

2.2 Certain Products in $\mathbb{Z}/\langle \ell \rangle$

How does the existence of multiplicative inverses impact products in modular arithmetic? We highlight a few famous formula.

2.2.0 Definition. For every positive $m \in \mathbb{Z}$, its *totient* $\phi(m)$ is the number of positive integers coprime to m ;

$$\phi(m) := \left| \{n \in \mathbb{N} \mid 1 \leq n \leq m \text{ and } \gcd(m, n) = 1\} \right|.$$

2.2.1 Remark. For the first few positive integers, the totient is

$$\begin{aligned} \phi(1) &= |\{1\}| = 1, & \phi(7) &= |\{1, 2, 3, 4, 5, 6\}| = 6, \\ \phi(2) &= |\{1\}| = 1, & \phi(8) &= |\{1, 3, 5, 7\}| = 4, \\ \phi(3) &= |\{1, 2\}| = 2, & \phi(9) &= |\{1, 2, 4, 5, 7, 8\}| = 6, \\ \phi(4) &= |\{1, 3\}| = 2, & \phi(10) &= |\{1, 3, 7, 9\}| = 4, \\ \phi(5) &= |\{1, 2, 3, 4\}| = 4, & \phi(11) &= |\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}| = 10, \\ \phi(6) &= |\{1, 5\}| = 2, & \phi(12) &= |\{1, 5, 7, 11\}| = 4. \end{aligned}$$

2.2.2 Lemma. A positive $p \in \mathbb{Z}$ is prime if and only if $\phi(p) = p - 1$.

Proof. Suppose that p is positive prime integer. Lemma 1.3.5 and Proposition 1.3.8 show that the integers in the set $\{1, 2, \dots, p-1\}$ are all coprime to p , so $\phi(p) = p - 1$.

Suppose that $\phi(p) = p - 1$. By definition, the integers in the set $\{1, 2, \dots, p-1\}$ are all coprime to p . Lemma 2.1.2 and Theorem 2.1.4 combine to establish that p is prime. $\square$

2.2.3 Theorem. Let $\ell \in \mathbb{Z}$ be positive. For all m coprime to ℓ , we have

$$m^{\phi(\ell)} \equiv 1 \pmod{\ell}.$$

Proof. Let $\{n_1, n_2, \dots, n_{\phi(\ell)}\} = \{n \in \mathbb{N} \mid 1 \leq n \leq \ell \text{ and } \gcd(n, \ell) = 1\}$. We first claim that the $\phi(\ell)$ congruence classes

$$[m n_1]_{\ell}, [m n_2]_{\ell}, \dots, [m n_{\phi(\ell)}]_{\ell}$$

are distinct. Given $\gcd(m, \ell) = 1$, Lemma 2.1.2 shows that $[m]_{\ell}$ has a multiplicative inverse in $\mathbb{Z}/\langle \ell \rangle$. Hence, for all $i, j \in \mathbb{Z}$ such that $1 \leq i, j \leq \phi(\ell)$, we have $[m n_i]_{\ell} = [m n_j]_{\ell}$ if and only if $[n_i]_{\ell} = [n_j]_{\ell}$. As $1 \leq n_i < \ell$ and $1 \leq n_j < \ell$, Proposition 2.0.4 establishes that $[n_i]_{\ell} = [n_j]_{\ell}$ if and only if $i = j$.

Since $\gcd(m n_i, \ell) = 1$ for all $1 \leq i \leq \phi(\ell)$, both

$$[m n_1]_{\ell}, [m n_2]_{\ell}, \dots, [m n_{\phi(\ell)}]_{\ell} \quad \text{and} \quad [n_1]_{\ell}, [n_2]_{\ell}, \dots, [n_{\phi(\ell)}]_{\ell}$$

list the same nonzero congruence classes (although not necessarily in the same order). We deduce that

$$[m^{\phi(\ell)}]_{\ell} [n_1 n_2 \cdots n_{\phi(\ell)}]_{\ell} = \prod_{j=1}^{\phi(\ell)} [m n_j]_{\ell} = \prod_{j=1}^{\phi(\ell)} [n_j]_{\ell} = [n_1 n_2 \cdots n_{\phi(\ell)}]_{\ell}.$$

Since $\gcd(n_1 n_2 \cdots n_{\phi(\ell)}, \ell) = 1$, Lemma 2.1.2 also demonstrates that $[n_1 n_2 \cdots n_{\phi(\ell)}]_{\ell}$ has multiplicative inverse in $\mathbb{Z}/\langle \ell \rangle$. It follows that $[m^{\phi(\ell)}]_{\ell} = [1]_{\ell}$ or $m^{\phi(\ell)} \equiv 1 \pmod{\ell}$. $\square$

2.2.4 Problem. Simplify $2^{1001} \pmod{15}$.

The word “totient” was created in J.J. Sylvester, *On Certain Ternary Cubic-Form Equations*, Amer. J. Math., 2 (1879) 357–393.

First published in L. Euler, *Theorematum arithmetica nova methodo demonstrata*, Novi Comment. Acad. Sci. Petropol., 8 (1763) 74–104.

When $\ell = 10$ and $m = 7$, we have

$$\begin{aligned} [7(1)]_{10} &= [7]_{10}, & [7(3)]_{10} &= [1]_{10}, \\ [7(7)]_{10} &= [9]_{10}, & [7(9)]_{10} &= [3]_{10}. \end{aligned}$$

It follows that

$$[7^4]_{10} [1(3)(7)(9)]_{10} = [1(3)(7)(9)]_{10}.$$

Since $[1(3)(7)(9)]_{10} = [9]_{10}$ and $[9]_{10}^2 = [1]_{10}$, multiplying both sides by $[9]_{10}$, we obtain $[7^4]_{10} = [1]_{10}$.

Solution. The previous theorem applies because $\gcd(2, 15) = 1$. An integer n satisfies $1 \leq n \leq 15$ and $\gcd(n, 15) = 1$ if and only if it belongs to the set $\{1, 2, 4, 7, 8, 11, 13, 14\}$, so we see that $\phi(15) = 8$. Since $2^8 \equiv 1 \pmod{15}$ and $1001 = 125(8) + 1$, we obtain

$$2^{1001} \equiv 2^{125(8)+1} \equiv (2^8)^{125}(2) \equiv 1(2) \equiv 2 \pmod{15}. \quad \square$$

The following special case is better known.

2.2.5 Fermat's Little Theorem. *Let $p \in \mathbb{Z}$ be a positive prime. For all $m \in \mathbb{Z}$, we have $[m]_p^p = [m]_p$. Equivalently, for all $m \in \mathbb{Z}$ that is not divisible by p , we have $m^{p-1} \equiv 1 \pmod{p}$.*

Pierre de Fermat stated this result in a letter dated October 18, 1640.

Proof. When $m \equiv 0 \pmod{p}$, we have $[m]_p^p = [0]_p = [m]_p$, so we may assume that m is not divisible by p . Since the positive integer p is prime, Theorem 2.1.4 shows that $\gcd(m, p) = 1$ and Lemma 2.2.2 shows that $\phi(p) = p - 1$. Theorem 2.2.3 yields $m^{p-1} \equiv 1 \pmod{p}$. $\square$

2.2.6 Lemma. *Let $p \in \mathbb{Z}$ be a positive prime. For all $m \in \mathbb{Z}$ such that $m^2 \equiv 1 \pmod{p}$, we have $m \equiv \pm 1 \pmod{p}$.*

Proof. The hypothesis $m^2 \equiv 1 \pmod{p}$ implies that

$$m^2 - 1 = (m - 1)(m + 1) \equiv 0 \pmod{p}.$$

From the definition of a prime, we deduce that $m - 1 \equiv 0 \pmod{p}$ or $m + 1 \equiv 0 \pmod{p}$. $\square$

2.2.7 Theorem (Wilson). *For every positive prime $p \in \mathbb{Z}$, we have*

$$(p - 1)! \equiv -1 \pmod{p}.$$

Proof. By Theorem 2.1.4, each element in the set $\{1, 2, \dots, p - 1\}$ has a unique multiplicative inverse in $\mathbb{Z}/\langle p \rangle$. From Lemma 2.2.6, we see that the only elements m in this set for which $[m]_p^2 = [1]_p$ are 1 and $p - 1$. Since the product of any element and its multiplicative inverse is $[1]_p$, the only two number that contribute to the product are 1 and $p - 1$. It follows that

$$(p - 1)! \equiv (1)(2)(3) \cdots (p - 1) \equiv (1)(p - 1) \equiv p - 1 \pmod{p}. \quad \square$$

This theorem was stated by Ibn al-Haytham circa 1000 and by John Wilson around 1770. It seems that the first proof appears in J.L. Lagrange, *Démonstration d'un théorème nouveau concernant les nombres premiers*, Nouv. Mém. Acad. Roy. Sci. Belles-Lettres Berlin, (1771) 125–137.

2.2.8 Remark. For small primes, we illustrate the partnering in the proof of the Wilson Theorem:

$1 \equiv 1$	$\pmod{2}$
$2! \equiv (1)(2) \equiv 2$	$\pmod{3}$
$4! \equiv (1)((2)(3))(4) \equiv 4$	$\pmod{5}$
$6! \equiv (1)((2)(4))((3)(5))(6) \equiv 6$	$\pmod{7}$
$10! \equiv (1)((2)(6))((3)(4))((5)(9))((7)(8))(10) \equiv 10$	$\pmod{11}$
$12! \equiv (1)((2)(7))((3)(9))((4)(10))((5)(8))((6)(11))(12) \equiv 12$	$\pmod{13}$
$16! \equiv (1)((2)(9))((3)(6))((4)(13))((5)(7))((8)(15))((10)(12))((11)(14))(16) \equiv 16$	$\pmod{17}$

3 Rings

Copyright © 2026, Gregory G. Smith
Last Updated: 2026-09-29

Commutative rings were conceived as a common generalization of algebraic structures in number theory, invariant theory, and the study of polynomial equations. Their **conceptualization** began in the 1870s and culminated in the 1920s.

3.0 Rings: mostly commutative

What algebraic structure unites the integers and polynomials?

3.0.0 Definition. A ring R is a set with two binary operations (called addition and multiplication) such that, for all elements $a, b, c \in R$, we have the following properties:

(associativity of addition)	$(a + b) + c = a + (b + c),$
(commutativity of addition)	$a + b = b + a,$
(existence of additive identity)	$a + 0 = a,$
(existence of additive inverses)	$a + (-a) = 0,$
(left distributivity)	$a(b + c) = ab + ac,$
(right distributivity)	$(a + b)c = ac + bc,$
(associativity of multiplication)	$a(bc) = (ab)c,$
(existence of multiplicative identity)	$1a = a1 = a.$

The ring R is *commutative* if it has the additional property:

(commutativity of multiplication)	$ab = ba.$
-----------------------------------	------------

3.0.1 Problem. Prove or disprove: the set $\mathbb{N}$ of nonnegative integers is not a ring under the usual operations.

Solution. The nonnegative integers satisfy all of the commutative ring axioms except for the existence of additive inverses. For instance, the number 1 has no additive inverse in $\mathbb{N}$. $\square$

3.0.2 Remark. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all commutative rings under the usual addition and multiplication.

3.0.3 Remark. For all $\ell \in \mathbb{N}$, Theorem 2.1.0 shows that the quotient $\mathbb{Z}/\langle \ell \rangle$ is a commutative ring under the addition and multiplication inherited from the set $\mathbb{Z}$.

We enumerate the basic properties of rings.

3.0.4 Proposition (Basic properties). *Let R be a ring.*

(unique 0) *There is a unique additive identity 0.*

(unique 1) *There is a unique multiplicative identity 1.*

(zero products) *For all $a \in R$, we have $0a = a0 = 0$.*

(unique inverse) *Every element in R has a unique additive inverse.*

(-1 products) *For the additive inverse $-a$, we have $(-1)(-a) = a$.*

Proof. Suppose 0 and 0' are additive identities in R . Their defining property, combined with the commutativity of addition, shows that $0 = 0 + 0' = 0' + 0 = 0'$.

David Hilbert introduced the word “ring” (more precisely, “number ring” or “Zahlring”) into mathematics. Rather than a ‘hollow circular object’, think of a network or organization acting to further its own interests, such as a *criminal ring* or *spy ring*, or an enclosed space such as a *circus ring* or *boxing ring*.

Contrary to some antiquated sources, rings *always* have a multiplicative identity 1. A compelling argument for this convention appears in B. Poonen, *Why All Rings Should Have a 1*, Math. Mag., 92 (2019) 58–62.

The symbols “0” and “1” are used to denote the additive and multiplicative identities in the ring R . These distinguished elements in R may not be the same as the integers 0 and 1.

Suppose 1 and $1'$ are multiplicative identities in R . Their defining property gives $1 = (1)(1') = 1'$.

For all $a \in R$, the additive identity and distributivity properties imply that $0a = (0+0)a = 0a + 0a$ and $a0 = a(0+0) = a0 + a0$. Adding the additive inverse $-0a$ to both sides of these equations gives $0a = 0$ and $a0 = 0$.

Suppose that b and c are additive inverses of an element a in R . Using the additive identity, additive inverse, associativity of addition and commutativity of addition gives

$$\begin{aligned} b &= b + 0 = b + (a + c) = (b + a) + c \\ &= (a + b) + c = 0 + c = c + 0 = c. \end{aligned}$$

For all $a \in R$, the additive-inverse and distributivity properties imply that $0 = 0(-a) = (-1+1)(-a) = (-1)(-a) + (-a)$. Adding a to both sides, the additive inverse and additive identity properties give $(-1)(-a) = a$. $\square$

3.0.5 Remark. Suppose that R is a ring with $1 = 0$. For all $a \in R$, we have $a = 1a = 0a = 0$, so R consists of a single element. This commutative ring is called the *zero ring*.

3.0.6 Remark. Let R be a commutative ring. For every $n \in \mathbb{N}$, the set $\text{Mat}(n, R)$ of all $(n \times n)$ -matrices with entries in R forms a ring. It is noncommutative whenever $n > 1$. When $n = 2$, we have

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

3.0.7 Definition. Polynomials in the indeterminate (or variable) x with coefficients in a commutative ring R form the commutative ring $R[x]$. The polynomials f and g in $R[x]$ have the form

$$\begin{aligned} f &:= a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0 & \text{and} \\ g &:= b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0 \end{aligned}$$

where the coefficients $a_m, a_{m-1}, \dots, a_0, b_n, b_{n-1}, \dots, b_0$ are elements in R , and m and n are nonnegative integers.

Addition in $R[x]$ is defined by

$$f + g = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0).$$

Associativity and commutativity of addition, and the existence of an additive identity and an additive inverse are all inherited from the corresponding property in the coefficient ring R .

Multiplication in $R[x]$ is defined by

$$fg = (a_m b_n)x^{m+n} + (a_m b_{n-1} + a_{m-1} b_n)x^{m+n-1} + \cdots + a_0 b_0;$$

for every $i \in \mathbb{N}$, the coefficient of the monomial x^i in the product is the sum $\sum_{j=0}^i a_{i-j} b_j$ in R . Distributivity in $R[x]$ just relies on the corresponding property in R . The associativity of multiplication, the existence of a multiplicative identity, and the commutativity of multiplication in $R[x]$ all depend on distributivity in R as well as the corresponding property in R .

Since every ring has an additive identity and a multiplicative identity, the zero ring is the smallest ring. In particular, the empty set cannot be equipped with the structure of a ring.

The word 'polynomial' first appears in English in 1696 in *Arithmetic* by Samuel Jeake. The original meaning was just an expression consisting of many terms.

By including terms in f or g with 0 as the coefficient, we may assume that $n \geq m$.

3.1 Examples of Rings

How do we get new rings from old ones? Functions with values in a ring produce new rings.

3.1.0 Definition. Let R be a ring and let $\mathcal{X}$ be a nonempty set. The set $R^{\mathcal{X}}$ of all maps from $\mathcal{X}$ to R , with the pointwise addition and multiplication, is itself a ring. For all $f: \mathcal{X} \rightarrow R$ and $g: \mathcal{X} \rightarrow R$, we have $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for all $x \in \mathcal{X}$. The constant function $x \mapsto 0_R$ is the additive identity and the constant function $x \mapsto 1_R$ is the multiplicative identity. When R is commutative, the ring of functions is also commutative.

Many “ring-like” structures without a multiplicative identity do occur, especially in analysis. Focusing on functions with compact support or using convolution as the product are natural examples.

A substructure is one of the most basic ideas in mathematics.

3.1.1 Definition. A subset S of a ring R is a *subring* if restricting the addition and multiplication on R to S produces a ring structure on S with the same additive and multiplicative identities.

3.1.2 Proposition. A nonempty subset S of a ring R is a subring if and only if the following three properties hold:

(differences) For all $f, g \in S$, the element $f - g$ is also in S .

(products) For all $f, g \in S$, the element fg is also in S .

(identity) The multiplicative identity 1_R is also in S .

Proof. Suppose that S is a subring of R . Each element g in S has an additive inverse $-g$ and the sum $f - g$ of the elements f and $-g$ in S is also in S . The product fg of elements f and g in S is also in S . Finally, the subring S has the same multiplicative identity as R , so the element 1_R belongs to S .

Conversely, suppose that S satisfies the three properties. Since associativity of addition, commutativity of addition, associativity of multiplication, and distributivity are inherited directly from the ring R , the binary operations on S induce a ring structure if and only if the following five conditions are satisfied:

(closure of addition) For all $f, g \in S$, the sum $f + g$ is in S .

(additive identity) The additive identity 0_R is in S .

(additive inverses) For all $f \in S$, we have $-f \in S$.

(closure of multiplication) For all $f, g \in S$, we have $fg \in S$.

(multiplicative identity) The multiplicative identity 1_R is in S .

As S is nonempty, there exists $f \in S$ and the first property implies that $0_R = f - f \in S$. For all $g \in S$, the first property establishes that $-g = 0_R - g \in S$. For all $f, g \in S$, we have $-g \in S$ and the first property gives $f + g = f - (-g) \in S$. Thus, the first property establishes the first three conditions. Finally, the last two properties are the last two conditions. $\square$

3.1.3 Remark. The inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are all subrings. Every subring of the integers $\mathbb{Z}$ or the quotient $\mathbb{Z}/\langle \ell \rangle$ contains 1 and hence must be equal to the whole ring.

3.1.4 Definition. The subset $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ forms a subring called the *Gaussian integers*.

3.1.5 Problem. Draw the multiples of the Gaussian integer $1 + 2i$.

Solution. Since $\arctan(2) \approx 1.10715\dots$, we see that

$$1 + 2i = \sqrt{5}(\cos(1.10715\dots) + i \sin(1.10715\dots)).$$

Multiples of $1 + 2i$ are obtained by scaling the Gaussian integers by $\sqrt{5}$ and rotating them counterclockwise by $1.10715\dots$ radians. The larger black circles in Figure 3.1 are the multiples of $1 + 2i$. $\square$

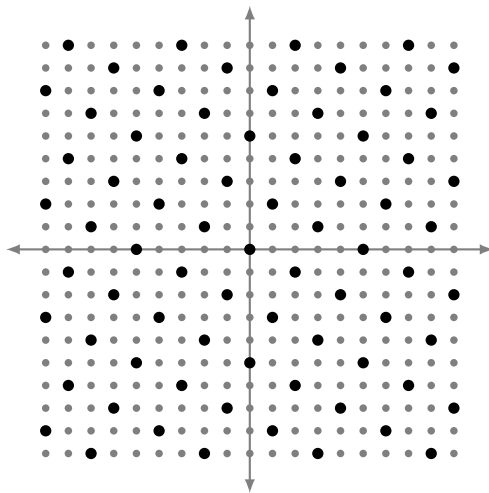


Figure 3.1: Multiples of the Gaussian integer $1 + 2i$

3.1.6 Definition. Let $\omega := \cos(2\pi/3) + i \sin(2\pi/3)$, so $\omega^2 = -1 - \omega$ and $\omega^3 = 1$. The subset $\mathbb{Z}[\omega] := \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ forms a subring called the *Eisenstein integers*.

We close by introducing a numerical invariant of a ring.

3.1.7 Definition. The *characteristic* of a ring R is the minimum positive number of terms equal to the multiplicative identity 1_R in R that sum to the additive identity 0_R in R . In other words, it is the smallest positive integer n such that

$$n 1_R = \underbrace{1_R + 1_R + \dots + 1_R}_{n \text{ times}} = 0_R.$$

When no such positive integer exists, the characteristic is 0.

3.1.8 Remark. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all of characteristic zero. For any positive $\ell \in \mathbb{N}$, the characteristic of the quotient $\mathbb{Z}/\langle \ell \rangle$ is ℓ .

3.1.9 Problem. When R has characteristic n , prove that, for every $a \in R$, we have $na = 0$

Proof. For all $a \in R$, the multiplicative identity, the associativity of multiplication, and the definition of characteristic give

$$na = n(1_R a) = (n 1_R) a = 0_R a = 0. \quad \square$$

Multiplication in the Eisenstein integers is given by

$$\begin{aligned} (a + b\omega)(c + d\omega) &= ac + (bc + ad)\omega + bd\omega^2 \\ &= (ac - bd) + (bc + ad - bd)\omega. \end{aligned}$$

3.3 Exercises

3.3.1 Problem. Determine which of the following statements are true. If a statement is false, provide a counterexample and, if possible, salvage it by modifying the statement so that it becomes true.

- i. A ring can be finite or infinite.
- ii. In every ring multiplication must be commutative.
- iii. In every ring addition must be commutative.
- iv. Every ring has a multiplicative identity
- v. Every ring has an additive identity.
- vi. The zero ring satisfies the axioms of a commutative ring.
- vii. For every ring R and every set $\mathcal{X}$, every nonzero element in $R^{\mathcal{X}}$ has a multiplicative inverse.
- viii. Every subring of a commutative ring is also commutative.
- ix. Every subring of a domain is also a domain.
- x. Every subring of a field is also a field.
- xi. A ring may have zerodivisors.
- xii. A field may have zerodivisors.
- xiii. Every domain is a field.
- xiv. Every field is a ring.
- xv. Every field has infinitely many elements.

3.3.2 Problem. Let $\mathcal{X}$ be a set. The *power set* $P(\mathcal{X})$ of $\mathcal{X}$ consists of all subsets of $\mathcal{X}$. For any two sets $\mathcal{A}$ and $\mathcal{B}$ in $P(\mathcal{X})$, the *symmetric difference* is $\mathcal{A} \triangle \mathcal{B} := (\mathcal{A} \setminus \mathcal{B}) \cup (\mathcal{B} \setminus \mathcal{A}) = (\mathcal{A} \cup \mathcal{B}) \setminus (\mathcal{A} \cap \mathcal{B})$. Determine whether the set $P(\mathcal{X})$ with the operators of addition and multiplication defined, for all subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathcal{X}$, by $\mathcal{A} \triangle \mathcal{B} := \mathcal{A} \triangle \mathcal{B}$ and $\mathcal{A} \triangle \mathcal{B} := \mathcal{A} \cap \mathcal{B}$, forms a commutative ring. If it is not, then list all of the defining axioms that fail to hold.

3.3.3 Problem. Determine whether the set $\mathbb{R} \cup \{\infty\}$ with addition and multiplication defined, for all x and y in $\mathbb{R} \cup \{\infty\}$, by $x \boxplus y := \min(x, y)$ and $x \boxtimes y := x + y$, forms a commutative ring. If it is not, then list all of the defining axioms that fail to hold.

3.3.4 Problem. Let R be a commutative ring and fix a nonnegative integer n . For any elements a and b in R , prove that

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}.$$

3.3.5 Problem. Let $\mathbb{F}_4$ denote the subset of all (2×2) -matrices of the form

$$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$$

where a and b are ring elements in the quotient $\mathbb{Z}/\langle 2 \rangle$.

- i. Show that $\mathbb{F}_4$ is a subring of the ring $\text{Mat}(n, n, \mathbb{Z}/\langle 2 \rangle)$ formed by (2×2) -matrices with entries in the quotient $\mathbb{Z}/\langle 2 \rangle$.
- ii. Verify that $\mathbb{F}_4$ is a commutative ring.
- iii. Demonstrate that every nonzero element in the ring $\mathbb{F}_4$ has a multiplicative inverse.

3.3.6 Problem. Let $\mathbb{F}_3 := \mathbb{Z}/\langle 3 \rangle$ denote the field with three elements. Consider the commutative ring

$$\mathbb{F}_3[i] := \{a + bi \mid a, b \in \mathbb{F}_3 \text{ and } i^2 \equiv -1 \equiv 2 \pmod{3}\}.$$

Verify that $\mathbb{F}_3[i]$ is a field.

3.3.7 Problem. Let $\mathbb{F}_5 := \mathbb{Z}/\langle 5 \rangle$ denote the field with five elements. Consider the commutative ring

$$\mathbb{F}_5[i] := \{a + bi \mid a, b \in \mathbb{F}_5 \text{ and } i^2 \equiv -1 \equiv 4 \pmod{5}\}.$$

Confirm that $\mathbb{F}_5[i]$ is not a domain.

3.3.8 Problem. Assume that the commutative ring R is a domain. Prove that R has characteristic 0 or has characteristic p where p is a positive prime number. When R has characteristic 0, show that it has a subring isomorphic to $\mathbb{Z}$. When R has characteristic p , show that it has a subring isomorphic to $\mathbb{Z}/\langle p \rangle$.