

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

How do multiplicative inverses impact products within modular arithmetic? The section highlights a few famous formula.

Definition 2.3.0. For any positive integer m, the *totient* $\phi(m)$ of m is the number of positive integers coprime to m;

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

The article, James Joseph Sylvester, On Certain Ternary Cubic-Form Equations, American Journal of Mathematics **2** (1879) 357–393, created the word "totient".

Remark 2.3.1. For the first few positive integers, the totient is:

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

Lemma 2.3.2. *A positive integer p is prime if and only if $\phi(p) = p - 1$.*

Proof. Let p be a positive integer.
$\Rightarrow$: Suppose that p is prime. By combining Proposition 2.1.4, Lemma 2.2.2, and Theorem 2.2.4, we see that the integers $\{1, 2, \dots, p-1\}$ are all coprime to p, so $\phi(p) = p - 1$.
$\Leftarrow$: Suppose that $\phi(p) = p - 1$. It follows that the integers $\{1, 2, \dots, p-1\}$ are all coprime to p. Thus, Lemma 2.2.2 and Theorem 2.2.4 establish that p is prime. □

Theorem 2.3.3 (Totient). *Let ℓ be a positive integer. For any integer m coprime to ℓ, we have $m^{\phi(\ell)} \equiv 1 \mod \ell$.*

Leonhard Euler published a proof of this theorem in 1763.

Proof. Let $\{n_1, n_2, \dots, n_{\phi(\ell)}\} = \{n \in \mathbb{N} \mid 1 \leqslant n \leqslant \ell \text{ and } \gcd(n, \ell) = 1\}$. 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 2.2.2 shows that $[m]_\ell$ has multiplicative inverse in $\mathbb{Z}/\langle \ell \rangle$. Hence, for any integers i and j such that $1 \leqslant i, j \leqslant \phi(\ell)$, we have $[m\, n_i]_\ell = [m\, n_j]_\ell$ if and only if $[n_i]_\ell = [n_j]_\ell$. As $1 \leqslant n_i < \ell$ and $1 \leqslant n_j < \ell$, Proposition 2.1.4 establishes that $[n_i]_\ell = [n_j]_\ell$ if and only if $i = j$.

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

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

list the same nonzero congruence classes (possibly in a different order). Thus, we deduce that

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

Because $\gcd(n_1\, n_2 \cdots n_{\phi(\ell)}, \ell) = 1$, Lemma 2.2.2 also shows 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 $m^{\phi(\ell)} \equiv 1 \mod \ell$. □

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 $[7^4]_{10} = [1]_{10}$.

Problem 2.3.4. Simplify $2^{1001} \bmod 15$.

Proof. We can apply the Totient Theorem because $\gcd(2, 15) = 1$. The integers n satisfying $1 \leqslant n \leqslant 15$ and $\gcd(n, 15) = 1$ are $\{1, 2, 4, 7, 8, 11, 13, 14\}$, so $\phi(15) = 8$. Since $2^8 \equiv 1 \bmod 15$ and $1001 = 125(8) + 1$, we obtain

$$2^{1001} \equiv 2^{125(8)+1} \equiv (2^8)^{125}(2) \equiv 1(2) \equiv 2 \mod 15\,. \qquad \square$$

The following special case is better known.

Corollary 2.3.5 (Fermat's Little Theorem)**.** *Let p be a positive prime integer. For any integer m, we have $[m]_p^p = [m]_p$. Equivalently, for any integer m that is not divisible by p, we have $m^{p-1} \equiv 1 \bmod p$.*

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

Proof. When $m \equiv 0 \bmod p$, we have $[m]_p^p = [0]_p = [m]_p$, so we may assume that m is not divisible by p. Since p is positive prime, Theorem 2.2.4 shows that $\gcd(m, p) = 1$ and Lemma 2.3.2 establishes that $\phi(p) = p - 1$. Hence, the Totient Theorem 2.3.3 yields $m^{p-1} \equiv 1 \bmod p$. $\square$

Lemma 2.3.6. *Let p be a positive prime integer. For any integer m satisfying $m^2 \equiv 1 \bmod p$, we have $m \equiv \pm 1 \bmod p$.*

Proof. The hypothesis $m^2 \equiv 1 \bmod p$ implies that

$$m^2 - 1 = (m-1)(m+1) \equiv 0 \mod p\,.$$

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

Theorem 2.3.7 (Wilson)**.** *For any positive prime integer p, we have $(p-1)! \equiv -1 \bmod p$.*

This theorem was stated by Ibn al-Haytham circa 1000 and by John Wilson around 1770. It seems that Joseph-Louis Lagrange gave the first proof in 1771.

Proof. By Theorem 2.2.4, each element in the set $\{1, 2, \dots, p-1\}$ has a unique multiplicative inverse in $\mathbb{Z}/\langle p \rangle$. From Lemma 2.3.6, 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

$$(p-1)! \equiv (1)(2)(3)\cdots(p-1) \equiv (1)(p-1) \equiv p - 1 \mod p\,. \qquad \square$$

Remark 2.3.8. For small primes, we illustrate the partnering in the proof of the Wilson Theorem:

$$\begin{aligned}
1 &\equiv 1 && \bmod 2 \\
2! &\equiv (1)(2) \equiv 2 && \bmod 3 \\
4! &\equiv (1)\big((2)(3)\big)(4) \equiv 4 && \bmod 5 \\
6! &\equiv (1)\big((2)(4)\big)\big((3)(5)\big)(6) \equiv 4 && \bmod 7 \\
10! &\equiv (1)\big((2)(6)\big)\big((3)(4)\big)\big((5)(9)\big)\big((7)(8)\big)(10) \equiv 10 && \bmod 11 \\
12! &\equiv (1)\big((2)(7)\big)\big((3)(9)\big)\big((4)(10)\big)\big((5)(8)\big)\big((6)(11)\big)(12) \equiv 12 && \bmod 13 \\
17! &\equiv (1)\big((2)(9)\big)\big((3)(6)\big)\big((4)(13)\big)\big((5)(7)\big)\big((8)(15)\big)\big((10)(12)\big)\big((11)(14)\big)(16) \equiv 16 && \bmod 17
\end{aligned}$$

Exercises

Problem 2.3.9. Demonstrate that the equation $x^6 + y^{12} = 703$ has no integer solutions.

Problem 2.3.10. Let ℓ be a reducible integer such that $\ell > 4$. Verify that $(\ell - 1)! \equiv 0 \mod \ell$.

Problem 2.3.11. Let p be a positive prime integer having the form $p = 2k + 1$ for some integer k. Prove that $(k!)^2 \equiv (-1)^{k+1} \mod p$.

3 *Rings*

Rings were originally devised as a common generalization for algebraic structures in number theory, invariant theory, and the study of polynomial equations. Their conceptualization began in 1870s and culminated in 1920s.

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 their own interests such as a *criminal ring* or *spy ring*, or an enclosed space such as a *circus ring* or *boxing ring*.

3.0 Rings: mostly commutative

What algebraic structure unites the integers and polynomials?

Definition 3.0.0. A *ring* R is a nonempty set with two binary operations, called addition and multiplication, such that, for any elements a, b, and c, we have the following properties:

$$\begin{aligned}
(a+b)+c &= a+(b+c) && \text{(associativity of addition)}\\
a+b &= b+a && \text{(commutativity of addition)}\\
a+0 &= a && \text{(existence of additive identity)}\\
a+(-a) &= 0 && \text{(existence of additive inverses)}\\
a\,(b\,c) &= (a\,b)\,c && \text{(associativity of multiplication)}\\
1\,a = a\,1 &= a && \text{(existence of multiplicative identity)}\\
a\,(b+c) &= a\,b+a\,c && \text{(distributivity)}\\
(a+b)\,c &= a\,c+b\,c
\end{aligned}$$

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

$$a\,b = b\,a \qquad \text{(commutativity of multiplication)}$$

Contrary to some antiquated sources, rings *always* have a multiplicative identity 1. A compelling argument for this convention is provided in Bjorn Poonen, Why All Rings Should Have a 1, Mathematics Magazine **92** (2019) 58–62.

Example 3.0.1. The set $\mathbb{N}$ of nonnegative integers is not a ring under the usual operations. It satisfies all of the commutative ring axioms except for the existence of additive inverses.

Example 3.0.2. Sets of numbers including $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all commutative rings under the usual addition and multiplication.

Example 3.0.3. For any nonnegative integer ℓ, the quotient $\mathbb{Z}/\langle \ell \rangle$ is a commutative ring where addition and multiplication are inherited from the set $\mathbb{Z}$ of integers.

We enumerate the basic properties of rings.

Proposition 3.0.4. *Let R be a ring.*

(i) *For any element a in R, we have $0\,a = a\,0 = 0$.*
(ii) *Every element in R has a unique additive inverse.*
(iii) *Given the additive inverse $-a$ of $a \in R$, we have $(-1)(-a) = a$.*
(iv) *There is a unique additive identity 0.*
(v) *There is a unique multiplicative identity 1.*

Proof. Let a be an element in the ring R.

(i) The additive identity and distributivity properties imply that $0\,a = (0+0)a = 0\,a + 0\,a$. Adding the additive inverse $-0\,a$ to both sides gives $0\,a = 0$. Similarly, the equalities $a\,0 = a(0+0) = a\,0 + a\,0$ imply that $0\,a = 0$.

(ii) Suppose that b and c are additive inverses of a. Using additive identity, additive inverse, associativity of addition abd commutativity of addition gives

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

(iii) The additive inverse and distributivity properties imply that $0 = (-1 + 1)(-a) = (-1)(-a) + (-a)$. Adding a to both sides, the additive inverse and additive identity properties give $(-1)(-a) = a$.

(iv) Suppose 0 and $0'$ are both additive identities in R. The additive identity property and commutative of addition give $0 = 0 + 0' = 0' + 0 = 0'$.

(v) Suppose 1 and $1'$ are both multiplicative identities in R. The multiplicative identity property gives $1 = 1\,1' = 1'$. □

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

Example 3.0.6. Let R be a commutative ring. For any two positive integers m and n, the set $\mathrm{M}_{m,n}(R)$ of all $(m \times n)$-matrices with entries in R forms a ring. It is non-commutative when $m\,n > 1$. For instance, when $m = n = 2$, we have

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

Definition 3.0.7. 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

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

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

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.

Addition in $R[x]$ is defined by

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

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

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

Multiplication in $R[x]$ is defined by

$$f\,g = (a_n\,b_m)x^{n+m} + (a_n\,b_{m-1} + a_{n-1}\,b_m)x^{n+m-1} + \cdots + a_0\,b_0\,;$$

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

Exercises

Problem 3.0.8. Let $\mathcal{X}$ be a set. The *power set* $\mathrm{P}(\mathcal{X})$ of $\mathcal{X}$ consists of all subsets of $\mathcal{X}$. For any two sets $\mathcal{A}$ and $\mathcal{B}$ in $\mathrm{P}(\mathcal{X})$, the *symmetric difference* is $\mathcal{A} \bigtriangleup \mathcal{B} := (\mathcal{A} \setminus \mathcal{B}) \cup (\mathcal{B} \setminus \mathcal{A}) = (\mathcal{A} \cup \mathcal{B}) \setminus (\mathcal{A} \cap \mathcal{B})$.

Determine whether the set $\mathrm{P}(\mathcal{X})$ with addition and multiplication defined, for all subsets $\mathcal{A}$ and $\mathcal{B}$ of $\mathcal{X}$, by

$$\mathcal{A} \mathbin{\triangle\!\!\!\!\!+} \mathcal{B} := \mathcal{A} \bigtriangleup \mathcal{B} \qquad \text{and} \qquad \mathcal{A} \mathbin{\triangle\!\!\!\!\times} \mathcal{B} := \mathcal{A} \cap \mathcal{B}\,,$$

forms a commutative ring. If it is not, then list all of the defining axioms that fail to hold.

Problem 3.0.9. Determine whether the set $\mathbb{R} \cup \{\infty\}$ with addition and multiplication defined, for all x and y in $\mathbb{R} \cup \{\infty\}$, by

$$x \boxplus y := \min(x, y) \qquad \text{and} \qquad x \boxtimes y := x + y\,,$$

forms a commutative ring. If it is not, then list all of the defining axioms that fail to hold.

3.1 Examples of Rings

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

Example 3.1.0. Let R be a ring and let $\mathcal{X}$ be a nonempty set. The set of maps from $\mathcal{X}$ to R equipped with the pointwise addition and multiplication is itself a ring. For all functions $f, g \colon \mathcal{X} \to R$, we have $(f+g)(x) = f(x) + g(x)$ and $(f\,g)(x) = f(x)\,g(x)$. 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 algebra.

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

Proposition 3.1.2. *A nonempty subset S of a ring R is a subring if and only if the following three properties hold.*
- *For any two elements f and g in S, the element $f - g$ is also in S.*
- *For any two elements f and g in S, the element $f\,g$ is also in S.*
- *The multiplicative identity 1_R is also in S.*

Proof. Let f, g, and h be elements in S.

$\Rightarrow$: 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 two elements f and $-g$ in S is also in S. The product $f\,g$ of two elements f and g in S is also in S. Finally, the subring S has the same multiplicative identity as R, so 1_R belongs to S.

$\Leftarrow$: 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 induces a ring structure if and only if the following five conditions are satisfied:
(closure of addition) For any f and g in S, the sum $f + g$ is in S.
(additive identity) The additive identity 0_R is in S.
(additive inverses) For any f in S, the additive inverse $-f \in S$.
(closure of multiplication) For any $f, g \in S$, we have $f\,g \in S$.
(multiplicative identity) The multiplicative identity 1_R is in S.
Since S is nonempty, there exists $f \in S$ and the first property implies that $0_R = f - f \in S$. For any g in S, the first property establishes that $-g = 0_R - g \in S$. For any f and 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 3 conditions. Finally, the last two properties are the last two conditions. □

Example 3.1.3. 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.

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

Problem 3.1.5. Draw the multiples of the Gaussian integer $1 + 2\,\mathrm{i}$.

Solution. Since $\arctan(2) \approx 1.1071487\ldots$, we see that

$$1 + 2\,\mathrm{i} = \sqrt{5}\big(\cos(1.1071487) + \mathrm{i}\,\sin(1.071487)\big)\,.$$

It follows that multiples of $1 + 2\,\mathrm{i}$ are obtained by scaling the Gaussian integers by $\sqrt{5}$ and rotating them counterclockwise by $1.07187\ldots$ radians. The larger black circles in Figure 3.1 are the multiples of $1 + 2\,\mathrm{i}$. □

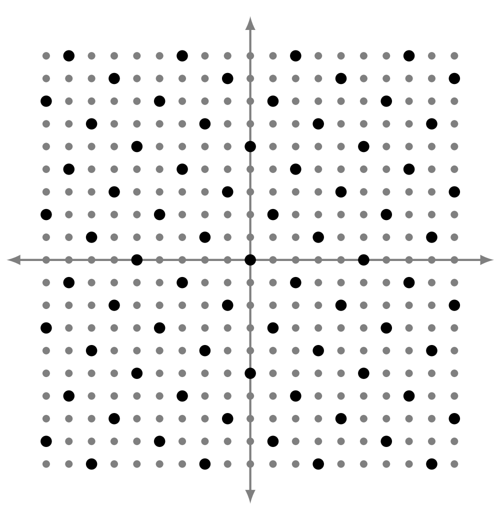

Figure 3.1: Multiples of the Gaussian integer $1 + 2\,\mathrm{i}$

Definition 3.1.6. The *characteristic* of a ring R is the smallest positive integer n such that

$$n\,1_R = \underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}} = 0_R\,;$$

if no such positive integer exists, then the characteristic is 0.

For $0 \in \mathbb{Z}$, we always have $0\,1_R = 0_R$. It follows that, for any ring R of characteristic n, we have $n\,1_R = 0_R$.

Example 3.1.7. The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all of characteristic zero. For any positive integer ℓ, the characteristic of the quotient ring $\mathbb{Z}/\langle \ell \rangle$ is ℓ.

Problem 3.1.8. When R has characteristic n, prove that, for any ring element a in R, we have $n\,a = 0$

Proof. For any ring element a in R, the multiplicative identity, the associativity of multiplication, and the definition of characteristic give $n\,a = n(1_R\,a) = (n\,1_R)\,a = 0_R\,a = 0$. □

Exercises

Problem 3.1.9. Let R be a commutative ring and let n be a nonnegative integer. For any ring elements a and b in R, prove that

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

Problem 3.1.10. Let $\mathbb{F}_4$ denote the subset of all (2×2)-matrices having 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)** Demonstrate that $\mathbb{F}_4$ is a subring of the ring formed by all (2×2)-matrices with entries in the quotient $\mathbb{Z}/\langle 2 \rangle$.
- **(ii)** Verify that $\mathbb{F}_4$ is a commutative ring.
- **(iii)** Show that any nonzero element in $\mathbb{F}_4$ has a multiplicative inverse.