Rings Through Modular Arithmetic

Rings provide a unifying language for algebraic systems ranging from integers and polynomials to modular arithmetic used in computation. This paper discovers core ring concepts using the modular ring $\mathbb{Z}/n\mathbb{Z}$ as a guiding example. We introduce congruence (modulo) classes, discuss orders and generators through the group structures naturally contained in rings, and characterize invertibility via units and the gcd. Along the way, we prove foundational results operations. We conclude with application in pitch-class arithmetic in music theory (mod 12), illustrating modular structures and invertible transformations in this case.

I. RINGS: A BRIEF OVERVIEW

Definition I.1. A *ring* $(R, +, \cdot)$ is a set R equipped with two operations such that:

Standard examples include $\mathbb{Z}$, polynomial rings $F[x]$, matrix rings $M_n(F)$, and the modular rings $\mathbb{Z}/n\mathbb{Z}$. A central theme is that ring axioms preserve enough arithmetic structure to support both theory (proofs) and computation (algorithms).

II. MODULO CLASSES AND THE RING $\mathbb{Z}/n\mathbb{Z}$

A. Congruence and residue (modulo) classes

Fix an integer $n \geq 2$. Define congruence modulo n by

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

This is an equivalence relation on $\mathbb{Z}$. The equivalence class of a is

$$[a] = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}.$$

B. Well-defined operations

Define addition and multiplication on classes by

$$[a] + [b] = [a + b], \qquad [a] \cdot [b] = [ab].$$

Theorem II.1. *If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then*

$$a+b \equiv a'+b' \pmod{n} \quad \textit{and} \quad ab \equiv a'b' \pmod{n}.$$

Hence, the definitions $[a] + [b] = [a + b]$ and $[a][b] = [ab]$ do not depend on the choice of representatives.

Proof. Since $n \mid (a - a')$ and $n \mid (b - b')$, we have

$$(a + b) - (a' + b') = (a - a') + (b - b')$$

which is divisible by n, so $a+b \equiv a'+b' \pmod{n}$. For products,

$$ab - a'b' = (a - a')b + a'(b - b'),$$

a sum of multiples of n. Thus $ab \equiv a'b' \pmod{n}$. □

Therefore $\mathbb{Z}/n\mathbb{Z}$ is a (commutative, unital) ring under these operations.

III. INVERTIBILITY IN $\mathbb{Z}/n\mathbb{Z}$: UNITS AND GCD

Definition III.1. Let R be a unital ring. An element $u \in R$ is a *unit* if there exists $v \in R$ such that $uv = vu = 1$. The set of units is denoted $R^{\times}$.

In the modular ring $\mathbb{Z}/n\mathbb{Z}$, invertibility is governed by the gcd.

Theorem III.2 (Units in $\mathbb{Z}/n\mathbb{Z}$)**.** *The class $[a] \in \mathbb{Z}/n\mathbb{Z}$ is a unit if and only if* $\gcd(a, n) = 1$.

Proof. ($\Rightarrow$) If $[a]$ is a unit, there exists $[b]$ with $[a][b] = [1]$, i.e. $ab \equiv 1 \pmod{n}$ so $ab - 1 = kn$ for some integer k. Any common divisor d of a and n divides ab and kn, hence, divides $ab - kn = 1$. Thus, $d = 1$ and $\gcd(a, n) = 1$.

($\Leftarrow$) If $\gcd(a, n) = 1$, integers x, y satisfy $ax + ny = 1$. Reducing modulo n yields $ax \equiv 1 \pmod{n}$, so $[a][x] = [1]$ and $[a]$ is a unit. □

IV. ORDERS AND GENERATORS INSIDE RINGS

Although a ring is not generally a group under multiplication, it contains natural groups:

- the additive group $(R, +)$;
- the multiplicative group of units $R^{\times}$ (when R is unital).

A. Additive order in $\mathbb{Z}/n\mathbb{Z}$

Definition IV.1. In a group $(G, +)$, the *order* of an element g is the least positive integer k such that $kg = 0$, if such a k exists.

Proof. □

B. Multiplicative order in $(\mathbb{Z}/n\mathbb{Z})^{\times}$

Definition IV.2. If $u \in R^{\times}$, the *multiplicative order* of u is the least positive integer k such that $u^k = 1$.

V. APPLICATIONS: MUSIC THEORY VIA PITCH CLASSES MOD 12

An application appears in *pitch-class* arithmetic, a standard abstraction in music theory.

a. Pitch classes as modulo classes. In equal temperament, pitches an octave apart are treated as equivalent. Label the twelve pitch classes by integers mod 12:

$$\mathrm{C} = 0,\ \mathrm{C\#} = 1,\ \ldots,\ \mathrm{B} = 11,$$

so the set of pitch classes is naturally $\mathbb{Z}/12\mathbb{Z}$.

b. Transposition as addition. Transposing every note up by k semitones corresponds to adding $[k]$:

$$T_k([x]) = [x] + [k] = [x + k] \quad \text{in } \mathbb{Z}/12\mathbb{Z}.$$

Because addition in $\mathbb{Z}/12\mathbb{Z}$ is well-defined, this does not depend on how notes are written enharmonically; it depends only on the pitch class.

c. Orders and cyclic structure: the "circle" phenomena. The additive order of $[k]$ in $\mathbb{Z}/12\mathbb{Z}$ is

$$\mathrm{ord}_{+}([k]) = \frac{12}{\gcd(k, 12)}.$$

For example:

- $[1]$ has order 12: repeatedly transposing by one semitone visits all 12 pitch classes.
- $[2]$ has order 6: whole-tone transposition cycles through 6 classes (the whole-tone scale).
- $[7]$ has order 12 because $\gcd(7, 12) = 1$: repeatedly adding 7 (a perfect fifth) cycles through all pitch classes, matching the "circle of fifths" idea as a single 12-step cycle.

d. Invertible transformations (units) and musical symmetries. Beyond pure transposition, music theory often studies affine maps on pitch classes:

$$f([x]) = [a][x] + [b] = [ax + b] \quad \text{in } \mathbb{Z}/12\mathbb{Z}.$$

Such a map is invertible exactly when $[a]$ is a unit. By the units theorem,

$$[a] \text{ is invertible mod } 12 \quad \Longleftrightarrow \quad \gcd(a, 12) = 1,$$

so the invertible multipliers are $a \in \{1, 5, 7, 11\}$.

VI. CONCLUSION

We discover core principles of, and relating to, modular rings:

- Congruence (modulo) classes
- Orders and generators
- Invertibility and GCD
- Applications to music theory

Our activity aims to cover these concepts using a custom computer program, Ring World, and instruction.

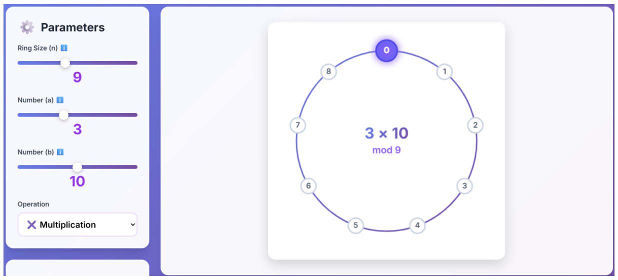
A. Ring World

Ring World provides easy-to-visualise explanations of the concepts listed above, as well as providing a clear picture of the basics needed to understand them in the first place; for example:

- Modular arithmetic
- Integers
- Pitch classes

The core operations are addition and multiplication, visualized as a ring-shaped set of circles from 0 to n-1, for integer modulo n. A user chooses the n, chooses a number in the modular set, chooses an operation (addition or multiplication), and chooses a second argument between 0 and 20. Then the press play, and the operation is visualized. In the case of multiplication: say, 3*10 in modulo 9, each addition of 3 is visualized with an arrow, and every number passed over (0, 3, 6) remains colored in with a less bright color. This also allows the user to visualize the idea of a generator.

Regarding applications to music theory, separate modes within the program permit a direct visual to ease the difficulty of understanding the link between pitch classes and modulo classes.

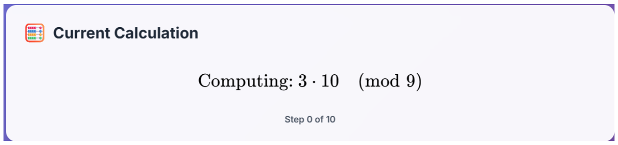

Parameters

Ring Size (n): 9

Number (a): 3

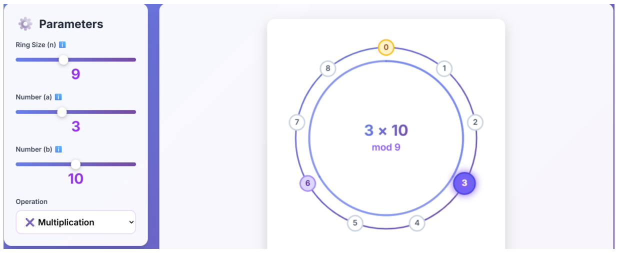
Number (b): 10

Operation: Multiplication


Current Calculation

Computing: $3 \cdot 10 \pmod 9$

Step 0 of 10

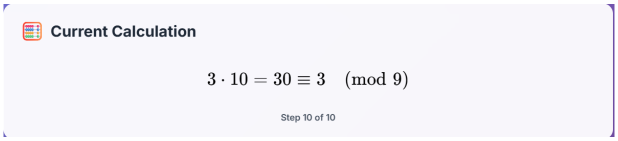

Parameters

Ring Size (n): 9

Number (a): 3

Number (b): 10

Operation: Multiplication


Current Calculation

$3 \cdot 10 = 30 \equiv 3 \pmod 9$

Step 10 of 10

B. Instruction

Along with Ring World, there is a set of Guiding Questions to help students utilize the program and ultimately draw their own, correct conclusions on what this paper lays out.

Coupled with verbal instruction, the activity can be tailored to specific students/groups with respect to background efficiently. Ultimately, we ended up not using the physical guiding question document; rather, we improvised, giving only verbal instruction; however, our verbal instruction mirrored quite closely what we had on our guiding questions, and thus the creating of the guiding questions was a useful way to brainstorm and prepare for our presentation.

We did give the students space for discussion and conversation during our presentation, and one student asked a good question that we had prepared for: why does this matter? Our answer was twofold: one, there are many practical applications of this, first and foremost, cryptography. But, also, mathematics tends to come up with things that seem to only exist in the world of mathematics, but which hundreds of years later have practical application (imaginary numbers, for example, which now form the backbone of core quantum physics equations).