THE GROUP $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ AS PERMUTATIONS OF $(\mathbb{Z}/n\mathbb{Z})^2$

ABSTRACT. The group $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ acts on $(\mathbb{Z}/n\mathbb{Z})^2$ by matrix multiplication. Each element gives a permutation of $(\mathbb{Z}/n\mathbb{Z})^2$, and we study its decomposition into disjoint cycles. We also consider the analogous problem for the semi-direct product $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^2$: for its element (M, v) we first act on $(\mathbb{Z}/n\mathbb{Z})^2$ with the matrix multiplication by M and then with the translation by v.

1. INTRODUCTION

Consider an integer $n \geq 2$. The group $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ acts on $(\mathbb{Z}/n\mathbb{Z})^2$ by matrix multiplication, and each matrix gives a bijection on $(\mathbb{Z}/n\mathbb{Z})^2$. Thus we can see $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ as a subgroup of the permutation group of $(\mathbb{Z}/n\mathbb{Z})^2$. The permutation group has size $(n^2)!$ while $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ has size less than n^4, so we only obtain very few permutations.

The aim of this paper is understanding the decomposition into disjoint cycles of the permutations stemming from $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Thanks to the Chinese Remainder Theorem we may reduce to the case in which $n = p^e$, where p is a prime number and $e \geq 1$. Our two main results are the following:

Theorem 1. *A permutation of $(\mathbb{Z}/p\mathbb{Z})^2$ stemming from $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has the following decomposition into disjoint cycles: the zero vector forms a 1-cycle; an eigenvector belongs to a cycle whose length is the order of the eigenvalue; any further vector belongs to a cycle whose length is the order of the matrix.*

Theorem 2. *Consider the permutation of $(\mathbb{Z}/p^e\mathbb{Z})^2$ stemming from $M \in \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ and let $w \in (\mathbb{Z}/p^e\mathbb{Z})^2$. Suppose that $M \equiv I \bmod p$, and that $M \equiv I \bmod 4$ in case $p = 2$. If $Mw = w$ then M is in a 1-cycle for M, otherwise it is in a cycle of length p^{e-v}, where p^v is the largest power of p dividing $(M - I)w$.*

Theorem 2 has an assumption (namely, $M \equiv I \bmod p$ and $M \equiv I \bmod 4$ in case $p = 2$) and it is an important special case: in Section 5 we describe how to reduce to this case.

We also consider the semi-direct product $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^2$: this group is again a subgroup of permutations of $(\mathbb{Z}/n\mathbb{Z})^2$. Indeed, for an element (M, v) and for $w \in (\mathbb{Z}/n\mathbb{Z})^2$ we define

$$(M, v)w = Mw + v\,.$$

In other words, we compose the bijection given by M with the translation by v. We have the following result:

Theorem 3. *Consider a permutation $(M, v) \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \ltimes (\mathbb{Z}/p\mathbb{Z})^2$. If $v \in \mathrm{Im}(M - I)$, then its structure is the same as the permutation given by M. Now suppose that $v \notin \mathrm{Im}(M-I)$ and let $w \in (\mathbb{Z}/p\mathbb{Z})^2$. If $Mw = w$, then w belongs to a p-cycle. Suppose that $Mw \neq w$: if the eigenvalues of M are $1, \lambda$ with $\lambda \neq 1$, then w belongs to a $p\,\mathrm{ord}(\lambda)$-cycle; if 1 is the only*

2020 *Mathematics Subject Classification.* 05A05, 15B36, 11C20.
Key words and phrases. Matrix, permutation, elliptic curve.

eigenvalue of M, then w belongs to a p-cycle unless $p = 2$ and $M \neq I$, in which case we have a 4-cycle.

For $e > 1$, we compare the cycle length at w for a permutation $(M, v) \in \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z}) \ltimes (\mathbb{Z}/p^e\mathbb{Z})^2$ with the one for $M \in \mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$: in particular, see the important special case covered in Theorem 36.

As an aside, we consider the permutations of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ modulo a subgroup of the scalars $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$: we explain the framework in Section 3.1 and address the generalization to $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z})$ in Section 5.1. The motivation is, by considering the full group of scalars, studying the action of $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ on the one-dimensional projective space over $\mathbb{Z}/p\mathbb{Z}$.

We have also studied $\mathrm{GL}_m(\mathbb{Z}/p\mathbb{Z})$ as permutations of $(\mathbb{Z}/p\mathbb{Z})^m$, for any $m \geq 2$. We may easily reduce to the case of a Jordan matrix and then, if $p \geq m$, the permutation structure is clear (see Proposition 14). Building on this result, we investigate the permutations of $\mathrm{GL}_m(\mathbb{Z}/p^e\mathbb{Z})$ on $(\mathbb{Z}/p^e\mathbb{Z})^m$: we cover an important special case in Theorem 24, and then for $m = 2, 3$ we show how to reduce to this case.

In this paper we only use elementary methods and we rely on standard facts about binomial coefficients, linear algebra and matrices over rings [2]. The results are of general interest, and they are relevant to elliptic curves:

Let E be an elliptic curve defined over $\mathbb{Q}$. For every $n \geq 2$ we consider the group $E[n]$ of torsion points in $\overline{\mathbb{Q}}$ of order dividing n. After choosing a basis for $E[n]$, this group can be identified to $(\mathbb{Z}/n\mathbb{Z})^2$ and the action of a Galois automorphism in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is given by multiplication with a matrix in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Suppose that $E(\mathbb{Q})$ contains a non-zero point P, and write $\frac{1}{n}P$ for the subset of $E(\overline{\mathbb{Q}})$ consisting of the points whose n-multiple is P. Fixing some $Q \in \frac{1}{n}P$ we have

$$\frac{1}{n}P = Q + E[n]\,.$$

If $T \in E[n]$ and $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then we have $g(Q + T) = g(Q) + g(T)$. We call $M_g \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ the element giving the action of g on $E[n]$ and we set $v_g := g(Q) - Q \in E[n]$. Then we have

$$g(Q + T) = Q + (M_g T + v_g)\,.$$

We deduce that the Galois action on $\frac{1}{n}P$ is described by the permutation of $E[n]$ stemming from $(M_g, v_g) \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ltimes (\mathbb{Z}/n\mathbb{Z})^2$. For an introduction to this framework for elliptic curves we refer to [1] (and to [3] for the basic notions). The results of this paper then shed light on the Galois action on the torsion points and on the division points of elliptic curves.

2. Preliminaries

To ease notation, we write R_n for the ring $\mathbb{Z}/n\mathbb{Z}$ and $\mathrm{GL}_m(n)$ for $\mathrm{GL}_m(R_n)$. We call *vectors* the elements of R_n^m, which we see as column vectors. We call I the identity matrix. We may consider the groups $\mathrm{GL}_m(n)$ and $\mathrm{GL}_m(n) \ltimes R_n^m$ as subgroups of the permutation group of R_n^m. Indeed, $M \in \mathrm{GL}_m(n)$ acts on R_n^m by the matrix multiplication by M while $(M, v) \in \mathrm{GL}_m(n) \ltimes R_n^m$ acts by the matrix multiplication by M followed by the translation by v.

Remark 4. The matrix $I \in \mathrm{GL}_m(n)$ (respectively, the identity $(I, 0) \in \mathrm{GL}_m(n) \ltimes R_n^m$) are the trivial permutation of R_n^m. An element $(I, v) \in \mathrm{GL}_m(n) \ltimes R_n^m$ with $v \neq 0$ acts on R_n^m via the translation by v: the permutation consists of cycles whose length is the order of v in R_n^m.

Remark 5. Replacing an element of $\mathrm{GL}_m(n)$ by a conjugated element does not change the permutation structure because this is independent from the choice of a R_n-basis of R_n^m. The same holds for $\mathrm{GL}_m(n) \ltimes R_n^m$ because this group can be embedded in $\mathrm{GL}_{m+1}(R_n)$, see Remark 9.

By acting on R_n^m with $\mathrm{GL}_m(n)$, the zero vector clearly forms a 1-cycle (so it would be equivalent to restrict the permutation to $R_n^m \setminus \{0\}$).

Remark 6. By acting on R_n^m with $(M, v) \in \mathrm{GL}_m(n) \ltimes R_n^m$, we have at least a 1-cycle if and only if there is some vector $w \in R_n^m$ such that $Mw + v = w$. This precisely means that v is in the image of $M - I$. In particular, there is at least a 1-cycle for any v if and only if the matrix $M - I$ is invertible.

Remark 7. Let A be in $\mathrm{GL}_m(n)$ (respectively, in $\mathrm{GL}_m(n) \ltimes R_n^m$) and let $w \in R_n^m$. If z is a positive integer, we have $A^z w = w$ if and only if z is a multiple of the length of the cycle of A containing w. Consequently, this length divides the order of A.

By the following remark we may suppose that $n = p^e$, where p is a prime number and e is a positive integer.

Remark 8. We write $n = \prod_{i=1}^r n_i$, where the integers $n_1, \dots, n_r$ are pairwise coprime prime powers larger than 1, and make use of the Chinese Remainder Theorem. Each element $a \in R_n^m$ can be written as

$$a = (a_1, \dots, a_r) \qquad \text{where} \qquad a_i \in R_{n_i}^m \quad \text{and} \quad a \equiv a_i \bmod n_i\,.$$

Thus a permutation σ on R_n^m is such that $\sigma(a) = (\sigma_1(a_1), \dots, \sigma_r(a_r))$, where σ_i is a permutation of $R_{n_i}^m$. The length of the cycle of σ containing a is the least common multiple of the length of the cycle of σ_i containing a_i, by varying $i = 1, \dots, r$.

Moreover, the tuple of the reduction maps modulo n_i (for $i = 1, \dots, r$) gives isomorphisms

$$\mathrm{GL}_m(n) \simeq \prod_i \mathrm{GL}_m(n_i) \qquad \text{and} \qquad \mathrm{GL}_m(n) \ltimes R_n^m \simeq \prod_i \mathrm{GL}_m(n_i) \ltimes R_{n_i}^m$$

and the reduction modulo n_i of an element which acts on R_n^m via σ acts on $R_{n_i}^m$ via σ_i.

Remark 9. We can embed $\mathrm{GL}_2(n) \ltimes R_n^2$ into $\mathrm{GL}_3(n)$ with the map

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e \\ f \end{pmatrix} \right) \mapsto \begin{pmatrix} a & b & e \\ c & d & f \\ 0 & 0 & 1 \end{pmatrix}$$

noting that we have

$$\begin{pmatrix} a & b & e \\ c & d & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix} \\ 1 \end{pmatrix}.$$

We can similarly embed $\mathrm{GL}_m(n) \ltimes (R_n^m)^s$ into $\mathrm{GL}_{m+s}(n)$ with the map

$$(M, (v_1, \dots, v_s)) \mapsto \begin{pmatrix} M & v_1 & \dots & v_s \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}.$$

Finally, we recall some results on the divisibility of binomial coefficients:

Remark 10. For any positive integers m, n the integer $\frac{n}{\gcd(m,n)}$ divides $\binom{n}{m}$. Indeed, for any integers x, y such that $\gcd(m,n) = mx + ny$ we have

$$\frac{\gcd(m,n)}{n}\binom{n}{m} = x\binom{n-1}{m-1} + y\binom{n}{m} \in \mathbb{Z}\,.$$

Consequently, the following holds:

- If t, a are positive integers such that $2 \le t \le a$, then $p^{a-v_p(t)}$ divides $\binom{p^a}{t}$. Indeed, we have $\frac{p^a}{\gcd(p^a,t)} = p^{a-v_p(t)}$. If $p \neq 2$, we may deduce that p^{a+2-t} divides $\binom{p^a}{t}$, while if $p = 2$ we may deduce that 2^{a+3-2t} divides $\binom{2^a}{t}$.
- If p is a prime number and $v_p(m) < v_p(n)$, then p divides $\binom{n}{m}$ because it divides $\frac{n}{\gcd(m,n)}$.

3. The action of $\mathrm{GL}_2(p)$

We keep the notation of Section 2. We let $M \in \mathrm{GL}_2(p)$ and call $\lambda_1, \lambda_2 \in \mathbb{F}_{p^2}^\times$ the (not necessarily distinct) eigenvalues of M. We let $w \in R_p^2$. As we have observed, we may suppose without loss of generality that $M \neq I$ and that $w \neq 0$. Recall from Remark 7 that the length of the cycle at w for M is the smallest positive integer z such that $w \in \ker(M^z - I)$ and we have $z \mid \mathrm{ord}(M)$ (and w is a 1-eigenvector for M^z).

Lemma 11. *Beyond the* 1*-cycle at* 0*, the lengths of the cycles of* M *belong to the set*

$$\{\mathrm{ord}(\lambda_1), \mathrm{ord}(\lambda_2), \mathrm{ord}(M)\}\,.$$

Proof. Fix $w \in R_p^2 \setminus \{0\}$ and call L the length of the cycle at w. We suppose that $L < \mathrm{ord}(M)$ and show that $L \in \{\mathrm{ord}(\lambda_1), \mathrm{ord}(\lambda_2)\}$. The matrix M^L has eigenvalues λ_1^L and λ_2^L and w is a 1-eigenvector for M^L hence without loss of generality we have $\mathrm{ord}(\lambda_1) \mid L$. Consider the following inclusions of $\mathbb{F}_{p^2}$-vector spaces:

$$\{0\} \subsetneq \ker(M - \lambda_1 I) \subseteq \ker(M^{\mathrm{ord}(\lambda_1)} - I) \subseteq \ker(M^L - I) \subsetneq \ker(M^{\mathrm{ord}(M)} - I) = \mathbb{F}_{p^2}^2\,.$$

A dimension argument gives us that the second and third inclusions are equalities. Thus $\ker(M^{\mathrm{ord}(\lambda_1)} - I) = \ker(M^L - I)$ hence the smallest positive integer z such that $w \in \ker(M^z - I)$ is $\mathrm{ord}(\lambda_1)$. □

Theorem 12. *A non-zero vector is in a cycle of length* $\mathrm{ord}(M)$*, unless it is a* λ*-eigenvector for some* $\lambda \in \mathbb{F}_p^\times$*, in which case it is in a cycle of length* $\mathrm{ord}(\lambda)$*.*

Proof. Let $w \in R_p^2 \setminus \{0\}$ and call L the length of the cycle of M at w. If w is a λ-eigenvector for M, then we must have $\lambda \in \mathbb{F}_p^\times$ and clearly $L = \mathrm{ord}(\lambda)$. Now suppose that w is not an eigenvector (in particular, M is not a scalar matrix). If M is diagonalizable over $\mathbb{F}_{p^2}$ (hence $\lambda_1 \neq \lambda_2$), then in a basis consisting of eigenvectors both coordinates of w are non-zero hence $L = \mathrm{lcm}(\mathrm{ord}(\lambda_1), \mathrm{ord}(\lambda_2)) = \mathrm{ord}(M)$. In the remaining case, up to conjugation we have

$$M = \lambda\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \qquad \text{with} \qquad \lambda \in \mathbb{F}_p^\times \quad \text{and} \quad b \neq 0\,.$$

Observe that L divides $\mathrm{ord}(M) = \mathrm{ord}(\lambda)p$. We claim that $p \mid L$. Then, since $M^p = \lambda I$, we must have $L = \mathrm{ord}(M)$. The claim holds because $M^{\mathrm{ord}(\lambda)} w \neq w$. Indeed, the 1-eigenspace of $M^{\mathrm{ord}(\lambda)}$ equals the λ-eigenspace of M and w is not an eigenvector for M. □

Proof of Theorem 1. The result follows from Theorem 12, considering that the zero vector forms a 1-cycle and that, for an eigenvector in R_p^2, the eigenvalue must be in $\mathbb{F}_p$. □

3.1. **The action of $\mathrm{GL}_2(p)$ modulo a group of scalars.** Consider the action of $\mathrm{GL}_2(p)$ on the set $S := R_p^2 \setminus \{0\}$. We fix a non-zero subgroup H of $R_p^\times$ and we call two vectors in S equivalent if one equals the other times a scalar in H. This is an equivalence relation on S, and we call S_H the set of the equivalence classes. We see the quotient group $G_H := \mathrm{GL}_2(p)/HI$ as a group of permutations of S_H.

Let $M \in \mathrm{GL}_2(p)$ and call $M_H \in G_H$ its residue class. We consider a vector $w \in S$ and call $w_H \in S_H$ its equivalence class. We have studied the length L of the cycle at w of M and we now investigate the length L_H of the cycle at w_H of M_H. The integer L_H is the smallest positive integer n such that $M^n w = hw$ holds for some $h \in H$. We deduce that $L_H \mid L$ and that L divides $L_H \cdot \#H$.

We call $\lambda_1, \lambda_2 \in \mathbb{F}_{p^2} \setminus \{0\}$ the (not necessarily distinct) eigenvalues of M and we let ℓ be the smallest positive integer for which λ_1^ℓ (equivalently, λ_2^ℓ) is in $R_p^\times$. We observe that $\ell \mid (p+1)$ and that $\ell \mid L_H$. If $r \in \mathbb{F}_{p^2}^\times$, then we write $\mathrm{ord}_H(r)$ for the smallest positive integer t such that $r^t \in H$.

Theorem 13. *If w is a λ_i^ℓ-eigenvector of M^ℓ, then we have $L_H = \mathrm{ord}_H(\lambda_i)$, for $i = 1, 2$. If w is not an eigenvector of M^ℓ, then we have $L_H = \mathrm{ord}(M)$ if $\lambda_1 \neq \lambda_2$ and $L_H = p\,\mathrm{ord}_H(\lambda_1)$ otherwise.*

Proof. Observing that L_H/ℓ is the length of the cycle at w_H for M_H^ℓ, we may replace M by M^ℓ and suppose that $\ell = 1$ or, equivalently, that $\lambda_1, \lambda_2 \in R_p^\times$.

If without loss of generality $Mw = \lambda_1 w$, then we clearly have $L_H = \mathrm{ord}_H(\lambda_1)$, so suppose that w is not an eigenvector of M (in particular, M is not a scalar matrix).

If $\lambda_1 \neq \lambda_2$, then the smallest positive integer n for which w is an eigenvector of M^n is $\mathrm{lcm}(\mathrm{ord}(\lambda_1), \mathrm{ord}(\lambda_2)) = \mathrm{ord}(M)$ and we conclude. Finally suppose that $\lambda_1 = \lambda_2$ and that M is not diagonalizable. By Theorem 12 we have $L = \mathrm{ord}(M)$ hence $p \mid L$. Since $\#H$ is coprime to p, we deduce that $p \mid L_H$. Moreover, we have $M^p = \lambda_1^p I$ and hence $L_H = p\,\mathrm{ord}_H(\lambda_1)$. □

4. The action of $\mathrm{GL}_m(p)$ on R_p^m

Let p be a prime number, $m \geq 2$ and set $q = p^{m!}$. We see $M \in \mathrm{GL}_m(\mathbb{F}_q)$ as a permutation of the vectors in $\mathbb{F}_q^m$. For our purposes, $M \in \mathrm{GL}_m(p)$ hence the permutation maps R_p^m to itself and all eigenvalues of M are in $\mathbb{F}_q$. We fix $w \in R_p^m \setminus \{0\}$ and study the length L of the cycle of M at w.

The permutation structure of M is invariant under a base change in $\mathrm{GL}_m(\mathbb{F}_q)$ so we may suppose that M is in Jordan normal form. The decomposition of M into Jordan blocks $J_1, \ldots, J_r$ naturally gives a decomposition of $\mathbb{F}_q^m$ as a sum of vector subspaces $V_1, \ldots, V_r$ (which only consider the coordinates corresponding to the various Jordan blocks). We may then write $w = (w_1, \ldots, w_r)$ with $w_i \in V_i$ for $i = 1, \ldots, r$ and we have

$$Mw = (J_1 w_1, \ldots, J_r w_r)\,.$$

Consequently, L is the least common multiple of the lengths of the cycle of J_i at w_i for $i = 1, \ldots, r$. So we reduce to the case where $M \in \mathrm{GL}_m(\mathbb{F}_q)$ consists of a single Jordan block J.

Calling λ the eigenvalue, we have

$$J = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}$$

By induction, for $k \geq 1$ we have

$$J^k = \begin{pmatrix} \lambda^k & \binom{k}{1}\lambda^{k-1} & \binom{k}{2}\lambda^{k-2} & \cdots & \binom{k}{m-1}\lambda^{k-m+1} \\ & \lambda^k & \binom{k}{1}\lambda^{k-1} & \cdots & \binom{k}{m-2}\lambda^{k-m+2} \\ & & & \cdots & \vdots \\ & & & \lambda^k & \binom{k}{1}\lambda^{k-1} \\ & & & & \lambda^k \end{pmatrix}. \tag{1}$$

Namely, J^k is an upper triangular matrix whose elements on the main diagonal are λ^k and the entry in row i and column $i+t$ (with $1 \leq t \leq m-i$) is $\binom{k}{t}\lambda^{k-t}$.

Proposition 14. *If w is a λ-eigenvector for J, then $L = \operatorname{ord}(\lambda)$. Otherwise, we have $L = p^x \operatorname{ord}(\lambda)$ for some positive integer x such that $p^{x-1} < m$ (thus, $L = p \operatorname{ord}(\lambda)$ if $p \geq m$).*

Proof. If w is a λ-eigenvector for J, the statement is immediate, so suppose that this is not the case. Since $0 \neq w \in \ker(J^L - I)$ we deduce from (1) that

$$0 = \det(J^L - I) = (\lambda^L - 1)^m$$

and hence $\operatorname{ord}(\lambda) \mid L$.

We now prove that $\ker(J^{\operatorname{ord}(\lambda)} - I)$ is the λ-eigenspace of J, which implies $L \neq \operatorname{ord}(\lambda)$. Since the diagonal entries of $J^{\operatorname{ord}(\lambda)} - I$ are zero, the kernel contains the λ-eigenspace. Moreover, the kernel is 1-dimensional because $p \nmid \operatorname{ord}(\lambda)$ implies $p \nmid \binom{\operatorname{ord}(\lambda)}{1}$ hence the first $m-1$ rows of $J^{\operatorname{ord}(\lambda)} - I$ are linearly independent.

To conclude it suffices to prove that $J^{p^z \operatorname{ord}(\lambda)} = I$ holds for the smallest positive integer z such that $p^z \geq m$. This is the case by (1) because $p \mid \binom{p^z \operatorname{ord}(\lambda)}{t}$ holds in particular for all $1 \leq t < m \leq p^z$ as $v_p(t) < v_p(p^z \operatorname{ord}(\lambda))$, see Remark 10. □

Remark 15. Let $p = 2$ and $m = 3$. If there are more than one Jordan blocks we may reduce to the case $m = 2 \leq p$ covered by Proposition 14, and if there is only one Jordan block J then the eigenvalue must be over $\mathbb{F}_p$ and hence 1. So we have

$$J^2 = \begin{pmatrix} 1 & 0 & 1 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \qquad \text{and} \qquad J^4 = I\,.$$

If w is a 1-eigenvector, then $L = 1$. Otherwise, we have $L = 2$ unless the last coordinate of w is non-zero, in which case $L = 4$.

5. The action of $\mathrm{GL}_m(p^e)$

Let p be a prime number and $e > 1$. We fix $M \in \mathrm{GL}_m(p^e)$ and $w \in R_{p^e}^m \setminus \{0\}$. For every $1 \leq s \leq e$ we call M_s (respectively, w_s) the reduction of M (respectively, w) modulo p^s and we call L_s the length of the cycle at w_s of the permutation M_s. We observe that L_s is the smallest positive integer satisfying

$$M^{L_s} w \equiv w \mod p^s \,.$$

Moreover, we remark that $L_s \mid L_{s+1}$ holds for all $1 \leq s < e$ and that for $m = 2, 3$ the number L_1 can be determined thanks to Proposition 14 and Remark 15.

Proposition 16. *Let* $1 \leq s < e$ *and write* $M^{L_s} w = w + p^s w'_s$ *for some* $w'_s \in R^m_{p^e}$. *Then* L_{s+1}/L_s *is the smallest positive integer* t *such that*

$$(w'_s \bmod p) \in \ker \left(\sum_{i=0}^{t-1} M_1^{L_s i} \right) . \tag{2}$$

Proof. Write $L_{s+1} = L_s t$ and $N = M^{L_s}$. Then t is the smallest positive integer such that

$$N^t w \equiv w \mod p^{s+1} \,.$$

Since (as it can be shown by induction) we have

$$N^t w = w + p^s \sum_{i=0}^{t-1} N^i w'_s \,,$$

we may conclude by rewriting the condition as

$$\sum_{i=0}^{t-1} N^i w'_s \equiv 0 \bmod p \,.$$

□

Remark 17. We have the following recursive formula for w'_s, for $s = 1, \dots, e-1$:

$$w'_{s+1} = \frac{(M^{L_{s+1}} - I)w}{p^{s+1}} = \frac{1}{p} \sum_{k=0}^{L_{s+1}/L_s - 1} M^{L_s k} \frac{(M^{L_s} - I)w}{p^s} = \frac{1}{p} \sum_{k=0}^{L_{s+1}/L_s - 1} M^{L_s k} w'_s. \tag{3}$$

Remark 18. Write $w = p^v w'$ with $0 \leq v < e$ maximal. Then the cycle length L_e is the same as the cycle length L'_{e-v} of M at w'. So up to replacing w by w' and e by $e-v$ we may suppose that $w_1 \neq 0$.

Remark 19. Suppose that $(w'_s \mod p) = 0$ and let h be the largest positive integer such that $p^h \mid w'_s$. Then we have $L_{s+x} = L_s$ for every $0 \leq x \leq h$ and $(w'_{s+h} \bmod p) \neq 0$. This is a consequence of Proposition 16 and (3) because $w'_{s+x} = p^{-x} w'_s$.

Example 20. Suppose that $e = 2$ and that $M = I + pM'$ holds for some matrix M'. We have $L_1 = 1$ because $M_1 = I$. Since $Mw = w + pM'w$, with the notation of Proposition 16 we have $w'_1 = M'w$. Since

$$\sum_{i=0}^{t-1} M^{L_1 i} \equiv tI \bmod p$$

by Proposition 16 we have $L_2 = 1$ (which means $Mw = w$) if $w'_1 \equiv 0 \bmod p$ and $L_2 = p$ otherwise.

Theorem 21. *Let $M \in \mathrm{GL}_m(p^e)$. Let $s \geq 1$ and let the matrix $M_1^{L_s}$ have Jordan normal form $\mathrm{diag}(J_1, \ldots, J_r)$ with J_j the Jordan blocks corresponding to an eigenvalue $\lambda_j \in \overline{\mathbb{F}_p}$ for $j = 1, \ldots, r$. Write $w'_s \mod p = (v_1, v_2, \ldots, v_r)$ with v_j a column vector with as many rows as J_j. Define*

$$d_j := \begin{cases} 1 & \text{if } v_j = 0; \\ \mathrm{ord}\,\lambda_j & \text{if } \lambda_j \neq 1 \text{ and } v_j = (a, 0, 0, \ldots, 0) \text{ with } a \in \overline{\mathbb{F}_p}^{\times}; \\ p \,\mathrm{ord}\,\lambda_j & \text{otherwise.} \end{cases}$$

Suppose that the size of each Jordan block is at most p and for the Jordan blocks with eigenvalue 1 strictly less than p. Then we have

$$L_{s+1}/L_s = \mathrm{lcm}(d_1, \ldots, d_m) .$$

Proof. We make use of Proposition 16. Condition (2) is equivalent to $v_j \in \ker(\sum_{k=0}^{t-1} J_j^k)$ for all $j = 1, 2, \ldots, r$ so we have reduced to consider a Jordan block J of $M_1^{L_s}$ corresponding to an eigenvalue λ and set $v := w'_s \mod p$. We clearly have $L_{s+1}/L_s = 1$ if and only if $v = 0$.

Suppose first that $\lambda = 1$ and that $v \neq 0$. By (1) and by the hockey-stick identity $\sum_{k=z}^{t-1} \binom{k}{z} = \binom{t}{z+1}$ all entries of $\sum_{k=0}^{p-1} J^k$ are 0 inside $\overline{\mathbb{F}_p}$. Thus by (2) L_{s+1}/L_s divides p and we may conclude.

Now suppose that $\lambda \neq 1$ and that $v \neq 0$. Then $\mathrm{ord}(\lambda)$ divides L_{s+1}/L_s because for $\mathrm{ord}(\lambda) \nmid t$ the triangular matrix $\sum_{k=0}^{t-1} J^k$ is invertible (the entries on the main diagonal are $\frac{\lambda^t - 1}{\lambda - 1}$). By (1) and Remark 10 we have $J^p = \lambda I$ hence

$$\sum_{k=0}^{p\,\mathrm{ord}\,\lambda - 1} J^k = \sum_{k=0}^{\mathrm{ord}\,\lambda - 1} \sum_{l=0}^{p-1} J^{kp+l} = \left(\sum_{k=0}^{\mathrm{ord}\,\lambda - 1} \lambda^k \right) \left(\sum_{l=0}^{p-1} J^l \right) = 0,$$

implying that L_{s+1}/L_s divides $p\,\mathrm{ord}(\lambda)$. We deduce that L_{s+1}/L_s equals $\mathrm{ord}(\lambda)$ or $p\,\mathrm{ord}(\lambda)$ and we are in the former case if and only if for $t := \mathrm{ord}(\lambda)$ the vector v is in the kernel of

$$\sum_{k=0}^{t-1} J^k .$$

This matrix is upper triangular with zero entries on the main diagonal. Moreover, we have

$$\sum_{k=0}^{t-1} k\lambda^{k-1} = \frac{(t-1)\lambda^t - t\lambda^{t-1} + 1}{(\lambda - 1)^2} = \frac{\mathrm{ord}\,\lambda(1 - \lambda^{-1})}{(\lambda - 1)^2} \neq 0$$

on the first superdiagonal. This implies $\ker(\sum_{k=0}^{t} J^k) = \langle (1, 0, \ldots, 0) \rangle$ and we may conclude. □

Remark 22. We adapt the proof of Theorem 21 supposing that $p, m \in \{2, 3\}, p \leq m$. Suppose first that J is a $m \times m$ Jordan block for the eigenvalue 1. In this case we have $\sum_{k=0}^{p^2-1} J^k = 0$ hence L_{s+1}/L_s divides p^2. Moreover, $L_{s+1}/L_s = 1$ if and only if $v = 0$ and $L_{s+1}/L_s = p^2$ if and only if the last entry of v is non-zero. Now suppose that J is a Jordan block for an eigenvalue $\lambda \neq 1$: considering that 1 is an eigenvalue of $M_1^{L_s}$, J is either 1×1 or 2×2 so the proof does not require any change.

Corollary 23. *Suppose that $m = 2$ and that $M_1^{L_s}$ has eigenvalues 1 and $\lambda \neq 1$ (thus, $p \neq 2$). We have*

$$L_{s+1}/L_s = \begin{cases} 1 & \textit{if } (w'_s \mod p) \textit{ is zero} \\ p & \textit{if } (w'_s \mod p) \textit{ is a } 1\textit{-eigenvector for } M_1^{L_s} \\ \operatorname{ord}(\lambda) & \textit{if } (w'_s \mod p) \textit{ is a } \lambda\textit{-eigenvector for } M_1^{L_s} \\ p\operatorname{ord}(\lambda) & \textit{otherwise.} \end{cases} \tag{4}$$

Proof. This is a special case of Theorem 21. □

In the following result we may suppose that $Mw \neq w$ because otherwise $L_e = 1$:

Theorem 24. *Let $e \geq 2$ and suppose that $M = I + pM'$ for some matrix M'. We suppose that $Mw \neq w$ and write uniquely $M'w = p^k u$ where $0 \leq k < e$ and $u \in R_{p^e}^m$ is such that $p \nmid u$. If $p = 2$, suppose additionally that $2 \mid M'$. Then we have $L_e = p^{e-k-1}$.*

Proof. Since $M_1 = I$, we have $L_1 = 1$. We prove that

$$L_i = \begin{cases} 1 & 1 \leq i \leq k+1 \\ p^{i-k-1} & k+1 < i \leq e\,. \end{cases}$$

Proposition 16 says that $L_{s+1}/L_s \in \{1, p\}$ and (since $M_1 = I$) that $L_{s+1} = L_s$ if and only if $w'_s \equiv 0 \bmod p$. We can write

$$Mw = w + pM'w = w + p^{k+1}u\,.$$

Supposing that $L_s = 1$ we have $w'_s = p^{k+1-s}u$ and hence $w'_s \equiv 0 \bmod p$ holds for $s \leq k$. Thus, $L_i = 1$ holds for $i = 1, \ldots, k+1$.

To conclude (recalling that $p \nmid u$) we prove by strong induction that $w'_s \equiv u \bmod p$ holds for $k+1 \leq s \leq e-1$. For $s = k+1$ (considering that $L_{k+1} = 1$) we have shown above that $w'_s = u$. Now suppose that $w'_i \equiv u \bmod p$ holds for all $k+1 \leq i \leq s$ (for some $k+1 \leq s \leq e-2$). We have to prove that $w'_{s+1} \equiv u \bmod p$. Our induction hypothesis implies that $L_{s+1} = p^{s-k}$. Making use of the binomial expansion we obtain

$$M^{L_{s+1}} = I + p^{s-k} \cdot pM' + \left(\sum_{t=2}^{p^{s-k}} \binom{p^{s-k}}{t} p^t (M')^{t-1} \right) M'\,.$$

If $p \neq 2$ we observe that $p^{s-k+2-t}$ divides $\binom{p^{s-k}}{t}$ for all $2 \leq t \leq s-k$ (see Remark 10). Recall that by definition we have $M^{L_{s+1}}w = w + p^{s+1}w'_{s+1}$ and $M'w = p^k u$. Then, applying w to the above formula we may conclude because we have

$$p^{s+1}w'_{s+1} \equiv p^{s+1}u \bmod p^{s+2}\,.$$

If $p = 2$ we adapt the previous case. Since $2^t(M')^{t-1}$ is divisible by 2^{2t-1} we only need to prove that $2^{s-k+3-2t}$ divides $\binom{2^{s-k}}{t}$ for all $2 \leq t \leq s-k$, and this holds by Remark 10. □

Proof of Theorem 2. The result is equivalent to Theorem 24. □

In what follows, we make use of the notation M_1, L_s and w'_s from Proposition 16. Since L_1 divides L_e, we may work with M^{L_1} thus $(w \bmod p)$ is a 1-eigenvector for $M_1^{L_1}$.

Remark 25. Let $m = 2, 3$ and $p \neq 2$. Recall that the case $M_1 = I$ is covered by Theorem 24.

Suppose that 1 is the only eigenvalue for $M_1^{L_1}$ hence by (1) the order of $M_1^{L_1}$ divides p. Since $\operatorname{ord}(M^{L_1})$ is a power of p, the same holds for L_e/L_1 hence we either have $L_e = L_1$ or we may replace M^{L_1} by M^{pL_1} and reduce to the case $M_1 = I$.

Now suppose that $M_1^{L_1}$ has, beyond the eigenvalue 1, at least one eigenvalue $\lambda \neq 1$ (over $\mathbb{F}_{p^2}$). For $m = 3$, the possible further eigenvalue that is not 1 has also order $\operatorname{ord}(\lambda)$. Up to a base change that preserves the affine structure, we let $R_p^m = E \oplus E_1$ where E_1 (respectively, E) is the vector subspace corresponding to the Jordan blocks with eigenvalue 1 (respectively, different from 1). In case that for some $1 \leq s < e$ the vector $(w'_s \mod p)$ has a non-trivial component in E, by Theorem 21 we have $\operatorname{ord}(\lambda) \mid L_e$ hence replacing M by $M^{L_s \operatorname{ord}(\lambda)}$ we may again reduce to the case $M_1 = I$. Moreover, if $(w'_s \mod p)$ also has a non-trivial component in E_1, we have $L_{s+1} = p \operatorname{ord}(\lambda) L_s$ hence $M^{L_s \operatorname{ord}(\lambda)} w - w$ is not divisible by p^{s+1}. Theorem 24 then gives $L_e = L_s \operatorname{ord}(\lambda) p^{e-s-1}$.

Remark 26. Let $m = 2, 3$ and $p = 2$. Recall that the case $M_2 = I$ is covered by Theorem 24.

Suppose that 1 is the only eigenvalue for $M_1^{L_1}$ (thus $\operatorname{ord}(M^{L_1})$ is a power of 2). Then the cycle of M^{L_1} at w has length 1 (if $M^{L_1} w = w$) or 2 (if $M^{L_1} w \neq w$ and $M^{2L_1} w = w$) or 4 (if $M^{2L_1} w \neq w$ and $M^{4L_1} w = w$) or a multiple of 8. In the last case, we may work with M^{8L_1} hence reduce to the case $M_2 = I$. We observe that, unless $m = 3$ and $M_1^{L_1}$ is a Jordan matrix, as soon as the cycle length is a multiple of 4 we may reduce to the case $M_2 = I$ by considering M^{4L_1}.

Now suppose that $M_1^{L_1} \in \mathrm{GL}_m(p)$ has (beyond the eigenvalue 1) an eigenvalue $\lambda \neq 1$, which implies that $m = 3$ and M_1 is diagonalizable over $\mathbb{F}_{p^2}$ of order $\operatorname{ord}(\lambda) = 3$ with three distinct eigenvalues $1, \lambda, \overline{\lambda}$. Having the information on whether 3 divides or not L_e/L_1 would allows us to work with M^{3L_1} instead, thus reducing to the previous case. Suppose that working with $M_1^{3L_1}$ instead we get a ratio L'_e/L_1. Then L_e is L'_e or $3L'_e$ and the latter case occurs if and only if $3 \mid L_e$. In turn, this occurs if and only if $M^{2^x L_1} w \neq w$ for any x. So by taking $x = e$ we are reduced to study whether w is a 1-eigenvector for a power of M^{L_1} that has order 3. This power equals $M_1^{L_1}$ interpreting the coefficients $0, 1$ as classes modulo 2^e (this can be seen by writing $I = (M_1^{L_1} + 2^f N)^3$ with f maximal and working modulo 2^{f+1} in case $f < e$).

Remark 27. Let $m = 2$ and $p \neq 2$. Suppose that M_1 has an eigenvalue $\lambda \neq 1$ and that $(w'_s \mod p)$ is a 1-eigenvector. Up to a base change, suppose that M_1 is diagonal and the second coordinate corresponds to the λ-eigenspace. Then $(w'_{s+1} \mod p)$ is either a 1-eigenvector for M_1 or it is neither zero nor an eigenvector, and the former case holds if and only if the second coordinate of $(w'_s \mod p^2)$ is zero. By Corollary 23, this can be shown by plugging $t = p$ and $y = 0$ in the following calculations: in a suitable basis, write

$$M^{L_s} \equiv \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} + p \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mod p^2 \qquad w'_s \equiv \begin{pmatrix} x + pe \\ y + pf \end{pmatrix} \mod p^2$$

with $a, b, c, d, e, f, x, y \in R_p$. By induction, for any $k \geq 0$ we have

$$M^{L_s k} w'_s \equiv p \begin{pmatrix} by\frac{\lambda^k - 1}{\lambda - 1} + kax + e \\ cx\frac{\lambda^k - 1}{\lambda - 1} + f\lambda^k + dyk\lambda^{k-1} \end{pmatrix} + \begin{pmatrix} x \\ y\lambda^k \end{pmatrix} \mod p^2$$

so that for $t = L_{s+1}/L_s$ we have by (3)

$$pw'_{s+1} \equiv p \begin{pmatrix} by\sum_{k=0}^{t-1} \frac{\lambda^k - 1}{\lambda - 1} + ax\frac{t(t-1)}{2} + et \\ cx\sum_{k=0}^{t-1} \frac{\lambda^k - 1}{\lambda - 1} + f\frac{\lambda^t - 1}{\lambda - 1} + dy\sum_{k=0}^{t-1} k\lambda^{k-1} \end{pmatrix} + \begin{pmatrix} tx \\ y\frac{\lambda^t - 1}{\lambda - 1} \end{pmatrix} \mod p^2.$$

Example 28. Let $m = 2$, $p^e = 27$ and let $M \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mod p$. We set $t_1 := L_1, t_2 := L_2/L_1$ and $t_3 := L_3/L_2$ so that $L_3 = t_1t_2t_3$. We characterize all possible values of the triple (t_1, t_2, t_3).

By Proposition 14, we have $t_1 \in \{1, 2\}$. If $t_1 = 2$, then $M_1^{L_1} = I$, so by Theorem 21 we have $t_2, t_3 \in \{1, 3\}$ and moreover $t_2 = 3$ implies $t_3 = 3$ by Theorem 24. Now suppose that $t_1 = 1$ hence by Corollary 23 we have $t_2 \in \{1, 2, 3, 6\}$.

- If $t_2 = 1$, then by Corollary 23 we have $t_3 \in \{1, 2, 3, 6\}$.
- If $t_2 = 2$, then $M_1^{L_2} = I$, so by Theorem 21 we have $t_3 \in \{1, 3\}$.
- If $t_2 = 3$, then by Corollary 23 we find that $w_2' \mod p$ is a 1-eigenvector for M_1^3, thus by Remark 27 we have $t_3 \in \{3, 6\}$.
- If $t_2 = 6$, then from Remark 25 $w_1' \bmod 3$ has a nontrivial component in E and E_1 and hence $t_3 = 3$.

All the twelve obtained triples are achievable, and even for one same M. Indeed, in the table below we can see the triples corresponding to the given values of w for $M = \begin{pmatrix} 13 & 12 \\ 12 & 17 \end{pmatrix}$:

w	(t_1, t_2, t_3)	w	(t_1, t_2, t_3)
$(0, 0)$	$(1, 1, 1)$	$(1, 24)$	$(1, 3, 3)$
$(0, 9)$	$(1, 1, 2)$	$(1, 6)$	$(1, 3, 6)$
$(3, 18)$	$(1, 1, 3)$	$(1, 0)$	$(1, 6, 3)$
$(3, 0)$	$(1, 1, 6)$	$(3, 1)$	$(2, 1, 1)$
$(0, 3)$	$(1, 2, 1)$	$(0, 1)$	$(2, 1, 3)$
$(3, 3)$	$(1, 2, 3)$	$(1, 1)$	$(2, 3, 3)$

5.1. **The action of $\mathrm{GL}_2(p^e)$ modulo a group of scalars.** Fix $M \in \mathrm{GL}_2(p^e)$ and a vector $w \in R_{p^e}^2$. We let $H \leq (\mathbb{Z}/p^e\mathbb{Z})^\times$ or simply $H = R_{p^e}$ and investigate the smallest positive integer n such that $M^n w = hw$ holds for some $h \in H$. We have already treated the case $H = \{1\}$ and in general we may proceed with the same strategy. We may suppose that $w \neq 0$ and (similarly to Remark 18) that $w_1 \neq 0$. For $1 \leq s \leq e$ we define $\widetilde{L_s}$ to be the smallest positive integer n such that there is $h \in H$ such that $M^n w \equiv hw \mod p^s$. We observe that those n satisfying the condition for a given s are precisely the multiples of $\widetilde{L_s}$ (because if $n_1 < n_2$ satisfy the condition, so does $n_2 - n_1$). Note that $\widetilde{L_1}$ can be computed using Theorem 13. Moreover, we have $\widetilde{L_s} \mid \widetilde{L_{s+1}}$ and $\widetilde{L_s} \mid L_s$.

We write $N = M^{\widetilde{L_s}}$ and $Nw = \mu w + p^s \widetilde{w_s}$ with $\mu \in H$. Then we have

$$N^n w = \mu^n w + p^s \left(\sum_{i=0}^{n-1} N^i \widetilde{w_s} \right).$$

Thus $\widetilde{L_{s+1}}/\widetilde{L_s}$ is the smallest positive integer n such that there is $h \in H$ such that

$$N^n w = \mu^n w + p^s \left(\sum_{i=0}^{n-1} N^i \right) \widetilde{w_s} \equiv hw \mod p^{s+1}. \tag{5}$$

If t is the smallest positive integer such that $\widetilde{w_s} \bmod p \in \ker \left(\sum_{i=0}^{t-1} N_1^i \right)$, then we have $\widetilde{L_{s+1}}/\widetilde{L_s} \leq t$ by setting $n = t$ and $h = \mu^t$ in (5).

Suppose that $H = R_{p^e}$. Then (5) is equivalent to

$$\left(\sum_{i=0}^{n-1} N_1^i\right) \widetilde{w_s} \bmod p \in \langle w_1 \rangle \,. \tag{6}$$

We deduce that $\widetilde{L_{s+1}}/\widetilde{L_s}$ divides t: if $n_1 < n_2$ satisfy (6), so does their difference because $N_1 w_1 \in \langle w_1 \rangle$ and we have

$$\sum_{i=0}^{(n_2-n_1)-1} N_1^i = \left(\sum_{i=0}^{n_2-1} N_1^i\right) - N_1^{n_1}\left(\sum_{i=0}^{n_1-1} N_1^i\right) .$$

We have $\widetilde{L_{s+1}} = \widetilde{L_s}$ if and only if $\widetilde{w_s} \bmod p$ is a multiple of w_1. So suppose that this is not the case. If $\widetilde{w_s} \bmod p$ is an eigenvector for N_1, then $\widetilde{L_{s+1}}/\widetilde{L_s} = t$ (and if it is a 1-eigenvector, then $t = p$). In general, $\widetilde{L_{s+1}}/\widetilde{L_s}$ divides $\mathrm{ord}(N_1)$ (respectively, 4 if $p = 2$ and N_1 is not diagonalizable) because the matrix sum in (6) is the zero matrix for this value.

6. The action of $\mathrm{GL}_2(p^e) \ltimes R_{p^e}^2$

6.1. **The action of** $\mathrm{GL}_2(p) \ltimes R_p^2$**.** Let p be a prime number and consider $(M, v) \in \mathrm{GL}_2(p) \ltimes R_p^2$ as a permutation of R_p^2. If (M, v) satisfies $v = (M - I)u$ for some $u \in R_p^2$, then we have

$$(I, u)(M, v)(I, u)^{-1} = (M, 0)$$

and the permutation given by $(M, 0)$ is the same as the one given by M (which was already discussed). So we may assume that v is not in the image of $M - I$, and in particular that 1 is an eigenvalue of M (so a further eigenvalue for M must be in $\mathbb{F}_p$). We may also suppose that $M \neq I$ by Remark 4.

Theorem 29. *Suppose that $M \neq I$ and $v \notin \mathrm{Im}(M - I)$. The following holds for (M, v):*

- *Suppose that the eigenvalues of M are $1, \lambda$ with $\lambda \neq 1$. The vectors in the 1-eigenspace of M form a p-cycle, while the other vectors form cycles of length $p\,\mathrm{ord}(\lambda)$.*
- *Suppose that 1 is the only eigenvalue of M. For $p = 2$ the permutation is a 4-cycle while for p odd the permutations consists of p-cycles.*

Proof. Suppose first that M has two distinct eigenvalues $1, \lambda$. Then up to conjugation we have

$$(M, v) = \left(\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} v_x \\ v_y \end{pmatrix}\right) \qquad v_x \neq 0 \,.$$

We compute

$$\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} 0 \\ t \end{pmatrix}\right)(M, v)\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \begin{pmatrix} 0 \\ t \end{pmatrix}\right)^{-1} = \left(\begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}, \begin{pmatrix} a v_x \\ a v_y + t(1-\lambda) \end{pmatrix}\right) .$$

By choosing $t = -a v_y/(1-\lambda)$ and $a = v_x^{-1}$, we may then assume that $v = (1, 0)^T$. Then (by induction) for any $k \in \mathbb{Z}$ we have

$$(M, v)^k \begin{pmatrix} x \\ y \end{pmatrix} = \left(\begin{pmatrix} 1 & 0 \\ 0 & \lambda^k \end{pmatrix}, \begin{pmatrix} k \\ 0 \end{pmatrix}\right)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + k \\ \lambda^k y \end{pmatrix} .$$

Thus (observing that $\mathrm{ord}(\lambda)$ is coprime to p) all vectors with $y = 0$ are in one same p-cycle while if $y \neq 0$ the vector $(x, y)^T$ is in a cycle of length $p\,\mathrm{ord}(\lambda)$.

Now assume that up to conjugation we have

$$(M,v) = \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} v_x \\ v_y \end{pmatrix} \right) \qquad v_y \neq 0\,.$$

By conjugating with $(I,(0,v_x)^T)$ we may assume that $v_x = 0$. Then, by conjugating with $(v_y^{-1}I, 0)$, we may assume that $v_y = 1$.

If $p = 2$, then (M,v) has order 4 hence the length of each cycle divides 4. Since $(M,v)^2 = (I,u)$ for some $u \neq 0$, this permutation has no fixed vectors hence (M,v) does not have cycles of length 1 or 2 and we conclude. If p is odd, a computation by induction gives

$$(M,v)^k \begin{pmatrix} x \\ y \end{pmatrix} = \left(\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} k(k-1)/2 \\ k \end{pmatrix} \right) \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + ky + k(k-1)/2 \\ y + k \end{pmatrix}$$

which is equal to $(x,y)^T$ if and only if $p \mid k$. Thus every vector is in a cycle of length p. □

Proof of Theorem 3. The result follows from Theorem 29 and the considerations at the beginning of this section. □

Remark 30. We have found that the permutation induced by (M,v) is of the same type of the one induced by M if and only if there is a 1-cycle if and only if $v \in \mathrm{Im}(M-I)$. In particular, if $M - I$ is invertible, then for any v the permutation (M,v) has the same structure as the permutation M. Moreover, beyond the distinction of whether v belongs or not to $\mathrm{Im}(M-I)$, we have seen that the type of the permutation does not depend on v.

6.2. **The action of** $\mathrm{GL}_2(p^e) \ltimes R^2_{p^e}$ **for** $e > 1$**.** Consider $(M,v) \in \mathrm{GL}_2(p^e) \ltimes R^2_{p^e}$ as a permutation of $R^2_{p^e}$. For every $n \geq 1$ (by induction) we have

$$(M,v)^n = \left(M^n, \sum_{i=0}^{n-1} M^i v \right)\,.$$

Let $w \in R^2_{p^e}$. The cycle length L'_e of (M,v) at w is the smallest positive integer n such that $(M,v)^n w = w$ or, equivalently, such that

$$(M-I)w + v \in \ker \sum_{i=0}^{n-1} M^i\,. \tag{7}$$

We similarly define L'_i by working modulo p^i for $i = 1, \dots, e$ and consider the analogous quantities L_i for the permutation given by M.

Remark 31. The permutation (M,v) has a 1-cycle if and only if $v \in \mathrm{Im}(M-I)$. In this case, the permutation (M,v) has the same structure as the permutation M. Moreover, if $w = 0$, then L'_e is clearly the order of $v \in R^2_{p^e}$.

Remark 32. The number L'_e divides the order of (M,v), which in turn divides $p^e \operatorname{ord}(M)$. Since

$$(M-I)w \in \ker \sum_{i=0}^{\operatorname{ord}(M)-1} M^i$$

the number L'_e does not divide $\operatorname{ord}(M)$ if and only if

$$v \notin \ker \sum_{i=0}^{\operatorname{ord}(M)-1} M^i\,.$$

For any positive integer n, we consider the condition

$$v \in \ker \sum_{i=0}^{n-1} M^i \tag{8}$$

and we call t the smallest positive integer satisfying (8).

Proposition 33. *The positive integers n satisfying* (8) *are precisely the multiples of t. Moreover, t divides* $\mathrm{ord}(M)p^e$.

Proof. Write $n = qt + r$, where r is the remainder of n after division by t. If $r = 0$, then (8) is satisfied because we have

$$\sum_{k=0}^{qt-1} M^k = \sum_{k=0}^{q-1}\sum_{l=0}^{t-1} M^{kt+l} = \left(\sum_{k=0}^{m-1} M^{kt}\right)\left(\sum_{l=0}^{t-1} M^l\right).$$

Now suppose that $r > 0$ and write

$$\sum_{k=0}^{n-1} M^k = M^r \sum_{k=0}^{qt-1} M^k + \sum_{k=0}^{r-1} M^k .$$

Then (8) does not hold for n because, by minimality of t, it does not hold for r. To prove the second assertion we take $n = \mathrm{ord}(M)p^e$ and observe that

$$\sum_{k=0}^{n-1} M^k = \sum_{k=0}^{p^e-1} M^{k\,\mathrm{ord}(M)} \sum_{l=0}^{\mathrm{ord}(M)-1} M^l = p^e \sum_{l=0}^{\mathrm{ord}(M)-1} M^l = 0 .$$

□

Remark 34. We show how to reduce to the case where L'_e is a power of p. If 1 is the only eigenvalue of M_1, then the order of (M, v) is a power of p and the same holds for L'_e. If the eigenvalues of M_1 are not 1, and $(M, v)w \neq w$ (which we exclude by saying that $v \notin \mathrm{Im}(M - I)$), then for the matrix $\sum_{k=0}^{L'_e-1} M^k$ to have a non-trivial kernel, we need that the order ℓ of one of the eigenvalues of M_1 divides L'_e hence we may replace M by M^ℓ and L'_e by L'_e/ℓ, reducing to the case where at least one eigenvalue is 1. We may now suppose that M_1 has two distinct eigenvalues $1, \lambda$ and, up to conjugation, that the two coordinates correspond to the 1-eigenspace and the λ-eigenspace respectively. In view of Remark 9, by Theorem 21 L'_e is a power of p possibly multiplied by $\mathrm{ord}(\lambda)$. Then we have only to determine whether $\mathrm{ord}(\lambda)$ divides L'_e. Analogously to Remark 26 we may replace (M, v) by $(M, v)^{p^x}$ for some large x we are left to consider an element (M_1, v') of order $\mathrm{ord}(\lambda)$, where the matrix is considered as a matrix modulo p^e and $v' = \sum_{i=0}^{p^x-1} M^i v$. We then only have to check whether $(M_1 - I)w + v' = 0$.

Remark 35. In Remark 34 we have seen how to reduce to the case where L'_e is a power of p. So, unless $L'_e = 1$ (which we may exclude with the condition $v \notin \mathrm{Im}(M - I)$) we may work with $(M, v)^p$ instead and hence without loss of generality replace M by a power such that $M_1 = I$. For $p = 2$, we may similarly reduce to the case $M_2 = I$.

Theorem 36. *Suppose that $M_1 = I$. If $L_e \neq t$, we have $L'_e = \mathrm{lcm}(L_e, t)$. Now suppose that $L_e = t$. We have $L'_e \mid L_e$ and, supposing additionally for $p = 2$ that $M_2 = I$, we have $L'_e = p^{e-k}$, where k (with $0 \leq k \leq e$) is the largest integer for which p^k divides $(M-I)w+v$.*

Proof. Write $(M-I)w+v=p^k w'$. Recall (7) and observe that L_e is the smallest positive integer n satisfying

$$(M-I)w \in \ker \sum_{i=0}^{n-1} M^i\,.$$

Then it is clear that L'_e divides $\mathrm{lcm}(L_e,t)$ and if $L_e \neq t$ (as L_e and t are powers of p) then (7) does not hold for the smallest of these numbers but it holds for the largest. Now suppose that $L_e = t$ and observe that $p \nmid w'$. If $k=e$, then clearly $L'_e=1$, so suppose that $k<e$. Then L'_e is the smallest positive integer n satisfying

$$w' \in \ker \sum_{i=0}^{n-1} M_{e-k}^i\,.$$

This condition holds for $n=p^{e-k}$ but it does not hold for $n=p^{e-k-1}$ by Lemma 37. □

Lemma 37. *Let $e\geq 1$ and suppose that $M_1=I$. Then we have*

$$\sum_{i=0}^{p^e-1} M^i = 0\,.$$

Supposing additionally for $p=2$ that $M_2=I$, the kernel of

$$\sum_{i=0}^{p^{e-1}-1} M^i$$

is pR^2_{e-1} (whose exponent is p^{e-1}).

Proof. Consider that $M_1=I$. The two assertions for $e=1$ follow immediately. For the first assertion, also observe (by the induction hypothesis) that

$$\sum_{i=0}^{p^{e-1}-1} M^i \equiv \sum_{i=0}^{p^{e-1}-1} M_{e-1}^i \equiv 0 \bmod p^{e-1}\,.$$

We deduce that

$$\sum_{i=0}^{p^e-1} M^i = \sum_{k=0}^{p-1} M^{p^{e-1}k} \cdot \sum_{i=0}^{p^{e-1}-1} M^i = 0\,.$$

By the first assertion, the kernel of

$$\sum_{i=0}^{p^{e-1}-1} M^i$$

contains pR^2_{e-1} so it suffices to prove that the exponent of the kernel is less than p^e. For $e=2$, the second assertion is clear for $p=2$ as $M=I$, so suppose that $p\neq 2$: writing $M=I+pN$, we may conclude because we have

$$\sum_{i=0}^{p-1} M^i = pI + \sum_{i=1}^{p-1} ipN = pI\,.$$

For $e \geq 3$ (as $M_2^p = I$) the exponent of the kernel of $\sum_{k=0}^{p-1} M^{p^{e-2}k}$ is p. We may then conclude (by the induction hypothesis) writing

$$\sum_{i=0}^{p^{e-1}-1} M^i = \sum_{k=0}^{p-1} M^{p^{e-2}k} \cdot \sum_{i=0}^{p^{e-2}-1} M^i \,.$$

□

Remark 38. Another viewpoint to study the action of $\mathrm{GL}_2(p^e) \ltimes R^2_{p^e}$ on $R^2_{p^e}$ is provided by Remark 9 because we have

$$\mathrm{GL}_2(p^e) \ltimes R^2_{p^e} < \mathrm{GL}_3(p^e) \qquad \text{and} \qquad R^2_{p^e} < R^3_{p^e} \,.$$

For this reason we may reduce to consider $M \in \mathrm{GL}_3(p^e)$ and $w \in R^3_{p^e}$ such that the last row of M is $(0, 0, 1)$ and the last component of w is 1.

Acknowledgements. During the preparation of this paper, Abel Lacabanne and Marusia Rebolledo have sent us the classification of the permutations stemming from $\mathrm{PGL}_2(\mathbb{F}_{p^n})$. We have opted to deduce the action of $\mathrm{PGL}_2(\mathbb{F}_p)$ from the action of $\mathrm{GL}_2(\mathbb{F}_p)$, however we thank them for their support. We also thank Fritz Hörmann for useful comments.

REFERENCES

[1] Alexandre Benoist and Antonella Perucca. Two variants of the Lang-Trotter conjecture on primitive points for elliptic curves. Submitted for publication (status: minor revisions), 2025.

[2] William C. Brown. *Matrices over commutative rings*, volume 169 of *Pure Appl. Math., Marcel Dekker*. New York: Marcel Dekker, 1993.

[3] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts Math.* New York, NY: Springer, 2nd ed. edition, 2009.