MA 437 Exam 1 Solutions

September 22, 2014 **Name:** $\underbrace{\hspace{8cm}}_{\text{By writing my name, I attest that I will adhere to the honor code.}}$

Read all of the following information before starting the exam:

- All solutions must be explained completely in order to earn full credit.
- This test has 4 problems and is worth 50 points. It is your responsibility to make sure that you have all of the pages!
- Since time is limited, it is crucial that you *think* before you write.
- Be sure to use proper mathematical notation. Incorrect or improvised notation will result in a loss of points.
- You may use (within reason) any results from class or the textbook, as long as you make it clear that you are doing so.
- Good luck!

1. Let $\mathbb{Z}$ be the set of integers. Define a relation $\sim$ on $\mathbb{Z}$ as follows: $a \sim b$ if and only if $a^2 = b^2$.

(a) Prove that $\sim$ is an equivalence relation.

Solution: To show that $\sim$ is an equivalence relation, we must show that $\sim$ is reflexive, symmetric, and transitive on $\mathbb{Z}$.

- For all $a \in \mathbb{Z}$, $a^2 = a^2$. It follows that $a \sim a$ for all $a \in \mathbb{Z}$. Thus, $\sim$ is reflexive.
- Suppose $a \sim b$. Then $a^2 = b^2$. By symmetry of equality, $b^2 = a^2$. Hence, $b \sim a$. So $\sim$ is symmetric.
- Suppose $a \sim b$ and $b \sim c$. Then $a^2 = b^2$ and $b^2 = c^2$. By transitivity of equality, $a^2 = c^2$. Thus, $a \sim c$, so $\sim$ is transitive.

(b) Calculate $[0]$, the equivalence class containing 0.

Solution: Let $x \in \mathbb{Z}$ such that $x \sim 0$. Then $x^2 = 0^2$, and hence $x = 0$. On the other hand, if $x = 0$, then $x \sim 0$, so $[0]$, which is defined as the set of all integers which are related to 0 under $\sim$, is equal to the set $\{0\}$.

(c) Calculate $[4]$, the equivalence class containing 4.

Solution: Let $x \in \mathbb{Z}$ such that $x \sim 4$. Then $x^2 = 4^2$, and hence $x = \pm 4$. On the other hand, if $x = \pm 4$, then $x \sim 4$, so $[4] = \{4, -4\}$.

2. Suppose that n is an integer which is not divisible by 5. Prove that $n^4 \bmod 5 = 1$.

(Hint: What could $n \bmod 5$ be?)

Solution: Since $5 \nmid n$, $n \bmod 5 \neq 0$. It follows that $n \bmod 5 = 1$, 2, 3, or 4. We proceed by cases.

- **Case 1.** If $n \bmod 5 = 1$, then
$$n^4 \bmod 5 = 1^4 \bmod 5 = 1 \bmod 5 = 1.$$
- **Case 2.** If $n \bmod 5 = 2$, then
$$n^4 \bmod 5 = 2^4 \bmod 5 = 16 \bmod 5 = 1.$$
- **Case 3.** If $n \bmod 5 = 3$, then
$$n^4 \bmod 5 = 3^4 \bmod 5 = 81 \bmod 5 = 1.$$
- **Case 4.** If $n \bmod 5 = 4$, then
$$n^4 \bmod 5 = 4^4 \bmod 5 = 256 \bmod 5 = 1.$$

Since $n^4 \bmod 5 = 1$ in all possible cases, the desired result follows.

Remark: If you want some extra practice, try the following similar exercises:

(a) Prove that if n is an integer which is not divisible by 7, then $n^6 \bmod 7 = 1$.

(b) Prove that if n is an odd integer which is not divisible by 5, then the last digit of n^4 is 1.

3. For a positive integer n, let $U(n) = \{x \in \mathbb{Z} \mid 0 < x < n \text{ and } \gcd(x,n) = 1\}$. Recall that $U(n)$ is a group under multiplication mod n.

For p a prime, let $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ and

$$\mathrm{GL}(2,\mathbb{Z}_p) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a,b,c,d \in \mathbb{Z}_p \text{ and } (ad-bc) \bmod p \neq 0 \right\}.$$

Recall that $\mathrm{GL}(2,\mathbb{Z}_p)$ is a group under matrix multiplication mod p.

(a) Find the inverse of 2 in the group $U(5)$.

Solution: Since $2 \cdot 3 \bmod 5 = 6 \bmod 5 = 1$, which is the identity in $U(5)$, the inverse of 2 in $U(5)$ is 3.

(b) Find the inverse of $\begin{bmatrix} 1 & 2 \\ 1 & 4 \end{bmatrix}$ in the group $\mathrm{GL}(2,\mathbb{Z}_5)$. Be sure to check that your calculation is correct.

Solution: Recall that the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $\mathrm{GL}(2,\mathbb{Z}_p)$ is the matrix $\begin{bmatrix} d(ad-bc)^{-1} & -b(ad-bc)^{-1} \\ -c(ad-bc)^{-1} & a(ad-bc)^{-1} \end{bmatrix}$ where all calculations are mod p and $(ad-bc)^{-1}$ denotes the inverse of the determinant mod p.
Note that $\det \begin{bmatrix} 1 & 2 \\ 1 & 4 \end{bmatrix} \bmod 5 = (1 \cdot 4 - 2 \cdot 1) \bmod 5 = 2 \bmod 5 = 2$. Thus, by part (a), the inverse of the determinant of the given matrix mod 5 is 3.
Hence, the inverse of $\begin{bmatrix} 1 & 2 \\ 1 & 4 \end{bmatrix}$ in $\mathrm{GL}(2,\mathbb{Z}_5)$ is

$$\begin{bmatrix} 4 \cdot 3 \bmod 5 & -2 \cdot 3 \bmod 5 \\ -1 \cdot 3 \bmod 5 & 1 \cdot 3 \bmod 5 \end{bmatrix} = \begin{bmatrix} 12 \bmod 5 & -6 \bmod 5 \\ -3 \bmod 5 & 3 \bmod 5 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 2 & 3 \end{bmatrix}.$$

4. For each, either prove that the given set is a group under the given operation or explain why the set is not a group under the operation.

(a) E, the set of even integers, under addition.

Solution: E is a group under addition. Indeed:

- If $x, y \in E$, then $x + y$ is even, so that $x + y \in E$. So $+$ is a binary operation on E.
- Addition of numbers is associative.
- The identity is 0: Since 0 is even, $0 \in E$. Furthermore, $x + 0 = 0 + x = x$ for all $x \in E$.
- The inverse of $a \in E$ is $-a$: If $a \in E$, then $-a$ is even, so $-a \in E$, and $a + (-a) = (-a) + a = 0$.

(b) $\mathbb{R}$, the set of real numbers, under multiplication.

Solution: Since $1 \cdot x = x \cdot 1 = x$ for all $x \in \mathbb{R}$, 1 would be the identity if $\mathbb{R}$ were a group under multiplication. However, since $0 \cdot x = 0$ for all $x \in \mathbb{R}$, there is no element $y \in \mathbb{R}$ for which $0 \cdot y$ is the identity. Hence, 0 does not have an inverse, and therefore $\mathbb{R}$ is not a group under multiplication.

Remark: You should check that $\mathbb{R}^*$, the set of nonzero real numbers, is a group under multiplication.

(c) $\mathbb{R}^*$, the set of nonzero real numbers, under division.

Solution: $\mathbb{R}^*$ is not a group under division since division is not associative. For example, $(8 \div 4) \div 2 = 1$, but $8 \div (4 \div 2) = 4$.

(d) *(Bonus!)* $\mathbb{R}^3$, the set of 3-dimensional real vectors, under cross products.

Solution: A fundamental property of the cross product is that $\mathbf{v} \times \mathbf{w}$ is *orthogonal* to both $\mathbf{v}$ and $\mathbf{w}$. Thus, given two nonzero vectors $\mathbf{v}$ and $\mathbf{w}$, $\mathbf{v} \times \mathbf{w}$ is neither equal to $\mathbf{v}$ nor $\mathbf{w}$. Hence, the operation of cross product does not allow for the existence of an identity element. So this is not a group.

Another reason that $\mathbb{R}^3$ is not a group under cross products is that the cross product is not associative (see any Calculus III textbook for an example).