Affine group of integers modulo *n*, conjugacy classes and representations

Affine Group of Integers Modulo *n*

Modular arithmetic is a system where numbers "wrap around" some integer called the modulus. For example, time uses modular arithmetic: 4 hours after 9 o'clock is 1 o'clock, which is expressed as

$$9 + 4 \equiv 1 \pmod{12}$$

using modular arithmetic. We write $\mathbb{Z}_n$ to denote the integers under modular arithmetic with modulus n and (k, n) to denote $\gcd(k, n)$. We also write $\mathbb{Z}_n^\times := \{k \in \mathbb{Z}_n : \gcd(k, n) = 1\}$ for the group of **units** (invertible elements) of $\mathbb{Z}_n$.

A **group** is a set G with an operation $\circ$ with certain properties (closure, associativity, identity, and invertibility). Some examples are the real numbers $\mathbb{R}$ with addition and $\mathbb{Z}_n$ with addition modulo n.

The **affine group of** $\mathbb{Z}_n$ is the group of invertible affine transformations

$$\mathrm{Aff}(\mathbb{Z}_n) := \{\pi_{a,b} : a \in \mathbb{Z}_n^\times, b \in \mathbb{Z}_n\},$$

an analog of scalings and translations of the real line $\mathbb{R}$ for the set $\mathbb{Z}_n$. Each $\pi_{a,b} \in \mathrm{Aff}(\mathbb{Z}_n)$ defines a **permutation** (shuffling) of $\mathbb{Z}_n$ by $\pi_{a,b}(x) \equiv ax + b \pmod{n}$.

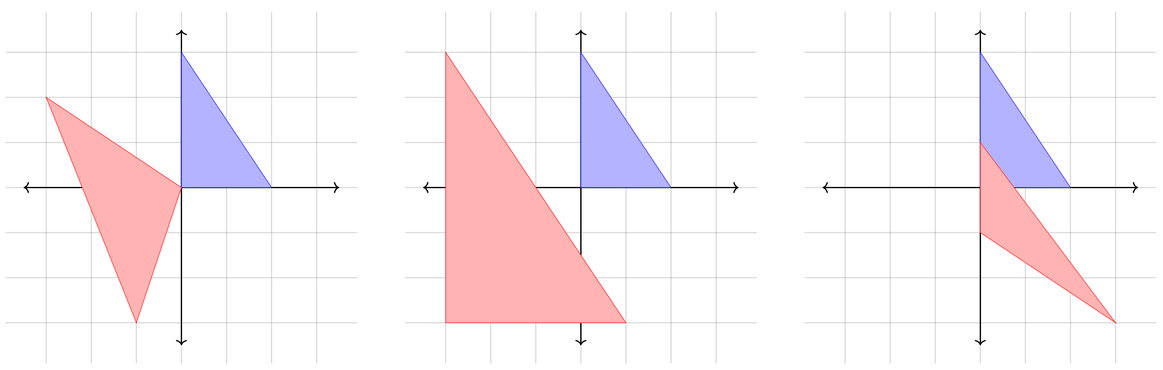

Figure 1. Affine transformations in $\mathbb{R}^2$. Graphic created by finalist using TikZ, 2026.

Affine group elements are used in crytography as **psuedo-random number generators** [3]. Some objects have natural $\mathrm{Aff}(\mathbb{Z}_n)$ symmetries, such as **Boolean functions** [1] and **tone rows** [2].

Conjugacy Classes

Two elements $a, b \in G$ are called **conjugate** if there exists some $g \in G$ such that

$$g^{-1}ag = b.$$

The **conjugacy class** of $a \in G$ are all $g \in G$ that are conjugate to a. We denote the conjugacy class of $\pi_{a,b} \in \mathrm{Aff}(\mathbb{Z}_n)$ by $\mathcal{O}_{a,b}$. To analyze $\mathcal{O}_{a,b}$, we consider a **fibration** (splitting) of $\mathbb{Z}_n$ by divisors of n.

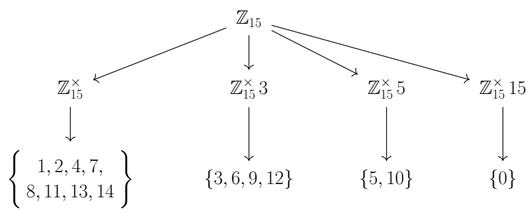

Figure 2. Fibration of $\mathbb{Z}_{15}$ by divisors. Graphic created by finalist using TikZ, 2026.

Each fiber, or **orbit**, are products of all invertible elements by a divisor. Let $[n]$ denote the set of all positive divisors of $n \in \mathbb{Z}$. Given $\alpha, b \in \mathbb{Z}$, we can consider subsets

$$[n]_{\alpha,b} := \{(\alpha t + b, n) : t \in \mathbb{Z}\} \subseteq [n].$$

Conjugacy classes are unions over fibers:

$$\mathcal{O}_{a,b} = \bigcup_{d \in [n]_{a-1,b}} \{\pi_{a,b'} : (b', n) = d\}.$$

For example, when $n = 15$, we have $\mathcal{O}_{4,0} = \{\pi_{4,3k} : k \in \mathbb{Z}_5\}$. Moreover, there are 15 conjugacy classes of $\mathrm{Aff}(\mathbb{Z}_{15})$. Indeed, for square-free n, there are n conjugacy classes of $\mathrm{Aff}(\mathbb{Z}_n)$.

Representation Theory

Representations allow us to analyze groups through the lens of linear algebra. Specifically, a representation $T : G \to \mathrm{Mat}(\mathbb{C}^n)$ maps group elements $g, h \in G$ into matrices while preserving the group operation:

$$T(g)T(h) = T(gh).$$

Given a representation, its **character** is its trace $\chi : G \to \mathbb{C}$. Moreover, it is **irreducible** if there are no non-trivial subspaces (subspaces other than $\{0\}$ and V) that all representation matrices preserve.

Representations are used in both classical and quantum physics to study **rotational symmetry** and its underlying partial differential equations, and representations of finite groups are used in chemistry to study **molecular structures** and its symmetries.

Permutational Representation

We call $P : S_n \to \mathrm{Mat}(\mathbb{C}^n)$ with $P(\sigma)e_i = e_{\sigma(i)}$ the **permutational representation**. It turns out that its irreducible subrepresentations live in the **same fibers** used to find conjugacy classes.

Specifically, we use an eigenbasis $\{v_k\}$ of $P(\pi_{1,1})$ (basis with each v satisfying $Pv = \lambda v$ for some $\lambda \in \mathbb{C}$). Let $\mathcal{N}_k := \mathbb{C}v_k$ and

$$\mathcal{N}_{(d)} := \bigoplus_{(k,n)=d} \mathcal{N}_k\,.$$

Then, we have that $P_{(d)} := P\big|_{\mathcal{N}_{(d)}}$ are irreducible and non-isomorphic for distinct d.

To describe the characters of $P_{(d)}$, we first introduce **Ramanujan sums** $c_n(x)$:

$$c_n(x) := \sum_{(k,n)=1} e^{\frac{2\pi i}{n} kx},$$

which are sums of primitive roots of unity. These sums were used to show **Vinogradov's Theorem**: every sufficiently large odd number is the sum of three primes.

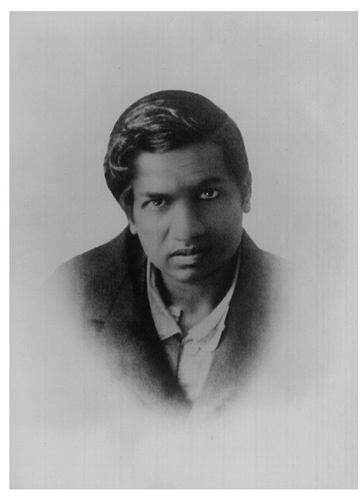

Figure 3. Wren Digital Library. Passport photo of Ramanujan [Photograph], Trinity College, Cambridge, 1913. (https://mss-cat.trin.cam.ac.uk/manuscripts/uv/view.php?n=Add.Ms.a.94.7#?c=0&m=0&s=0&cv=6&xywh=2282%2C-1%2C05%2C4733). CC BY 4.0.

Using Ramanujan sums, we have a formula for the **character**:

$$\chi_{(d)}(\pi_{a,b}) := \chi_{P_{(d)}}(\pi_{a,b}) = \mathbb{1}_{(\mathbb{Z}_n^\times)_d}(a)\, c_{n/d}(b). \tag{1}$$

Panstochastic Matrices

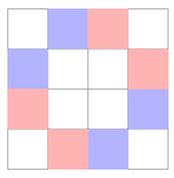

Figure 4. A broken diagonal and anti-diagonal. Graphic created by finalist using TikZ, 2026.

1	0	0	0	0
0	0	0	1	0
0	1	0	0	0
0	0	0	0	1
0	0	1	0	0

Table 1. A 5×5 panmagic permutation matrix derived from $\pi_{2,4} \in \mathrm{Aff}(\mathbb{Z}_5)$.

A matrix is **panstochastic** if its entries are all nonnegative and its row, column and broken diagonal and anti-diagonal sums are all 1 and **panmagic** if it lives in the span of panstochastic matrices.

Panmagic permutation matrices (images of P) are solutions to the **modular n-queens problem**, where n mutually nonattacking queens are placed on a cylindrical chessboard.

Theorem 1. *Let $p \geq 5$ be prime. Then, panmagic permutation matrices from $P(\mathrm{Aff}(\mathbb{Z}_p))$ span the same space (of **panmagic matrices**) as all panmagic permutation matrices.*

Irreducible Representations

Serre [4] describes irreducible representations for certain groups with commutative characteristics. We apply this to $\mathrm{Aff}(\mathbb{Z}_n)$.

Theorem 2. *All irreducible representations of $\mathrm{Aff}(\mathbb{Z}_n)$ are given by $\theta_{d,\rho}$, where $d \mid n$ and ρ is a character of $(\mathbb{Z}_n^\times)_d$, and $\dim \theta_{d,\rho} = \varphi(n/d)$.*

Once again, **Ramanujan sums** allow us to find the character

$$\chi_{d,\rho}(\pi_{a,b}) := \chi_{\theta_{d,\rho}}(\pi_{a,b}) = \mathbb{1}_{(\mathbb{Z}_n^\times)_d}\, \rho(a)\, c_{n/d}(b). \tag{2}$$

Comparing (2) with (1) and using 1 as the trivial character, we have

$$\chi_{(d)}(\pi_{a,b}) = \mathbb{1}_{(\mathbb{Z}_n^\times)_d}(a)\, c_{n/d}(b) = \chi_{d,1}(\pi_{a,b}),$$

so $P_{(d)} = \theta_{d,1}$. Thus, the irreducible permutational representations are the 'simplest' ones of $\mathrm{Aff}(\mathbb{Z}_n)$ under Serre's construction.

Future Directions

1. What is the explicit cycle type of $\pi_{a,b}$ for general $a \in \mathbb{Z}_n^\times$ and $b \in \mathbb{Z}_n$?
2. Affine panmagic permutation matrices cannot span all panmagic matrices. Is the span of **all** panmagic permutation matrices the set of panmagic matrices?
3. What are the descriptions of the irreducible characters of $(\mathbb{Z}_n^\times)_d$?

References

[1] T. Cusick, K. Lakshmy, M. Sethumadhavan, Affine equivalence of monomial rotation symmetric Boolean functions: a Pólya's theorem approach, *Journal of Mathematical Cryptology*, **10** (2016), 145-156.

[2] H. Fripertinger, Enumeration of mosaics, *Discrete Mathematics*, **199** (1999), 49-60.

[3] G. Marsaglia, The structure of linear congruential sequences, in *Applications of Number Theory to Numerical Analysis, S. Zaremba, editor*, 1972, 249-285.

[4] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York-Heidelberg, 1977.

Lee J.