THE DISTRIBUTION AND GROWTH OF THE ELEMENTARY DIVISORS OF THE REDUCTIONS OF AN ELLIPTIC CURVE OVER A FUNCTION FIELD

ALINA-CARMEN COJOCARU AND ÁRPÁD TÓTH

ABSTRACT. Let K be a global field of characteristic $p \geq 5$ and let E/K be a non-isotrivial elliptic curve. For places v of K of good reduction for E, let E_v/k_v be the reduction of E modulo v. Then $E_v(k_v) \simeq \mathbb{Z}/d_v\mathbb{Z} \times \mathbb{Z}/d_v e_v\mathbb{Z}$ for positive integers d_v, e_v, uniquely determined by E and v. We study the distribution of d_v and the growth of $d_v e_v$ as v varies over places of degree n and $n \to \infty$.

1. INTRODUCTION

Let K be a global field of characteristic $p \geq 5$ and genus g_K, and let $\mathbb{F}_q \subset K$ be the algebraic closure of $\mathbb{F}_p$ in K. We denote by V_K the set of places of K; for $v \in V_K$, we denote by k_v the residue field of K at v, and by $\deg v := [k_v : \mathbb{F}_q]$ the degree of v.

Let E/K be an elliptic curve over K with j-invariant $j_E \notin \mathbb{F}_q$, which we shall standardly call **non-isotrivial**. We denote by $V_{E/K}$ the set of places of K for which the reduction E_v/k_v is smooth, and by $\left|\overline{V}_{E/K}\right| := \sum_{v \notin V_{E/K}} \deg v$. From the theory of elliptic curves we know that $E_v(k_v) \simeq \mathbb{Z}/d_v\mathbb{Z} \times \mathbb{Z}/d_v e_v\mathbb{Z}$ for nonzero integers d_v, e_v, uniquely determined by E and v. We call the integers d_v and $d_v e_v$ the **elementary divisors** of E_v. Clearly, the product $d_v e_v$ is the **exponent** of the group $E_v(k_v)$ (that is, $d_v e_v$ is the smallest $m \in \mathbb{N}\backslash\{0\}$ such that $mP = \mathcal{O}$ for all $P \in E_v(k_v)$).

The purpose of this series of papers is to study questions about the distribution of the places $v \in V_{E/K}$ for which $E_v(k_v)$ is a cyclic group. Such questions have been vastly investigated for the reductions of an elliptic curve defined over $\mathbb{Q}$ (e.g. in [BaSh], [Co1], [Co2], [CoMu], [GuMu], [Mu1], [Mu2], [Se]), mainly in relation with the elliptic curve analogue of Artin's primitive root conjecture formulated by Lang and Trotter in [LaTr]. This latter conjecture was investigated in the function field setting E/K by Clark and Kuwata [ClKu], and by Hall and Voloch [HaVo] (see also Voloch's work on constant curves [Vo1], [Vo2]). In [ClKu], a particular emphasis was placed on the study of the cyclicity of $E_v(k_v)$. Unfortunately, the arguments given in their paper are incomplete and also contain some errors, as we will point out in Remark 16 of Section 4.

In this paper we obtain an explicit asymptotic formula for the number of places $v \in V_{E/K}$, of fixed degree, for which $E_v(k_v)$ is cyclic, or, more generally, for which d_v is fixed. Our result not only sharpens the one in

A.C. Cojocaru's work on this material was partially supported by the National Science Foundation under agreements No. DMS-0747724 and No. DMS-0635607. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. Á. Tóth's work on this material was supported by OTKA grant K72731.

[ClKu], but also has it as a direct consequence. Additionally, we determine the growth of the exponent of $E_v(k_v)$ and prove a result similar to its rational counterpart obtained by Duke in [Du]. More precisely, we show:

Theorem 1. *Let K be a global function field of characteristic $p \geq 5$ and let $\mathbb{F}_q \subset K$ be the algebraic closure of $\mathbb{F}_p$ in K. Let E/K be a non-isotrivial elliptic curve. Let $d \in \mathbb{N}$, $(d,p)=1$. Then the following statements hold.*

1. *Let $n \in \mathbb{N}\backslash\{0\}$ and let*

$$V_{E/K}(n) := \{v \in V_{E/K} : \deg v = n\}.$$

Assume that $d|q^n-1$ and $d \leq q^{\frac{n}{2}}+1$. Then, $\forall\ \varepsilon > 0\ \exists c(K,E,\varepsilon) > 0$ such that

$$\left| \#\{v \in V_{E/K}(n) : d_v = d\} - \delta(E/K,d,n)\frac{q^n}{n} \right| \leq c(K,E,\varepsilon)\frac{q^{n\left(\frac{1}{2}+\varepsilon\right)}}{n},$$

where

$$\delta(E/K,d,n) := \sum_{\substack{m\geq 1 \\ (m,p)=1 \\ dm|q^n-1}} \frac{\mu(m)\,\mathrm{ord}_{dm}(q)}{[K(E[dm]):K]}, \tag{1}$$

$\mu(m)$ is the Möbius function of m, $K(E[dm])$ is the division field of E of level dm, and $\mathrm{ord}_{dm}(q)$ is the multiplicative order of q modulo dm.

2. *The Dirichlet density of the set $\{v \in V_{E/K} : d_v = d\}$ exists and equals*

$$\delta(E/K,d) := \sum_{\substack{m\geq 1 \\ (m,p)=1}} \frac{\mu(m)}{[K(E[dm]):K]}.$$

3. *Let $f : [5,\infty) \longrightarrow (0,\infty)$ be such that $f(n) \leq q^{\frac{n}{2}}+1\ \forall n$ and $\lim_{n\to\infty} f(n) = \infty$. Then $\exists c(K,E) > 0$ and $\forall \varepsilon > 0\ \exists c(K,E,\varepsilon)$ such that*

$$\left| \#\left\{ v \in V_{E/K}(n) : d_v e_v > \frac{q^n}{f(n)} \right\} - \frac{q^n}{n} \right| \leq c(K,E)\frac{q^n}{nf(n)^2} + c(K,E,\varepsilon)\frac{q^{n\left(\frac{1}{2}+\varepsilon\right)}}{n}.$$

4. *Let $f : [5,\infty) \longrightarrow (0,\infty)$ be such that $f(n) \leq q^{\frac{n}{2}}+1\ \forall n$ and $\lim_{n\to\infty} f(n) = \infty$. Then the Dirichlet density of the set $\left\{ v \in V_{E/K} : d_v e_v > \frac{q^{\deg v}}{f(\deg v)} \right\}$ exists and equals 1.*

The proofs of the above may be summarized as an application of the following emerging Chebotarev type result:

Theorem 2. *Let K be a global function field of characteristic $p \geq 5$ and let $\mathbb{F}_q \subset K$ be the algebraic closure of $\mathbb{F}_p$ in K. Let E/K be a non-isotrivial elliptic curve.*

Let $n \in \mathbb{N}\backslash\{0\}$. Then $\forall \varepsilon > 0\ \exists c(K,E,\varepsilon)$ such that

$$\left| \sum_{\substack{m\geq 1 \\ (m,p)=1 \\ m|q^n-1}} \#\{v \in V_{E/K}(n) : v \text{ splits completely in } K(E[m])/K\} - \delta^{split}(E/K,n)\frac{q^n}{n} \right| \leq c(K,E,\varepsilon)\frac{q^{n\left(\frac{1}{2}+\varepsilon\right)}}{n},$$

where

$$\delta^{split}(E/K,n) := \sum_{\substack{m\geq 1\\(m,p)=1\\m|q^n-1}} \frac{\mathrm{ord}_m(q)}{[K(E[m]):K]}.$$

Overall, these theorems exemplify, once again, the stimulating parallel between number fields and function fields. However, in some ways, the situation over K versus that over $\mathbb{Q}$ is much easier. For once, the results are unconditional (thanks to Weil's Riemann Hypothesis [We]). Moreover, the proofs of parts 1 and 3 of Theorem 1 (essentially, of part 1 of Theorem 2) are direct applications of the effective version of the Chebotarev density theorem, which is a particular feature of E/K and does not happen for $E/\mathbb{Q}$ (or even for rank 2 Drinfeld modules [CoSh]). This special feature is a consequence of the properties of the division fields of E/K, reviewed in detail in Section 2. The divergent difficulty when investigating E/K versus $E/\mathbb{Q}$ occurs in the study of the positivity of the densities $\delta(E/K,d)$, on which we will comment in Section 4. More remarks regarding the comparison between the two situations are also included in Section 4. Finally, our restriction on characteristic $p \geq 5$ is for simplification of the presentation of the proofs, as we will point out in Remark 5.

Notation. In what follows, p and q are fixed, and $\mathbb{F}_p, \mathbb{F}_q, K, E/K$ are as above. We denote by $\overline{\mathbb{F}}_q$ an algebraic closure of $\mathbb{F}_q$, by ℓ a rational prime, and by d,k,m,n positive integers. We denote by $\mathrm{ord}_m(q)$ the multiplicative order of $q (\mathrm{mod}\, m)$. For positive integers m_1, m_2, we denote by (m_1,m_2) their greatest common divisor, and by $[m_1,m_2]$ their least common multiple. We denote by $\tau(k)$ the divisor function and by $\phi(k)$ the Euler function of k. In other words,

$$\tau(k) := \#\{1 \leq k' \leq k : k'|k\} = \prod_{\ell^j || m} (j+1)\,,$$

$$\phi(k) := \#\{1 \leq k' \leq k : (k,k') = 1\} = k \prod_{\ell | k} \left(1 - \frac{1}{\ell}\right).$$

We also define

$$\psi(k) := k \prod_{\ell | k} \left(1 + \frac{1}{\ell}\right).$$

We recall that $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$ denotes the general linear group, $\mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z})$ the special linear group, and $\#\,\mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z}) = k\phi(k)\psi(k)$. For two functions $f, g : D \longrightarrow \mathbb{R}$, with $D \subseteq \mathbb{C}$ and g positive, we write $f(x) = \mathrm{O}(g(x))$ or $f(x) \ll g(x)$ if there is a positive constant c such that $|f(x)| \leq cg(x)$ for all $x \in D$. If c depends on another specified constant d, we write $f(x) = \mathrm{O}_d(g(x))$ or $f(x) \ll_d g(x)$. We write $f(x) \sim g(x)$ if $\lim\limits_{x\to\infty} \dfrac{f(x)}{g(x)} = 1$.

2. Preliminaries

2.1. **Division fields of E/K.** Let K and E/K be as in Section 1. Let $\overline{K}$ be an algebraic closure of K and $K^s \subseteq \overline{K}$ the separable closure of K. Let m denote positive integers and ℓ rational primes which are invertible in K, i.e. $(m,p) = (\ell,p) = 1$. We write $E[m]$ for the group of m-division points of E and $K(E[m])$

for the m-division field of E. We denote by $\mathbb{F}_{q^{c_m}}$ the algebraic closure of $\mathbb{F}_q$ in $K(E[m])$. In this section, we present the main properties of $K(E[m])$ needed in our proof of Theorem 1. For proofs of these properties and further references, we direct the reader to [Ig], [BaLoVi] and [Si].

We recall that the group $E[m] = E(\overline{K})[m]$ is contained in $E(K^s)[m]$ and is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Moreover, it is equipped with a natural continuous action of $\mathrm{Gal}(K^s/K)$, which gives rise to a continuous Galois representation $\bar{\rho}_{E,m} : \mathrm{Gal}(K^s/K) \longrightarrow \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, or, implicitly, to an injective representation

$$\bar{\rho}_{E,m} : \mathrm{Gal}(K(E[m])/K) \hookrightarrow \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}). \tag{2}$$

The representations $\bar{\rho}_{E,m}$ form a compatible system and, put together, give rise to an absolute Galois representation $\rho_E : \mathrm{Gal}(K^s/K) \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}_{(p)})$, where $\hat{\mathbb{Z}}_{(p)} := \prod_{\ell \neq p} \mathbb{Z}_\ell$ is the prime-to-p profinite completion of $\mathbb{Z}$. Futhermore, the composition of $\bar{\rho}_{E,m}$ with the determinant map $\det : \mathrm{Aut}(E[m]) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$ gives rise to a group homomorphism $\mathrm{Gal}(K^s/K) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$ associated to E and m.

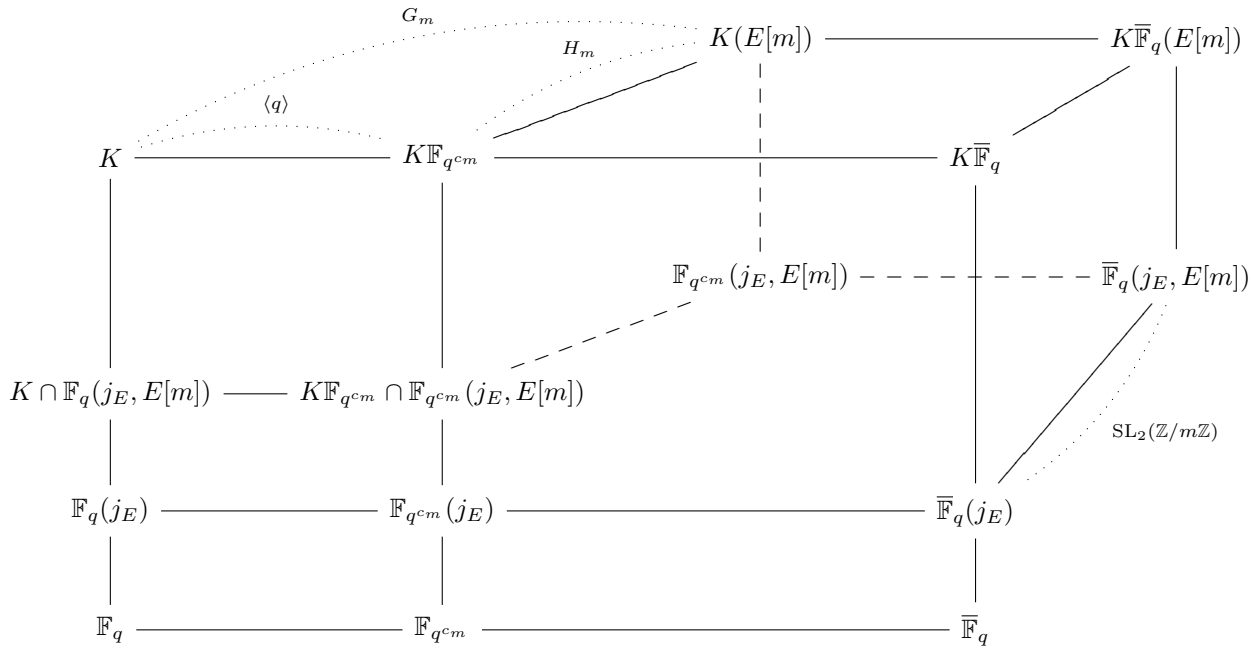
We denote by $\langle q \rangle = \langle q (\mathrm{mod}\, m) \rangle \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ the cyclic group generated by $q (\mathrm{mod}\, m)$, and by ζ_m an m-th root of unity in K^s. Then $\langle q \rangle \simeq \mathrm{Gal}(\mathbb{F}_q(\zeta_m)/\mathbb{F}_q)$, and $|\langle q \rangle|$ equals $\mathrm{ord}_m(q)$ and is thus a divisor of $\phi(m)$.

Finally, we denote by Γ_m the (unique) subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ defined via the short exact sequence $1 \longrightarrow \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \longrightarrow \Gamma_m \longrightarrow \langle q \rangle \longrightarrow 1$, i.e. $\Gamma_m = \det^{-1}(\langle q \rangle) \subseteq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. By passing to the inverse limit over all integers m with $(m, p) = 1$, the groups Γ_m give rise to an exact sequence of profinite groups $1 \longrightarrow \mathrm{SL}_2(\hat{\mathbb{Z}}_{(p)}) \longrightarrow \hat{\Gamma} \longrightarrow \hat{\langle q \rangle} \longrightarrow 1$, where $\hat{\Gamma}$ is closed in $\mathrm{GL}_2\left(\hat{\mathbb{Z}}_{(p)}\right)$ and $\hat{\langle q \rangle}$ is the subgroup of $\hat{\mathbb{Z}}^*_{(p)}$ topologically generated by the q-th power Frobenius.

In summary, if we let $G_m := \mathrm{Gal}(K(E[m])/K)$, then, at level m, we obtain the following commutative diagram, with exact rows and injective vertical arrows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & H_m & \longrightarrow & G_m & \xrightarrow{\det} & \det G_m & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \bar{\rho}_{E,m}} & & \| & & \\
1 & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) & \longrightarrow & \Gamma_m & \xrightarrow{\det} & \langle q \rangle & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) & \xrightarrow{\det} & (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & 1.
\end{array}$$

We also obtain the following diagram of fields (and some of their Galois groups):



In what follows we record some of the properties of the fields occurring in this diagram.

Proposition 3.

1. *$K(E[m])$ contains the cyclotomic field $K(\zeta_m) = K\mathbb{F}_{q^{c_m}}$; in particular,*
   (a) *$c_m = |\langle q \rangle| = \mathrm{ord}_m(q)$;*
   (b) *$c_m = 1$ if and only if $m | q-1$;*
   (c) *$\mathrm{ord}_m(q) \Big| [K(E[m]) : K]$;*
2. *If $v \in V_K$ splits completely in $K(E[m])/K$, then $m | q^{\deg v} - 1$.*

Proof. The first assertion of part 1 can be found in [Ig, p.459]; parts (a), (b), (c) are then immediate consequences. Part 2 is deduced from part 1, combined with the properties of $K(\zeta_m)$ (as in [Ro, Prop.10.2, p.151]). □

Theorem 4. *(Igusa)*

1. *$K(E[m])/K$ is unramifed at each place $v \in V_{E/K}$.*
2. *$K(E[m])/K$ is at most tamely ramified at all places away from $V_{E/K}$.*

Proof. The theorem is derived from [Ig, Thm.6, p.472]. □

Remark 5. It is part 2 of the above theorem that requires that the characteristic of K be ≥ 5. For characteristic $2, 3$, other precise ramifications statements are proven in [Ig]. In order to illustrate the proof of our main result as a clean application of the Chebotarev density theorem (Theorem 11 in what follows), we are focusing solely on $p \geq 5$. The other cases are left to the interested reader.

Theorem 6. *(Igusa)*

1. *For all but finitely many primes ℓ,*

$$K \cap \mathbb{F}_q(j_E, E[\ell]) = \mathbb{F}_q(j_E).$$

More precisely, there exists an explicit constant $c(K)$, depending at most on the genus of K, such that, for every prime $\ell \geq c(K)$,

$$\mathrm{Gal}(K(E[\ell])/K\mathbb{F}_{q^{c_\ell}}) \simeq \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

that is,

$$\mathrm{Gal}(K(E[\ell])/K) \simeq \Gamma_\ell.$$

2. *The profinite group $\rho_E(\mathrm{Gal}(K^s/K))$ is open in $\hat{\Gamma}$.*

Proof. Part 1 is the refinement of [Ig, Thm.4, p.470] proved in [CoHa, Thm.1.1, p.3066]. Part 2 is the reformulation of part 1 as in [BaLoVi, Thm.1.3, p.179]. □

Yet another reformulation of (part 2 of) Theorem 6 is that $\rho_E(\mathrm{Gal}(K^s/K))$ has finite index in $\hat{\Gamma}$. Thus there exists a positive integer m such that

$$\rho_E(\mathrm{Gal}(K^s/K)) = \pi^{-1}(\bar{\rho}_{E,m}(\mathrm{Gal}(K(E[m])/K))), \tag{3}$$

where the map π in

$$\begin{array}{ccc} \mathrm{Gal}(K^s/K) & \xrightarrow{\rho_E} & \hat{\Gamma} \\ & \searrow^{\bar{\rho}_{E,m}} & \downarrow \pi \\ & & \Gamma_m \end{array}$$

is the natural projection. Inspired by [Jo], we introduce:

Definition 7. *Let K be a global function field of characteristic $p \geq 5$ and let E/K be a non-isotrivial elliptic curve over K. We define the* **torsion conductor** *m_E of E to be the smallest positive integer m so that (3) holds.*

We now infer the following corollary to Theorem 6:

Corollary 8. *Let m_1, m_2 be positive integers such that $(m_1, p) = (m_2, p) = (m_2, m_E) = 1$ and m_1 is composed of primes dividing m_E. Then*

1. $K(E[m_1]) \cap K(E[m_2]) = K\mathbb{F}_{q^{(c_{m_1}, c_{m_2})}}$;

2. $K\mathbb{F}_{q^{c_{m_2}}} \cap \mathbb{F}_{q^{c_{m_2}}}(j_E, E[m_2]) = \mathbb{F}_{q^{c_{m_2}}}(j_E)$; *equivalently,*

$$\mathrm{Gal}(K(E[m_2])/K\mathbb{F}_{q^{c_{m_2}}}) \simeq \mathrm{SL}_2(\mathbb{Z}/m_2\mathbb{Z}), \quad \textit{that is,}\ \mathrm{Gal}(K(E[m_2])/K) \simeq \Gamma_{m_2}.$$

2.2. **Reductions of E/K.** Let K be as in Section 1. Let E/K be an elliptic curve over K (not necessarily non-isotrivial). We let v denote places in $V_{E/K}$ and keep all the other related notation introduced in the previous sections.

We recall that $E_v[p]$ is always a cyclic group, while $E_v[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ for all rational primes $\ell \neq p$. We also recall the following standard facts about E_v. If we write $\#E_v(k_v) = q^{\deg v} + 1 - a_v$ for some integer a_v, then we have the Hasse bound $|a_v| \leq 2q^{\frac{\deg v}{2}}$. Let π_v, $\bar{\pi}_v$ be defined by $X^2 - a_v X + q^{\deg v} = (X - \pi_v)(X - \bar{\pi}_v)$. We identify π_v with the $q^{\deg v}$-power Frobenius endomorphism on $E_v(k_v)$ and consider the subring $R := \mathbb{Z}[\pi_v]$ of the endomorphism ring $\mathrm{End}_{k_v}(E_v)$. Following [DuTo], if $R = \mathbb{Z}$, we define $\Delta_v := 1$ and $b_v := 0$; otherwise, R is an imaginary quadratic order in $\mathbb{Q}(\pi_v)$, whose discriminant we denote by Δ_v and conductor by b_v; we obtain the relation

$$a_v^2 - 4q^{\deg v} = b_v^2 \Delta_v.$$

As explained in [DuTo], the integers a_v, b_v, Δ_v completely characterize the class of the Frobenius at v in the division fields of E/K. More precisely:

Theorem 9. *Let K be a global function field of characteristic $p \geq 5$. Let E/K be an elliptic curve over K. Let $m \in \mathbb{N}$, $(m, p) = 1$, and let $v \in V_{E/K}$. Let $\delta_v := 0, 1$ according to whether $\Delta_v \equiv 0, 1 (\mathrm{mod}\, 4)$. Then the reduction modulo m of the integral matrix*

$$\sigma_v := \begin{pmatrix} \frac{a_v + b_v\delta_v}{2} & b_v \\ \frac{b_v(\Delta_v - \delta_v)}{4} & \frac{a_v - b_v\delta_v}{2} \end{pmatrix}$$

represents the $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$-conjugacy class of the Frobenius at v in $K(E[m])/K$. Moreover,

$$d_v = \left(b_v, \frac{a_v + b_v\delta_v - 2}{2}\right), \quad e_v = \frac{q^{\deg v} + 1 - a_v}{d_v^2}.$$

Proof. This follows from obvious modifications of the proof of [DuTo, Thm.2.1], see especially page 558. □

As an immediate application of this theorem, we have:

Corollary 10. *Let K be a global function field of characteristic $p \geq 5$. Let E/K be an elliptic curve over K. Let $m, d \in \mathbb{N}$, $(m, p) = (d, p) = 1$, and let $v \in V_{E/K}$. Then:*

1. *$E_v(k_v) \supseteq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ if and only if v splits completely in $K(E[m])/K$;*
2. *$d_v = d$ if and only if v splits completely in $K(E[d])/K$ and does not split completely in $K(E[d\ell])/K$ for any rational prime $\ell \nmid p$.*

2.3. **The Chebotarev density theorem.** The main result of our paper is essentially an application of the Chebotarev density theorem over function fields, which we recall below.

Theorem 11. *Let F/L be a finite, tamely ramified, Galois extension of global function fields, with constant field $\mathbb{F}_q$, and unramified away from a set of places S. Let g_L denote the genus of L. Let $\mathbb{F}_{q^c}$ be the algebraic closure of $\mathbb{F}_q$ in F. Let $n \in \mathbb{N}\backslash\{0\}$ and let $V_L(n)$ denote the places of L, unramified in F and of degree n. Let*

$$\pi_1(n, F/L) := \#\{v \in V_L(n) : \ v \text{ splits completely in } F/L\}.$$

If $c|n$, then

$$\left|\pi_1(n, F/L) - c\frac{1}{[F:L]}\#V_L(n)\right| \leq 2\left((3g_L + |S|)\frac{q^{\frac{n}{2}}}{n} + \frac{|S|}{2n}\right) + |S|,$$

where $|S| := \sum_{v\in S} \deg v$. Otherwise, $\pi_1(n, F/L) = 0$.

Proof. This is [MuSc, Thm.2, p.525]. □

As an immediate application, we have:

Proposition 12. *Let K be a global function field of characteristic $p \geq 5$ and let $\mathbb{F}_q \subset K$ be the algebraic closure of $\mathbb{F}_p$ in K. Let E/K be a non-isotrivial elliptic curve over K. Let $m, n \in \mathbb{N}\backslash\{0\}$, with $(m, p) = 1$ and $c_m|n$. Then*

$$\begin{aligned} &\left|\pi_1(n, K(E[m])/K) - c_m\frac{1}{[K(E[m]) : K]} \cdot \frac{q^n}{n}\right| \\ \leq \ & 2\left((3g_K + |\overline{V}_{E/K}|)\frac{q^{\frac{n}{2}}}{n} + \frac{|\overline{V}_{E/K}|}{2n}\right) + |\overline{V}_{E/K}|. \end{aligned}$$

Proof. We apply Theorems 4 and 11 to the extension $K(E[m])/K$. □

3. Proof of Theorems 1 and 2

As will be clear below, we may solely focus on Theorem 1.

1. Using part 2 of Corollary 10, together with the inclusion-exclusion principle, we obtain

$$\#\{v \in V_{E/K}(n) : d_v = d\} = \sum_m \mu(m)\pi_1(n, K(E[dm])/K), \tag{4}$$

where all integers m above (and throughout the proof) are positive, squarefree and satisfy $(m, p) = 1$. Moreover, their range is very restricted. Indeed, for such m, we are counting places $v \in V_{E/K}(n)$ which split completely in $K(E[dm])$. On one hand, by part 1 of Corollary 10, we deduce that $d^2m^2|q^n + 1 - a_v$; hence, by the Hasse bound, $dm \leq q^{\frac{n}{2}} + 1$. On the other hand, by part 2 of Proposition 3, $dm|q^n - 1$. Thus we obtain the justification of our hypothesis on d (made in the statement of Theorem 1), as well as a simplification of equation (4):

$$\#\{v \in V_{E/K}(n) : d_v = d\} = \sum_{\substack{dm \leq q^{\frac{n}{2}}+1 \\ dm|q^n-1}} \mu(m)\pi_1(n, K(E[dm])/K). \tag{5}$$

A straightforward application of Proposition 12 (note that $dm|q^n-1$ implies that $c_{dm}|n$) immediately gives

$$\left| \#\{v \in V_{E/K}(n) : d_v = d\} - \sum_{\substack{1 \le m \le \frac{q^{\frac{n}{2}}+1}{d} \\ (m,p)=1 \\ dm \mid q^n-1}} \frac{\mu(m)c_{dm}}{[K(E[dm]):K]} \cdot \frac{q^n}{n} \right| \le c(K,E)\frac{q^{\frac{n}{2}}}{n}\tau\left(q^n-1\right),$$

where $c(K,E)$ is a positive constant depending on g_K and $|\overline{V}_{E/K}|$. Since $\tau\left(q^n-1\right) \ll_\varepsilon q^{n\varepsilon}$ $\forall \varepsilon > 0$ and since, by part 1(a) of Proposition 3 and Corollary 8,

$$\sum_{\substack{dm > q^{\frac{n}{2}}+1 \\ dm \mid q^n-1}} \frac{\mu(m)c_{dm}}{[K(E[dm]):K]} \ll_{K,E,d} q^{-n},$$

the proof of the first part of Theorem 1 is completed.

2. Let us determine the Dirichlet density of the places v for which $d_v = d$, namely

$$\lim_{s \to 1+} \frac{\displaystyle\sum_{\substack{v \in V_{E/K} \\ d_v = d}} q^{-s \deg v}}{\displaystyle\sum_v q^{-s \deg v}}$$

(provided the limit exists). By part 1 of the theorem, the numerator becomes:

$$\begin{aligned} \sum_{\substack{v \in V_{E/K} \\ d_v = d}} q^{-s \deg v} &= \sum_{n \ge 1} q^{-sn} \#\{v \in V_{E/K}(n) : d_v = d\} \\ &= \sum_{n \ge 1} \frac{q^{n(1-s)}}{n} \sum_{dm \mid q^n-1} \frac{\mu(m)c_{dm}}{[K(E[dm]):K]} + \mathrm{O}_{K,E,\varepsilon}\left(\sum_{n \ge 1} \frac{q^{n\left(\frac{1}{2}+\varepsilon-s\right)}}{n} \right). \end{aligned}$$

For the first sum above, using that $dm|q^n-1$ and $c_{dm} = \mathrm{ord}_{dm}(q)$, we write $n = c_{dm}k$ for some $k \ge 1$; thus

$$\begin{aligned} \sum_{n \ge 1} \frac{q^{n(1-s)}}{n} \sum_{dm \mid q^n-1} \frac{\mu(m)c_{dm}}{[K(E[dm]):K]} &= \sum_{m \ge 1} \frac{\mu(m)c_{dm}}{[K(E[dm]):K]} \sum_{k \ge 1} \frac{q^{k \,\mathrm{ord}_{dm}(q)\cdot(1-s)}}{k \,\mathrm{ord}_{dm}(q)} \\ &= -\sum_{m \ge 1} \frac{\mu(m)}{[K(E[dm]):K]} \log\left(1 - q^{\mathrm{ord}_{dm}(q)\cdot(1-s)}\right). \end{aligned}$$

Since

$$\lim_{s \to 1+} \frac{\displaystyle\sum_{n \ge 1} \frac{q^{n\left(\frac{1}{2}+\varepsilon-s\right)}}{n}}{\displaystyle\sum_v q^{-s \deg v}} = \lim_{s \to 1+} \frac{\log\left(1 - q^{\frac{1}{2}+\varepsilon-s}\right)}{\log\left(1-q^{1-s}\right)} = \lim_{x \to 1-} \frac{\log\left(1 - xq^{-\frac{1}{2}+\varepsilon}\right)}{\log(1-x)} = 0,$$

it remains to determine the limit

$$\mathcal{L} := \lim_{s \to 1+} \frac{-\displaystyle\sum_{m \ge 1} \frac{\mu(m)}{[K(E[dm]):K]} \log\left(1 - q^{\mathrm{ord}_{dm}(q)\cdot(1-s)}\right)}{\displaystyle\sum_v q^{-s \deg v}}.$$

We observe that

$$\begin{aligned}\mathcal{L} &= \lim_{s\to 1+}\sum_{m\geq 1}\frac{\mu(m)}{[K(E[dm]):K]}\cdot\frac{\log\left(1-q^{\mathrm{ord}_{dm}(q)(1-s)}\right)}{\log\left(1-q^{1-s}\right)}\\ &= \lim_{x\to 1-}\sum_{m\geq 1}\frac{\mu(m)}{[K(E[dm]):K]}\cdot\frac{\log\left(1-x^{\mathrm{ord}_{dm}(q)}\right)}{\log(1-x)}.\end{aligned}$$

Also, by Corollary 8,

$$\delta(E/K,d):=\sum_{m\geq 1}\frac{\mu(m)}{[K(E[dm]):K]}<\infty \text{ and } \sum_{m\geq 1}\frac{c_{dm}}{[K(E[dm]):K]}<\infty.$$

Therefore

$$\begin{aligned}&\lim_{x\to 1-}\left|\sum_{m\geq 1}\frac{\mu(m)}{[K(E[dm]):K]}\cdot\frac{\log\left(1-x^{\mathrm{ord}_{dm}(q)}\right)}{\log(1-x)}-\delta(E/K,d)\right|\\ =\ &\lim_{x\to 1-}\frac{1}{|\log(1-x)|}\left|\sum_{m\geq 1}\frac{\mu(m)}{[K(E[dm]):K]}\log\frac{1-x^{\mathrm{ord}_{dm}(q)}}{1-x}\right|\\ \leq\ &\lim_{x\to 1-}\frac{1}{|\log(1-x)|}\sum_{m\geq 1}\frac{c_{dm}}{[K(E[dm]):K]}=0.\end{aligned}$$

This implies that $\mathcal{L}=\delta(E/K,d)$, hence the Dirichlet density of the places v with $d_v=d$ exists and equals $\delta(E/K,d)$.

3. Using the Hasse bound, it is enough to prove that

$$\lim_{n\to\infty}\frac{\#\left\{v\in V_{E/K}(n):d_v>f(n)\right\}}{\frac{q^n}{n}}=0.$$

Let us fix $n\in\mathbb{N}\backslash\{0\}$ and observe that, as in the proof of Theorem 1, Corollary 10 implies that

$$\#\left\{v\in V_{E/K}(n):d_v>f(n)\right\}\ \leq\ \sum_{\substack{f(n)<d\leq q^{\frac{n}{2}}+1\\ d\mid q^n-1}}\ \sum_{\substack{v\in V_{E/K}(n)\\ d\mid d_v}}1=\sum_{\substack{f(n)<d\leq q^{\frac{n}{2}}+1\\ d\mid q^n-1}}\pi_1(n,K(E[d])/K),$$

where all the integers d above satisfy $(d,p)=1$. As in the proof of part 1, by Proposition 12, the above is

$$=\sum_{\substack{f(n)<d\leq q^{\frac{n}{2}}+1\\ d\mid q^n-1}}\frac{c_d}{[K(E[d]):K]}\cdot\frac{q^n}{n}+\mathrm{O}_{K,E,\varepsilon}\left(\frac{q^{n\left(\frac{1}{2}+\varepsilon\right)}}{n}\right).$$

Finally, Corollary 8 implies that $\sum_{\substack{f(n)<d\leq q^{\frac{n}{2}}+1\\ d\mid q^n-1}}\frac{c_d}{[K(E[d]):K]}\ll_{K,E} f(n)^{-2}$, which proves part 3.

4. One proceeds as in part 2 and obtains that the Dirichlet density of $v\in V_{E/K}$ for which $d_v>f(\deg v)$ is 0. Thus the Dirichlet density of $v\in V_{E/K}$ for which $d_ve_v>\frac{f\left(q^{\deg v}\right)}{f(\deg v)}$ is 1.

Finally, the proof of Theorem 2 is essentially the same as that of part 1 of Theorem 1 and, as such, is omitted. □

4. Concluding remarks

Remark 13. Unlike the rational case, its function field analogue is simply an application of the effective Chebotarev density theorem and requires no extra sieving. This feature is a consequence of the additional restriction $m|q^n-1$ in our range of m, which does not occur when working with E defined over $\mathbb{Q}$.

Remark 14. The error term in part 1 of Theorem 1 is as good as one might hope it to be. This prompts the question whether the same is true for number fields: given an elliptic curve $E/\mathbb{Q}$ and $d \in \mathbb{N}\backslash\{0\}$, is it true that, as $x \to \infty$,

$$\#\{p \leq x : d_p = d\} = \sum_m \frac{\mu(m)}{[\mathbb{Q}(E[dm]) : \mathbb{Q}]} \operatorname{li} x + \mathrm{O}_{d,E,\varepsilon}\left(x^{\frac{1}{2}+\varepsilon}\right)?$$

Related to this question, we recall that the best error terms obtained so far for $E/\mathbb{Q}$, under GRH, are $\mathrm{O}_{d,E}\left(x^{\frac{5}{6}}(\log x)^{\frac{2}{3}}\right)$ if E does not have complex multiplication (non-CM) and $\mathrm{O}_{d,E}\left(x^{\frac{3}{4}}(\log x)^{\frac{1}{2}}\right)$ if E has complex multiplication (CM). Further improvements can also be obtained under additional hypotheses; see [CoMu, Thm. 1.1, Thm. 1.2] and [Co3, Thm. 2].

Remark 15. The proof of Theorem 1 does not require the full strength of the Riemann Hypothesis for curves over finite fields, but rather *any* quasi-Riemann Hypothesis in this context (and, as explained in [Ro, Ch.5], such a quasi-Riemann Hypothesis is much easier to prove).

Remark 16. In [ClKu], the authors prove the existence of the Dirichlet density $\delta(E/K,1)$ without passing through the analysis of the Dirichlet densities of $\{v \in V_{E/K}(n) : d_v = 1\}$. Unfortunately, their paper is abundant in typos which make the understanding of the proofs hardly possible. Moreover, when applying their general result to the context of E/K, they state (and use) that $\mathrm{ord}_\ell(q)$ "equals $\ell-1$ for almost all ℓ" [ClKu, p.171], which is false.

Remark 17. It is desirable to have a concise criterion for when the density $\delta(E/K,d)$ is positive. For example, when $d=1$, we see that, if there exists a prime $\ell|q-1$ such that $K(E[\ell]) = K$, then $\delta(E/K,1) = 0$. Indeed,

$$\begin{aligned}\delta(E/K,1) &= \sum_{\substack{m\geq 1\\(m,p)=1\\ \ell|m}} \frac{\mu(m)}{[K(E[m]):K]} + \sum_{\substack{m\geq 1\\(m,p)=1\\ \ell\nmid m}} \frac{\mu(m)}{[K(E[m]):K]} \\ &= -\sum_{\substack{m\geq 1\\(m,p)=1\\ \ell\nmid m}} \frac{\mu(m)}{[K(E[\ell m]):K]} + \sum_{\substack{m\geq 1\\(m,p)=1\\ \ell\nmid m}} \frac{\mu(m)}{[K(E[m]):K]} = 0,\end{aligned}$$

since, for $\ell \nmid m$, $K(E[\ell m]) = K(E[\ell,m]) = K(E[\ell])K(E[m])$, which is $K(E[m])$ by our assumption.
Moreover, when $K = \mathbb{F}_q(j_E)$, the positivity of $\delta(E/\mathbb{F}_q(j_E),1,n)$ is easier to establish, thanks to Igusa's

results and the multiplicativity of $\#\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$. Indeed,

$$\begin{aligned}\delta(E/\mathbb{F}_q(j_E),1,n) &= \sum_{\substack{m\geq 1\\(m,p)=1\\m\mid q^n-1}} \frac{\mu(m)c_m}{[\mathbb{F}_q(j_E)(E[m]):\mathbb{F}_q(j_E)]} = \sum_{\substack{m\geq 1\\(m,p)=1\\m\mid q^n-1}} \frac{\mu(m)}{[\mathbb{F}_q(j_E)(E[m]):\mathbb{F}_{q^{c_m}}(j_E)]}\\ &= \sum_{\substack{m\geq 1\\(m,p)=1\\m\mid q^n-1}} \frac{\mu(m)}{\#\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})} = \prod_{\substack{\ell\neq p\\ \ell\mid q^n-1}} \left(1-\frac{1}{\ell\,(\ell^2-1)}\right).\end{aligned}$$

Similar, but more involved, sufficient conditions may also be written for $\delta(E/K,d)=0$ and $\delta(E/\mathbb{F}_q(j_E),d,n)=0$. We plan to address the complete positivity criterion for these densities in a future paper.

Remark 18. Let $p\geq 5$ and let us consider the curve $E/\mathbb{F}_p(t): y^2+xy=x^3+\frac{36}{1728-t}+\frac{1}{1728-t}$, for which $j_E(t)=t$. In view of the above remark, Theorem 1 implies

$$\#\{t_0\in\mathbb{F}_p : E_{t_0}(\mathbb{F}_p) \text{ is cyclic}\} = p\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell^3-\ell}\right)+\mathrm{O}_{E,\varepsilon}\left(p^{\frac{1}{2}+\varepsilon}\right).$$

The following tables illustrate this formula with $f(p):=\#\{t_0\in\mathbb{F}_p : E_{t_0}(\mathbb{F}_p) \text{ is cyclic }\}$ and $g(p):=p\prod_{\ell\mid p-1}\left(1-\frac{1}{\ell^3-\ell}\right)$.

p	11	13	17	19	23	29	31	37	41	43
$f(p)$	9	10	14	14	19	24	23	30	34	33
$g(p)$	9.09	10.38	14.16	15.17	19.15	24.09	24.55	29.54	33.88	34.23

p	101	103	107	109	113	127	131	137	139	149
$f(p)$	84	84	89	86	94	101	108	114	111	124
$g(p)$	83.46	82.24	89.16	87.04	93.88	101.1	108.2	114.1	110.9	124.1

p	1009	1013	1019	1021	1031	1033	1039	1049
$f(p)$	809	844	849	807	851	819	824	874
$g(p)$	803.40	843.45	849.16	808.42	852.00	824.95	829.75	874.16

These numbers are quite surprising, since the approximations are much better than expected. At the moment, we do not have a satisfactory explanation for this phenomenon.

Acknowledgments. The authors are grateful to Chris Hall and Nathan Jones for useful conversations on the topic of the paper. Some of the work on this paper was done while A.C Cojocaru was a member at the Max Planck Institute for Mathematics in Bonn, Germany, and at the Institute for Advanced Study in Princeton, USA; she is grateful to both institutes for funding and excellent work facilities.

References

[BaLoVi] A. Bandini, I. Longhi and S. Vigni, *Torsion points on elliptic curves over function fields and a theorem of Igusa*, Expositiones Mathematicae 27, 2009, pp. 175–209.

[BaSh] W.D. Banks and I.E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height,* Israel J. Math. 173, 2009, pp, 253–277.

[ClKu] D.A. Clark and M. Kuwata, *Generalized Artin's conjecture for primitive roots and cyclicity mod* $\mathfrak{p}$ *of elliptic curves over function fields*, Canad. Math. Bull. Vol. 38 (2), 1995, pp. 167–173.

[Co1] A.C. Cojocaru, *On the cyclicity of the group of* $\mathbb{F}_p$*-rational points of non-CM elliptic curves*, J. Number Theory 96, 2002, no. 2, pp. 335–350.

[Co2] A.C. Cojocaru, *Cyclicity of CM elliptic curves modulo p*, Trans. Amer. Math. Soc. 355, 2003, no. 7, pp. 2651–2662.

[Co3] A.C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, Number Theory, pp. 61–79, CRM Proc. Lecture Notes 36, Amer. Math. Soc., Providence, RI, 2004.

[CoHa] A.C. Cojocaru and C. Hall, *Uniform results for Serre's theorem for elliptic curves*, Int. Mat. Res. Not. 2005, no. 50, pp. 3065–3080.

[CoMu] A.C. Cojocaru and M.R. Murty, *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik's problem*, Math. Ann. 330, 2004, pp. 601-625.

[CoSh] A.C. Cojocaru and D. Shulman, *Almost all reductions of a generic Drinfeld module of arbitrary rank have a large exponent,* preprint.

[Du] W. Duke, *Almost all reductions modulo p of an elliptic curve have large exponent*, C.R. Acad. Sci. Paris, Ser. I 337, 2003, pp. 689–692.

[DuTo] W. Duke and Á. Tóth, *The splitting of primes in division fields of elliptic curves* , Experimental Math. 11, 2002, no. 4, pp. 555–565.

[GuMu] R. Gupta and M.R. Murty, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. 101, no. 1, 1990, pp. 225–235.

[HaVo] C. Hall and J.F. Voloch, *Towards Lang-Trotter for elliptic curves over function fields*, Pure Appl. Math. Q. 2, no. 1, part 1, 2006, pp. 163–178.

[Ig] J-I. Igusa, *Fibre systems of Jacobian varieties (III. Fibre systems of elliptic curves)*, Amer. J. Math. 81, 1959, pp. 453–476.

[Jo] N. Jones, *A bound for the torsion conductor of a non-CM elliptic curves*, Proc. Amer. Math. Soc. 137, no. 1, 2009, pp. 37–43.

[LaTr] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. vol. 83, no 2, 1977, pp. 289–292.

[Mu1] M.R. Murty, *On Artin's conjecture*, J. Number Theory 16, no. 2, 1983, pp. 147–168.

[Mu2] M.R. Murty, *On the supersingular reduction of elliptic curves*, Proc. Indian Acad. Sci. 97, no. 1-3, 1987, pp. 247–250.

[MuSc] V.K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields* , C.R. Acad. Sci. Paris, t. 319, Série I, 1994, pp. 523–528.

[Ro] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **201**, Springer-Verlag, New York, 2002.

[Se] J-P. Serre, *Summaries of courses of the 1977-78 academic year* (French), pp. 67–71, Collège de France, Paris, 1978.

[Si] J.H. Silverman, *The arithmetic of elliptic curves*, Springer Verlag, GTM 106, Newy York, 1986.

[Vo1] J.F. Voloch, *A note on elliptic curves over finite fields*, Bulletin de la S.M.F., tome 116, no 4 (1988), pp. 455–458.

[Vo2] J.F. Voloch, *Primitive points on constant elliptic curves over function fields*, Bol. Soc. Bras. Mat., Vol. 21, no. 1, 1990, pp. 91–94.

[We] A. Weil, *Courbes algébriques et variétés abéliennes*, Paris, Hermann, 1971.

(Alina-Carmen Cojocaru)

- Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 S Morgan St, 322 SEO, Chicago, 60607, IL, USA;
- Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei St, Bucharest, 010702, Sector 1, Romania;

E-mail address, Alina-Carmen Cojocaru: cojocaru@math.uic.edu

(Árpád Tóth)

- Eötös Lóránd University, Department of Analysis, Mathematical Institute, Pázmány Péter sétány 3/c, Budapest, Hungary.

E-mail address, Árpád Tóth: toth@cs.elte.hu