equal to $F_4 \circ R_{\frac{\pi}{2}}$.

F_3

Part II: Proofs

Instructions: Complete any three of the following four problems.

7. [8 points] Let $f\colon A \to B$ and $g\colon B \to C$ be functions. Prove that if $g \circ f$ is injective and f is surjective, then g is injective.

Let $b_1, b_2 \in B$ s.t. $g(b_1) = g(b_2)$.

NTS $b_1 = b_2$

As f is surjective, $\exists\, a_1, a_2 \in A$ s.t. $f(a_1) = b_1$ and $f(a_2) = b_2$.

Now, $(g \circ f)(a_1) = g(f(a_1)) = g(b_1) = g(b_2) = g(f(a_2)) = (g \circ f)(a_2)$

As $g \circ f$ injective, $a_1 = a_2$. Hence, $b_1 = f(a_1) = f(a_2) = b_2$. ∎

8. [8 points] Let $n \in \mathbb{N}$ and $a \in \mathbb{Z} \setminus \{0\}$ be relatively prime. Prove that if $b \equiv a \pmod{n}$, then b and n are relatively prime. (****This is an easier version of a homework problem: do not reference any homework exercises in your proof.*)

$b \equiv a \mod n$

$\Rightarrow n \mid b-a$

$\Rightarrow \exists\, q \in \mathbb{Z}$ s.t. $qn = b-a$

$\Rightarrow a = b - qn$

Let $d = \gcd(b, n)$.

As $d \mid b$ and $d \mid n$, $d \mid (b - qn)$

$\Rightarrow d \mid a$ and $d \mid n$

The only common divisor of a and n is 1,

so $d = 1$. ∎

9. [8 points] Use induction to prove that 3 divides $10^{n+1} + 10^n + 1$ for every $n \in \mathbb{N}$.

Base case: If $n=1$, then $10^{n+1}+10^n+1 = 111$ and $3 \mid 111$ ($111 = 3 \cdot 37$).

Inductive step: Suppose $3 \mid (10^{n+1}+10^n+1)$ for some $n \in \mathbb{N}$.

NTS $3 \mid (10^{n+2}+10^{n+1}+1)$

$10^{n+2}+10^{n+1}+1 = 10(10^{n+1}+10^n+1) - 9$

As $3 \mid 9$ and $3 \mid (10^{n+1}+10^n+1)$, $3 \mid (10^{n+2}+10^{n+1}+1)$.

□

10. [8 points] Let G be a group and suppose that $(ab)^2 = a^2b^2$ for all $a, b \in G$. Prove that G is an abelian group.

Let $a, b \in G$.

$(ab)^2 = abab$

So, $abab = a^2b^2 = aabb$

$\Rightarrow a^{-1}(abab) = a^{-1}(aabb)$

$\Rightarrow bab = abb$

$\Rightarrow (bab)b^{-1} = (abb)b^{-1}$

$\Rightarrow ba = ab.$

□