Introduction to Abstract Algebra II: Homework 2

Due on January 21, 2026 at 23:59

Victor Ostrik 10:00

Hashem A. Damrah
UO ID: 952102243

Exercise 23.4. Find all solutions of $x^2 + 2x + 4 = 0$ in $\mathbb{Z}_6$.

Solution. Trying all possible values of x in $\mathbb{Z}_6$:

$$\begin{aligned}
x = 0 &: 0^2 + 2 \cdot 0 + 4 \equiv 4 && \pmod 6 \\
x = 1 &: 1^2 + 2 \cdot 1 + 4 \equiv 7 \equiv 1 && \pmod 6 \\
x = 2 &: 2^2 + 2 \cdot 2 + 4 \equiv 12 \equiv 0 && \pmod 6 \\
x = 3 &: 3^2 + 2 \cdot 3 + 4 \equiv 19 \equiv 1 && \pmod 6 \\
x = 4 &: 4^2 + 2 \cdot 4 + 4 \equiv 28 \equiv 4 && \pmod 6 \\
x = 5 &: 5^2 + 2 \cdot 5 + 4 \equiv 39 \equiv 3 && \pmod 6.
\end{aligned}$$

Therefore, the solutions is $x \equiv 2 \pmod 6$ □

Exercise 23.10. Find the characteristic of the given ring $\mathbb{Z}_6 \times \mathbb{Z}_{15}$.

Solution. The characteristic of a product ring is the least common multiple of the characteristics of the component rings. The characteristic of $\mathbb{Z}_6$ is 6, and the characteristic of $\mathbb{Z}_{15}$ is 15. Therefore, the characteristic of $\mathbb{Z}_6 \times \mathbb{Z}_{15}$ is $\operatorname{lcm}(6, 15) = 30$. □

Exercise 23.12. Classify each nonzero element of the ring $\mathbb{Z}_8$ as a unit, a divisor of 0, or neither.

Solution. In $\mathbb{Z}_8$, the nonzero elements are 1, 2, 3, 4, 5, 6, and 7. The units of $\mathbb{Z}_8$ are 1, 3, 5, and 7, while the divisors of zero are 2, 4, and 6. □

Exercise 23.20. Show that the matrix $\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}$ is a divisor of zero in $M_2(\mathbb{Z})$.

Solution. The matrix A is a zero divisor if there exists a nonzero matrix B such that $AB = 0$. Let $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. Then,

$$AB = \begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a + 2c & b + 2d \\ 2a + 4c & 2b + 4d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

This gives us the system of equations:

$$a + 2c = 0, \quad b + 2d = 0, \quad 2a + 4c = 0, \quad \text{and} \quad 2b + 4d = 0.$$

From the first equation, we have $a = -2c$. Substituting into the second equation gives $b = -2d$. Choosing $c = 1$ and $d = 1$, we get $a = -2$ and $b = -2$. Thus, we can take

$$B = \begin{bmatrix} -2 & -2 \\ 1 & 1 \end{bmatrix}.$$

Therefore, A is a divisor of zero in $M_2(\mathbb{Z})$. □

Exercise 23.29. An element a of a ring R is *idempotent* if $a^2 = a$. Show that a division ring contains exactly two idempotent elements.

Solution. Let R be a division ring and let $a \in R$ be an idempotent element, so $a^2 = a$. Rearranging gives $a^2 - a = 0$, or $a(a - 1) = 0$. Since R is a division ring, it has no zero divisors, so either $a = 0$ or $a = 1$. Therefore, the only idempotent elements in a division ring are 0 and 1. □

Exercise 23.35. Show that the characteristic of an integral domain D must be either 0 or a prime p. [Hint: If the characteristic of D is mn, consider $(m \cdot 1)(n \cdot 1)$ in D.]

Solution. Let the characteristic of the integral domain D be k. If $k = 0$, we are done. Suppose k is a positive integer that is not prime, so $k = mn$ for some integers $m, n > 1$. Then,

$$(m \cdot 1)(n \cdot 1) = (mn) \cdot 1 = k \cdot 1 = 0.$$

Since D is an integral domain, it has no zero divisors, so either $m \cdot 1 = 0$ or $n \cdot 1 = 0$. This contradicts the assumption that k is the smallest positive integer such that $k \cdot 1 = 0$. Therefore, if the characteristic of D is positive, it must be prime. □

Exercise 24.2. Show that the multiplicative group of nonzero elements of the field $\mathbb{Z}_{11}$ is cyclic. Illustrate this by finding a generator for this group for the finite field. $\mathbb{Z}_{11}$.

Solution. Let $F^\times$ denote the set of all non-zero elements of the field $\mathbb{Z}_{11}$. We will show that $F^\times$ is cyclic by finding a generator. The order of $F^\times$ is $11 - 1 = 10$. Notice that the set $\langle 2 \rangle$ generates $F^\times$ since the powers of 2 modulo 11 yield all non-zero elements of $\mathbb{Z}_{11}$

$$\begin{gathered} 2^1 \equiv 2 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 2^3 \equiv 8 \pmod{11}, \quad 2^4 \equiv 5 \pmod{11}, \quad 2^5 \equiv 10 \pmod{11} \\ 2^6 \equiv 9 \pmod{11}, \quad 2^7 \equiv 7 \pmod{11}, \quad 2^8 \equiv 3 \pmod{11}, \quad 2^9 \equiv 6 \pmod{11}, \quad 2^{10} \equiv 1 \pmod{11}. \end{gathered}$$

Thus, $F^\times$ is cyclic with generator 2. □

Exercise 24.6. Compute the remainder of $2^{\left(2^{17}\right)}$ when divided by 19. [Hint: You will need to compute the remainder of 2^{17} modulo 18.]

Solution. We will first compute 2^{17} module 18. Notice that the powers of 2 modulo 18 are:

$$\begin{gathered} 2^1 \equiv 2 \pmod{18}, \quad 2^2 \equiv 4 \pmod{18}, \quad 2^3 \equiv 8 \pmod{18}, \quad 2^4 \equiv 16 \pmod{18}, \quad 2^5 \equiv 14 \pmod{18} \\ 2^6 \equiv 10 \pmod{18}, \quad 2^7 \equiv 2 \pmod{18}. \end{gathered}$$

Thus, the powers of 2 modulo 18 repeat every 6 powers. Therefore,

$$2^{17} \equiv 2^{(6 \cdot 2 + 5)} \equiv 2^5 \equiv 14 \pmod{18}.$$

Now, we need to compute 2^{14} modulo 19. The powers of 2 modulo 19 are:

$$\begin{gathered} 2^1 \equiv 2 \pmod{19}, \quad 2^2 \equiv 4 \pmod{19}, \quad 2^3 \equiv 8 \pmod{19}, \quad 2^4 \equiv 16 \pmod{19}, \quad 2^5 \equiv 13 \pmod{19} \\ 2^6 \equiv 7 \pmod{19}, \quad 2^7 \equiv 14 \pmod{19}, \quad 2^8 \equiv 9 \pmod{19}, \quad 2^9 \equiv 18 \pmod{19}, \quad 2^{10} \equiv 17 \pmod{19} \\ 2^{11} \equiv 15 \pmod{19}, \quad 2^{12} \equiv 11 \pmod{19}, \quad 2^{13} \equiv 3 \pmod{19}, \quad 2^{14} \equiv 6 \pmod{19} \end{gathered}$$

Therefore, the remainder of $2^{\left(2^{17}\right)}$ when divided by 19 is 6. □

Exercise 24.27. Show that 1 and $p-1$ are the only elements of the field $\mathbb{Z}_p$ that are their own multiplicative inverse. [Hint: Consider the equation $x^2 - 1 = 0$.]

Solution. Solving the equation $x^2 - 1 = 0$ in $\mathbb{Z}_p$, we have $(x - 1)(x + 1) = 0$. The only two solutions in $\mathbb{Z}_p$ are 1 and -1, which is congruent to $p - 1$ modulo p. Therefore, the only elements of $\mathbb{Z}_p$ that are their own multiplicative inverse are 1 and $p - 1$. □

Exercise 25.8. The public key is $n = 1457$ and $s = 239$.

(i) Compute the value of y if the message is $m = 999$.

(ii) Find r. (Computer Algebra Systems have built-in functions to compute in $\mathbb{Z}_m$.)

(iii) Use your answers to parts (i) and (ii) to decrypt y.

Solution to (i). Breaking up $n = 1457$ into a product of primes, we get $n = 31 \times 47$. Therefore, $p = 31$ and $q = 47$. Next, we compute $\varphi(n) = (p-1)(q-1) = 30 \times 46 = 1380$. To compute y, we use the formula $y \equiv m^s \pmod{n}$. Thus,

$$y \equiv 999^{239} \pmod{1457}.$$

Using modular exponentiation, we find that $y \equiv 1000 \pmod{1457}$. □

Solution to (ii). To find r, we need to compute the modular inverse of s modulo $\varphi(n)$. We need to find r such that $sr \equiv 1 \pmod{1380}$. Using the Extended Euclidean Algorithm, we find that $r \equiv 1159 \pmod{1380}$. □

Solution to (iii). To decrypt y, we use the formula $m \equiv y^r \pmod{n}$. Thus,

$$m \equiv 1000^{1159} \pmod{1457}.$$

Using modular exponentiation, we find that $m \equiv 999 \pmod{1457}$, which matches our original message. □