R. Bell et al. *Res. Number Theory (2020)6:1*
https://doi.org/10.1007/s40993-019-0175-9

Research in Number Theory

RESEARCH

Constants in Titchmarsh divisor problems for elliptic curves

Renee Bell[1,2], Clifford Blakestad[3], Alina Carmen Cojocaru[4,5*], Alexander Cowan[6], Nathan Jones[5], Vlad Matei[7], Geoffrey Smith[6] and Isabel Vogt[8]

*Correspondence: cojocaru@uic.edu
[5]Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 South Morgan Street, Chicago, IL 60607, USA
Full list of author information is available at the end of the article

ACC's work on this material was partially supported by the Simons Collaboration Grant under Award No. 318454. IV's work was partially supported by the NSF Graduate Research Fellowship Program and Grant DMS-1601946

Abstract

Inspired by the analogy between the group of units $\mathbb{F}_p^\times$ of the finite field with p elements and the group of points $E(\mathbb{F}_p)$ of an elliptic curve $E/\mathbb{F}_p$, E. Kowalski, A. Akbary & D. Ghioca, and T. Freiberg & P. Kurlberg investigated the asymptotic behaviour of elliptic curve sums analogous to the Titchmarsh divisor sum $\sum_{p\le x}\tau(p+a)\sim Cx$. In this paper, we present a comprehensive study of the constants $C(E)$ emerging in the asymptotic study of these elliptic curve divisor sums in place of the constant C above. Specifically, by analyzing the division fields of an elliptic curve $E/\mathbb{Q}$, we prove bounds for the constants $C(E)$ and, in the generic case of a Serre curve, we prove explicit closed formulae for $C(E)$ amenable to concrete computations. Moreover, we compute the moments of the constants $C(E)$ over two-parameter families of elliptic curves $E/\mathbb{Q}$. Our methods and results complement recent studies of average constants occurring in other conjectures about reductions of elliptic curves by addressing not only the average behaviour, but also the individual behaviour of these constants, and by providing explicit tools towards the computational verifications of the expected asymptotics.

Keywords: Titchmarsh divisor, Divisor sum, Serre curve, Elliptic curve, Galois representation

Mathematics Subject Classification: 11A25: arithmetic functions, related numbers, inversion formulas, 11G05: elliptic curves over global fields, 11G20: curves over finite and local fields, 11N37: asymptotic results on arithmetic functions, 11Y60: evaluation of constants

1 Introduction

The Titchmarsh divisor problem concerns the asymptotic behaviour of the sum $\sum_{p\le x}\tau(p+a)$, as a function of x, where p denotes a rational prime, $\tau(n):=\#\{d\ge 1: d\mid n\}$ denotes the divisor function, and a denotes a fixed integer. The study of this sum has spanned over five decades and is intimately related to some of the most significant research in analytic number theory (see [6,15,21,30,37], and [33]). By results about primes in arithmetic progressions which have become standard, we now know that, as $x\to\infty$,

$$\sum_{p\le x}\tau(p+a)\sim\frac{\zeta(2)\zeta(3)}{\zeta(6)}\prod_{\ell\mid a}\left(1-\frac{\ell}{\ell^2-\ell+1}\right)x, \tag{1}$$

where $\zeta(\cdot)$ denotes the Riemann zeta function and ℓ denotes a rational prime.

Divisor problems similar to that of Titchmarsh may be formulated in other settings, such as the setting of elliptic curves, as we now describe. Let $E/\mathbb{Q}$ be an elliptic curve defined over the field of rational numbers. For a prime p of good reduction for E, let $\overline{E}/\mathbb{F}_p$ be the reduction of E modulo p. From the basic theory of elliptic curves (see [36, Chap. III, §6]), it is known that the group $\overline{E}(\mathbb{F}_p)$ may be expressed as a product of two cyclic groups,

$$\overline{E}(\mathbb{F}_p) \simeq \mathbb{Z}/d_{1,p}\mathbb{Z} \times \mathbb{Z}/d_{2,p}\mathbb{Z},$$

where $d_{1,p} = d_{1,p}(E), d_{2,p} = d_{2,p}(E)$ are uniquely determined positive integers satisfying $d_{1,p} \mid d_{2,p}$. Determining the asymptotic behaviour of sums over $p \leq x$ of arithmetic functions evaluated at the elementary divisors $d_{1,p}$ and $d_{2,p}$ may be viewed as Titchmarsh divisor problems for elliptic curves. Such problems unravel striking similarities, but also intriguing contrasts, to the original Titchmarsh divisor problem, as illustrated in [1,2,7, 8,13,14,17,18,28,29,32], and [41].

The focus of our paper is on the constants emerging in the following three Titchmarsh divisor problems for elliptic curves. In all the expressions below, the letters p and ℓ denote primes, with p being a prime of good reduction for the given elliptic curve.

Conjecture 1 (Kowalski [29, Sect. 3.2])
Let $E/\mathbb{Q}$ be an elliptic curve. Then, as $x \to \infty$,

$$\sum_{p \leq x} d_{1,p} \sim C_{d_1,non\text{-}CM}(E)\ \mathrm{li}(x), \quad \text{if } E \text{ is without complex multiplication,} \tag{2}$$

$$\sum_{p \leq x} d_{1,p} \sim C_{d_1,CM}(E)\, x, \quad \text{if } E \text{ is with complex multiplication,} \tag{3}$$

where

$$C_{d_1,non\text{-}CM}(E) := \sum_{m \geq 1} \frac{\phi(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]}, \tag{4}$$

$$C_{d_1,CM}(E) := \lim_{\sigma \to 0^+} \sigma \sum_{m \geq 1} \frac{\phi(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]}\, m^{-\sigma}, \tag{5}$$

with $\phi(m) := \#\{1 \leq k \leq m : (k, m) = 1\}$ denoting the Euler function of m, $\mathbb{Q}(E[m])$ denoting the m-division field of E, and $\mathrm{li}(x) := \int_2^x \frac{1}{\log t}\, dt$ denoting the standard logarithmic integral.

Conjecture 2 (Akbary-Ghioca [2, Sect. 1])
Let $E/\mathbb{Q}$ be an elliptic curve, with or without complex multiplication. Then, as $x \to \infty$,

$$\sum_{p \leq x} \tau(d_{1,p}) \sim C_{\tau(d_1)}(E)\ \mathrm{li}(x), \tag{6}$$

where

$$C_{\tau(d_1)}(E) := \sum_{m \geq 1} \frac{1}{[\mathbb{Q}(E[m]) : \mathbb{Q}]}. \tag{7}$$

We note that in the above definitions of the constants C_{d_1}, $C_{\tau(d_1)}$, as well as in those of the forthcoming constants $C_{d_1,\mathrm{CM}}(O)$, $C_{\tau(d_1),\mathrm{CM}}(O)$, $B_{d_1,\mathrm{CM}}(O)$, $B_{\tau(d_1),\mathrm{CM}}(O)$, the notation d_1 and $\tau(d_1)$ does not refer to specific integers and is purely symbolic; regardless of coinciding values of $d_{1,p}$ and $\tau(d_{1,p})$, the definitions of C_{d_1}, $C_{\tau(d_1)}$, as well as their variations, are distinct and independent. We also note that a natural question is whether a conjecture similar to Conjecture 2 may be formulated regarding the behaviour of $\tau(d_{2,p})$. Since we have not found such an investigation in the literature, we relegate it to future research.

Conjecture 3 (Freiberg–Kurlberg [17, Sect. 1])
Let $E/\mathbb{Q}$ be an elliptic curve, with or without complex multiplication. Then, as $x \to \infty$,

$$\sum_{p \le x} d_{2,p} \sim \frac{1}{2} C_{d_2}(E)\ \mathrm{li}\left(x^2\right), \tag{8}$$

where

$$C_{d_2}(E) := \sum_{m \ge 1} \frac{(-1)^{\omega(m)} \phi(\mathrm{rad}\, m)}{m[\mathbb{Q}(E[m]) : \mathbb{Q}]}, \tag{9}$$

with $\omega(m) := \sum_{\ell \mid m} 1$ denoting the number of distinct prime factors of m and $\mathrm{rad}(m) := \prod_{\ell \mid m} \ell$ denoting the product of distinct prime factors of m.

The constants $C_{d_1,\text{non-CM}}(E)$, $C_{d_1,\mathrm{CM}}(E)$, $C_{\tau(d_1)}(E)$, and $C_{d_2}(E)$ appearing in these conjectures are deeply related to the arithmetic of the elliptic curve $E/\mathbb{Q}$ and are heuristically derived via the Chebotarev density theorem by considering the action of a Frobenius element at p on $E[m]$.

Conjecture 1 was investigated by Freiberg and Pollack [18] in the case that E has complex multiplication; precisely, they proved that $\sum_{p \le x} d_{1,p} \asymp_E x$. A similar result is not yet known if E does not have complex multiplication, even under the Generalized Riemann Hypothesis. Conjecture 2 was investigated by Akbary and Ghioca [2]; precisely, they proved (6) under the Generalized Riemann Hypothesis if E is without complex multiplication and unconditionally if E is with complex multiplication. Conjecture 3 was investigated by Freiberg and Kurlberg [17]; precisely, they proved (8) under the Generalized Riemann Hypothesis if E is without complex multiplication, and unconditionally if E is with complex multiplication. The proofs of the main results in [2] and [17] rely upon the methods of [8] and have been refined in several subsequent works, including [1], [13,14,28], and [41].

Using ideas originating in [16], Conjectures 1–3 may also be investigated on average over elliptic curves in families. For any elliptic curve $E/\mathbb{Q}$, there is a unique Weierstrass equation $E_{a,b} : Y^2 = X^3 + aX + b$ with coefficients $a, b \in \mathbb{Z}$ satisfying that $\gcd(a^3, b^2)$ is 12-th power free and $E_{a,b} \simeq_{\mathbb{Q}} E$. We will refer to a Weierstrass model $E_{a,b}$ of this form as the distinguished model of E. We define the discriminant and height of E by

$$\Delta(E) := -16(4a^3 + 27b^2) \neq 0, \quad H(E) := \max\left\{|a|^3, |b|^2\right\}, \tag{10}$$

where the integers a and b are those associated to the distinguished model $E_{a,b}$ of E. Finally, for parameters $A, B > 2$, we consider the family $\mathcal{C}(A, B)$ of $\mathbb{Q}$-isomorphism classes

of elliptic curves defined by distinguished models $E_{a,b}$ with $|a| \le A$, $|b| \le B$. Our goal is to average the Titchmarsh divisor sums of Conjectures 1–3 over $E \in \mathcal{C}(A,B)$.

In this context, it is natural to consider the following universal versions of the constants $C_{d_1,\text{non-CM}}(E)$, $C_{\tau(d_1)}(E)$, and $C_{d_2}(E)$,

$$C_{d_1} := \sum_{m\ge 1} \frac{\phi(m)}{|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|} = \prod_{\ell}\left(1+\frac{\ell^2}{(\ell^2-1)(\ell^3-1)}\right) = 1.25844835\ldots, \quad (11)$$

$$C_{\tau(d_1)} := \sum_{m\ge 1} \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|} = \prod_{\ell}\left(1+\frac{\ell^3}{(\ell-1)(\ell^2-1)(\ell^4-1)}\right) = 1.2059016\ldots, \quad (12)$$

$$C_{d_2} := \sum_{m\ge 1} \frac{(-1)^{(\omega(m))}\phi(\operatorname{rad}(m))}{m|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|} = \prod_{\ell}\left(1+\frac{\ell^3}{(\ell^2-1)(\ell^5-1)}\right) = 0.89922825\ldots, \quad (13)$$

together with the constants

$$C_{d_1,\text{CM}}(O) := \lim_{\sigma\to 0^+} \sigma \sum_{m\ge 1} \frac{\phi(m)}{|(O/mO)^\times|} m^{-\sigma},$$

$$C_{\tau(d_1),\text{CM}}(O) := \sum_{m\ge 1} \frac{1}{|(O/mO)^\times|},$$

$$B_{d_1,\text{CM}}(O) := |\operatorname{Aut}(O)| L(1,\chi_O) \times \min_{\substack{E'/\mathbb{Q} \\ \operatorname{End}_{\overline{\mathbb{Q}}}(E')\simeq O}} \left\{ \prod_{\ell \mid m_{E'}} \left(1-\frac{1}{\ell}\right)^{-1} \left(\sum_{m \mid m_{E'}} \frac{\phi(m)}{[K(E'[m]):K]} \right) \right\},$$

$$B_{\tau(d_1),\text{CM}}(O) := |\operatorname{Aut}(O)| \min_{\substack{E'/\mathbb{Q} \\ \operatorname{End}_{\overline{\mathbb{Q}}}(E')\simeq O}} \left\{ \sum_{m\ge 1} \frac{1}{[K(E'[m]):K]} \right\}$$

defined for each imaginary quadratic order O of class number 1, with field of fractions K, where for any elliptic curve $E'/\mathbb{Q}$ with CM by O, the integer $m_{E'}$ is as in Theorem 11 of Sect. 2.3. The convergence of these four latter constants is explained in the course of the proof of part (i) of Theorem 4.

The *universal constants* C_{d_1}, $C_{\tau(d_1)}$, C_{d_2} turn out to be the *average constants* for Conjectures 1–3, in the following sense. In [1, Cor 1.6], Akbary and Felix proved that for any $c > 1$ and $x > e$, there exists $c_1 > 0$ such that, for any $A = A(x)$, $B = B(x)$ with $A, B > \exp(c_1(\log x)^{1/2})$ and $AB > x(\log x)^{4+2c}$, we have

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{E\in\mathcal{C}(A,B)} \sum_{\substack{p\le x \\ p\nmid\Delta(E)}} \tau(d_{1,p}(E)) = C_{\tau(d_1)} \operatorname{li}(x) + \mathrm{O}\left(\frac{x}{(\log x)^c}\right), \quad (14)$$

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{E\in\mathcal{C}(A,B)} \sum_{\substack{p\le x \\ p\nmid\Delta(E)}} d_{2,p}(E) = \frac{1}{2} C_{d_2} \operatorname{li}(x^2) + \mathrm{O}\left(\frac{x^2}{(\log x)^c}\right). \quad (15)$$

These results confirm Conjectures 2–3 on average. Conjecture 1 is also expected to hold on average; that is, for suitably large $A = A(x)$, $B = B(x)$, we expect

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{\substack{E\in\mathcal{C}(A,B) \\ E \text{ without CM}}} \sum_{\substack{p\le x \\ p\nmid\Delta(E)}} d_{1,p}(E) = C_{d_1} \operatorname{li}(x) + \mathrm{o}\left(\frac{x}{\log x}\right). \quad (16)$$

While this average is open, Akbary and Felix proved related results supporting it (see [1, Remark 1.7]).

In this paper we investigate the constants $C_{d_1,\text{non-CM}}(E)$, $C_{d_1,\text{CM}}(E)$, $C_{\tau(d_1)}(E)$, and $C_{d_2}(E)$, in relation to the universal constants C_{d_1}, $C_{\tau(d_1)}$, C_{d_2}, $C_{d_1,\text{CM}}(O)$, $C_{\tau(d_1),\text{CM}}(O)$, $B_{d_1,\text{CM}}(O)$, $B_{\tau(d_1),\text{CM}}(O)$. Specifically, using properties of the division fields of $E/\mathbb{Q}$, which we derive from the celebrated open image theorems for elliptic curves with complex multiplication (due to Weil in the adelic setting and to Deuring in the classical setting), respectively without complex multiplication (due to Serre), we prove the following theorem, which gives upper and lower bounds for the conjectural constants under consideration.

Theorem 4 *Let $E/\mathbb{Q}$ be an elliptic curve.*

(i) *Assume that* $\text{End}_{\overline{\mathbb{Q}}}(E) \simeq O \not\simeq \mathbb{Z}$. *Then, denoting by K the field of fractions of O, by G_K the absolute Galois group of K, by* $\widehat{O} := \varprojlim_m O/mO$, *and by $\varphi_E : G_K \longrightarrow \widehat{O}^\times$ the absolute Galois representation associated to E (as described in Sect. 2.1 below),*

$$\begin{aligned} 0 &< \frac{1}{2}\, C_{d_1,CM}(O) \le C_{d_1,CM}(E) \\ &\le \min\left\{B_{d_1,CM}(O), \left[\hat{O}^\times : \varphi_E(G_K)\right] C_{d_1,CM}(O)\right\} \ll 1, \\ 0 &< \frac{1}{2}\, C_{\tau(d_1),CM}(O) \le C_{\tau(d_1)}(E) \\ &\le \min\left\{B_{\tau(d_1),CM}(O), \left[\hat{O}^\times : \varphi_E(G_K)\right] C_{\tau(d_1),CM}(O)\right\} \ll 1. \end{aligned}$$

(ii) *Assume that* $\text{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. *There exists positive absolute constants β and γ such that*

$$\begin{aligned} 0 < C_{d_1} \le C_{d_1,non\text{-}CM}(E) &\ll \left(\max\left\{1, \log H(E)\right\}\right)^\gamma, \\ 0 < C_{\tau(d_1)} \le C_{\tau(d_1)}(E) &\ll \left(\log\log\left(\max\left\{6, H(E)\max\{1, \log H(E)\}^\gamma\right\}\right)\right)^\beta, \end{aligned}$$

where $H(E)$ is the height of the distinguished model of E, as in (10).

The $\ll$-constants are absolute.

Possible uniform upper bounds for $C_{d_1,\text{non-CM}}(E)$ and $C_{\tau(d_1)}(E)$ will be addressed in Remark 21 of Sect. 2.5. Note also that while the upper bounds for $C_{\tau(d_1)}(E)$ of Theorem 4 also hold for $C_{d_2}(E)$, uniform lower and upper bounds for this constant were already addressed by Freiberg and Kurlberg [17]. Specifically, they prove that, for any elliptic curve $E/\mathbb{Q}$,

$$0 < C_{d_2}(E) < 1.$$

Additionally, they prove that

$$\sum_{m\ge 1} \frac{\mu(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} \le C_{d_2}(E) \le \frac{1}{2}\left(1 + \sum_{m\ge 1} \frac{\mu(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]}\right),$$

with $\mu(m)$ denoting the Möbius function of m. For these bounds, note that it is known that the constant $\sum_{m\ge 1} \frac{\mu(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]}$ may be zero, which happens exactly in the case $\mathbb{Q}(E[2]) = \mathbb{Q}$.

Next, by focusing on elliptic curves with maximal Galois action on their torsion points, we prove explicit formulae for our Titchmarsh divisor constants:

Theorem 5 *Let $E/\mathbb{Q}$ be a Serre curve, that is, an elliptic curve over $\mathbb{Q}$ whose adelic Galois representation has maximal image. Let*

$$m_E = \begin{cases} 2\left|\Delta_{\mathrm{sf}}(E)\right| & \text{if } \Delta_{\mathrm{sf}}(E) \equiv 1 (\mathrm{mod}\ 4), \\ 4\left|\Delta_{\mathrm{sf}}(E)\right| & \text{otherwise,} \end{cases} \tag{17}$$

where $\Delta_{\mathrm{sf}}(E)$ denotes the squarefree part of the discriminant of any Weierstrass model of E. Then

$$C_{d_1,non-CM}(E) = C_{d_1}\left(1 + \frac{1}{m_E^3}\prod_{\ell \mid m_E}\frac{1}{(1-\ell^{-2})(1-\ell^{-3})+\ell^{-3}}\right), \tag{18}$$

$$C_{\tau(d_1)}(E) = C_{\tau(d_1)}\left(1 + \frac{1}{m_E^4}\prod_{\ell \mid m_E}\frac{1}{(1-\ell^{-1})(1-\ell^{-2})(1-\ell^{-4})+\ell^{-4}}\right), \tag{19}$$

$$C_{d_2}(E) = C_{d_2}\left(1 + \frac{(-1)^{\omega(m_E)}}{m_E^4}\prod_{\ell \mid m_E}\frac{1}{(1-\ell^{-2})(1-\ell^{-5})-\ell^{-4}}\right). \tag{20}$$

Finally, we use the above two results to prove that the average of the individual constants gives rise to the universal constant:

Theorem 6 *For any $A(x), B(x) > 2$, tending to infinity with x such that the ratios of their logarithms remain bounded, we have*

$$\lim_{x\to\infty}\frac{1}{|\mathcal{C}(A(x),B(x))|}\sum_{E\in\mathcal{C}(A(x),B(x))} C(E) = C. \tag{21}$$

Here, the pair $(C(E), C)$ is, respectively, $(C_{d_1}(E), C_{d_1})$, $(C_{\tau(d_1)}(E), C_{\tau(d_1)})$, and $(C_{d_2}(E), C_{d_2})$, with $C_{d_1}(E)$ denoting $C_{d_1,non\text{-}CM}(E)$ if E is without complex multiplication, and $C_{d_1,CM}(E)$ if E is with complex multiplication.

Remark 7

(i) The constant γ occurring in Theorem 4 is known as the Masser-Wüstholz constant, originates in [31], and was studied computationally in [27]. The constant m_E occurring in Theorem 5 was first introduced in [24] in relation to Serre's open image theorem from [35]. In Sect. 2, we will revisit its original definition (see Theorem 10) and we will confirm that it satisfies Eq. (17) above (see Proposition 17).

(ii) It is a difficult problem to calculate the constants $C_{d_1,\text{non-CM}}(E)$, $C_{d_1,\text{CM}}(E)$, $C_{\tau(d_1)}(E)$, and $C_{d_2}(E)$ for an arbitrary elliptic curve $E/\mathbb{Q}$. However, the explicit formulae of Theorem 5 can be used to calculate these constants for Serre curves and to study Conjectures 1–3 numerically, as done in [9]. Numerical computations of the constants $C_{d_1,\text{CM}}(O)$, $C_{\tau(d_1),\text{CM}}(O)$, $B_{d_1,\text{CM}}(O)$, $B_{\tau(d_1),\text{CM}}(O)$, $\left[\hat{O}^\times : \varphi_E(G_K)\right]$ occurring in part (i) of Theorem 4 are also doable and will be pursued in a different project.

(iii) The universal constants C_{d_1} and $C_{\tau(d_1)}$ provide *strict* lower bounds for the constants $C_{d_1,\text{non-CM}}(E)$ and $C_{\tau(d_1)}(E)$ for any elliptic curve $E/\mathbb{Q}$. Furthermore, Theorem 5 shows that these lower bounds are sharp, since one may take a sequence of Serre curves E_i with m_{E_i} approaching infinity, and deduce that $C_{d_1,\text{non-CM}}(E_i)$ approaches

C_{d_1} (respectively $C_{\tau(d_1)}(E_i)$ approaches $C_{\tau(d_1)}$). Regarding the constant of Conjecture 3, Theorem 5 implies that $C_{d_2}(E)$ is never equal to C_{d_2} when E is a Serre curve. In summary, the constants $C_{d_1,\text{non-CM}}(E)$ and $C_{\tau(d_1)}(E)$ of Conjectures 1 and 2 are never equal to the universal constants C_{d_1}, and $C_{\tau(d_1)}$, and the constant $C_{d_2}(E)$ is never equal to the universal constant C_{d_2} when E is a Serre curve. This is in contrast to other questions about reductions of elliptic curves, such as Koblitz's Conjecture about the primality of $\left|\overline{E}(\mathbb{F}_p)\right|$.

(iv) In Sect. 5, we will actually prove a stronger result than (21) of Theorem 6 by bounding, from above,

$$\frac{1}{|\mathcal{C}(A,B)|}\sum_{E\in\mathcal{C}(A,B)}\left|C(E)-C\right|^n$$

for any integer $n \geq 1$ and for any $A, B > 2$; see equations (48), (49), (50), and (51).

(v) Theorem 6 contributes to the research on averages of constants arising in the study of *reductions* of elliptic curves over $\mathbb{Q}$, as pursued in [3–5,10], and [23]. It also complements research on averages of constants arising in the study of *all* elliptic curves over the field $\mathbb{F}_p$, as pursued in [12,19,22,26], and [38]. The connection between the former "global" viewpoint and the latter "local" viewpoint involves the question of to what extent the reductions of a fixed elliptic curve $E/\mathbb{Q}$ behave like random elliptic curves over $\mathbb{F}_p$. In our average approach we follow the methods of [23] and realize the global-to-local connection via Theorem 5 and Jones' result that most elliptic curves over $\mathbb{Q}$ are Serre curves [24]. A conceptual reason of why a result such as the one of Theorem 6 should hold is given in Remark 23 at the end of Sect. 5.

Notation Throughout the paper, we follow the following standard notation.

- The letters p and ℓ denote rational primes. The letters d, k, m, n denote rational integers. The letters ϕ, τ, ω denote the Euler function, the divisor function, and the prime factor counting function. For an integer m, $|m|$ denotes its absolute value, $\text{rad}(m)$ its radical, and $v_\ell(m)$ its valuation at a prime ℓ. For nonzero integers m, n, $m \mid n^\infty$ denotes that every prime divisor of m divides n.
- For two functions $f, g : D \longrightarrow \mathbb{R}$, with $D \subseteq \mathbb{C}$ and g positive, we write $f(x) = \text{O}(g(x))$ or $f(x) \ll g(x)$ if there is a positive constant c_1 such that $|f(x)| \leq c_1 g(x)$ for all $x \in D$. If c_1 depends on another specified constant c_2, we may write $f(x) = \text{O}_{c_2}(g(x))$ or $f(x) \ll_{c_2} g(x)$. If $c := \lim_{x\to\infty} \frac{f(x)}{g(x)}$ exists, we write $f(x) \sim c\, g(x)$.
- For a field K, we write $\overline{K}$ for a fixed algebraic closure and G_K for the absolute Galois group $\text{Gal}\left(\overline{K}/K\right)$.

2 Generalities about elliptic curves

In this section, we review the main properties of elliptic curves needed in the proofs of our main results. While many of these properties are standard (Theorems 8–11), the ones towards the end of the section (Corollary 13–Theorem 19) are less known, but crucial to our approach.

2.1 General notation

For an elliptic curve $E/\mathbb{Q}$, we use the following notation. We denote by $j = j(E)$ the j-invariant of E. We denote by $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ and $\mathrm{Aut}_{\overline{\mathbb{Q}}}(E)$ the endomorphism ring and the automorphism group of E over $\overline{\mathbb{Q}}$. We denote by $E(\mathbb{Q})$ and $E(\overline{\mathbb{Q}})$ the groups of $\mathbb{Q}$-rational and $\overline{\mathbb{Q}}$-rational points of E, and by $E(\mathbb{Q})_{\mathrm{tors}}$ and $E_{\mathrm{tors}} := E(\overline{\mathbb{Q}})_{\mathrm{tors}}$ their respective torsion subgroups.

For an integer $m \geq 1$, we denote by $E[m] := E(\overline{\mathbb{Q}})[m]$ the group of m-division points of $E(\overline{\mathbb{Q}})$. This has the structure of a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2, with a $\mathbb{Z}/m\mathbb{Z}$-linear action of the absolute Galois group $G_{\mathbb{Q}}$. Thus, fixing an isomorphism $(\mathbb{Z}/m\mathbb{Z})^2 \to E[m]$, which amounts to choosing a $\mathbb{Z}/m\mathbb{Z}$-basis for $E[m]$, we obtain a Galois representation

$$\varphi_{E,m} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Note that the m-division field $\mathbb{Q}(E[m])$ of E, defined by adjoining to $\mathbb{Q}$ the x and y coordinates of the points in $E[m]$, satisfies

$$\mathbb{Q}(E[m]) = \overline{\mathbb{Q}}^{\mathrm{Ker}\,\varphi_{E,m}} \text{ and } [\mathbb{Q}(E[m]) : \mathbb{Q}] = \left|\mathrm{Im}(\varphi_{E,m})\right|.$$

Choosing compatible bases for all $E[m]$, we form the inverse limit over m ordered by divisibility and obtain a continuous adelic Galois representation

$$\varphi_E : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}), \tag{22}$$

where $\hat{\mathbb{Z}} := \varprojlim_m \mathbb{Z}/m\mathbb{Z}$.

2.2 Endomorphisms

Theorem 8 ([11, Thm 7.30 and p. 261]) *Let $E/\mathbb{Q}$ be an elliptic curve. The following statements hold.*

(i) *Either* $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$, *in which case we say that E is without complex multiplication (without CM), or* $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ *is an order O in an imaginary quadratic field K, in which case we say that E is with complex multiplication (with CM) by K.*

(ii) *Furthermore, if* $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq O \not\simeq \mathbb{Z}$, *then O has class number* 1 *and* $j(E) \in \{j_1{:=}0, j_2{:=}1728, j_3, \ldots, j_{13}\}$ *is one of* 13 *possible j-invariants.*

Note that two elliptic curves of the same j-invariant, while isomorphic over $\overline{\mathbb{Q}}$, may fail to be isomorphic over $\mathbb{Q}$; we call such curves twists of each other. An explicit computation of the Galois cohomology group classifying twists [36, Chap. 3, Cor. 10.2] gives the following:

Lemma 9 *Let $E/\mathbb{Q}$, $E'/\mathbb{Q}$ be elliptic curves with $j(E) = j(E')$. Then there exists an extension $L/\mathbb{Q}$ with*

$$[L : \mathbb{Q}] \leq |\,\mathrm{Aut}_{\overline{\mathbb{Q}}}(E)| = \begin{cases} 6 & \text{if } j(E) = 0, \\ 4 & \text{if } j(E) = 1728, \\ 2 & \text{else,} \end{cases}$$

such that after base change to L, $E_L \simeq (E')_L$.

2.3 Open image theorems

Theorem 10 ([35]) *Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. Then φ_E has open image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, that is, $|\mathrm{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})| < \infty$. In particular, there exists a smallest integer $m_E \geq 1$ such that for any integer $m = m_1 m_2$ with $m_1 \mid m_E^\infty$ and $\gcd(m_2, m_E) = 1$,*

$$\varphi_{E,m}(G_{\mathbb{Q}}) \simeq \mathrm{pr}_{m_1,d}^{-1}(\varphi_{E,d}(G_{\mathbb{Q}})) \times \mathrm{GL}_2(\mathbb{Z}/m_2\mathbb{Z}),$$

where $d := \gcd(m_1, m_E)$, and $\mathrm{pr}_{m_1,d} : \mathrm{GL}_2(\mathbb{Z}/m_1\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$ is the natural projection.

If $E/\mathbb{Q}$ has complex multiplication by an order O in an imaginary quadratic field K, then φ_E is constrained to respect the extra O-module structure. The projective limit $\widehat{O} := \varprojlim_m O/mO$ is a free $\hat{\mathbb{Z}}$-module of rank 2 and $K(E_{\mathrm{tors}}) = \mathbb{Q}(E_{\mathrm{tors}})$ is a free $\widehat{O}$-module of rank 1 with an $\widehat{O}$-linear action of G_K. Therefore $\varphi_E|_{G_K}$ factors:

$$\begin{array}{ccc} G_K & \xrightarrow{\varphi_E|_{G_K}} & \mathrm{GL}_2(\hat{\mathbb{Z}}) \\ & \searrow \quad \nearrow & \\ & \widehat{O}^\times & \end{array}$$

Theorem 11 ([39,40]) *Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq O \not\simeq \mathbb{Z}$ and let $K := O \otimes_{\mathbb{Z}} \mathbb{Q}$ be the associated CM field. Then the representation*

$$\varphi_E|_{G_K} : G_K \longrightarrow \widehat{O}^\times \tag{23}$$

has open image in $\widehat{O}^\times$, that is, $\left|\widehat{O}^\times : \varphi_E(G_K)\right| < \infty$. In particular, there exists a smallest integer $m_E \geq 1$ such that for any integer $m = m_1 m_2$ with $m_1 \mid m_E^\infty$ and $\gcd(m_2, m_E) = 1$,

$$\varphi_{E,m}(G_K) \simeq \mathrm{pr}_{m_1,d}^{-1}(\varphi_{E,d}(G_K)) \times (O/m_2O)^\times,$$

where $d := \gcd(m_1, m_E)$, and $\mathrm{pr}_{m_1,d} : (O/m_1O)^\times \longrightarrow (O/dO)^\times$ is the natural projection.

For potential future applications, we record below a uniform bound for $\left[\hat{O}^\times : \varphi_E(G_K)\right]$:

Proposition 12 *Let O be an imaginary quadratic order associated to some elliptic curve $E/\mathbb{Q}$ (i.e. $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq O \not\simeq \mathbb{Z}$) and let $K := O \otimes_{\mathbb{Z}} \mathbb{Q}$ be the associated CM field. Then, for any other elliptic curve E' over $\mathbb{Q}$ which satisfies $\mathrm{End}_{\overline{\mathbb{Q}}}(E') \simeq O$, we have*

$$\frac{1}{\left|\mathrm{Aut}(O)\right|}\left[\widehat{O}^\times : \varphi_E(G_K)\right] \leq \left[\widehat{O}^\times : \varphi_{E'}(G_K)\right] \leq \left|\mathrm{Aut}(O)\right|\left[\widehat{O}^\times : \varphi_E(G_K)\right].$$

Proof. Lemma 9 implies that there is an isomorphism $E \longrightarrow E'$ defined over a number field L satisfying $[L : \mathbb{Q}] \leq |\mathrm{Aut}(O)|$. Thus, E_{tors} and E'_{tors} are isomorphic as G_L-modules, and the proposition follows. □

A useful consequence of these open image theorems is:

Corollary 13 *Let $E/\mathbb{Q}$ be an elliptic curve and let m_E be as in Theorem 10, respectively Theorem 11. Let $\ell \mid m_E$ and $d \mid m_E$ with $\ell \nmid d$ (recall that ℓ denotes a rational prime).*

(i) *If $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$, then*

$$\left[\mathbb{Q}\left(E\left[\ell^{\nu_\ell(m_E)+\delta}d\right]\right) : \mathbb{Q}\right] = \ell^{4\delta}\left[\mathbb{Q}\left(E\left[\ell^{\nu_\ell(m_E)}d\right]\right) : \mathbb{Q}\right] \quad \forall\, \delta \in \mathbb{N}.$$

(ii) *If* $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$, *then*

$$\left[K\left(E\left[\ell^{\nu_\ell(m_E)+\delta}d\right]\right):K\right] = \ell^{2\delta}\left[K\left(E\left[\ell^{\nu_\ell(m_E)}d\right]\right):K\right] \quad \forall\, \delta \in \mathbb{N},$$

where $K \simeq \mathrm{End}_{\overline{\mathbb{Q}}}(E) \otimes \mathbb{Q}$.

Proof. This follows from Theorems 10 and 11, with $m := \ell^{\nu_\ell(m_E)+\delta}d$, since when $\nu_\ell(m_E) > 0$,

$$\#\,\mathrm{Ker}\left(\mathrm{GL}_2\left(\mathbb{Z}/\ell^{\nu_\ell(m_E)+\delta}d\mathbb{Z}\right) \to \mathrm{GL}_2\left(\mathbb{Z}/\ell^{\nu_\ell(m_E)}d\mathbb{Z}\right)\right) = \ell^{4\delta},$$
$$\#\,\mathrm{Ker}\left(\left(O/\ell^{\nu_\ell(m_E)+\delta}dO\right)^\times \longrightarrow \left(O/\ell^{\nu_\ell(m_E)}dO\right)^\times\right) = \ell^{2\delta}.$$

□

In applications, it is desirable to explicitly bound m_E in terms of the size of the coefficients of E.

Proposition 14 *Let* $E/\mathbb{Q}$ *be an elliptic curve such that* $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. *Let* m_E *be as in Theorem 10 and let* $H(E)$ *be the height of the distinguished model of* E. *Then there exists a positive absolute constant* γ *such that*

$$|\,\mathrm{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})| \ll \left(\max\left\{1, \log H(E)\right\}\right)^\gamma,$$
$$m_E \ll H(E)\left(\max\left\{1, \log H(E)\right\}\right)^\gamma,$$

where the $\ll$*-constants are absolute.*

Proof. Denote by $\Delta(E)$ the discriminant of the distinguished model of E. The bound $m_E \le 2\,|\,\mathrm{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})|\ \mathrm{rad}(|\Delta(E)|)$ follows from the main result in [25], while the bound $|\,\mathrm{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})| \ll \max\{1, \log H(E)\}^\gamma$ follows from [42, Theorem 1.1] (see also [31]). The bound $\mathrm{rad}(|\Delta(E)|) \ll H(E)$ is straightforward. □

2.4 Serre curves

Lemma 15 ([35, Sect. 5.5]) *Let* $E/\mathbb{Q}$ *be an elliptic curve. Then* $\left|\mathrm{GL}_2\left(\hat{\mathbb{Z}}\right) : \varphi_E(G_{\mathbb{Q}})\right| \ge 2$.

In particular, no elliptic curve $E/\mathbb{Q}$ satisfies $\left|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \varphi_{E,m}(G_{\mathbb{Q}})\right| = 1$ for all integers $m \ge 1$. Rather, the best we can hope for is captured in the following definition:

Definition 16 An elliptic curve $E/\mathbb{Q}$ is called a **Serre curve** if $\left|\mathrm{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})\right| = 2$, or, equivalently, if

$$\left|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \varphi_{E,m}(G_{\mathbb{Q}})\right| \le 2 \quad \forall m \ge 1. \tag{24}$$

Given $E/\mathbb{Q}$ and denoting by $\Delta_{\mathrm{sf}}(E)$ the squarefree part of the discriminant $\Delta(E)$ of a (equivalently any) Weierstrass model for E, in particular of the distinguished model, the bound in Lemma 15 arises from the containments

$$\mathbb{Q}\left(\sqrt{\Delta(E)}\right) \subseteq \mathbb{Q}\left(E[2]\right), \qquad \mathbb{Q}\left(\sqrt{\Delta(E)}\right) \subseteq \mathbb{Q}\left(\zeta_{|d_E|}\right) \subseteq \mathbb{Q}\left(E[|d_E|]\right), \tag{25}$$

where

$$d_E := \operatorname{disc}\left(\mathbb{Q}\left(\sqrt{\Delta(E)}\right)\right) = \begin{cases} \Delta_{\mathrm{sf}}(E) & \text{if } \Delta_{\mathrm{sf}}(E) \equiv 1 (\mathrm{mod}\, 4), \\ 4\Delta_{\mathrm{sf}}(E) & \text{otherwise.} \end{cases}$$

The existence of an integer d_E satisfying (25) is guaranteed by the Kronecker-Weber Theorem, since $\mathbb{Q}\left(\sqrt{\Delta(E)}\right)$ is abelian over $\mathbb{Q}$; this value of d_E minimizes $|d_E|$ subject to (25).) It follows that

$$\varphi_E(G_{\mathbb{Q}}) \subseteq \{g \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : \epsilon(g) = \chi_E(g)\}, \tag{26}$$

where the two maps

$$\epsilon : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3 \to \{\pm 1\},$$
$$\chi_E : \mathrm{GL}_2(\hat{\mathbb{Z}}) \to \hat{\mathbb{Z}}^\times \to (\mathbb{Z}/|d_E|\mathbb{Z})^\times \to \{\pm 1\}$$

are defined as follows: ϵ is the projection modulo 2 followed by the signature character on the permutation group S_3 (which is also the unique non-trivial multiplicative character on $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$); χ_E is the determinant map, followed by the reduction modulo $|d_E|$, and then followed by the Kronecker symbol $\left(\frac{d_E}{\cdot}\right)$.

Proposition 17 *Let $E/\mathbb{Q}$ be a Serre curve. Then:*

(i) $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$*;*
(ii) $E(\mathbb{Q})_{\mathrm{tors}}$ *is trivial;*
(iii) *The integer m_E introduced in Theorem 10 satisfies*

$$m_E = \begin{cases} 2\left|\Delta_{\mathrm{sf}}(E)\right| & \text{if } \Delta_{\mathrm{sf}}(E) \equiv 1 (\mathrm{mod}\, 4), \\ 4\left|\Delta_{\mathrm{sf}}(E)\right| & \text{otherwise,} \end{cases} \tag{27}$$

where $\Delta_{\mathrm{sf}}(E)$ denotes the squarefree part of $\Delta(E)$;
(iv) *For any integer $m \geq 1$,*

$$[\mathbb{Q}(E[m]) : \mathbb{Q}] = \begin{cases} |\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})| & \text{if } m_E \nmid m, \\ \frac{1}{2}|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})| & \text{otherwise.} \end{cases} \tag{28}$$

Proof. (i) We proceed by contradiction. Suppose that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq O \not\simeq \mathbb{Z}$ and let $K = \mathrm{Frac}\, O$. For an element $a \in O \backslash \mathbb{Z}$, there exists a rational prime ℓ such that the characteristic polynomial of the action of a on $E[\ell]$ has two distinct roots modulo ℓ. The action of G_K preserves the two eigenspaces of a mod ℓ, which implies that, written relative to an eigenbasis, we have

$$\varphi_{E,\ell}(G_K) \leq \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\} < \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

We thus have $\left|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \varphi_{E,\ell}(G_{\mathbb{Q}})\right| \geq \ell(\ell+1) > 2$, contradicting (24).

(ii) A nontrivial ℓ-torsion point would similarly give $\left|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \varphi_{E,\ell}(G_{\mathbb{Q}})\right| \geq (\ell+1)(\ell-1) > 2$, contradicting (24).

(iii) Since the subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ where χ_E and ϵ agree is already of index 2, and since E is a Serre curve, we must have equality in (26). The subgroup defined therein is determined by its image at level

$$m_E = \mathrm{lcm}(2, |d_E|) = \begin{cases} 2|\Delta_{\mathrm{sf}}(E)| & \text{if } \Delta_{\mathrm{sf}}(E) \equiv 1 (\mathrm{mod}\, 4), \\ 4|\Delta_{\mathrm{sf}}(E)| & \text{otherwise,} \end{cases}$$

verifying (17) and (27).

(iv) Let $d \mid m_E$ and denote by $\mathrm{pr}_{m_E,d} : \mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z})$ the canonical projection. Since $\left|\mathrm{GL}_2(\mathbb{Z}/m_E\mathbb{Z}) : \varphi_{E,m_E}(G_{\mathbb{Q}})\right| = 2$, it follows from the minimality of m_E that

$$\varphi_{E,d}(G_{\mathbb{Q}}) = \mathrm{pr}_{m_E,d}\left(\varphi_{E,m_E}(G_{\mathbb{Q}})\right) = \begin{cases} \text{index 2 subgroup of } \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}) & \text{if } d = m_E, \\ \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) & \text{if } d < m_E. \end{cases}$$

By Theorem 10, this proves (28).

□

2.5 Two-parameter families of elliptic curves

Lemma 18 *Let $A, B > 2$ and consider the family $\mathcal{C}(A, B)$ of $\mathbb{Q}$-isomorphism classes of elliptic curves $E = E_{a,b}$ defined by $Y^2 = X^3 + aX + b$ with $a, b \in \mathbb{Z}$ and $|a| \le A$, $|b| \le B$. Then*

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{\substack{E \in \mathcal{C}(A,B) \\ E \text{ CM}}} 1 \ll \frac{1}{A} + \frac{1}{B}.$$

More precisely,

$$\#\{E \in \mathcal{C}(A,B) : j(E) = 0\} \sim \frac{2}{\zeta(6)} B,$$
$$\#\{E \in \mathcal{C}(A,B) : j(E) = 1728\} \sim \frac{2}{\zeta(4)} A,$$

and, for each of the j-invariants of Theorem 8 (ii) with $j \neq 0, 1728$,

$$\#\{E \in \mathcal{C}(A,B) : j(E) = j\} \ll_\varepsilon \min\left\{A^{\frac{1}{2}+\varepsilon}, B^{\frac{1}{3}+\varepsilon}\right\}$$

for any $\varepsilon > 0$. The $\ll$-constant is absolute, while the $\ll_\varepsilon$-constant depends on ε.

Proof. We recall that associated to an elliptic curve $E_{a,b}/\mathbb{Q}$, and in particular to a Weierstrass equation $Y^2 = X^3 + aX + b$, we have the j-invariant $j(a,b) := 1728\frac{4a^3}{4a^3+27b^2}$, which encodes the $\overline{\mathbb{Q}}$-isomorphism class of $E_{a,b}$: two elliptic curves $E_{a,b}/\mathbb{Q}, E_{a',b'}/\mathbb{Q}$ are $\overline{\mathbb{Q}}$-isomorphic if and only if $j(a,b) = j(a',b')$; furthermore, $E_{a,b}/\mathbb{Q}, E_{a',b'}/\mathbb{Q}$ are $\mathbb{Q}$-isomorphic if and only if

$$\exists\, u \in \mathbb{Q}^\times \text{ such that } a = u^4 a' \text{ and } b = u^6 b'. \tag{29}$$

In view of the above and of Theorem 8(ii), it suffices to estimate the cardinality of

$$\mathcal{C}_j(A,B) := \left\{(a,b) \in \mathbb{Z} \times \mathbb{Z} : |a| \le A, |b| \le B, \right.$$
$$\left. \Delta(a,b) \neq 0, \gcd\left(a^3, b^2\right) \text{ is 12th power free, } j(a,b) = j\right\}$$

for each of the 13 occurring j-invariants. We will consider the cases $j = 0$, $j = 1728$, and $j \neq 0, 1728$ separately.

Note that $j(a, b) = 0$ is equivalent to $a = 0$. Thus

$$\left|\mathcal{C}_0(A, B)\right| = \#\left\{b \in \mathbb{Z}\backslash\{0\} : b \text{ is 6th power free}, |b| \leq B\right\} \sim \frac{2}{\zeta(6)}B \tag{30}$$

(see [20, p.355] for a standard approach towards such asymptotics).

Similarly, note that $j(a, b) = 1728$ is equivalent to $b = 0$. Thus

$$\left|\mathcal{C}_{1728}(A, B)\right| = \#\left\{a \in \mathbb{Z}\backslash\{0\} : a \text{ is 4th power free}, |a| \leq A\right\} \sim \frac{2}{\zeta(4)}A. \tag{31}$$

Now let us fix $j \neq 0, 1728$. We set $c(j) := \frac{4}{27}\left(\frac{1728}{j} - 1\right) \in \mathbb{Q}^\times\backslash\{0\}$,

$$S_j(A) := \left\{a \in \mathbb{Z}\backslash\{0\} : |a| \leq A, c(j)a^3 = \beta^2 \text{ for some } \beta \in \mathbb{Z}\backslash\{0\}\right\}$$

and

$$T_j(B) := \left\{b \in \mathbb{Z}\backslash\{0\} : |b| \leq B, \frac{1}{c(j)}b^2 = \alpha^3 \text{ for some } \alpha \in \mathbb{Z}\backslash\{0\}\right\},$$

and we denote $N_j(A) := |S_j(A)|$ and $M_j(B) = |T_j(B)|$. Noting that $1728\frac{4a^3}{4a^3+27b^2} = j$ if and only if $a^3c(j) = b^2$, we obtain

$$\left|\mathcal{C}_j(A, B)\right| \leq \min\left\{N_j(A), M_j(B)\right\}. \tag{32}$$

Now we bound $N_j(A)$. Let a be an element of $S_j(A)$, and write $a = a_j\tilde{a}$, where $\tilde{a}$ is the largest positive factor of a which is relatively prime to $c(j)$. Since $c(j)a_j^3\tilde{a}^3$ is the square of an integer, $\tilde{a}$ must also be the square of an integer, and since $|a| \leq A$, there are at most $\sqrt{A}$ possibilities for $\tilde{a}$. Let k be the number of primes for which the valuation of $c(j)$ is nonzero. Again, since $|a| \leq A$, the number of choices for a_j is on the order of $(\log A)^k$. Thus,

$$N_j(A) \ll (\log A)^k\sqrt{A} \ll_\varepsilon A^{\frac{1}{2}+\varepsilon}.$$

Similarly, $M_j(B) \ll_\varepsilon B^{\frac{1}{3}+\varepsilon}$. Thus, by (32), $\left|\mathcal{C}_j(A, B)\right| \ll_\varepsilon \min\left\{A^{\frac{1}{2}+\varepsilon}, B^{\frac{1}{3}+\varepsilon}\right\}$ for any $\varepsilon > 0$. Combining this with (30) and (31) completes the proof of the lemma. □

Theorem 19 ([24, Thm. 4])
Let $A, B > 2$ and consider the family $\mathcal{C}(A, B)$ of $\mathbb{Q}$-isomorphism classes of elliptic curves $E = E_{a,b}$ defined by $Y^2 = X^3 + aX + b$ with $a, b \in \mathbb{Z}$ and $|a| \leq A$, $|b| \leq B$. Then there exists a positive absolute constant γ' such that

$$\frac{1}{|\mathcal{C}(A, B)|} \sum_{\substack{E \in \mathcal{C}(A,B) \\ E \text{ is not a Serre curve}}} 1 \ll \frac{(\log \min\{A, B\})^{\gamma'}}{\sqrt{\min\{A, B\}}},$$

where the $\ll$-constant is absolute.

3 Constants for non-Serre curves: proof of Theorem 4

In this section we prove Theorem 4, establishing bounds for the constants appearing in Conjectures 1–3. The key ingredients in the proof are Theorems 10 and 11, Corollary 13, Proposition 14, and the following lemma about arithmetic functions:

Lemma 20 *Let $f, g : \mathbb{N}\backslash\{0\} \longrightarrow \mathbb{C}^\times$ be arithmetic functions satisfying:*

(i) *g is multiplicative;*
(ii) $\sum_{m\geq 1} |g(m)|$ *converges.*

Assume that $\exists\, M \in \mathbb{N}\backslash\{0\}$ and $\exists\, \kappa \in \mathbb{C}$ with $\mathrm{Re}\,\kappa > 0$ such that:

(iii) *$\forall\, m_1 \mid M^\infty$ and $\forall m_2$ with $\gcd(m_2, M) = 1$, we have $f(m_1 m_2) = f(m_1)g(m_2)$;*
(iv) *$\forall\, d \mid M^\infty$, $\forall\, \ell \mid M$ with $\ell \nmid d$, and $\forall\, \delta \in \mathbb{N}$, we have $f(\ell^{\nu_\ell(M)+\delta} d) = \ell^{-\delta\kappa} f(\ell^{\nu_\ell(M)} d)$.*

Then

$$\sum_{m\geq 1} |f(m)| \leq \prod_{\ell \mid M} \left(1 - \frac{1}{|\ell^\kappa|}\right)^{-1} \left(\sum_{m \mid M} |f(m)|\right) \left(\sum_{m\geq 1} |g(m)|\right).$$

Proof. By (iii) we have the almost-product formula

$$\sum_{m\geq 1} |f(m)| = \left(\sum_{m \mid M^\infty} |f(m)|\right) \left(\prod_{\ell \nmid M} g_\ell\right),$$

where, for each rational prime ℓ, $g_\ell := \sum_{r\geq 0} |g(\ell^r)| = 1 + \sum_{r\geq 1} |g(\ell^r)|$. Since

$$\prod_{\ell \nmid M} g_\ell \leq \prod_{\ell} g_\ell = \sum_{m\geq 1} |g(m)|,$$

it remains to bound $\sum_{m \mid M^\infty} |f(m)|$.

Let $M = \ell_1^{\alpha_1} \dots \ell_n^{\alpha_n}$ be the prime factorization of M. For each subset $I \subseteq \{1, \dots, n\}$, possibly empty, define

$$M_I := \prod_{i \in \{1,\dots,n\}\backslash I} \ell_i^{\alpha_i - 1},$$

and for each $m \mid M^\infty$, whose unique prime factorization we write as $m = \ell_1^{\beta_1} \dots \ell_n^{\beta_n}$ with $\beta_1 \geq 0, \dots \beta_n \geq 0$, define

$$I_m := \{1 \leq i \leq n : \beta_i \geq \alpha_i\}.$$

Partitioning the integers $m \mid M^\infty$ according to the subsets $I_m \subseteq \{1, \dots, n\}$ and using property (iv) of f, we obtain

$$\begin{aligned}\sum_{m|M^\infty} |f(m)| &= \sum_{I\subseteq\{1,\dots,n\}} \sum_{\substack{m|M^\infty \\ I_m = I}} |f(m)| = \sum_{I\subseteq\{1,\dots,n\}} \sum_{d|M_I} \sum_{\substack{(\delta_i)_{i\in I} \\ \delta_i\in\mathbb{N}\ \forall i}} \left| f\left(\prod_{i\in I} \ell_i^{\alpha_i+\delta_i} d\right)\right| \\ &= \sum_{I\subseteq\{1,\dots,n\}} \left(\sum_{d|M_I} \left|f\left(\prod \ell_i^{\alpha_i} d\right)\right|\right) \left(\prod_{i\in I} \sum_{\delta_i\in\mathbb{N}} \left|\frac{1}{\ell_i^{\kappa\delta_i}}\right|\right) \\ &\le \prod_{\ell|M} \left(1 - \frac{1}{|\ell^\kappa|}\right)^{-1} \sum_{m|M} |f(m)|.\end{aligned}$$

This completes the proof. □

Proof of part (i) of Theorem 4 Now assume that E is with CM by an order O in an imaginary quadratic field K.

For lower bounds, we have

$$\begin{aligned}0 < C_{d_1,\mathrm{CM}}(O) &= \lim_{\sigma\to 0^+} \sigma \sum_{m\ge 1} \frac{\phi(m)}{|(O/mO)^\times|} m^{-\sigma} \le 2 \lim_{\sigma\to 0^+} \sigma \sum_{m\ge 1} \frac{\phi(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]} m^{-\sigma} \\ &= 2C_{d_1,\mathrm{CM}}(E), \\ 0 < C_{\tau(d_1),\mathrm{CM}}(O) &= \sum_{m\ge 1} \frac{1}{|(O/mO)^\times|} \le 2 \sum_{m\ge 1} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]} = 2C_{\tau(d_1)}(E). \end{aligned} \tag{33}$$

Regarding upper bounds, we first observe that

$$\begin{aligned}C_{d_1,\mathrm{CM}}(E) &\le \lim_{\sigma\to 0^+} \sigma \sum_{m\ge 1} \frac{\phi(m)}{|\varphi_{E,m}(G_K)|} m^{-\sigma} \\ &= \lim_{\sigma\to 0^+} \sigma \sum_{m\ge 1} \frac{\phi(m)[(O/mO)^\times : \varphi_{E,m}(G_K)]}{|(O/mO)^\times|} m^{-\sigma} \\ &\le \left[\widehat{O}^\times : \varphi_E(G_K)\right] C_{d_1,\mathrm{CM}}(O), C_{\tau(d_1)}(E) \le \sum_{m\ge 1} \frac{[(O/mO)^\times : \varphi_{E,m}(G_K)]}{|(O/mO)^\times|} \\ &\le \left[\widehat{O}^\times : \varphi_E(G_K)\right] C_{\tau(d_1),CM}(O).\end{aligned}$$

In each of these upper bounds, the final inequality is likely not sharp. In what follows, we will prove another upper bound by using Lemma 20 to compute directly.

First we verify that, for the arbitrary elliptic curve $E/\mathbb{Q}$ with CM by the order O in the imaginary quadratic field K, we have

$$\sum_{m\ge 1} \frac{1}{[K(E[m]):K]} < \infty. \tag{34}$$

Note that this verification is also implicit in the proving convergence of the sums defining the constants $C_{\tau(d_1),CM}(O)$ and $B_{\tau(d_1),\mathrm{CM}}(O)$ and was alluded to in Sect. 1.

By Theorem 11, for any integer $m \ge 1$, written uniquely as $m = m_1 m_2$ with $m_1 \mid m_E^\infty$ and $(m_2, m_E) = 1$, we have

$$[K(E[m]):K] = [K(E[m_1]):K] \cdot \Phi_O(m_2), \tag{35}$$

where Φ_O denotes the Euler function on O, that is, $\Phi_O(n) := \left|(O/nO)^\times\right|$ for any positive integer n. Defining

$$f(m) := \frac{1}{[K(E[m]) : K]},\ g(m) := \frac{1}{\Phi_O(m)},$$

we wish to apply Lemma 20 with $M = m_E$ and $\kappa = 2$. Condition (i) follows from the Chinese Remainder Theorem; if $(m, m') = 1$, then we have

$$\Phi_O(mm') := |(O/mm'O)^\times| = |(O/mO)^\times \times (O/m'O)^\times| = \Phi_O(m)\Phi_O(m').$$

Furthermore, since $\Phi_O(\ell^r) = \ell^{2(r-1)}\Phi_O(\ell)$ for all $r \geq 1$ and

$$\Phi_O(\ell) = \begin{cases} (\ell+1)(\ell-1) & \text{if } \ell \text{ is inert in } O, \\ (\ell-1)^2 & \text{if } \ell \text{ splits in } O, \\ \ell(\ell-1) & \text{if } \ell \text{ ramifies in } O, \end{cases}$$

we have $\Phi_O(\ell^r) \geq \phi(\ell^r)^2$ for all $r \geq 1$. Therefore $\Phi_O(m) \geq \phi(m)^2$ for all $m \geq 1$. Condition (ii) hence follows from the convergence of the series $\sum_{m\geq 1} \frac{1}{\phi(m)^2}$. Conditions (iii) and (iv) follow from (35) and Corollary 13(ii). By Lemma 20, we obtain

$$\begin{aligned} \sum_{m\geq 1} \frac{1}{[K(E[m]) : K]} &\leq \zeta(2) \left(\sum_{m | m_E} \frac{1}{[K(E[m]) : K]} \right) \left(\sum_{m\geq 1} \frac{1}{\Phi_O(m)} \right) \\ &\leq \zeta(2) \left(\sum_{m | m_E} \frac{1}{[K(E[m]) : K]} \right) \left(\sum_{m\geq 1} \frac{1}{\phi(m)^2} \right) < \infty. \end{aligned} \tag{36}$$

which establishes (34).

Our goal is now to establish the bound

$$\sum_{m\geq 1} \frac{1}{[K(E[m]) : K]} \leq |\operatorname{Aut}_{\overline{\mathbb{Q}}}(E)| \min_{\substack{E'/\mathbb{Q} \\ \operatorname{End}_{\overline{\mathbb{Q}}}(E') \simeq O}} \left\{ \sum_{m\geq 1} \frac{1}{[K(E'[m]) : K]} \right\} = B_{\tau(d_1),\mathrm{CM}}(O). \tag{37}$$

Recall that, since E is assumed to have CM by O, we have $\operatorname{Aut}_{\overline{\mathbb{Q}}}(E) \simeq \operatorname{Aut}(O)$, hence the given expression on the right hand side above is indeed equal to $B_{\tau(d_1),\mathrm{CM}}(O)$.

Fix any elliptic curve E' over $\mathbb{Q}$ satisfying $\operatorname{End}_{\overline{\mathbb{Q}}}(E') \simeq O$ and note that, by Lemma 9, there exists a number field L such that $[L : \mathbb{Q}] \leq |\operatorname{Aut}_{\overline{\mathbb{Q}}}(E)| \leq 6$ and $E' \simeq_L E$. Moreover, we claim that, for any integer $m \geq 1$,

$$\frac{1}{|\operatorname{Aut}_{\overline{\mathbb{Q}}}(E)|}[K(E'[m]) : K] \leq [LK(E'[m]) : LK] \leq [K(E[m]) : K]. \tag{38}$$

Indeed, we have

$$\begin{aligned} [K(E'[m]) : K] &= [K(E'[m]) : LK \cap K(E'[m])] \cdot [LK \cap K(E'[m]) : K] \\ &= [LK(E'[m]) : LK] \cdot [LK \cap K(E'[m]) : K] \\ &\leq [LK(E'[m]) : LK] \cdot [L : \mathbb{Q}] \\ &\leq [LK(E'[m]) : LK] \cdot |\operatorname{Aut}_{\overline{\mathbb{Q}}}(E)| \end{aligned}$$

and

$$[LK(E'[m]) : LK] = [LK(E[m]) : LK] = [K(E[m]) : LK \cap K(E[m])] \leq [K(E[m]) : K].$$

This establishes (38), and, since E' was arbitrary such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E') \simeq O$, (37) follows.

We deduce from (37) that

$$C_{\tau(d_1)}(E) = \sum_{m\geq 1} \frac{1}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} \leq \sum_{m\geq 1} \frac{1}{[K(E[m]) : K]} \leq B_{\tau(d_1),\mathrm{CM}}(O).$$

Next we prove that

$$C_{d_1,\mathrm{CM}}(E) = \lim_{\sigma\to 0^+} \left(\sigma \sum_{m\geq 1} \frac{\phi(m)}{[\mathbb{Q}(E[m]) : \mathbb{Q}]} m^{-\sigma} \right) \leq B_{d_1,\mathrm{CM}}(O),$$

proceeding much as above, as follows. Note that the convergence of the above two constants follows from (36).

Fix $\sigma > 0$, let E' be any elliptic curve over $\mathbb{Q}$ with $\mathrm{End}_{\overline{\mathbb{Q}}}(E') \simeq O$, and define

$$f_\sigma(m) := \frac{\phi(m)}{[K(E'[m]) : K]} m^{-\sigma}, \quad g_\sigma(m) := \frac{\phi(m)}{\Phi_O(m)} m^{-\sigma}.$$

We wish to apply Lemma 20 with $M = m_{E'}$ and $\kappa = 1 + \sigma$. Condition (i) follows from the observation that a product of multiplicative functions is multiplicative. Condition (ii) follows from the calculation

$$\begin{aligned} \sum_{m\geq 1} |g_\sigma(m)| &= \sum_{m\geq 1} \frac{\phi(m)}{\Phi_O(m)} m^{-\sigma} \\ &= \prod_\ell \left(1 - \frac{\chi_O(\ell)}{\ell}\right)^{-1} \left(1 - \frac{1}{\ell^{1+\sigma}}\right)^{-1} \\ &= L(1, \chi_O)\zeta(1+\sigma) < \infty, \end{aligned}$$

where χ_O is the character defined by

$$\Phi_O(\ell^r) = \ell^{2r} \left(1 - \frac{1}{\ell}\right) \left(1 - \frac{\chi_O(\ell)}{\ell}\right)$$

and $L(1, \chi_O) = \prod_\ell \left(1 - \frac{\chi_O(\ell)}{\ell}\right)^{-1}$. Conditions (iii) and (iv) follow, as before, from (35) and Corollary 13(ii). By Lemma 20, we obtain

$$\begin{aligned} \sum_{m\geq 1} \frac{\phi(m)}{[K(E'[m]) : K]} m^{-\sigma} \leq \prod_{\ell | m_{E'}} \left(1 - \frac{1}{\ell^{1+\sigma}}\right)^{-1} \left(\sum_{m | m_{E'}} \frac{\phi(m)}{[K(E'[m]) : K]} m^{-\sigma} \right) \\ \times \left(\sum_{m\geq 1} \frac{\phi(m)}{\Phi_O(m)} m^{-\sigma} \right) < \infty. \end{aligned}$$

Observing that

$$\lim_{\sigma\to 0^+} \sigma \sum_{m\geq 1} \frac{\phi(m)}{\Phi_O(m)} m^{-\sigma} = L(1, \chi_O) \lim_{\sigma\to 0^+} \sigma\zeta(1+\sigma) = L(1, \chi_O),$$

we deduce that

$$\lim_{\sigma\to 0^+} \sigma \sum_{m\geq 1} \frac{\phi(m)}{[K(E'[m]) : K]} m^{-\sigma} \leq \prod_{\ell | m_E} \left(1 - \frac{1}{\ell}\right)^{-1} \left(\sum_{m | m_E} \frac{\phi(m)}{[K(E'[m]) : K]} \right) L(1, \chi_O).$$

(39)

Using (38) again and recalling that E' was arbitrary such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E') \simeq O$, we deduce that

$$\lim_{\sigma\to 0^+} \sigma \sum_{m\geq 1} \frac{\phi(m)}{[K(E[m]):K]} m^{-\sigma} \leq |\operatorname{Aut}(O)| L(1,\chi_O) \min_{\substack{E'/\mathbb{Q} \\ \mathrm{End}_{\overline{\mathbb{Q}}}(E')\simeq O}} \prod_{\ell \mid m_{E'}} \times \left(1-\frac{1}{\ell}\right)^{-1} \left(\sum_{m \mid m_{E'}} \frac{\phi(m)}{[K(E'[m]):K]} \right),$$

where the right-hand expression is exactly the constant $B_{d_1,\mathrm{CM}}(O)$. The bound $C_{d_1,\mathrm{CM}}(E) \leq B_{d_1,\mathrm{CM}}(O)$ now follows by noting that $[K(E[m]):K] \leq [\mathbb{Q}(E[m]):\mathbb{Q}]$. This completes part (i) of Theorem 4. □

Proof of part (ii) of Theorem 4. We are now assuming that E is without CM, in which case the first two lower bounds follow directly from the definition. Indeed,

$$0 < C_{d_1} = \sum_{m\geq 1} \frac{\phi(m)}{|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|} \leq \sum_{m\geq 1} \frac{\phi(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]} = C_{d_1,\text{non-CM}}(E),$$
$$0 < C_{\tau(d_1)} = \sum_{m\geq 1} \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|} \leq \sum_{m\geq 1} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]} = C_{\tau(d_1)}(E).$$

Next, we observe that we have the upper bounds

$$\begin{aligned} C_{d_1,\text{non-CM}}(E) &= \sum_{m\geq 1} \frac{\phi(m)}{|\operatorname{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})|} \\ &= \sum_{m\geq 1} \frac{\phi(m)[\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \operatorname{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})]}{|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|} \\ &\leq [\operatorname{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})] C_{d_1}, \\ C_{\tau(d_1)}(E) &= \sum_{m\geq 1} \frac{1}{|\operatorname{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})|} = \sum_{m\geq 1} \frac{[\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \operatorname{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})]}{|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|} \\ &\leq [\operatorname{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})] C_{\tau(d_1)}. \end{aligned} \tag{40}$$

In the case of the constant $C_{d_1,\text{non-CM}}(E)$, the above upper bound together with Proposition 14 proves part (ii) of Theorem 4. For the remaining constants, we will establish the (stronger, in this case) bound

$$C_{\tau(d_1)}(E) \ll (\log\log m_E)^{\beta} \tag{41}$$

for some positive constant β, where m_E is the positive integer appearing in Theorem 10. This bound, together with the upper bound for m_E from Proposition 14, will finish the proof of part (ii) of Theorem 4.

Defining $f(m) := \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}$ and $g(m) := \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|}$, we apply Lemma 20 with $M = m_E$ and $\kappa = 4$. Note that condition (i) follows immediately from the Chinese Remainder Theorem, condition (ii) follows immediately from

$$\sum_{m\geq 1} \frac{1}{|\operatorname{GL}_2(\mathbb{Z}/m\mathbb{Z})|} < \sum_{m\geq 1} \frac{1}{m^2\phi(m)^2} < \infty,$$

and conditions (iii) and (iv) follow from Theorem 10 and Corollary 13(i). We obtain

$$C_{\tau(d_1)} = \sum_{m\geq 1} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]} \leq \zeta(4) \left(\sum_{m|m_E} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]} \right) \left(\sum_{m\geq 1} \frac{1}{|\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})|} \right)$$
$$\ll \sum_{m|m_E} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}. \tag{42}$$

To analyze the last sum, recall that for any integer $m \geq 1$, denoting by ζ_m a primitive m-th root of unity, we have $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(E[m])$; in particular, we have $\phi(m) \mid [\mathbb{Q}(E[m]):\mathbb{Q}]$. Then

$$\sum_{m|m_E} \frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]} \leq \sum_{m|m_E} \frac{1}{\phi(m)} \leq \prod_{\ell|m_E} \left(1 + \frac{1}{\ell-1} \sum_{r\geq 0} \frac{1}{\ell^r} \right) = \prod_{\ell|m_E} \left(1 + \frac{\ell}{(\ell-1)^2} \right)$$
$$= \prod_{\ell|m_E} \left(1 + \frac{1}{\ell} \right) \cdot \prod_{\ell|m_E} \left(1 + \frac{2\ell-1}{\ell^3 - \ell^2 - \ell + 1} \right)$$
$$\ll \prod_{\ell|m_E} \left(1 + \frac{1}{\ell} \right) \leq \exp\left(\sum_{\ell|m_E} \frac{1}{\ell} \right), \tag{43}$$

where, in the last line, we used the elementary inequality $1 + t \leq \exp t$. To understand the last sum, we proceed in a standard way. We let ℓ_i denote the i-th prime and we recall that it satisfies the bound $\ell_i \leq i(\log i + \log\log i)$ (see [34, Theorem 3, p. 69]). Then

$$\sum_{\ell|m_E} \frac{1}{\ell} \leq \sum_{i\leq \omega(m_E)} \frac{1}{\ell_i} = \log\log \ell_{\omega(m_E)} + \mathrm{O}(1)$$
$$\leq \log\log \omega(m_E) + \log\log\log \omega(m_E) + \mathrm{O}(1)$$
$$\ll \log\log\log m_E, \tag{44}$$

where, in the second line, we used Mertens' Theorem $\sum_{\ell\leq n} \frac{1}{\ell} = \log\log n + \mathrm{O}(1)$, and, in the last line, we used the bound $\omega(n) \leq \log n$. The desired bound (41) is obtained by combining (42), (43) and (44). This finishes the proof of Theorem 4. □

Remark 21 Denoting by $C(E)$ any of the constants $C_{d_1,\text{non-CM}}(E)$, $C_{d_1,\text{CM}}(E)$, or $C_{\tau(d_1)}(E)$, and by C the corresponding universal constant, we observe that the upper bounds

$$C(E) \leq \left[\widehat{O}^\times : \varphi_E(G_K)\right] \cdot C, \quad \text{if } E \text{ is with CM by the order } O, \tag{45}$$
$$C(E) \leq \left[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})\right] \cdot C, \quad \text{if } E \text{ is without CM}, \tag{46}$$

established in Theorem 4, are of a fundamentally different nature one from the other in terms of what further unconditional upper bounds they may lead to. When E is with CM by the order O in K, since there are only finitely many j-invariants associated to CM elliptic curves over $\mathbb{Q}$ and since the index $\left[\widehat{O}^\times : \varphi_E(G_K)\right]$ remains bounded in twist families (see Proposition 12 above), (45) leads to uniform upper bounds for the constants $C(E)$. In contrast, when E is without CM, the uniform boundedness of the index $\left[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})\right]$ is equivalent to an affirmative answer to an open question of Serre, known as Serre's uniformity question; see [35, Sect. 4.3]. Assuming an affirmative answer to this question,

it is shown in [43, Theorem 1.3] that, except possibly for elliptic curves with j-invariants belonging to an ineffective finite set, we have $\left[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \varphi_E(G_{\mathbb{Q}})\right] \leq 1536$. Thus, assuming an affirmative answer to Serre's uniformity question, (46) leads to the ineffective uniform upper bounds

$$C_{\tau(d_1)}(E) \ll 1, \quad C_{d_1}(E) \ll 1. \tag{47}$$

Further improving (47) to conditional *effective* uniform upper bounds is an interesting future topic to explore that would involve techniques different from the ones of our present paper, in particular techniques used to determine rational points on higher genus modular curves.

4 Constants for Serre curves: proof of Theorem 5

In this section we prove closed formulae relating the constants of Conjectures 1–3 to the universal constants (11)–(13), as stated in Theorem 5. The key ingredients in the proof are Theorem 10 and the following lemma:

Lemma 22 ([29, Lemma 3.12]). *Let $f, g : \mathbb{N}\backslash\{0\} \longrightarrow \mathbb{C}^\times$ be arithmetic functions satisfying the following:*

(i) *g is multiplicative;*
(ii) $\sum_{m\geq 1} |g(m)|$ *converges.*

Assume that $\exists\, M \in \mathbb{N}\backslash\{0\}$, $\exists\, \alpha \in (0,\infty)$ and $\exists\, \kappa \in \mathbb{N}\backslash\{0,1\}$ such that:

(iii) $\forall m \in \mathbb{N}\backslash\{0\}$, *we have*

$$f(m) = \begin{cases} \alpha g(m) & \text{if } M \mid m, \\ g(m) & \text{else;} \end{cases}$$

(iv) $\forall\ m \mid M^\infty$, *we have* $g(mM) = m^{-\kappa} g(M)$.

Then

$$\sum_{m\geq 1} f(m) = \left(1 + (\alpha - 1)g(M) \prod_{\ell \mid M} g_\ell^{-1}(1-\ell^{-\kappa})^{-1}\right) \prod_{\ell} g_\ell,$$

where, for any rational prime ℓ, $g_\ell := \sum_{r\geq 0} g(\ell^r)$.

Proof of Theorem 5. The proposition follows from part (iv) of Proposition 17, Lemma 22 with $M = m_E$ and f, g, α, κ as described below, and from summing geometric series. Note that, by definition, $\prod_\ell g_\ell$ is the universal constant C_{d_1}, $C_{\tau(d_1)}$, respectively C_{d_2}. □

	$f(m)$	$g(m)$	α	κ	g_ℓ
$C_{d_1,non-CM}(E)$	$\frac{\phi(m)}{[\mathbb{Q}(E[m]):\mathbb{Q}]}$	$\frac{\phi(m)}{\lvert\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})\rvert}$	$\alpha = 2$	$\kappa = 3$	$1 + \frac{1}{\ell^3(1-\ell^{-2})(1-\ell^{-3})}$
$C_{\tau(d_1)}(E)$	$\frac{1}{[\mathbb{Q}(E[m]):\mathbb{Q}]}$	$\frac{1}{\lvert\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})\rvert}$	$\alpha = 2$	$\kappa = 4$	$1 + \frac{1}{\ell^4(1-\ell^{-1})(1-\ell^{-2})(1-\ell^{-4})}$
$C_{d_2}(E)$	$\frac{(-1)^{\omega(m)}\phi(\mathrm{rad}(m))}{m[\mathbb{Q}(E[m]):\mathbb{Q}]}$	$\frac{(-1)^{\omega(m)}\phi(\mathrm{rad}(m))}{m\lvert\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})\rvert}$	$\alpha = 2$	$\kappa = 5$	$1 - \frac{1}{\ell^4(1-\ell^{-2})(1-\ell^{-5})}$.

5 Averaging the constants over a family: proof of Theorem 6

In this section we prove Theorem 6 using the results of Sects. 2–4 and following the approach initiated in [23]. For this, let $A, B > 2$ and $n \in \mathbb{N}\backslash\{0\}$ be fixed and consider the moment

$$\frac{1}{|\mathcal{C}(A,B)|}\sum_{E\in\mathcal{C}(A,B)}|C(E)-C|^n,$$

where the pair $(C(E), C)$ is, respectively, $(C_{d_1}(E), C_{d_1})$, $(C_{\tau(d_1)}(E), C_{\tau(d_1)})$, and $(C_{d_2}(E), C_{d_2})$, and where $C_{d_1}(E)$ is $C_{d_1,\text{non-CM}}(E)$ if E is without complex multiplication, and $C_{d_1,\text{CM}}(E)$ if E is with complex multiplication. Our strategy is to partition $\mathcal{C}(A,B)$ into the subset of elliptic curves with complex multiplication (CM curves), the subset of elliptic curves without complex multiplication and which are not Serre curves (non-CM & non-Serre curves), and the subset of Serre curves; we then estimate each emerging subsum via different techniques.

To handle the contribution from elliptic curves with complex multiplication, using part (i) of Theorem 4 and Lemma 18, we obtain

$$\frac{1}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E\text{ CM}}}|C(E)-C|^n \ll_n \frac{1}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E\text{ CM}}}1 \ll \frac{1}{A}+\frac{1}{B}. \tag{48}$$

To handle the contribution from elliptic curves without complex multiplication, which are not Serre curves, using part (ii) of Theorem 4, as well as Theorem 19, we obtain

$$\begin{aligned}&\frac{1}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E\text{ non-CM,}\\ \text{non-Serre}}}|C(E)-C|^n\\ &\ll_n \frac{\left(\log\log\left\{\max\{A^3,B^2\}\cdot\log(\max\{A^3,B^2\})^{\gamma}\right\}\right)^{\beta n}\cdot(\log\min\{A,B\})^{\gamma'}}{\sqrt{\min\{A,B\}}}\end{aligned} \tag{49}$$

for $(C(E), C)$ equal to $(C_{\tau(d_1)}(E), C_{\tau(d_1)})$ or $(C_{d_2}(E), C_{d_2})$, and

$$\begin{aligned}&\frac{1}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E\text{ non-CM,}\\ \text{non-Serre}}}|C(E)-C|^n\\ &\ll_n \frac{\log(\max\{A^3,B^2\})^{\gamma n}\cdot(\log\min\{A,B\})^{\gamma'}}{\sqrt{\min\{A,B\}}}\end{aligned} \tag{50}$$

for $(C(E), C)$ equal to $(C_{d_1,\text{non-CM}}(E), C_{d_1})$.

To handle the contribution from Serre curves, using Theorem 5 and part (iii) of Proposition 17, we obtain

$$\frac{1}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E\text{ Serre}}}|C(E)-C|^n \ll \frac{C^n}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E\text{ Serre}}}\frac{1}{|\Delta_{\text{sf}}(E)|^{3n}}.$$

Next, following the approach of [23, Sect. 4.2], we choose a parameter $z = z(A,B)$ and partition the Serre curves E in $\mathcal{C}(A,B)$ according to whether $|\Delta_{\text{sf}}(E)| \le z$ or not. For the first subsum we use [23, Lemma 22, p. 705], while for the second subsum we use trivial

estimates:

$$\begin{aligned}
&\frac{C^n}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E \text{ Serre}\\ |\Delta_{\mathrm{sf}}(E)|\le z}}\frac{1}{|\Delta_{\mathrm{sf}}(E)|^{3n}}+\frac{C^n}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E \text{ Serre}\\ |\Delta_{\mathrm{sf}}(E)|> z}}\frac{1}{|\Delta_{\mathrm{sf}}(E)|^{3n}}\\
&\ll_n \frac{1}{AB}\Big(\#\big\{(a,b)\in\mathbb{Z}^2 : |a|\le A, |b|\le B, 4a^3\\
&\qquad\qquad +27b^2\neq 0, |(4a^3+27b^2)_{\mathrm{sf}}|\le z\big\}+\frac{1}{z^{3n}}\Big)\\
&\ll \frac{1}{A}+\frac{z(\log A)^7(\log B)}{B}+\frac{1}{z^{3n}AB}.
\end{aligned}$$

Upon choosing

$$z\asymp\left(\frac{1}{A(\log A)^7(\log B)}\right)^{\frac{1}{3n+1}},$$

we deduce that

$$\frac{1}{|\mathcal{C}(A,B)|}\sum_{\substack{E\in\mathcal{C}(A,B)\\ E \text{ Serre}}}|C(E)-C|^n\ll_n\frac{1}{A}+\frac{(\log A)^{\frac{21n}{3n+1}}(\log B)^{\frac{3n}{3n+1}}}{A^{\frac{1}{3n+1}}B}. \tag{51}$$

Now let $A=A(x)$ and $B=B(x)$ be functions tending to infinity with x and such that

$$\limsup_{x\to\infty}\frac{\log A(x)}{\log B(x)}<\infty,\quad \limsup_{x\to\infty}\frac{\log B(x)}{\log A(x)}<\infty. \tag{52}$$

Then

$$\frac{\log\max\{A(x)^3,B(x)^2\}}{\log\min\{A(x)^3,B(x)^2\}}\ll 1,$$

which implies that there exists a $\varepsilon>0$ for which

$$\frac{1}{\min\{A(x)^3,B(x)^2\}}\le\frac{1}{\max\{A(x)^3,B(x)^2\}^{\varepsilon}}.$$

From this it follows that

$$\lim_{x\to\infty}\frac{\big(\log\log\{\max\{A(x)^3,B(x)^2\}\cdot\log(\max\{A(x)^3,B(x)^2\})^{\gamma}\}\big)^{\beta n}}{\sqrt{\min\{A(x),B(x)\}}/(\log\min\{A(x),B(x)\})^{\gamma'}}=0$$

and, similarly

$$\lim_{x\to\infty}\frac{\log(\max\{A(x)^3,B(x)^2\})^{\gamma n}}{\sqrt{\min\{A(x),B(x)\}}/(\log\min\{A(x),B(x)\})^{\gamma'}}=0.$$

Recalling (48), (49), (50), and (51), it then follows that

$$\lim_{x\to\infty}\frac{1}{|\mathcal{C}(A(x),B(x))|}\sum_{E\in\mathcal{C}(A(x),B(x))}|C(E)-C|^n=0,$$

finishing the proof of Theorem 6.

Remark 23 One may view the results of Theorems 5 and 6 in the following light. The universal elliptic curve

$$\mathcal{E}: y^2=x^3-\frac{108j}{j-1728}x-\frac{432j}{j-1728}$$

over the rational function field $\mathbb{Q}(j)$, where j is a formal variable, satisfies $j(\mathcal{E})=j$; thus, for *any* elliptic curve $E_0/\mathbb{Q}$, the specialization $\mathcal{E}_{j_0}$ of $\mathcal{E}$ at $j_0:=j(E_0)$ yields an elliptic curve

over $\mathbb{Q}$ that is $\overline{\mathbb{Q}}$-isomorphic to E_0. Furthermore, the Galois representation associated to the generic fiber is onto $\mathrm{GL}_2\left(\hat{\mathbb{Z}}\right)$, i.e.

$$\varphi_{\mathcal{E}}\left(\mathrm{Gal}\left(\overline{\mathbb{Q}(j)}/\mathbb{Q}(j)\right)\right) = \mathrm{GL}_2\left(\hat{\mathbb{Z}}\right).$$

(This follows, for instance, by considering specializations that give Serre curves $E/\mathbb{Q}$ with distinct values of $\Delta_{sf}(E)$.) Using our previous general notation for the constants considered, since each universal constant C is the individual constant $C(\mathcal{E})$ associated to $\mathcal{E}$, the fact that all elliptic curves $E/\mathbb{Q}$ (up to $\overline{\mathbb{Q}}$-isomorphism) arise as specializations of the elliptic curve $\mathcal{E}/\mathbb{Q}(j)$, whose generic fiber has surjective Galois image, may explain, conceptually, why elliptic curves $E/\mathbb{Q}$ have constants $C(E)$ that average out to C.

Author details
[1]University of Pennsylvania, Philadelphia, PA, USA,

[2]Present address: Université Paris-Sud, Bât. 307, 91405 Orsay Cedex, France,

[3]Pohang Mathematics Institute, Pohang University of Science and Technology, Pohang, Republic of Korea,

[4]Institute of Mathematics "Simion Stoilow" of the Romanian Academy, 21 Calea Grivitei Street, Sector 1, 010702 Bucharest, Romania,

[5]Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago, 851 South Morgan Street, Chicago, IL 60607, USA,

[6]Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA,

[7]Department of Mathematics, University of California at Irvine, Irvine, CA 92697, USA,

[8]Department of Mathematics, Stanford University, 450 Jane Stanford Way, Building 380, Stanford, CA 94305-2125, USA.

Acknowlegements
This research started during the *Arizona Winter School 2016: Analytic Methods in Arithmetic Geometry*, organized at the University of Arizona, Tucson, USA, during March 12-16, 2016. We thank the conference organizers Alina Bucur, David Zureick-Brown, Bryden Cais, Mirela Ciperiani, and Romyar Sharifi for all their time and support, and we thank the National Science Foundation for sponsoring our participation in this conference. Moreover, we thank the referees for carefully reading the original manuscript and for all their comments and suggestions, which enabled us to improve the results of the paper.

Received: 25 January 2019 Accepted: 20 October 2019
Published online: 13 November 2019

References

1. Akbary, A., Felix, A.T.: On invariants of elliptic curves on average. Acta Arith. **168**(1), 31–70 (2015)
2. Akbary, A., Ghioca, D.: A geometric variant of Titchmarsh divisor problem. Int. J. Number Theory **8**(1), 53–69 (2012)
3. Akhtari, S., David, C., Hahn, H., Thompson, L.: Distribution of squarefree values of sequences associated with elliptic curves. Contemp. Math. **606**, 171–188 (2013)
4. Balog, A., Cojocaru, A.C., David, C.: Average twin prime conjecture for elliptic curves. Am. J. Math. **133**(5), 1179–1229 (2011)
5. Banks, W.D., Shparlinski, I.E.: Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. Isr. J. Math. **173**, 253–277 (2009)
6. Bombieri, E., Friedlander, J., Iwaniec, H.: Primes in arithmetic progressions to large moduli. Acta Math. **156**, 203–251 (1986)
7. Cojocaru, A.C.: Primes, elliptic curves and cyclic groups: a synopsis. Revue Roumain de Mathématiques Pures et Appliquées, Invited contributions to the Eighth Congress of Romanian Mathematicians (Iasi, 2015). Tome LXII No. 1 (2017)
8. Cojocaru, A.C., Murty, M.R.: Cyclicity of elliptic curves modulo *p* and elliptic curve analogues of Linnik's problem. Math. Ann. **330**, 601–625 (2004)
9. Cojocaru, A.C., Fitzpatrick, M., Insley, T., Yilmaz, H.: Reductions modulo primes of Serre curves: computational data, appendix to primes, elliptic curves and cyclic groups by A.C. Cojocaru. Contemp. Math. (to appear)
10. Cojocaru, A.C., Iwaniec, H., Jones, N.: The average asymptotic behaviour of the Frobenius fields of an elliptic curve (preprint)
11. Cox, D.A.: Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication. Pure and Applied Mathematics, 2nd edn. Wiley, Hoboken (2013)
12. David, C., Koukoulopoulos, D., Smith, E.: Sums of Euler products and statistics on elliptic curves. Math. Ann. http://www.mathstat.concordia.ca/faculty/cdavid/PAPERS/random-euler-products.pdf (to appear)
13. Felix, A.T.: Generalizing the Titchmash divisor problem. Int. J. Number Theory **8**(3), 613–629 (2012)
14. Felix, A.T., Murty, M.R.: On the asymptotics for invariants of elliptic curves modulo *p*. J. Ramanujan Math. Soc. **28**(3), 271–298 (2013)

15. Fouvry, É.: Sur le problem des diviseurs de Titchmarsh. J. Reine Angew. Math. **357**, 51–76 (1984)
16. Fouvry, É., Murty, M.R.: On the distribution of supersingular primes. Can. J. Math. **48**(1), 81–104 (1996)
17. Freiberg, T., Kulberg, P.: On the average exponent of elliptic curves modulo *p*. Int. Math. Res. Not. **8**, 2265–2293 (2014)
18. Freiberg, T., Pollack, P.: The average of the first invariant factor for reductions of CM elliptic curves mod *p*. Int. Math. Res. Not. **21**, 11333–11350 (2015)
19. Gekeler, E.-U.: Statistics about elliptic curves over finite prime fields. Manuscr. Math. **127**(1), 55–67 (2008)
20. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 6th edn. Oxford University Press, Oxford (2008). Revised by D. R. Heath-Brown and J. H. Silverman, with a foreword by A. Wiles
21. Halberstam, H.: Footnote to the Titchmarsh-Linnik divisor problem. Proc. Am. Math. Soc. **18**, 187–188 (1967)
22. Howe, E.W.: On the group orders of elliptic curves over finite fields. Compos. Math. **85**, 229–247 (1993)
23. Jones, N.: Averages of elliptic curve constants. Math. Ann. **345**, 685–710 (2009)
24. Jones, N.: Almost all elliptic curves are Serre curves. Trans. Am. Math. Soc. **362**(3), 1547–1570 (2010)
25. Jones, N.: A bound for the conductor of an open subgroup of GL_2 associated to an elliptic curve. arXiv:1904.10431 (preprint)
26. Kaplan, N., Petrow, I.: Elliptic curves over a finite field and the trace formula. arXiv:1510.03980 (preprint)
27. Kawamura, T.: The effective surjectivity of mod ℓ Galois representations of 1- and 2-dimensional abelian varieties with trivial endomorphism ring. Comment. Math. Helv. **78**, 486–493 (2003)
28. Kim, S.: Average behaviors of invariant factors in Mordell-Weil groups of CM elliptic curves modulo *p*. Finite Fields Appl. **30**, 178–190 (2014)
29. Kowalski, E.: Analytic problems for elliptic curves. J. Ramanujan Math. Soc. **21**(1), 19–114 (2006)
30. Linnik, J.V.: The Dispersion Method in Binary Additive Problems. Translations of Mathematical Monographs, vol. 4. American Mathematical Society, Providence (1963)
31. Masser, D., Wüstholz, G.: Galois properties of division fields of elliptic curves. Bull. Lond. Math. Soc. **25**, 247–254 (1993)
32. Pollack, P.: A Titchmarsh divisor problem for elliptic curves. Math. Proc. Camb. Philos. Soc. **160**(1), 167–189 (2016)
33. Rodriquez, G.: Sul problema dei divisori di Titchmarsh. Boll. Unione Math. Ital. Serie 3 **20**, 358–366 (1965)
34. Barkley Rosser, J., Schoenfeld, L.: Approximate formulas for some functions of prime numbers. Ill. J. Math. **6**, 64–94 (1962)
35. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972)
36. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106. Springer, New York (2000)
37. Titchmarsh, E.C.: A divisor problem. Rend. Circ. Mat. Palermo **54**, 414–429 (1930)
38. Vladut, S.G.: Cyclicity statistics for elliptic curves over finite fields. Finite Fields Appl. **5**, 13–25 (1999)
39. Weil, A.: On a certain type of characters of the idèle-class group of an algebraic number-field. In: Proceedings of the International Symposium on Algebraic Number Theory, Tokyo-Nikko, pp. 1–7 (1955)
40. Weil, A.: On the theory of complex multiplication. In: Proceedings of the International Symposium on Algebraic Number Theory, Tokyo-Nikko, pp. 9–22 (1955)
41. Wu, J.: The average exponent of elliptic curves modulo *p*. J. Number Theory **135**, 28–35 (2014)
42. Zywina, D.: Bounds for Serre's open image theorem. http://www.math.cornell.edu/~zywina/papers/Serre-Bound.pdf (preprint)
43. Zywina, D.: Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$. http://pi.math.cornell.edu/~zywina/papers/PossibleIndices/PossibleIndices.pdf (preprint)

Publisher's Note