ON THE INDEPENDENCE OF DIVISIBILITY CONDITIONS FOR ELLIPTIC CURVES

ALEXANDRE BENOIST, SZABOLCS BUZOGÁNY AND ANTONELLA PERUCCA

ABSTRACT. If E/K is an elliptic curve defined over a number field and $R \in E(K)$, we investigate the dependency of the divisibility conditions for the reductions of R. More precisely, we let p, q be prime numbers, and suppose that for almost all primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ is p-divisible or q-divisible in the group $E(k_\mathfrak{p})$, where $k_\mathfrak{p}$ is the residue field at $\mathfrak{p}$. We then ask whether $(R \bmod \mathfrak{p})$ is p-divisible for almost all primes $\mathfrak{p}$, or q-divisible for almost all primes $\mathfrak{p}$. We present both positive results and counterexamples, also giving a classification of the smallest possible counterexamples.

1. INTRODUCTION

Let E/K be an elliptic curve defined over a number field, and let $R \in E(K)$. For all primes $\mathfrak{p}$ of K that are of good reduction for E we consider the reduction $(R \bmod \mathfrak{p}) \in E(k_\mathfrak{p})$, where $k_\mathfrak{p}$ is the residue field at $\mathfrak{p}$. If n is a positive integer, we say that $(R \bmod \mathfrak{p})$ is n-divisible if there is some $R' \in E(k_\mathfrak{p})$ such that $[n]R' = (R \bmod \mathfrak{p})$.

We consider divisibility conditions that hold for almost all primes of K, by which we mean a set of primes of K of good reduction for E that has density 1. The *local-global principle for divisibility* – in the case of prime numbers – is the following result [7, Theorem 3.1]:

Theorem 1 (Dvornicich and Zannier). *Let p be a prime number and suppose that for almost all primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ is p-divisible. Then there is some $R' \in E(K)$ such that $[p]R' = R$.*

The analogous question for the n-divisibility easily reduces to the case where n is the power of a prime number p. For elliptic curves over $\mathbb{Q}$, if $p \neq 2, 3$ then the local-global principle for divisibility holds for all powers of p, as shown by Paladino, Ranieri and Viada. In general, various counterexamples are known, and we refer to the survey by Dvornicich and Paladino [6] and to the recent work [1] by Alessandrì and Paladino.

The aim of this work is comparing divisibility conditions for different prime numbers. We investigate the following question:

Question 2. Let p and q be distinct prime numbers, and suppose that for almost all primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ is p-divisible or q-divisible. Is then $(R \bmod \mathfrak{p})$ p-divisible for almost all primes $\mathfrak{p}$, or q-divisible for almost all primes $\mathfrak{p}$?

One positive result is the following:

Theorem 3. *If $2 \neq p < q$ and $q \not\equiv \pm 1 \bmod p$, then Question 2 has a positive answer. Moreover, fixing E/K and R, if p and q are sufficiently large, then Question 2 has a positive answer.*

We may rephrase Question 2 in terms of the image of the $\bmod pq$ torsion-Kummer representation. By the Chinese remainder theorem, the image of a Galois automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$ is a pair, that we denote by $A_{p,\sigma} \times A_{q,\sigma}$, whose components are the image of σ under the $\bmod p$ (respectively, $\bmod q$) torsion-Kummer representation. Now consider the $\bmod p$ representation (the $\bmod q$ representation being analogous). Up to choosing a basis for $E[p]$ and a point $R_p \in E(\bar{K})$ such that $[p]R_p = R$, we can write

$$A_{p,\sigma} = (M_{p,\sigma}, v_{p,\sigma}) \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \ltimes (\mathbb{Z}/p\mathbb{Z})^2$$

where the matrix $M_{p,\sigma}$ describes the action of σ on $E[p]$ (in the given basis) and where $v_{p,\sigma}$ is the point $\sigma(R_p) - R_p \in E[p]$ (expressed in the given basis).

We call $\frac{1}{p}R$ the set of points in $E(\overline{K})$ whose p-multiple equals R and write $K\big(\frac{1}{p}R\big)/K$ for the Galois extension obtained by adding the coordinates of the points in $\frac{1}{p}R$. Suppose that $\mathfrak{p}$ is a prime of K of good reduction for E that is not over p. Then the point $(R \bmod p)$ is p-divisible if and only if, for some (equivalently, for all) σ in the Frobenius conjugacy class of $\mathfrak{p}$ in $\mathrm{Gal}(K\big(\frac{1}{p}R\big)/K)$, the element $A_{p,\sigma}$ is *divisible*, by which we mean

$$v_{p,\sigma} \in \mathrm{Im}(M_{p,\sigma} - I)$$

where I is the 2×2 identity matrix. We refer e.g. to [2] for an introduction to the torsion-Kummer representations and this notion of divisibility.

Remark 4. The answer of Question 2 is negative if and only if the image of the $\bmod pq$ torsion-Kummer representation is an *admissible group*, by which we mean a subgroup Γ of

$$\mathrm{GL}_2(\mathbb{Z}/pq\mathbb{Z}) \ltimes (\mathbb{Z}/pq\mathbb{Z})^2$$

that has the following properties, denoting by $A = (A_p, A_q)$ its elements: for all $A \in \Gamma$, A_p is divisible or A_q is divisible; there is $A \in \Gamma$ such that A_p is not divisible; there is $B \in \Gamma$ such that B_q is not divisible.

We investigate the *minimal* admissible groups, by which we mean the admissible groups Γ that do not contain proper subgroups that are admissible. In particular, with the above notation, we must have $\Gamma = \langle A, B \rangle$. We suppose without loss of generality that $p < q$: the description of the minimal admissible groups is then achieved in Theorem 16 if $p \neq 2$ and $p \mid (q+1)$ and in Theorem 17 if $pq \neq 6$ and $p \mid (q-1)$. The remaining case $pq = 6$ is treated separately in Section 4, and in this case we can describe all admissible groups. Finally, in Section 5 we consider the generalization of Question 2 where we replace p, q by finitely many prime numbers.

This work stems from the Indivisibility-LT Conjecture stated in [2] (which is a variant of the Lang-Trotter conjecture on primitive points that allows for non-cyclic group of points $E(k_{\mathfrak{p}})$). The conjecture aims at understanding the set S of primes $\mathfrak{p}$ of K for which $(R \bmod \mathfrak{p})$ is not ℓ-divisible for any prime ℓ. Based on our investigation of Question 2 we can construct an example over $\mathbb{Q}$ such that the set S has density zero but for any prime ℓ there is a positive density of primes $\mathfrak{p}$ of K for which $(R \bmod \mathfrak{p})$ is not ℓ-divisible, see Example 30. In other words (by Theorem 1) the set S can have zero density even if the point R is not ℓ-divisible in $E(K)$ for any prime ℓ. We would also like to signal that the original Lang-Trotter conjecture lead to the question of constructing points in $E(K)$ that are not divisible but that are *locally imprimitive*, namely that fail to generate the group $E(k_{\mathfrak{p}})$ for (almost) all primes $\mathfrak{p}$. This problem has been studied in detail by N.Jones, Pappalardi and Stevenhagen in [9].

We now consider the setting of number fields, where K is a number field, $\alpha \in K^\times$ and we restrict to the primes $\mathfrak{p}$ of K for which $(\alpha \bmod \mathfrak{p})$ is well-defined. The local-global question for n-divisibility has been settled by Grunwald and Wang (see [6, Theorem 2.1]). Namely, if $(\alpha \bmod \mathfrak{p})$ is an n-th power in $k_\mathfrak{p}^\times$ for almost all $\mathfrak{p}$, then α is an n-th power in $K^\times$ unless $\zeta_4 \notin K$ and, calling h the largest positive integer such that $\zeta_{2^h} + \zeta_{2^h}^{-1} \in K$, we have $2^{h+1} \mid n$ and $\zeta_4(\zeta_{2^{h+1}} + \zeta_{2^{h+1}}^{-1}) \notin K$. The analogue of Question 2 for number fields would be the following. Let $\alpha \in K^\times$ be such that for almost all primes $\mathfrak{p}$ of K the element $(\alpha \bmod \mathfrak{p})$ is a p-th power or a q-th power in $k_\mathfrak{p}^\times$: does it follow that α is a p-th power or a q-th power in $K^\times$? A counterexample is $-3 \in \mathbb{Q}^\times$ because it is neither a square nor a cube but it is a square or a cube modulo any prime number $\mathfrak{p}$ (it is not a cube only if $\mathfrak{p} \equiv 1 \bmod 3$ and in this case it is a square, as $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$). We have the following definite result:

Theorem 5. *Let $\alpha \in K^\times$, let I be a finite set with at least two elements, and let ℓ_i for $i \in I$ be distinct prime numbers. Suppose that there is no $i \in I$ such that $\alpha \in K^{\times \ell_i}$. Then the following are equivalent: for almost all primes $\mathfrak{p}$ of K the element $(\alpha \bmod \mathfrak{p})$ is an ℓ_i-th power for some $i \in I$; there is some $i \in I$ such that $\zeta_{\ell_i} \in K$ and $\sqrt[\ell_i]{\alpha}$ is contained in $K(\zeta_{\ell_j} : j \in I, j \neq i)$.*

The last two sections of the paper contain various examples. The code supporting the numerical computations is available on GitHub at `https://github.com/alexandrebenoist/independence_divisibility_conditions_EC`.

2. Preliminaries on matrix groups

Fix a prime number p. We first recall some well-known facts: we have

$$\#\mathrm{GL}_2(\mathbb{F}_p) = p(p-1)^2(p+1)\,;$$

a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ of order divisible by p either contains $\mathrm{SL}_2(\mathbb{F}_p)$ or is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$; the matrices

$$S := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

generate $\mathrm{SL}_2(\mathbb{F}_p)$.

Lemma 6. *The matrix T has order p and any $M \in \mathrm{GL}_2(\mathbb{F}_p)$ of order p is a conjugate of T.*

Proof. The first assertion is because (by induction) for any $k > 0$ we have $T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$. Since $p^2 \nmid \#\mathrm{GL}_2(\mathbb{F}_p)$, the subgroup generated by M (respectively, T) is a p-Sylow subgroup. All p-Sylow subgroups are conjugate hence M is conjugate to T^k for some integer k coprime to p. We conclude because

$$T^k = \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} T \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}^{-1}.$$

□

We consider the semi-direct product $\mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2$, whose group law is

$$(M, v) \cdot (M', v') = (MM', Mv' + v)\,.$$

One may easily check that the inverse of (M, v) is $(M, v)^{-1} = (M^{-1}, -M^{-1}v)$. We denote by I the identity matrix of $\mathrm{GL}_2(\mathbb{F}_p)$. We may also compute the conjugate element

$$\begin{aligned}(N, w)(M, v)(N, w)^{-1} &= (NM, Nv + w)(N^{-1}, -N^{-1}w)\\ &= (NMN^{-1}, Nv - (NMN^{-1} - I)w)\,.\end{aligned} \tag{1}$$

Moreover, by induction, for every positive integer k we have

$$(M, v)^k = \left(M^k, \left(\sum_{j=0}^{k-1} M^j\right) v\right). \tag{2}$$

We observe that the order of (M, v) is a multiple of the order of M and it divides $p \cdot \mathrm{ord}(M)$ (an element of the form (I, w) has order dividing p).

The following map is an injective group homomorphism

$$\mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2 \to \mathrm{GL}_3(\mathbb{F}_p)$$

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

and we identify $\mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2$ with its image.

Remark 7. If $p \neq 2$, then p^2 does not divide the exponent of $\mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2$. Indeed, let (M, v) be an element which has order a power of p. As $p^2 \nmid \#\mathrm{GL}_2(\mathbb{F}_p)$ we have $M^p = I$. If $M = I$ then $(M, v)^p = (I, pv) = (I, 0)$. If $\mathrm{ord}(M) = p$, then by Lemma 6 up to a base change we may suppose that $M = T$. Since

$$\sum_{i=0}^{p-1} T^i = \sum_{i=0}^{p-1} \begin{pmatrix} 1 & i \\ 0 & 1\end{pmatrix} = 0,$$

by (2) we have $(T, v)^p = (I, 0)$ for all $v \in \mathbb{F}_p^2$. Moreover, 8 does not divide the exponent of $\mathrm{GL}_2(\mathbb{F}_2) \ltimes \mathbb{F}_2^2$ because (as $4 \nmid \#\mathrm{GL}_2(\mathbb{F}_2)$) the square of an element of order a power of 2 is of the form (I, v), whose order divides 2.

Definition 8. We say that (M, v) is *divisible* if $v \in \mathrm{Im}(M - I)$. If R is a ring with a morphism $R \to \mathbb{F}_p$ (typically, $R = \mathbb{Z}/pq\mathbb{Z}$ for some prime number q or $R = \mathbb{Z}$), then we have the reduction modulo p

$$\mathrm{GL}_2(R) \ltimes R^2 \to \mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2$$

and we call an element in $\mathrm{GL}_2(R) \ltimes R^2$ *p-divisible* if its reduction modulo p is divisible.

We observe that the rank of $M - I$ is invariant under conjugation of M (equivalently, of $M - I$). In the following result we investigate the effect of conjugation on divisible elements:

Proposition 9. *Let $(M, v) \in \mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2$.*

(i) *The element (M, v) is divisible if and only if $(N, w)(M, v)(N, w)^{-1}$ is divisible for each $(N, w) \in \mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2$.*

(ii) *If $N \in \mathrm{GL}_2(\mathbb{F}_p)$, then (M, v) is divisible if and only if (NMN^{-1}, Nv) is divisible.*

(iii) *The element (M, v) is divisible if and only if $(M, v + (M - I)w)$ is divisible for each $w \in \mathbb{F}_p^2$.*

(iv) *Given a divisible element (M, v), the conjugation with (I, w) such that $(M - I)w = v$ turns (M, v) into $(M, 0)$.*

Proof. If a matrix A is the conjugate of a matrix B, then B is a conjugate of A, so for (i) we only have to prove that the conjugate of a divisible matrix is divisible. Recall from (1) that we have

$$(N,w)(M,v)(N,w)^{-1} = (NMN^{-1}, Nv - (NMN^{-1} - I)w)\,.$$

Suppose that (M,v) is divisible and write $v = (M-I)u$. Then $Nv - (NMN^{-1} - I)w$ is in the image of $NMN^{-1} - I$ because

$$(NMN^{-1} - I)(Nu - w) = N(M-I)u - (NMN^{-1} - I)w = Nv - (NMN^{-1} - I)w.$$

Assertion (ii) (respectively, (iii) or (iv)) is evident by taking $w = 0$ (respectively, $N = I$) in the conjugation formula above. □

In the following result we investigate the notion of divisibility for powers:

Proposition 10. *Let $(M,v) \in \mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2$.*

(i) If (M,v) is divisible, then all powers of (M,v) are divisible.
(ii) If (M,v) is not divisible and k is an integer coprime to p, then $(M,v)^k$ is not divisible.
(iii) If (M,v) is not divisible, then its order is divisible by p.
(iv) Suppose that (M,v) is not divisible. If $p \neq 2$, then $(M,v)^p$ is divisible. If $p = 2$, then $(M,v)^4$ is divisible, while $(M,v)^2$ is divisible if and only if $M = I$.

Proof. Assertion (iii) is a consequence of (ii), observing that the identity element $(I,0)$ is divisible. Since we are working with a finite group, for (ii) we may suppose that k is positive. By (2) the element $(M,v)^k$ is divisible if and only if there is some $w \in \mathbb{F}_p^2$ such that

$$\left(\sum_{j=0}^{k-1} M^j\right) v = (M^k - I)w = \left(\sum_{j=0}^{k-1} M^j\right)(M-I)w.$$

If (M,v) is divisible, then we may take w such that $(M-I)w - v = 0$ and hence (i) holds. Now suppose that (M,v) is not divisible and that k is coprime to p. We remark that 1 is an eigenvalue of M. To prove (ii) we show that there is no $w \in \mathbb{F}_p^2$ such that

$$(M-I)w - v \in \ker\left(\sum_{j=0}^{k-1} M^j\right). \tag{3}$$

Suppose first that M has an eigenvalue $\lambda \neq 1$. By Proposition 9(i) we may, up to a base change, suppose that $M = \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$ and hence $\sum_{j=0}^{k-1} M^j = \begin{pmatrix} k & 0 \\ 0 & \sum_{j=0}^{k} \lambda^j \end{pmatrix}$. If w satisfies (3), the first component of $(M-I)w - v$ is zero. This is impossible because the first component of $(M-I)w$ is zero while the first component of v is non-zero as (M,v) is non-divisible.

Now suppose that M has only the eigenvalue 1. If $M = I$ the assertion is evident because $(M,v)^k = (I,kv)$ with $kv \neq 0$, so suppose that $M \neq I$. We conclude by proving that $\sum_{j=0}^{k-1} M^j$ is invertible. Up to a base change, we may suppose that $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Then we have $\sum_{j=0}^{k-1} M^j = \begin{pmatrix} k & k(k-1)/2 \\ 0 & k \end{pmatrix}$ and we conclude because $p \nmid k$.

In order to prove (iv), write $\mathrm{ord}(M,v) = p^e k$ with $p \nmid k$. By (ii) we know that $(M,v)^{p^e}$ is divisible (as its k-th power is $(I,0)$, which is divisible). For p odd we conclude by Remark 7. For $p = 2$, Remark 7 implies that $(M,v)^4$ is divisible and, as (M,v) is not divisible, we have two possibilities. Firstly, we may have $(M,v) = (I,v)$ and $v \neq 0$, in which case $(M,v)^2 = (I,0)$ is divisible. Secondly, we may have $\operatorname{ord}(M) = 2$ and hence, up to conjugation, $(M,v) = \left(T, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$, in which case $(M,v)^2 = \left(I, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right)$ is not divisible.

□

Example 11. If (M,v) is not divisible and $p \mid k$ then $(M,v)^k$ may be divisible or non-divisible. As an example for the former case we may take as k the order of (M,v). For the latter case we may take $p = k = 2$: both of the following elements are non-divisible

$$(M,v) = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) \qquad (M,v)^2 = \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right).$$

Another example is as follows: for $p = 3$, the element

$$(M,v) = \left(\begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix}\right)$$

is non-divisible of order 6, and in the cyclic group generated by it there are two elements which are divisible, namely the identity and $(M,v)^3$.

Proposition 12. *Suppose that $p \neq 2$. Let H be a subgroup of $\mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2$ that contains a non-divisible element and whose projection to $\mathrm{GL}_2(\mathbb{F}_p)$ contains $\mathrm{SL}_2(\mathbb{F}_p)$. Then H contains (I,w) for every $w \in \mathbb{F}_p^2$.*

Proof. We first prove that there is some non-zero $w \in \mathbb{F}_p^2$ such that $(I,w) \in H$. Let (M,v) be a non-divisible element in H. Up to replacing it by a power, by Proposition 10(ii) we may suppose that the order of (M,v) is a power of p hence it is 1 or p by Remark 7. If $M = I$, we may take $w = v$. Otherwise, by Lemma 6 and Proposition 9(i), we may suppose that $M = T$. By assumption there is some $z \in \mathbb{F}_p^2$ such that $(S,z) \in H$. Denoting by v_i (respectively, z_i) the components of v (respectively, z) for $i = 1,2$ we compute that

$$(S,z)(T,v)(S,z)^{-1}(T,v)(S,z)(T,v)^{-1} = \left(I, \begin{pmatrix} v_2 + z_1 \\ 2v_2 \end{pmatrix}\right)$$

is in H. The vector $w := \begin{pmatrix} v_2 + z_1 \\ 2v_2 \end{pmatrix}$ is non-zero because $v_2 \neq 0$ as (T,v) is non-divisible. We also have $(I,Tw) = (T,v)(I,w)(T,v)^{-1} \in H$. We may conclude because the vectors w and Tw are independent (as w is not an eigenvector for T). □

3. Admissible groups for $pq \neq 6$

Let p and q be primes with $p < q$. By an *admissible group* we mean a subgroup Γ of

$$\mathrm{GL}_2(\mathbb{Z}/pq\mathbb{Z}) \ltimes \mathbb{Z}/pq\mathbb{Z}^2$$

such that all elements of Γ are p-divisible or q-divisible but there exists $A \in \Gamma$ which is p-divisible but not q-divisible and there exists $B \in \Gamma$ which is q-divisible but not p-divisible. We call Γ_p (respectively, Γ_q) the group Γ modulo p (respectively, q).

We say that an admissible group is *minimal* if it contains no proper subgroups that are admissible groups, so in particular we have $\Gamma = \langle A, B \rangle$. If $Z \in \Gamma$, then we write Z as the pair $Z_p \times Z_q$ of its reductions modulo p and modulo q. We also denote by π the projection onto the first factor of the semi-direct product. Considering a word in A and B, we call the exponent of A (respectively, B) in the word the number of times that A (respectively, B) appears in the word.

No cyclic group can be an admissible group because if the generator is e.g. p-divisible, the same holds for all of its powers (see Proposition 10).

Lemma 13. *If $pq \neq 6$, then any admissible group Γ contains elements*

$$A = (I, 0) \times (N', u) \qquad \textit{and} \qquad B = (M, v) \times (N, w)$$

such that all of the following hold: the order of A is q; the order of B_p is p, B_p is not divisible and B_p^p is divisible; A_q is not divisible; B_q is divisible or order a power of p; $N \neq I$. Up to conjugation in the modulo q part, we may suppose that $w = 0$.

Proof. The last assertion follows from the others by Proposition 9(iv). Up to replacing A and B by a power, we may suppose by Proposition 10 that the order of A is a power of q and the order of B is a power of p such that B^p is p-divisible (by Remark 7 we deduce the assertion on the order of A and B). Since $q > p+1$ we have $q \nmid \#(\mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2)$ and hence $A_p = (I, 0)$. Moreover, the order of N' divides q because $q^2 \nmid \#\mathrm{GL}_2(\mathbb{F}_q)$. To conclude, we show that $N \neq I$. Suppose that $N = I$ and hence $B_q = (I, 0)$ as B is q-divisible. Then Γ contains the element $AB = (M, v) \times (N', u)$ that is neither p-divisible nor q-divisible, contradiction. □

Proposition 14. *If Γ_q contains a vector (N, w) with $N \in \{S, T, I\}$, then Γ contains $(I, 0) \times (N, w)$. Moreover, if $q > 3$, then $\pi(\Gamma_q)$ cannot contain both S and T.*

Proof. Since the order of N divides q, then by Remark 7 the same holds for (N, w). Considering that the order of $\mathrm{GL}_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^2$ is coprime to q, any preimage of (N, w) in Γ, raised to a suitable power, is of the form $(I, 0) \times (N, w)$.

Suppose that $\pi(\Gamma_q)$ contains both S and T. By the first assertion, there are some $s, t \in \mathbb{F}_q^2$ with $(I, 0) \times (S, s)$ and $(I, 0) \times (T, t)$ in Γ. Moreover, by Lemma 13 the group Γ contains a non q-divisible element $A = (I, 0) \times (N', u)$. Thus by Proposition 12, applied to the subgroup $\{(N, w) | (I, 0) \times (N, w) \in \Gamma\} \leq \mathrm{GL}_2(\mathbb{F}_q) \ltimes \mathbb{F}_q^2$, we conclude that Γ contains all elements of the form $(I, 0) \times (I, z)$. We easily deduce (setting $z = s, t$ and considering suitable products) that Γ also contains $(I, 0) \times (S, 0)$ and $(I, 0) \times (T, 0)$.
Up to conjugation, we let $B = (M, v) \times (N, 0)$ be as in Lemma 13. We claim that there is an element U with $\det(U) = 1$ and $\mathrm{rank}(NU - I) \neq 2$. Indeed, we can fix $u \in \mathbb{F}_q^2$ and exhibit U with $\det(U) = 1$ and $NUu = u$. Setting $u' := N^{-1}u$ and $u := (u_1, u_2)^T$, we can take $U = U_2 U_1^{-1}$, where $U_1 \in \mathrm{SL}_2(\mathbb{F}_q)$ is, according to whether $u_1 \neq 0$ or $u_2 \neq 0$, the matrix

$$\begin{pmatrix} u_1 & 0 \\ u_2 & u_1^{-1} \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} u_1 & -u_2^{-1} \\ u_2 & 0 \end{pmatrix}$$

and where $U_2 \in \mathrm{SL}_2(\mathbb{F}_q)$ is analogously defined for u'. Indeed, U_1 maps $(1, 0)^T$ to u while U_2 maps $(1, 0)^T$ to u' hence $Uu = N^{-1}u$.

Let $z \in \mathbb{F}_q^2$ be such that $z \notin \mathrm{Im}(NU - I)$. Since S and T generate $\mathrm{SL}_2(\mathbb{F}_q)$, we have $(I, 0) \times (U, 0) \in \Gamma$. Then the following element in Γ is neither p-divisible nor q-divisible, giving a contradiction:

$$(I, 0) \times (I, z) \cdot B \cdot (I, 0) \times (U, 0) = (M, v) \times (NU, z)\,.$$

□

Lemma 15. *There can only be admissible groups if $p \mid (q^2-1)$. Moreover, if $p \neq 2$ and Γ is an admissible group with $q \mid \#\pi(\Gamma_q)$, then $p \mid (q-1)$ and $\pi(\Gamma_q)$ is contained in a Borel subgroup.*

Proof. The statement is trivial if $pq = 6$, so we can exclude this case. By Lemma 13, a necessary condition to have admissible groups is that $p \mid (q^2-1)$ because the order of N is a nontrivial power of p which divides $\#\mathrm{GL}_2(\mathbb{F}_q)$. To conclude we prove that for $p \neq 2$ and $q \mid \#\pi(\Gamma_q)$ we cannot have $p \mid (q+1)$. By Proposition 14 the group $\pi(\Gamma_q)$ does not contain both S and T hence (as it does not contain $\mathrm{SL}_2(\mathbb{F}_q)$) it must be contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. The size of this group is $(q-1)^2q$ and it contains N, so $p \mid (q-1)$. □

Theorem 16. *Suppose that $p \mid (q+1)$ and $p \neq 2$. Let $\Omega = \langle A, B\rangle$, where*

$$A = (I,0) \times (I,u)$$
$$B = (M,v) \times (N,0)$$

such that $u \neq 0$, B_p is non-divisible of order p, $N \neq I$ and $\mathrm{ord}(N)$ is a power of p. Then the following holds:

(i) The group Ω is a minimal admissible group. We have

$$\Omega = \{(M,v)^k \times (N^k, z) | k \in \mathbb{Z}, z \in \mathbb{F}_q^2\}\,.$$

In particular, $\Omega \simeq \langle N\rangle \ltimes \mathbb{F}_q^2$ and it has order $p^v q^2$, where $v = \mathrm{ord}(N) > 0$.

(ii) Any admissible group contains some conjugate of a group of the form Ω.

Proof. Let Γ be admissible. Our starting point is Lemma 13 (by Remark 7, B_p^p is the identity). Since $p \neq 2$ and $p \nmid (q-1)$, by Lemma 15 we have $q \nmid \#\pi(\Gamma_q)$ and hence $\mathrm{ord}(N') = 1$. Thus Γ contains a conjugate copy of Ω.

We have $\det(N) = 1$ because $\mathrm{ord}(N)$ is coprime to $q-1$. If N would have an eigenvalue 1 then, up to conjugation, it would be a power of T and hence it would have order dividing q, contradiction. Thus, $N - I$ has rank 2. The matrix N cannot be diagonalizable over $\mathbb{F}_q$ because its order is larger than 1 and coprime to $q-1$. Thus its eigenvalues are in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. In particular, u is not an eigenvector for N and hence u and Nu span $\mathbb{F}_q^2$. Since Ω contains $BAB^{-1} = (I,0) \times (I, Nu)$, we deduce that Ω contains every vector of the form $(I,0) \times (I,z)$ with $z \in \mathbb{F}_q^2$. The assertions on the group structure of Ω follow because Ω is generated by B and by $(I,0) \times (I,z)$ with $z \in \mathbb{F}_q^2$.

Since A_q and B_p are not divisible, to show that Ω is admissible note that the word $(M,v)^k \times (N^k, z) \in \Omega$ is p-divisible if $p \mid k$ and q-divisible if $p \nmid k$ (because in the latter case $N^k - I$ has rank 2). We observe that Ω is minimal because if it only contains elements of the form $(M,v)^k \times (N^k, z)$ with $p \mid k$ then all elements of Ω are p-divisible. Otherwise, up to conjugation, it contains B (and after this conjugation A becomes $(I,0) \times (I,u')$ for some $u' \neq 0$) hence we have a group isomorphic to Ω. □

In the following result, we observe that for the matrix N from Lemma 13, if N is upper triangular and $N - I$ has rank 2, then the eigenvalues of N are in $\mathbb{F}_q^\times$ and have order a power of p (and, if there is only one eigenvalue, N is a scalar matrix).

Theorem 17. *Suppose that $p \mid (q-1)$ and that $pq \neq 6$.*

(i) *Let* $\Omega = \langle A, B\rangle$*, where*

$$A = (I,0)\times(I,u)$$
$$B = (M,v)\times(N,0)$$

are such that the following holds: $u\neq 0$*;* B_p *not divisible of order* p*;* $Nu=\lambda u$ *for some* $\lambda\in\mathbb{F}_q$*,* $\lambda\neq 0,1$*. We have* $BAB^{-1}=A^\lambda$ *and*

$$\Omega = \{(M,v)^k\times(N^k,\mu u)|k\in\mathbb{Z},\mu\in\mathbb{F}_q\}\simeq\langle N\rangle\ltimes\langle u\rangle \tag{4}$$

and Ω *is a minimal admissible group that has order* pq*.*

(ii) *Let* $\Omega'=\langle A,B\rangle$*, where*

$$A = (I,0)\times(T,w)$$
$$B = (M,v)\times(N,0)$$

such that the following holds: $w=\begin{pmatrix}w_1\\w_2\end{pmatrix}$ *with* $w_2\neq 0$ *(*A_q *is not divisible);* B_p *is not divisible of order* p*;* $N\neq I$ *and* $\operatorname{ord}(N)$ *is a power of* p*;*

$$N=\begin{pmatrix}\lambda_1 & b\\ 0 & \lambda_2\end{pmatrix}\qquad \text{for some } b\in\mathbb{F}_q\,.$$

- *If* $\lambda_1,\lambda_2\neq 1$*, then* Ω' *is an admissible group contained in the admissible group*

  $$\Omega'':=\{(M,v)^k\times\left(\begin{pmatrix}\lambda_1^k & z\\ 0 & \lambda_2^k\end{pmatrix},\begin{pmatrix}x\\y\end{pmatrix}\right)|k\in\mathbb{Z},x,y,z\in\mathbb{F}_q\}\,.$$

  If Ω' *contains an element of the form* $(I,0)\times(I,u)$ *with* $u\neq 0$*, then it contains a proper subgroup of the form* Ω *and in particular it is not minimal. If* Ω' *does not contain an element of the form* $(I,0)\times(I,u)$ *with* $u\neq 0$ *it has order* pq*, and is minimal. The latter case holds if and only if*

  $$\lambda_1=\lambda_2^2\qquad\text{and}\qquad b=(\lambda_2^2-\lambda_2)\Big(\frac{1}{2}-\frac{w_1}{w_2}\Big)\,,$$

  in which case we have $A^q=B^p=I$ *and* $BAB^{-1}=A^{\lambda_2}$*.*
- *If* $\lambda_1=1$ *or* $\lambda_2=1$*, then* Ω' *is an admissible group if and only if* $p=2$*,*

  $$N=\begin{pmatrix}1 & b\\ 0 & -1\end{pmatrix}\quad\text{and}\quad w\in\langle\begin{pmatrix}b-1\\-2\end{pmatrix}\rangle\,.$$

  In this case, Ω' *is minimal and isomorphic to the dihedral group* D_{2q} *and* Ω' *does not contain an element of the form* $(I,0)\times(I,u)$ *with* $u\neq 0$*.*

(iii) *If an admissible group* Γ *contains (respectively, does not contain) an element of the form* $(I,0)\times(I,u)$ *with* $u\neq 0$*, then it contains a subgroup of the form* Ω *(respectively,* Ω'*).*

Proof. Proof of (i). The statement $BAB^{-1}=A^\lambda$ follows from (1) and $Nu=\lambda u$. From this it follows that all elements of Ω are of the form $A^\mu B^\nu$ for some integers μ,ν, hence (4) holds (in particular Ω has order pq). Such an element is p-divisible if $p\mid\nu$ and otherwise it is q-divisible because $\langle u\rangle$ is in the image of $N^\nu-I$ (as $\lambda\neq 1$). Thus, Ω is admissible (considering that A is not q-divisible and B is not p-divisible). Since by Lemma 13 an admissible group must contain an element of order p (respectively, q) we deduce that Ω is minimal.

Proof of (iii). By Lemma 13, up to conjugation, Γ contains elements

$$A=(I,0)\times(N',w)\qquad\text{and}\qquad B=(M,v)\times(N,0)$$

with A_q not divisible, $\operatorname{ord}(N') \mid q$, $\operatorname{ord}(N)$ a non-trivial power of p, B_p not divisible and B_p^p divisible. We observe that the eigenvalues of N are in $\mathbb{F}_q$ (because $p \mid (q-1)$) and at least one eigenvalue λ of N is not 1 (because $\operatorname{ord}(N) \neq 1, q$).

In the former case, up to replacing Γ by a subgroup, we may suppose that $A = (I,0) \times (I,w)$. Consider the element $BAB^{-1} = (I,0) \times (I,Nw)$. If w is an eigenvector for N, it is not a 1-eigenvector (otherwise, $Nw = w$ and $B(BAB^{-1})$ is neither p-divisible nor q-divisible) and hence $\langle A, B\rangle$ is of the form Ω. If w is not an eigenvector for N, then, w and Nw are $\mathbb{F}_q$-linearly independent hence Γ contains $(I,0) \times (I,z)$ for any $z \in \mathbb{F}_q^2$. We may then take for z an eigenvector of N, which case we have already covered.

In the latter case, $\operatorname{ord}(N') = q$ hence $q \mid \#\pi(\Gamma_q)$. By Proposition 14, $\pi(\Gamma_q)$ must be contained in a Borel subgroup, thus N is upper triangular, thus Γ contains a subgroup that is of the form Ω'.

Proof of (ii). We first suppose that $\lambda_1, \lambda_2 \neq 1$. The elements of Ω'' are p-divisible if $p \mid k$ and otherwise they are q-divisible because $\begin{pmatrix}\lambda_1^k - 1 & b\\ 0 & \lambda_2^k - 1\end{pmatrix}$ has rank 2. Since Ω' is a subgroup of Ω'' (considering that A is not q-divisible and B is not p-divisible) both Ω' and Ω'' are admissible groups.

If Ω' contains an element of the form $A' = (I,0) \times (I,u)$ for some $u \neq 0$, by (iii) Ω' contains a subgroup the form Ω (we cannot have $\Omega = \Omega'$ because T is not a power of N). Since

$$BAB^{-1} = (I,0) \times \Big(\begin{pmatrix}1 & \lambda_1/\lambda_2\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\lambda_1 w_1 + b w_2\\ \lambda_2 w_2\end{pmatrix} \Big) \qquad \text{and}$$

$$A^{\lambda_1/\lambda_2} = (I,0) \times \Big(\begin{pmatrix}1 & \lambda_1/\lambda_2\\ 0 & 1\end{pmatrix}, \begin{pmatrix}\frac{\lambda_1}{\lambda_2} w_1 + \frac{1}{2} w_2((\frac{\lambda_1}{\lambda_2})^2 - \frac{\lambda_1}{\lambda_2})\\ \frac{\lambda_1}{\lambda_2} w_2\end{pmatrix} \Big)$$

if $BAB^{-1} \neq A^{\lambda_1/\lambda_2}$ then Ω' contains an element of the form A'. Comparing the components of the vectors, the condition $BAB^{-1} = A^{\lambda_1/\lambda_2}$ is equivalent to

$$\lambda_1 = \lambda_2^2 \qquad \text{and} \qquad b = (\lambda_2^2 - \lambda_2)(\frac{1}{2} - \frac{w_1}{w_2})$$

and it implies that Ω' has order pq and hence it is minimal.

Now suppose that N is of the form $\begin{pmatrix}\lambda & b\\ 0 & 1\end{pmatrix}$ or $\begin{pmatrix}1 & b\\ 0 & \lambda\end{pmatrix}$ with $\lambda \neq 1$ having order a power of p. The former case is impossible otherwise AB is not divisible, as $AB_p = B_p$ and (recalling that $w_2 \neq 0$)

$$AB_q = \Big(\begin{pmatrix}\lambda & b+1\\ 0 & 1\end{pmatrix}, w \Big).$$

We consider the latter case: we have

$$AB_q = \Big(\begin{pmatrix}1 & b+\lambda\\ 0 & \lambda\end{pmatrix}, \begin{pmatrix}w_1\\ w_2\end{pmatrix} \Big) \quad \text{and} \quad A^2 B_q = \Big(\begin{pmatrix}1 & b+2\lambda\\ 0 & \lambda\end{pmatrix}, \begin{pmatrix}2w_1 + w_2\\ 2w_2\end{pmatrix} \Big).$$

Since these elements are divisible, we deduce that $\begin{pmatrix}w_1\\ w_2\end{pmatrix} = c\begin{pmatrix}b+\lambda\\ -1+\lambda\end{pmatrix}$ and $\begin{pmatrix}2w_1 + w_2\\ 2w_2\end{pmatrix} = 2c\begin{pmatrix}b+2\lambda\\ -1+\lambda\end{pmatrix}$ holds for some $c \in \mathbb{F}_q^\times$. We deduce that $\lambda = -1$ hence $p = 2$.

So suppose that $p = 2$,

$$N = \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad w \in \langle \begin{pmatrix} b-1 \\ -2 \end{pmatrix} \rangle .$$

We have $\operatorname{ord}(A) = q$ (see Remark 7), $\operatorname{ord}(B) = 2$ and $AB = BA^{-1}$. Thus Ω' is isomorphic to the dihedral group D_{2q}. All powers of A are p-divisible while all elements of the form A^nB are q-divisible because (by induction on n) we can write

$$A^nB_q = \Big(\begin{pmatrix} 1 & b-n \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} nw_1 + \frac{n(n-1)}{2} w_2 \\ nw_2 \end{pmatrix} \Big) .$$

Since Ω' has order $2q$ (and A is not q-divisible and B is not p-divisible), we conclude that it is a minimal admissible group. □

Remark 18. Note that the condition $pq > 6$ is necessary here. We will see that if $pq = 6$ and Γ is the (up to conjugacy unique) admissible group of order 432, then $\pi(\Gamma_q)$ does contain S and T.

Example 19. There are admissible groups modulo $2q$ for every odd prime number $q > 3$ (for $q = 3$ there are as well, see Section 4). Indeed, as a special case of Theorem 17, we can take

$$A = (I, 0) \times (T, u)$$
$$B = (I, v) \times (-I, 0)$$

with any $v \neq 0$ and $u \notin \operatorname{Im}(T - I)$.

Example 20. There are admissible groups modulo pq for every $p \neq 2$ such that $p \mid (q-1)$. Indeed, by Theorem 17, we can take

$$A = (I, 0) \times (I, u)$$
$$B = (T, v) \times (\lambda I, 0)$$

where λ has order p in $\mathbb{F}_q^\times$.

Example 21. There are admissible groups modulo pq for every $p \neq 2$ such that $p \mid (q+1)$. Indeed, by Theorem 16 we can take

$$A = (I, 0) \times (I, u)$$
$$B = (T, v) \times \Big(\begin{pmatrix} 0 & 1 \\ -1 & d \end{pmatrix}, 0 \Big)$$

with any $u \neq 0$ and $v \notin \operatorname{Im}(T - I)$, and where $x^2 - dx + 1$ is the minimal polynomial modulo q of a root of unity of order p (this cyclotomic field is quadratic because $p \mid \#\mathbb{F}_{q^2}^\times$). Indeed, by construction, the eigenvalues of $\pi(B_q)$ over $\mathbb{F}_{q^2}$ have order p (and they are distinct because their product is 1).

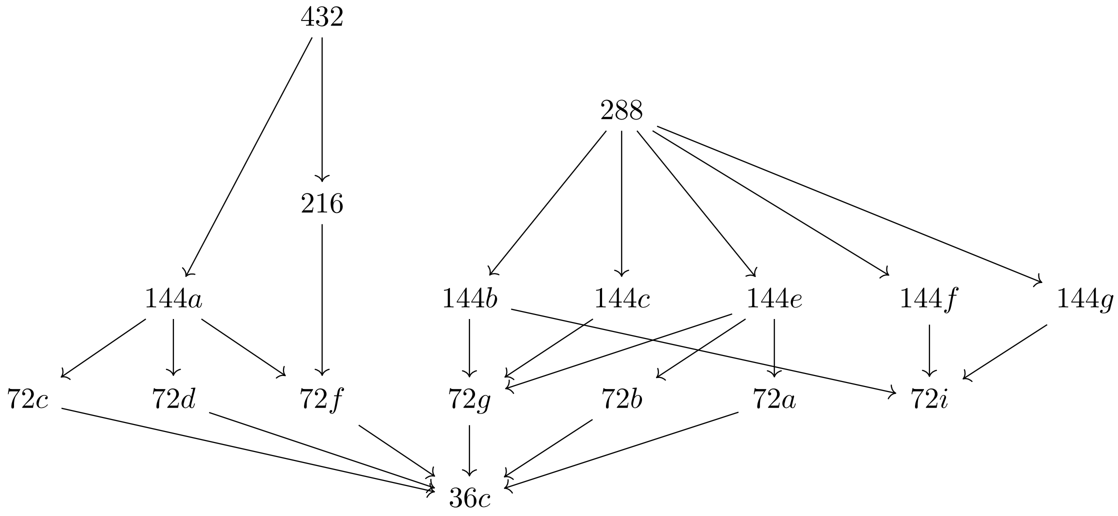
4. Admissible groups for $pq = 6$

With [5] we have computed the list of all admissible groups modulo 6. Since there are 2891 such admissible groups, we consider them up to conjugation in the group

$$\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) \ltimes (\mathbb{Z}/6\mathbb{Z})^2 .$$

We have labeled their conjugacy classes as in the following examples: the admissible group 432 is the only one, up to conjugation, with order 432; the admissible groups $108a$ and $108b$

FIGURE 1. We display, up to conjugacy, the graph of the admissible subgroups contained in an admissible group of order 432 or of order 228.



are those up to conjugation, with order 108. These labels are described in the auxiliary file, where we give generators modulo 6 for one group in each conjugacy class.

With the code presented in the auxiliary file as a Jupyter Notebook we have computed the graphs presented in Figures 1, 2, 3 and 4. In these graphs, each node is a conjugacy class of admissible groups modulo 6, and the edges depict inclusions in the following sense: an edge from X to Y means that some admissible group that is conjugate to Y is a subgroup of X. We then have the following observations:

- There are 54 conjugacy classes of admissible groups modulo 6.
- There are, up to conjugation, 7 minimal admissible groups.
- There are, up to conjugation, 8 maximal admissible groups (namely, admissible groups that are not up to conjugation proper subgroups of another admissible group).
- It is possible that an admissible group is contained into two larger admissible groups that are not one a subgroup of the other. This is the case for the admissible groups of size 54 (see Figure 3) because each of them is contained in a subgroup in the class $108a$ and in a subgroup of the class $108b$.
- There are admissible subgroups of the same order that are not conjugate (for example, $108a$ and $108b$). Moreover, there are isomorphic admissible subgroups that are not conjugate, for example the admissible groups of order 6 are all isomorphic to the dihedral group D_6 but $6b$, contrary to $6a$ and $6c$, does not contain any element (I, u) modulo 6 with $u \neq 0$.
- The largest order for an admissible group is 432 (this group is described in Section 4.1). The smallest order for an admissible group is 6.
- The group 432 contains a subgroup that is isomorphic to D_6 but none of the admissible groups of order 6.

4.1. **The admissible group of order** 432**.** The admissible group Γ of order 432 (which is unique up to conjugation) is a subgroup of index 24 of $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) \ltimes (\mathbb{Z}/6\mathbb{Z})^2$. The group Γ

FIGURE 2. We display, up to conjugation, the graph of the admissible subgroups contained in $144d$.

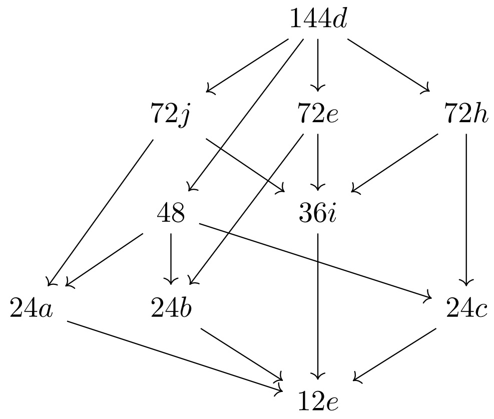
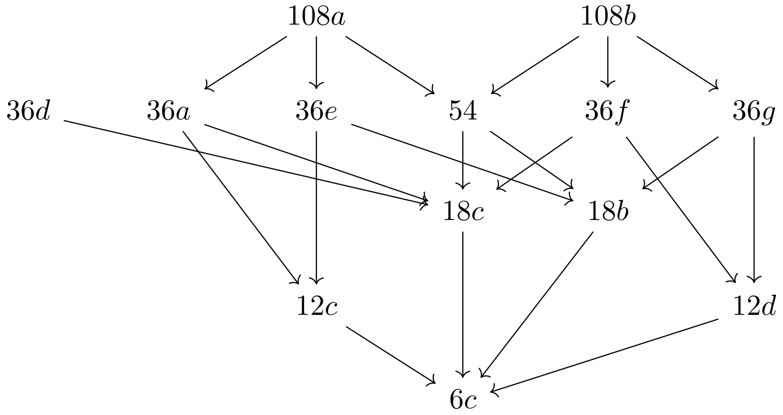


FIGURE 3. We display, up to conjugation, the graph of the admissible subgroups contained in $108a$ or $108b$.



contains $(I,0)\times(I,z)$ for every $z\in\mathbb{F}_3^2$. Moreover, Γ contains $(I,0)\times(-I,0)$. We may then neglect the vector in $\mathbb{F}_3$ and consider the matrices in $\pi(\Gamma_3)$ up to a non-zero scalar, so we are left to describe a group of order 24. A precise description of Γ is as follows: up to conjugation, we have

$$\Gamma=\{\phi(M)\times(M,v)|(M,v)\in\mathrm{GL}_2(\mathbb{F}_3)\ltimes\mathbb{F}_3^2\}.$$

where the map

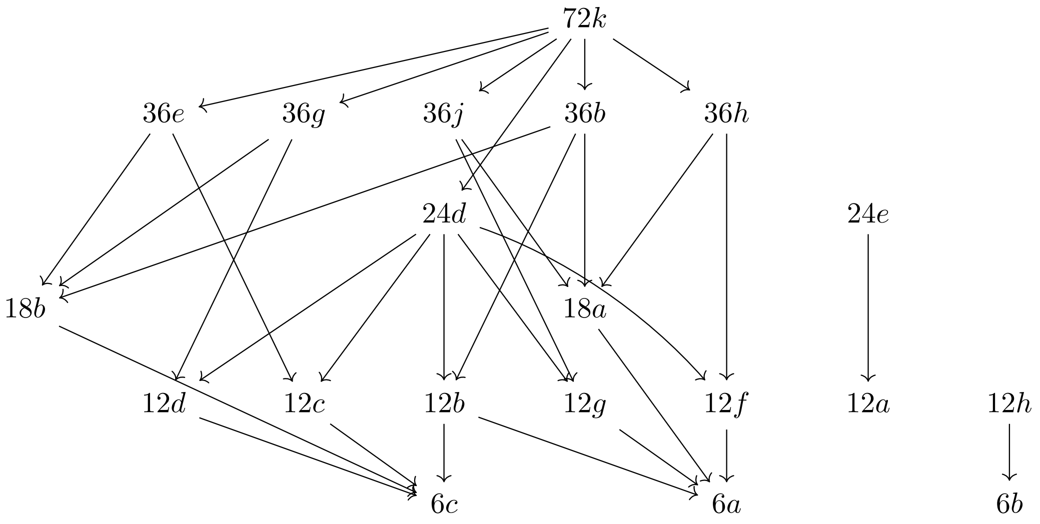
$$\phi:\mathrm{GL}_2(\mathbb{F}_3)\to\mathrm{GL}_2(\mathbb{F}_2)\ltimes(\mathbb{F}_2)^2$$

is determined by

$$\phi\begin{pmatrix}1&0\\0&2\end{pmatrix}=\left(\begin{pmatrix}0&1\\1&0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\right),$$

$$\phi\begin{pmatrix}1&1\\0&1\end{pmatrix}=\left(\begin{pmatrix}0&1\\1&1\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix}\right),$$

FIGURE 4. We display, up to conjugation, the graph of the admissible subgroups contained in $72k$, $24e$ and $12h$.



$$\phi\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}=\left(\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix},\begin{pmatrix}1\\ 1\end{pmatrix}\right),$$

and it is a surjective group homomorphism whose kernel is $\{\pm I\}$. Note that the map $\Gamma\to\Gamma_q$ is surjective. The homomorphism ϕ satisfies the following property: whenever $\operatorname{rank}(M-I)\neq 2$ or $\operatorname{rank}(M-2I)\neq 2$, the element $\phi(M)$ is divisible. Here we remark that the group $\mathrm{GL}_2(\mathbb{F}_3)$ has 30 elements such that $\operatorname{rank}(M-I)\neq 2$ and $\operatorname{rank}(M-2I)\neq 2$ and 18 element such that this is not the case. The group $\mathrm{GL}_2(\mathbb{F}_2)\ltimes(\mathbb{F}_2)^2$ contains 15 divisible elements (4 elements for each matrix of rank 2, 2 elements for each matrix of rank 1, and the identity) and 9 indivisible elements. We observe that $A\in\Gamma$ is 3-divisible if and only if $\pi(A_3)-I$ has rank 2 (because the vector a_3 can be any vector). Considering that $\pi(A_3)$ and $-\pi(A_3)$ have the same image under ϕ we deduce the following: if $\pi(A_3)$ has an eigenvalue 1 or -1 (which means that $\pi(A_3)-I$ or $-\pi(A_3)-I$ do not have rank 2) then $\phi(A_3)$ is divisible. Requiring that the eigenvalues are 1 or -1 gives 15 classes modulo $-I$. Thus ϕ must map the elements in these 15 classes to the 15 divisible elements of $\mathrm{GL}_2(\mathbb{F}_2)\ltimes(\mathbb{F}_2)^2$.

5. QUESTION 2 AND ITS VARIANTS

Let E/K be an elliptic curve defined over a number field, and let $R\in E(K)$. The p-divisibility of the reductions of the point R can be studied by investigating the $\bmod p$ torsion-Kummer representation. Recall that $\frac{1}{p}R$ is the set of points in $E(\overline{K})$ whose p-multiple equals R and consider the Galois group of the extension $K(\frac{1}{p}R)/K$. Then the set of primes $\mathfrak{p}$ of K such that $(R \bmod \mathfrak{p})$ is p-divisible admits a natural density, which is the proportion of certain automorphisms in the above Galois group. The same holds if we replace p by any positive integer n, and we call $\operatorname{dens}(n)$ this density. For an introduction to this framework, we refer to [2].

Remark 22. There are open image theorems for the torsion-Kummer representations of non-CM elliptic curves, or for CM elliptic curves whose complex multiplication is defined over K (combining [11, Théorème 3] and [3, Theorem 1] as explained in [2]). In particular, for all sufficiently large p and q the extensions $K\left(\frac{1}{p}R\right)$ and $K\left(\frac{1}{q}R\right)$ are linearly disjoint over K. If the complex multiplication is not defined over K, those fields are linearly disjoint over the CM field.

Proof of Theorem 3. The first assertion is proven in Lemma 15, so consider the second assertion. If the $\mathrm{mod} pq$ torsion-Kummer representation is the product of the $\mathrm{mod} p$ and the $\mathrm{mod} q$ torsion-Kummer representations we have

$$\mathrm{dens}(pq) = \mathrm{dens}(p) \cdot \mathrm{dens}(q)\,.$$

This formula implies that Question 2 has a positive answer. Indeed, by the Inclusion-exclusion principle, the density of the set of primes $\mathfrak{p}$ of K such that $(R \bmod \mathfrak{p})$ is neither p-divisible nor q-divisible is

$$(1 - \mathrm{dens}(p))(1 - \mathrm{dens}(q))$$

which can only be 0 if $\mathrm{dens}(p) = 1$ or $\mathrm{dens}(q) = 1$. By the open image theorems on the torsion-Kummer representations (see Remark 22) we are left to deal with the case where E has complex multiplication that is not defined over K. Calling F the CM field and reasoning over FK (applying a known case and Theorem 1) we deduce that there is some point R' over the CM field such that $[p]R' = R$ or $[q]R' = R$. This cannot happen if p and q are sufficiently large: by the maximality of the torsion-Kummer extensions over FK, any extension of K containing a point whose p-multiple (respectively, q-multiple) is R has degree that is a multiple of p (respectively, q) so such an extension is not contained in FK. □

Question 23. Let $I = \{1, \dots, n\}$ for some $n \geq 2$ and let p_i for $i \in I$ be distinct prime numbers. Suppose that for almost all primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ is p_i-divisible for some $i \in I$. Does there exists $i_0 \in I$ such that $(R \bmod \mathfrak{p})$ is p_{i_0}-divisible for almost all primes $\mathfrak{p}$ of K?

Remark 24. Consider Question 23, denoting by P the product of the $p_i's$. In the same spirit of Theorem 3 (with a completely analogue proof), if the $\mathrm{mod} P$ torsion-Kummer representation is the product of the $\mathrm{mod} p_i$ torsion-Kummer representations for $i = 1, \dots, n$, then Question 23 has a positive answer.

Remark 25. In Question 23, partition the set I into I' and I'' and call P' (respectively P'') the product of the primes p_i for $i \in I'$ (respectively, I''). Suppose that the $\mathrm{mod} P$ torsion-Kummer representation is the product of the $\mathrm{mod} P'$ and the $\mathrm{mod} P''$ torsion-Kummer representations. Then for Question 23 (with a straight-forward proof variant with respect to Theorem 3) we can say that for almost all primes $\mathfrak{p}$ of K there is some $i \in I'$ such that $(R \bmod \mathfrak{p})$ is p_i-divisible or for almost all primes $\mathfrak{p}$ of K there is some $i \in I''$ such that $(R \bmod \mathfrak{p})$ is p_i-divisible.

Example 26. We now construct a counterexample to Question 23 for any $n \geq 2$. Let p_1 be an odd prime and for every $i \in I$ with $i > 1$ choose a prime p_i such that $p_i \equiv 1 \bmod p_h$ for every $h \in I$ with $h < i$. For every $i, j \in I$ with we then denote by λ_{ij} an element of $\mathbb{F}_{p_j}^{\times}$ that has order p_i. We define elements $A_1, \dots, A_n$ as follows:

$A_i \bmod p_j = (I, 0)$ if $j < i$; $A_i \bmod p_i = \left(I, \begin{pmatrix}1\\0\end{pmatrix}\right)$; $A_i \bmod p_j = (\lambda_{ij} I, 0)$ if $j > i$.

The elements A_i's have order p_i and are not p_i-divisible. So we only have to prove that every element in the group $\langle A_1, \dots, A_n\rangle$ is p_j-divisible for some $j \in I$. Consider a word W in the letters $A_1, \dots, A_n$. The word $W \bmod p_1$ is a word only in $A_1 \bmod p_1$ so it is p_1-divisible if the exponent of A_1 in W is divisible by p_1. In the remaining case, for $j > 1$ we have

$\pi(W \bmod p_j)$ is a scalar matrix that is not the identity (as its order is a multiple of p_1) hence $\pi(W \bmod p_j) - I$ has rank 2 and we deduce that W is p_j-divisible.

Example 27. We now construct a counterexample to Question 23 for primes p_1, p_2, p_3 even with the stronger assumption that for almost all primes $\mathfrak{p}$ the point $(R \bmod \mathfrak{p})$ is p_i-divisible and p_j-divisible for some $i, j \in \{1, 2, 3\}$ with $i \neq j$. We suppose that $p_2 \equiv 1 \bmod p_1$ and $p_3 \equiv 1 \bmod p_1 p_2$. We consider the group $\Gamma = \langle A, B, C\rangle$ where we set

$$A = (I, v) \times (N, 0) \times (\lambda_{p_1} I, 0)$$
$$B = (I, 0) \times (T, u) \times (\lambda_{p_2} I, 0)$$
$$C = (I, 0) \times (I, 0) \times (I, w)\,.$$

The vectors v, w are non-zero, the scalar λ_{p_i} has order p_i in $\mathbb{F}_{p_3}^\times$, and $(N, 0)$ and (T, u) are as in Theorem 17 in the case Ω' minimal with $\lambda_1, \lambda_2 \neq 1$. The element A is not p_1-divisible, the element B is not p_2-divisible, and C is not p_3-divisible. Consider a word $W = W(A, B, C)$. If the exponent of A is not a multiple of p_1, then W is p_2-divisible and p_3-divisible; if the exponent of A is a multiple of p_1 then W is p_1-divisible. If the exponent of B is not a multiple of p_2, then W is p_3-divisible and otherwise W is p_2-divisible (this is because, by the proof of Theorem 17, each word in $\pi(A_{p_2})$ and $\pi(B_{p_2})$ is a power of $\pi(A_{p_2})$ times a power of $\pi(B_{p_2})$ and the group $\langle A_{p_2}, B_{p_2}\rangle$ does not contain any element of the form (I, z) with $z \neq 0$).

Example 28. To see that the admissible groups correspond to counterexamples to Question 2 there is a general strategy: suppose that E/K and $R \in E(K)$ are such that the $\bmod pq$ torsion-Kummer representation is surjective. Then with an appropriate field extension we obtain that any admissible group modulo $\bmod pq$ is the image of the $\bmod pq$ torsion-Kummer representation.

Example 29. For a Serre curve Question 2 has an affirmative answer for all primes $p < q$ such that $pq \neq 6$ by Proposition 14 as the $\bmod q$ torsion representation is surjective. Indeed, if $p < q$ and $q > 3$, as soon as the image of the $\bmod q$ torsion representation contains $\mathrm{SL}_2(\mathbb{F}_q)$, Question 2 has an affirmative answer.

Example 30. Let $E/\mathbb{Q}$ be $y^2 = x^3 - 9x - 12$ (LMFDB label 7776.m1 [12]) and consider the point $R = (4, 4)$. For $pq = 6$, Question 2 has a negative answer. Indeed, with [4] we have computed the following: the image of $\bmod 2$ and of the $\bmod 3$ torsion-Kummer representations are surjective; the field $\mathbb{Q}(\frac{1}{2}R)$ is contained in $\mathbb{Q}(E[3])$; the image of the $\bmod 6$ torsion-Kummer representation has index 24 in $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}) \ltimes (\mathbb{Z}/6\mathbb{Z})^2$; $\mathrm{Gal}(\mathbb{Q}(\frac{1}{6}R)/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_3) \ltimes \mathbb{F}_3^2$ and it is (up to conjugation) the admissible subgroup of size 432 of Section 4.

We conclude by proving Theorem 5, which settles the analogue of Question 2 in the setting of number fields.

Proof of Theorem 5. We exclude the finitely many primes $\mathfrak{p}$ for which $(\alpha \bmod \mathfrak{p})$ is not well-defined or it is zero, or which lie above the primes ℓ_i's. We suppose that for no $i \in I$ we have $\alpha \in K^{\times \ell_i}$. Call $F_i := K(\zeta_{\ell_j} : j \in I, j \neq i)$. By Schinzel's theorem on abelian radical extensions [10, Theorem 2] we can have $\sqrt[\ell_i]{\alpha} \in F_i$ (for some choice of the root) only if $\zeta_{\ell_i} \in K$.

Suppose that for some $i \in I$ we have $\sqrt[\ell_i]{\alpha} \in F_i$ and consider a prime $\mathfrak{p}$. If $(\alpha \bmod \mathfrak{p})$ is not an ℓ_j-th power for all $j \neq i$ then $\mathfrak{p}$ splits completely in F_i and hence $(\alpha \bmod \mathfrak{p})$ is a ℓ_i-th power.

Now consider the remaining case. By coprimality of the degrees $\sqrt[\ell_i]{\alpha}$ is also not contained in $F = K(\zeta_{\ell_j} : j \in I)$, and that this property holds for every $i \in I$.

As the extensions $F(\sqrt[\ell_i]{\alpha_i})/F$ are not trivial and have pairwise coprime degrees, we may find a Galois automorphism σ of their compositum that is the identity on F and does not fix any $\sqrt[\ell_i]{\alpha_i}$. The primes $\mathfrak{p}$ (which are a positive density) such that the conjugacy class of σ is the conjugacy class of the Frobenius at $\mathfrak{p}$ (they are unramified in $F(\sqrt[\ell_i]{\alpha_i})/F$ for every $i \in I$ by [8, Lemma C.1.7]) are such that $(\alpha \bmod \mathfrak{p})$ is not an ℓ_i-th power for any $i \in I$ hence the assumption does not hold. □

Acknowledgements

We thank Pierre Parent for an interesting mathematical discussion related to this problem, Mike Daas for suggesting the analogue question for number fields (and the counterexample -3), Leolin Nkuete for support with the computations for Example 30, and the student Irma Skrijelj for presenting the divisibility of matrices as a student project. This research was funded in whole, or in part, by the Luxembourg National Research Fund (FNR), grant reference PRIDE23/18685085. For the purpose of open access, and in fulfilment of the obligations arising from the grant agreement,the author has applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

References

[1] J. Alessandrì and L. Paladino. *On the Hasse principle for divisibility in elliptic curves*. 2025. arXiv: `2511.02078`.

[2] A. Benoist and A. Perucca. *Two naturals variants of the Lang-Trotter conjecture on primitive points for elliptic curves*. `https://hdl.handle.net/10993/64259`. 2025.

[3] D. Bertrand. "Galois representations and transcendental numbers". In: (1988). in: A. Baker (Ed.), New Advances in Transcendence Theory (Durham 1986), pp. 37–55.

[4] W. Bosma, J. Cannon and C. Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.

[5] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.3)*. Version 10.3. 2024. URL: `https://www.sagemath.org`.

[6] R. Dvornicich and L. Paladino. "Local-global questions for divisibility in commutative algebraic groups". In: *Eur. J. Math.* 8.2 (2022), S599–S628.

[7] R. Dvornicich and U. Zannier. "Local-global divisibility of rational points in some commutative algebraic groups". In: *Bull. Soc. Math. France* 129.3 (2001), pp. 317–338.

[8] M. Hindry and J. H. Silverman. *Diophantine geometry: an introduction*. Springer-Verlag, 2000.

[9] F. Pappalardi N. Jones and P. Stevenhagen. *Locally imprimitive points on elliptic curves*. 2023. arXiv: `2304.03964`.

[10] A. Schinzel. "Abelian binomials, power residues and exponential congruences". In: *Acta Arith.* 32 (1977), pp. 245–274.

[11] J.-P. Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques". In: *Invent. Math.* (1972), pp. 259–331.

[12] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. `https://www.lmfdb.org`. accessed in 2025.