Solutions to Assignment 4

7A

15. We know that elements in \( \mathbb{Z}/m\mathbb{Z} \) are either units or zero divisors. We also know the units in \( \mathbb{Z}/m\mathbb{Z} \) are all of the form \([a]\) where \((a, m) = 1\). So the units are:

- \( \mathbb{Z}/6\mathbb{Z} : [1], [5] \)
- \( \mathbb{Z}/7\mathbb{Z} : [1], [2], [3], [4], [5], [6] \)
- \( \mathbb{Z}/8\mathbb{Z} : [1], [3], [5], [7] \)

23. Obviously, \( x = 0 \) is a solution of the equation \( ax = 0 \).

Since \( a \) is a zero divisor, there is a nonzero element \( y \) so that \( ay = 0 \). But then \( x = 0 \) and \( x = y \) are two different solutions of the equation.

30. As in the first question, the zero divisors of \( \mathbb{Z}/18\mathbb{Z} \) are the elements \([a]\) with \((a, 18) \neq 1\). The complementary zero divisors are:

- \([2] : [9] \)
- \([3] : [6], [12] \)
- \([6] : [3], [6], [9], [12], [15] \)
- \([8] : [9] \)
- \([9] : [2], [4], [6], [8], [10], [12], [14], [16] \)
- \([10] : [9] \)
- \([12] : [3], [6], [9], [12], [15] \)
- \([14] : [9] \)
- \([15] : [6], [12] \)
- \([16] : [9] \)

32. We need to solve \( ax \equiv 1 (mod 365) \) for \( a = 53, 73, 93, 113 \). First note that \((73, 365) = 73 \) so \([73]\) is not a unit, hence it has no multiplicative inverse. For the other cases, we just need to solve the above equation as in previous homeworks:

- \([53]^{-1} = [62] \)
- \([93]^{-1} = [157] \)
- \([113]^{-1} = [42] \)

35. (i) The elements are \( \{0 + 0i, 1 + 0i, 2 + 0i, 0 + i, 1 + i, 2 + i, 0 + 2i, 1 + 2i, 2 + 2i\} \).

(ii) \( 1^{-1} = 1, 2^{-1} = 2, i^{-1} = 2i, (2i)^{-1} = i, (1 + i)^{-1} = 2 + i, (2 + i)^{-1} = 1 + i, (2 + 2i)^{-1} = 1 + 2i, (1 + 2i)^{-1} = 2 + 2i \). For instance,

\[
(1 + 2i)(2 + 2i) = 2 + 4i + 2i + 4i^2 = 2 + 4i^2 + 6i = 2 - 4 + 6i \equiv -2 + 0i \equiv 1
\]

(iii) \( (1 + i)^2 = 2i, (2i)^2 = -4 \equiv 2, 2^2 \equiv 1 \). Therefore \( (1 + i)^8 = 1 \). And hence the order of \( 1 + i \) must be a factor of 8, i.e. 1, 2 or 4. However, we have already seen from the above computation that \((1 + i)^2, (1 + i)^4 \) are not equal to 1. Hence the order of \( 1 + i \) must be 8.
36. The four elements are \( \{0, 1, i, 1 + i\} \). Obviously \( 1^2 = 1 = i^2 \) so both 1 and \( i \) have themselves as inverses. However, \( (1 + i)(1 + i) = 2i \equiv 0 \). It is a zero divisor, which has no inverses.

7D

40. We need to check \( f \circ g \) satisfies the first three conditions in page 140.

(i) \( f \circ g(a + b) = f(g(a + b)) = f(g(a) + g(b)) = f(g(a)) + f(g(b)) = f \circ g(a) + f \circ g(b) \).

(ii) \( f \circ g(a \cdot b) = f(g(a \cdot b)) = f(g(a) \cdot g(b)) = f(g(a)) \cdot f(g(b)) = f \circ g(a) \cdot f \circ g(b) \).

(iii) \( f \circ g(1) = f(g(1)) = f(1) = 1 \).

The other conditions can be deduced from the first three.

42. Again, check the first three conditions in page 140:

(i) \( f(a + b) = \begin{pmatrix} a + b & 0 \\ 0 & a + b \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = f(a) + f(b) \)

(ii) \( f(ab) = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = f(a)f(b) \)

(iii) \( f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_{d_2} \), the identity matrix. Note that the identity matrix is the multiplicative identity in \( M_2(R) \), hence we are done.

9A

2. The units are \([1], [2], [4], [5], [7], [8] \). Note that


Hence the order of \([2]\) is 6. By proposition 3 in page 174:

order of \([4]\) = 6/(2, 6) = 3

order of \([8]\) = 6/(3, 6) = 2

order of \([7]\) = 6/(4, 6) = 3

order of \([5]\) = 6/(5, 6) = 6

order of \([1]\) = 6/(6, 6) = 1


order of \([4]\) = 10/(2, 10) = 5

order of \([8]\) = 10/(3, 10) = 10

order of \([5]\) = 10/(4, 10) = 5

order of \([10]\) = 10/(5, 10) = 2

order of \([9]\) = 10/(6, 10) = 5

order of \([7]\) = 10/(7, 10) = 10

order of \([3]\) = 10/(8, 10) = 5

order of \([6]\) = 10/(9, 10) = 10

order of \([1]\) = 10/(10, 10) = 1

13. Again, by proposition 3 in page 174: order of \([3^{26}] = 162/(26, 162) = 81 \)

order of \([3^{27}] = 162/(27, 162) = 6 \)

9B

19. We have seen in the 9A Q4 that \([2]^9 = [6] \). So

20. By proposition 5, the order of \([3]\) in \(\mathbb{Z}/23\mathbb{Z}\) is divisible by 22 = 23 - 1. Hence the order of \([3]\) must be either 1, 2, 11, or 22. Obviously, \([3]^1 \neq 1\), \([3]^2 \neq 1\). Check that \([3]^{11}\) is indeed congruent to 1, hence the order of \([3]\) is 11.

27. Note that \(n^5/5 + n^3/3 + 7n/15 = \frac{3n^5 + 5n^3 + 7n}{15}\). We want to show the numerator \(3n^5 + 5n^3 + 7n\) is divisible by 15, i.e. it is divisible by both 3 and 5.

\[3n^5 + 5n^3 + 7n \equiv 2n^3 + n (\text{mod} 3) = n(2n^2 + 1)(\text{mod} 3)\]

If \((3, n) \neq 1\), then it must be equal to 3, i.e. \(n\) is a multiple of 3. Therefore,

\[n(2n^2 + 1) \equiv 0 (\text{mod} 3)\]

If \((3, n) = 1\), then by Fermat’s Little Theorem \(n^2 \equiv 1 (\text{mod} 3)\), and hence the above equation reads

\[n(2n^2 + 1) \equiv n(2 + 1) = 3n \equiv 0 (\text{mod} 3)\]

In both cases, \(3n^5 + 5n^3 + 7n \equiv 0 (\text{mod} 3)\).

The case for divisibility of 5 is similar:

\[3n^5 + 5n^3 + 7n \equiv 3n^5 + 2n (\text{mod} 5) = n(3n^4 + 2)(\text{mod} 3)\]

If \((5, n) \neq 1\), then it must be equal to 5, i.e. \(n\) is a multiple of 5. Therefore,

\[n(3n^4 + 2) \equiv 0 (\text{mod} 5)\]

If \((5, n) = 1\), then by Fermat’s Little Theorem \(n^4 \equiv 1 (\text{mod} 5)\), and hence the above equation reads

\[n(3n^4 + 2) \equiv n(3 + 2) = 5n \equiv 0 (\text{mod} 3)\]

In both cases, \(3n^5 + 5n^3 + 7n \equiv 0 (\text{mod} 5)\).

36. \(2^9 = 512 \equiv 1 (\text{mod} 511)\). Note that \(2^8 = 256 < 511\) so 9 is the order of 2 in \((\text{mod} 511)\).

If 511 were prime, then by Fermat \(2^{510} \equiv 1 (\text{mod} 511)\). By \((i)\), the order of 2 is 9, and hence 510 must be a multiple of the order of 2, i.e. \(9|510\). However, this is not the case.