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

SZABOLCS BUZOGÁNY AND ANTONELLA PERUCCA

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 $n = p^e$, where p is a prime number and $e \geq 1$ (see the general Remark 9).

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 $(M - I)w$.*

This result shows that, for any M as in the statement, the cycle lengths of the associated permutation are $1, p, \ldots, p^a$ for some $a \geq 0$. 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 treat the general 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:

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

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 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 42.

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 5.3. 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 address the computational problem of determining the permutation structure of a matrix in $\mathrm{GL}_m(\mathbb{Z}/p^e\mathbb{Z})$. The zero vector forms a cycle of length 1. We then fix a non-zero column vector $w \in (\mathbb{Z}/p^e\mathbb{Z})^m$ and compute the length L of the cycle of M starting at w (it turns out that, by varying w, we only have a small case distinction). We call M_s (respectively, w_s) the reduction of M (respectively, w) modulo p^s for $1 \leq s \leq e$. We call L_s the length of the cycle of M_s starting at w_s, observing that $L = L_e$. We call F the fields with $p^{m!}$ element and consider the eigenvalues over F. In the following statement we rely on standard linear algebra algorithms.

Theorem 4. *Let $M \in \mathrm{GL}_m(\mathbb{Z}/p^e\mathbb{Z})$ and $w \neq 0$. The cycle length L_1 (respectively, the ratio L_{s+1}/L_s for $s = 1, \ldots, e-1$) is a power of p with exponent at most $\lceil \log_p(m+1) \rceil$ possibly times the least common multiple of the order of certain eigenvalues of M_1 (respectively, $M_1^{L_s}$).*

A more precise version of the above result is Theorem 27. In Section 5 we present an explicit finite procedure to compute the cycle length for any $M \in \mathrm{GL}_m(\mathbb{Z}/p^e\mathbb{Z})$ and for any w: the general case is Theorem 27 and specific observations for the special cases $m = 2, 3$ can be found in Section 5.2.

In case we are working with $\mathrm{GL}_2(\mathbb{Z}/p^e\mathbb{Z}) \ltimes (\mathbb{Z}/p^e\mathbb{Z})^2$, we outline two options: embedding this group into $\mathrm{GL}_3(\mathbb{Z}/p^e\mathbb{Z})$ as customary (see Remark 10) and apply the above algorithm; work directly with this group and apply the method presented in Section 6.

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 5. 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 6. 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 10.

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 7. 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 8. 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 9. We write $n = \prod_{i=1}^{r} n_i$, where the integers $n_1, \ldots, n_r$ 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

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

Thus a permutation σ on R_n^m is such that $\sigma(a) = (\sigma_1(a_1), \ldots, \sigma_r(a_r))$, 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 $i = 1, \ldots, r$.

Moreover, the tuple of the reduction maps modulo n_i (for $i = 1, \ldots, r$) 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 10. 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

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

Remark 11. In many settings, we consider a finite group of matrices acting on a finite abelian group G. Consider an invertible matrix A in this ring and fix $g \in G$. The set of integers n such that $A^n g = g$ clearly form a non-zero ideal of $\mathbb{Z}$. Now consider the set of the positive integers n such that

$$\sum_{i=0}^{n-1} A^i g \in G'$$

for some fixed subgroup G' of G such that $AG' = G'$. This set, if non-empty, it consists of the multiples of its smallest element. Indeed, if $n_1 < n_2$ belong to the set, then so does their difference because we can write

$$\sum_{i=0}^{(n_2-n_1)-1} A^i g = \sum_{i=0}^{n_2-1} A^i g - A^{n_2-n_1} \sum_{i=0}^{n_1-1} A^i g\,.$$

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

Remark 12. 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 $\frac{n}{\gcd(m,n)}$.

Remark 13. Lucas's theorem says the following: if p is a prime number and $z = \sum_i z_i p^i$ and $n = \sum_i n_i p^i$ are integers written in base p expansion, then we have

$$\binom{z}{n} \equiv \prod_{i \ge 0} \binom{z_i}{n_i} \mod p$$

where we use the convention that $\binom{z}{n} = 0$ if $z < n$.
We deduce that, for any positive integer x, setting $k := \lceil \log_p(x) \rceil$, we have

$$S_x := \{z \geq 1 \text{ such that } p \mid \binom{z}{n} \text{ for all } n = 1, 2, \ldots, x-1\} = p^k \mathbb{Z}_{\geq 1}\,.$$

This is clear for $x = 1$ so now suppose that $x \geq 2$. If $z \in S_x$, then we have $z_y = 0$ for all $0 \leq y < k$ by taking $n = p^y$ and applying Lucas's theorem hence $z \in p^k\mathbb{Z}_{\geq 1}$. Conversely, if $z \in p^k\mathbb{Z}_{\geq 1}$, then $z_i = 0$ for all $i = 0, \ldots, k-1$. For any $n = 1, 2, \ldots, x-1$ there is an index $0 \leq y < k$ such that $n_y \neq 0$, so $\binom{z_y}{n_y} = 0$ hence $\binom{z}{n} \equiv 0 \mod p$ by Lucas's theorem.

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 8 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 14. *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 15. *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 15, 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. If $r \in \mathbb{F}_{p^2}^\times$, then we write $\mathrm{ord}_H(r)$ for the smallest positive integer t such that $r^t \in H$. We observe that $\mathrm{ord}(r)/\mathrm{ord}_H(r)$ divides $p-1$.

Theorem 16. *If w is a λ_i-eigenvector of M, then we have $L_H = \mathrm{ord}_H(\lambda_i)$, for $i = 1, 2$. Now suppose that w is not an eigenvector of M. If $\lambda_1 \neq \lambda_2$ or M is a scalar matrix, then we have*

$$L_H = \mathrm{lcm}(\mathrm{ord}_H(\lambda_1), \mathrm{ord}_H(\lambda_2), \mathrm{ord}(\lambda_1\lambda_2^{-1}))\,.$$

In the remaining case, we have $\lambda_1 = \lambda_2$ and

$$L_H = p\,\mathrm{ord}_H(\lambda_1)\,.$$

Proof. The statement for λ_i-eigenvectors is clear because $M^n w = \lambda_i^n w$. Now suppose that w is not an eigenvector of M. If M is diagonalizable over $\mathbb{F}_{p^2}$, then L_H is the smallest positive integer n such that $\lambda_1^n = \lambda_2^n$ and this element is in H. We may then conclude because $\lambda_i^n \in H$ is equivalent to $\mathrm{ord}_H(\lambda_i) \mid n$ while $\lambda_1^n = \lambda_2^n$ is equivalent to $n \mid \mathrm{ord}(\lambda_1\lambda_2^{-1})$. In the remaining case, M has a unique eigenvalue $\lambda \in \mathbb{F}_p$ and, up to a base change, we have $M = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. Since $M^n = \begin{pmatrix} \lambda^n & n\lambda^{n-1} \\ 0 & \lambda^n \end{pmatrix}$ we get that L_H is the smallest positive integer n such that

$$\lambda^n \in H, \quad n\lambda^{n-1} \equiv 0 \bmod p,$$

and we may conclude. □

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

Let p be a prime number, $m \geq 2$. We call F the field with $p^{m!}$ elements. We see $M \in \mathrm{GL}_m(F)$ as a permutation of the vectors in F^m. For our purposes, $M \in \mathrm{GL}_m(p)$ hence the permutation maps F^m to itself and all eigenvalues of M are in F. We fix $w \in F^m$ and study the length L of the cycle of M at w. To ease notation, we let 1 be the least common multiple of an empty set of numbers.

The permutation structure of M is invariant under a base change in $\mathrm{GL}_m(F)$ 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 F^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 $i = 1, \dots, r$. So we reduce to the case where $M \in \mathrm{GL}_m(F)$ consists of a single Jordan block J.

Remark 17. 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 $\binom{k}{t}\lambda^{k-t}$. We observe that, by Remark 13, the order of J is

$$\mathrm{ord}(\lambda) p^{\lceil \log_p(m) \rceil}.$$

Theorem 18. *With the above notation, if $w = 0$, then $L = 1$. If $w \neq 0$, writing $w = (a_1, \dots, a_x, 0 \dots, 0)$ with $a_x \neq 0$ and $1 \leq x \leq m$, we have*

$$L = p^{\lceil \log_p(x) \rceil} \operatorname{ord} \lambda.$$

Proof. The statement is clear if $w = 0$, so suppose that $w \neq 0$. Consider the smallest positive integer L such that $w \in \ker(J^L - I)$. We apply Lemma 20 to $T := J^L - I$ hence we have $t_1 := \lambda^L - 1$ and $t_{i+1} := \binom{L}{i}\lambda^{L-i}$ for $1 \leq i \leq m-1$ by (1). We then have $w \in \ker(T)$ if and only if

$$\lambda^L = 1, \quad p \mid \binom{L}{n} \text{ for all } n = 1, 2, \dots, x-1 \tag{2}$$

holds. The former condition means that $\mathrm{ord}(\lambda) \mid L$. The other conditions, by Remark 13, mean that $p^{\lceil \log_p(x) \rceil} \mid L$ and we conclude because $\mathrm{ord}(\lambda)$ is coprime to p. □

Corollary 19. *With the above notation, assume that $p \geq m$. Then we have*

$$L = \begin{cases} 1, & \text{if } w = 0 \\ \operatorname{ord} \lambda, & \text{if } w \text{ is a } \lambda\text{-eigenvector for } J \\ p \operatorname{ord} \lambda, & \text{otherwise.} \end{cases}$$

Proof. The first two cases are clear (if w is a λ-eigenvector we have $x = 1$ hence the assertion also follows from Theorem 18). In the last case we have $1 < x \leq p$ so $\lceil \log_p(x) \rceil = 1$. □

Lemma 20. *Let $t_1, \dots, t_m \in F$. Let $\{e_1, \dots, e_m\}$ be the standard basis of F^m and consider the matrix*

$$T = \begin{pmatrix} t_1 & t_2 & t_3 & \dots & t_m \\ & t_1 & t_2 & \cdots & t_{m-1} \\ & & \ddots & & \vdots \\ & & & t_1 & t_2 \\ & & & & t_1 \end{pmatrix}.$$

(i) If $t_1 \neq 0$, then T is invertible. If $t_1 = 0$, the kernel of T is spanned by $e_1, \dots, e_x$, where x is the last index such that $t_x = 0$.
(ii) If $t_1 = 0$, a vector $a = (a_1, \dots, a_x, 0, \dots, 0) \in F^m$ with $a_x \neq 0$ is in the kernel of T if and only if $t_1 = t_2 = \dots = t_x = 0$.

Proof. The first assertion is evident, so suppose that $t_1 = 0$. The vectors $Te_1, \dots Te_x$ are zero while $Te_{x+1}, \dots Te_m$ are linearly independent. So the kernel of T is spanned by $e_1, \dots, e_x$ and (ii) easily follows. □

Example 21. Let $p \equiv 3 \bmod 4$ and let $i \in F$ be a fourth root of unity. Let $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $w = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. The eigenvalues of M are $\pm i$ with eigenvectors $f_1 = \begin{pmatrix} 1 \\ -i \end{pmatrix}$ and $f_2 = \begin{pmatrix} 1 \\ i \end{pmatrix}$. Changing the base to $\{f_1, f_2\}$, we have the diagonal matrix $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $w = \frac{1}{2}f_1 + \frac{1}{2}f_2$, so $w_1 = w_2 = \frac{1}{2}$. For each Jordan block, by Theorem 18 the contribution to L is given by $\mathrm{ord}(\pm i) = 4$. Thus we have $L = \mathrm{lcm}(4, 4) = 4$.

We observe that x in Theorem 18 can be any index from 1 to m. For a general matrix M, if we start from a vector $w \in R_p^m$ and base change so that the matrix is in Jordan normal form, then one can see that the vector w_i in a Jordan block can be zero or its last non-zero entry can be any entry (the condition that $w \in R_p^m \subseteq F^m$ only translates to relations between Jordan blocks and corresponding Jordan blocks with the conjugate eigenvalue).

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 the number L_1 can be determined thanks to Theorem 18.

Proposition 22. *Let $1 \leq s < e$ and write $M^{L_s} w = w + p^s w'_s$ for some $w'_s \in R_{p^e}^m$. Then L_{s+1}/L_s is the smallest positive integer t such that*

$$(w'_s \bmod p) \in \ker \left(\sum_{i=0}^{t-1} M_1^{L_s\, i} \right). \tag{3}$$

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

$$w'_{s+1} = \frac{(M^{L_{s+1}} - I)w}{p^{s+1}} = \frac{1}{p} \sum_{k=0}^{L_{s+1}/L_s - 1} M^{L_s k} \frac{(M^{L_s} - I)w}{p^s} = \frac{1}{p} \sum_{k=0}^{L_{s+1}/L_s - 1} M^{L_s k} w'_s. \tag{4}$$

Remark 24. 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 25. 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 22 and (4) because $w'_{s+x} = p^{-x} w'_s$.

Example 26. 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 22 we have $w'_1 = M'w$. Since

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

by Proposition 22 we have $L_2 = 1$ (which means $Mw = w$) if $w'_1 \equiv 0 \bmod p$ and $L_2 = p$ otherwise.

Theorem 27. *The quantities L_1 to L_e can be found recursively using the following finite procedure:*

(i) We find a matrix $A \in \mathrm{GL}_m(F)$ such that

$$AM_1A^{-1} = \mathrm{diag}(J_1, \ldots, J_r)$$

where J_i (for $i = 1, \ldots, r$) is a Jordan block corresponding to the eigenvalue λ_i. Let $v = Aw_1$. By grouping components we write $v = (v_1, \ldots, v_r)$ such that v_i and J_i have the same number of rows. If $v_i \neq 0$, we write

$$v_i = (a_1, \ldots, a_{x_i}, 0, \ldots, 0)$$

with $1 \leq x_i \leq m$ and $a_{x_i} \neq 0$. We let D be the set of indices for which $v_i \neq 0$. Then we have

$$L_1 = \mathrm{lcm}_{i \in D}\, p^{\lceil \log_p(x_i) \rceil} \operatorname{ord} \lambda_i.$$

(ii) Let $s \in \{1, \dots, e-1\}$ and write $(M^{L_s} - I)w = p^s w'_s$ for some $w'_s \in (\mathbb{Z}/p^e\mathbb{Z})^m$. We define A, r, J_i, λ_i as above for the matrix $M_1^{L_s}$, so we have

$$AM_1^{L_s}A^{-1} = \mathrm{diag}(J_1, \dots, J_r)\,.$$

We define $v = A(w'_s \mod p)$ and then, as in (i), consider the quantities v_i, x_i, and D. Then we have

$$L_{s+1} = L_s \cdot \mathrm{lcm}_{i \in D}(d_i)$$

where

$$d_i := \begin{cases} p^{\lceil \log_p(x_i+1) \rceil} & \text{if } v \neq 0 \text{ and } \lambda_i = 1 \\ \mathrm{ord}\,\lambda_i\, p^{\lceil \log_p(x_i) \rceil} & \text{if } v \neq 0 \text{ and } \lambda_i \neq 1\,. \end{cases}$$

Proof. Part (i) is equivalent to Theorem 18 so we only consider (ii).

As explained in the general setup, we may suppose that $M_1^{L_s}$ is in Jordan normal form. Thus w.l.o.g. we have $A = I$ and $v = (w'_s \bmod p)$ is a vector in F^m.

We make use of Proposition 22. Condition (3) is equivalent to $v_i \in \ker(\sum_{k=0}^{t-1} J_i^k)$ for all $i = 1, 2, \dots, r$ so we have reduced to consider a Jordan block J of $M_1^{L_s}$ corresponding to an eigenvalue λ and set $v := w'_s \mod p$ and $x := x_i$. We clearly have $L_{s+1}/L_s = 1$ if and only if $v = 0$. So suppose that $v \neq 0$. By (1), the matrix $T := \sum_{k=0}^{y-1} J^k$ is as in Lemma 20 with $t_n = \sum_{k=0}^{y-1} \binom{k}{n-1} \lambda^{k-n+1}$, so L_{s+1}/L_s is the smallest positive integer y such that p divides t_n for every $n = 1, \dots, x$.

If $\lambda = 1$, then by the hockey-stick identity we have $t_n = \binom{y}{n}$, so L_{s+1}/L_s is the smallest positive integer y such that p divides $\binom{y}{n}$ for $n = 1, 2, \dots, x$, which by Remark 13 is $p^{\lceil \log_p(x+1) \rceil}$.

Now suppose that $\lambda \neq 1$. For $j = 0, 1, \dots, x-1$, let

$$S_{j,y}(X) := \sum_{k=0}^{y-1} \binom{k}{j} X^{k-j} \in \mathbb{Z}[X]\,.$$

Then L_{s+1}/L_s is the smallest positive integer y such that p divides $S_{j,y}(\lambda)$ for every $y = 1, 2, \dots, x-1$. By comparing the corresponding coeffients, an easy computation gives:

$$S_{0,y}(X) = \frac{X^y - 1}{X - 1}, \quad (X-1)S_{j,y}(X) + S_{j-1,y}(X) = \binom{y}{j} X^{y-j}.$$

Evaluating these polynomials at λ we get that L_{s+1}/L_s is the smallest positive integer y such that

$$\lambda^y = 1, \quad p \mid \binom{y}{n} \text{ for each } n = 1, 2, \dots, x-1$$

so we may conclude by Remark 13. □

Proof of Theorem 4. This is a direct consequence of Theorem 27. □

Example 28. Suppose that $m = 2$ and that $M_1^{L_s}$ has distinct eigenvalues 1 and λ. We have

$$L_{s+1}/L_s = \begin{cases} 1 & \text{if } (w'_s \mod p) \text{ is zero} \\ p & \text{if } (w'_s \mod p) \text{ is a 1-eigenvector for } M_1^{L_s} \\ \mathrm{ord}(\lambda) & \text{if } (w'_s \mod p) \text{ is a } \lambda\text{-eigenvector for } M_1^{L_s} \\ p\,\mathrm{ord}(\lambda) & \text{otherwise.} \end{cases} \tag{5}$$

Corollary 29. *For every $s = 1, \dots, e$ we can write*

$$F^m = E^{(s)} \oplus E_1^{(s)}$$

where $E_1^{(s)}$ is the $F-$vector subspace corresponding to the Jordan blocks of $M_1^{L_s}$ with eigenvalue 1 (respectively, different from 1). Then, if $s < e$, we have $E_1^{(s)} \subseteq E_1^{(s+1)}$. Moreover, $E_1^{(s)} = E_1^{(s+1)}$ is equivalent to $w'_s \in E_1^{(s)}$.

Proof. The inclusion holds because $M_1^{L_{s+1}}$ is a power of $M_1^{L_s}$. We observe that the dimension of $E_1^{(s)}$ is the algebraic multiplicity of the eigenvalue 1 for $M_1^{L_s}$. If $w'_s \in E_1^{(s)}$, then by Theorem 27 L_{s+1}/L_s is a power of p hence the algebraic multiplicity of the eigenvalue 1 for $M_1^{L_{s+1}}$ is the same as that of $M_1^{L_s}$. Conversely, if $w'_s \in E_1^{(s)}$, then there is some eigenvalue $\lambda \neq 1$ of $M_1^{L_s}$ such that $\mathrm{ord}(\lambda)$ divides L_{s+1}/L_s which implies that the λ-eigenvectors of $M_1^{L_s}$ are 1-eigenvectors for $M_1^{L_{s+1}}$ so $E_1^{(s+1)}$ is strictly larger than $E_1^{(s)}$. □

5.1. **Special case $M \equiv I \mod p$.** In what follows, we make use of the notation w'_s from Proposition 22.

Corollary 30. *Assume that $M^{L_s} \equiv I \mod p$. Then we have*

$$L_{s+1}/L_s = \begin{cases} 1 & \text{if } w'_s \equiv 0 \mod p \\ p & \text{if } w'_s \not\equiv 0 \mod p. \end{cases}$$

Proof. This is a special case of Theorem 27. □

We observe that $Mw = w$ implies $L_e = 1$.

Theorem 31. *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 $p = 2$, we suppose additionally that $2 \mid M'$. Then we have*

$$w'_s \bmod p = \begin{cases} 0 \bmod p & \text{if } 1 \leq s \leq k \\ u \bmod p & \text{if } k < s < e \end{cases}$$

and $L_e = p^{e-k-1}$.

Proof. We observe that $L_1 = 1$ because $M_1 = I$. The latter assertion in the statement then follows from the former by multiple applications of Corollary 30.

Suppose that $k \geq 1$ and let $1 \leq s \leq k$. We prove that $w'_s \equiv 0 \bmod p$ and $L_s = 1$ by induction. For $s = 1$, the property is clear (as $k \geq 1$) so now fix $1 \leq s < k$. By Corollary 30, we have $L_{s+1} = L_s = 1$. We have

$$Mw = w + pM'w = w + p^{k+1}u \tag{6}$$

hence $w'_{s+1} = p^{k+1-(s+1)}u \equiv 0 \bmod p$.

By Corollary 30 we also deduce (from the case $s = k$) that $L_{k+1} = 1$. Then (6) gives $w'_{k+1} = u$. We now prove by strong induction that $w'_s \equiv u \bmod p$ holds for $k + 1 \leq s \leq e - 1$. We are left to prove the induction step: we fix $s \leq e - 2$, suppose that $w'_i \equiv u \bmod p$ holds for all

$k+1 \leq i \leq s$ and prove $w'_{s+1} \equiv u \bmod p$. The induction hypothesis implies by Corollary 30 that $L_{s+1} = p^{s-k}$. By 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 12). 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 12. □

Proof of Theorem 2. The result is equivalent to Theorem 31. □

5.2. **The special cases $\mathrm{GL}_2(p^e)$ and $\mathrm{GL}_3(p^e)$.** In what follows, we make use of the notation w'_s from Proposition 22.

Remark 32. Let $m = 2, 3$ and suppose that $p \neq 2$.

(i) Suppose that there exists $1 \leq s \leq e-1$ such that $M_1^{L_s} = I$. Then we can apply Theorem 31 to M^{L_s}: writing $M^{L_s} w = w + p^k u$ with $p \nmid u$ we deduce that $L_e = L_s p^{e-k-1}$.

(ii) Suppose that there exists $1 \leq s \leq e-1$ such that $M_1^{L_s}$ only has eigenvalues 1 over F. Then by Theorem 27 we have $L_{s+1}/L_s \in \{1, p\}$ and it is p if and only if the vector v is non-zero. Suppose that there is $s \leq s' \leq e-1$ such that $L_{s'+1}/L_{s'} = p$ (otherwise, we clearly have $L_e = L_s$). By (1) we have $M_1^{L_{s'}} = I$ so we can apply case (i) to determine L_e.

(iii) In general, let $1 \leq s \leq e-1$ and call k_s be the least common multiple of the order of the eigenvalues of $M_1^{L_s}$ (it is coprime to p). We can apply (ii) to $M^{k_s L_s}$, finding the cycle lengths $(L'_i)_{i \geq s}$, which are powers of p with the same p-adic valuation as $(L_i)_{i \geq s}$ because the ratio between L_s and L'_s divides k_s. By Theorem 27 the ratio k_s/k_{s+1} is the least common multiple of the order of the eigenvalues λ_i for $i \in D$ and hence it is the part coprime to p of the ratio $\frac{L_{s+1}}{L_s}$. We deduce that

$$\frac{L_{s+1}}{L_s} = \frac{k_s}{k_{s+1}} \cdot \frac{L'_{s+1}}{L'_s} .$$

Example 33. Let $m = 2$ and suppose that $p \neq 2$ and $M \equiv \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix} \mod p$ for some $\lambda \neq 1$. By Theorem 27(i), L_1 is 1 or $\mathrm{ord}(\lambda)$. We define $r_1 := L_1$ and for $1 < i \leq e$, $r_i = L_i/L_{i-1}$ so that $L_e = r_1 r_2 \cdots r_e$. We characterize all possible values of the tuple $(r_1, \ldots, r_e)$. We claim that we can write

$$r_i = p^{f_i} (\mathrm{ord}\, \lambda)^{g_i}$$

for some $f_i, g_i \in \{0, 1\}$ with f_i increasing, $f_1 = 0$ and $g_i = 1$ for at most one index. Let $M' = M^{\mathrm{ord}\, \lambda}$ and define L'_i, r'_i similarly. We make use of the notation of Remark 32. If w'_s is in the 1-eigenspace of $M_1^{L_s}$, then $k_s/k_{s+1} = 1$, and otherwise we have $k_s/k_{s+1} = \mathrm{ord}(\lambda)$, leading to $\mathrm{ord}(\lambda) \mid L_n$ and hence $L_n = \mathrm{ord}(\lambda) L'_n$ for every $s < n \leq e$. If for every $1 \leq s \leq e-1$ w'_s is in the 1-eigenspace of $M_1^{L_s}$, then L_e/L_1 is a power of p. We are left to

determine the p-adic valuation of r_i, which is the same as the one of r_i' for every $i = 1, \dots, s$. We conclude the proof of the claim by case (i) of Remark 32.

For example, if $p^e = 27$ and $\lambda = 2$, there are at most 12 possible tuples. For the matrix $M = \begin{pmatrix} 13 & 12 \\ 12 & 17 \end{pmatrix}$ we find all tuples by varying w:

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

Remark 34. Let $m = 2, 3$ and $p = 2$. Recall that the case $M_2 = I$ is covered by Theorem 31.

(i) Suppose that there exists $1 \leq s \leq e-1$ such that $M_2^{L_s} = I$. Then by applying Theorem 31 to M^{L_s}, writing $M^{L_s} w = w + p^k u$ with $p \nmid u$ we deduce that $L_e = L_s p^{e-k-1}$.

(ii) Suppose that there exists $1 \leq s \leq e-1$ such that 1 is the only eigenvalue of $M_1^{L_s}$ over F. We observe that $\mathrm{ord}(M^{L_s})$ is a power of 2 (see also Remark 17) hence the same holds for L_{n+1}/L_n for every $s \leq n \leq e-1$. Since $\mathrm{GL}_2(4)$ (respectively, $\mathrm{GL}_3(4)$) has exponent 12 (respectively, 24) we have $M_2^{L_s 2^m} = I$. We may then reduce to case (i) after having found two (respectively, three) ratios L_{n+1}/L_n that are larger than 1.

(iii) In the remaining case, we take s such that $M_1^{L_s}$ has two eigenvalues λ and λ' different from 1 and defined over F (with $\mathrm{ord}(\lambda) = \mathrm{ord}(\lambda')$) and, if $m = 3$, with additionally the eigenvalue 1. We observe that part (iii) of Remark 32 also applies for $p = 2$.

5.3. **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 $H \leq R_{p^e}^\times$ 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 24) 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 $\widetilde{L_s}$ (see Remark 11). Note that $\widetilde{L_1}$ can be computed using Theorem 16. 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

$$N^n w = \mu^n w + p^s \left(\sum_{i=0}^{n-1} N^i \right) \widetilde{w_s} \equiv hw \mod p^{s+1}. \tag{7}$$

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 (7).

Now suppose that $H = R_{p^e}$. Then (7) is equivalent to

$$\left(\sum_{i=0}^{n-1} N_1^i\right) \widetilde{w_s} \bmod p \in \langle w_1 \rangle \,. \tag{8}$$

We can apply Remark 11 to $A = N_1$, $g = \widetilde{w_s} \bmod p$, $G' = \langle w_1 \rangle$, recalling that $N_1\langle w_1\rangle = \langle w_1\rangle$. We deduce that $\widetilde{L_{s+1}}/\widetilde{L_s}$ divides every positive integer n satisfying (8). In particular, it divides t and $\mathrm{ord}(N_1)$ (respectively, 4 if $p = 2$ and N_1 is not diagonalizable) because the matrix sum in (8) is the zero matrix for this value. We remark the following:

- We have $\widetilde{L_{s+1}}/\widetilde{L_s} = 1$ if and only if $\widetilde{w_s} \bmod p$ is a multiple of w_1.
- If $\widetilde{w_s} \bmod p$ is not a multiple of w_1 and it is an eigenvector for N_1, then $\widetilde{L_{s+1}}/\widetilde{L_s} = t$. In the special case that the eigenvalue is 1, we get $t = p$.

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 5.

Theorem 35. *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

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

By choosing $t = -av_y/(1 - \lambda)$ 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 35 and the considerations at the beginning of this section. □

Remark 36. 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 $\mathrm{GL}_2(p^e) \ltimes R_{p^e}^2$ for $e > 1$.** Consider $(M, v) \in \mathrm{GL}_2(p^e) \ltimes R_{p^e}^2$ as a permutation of $R_{p^e}^2$. 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 $w \in R_{p^e}^2$. 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

$$(M - I)w + v \in \ker \sum_{i=0}^{n-1} M^i. \tag{9}$$

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

Remark 37. 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 $v \in R_{p^e}^2$.

Remark 38. 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

$$v \in \ker \sum_{i=0}^{n-1} M^i \tag{10}$$

and we call t the smallest positive integer satisfying (10).

‘

Proposition 39. *The positive integers n satisfying* (10) *are precisely the multiples of t. Moreover, t divides* $\mathrm{ord}(M)p^e$.

Proof. For the first assertion, we apply Remark 11. 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 40. 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 10, by Theorem 27 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 34 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 41. In Remark 40 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 42. *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 (9) 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 (9) 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 43. □

Lemma 43. *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 (we reason by induction) that

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

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 44. 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 10 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.

Consider an element $(A, a) \in \mathrm{GL}_2(p^e) \ltimes R^2_{p^e}$ and call A' the image of this element in $\mathrm{GL}_3(p^e)$. Up to a base change in $\mathrm{GL}_3(p^e)$ that is induced by a conjugation in $\mathrm{GL}_2(p^e) \ltimes R^2_{p^e}$ (see the

proof of Theorem 35), we can make sure that the last column of A' is either

$$\begin{pmatrix}0\\0\\1\end{pmatrix} \quad \text{or} \quad \begin{pmatrix}0\\1\\1\end{pmatrix}$$

and A and A' are in Jordan normal form. Even in this different basis, the vector w can be any vector with the last coordinate equal to 1. Thus, we can apply our results on $\mathrm{GL}_3(p^e)$ to study $\mathrm{GL}_2(p^e) \ltimes R_{p^e}^2$, observing that the last component of w'_s is 0 in this special case.

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.

Competing interest declaration. Competing interests: The authors declare none.

REFERENCES

[1] Alexandre Benoist and Antonella Perucca. Two variants of the Lang-Trotter conjecture on primitive points for elliptic curves. Research in Number Theory, to appear, 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.

(Szabolcs Buzogány) UNIVERSITY OF LUXEMBOURG, DEPARTMENT OF MATHEMATICS. 6, AVENUE DE LA FONTE, L-4364 ESCH-SUR-ALZETTE, LUXEMBOURG

Email address: szabolcs.buzogany@uni.lu

(Antonella Perucca) UNIVERSITY OF LUXEMBOURG, DEPARTMENT OF MATHEMATICS. 6, AVENUE DE LA FONTE, L-4364 ESCH-SUR-ALZETTE, LUXEMBOURG
ORCID: 0000-0003-3173-6988

Email address: antonella.perucca@uni.lu