AIMS Mathematics, 11(11): 38676–38696.
DOI: 10.3934/math.20261492
Received: 28 September 2026
Revised: 09 November 2026
Accepted: 12 November 2026
Published: 19 November 2026

https://www.aimspress.com/journal/Math

Research article

Pochhammer products of matrices over prime fields

Youngho Woo[1], **Chi Young Ahn**[1] **and Daeyeoul Kim**[2,*]

[1] Department of Industrial Mathematics, National Institute for Mathematical Sciences, Daejeon 34047, South Korea; youngw@nims.re.kr, chiyoung@nims.re.kr

[2] Department of Mathematics and Institute of Pure and Applied Mathematics, Jeonbuk National University, Jeonju 54896, South Korea

* **Correspondence:** Email: kdaeyeoul@jbnu.ac.kr; Tel: +82632703575.

Abstract: For a square matrix A over a prime field $\mathbb{F}_p$, we study the matrix Pochhammer products $P_k(A) = A(A+I)\cdots(A+(k-1)I)$, whose increment is the identity matrix. The sequence $(P_k(A))_{k\geq 1}$ is eventually periodic by finiteness, and primary decomposition is a standard tool. Our contributions are exact invariants, a realizability criterion, and the resulting distributions. We determine the pre-period and the period exactly from the primary factorization of the minimal polynomial and characterize the pairs realizable in a prescribed matrix size. For periods that arise from irreducible quadratic factors in odd characteristic, we compute the minimum required dimension. We give the complete joint distribution for two-by-two matrices, which extends the identity-increment case of the classification over $\mathbb{F}_2$ by Lee and Kim. The labels Stable, Amicable, and Sociable denote periods 1, 2, and greater than 2, respectively. For matrices of arbitrary size, we express the joint counts and Amicable totals as finite cycle-index sums; the Stable total recovers the known number of triangularizable matrices, and the Sociable total follows by subtraction. The set of periods attained by all two-by-two matrices has exactly two elements if and only if the characteristic is two or a Fermat prime. At an odd Fermat prime, all matrices with irreducible quadratic characteristic polynomials have the same period.

Keywords: Pochhammer products; matrix algebras; finite fields; matrix dynamics; rational canonical form; eventual periodicity
Mathematics Subject Classification: 11B83, 12E20, 15B33, 37P25

1. Introduction

The rising factorial $x(x+1)\cdots(x+k-1)$ naturally appears in hypergeometric series [1, Section 1.2]. Replacing x by a square matrix A and the scalar increment by the identity gives a matrix Pochhammer product. Jódar and Cortés [2] used these products to define hypergeometric matrix functions.

We consider $A \in M_N(\mathbb{F}_p)$, where p is prime, and study the following:

$$P_k(A) = A(A + I) \cdots (A + (k - 1)I).$$

The sequence is eventually periodic: the augmented state $(X, r) \in \mathbb{F}_p[A] \times \mathbb{F}_p$ evolves by the fixed recurrence $(X, r) \mapsto (X(A + rI), r + 1)$, starting at $(I, 0)$. Here, the exact invariants will follow from ordinary polynomial arithmetic in $\mathbb{F}_p[A]$.

Our motivation comes, in part, from the work of Kim, Ahn, and their collaborators on matrix iteration over finite rings. For power iteration over prime fields, Jung et al. [3] studied powers of two-by-two matrices over $\mathbb{F}_7$, and Yang et al. [4] classified powers over $M_2(\mathbb{F}_5)$ and their induced subgroup actions.

Fan et al. [5, Section 2.4] defined right and left matrix Pochhammer symbols with arbitrary increments.

For related finite-ring dynamics, Fan et al. [5] classified powers over $M_2(\mathbb{Z}_9)$. Other iterations occur modulo four [6] and on elliptic-curve 4-torsion [7].

We retain the labels Stable, Amicable, and Sociable for the eventual periods 1, 2, and greater than 2, respectively. Their arithmetic counterparts occur for restricted divisor-function iterations [8, 9]; for the full sum-of-divisors iteration, see Cohen and te Riele [10].

The closest predecessor is the work of Lee and Kim [11]. They classified right and reverse products $A(A + B) \cdots (A + (k - 1)B)$ for pairs in $M_2(\mathbb{F}_2)$. When $B = I$, the factors commute and both product orders become our sequence. Their Theorem 2.15 and Tables 2–5, in which the index Ord equals our pre-period τ, give 14 Stable and 2 Amicable matrices with $B = I$. Theorem 3.4 recovers these results, including the Stable pre-period counts 1, 7, 3, and 3 at $\tau = 1$, 2, 3, and 4, respectively, and pre-period 1 for both Amicable matrices. We keep the identity increment and treat every matrix size and prime characteristic; arbitrary matrix increments remain outside our scope.

Eventual periodicity and primary decomposition are standard tools. The results here determine the exact pre-period and period from the minimal polynomial, characterize the pairs realizable in a fixed dimension, and count matrices with these invariants. The nonlinear dimension cost gives an exact feasibility criterion and, in odd characteristic, an explicit minimum for the quadratic periods. The complete two-by-two distribution also shows that the period spectrum of $M_2(\mathbb{F}_p)$ has exactly two elements if and only if $p = 2$ or p is a Fermat prime. For matrices of any size, the joint counts and Amicable totals use classical similarity-class weights and the matrix cycle index of Kung [12] and Stong [13], in the form given by Morrison [14, Section 2.1]. The Stable total recovers the known count of triangularizable matrices [14, Lemma 2.3], and the Sociable total follows by subtraction; the enumeration machinery itself is not new.

Other finite-field products have different definitions. Gauss factorials [15] and their polynomial analogues [16] select factors by coprimality conditions. Panja [17] studied periodic points of the fixed power map $x \mapsto x^L$ in finite matrix groups and algebras, and Qureshi and Reis [18] studied the functional graphs of power maps on finite groups, including $\mathrm{PGL}_2(\mathbb{F}_q)$. In the present product, by contrast, the factors depend on the length of the product.

The paper is organized as follows.

- **Section 2: Exact pre-periods and periods.** Theorem 2.6 assembles the local primary-factor formulas. Corollaries 2.7 and 2.9 treat quadratic factors and Fermat primes. Additionally, we characterize Stable and Amicable elements and prove the sharp maximum pre-period Np.

- **Section 3: Possible pairs and matrix counts.** Theorem 3.2 decides the pair feasibility by matrix size, and Corollary 3.3 gives the minimum for quadratic periods in odd characteristic. Theorem 3.4 gives the two-by-two joint distribution. The later subsections compare other algebras, give general-size cycle-index sums, and discuss computation. The number of Stable matrices is obtained from the specialization of the matrix cycle index to the linear irreducible polynomials [14, Lemma 2.3]; Kaylor and Offner [19] also counted matrices over a finite field with all eigenvalues in the field. Additionally, see Fulman [20] for the group case.
- **Section 4: Conclusions and further questions.** We compare the characteristics, distinguish the exact finite formulas from simpler closed forms, and discuss coefficient-field extensions and lift-dependent residue-ring questions.

Conventions: Throughout this paper, we let p be prime, $N \geq 1$, and $I = I_N$ be the identity matrix. The minimal polynomial of $A \in M_N(\mathbb{F}_p)$ is denoted by μ_A. Additionally, we use finite-dimensional $\mathbb{F}_p$-algebras in the proofs. All such algebras are assumed to be nonzero, associative, and unital. For an algebra $\mathcal{A}$, write $D = \dim_{\mathbb{F}_p} \mathcal{A}$. For $a \in \mathcal{A}$, $\mu_a \in \mathbb{F}_p[y]$ is the monic polynomial of least positive degree with $\mu_a(a) = 0$.

Definition 1.1. *For $A \in M_N(\mathbb{F}_p)$ and $k \geq 0$, define the following:*

$$P_0(A) = I, \qquad P_k(A) = \prod_{j=0}^{k-1} (A + jI). \tag{1.1}$$

The factors commute because they are polynomials in A. For a in a finite-dimensional algebra $\mathcal{A}$, define

$$P_0(a) = 1_{\mathcal{A}} \quad \textit{and} \quad P_k(a) = \prod_{j=0}^{k-1} (a + j1_{\mathcal{A}})$$

in the same way.

Previous papers [4, 5, 8, 9, 11] have used the term "order", which can be confused with the order of a group element. In this paper, we use the terms pre-period and period, defined as follows.

Definition 1.2. *The* pre-period *of the sequence $(P_k(A))_{k\geq 1}$ is defined as follows:*

$$\tau(A) = \min \left\{ k \geq 1 : \begin{array}{l} \textit{there exists } t \geq 1 \textit{ such that} \\ P_{\ell+t}(A) = P_\ell(A) \textit{ for every } \ell \geq k \end{array} \right\}. \tag{1.2}$$

The smallest positive t for which the equality holds from $k = \tau(A)$ onward is the period $\pi(A)$*. We write the two values as the pair (τ, π), and call A* Stable*,* Amicable*, or* Sociable *according as $\pi(A)$ is* 1*,* 2*, or greater than* 2*, respectively.*

For convenience, we use the same definitions for elements of $\mathcal{A}$ and write $\tau_{\mathcal{A}}(a)$ and $\pi_{\mathcal{A}}(a)$. Thus,

$$\tau(A) = \tau_{M_N(\mathbb{F}_p)}(A) \quad \text{and} \quad \pi(A) = \pi_{M_N(\mathbb{F}_p)}(A).$$

We use *pre-period* for the first positive index of the periodic part and *period* for its smallest positive period. In particular, $\tau = 1$ means that the sequence is periodic from P_1, and the tail length, namely the

number of terms before the periodic part, is $\tau - 1$. Gassert [21] called this tail length the preperiod, and Hutz and Patel [22] called it the tail; both reported it rather than τ. We keep $\tau \geq 1$ in every formula. Lemma 2.1 collects the facts about eventually periodic sequences that we need.

Since the sequence is eventually periodic, as explained in the introduction, the pre-period and the period are well defined, both for matrices and for elements of a finite-dimensional $\mathbb{F}_p$-algebra.

We can calculate the matrix products in the algebra generated by the matrix. More generally, for an element a, put $\mu = \mu_a$, $R = \mathbb{F}_p[y]/(\mu)$, and $\xi = y + (\mu)$. Evaluation at a is an isomorphism $R \to \mathbb{F}_p[a]$ carrying ξ to a, and each P_k is a polynomial expression over $\mathbb{F}_p$, so

$$(\tau_{\mathcal{A}}(a), \pi_{\mathcal{A}}(a)) = (\tau_R(\xi), \pi_R(\xi)).$$

Thus, the matrix calculation takes place in $\mathbb{F}_p[y]/(\mu_A)$. The pair for a matrix depends only on its minimal polynomial. However, matrices with the same minimal polynomial need not be similar. Therefore, to count matrices, we must also know how many matrices have each rational canonical form. For a monic polynomial g of positive degree, $C(g)$ denotes its *companion matrix*. It has a size of $\deg g$, and both its characteristic polynomial and minimal polynomial are g. These matrices are used in Section 3 to construct matrices with a prescribed pre-period and period.

2. Exact pre-periods and periods

We separately calculate the products modulo each primary component of the minimal polynomial. For a linear factor, the products become zero after enough occurrences of one particular shift. For a nonlinear factor, every shift is invertible, and a block of p shifts gives $A^p - A$ on that component. Its multiplicative order determines the local period. Therefore, the pre-period comes from the linear components and the period from the nonlinear ones.

Lemma 2.1. *Let $x^{(1)}, \ldots, x^{(r)}$ be eventually periodic sequences with pre-periods τ_i and periods d_i in the sense of Definition 1.2. For the tuple sequence $X_k = (x_k^{(1)}, \ldots, x_k^{(r)})$,*

$$\tau(X) = \max_i \tau_i, \qquad \pi(X) = \operatorname*{lcm}_i d_i.$$

Moreover, if a sequence $(x_k)_{k\geq 1}$ satisfies $x_{k+t} = x_k$ for every $k \geq b$, where $b, t \geq 1$, then it is eventually periodic and its period divides t.

Proof. First, let a sequence $(x_k)_{k\geq 1}$ have a pre-period a and a period d, and suppose that $x_{k+t} = x_k$ for every $k \geq b$. For $k \geq a$, choose $n \geq 0$ with $k + nd \geq b$. Then,

$$x_{k+t} = x_{k+t+nd} = x_{k+nd} = x_k.$$

Thus, t is already a period from a. Write $t = sd + \delta$, with $0 \leq \delta < d$. Periodicity by d gives $x_{k+\delta} = x_{k+t} = x_k$ for every $k \geq a$. If $\delta > 0$, then this contradicts the minimality of d, so $d \mid t$.

For the tuple, put $a = \max_i \tau_i$ and $d = \operatorname{lcm}_i d_i$. The tuple is periodic from a with a period of d. If it were periodic from an index smaller than a, then so would be a component attaining a, which is impossible. Finally, a period t of the tuple from index a is a period of each component from a, and hence is divisible by every d_i by the first paragraph of this proof. Therefore, the least period of the tuple is d. □

2.1. Primary decomposition and local notation

We write the primary factorization as follows:

$$\mu_a(y) = \prod_i g_i(y)^{f_i},$$

where the g_i are distinct monic irreducibles, and f_i is the exponent of g_i in the minimal polynomial. A linear primary factor is a power of a degree-one polynomial. A nonlinear primary factor is a power of an irreducible polynomial of degree at least two. The polynomial Chinese remainder theorem gives the following:

$$\mathbb{F}_p[a] \simeq \prod_i \mathbb{F}_p[y]/(g_i^{f_i}).$$

We use two standard facts about finite fields [23, Chapter 2]. The group $\mathbb{F}_{p^d}^{\times}$ is cyclic, and the roots of an irreducible polynomial are Frobenius conjugates.

A calculation in one quotient $\mathbb{F}_p[y]/(g_i^{f_i})$ is called *local*.

For each linear factor, write $g = y + \lambda$ with $\lambda \in \{0, 1, \ldots, p-1\}$, identified with its image in $\mathbb{F}_p$. The first shift at which $y + \lambda$ occurs is included at a product length of $\lambda + 1 \in \{1, \ldots, p\}$.

Remark 2.2. *In every pre-period formula, λ is the unique integer representative in $\{0, \ldots, p-1\}$, and the ordered shifts $0, 1, \ldots$ account for the term $\lambda + 1$. Both invariants are determined by the minimal polynomial, but in different ways. By* (2.3) *in Theorem 2.6, the period depends only on the nonlinear primary factors, whereas by* (2.2)*, the pre-period depends only on the linear ones, through their exponents f_i and integer labels λ_i. For instance, if $\gamma \in \mathbb{F}_p$, then $\mu_{A+\gamma I}(y) = \mu_A(y - \gamma)$, and $(\alpha + \gamma)^p - (\alpha + \gamma) = \alpha^p - \alpha$ for every root α of μ_A, so each $\eta(g_i)$ (defined below) is unchanged; hence, $\pi(A + \gamma I) = \pi(A)$. However, the labels of the linear factors are shifted, so $\tau(A + \gamma I)$ can differ from $\tau(A)$; for example, $\tau(0_N) = 1$, whereas $\tau(I_N) = p$. Thus, the pre-period depends on the positions of the linear roots in the ordered shift cycle, whereas the period is invariant under translations by elements of $\mathbb{F}_p$.*

For a monic irreducible polynomial g of degree $d \geq 2$, choose a root $\alpha \in \mathbb{F}_{p^d}$ and define the following:

$$\eta(g) = \mathrm{ord}_{\mathbb{F}_{p^d}^{\times}}(\alpha^p - \alpha).$$

Here, the multiplicative order is the smallest positive integer h for which $(\alpha^p - \alpha)^h = 1$. If $\alpha' = \alpha^{p^r}$ is another root, then $(\alpha')^p - \alpha' = (\alpha^p - \alpha)^{p^r}$. Since Frobenius preserves the multiplicative order, $\eta(g)$ is independent of the choice of root. In general, $\mathrm{ord}_G(x)$ denotes the multiplicative order of an element x of a finite group G, and we write $\mathrm{ord}(x)$ when $G = \mathbb{F}_p^{\times}$.

2.2. Linear primary factors

Proposition 2.3. *Let*

$$S = \mathbb{F}_p[y]/((y + \lambda)^f), \qquad \lambda \in \{0, 1, \ldots, p-1\},$$

and let ξ denote the image of y. The local product first becomes zero at $(f-1)p + \lambda + 1$. This is the pre-period, and the period is 1.

Proof. With $n = \xi + \lambda$, we have $n^f = 0$ and $n^{f-1} \neq 0$. Among the factors $\xi + j$, only those with $j \equiv \lambda \pmod{p}$ are nonunits, and each of them equals n. Therefore, the product is a unit multiple of n^r, where r counts these occurrences. The f-th occurrence is included at length $(f-1)p + \lambda + 1$. This is the first zero, and all later products are zero. If the sequence were periodic from an earlier index, a nonzero term would recur among the later terms, all of which are zero; this is impossible. □

2.3. Nonlinear primary factors

Lemma 2.4. *Let $g \in \mathbb{F}_p[y]$ be monic irreducible of degree at least two, let $S = \mathbb{F}_p[y]/(g^f)$, and let ξ be the image of y. Then, $\xi^p - \xi$ is a unit of S, the local sequence has a pre-period of 1, and its period is*

$$p \operatorname{ord}_{S^\times}(\xi^p - \xi).$$

Proof. Each $y + j$, $j \in \mathbb{F}_p$, is coprime to g, so all $\xi + j$ and their product $u = \xi^p - \xi$ are units. For every $k \geq 0$ and $m \geq 1$, a product of pm consecutive shifts contains each residue m times, giving the following:

$$P_{k+pm}(\xi) P_k(\xi)^{-1} = u^m.$$

The order $d = \operatorname{ord}_{S^\times}(u)$ is finite. Taking $m = d$ shows that the sequence is periodic from $k = 0$, so it has a pre-period of 1 under Definition 1.2.

For an integer n, write $\bar{n}\, 1_S$ for its image in S. Suppose that $P_{k+t}(\xi) = P_k(\xi)$ for every sufficiently large k. Then, for every such k,

$$1 = P_{k+t}(\xi) P_k(\xi)^{-1} = \prod_{j=0}^{t-1} (\xi + \overline{k+j}\, 1_S).$$

Dividing this identity at $k+1$ by the identity at k leaves

$$(\xi + \overline{k+t}\, 1_S)/(\xi + \bar{k}\, 1_S) = 1,$$

so $p \mid t$. Writing $t = pm$, the first identity then gives $u^m = 1$, and thus $d \mid m$. Hence, every such t is a multiple of pd, which is already a period from the beginning. □

Proposition 2.5. *In the setting of Lemma 2.4,*

$$\operatorname{ord}_{S^\times}(\xi^p - \xi) = \eta(g) p^{\lceil \log_p f \rceil}.$$

Thus, the products in S are periodic from the first term, and their period is

$$p^{1+\lceil \log_p f \rceil} \eta(g).$$

Proof. Set $Q(y) = y^p - y$, $\eta = \eta(g)$, and $H(y) = Q(y)^\eta - 1$. For a root α of g, $H(\alpha) = 0$ and $H'(\alpha) = -\eta Q(\alpha)^{\eta-1} \neq 0$. Here, $Q(\alpha) \neq 0$, and $p \nmid \eta$ because η divides $p^{\deg g} - 1$. Consequently, $H = gW$ with $\gcd(g, W) = 1$. In S, put $q = Q(\xi)$ and $h = g(\xi)W(\xi)$. Then, $q^\eta = 1 + h$, and, since $W(\xi)$ is a unit,

$$h^m = 0 \quad \Longleftrightarrow \quad m \geq f.$$

For $f = 1$, the element $1 + h$ equals one. For $f > 1$, let $e = \lceil \log_p f \rceil$, so $p^{e-1} < f \le p^e$. The identity $(1+h)^{p^r} = 1 + h^{p^r}$ gives $(1+h)^{p^{e-1}} \neq 1$ and $(1+h)^{p^e} = 1$. Thus, $1 + h$ has an order of p^e, and this also holds for $f = 1$ with $e = 0$.

If $q^m = 1$, then reduction modulo g forces $\eta \mid m$. For $m = \eta s$, we have $q^m = (1+h)^s$, which equals one exactly when $p^e \mid s$. Hence, q has an order of ηp^e. Lemma 2.4 gives the period of the product sequence. □

The factor $p^{\lceil \log_p f \rceil}$ is the one in the classical formula for the order of a power of an irreducible polynomial [23, Chapter 3]; here, it arises for the unit $\xi^p - \xi$ rather than for ξ.

2.4. The general formulas

Theorem 2.6. *Let $A \in M_N(\mathbb{F}_p)$, and factor*

$$\mu_A(y) = \prod_i g_i(y)^{f_i} \tag{2.1}$$

into distinct monic irreducibles, with linear factors written $g_i = y + \lambda_i$, $\lambda_i \in \{0, 1, \ldots, p-1\}$, as in Section 2.1. Then,

$$\tau(A) = \max\left(\{1\} \cup \{(f_i - 1)p + \lambda_i + 1 : \deg g_i = 1\}\right) \tag{2.2}$$

and

$$\pi(A) = \operatorname*{lcm}_{\deg g_i \ge 2} \left(p^{1+\lceil \log_p f_i \rceil} \eta(g_i) \right), \tag{2.3}$$

where the least common multiple over the empty set is 1.

The same formulas hold for a in any finite-dimensional $\mathbb{F}_p$-algebra $\mathcal{A}$, with μ_a, $\tau_{\mathcal{A}}(a)$ and $\pi_{\mathcal{A}}(a)$ in place of μ_A, $\tau(A)$, and $\pi(A)$.

Proof. The Chinese remainder theorem identifies $\mathbb{F}_p[a]$ with $\prod_i \mathbb{F}_p[y]/(g_i^{f_i})$. We apply Proposition 2.3 or Proposition 2.5 to each factor, according to whether g_i is linear or nonlinear. By Lemma 2.1, the maximum of the local pre-periods and the least common multiple of the local periods give the two displayed formulas. The matrix case is $\mathcal{A} = M_N(\mathbb{F}_p)$, $a = A$. □

For quadratic factors, we can express $\eta(g)$ in terms of the order of the discriminant.

Corollary 2.7. *Let p be odd and let*

$$g = y^2 - cy + d \in \mathbb{F}_p[y]$$

be irreducible, with the discriminant $\Delta = c^2 - 4d$. Then, Δ is a nonsquare in $\mathbb{F}_p^\times$, its multiplicative order $m = \operatorname{ord}(\Delta)$ is an even divisor of $p-1$ not dividing $(p-1)/2$, and

$$\eta(g) = 2m = 2\operatorname{ord}(\Delta). \tag{2.4}$$

Consequently, if $S = \mathbb{F}_p[y]/(g^f)$ and ξ is the class of y, then

$$\tau_S(\xi) = 1 \quad \text{and} \quad \pi_S(\xi) = 2m\, p^{1+\lceil \log_p f \rceil}.$$

For $A \in M_N(\mathbb{F}_p)$, if every nonlinear factor of μ_A is quadratic, with discriminants Δ_i and exponents f_i, then

$$\pi(A) = 2 \operatorname*{lcm}_i(\operatorname{ord}(\Delta_i))\, p^{1+\max_i \lceil \log_p f_i \rceil}, \tag{2.5}$$

and $\pi(A) = 1$ if there is no nonlinear factor. In particular, if $A \in M_2(\mathbb{F}_p)$ has an irreducible quadratic characteristic polynomial with the discriminant Δ, then A has a pre-period of 1 and a period of $2p \operatorname{ord}(\Delta)$.

Proof. The irreducibility makes Δ a nonzero nonsquare. The square subgroup of $\mathbb{F}_p^\times$ has an order of $(p-1)/2$. Hence, the order m of Δ divides $p-1$ but not $(p-1)/2$, and is even. The two roots of g are α and $\alpha^p = c - \alpha$. For $B = \alpha^p - \alpha$, we have $B = c - 2\alpha$ and $B^2 = \Delta$. Since $\operatorname{ord}(B^2) = m$, the order of B is either m or $2m$. The first possibility cannot occur because

$$B^m = \Delta^{m/2} \neq 1.$$

Hence, $\eta(g) = 2m$. The local period follows from Proposition 2.5. For several quadratic factors, Theorem 2.6 takes their least common multiple. Each $\operatorname{ord}(\Delta_i)$ is coprime to p, so the p-part of the period is determined by the largest exponent. □

Remark 2.8. *Over $\mathbb{F}_2$, the unique irreducible quadratic is $g = y^2 + y + 1$. A root satisfies $\alpha^2 - \alpha = 1$, so $\eta(g) = 1$. By Proposition 2.5, the primary power g^f has a local period of $2^{1+\lceil \log_2 f \rceil}$.*

Corollary 2.9. *Let p be an odd Fermat prime, that is, $p = 2^v + 1$ with v a power of two. For every irreducible quadratic $g \in \mathbb{F}_p[y]$, $\eta(g) = 2(p-1)$. In particular, if $A \in M_2(\mathbb{F}_p)$ has an irreducible quadratic characteristic polynomial, then*

$$\tau(A) = 1, \qquad \pi(A) = 2p(p-1).$$

Proof. Since $p - 1$ is a power of two, every nonsquare in $\mathbb{F}_p^\times$ has an order of $p - 1$. Apply Corollary 2.7 to the discriminant. □

For example, a nonsquare in $\mathbb{F}_7$ has an order of either $m = 2$ or $m = 6$. Therefore, the 21 irreducible quadratics satisfy $\eta(g) \in \{4, 12\}$. Section 3.2 determines how many quadratics correspond to each order.

2.5. Stable and amicable elements

Lemma 2.10. *For $a \in \mathcal{A}$, the following are equivalent:*

(i) a is Stable;
(ii) $P_k(a)$ is eventually zero; and
(iii) μ_a splits completely over $\mathbb{F}_p$.

For $A \in M_N(\mathbb{F}_p)$, these conditions are also equivalent to triangularizability over $\mathbb{F}_p$.

Proof. If the eventual constant is z, then two consecutive recurrence relations give the following:

$$z(a + k1_{\mathcal{A}}) = z = z(a + (k+1)1_{\mathcal{A}}).$$

Subtracting yields $z = 0$. Conversely, an eventually zero sequence has a period of 1. Theorem 2.6 shows that a period of 1 is equivalent to the absence of nonlinear factors. For matrices, a split minimal polynomial is equivalent to triangularizability over the base field, by successively choosing an eigenvector and passing to the quotient. □

Corollary 2.11. *Let*

$$\nu(\mathcal{A}) = \max\{\mathrm{nilind}(n) : n \in \mathcal{A} \text{ is nilpotent}\},$$

where $\mathrm{nilind}(n) = \min\{s \geq 1 : n^s = 0\}$. *Then,* $1 \leq \nu(\mathcal{A}) \leq D$,

$$\tau_{\mathcal{A}}(a) \leq p\,\nu(\mathcal{A}) \quad \text{for every } a \in \mathcal{A},$$

and equality is attained by a Stable element.

In particular, for matrices, $\max_{A \in M_N(\mathbb{F}_p)} \tau(A) = Np$. *Equality holds for* $A = I + J_N(0)$, *where* $J_N(0)$ *is the nilpotent Jordan block of size* N.

Proof. For a linear primary factor $(y+\lambda)^f$, the Chinese remainder theorem supplies an idempotent $e_\lambda(a)$ that is one on this component and zero on the others. The element $(a+\lambda 1_{\mathcal{A}})e_\lambda(a)$ has a nilpotency index f, whence $f \leq \nu(\mathcal{A})$. Its local pre-period is at most $fp \leq p\nu(\mathcal{A})$. Nonlinear components have a pre-period of 1.

Choose a nilpotent n of index $\nu(\mathcal{A})$. The element $1_{\mathcal{A}} + n$ has a minimal polynomial $(y-1)^{\nu(\mathcal{A})}$, so its pre-period is $p\nu(\mathcal{A})$ by Theorem 2.6. Recall that a nilpotent of index s has linearly independent powers $1, n, \ldots, n^{s-1}$. Hence, $\nu(\mathcal{A}) \leq D$. In $M_N(\mathbb{F}_p)$, the Cayley–Hamilton theorem bounds the nilpotency index by N, and $J_N(0)$ attains it. Thus, the maximal pre-period is Np, attained by $I + J_N(0)$. □

For comparison, $J_N(0)$ has a minimal polynomial y^N and a pair $((N-1)p+1, 1)$, so its pre-period is strictly below Np. For a non-Stable example over $\mathbb{F}_3$, set

$$A_c = (cI_2 + J_2(0)) \oplus C(y^2+1), \qquad c \in \mathbb{F}_3.$$

The polynomial $y^2 + 1$ is irreducible with a discriminant of 2, of order 2 in $\mathbb{F}_3^\times$, so its companion block has pair $(1, 12)$. The linear block of A_1 has a pair $(6, 1)$; hence, A_1 has a pair $(6, 12)$, and $6 < 4 \cdot 3$. On the other hand,

$$\mathcal{B} = \mathbb{F}_3[A_1] \simeq \mathbb{F}_3[t]/(t^2) \times \mathbb{F}_9.$$

Every nilpotent in $\mathcal{B}$ has a zero field component and first component a multiple of t, so $\nu(\mathcal{B}) = 2$. Thus, the same element attains the algebra bound $3\nu(\mathcal{B}) = 6$ with a nontrivial period, although the full matrix-algebra bound is strict.

Additionally, the family illustrates the role of the integer root labels: for $c = 0$, 2, and 1, the factor $y - c = y + \lambda$ has representative $\lambda = 0$, 1, and 2, respectively. Formula (2.2) gives $\tau(A_c) = 3 + \lambda + 1$, while the fixed nonlinear block gives $\pi(A_c) = 12$. Hence, A_0, A_2, and A_1 have pairs $(4, 12)$, $(5, 12)$, and $(6, 12)$, respectively: changing the linear label changes the pre-period while leaving the period unchanged.

Theorem 2.12. *If* p *is odd, then there is no Amicable matrix in* $M_N(\mathbb{F}_p)$. *If* $p = 2$, *then a matrix* A *is Amicable if and only if the nonlinear part of* μ_A *is exactly* $y^2 + y + 1$ *to exponent one. The same*

conclusions hold for elements of finite-dimensional $\mathbb{F}_p$-algebras: if p is odd, then no element has period 2; and if $p = 2$, then an element a has period 2 if and only if the nonlinear part of μ_a is exactly $y^2 + y + 1$ to exponent one.

Proof. By Theorem 2.6, every period greater than 1 is divisible by p, ruling out period 2 when p is odd. Now, let $p = 2$. A nonlinear local period equals 2 precisely when its exponent is one and $\eta(g) = 1$. Then, a root satisfies $\alpha^2 - \alpha = 1$, so $g = y^2 + y + 1$. The least common multiple of all local periods is 2 exactly when this is the only nonlinear factor and it occurs to exponent one. □

3. Possible pairs and matrix counts

By Lemma 2.10, the Stable matrices in $M_N(\mathbb{F}_p)$ are exactly the triangularizable ones, which are counted by a classical cycle-index formula [14, Lemma 2.3]; additionally, see [19]. Since the maximum nilpotency index in $M_N(\mathbb{F}_p)$ is N, Corollary 2.11 gives the sharp maximum pre-period Np. Theorem 2.12 restricts matrices with a period of 2 to $p = 2$, with $(y^2 + y + 1)$-primary partition (1^ℓ) for some $\ell \geq 1$ (see Section 3.4).

Matrices are counted individually, not up to similarity, but the counting is organized by similarity classes.

3.1. Realizable pairs and conjugacy classes

Recall that conjugation by an invertible matrix gives a similar matrix. More generally, the unit group $\mathcal{A}^\times$ acts by conjugation. Let C be the set of elements with a prescribed pair, or the set of Stable, Amicable, or Sociable elements. We write Cl_C for the collection of conjugacy classes contained in C. For an element a, $C_{\mathcal{A}^\times}(a)$ is the group of invertible elements that commute with a.

Proposition 3.1. *For each such set of elements,*

$$|C| = \sum_{[a]\in \mathrm{Cl}_C} \frac{|\mathcal{A}^\times|}{|C_{\mathcal{A}^\times}(a)|}.$$

For $\mathcal{A} = M_N(\mathbb{F}_p)$, the acting group is $\mathrm{GL}_N(\mathbb{F}_p)$, and the sum is over matrix similarity classes.

Proof. Conjugation preserves both values, since

$$P_k(uau^{-1}) = uP_k(a)u^{-1}.$$

By the orbit-stabilizer theorem, the quotient in the sum is the number of elements in the conjugacy class of a. Adding these class sizes counts every element of C once. □

For a full matrix algebra, these orbits are the similarity classes described by rational canonical form, which also determines their centralizer orders. By Theorem 2.6, every nontrivial period is divisible by p. The periods that occur in $M_N(\mathbb{F}_p)$ are the least common multiples $\mathrm{lcm}_i(p^{1+\lceil \log_p f_i \rceil}\eta(g_i))$ for collections of distinct nonlinear irreducibles satisfying $\sum_i f_i \deg g_i \leq N$. In the next theorem, we will also take the pre-period into account.

For a positive integer t, we choose nonlinear companion blocks whose local periods have a least common multiple t. A block $C(g_i^{f_i})$ has a size of $f_i \deg g_i$. The smallest possible total size of these blocks is called the *nonlinear dimension cost*:

$$\kappa_p(t) = \min\left\{ \sum_{i=1}^{n} f_i \deg g_i : \begin{array}{l} n \geq 0, \quad g_1, \ldots, g_n \text{ are distinct monic irreducibles,} \\ \deg g_i \geq 2, \quad f_i \geq 1, \\ \operatorname{lcm}_{1\leq i\leq n}\left(p^{1+\lceil \log_p f_i\rceil}\eta(g_i)\right) = t \end{array} \right\},$$

where the empty collection gives $\kappa_p(1) = 0$, and we set $\kappa_p(t) = \infty$ when no collection gives a period of t. The following theorem shows that if a period of $t > 1$ occurs, then $\kappa_p(t)$ is the smallest matrix size in which it occurs. Every such period is divisible by p. Write $v_p(t)$ for the exponent of p in t. Since each $\eta(g_i)$ divides $p^{\deg g_i} - 1$ and is therefore prime to p, for $t > 1$, every collection in the definition of $\kappa_p(t)$ satisfies $v_p(t) = 1 + \max_i \lceil \log_p f_i \rceil$. Hence, if $v_p(t) = r + 1 \geq 2$, then at least one nonlinear factor satisfies $\lceil \log_p f_i \rceil = r$, and so $f_i \geq p^{r-1} + 1$. Its degree is at least two, giving the following:

$$\kappa_p(t) \geq 2(p^{r-1} + 1), \qquad v_p(t) = r + 1, \quad r \geq 1.$$

If $v_p(t) = 1$, then a nontrivial period still requires a nonlinear factor, so $\kappa_p(t) \geq 2$.

Theorem 3.2. *Fix a prime p, a size $N \geq 1$, and positive integers τ, t. There exists a matrix $A \in M_N(\mathbb{F}_p)$ with $(\tau(A), \pi(A)) = (\tau, t)$ if and only if*

$$\begin{cases} \kappa_p(t) \leq N, & \tau = 1, \\ \kappa_p(t) + \left\lceil \dfrac{\tau}{p} \right\rceil \leq N, & \tau \geq 2. \end{cases} \tag{3.1}$$

Equivalently, put $\kappa = \kappa_p(t)$. If $\kappa > N$, then a period of t does not occur in $M_N(\mathbb{F}_p)$. If $\kappa \leq N$, then the set of all pre-periods that occur together with period t is as follows:

$$\mathcal{T}_{N,p}(t) = \begin{cases} \{1\}, & \kappa = N, \\ \{1, 2, \ldots, p(N - \kappa)\}, & \kappa < N. \end{cases} \tag{3.2}$$

Proof. Suppose A has a pair (τ, t), and let D_{nl} be the degree of the nonlinear part of μ_A. Its local periods have a least common multiple t, so $\kappa_p(t) \leq D_{\mathrm{nl}} \leq \deg \mu_A \leq N$. If $\tau \geq 2$, then a linear factor $(y + \lambda)^f$ must attain this pre-period. From $\tau = (f - 1)p + \lambda + 1$, with $0 \leq \lambda < p$, we obtain $f = \lceil \tau/p \rceil$. This factor is coprime to the nonlinear part, and therefore

$$N \geq \deg \mu_A \geq D_{\mathrm{nl}} + f \geq \kappa_p(t) + \lceil \tau/p \rceil.$$

Conversely, assume the stated dimension bound. Let B be the block diagonal sum of nonlinear companion blocks with a combined period of t and a total size of $\kappa_p(t)$, taking B empty if $t = 1$. For $\tau = 1$, the matrix $B \oplus 0_{N-\kappa_p(t)}$ has the required pair. For $\tau \geq 2$, set $f = \lceil \tau/p \rceil$ and $\lambda = \tau - (f - 1)p - 1$. Then, $0 \leq \lambda < p$, and

$$A = B \oplus C((y + \lambda)^f) \oplus 0_{N-\kappa_p(t)-f}.$$

The middle block has a pre-period of τ and a period of 1. Its linear primary factor is coprime to every nonlinear factor used in B. A positive-size zero block has a pair $(1, 1)$, so Lemma 2.1 shows that it

changes neither the pre-period nor the period. In terms of the minimal polynomial, it contributes y to exponent one. If $\lambda = 0$, then that factor is already present to exponent f, so its exponent remains f; otherwise, it is an additional exponent-one factor, with a local pair $(1, 1)$.

Zero-size summands are omitted. Solving the dimension bound for τ gives the stated set of pre-periods, including $\{1\}$ when $\kappa_p(t) = N$. □

For every positive integer h, the direct-sum identities are as follows:

$$(\tau(A \oplus 0_h), \pi(A \oplus 0_h)) = (\tau(A), \pi(A)),$$
$$(\tau(A \oplus I_h), \pi(A \oplus I_h)) = (\max\{\tau(A), p\}, \pi(A)).$$

Indeed, 0_h has a pair $(1, 1)$, whereas I_h has a pair $(p, 1)$. The construction above uses zero padding.

To decide whether $\kappa_p(t) \le N$, it suffices to consider irreducibles of degree at most N, exponents $1 \le f \le \lfloor N/\deg g \rfloor$, and collections with a total size of at most N. This is a finite feasibility search. Failure to find a realization within this dimension bound does not imply $\kappa_p(t) = \infty$.

Corollary 3.3. *Let p be odd, let m be an even divisor of $p - 1$ not dividing $(p - 1)/2$, let r be a nonnegative integer, and put $t = 2m\,p^{r+1}$. Then,*

$$\kappa_p(t) = \begin{cases} 2, & r = 0, \\ 2(p^{r-1} + 1), & r \ge 1. \end{cases} \tag{3.3}$$

Consequently, with $\kappa = \kappa_p(t)$, the pair (τ, t) occurs in $M_N(\mathbb{F}_p)$ exactly when $N \ge \kappa$ and either $\tau = 1$ or $2 \le \tau \le p(N - \kappa)$. For an odd Fermat prime, the only admissible m is $p - 1$, and these periods are $t_r = 2(p - 1)p^{r+1}$.

Proof. First, we prove the lower bound. If $r = 0$, then any realization of the nontrivial period t requires a nonlinear factor, and hence at least two dimensions. If $r \ge 1$, then $v_p(t) = r + 1$. Since every $\eta(g_i)$ is prime to p, any realization satisfies $v_p(t) = 1 + \max_i \lceil \log_p f_i \rceil$, so at least one nonlinear primary exponent f_i satisfies $\lceil \log_p f_i \rceil = r$. Thus, $f_i \ge p^{r-1} + 1$, and its degree is at least two, giving a dimension of at least $2(p^{r-1} + 1)$.

For a matching construction, choose $\Delta \in \mathbb{F}_p^\times$ of order m, which is possible because $\mathbb{F}_p^\times$ is cyclic. It is a nonsquare because $m \nmid (p - 1)/2$. Therefore, $g = y^2 - \Delta/4$ is irreducible, with a discriminant Δ and $\eta(g) = 2m$ by Corollary 2.7. Set $f = 1$ if $r = 0$, and $f = p^{r-1} + 1$ if $r \ge 1$. Then, $\lceil \log_p f \rceil = r$, so the single quadratic-primary companion block $C(g^f)$ has a size of $2f$ and a period of

$$2m\,p^{1+\lceil \log_p f \rceil} = 2m\,p^{r+1} = t.$$

It attains the lower bound. For $r \ge 1$, this is one companion block with a size of $2f$, rather than a two-by-two block. Theorem 3.2 gives the possible pre-periods, and Corollary 2.9 gives the Fermat-prime case. □

For $p = 3$, the period 12 has a minimum dimension of 2. For this period, the possible pre-periods in matrix sizes 2, 3, and 4 are, respectively,

$$\{1\}, \qquad \{1, 2, 3\}, \qquad \{1, 2, 3, 4, 5, 6\}.$$

The periods 36 and 108 require dimensions 4 and 8, respectively. More generally, for $N \geq 3$ and $2 \leq \tau \leq p(N-2)$, put $f = \lceil \tau/p \rceil$ and $\lambda = \tau - (f-1)p - 1$. The explicit matrix

$$C(g) \oplus C((y+\lambda)^f) \oplus 0_{N-2-f}$$

has a pair $(\tau, 2m\,p)$ for any irreducible quadratic g whose discriminant Δ satisfies $\mathrm{ord}(\Delta) = m$.

3.2. Pre-periods and periods of two-by-two matrices

Theorem 3.4. *Let p be any prime. In $M_2(\mathbb{F}_p)$, for every $1 \leq s \leq p$,*

$$\#\{A : (\tau(A), \pi(A)) = (s,1)\} = 1 + (s-1)p(p+1), \quad \#\{A : (\tau(A), \pi(A)) = (p+s,1)\} = p^2 - 1, \quad (3.4)$$

so there are $p^4 - p^2(p-1)^2/2$ Stable matrices. The remaining $p^2(p-1)^2/2$ matrices have a pre-period of 1. If p is odd, then for every even divisor m of $p-1$ not dividing $(p-1)/2$,

$$\#\{A : (\tau(A), \pi(A)) = (1, 2pm)\} = p^2(p-1)\varphi(m), \quad (3.5)$$

where φ is Euler's function, and there are no other pairs. If $p = 2$, then the two non-Stable matrices have pair $(1,2)$. Thus, the set of all possible periods, called the period spectrum, is

$$\{1\} \cup \{2pm : m \mid p-1,\ m \text{ even},\ m \nmid (p-1)/2\} \quad (p \text{ odd}), \qquad \{1,2\} \quad (p=2), \quad (3.6)$$

and this set has exactly two elements if and only if $p = 2$ or p is a Fermat prime.

Proof. Up to similarity, there are three types of matrices with split characteristic polynomials, namely, scalar matrices, diagonal matrices with distinct eigenvalues, and single Jordan blocks. All are Stable. Fix $1 \leq s \leq p$ and write $\lambda = s - 1$. The scalar $-\lambda I$ has a pair $(s,1)$. For distinct eigenvalues $-\lambda_1, -\lambda_2$, ordered by $0 \leq \lambda_1 < \lambda_2 < p$, the pre-period is $\lambda_2 + 1$. Thus, $\lambda_2 = s - 1$ leaves $s-1$ choices for λ_1. Each class has a size of $p(p+1)$, since its invertible centralizer has an order of $(p-1)^2$. The Jordan block at $-\lambda$ has a pair $(p+s,1)$ and a class size of p^2-1, from the centralizer order $p(p-1)$. These contributions give the two Stable formulas.

The remaining matrices have an irreducible quadratic characteristic polynomial g. Their class size is $p(p-1)$, from the centralizer $\mathbb{F}_{p^2}^{\times}$, and their pair is $(1, p\eta(g))$. For an odd prime p, each nonsquare discriminant gives p monic quadratics, with the trace chosen freely. There are $\varphi(m)$ nonsquares of each admissible order m. Hence, the number with the pair $(1, 2pm)$ is $p\varphi(m) \cdot p(p-1) = p^2(p-1)\varphi(m)$. The $(p-1)/2$ nonsquare discriminants account for all irreducible quadratics and hence all nonsplit matrices. In characteristic two, the unique irreducible quadratic gives two matrices of period 2.

For an odd prime p, write $p - 1 = 2^v u$, with u an odd integer. The admissible orders are $m = 2^v u'$, $u' \mid u$. Exactly one such order occurs if and only if $u = 1$, so $p = 2^v + 1$. Since $2^v + 1$ is prime, v must be a power of two. Conversely, a Fermat prime has $p - 1$ a power of two. This is precisely the definition used in Corollary 2.9. □

Table 1 displays the four similarity families underlying the count. In the first three rows, $1 \leq s \leq p$ and $\lambda = s - 1$. In the last row, p is odd and $m \mid p-1$, $m \nmid (p-1)/2$.

Table 1. Similarity families in $M_2(\mathbb{F}_p)$.

Family	Pair	Classes	Class size	Matrices
Scalar $-\lambda I$	$(s, 1)$	1	1	1
Distinct eigenvalues $-\lambda_1, -\lambda, 0 \le \lambda_1 < \lambda$	$(s, 1)$	$s-1$	$p(p+1)$	$(s-1)p(p+1)$
Jordan block $-\lambda I + J_2(0)$	$(p+s, 1)$	1	p^2-1	p^2-1
Irreducible quadratic, discriminant order m	$(1, 2pm)$	$p\varphi(m)$	$p(p-1)$	$p^2(p-1)\varphi(m)$

For $p = 2$, the last family instead consists of one class of size two with a pair $(1, 2)$. Summing over s and, when p is odd, over the admissible m, the four families exhaust all matrices as follows:

$$p + \binom{p}{2} p(p+1) + p(p^2-1) + \frac{p^2-p}{2}\, p(p-1) = p^4.$$

For $p = 7$, the two admissible orders $m = 2, 6$ give 7 irreducible quadratics with $\eta(g) = 4$ and 14 with $\eta(g) = 12$. Thus, the period spectrum of $M_2(\mathbb{F}_7)$ is $\{1, 28, 84\}$. At an odd Fermat prime, it is $\{1, 2p(p-1)\}$, with $p^2(p-1)^2/2$ matrices with a nontrivial period.

In higher dimensions, further periods occur even at Fermat primes. For $p = 3$, the polynomial $g = y^3 + 2y + 2$ has no root in $\mathbb{F}_3$ and is irreducible. A root satisfies $\alpha^3 - \alpha = 1$, so the companion matrix of g has a period of 3. For every odd p, the companion matrix of g^2, with g being an irreducible quadratic of discriminant Δ, belongs to $M_4(\mathbb{F}_p)$ and has a period of $2\,\mathrm{ord}(\Delta)p^2$. Adding zero blocks gives matrices with the same periods in every larger dimension.

3.3. Examples of other algebras

The local formulas apply to any finite-dimensional algebra, but the element counts depend on the algebra. The dual numbers and the quadratic field extension show this. Both have a dimension of two over $\mathbb{F}_p$. Both have exactly one element of each pair $(s, 1)$, $1 \le s \le p$, but their remaining contributions are different.

Example 3.5. *Consider $\mathcal{A} = \mathbb{F}_p[\varepsilon]/(\varepsilon^2)$. For $a \in \mathbb{F}_p$, write $a = -\lambda(a)$, where $\lambda(a) \in \{0, 1, \ldots, p-1\}$. If $b \neq 0$, then $a + b\varepsilon + \lambda(a) = b\varepsilon$ is nonzero and has square zero. Therefore, Proposition 2.3 gives*

$$\mu_{a+b\varepsilon}(y) = \begin{cases} y + \lambda(a), & b = 0, \\ (y + \lambda(a))^2, & b \neq 0, \end{cases} \qquad \tau_{\mathcal{A}}(a + b\varepsilon) = \begin{cases} \lambda(a) + 1, & b = 0, \\ p + \lambda(a) + 1, & b \neq 0, \end{cases}$$

for the minimal polynomial and pre-period. All elements are Stable, and their pre-periods have the distribution

$$\#\{x \in \mathcal{A} : \tau_{\mathcal{A}}(x) = s\} = \begin{cases} 1, & 1 \le s \le p, \\ p-1, & p+1 \le s \le 2p, \\ 0, & \textit{otherwise}. \end{cases}$$

Thus, $(|\mathrm{Stable}|, |\mathrm{Amicable}|, |\mathrm{Sociable}|) = (p^2, 0, 0)$, *$\nu(\mathcal{A}) = 2$, and* $\max_x \tau_{\mathcal{A}}(x) = 2p$.

Example 3.6. *Now let $\mathcal{A} = \mathbb{F}_{p^2}$. The Stable elements are precisely the p elements of $\mathbb{F}_p$, with pre-periods $1, \ldots, p$. If $a \notin \mathbb{F}_p$, then its minimal polynomial is an irreducible quadratic, say g, and a has*

$\tau_{\mathcal{A}}(a) = 1$ *and* $\pi_{\mathcal{A}}(a) = p\,\eta(g)$*. Each quadratic contributes two roots. For an odd prime* p*, the counting argument of Theorem 3.4 gives*

$$\#\{a \in \mathbb{F}_{p^2} : \pi_{\mathcal{A}}(a) = 2pm\} = 2p\varphi(m)$$

for every even divisor m *of* $p-1$ *not dividing* $(p-1)/2$*, and all* $p^2 - p$ *elements outside the base field are Sociable. For* $p = 2$*, the two elements outside the base field are Amicable. Thus,*

$$(|\text{Stable}|, |\text{Amicable}|, |\text{Sociable}|) = \begin{cases} (2, 2, 0), & p = 2, \\ (p, 0, p^2 - p), & p \text{ odd}, \end{cases} \qquad \nu(\mathcal{A}) = 1, \qquad \max_x \tau_{\mathcal{A}}(x) = p.$$

For $p = 3$ *and* $p = 5$*, every element outside the base field has a period of* 12 *and* 40*, respectively.*

3.4. Cycle-index counting for matrices

We will count matrices with the same rational canonical form together using Proposition 3.1. For each monic irreducible g, write $\rho_g = (\rho_{g,1}, \rho_{g,2}, \ldots)$ for the list of exponents of its companion blocks, in nonincreasing order. The block for the exponent $\rho_{g,j}$ has a size of $(\deg g)\rho_{g,j}$. Such a list is a partition, and the collection of these partitions specifies one similarity class. They satisfy

$$\sum_g (\deg g)|\rho_g| = N,$$

and an absent factor is assigned the empty partition. The largest part gives the exponent of g in the minimal polynomial. We set $\max \varnothing = 0$ for an absent factor. Therefore, applying Theorem 2.6 to

$$\mu = \prod_g g^{\max \rho_g}$$

determines the invariants $\tau((\rho_g)_g)$ and $\pi((\rho_g)_g)$ of each type.

For a partition ρ, let $c_q(\rho)$ be the number of invertible $\mathbb{F}_q[y]$-module maps from $\bigoplus_j \mathbb{F}_q[y]/(y^{\rho_j})$ to itself, and set $c_q(\varnothing) = 1$. If ρ' is the conjugate partition and $m_j(\rho)$ is the number of parts equal to j, then

$$c_q(\rho) = q^{\sum_i (\rho_i')^2} \prod_{j \geq 1} \prod_{h=1}^{m_j(\rho)} (1 - q^{-h}).$$

This is equivalent to Kung's formula [12], reproduced in the proof of [14, Lemma 2.2]. For a degree-d irreducible g, the residue field $\mathbb{F}_p[y]/(g)$ has a size of $q = p^d$. The automorphism count of the corresponding g-primary module depends only on this residue-field size and the partition; it is $c_{p^d}(\rho_g)$. This explains the change from p to $p^{\deg g}$, without changing the original coefficient field of the matrix. Maps commuting with the matrix preserve its primary summands, so, by [14, Lemma 2.1 and the proof of Lemma 2.2], its invertible centralizer has an order of

$$\prod_g c_{p^{\deg g}}(\rho_g).$$

The partition sums have coefficients

$$\sum_\rho \frac{u^{|\rho|}}{c_q(\rho)} = \sum_{n \geq 0} b_n(q) u^n, \qquad b_n(q) = \frac{q^{n(n-1)/2}}{\prod_{j=1}^n (q^j - 1)}, \qquad b_0(q) = 1,$$

that is, $b_n(q) = \sum_{|\rho|=n} 1/c_q(\rho)$ [14, Lemma 2.2 and its proof]. Equivalently,

$$\sum_{n\geq 0} b_n(q)u^n = \prod_{j\geq 1}\left(1-\frac{u}{q^j}\right)^{-1} \qquad (|u|<q),$$

where the infinite product converges. Exact coefficient calculations through the degree N use only $b_0(q),\dots,b_N(q)$; no truncation of the infinite product is involved. For a prime power q, put

$$\Gamma_n(q) = |\operatorname{GL}_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i), \qquad \Gamma_0(q) = 1.$$

Let $J_{N,p}(s,t)$ be the number of matrices with a pre-period of s and a period of t. Adding the sizes of the classes with these invariants gives the following:

$$J_{N,p}(s,t) = \Gamma_N(p) \sum_{\substack{\sum_g (\deg g)|\rho_g|=N \\ \tau((\rho_g)_g)=s,\ \pi((\rho_g)_g)=t}} \frac{1}{\prod_g c_{p^{\deg g}}(\rho_g)}.$$

Theorem 3.2 decides exactly when this count is positive, that is, when at least one matrix has the prescribed pair. For Stable matrices, only the p linear irreducibles can occur (Lemma 2.10). Restricting the sum to them [14, Lemmas 2.2 and 2.3] gives the total number of Stable matrices (additionally, see [19]):

$$S_{N,p} = \Gamma_N(p) \sum_{\substack{n_0+\cdots+n_{p-1}=N \\ n_i\geq 0}} \prod_{i=0}^{p-1} b_{n_i}(p),$$

where n_i is the partition size for the i-th linear factor. For Amicable matrices in characteristic two, the only nonlinear factor is $g = y^2 + y + 1$. Its partition is $\rho_g = (1^\ell)$, meaning $\ell \geq 1$ companion blocks for g, each of size two. These blocks contribute the centralizer factor $c_4((1^\ell)) = \Gamma_\ell(4)$. If the two linear partitions have sizes n_0, n_1, then $n_0 + n_1 + 2\ell = N$. Therefore, by [14, Lemma 2.5], the total number of Amicable matrices is as follows:

$$A_{N,2} = \Gamma_N(2) \sum_{\ell=1}^{\lfloor N/2\rfloor} \frac{1}{\Gamma_\ell(4)} \sum_{\substack{n_0+n_1=N-2\ell \\ n_0,n_1\geq 0}} b_{n_0}(2)b_{n_1}(2).$$

Corollary 3.7. *Let $N \geq 1$. For odd p,*

$$(|\text{Stable}|, |\text{Amicable}|, |\text{Sociable}|) = (S_{N,p}, 0, p^{N^2} - S_{N,p}).$$

For $p = 2$,

$$(|\text{Stable}|, |\text{Amicable}|, |\text{Sociable}|) = (S_{N,2}, A_{N,2}, 2^{N^2} - S_{N,2} - A_{N,2}).$$

Proof. The primary factors allowed by Lemma 2.10 and Theorem 2.12 are precisely those summed in $S_{N,p}$ and $A_{N,2}$. Multiplying their reciprocal centralizer sums by $\Gamma_N(p)$ counts the corresponding matrices. All other matrices are Sociable, so their number is p^{N^2} minus these two counts. □

As a worked instance, take $N = p = 2$. We have $\Gamma_2(2) = 6$, $b_0(2) = b_1(2) = 1$, and

$$c_2((2)) = 2, \qquad c_2((1,1)) = 6, \qquad b_2(2) = \frac{1}{2} + \frac{1}{6} = \frac{2}{3}.$$

Therefore, the three compositions $(n_0, n_1) = (2,0), (1,1), (0,2)$ give the following:

$$S_{2,2} = 6(b_2(2)b_0(2) + b_1(2)^2 + b_0(2)b_2(2)) = 6\left(\frac{2}{3} + 1 + \frac{2}{3}\right) = 14.$$

An Amicable type in dimension two has one exponent-one block for $y^2 + y + 1$ and no linear blocks. Its centralizer factor is $c_4((1)) = \Gamma_1(4) = 3$, so

$$A_{2,2} = \frac{\Gamma_2(2)}{\Gamma_1(4)} = \frac{6}{3} = 2.$$

Thus, all 16 matrices are accounted for and none is Sociable, in agreement with Theorem 3.4. For an odd prime p, the same formulas give

$$S_{2,p} = p^4 - p^2(p-1)^2/2.$$

For $N = 3$, they give $(352, 112, 48)$ at $p = 2$ and $S_{3,3} = 9909$.

3.5. Computational aspects

For a given matrix, the minimal polynomial μ_A is the largest invariant factor of the Frobenius normal form and can be deterministically computed with $O(N^3)$ operations in $\mathbb{F}_p$ [24]. The probabilistic algorithm of Cantor and Zassenhaus factors μ_A over $\mathbb{F}_p$ in an expected running time that is polynomial in N and $\log p$ [25, Chapter 14]. These standard computations should be distinguished from the multiplicative-order step. If $d = \deg g$, then $\eta(g)$ is the order of $\alpha^p - \alpha$ in the cyclic group $\mathbb{F}_{p^d}^{\times}$ of order $p^d - 1$. Given the prime factorization of $p^d - 1$, repeated squaring in $\mathbb{F}_p[y]/(g)$ and successive divisor tests determine this order: start with $p^d - 1$ and remove a prime factor whenever the corresponding power is still one (see [26, Algorithm 4.79] for the standard procedure). No classical algorithm is known that factors integers in a running time that is polynomial in their number of digits [25, Chapter 19], so the formulas do not by themselves give a general polynomial-time order algorithm. For a quadratic factor and an odd prime p, only $p - 1$ must be factored, because $\eta(g) = 2\,\mathrm{ord}(\Delta)$ by Corollary 2.7.

Once the irreducible factors and primary exponents have been selected, the companion-block constructions in Theorem 3.2 are explicit. When the coefficient lists of the selected primary polynomials are available, assembling their companion blocks and zero padding takes $O(N^2)$ entry writes in a dense representation; selecting suitable primary factors and forming their powers are separate costs. The dimension-capped search is finite but can involve many irreducibles and primary types. Therefore, the finite feasibility test for $\kappa_p(t) \le N$ and the finite sum for $J_{N,p}(s,t)$ do not imply practical efficiency at all dimensions.

The aggregate Stable and Amicable totals are more accessible. Define

$$B_p(u) = \sum_{n \ge 0} b_n(p) u^n,$$

and write $[u^N]F$ for the coefficient of u^N in a power series F. The Stable total is $\Gamma_N(p)[u^N]B_p(u)^p$, and the characteristic-two Amicable total is

$$\Gamma_N(2)[u^N]\left(B_2(u)^2 \sum_{\ell \geq 1} \frac{u^{2\ell}}{\Gamma_\ell(4)}\right).$$

Only coefficients through degree N are needed, so truncated polynomial multiplication computes these totals without enumerating p^{N^2} matrices. The full joint count requires the more detailed restrictions on primary factors and their largest parts. This distinction explains why aggregate totals can be feasible when a complete joint census is much more costly.

4. Conclusions and further questions

Theorem 2.6 determines the pre-period and period from the primary factors of the minimal polynomial, and Corollaries 2.7 and 2.9 make the quadratic case explicit. Theorem 3.2 gives the exact dimension criterion for a prescribed pair, Corollary 3.3 evaluates the cost for quadratic periods in odd characteristic, and Theorem 3.4 gives the complete two-by-two distribution. For matrices of arbitrary size, the joint count is an exact finite sum over similarity types.

The difference between odd characteristic and characteristic two is especially simple for a period of 2. At an odd prime p, every nontrivial period is divisible by p, so no matrix is Amicable. At $p = 2$, the nonlinear part of an Amicable minimal polynomial is exactly $y^2 + y + 1$ to exponent one, although the rational canonical form may contain several exponent-one blocks for that factor. The resulting aggregate counts can be computed by the truncated coefficient formulas in Section 3.5; a complete joint census involves more primary data.

Two questions concern the simplification of the exact formulas. Can the nonlinear dimension cost $\kappa_p(t)$ be expressed by a uniform arithmetic formula for periods involving higher-degree factors? For fixed $N \geq 3$ and p, can the finite sum for each joint count $J_{N,p}(s,t)$ be simplified to a more direct formula? The feasibility theorem and the cycle-index sums settle the structural questions without providing such simplifications in full generality.

For example, in characteristic three the irreducible polynomial $y^3 + 2y + 2$ from Section 3.2 has a companion matrix of size three and period 3. All one-dimensional matrices are Stable, and Theorem 3.4 gives the period spectrum $\{1, 12\}$ in size two; hence, $\kappa_3(3) = 3$. In size four, $C((y^2 + 1)^2)$ has a period of 36: the irreducible quadratic $y^2 + 1$ has a discriminant of 2, of order 2, and its primary exponent is 2. Corollary 3.3, with $m = 2$ and $r = 1$, proves $\kappa_3(36) = 4$, so this construction is minimal. A non-quadratic example in size four is $g = y^4 + y^3 + 2$. It has no root in $\mathbb{F}_3$ and is divisible by none of the irreducible quadratics $y^2 + 1$, $y^2 + y + 2$, and $y^2 + 2y + 2$, so it is irreducible. For a root α, the element $\beta = \alpha^3 - \alpha$ satisfies $\beta^{40} = 1$, $\beta^8 \neq 1$, and $\beta^{20} \neq 1$, so $\eta(g) = 40$ and the companion matrix of g has a period of 120. Since 5 divides none of $3 - 1$, $3^2 - 1$, and $3^3 - 1$, Theorem 2.6 excludes a period of 120 in sizes up to three, and $\kappa_3(120) = 4$. These examples give exact answers in dimensions three and four; the general lower bound before Theorem 3.2 and the dimension-capped feasibility test following it provide bounds and a finite method for other prescribed periods.

Over a coefficient field $\mathbb{F}_q$, $q = p^n$, a finite-dimensional algebra is also a finite-dimensional $\mathbb{F}_p$-algebra. Thus, Theorem 2.6 already applies using the minimal polynomial over $\mathbb{F}_p$. If we instead factor over $\mathbb{F}_q$, then the irreducible factors that divide some shift $y + j$, $j \in \mathbb{F}_p$, are exactly the factors

$y+\lambda$ with $\lambda \in \mathbb{F}_p$, and their primary powers behave as in Proposition 2.3. Every other irreducible factor, including a linear factor with root outside $\mathbb{F}_p$, is coprime to every shift. For such a primary power g^f, a root $\alpha \in \mathbb{F}_{q^{\deg g}}$ gives local pair

$$\left(1,\ p^{1+\lceil \log_p f \rceil} \operatorname{ord}_{\mathbb{F}_{q^{\deg g}}^{\times}}(\alpha^p - \alpha)\right).$$

Indeed, the block identity remains

$$\prod_{j \in \mathbb{F}_p} (y + j) = y^p - y,$$

and its derivative is -1, so the proofs of Lemma 2.4 and Proposition 2.5 are unchanged. The shift modulus is still p. Stability requires all roots of the minimal polynomial to lie in $\mathbb{F}_p$ and is stronger than triangularizability over $\mathbb{F}_q$. Therefore, the prime-field quadratic and Fermat-prime counting formulas require modification over extension fields.

Over residue rings $\mathbb{Z}/p^e\mathbb{Z}$, $e \geq 2$, the unit orders also depend on the lift of the matrix, so, in general, the reduction modulo p alone does not determine the period. For example, over $\mathbb{Z}/9\mathbb{Z}$, let A_1 and A_2 be the companion matrices of $y^4 + 2y^2 + 1$ and $y^4 - y^2 + 1$, respectively; both reduce modulo 3 to the companion matrix of $(y^2 + 1)^2$. Since $y^2 + 1$ has no root modulo 3, every shift $A_i + jI$ is invertible. Put

$$U_i = \prod_{j=0}^{8} (A_i + jI).$$

The block-and-cancellation argument of Lemma 2.4, with shift modulus 9, shows that each sequence is periodic from P_1 with period equal to nine times the multiplicative order of U_i. Direct calculation gives $U_1^6 = -I$, $U_1^4 \neq I$, and $U_2^2 = -I$. Thus, the orders of U_1 and U_2 are 12 and 4, respectively, and the pairs are $(1, 108)$ and $(1, 36)$. Uniform formulas for these lift-dependent orders and general joint counts remain difficult. For composite moduli, the Chinese remainder theorem reduces the questions to prime-power components.

Author contributions

Youngho Woo: methodology, formal analysis, writing – original draft, writing – review & editing; Chi Young Ahn: investigation, validation, writing – review & editing; Daeyeoul Kim: conceptualization, supervision, validation, writing – review & editing. All authors have read and approved the final version of the manuscript for publication.

Use of Generative-AI tools declaration

ChatGPT and Claude were used for language editing only, including grammar and sentence structure. The authors reviewed the final manuscript and take full responsibility.

Acknowledgments

This research was partially supported by the National Institute for Mathematical Sciences (NIMS), No. B26A10000. The corresponding author was also supported by the Global-Learning & Academic

Research Institution for Master's and PhD Students, and Postdocs (LAMP) Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (Grant No. RS-2024-00443714).

Conflict of interest

The authors declare no conflicts of interest.

References

1. G. Gasper, M. Rahman, *Basic hypergeometric series*, 2 Eds., Cambridge University Press, 2004. https://doi.org/10.1017/CBO9780511526251
2. L. Jódar, J. C. Cortés, On the hypergeometric matrix function, *J. Comput. Appl. Math.*, **99** (1998), 205–217. https://doi.org/10.1016/S0377-0427(98)00158-7
3. S. Jung, J. S. Moon, D. Kim, On the movements induced by the iterative product of 2×2 matrices defined in modulo 7, *Montes Taurus J. Pure Appl. Math.*, **7** (2025), 16–32.
4. J. Yang, C. Y. Ahn, D. Kim, Iterated matrix sequences modulo 5 and their stable, amicable, and sociable structures, *J. Appl. Pure Math.*, **8** (2026), 123–161.
5. Y. Fan, D. Kim, C. Y. Ahn, Iterated matrix sequences over $M_2(\mathbb{Z}_9)$, *J. Appl. Math. Inform.*, **44** (2026), 1161–1182. https://doi.org/10.14317/jami.2026.1161
6. D. Kim, Iteration of 2×2 matrices in $\mathbb{Z}_4$ and their four color expressions (I), *J. Appl. Pure Math.*, **6** (2024), 37–45.
7. Y. Fan, C. Y. Ahn, D. Kim, Iterations of endomorphisms for 4-torsion subgroups of elliptic curve, *Math. Methods Appl. Sci.*, **49** (2026), 15696–15729. https://doi.org/10.1002/mma.70836
8. D. Kim, A. Bayad, Polygon numbers associated with the sum of odd divisors function, *Exp. Math.*, **26** (2017), 287–297. https://doi.org/10.1080/10586458.2016.1162231
9. D. Kim, A. Bayad, S. H. Park, Iterated stable numbers and iterated amicable pairs, *Math. Methods Appl. Sci.*, **44** (2021), 12479–12499. https://doi.org/10.1002/mma.7555
10. G. L. Cohen, H. J. J. te Riele, Iterating the sum-of-divisors function, *Exp. Math.*, **5** (1996), 91–100. https://doi.org/10.1080/10586458.1996.10504580
11. H. K. Lee, D. Kim, A study of sound numbers derived from iterated products of matrices in $\mathbb{Z}_2$, *Montes Taurus J. Pure Appl. Math.*, **8** (2026), 1–28.
12. J. P. S. Kung, The cycle structure of a linear transformation over a finite field, *Linear Algebra Appl.*, **36** (1981), 141–155. https://doi.org/10.1016/0024-3795(81)90227-5
13. R. Stong, Some asymptotic results on finite vector spaces, *Adv. Appl. Math.*, **9** (1988), 167–199. https://doi.org/10.1016/0196-8858(88)90012-7
14. K. E. Morrison, Integer sequences and matrices over finite fields, *J. Integer Seq.*, **9** (2006), 06.2.1. Available from: `https://cs.uwaterloo.ca/journals/JIS/VOL9/Morrison/morrison37.html`.

15. J. B. Cosgrave, K. Dilcher, An introduction to Gauss factorials, *Amer. Math. Mon.*, **118** (2011), 812–829. https://doi.org/10.4169/amer.math.monthly.118.09.812

16. X. Li, M. Sha, Gauss factorials of polynomials over finite fields, *Int. J. Number Theory*, **13** (2017), 2039–2054. https://doi.org/10.1142/S1793042117501093

17. S. Panja, Periodic points of power maps in finite matrix groups and algebras, *ArXiv*, 2026. https://doi.org/10.48550/arXiv.2603.12295

18. C. Qureshi, L. Reis, On the functional graph of the power map over finite groups, *Discrete Math.*, **346** (2023), 113393. https://doi.org/10.1016/j.disc.2023.113393

19. L. Kaylor, D. Offner, Counting matrices over a finite field with all eigenvalues in the field, *Involve*, **7** (2014), 627–645. https://doi.org/10.2140/involve.2014.7.627

20. J. Fulman, Cycle indices for the finite classical groups, *J. Group Theory*, **2** (1999), 251–289. https://doi.org/10.1515/jgth.1999.017

21. T. A. Gassert, Chebyshev action on finite fields, *Discrete Math.*, **315–316** (2014), 83–94. https://doi.org/10.1016/j.disc.2013.10.014

22. B. Hutz, T. Patel, Periodic points and tail lengths of split polynomial maps modulo primes, *Involve*, **15** (2022), 185–206. https://doi.org/10.2140/involve.2022.15.185

23. R. Lidl, H. Niederreiter, *Finite fields*, 2 Eds., Cambridge University Press, 1997. https://doi.org/10.1017/CBO9780511525926

24. A. Storjohann, An $O(n^3)$ algorithm for the Frobenius normal form, *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation*, 1998, 101–105. https://doi.org/10.1145/281508.281570

25. J. von zur Gathen, J. Gerhard, *Modern computer algebra*, 3 Eds., Cambridge University Press, 2013. https://doi.org/10.1017/CBO9781139856065

26. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.



AIMS Press

© 2026 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0)