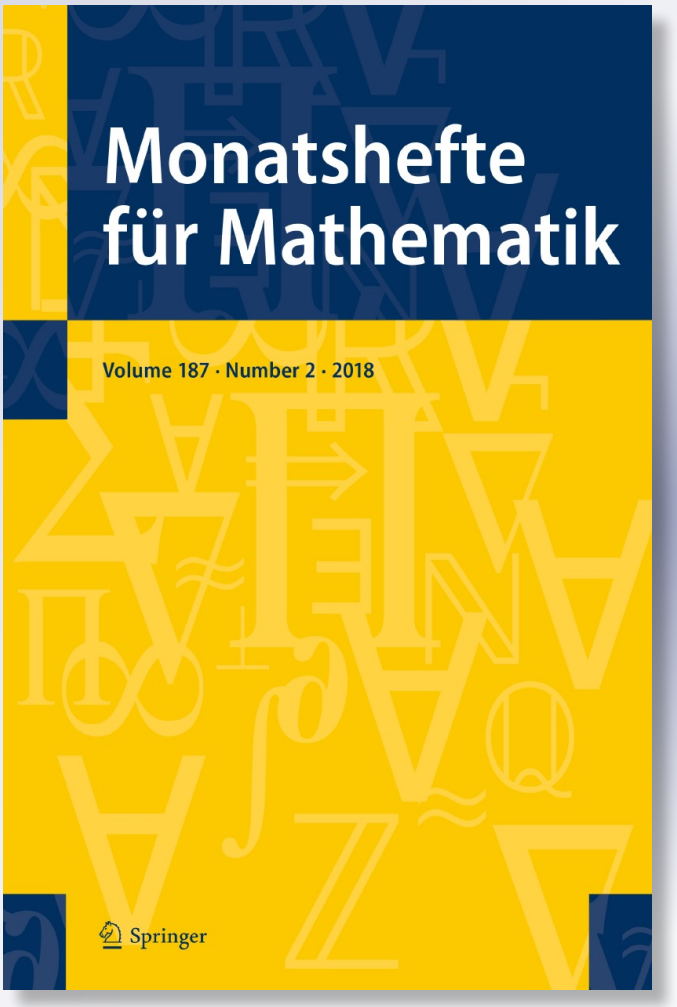
Arithmetic properties of coefficients of L-functions of elliptic curves

Ahmet M. Güloğlu, Florian Luca & Aynur Yalçiner

Monatshefte für Mathematik

ISSN 0026-9255
Volume 187
Number 2

Monatsh Math (2018) 187:247-273
DOI 10.1007/s00605-018-1175-x



Springer

Monatsh Math (2018) 187:247–273
https://doi.org/10.1007/s00605-018-1175-x

Arithmetic properties of coefficients of L-functions of elliptic curves

Ahmet M. Güloğlu[1] · **Florian Luca**[2,3,4] · **Aynur Yalçiner**[5]

Received: 29 June 2017 / Accepted: 26 February 2018 / Published online: 3 March 2018

Abstract Let $\sum_{n\geqslant 1} a_n n^{-s}$ be the L-series of an elliptic curve E defined over the rationals without complex multiplication. In this paper, we present certain similarities between the arithmetic properties of the coefficients $\{a_n\}_{n=1}^{\infty}$ and Euler's totient function $\varphi(n)$. Furthermore, we prove that both the set of n such that the regular polygon with $|a_n|$ sides is ruler-and-compass constructible, and the set of n such that $n - a_n + 1 = \varphi(n)$ have asymptotic density zero. Finally, we improve a bound of Luca and Shparlinski on the counting function of elliptic pseudoprimes.

Keywords Rational elliptic curves · Chebotarev Density Theorem · Arithmetic functions · L-functions · Euler's totient function · Elliptic pseudoprimes

Communicated by A. Constantin.

✉ Ahmet M. Güloğlu
guloglua@fen.bilkent.edu.tr

Florian Luca
florian.luca@wits.ac.za

Aynur Yalçiner
aynuryalciner@gmail.com

1 Department of Mathematics, Bilkent University, 06800 Bilkent, Ankara, Turkey

2 School of Mathematics, University of the Witwatersrand, Private Bag X3, Wits 2050, South Africa

3 Department of Mathematics, Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany

4 Faculty of Sciences, University of Ostrava, 30. dubna 22, 701 03 Ostrava 1, Czech Republic

5 Department of Mathematics, Selçuk University, Campus, 42075 Konya, Turkey

Mathematics Subject Classification 11N36 · 11G05 · 11G20

1 Introduction

Let E be an elliptic curve over the field of rational numbers $\mathbb{Q}$ given by the minimal *global Weierstraß equation* (cf. [15, Corollary 8.3])

$$E \ : \ y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6 \qquad (A_i \in \mathbb{Z}) \tag{1}$$

with discriminant Δ_E and conductor N_E. For each prime p, we put

$$a_p = p + 1 - \#E(\mathbb{F}_p),$$

where $E(\mathbb{F}_p)$ is the reduction of E modulo p. If $p \mid \Delta_E$, then $E(\mathbb{F}_p)$ has a singularity and

$$a_p = \begin{cases} 0, & \text{for the case of a cusp,} \\ 1, & \text{for the case of a split node,} \\ -1, & \text{for the case of a non–split node.} \end{cases}$$

It was conjectured by Artin and proved by Hasse (cf. [15, Ch.5 Theorem 1.1]) that the inequality $|a_p| < 2\sqrt{p}$ holds for all primes p. The L-function associated with E is defined by

$$L(s, E) = \prod_{p|\Delta_E} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid\Delta_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

where the infinite product converges for $\mathrm{Re}(s) > 3/2$, and thus yields the convergent series $L(s, E) = \sum_{n\geqslant 1} a_n n^{-s}$. The function $n \mapsto a_n$ is multiplicative, and for a prime number p the formula

$$a_{p^n} = a_p a_{p^{n-1}} - p\chi_0(p)a_{p^{n-2}}, \qquad (n \geqslant 2)$$

holds, where χ_0 is the trivial character modulo Δ_E. Thus, we see that $a_n \in \mathbb{Z}$ for all $n \in \mathbb{N}$.

In this paper we study certain arithmetical properties of the sequence $\{a_n\}_{n\geqslant 1}$ determined by an elliptic curve E over $\mathbb{Q}$ without *complex multiplication* (CM), for which $\mathrm{End}(E) \simeq \mathbb{Z}$; that is, the endomorphisms are given by $n : E \to E$ which map P to nP for $n \in \mathbb{Z}$.

Let $\varphi(n)$ be Euler's totient function. In [11, Lemma 2], it was proved that there exists a positive constant c_1 such that the set

$$\mathcal{F} = \{n \geqslant 1 : q \mid \varphi(n) \quad \forall q < c_1 \log_2 n / \log_3 n\} \tag{2}$$

is of asymptotic density 1, where here and in what follows q denotes a prime power and $\log_k x$ is defined in Sect. 2.1. The upper bound for the counting function for the

exceptional set was not very good. Our first result shows that the above property holds also for the sequence $\{a_n\}_{n\geqslant 1}$ of coefficients. More precisely, for a fixed $\kappa > 0$, let

$$\mathcal{G}_\kappa = \{n \geqslant 1 : q \mid a_n \quad \forall q < \kappa \log_2 n/\log_3 n\}. \tag{3}$$

As usual, for a subset $\mathcal{A}$ of positive integers and a positive real number x, we write $\mathcal{A}(x) := \mathcal{A} \cap [1, x]$.

Proposition 1 *If $\kappa < 1/100$, then $\mathcal{G}_\kappa(x)$ contains all integers $n \leqslant x$ with $O_E(x/(\log_2 x)^{1/(3\kappa)})$ exceptions.*

Next, we list some consequences of Proposition 1. Let $\tau(n)$, $\Omega(n)$, and $\omega(n)$ denote the number of divisors of n, and the number of prime divisors of n with and without repetitions, respectively. Sets of positive integers such that one of these functions divide a given arithmetic function $f(n)$ have already been studied in the literature when $f(n) = \varphi(n)$, or $\sigma(n)$, when $f(n)$ is a polynomial, or when $f(n)$ is the nth term of any linearly recurrent sequence (see [1,3,8–10,12,17]).

Theorem 2 *The sets*

$$\mathcal{A}_\omega = \{n \geqslant 1 : \omega(n) \mid a_n\}, \text{ and } \mathcal{A}_\Omega = \{n \geqslant 1 : \Omega(n) \mid a_n\}$$

both are of asymptotic density 1.

We have not succeeded in proving an analog of Theorem 2 for the function $\tau(n)$, yet we claim the following:

Conjecture *The set $\mathcal{A}_\tau = \{n \geqslant 1 : \tau(n) \mid a_n\}$ is also dense.*

We shall prove this conjecture under some additional conditions.

Theorem 3 *$\mathcal{A}_\tau$ is of asymptotic density 1 provided that one of the following holds:*

(i) E has a torsion point of order 2.
(ii) Δ_E is odd and the Galois representation ρ_2 associated with 2-division points (see Sect. 2.3) is surjective.

Remark 1 Condition (ii) above is not too restrictive. Via Weierstrass equations (see Sect. 2.2), we may assume that E is given by

$$y^2 = x^3 + Ax + B$$

with some integers A and B. If the cubic polynomial on the right is irreducible and has odd discriminant which is not a perfect square, then condition (ii) holds.

For the next result, recall that a regular n-gon is ruler-and-compass constructible if and only if $\varphi(n)$ is a power of 2 (Gauss-Wantzel theorem). Below we address the

instance in which the regular polygon with $|a_n|$ sides is thus constructible. First, we discard the cases in which $a_n = 0$ by recalling (cf. [14, Théorème 16]) that

$$\mathcal{Z}_E = \{n \geqslant 1 : a_n \neq 0\} \gg x,$$

and consider the set

$$\mathcal{C}_E = \{n \in \mathcal{Z}_E : \varphi(|a_n|) \text{ is a power of } 2\}.$$

By Proposition 1, it follows that $7 \mid a_n$ for almost all n. Thus, $3 \mid \varphi(|a_n|)$ for almost all $n \in \mathcal{Z}_E$ and we can immediately conclude that $\mathcal{C}_E$ is of asymptotic density 0. Below we give a slightly better version of this result.

Theorem 4 *The estimate*

$$\#\mathcal{C}_E(x) \ll_E \frac{x(\log_2 x)^{49/12}(\log_3 x)^{-13/12}}{(\log x)^{13/12}}$$

holds for all $x > 100$.

For the following result, we note that since the sets in (2) and (3) are dense, both a_n and $\varphi(n)$ are divisible by all small prime powers for most n, where *small* means up to a certain multiple of $\log_2 n / \log_3 n$. Furthermore, since $|a_n| \leqslant \tau(n)n^{1/2} \ll \varphi(n)$ for large n, one may ask whether it could happen that $a_n \mid \varphi(n)$. Below, we provide only an upper bound for such n up to x.

Theorem 5 *The estimate*

$$\#\mathcal{D}_E(x) \ll_E \frac{x}{\log_2 x}$$

holds for all $x > 100$, *where* $\mathcal{D}_E = \{n \in \mathcal{Z}_E : a_n \mid \varphi(n)\}$.

Note that whenever $a_p = 2$, we get $p - a_p + 1 = p - 1 = \varphi(p)$. Motivated by this observation, we give, in the next result, an upper bound for the counting function of the set

$$\mathcal{F}_E = \{n \geqslant 1 : n - a_n + 1 = \varphi(n)\}.$$

Theorem 6 *The estimate*

$$\#\mathcal{F}_E(x) \ll_E \frac{x(\log_2 x)^{1/2}(\log_3 x)^{1/4}}{(\log x)^{5/4}}$$

holds for all $x > 100$.

Remark 2 One may ask what we can conjecture about the true order of magnitude of $\mathcal{C}_E(x)$, $\mathcal{D}_E(x)$ and $\mathcal{F}_E(x)$. We conjecture that all these cardinalities have order of magnitude $x^{1/2+o(1)}$ as $x \to \infty$. For example, for $\mathcal{C}_E(x)$, the accepted heuristic is that there are only finitely many Fermat primes. If true, then there are only finitely many odd integers m such that $\phi(m)$ is a power of 2. Hence, every positive integer whose Euler function is a power of 2 should be just a product between one of these finitely many odd numbers m and a power of 2. The number of such numbers which are $\leqslant \max\{|a_n| : n \leqslant x\}$ is $O(\log x)$. Assuming that the multiplicity of each element in $\{|a_n| : n \leqslant x\}$ is $x^{1/2+o(1)}$ on the average as $x \to \infty$, we get the heuristic for $\#\mathcal{C}_E(x)$. For $\mathcal{D}_E(x)$, it is reasonable to conjecture that a_n and $\phi(n)$ have very different arithmetical behaviors except from the fact that they are both divisible by all small primes for most n. Thus, the "probability" that $a_n \mid \phi(n)$ should roughly be $1/n^{1/2+o(1)}$ as $n \to \infty$. Summing this up over all $n \leqslant x$, we get that the cardinality of $\mathcal{D}_E(x)$ should be about $x^{1/2+o(1)}$ as $x \to \infty$. Finally, for $\mathcal{F}_E(x)$, the proof of Theorem 6 shows that most elements $n \in \mathcal{F}_E(x)$ are of the form $n = pq$, where p, q are primes of size around $\sqrt{x}$. Thus, a_n and $n - \phi(n) + 1 = p + q$ are both of size $x^{1/2}$. Assuming that these two quantities are independent, the probability that they coincide should be $x^{-1/2}$. Summing this up over all numbers $n = pq \leqslant x$ of the above form, we get an answer of size $x^{1/2+o(1)}$.

For a positive integer n with prime factorization $n = p_1^{e_1} \dots p_k^{e_k}$, we put

$$E_n = \prod_{i=1}^{k} \#E\left(\mathbb{F}_{p_i^{e_i}}\right).$$

The next result is reminiscent of Proposition 1. For a fixed $\kappa > 0$, put

$$\mathcal{G}_{E,\kappa} = \{n \geqslant 1 : q \mid E_n \quad \forall q < \kappa \log_2 n / \log_3 n\}.$$

Proposition 7 *If $\kappa < 1/100$, then $\mathcal{G}_{E,\kappa}(x)$ contains all positive integers $n \leqslant x$ with $O_E(x/(\log_2 x)^{1/(3\kappa)})$ exceptions.*

Finally, Luca and Shparlinski (cf. [13]), motivated by Silverman's paper [16], put t_{p^e} for the exponent of the group $E(\mathbb{F}_{p^e})$, whenever $e \geqslant 1$ and $p \nmid \Delta_E$, and considered the set

$$\mathcal{EC}_E = \{n : \omega(n) > 1,\ \gcd(n, \Delta_E) = 1, t_{p^e} \mid n - a_n + 1 \text{ for } p^e \| n\}.$$

The positive integers n belonging to $\mathcal{EC}_E$ present certain similarities to Carmichael numbers in the sense that although n is not a prime power, $n - a_n + 1$ acts as an annihilator for any point $P \in E(\mathbb{F}_q)$ for all prime powers $q \| n$. They showed that

$$\#\mathcal{EC}_E(x) = O\left(\frac{x \log_3 x}{\log_2 x}\right).$$

Here, we improve this result as follows:

Theorem 8 *We have*

$$\#\mathcal{EC}_E(x) \leqslant \frac{x}{\exp\left((1+o(1))\sqrt{\log_2 x}\right)} \quad \text{as } x \to \infty.$$

2 Preliminaries and notation

2.1 Notation

The letters ℓ, p and r below, with or without subscripts, stand for prime numbers, while q denotes a prime power. We use $\mu(n)$, $\Omega(n)$, $\omega(n)$ and $\tau(n)$ for the Möbius function of n, the number of prime divisors of n with and without repetitions, and the number of positive divisors of n, respectively. For a subset $\mathcal{P}$ of primes, we use $\omega_{\mathcal{P}}(n)$ for the number of distinct prime factors of n which belong to $\mathcal{P}$. We write $P^+(n)$ for the largest prime factor of n, and $\mathrm{rad}(n)$ for the *radical* of n, which is the product of all distinct prime factors of n. We use κ_1, κ_2, etc. for absolute constants.

For a positive real number x, we define $\log_1 x = \max\{1, \log x\}$ and for $k \geqslant 2$, we define $\log_k x$ recursively by $\log_k x = \log_1(\log_{k-1} x)$. Note that $\log_k x$ coincides with the k-fold iterate of $\log x$ for large x, and equals 1 otherwise. For $k = 1$, we omit the subscript but continue to assume that $\log x \geqslant 1$.

Finally, we use the Landau notation O and o as well as the Vinogradov's notations $\ll$ and $\gg$ with their regular meanings, where the implied constants may depend on the curve E.

2.2 Weierstrass equations

Using the standard birational transformation (cf. [15, Ch.III § 1]), replacing y in (1) by $(y - A_1x - A_3)/2$ gives an equation of the form

$$y^2 = 4x^3 + B_2x^2 + 2B_4x + B_6,$$

where

$$B_2 = A_1^2 + 4A_2; \quad B_4 = 2A_4 + A_1A_3; \quad B_6 = A_3^2 + 4A_6.$$

Furthermore, defining the quantities

$$\begin{aligned} B_8 &= A_1^2A_6 + 4A_2A_6 - A_1A_3A_4 + A_2A_3^2 - A_4^2, \\ C_4 &= B_2^2 - 24B_4, \\ C_6 &= -B_2^3 + 36B_2B_4 - 216B_6, \end{aligned}$$

and then replacing (x, y) by $((x - 3B_2)/36, y/108)$ yields the simpler Weierstrass equation

$$E \ : \ y^2 = x^3 + Ax + B,$$

where $A = -27C_4$ and $B = -54C_6$. From now on, we shall work with this equation, at least for $p > 3$, when the above transformations are well-defined modulo p.

2.3 Primes p with a_p in a fixed residue class

We follow the exposition in [4, § 2]. We need to understand primes p with a_p lying in a fixed residue class modulo an integer $m \geqslant 2$.

Let $E[m] = \{P \in E(\bar{\mathbb{Q}}) : mP = 0_E\}$ be the group of m-torsion points of E. By [15, Ch. III. Corollary 6.4b], $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Let $\mathbb{L}_m = \mathbb{Q}(E[m])$ be the Galois extension over $\mathbb{Q}$ obtained by adjoining the coordinates of m-torsion points to $\mathbb{Q}$. The action $P \to P^\sigma$ of the Galois group $G_m = \mathrm{Gal}(\mathbb{L}_m/\mathbb{Q})$ on $E[m]$ gives a faithful representation (i.e., an injective homomorphism)

$$\rho_m : G_m \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

and we put $G(m) = \rho_m(G_m)$.

If $p \nmid mN_E$, it follows from [5, Theorem 2.1] that

$$\mathrm{tr}(\rho_m(\sigma_p)) \equiv a_p \pmod m, \qquad \text{and} \qquad \det(\rho_m(\sigma_p)) \equiv p \pmod m, \tag{4}$$

where $\sigma_p = [p, \mathbb{L}_m/\mathbb{Q}]$ is the conjugacy class of the Frobenius automorphisms of G_m associated with p.

Define the sets

$$\begin{aligned} T_a(m) &= \{g \in G(m) : \ \mathrm{tr}(g) \equiv a \pmod m\}, \\ C_a(m) &= \{g \in G(m) : \ \det(g) + 1 - \ \mathrm{tr}(g) \equiv a \pmod m\}. \end{aligned}$$

Note that $C_0(m) \neq \emptyset$ since the identity matrix lies in it.

Serre proved (cf. [14]) that there exists a positive integer M_E, depending only on E, such that ρ_m is surjective whenever $(m, M_E) = 1$. Taking any prime $\ell \nmid M_E$, one can show (cf. [4, eqn. (2.1)]) that

$$\#C_r(\ell) = \begin{cases} \ell(\ell^2 - 2) & \text{if } r \equiv 0 \pmod \ell, \\ \ell(\ell^2 - \ell - 1) & \text{if } r \equiv 1 \pmod \ell, \\ \ell(\ell^2 - \ell - 2) & \text{if } r \not\equiv 0, 1 \pmod \ell. \end{cases}$$

Similarly, [2, Lemma 2.7] yields that when $\ell > 2$ and $d \not\equiv 0 \pmod \ell$,

$$\#\mathcal{A}_{d,a} = \ell^2 + \ell\Big(\frac{a^2 - 4d}{\ell}\Big),$$

where $\big(\frac{\cdot}{\ell}\big)$ is the Legendre symbol and

$$\mathcal{A}_{d,a} = \{g \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \ \det(g) \equiv d, \ \mathrm{tr}(g) \equiv a \pmod \ell\}. \tag{5}$$

Thus, we conclude that

$$\#T_a(\ell) = \sum_{d=1}^{\ell-1} \#\mathcal{A}_{d,a} = \begin{cases} \ell^2(\ell-1) & \text{if } a \equiv 0 \pmod{\ell}, \\ \ell(\ell^2-\ell-1) & \text{if } a \not\equiv 0 \pmod{\ell}. \end{cases} \tag{6}$$

Furthermore, $\#T_0(2) = 4$ provided that ρ_2 is surjective. Finally, put

$$\pi_{C_r(n)}(x) = \#\{p \leqslant x : p \nmid nN_E \text{ and } \rho_n(\sigma_p) \in C_r(n)\},$$
$$\pi_{T_a(n)}(x) = \#\{p \leqslant x : p \nmid nN_E \text{ and } \rho_n(\sigma_p) \in T_a(n)\}.$$

Lemma 1 ([4, Proposition 2.1]). *Let E be an elliptic curve defined over $\mathbb{Q}$ without CM. Let $n = dm$ be any positive integer where $(d, M_E) = 1$, and $\mathrm{rad}(m) \mid M_E$. Then, uniformly for $n^{12}\log n \ll \log x$,*

$$\pi_{C_r(n)}(x) = \frac{\#C_r(m)}{\#G(m)} \left(\prod_{\ell^k \| d} \frac{\#C_r(\ell^k)}{\#G(\ell^k)} \right) Li(x) + O_E\big(x \exp(-An^{-2}\sqrt{\log x})\big),$$

where the implied constants depend only on E, and $A > 0$ is absolute. A similar estimate holds with C_r replaced by T_a, or by $A_{b,a}$ when $(b, n) = 1$ with $(n, M_E) = 1$.

2.4 Primes p with fixed a_p

Lemma 2 (Elkies, see [6]). *There exist infinitely many supersingular primes; that is, primes p such that $a_p = 0$.*

Lemma 3 (Serre, [14, Théorème 20]). *Let $a \neq 0$ and put $\mathcal{P}_a = \{p : a_p = a\}$. Then,*

$$\#\mathcal{P}_a(x) \ll \begin{cases} \dfrac{x(\log_2 x)^{1/2}(\log_3 x)^{1/4}}{(\log x)^{5/4}} & \text{if } a = \pm 2, \\ \dfrac{x(\log_2 x)^{2/3}(\log_3 x)^{1/3}}{(\log x)^{4/3}} & \text{if } a \neq \pm 2. \end{cases}$$

2.5 A couple of useful estimates

Below we collect two useful estimates that we use frequently in what follows. Recall that a *squarefull* number has the property that the exponent of every prime factor in its factorization is at least 2.

Lemma 4 *Uniformly in $1 \leqslant y \leqslant x$ we have*

$$\mathcal{E}_{\square}(x; y) = \#\{n \leqslant x : \exists \text{ squarefull } s \mid n \text{ with } s > y\} \ll \frac{x}{\sqrt{y}},$$

$$\mathcal{E}_\omega(x;\, y) = \#\{n \leqslant x : |\omega(n) - \log_2 x| > y\sqrt{\log_2 x}\} \ll \frac{x}{y^2}.$$

Proof The claim about $\mathcal{E}_\square(x;\, y)$ follows by partial summation from the fact that the number of squarefull $s \leqslant t$ is $O(\sqrt{t})$ (which can be seen by writing each s in the form a^2b^3). Namely, fix a squarefull $s > y$. The number of $n \leqslant x$ which are multiples of s is $\lfloor x/s \rfloor \leqslant x/s$. Hence,

$$\#\mathcal{E}_\square(x;\, y) \leqslant \sum_{\substack{s>y \\ s \text{ squarefull}}} \frac{x}{s} \ll \frac{x}{\sqrt{y}}.$$

The claim about $\mathcal{E}_\omega(x;\, y)$ follows immediately from the Túran-Kubilius estimate (cf. [19])

$$\sum_{n\leqslant x} (\omega(n) - \log_2 x)^2 = O(x \log_2 x).$$

□

3 Proofs of the results

3.1 Proof of Proposition 1

Given any fixed prime ℓ, it follows from Lemma 2 that there are infinitely many supersingular primes $p \nmid \ell N_E$. In particular, (4) implies that $\mathrm{G}(\ell)$ contains zero-trace elements of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Therefore, $T_0(\ell) \neq \emptyset$, and

$$\delta_\ell := \frac{\#T_0(\ell)}{\#\,\mathrm{G}(\ell)} \in \mathbb{Q}^\times$$

satisfies

$$\frac{1}{\ell^4} \ll \delta_\ell \ll \frac{1}{\ell}. \tag{7}$$

For odd $\ell \nmid M_E$, (6) and the fact that $\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \ell(\ell-1)(\ell^2-1)$ imply that

$$\delta_\ell = \frac{\ell}{\ell^2-1} \in \Big(\frac{1}{\ell}, \frac{1}{\ell-1}\Big). \tag{8}$$

Assume that x is large, $\kappa < 1$, $y := \frac{\log_2 x}{\log_3 x}$, and consider primes $\ell \leqslant \kappa y$. Set

$$z = \exp\Big((\log_2 x)^{13}\Big) \qquad \text{and} \qquad w = \exp\Big(\sqrt{\log x}\Big)$$

and assume $t \in (z, x]$. Then, $\ell^{12}\log\ell = o(\log t)$ and Lemma 1 yields

$$\pi_{T_0(\ell)}(t) = \delta_\ell \mathrm{Li}(t) + O_E(t\exp(-B(\log t)^{1/3})) \tag{9}$$

uniformly for $\ell \leqslant \kappa y$. Put

$$S_t^{(\ell)} := \sum_{\substack{p \leqslant t \\ \ell \mid a_p}} \frac{1}{p} = \sum_{\substack{p \leqslant z \\ \ell \mid a_p}} \frac{1}{p} + \sum_{\substack{z < p \leqslant t \\ \ell \mid a_p}} \frac{1}{p}.$$

Assume that $t \in [w, x]$. Using the formula

$$\sum_{p \leqslant z} \frac{1}{p} = \log\log z + C + O(1/\log z)$$

to bound the first sum on the right, and partial integration together with (9) for the second sum, we obtain

$$\begin{aligned} S_t^{(\ell)} &= \delta_\ell \log_2 t + A \log_2 z + O(1) \qquad (|A| < 1) \\ &= \delta_\ell \log_2 t + O(\log_3 t), \end{aligned} \tag{10}$$

where the implied constant can be taken as 14 for sufficiently large x. Note also that the first term above is $\geqslant (2\kappa)^{-1} \log_3 x$ for $t \in [w, x]$ and any $\ell \leqslant \kappa y$. In particular,

$$S_t^{(\ell)} \in \left[0.5\delta_\ell \log_2 t, 2\delta_\ell \log_2 t\right] \tag{11}$$

provided $\kappa \leqslant 1/56$. In fact, the above argument also gives

$$S_t^{(\ell)} = (1 + o(1))\delta_\ell \log_2 t \quad \text{if} \quad \ell = o(y) \quad \text{as} \quad x \to \infty. \tag{12}$$

The above estimates (11) and (12) hold uniformly for $t \in [w, x]$ and large x. Set

$$\mathcal{E}_{\kappa,1}(x) = \{n \leqslant x : p^2 \mid n \text{ for some prime } p > s\},$$

where $s = (\log_2 x)^{1/(3\kappa)}$. Clearly, $\mathcal{E}_{\kappa,1}(x) \subset \mathcal{E}_\square(x, s^2)$, therefore, by Lemma 4,

$$\#\mathcal{E}_{\kappa,1}(x) \leqslant \#\mathcal{E}_\square(x; s^2) \ll \frac{x}{(\log_2 x)^{1/(3\kappa)}}. \tag{13}$$

Hence, we can and shall assume that $n \notin \mathcal{E}_{\kappa,1}(x)$. Set $L_\ell := \lfloor (\log_3 x)/\log \ell \rfloor$. Since

$$\ell^{L_\ell + 1} > \ell^{(\log_3 x)/\log \ell} = \log_2 x > \kappa y,$$

the largest power of ℓ not exceeding κy can be at most L_ℓ. Write $n = u_\ell v_\ell$, where $\gcd(u_\ell, v_\ell) = 1$, and v_ℓ is made up only of primes $p > s$ with $\ell \mid a_p$. Note that v_ℓ is square-free since $n \notin \mathcal{E}_{\kappa,1}(x)$. Therefore, if $\omega(v_\ell) \geqslant L_\ell$,

$$\ell^{L_\ell} \mid \ell^{\omega(v_\ell)} \mid a_{v_\ell} \mid a_n.$$

By the above remark, the largest power of ℓ not exceeding κy also divides a_n. If $\omega(v_\ell) > L_\ell$ for all $\ell \leqslant \kappa y$, then $n \in \mathcal{G}_\kappa(x)$. Hence, we need to estimate the sets

$$\mathcal{E}_{\kappa,\ell}(x) = \{n = u_\ell v_\ell \leqslant x : \omega(v_\ell) \leqslant L_\ell\}$$

for $\ell \leqslant \kappa y$. We fix ℓ, v_ℓ and for simplicity of notation, drop the indices on u and v. We see that $u \leqslant x/v$ is a number that is free of primes $p > s$ with $\ell \mid a_p$. We distinguish two cases.

Case 1. Assume $x/v > w$.
Then, by Brun's sieve, the number of choices for u is

$$\begin{aligned}
&\ll \frac{x}{v} \prod_{\substack{s<p\leqslant x/v \\ \ell \mid a_p}} \left(1 - \frac{1}{p}\right) \leqslant \frac{x}{v} \prod_{\substack{s<p\leqslant w \\ \ell \mid a_p}} \left(1 - \frac{1}{p}\right) \\
&\leqslant \frac{x}{v} \exp\Big(-S_w^{(\ell)} + \log_4 x + O(1)\Big) \ll \frac{x \log_3 x}{v \exp(S_w^{(\ell)})}.
\end{aligned}$$

Summing over square-free v with at most L_ℓ prime factors $p > s$ with $\ell \mid a_p$, we see that the contribution to $\mathcal{E}_{\kappa,\ell}(x)$ in Case 1 is

$$\ll x \log_3 x \exp\left(-S_w^{(\ell)}\right) T_x^{(\ell)}, \tag{14}$$

where

$$\begin{aligned}
T_x^{(\ell)} &= \sum_{k \leqslant L_\ell} \sum_{\substack{\mu^2(v)=1,\ \omega(v)=k \\ p \mid v \Rightarrow (\ell \mid a_p \text{ and } p>s)}} \frac{1}{v} \\
&\leqslant \sum_{k \leqslant L_\ell} \frac{1}{k!} \left(\sum_{\substack{s<p\leqslant x \\ \ell \mid a_p}} \frac{1}{p} \right)^k \leqslant \sum_{k \leqslant L_\ell} \frac{(S_x^{(\ell)})^k}{k!} \ll \frac{(S_x^{(\ell)})^{L_\ell}}{L_\ell!}.
\end{aligned}$$

Here, the last estimate holds uniformly for $\ell \leqslant y$ and follows easily since

$$\frac{\left(S_x^{(\ell)}\right)^{k+1}/(k+1)!}{\left(S_x^{(\ell)}\right)^{k}/k!} \gg \frac{\delta_\ell \log_2 x}{L_\ell} \gg \delta_\ell \log \ell \left(\frac{\log_2 x}{\log_3 x}\right) \gg \log_3 x,$$

whether $\ell \mid M_E$ or not. Using the inequality $k! \geqslant (k/e)^k$ with $k = L_\ell$, we obtain by (11) that

$$T_x^{(\ell)} \ll \left(\frac{S_x^{(\ell)}}{L_\ell}\right)^{L_\ell} \leqslant \left(\frac{c_1 \delta_\ell \log \ell \log_2 x}{\log_3 x}\right)^{\log_3 x/\log \ell},$$

where we can take $c_1 := 2e$. If $\ell \mid M_E$,

$$T_x^{(\ell)} = \exp\left(O_E\left((\log_3 x)^2\right)\right).$$

By (11), we have $S_w^{(\ell)} \gg_E \log_2 x$ so that

$$T_x^{(\ell)} \leqslant \exp\left(o\left(S_w^{(\ell)}\right)\right) \qquad \text{when } \ell \mid M_E \text{ and as } x \to \infty. \tag{15}$$

If $\ell \nmid M_E$, then $\delta_\ell < 1/(\ell-1) \leqslant 2/\ell$, yielding

$$T_x^{(\ell)} \leqslant \left(\frac{2c_1 \log \ell \log_2 x}{\ell \log_3 x}\right)^{\log_3 x/\log \ell}.$$

To show that

$$T_x^{(\ell)} \leqslant \exp\left(o\left(S_w^{(\ell)}\right)\right) \qquad \text{when } \ell \nmid M_E \text{ and } \ell \leqslant y \tag{16}$$

holds as $x \to \infty$, we take logarithms of both sides and use (11), then the problem reduces to establishing that

$$\left(\frac{\log_3 x}{\log \ell}\right) \log\left(\frac{2c_1 \log \ell \log_2 x}{\ell \log_3 x}\right) = o\left(\frac{\log_2 x}{\ell}\right).$$

Rewriting this as

$$X \log\left(\frac{eY}{X}\right) = o\left(\frac{\log_2 x}{\log_3 x}\right), \tag{17}$$

where $X := \ell/\log \ell$ and $Y := (2c_1 e^{-1}) \log_2 x/\log_3 x := c_2 y$, where $c_2 := 2c_1 e^{-1} = 4$, it is easy to see that the function $X \mapsto X \log(eY/X)$ is increasing for $X \leqslant Y$. Since $X = \ell/\log \ell = o(\log_2 x/\log_3 x) = o(Y)$, it follows that the maximum on the right is obtained when $\ell = y$, in which case the left-hand side of (17) yields a contribution

$$O\left(\frac{\log_2 x \log_4 x}{(\log_3 x)^2}\right),$$

which gives the desired estimate as $x \to \infty$. Thus, (16) holds uniformly for $\ell \leqslant y$. Inserting the estimates (15) and (16) into (14), together with the estimate

$$\log_3 x = \exp(\log_4 x) = \exp\left(o\left(S_w^{(\ell)}\right)\right) \qquad \text{as } x \to \infty,\ \forall \ell \leqslant y,$$

we see that the contribution to $\mathcal{E}_{\kappa,\ell}(x)$ in Case 1 is

$$\leqslant \frac{x}{\exp\left((1+o(1))S_w^{(\ell)}\right)}$$

as $x \to \infty$ uniformly for $\ell \leqslant y$.

Case 2. Assume $x/v \leqslant w$. In this case, $u \leqslant w$. Furthermore, $v \geqslant x/w \geqslant x^{1/2}$ for sufficiently large x. Since $L_\ell \leqslant 2\log_3 x$, it follows that $P = P^+(v) \geqslant x^{1/(4\log_3 x)}$. Write $v = Pv_1$ and fix $v_1 u$. Then, the number of choices for the prime $P \leqslant x/(v_1 u)$ is

$$\pi\left(\frac{x}{uv_1}\right) \ll \frac{x}{uv_1 \log(x/uv_1)} \ll \frac{x\log_3 x}{uv_1},$$

where we used the fact that $x/(uv_1) \geqslant P > x^{1/(4\log_3 x)}$. Summing over all $u \leqslant w$ and square-free v_1 with less than L_ℓ prime factors $p > s$ with $\ell \mid a_p$, we get a contribution to $\mathcal{E}_{\kappa,\ell}(x)$ which is

$$\ll \frac{x\log_3 x}{\log x} \sum_{u\leqslant w} \frac{1}{u} \cdot \left(\sum_{k<L_\ell} \sum_{\substack{\mu^2(v_1)=1,\ \omega(v_1)=k \\ p\mid v \Rightarrow (\ell \mid a_p \text{ and } p>s)}} \frac{1}{v_1} \right) \ll \frac{x(\log_3 x)T_x^{(\ell)}}{\sqrt{\log x}}.$$

Using the bounds on $T_x^{(\ell)}$ (the bound (15) for small ℓ, say $\ell \leqslant 10$ or $\ell \mid M_E$, and the bound (16) for large ℓ, say $\ell \nmid M_E$ and $11 \leqslant \ell \leqslant y$), the above contribution is seen to be

$$\leqslant \frac{x}{(\log x)^{1/2+o(1)}}.$$

Finally combining the estimates from both cases, we conclude that

$$\#\mathcal{E}_{\kappa,\ell}(x) \leqslant \frac{x}{\left(\min\left\{\exp\left(S_w^{(\ell)}\right), (\log x)^{1/2}\right\}\right)^{1+o(1)}}.$$

It follows from (10) that

$$\exp\left(S_w^{(\ell)}\right) \geqslant (\log_2 x)^{1/(2\kappa)-14}$$

uniformly for $\ell \leqslant \kappa y$, and large x. Hence, for $\kappa < 1/100$,

$$\#\mathcal{E}_{\kappa,\ell}(x) \leqslant \frac{x}{(\log_2 x)^{18/(51\kappa)}}$$

uniformly for $\ell \leqslant \kappa y$. Summing this over all ℓ, we conclude that

$$\sum_{\ell\leqslant\kappa y} \#\mathcal{E}_{\kappa,\ell}(x) \ll \frac{xy}{(\log_2 x)^{18/(51\kappa)}} \leqslant \frac{x}{(\log_2 x)^{18/(51\kappa)-1}} \leqslant \frac{x}{(\log_2 x)^{1/(3\kappa)}},$$

which together with the bound (13) finishes the proof of Proposition 1.

Remark 3 The above argument also shows the following. Let $2 \leqslant y \leqslant x$ be such that $y \to \infty$ and $y = o(\log_2 x/\log_3 x)$ as $x \to \infty$. Let

$$\mathcal{E}_y(x) = \{n \leqslant x : q \nmid a_n \text{ for some prime power } q \leqslant y\}.$$

Then,

$$\#\mathcal{E}_y(x) = \frac{x}{(\log x)^{(1+o(1))/y}}$$

as $x \to \infty$.

3.2 The Proof of Theorem 2

I. $\mathcal{A}_\omega$ is dense. Let x be large. Put

$$\mathcal{A}_{\omega,1}(x) = \left\{n \leqslant x : |\omega(n) - \log_2 x| > y\sqrt{\log_2 x}\right\}$$

for some $y \leqslant \sqrt{\log_2 x}$ to be determined below. By Lemma 4, we have

$$\#\mathcal{A}_{\omega,1}(x) = \#\mathcal{E}_\omega(x; y) \ll \frac{x}{y^2}. \tag{18}$$

Assume in what follows that $n \notin \mathcal{A}_{\omega,1}(x)$. Set $z := \kappa \log_2 x/\log_3 x$ with $\kappa = 10^{-3}$, and consider those n satisfying $x/\log x < n \in \mathcal{G}_{2\kappa}(x)$. For sufficiently large x, $z < 2\kappa \log_2 n/\log_3 n$. Since $n \in \mathcal{G}_{2\kappa}(x)$, $\omega(n) \mid \prod_{q \leqslant z} q \mid a_n$, provided that each prime power q dividing $\omega(n)$ satisfies $q \leqslant z$.

Next, we bound $n \leqslant x$ with $\omega(n) = k = qm$ for some $q > z$, and fixed k. Since $n \notin \mathcal{A}_{\omega,1}(x)$,

$$m < k/z \leqslant 1000 \log_3 x \left(1 + \frac{y}{\sqrt{\log_2 x}}\right) \leqslant 2000 \log_3 x.$$

Fixing m, the Brun-Titchmarsh inequality (cf. [18, Theorem 9, page 93]) implies that

$$\#\left\{q : \frac{\log_2 x - y\sqrt{\log_2 x}}{m} \leqslant q \leqslant \frac{\log_2 x + y\sqrt{\log_2 x}}{m}\right\} \ll \frac{y\sqrt{\log_2 x}}{m \log_3 x}.$$

Thus, the contribution from these n is

$$\ll \frac{y\sqrt{\log_2 x}}{\log_3 x} \sum_{m < 2000 \log_3 x} \frac{1}{m} \ll \frac{y\sqrt{\log_2 x}\log_4 x}{\log_3 x}. \tag{19}$$

By [7, page 303]) we have the uniform bound

$$\pi_k(x) = \#\{n \leqslant x : \omega(n) = k\} \ll \frac{x}{\sqrt{\log_2 x}}. \tag{20}$$

Therefore, multiplying the bounds in (19) and (20), we obtain

$$\#\{n \leqslant x : n \notin \mathcal{A}_{\omega,1}(x) \text{ and } q \mid \omega(n) \text{ for some } q > z\} \ll \frac{xy \log_4 x}{\log_3 x}. \tag{21}$$

Choosing $y := (\log_3 x/\log_4 x)^{1/3}$ balances the bounds in (18) and (21), and yields that $\mathcal{A}_\omega(x)$ contains all $n \leqslant x$ with

$$\ll x \left(\frac{\log_4 x}{\log_3 x}\right)^{2/3} \tag{22}$$

exceptions, finishing the first part of the proof..

II. $\mathcal{A}_\Omega$ is dense. Let $\mathcal{A}_{\Omega,1}(x)$ be the set of $n \leqslant x$ having a squarefull divisor s exceeding $(\log_3 x)^2$. By Lemma 4,

$$\#\mathcal{A}_{\Omega,1}(x) \leqslant \#\mathcal{E}_\square(x; (\log_3 x)^2) \ll \frac{x}{\log_3 x}.$$

We assume below that $n \notin \mathcal{A}_{\Omega,1}(x)$. Writing $n = n_1 s$, with $(n_1, s) = 1$, n_1 squarefree and s squarefull, we have $\Omega(n) = \omega(n_1) + \Omega(s)$. Since $s \leqslant (\log_3 x)^2$, it follows that $\Omega(s) < J = \lfloor 4 \log_4 x \rfloor$. Fix s. Then, $n_1 \leqslant x/s$. It follows from Proposition 1 and the estimate

$$\sum_{s \text{ squarefull}} \frac{1}{s} = O(1), \tag{23}$$

that the number of $n \leqslant x$ for which $n_1 \notin \mathcal{G}_{2\kappa}(x/s)$ with $\kappa = 0.001$ has cardinality $O(x/(\log_2 x)^{666})$.

Using (23) together with Lemma 4 we see that the set

$$\mathcal{A}_{\Omega,2}(x) = \{n \leqslant x : n \notin \mathcal{A}_{\Omega,1}(x), |\omega(n_1) - \log_2(x/s)| > y\sqrt{\log_2(x/s)}\}$$

is $\ll x/y^2$. We shall henceforth assume that $n \notin \mathcal{A}_{\Omega,2}(x) \cup \mathcal{A}_{\Omega,1}(x)$. Put $j := \Omega(s)$ and $k := \omega(n_1)$. As in the proof of the first part, if we consider those n satisfying $x/\log x < n \in \mathcal{G}_{2\kappa}(x)$ and if all prime powers of $k+j$ are at most $z = \kappa \log_2 x/\log_3 x$, then $\Omega(n) \mid a_n$. So, it suffices to count the cardinality of the set $\mathcal{A}_{\Omega,3}(x)$ of $n \leqslant x$ such that $k + j = qm$, where $q > z$ is some prime power. Then, $m < 2000 \log_3 x$ for large x and

$$q \in \left[\frac{\log_2(x/s)+j+y\sqrt{\log_2(x/s)}}{m}, \frac{\log_2(x/s)+j-y\sqrt{\log_2(x/s)}}{m}\right].$$

The number of such q, as in the preceding case, is $\ll y\sqrt{\log_2 x}/(m \log_3 x)$ uniformly in $m \leqslant 2000 \log_3 x$, in $j \in \{0, 1, \ldots, J\}$, and in $s \leqslant (\log_3 x)^2$. Summing over m, we get that the number of such k is of order

$$\frac{y\sqrt{\log_2 x}(\log_4 x)}{m \log_3 x}.$$

Multiplying this bound with $x/(s\sqrt{\log_2 x})$, the maximum order of $\pi_k(x/s)$ as given in (20), we conclude that the number of such $n_1 \leqslant x/s$ is

$$\ll \frac{xy(\log_4 x)}{s \log_3 x}.$$

Finally, summing over s yields

$$\#\mathcal{A}_{\Omega,3}(x) \ll \frac{xy(\log_4 x)}{\log_3 x},$$

which is the same as in the first proof. The optimal choice for y is also the same and shows that the number of $n \leqslant x$ for which $\Omega(n) \nmid a_n$ is of the order shown in (22). This completes the proof of the second part of Theorem 2.

3.3 The Proof of Theorem 3

As in the proof of Theorem 2, by Lemma 4, we have

$$\begin{aligned}\#\mathcal{A}_{\tau,1}(x) &= \#\{n \leqslant x : s \mid n \text{ for some squarefull } s > \log_2 x\} \\ &\ll \frac{x}{(\log_2 x)^{1/2}}.\end{aligned}$$

From now on, assume that $n \leqslant x$ and $n \notin \mathcal{A}_{\tau,1}(x)$. Write $n = n_1 s$, where n_1 is the square-free part of n. Then, $\tau(n) = 2^{\omega(n_1)}\tau(s)$. Since $s \leqslant \log_2 x$ and $\tau(s) = s^{o(1)}$ as $s \to \infty$, it follows that $\tau(s) \leqslant \kappa \log_2 x/(2 \log_3 x)$ with $\kappa = 0.001$, provided that x is large enough. By Proposition 1, it follows that if $x/\log x < n \in \mathcal{G}_\kappa(x)$, then the largest odd divisor of $\tau(n)$ (hence, all odd divisors of $\tau(n)$) divides a_n, and that $\mathcal{G}_\kappa(x)$ contains all integers $n \leqslant x$ with $O(x/(\log_2 x)^{333})$ exceptions. Thus, it is sufficient to consider, as we shall do below, numbers in $\mathcal{G}_\kappa(x)\backslash\mathcal{A}_{\tau,1}(x)$.

Let $\varepsilon > 0$ be small but fixed. By Lemma 4, it follows that

$$\#\mathcal{A}_{\tau,2}(x) = \#\{n \leqslant x : |\omega(n) - \log_2 x| > \varepsilon \log_2 x\} = O_\varepsilon\left(\frac{x}{\log_2 x}\right).$$

From now on, we assume that $n \notin \mathcal{A}_{\tau,2}(x)$. Writing $\nu_2(m)$ for the exponent of 2 in the factorization of m, we have

$$\nu_2(\tau(n)) = \omega(n_1) + \nu_2(\tau(s)) = \omega(n_1) + O(\log_3 x),$$

so $\nu_2(\tau(n)) \in [(1-2\varepsilon)\log_2 x, (1+2\varepsilon)\log_2 x]$, provided that $x > x_\varepsilon$, since $s \leqslant \log_2 x$ and $n \notin \mathcal{A}_{\tau,2}(x)$.

Let $\mathcal{P}$ be a subset of primes of positive density $\delta_{\mathcal{P}}$ satisfying

$$\#\mathcal{P}(t) = \delta_{\mathcal{P}} \frac{t}{\log t}\Big(1 + O_{\mathcal{P}}\Big(\frac{1}{\log t}\Big)\Big). \tag{24}$$

Then, the estimate (see [19] or [18, Ch. 3.4])

$$\sum_{n \leqslant x} |\omega_{\mathcal{P}}(n) - \delta_{\mathcal{P}} \log_2 x|^2 = O_{\mathcal{P}}(x \log_2 x)$$

holds, where $\omega_{\mathcal{P}}(n)$ is the number of primes divisors of n in $\mathcal{P}$. Thus, as before

$$\#\mathcal{A}_{\tau,3}(x) = \#\{n \leqslant x : |\omega_{\mathcal{P}}(n) - \delta_{\mathcal{P}} \log_2 x| > \varepsilon \log_2 x\} \ll_{\varepsilon,\mathcal{P}} \frac{x}{\log_2 x}.$$

Assume condition (i) of the theorem. Then, for all odd $p \nmid N_E$, we have that $E(\mathbb{F}_p)$ has even order (cf. [15, Ch VII, Prop 3.1b]). Hence, a_p is even. Let $\mathcal{P}$ be the set of primes such that $4 \mid a_p$. By Lemma 2, $4 \mid a_p$ for infinitely many super-singular odd primes $p \nmid N_E$. Thus, $T_0(4) \neq \emptyset$ and Lemma 1 can be used to conclude that $\mathcal{P}$ has positive density $\delta_{\mathcal{P}}$ and estimate (24) holds. We shall assume below that $n \notin \mathcal{A}_{\tau,3}(x)$. Then, n_1 is divisible by at least $(1 - \delta_{\mathcal{P}} - 2\varepsilon)\log_2 x$ odd primes not in $\mathcal{P}$ and by at least $(\delta_{\mathcal{P}} - 2\varepsilon)\log_2 x$ odd primes in $\mathcal{P}$. We deduce by the multiplicativity of a_n that

$$\nu_2(a_n) \geqslant (1 + \delta_{\mathcal{P}} - 6\varepsilon)\log_2 x > (1 + 2\varepsilon)\log_2 x \geqslant \nu_2(\tau(n))$$

for all sufficiently large n, provided $\varepsilon < \delta_{\mathcal{P}}/8$. Thus, $\tau(n) \mid a_n$ for such n, since the largest odd divisor of $\tau(n)$ already divides a_n as mentioned above.

Assume condition (ii) of the theorem now. Then, it is easy to compute the density δ_k of the primes p such that $a_p \equiv 0 \pmod{2^k}$. Indeed, all we have to compute is the number of matrices in $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$. These matrices are either of the form

$$\begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix}, \quad \text{or} \quad a\begin{pmatrix} 1 & b/a \\ c/a & -1 \end{pmatrix}$$

modulo 2^k, where on the left b and c are odd, while on the right, a is odd and the product of (b/a) and (c/a) is not 1 modulo 2^k. The number of possibilities on the left is $\varphi(2^k)^2 = 2^{2k-2}$, while the number of possibilities on the right is

$$\varphi(2^k)(2^k + 2^k - 1 + \varphi(2^k)(\varphi(2^k) - 1)) = 2^{k-1}(2^{k+1} - 1 + 2^{2k-2} - 2^{k-1}).$$

Hence, the total number of elements is

$$2^{k-1}(2^{2k-2} + 2^{k+1} - 1),$$

and $\#\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) = 6 \cdot 2^{4k-4}$ since each one of the 6 elements of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ has $(2^{k-1})^4$ lifts to $\mathrm{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$. Hence,

$$\delta_k = \frac{2^{k-1}(2^{2k-2} + 2^{k+1} - 1)}{6 \times 2^{4(k-1)}} = \frac{1}{6} \cdot \frac{1}{2^{k-1}} + \frac{2}{3} \cdot \frac{1}{4^{k-1}} - \frac{1}{6} \cdot \frac{1}{8^{k-1}}.$$

Then,

$$\sum_{k \geqslant 1} \delta_k = \frac{1}{6} \sum_{k \geqslant 1} \frac{1}{2^{k-1}} + \frac{2}{3} \sum_{k \geqslant 1} \frac{1}{4^{k-1}} - \frac{1}{6} \sum_{k \geqslant 1} \frac{1}{8^{k-1}} = \frac{2}{3} + \frac{8}{9} - \frac{4}{21} = \frac{67}{65} > 1.$$

This shows via the preceding arguments that for all fixed $\varepsilon > 0$, the exponent of 2 in the factorization of a_n is at least $(67/65 - \varepsilon) \log_2 x$ for all $n \leqslant x$ with $O_\varepsilon(x/\log_2 x)$ exceptions. If ε is chosen such that $67/65 - \varepsilon > 1 + 2\varepsilon$ (so $\varepsilon < 2/195$), then $\tau(n) \mid a_n$ as claimed.

3.4 The Proof of Theorem 5

As in the previous subsections,

$$\begin{aligned} \#\mathcal{D}_{E,1}(x) &= \#\left\{n \leqslant x : s \mid n \text{ for some squarefull } s > (\log_2 x)^2\right\} \\ &\ll \frac{x}{\log_2 x}. \end{aligned} \tag{25}$$

Let $y := \exp(\log x / \log_3 x)$ and

$$\mathcal{D}_{E,2}(x) = \{n \leqslant x : P^+(n) \leqslant y\}.$$

By [18, III.5.3. Theorem 6], uniformly for $x \geqslant y \geqslant 2$, we have

$$\#\mathcal{D}_{E,2}(x) = \Psi(x, y) = x\rho(u) + O\Big(\frac{x}{\log y}\Big),$$

where $\rho(u)$ is the Dickman's function and $u = \log x / \log y$. Since $u = \log_3 x$, $u \log u = (\log_3 x)(\log_4 x)$, and ρ satisfies $\rho(u) < e^{u - u\log u + O(1)}$ (cf. [18, III.5.3. Theorem 5 (iv)], we obtain

$$\#\mathcal{D}_{E,2}(x) \ll \frac{x}{\log_2 x}. \tag{26}$$

Assume that $n \in \mathcal{D}_E(x) \setminus \big(\mathcal{D}_{E,1}(x) \cup \mathcal{D}_{E,2}(x)\big)$. Write $n = Pm$, where $P = P^+(n) > y$, and fix m. Then, $P \leqslant x/m$ can be chosen in

$$\pi\left(\frac{x}{m}\right) \ll \frac{x}{m \log(x/m)} \ll \frac{x(\log_3 x)}{m \log x} \tag{27}$$

ways. We put $w = \exp(\sqrt{\log x})$, and write $m = m_1 m_2$ with $P^+(m_1) \leqslant w$, and $p > w$ for all $p \mid m_2$. Fix m_2 and sum up the bound (27) over m_1 with $P(m_1) \leqslant w$. We then obtain a bound

$$\ll \frac{x(\log_3 x)}{m_2 \log x} \cdot \sum_{P(m_1)\leqslant w} \frac{1}{m_1} \ll \frac{x(\log_3 x)}{m_2\sqrt{\log x}}, \tag{28}$$

by using the fact that

$$\sum_{P(m_1)\leqslant w} \frac{1}{m_1} = \prod_{p\leqslant w} \left(1 - \frac{1}{p}\right)^{-1} \ll \exp\left(\sum_{p\leqslant w} \frac{1}{p}\right) \ll \sqrt{\log x}.$$

Suppose there is at least one prime $p \mid m_2$ satisfying the following:

Condition A. *a_p has a prime factor $\ell_p \in \mathcal{I}_p = [(\log_2 p)^3, (\log p)^{1/(130\log_3 p)}]$ such that $\ell_p \nmid p - 1$.*

Since $p > w$, $\ell_p \gg (\log_2 x)^3$. Since p is large and $n \notin \mathcal{D}_{E,1}(x)$, it follows that $p \| n$. Thus, $\ell_p \mid a_p \mid a_n \mid \varphi(n)$. It is not possible that $\ell_p^2 \mid n$ for large x because $\ell_p \gg (\log_2 x)^3$ and $n \notin \mathcal{D}_{E,1}(x)$. Thus, there exists a prime factor $r \neq p$ of n such that $\ell_p \mid r - 1$. Then, $pr \mid n$ with $\ell_p \mid a_p$ and $\ell_p \in \mathcal{I}_p$. Let $\mathcal{D}_{E,3}(x)$ be the set of such n. Then,

$$\#\mathcal{D}_{E,3}(x) \ll \sum_{p\in[w,x]} \frac{x}{p} \sum_{\substack{r\leqslant x \\ r\equiv 1 \,(\mathrm{mod}\, \ell_p)}} \frac{1}{r} \ll \sum_{p\in[w,x]} \frac{x}{p(\log_2 x)^2} \ll \frac{x}{\log_2 x}. \tag{29}$$

It turns out that we have to bound the set $\mathcal{D}_{E,4}(x)$ of $n \leqslant x$ for which Condition A fails for all prime factors p of m_2. In this case, every prime divisor p of m_2 satisfies one of the following:

(i) There exists a prime factor $\ell_p \in \mathcal{I}_p$ of a_p such that $\ell_p \mid p - 1$,
(ii) a_p is free of primes in $\mathcal{I}_p$.

Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be the sets of primes p satisfying (i) and (ii), respectively. We show that both sets have small counting functions so that $\#\mathcal{D}_{E,4}(x)$ is negligible, thus completing the proof.

For $\mathcal{P}_1$, let t be a large real number and let $p \in \mathcal{P}_1(t)$. We may assume that $p > t/(\log_2 t)^2$. Let $y = 0.5(\log_2 t)^3$ and $z = (\log t)^{1/(130\log_3 x)}$. Fix an $\ell \in \mathcal{J}_t = [y, z]$. We count $p \in \mathcal{P}_1(x)$ for which $\ell = \ell_p$. Let $\mathcal{P}_{1,\ell}(t)$ be the set of such primes. Thus,

$$p \equiv 1 \,(\mathrm{mod}\, \ell), \qquad a_p \equiv 0 \,(\mathrm{mod}\, \ell).$$

Note that there exist matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ of determinant 1 and trace 0, such as $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. For t large enough, $y > N_E$ so that $\ell \nmid N_E$. By Lemma 1 and (5), we have that $\mathcal{P}_{1,\ell}(t)$ has cardinality

$$\#\mathcal{P}_{1,\ell}(t) \ll \frac{\#\mathcal{A}_{1,0}(\ell)\pi(t)}{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} \ll \frac{t}{\ell^2 \log t}$$

so that

$$\#\mathcal{P}_1(t) \ll \frac{t}{\log t} \sum_{\ell\in\mathcal{J}_t} \frac{1}{\ell^2} \ll \frac{t}{(\log t)(\log_2 t)^3}.$$

We deduce that

$$\sum_{p\in\mathcal{P}_1} \frac{1}{p} = O(1). \tag{30}$$

Now we deal with $\mathcal{P}_2$. Apply the Brun-pure sieve (see Corollary 1.1 and its proof on Page 58 in [18]) to the set of a_p with $p \in \mathcal{P}_2(t)$. Put $P := \prod_{\ell\in\mathcal{J}_t} \ell$ where $w \leqslant t \leqslant x$. Then,

$$\#\mathcal{P}_2(t) \leqslant \sum_{\substack{d\mid P\\ \omega(d)\leqslant 2h}} \mu(d)\pi_{T_0(d)}(t),$$

where $2h$ is chosen as the largest even number not exceeding $10\log_3 t$ so that all moduli d satisfy $d^{12}\log d \ll \log t$ for large t. Then, by Lemma 1

$$\pi_{T_0(d)}(t) = \delta_d \pi(t) + O(t/\log^2 t),$$

uniformly for all d above, where $\delta_d = \prod_{\ell\mid d}\delta_\ell$ is the product of densities. Since $\delta_\ell \ll \ell^{-1}$, we obtain

$$\begin{aligned}\#\mathcal{P}_2(t) &\leqslant \sum_{\substack{d\mid P\\ \omega(d)\leqslant 2h}} \mu(d)\left(\delta_d\pi(t) + O(t/\log^2 t)\right)\\ &= \pi(t)\sum_{d\mid P}\mu(d)\delta_d + O_E\left(\frac{t}{(\log t)^2}\sum_{\substack{d\mid P\\ \omega(d)\leqslant 2h}} 1 + \frac{t}{\log t}\sum_{\substack{d\mid P\\ \omega(d)>2h}}\frac{1}{d}\right).\end{aligned}$$

The first term above is

$$\ll \pi(t)\prod_{\ell\in\mathcal{J}_t}(1-\delta_\ell) \ll \pi(t)\left(\frac{(\log_3 t)^2}{\log_2 t}\right),$$

which dominates the other error terms with our choice of the parameters. Thus, given a large x, partial summation gives

$$\sum_{\substack{w\leqslant p\leqslant x\\ p\in\mathcal{P}_2}}\frac{1}{p} \ll \int_w^x \frac{(\log_3 t)^2 dt}{t(\log t)(\log_2 t)} \ll (\log_3 t)^3\Big|_{t=w}^{t=x} \ll (\log_3 x)^2. \tag{31}$$

Write $m_2 = k_1 k_2$ such that all prime factors of k_i lie in $\mathcal{P}_i$. Going back to equation (28) and summing up over all possible values of k_1 and k_2, we derive using (30), (31) that

$$\begin{aligned}\frac{|\mathcal{D}_{E,4}(x)|\sqrt{\log x}}{x \log_3 x} &\ll \left(\sum_{\substack{\mu^2(k_1)=1\\ p|k_1 \Rightarrow p\in\mathcal{P}_1}} \frac{1}{k_1}\right)\left(\sum_{\substack{\mu^2(k_2)=1\\ p|k_2 \Rightarrow p\in\mathcal{P}_2\cap[w,x]}} \frac{1}{k_2}\right)\\ &\ll \prod_{p\in\mathcal{P}_1}\left(1+\frac{1}{p}\right)\prod_{\substack{p\in\mathcal{P}_2\\ w\leqslant p\leqslant x}}\left(1+\frac{1}{p}\right)\\ &\ll \exp\left(\sum_{p\in\mathcal{P}_1}\frac{1}{p}+\sum_{\substack{p\in\mathcal{P}_2\\ w\leqslant p\leqslant x}}\frac{1}{p}\right) = \exp(O((\log_3 x)^2)).\end{aligned}$$

Thus,

$$\#\mathcal{D}_{E,4}(x) \leqslant \frac{x}{(\log x)^{1/2+o(1)}}.$$

Combining this with (25), (26) and (29), we obtain the claimed result.

3.5 The Proof of Theorem 4

Define

$$\mathcal{P} = \{p : \varphi(|a_p|) \text{ is a power of } 2\}.$$

We shall prove that

$$\#\mathcal{P}(t) \ll \frac{t(\log_2 t)^3}{(\log t)^{13/12}}. \tag{32}$$

Let c_4 be the constant appearing in the statement of Lemma 1 in the inequality $n^{12}\log n \leqslant c_4 \log x$. Assume t is large, and let $U := U(t)$ be maximal such that $n := 2^{U(t)}$ satisfies $n^{12}\log n \leqslant c_4 \log t$. Clearly, the inequality $n^{12}\log n > c_5 \log t$ holds for t large enough, where we can take $c_5 := c_4/3$. Recall that if $\varphi(m)$ is a power of 2, then

$$m = 2^{\alpha} F_{n_1} F_{n_2} \dots F_{n_t},$$

where $\alpha \geqslant 0$ and $0 \leqslant n_1 < n_2 < \cdots < n_t$ are such that $F_{n_i} = 2^{2^{n_i}} + 1$ are primes for $i = 1, \ldots, t$. Put

$$\mathcal{A}(t) = \left\{ \pm 2^{\alpha} F_{n_1} \ldots F_{n_s} : \alpha \leqslant U(t), \text{ and } 2^{n_s} < U(t) \right\}.$$

Since $\alpha \leqslant U(t)$ and $2^{12U(t)} \log(2^{U(t)}) \leqslant c_4 \log t$, we have $U(t) = O(\log_2 t)$, and hence, $\alpha = O(\log_2 t)$. Furthermore, we have $2^{n_s} = O(\log_2 t)$, so $n_s \leqslant (1/\ln 2) \log_3 t + c_6$, we see that $n_i \in \{0, 1, \ldots, \lfloor (1/\ln 2) \log_3 t + c_6 \rfloor\}$. The number of subsets of this set is at most

$$2^{(1/\ln 2) \log_3 t + c_6 + 1} = O(\log_2 t).$$

Thus, α and $\prod_i F_{n_i}$ can be chosen in $O(\log_2 t)$ ways, showing that

$$\#\mathcal{A}(t) \ll (\log_2 t)^2.$$

Take $p \in \mathcal{P}(t)$. Write

$$a_p = \pm 2^{\alpha_1} F_{n_1} \ldots F_{n_s} \ldots F_{n_{s+1}} \ldots F_{n_t},$$

where $0 \leqslant n_1 < \cdots < n_t$, and n_s is maximal such that $2^{n_s} \leqslant U(t)$. Since $2^{2^{n_i}} \geqslant 2^{U(t)}$ for $i \geqslant s + 1$, we see that

$$a_p \equiv a \pmod{2^{U(t)}},$$

for some a either zero (say if $\alpha_1 \geqslant U(t)$), or in $\mathcal{A}(t)$. This can be done is $\#\mathcal{A}(t) + 1 = O((\log_2 t)^2)$ ways. For each such choice, Lemma 1 implies

$$\pi_{T_a(2^{U(t)})}(t) \ll \left(\frac{\#T_a(2^{U(t)})}{\#\mathrm{G}(2^{U(t)})} \right) \frac{t}{\log t}.$$

It is clear that $\#T_a(2^{U(t)}) = O(2^{3U(t)})$. In fact, certainly the number of matrices in $\mathrm{GL}_2(\mathbb{Z}/2^{U(t)}\mathbb{Z})$ having trace congruent to $a \pmod{2^{U(t)}}$ is $O(2^{3U(t)})$, while $\#\mathrm{G}(2^{U(t)}) \gg 2^{4U(t)}$. Thus, for a fixed a,

$$\pi_{T_a(2^{U(t)})}(t) \ll \frac{t}{2^{U(t)} \log t} \ll \frac{t (\log_2 t)}{(\log t)^{13/12}}.$$

Summing over all $a \in \mathcal{A}(t)$, we obtain

$$\#\mathcal{P}(t) \ll \frac{t (\log_2 t) \#\mathcal{A}(t)}{(\log t)^{13/12}} \ll \frac{t (\log_2 t)^3}{(\log t)^{13/12}},$$

which is what we wanted. It follows that $\sum_{p \in \mathcal{P}} p^{-1} = O(1)$.

Let x be large and let $\mathcal{C}_{E,1}(x)$ be the set of $n \leqslant x$ which have a squarefull factor $s \geqslant (\log x)^4$. As before,

$$\#\mathcal{C}_{E,1}(x) \ll \frac{x}{(\log x)^2}. \tag{33}$$

Put $y = \exp\big(\log x \log_3 x/2\log_2 x\big)$, and consider

$$\mathcal{C}_{E,2} := \{n \leqslant x : P^+(n) \leqslant y\}.$$

By [18, III.5.5 Corollary 9.3], uniformly for

$$x \geqslant 2 \quad \text{and} \quad \exp\big((\log x)^{5/3+\epsilon}\big) \leqslant y \leqslant x,$$

we have

$$\#\mathcal{C}_{E,2}(x) = \Psi(x, y) = x\rho(u)\Big\{1 + O\Big(\frac{\log(u+1)}{\log y}\Big)\Big\} \ll xe^{u-u\log u+O(1)},$$

where $u = \log x/\log y$. For $u = 2\log_2 x/\log_3 x$, it follows that $u\log u = (2 + o(1))\log_2 x$. Therefore,

$$\#\mathcal{C}_{E,2}(x) \leqslant \frac{x}{(\log x)^{2+o(1)}} \quad \text{as} \quad x \to \infty. \tag{34}$$

Assume that $n \in \mathcal{C}_E(x)\setminus\big(\mathcal{C}_{E,1}(x) \cup \mathcal{C}_{E,2}(x)\big)$. Write $n = Pm$, where $P = P^+(n) > y$. Since $y > (\log x)^4$ for large x and $n \notin \mathcal{C}_{E,1}(x)$, $P \nmid m$. For fixed m, by multiplicativity of a_n, $P \in \mathcal{P}(x/m)$. So, by (32), we obtain that the number of choices for $P \leqslant x/m$ is

$$\ll \frac{x(\log_2 x)^3}{m(\log(x/m))^{13/12}} \ll \frac{x(\log_2 x)^{49/12}(\log_3 x)^{-13/12}}{m(\log x)^{13/12}}.$$

Write $m = m_1 s$, where m_1 is squarefree. Then, every prime dividing m_1 is in $\mathcal{P}$. Summing up the above bound over all possible m_1 and s, we derive that

$$\#\mathcal{C}_{E,3} \ll \frac{x(\log_2 x)^{49/12}(\log_3 x)^{-13/12}}{(\log x)^{13/12}}. \tag{35}$$

The desired conclusion follows now from estimates (33), (34) and (35).

3.6 The Proof of Theorem 6

Let x be large and $n \in \mathcal{F}_E(x)$. Then, $n - \varphi(n) = a_n - 1$. If p is the smallest prime factor of n, then

$$\frac{n}{p} \leqslant n - \varphi(n) = |a_n - 1| \leqslant n^{1/2}\tau(n) + 1 \leqslant n^{1/2+o(1)}. \qquad (n \to \infty)$$

Therefore, $p > n^{1/2-o(1)}$ as $n \to \infty$. In particular, $p > n^{0.49}$ if n is sufficiently large. This shows that $n = p,\ p^2$ or pq for primes p and q with $p \neq q$. Let $\mathcal{F}_{E,1}(x)$ be the set of such $n \leqslant x$ with $n = p$ a prime. Then, $p - a_p + 1 = \varphi(p) = p - 1$, so $a_p = 2$ as noted in the introduction. The set of numbers $p \leqslant x$ with this property has counting function

$$\#\mathcal{F}_{E,1}(x) \ll \frac{x(\log_2 x)^{1/2}(\log_3 x)^{1/4}}{(\log x)^{5/4}} \qquad (36)$$

by Serre's result, Lemma 3. Let $\mathcal{F}_{E,2}(x)$ be the set of $n \leqslant x$ with $n = p^2$. Then, $p^2 - (a_p^2 - 2p) + 1 = \varphi(p^2) = p^2 - p$, so $a_p^2 = 3p + 1$. This gives $(a_p - 1)(a_p + 1) = 3p$. Thus, either $a_p \pm 1 = \pm 1$ and $a_p \mp 1 = \pm 3p$, or $a_p \pm 1 = \pm 3$ and $a_p \mp 1 = \pm p$. The only possibilities are $p = 5$ and $a_p = \pm 4$. Thus, $\mathcal{F}_{E,2}(x)$ contains at most one element, namely 25.

Let $\mathcal{F}_{E,3}(x)$ be the set of $n = pq$. Then,

$$pq - a_p a_q + 1 = (p-1)(q-1) = pq - p - q + 1,$$

so $a_p a_q = p + q$. Assume $p < q$. Then,

$$\sqrt{\frac{q}{p}} < \sqrt{\frac{p}{q}} + \sqrt{\frac{q}{p}} = \frac{|a_p a_q|}{\sqrt{pq}} < 4,$$

showing that $q < 16p$. Since $pq \leqslant x$, we have $p < \sqrt{x}$. Furthermore, given a fixed q, we have that $q \in (p, 16p)$ and $q \equiv -p \pmod{a_p}$. Brun-Titchmarsh inequality implies that the number of such q is at most

$$\pi\left(x/p; a_p, -p\right) \ll \frac{x}{p\varphi(|a_p|)\log(x/p|a_p|)} \ll \frac{x \log_2 x}{p|a_p| \log x},$$

where we used $p|a_p| \leqslant 2x^{3/4}$, so $\log(x/(p|a_p|)) \gg \log x$, and that $\varphi(a)/a \gg 1/\log_2 x$ for $a \leqslant x$. Assume that $n \in [x/2, x]$. Then,

$$p < q + p = |a_p a_q| \leqslant 2|a_p|\sqrt{q} \leqslant 8p^{1/2}|a_p|,$$

so $|a_p| > p^{1/2}/8$. Furthermore, $x/2 \leqslant n = pq \leqslant 16p^2$, so $p \geqslant c_3 x^{1/2}$ with $c_3 := 2^{-2.5}$. Thus, $|a_p| \gg p^{1/2} \gg x^{1/4}$. Hence,

$$\begin{aligned} \#\left(\mathcal{F}_{E,3}(x)\backslash\mathcal{F}_{E,3}(x/2)\right) &\ll \frac{x(\log_2 x)}{(\log x)^2} \sum_{c_3 x^{1/2} \leqslant p \leqslant x} \frac{1}{p|a_p|} \\ &\ll \frac{x^{3/4}\log_2 x}{(\log x)^2} \sum_{c_3 x^{1/2} \leqslant p \leqslant x} \frac{1}{p} \\ &\ll \frac{x^{3/4}\log_2 x}{(\log x)^2} \end{aligned}$$

Replacing x by $x/2$, then by $x/4$, etc., and summing up the resulting inequalities, we conclude that

$$\#\mathcal{F}_{E,3}(x) \ll \frac{x^{3/4}\log_2 x}{(\log x)^2},$$

which together with (36) and the fact that $\mathcal{F}_{E,2}(x)$ has at most one element gives us the desired conclusion.

3.7 The Proof of Proposition 7

This is identical with the proof of Proposition 1. It is based on the fact that $C_0(n)$ is non-empty since it always contains the identity element in $G(n)$. Furthermore, if we put

$$\rho_\ell := \frac{\#C_0(\ell)}{\#\,\mathrm{G}(\ell)},$$

then ρ_ℓ is a positive rational number satisfying the same structural properties as δ_ℓ from the proof of Proposition 1 for primes $\ell \leqslant y$. In particular, estimates (7) and (8) hold for $\ell \nmid M_E$ because of (6) and the fact that $\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \ell(\ell-1)(\ell^2-1)$. Furthermore, the estimate (9) holds with T_0 replaced by C_0 by Lemma 1 uniformly for $\ell \leqslant y$ and $t \in (z, x]$. Thus, the proof carries through identically and even Remark 3 holds if we replace a_n by E_n.

3.8 The Proof of Theorem 8

Let $t_n := \mathrm{LCM}\{t_{p^e} : p^e \| n\}$. Since $E(\mathbb{F}_{p^e}) = \mathbb{Z}/t_{p^e}\mathbb{Z} \times \mathbb{Z}/d_{p^e}\mathbb{Z}$ holds with some divisor d_{p^e} of t_{p^e}, it follows easily that

$$\mathrm{rad}(E_n) = \mathrm{rad}(t_n). \tag{37}$$

Let x be large and y be some parameter tending to infinity with x such that $y = o(x)$. By Remark 3 and its analogue concerning the exceptional set of numbers $n \leqslant x$ such that E_n is not a multiple of every prime power $q \leqslant y$, we obtain

$$\#\mathcal{EC}_{E,1}(x) = \#\{n \leqslant x : q \nmid \gcd(a_n, E_n) \text{ for some prime power } q \leqslant y\}$$
$$\leqslant \frac{x}{(\log x)^{(1+o(1))/y}} \quad \text{as } x \to \infty.$$

Assume now that $n \in \mathcal{EC}_{E,2}(x) := \mathcal{EC}_E(x) \backslash \mathcal{EC}_{E,1}(x)$. From (37) it follows that for such n, both t_n and a_n are divisible by all primes $\ell \leqslant y$. Since $t_n \mid n - a_n + 1$, $n \equiv -1 \pmod{M}$, where $M = \prod_{\ell \leqslant y} \ell$. The number of such $n \leqslant x$ is at most $\lfloor x/M \rfloor + 1 \leqslant 2x/M$. By the Prime Number Theorem, $M = \exp((1 + o(1))y)$. Hence,

$$\#\mathcal{EC}_{E,2}(x) \leqslant \frac{x}{\exp((1 + o(1))y)},$$

and therefore,

$$\#\mathcal{EC}_E(x) \leqslant \frac{x}{(\log x)^{(1+o(1))/y}} + \frac{x}{\exp((1 + o(1))y)}. \tag{38}$$

The optimal choice for y is $y = \sqrt{\log_2 x}$, which leads to the desired conclusion via inequality (38).

Acknowledgements We thank the referee for comments which improved the quality of this paper. This work was initiated during Luca's visit to Turkey in October of 2012. He thanks TÜBİTAK for the financial support and thank the mathematics departments of Bilkent University and Selçuk University for their hospitality.

Funding The first author is supported by the Scientific and Technological Research Council of Turkey [114F404]. The second author was partially supported by Grant CPRR160325161141 and an A-rated scientist award both from the NRF of South Africa and by Grant No. 17-02804S of the Czech Granting Agency.

References

1. Banks, W., Luca, F., Shparlinski, I.E.: Some divisibility properties of the Euler function. Glasgow Math. J. **47**, 517–528 (2005)
2. Cojocaru, A.C., Fouvry, É., Murty, M.R.: The square sieve and the Lang–Trotter conjecture. Can. J. Math. **57**, 1155–1177 (2005)
3. Cooper, C.N., Kennedy, R.N.: Chebyshev's inequality and natural density. Am. Math. Mon. **96**, 118–124 (1989)
4. David, C., Wu, J.: Pseudoprime reductions of elliptic curves. Can. J. Math. **64**, 81–101 (2012)
5. Duke, W., Tóth, Á.: The splitting of primes in division fields of elliptic curves. Exp. Math. **11**(4), 555–565 (2002)
6. Elkies, N.D.: The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. Invent. Math. **89**, 561–567 (1987)
7. Elliott, P.D.T.A.: Probabilistic Number Theory II. Springer, New York (1980)
8. Erdős, P., Pomerance, C.: On a theorem of Besicovitch: values of arithmetic functions that divide their arguments. Indian J. Math. **32**, 279–287 (1990)
9. Luca, F.: On numbers n for which $\Omega(n)$ divides F_n. Fibonacci Q. **41**, 365–371 (2003)
10. Luca, F.: On $f(n)$ modulo $\omega(n)$ and $\Omega(n)$ with f a polynomial. J. Aust. Math. Soc. **77**, 149–164 (2004)
11. Luca, F., Pomerance, C.: On some problems of Mąkowski–Schinzel and Erdős concerning the arithmetical functions φ and σ. Colloq. Math. **92**, 111–130 (2002)

12. Luca, F., Sankaranarayanan, A.: On the positive integers n divisible by $\ell^{\omega(n)}$. Publ. Math. (Beograd) **76**(90), 89–99 (2004)
13. Luca, F., Shparlinski, I.E.: On the counting function of elliptic Carmichael numbers. Can. Math. Bull. **57**, 105–112 (2014)
14. Serre, J.P.: Quelques applications du théorème de densité de Chebotarev. Inst. Hautes Études Sci. Publ. Math. **54**, 123–201 (1981)
15. Silverman, J.H.: The Arithmetic of Elliptic Curves. Springer, Berlin (1995)
16. Silverman, J.H.: Carmichael numbers and elliptic Korselt criteria. Acta Arith. **155**(3), 233–246 (2012)
17. Spiro, C.: The frequency with which an integral-valued, prime-independent, multiplicative or additive function of n divides a polynomial function of n. Ph.D. Thesis, University of Illinois, Urbana-Champaign (1981)
18. Tenenbaum, G.: Introduction to Analytic and Probabilistic Number Theory. Cambridge University Press, Cambridge (1995)
19. Túran, P.: On a theorem of Hardy and Ramanujan. J. Lond. Math. Soc. **9**, 274–276 (1934)