# GALOIS THEORY TOPIC IV
# MODULAR ARITHMETIC

PAUL L. BAILEY

Abstract. Modular arithmetic involves computing remainders upon addition and multiplication, and has wide ranges applications. Our interest in modular arithmetic is its uses for study polynomials with integer coefficients, which will come in the next topic.

## 1. Congruence Modulo $n$

**Definition 1.** Let $n \in \mathbb{Z}$ with $n \geq 2$. Let $a, b \in \mathbb{Z}$. We say that $a$ *is congruent to* $b$ *modulo* $n$, and write $a \equiv b \pmod{n}$, if the difference $a - b$ is divisible by $n$:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid (a - b).$$

**Proposition 1.** *Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $a, b, c \in \mathbb{Z}$. Then*

- **(a)** *$a \equiv a \pmod{n}$ (Reflexivity);*
- **(b)** *if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$ (Symmetry);*
- **(c)** *if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$ (Transitivity).*

*Proof.*
(*Reflexivity*) Note that $0 \cdot n = 0 = a - a$; thus $n \mid (a - a)$, so $a \equiv a$. Therefore $\equiv$ is reflexive.
(*Symmetry*) Let $a, b \in \mathbb{Z}$. Suppose that $a \equiv b$; then $n \mid (a - b)$. Then there exists $k \in \mathbb{Z}$ such that $nk = a - b$. Then $n(-k) = b - a$, so $n \mid (b - a)$. Thus $b \equiv a$. Similarly, $b \equiv a \Rightarrow a \equiv b$. Therefore $\equiv$ is symmetric.
(*Transitivity*) Let $a, b, c \in \mathbb{Z}$, and suppose that $a \equiv b$ and $b \equiv c$. Then $nk = a - b$ and $nl = b - c$ for some $k, l \in \mathbb{Z}$. Then $a - c = nk - nl = n(k - l)$, so $n \mid (a - c)$. Thus $a \equiv c$. Therefore $\equiv$ is transitive. □

**Proposition 2.** *Let $n \in \mathbb{N}$ and let $a_1, a_2 \in \mathbb{Z}$. By the Division Algorithm, there exist unique integers $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that*

- *$a_1 = nq_1 + r_1$, where $0 \leq r_1 < n$;*
- *$a_2 = nq_2 + r_2$, where $0 \leq r_2 < n$.*

*Then $a_1 \equiv a_2 \pmod{n}$ if and only if $r_1 = r_2$.*

*Proof.*
($\Rightarrow$) Suppose that $a_1 \equiv a_2$. Then $n \mid (a_1 - a_2)$. This means that $nk = a_1 - a_2$ for some $k \in \mathbb{Z}$. But $a_1 - a_2 = n(q_1 - q_2) + (r_1 - r_2)$. Then $n(k + q_1 - q_2) = r_1 - r_2$, so $n \mid r_1 - r_2$.

Multiplying the inequality $0 \leq r_2 < n$ by $-1$ gives $-n < -r_2 \leq 0$. Adding this inequality to the inequality $0 \leq r_1 < n$ gives $-n < r_1 - r_2 < n$. But $r_1 - r_2$ is an integer multiple of $n$; the only possibility, then, is that $r_1 - r_2 = 0$. Thus $r_1 = r_2$.

---

*Date*: October 16, 2006.

($\Leftarrow$) Suppose that $r_1 = r_2$. Then $a_1 - a_2 = nq_1 - nq_2 = n(q_1 - q_2)$. Thus $n \mid (a_1 - a_2)$, so $a_1 \equiv a_2$. $\square$

## 2. The Residue Map

Let $n \in \mathbb{Z}$ with $n \geq 2$. For each $a \in \mathbb{Z}$, there is a unique $r$ in the range $0 \leq r < n$ such that $r$ is congruent to $a$ modulo $n$. We say that $r$ *represents* $a$, and we see that, if $b$ is congruent to $a$, then $r$ represents $b$ also. To study this, it is convenient to focus on the set of possible representatives.

**Definition 2.** Let $n \in \mathbb{Z}$ with $n \geq 2$. The *set of integers modulo* $n$ is

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

Thus $\mathbb{Z}_n$ denotes the set of integers which are the possible remainders upon division by $n$. For example,

$$\mathbb{Z}_3 = \{0, 1, 2\} \quad \text{and} \quad \mathbb{Z}_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.$$

The next definition formalizes the function which takes an integer and returns its representative in $\mathbb{Z}_n$.

**Definition 3.** Let $n \in \mathbb{Z}$ with $n \geq 2$.

The *residue map modulo* $n$ is the function

$$\xi_n : \mathbb{Z} \to \mathbb{Z}_n \quad \text{given by} \quad \xi_n(a) = \text{ the remainder when } n \text{ is divided by } a.$$

We call $\xi_n(a)$ the *residue* of $a$ modulo $n$.

We restate Proposition 2 in terms of this function.

**Proposition 3.** *Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $a, b \in \mathbb{Z}$. Then*

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad \xi_n(a) = \xi_n(b).$$

We give some examples of where these concepts arise.

**Example 1.** If the time now is 5 pm, what time will it be in 87 hours?

*Solution.* Using a 24 hour clock, 5 pm is 17. Now compute modulo $n = 24$ to obtain

$$17 + 87 \equiv 104 \equiv 8 \pmod{24},$$

so the time in 87 hours will be 8 am. □

**Example 2.** If today is Thursday, what day will it be in 258 days?

*Solution.* Let's set 0 = Sunday, 1 = Monday, 2 = Tuesday, 3 = Wednesday, 4 = Thursday, 5 = Friday, and 6 = Saturday. Now compute modulo $n = 7$ to obtain

$$2 + 258 \equiv 260 \equiv 1 \pmod{7}.$$

Since 1 = Monday, it will be Monday in 258 days. □

**Example 3.** Let $i \in \mathbb{C}$ with $i^2 = -1$. Find $i^{1571}$.

*Proof.* Here, we compute modulo 4. Now $1571 = 4(392) + 3$, so

$$i^{1571} = i^{4(392)+3} = (i^4)^{392} i^3 = 1^{392} i^3 = i^3 = -i.$$

□

In Example 3, it was more convenient to avoid the congruence notation, and one finds that this is often the case. What matters is understanding congruence and its applications. As a matter of convenience, we *redefine* the operations of addition and multiplication on congruence representatives to always compute modulo $n$.

## 3. Modular Arithmetic

*Modular Arithmetic* is the study of addition and multiplication of the residues modulo $n$. To isolate this, we consider only the set of numbers from 0 to $n-1$, and define operations of addition and multiplication which are closed on this set.

**Definition 4.** Define operations of *addition modulo* $n$ and *multiplication modulo* $n$ on the set $\mathbb{Z}_n$ by

$$a + b \triangleq \xi_n(a+b) \quad \text{and } ab \triangleq \xi_n(ab),$$

where the symbol $\triangleq$ means "is defined to be".

It is important to keep in mind that for $a, b \in \mathbb{Z}_n$, when we write $a + b = \overline{a+b}$, the addition on the left is a *different operation* than the addition on the right; on the left is addition in $\mathbb{Z}_n$ (modulo $n$), and on the right it is addition in the integers. One must make the distinction from the context. Analogous remarks apply to multiplication.

The following properties of the residue map are critical in all that follows.

**Proposition 4.** *Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $a, b \in \mathbb{Z}$. Then*

**(a)** $\xi_n(a+b) = \xi_n(a) + \xi_n(b)$;
**(b)** $\xi_n(ab) = \xi_n(a)\xi_n(b)$.

*Proof.* Exercise. □

Again, we point out that, for example in **(b)**, in the equation

$$\xi_n(a+b) = \xi_n(a) + \xi_n(b),$$

the addition on the left is in $\mathbb{Z}$, whereas the addition on the right is in $\mathbb{Z}_n$, and is performed modulo $n$.

Just as the congruence notation becomes cumbersome, so does the residue notation; thus we use the following BAR notation when $n$ is understood. Let $n \in \mathbb{Z}$ with $n \geq 2$. For $a \in \mathbb{Z}$, let $\overline{a}$ denote the remainder when $a$ is divided by $n$. Also, for $a \in \mathbb{Z}_n$, let $-a$ denote the additive inverse of $a$, given by $a = \overline{n-a}$, so that $a + (-a) = 0$.

**Example 4.** Let $n = 7$. Then $\mathbb{Z}_n = \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. The following are modular computations in this set.

- $3 + 5 = \overline{3+5} = \overline{8} = 1$
- $-5 = \overline{-5} = \overline{7-5} = 2$, so $4 - 5 = 1 + 2 = 3$
- $3 \cdot 5 = \overline{15} = 1$
- $5^2 = \overline{25} = 4$

**Example 5.** Let $n = 12$. Then $\mathbb{Z}_n = \mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. The following are modular computations in this set.

- $4 + 8 = \overline{12} = 0$; thus $8 = -4$
- $8 + 11 = \overline{19} = 7$
- $6 \cdot 10 = \overline{60} = 0$
- $5 \cdot 7 = \overline{35} = 11$, which is $-1$
- $11^2 = 1$, since $11 = -1$

The next proposition states that $\mathbb{Z}_n$ is a *ring*, which we will formally define later.

**Proposition 5.** *Let $n \in \mathbb{Z}$ with $n \geq 2$. Then addition and multiplication on $\mathbb{Z}_n$ satisfies:*

**(A1)** $a + b = b + a$ *for every* $a, b \in \mathbb{Z}_n$;
**(A2)** $a + (b + c) = (a + b) + c$ *for every* $a, b, c \in \mathbb{Z}_n$;
**(A3)** $0 + a = a$ *for every* $a \in \mathbb{Z}_n$;
**(A4)** $a + (-a) = 0$ *for every* $a \in \mathbb{Z}_n$, *where* $-a = n - a$;
**(M1)** $ab = ba$ *for every* $a, b \in \mathbb{Z}_n$;
**(M2)** $a(bc) = (ab)c$ *for every* $a, b, c \in \mathbb{Z}_n$;
**(M3)** $1 \cdot a = a$ *for every* $a \in \mathbb{Z}_n$;
**(DL)** $a(b + c) = ab + ac$ *for every* $a, b, c \in \mathbb{Z}_n$.

*Proof.* All of these properties follow from the corresponding properties in $\mathbb{Z}$. □

## 4. Invertible Elements

**Definition 5.** Let $n \in \mathbb{Z}$ with $n \geq 2$. An element $a \in \mathbb{Z}_n$ is called *invertible* if there exists an element $b \in \mathbb{Z}_n$ such that $a \cdot b = 1$.

**Proposition 6.** *Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $a, b, c \in \mathbb{Z}_n$. Suppose that $ab = ac = 1$. Then $b = c$.*

*Proof.* Since $ab = ac = 1$, and multiplication is commutative, we have $b = b \cdot 1 = bac = abc = 1 \cdot c = c$. □

Thus if $a$ is invertible, there is a *unique* $b$ such that $ab = 1$. We call $b$ the *inverse* of $a$, and let $a^{-1}$ denote this inverse.

**Lemma 1. (Relative Primeness Criterion)**
*Let $m, n \in \mathbb{Z}$. Then $\gcd(m, n) = 1$ if and only if there exist integers $x, y \in \mathbb{Z}$ such that $xm + yn = 1$.*

*Proof.* We have previously seen that if $d = \gcd(m, n)$, then there exist $x, y \in \mathbb{Z}$ such that $xm + yn = d$. In the case of $d = 1$, we wish to prove the converse.

Suppose that $xm + yn = 1$, and let $d = \gcd(m, n)$. Then $d \mid m$ and $d \mid n$, so $d \mid xm + yn$, that is, $d \mid 1$. Since $d \mid 1$ and $d \geq 1$, we see that $d = 1$. □

**Proposition 7.** *Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}_n$.*
*Then $a$ is invertible if and only if $\gcd(a, n) = 1$.*

*Proof.*

($\Rightarrow$) Suppose that $a$ is invertible, and let $b$ be its inverse. Then $\overline{ab} = \overline{1}$, so $ab \equiv 1 \pmod{n}$. That is, $kn = ab - 1$ for some $k \in \mathbb{Z}$. Thus $ab + (-k)n = 1$. Therefore $\gcd(a, n) = 1$ by Lemma 1.

($\Leftarrow$) Suppose that $\gcd(a, n) = 1$. Then there exist $x, y \in \mathbb{Z}$ such that $xa + yn = 1$. Then $\overline{x} \cdot \overline{a} + \overline{y} \cdot \overline{n} = \overline{1}$. But $\overline{n} = \overline{0}$, so $\overline{y} \cdot \overline{n} = \overline{0}$. Thus $\overline{x} \cdot a = \overline{1}$, and $\overline{x}$ is the inverse of $a$, so $a$ is invertible. □

**Proposition 8.** *Let $p \in \mathbb{N}$ be a prime number.*
*Then every nonzero element of $\mathbb{Z}_p$ is invertible.*

*Proof.* Exercise. □

## 5. Zero Divisors

**Definition 6.** Let $n \in \mathbb{Z}$ with $n \geq 2$. Let $a \in \mathbb{Z}$ be nonzero. We say that $a$ is a *zero divisor* if there exists $b \in \mathbb{Z}$ which is nonzero such that $ab = 0$.

**Lemma 2.** *Let $n \in \mathbb{Z}$ with $n \geq 2$. Then $0 \cdot a = 0$ for every $a \in \mathbb{Z}$.*

*Proof.* By definition of multiplication in $\mathbb{Z}_n$, $0 \cdot a = \overline{0 \cdot a} = 0$. □

**Proposition 9.** *Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $a \in \mathbb{Z}_n$. If $a$ is invertible, then $a$ is not a zero divisor.*

*Proof.* Suppose $a$ is invertible, and let $b \in \mathbb{Z}$ such that $ab = 0$. Multiply on the left by $a^{-1}$ to get $a^{-1}ab = a^{-1} \cdot 0$, whence $b = 0$. This shows that $a$ is not a zero divisor, because the only element in $\mathbb{Z}_n$ which can be multiplied with $a$ to produce 0 is 0 itself. □

**Example 6.** Let $n = 6$; in $\mathbb{Z}_6$, the invertible elements are 1 and 5. The zero divisors are 2, 3, and 4. To see this, consider $2 \cdot 3 = \overline{6} = 0$, and $3 \cdot 4 = \overline{12} = 0$.

**Proposition 10.** *Let $n \in \mathbb{Z}$ with $n \geq 2$. Let $a \in \mathbb{Z}_n$.*
*Then $a$ is a zero divisor if and only if* $\gcd(a, n) \geq 2$.

*Proof.* Let $d = \gcd(a, n)$.

Suppose that $d = 1$. Then $a$ is invertible by Proposition 7, so $a$ is not a zero divisor by Proposition 9.

Suppose that $d \geq 2$. Using arithmetic in $\mathbb{Z}$, the Euclidean algorithm dictates that there exist $x, y \in \mathbb{Z}$ such that $ax + ny = d$. We also have $d \mid n$. Then there exists $b \in \mathbb{Z}$ such that $bd = n$, and since $d \geq 2$, we have $0 < b < n$. Applying the residue map to $ax + ny = d$ gives Then $\overline{ax} + \overline{ny} = \overline{d}$, and since $\overline{n} = 0$, we have $\overline{ax} = \overline{d}$. Multiply this equation by $\overline{b}$ to get

$$\overline{ax}\overline{b} = \overline{db} = \overline{n} = \overline{0}.$$

Thus $a$ is a zero divisor. □

**Proposition 11.** *If $n \in \mathbb{N}$ is not a prime number, then $\mathbb{Z}_n$ contains zero divisors.*

*Proof.* Exercise. □

**Proposition 12.** *Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}_n$ be a nonzero element.*
*Then $a$ is invertible if and only if $a$ is not a zero divisor.*

*Proof.* Exercise. □

## 6. Additive Order of an Element in $\mathbb{Z}_n$

For any $k \in \mathbb{N}$ and any $a \in \mathbb{Z}_n$, define $ka$ to be $a$ added to itself $k$ times modulo $n$, that is, added in the set $\mathbb{Z}_n$:

$$ka = \sum_{i=1}^{k} a.$$

It is clear that $ka = \overline{ka}$.

**Definition 7.** Let $a \in \mathbb{Z}_n$. Define the *additive order* of $a$ to be smallest positive integer $k$ such that $ka = 0$. The additive order of $a$ is denoted $\text{ord}_+(a)$.

**Proposition 13.** *Let $a \in \mathbb{Z}_n$ and let $\text{ord}_+(a) = k$. Then*

**(a)** $ja = 0 \Leftrightarrow k \mid j$;
**(b)** $na = 0$;
**(c)** $k \mid n$.

*Proof.*

**(a)** If $k \mid j$, then $j = lk$ for some $l \in \mathbb{Z}$. In this case, $ja = lka = l \cdot 0 = 0$.

Conversely, suppose that $ja = 0$. Write $j = qk + r$, where $0 \leq r < k$. Then $ja = qka + ra = ra$ since $ka = 0$. But $k$ is the smallest positive integer such that $ka = 0$. Thus $r = 0$, and $j = qk$. Thus $k \mid j$.

**(b)** Note that $na = \overline{na} = 0$. Thus $na = 0$.

**(c)** By (b), $na = 0$. Thus $k \mid n$ by part (a). □

**Proposition 14.** *Let $a \in \mathbb{Z}_n$ and let $d = \gcd(a, n)$.*
*Then $\text{ord}_+(a) = \frac{n}{d}$.*

*Proof.* Exercise. □

**Example 7.** Let $n = 24$ and $a = 20$. Now $\gcd(a, n) = 4$, so $\text{ord}_+(a) = \frac{24}{4} = 6$. Indeed, $6 \cdot 20 = 120$ is the smallest multiple of 20 which is divisible by 24.

**Example 8.** Let $p = 7$ and consider $\mathbb{Z}_p$. The order of every nonzero element is 7.

## 7. The Multiplicative Order of an Invertible Element

**Definition 8.** Let $n \in \mathbb{Z}$ with $n \geq 2$. The set of invertible elements in $\mathbb{Z}_n$ is denoted $\mathbb{Z}_n^*$.

Let $a \in \mathbb{Z}_n$. The *multiplicative order* of $a$ is the smallest positive integer $k$ such that $a^k = 1$. The multiplicative order of $a$ is denoted $\text{ord}_*(a)$.

**Example 9.** Let $n = 20$ and $a = 3$. Now $a^2 = 9$, $a^3 = \overline{27} = 7$, $a^4 = \overline{21} = 1$, so $\text{ord}_*(a) = 4$.

## 8. Algebraic Equations in $\mathbb{Z}_n$

We now turn our attention to the question of when an equation, such as $14x = 1$ or $x^2 + 1 = 0$, has a solution in $\mathbb{Z}_n$, and how many solutions it has. For example, $14x = 1$ has a solution if and only if 14 is invertible in $\mathbb{Z}_n$, and this is the case if and only if $n$ and 14 are relatively prime. In fact, we have an explicit technique for finding the inverse 14. This technique makes repeated use of the division algorithm.

Suppose $n = 33$. Then 14 and 33 are relatively prime, so there exist integers $x$ and $y$ such that $14x + 33y = 1$. To find them, we divide:

- $33 = 14 \cdot 2 + 5$;
- $14 = 5 \cdot 2 + 4$
- $5 = 4 \cdot 1 + 1$;
- $2 = 1 \cdot 2 + 0$.

The second to last remainder is 1, so $\gcd(14, 33) = 1$. Now work backwards to find $x$ and $y$:

- $1 = 5 - 4$;
- $1 = 5 - (14 - 5 \cdot 2) = 5 \cdot 3 - 14 \cdot 1$;
- $1 = (33 - 14 \cdot 2) \cdot 3 - 14 \cdot 1 = 33 \cdot 3 - 14 \cdot 7$.

Thus the inverse of 14 in $\mathbb{Z}_{33}$ is $-7 = 26$.

The equation $x^2 + 1 = 0$ is more interesting. To understand it, note that $-1$ exists in $\mathbb{Z}_n$ as $\overline{n-1}$. So a solution to the equation $x^2 + 1 = 0$ would be a square root of negative 1 in $\mathbb{Z}_n$. For example, in $\mathbb{Z}_5$, we have $2^2 = 4 = -1 \pmod 5$.

It is also possible that a quadratic equation, such as $x^2 - 1 = 0$, can have more than two solutions in $\mathbb{Z}_n$. Note that $x^2 - 1 = (x + 1)(x - 1)$, even in $\mathbb{Z}_n$. Suppose that $n = 15$. Then $x = 1$ and $x = -1 = 14$ are solutions, but so is 4, since $(4 + 1)(4 - 1) = 5 \cdot 3 = 0$ (modulo 15).

However, suppose that $n = p$ is a prime number. Then in $\mathbb{Z}_p$, a quadratic equation can have at most 2 roots. This is because $\mathbb{Z}_p$ has no zero divisors. If the quadratic has a root, it factors; then if the product of the factors is zero, one of them must be zero.

For example, let us find the roots of $x^2+8x+1 = 0$ in $\mathbb{Z}_{11}$. Now $8 \equiv -3 \pmod{11}$ and $1 \equiv -10 \pmod{11}$, so our equation becomes $x^2 - 3x - 10 = 0$. This factors as $(x - 5)(x + 2) = 0$. Since 11 is prime, the only roots are 5 and $-2 = 8$.

## 9. Exercises

**Exercise 1.** Let $a \in \mathbb{Z}_n$ and let $d = \gcd(a, n)$.
Then $\text{ord}_+(a) = \frac{n}{d}$. (Hint: let $k = \text{ord}_+(a)$, and show that $k \mid \frac{n}{d}$ and that $\frac{n}{d} \mid k$.)

**Exercise 2.** Find the additive order of 6, 11, 18, and 28 in $\mathbb{Z}_{36}$.

**Exercise 3.** Let $p \in \mathbb{N}$ be a prime number.
Show that every nonzero element of $\mathbb{Z}_p$ is invertible.

**Exercise 4.** Show that if $n \in \mathbb{N}$ is not a prime number, then $\mathbb{Z}_n$ contains zero divisors.

**Exercise 5.** Let $n \in \mathbb{N}$ and let $\overline{a} \in \mathbb{Z}_n$ be a nonzero element.
Show that $\overline{a}$ is invertible if and only if $\overline{a}$ is not a zero divisor.

**Exercise 6.** Find the inverse of 15 in $\mathbb{Z}_{49}$.

**Exercise 7.** Solve the equation $17x = 23$ in $\mathbb{Z}_{71}$.

**Exercise 8.** Solve the equation $x^2 - 5x - 2 = 0$ in $\mathbb{Z}_{11}$.

**Exercise 9.** Solve the equation $x^2 - 5x + 4 = 0$ in $\mathbb{Z}_6$.

**Exercise 10.** Find all square roots of $-1$ in $\mathbb{Z}_{101}$.

Department of Mathematics and CSci, Southern Arkansas University
*E-mail address*: plbailey@saumag.edu