MATH 521A: Abstract Algebra

Homework 3 Solutions

1. Let $n, c \in \mathbb{N}$, and let $a, b \in \mathbb{Z}$. Suppose that $a \equiv b \pmod{n}$. Prove that $ac \equiv bc \pmod{n}$. Show that the converse does not hold [by giving an example of a, b, c, n where $ac \equiv bc \pmod{n}$ but $a \not\equiv b \pmod{n}$].

   Since $a \equiv b \pmod{n}$, $n|(a-b)$. Thus, there is some $k \in \mathbb{Z}$ with $a - b = kn$. Multiplying both sides by c gives $ac - bc = (kc)n$. Since $kc \in \mathbb{Z}$, we have $n|(ac - bc)$ and hence $ac \equiv bc \pmod{n}$.

   Many counterexamples are possible; one is $n = 4, a = 0, b = 2, c = 2$. We have $ac = 0 \equiv 4 = bc \pmod{n}$, but $a = 0 \not\equiv 2 = b \pmod{n}$.

2. Find an integer x such that $x^2 \equiv 2 \pmod{31}$.

   A bit of trial and error gives us $x = 8$, or $x = 23$ (i.e. -8). These are the only integers with $0 \leq x \leq 30$ that are modular square roots of 2.

3. Which of $[0], [1], [2], [3], [4]$ is equal to $[2^{(3^{45})}]$, in $\mathbb{Z}_5$?

   We start by calculating $[2^1] = [2], [2^2] = [4], [2^3] = [3], [2^4] = [1], [2^5] = [2], \ldots$, all in $\mathbb{Z}_5$. Note that the pattern repeats after $[2^4]$, i.e. after every FOUR exponents. Hence, to find $[2^n]$ in $\mathbb{Z}_5$, we need to find $n \mod 4$. Now, $3^1 \mod 4 = 3, 3^2 \mod 4 = 1, 3^3 \mod 4 = 3, \ldots$. Hence, to find $[3^m]$ in $\mathbb{Z}_4$, we need to find $m \mod 2$. Here we have $m = 45$, so $m \mod 2 = 1$. Hence $[3^m] = [3^1]$ in $\mathbb{Z}_4$, so $n \mod 4 = 3$. Hence $[2^n] = [2^3] = [3]$ in $\mathbb{Z}_5$.

4. Let $a, b \in \mathbb{Z}$. Prove that $(a+b)^3 \equiv a^3 + b^3 \pmod{3}$. This is (a special case of) a theorem called the Freshman's Dream.

   We calculate $(a+b)^3 - (a^3 + b^3) = (a^3 + 3a^2b + 3ab^2 + b^3) - (a^3 + b^3) = 3(a^2b + ab^2)$. Since $a^2b + ab^2 \in \mathbb{Z}$, we have $3|(a+b)^3 - (a^3 + b^3)$ and hence $(a+b)^3 \equiv a^3 + b^3 \pmod{3}$.

5. Let $n \in \mathbb{N}$, and $a, b \in \mathbb{Z}$. Suppose that $a \equiv b \pmod{n}$. Prove that $\gcd(a, n) = \gcd(b, n)$.

   By the symmetry between a and b, it suffices to prove that $\gcd(a, n) \leq \gcd(b, n)$. Set $d = \gcd(a, n)$ for convenience. Since $a \equiv b \pmod{n}$, $n|(a-b)$. Thus there is some integer k with $a - b = kn$. We rearrange to $b = a - kn$. Since $d|a$ and $d|n$, we can write $a = da', n = dn'$ for some integers a', n'. We now have $b = da' - kdn' = d(a' - kn')$. Hence $d|b$. But we also have $d|n$, so d is a common factor of b, n. Thus, by definition of gcd, we have $d \leq \gcd(b, n)$.

6. Write the $\oplus$-addition and $\odot$-multiplication tables of $\mathbb{Z}_9$.

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[2]	[0]	[2]	[4]	[6]	[8]	[1]	[3]	[5]	[7]
[3]	[0]	[3]	[6]	[0]	[3]	[6]	[0]	[3]	[6]
[4]	[0]	[4]	[8]	[3]	[7]	[2]	[6]	[1]	[5]
[5]	[0]	[5]	[1]	[6]	[2]	[7]	[3]	[8]	[4]
[6]	[0]	[6]	[3]	[0]	[6]	[3]	[0]	[6]	[3]
[7]	[0]	[7]	[5]	[3]	[1]	[8]	[6]	[4]	[2]
[8]	[0]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

7. For $\mathbb{Z}_9$, find the neutral additive element, the neutral multiplicative element, and all zero divisors. Be sure to justify your answer.

The neutral additive element is [0] and the neutral multiplicative element is [1]. The zero divisors are those elements that have a factor in common with 9, namely [3] and [6]. To justify, note that $[3] \odot [3] = [6] \odot [3] = [6] \odot [6] = [0]$.

8. For $\mathbb{Z}_9$, find all the units and specify each inverse.

We have $[1] \odot [1] = [2] \odot [5] = [4] \odot [7] = [8] \odot [8]$, so $[1], [2], [4], [5], [7], [8]$ are the units.

We define $\mathbb{Z}_3 \times \mathbb{Z}_3 = \{(a, b) : a \in \mathbb{Z}_3, b \in \mathbb{Z}_3\}$, the set of ordered pairs of elements, one from $\mathbb{Z}_3$ and one from another copy of $\mathbb{Z}_3$. We define operations in the natural way, i.e. componentwise: $(a, b) \oplus (a', b') = (a \oplus_3 a', b \oplus_3 b')$ and $(a, b) \odot (a', b') = (a \odot_3 a', b \odot_3 b')$.

9. Write the $\oplus$-addition and $\odot$-multiplication tables of $\mathbb{Z}_3 \times \mathbb{Z}_3$.

$\oplus$	([0],[0])	([0],[1])	([0],[2])	([1],[0])	([1],[1])	([1],[2])	([2],[0])	([2],[1])	([2],[2])
([0],[0])	([0],[0])	([0],[1])	([0],[2])	([1],[0])	([1],[1])	([1],[2])	([2],[0])	([2],[1])	([2],[2])
([0],[1])	([0],[1])	([0],[2])	([0],[0])	([1],[1])	([1],[2])	([1],[0])	([2],[1])	([2],[2])	([2],[0])
([0],[2])	([0],[2])	([0],[0])	([0],[1])	([1],[2])	([1],[0])	([1],[1])	([2],[2])	([2],[0])	([2],[1])
([1],[0])	([1],[0])	([1],[1])	([1],[2])	([2],[0])	([2],[1])	([2],[2])	([0],[0])	([0],[1])	([0],[2])
([1],[1])	([1],[1])	([1],[2])	([1],[0])	([2],[1])	([2],[2])	([2],[0])	([0],[1])	([0],[2])	([0],[0])
([1],[2])	([1],[2])	([1],[0])	([1],[1])	([2],[2])	([2],[0])	([2],[1])	([0],[2])	([0],[0])	([0],[1])
([2],[0])	([2],[0])	([2],[1])	([2],[2])	([0],[0])	([0],[1])	([0],[2])	([1],[0])	([1],[1])	([1],[2])
([2],[1])	([2],[1])	([2],[2])	([2],[0])	([0],[1])	([0],[2])	([0],[0])	([1],[1])	([1],[2])	([1],[0])
([2],[2])	([2],[2])	([2],[0])	([2],[1])	([0],[2])	([0],[0])	([0],[1])	([1],[2])	([1],[0])	([1],[1])

$\odot$	([0],[0])	([0],[1])	([0],[2])	([1],[0])	([1],[1])	([1],[2])	([2],[0])	([2],[1])	([2],[2])
([0],[0])	([0],[0])	([0],[0])	([0],[0])	([0],[0])	([0],[0])	([0],[0])	([0],[0])	([0],[0])	([0],[0])
([0],[1])	([0],[0])	([0],[1])	([0],[2])	([0],[0])	([0],[1])	([0],[2])	([0],[0])	([0],[1])	([0],[2])
([0],[2])	([0],[0])	([0],[2])	([0],[1])	([0],[0])	([0],[2])	([0],[1])	([0],[0])	([0],[2])	([0],[1])
([1],[0])	([0],[0])	([0],[0])	([0],[0])	([1],[0])	([1],[0])	([1],[0])	([2],[0])	([2],[0])	([2],[0])
([1],[1])	([0],[0])	([0],[1])	([0],[2])	([1],[0])	([1],[1])	([1],[2])	([2],[0])	([2],[1])	([2],[2])
([1],[2])	([0],[0])	([0],[2])	([0],[1])	([1],[0])	([1],[2])	([1],[1])	([2],[0])	([2],[2])	([2],[1])
([2],[0])	([0],[0])	([0],[0])	([0],[0])	([2],[0])	([2],[0])	([2],[0])	([1],[0])	([1],[0])	([1],[0])
([2],[1])	([0],[0])	([0],[1])	([0],[2])	([2],[0])	([2],[1])	([2],[2])	([1],[0])	([1],[1])	([1],[2])
([2],[2])	([0],[0])	([0],[2])	([0],[1])	([1],[0])	([1],[2])	([1],[1])	([2],[0])	([2],[2])	([2],[1])

10. For $\mathbb{Z}_3 \times \mathbb{Z}_3$, find the neutral additive element, the neutral multiplicative element, and all zero divisors. Be sure to justify your answer.

The neutral additive element is $([0], [0])$ and the neutral multiplicative element is $([1], [1])$. Just half of the nonzero elements are zero divisors: $([0], [1]) \odot ([1], [0]) = ([0], [2]) \odot ([2], [0]) = ([0], [0])$. Note that although $\mathbb{Z}_3 \times \mathbb{Z}_3$ and $\mathbb{Z}_9$ both have nine elements, they have different multiplicative structure.

11. For $\mathbb{Z}_3 \times \mathbb{Z}_3$, find all the units and specify each inverse.

Just half of the nonzero elements are units (those that are not zero divisors): $([1], [1]) \odot ([1], [1]) = ([2], [1]) \odot ([2], [1]) = ([1], [2]) \odot ([1], [2]) = ([2], [2]) \odot ([2], [2]) = ([1], [1])$. Note that every invertible element happens to be its own inverse, in this ring. This is quite unusual.