Cyclic reduction of Elliptic Curves

Campagna, Francesco; Stevenhagen, Peter

Publication date:
2019

Document version
Early version, also known as pre-print

Citation for published version (APA):
Cyclic Reduction of Elliptic Curves

FRANCESCO CAMPAGNA, PETER STEVENHAGEN

Abstract. For an elliptic curve $E$ defined over a number field $K$, we study the density of the set of primes of $K$ for which $E$ has cyclic reduction. For $K = \mathbb{Q}$, Serre proved that, under GRH, the density equals an inclusion-exclusion sum $\delta_{E/\mathbb{Q}}$ involving the field degrees of an infinite family of division fields of $E$. We extend this result to arbitrary number fields $K$, and prove that, for $E$ without complex multiplication, $\delta_{E/K}$ equals the product of a universal constant $A_\infty \approx 8.137519$ and a rational correction factor $c_{E/K}$. Unlike $\delta_{E/K}$ itself, $c_{E/K}$ is a finite sum of rational numbers that can be used to study the vanishing of $\delta_{E}$, which is a non-trivial phenomenon over number fields $K \neq \mathbb{Q}$. We include several numerical illustrations.

1. Introduction

Let $E$ be an elliptic curve defined over a number field $K$, and $p$ a prime of $K$ for which $E$ has good reduction. Then the point group $E_p(k_p)$ of the reduced curve over the residue class field $k_p$ is a finite abelian group on at most two generators [17, III, 6.4]. If one generator suffices, we call $p$ a prime of cyclic reduction of $E$. The question considered in this paper is whether the set $S_{E/K}$ of primes of cyclic reduction of $E$ is infinite and, if so, whether it has a density inside the set of all primes of $K$.

Serre [15] observed in 1977 that this problem is very similar to the Artin primitive root problem, which asks for the density of the set of primes $p$ of $K$ for which a fixed element $a \in K^*$ is a primitive root modulo $p$. In this situation, these primes are (up to finitely many primes of ‘bad reduction’ for $a$) the primes $p$ that do not split completely in any of the ‘$\ell$-division fields’ $K_\ell = K(\zeta_\ell, \sqrt[\ell]{a}) = \text{Split}_K(X^\ell - a)$ of the element $a$ at primes $\ell \in \mathbb{Z}$. A heuristic inclusion-exclusion argument [1, pp.viii-ix] that goes back to Artin (1927) suggests that the set of such primes has a natural density that can be expressed in terms of the degrees of the $m$-division fields $K_m$ as

$$\delta_{a,K} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : K]}.$$  


The set $S_{E/K}$ of primes of cyclic reduction of an elliptic curve $E/K$ can be characterized in a similar way (Corollary 2.2). It is, up to finitely many $p$, the set of primes that do not split completely in any of the elliptic division fields $K_\ell = K(E[\ell](\mathbb{K}))$ of $E$ at the primes $\ell \in \mathbb{Z}$. Unsurprisingly, the associated heuristic density for $S_{E/K}$ is given by an
inclusion-exclusion sum

\[(2) \quad \delta_{E/K} = \sum_{m=1}^{\infty} \frac{\mu(m)}{[K_m : K]} \]

that, at least typographically, is identical to (1). It is the limit of the finite sums

\[(3) \quad \delta_{E/K}(n) = \sum_{m|n} \frac{\mu(m)}{[K_m : K]} \]

for \(n\) tending to infinity under the partial ordering of divisibility. Under this ordering, we have

\[(4) \quad m|n \Rightarrow \delta_{E/K}(m) \geq \delta_{E/K}(n) \geq 0, \]

so the limit exists and is non-negative. Each value \(\delta_{E/K}(n)\) is an upper bound for the upper density of the set \(S_{E/K}\), but proving unconditionally that \(S_{E/K}\) is infinite in case \(\delta_{E/K}\) is positive is an open problem, just like it still is in Artin's original setting in (1).

For \(K = \mathbb{Q}\), Serre showed that, under GRH, the set \(S_{E/\mathbb{Q}}\) does have density \(\delta_{E/\mathbb{Q}}\) as in (2). His proof, which is along Hooley’s lines, was published in 1983 by Murty [10].

In order to study cyclic reduction densities over arbitrary number fields, we first extend Serre’s result to this case, in Section 2.

**Theorem 1.1.** Let \(E\) be an elliptic curve defined over a number field \(K\). Under GRH, the set \(S_{E/K}\) of primes of \(K\) of cyclic reduction has the density \(\delta_{E/K}\) defined by (2).

The number \(\delta_{E/K}\) in (2) is defined by a series that converges rather slowly, and it is unclear when it vanishes. Under the assumption that \(E\) is without CM, i.e., that \(E\) does not have complex multiplication over its algebraic closure, we will show that there exists a squarefree number \(N = N(E, K)\) such that the union \(\bigcup_{n \text{ squarefree}} K_n \subset \overline{K}\) determining \(\delta_{E/K}\) can be obtained over \(K\) as the linearly disjoint ‘span’ of \(K_N\) and the fields \(K_\ell\) for primes \(\ell \nmid N\). We then factor \(\delta_{E/K}\) accordingly, in Section 3.

**Theorem 1.2.** Let \(E/K\) be an elliptic curve without CM. Then there exists an integer \(N = N(E, K) \in \mathbb{Z}_{>0}\) such that \(\delta_{E/K}\) can be factored as

\[
\delta_{E/K} = \delta_{E/K}(N) \cdot \prod_{\ell|N, \ell \text{ prime}} \left(1 - \frac{1}{[K_\ell : K]}\right).
\]

For \(N = N(E, K)\), one may take (Theorem 3.2) the product of the small primes 2 and 3, the primes dividing the discriminant \(\Delta_K\) of \(K\), the primes dividing the norms of the primes of bad reduction of \(E\) and the finitely many primes \(\ell\) for which \(K_\ell\) does not have the maximal degree

\[(5) \quad [K_\ell : K] = \# \text{GL}_2(F_\ell) = (\ell^2 - 1)(\ell^2 - \ell).\]

It follows that, just as for \(\delta_{a,K}\) in (1), \(\delta_{E/K}\) can be written as a product

\[(6) \quad \delta_{E/K} = c_{E/K} \cdot A_{\infty}\]

of a rational number \(c_{E/K} \in \mathbb{Q}_{>0}\) and a universal non-CM elliptic Artin constant

\[(7) \quad A_{\infty} = \prod_{\ell \text{ prime}} \left(1 - \frac{1}{(\ell^2 - 1)(\ell^2 - \ell)}\right) \approx 0.8137519.\]
We have $c_{E/K} = 1$ when the division fields $K_\ell$ for $\ell$ prime all assume the maximal degree as in (5) and they form a linearly disjoint family over $K$ in the sense of Definition 3.1. The first condition is often not satisfied, and a more satisfactory decomposition than (6) is given in (14) in Section 4 as $\delta_{E/K} = \alpha_{E/K} \cdot \alpha_{E/K}$, with $\alpha_{E/K}$ a naive density that depends only on the degrees $[K_\ell : K]$ and $\alpha_{E/K} \in \mathbb{Q}_{\geq 0}$ an entanglement correction factor that reflects the relations between finitely many critical $K_\ell$.

If $\delta_{E/K}$ vanishes, there is a finite rational sum $\delta_{E/K}(N)$ in Theorem 1.2 that vanishes. In this case we know unconditionally that $S_{E/K}$ is a finite set, as there is some `finite' obstruction to cyclic reduction in the division field $K_N$. This obstruction may be non-trivial, in the sense that the naive density $\alpha_{E/K}$ above is non-zero, meaning that none of the division fields $K_\ell$ for $\ell$ prime is equal to $K$, but the entanglement correction factor $\alpha_{E/K}$ vanishes. We construct many examples of this phenomenon in Section 4, and provide some explicit computations of $\delta_{E/K}$ in Section 5.

For our results on CM-elliptic curves, we refer to [3]. In this case, there is no general ‘factorization’ as in Theorem 1.2, as the entanglement of the division fields can be of a different nature, leading to simple rational densities.

ACKNOWLEDGMENTS

We thank D. Lombardo and S. Tronto for pointing out Lemma 3.3 in group theory, and Fabien Pazuki for pushing us to write up the ideas in this paper.

This project has received funding from the European Union Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 801199.

2. DENSITY OF THE SET $S_{E/K}$

Let $E$ be an elliptic curve defined by an integral Weierstrass equation $y^2 = x^3 + Ax + B$ with coefficients $A, B$ in the ring of integers $\mathcal{O}_K$ of a number field $K$. To $E$ we associate its discriminant

$$\Delta_E = -16(4A^3 + 27B^2) \in \mathcal{O}_K \setminus \{0\}.$$  \hfill (8)

The primes $p$ of $K$ coprime to $\Delta_E$ are the primes of good reduction of $E$. For such $p$, reduction modulo $p$ yields an elliptic curve $E_p$ over the residue class field $k_p$. Note that with this model of $E$, primes $p$ of $K$ over 2 are never primes of good reduction.

We begin by formally stating the criterion for a prime $p$ of good reduction of $E$ to be a prime of cyclic reduction of $E$, i.e., a prime for which the finite group $E_p(k_p)$ is cyclic.

**Lemma 2.1.** For a prime $p$ of good reduction of $E$, the following are equivalent:

1. $p$ is a prime of cyclic reduction of $E$;
2. for no prime number $\ell$ coprime to $p$, the prime $p$ splits completely in $K \subset K_\ell$, with $K_\ell$ the $\ell$-division field of $E$.

**Proof.** Let $p$ be a prime of good reduction for $E$. Then $E_p(k_p)$ is a cyclic group if and only if for no prime $\ell$, its $\ell$-torsion subgroup $E_p[\ell](k_p)$ has order $\ell^2$. For $\ell = \text{char}(k_p)$, it is a generality on elliptic curves in positive characteristic that the group $E_p[\ell](k_p)$ is cyclic, so we further assume $\ell \neq \text{char}(k_p)$. Then $p$ is unramified in the Galois extension $K \subset K_\ell$ as it is a prime of good reduction of $E$ coprime to $\ell$.

The group $E[\ell](k_\ell)$ has order $\ell^2$ by definition of $K_\ell$, and at every prime $q | p$ of $K_\ell$, the natural reduction map $E[\ell](K_\ell) \to E_q(k_q)$ is injective as $q \nmid \ell \Delta_E$ is a prime of good reduction of $E$ in $K_\ell$. Thus $E_q[\ell](k_q)$ has order $\ell^2$. Now $k_q$ is generated over $k_p$ by the
coordinates of the points in $E_q[\ell](k_q)$, as $K \subset K_\ell$ is generated by the coordinates of the $\ell$-torsion points of $E$. It follows that the natural inclusion $k_p \subset k_q$ is an equality

for all $q|p$ in $K_\ell$, i.e., $p$ splits completely in $K \subset K_\ell$, if and only if the natural inclusion $E_p[\ell](k_p) \subset E_q[\ell](k_q)$ is an equality. As $E_q[\ell](k_q)$ has order $\ell^2$, this proves the lemma. \hfill \Box

If $p$ is a prime of good reduction of $E$ of characteristic $p$ coprime to the discriminant $\Delta_K$ of $K$, then $p$ can not split completely in the division field $K_p$, as it is totally ramified in the subextension $K \subset K(\zeta_p)$ of degree $p-1 > 1$ of $K_p$ that is generated by a primitive $p$-th root of unity $\zeta_p$. This shows that, for primes $p$ coprime to both $\Delta_E$ and $\Delta_K$, being in the set $S_{E/K}$ of primes of cyclic reduction of $E$ is tantamount to not splitting completely in any division field extension $K \subset K_\ell$ at a rational prime $\ell$.

**Corollary 2.2.** For a prime $p \nmid \Delta_E \Delta_K$, we have $p \in S_{E/K}$ if and only if $p$ does not split completely in any of the division fields $K_\ell$, with $\ell \in \mathbb{Z}$ prime.

The proof of Lemma 2.1 shows that if a prime $p \nmid \Delta_E \Delta_K$ splits completely in $K \subset K_\ell$, then $E_p(k_p)$ has complete $\ell$-torsion, so we have $\ell \leq \sqrt{N_{K/Q}(p)} + 1$ by the Hasse-Weil bound. For a squarefree integer $m$ and a prime $p \nmid \Delta_E$, we similarly obtain

(9) \quad $p \nmid \Delta_E \Delta_K$ splits completely in $K_m \implies m \leq \sqrt{N_{K/Q}(p)} + 1$.

In order to count the cardinality $\#S_{E/K}(x)$ of primes $p$ in the set $S_{E/K}$ of good reduction of norm $N_{K/Q}(p) \leq x \in \mathbb{R}_{>0}$, we introduce the counting function

$$
\pi_K(x, K_m) = \# \{ p \nmid \Delta_E \Delta_K : N_{K/Q}(p) \leq x \text{ and } p \text{ splits completely in } K \subset K_m \}.
$$

The function $\pi_K(x, K)$ counts primes $p \mid \Delta_K$ of good reduction of $E$ of norm at most $x$, and, disregarding the primes $p \mid \Delta_K$ in $S_{E/K}$, Corollary 2.2 and inclusion-exclusion yield

(10) \quad $\#S_{E/K}(x) = \sum_{m=1}^{\infty} \mu(m) \pi_K(x, K_m)$.

Note that by (9), the function $\pi_K(x, K_m)$ vanishes for $m > \sqrt{x} + 1$, so the infinite sum of integers in (10) is actually finite, and therefore convergent.

In order to obtain the desired asymptotic relation $\#S_{E/K}(x) \sim \delta_{E/K} \cdot x/\log x$ claimed in Theorem 1.1, we want to use the asymptotic relations $\pi_K(x, K_m) \sim \frac{1}{[K_m:k]} \cdot x/\log x$. Dividing both sides in (10) by $x/\log x$, it comes down to interchanging the infinite sum and the limit $x \to \infty$ in the right hand side of (10). This requires GRH to bound the error terms in these asymptotic relations, and a variant of Hooley’s argument in [4]. Murty [10, Theorem 1] has shown that in this setting, one can prove under GRH that the inclusion-exclusion density is correct if $[K_m : K]$ grows sufficiently rapidly with $m$ (as it does in our case) and two conditions are satisfied. The first condition is that the root discriminant of the division fields $K_m$ does not grow too rapidly with $m$, as follows.

**Proposition 2.3.** For $m \in \mathbb{Z}_{>0}$ tending to infinity, we have

$$
\frac{1}{[K_m : K]} \log |\Delta_{K_m}| = O(\log m)
$$

Note that the quantity in the Proposition is $[K : \mathbb{Q}]$ times the logarithm of the ordinary root discriminant $|\Delta_{K_m}|^{1/[K_m : \mathbb{Q}]}$. 
The second condition is that ‘not too many’ primes $p$ of $K$ split in the division fields $K_\ell$ for ‘large’ primes $\ell$, in the following sense.

**Proposition 2.4.** The number of primes $p$ of $K$ of norm $N_{K/Q}(p) \leq x$ that split completely in $K \subset K_\ell$ for some prime $\ell > \frac{x^{1/2}}{\log x}$ is $o\left(\frac{x}{\log x}\right)$ for $x \to \infty$.

**Proof of Proposition 2.3.** Bounding absolute root discriminants already dates back to Hensel [13, p. 58]. For the relative extension $K \subset K_m$ we can use the version found in [11, p. 44]. It states that for a finite Galois extension of number fields $K \subset L$ with relative discriminant $\Delta_{L/K}$ of norm $D(L/K) = N_{K/Q}(\Delta_{L/K}) \in \mathbb{Z}_{>0}$, we have

$$\log D(L/K) \leq ([L : Q] - [K : Q]) \sum_{p \mid D(L/K)} \log p + [L : Q] \log([L : K]).\tag{11}$$

As the absolute discriminant of $L$ equals $|\Delta_L| = D(L/K)|\Delta_K|^{[L : K]}$, the identity

$$\log D(L/K) = \log |\Delta_L| - [L : K] \log |\Delta_K|$$

can be combined with the inequality (11) in the case $L = K_m$ to obtain, after division by $n(m) = [K_m : K]$, the estimate

$$\frac{1}{n(m)} \log |\Delta_{K_m}| - \log |\Delta_K| \leq \frac{[K_m : Q] - [K : Q]}{n(m)} \sum_{p \mid D(K_m/K)} \log p + \frac{[K_m : Q]}{n(m)} \log n(m)$$

$$\leq [K : Q] \left( \sum_{p \mid D(K_m/K)} \log p + \log n(m) \right).$$

The primes $p \mid D(K_m/K)$ either divide $m$, or they lie under one of the finitely many primes of bad reduction of $E$, so we have $\sum_{p \mid D(K_m/K)} \log p \leq C_E + \log m$ for some constant $C_E$ depending only on $E$. We obtain

$$\frac{1}{n(m)} \log |\Delta_{K_m}| \leq [K : Q] \cdot (\log |\Delta_K| + C_E + \log m + \log n(m)).$$

As we have $n(m) = O(m^4)$, this yields the desired asymptotic relation. \qed

**Proof of Proposition 2.4.** When showing that the cardinality of the set of primes $p$ of $K$ of norm $N_{K/Q}(p) \leq x$ that split completely in $K \subset K_\ell$ for some prime $\ell > \frac{x^{1/2}}{\log x}$ is asymptotically $o\left(\frac{x}{\log x}\right)$, we may disregard primes $p \mid \Delta_K \Delta_E$, as they are finite in number, and primes $p$ that are not of degree 1, as there are no more than $o(\sqrt{x})$ of them.

Suppose now that $p \nmid \Delta_K \Delta_E$ is of prime norm $N_{K/Q}(p) = p \leq x$, and that $p$ splits completely in an $\ell$-division field $K_\ell$ with $\ell > 2$. By (9), this implies $\ell \leq \sqrt{x} + 1$. As $p \nmid \Delta_K$ necessarily splits completely in the subextension $K \subset K(\zeta_\ell)$, we have $p \nmid \ell$, and $p$ lies over a rational prime $p \equiv 1 \mod \ell$. Any such $p$ gives rise to at most $[K : Q]$ primes $p$ in $K$ of norm $p$. Thus, the number $B(x)$ of such $p$ can be bounded by

$$\frac{1}{x^{1/2} \log^2 x} \sum_{\ell \leq x^{1/2} + 1} \pi(x, 1, \ell), \tag{12}$$
with \(\pi(x, 1, \ell)\) denoting the number of primes \(p \leq x\) satisfying \(p \equiv 1 \bmod \ell\). By the Brun-Titchmarsh theorem, we have
\[
\pi(x, 1, \ell) \leq \frac{2x}{\varphi(\ell) \log(\frac{x}{\ell})} \leq \frac{x}{\ell \log(\frac{x}{\ell})},
\]
so we obtain
\[
B(x) \ll \sum_{x^{1/2} \log^2 x < \ell < x^{1/2} + 1} \frac{x}{\ell \log(\frac{x}{\ell})} \ll \frac{x}{\log(x)} \cdot \sum_{x^{1/2} \log^2 x < \ell < x^{1/2} + 1} \frac{1}{\ell}.
\]
It now suffices to show that
\[
\sum_{x^{1/2} \log^2 x < \ell < x^{1/2}} \frac{1}{\ell}
\]
tends to zero for \(x \to \infty\). This follows from the well-known estimate \([2, \text{Theorem 4.12}]\)
\[
(13)
\sum_{\ell \leq X, \ell \text{ prime}} \frac{1}{\ell} = \log \log X + C + O\left(\frac{1}{\log X}\right)
\]
with \(C\) some absolute positive constant. Applying (13) for \(X = x^{1/2}\) and \(X = x^{1/2} / \log^2 x\) and subtracting, we do obtain a quantity tending to zero for \(x \to \infty\):
\[
\sum_{x^{1/2} \log^2 x < \ell < x^{1/2}} \frac{1}{\ell} = \log x^{1/2} - \log \left(\frac{x^{1/2}}{\log x}\right) + O\left(\frac{1}{\log x^{1/2}}\right)
\]
\[
= \log \left(\frac{1}{2} \log x - 2 \log \log x\right) + O\left(\frac{1}{\log x}\right). \quad \square
\]

**Proof of Theorem 1.1.** By [10, Theorem 1], this follows from Propositions 2.3 and 2.4. \quad \square

3. Factorization of \(\delta_{E/K}\) in the non-CM case

The conjectural density \(\delta_{E/K}\) in Theorem 1.1 has an explicit definition (2) that is ill-suited to determine either its approximate value or its vanishing. Theorem 1.2 allows us to approximate it with high precision from fewer data, and to determine whether it vanishes. Its proof amounts to determining the entanglement of the division fields \(K_\ell\), which, by the open image theorem of Serre [14], is ‘of finite nature’ for \(E\) without CM.

**Definition 3.1.** Let \(F\) be a field and let \(\mathcal{F} = \{F_n\}_{n \in X}\) a family of Galois extensions of \(F\) inside an algebraic closure of \(F\). We call \(\mathcal{F}\) linearly disjoint over \(F\) if for the compositum \(L\) of the fields \(F_n\), the natural inclusion map
\[
\text{Gal}(L/F) \hookrightarrow \prod_{n \in X} \text{Gal}(F_n/F)
\]
is an isomorphism. If this is not the case, we call the family \(\mathcal{F}\) entangled over \(K\).

A family as in Definition 3.1, which can be either finite or infinite, depending on \(X\), is linearly disjoint over \(F\) if and only if for every individual field \(F_n \in \mathcal{F}\), the field \(F_n\) and the compositum of the fields \(F_m\) with \(m \neq n\) are linearly disjoint over \(F\).

The family of \(\ell\)-division fields \(K_\ell\) with \(\ell\) prime is not necessarily linearly disjoint over a number field \(K\) for an elliptic curve \(E/K\) without CM, but we can make it linearly
disjoint by grouping together finitely many $K_\ell$ in their compositum. This crucial fact can be formulated in the following way.

**Theorem 3.2.** Let $K$ be a number field, $E/K$ an elliptic curve without CM, and $N = N(E, K) \in \mathbb{Z}_{>0}$ any integer divisible by all prime numbers $\ell$ satisfying one of

1. $\ell \mid 2 \cdot 3 \cdot 5 \cdot \Delta_K$;
2. $\ell$ lies below a prime of bad reduction of $E$;
3. the Galois group $\text{Gal}(K_\ell/K)$ is not isomorphic to $\text{GL}_2(F_\ell)$.

Then the family consisting of $K_N$ and $\{K_\ell\}_{\ell \mid N}$ is linearly disjoint over $K$.

The proof of Theorem 3.2 relies on a group theoretical result on the Jordan-Hölder factors that can occur in subgroups of $H \subset \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

**Lemma 3.3.** Let $N \in \mathbb{Z}_{>0}$ be an integer and $H \subset \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ a subgroup. Suppose $S$ is a non-abelian simple group that occurs in $H$. Then $S$ is isomorphic to either $A_5$ or $\text{PSL}_2(\mathbb{F}_5)$, with $\ell$ a prime dividing $N$.

**Proof.** We may assume $H \subset \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{\ell \mid N} \text{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ as we only care about non-abelian simple Jordan-Hölder factors. In addition, we may assume that $N$ is squarefree, i.e., equal to its own radical $N_0 = \text{rad}(N)$; indeed, the natural map $r : \text{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to \text{SL}_2(\mathbb{Z}/N_0\mathbb{Z})$ has a solvable kernel that is a product of $\ell$-groups, and the groups $H$ and $H/(H \cap \ker r) \subset \text{SL}_2(\mathbb{Z}/N_0\mathbb{Z})$ have the same non-abelian simple Jordan-Hölder factors. Thus, every non-abelian simple group that occurs in $H$ occurs in a subgroup of some $\text{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, so we can reduce to the case that $N = \ell$ is prime. In this case the statement is a classical result that can be found in [16, p. IV-23].

**Proof of Theorem 3.2.** It suffices to show that for a number $N = N(E, K)$ satisfying the hypotheses (1)-(3) and $l \nmid N$ a prime number, we have $K_N \cap K_\ell = K$. Take such $N$ and $\ell$. Then $\ell \nmid N$ is unramified in the tower $\mathbb{Q} \subset K \subset K_N$ by (2), and since $K \subset K(\zeta_\ell)$ is totally ramified over $\ell$ of degree $\ell - 1 > 1$ by (1), the fields $K_N$ and $K(\zeta_\ell)$ are $K$-linearly disjoint. It now suffices to prove that the normal extensions $K(\zeta_\ell) \subset K_\ell$ and $K(\zeta_\ell) \subset K_N$ are linearly disjoint.

We have $\text{Gal}(K_\ell/K(\zeta_\ell)) \cong \text{SL}_2(F_\ell)$ by (3), and for $\ell \geq 5$ this group has a unique non-trivial normal subgroup $\{ \pm \text{id}_F \}$ with simple quotient $\text{PSL}_2(F_\ell)$. If $K_\ell \cap K_N(\zeta_\ell)$ is not equal to $K$, we find that the non-abelian simple group $\text{PSL}_2(F_\ell)$, which is not $A_5$ as we assume $\ell \neq 5$ by (1), is a Jordan-Hölder factor of $\text{Gal}(K_N(\zeta_\ell)/K(\zeta_\ell)) \cong \text{Gal}(K_N/K)$. As we can view $\text{Gal}(K_N/K)$ as a subgroup of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$, this contradicts Lemma 3.3, since we have $\ell \nmid N$.

**Proof of Theorem 1.2.** We simply note that the quantity $\delta_{E/K}(n)$ in (3) is the inclusion-exclusion fraction of elements in the Galois group $\text{Gal}(K_n/K)$ that have non-trivial restriction on every subfield $K_\ell$ with $\ell|N$. Thus, if $n_1$ and $n_2$ are coprime numbers for which the division fields $K_{n_1}$ and $K_{n_2}$ are $K$-linearly disjoint, we have an equality $\delta_{E/K}(n_1n_2) = \delta_{E/K}(n_1)\delta_{E/K}(n_2)$. If $N'$ is any squarefree multiple of the number $N = N(E, K)$ in Theorem 3.2, this yields

$$\delta_{N'}(E) = \delta_N(E) \cdot \prod_{\ell|N'/N, \ \ell \text{ prime}} \left(1 - \frac{1}{[K_\ell : K]}\right).$$

Taking the limit $N' \to \infty$ with respect to the divisibility ordering yields Theorem 1.2.
For our purposes, we only need to apply Theorem 3.2 for squarefree values of \( N \). We can however strengthen its conclusion a bit and reformulate it in the following way, as an explicit form of Serre’s open image theorem. This is the form used by Lombardo and Tronto in [9].

**Theorem 3.4.** Let \( K \) be a number field, \( E/K \) an elliptic curve without CM, and \( S \) the set of prime numbers \( \ell \) satisfying one of

1. \( \ell \mid 2 \cdot 3 \cdot 5 \cdot \Delta_K \);
2. \( \ell \) lies below a prime of bad reduction of \( E \);
3. the Galois group \( \text{Gal}(K_\ell/K) \) is not isomorphic to \( \text{GL}_2(F_\ell) \).

Write \( K_{\ell^\infty} \) for the compositum of all \( \ell \)-power division fields of \( E \) over \( K \), and \( K_S \) for the compositum of the fields \( K_{\ell^\infty} \) with \( \ell \in S \). Then the family consisting of \( K_S \) and \( \{ K_{\ell^\infty} \}_{\ell \notin S} \) is linearly disjoint over \( K \).

**Proof.** It suffices to show that for \( N \) an integer divisible by all primes in \( S \) and \( \ell \nmid N \) prime, we have \( K_N \cap K_{\ell^n} = K \) for every \( n \in \mathbb{Z}_{>0} \). For \( n = 1 \), this is Theorem 3.2.

As \( K \subset K_N \) is unramified over \( \ell \nmid N \) by condition (2), the intersection is \( K \)-linearly disjoint from \( K(K_\ell) \) by the condition \( \ell \nmid \Delta_K \) in (1), and it is \( K \)-linearly disjoint from \( K_\ell \) by Theorem 3.2. It therefore corresponds to a subgroup of \( \text{Gal}(K_{\ell^n}/K) \subset \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \) that maps surjectively to \( \text{Gal}(K_\ell/K) = \text{GL}_2(F_\ell) \) by (3) and has surjective image \( (\mathbb{Z}/\ell^n\mathbb{Z})^* \) under the determinant map. By a result of Serre [16, p. IV-23, Lemma 3], valid for \( \ell \geq 5 \), such a group is the full group \( \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}) \), proving \( K_N \cap K_{\ell^n} = K \). \( \square \)

4. **Vanishing of \( \delta_{E/K} \) in the non-CM case**

As almost all division fields \( K_\ell \) for \( E \) without CM have maximal degree \( (\ell^2 - 1)(\ell^2 - \ell) \), it follows from Theorem 1.2 that the associated densities \( \delta_{E/K} \) are rational multiples of the universal non-CM elliptic Artin constant \( A_\infty \) from (7).

A factorization of \( \delta_{E/K} \) that is in many ways more enlightening than the identity \( \delta_{E/K} = c_{E/K} \cdot A_\infty \) in (6) is the factorization

\[
\delta_{E/K} = \alpha_{E/K} \cdot A_{E/K}
\]

of \( \delta_{E/K} \) into a rational entanglement correction factor \( \alpha_{E/K} \in \mathbb{Q}_{\geq 0} \) and a naive density

\[
A_{E/K} = \prod_{\ell \text{ prime}} \left( 1 - \frac{1}{[K_\ell : K]} \right).
\]

The naive density equals the actual density (under GRH) when the family of division fields \( \{ K_\ell \}_\ell \) is linearly disjoint over \( K \).

From the factorization (14), it is clear that there are two possible causes for the vanishing of \( \delta_{E/K} \). If the naive density \( A_{E/K} \) vanishes, at least one \( \ell \)-division field \( K_\ell \) is equal to \( K \). For such \( \ell \), the full \( \ell \)-torsion of \( E \) is defined over \( K \), and therefore over almost all residue class fields \( k_p \), making \( S_{E/K} \) finite. We call this the trivial vanishing of the density. Note that \( K = K_\ell \) can only occur for primes \( \ell \nmid 2\Delta_K \).

The more subtle cause of vanishing of \( \delta_{E/K} \) that we refer to as non-trivial vanishing occurs when we have

\[
\delta_{E/K} = 0 \quad \text{and} \quad A_{E/K} > 0,
\]

i.e., when the naive density \( A_{E/K} \) is positive but the entanglement correction factor \( \alpha_{E/K} \) vanishes. In this case all \( K_\ell \) are different from \( K \), but the non-splitting conditions in the
occurrence, but we can make it happen by base changing elliptic curves $E$ defined over a small field such as $\mathbb{Q}$ to a well-chosen number field.

The underlying idea is an elliptic analogue of a similar construction in the multiplicative setting [5, Example 2.1]. One starts with a non-CM elliptic curve $E/K$ and considers it over an extension $K \subset K'$ for which the $\ell$-division fields $K'_\ell$ of $E$ over $K'$ for primes $\ell_1, \ell_2, \ell_3$ are different quadratic extensions of $K'$, but with compositum $K'_{\ell_1 \ell_2 \ell_3}$ a multi-quadratic extension of $K'$ of degree 4, and not 8. In this case, no prime of $K'$ can be inert in all three subextensions $K'_\ell$, and almost all reduced curves at primes of $K'$ will have complete $\ell$-torsion for at least one value $\ell \in \{p_1, p_2, p_3\}$, implying that $S_{E/K'}$ is finite. The construction has many degrees of freedom, leading to infinitely many different curves and number fields for which non-trivial vanishing as in (16) occurs.

**Theorem 4.1.** Let $E$ be an elliptic curve without CM defined over a number field $K$, with naive density $A_{E/K} > 0$. Then for any finite normal extension $K \subset L$, there exists a linearly disjoint normal extension $K \subset K'$ for which $\delta_{E/K'}$ vanishes non-trivially.

**Proof of Theorem 4.1.** Let $N = N(E, K)$ be as in Theorem 3.2. Then the $N$-division field $K_N$ and the $\ell$-division fields $K'_\ell$ at $\ell \nmid N$ of $E$ form a linearly disjoint family over $K$. Now let $K \subset L$ be a finite normal extension, and replace $K_N$ by the compositum $LK_N$. Then the family may no longer be $K$-linearly disjoint, but it becomes $K$-linearly disjoint again after leaving out finitely many well-chosen $K'_\ell$ from the family. This is because any finite extension of $K$ contained in the compositum of some $K$-linearly disjoint family of division fields $K'_\ell$ is contained in the compositum of finitely many $K'_\ell$, and these are the ones that we leave out.

Now pick any set $\{\ell_1, \ell_2, \ell_3\}$ of primes that have not been left out. Then the $\ell_1 \ell_2 \ell_3$-division field $K'_{\ell_1 \ell_2 \ell_3}$ of $E$ is Galois over $K$ with group

$$G = \text{GL}_2(\mathbb{Z}/\ell_1 \ell_2 \ell_3 \mathbb{Z}) = \prod_{i=1}^3 \text{GL}_2(\mathbb{F}_{\ell_i}).$$

Every $\text{GL}_2(\mathbb{F}_{\ell_i})$ contains a normal subgroup $\langle -1 \rangle$ generated by $-\text{id}_{\ell_i} \in \text{GL}_2(\mathbb{F}_{\ell_i})$, so the center of $G$ contains an elementary abelian 2-group $H' = \prod_{i=1}^3 \langle -1 \rangle \subset G$ of order 8. We let $H \subset H'$ be the ‘normal 1-subgroup’ of order 4 consisting of elements $(e_i)^3 \in H$ with $e_1 e_2 e_3 = 1$. Then $H$ is normal in $G$, and we take for $K'$ the invariant field $K' = K'_{\ell_1 \ell_2 \ell_3}$.

We now view $E$ as an elliptic curve over the finite normal extension $K'$ of $K$, and note that the division field $K'_{\ell_1 \ell_2 \ell_3} = K'_{\ell_1 \ell_2 \ell_3}$ is by construction Galois over $K'$ with group isomorphic to the Klein four-group $H$. As every non-trivial element of $H$ is the identity on exactly one of the division fields $K'_\ell$, the three intermediate quadratic extensions of $K' \subset K'_{\ell_1 \ell_2 \ell_3}$ are the division fields $K'_\ell$, and no prime of $K'$ will be inert in all three of them. This implies that we have $\delta_{E/K'} = 0$.

As the naive density $A_{E/K'}$ in (15) differs from $A_{E/K} > 0$ only in the three factors corresponding to the primes $\ell_i$, with the degree $[K'_\ell : K] = \# \text{GL}_2(\mathbb{F}_{\ell_i})$ being replaced by $[K'_{} : K'] = 2$, we still have $A_{E/K'} > 0$, so the vanishing of $\delta_{E/K'}$ is non-trivial. □

**Remark 4.2.** Our proof of Theorem 4.1 only uses the fact that $-\text{id}_{\ell_i}$ is contained in $\text{Gal}(K_{\ell_i}/K) \subset \text{GL}_2(\mathbb{F}_{\ell_i})$, and that the Klein four-group $H$ in the proof is contained in...
G = Gal(K_{\ell_1\ell_2\ell_3}/K) \subset \prod_{i=1}^{3} GL_2(F_{\ell_i}). This observation is useful when constructing an explicit example of an elliptic curve E over a ’small’ normal number field K’ for which \delta_{E/K’} vanishes non-trivially. If one does not insist on K’ being normal over K = \mathbb{Q}, one can use any element of order 2 in Gal(K_{\ell_1}/K) \subset GL_2(F_{\ell_1}) instead of –id_{\ell_1}, and use small primes \ell_i for which K_{\ell_i} is of small degree.

Example 4.3. The elliptic curve E defined over K = \mathbb{Q} by the minimal Weierstrass equation

\[ y^2 + xy + y = x^3 - 76x + 298 \]

has discriminant \( \Delta_E = -2^5 \cdot 5^8 \) and, according to LMFDB [8], its mod \( \ell \) Galois representations are maximal at \( \ell \neq 3, 5 \). The division field \( K_3 \) is non-abelian of degree 6, smaller than the generic degree 48 = \# GL_2(F_3), and at \( \ell = 5 \) it is Galois with group \( A_{20} = C_5 \times \text{Aut}(C_5) \), the affine group over \( F_5 \) of order 20, much smaller than the generic group \( GL_2(F_5) \) of order 480. As the division fields \( K_2 \) and \( K_3 \) are non-abelian of degree 6 with different quadratic subfields \( \mathbb{Q}(\sqrt{-\Delta_E}) = \mathbb{Q}(\sqrt{-2}) \) and \( \mathbb{Q}(\zeta_3) \), they are linearly disjoint over \( K = \mathbb{Q} \). As \( K_6 \) and \( K_5 \) are solvable extensions of \( \mathbb{Q} \) with maximal abelian subfields \( \mathbb{Q}(\sqrt{-2}, \zeta_3) \) and \( \mathbb{Q}(\zeta_3) \) that are linearly disjoint over \( \mathbb{Q} \), the division fields \( K_2 \), \( K_3 \) and \( K_5 \) are \( \mathbb{Q} \) linearly disjoint of even degree, so \( \text{Gal}(K_30/\mathbb{Q}) \cong S_3 \times S_3 \times A_{20} \) does contain an elementary abelian 2-subgroup \( H’ \) of order 8 as in the proof of Theorem 4.1.

We can therefore find a non-normal field \( K’ \) of degree \( |K’ : \mathbb{Q}| = 6 \cdot 6 \cdot 20/4 = 180 \) inside \( K_{30} \) for which \( \delta_{E/K’} \) vanishes non-trivially.

We do not know whether there exist examples of non-trivial vanishing over number fields of degree less than 180. We also do not know if there are examples that do not arise by base change, i.e., an example in which \( \delta_{E/K} \) vanishes non-trivially for \( K = \mathbb{Q}(j(E)) \).

5. Numerical examples

In order to compute \( \delta_{E/K} = \alpha_{E/K} \cdot A_{E/K} \) for a non-CM elliptic curve \( E/K \) as in (14), one starts by finding \( [K_{\ell} : K] \) at all primes \( \ell \) where \( K_{\ell} \) has non-maximal degree. This easily can be done for small examples using LMFDB [8], which provides a list of non-maximal degrees \( [K_{\ell} : K] \). This enables us to find the naive density \( A_{E/K} \) as a rational multiple of the universal constant \( A_{\infty} \) from (7). Typically, \( A_E \) has a value close to \( \delta_{E/K} \), and its approximate correctness can be confirmed by a computer count of the fraction of primes of cyclic reduction among primes of norm below some modest bound. Finding the exact entanglement correction factor \( \alpha_{E/K} \) can be more complicated. It typically involves group theory and ramification arguments. This section provides some easy examples.

We treat the five non-CM elliptic curves \( E/\mathbb{Q} \) listed in the table below. There are 78,498 rational primes below \( 10^6 \), and the table lists the number of them that give rise to cyclic reduction, and the fraction \( d(E) \) this represents.

<table>
<thead>
<tr>
<th>Equation</th>
<th>( p &lt; 10^6 ) of cyclic reduction</th>
<th>( d(E) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( y^2 = x^3 - 3x + 1 )</td>
<td>51,105</td>
<td>0.6510</td>
</tr>
<tr>
<td>( y^2 = x^3 + 2x + 3 )</td>
<td>38,383</td>
<td>0.4889</td>
</tr>
<tr>
<td>( y^2 = x^3 - 12096x - 544752 )</td>
<td>32,652</td>
<td>0.4159</td>
</tr>
<tr>
<td>( y^2 = x^3 + x + 3 )</td>
<td>63,910</td>
<td>0.8141</td>
</tr>
<tr>
<td>( y^2 = x^3 - 13392x - 1080432 )</td>
<td>48,026</td>
<td>0.6118</td>
</tr>
</tbody>
</table>
Example 5.1. For the elliptic curve \( E/Q \) defined by
\[
E : y^2 = x^3 - 3x + 1
\]
we have \( \Delta_E = 2^4 \cdot 3^4 \), and \( K_2 \), the splitting field of the polynomial \( x^3 - 3x + 1 \) of discriminant \( 3^4 \), is the real subfield of \( Q(\zeta_9) \), which is cubic, and not of maximal degree 6.

All other division fields \( K_\ell \) have maximal degree, so the naive density equals
\[
A_{E/Q} = \prod_{\ell \text{ prime}} \left( 1 - \frac{1}{[K_\ell : Q]} \right) = \frac{2}{3} \cdot \frac{6}{5} \cdot A_\infty \approx 0.6510015.
\]
The cyclic cubic field \( K_2 \) is not a subfield of \( K_3 \) as \( \text{Gal}(K_3/Q) \cong GL_2(F_3) \) has no quotient of order 3, so \( K_6 \) is a linearly disjoint compositum of \( K_2 \) and \( K_3 \). We have \( K_6 \cap K_5 = K \) as the intersection is solvable over \( K \), but does not contain \( \sqrt{5} \notin K_6 \). As we can take \( N(E,Q) = 2 \cdot 3 \cdot 5 \) in Theorem 3.2, we find that the family of \( \ell \)-division fields \( K_\ell \) is \( Q \)-linearly disjoint. In this case there is no entanglement correction, and \( \delta_{E/Q} \) is equal to the naive density \( A_{E/Q} \). The numerical agreement is excellent.

Example 5.2. The elliptic curve \( E/Q \) defined by
\[
E : y^2 = x^3 + 2x + 3 = (x + 1)(x^2 - x + 3)
\]
of discriminant \( \Delta_E = -2^4 \cdot 5^2 \cdot 11 \) has a unique rational torsion point of order 2, and \( K_2 = Q(\sqrt{-11}) \). For \( \ell > 2 \), the degree of \( K_\ell \) is maximal, so the naive density equals
\[
A_{E/Q} = \frac{1}{2} \cdot \frac{6}{5} \cdot A_\infty \approx 0.48825114.
\]
We can take \( N(E,Q) = 2 \cdot 3 \cdot 5 \cdot 11 \) in Theorem 3.2. As \( K_2 \) is not the unique quadratic subfield \( Q(\zeta_3) \) of \( K_3 \), the extension \( K_6 \) is a linearly disjoint compositum of \( K_2 \) and \( K_3 \). Again, \( K_6 \) is solvable and does not contain \( \sqrt{5} \), so it is linearly disjoint from \( K_5 \).

We now know that the family of division fields \( \{K_\ell\}_{\ell \neq 11} \) is linearly disjoint over \( Q \). As \( K_{11} \) contains the quadratic field \( K_2 = Q(\sqrt{-11}) \subset Q(\zeta_{11}) \), any rational prime that does not split completely in \( K_2 \) automatically does not split completely in \( K_{11} \), making the non-splitting condition in \( K_{11} \) for primes of cyclic reduction superfluous. Thus, the entanglement correction in this case amounts to leaving out the factor \( 1 - 1/[K_{11} : Q] = \frac{12000}{13199}A_{E/Q} \approx 0.4882881 \) is so close to the naive density that the correction is not easily detected numerically. Our value of \( d(E) \) obtained by checking less than 80,000 primes is less than .15% away from either of these values: a good match.

Example 5.3. The elliptic curve \( E/Q \) defined by
\[
E : y^2 = x^3 - 12096x - 544752
\]
of discriminant \( \Delta_E = -2^{12} \cdot 3^{12} \cdot 19^3 \) has division fields \( K_\ell \) of maximal degree at all primes \( \ell \neq 3 \), and a minimal 3-division field \( K_3 = Q(\zeta_9) \). This makes the naive density equal to
\[
A_{E/Q} = \frac{48}{47} \cdot \frac{1}{2} A_\infty \approx 0.4155329.
\]
We can take \( N(E,Q) = 2 \cdot 3 \cdot 5 \cdot 19 \) in this case. The quadratic subfield \( Q(\sqrt{-19}) \) of \( K_2 \) is different from \( K_3 = Q(\zeta_9) \), and again \( K_2, K_3 \) and \( K_5 \) are linearly disjoint as we have \( \sqrt{5} \notin K_6 \). This time \( \{K_\ell\}_{\ell \neq 19} \) a linearly disjoint family over \( Q \), and \( K_2 \) has a non-trivial intersection \( K_2 \cap K_{19} = Q(\sqrt{-19}) \), but not an inclusion \( K_2 \subset K_{19} \).
This is a very common form of entanglement over \( K = \mathbb{Q} \): if the quadratic subfield \( \mathbb{Q}(\sqrt{\Delta_E}) \) of \( K_2 \) has odd discriminant \( D \), it is a subfield of the cyclotomic field \( \mathbb{Q}(\zeta_{2D}) \), and therefore of the compositum \( K_D \) of the division fields \( K_\ell \) with \( \ell \mid D \). If this quadratic intersection between \( K_2 \) and \( K_D \) is the only entanglement between the fields \( K_\ell \), then \( G = \text{Gal}(K_{2|D}/\mathbb{Q}) \subset G' = \prod_{\ell \mid 2D} \text{Gal}(K_\ell/\mathbb{Q}) \) is a subgroup of index 2 arising as the kernel of a quadratic character on \( G' \). In this case we can apply the character sum method \([7, \text{Theorem 8.4}]\), which gives an entanglement correction

\[
\alpha_{E/\mathbb{Q}} = 1 + \prod_{\ell \mid 2D, \ell \text{ prime}} \frac{1}{|K_\ell : \mathbb{Q}| - 1}.
\]

For \( D = -19 \) we obtain \( \alpha_{E/\mathbb{Q}} = \frac{615596}{615595} \) and \( \delta_{E/\mathbb{Q}} = 0.4155335 \), a figure which is not noticeably different from the naive density from a numerical point of view.

**Example 5.4.** Let \( E \) be the elliptic curve in the table defined by

\[ E : y^2 = x^3 + x + 3 \]

with discriminant \( \Delta_E = -2^4 \cdot 13 \cdot 19 \). In this case the mod \( \ell \) Galois representation associated to \( E \) has maximal image \( \text{GL}_2(\mathbb{F}_\ell) \) for all primes \( \ell \), so the naive density is equal to \( A_\infty \). We can take \( N(E, \mathbb{Q}) = 2 \cdot 3 \cdot 5 \cdot 13 \cdot 19 \) in Theorem 3.2. One can check that the only entanglement here comes from the quadratic subfield \( \mathbb{Q}(\sqrt{-13 \cdot 19}) \) of discriminant \( -13 \cdot 19 = -247 \) of \( K_2 \), which is contained in the compositum of \( K_{13} \) and \( K_{19} \). The entanglement correction factor given by the character sum formula \((17)\)

\[
\alpha_{E/\mathbb{Q}} = 1 + \prod_{\ell \mid 2 \cdot 13 \cdot 19} \frac{-1}{|K_\ell : \mathbb{Q}| - 1} \approx 0.99999999938,
\]

making \( \delta_{E/K} \) numerically indistinguishable from \( A_\infty \).

**Example 5.5.** The final elliptic curve in our table, which is defined by

\[ y^2 = x^3 - 13392x - 1080432, \]

has discriminant \( \Delta_E = -2^{12} \cdot 3^{12} \cdot 11^5 \) and is special for having minimal 5-division field \( K_5 = \mathbb{Q}(\zeta_5) \) of degree 4. At primes \( \ell \neq 5 \) the degree of \( K_\ell \) is maximal, so the naive density equals

\[ A_{E/\mathbb{Q}} = \frac{3}{4} \cdot \frac{480}{479} \approx 0.6115881, \]

very close to the fraction \( d(E) \) we computed. We take \( N(E, \mathbb{Q}) = 2 \cdot 3 \cdot 5 \cdot 11 \) and check easily that the only entanglement comes from the non-trivial intersection \( K_2 \cap K_{11} = \mathbb{Q}(\sqrt{-11}) \).

As in the previous example, the entanglement correction factor

\[
\alpha_{E/\mathbb{Q}} = 1 + \prod_{\ell \mid 2 \cdot 11} \frac{-1}{|K_\ell : \mathbb{Q}| - 1} = 1 + \frac{1}{5 \cdot 13199}
\]

yields \( \delta_{E/\mathbb{Q}} = 0.6115973 \), and is too small to be observed numerically.

**References**


Mathematisch Instituut, Universiteit Leiden, Leiden, Netherlands
Email address: psh@math.leidenuniv.nl

Institut for Matematiske Fag, Københavns Universitet, Copenhagen, Denmark
Email address: campagna@math.ku.dk