

1.4 SOLUTIONS

30. Find the multiplicative inverse of each nonzero element of
- \mathbf{Z}_7
- .

Solution: Since $6 \equiv -1 \pmod{7}$, the class $[6]_7$ is its own inverse. Furthermore, $2 \cdot 4 = 8 \equiv 1 \pmod{7}$, and $3 \cdot 5 = 15 \equiv 1 \pmod{7}$, so $[2]_7$ and $[4]_7$ are inverses of each other, and $[3]_7$ and $[5]_7$ are inverses of each other.

31. Find the multiplicative inverse of each nonzero element of
- \mathbf{Z}_{13}
- .

Comment: If $ab \equiv 1 \pmod{n}$, then $[a]_n$ and $[b]_n$ are inverses, as are $[-a]_n$ and $[-b]_n$. If $ab \equiv -1 \pmod{n}$, then $[a]_n$ and $[-b]_n$ are inverses, as are $[-a]_n$ and $[b]_n$. It is useful to list the integers with m with $m \equiv \pm 1 \pmod{n}$, and look at the various ways to factor them.

Solution: Note that 14, 27, and 40 are congruent to 1, while 12, 25, and 39 are congruent to -1 . Using 14, we see that $[2]_{13}$ and $[7]_{13}$ are inverses. Using 12, and we see that $[3]_{13}$ and $[-4]_{13}$ are inverses, as are the pairs $[4]_{13}$ and $[-3]_{13}$, and $[6]_{13}$ and $[-2]_{13}$. Using 40, we see that $[5]_{13}$ and $[8]_{13}$ are inverses. Finally, here is the list of inverses: $[2]_{13}^{-1} = [7]_{13}$; $[3]_{13}^{-1} = [9]_{13}$; $[4]_{13}^{-1} = [10]_{13}$; $[5]_{13}^{-1} = [8]_{13}$; $[6]_{13}^{-1} = [11]_{13}$; Since $[12]_{13}^{-1} = [-1]_{13}^{-1} = [-1]_{13} = [12]_{13}$, this takes care of all of the nonzero elements of \mathbf{Z}_{13} .

32. Find
- $[91]_{501}^{-1}$
- , if possible (in
- \mathbf{Z}_{501}^\times
-).

Solution: We need to use the Euclidean algorithm.

$$\begin{bmatrix} 1 & 0 & 501 \\ 0 & 1 & 91 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -5 & 46 \\ 0 & 1 & 91 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -5 & 46 \\ -1 & 6 & 45 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & -11 & 1 \\ -1 & 6 & 45 \end{bmatrix}$$

$$\text{Thus } [91]_{501}^{-1} = [-11]_{501} = [490]_{501}.$$

33. Find
- $[3379]_{4061}^{-1}$
- , if possible (in
- \mathbf{Z}_{4061}^\times
-).

Solution: The inverse does not exist. $\begin{bmatrix} 1 & 0 & 4061 \\ 0 & 1 & 3379 \end{bmatrix} \rightsquigarrow$

$$\begin{bmatrix} 1 & -1 & 682 \\ 0 & 1 & 3379 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 682 \\ -4 & 5 & 651 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 5 & -6 & 31 \\ -4 & 5 & 651 \end{bmatrix}$$

At the next step, $31 \mid 651$, and so $(4061, 3379) = 31$.

34. In
- \mathbf{Z}_{20}
- : find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.

Comment: We know that \mathbf{Z}_n has $\varphi(n)$ units. They occur in pairs, since $\gcd(a, n) = 1$ if and only if $\gcd(n - a, n) = 1$. This helps to check your list.

Solution: The units of \mathbf{Z}_{20} are the equivalence classes represented by 1, 3, 7, 9, 11, 13, 17, and 19. We have $[3]_{20}^{-1} = [7]_{20}$, $[9]_{20}^{-1} = [9]_{20}$, $[11]_{20}^{-1} = [11]_{20}$, $[13]_{20}^{-1} = [17]_{20}$, and $[19]_{20}^{-1} = [19]_{20}$.

The idempotent elements of \mathbf{Z}_{20} can be found by using trial and error. They are $[0]_{20}$, $[1]_{20}$, $[5]_{20}$, and $[16]_{20}$. If you want a more systematic approach, you can use the hint in Exercise 1.4.13 of the text: if $n = bc$, with $\gcd(b, c) = 1$, then any solution to the congruences $x \equiv 1 \pmod{b}$ and $x \equiv 0 \pmod{c}$ will be idempotent modulo n .

The nilpotent elements of \mathbf{Z}_{20} can be found by using trial and error, or by using Problem 1.4.40. They are $[0]_{20}$ and $[10]_{20}$.

35. In \mathbf{Z}_{24} : find all units (list the multiplicative inverse of each); find all idempotent elements; find all nilpotent elements.

Solution: The units of \mathbf{Z}_{24} are the equivalence classes represented by 1, 5, 7, 11, 13, 17, 19, and 23. For each of these numbers we have $x^2 \equiv 1 \pmod{24}$, and so each element is its own inverse.

The idempotent elements are $[0]_{24}$, $[1]_{24}$, $[9]_{24}$, $[16]_{24}$, and the nilpotent elements are $[0]_{24}$, $[6]_{24}$, $[12]_{24}$, $[18]_{24}$.

36. Show that \mathbf{Z}_{17}^\times is cyclic.

Comment: To show that \mathbf{Z}_{17}^\times is cyclic, we need to find an element whose multiplicative order is 16. The solution just uses trial and error. It is known that if p is prime, then \mathbf{Z}_p^\times is cyclic, but there is no known algorithm for actually finding the one element whose powers cover all of \mathbf{Z}_p^\times .

Solution: We begin by trying $[2]$. We have $[2]^2 = [4]$, $[2]^3 = [8]$, and $[2]^4 = [16] = [-1]$. Problem 39 shows that the multiplicative order of an element has to be a divisor of 16, so the next possibility to check is 8. Since $[2]^8 = [-1]^2 = [1]$, it follows that $[2]$ has multiplicative order 8.

We next try $[3]$. We have $[3]^2 = [9]$, $[3]^4 = [81] = [-4]$, and $[3]^8 = [16] = [-1]$. The only divisor of 16 that is left is 16 itself, so $[3]$ does in fact have multiplicative order 16, and we are done.

37. Show that \mathbf{Z}_{35}^\times is not cyclic but that each element has the form $[8]_{35}^i[-4]_{35}^j$, for some positive integers i, j .

Solution: We first compute the powers of $[8]$: $[8]^2 = [-6]$, $[8]^3 = [8][-6] = [-13]$, and $[8]^4 = [-6]^2 = [1]$, so the multiplicative order of $[8]$ is 4, and the powers we have listed represent the only possible values of $[8]^i$.

We next compute the powers of $[-4]$: $[-4]^2 = [16]$, $[-4]^3 = [-4][16] = [6]$, $[-4]^4 = [-4][6] = [11]$, $[-4]^5 = [-4][11] = [-9]$, and $[-4]^6 = [-4][-9] = [1]$, so the multiplicative order of $[-4]$ is 6.

There are 24 possible products of the form $[8]^i[-4]^j$, for $0 \leq i < 4$ and $0 \leq j < 6$. Are these all different? Suppose that $[8]^i[-4]^j = [8]^m[-4]^n$, for some $0 \leq i < 4$ and $0 \leq j < 6$ and $0 \leq m < 4$ and $0 \leq n < 6$. Then $[8]^{i-m} = [-4]^{n-j}$, and since the only power of $[8]$ that is equal to a power of $[-4]$ is $[1]$ (as shown by our computations), this forces $i = m$ and $n = j$.

We conclude that since there are 24 elements of the form $[8]^i[-4]^j$, every element in \mathbf{Z}_{35} must be of this form.

Finally, $([8]^i[-4]^j)^{12} = ([8]^4)^{3i}([-4]^6)^{2j} = [1]$, so no element of \mathbf{Z}_{35} has multiplicative order 24, showing that \mathbf{Z}_{35} is not cyclic.

38. Solve the equation $[x]_{11}^2 + [x]_{11} - [6]_{11} = [0]_{11}$.

Solution: We can factor $[x]^2 + [x] - [6] = ([x] + [3])([x] - [2])$. Corollary 1.4.6 implies that either $[x] + [3] = [0]$ or $[x] - [2] = [0]$, and so the solution is $[x] = [-3]$ or $[x] = [2]$.

39. Let n be a positive integer, and let $a \in \mathbf{Z}$ with $\gcd(a, n) = 1$. Prove that if k is the smallest positive integer for which $a^k \equiv 1 \pmod{n}$, then $k \mid \varphi(n)$.

Solution: Assume that k is the smallest positive integer for which $a^k \equiv 1 \pmod{n}$. We can use the division algorithm to write $\varphi(n) = qk + r$, where $0 \leq r < k$, and $q \in \mathbf{Z}$. Since $a^k \equiv 1 \pmod{n}$, we know that $\gcd(a, n) = 1$, and so we can apply Theorem 1.4.11, which shows that $a^{\varphi(n)} \equiv 1 \pmod{n}$. Thus $a^r = a^{\varphi(n) - kq} = a^{\varphi(n)}(a^k)^{-q} \equiv 1 \pmod{n}$, so we must have $r = 0$ since $r < k$ and k is the smallest positive integer with $a^k \equiv 1 \pmod{n}$.

40. Prove that $[a]_n$ is a nilpotent element of \mathbf{Z}_n if and only if each prime divisor of n is a divisor of a .

Solution: First assume that each prime divisor of n is a divisor of a . If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ is the prime factorization of n , then we must have $a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t} d$, where $0 \leq \beta_j \leq \alpha_j$ for all j . If k is the smallest positive integer such that $k\beta_i \geq \alpha_i$ for all i , then $n \mid a^k$, and so $[a]_n^k = [0]_n$.

Conversely, if $[a]_n$ is nilpotent, with $[a]_n^k = [0]$, then $n \mid a^k$, so each prime divisor of n is a divisor of a^k . But if a prime p is a divisor of a^k , then it must be a divisor of a , and this completes the proof.