Canad. J. Math. Vol. **68** (4), 2016 pp. 721–761
http://dx.doi.org/10.4153/CJM-2015-013-1

The Frequency of Elliptic Curve Groups over Prime Finite Fields

Vorrapan Chandee, Chantal David, Dimitris Koukoulopoulos, and Ethan Smith

Abstract. Letting p vary over all primes and E vary over all elliptic curves over the finite field $\mathbb{F}_p$, we study the frequency to which a given group G arises as a group of points $E(\mathbb{F}_p)$. It is well known that the only permissible groups are of the form $G_{m,k} := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$. Given such a candidate group, we let $M(G_{m,k})$ be the frequency to which the group $G_{m,k}$ arises in this way. Previously, C. David and E. Smith determined an asymptotic formula for $M(G_{m,k})$ assuming a conjecture about primes in short arithmetic progressions. In this paper, we prove several unconditional bounds for $M(G_{m,k})$, pointwise and on average. In particular, we show that $M(G_{m,k})$ is bounded above by a constant multiple of the expected quantity when $m \le k^A$ and that the conjectured asymptotic for $M(G_{m,k})$ holds for almost all groups $G_{m,k}$ when $m \le k^{1/4-\epsilon}$. We also apply our methods to study the frequency to which a given integer N arises as a group order $\#E(\mathbb{F}_p)$.

1 Introduction

Given an elliptic curve E over the prime finite field $\mathbb{F}_p$, we let $E(\mathbb{F}_p)$ denote its set of $\mathbb{F}_p$ points. It is well known that $E(\mathbb{F}_p)$ admits the structure of an abelian group, and in fact, $E(\mathbb{F}_p) \cong G_{m,k} := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ for some positive integers m and k. It is natural to wonder which groups of the form $G_{m,k}$ arise in this way and how often they occur as p varies over all primes and E varies over all elliptic curves over $\mathbb{F}_p$. The former problem of characterizing which groups are realized in this way was studied in [BPS12, CDKS], while the frequency of occurrence was studied by C. David and E. Smith [DS14b]. In the present work, we explore the frequency of occurrence further.

Given a group G of the form $G_{m,k} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$, we set $N = |G| = m^2k$ and let $M_p(G)$ denote the weighted number of isomorphism classes of elliptic curves over $\mathbb{F}_p$ with group isomorphic to G, that is to say,

$$M_p(G) = \sum_{\substack{E/\mathbb{F}_p \\ E(\mathbb{F}_p)\cong G}} \frac{1}{|\operatorname{Aut}_p(E)|},$$

where the sum is taken over all isomorphism classes of elliptic curves over $\mathbb{F}_p$ and $|\operatorname{Aut}_p(E)|$ is the number of $\mathbb{F}_p$-automorphisms of E. It is worth noting here that $|\operatorname{Aut}_p(E)| = 2$ for all but a bounded number of isomorphism classes E over $\mathbb{F}_p$, and

Received by the editors August 25, 2014.
Published electronically April 27, 2016.
AMS subject classification: **11G07**, 11N45, 11N13, 11N36.
Keywords: average order, elliptic curves, primes in short intervals.

hence

$$M_p(G) = \frac{1}{2}\#\{E/\mathbb{F}_p : E(\mathbb{F}_p) \cong G\} + O(1),$$

In [DS14b, DS14c], the authors studied the weighted number of isomorphism classes of elliptic curves over any prime finite field with its group of points isomorphic to G, *i.e.*, they studied $M(G) := \sum_p M_p(G)$. The primes counted by $M(G)$ must lie in a very short interval near $N = |G|$. This is because the Hasse bound implies that $p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p}$, which is equivalent to saying that $N^- := N+1-2\sqrt{N} < p < N+1+2\sqrt{N} =: N^+$. Even the Riemann hypothesis does not guarantee the existence of a prime in such a short interval. Hence the main theorem of [DS14b] can only be proved under an appropriate conjecture concerning the distribution of primes in short intervals. In the statement below, we refer to the conjecture assumed in [DS14b] as the Barban-Davenport-Halberstam (BDH) estimate for short intervals.

Before stating the main theorem of [DS14b], we fix some more notation. Given a group $G = G_{m,k}$, we let $\mathrm{Aut}(G)$ denote its automorphism group (as a group). This should not be confused with $\mathrm{Aut}_p(E)$ as defined above, which refers to the set of $\mathbb{F}_p$-automorphisms of the elliptic curve E. We also define the function

$$K(G) = \prod_{\ell \nmid N}\Big(1 - \frac{\left(\frac{N-1}{\ell}\right)^2 \ell + 1}{(\ell-1)^2(\ell+1)}\Big) \prod_{\ell \mid m}\Big(1 - \frac{1}{\ell^2}\Big) \prod_{\substack{\ell \mid k \\ \ell \nmid m}}\Big(1 - \frac{1}{\ell(\ell-1)}\Big), \tag{1.1}$$

where the products are taken over all primes ℓ satisfying the stated conditions and $(\frac{\cdot}{\ell})$ denotes the usual Kronecker symbol. In [DS14b], the function $K(G)$ was only computed for odd order groups and its definition contained a mistake. It was corrected to the form that we give here in [DS14c]. Note that the function $K(G)$ is bounded between two constants independently of the the parameters m and k. In paraphrased form, the main theorem of [DS14b] is as follows.

Theorem 1.1 (David-Smith) *Assume that the BDH estimate for short intervals holds. Fix $A, B > 0$. Then for every nontrivial, odd order group $G = G_{m,k}$, we have that*

$$M(G) = \Big(K(G) + O_{A,B}\Big(\frac{1}{(\log|G|)^B}\Big)\Big)\frac{|G|^2}{|\mathrm{Aut}(G)|\log|G|} \asymp \frac{mk^2}{\phi(m)\phi(k)\log k},$$

provided that $m \le (\log k)^A$.

For precise details concerning the conjecture assumed to prove Theorem 1.1, we refer the reader to [DS14b]. We note that the result of Theorem 1.1 is restricted to the range $m \le (\log k)^A$. However, we believe that it should hold in the range $m \le k^A$. Proving such a result at the present time would, however, require an even stronger hypothesis than the one assumed in [DS14b]. Unconditionally, it is possible to obtain upper bounds of the correct order of magnitude in this larger range. This is the context of our first theorem.

Theorem 1.2 *Fix $A > 0$ and consider integers m and k with $1 \le m \le k^A$. Let $G = G_{m,k}$, $N = |G| = m^2 k$, and*

$$\delta = \frac{1}{N/(\phi(m)\log(2N))} \sum_{\substack{N^- < p \le N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \sqrt{(p - N^-)(N^+ - p)},$$

and note that $\delta \ll 1$ by the Brun-Titchmarsch inequality. For any fixed $\lambda > 1$,

$$\delta^\lambda \cdot \frac{|G|^2}{|\operatorname{Aut}(G)|\log(2|G|)} \ll M(G) \ll \delta^{1/\lambda} \cdot \frac{|G|^2}{|\operatorname{Aut}(G)|\log(2|G|)},$$

the implied constants depending at most on A and λ.

Employing the above result together with the Bombieri-Vinogradov theorem, we also show that the lower bound implicit in Theorem 1.1 holds for a positive proportion of groups G.

Theorem 1.3 *Consider numbers x and y with $1 \le x \le \sqrt{y}$. Then there are absolute positive constants c_1 and c_2 such that*

$$M(G_{m,k}) \ge c_1 \cdot \frac{|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})|\log(2|G_{m,k}|)}$$

for at least $c_2 x y$ pairs (m, k) with $m \le x$ and $k \le y$.

Remark 1.4 It is not possible for such a lower bound to hold for all groups $G = G_{m,k}$. As was noted in [BPS12], several groups of this form do not arise in this way at all. For example, the group $G_{11,1}$ never occurs as the group of points on any elliptic curve over any finite field.

Our final result for $M(G_{m,k})$ is that on average the full asymptotic of Theorem 1.1 holds unconditionally.

Theorem 1.5 *Fix $\epsilon > 0$ and $A \ge 1$. For $2 \le x \le y^{1/4-\epsilon}$ we have that*

$$\frac{1}{xy} \sum_{\substack{m \le x,\, k \le y \\ mk > 1}} \left| M(G_{m,k}) - \frac{K(G_{m,k})|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})|\log|G_{m,k}|} \right| \ll \frac{y}{(\log y)^A},$$

the implied constant depending at most on A and ϵ. Moreover, if the generalized Riemann hypothesis is true, then the same result is true for $x \le y^{1/2-\epsilon}$.

In [DS13, DS14a], David and Smith studied the related question of how many elliptic curves over $\mathbb{F}_p$ have a given number of points, that is to say, the asymptotic behaviour of

$$M(N) := \sum_p \sum_{\substack{E/\mathbb{F}_p \\ \#E(\mathbb{F}_p) = N}} \frac{1}{|\operatorname{Aut}_p(E)|}.$$

It was shown in [DS13, DS14a] that

$$M(N) \sim K(N) \cdot \frac{N^2}{\phi(N)\log N} \qquad (N \to \infty)$$

under suitable assumptions on the distribution of primes in short arithmetic progressions where

$$K(N) = \prod_{\ell \nmid N} \Big(1 - \frac{\left(\frac{N-1}{\ell}\right)^2 \ell + 1}{(\ell-1)^2(\ell+1)}\Big) \prod_{\ell \mid N} \Big(1 - \frac{1}{\ell^{v_\ell(N)}(\ell-1)}\Big). \tag{1.2}$$

Here $v_\ell(N)$ denotes the usual ℓ-adic valuation of N. As one might expect, the methods of this paper apply to the study of $M(N)$ as well.

We start by recording the obvious identity $M(N) = \sum_{m^2 k = N} M(G_{m,k})$. Then it is possible to show that, as expected, most of the contribution to $M(N)$ comes from groups $G_{m,k}$ with m small, that is to say, groups that are nearly cyclic.

Theorem 1.6 *For $N \geq 1$ and $x \geq 1$, we have that*

$$M(N) = \sum_{\substack{m^2 k = N \\ m \leq x}} M(G_{m,k}) + O\Big(\frac{N^2}{x\phi(N)\log(2N)}\Big).$$

Finally, we conclude with two more results on $M(N)$.

Theorem 1.7 *Let $N \geq 1$, set*

$$\eta = \frac{1}{N/(\log(2N))} \sum_{\substack{N^- < p \leq N^+ \\ p \equiv 1 \pmod m}} \sqrt{(p - N^-)(N^+ - p)},$$

and note that $\eta \ll 1$ by the Brun–Titchmarsch inequality. For any fixed $\lambda > 1$,

$$\eta^\lambda \cdot \frac{N^2}{\phi(N)\log(2N)} \ll M(N) \ll \eta^{1/\lambda} \cdot \frac{N^2}{\phi(N)\log(2N)},$$

the implied constants depending at most on λ.

Theorem 1.8 *Fix $A > 0$. For $x \geq 1$, we have that*

$$\frac{1}{x} \sum_{1 < N \leq x} \left| M(N) - \frac{K(N)N^2}{\phi(N)\log N} \right| \ll_A \frac{x}{(\log x)^A}.$$

The present paper also includes an appendix (by G. Martin, C. David, and E. Smith) giving a probabilistic interpretation to the Euler factors arising in the constants $K(N)$ and $K(G)$ defined by (1.1) and (1.2), respectively. This interpretation is similar to the heuristic leading to the conjectural constants in related conjectures on properties of the reductions of a fixed global elliptic curve E over the rationals *e.g.*, the Lang-Trotter conjectures [LT76] and the Koblitz [Kob88] conjecture, with the additional feature that the Euler factors at the primes ℓ dividing N or $|G|$ are related to certain matrix counts over $\mathbb{Z}/\ell^e\mathbb{Z}$ for e large enough.

Notation Given a natural number n, we denote with $P^+(n)$ and $P^-(n)$ its largest and smallest prime factor, respectively, with the convention that

$$P^+(1) = 1 \quad \text{and} \quad P^-(1) = \infty.$$

Moreover, we let $\tau_r(n)$ denote the coefficient of $1/n^s$ in the Dirichlet series $\zeta(s)^r$. In particular, $\tau_r(n) = r^{\omega(n)}$ for square-free integers n, where $\omega(n)$ denotes the number of distinct prime factors of n. In the special case when $r = 2$, we simply write $\tau(n)$ in place of $\tau_2(n)$, which counts the number of divisors of n. We write $f * g$ to denote the Dirichlet convolution of the arithmetic functions f and g, defined by $(f * g)(n) = \sum_{ab=n} f(a)g(b)$. As usual, given a Dirichlet character χ, we write $L(s, \chi)$ for its Dirichlet series. In addition, we make use of the notation

$$E(x, h; q) := \max_{(a,q)=1} \Big| \sum_{\substack{x<p\le x+h \\ p\equiv a \pmod q}} \log p - \frac{h}{\phi(q)} \Big|.$$

Finally, for $d \in \mathbb{Z}$ that is not a square and for $z \ge 1$, we let

$$\mathcal{L}(d) = L\Big(1, \big(\frac{d}{\cdot}\big)\Big) = \prod_{\ell} \Big(1 - \frac{\big(\frac{d}{\ell}\big)}{\ell}\Big)^{-1} \quad \text{and} \quad \mathcal{L}(d; z) = \prod_{\ell \le z} \Big(1 - \frac{\big(\frac{d}{\ell}\big)}{\ell}\Big)^{-1}.$$

2 Outline of the Proofs

In this section, we outline the chief ideas that go into the proofs of our main results. However, most of our remarks concern the proofs of Theorems 1.2 and 1.5. This is primarily because the remaining results are essentially corollaries of these theorems. In particular, the main ingredient in the proof of Theorem 1.6 is Theorem 1.2, and the main ingredients in the proof of Theorem 1.8 are Theorems 1.5 and 1.6 together with a short computation. Theorem 1.7 is not truly a corollary, but its proof is essentially the same as that of Theorem 1.2. The proof of Theorem 1.3 is somewhat different. The ideas involved in its proof are essentially the same as those used to show Theorem 1.6 of [CDKS] together with an application of Theorem 1.2. All of this will be expounded further in Section 3 where we complete the proofs of all six results.

For the remainder of this section, we focus our attention on outlining the main ingredients in the proofs of Theorems 1.2 and 1.5. Throughout, we fix a group $G = G_{m,k} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$, and we set $N = |G| = m^2k$. Moreover, given a prime $p \equiv 1 \pmod m$, we set

$$d_{m,k}(p) = \frac{(p-1-N)^2 - 4N}{m^2} = \Big(\frac{p-1}{m} - mk\Big)^2 - 4k. \tag{2.1}$$

Often, when the dependence on m and k is clear from the context, we will simply write $d(p)$ in place of $d_{m,k}(p)$. Our starting point is the following lemma, whose proof is based on Deuring's work [Deu41] and its generalization due to Schoof [Sch87]. We shall give the details of its proof in Section 4.

Lemma 2.1 *For any $m, k \in \mathbb{N}$, we have that*

$$M(G_{m,k}) = \sum_{\substack{N^- < p < N^+ \\ p\equiv 1 \pmod m}} \sum_{\substack{f^2 \mid d(p),\, (f,k)=1 \\ d(p)/f^2 \equiv 1,0 \pmod 4}} \frac{\sqrt{|d(p)|}\,\mathcal{L}(d(p)/f^2)}{2\pi f}.$$

For the proof of Theorem 1.2, we shall use the following simplified but weaker version of Lemma 2.1.

Corollary 2.2 *For any $m, k \in \mathbb{N}$, we have that*

$$\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \sqrt{|d(p)|}\mathcal{L}(d(p)) \ll M(G_{m,k}) \ll \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \frac{|d(p)|^{3/2}}{\phi(|d(p)|)}\mathcal{L}\big(d(p)\big).$$

Proof For the lower bound, note that the term $f = 1$ in Lemma 2.1 always contributes to $M(G_{m,k})$, since $d(p) \equiv 0, 1 \,(\mathrm{mod}\, 4)$ for all m, k and $p \equiv 1 \,(\mathrm{mod}\, m)$. For the upper bound, notice that

$$\mathcal{L}(d(p)/f^2) \le \frac{f}{\phi(f)}\mathcal{L}\big(d(p)\big).$$

Since $\sum_{f|n} \frac{1}{\phi(f)} \ll \frac{n}{\phi(n)}$, the claimed upper bound follows. ∎

Evidently, Lemma 2.1 and Corollary 2.2 reduce the estimation of $M(G_{m,k})$ to estimating an average of Dirichlet series evaluated at 1. In order to do so, we expand the Dirichlet series as an infinite sum and invert the order of summation by putting the sum over primes p inside. For each fixed n in the Dirichlet sum, understanding this sum over primes involves understanding the distribution of the set

$$\left\{ \frac{p-1}{m} : N^- < p < N^+,\ p \equiv 1 \,(\mathrm{mod}\, m) \right\} \tag{2.2}$$

in arithmetic progressions $a \,(\mathrm{mod}\, b)$, where the modulus $b = b(n)$ depends on n and other parameters which are less essential. Already when $b = m = 1$, this problem is very hard and unsolved, even if we assume the validity of the Riemann hypothesis. In order to limit the size of the moduli b that are involved, we need to truncate the Dirichlet series that appear before inverting the order of summation. We could do this for each individual Dirichlet series using character sum estimates such as the Pólya-Vinogradov inequality or Burgess's bounds as in [DS13, DS14b], but this would still leave us to deal with rather large moduli b. Instead, we use the following result, which implies that for *most* characters χ, $L(1, \chi)$ can be approximated by a very short Euler product, and then by a sum over integers n supported only on small primes.

Lemma 2.3 *Let $\alpha \ge 1$ and $Q \ge 3$. There is a set $\mathcal{E}_\alpha(Q) \subset [1, Q] \cap \mathbb{Z}$ of at most $Q^{2/\alpha}$ integers such that if χ is a Dirichlet character modulo $q \le \exp\{(\log Q)^2\}$ whose conductor does not belong to $\mathcal{E}_\alpha(Q)$, then*

$$L(1, \chi) = \prod_{\ell \le (\log Q)^{8\alpha^2}} \Big(1 - \frac{\chi(\ell)}{\ell}\Big)^{-1} \Big(1 + O_\alpha\Big(\frac{1}{(\log Q)^\alpha}\Big)\Big).$$

Proof By a classical result essentially due to Elliott (see [GS03, Proposition 2.2]), we know that there is a set $\mathcal{E}_\alpha(Q)$ of at most $Q^{2/\alpha}$ integers from $[1, Q]$ such that

$$L(1, \psi) = \prod_{\ell \le (\log Q)^{8\alpha^2}} \Big(1 - \frac{\psi(\ell)}{\ell}\Big)^{-1} \Big(1 + O\Big(\frac{\alpha}{(\log Q)^\alpha}\Big)\Big)$$

for all primitive characters ψ of conductor in $[1, Q] \setminus \mathcal{E}_\alpha(Q)$. So if χ is a Dirichlet character modulo $q \le \exp\{(\log Q)^2\}$ induced by ψ and the conductor of ψ is in $[1, Q] \setminus \mathcal{E}_\alpha(Q)$, then

$$\begin{aligned} L(1,\chi) &= \prod_{\ell \mid q} \Big(1 - \frac{\psi(\ell)}{\ell}\Big) \prod_{\ell \le (\log Q)^{8\alpha^2}} \Big(1 - \frac{\psi(\ell)}{\ell}\Big)^{-1} \Big(1 + O\Big(\frac{\alpha}{(\log Q)^\alpha}\Big)\Big) \\ &= \prod_{\ell \mid q,\, \ell > (\log Q)^{8\alpha^2}} \Big(1 - \frac{\psi(\ell)}{\ell}\Big) \prod_{\ell \le (\log Q)^{8\alpha^2}} \Big(1 - \frac{\chi(\ell)}{\ell}\Big)^{-1} \Big(1 + O\Big(\frac{\alpha}{(\log Q)^\alpha}\Big)\Big). \end{aligned}$$

Finally, note that

$$\begin{aligned} \log\Big(\prod_{\ell \mid q, \ell > (\log Q)^{8\alpha^2}} \Big(1 - \frac{\psi(\ell)}{\ell}\Big)\Big) &\ll \sum_{\ell \mid q, \ell > (\log Q)^{8\alpha^2}} \frac{1}{\ell} \le \frac{\omega(q)}{(\log Q)^{8\alpha^2}} \\ &\ll \frac{1}{(\log Q)^{8\alpha^2 - 2}}, \end{aligned}$$

since $\omega(q) \le \log q / \log 2 \ll (\log Q)^2$, which completes the proof of the lemma. ∎

Expanding the short product in the above lemma leads to an approximation of $L(1, \chi)$ by a sum over $(\log Q)^A$-smooth integers, and we know that very few of them get $> Q^\epsilon$.

Lemma 2.4 *Let $f : \mathbb{N} \to \{z \in \mathbb{C} : |z| \le 1\}$ be a completely multiplicative function. For $u \ge 1$ and $x \ge 10$ we have that*

$$\prod_{p \le x} \Big(1 - \frac{f(p)}{p}\Big)^{-1} = \sum_{\substack{P^+(n) \le x \\ n \le x^u}} \frac{f(n)}{n} + O\Big(\frac{\log x}{e^u}\Big).$$

Proof We have that

$$\begin{aligned} &\Big|\prod_{p \le x} \Big(1 - \frac{f(p)}{p}\Big)^{-1} - \sum_{\substack{P^+(n) \le x \\ n \le x^u}} \frac{f(n)}{n}\Big| \\ &\qquad = \Big|\sum_{\substack{P^+(n) \le x \\ n > x^u}} \frac{f(n)}{n}\Big| \le \frac{1}{e^u} \sum_{P^+(n) \le x} \frac{1}{n^{1 - 1/\log x}} \ll \frac{1}{e^u} \exp\Big\{\sum_{p \le x} \frac{1}{p^{1 - 1/\log x}}\Big\}. \end{aligned}$$

So using the formula $p^{1/\log x} = 1 + O(\log p / \log x)$ and the prime number theorem, we obtain the claimed result. ∎

Combining Lemmas 2.3 and 2.4, we may replace $L(1, \chi)$ by a very short sum for most characters χ, which means that we only need information for the distribution of the set (2.2) for very small moduli. This leads to the following fundamental result, which is an improvement of Theorem 1.1. It will be proved in Section 7.

Theorem 2.5 *Fix $\alpha \ge 1$ and $\epsilon \le 1/3$ and consider integers m and k with $1 \le m \le k^\alpha$. Assume k is large enough so that $k^{\frac{1}{2} - \epsilon} \ge (\log k)^{\alpha + 2}$. Set $G = G_{m,k}$ and consider*

$h \in [mk^{\epsilon}, m\sqrt{k}/(\log k)^{\alpha+2}]$. *Then*

$$M(G) = \frac{K(G)|G|^2}{|\operatorname{Aut}(G)|\log|G|} + O_{\alpha,\epsilon}\Big(\frac{k}{(\log k)^{\alpha}} + \frac{\sqrt{k}}{h}\sum_{q\le k^{\epsilon}}\tau_3(q)\int_{N^-}^{N^+} E(y,h;qm)\,\mathrm{d}y\Big),$$

where $K(G)$ *is defined by* (1.1).

Even though we cannot estimate the error term for any given values of m and k, we can do so if we average over m and k using the following result which is a consequence of Theorem 1.1 in [Kou14].

Lemma 2.6 *Fix* $\epsilon > 0$ *and* $A \ge 1$. *For* $x \ge h \ge 2$ *and* $1 \le Q^2 \le h/x^{1/6+\epsilon}$, *we have that*

$$\int_x^{2x}\sum_{q\le Q} E(y,h;q)\,\mathrm{d}y \ll \frac{xh}{(\log x)^A}.$$

If, in addition, the Riemann hypothesis for Dirichlet L-functions is true, then the above estimate holds when $1 \le Q^2 \le h/x^{\epsilon}$.

Theorem 2.5 and Lemma 2.6 lead to a proof of Theorem 1.5 in a fairly straightforward way as we will see in Section 3.

Next we turn to the proof of Theorem 1.2. Using Corollary 2.2 and Hölder's inequality, we reduce the proof of this result to that of controlling sums of the form

$$\sum_{\substack{N^-<p<N^+\\ p\equiv 1 \,(\mathrm{mod}\, m)}} \Big(\frac{|d(p)|}{\phi(|d(p)|)}\Big)^s \mathcal{L}\big(d(p)\big)^r, \tag{2.3}$$

where we take $r > 0$ to prove the implicit upper bound and $r < 0$ for the lower bound. Nevertheless, we only seek an upper bound for the sum in (2.3), even for the lower bound in Theorem 1.2. Therefore, we can replace the sum over primes with a sum over almost primes and use sieve methods to detect the latter kind of integers. More precisely, we will majorize the characteristic function of primes $\le 2N$ by a convolution $\lambda * 1$, where λ is a certain truncation of the Möbius function. This will be done using the *fundamental lemma of sieve methods*, which we state below in the form found in [FI78, Lemma 5]. We could have also used Selberg's sieve, but the calculations are actually simpler when using Lemma 2.7.

Lemma 2.7 *Let* $y \ge 2$ *and* $D = y^u$ *with* $u \ge 2$. *There exist two arithmetic functions* $\lambda^{\pm} : \mathbb{N} \to [-1,1]$, *supported on* $\{d \in \mathbb{N} : P^+(d) \le y,\ d \le D\}$, *for which*

$$\begin{cases} (\lambda^- * 1)(n) = (\lambda^+ * 1)(n) = 1 & \text{if } P^-(n) > y,\\ (\lambda^- * 1)(n) \le 0 \le (\lambda^+ * 1)(n) & \text{otherwise.}\end{cases}$$

Moreover, if $g\colon \mathbb{N} \to \mathbb{R}$ is a multiplicative function with $0 \le g(p) \le \min\{2, p-1\}$ for all primes $p \le y$ and $\lambda \in \{\lambda^+, \lambda^-\}$, then

$$\sum_d \frac{\lambda(d)g(d)}{d} = (1 + O(e^{-u})) \prod_{p \le y} \Big(1 - \frac{g(p)}{p}\Big).$$

Combining Lemmas 2.3 and 2.7, we are led to the following key result, which will be proved in Section 6. As we will see in the same section, Theorem 1.2 is an easy consequence of this intermediate result.

Proposition 2.8 *Let $m, k \in \mathbb{N}$ and set $N = m^2 k$. For any $r \in \mathbb{R}$ and $s \ge 0$, we have that*

$$\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} \Big(\frac{|d(p)|}{\phi(|d(p)|)}\Big)^s \mathcal{L}(d(p))^r \ll_{r,s} \Big(\frac{k}{\phi(k)}\Big)^r \frac{\sqrt{N}}{\phi(m)\log(2k)}.$$

3 Completion of the Proof of the Main Results

In this section we prove Theorems 1.2–1.8. We start by stating a preliminary result which is Lemma 15 of [DS14b] in slightly altered form.

Lemma 3.1 *For $m, k \in \mathbb{N}$, we have that*

$$\frac{|\mathrm{Aut}(G_{m,k})|}{|G_{m,k}|} = m\phi(m)\frac{\phi(k)}{k} \prod_{\substack{\ell \mid m \\ \ell \nmid k}} \Big(1 - \frac{1}{\ell^2}\Big).$$

Proof of Theorem 1.2 The claimed inequalities are a consequence of Corollary 2.2, Proposition 2.8, and Hölder's inequality. Indeed, let $\mu = \lambda/(\lambda-1)$, so that $1/\lambda + 1/\mu = 1$. Then we have that

$$\begin{aligned} M(G_{m,k}) &\ll \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} \sqrt{|d(p)|}\frac{|d(p)|}{\phi(|d(p)|)}\mathcal{L}(d(p)) \\ &\le \Big(\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} \sqrt{|d(p)|}\Big)^{\frac{1}{\lambda}} \Bigg(\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} \sqrt{|d(p)|}\Big(\frac{|d(p)|}{\phi(|d(p)|)}\Big)^{\mu} \mathcal{L}\big(d(p)\big)^{\mu}\Bigg)^{\frac{1}{\mu}} \\ &\ll \Big(\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} \frac{\sqrt{(N^+ - p)(p - N^-)}}{m}\Big)^{\frac{1}{\lambda}} \\ &\quad \times \Big(\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} \sqrt{k}\Big(\frac{|d(p)|}{\phi(|d(p)|)}\Big)^{\mu} \mathcal{L}\big(d(p)\big)^{\mu}\Big)^{\frac{1}{\mu}}, \end{aligned}$$

since $|d(p)| = (N^+ - p)(p - N^-)/m^2 \ll N/m^2 = k$. So the definition of δ and Proposition 2.8 imply that

$$M(G_{m,k}) \ll_{\lambda,A} \delta^{1/\lambda} \frac{km}{\phi(m)\log(2N)} \frac{k}{\phi(k)}.$$

Hence the upper bound in Theorem 1.2 follows by Lemma 3.1.

The proof of the lower bound is similar, having as a starting point the inequality

$$\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \sqrt{|d(p)|} \leq \Big(\sum_{\substack{N^- < p \leq N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \sqrt{|d(p)|}\mathcal{L}\big(d(p)\big) \Big)^{\frac{1}{\lambda}} \Big(\sum_{\substack{N^- < p \leq N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \frac{\sqrt{|d(p)|}}{\mathcal{L}\big(d(p)\big)^{\mu/\lambda}} \Big)^{\frac{1}{\mu}}. \quad \blacksquare$$

Proof of Theorem 1.7 The proof of Theorem 1.7 is completely analogous to the proof of Theorem 1.2. The only difference is that instead of starting with Corollary 2.2, we observe that

$$\sum_{N^- < p < N^+} \sqrt{|D_N(p)|}\mathcal{L}\big(D_N(p)\big) \ll M(N) \ll \sum_{N^- < p < N^+} \frac{|D_N(p)|^{3/2}}{\phi(|D_N(p)|)}\mathcal{L}\big(D_N(p)\big),$$

a consequence of relation (4.2) below with $n = 1$. $\blacksquare$

Proof of Theorem 1.3 Note that when $m = k = 1$ and $N = 1$, then $N^+ = 4$ and $N^- = 0$ and thus the primes 2 and 3 belong to the set $\{N^- < p \leq N^+ : p \equiv 1 \,(\mathrm{mod}\, m)\}$. So by Theorem 1.2, it suffices to show Theorem 1.3 when y is large enough. We further assume that $x \in \mathbb{N}$ which we may certainly do. Observe that $(N^+ - p)(p - N^-) \asymp N$ for $p \in \big((\sqrt{N} - 1/2)^2, (\sqrt{N} + 1/2)^2 \big)$, and thus

$$\frac{1}{N/(\phi(m)\log(2N))} \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, p)}} \sqrt{(N^+ - p)(p - N^-)} \gg \frac{\phi(m)}{\sqrt{N}} \sum_{\substack{(\sqrt{N}-1/2)^2 < p < (\sqrt{N}+1/2)^2 \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \log p.$$

So, if we set

$$C(m,k) = \frac{|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})|\log(2G_{m,k})} \asymp \frac{mk^2}{\phi(m)\phi(k)\log(mk)},$$

then Theorem 1.2 with $\lambda = 2$ implies that

$$\sum_{\substack{3x/4<m\le x\\ y/100<k\le y}} \sqrt{\frac{M(G_{m,k})}{C(m,k)}}$$

$$\gg \sum_{\substack{3x/4<m\le x\\ y/100<k\le y}} \frac{\phi(m)}{x\sqrt{y}} \sum_{\substack{(m\sqrt{k}-1/2)^2<p<(m\sqrt{k}+1/2)^2\\ p\equiv 1 \pmod m}} \log p$$

$$\ge \sum_{3x/4<m\le x} \sum_{\substack{x^2y/3<p\le 4x^2y/9\\ p\equiv 1 \pmod m}} \frac{\phi(m)\log p}{x\sqrt{y}} \sum_{\substack{y/100<k\le y\\ (\sqrt{p}-1/2)^2/m^2<k<(\sqrt{p}+1/2)^2/m^2}} 1,$$

provided that y is large enough. Note that

$$\frac{(\sqrt{p}+1/2)^2-(\sqrt{p}-1/2)^2}{m^2} = \frac{2\sqrt{p}}{m^2} \ge \frac{2x\sqrt{y/3}}{x^2} > 1,$$

by our assumptions that $x \le \sqrt{y}$. Since we also have that $(\sqrt{p}-1/2)^2/m^2 > y/100$ and that $(\sqrt{p}+1/2)^2/m^2 \le y$ for y large enough and m and p as above, we conclude that

$$\sum_{\substack{3x/4<m\le x\\ y/100<k\le y}} \sqrt{\frac{M(G_{m,k})}{C(m,k)}} \gg \frac{1}{x^2} \sum_{3x/4<m\le x} \phi(m) \sum_{\substack{x^2y/3<p\le 4x^2y/9\\ p\equiv 1 \pmod m}} \log p.$$

This last double sum equals

$$\sum_{3x/4<m\le x} \phi(m)\cdot\frac{x^2y}{9\phi(m)} + O_A\Big(\frac{x^3y}{(\log y)^A}\Big) \gg x^3y,$$

by the Bombieri–Vinogradov theorem. Therefore we conclude that

$$\sum_{\substack{3x/4<m\le x\\ y/100<k\le y}} \sqrt{\frac{M(G_{m,k})}{C(m,k)}} \gg xy.$$

Since the summands are all $\ll 1$ in this range by Theorem 1.2 (recall that $\delta \ll 1$ there), we obtain Theorem 1.3. ∎

Proof of Theorem 1.5 Let θ be a parameter, which we take to be $\frac{1}{2}$ or $\frac{1}{4}$, according to whether we assume the generalized Riemann hypothesis or not. We then suppose that $1 \le x \le y^{\theta-\epsilon}$. Note that Theorem 1.2 and Lemma 3.1 imply that

$$\sum_{\substack{m\le x,\ k\le y/(\log y)^A\\ mk>1}} \Big| M(G_{m,k}) - \frac{K(G_{m,k})|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})|\log|G_{m,k}|}\Big| \ll \frac{xy^2}{(\log y)^A}.$$

We break the remaining range of m and k into dyadic intervals, hence reducing Theorem 1.5 to showing that

$$E := \sum_{\substack{x/2<m\le x\\ y/2<k\le y}} \Big| M(G_{m,k}) - \frac{K(G_{m,k})|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})|\log|G_{m,k}|}\Big| \ll_{\epsilon,A} \frac{xy^2}{(\log y)^A}$$

for $x \le y^{\theta-\epsilon}$. (Note that these might be different values of x, y, and ϵ than the ones we started with.) We apply Theorem 2.5 with $h = (x^2y)^{1/2}/(\log y)^{A+2}$ for all $m \in [x/2, x]$ and $k \in [y/2, y]$, to deduce that

$$\begin{aligned} E &\ll \frac{\sqrt{y}}{h} \sum_{\substack{x/2<m\le x\\ y/2<k\le y}} \sum_{q\le k^\epsilon} \tau_3(q) \int_{(m^2k)^-}^{(m^2k)^+} E(t,h;qm)\,\mathrm{d}t + \frac{xy^2}{(\log y)^A} \\ &=: E' + \frac{xy^2}{(\log y)^A}, \end{aligned}$$

say. Putting the sum over k inside, we find that

$$\begin{aligned} E' &\ll \frac{\sqrt{y}}{h} \sum_{x/2<m\le x} \sum_{q\le y^\epsilon} \tau_3(q) \int_{x^2y/10}^{2x^2y} E(t,h;qm)\Big(\sum_{\substack{y/2<k\le y\\ t^-/m^2<k<t^+/m^2}} 1\Big)\,\mathrm{d}t \\ &\ll \frac{y}{hx} \sum_{m\le x} \sum_{q\le y^\epsilon} \tau_3(q) \int_{x^2y/10}^{2x^2y} E(t,h;qm)\,\mathrm{d}t \\ &\le \frac{y}{hx} \sum_{m\le x} \sum_{q\le y^\epsilon} \tau_4(q) \int_{x^2y/10}^{2x^2y} E(t,h;q)\,\mathrm{d}t. \end{aligned}$$

We note that $E(u,h;b) \ll \sqrt{h/\phi(b)}\sqrt{E(u,h;b)}$ by the Brun-Titchmarsch inequality. So the Cauchy-Schwarz inequality and Lemma 2.6 imply that

$$\begin{aligned} E' &\ll \frac{y}{xh}\Big(\sum_{b\le xy^{3\epsilon}} \tau_4(b)^2 \int_{x^2y/10}^{2x^2y} \frac{h}{\phi(b)}\,\mathrm{d}t\Big)^{\frac12} \Big(\sum_{b\le xy^{3\epsilon}} \int_{x^2y/10}^{2x^2y} E(t,h;b)\,\mathrm{d}t\Big)^{\frac12} \\ &\ll \frac{y}{xh}\Big(x^2yh(\log y)^{16} \cdot \frac{x^2yh}{(\log y)^{2A+16}}\Big)^{\frac12} = \frac{xy^2}{(\log y)^A}, \end{aligned}$$

which completes the proof of Theorem 1.5. ∎

Proof of Theorem 1.6 Theorem 1.2 implies that

$$M(G_{m,k}) \ll \frac{k^{3/2}}{\phi(k)} \frac{\sqrt{N}}{\phi(m)\log(2k)} = \frac{mk^2}{\phi(k)\phi(m)\log(2k)} \le \frac{Nmk}{\phi(N)\phi(m)\log(2k)}.$$

Therefore,

$$\sum_{\substack{m^2k=N\\ m>x}} M(G_{m,k}) \ll \sum_{\substack{m^2\mid N\\ x<m\le\sqrt{N}}} \frac{N^2}{m\phi(m)\phi(N)\log(2N/m^2)} \ll \frac{N^2}{x\phi(N)\log(2N)},$$

which completes the proof of Theorem 1.6. ∎

Proof of Theorem 1.8 In view of Theorem 1.6, it suffices to show that

$$\sum_{1<N\le x} \Big| \sum_{\substack{m^2k=N\\ m\le(\log x)^A}} M(G_{m,k}) - \frac{K(N)N^2}{\phi(N)\log N}\Big| \ll_A \frac{x^2}{(\log x)^A},$$

where $K(N)$ is defined by (1.2). Note that

$$\begin{aligned}
&\sum_{1<N\le x}\Big|\sum_{\substack{m^2k=N\\ m\le(\log x)^A}} M(G_{m,k}) - \sum_{\substack{m^2k=N\\ m\le(\log x)^A}} \frac{K(G_{m,k})|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})|\log|G_{m,k}|}\Big|\\
&\quad\le \sum_{\substack{1<m^2k\le x\\ m\le(\log x)^A}}\Big|M(G_{m,k}) - \frac{K(G_{m,k})|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})|\log|G_{m,k}|}\Big|\\
&\quad\le \sum_{1\le 2^j\le(\log x)^A}\ \sum_{\substack{k\le x/4^j\\ 2^j\le m<2^{j+1}\\ m^2k>1}}\Big|M(G_{m,k}) - \frac{K(G_{m,k})|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})|\log|G_{m,k}|}\Big|\\
&\quad\ll_A \sum_{1\le 2^j\le(\log x)^A}\frac{x^2}{8^j(\log x)^A}\ll\frac{x^2}{(\log x)^A}
\end{aligned}$$

by Theorem 1.5. So it suffices to show that

$$\sum_{1<N\le x}\frac{N}{\log N}\Big|\sum_{\substack{m^2k=N\\ m\le(\log x)^A}}\frac{K(G_{m,k})|G_{m,k}|}{|\operatorname{Aut}(G_{m,k})|} - \frac{K(N)N}{\phi(N)}\Big| \ll_A \frac{x^2}{(\log x)^A}. \tag{3.1}$$

In fact, Lemma 3.1 implies that

$$\begin{aligned}
&\frac{K(G_{m,k})|G_{m,k}|}{|\operatorname{Aut}(G_{m,k})|}\\
&\quad=\frac{k}{m\phi(m)\phi(k)}\prod_{\substack{\ell\mid m\\ \ell\nmid k}}\Big(1-\frac{1}{\ell^2}\Big)^{-1}K(G_{m,k})\\
&\quad=\frac{N}{m^2\phi(N)}\prod_{\ell\mid(m,k)}\Big(1-\frac{1}{\ell}\Big)^{-1}\prod_{\substack{\ell\mid m\\ \ell\nmid k}}\Big(1-\frac{1}{\ell^2}\Big)^{-1}K(G_{m,k})\\
&\quad=\frac{N}{m^2\phi(N)}\prod_{\ell\nmid N}\Big(1-\frac{\big(\frac{N-1}{\ell}\big)^2\ell+1}{(\ell-1)^2(\ell+1)}\Big)\prod_{\ell\mid(m,k)}\Big(1+\frac{1}{\ell}\Big)\prod_{\substack{\ell\mid k\\ \ell\nmid m}}\Big(1-\frac{1}{\ell(\ell-1)}\Big).
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\sum_{\substack{m^2k=N\\ m\le(\log x)^A}}\frac{K(G_{m,k})|G_{m,k}|}{|\operatorname{Aut}(G_{m,k})|}\\
&\qquad=\sum_{m^2k=N}K(G_{m,k})\frac{|G_{m,k}|}{|\operatorname{Aut}(G_{m,k})|}+O\Big(\frac{N}{(\log x)^A\phi(N)}\Big)\\
&\qquad=\frac{N}{\phi(N)}\prod_{\ell\nmid N}\Big(1-\frac{\big(\frac{N-1}{\ell}\big)^2\ell+1}{(\ell-1)^2(\ell+1)}\Big)\cdot S(N)+O\Big(\frac{N}{(\log x)^A\phi(N)}\Big),
\end{aligned}$$

where

$$S(N) = \sum_{m^2k=N} \frac{1}{m^2} \prod_{\ell \mid (m,k)} \Big(1+\frac{1}{\ell}\Big) \prod_{\substack{\ell \mid k \\ \ell \nmid m}} \Big(1-\frac{1}{\ell(\ell-1)}\Big).$$

Note that

$$\begin{aligned} S(\ell^\nu) &= 1 - \frac{1}{\ell(\ell-1)} + \sum_{1\le j\le \nu/2} \frac{1}{\ell^{2j}} \Big(1+\frac{\mathbf{1}_{j<\nu/2}}{\ell}\Big) \\ &= 1 - \frac{1}{\ell(\ell-1)} + \sum_{1\le j\le \nu/2} \frac{1}{\ell^{2j}} + \sum_{1\le j\le \nu/2} \frac{\mathbf{1}_{j<\nu/2}}{\ell^{2j+1}} \\ &= 1 - \frac{1}{\ell(\ell-1)} + \sum_{i=2}^{\nu} \frac{1}{\ell^i} = 1 - \frac{1}{\ell^\nu(\ell-1)}. \end{aligned}$$

So we conclude that

$$\sum_{\substack{m^2k=N \\ m\le (\log x)^A}} \frac{K(G_{m,k})|G_{m,k}|}{|\operatorname{Aut}(G_{m,k})|} = \frac{K(N)N}{\phi(N)} + O\Big(\frac{N}{(\log x)^A \phi(N)}\Big),$$

which yields relation (3.1), thus completing the proof of Theorem 1.8. ∎

4 Reduction to an Average of Dirichlet Series

In this section, we prove Lemma 2.1 using the theory developed by Deuring [Deu41] and somewhat generalized by Schoof [Sch87]. As before, we fix a group $G = G_{m,k} = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$, and we set $N = |G| = m^2k$. Given a prime p and an integer n such that $n^2|N$, we define

$$M_p(N;n) = \sum_{\substack{E/\mathbb{F}_p \\ \#E(\mathbb{F}_p)=N \\ E(\mathbb{F}_p)[n]\cong G_{n,1}}} \frac{1}{|\operatorname{Aut}_p(E)|},$$

the weighted number of isomorphism classes of elliptic curves over any prime finite field which have exactly N rational points and whose rational n-torsion subgroup is isomorphic to $G_{n,1} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. It is not hard to relate $M_p(G)$ to a sum involving $M_p(N;n)$. This is accomplished via an inclusion-exclusion argument, which gives the relation

$$M_p(G) = \sum_{r^2\mid k} \mu(r) M_p(N; rm). \tag{4.1}$$

Schoof [Sch87] essentially gave a formula for $M_p(N;n)$ in terms of class numbers. However, one needs to exercise care here as Schoof counts each $\mathbb{F}_p$-isomorphism class E with weight 1 instead of with weight $1/|\operatorname{Aut}_p(E)|$ as we do here. Given a negative discriminant D, we let $H(D)$ denote the *Kronecker class number* which is defined as

$$H(D) = \sum_{\substack{f^2\mid D \\ D/f^2 \equiv 0,1 \pmod 4}} \frac{h(D/f^2)}{w(D/f^2)}.$$

Here, as usual, $h(d)$ denotes the (ordinary) class number of the unique imaginary quadratic order of discriminant d, and $w(d)$ denotes the cardinality of its unit group. Then letting $D_N(p) = (p+1-N)^2 - 4p = (p-1-N)^2 - 4N$ and reworking the proofs of [Sch87, Lemma 4.8 and Theorem 4.9] to count each class E with weight $1/|\operatorname{Aut}_p(E)|$, we arrive at the formula

$$M_p(N;n) = \begin{cases} H\Big(\dfrac{D_N(p)}{n^2}\Big) & \text{if } p \in (N^-, N^+) \text{ and } p \equiv 1 \pmod{n}, \\ 0 & \text{otherwise.} \end{cases} \tag{4.2}$$

Note here that $D_N(p)/n^2$ is a negative discriminant whenever $p \in (N^-, N^+)$, $p \equiv 1 \pmod{n}$, and $n^2 \mid N$.

Lemma 4.1 *Let $m, k \in \mathbb{N}$ and recall that $d(p) = d_{m,k}(p)$ is defined by (2.1). If $p \in (N^-, N^+)$ and $p \equiv 1 \pmod{m}$, then*

$$M_p(G_{m,k}) = \sum_{\substack{f^2 \mid d(p),\ (f,k)=1 \\ \frac{d(p)}{f^2} \equiv 0,1 \pmod 4}} \frac{h(d(p)/f^2)}{w(d(p)/f^2)}.$$

Otherwise, $M_p(G_{m,k}) = 0$.

Remark 4.2 The above formula is amenable to computation. Indeed, given a prime p and any m and k, very simple modifications to the usual quadratic forms algorithm for computing class numbers (see [BV07, pp. 99–100] for example) make it possible to compute $M_p(G_{m,k})$, using at most $O(k)$ arithmetic operations which is reasonable for small k. If we put

$$H_k(D) = \sum_{\substack{f^2 \mid D,\ (f,k)=1 \\ \frac{D}{f^2} \equiv 0,1 \pmod 4}} \frac{h(D/f^2)}{w(D/f^2)}$$

for each negative discriminant D and each positive integer k, then the only modifications needed are as follows. When the algorithm produces the (not necessarily primitive) form $ax^2 + bxy + cy^2$, say with $(a,b,c) = f \geq 1$, it is counted subject to the following rules, provided that $(f,k) = 1$.

(i) Forms proportional to $x^2 + y^2$ are counted with weight $1/4$.
(ii) Forms proportional to $x^2 + xy + y^2$ are counted with weight $1/6$.
(iii) All other forms are counted with weight $1/2$.

Similarly, tables of $M(G_{m,k})$ or $M_p(G_{m,k})$ values can be computed for m and k of modest size by simultaneously computing a table of values of $H_k(D)$.

Proof It follows from (4.2) that $M_p(G) = 0$ unless $p \in (N^-, N^+)$ and $p \equiv 1 \pmod{m}$. Therefore, assume that $p \in (N^-, N^+)$ and $p \equiv 1 \pmod{m}$, and write $k = s^2 t$ with t square-free. Combining relations (4.1) and (4.2) with the definition of the Kronecker

class number, we find that

$$\begin{aligned} M_p(G) &= \sum_{\substack{r\mid s\\ p\equiv 1 \,(\mathrm{mod}\, rm)}} \mu(r) H\Big(\frac{D_N(p)}{(rm)^2}\Big) \\ &= \sum_{\substack{r\mid s\\ p\equiv 1 \,(\mathrm{mod}\, rm)}} \mu(r) H\Big(\frac{d(p)}{r^2}\Big) \\ &= \sum_{\substack{r\mid s\\ p\equiv 1 \,(\mathrm{mod}\, rm)}} \mu(r) \sum_{\substack{f^2 \mid \frac{d(p)}{r^2}\\ \frac{d(p)}{(rf)^2}\equiv 0,1 \,(\mathrm{mod}\, 4)}} \frac{h(d(p)/(rf)^2)}{w(d(p)/(rf)^2)} \\ &= \sum_{\substack{r\mid s\\ p\equiv 1 \,(\mathrm{mod}\, rm)}} \mu(r) \sum_{\substack{f^2 \mid d(p),\, r\mid f\\ \frac{d(p)}{f^2}\equiv 0,1 \,(\mathrm{mod}\, 4)}} \frac{h(d(p)/f^2)}{w(d(p)/f^2)}. \end{aligned}$$

Now interchanging the sum over r with the sum over f and recalling the identity

$$\sum_{r\mid n} \mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise,} \end{cases}$$

we arrive at the formula

$$M_p(G) = \sum_{\substack{f^2 \mid d(p)\\ (f,s,(p-1)/m)=1\\ \frac{d(p)}{f^2}\equiv 0,1 \,(\mathrm{mod}\, 4)}} \frac{h\big(d(p)/f^2\big)}{w\big(d(p)/f^2\big)}.$$

In order to complete the proof it is sufficient to show that in the above sum the condition $(f, s, (p-1)/m) = 1$ implies the simpler condition $(f, k) = 1$, the converse implication being immediate. To this end, we write $p = 1 + jm$ and assume that $(f, s, (p-1)/m) = (f, s, j) = 1$. Then $d(p) = (j - mk)^2 - 4k$, and the condition $d(p)/f^2 \equiv 0, 1 \,(\mathrm{mod}\, 4)$ may be rewritten as

$$(j - mk)^2 - 4k \equiv 0, f^2 \ (\mathrm{mod}\, 4f^2). \tag{4.3}$$

Now let ℓ be any prime dividing (f, k). Then the above congruence implies that $\ell | j$, but that implies that $\ell^2 | (j - mk)^2$. Whence $\ell^2 | 4k$. If ℓ is odd, then we have that $\ell^2 | k$, and hence $\ell | (f, s, j) = 1$, which is a contradiction. If $\ell = 2$, then we divide (4.3) through by 4 to obtain

$$\Big(\frac{j}{2} - m\frac{k}{2}\Big)^2 - k \equiv 0, \frac{f^2}{4} \,(\mathrm{mod}\, f^2).$$

Since $\ell = 2 | (f, k)$, we have that k is even and congruent to a difference of two squares modulo 4. This in turn implies that $k \equiv 0 \,(\mathrm{mod}\, 4)$, *i.e.*, $2 | s$. Thus, in this case we also have the contradiction $\ell = 2 | (f, s, j) = 1$. Therefore, we conclude that $(f, k) = 1$, and this completes the proof of the lemma. ∎

Lemma 4.1 together with the class number formula immediately yields Lemma 2.1.

5 Local Computations

In this section we gather some local computations which we will need in the proofs of Theorem 2.5 and Proposition 2.8. As before, we continue to assume that m, k, and N are positive integers with $N = |G_{m,k}| = m^2 k$.

Lemma 5.1 *Let ℓ be an odd prime. For $e \geq 1$, $(d, \ell) = 1$, and $(a, b) = 1$, we have that*

$$\#\{ j \in \mathbb{Z}/\ell^e\mathbb{Z} : j^2 \equiv d \pmod{\ell^e} \} = 1 + \left(\frac{d}{\ell}\right)$$

and

$$\#\{ j \in \mathbb{Z}/\ell^e\mathbb{Z} : j^2 \equiv d \pmod{\ell^e},\ (a + bj, \ell) = 1 \} = 1 + \left(\frac{a^2 - db^2}{\ell}\right)^2 \left(\frac{d}{\ell}\right).$$

Proof The first formula is classical. For the second, we first note that if $(\frac{d}{\ell}) = -1$, then $(\frac{a^2-db^2}{\ell})^2 = 1$ and the formula holds. Now assume that $(\frac{d}{\ell}) = 1$, so that there are exactly two solutions to the congruence $j^2 \equiv d \pmod{\ell^e}$, say $\pm j_0$. If $\ell | b$, then the condition $(a + bj, \ell) = 1$ is satisfied trivially for all $j \in \mathbb{Z}$ and the claimed result follows. Finally, if $\ell \nmid b$, then we need to exclude exactly one of the solutions when $a \equiv \pm b j_0 \pmod{\ell}$, that is to say when $a^2 \equiv b^2 d \pmod{\ell}$. So the claimed formula holds in this last case, too. ∎

We set

(5.1)

$$T(n) = \sum_{d \pmod n} \left(\frac{d - 4k}{n}\right) \#\{ j \pmod n : j^2 \equiv d \pmod n,\ (N + 1 + jm, n) = 1 \}.$$

Proposition 5.2 *Let ℓ be a prime not dividing $2k$ and $w \geq 1$. Then*

$$\frac{T(\ell^w)}{\ell^{w-1}} = -\left(\frac{m(N-1)}{\ell}\right)^2 + \begin{cases} \ell - 1 - (\frac{k}{\ell}) & \text{if } w \text{ is even,} \\ -1 & \text{if } w \text{ is odd.} \end{cases}$$

Proof We write $T(\ell^w) = T_1(\ell^w) + T_2(\ell^w)$, where $T_1(\ell^w)$ is the same sum as $T(\ell^w)$ with the additional restriction that $\ell | d$ and $T_2(\ell^w)$ is the remaining sum. First, we calculate $T_1(\ell^w)$. We have that

$$\begin{aligned} T_1(\ell^w) &= \sum_{\substack{d \pmod{\ell^w} \\ \ell | d}} \left(\frac{d - 4k}{\ell^w}\right) \sum_{\substack{j \pmod{\ell^w} \\ j^2 \equiv d \pmod{\ell^w}}} \left(\frac{N + 1 + jm}{\ell}\right)^2 \\ &= \sum_{\substack{d \pmod{\ell^w} \\ \ell | d}} \left(\frac{-4k}{\ell}\right)^w \left(\frac{N+1}{\ell}\right)^2 \sum_{\substack{j \pmod{\ell^w},\ \ell | j \\ j^2 \equiv d \pmod{\ell^w}}} 1 \\ &= \left(\frac{-k}{\ell}\right)^w \left(\frac{N+1}{\ell}\right)^2 \sum_{\substack{j \pmod{\ell^w} \\ \ell | j}} 1 = \left(\frac{-k}{\ell}\right)^w \left(\frac{N+1}{\ell}\right)^2 \ell^{w-1}. \end{aligned}$$

Finally, we compute $T_2(\ell^w)$. Applying Lemma 5.1, we find that

$$T_2(\ell^w) = \sum_{\substack{d \,(\mathrm{mod}\, \ell^w)\\(d,\ell)=1}} \Big(\frac{d-4k}{\ell}\Big)^w \Big(1+\Big(\frac{(N+1)^2-dm^2}{\ell}\Big)^2\Big(\frac{d}{\ell}\Big)\Big)$$

$$= \ell^{w-1} \sum_{d \,(\mathrm{mod}\, \ell)} \Big(\frac{d-4k}{\ell}\Big)^w \Big(1+\Big(\frac{(N+1)^2-dm^2}{\ell}\Big)^2\Big(\frac{d}{\ell}\Big)\Big) - \ell^{w-1}\Big(\frac{-k}{\ell}\Big)^w.$$

If $\ell | m$, then $\big(\frac{(N+1)^2-dm^2}{\ell}\big) = 1$ for all $d \,(\mathrm{mod}\, \ell)$. On the other hand, if $\ell \nmid m$, then there is precisely one $d \,(\mathrm{mod}\, \ell)$ such that $(N+1)^2 - dm^2 \equiv 0 \,(\mathrm{mod}\, \ell)$ for which we have that

$$\Big(\frac{d-4k}{\ell}\Big)^w = \Big(\frac{m^2 d - 4m^2 k}{\ell}\Big)^w = \Big(\frac{(N-1)^2}{\ell}\Big)^w = \Big(\frac{N-1}{\ell}\Big)^2$$

and

$$\Big(\frac{d}{\ell}\Big) = \Big(\frac{N+1}{\ell}\Big)^2.$$

Thus, whether ℓ divides m or not, we have

$$\frac{T_2(\ell^w)}{\ell^{w-1}} = -\Big(\frac{-k}{\ell}\Big)^w - \Big(\frac{m(N-1)(N+1)}{\ell}\Big)^2 + \sum_{d \,(\mathrm{mod}\, \ell)} \Big(\frac{d-4k}{\ell}\Big)^w \Big(1+\Big(\frac{d}{\ell}\Big)\Big),$$

which implies that

$$\frac{T(\ell^w)}{\ell^{w-1}} = \Big(\frac{-k}{\ell}\Big)^w \Big(\frac{N+1}{\ell}\Big)^2 - \Big(\frac{-k}{\ell}\Big)^w - \Big(\frac{m(N-1)(N+1)}{\ell}\Big)^2 + \sum_{d \,(\mathrm{mod}\, \ell)} \Big(\frac{d-4k}{\ell}\Big)^w \Big(1+\Big(\frac{d}{\ell}\Big).$$

Note that if $\ell | N+1$, then $\big(\frac{-k}{\ell}\big) = 1$ and thus

$$\Big(\frac{-k}{\ell}\Big)^w \Big(\frac{N+1}{\ell}\Big)^2 - \Big(\frac{-k}{\ell}\Big)^w - \Big(\frac{m(N-1)(N+1)}{\ell}\Big)^2 = -1 = -\Big(\frac{m(N-1)}{\ell}\Big)^2,$$

whereas if $\ell \nmid N+1$, then

$$\Big(\frac{-k}{\ell}\Big)^w \Big(\frac{N+1}{\ell}\Big)^2 - \Big(\frac{-k}{\ell}\Big)^w - \Big(\frac{m(N-1)(N+1)}{\ell}\Big)^2 = -\Big(\frac{m(N-1)}{\ell}\Big)^2.$$

So

$$\frac{T(\ell^w)}{\ell^{w-1}} = -\Big(\frac{m(N-1)}{\ell}\Big)^2 + \sum_{d \,(\mathrm{mod}\, \ell)} \Big(\frac{d-4k}{\ell}\Big)^w \Big(1+\Big(\frac{d}{\ell}\Big)\Big).$$

If now w is odd, then

$$\sum_{d \,(\mathrm{mod}\, \ell)} \Big(\frac{d-4k}{\ell}\Big)^w \Big(1+\Big(\frac{d}{\ell}\Big)\Big) = \sum_{d \,(\mathrm{mod}\, \ell)} \Big(\frac{d-4k}{\ell}\Big)\Big(\frac{d}{\ell}\Big) = -1,$$

using for example [Ste94, Exercise 1.1.9] since $(2k, \ell) = 1$. Finally, if w is even, then

$$\sum_{d \,(\mathrm{mod}\, \ell)} \Big(\frac{d-4k}{\ell}\Big)^w \Big(1+\Big(\frac{d}{\ell}\Big)\Big) = \ell - 1 + \sum_{\substack{d \,(\mathrm{mod}\, \ell)\\ d \not\equiv 4k \,(\mathrm{mod}\, \ell)}} \Big(\frac{d}{\ell}\Big) = \ell - 1 - \Big(\frac{k}{\ell}\Big),$$

which completes the proof of the proposition. ∎

Corollary 5.3 *For a prime ℓ not dividing $2k$, we have that*

$$P(\ell) := 1 + \sum_{w\geq 1} \frac{T(\ell^w)}{\ell^{2w-1}(\ell - (\frac{m}{\ell})^2)} = \frac{\ell^3 - (\frac{m}{\ell})^2\ell^2 - (1 + (\frac{m}{\ell})^2\left(\frac{N-1}{\ell}\right)^2)\ell - 1 - (\frac{N-1}{\ell})^2(\frac{k}{\ell})}{(\ell^2-1)(\ell - (\frac{m}{\ell})^2)}.$$

Proof Lemma 5.2 and a straightforward computation imply that

$$P(\ell) = \frac{\ell^3 - (\frac{m}{\ell})^2\ell^2 - (1 + (\frac{m}{\ell})^2(\frac{N-1}{\ell})^2)\ell + (\frac{m}{\ell})^2 - (\frac{m(N-1)}{\ell})^2 - 1 - (\frac{k}{\ell})}{(\ell^2-1)(\ell - (\frac{m}{\ell})^2)}.$$

Finally, note that

$$\left(\frac{m(N-1)}{\ell}\right)^2 + \left(\frac{k}{\ell}\right) - \left(\frac{m}{\ell}\right)^2 = \left(\frac{N-1}{\ell}\right)^2\left(\frac{k}{\ell}\right),$$

since $(\frac{k}{\ell}) = (\frac{m}{\ell})^2 = 1$ if $\ell | N-1$. ∎

6 Proof of Proposition 2.8

This section is dedicated to the proof of Proposition 2.8, which gives an upper bound of the conjectured order of magnitude for the average of special values

$$\mathcal{L}(d(p)) = L\left(1, \left(\frac{d(p)}{\cdot}\right)\right),$$

summed over integers with no small prime factors. A key role will be played by the fundamental lemma of sieve methods, *i.e.*, Lemma 2.7.

Proof of Proposition 2.8 We shall employ the notation

$$\rho(n) := \frac{|n|}{\phi(|n|)} = \prod_{\ell | n}\left(1 - \frac{1}{\ell}\right)^{-1}.$$

We will simplify the sum we are estimating with an application of the Cauchy-Schwarz inequality but, first, we massage the L-functions that appear in it. Note that if $p = 1 + jm$, then $d(p) = (j - mk)^2 - 4k \equiv j^2 \pmod{k}$. So

$$\mathcal{L}(d(p))^r = \prod_{\substack{\ell | k \\ \ell \nmid j}}\left(1 - \frac{1}{\ell}\right)^{-r} \prod_{\ell \nmid k}\left(1 - \frac{(\frac{d(p)}{\ell})}{\ell}\right)^{-r} \ll_r \rho(k)^r \rho((j,k))^{|r|} \mathcal{L}\left(k^2 d\left(\tfrac{p}{\cdot}\right)\right)^r,$$

and consequently,

$$S := \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod{m}}} \rho(d(p))^s \mathcal{L}(d(p))^r \ll_r \rho(k)^r \sum_{\substack{N^- < p < N^+ \\ p = 1 + jm,\, j \in \mathbb{N}}} \rho((j,k))^{|r|} \rho(d(p))^s \mathcal{L}(k^2 d(p))^r.$$

Hence the Cauchy-Schwarz inequality yields that

$$\frac{S}{\rho(k)^r} \ll_r \Big(\sum_{\substack{N^-<p<N^+\\ p\equiv 1+jm}} \rho((j,k))^{2|r|}\rho(d(p))^{2s}\Big)^{\frac12}\Big(\sum_{\substack{N^-<p<N^+\\ p\equiv 1 \,(\mathrm{mod}\, m)}} \mathcal{L}(k^2 d(p))^{2r}\Big)^{\frac12} =: \sqrt{S_1 S_2}, \tag{6.1}$$

say.

First, we estimate S_1. Note that

$$\rho(n)^\nu \asymp_\nu \prod_{\ell\mid n}\Big(1+\frac{\nu}{\ell}\Big) = \sum_{a\mid n}\frac{\mu^2(a)\tau_\nu(a)}{a},$$

for any $\nu \geq 0$. Since

$$\sum_{\substack{a\mid n\\ a>x}}\frac{\mu^2(a)\tau_\nu(a)}{a} \leq \frac1x\sum_{a\mid n}\mu^2(a)\nu^{\omega(a)} = \frac{(\nu+1)^{\omega(n)}}{x} \ll_{\nu,\epsilon} \frac{n^\epsilon}{x},$$

we find that

$$S_1 \ll_r \sum_{\substack{N^-<p<N^+\\ p\equiv 1+jm}}\Big(\sum_{\substack{a\mid(k,j)\\ a\leq k^{1/5}}}\frac{\mu^2(a)\tau_{2|r|}(a)}{a} + O_r(k^{-1/6})\Big)\Big(\sum_{\substack{b\mid d(p)\\ b\leq k^{1/5}}}\frac{\mu^2(b)\tau_{2s}(b)}{b} + O_s(k^{-1/6})\Big) \tag{6.2}$$

$$= \sum_{\substack{a,b\leq k^{1/5}\\ a\mid k}}\frac{\mu^2(a)\mu^2(b)\tau_{2|r|}(a)\tau_{2s}(b)}{ab}\sum_{\substack{N^-<p<N^+\\ p\equiv 1+jm\\ a\mid j,\ b\mid d(p)}} 1 + O_{r,s}(k^{11/30}),$$

using the trivial estimate $\#\{N^- < p < N^+ : p \equiv 1 \,(\mathrm{mod}\, m)\} \ll \sqrt{N}/m = \sqrt{k}$. The innermost sum in the second line of (6.2) equals

$$\sum_{\substack{h\in\mathbb{Z}/[a,b]\mathbb{Z}\\ h\equiv 0\,(\mathrm{mod}\,a)\\ (h-mk)^2\equiv 4k\,(\mathrm{mod}\,b)}}\ \sum_{\substack{N^-<p<N^+\\ p\equiv 1+jm\\ j\equiv h\,(\mathrm{mod}\,[a,b])}} 1 \ll \frac{\sqrt{N}}{\phi(m[a,b])\log(2k)}\sum_{\substack{h\in\mathbb{Z}/[a,b]\mathbb{Z}\\ h\equiv 0\,(\mathrm{mod}\,a)\\ (h-mk)^2\equiv 4k\,(\mathrm{mod}\,b)}} 1 \leq \frac{\sqrt{N}\tau(b)}{\phi(m[a,b])\log(2k)},$$

where the first inequality follows from the Brun–Titchmarsch inequality and the second from the fact that b is square-free. Since $\phi(m[a,b]) \geq \phi(m)\phi([a,b])$, relation (6.2) becomes

$$S_1 \ll_{r,s} \frac{\sqrt{N}}{\phi(m)\log(2k)}\sum_{\substack{a,b\leq k^{1/5}\\ a\mid k}}\frac{\mu^2(a)\mu^2(b)\tau_{2|r|}(a)\tau_{2s}(b)^2}{a\cdot b\cdot\phi([a,b])} + k^{11/30} \ll_{r,s} \frac{\sqrt{N}}{\phi(m)\log(2k)}. \tag{6.3}$$

Next, we turn to the estimation of

$$S_2 = \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \mathcal{L}(k^2 d(p))^{2r}.$$

Our first task is to replace the L-values that appear in the above sum with truncated Euler products. We set

$$S_3 = \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \mathcal{L}(k^2 d(p); z^{80000})^{2r}$$

with $z = \log(4k)$ and estimate the error $R := S_2 - S_3$ using Lemma 2.3. First note that since $d(p)$ is a discriminant and $|d(p)| \le 4k$ for $p \in (N^-, N^+)$, it follows that

$$\left(\frac{k^2 d(p)}{\cdot}\right) \tag{6.4}$$

is periodic modulo $k|d(p)| \le 4k^2$ and its conductor cannot exceed $|d(p)| \le 4k$. Thus, we may apply Lemma 2.3 with $\alpha = 100$ and $Q = 4k$. Now let $d_1 = d_1(p)$ be the discriminant of the quadratic number field $\mathbb{Q}\big(\sqrt{d(p)}\big)$, so that the character in (6.4) is induced by the primitive character $\left(\frac{d_1}{\cdot}\right)$. If $|d_1| \notin \mathcal{E}_{100}(4k)$, then we can approximate $\mathcal{L}(k^2 d(p))^{2r}$ very well by $\mathcal{L}(k^2 d(p); z^{80000})^{2r}$. Otherwise, we write $d(p) = d_1 b^2$ and note that

$$\mathcal{L}(k^2 d(p))^{2r} \le \rho(kb)^{2|r|} \mathcal{L}(d_1)^{2r} \ll_r \rho(kb)^{2|r|} \cdot \begin{cases} (\log |d_1|)^{2r} & \text{if } r \ge 0, \\ |d_1|^{1/8} & \text{if } r < 0, \end{cases}$$

the second estimate being a consequence of Siegel's theorem. In any case, we find that

$$\mathcal{L}(k^2 d(p))^{2r} \ll_r (\rho(kb))^{2|r|} |d_1|^{1/8} \ll_r (kb|d_1|)^{1/8} \le (k|d(p)|)^{1/8} \le (2k)^{1/4}.$$

Combining the above, we arrive at the estimate

$$R \ll_r \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \frac{(\log\log k)^{2|r|}}{\log^{100}(2k)} + \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m) \\ |d_1| \in \mathcal{E}_{100}(4k)}} k^{1/4}.$$

Note that if $p = 1 + jm$ is such that $|d_1| \in \mathcal{E}_{100}(4k)$, then $d(p) = d_1 b^2$ for some $b \in \mathbb{N}$, or equivalently, $(j - mk)^2 - d_1 b^2 = 4k$. So for each fixed d_1 with $|d_1| \in \mathcal{E}_{100}(4k)$, there are at most $4\tau(4k) \ll k^{1/100}$ admissible values of j (and hence of p). Consequently,

$$R \ll_r \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \frac{(\log\log k)^{2|r|}}{\log^{100}(2k)} + k^{1/4} \cdot k^{1/100} \cdot |\mathcal{E}_{100}(4k)| \ll_r \frac{\sqrt{N}}{\log(2k)\phi(m)}, \tag{6.5}$$

by Lemma 2.3 and the Brun-Titchmarsch inequality.

Finally, we turn to the estimation of S_3. First, note that

$$\mathcal{L}(k^2 d(p); z^{80000})^{2r} \ll_r \mathcal{L}(k^2 d(p); \sqrt{z})^{2r} \ll_r \prod_{\substack{\ell \nmid 2pk \\ 2|r|+1 < \ell \le \sqrt{z}}} \left(1 + 2r \cdot \frac{\left(\frac{d(p)}{\ell}\right)}{\ell}\right),$$

by Mertens' estimate, which immediately implies that

$$S_3 \ll_r \sum_{\substack{N^-<p<N^+\\ p\equiv 1 \,(\mathrm{mod}\, m)}} \prod_{\substack{\ell \nmid 2pk\\ 2|r|+1<\ell\le\sqrt{z}}} \Big(1+2r\cdot \frac{\big(\frac{d(p)}{\ell}\big)}{\ell}\Big).$$

We cannot estimate this sum as it is because that would require information about primes in arithmetic progressions that are currently not available. We refer the reader to [DS14b] for a more detailed discussion about this issue. Instead, we extend the summation from primes p to integers n with no prime factors $\le k^{1/8}$ and we apply Lemma 2.7 with $D = k^{1/4}$ and $y = k^{1/8}$. Hence

$$S_3 \ll_r \sum_{\substack{N^-<n<N^+\\ n\equiv 1 \,(\mathrm{mod}\, m)}} (\lambda^+ * 1)(n) \prod_{\substack{2|r|+1<\ell\le\sqrt{z}\\ \ell \nmid 2nk}} \Big(1+2r\cdot \frac{\big(\frac{d(n)}{\ell}\big)}{\ell}\Big) =: S_4, \tag{6.6}$$

by the positivity of the above Euler product. Expanding this product to a sum, opening the convolution $(\lambda^+ * 1)(n)$, and interchanging the order of summation yields

$$\begin{aligned} S_4 &= \sum_{\substack{\ell \mid a \Rightarrow 2|r|+1<\ell\le\sqrt{z}\\ (a,2k)=1}} \frac{\mu^2(a)\tau_{2r}(a)}{a} \sum_{\substack{N^-<n<N^+\\ (n,a)=1\\ n\equiv 1 \,(\mathrm{mod}\, m)}} (\lambda^+ * 1)(n)\Big(\frac{d(n)}{a}\Big)\\ &= \sum_{\substack{\ell \mid a \Rightarrow 2|r|+1<\ell\le\sqrt{z}\\ (a,2k)=1}} \frac{\mu^2(a)\tau_{2r}(a)}{a} \sum_{\substack{b\le k^{1/4}\\ (b,am)=1}} \lambda^+(b) \sum_{\substack{N^-<n<N^+\\ (n,a)=1,\, b\mid n\\ n\equiv 1 \,(\mathrm{mod}\, m)}} \Big(\frac{d(n)}{a}\Big). \end{aligned}$$

Splitting the integers $n \in (N^-, N^+)$ according to the congruence class of $d(n) \,(\mathrm{mod}\, a)$, we deduce that

$$S_4 = \sum_{\substack{\ell \mid a \Rightarrow 2|r|+1<\ell\le\sqrt{z}\\ (a,2k)=1}} \frac{\mu^2(a)\tau_{2r}(a)}{a} \sum_{\substack{b\le k^{1/4}\\ (b,am)=1}} \lambda^+(b) \sum_{c\in\mathbb{Z}/a\mathbb{Z}} \Big(\frac{c}{a}\Big) S(a,b,c), \tag{6.7}$$

where

$$S(a,b,c) := \#\Big\{ N^- < n < N^+ : n \equiv 1 \,(\mathrm{mod}\, m), (n,a) = 1, \\ n \equiv 0 \,(\mathrm{mod}\, b), d(n) \equiv c \,(\mathrm{mod}\, a)\Big\}.$$

We fix a, b, and c as above and calculate $S(a,b,c)$. Set $n = 1 + jm$, and define $\Delta(j) = (j - mk)^2 - 4k$, so that $d(n) = \Delta(j)$. Note that n is counted by $S(a,b,c)$ if and only if $mk - 2\sqrt{k} < j < mk + 2\sqrt{k}$, $\Delta(j) \equiv c \,(\mathrm{mod}\, a)$, $1 + jm \equiv 0 \,(\mathrm{mod}\, b)$, and $(1 + jm, a) = 1$. Thus we have that

$$S(a,b,c) = \Big(\frac{4\sqrt{k}}{ab} + O(1)\Big) J(a,b,c), \tag{6.8}$$

where

$$J(a,b,c) := \#\{j \in \mathbb{Z}/ab\mathbb{Z} : \Delta(j) \equiv c \,(\mathrm{mod}\, a),\ 1 + jm \equiv 0 \,(\mathrm{mod}\, b),\ (1 + jm, a) = 1\}.$$

By the Chinese remainder theorem, we find that

$$J(a,b,c) = U(a,c) := \#\{j \in \mathbb{Z}/a\mathbb{Z} : \Delta(j) \equiv c \,(\mathrm{mod}\, a),\ (1 + jm, a) = 1\},$$

since $(b, m) = 1$, and thus there is exactly one solution modulo b to the equation $1 + jm \equiv 0 \pmod{b}$. Note that $U(a, c) \le \tau(a)$ by Lemma 5.1 and that

$$\sum_{c \in \mathbb{Z}/a\mathbb{Z}} \left(\frac{c}{a}\right) U(a, c) = T(a),$$

where $T(a)$ is defined by relation (5.1). Together with relations (6.7) and (6.8) this implies that

$$S_4 = 4\sqrt{k} \sum_{\substack{\ell \mid a \Rightarrow 2|r|+1 < \ell \le \sqrt{z} \\ (a,2k)=1}} \frac{\mu^2(a)\tau_{2r}(a)T(a)}{a^2} \sum_{\substack{b \le k^{1/4} \\ (b,am)=1}} \frac{\lambda^+(b)}{b} + O\Big(k^{1/4} \sum_{P^+(a) \le \sqrt{z}} \mu^2(a)\tau_{2|r|}(a)\tau(a)\Big).$$

The error term in the above estimate is

$$\ll k^{1/4} \sum_{P^+(a) \le \sqrt{z}} \mu^2(a)\tau_{2|r|}(a)\tau(a) = k^{1/4} \prod_{\ell \le \sqrt{z}} (1 + 4|r|) \ll_r k^{1/3}.$$

Finally, note that $|T(a)| \le \tau(a)$ for square-free values of a by Proposition 5.2. So applying Lemma 2.7 we conclude that

$$\begin{aligned} S_4 &\ll_r \sqrt{k} \sum_{\substack{P^+(a) \le \sqrt{z} \\ (a,2k)=1}} \frac{\mu^2(a)\tau(a)\tau_{2|r|}(a)}{a^2} \prod_{\substack{\ell \le k^{1/8} \\ \ell \nmid am}} \left(1 - \frac{1}{\ell}\right) + k^{1/3} \\ &\ll \sqrt{k} \sum_{\substack{P^+(a) \le \sqrt{z} \\ (a,2k)=1}} \frac{\mu^2(a)\tau(a)\tau_{2|r|}(a)}{a^2} \frac{1}{\log(2k)} \frac{m}{\phi(m)} \frac{a}{\phi(a)} + k^{1/3}. \end{aligned}$$

Inserting this estimate in (6.6), we obtain the upper bound

$$S_3 \ll_r \frac{\sqrt{k}}{\log(2k)} \frac{m}{\phi(m)} \sum_{(a,2k)=1} \frac{\mu^2(a)\tau(a)\tau_{2|r|}(a)}{a\phi(a)} \ll_r \frac{\sqrt{k}}{\log(2k)} \frac{m}{\phi(m)}.$$

Combining the above inequality with relations (6.1), (6.3), and (6.5) completes the proof of the proposition. ∎

7 Approximating $M(G)$

In this section, we prove Theorem 2.5. We start with a preliminary lemma.

Lemma 7.1 *Let $N = m^2 k > 1$ and $d(p) = d_{m,k}(p)$. If $1 \le q \le h \le \sqrt{N}$ and $(a, q) = 1$, then*

$$\sum_{\substack{N^- < p \le N^+ \\ p \equiv a \pmod{q}}} \sqrt{|d(p)|} = \frac{2\pi mk}{\phi(q) \log N} + O\Big(\frac{h}{\sqrt{N}} \cdot \frac{mk}{q} + \frac{\sqrt{k}}{h \log N} \int_{N^-}^{N^+} E(y, h; q)\mathrm{d}y\Big).$$

Proof We note the trivial bound $\#\{t < p \le t+h : p \equiv a \pmod q\} \ll h/q$ which we will use several times throughout the proof. We have that

$$\sum_{\substack{N^- < p \le N^+ \\ p \equiv a \,(\mathrm{mod}\, q)}} \sqrt{|d(p)|} = \sum_{\substack{N^- < p \le N^+ \\ p \equiv a \,(\mathrm{mod}\, q)}} \frac{\sqrt{|d(p)|}\log p}{\log N} + O\Big(\frac{\sqrt{k}}{q}\Big). \tag{7.1}$$

Note that if $t = N + 1 + 2\sqrt{N}u_0$ and $u_0 \in [-1+2\eta, 1-\eta]$ with $\eta := h/\sqrt{4N}$, then

$$\begin{aligned}\sqrt{|d(t)|} = 2\sqrt{k}\cdot\sqrt{1-u_0^2} &= \frac{2\sqrt{k}}{\eta}\int_{u_0-\eta}^{u_0}\sqrt{1-u^2}\,\mathrm{d}u + O\Big(\frac{\eta\sqrt{k}}{\sqrt{1-u_0^2}}\Big)\\ &= \frac{4mk}{h}\int_{u_0-\eta}^{u_0}\sqrt{1-u^2}\,\mathrm{d}u + O\Big(\frac{h\sqrt{k}}{\sqrt{4N-(N+1-t)^2}}\Big).\end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{\substack{N^- < p \le N^+ \\ p \equiv a \,(\mathrm{mod}\, q)}} \frac{\sqrt{|d(p)|}\log p}{\log N} &= \sum_{\substack{10h+N^- < p \le -10h+N^+ \\ p \equiv a \,(\mathrm{mod}\, q)}} \frac{\sqrt{|d(p)|}\log p}{\log N} + O\Big(\frac{h^{1/2}N^{1/4}}{m}\cdot\frac{h}{q}\Big)\\ &= \frac{4mk}{h\log N}\sum_{\substack{N^-+10h < p \le N^+-10h \\ p \equiv a \,(\mathrm{mod}\, q)}}(\log p)\int_{\frac{p-N-1-h}{2\sqrt{N}}}^{\frac{p-N-1}{2\sqrt{N}}}\sqrt{1-u^2}\,\mathrm{d}u\\ &\quad + O\Big(\sum_{\substack{N^-+10h < p \le N^+-10h \\ p \equiv a \,(\mathrm{mod}\, q)}}\frac{h\sqrt{k}}{\sqrt{(N^+-p)(p-N^-)}} + \frac{h^{3/2}N^{1/4}}{mq}\Big)\\ &= \frac{4mk}{h\log N}\int_{-1+9\eta}^{1-10\eta}\sqrt{1-u^2}\sum_{\substack{N+1+2u\sqrt{N} < p \le N+1+2u\sqrt{N}+h \\ N^-+10h < p \le N^+-10h \\ p \equiv a \,(\mathrm{mod}\, q)}}(\log p)\,\mathrm{d}u\\ &\quad + O\Big(\sum_{\substack{N^-+10h < p \le N^+-10h \\ p \equiv a \,(\mathrm{mod}\, q)}}\frac{h\sqrt{k}}{\sqrt{(N^+-p)(p-N^-)}} + \frac{h^{3/2}N^{1/4}}{mq}\Big).\end{aligned}$$

First, we simplify the main term. If $u \in [-1+10\eta, 1-11\eta]$, then the condition that $N^- + 10h < p \le N^+ - 10h$ can be discarded. On the other hand, if

$$u \in [-1,1] \smallsetminus [-1+10\eta, 1-11\eta],$$

then

$$\begin{aligned}\sqrt{1-u^2}\sum_{\substack{N+1+2u\sqrt{N} < p \le N+1+2u\sqrt{N}+h \\ N^-+10h < p \le N^+-10h \\ p \equiv a \,(\mathrm{mod}\, q)}}(\log p) &\le \sqrt{1-u^2}\sum_{\substack{N+1+2u\sqrt{N} < p \le N+1+2u\sqrt{N}+h \\ p \equiv a \,(\mathrm{mod}\, q)}}(\log p)\\ &\ll \sqrt{\eta}\cdot\frac{h\log N}{q}.\end{aligned}$$

Therefore,

$$\begin{aligned}
&\int_{-1+9\eta}^{1-10\eta} \sqrt{1-u^2} \sum_{\substack{N+1+2u\sqrt{N}<p\le N+1+2u\sqrt{N}+h\\ N^-+10h<p\le N^+-10h\\ p\equiv a \pmod q}} (\log p)\,\mathrm{d}u \\
&\quad = \int_{-1}^{1} \sqrt{1-u^2} \sum_{\substack{N+1+2u\sqrt{N}<p\le N+1+2u\sqrt{N}+h\\ p\equiv a \pmod q}} (\log p)\,\mathrm{d}u + O\Big(\frac{\eta^{3/2} h \log N}{q}\Big) \\
&\quad = \int_{-1}^{1} \sqrt{1-u^2}\frac{h}{\phi(q)}\,\mathrm{d}u + O\Big(\int_{-1}^{1} E(N+1+2u\sqrt{N},h;q)\,\mathrm{d}u + \frac{h^{5/2}\log N}{N^{3/4}q}\Big) \\
&\quad = \frac{\pi}{2}\cdot\frac{h}{\phi(q)} + O\Big(\frac{1}{\sqrt{N}}\int_{N^-}^{N^+} E(y,h;q)\,\mathrm{d}y + \frac{h^{5/2}\log N}{N^{3/4}q}\Big).
\end{aligned}$$

Consequently,

$$\begin{aligned}
\sum_{\substack{N^-<p\le N^+\\ p\equiv a \pmod q}} \sqrt{|d(p)|} &= \frac{2\pi m k}{\phi(q)\log N} + O\Big(\sum_{\substack{N^-+10h<p\le N^+-10h\\ p\equiv a \pmod q}} \frac{h\sqrt{k}}{\sqrt{(N^+-p)(p-N^-)}}\Big) \\
&\quad + O\Big(\frac{\sqrt{k}}{h\log N}\int_{N^-}^{N^+} E(y,h;q)\,dy + \frac{\sqrt{k}}{q} + \frac{h^{3/2}N^{1/4}}{mq}\Big),
\end{aligned}$$

where the term $\sqrt{k}/q$ inside the big-Oh comes from (7.1). It remains to bound

$$\sum_{\substack{N^-+10h<p\le N^+-10h\\ p\equiv a \pmod q}} \frac{1}{\sqrt{(N^+-p)(p-N^-)}}.$$

We break this sum into two pieces, according to whether $p \le N+1$ or $p > N+1$. Note that

$$\sum_{\substack{N^-+10h<p\le N+1\\ p\equiv a \pmod q}} \frac{1}{\sqrt{(N^+-p)(p-N^-)}} \ll N^{-1/4} \sum_{\substack{N^-+10h<n\le N+1\\ n\equiv a \pmod q}} \frac{1}{\sqrt{n-N^-}}.$$

We cover the range of summation by intervals of length h to find that

$$\begin{aligned}
\sum_{\substack{N^-+10h<p\le N+1\\ p\equiv a \pmod q}} \frac{1}{\sqrt{(N^+-p)(p-N^-)}} &\ll N^{-1/4} \sum_{1\le j\le 2\sqrt{N}/h} \frac{1}{\sqrt{jh}} \cdot \sum_{\substack{N^-+jh<n\le N^-+jh+h\\ n\equiv a \pmod q}} 1 \\
&\ll \frac{\sqrt{h}}{N^{1/4}q} \sum_{1\le j\le 2\sqrt{N}/h} \frac{1}{\sqrt{j}} \ll \frac{1}{q},
\end{aligned}$$

and

$$\sum_{\substack{N+1<p\le N^+-10h\\ p\equiv a \pmod q}} \frac{1}{\sqrt{(N^+-p)(p-N^-)}} \ll \frac{1}{q},$$

which implies that

$$\sum_{\substack{N^-<p\le N^+\\ p\equiv a \,(\mathrm{mod}\, q)}} \sqrt{|d(p)|} = \frac{2\pi mk}{\phi(q)\log N} + O\Big(\frac{\sqrt{k}}{h\log N}\int_{N^-}^{N^+} E(y,h;q)\,dy + \frac{h\sqrt{k}}{q} + \frac{h^{3/2}N^{1/4}}{mq}\Big).$$

Since $h^{3/2} = N^{3/4}(h/\sqrt{N})^{3/2} \le N^{3/4}(h/\sqrt{N})$, the lemma follows. ∎

Using the above result and the results of Section 5, we will prove Theorem 2.5. But first we need to introduce some additional notation and state another intermediate result. Set

$$J_r(v) = \big\{1 \le j \le 2^{2v+3} : (j-mk)^2 \equiv 4k + 4^v r \,(\mathrm{mod}\, 2^{2v+3}),\ jm \equiv 0 \,(\mathrm{mod}\, 2)\big\} \tag{7.2}$$

and

$$\mathcal{J}(v) = \frac{1}{2^{v_0-1}} \sum_{r\in\{0,1,4,5\}} \frac{|J_r(v)|}{2-\left(\frac{r}{2}\right)}, \quad \text{where} \quad v_0 = \begin{cases} 2 & \text{if } 2\nmid m,\\ 3 & \text{if } 2\mid m. \end{cases} \tag{7.3}$$

Finally, set

$$\mathcal{J} = \sum_{\substack{v\ge 0\\ (2^v,k)=1}} \frac{\mathcal{J}(v)}{8^v}.$$

Then we have the following formula.

Lemma 7.2

$$\mathcal{J} = \begin{cases} \frac{2}{3} & \text{if } 2\nmid mk,\\ \frac{3}{2} & \text{if } 2\mid (m,k),\\ 1 & \text{if } 2\mid mk,\ 2\nmid (m,k). \end{cases}$$

We postpone the proof of this lemma until the last section.

Proof of Theorem 2.5 We will show the theorem with $8\epsilon \in (0,1/3]$ in place of ϵ and when k is large enough in terms of ϵ, which is clearly sufficient. Our starting point is Lemma 2.1, which states that

$$M(G) = \sum_{\substack{N^-<p<N^+\\ p\equiv 1 \,(\mathrm{mod}\, m)}} \sum_{\substack{f^2\mid d(p),\,(f,k)=1\\ d(p)/f^2\equiv 1,0 \,(\mathrm{mod}\, 4)}} \frac{\sqrt{|d(p)|}\mathcal{L}(d(p)/f^2)}{2\pi f},$$

where $N = m^2k$ and $d(p) = d_{m,k}(p) = ((p-N-1)^2-4N)/m^2$ as usual. If $p = 1+jm$, then $d(p) = (j-mk)^2-4k$. Therefore, if ℓ is an odd prime dividing k so that $(\ell, f) = 1$ for f as in the above sum, then

$$\Big(\frac{d(p)/f^2}{\ell}\Big) = \Big(\frac{d(p)}{\ell}\Big) = \Big(\frac{j}{\ell}\Big)^2.$$

Next, we write $f = 2^v g$ with g odd and consider $r \in \{0,1,4,5\}$ such that $d(p)/f^2 \equiv r \,(\mathrm{mod}\, 8)$. Then we have that $\big(\frac{d(p)/f^2}{2}\big) = \big(\frac{r}{2}\big)$. Moreover, since $g^2 \equiv 1 \,(\mathrm{mod}\, 8)$, we have that $d(p)/f^2 \equiv d(p)/2^{2v} \,(\mathrm{mod}\, 8)$, Therefore, the conditions $f^2\mid d(p)$ and

$d(p)/f^2 \equiv r \pmod 8$ are equivalent to having $d(p) \equiv 4^\nu r \pmod{2^{2\nu+3}}$ and $g^2 | d(p)$. Setting

$$\rho(g,d) = \prod_{\ell | g} \Big(1 - \frac{\left(\frac{d}{\ell}\right)}{\ell}\Big)^{-1},$$

then gives us that

$$\mathcal{L}\big(d(p)/f^2\big) = \mathcal{L}\big((2kg)^2 d(p)\big) \frac{\rho(g, d(p)/g^2)}{1 - \left(\frac{r}{2}\right)/2} \prod_{\ell | k,\, \ell \nmid 2j} \Big(1 - \frac{1}{\ell}\Big)^{-1}.$$

Since

$$\prod_{\ell | k,\, \ell \nmid 2j} \Big(1 - \frac{1}{\ell}\Big)^{-1} = \sum_{\substack{a | k \\ (a, 2j) = 1}} \frac{\mu^2(a)}{\phi(a)},$$

we deduce that

$$M(G) = \sum_{r \in \{0,1,4,5\}} \frac{1}{2 - \left(\frac{r}{2}\right)} \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} \sum_{\substack{a | k \\ (a, 2j) = 1}} \sum_{\substack{\nu \geq 0,\, (2^\nu, k) = 1 \\ d(p) \equiv 4^\nu r \pmod{2^{2\nu+3}}}} \sum_{\substack{g^2 | d(p) \\ (g, 2k) = 1}} \frac{\mu^2(a) \sqrt{|d(p)|}}{\pi 2^\nu \phi(a) g} \rho(g, d(p)/g^2) \mathcal{L}((2kg)^2 d(p)).$$

We now use Lemma 2.3 to replace the L-value $\mathcal{L}((2kg)^2 d(p))$ by a suitably truncated product. Arguing as in the proof of relation (6.5), we note that $\left(\frac{(2kg)^2 d(p)}{\cdot}\right)$ is a character modulo $2kg|d(p)| \leq 16k^{5/2}$ with conductor not exceeding $|d(p)| \leq 4k$. Thus, we may apply Lemma 2.3 with $Q = 4k$ and 5α in place of α to replace $\mathcal{L}((2kg)^2 d(p))$ by $\mathcal{L}((2kg)^2 d(p); z)$ where we take $z = (\log(4k))^{200\alpha^2}$. The result is that

$$M(G) = \sum_{r \in \{0,1,4,5\}} \frac{1}{2 - \left(\frac{r}{2}\right)} \sum_{\substack{N^- < p < N^+ \\ p = 1 + jm,\, j \geq 1}} \sum_{\substack{a | k \\ (a, 2j) = 1}} \sum_{\substack{(2^\nu, k) = 1 \\ d(p) \equiv 4^\nu r \pmod{2^{2\nu+3}}}} \sum_{\substack{g^2 | d(p) \\ (g, 2k) = 1}} \frac{\mu^2(a) \sqrt{|d(p)|}}{\pi 2^\nu \phi(a) g} \rho(g, d(p)/g^2) \mathcal{L}((2kg)^2 d(p); z) + O_\alpha\Big(\frac{k}{(\log k)^\alpha}\Big).$$

Next, we notice that we can truncate the sums over a, g, and ν at the cost of a small error term. More precisely, using the crude bound

$$\rho(g, d(p)/g^2) \mathcal{L}((2kg)^2 d(p); z) \ll \frac{g}{\phi(g)} \log(2kg|d(p)|) \ll (\log k)^2,$$

we find that the contribution to $M(G)$ by those summands with $\max\{a, g, 2^\nu\} > k^\epsilon$ is

$$\ll \frac{\sqrt{k} (\log k)^3}{k^\epsilon} \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} \sum_{\substack{a | k \\ (2^\nu g)^2 | d(p)}} 1 \ll_\epsilon k^{(1-\epsilon)/2} \sum_{\substack{N^- < n < N^+ \\ n \equiv 1 \pmod m}} 1 \ll k^{1-\epsilon/2} \tag{7.4}$$

by the bound $\tau(n) \ll_\delta n^\delta$, with $\delta < \epsilon/4$. Moreover,

$$\begin{aligned}\mathcal{L}\big((2kg)^2 d(p); z\big) &= \sum_{\substack{P^+(n)\le z\\(n,2kg)=1}} \frac{\left(\frac{d(p)}{n}\right)}{n}\\ &= \sum_{\substack{P^+(n)\le z,\ n\le k^\epsilon\\(n,2kg)=1}} \frac{\left(\frac{d(p)}{n}\right)}{n} + O_{\epsilon,\alpha}\big((\log k)^{-\alpha-10}\big)\end{aligned}$$

by Lemma 2.4. Therefore,

$$\begin{aligned}M(G) = \sum_{r\in\{0,1,4,5\}} \frac{1}{2-\left(\frac{r}{2}\right)} \sum_{\substack{a\mid k,\ a\le k^\epsilon\\(a,2)=1}} \sum_{\substack{2^\nu\le k^\epsilon\\(2^\nu,k)=1}} \sum_{\substack{g\le k^\epsilon\\(g,2k)=1}} \sum_{\substack{P^+(n)\le z,\ n\le k^\epsilon\\(n,2kg)=1}} \frac{\mu^2(a)}{\pi 2^\nu \phi(a) g n}\\ \times \sum_{\substack{N^-<p<N^+\\p=1+jm,\ j\ge 1\\(a,j)=1,\ g^2\mid d(p)\\d(p)\equiv 4^\nu r \pmod{2^{2\nu+3}}}} \rho(g, d(p)/g^2)\Big(\frac{d(p)}{n}\Big)\sqrt{|d(p)|} + O_{\alpha,\epsilon}\Big(\frac{k}{(\log k)^\alpha}\Big).\end{aligned}$$

We note that if $d(p)/g^2 \equiv b \pmod g$, then $\left(\frac{d(p)/g^2}{\ell}\right) = \left(\frac{b}{\ell}\right)$ for all $\ell \mid g$ and consequently, $\rho(g, d(p)/g^2) = \rho(g, b)$. So, summing over possible choices for

$$d(p)/g^2 \pmod g \quad \text{and} \quad d(p) \pmod n,$$

we deduce that

$$\begin{aligned}M(G) = \sum_{r\in\{0,1,4,5\}} \frac{1}{2-\left(\frac{r}{2}\right)} \sum_{\substack{a\mid k,\ a\le k^\epsilon\\(a,2)=1}} \sum_{\substack{2^\nu\le k^\epsilon\\(2^\nu,k)=1}} \sum_{\substack{g\le k^\epsilon\\(g,2k)=1}} \sum_{\substack{P^+(n)\le z,\ n\le k^\epsilon\\(n,2kg)=1}} \frac{\mu^2(a)}{\pi 2^\nu \phi(a) g n}\\ \times \sum_{b=1}^{g} \rho(g,b) \sum_{c=1}^{n} \left(\frac{c}{n}\right) S_r(\nu, a, g, b, n, c) + O_{\alpha,\epsilon}\Big(\frac{k}{(\log k)^\alpha}\Big),\end{aligned}$$

where

$$S_r(\nu, a, g, b, n, c) := \sum_{\substack{N^-<p\le N^+\\p=1+jm,\ j\ge 1,\ (j,a)=1\\d(p)\equiv bg^2 \pmod{g^3}\\d(p)\equiv 4^\nu r \pmod{2^{2\nu+3}},\ d(p)\equiv c \pmod n}} \sqrt{|d(p)|}.$$

We write $p = 1 + jm$ and note that $(1 + jm, 2agn) = 1$ if k is large enough since $2agn \le 2k^{3\epsilon} \le 2k^{1/8}$ by assumption and $p > N^- = (m\sqrt{k} - 1)^2$. Moreover, with this notation we have that $d(p) = \Delta(j) := (j - mk)^2 - 4k$. So if we set

$$\begin{aligned}J_r(\nu, a, g, b, n, c) = \Big\{ j \pmod{2^{2\nu+3} a g^3 n} : \ &\Delta(j) \equiv 4^\nu r \pmod{2^{2\nu+3}},\\ &\Delta(j) \equiv bg^2 \pmod{g^3},\\ &\Delta(j) \equiv c \pmod n, (j,a) = 1,\\ &(1 + jm, agn) = 1, jm \equiv 0 \pmod 2 \Big\},\end{aligned}$$

then we find that

$$S_r(v,a,g,b,n,c) = \sum_{j\in J_r(v,a,g,b,n,c)} \sum_{\substack{N^-<p\le N^+\\ p\equiv 1+jm \pmod{2^{2v+3}ag^3nm}}} \sqrt{|d(p)|}.$$

Applying Lemma 7.1 with h as in the statement of the theorem, we deduce that

$$\frac{S_r(v,a,g,b,n,c)}{|J_r(v,a,g,b,n,c)|} = \frac{2\pi mk}{\phi(2^{2v+3}ag^3nm)\log N} + O\Big(\frac{k}{4^v ag^3n(\log k)^{\alpha+1}} + \frac{\sqrt{k}}{h\log k}\int_{N^-}^{N^+} E(y,h;2^{2v+3}ag^3nm)\,\mathrm{d}y\Big),$$

by our assumption that $h \le m\sqrt{k}/(\log k)^{\alpha+1}$ and that $m \le \sqrt{k}$. In order to compute the contribution of the above error term to $M(G)$, we note that

$$\begin{aligned}\sum_{b=1}^{g}\rho(b,g)\sum_{c=1}^{n}\big|J_r(b,v,g,a,n,c)\big| &\le \sum_{b=1}^{g}\sum_{c=1}^{n}\sum_{\substack{j \pmod{2^{2v+3}ag^3n}\\ \Delta(j)\equiv bg^2 \pmod{g^3}\\ \Delta(j)\equiv 4^v r \pmod{2^{2v+3}}\\ 2\mid jm,\ \Delta(j)\equiv c \pmod n}} \frac{g}{\phi(g)}\\ &= \sum_{\substack{j \pmod{2^{2v+3}ag^3n}\\ g^2\mid\Delta(j),\ 2\mid jm\\ \Delta(j)\equiv 4^v r \pmod{2^{2v+3}}}} \frac{g}{\phi(g)}\\ &= \frac{g}{\phi(g)}agn \sum_{\substack{j \pmod{2^{2v+3}g^2}\\ 2\mid jm,\ g^2\mid\Delta(j)\\ \Delta(j)\equiv 4^v r \pmod{2^{2v+3}}}} 1\\ &\ll \frac{ag^2n}{\phi(g)}\cdot\tau(g)\cdot|J_r(v)|\end{aligned}$$

by the Chinese remainder theorem and Lemma 5.1 where $J_r(v)$ is defined by (7.2). Since we also have that $|J_r(v)| \ll \mathcal{J}(v) \ll 1$ by Lemmas 8.2 and 8.3 below, we conclude that

$$\begin{aligned}M(G) = \frac{2mk}{\log N}\sum_{r\in\{0,1,4,5\}}\frac{1}{2-\left(\frac{r}{2}\right)}\sum_{\substack{a\mid k,\ a\le k^\epsilon\\ (a,2)=1}}\sum_{\substack{2^v\le k^\epsilon\\ (2^v,k)=1}}\sum_{\substack{g\le k^\epsilon\\ (g,2k)=1}}\\ \sum_{\substack{P^+(n)\le z,\ n\le k^\epsilon\\ (n,2kg)=1}}\frac{\mu^2(a)}{2^{3v+v_0}\phi(a)\phi(g^4an^2m)}\sum_{b=1}^{g}\rho(g,b)\sum_{c=1}^{n}\left(\frac{c}{n}\right)|J_r(b,v,g,a,n,c)|\\ + O_{\alpha,\epsilon}\Big(\frac{k}{(\log k)^\alpha}+E\Big),\end{aligned}$$

where v_0 is defined by (7.3) and

$$E := \frac{\sqrt{k}}{h}\sum_{q\le 8k^{7\epsilon}}\tau_3(q)\int_{N^-}^{N^+}E(y,h;mq)\,\mathrm{d}y,$$

since for any $q \in \mathbb{N}$ we have that

$$\sum_{\substack{q=2^{2\nu+3}ag^3n \\ a|k,\ (a,2)=(gn,2k)=1}} \tau(g) \le \sum_{g|q} \tau(g) = \tau_3(q).$$

If we set $I(g,b) = \#\big\{1 \le j \le g^3 : \Delta(j) \equiv bg^2 \pmod{g^3},\ (1+jm,g) = 1\big\}$ and $F(a) = \#\big\{1 \le j \le a : (j,a) = 1,\ (1+jm,a) = 1\big\} = \prod_{\ell^w \| a} \ell^{w-1}\big(\ell - 1 - (\frac{m}{\ell})^2\big)$, then the Chinese remainder theorem implies that

$$\begin{aligned}\sum_{c=1}^{n}\Big(\frac{c}{n}\Big)|J_r(\nu,a,g,b,n,c)| &= F(a)\cdot|J_r(\nu)|\cdot I(g,b)\sum_{c=1}^{n}\Big(\frac{c}{n}\Big)\sum_{\substack{j \pmod n \\ \Delta(j)\equiv c \pmod n \\ (1+jm,n)=1}} 1 \\ &= F(a)\cdot|J_r(\nu)|\cdot I(g,b)\cdot T(n),\end{aligned}$$

where $T(n)$ is defined by (5.1). Therefore,

$$M(G) = \frac{mk}{\phi(m)\log N} S_1S_2S_3 + O_{\alpha,\epsilon}\Big(\frac{k}{(\log k)^\alpha} + E\Big),$$

where

$$S_1 = \sum_{r\in\{0,1,4,5\}} \frac{2}{2-\left(\frac{r}{2}\right)} \sum_{\substack{2^\nu \le k^\epsilon \\ (2^\nu,k)=1}} \frac{|J_r(\nu)|}{2^{3\nu+\nu_0}} = \mathcal{J} + O(k^{-\epsilon}),$$

by the trivial estimate $|J_r(\nu)| \ll 4^\nu$,

$$\begin{aligned}S_2 &= \sum_{\substack{a|k,\ a\le k^\epsilon \\ (a,2)=1}} \frac{\mu^2(a)F(a)}{\phi(a)a} \prod_{\ell|a,\ \ell\nmid m} \frac{\ell}{\ell-1} = \prod_{\substack{\ell|k \\ \ell\ne 2}}\Big(1 + \frac{\ell - 1 - (\frac{m}{\ell})^2}{(\ell-1)(\ell - \left(\frac{m}{\ell}\right)^2)}\Big) + O(k^{-\epsilon/2}) \\ &= \prod_{\substack{\ell|k \\ \ell\ne 2}} \frac{\ell^2 - \left(\frac{m}{\ell}\right)^2 \ell - 1}{(\ell-1)(\ell-(\frac{m}{\ell})^2)} + O(k^{-\epsilon/2}),\end{aligned}$$

by arguing as in relation (7.4) and

$$S_3 = \sum_{\substack{g\le k^\epsilon \\ (g,2k)=1}} \sum_{b=1}^{g} \frac{\rho(g,b)I(g,b)S_4(g)}{g^4} \prod_{\ell|g,\ \ell\nmid m} \frac{\ell}{\ell-1}$$

with

$$S_4(g) = \sum_{\substack{P^+(n)\le z,\ n\le k^\epsilon \\ (n,2kg)=1}} \frac{T(n)}{n^2} \prod_{\ell|n,\ \ell\nmid m} \frac{\ell}{\ell-1}.$$

In the above, to factor $\phi(g^4an^2m)$, we have used the identity

$$\phi(g^4an^2m) = \phi(m)g^4an^2 \prod_{\ell|g,\ \ell\nmid m} \frac{\ell-1}{\ell} \prod_{\ell|a,\ \ell\nmid m} \frac{\ell-1}{\ell} \prod_{\ell|n,\ \ell\nmid m} \frac{\ell-1}{\ell}$$

which holds since a, n, and g are pairwise coprime. Note that

$$\begin{aligned} I(g,b) &= \prod_{\ell^w \| g} \#\{j \,(\mathrm{mod}\, \ell^{3w}) : (j-mk)^2 \equiv 4k + bg^2 \,(\mathrm{mod}\, \ell^{3w}),\ (1+jm,\ell) = 1\} \\ &= \prod_{\ell \mid g} \Big(1 + \Big(\frac{(N+1)^2 - (4k+bg^2)m^2}{\ell}\Big)^2 \Big(\frac{4k+bg^2}{\ell}\Big)\Big) \\ &= \Big(1 + \Big(\frac{N-1}{\ell}\Big)^2 \Big(\frac{k}{\ell}\Big)\Big)^{\omega(g)} \end{aligned}$$

by Lemma 5.1, which is applicable here because $4k + bg^2 \equiv 4k \not\equiv 0 \,(\mathrm{mod}\, \ell)$ for all primes $\ell | g$. So we see that $I(g,b)$ is independent of b, which implies that

$$\begin{aligned} \sum_{b=1}^{g} \rho(g,b) I(g,b) &= I(g,0) \prod_{\ell^w \| g} \Big(\sum_{b=1}^{\ell^w} \frac{1}{1 - (\frac{b}{\ell})/\ell} \Big) \\ &= I(g,0) \prod_{\ell^w \| g} \Big(\ell^{w-1} + \ell^{w-1} \frac{\ell-1}{2} \frac{1}{1-1/\ell} + \ell^{w-1} \frac{\ell-1}{2} \frac{1}{1+1/\ell} \Big) \\ &= g I(g,0) \prod_{\ell \mid g} \frac{\ell^2 + \ell + 1}{\ell(\ell+1)}. \end{aligned}$$

Thus we conclude that

$$S_3 = \sum_{\substack{g \le k^{\epsilon} \\ (g,2k)=1}} \frac{S_4(g)}{g^3} \prod_{\ell \mid g} \frac{\big(1 + (\frac{N-1}{\ell})^2 (\frac{k}{\ell})\big)(\ell^2 + \ell + 1)}{\big(\ell - (\frac{m}{\ell})^2\big)(\ell+1)}.$$

Moreover, if $P(\ell)$ is as in Corollary 5.3, then we have that

$$S_4(g) = \frac{P}{\prod_{\ell \mid g} P(\ell)} \Big(1 + O\Big(\frac{1}{(\log k)^{\alpha+1}}\Big)\Big), \quad \text{where} \quad P := \prod_{\ell \nmid 2k} P(\ell).$$

Therefore

$$\begin{aligned} S_3 \Big(1 + O\Big(\frac{1}{(\log k)^{\alpha+1}}\Big)\Big) &= P \cdot \prod_{\ell \nmid 2k} \Big(1 + \sum_{w \ge 1} \frac{(1 + (\frac{N-1}{\ell})^2 (\frac{k}{\ell}))(\ell^2 + \ell + 1)}{\ell^{3w} (\ell - (\frac{m}{\ell})^2)(\ell+1) P(\ell)}\Big) \\ &= \prod_{\ell \nmid 2k} \Big(P(\ell) + \frac{1 + (\frac{N-1}{\ell})^2 (\frac{k}{\ell})}{(\ell^2-1)(\ell - (\frac{m}{\ell})^2)} \Big) \\ &= \prod_{\ell \nmid 2k} \frac{\ell^3 - (\frac{m}{\ell})^2 \ell^2 - \big(1 + (\frac{m(N-1)}{\ell})^2\big)\ell}{(\ell^2-1)(\ell - (\frac{m}{\ell})^2)} \\ &= \prod_{\ell \nmid 2N} \Big(1 - \frac{\ell (\frac{N-1}{\ell})^2 + 1}{(\ell^2-1)(\ell-1)}\Big). \end{aligned}$$

Consequently,

$$M(G) = \frac{\mathcal{J}mk}{\phi(m)\log N}\prod_{\ell\nmid 2N}\Big(1-\frac{\ell(\frac{N-1}{\ell})^2+1}{(\ell^2-1)(\ell-1)}\Big)\prod_{\substack{\ell\mid k\\ \ell>2}}\Big(1+\frac{\ell-1-(\frac{m}{\ell})^2}{(\ell-1)\big(\ell-(\frac{m}{\ell})^2\big)}\Big)$$
$$+ O_{\alpha,\epsilon}\Big(\frac{k}{(\log k)^\alpha}+E\Big).$$

So the theorem follows by the above estimates together with Lemmas 3.1 and 7.2. ∎

8 Powers of 2

The goal of this section is to show Lemma 7.2 which gives the value of

$$\mathcal{J} = \sum_{\substack{\nu\geq 0\\ (2^\nu,k)=1}}\frac{\mathcal{J}(\nu)}{8^\nu},$$

where

$$\mathcal{J}(\nu) = \frac{1}{2^{\nu_0-1}}\sum_{r\in\{0,1,4,5\}}\frac{|J_r(\nu)|}{2-\left(\frac{r}{2}\right)}, \qquad \nu_0 = \begin{cases}2 & \text{if } 2\nmid m,\\ 3 & \text{if } 2\mid m,\end{cases}$$

and

$$J_r(\nu) = \big\{1\leq j\leq 2^{2\nu+3} : (j-mk)^2\equiv 4k+4^\nu r \pmod{2^{2\nu+3}},\ jm\equiv 0\pmod 2\big\}.$$

We start with the following standard lemma.

Lemma 8.1 *We have that*

$$\#\big\{j\in\mathbb{Z}/8\mathbb{Z} : j^2\equiv d\pmod 8\big\} = \begin{cases}2 & \text{if } d\equiv 0,4\pmod 8,\\ 4 & \text{if } d\equiv 1\pmod 8,\\ 0 & \text{otherwise.}\end{cases}$$

Moreover, if d is odd and $e\geq 3$, then

$$\#\big\{j\in\mathbb{Z}/2^e\mathbb{Z} : j^2\equiv d\pmod{2^e}\big\} = \begin{cases}4 & \text{if } d\equiv 1\pmod 8,\\ 0 & \text{otherwise.}\end{cases}$$

We shall use the above lemma to calculate $|J_r(\nu)|$ and $\mathcal{J}(\nu)$ when $(2^\nu,k)=1$. First, we note that if $\nu\geq 1$, then k must be odd and

$$|J_r(\nu)| = \begin{cases}2\cdot\#\{j\pmod{2^{2\nu+1}} : j^2\equiv k+4^{\nu-1}r\pmod{2^{2\nu+1}}\} & \text{if } 2\mid m,\\ 0 & \text{if } 2\nmid m.\end{cases} \tag{8.1}$$

Indeed, when $\nu\geq 1$, the relation $(j-mk)^2\equiv 4k+4^\nu r\pmod{2^{2\nu+3}}$ implies that $2|(j-mk)$. Since k is odd and we also have that $jm\equiv 0\pmod 2$, we deduce that $2\mid(m,j)$. Hence, $|J_r(\nu)|=0$ when $2\nmid m$. Assuming that $2\mid m$, we write $j=mk+2j'$ and find that

$$|J_r(\nu)| = \#\big\{j'\pmod{2^{2\nu+2}} : j'^2\equiv k+4^{\nu-1}r\pmod{2^{2\nu+1}}\big\}$$
$$= 2\cdot\#\big\{j\pmod{2^{2\nu+1}} : j^2\equiv k+4^{\nu-1}r\pmod{2^{2\nu+1}}\big\},$$

as claimed.

Lemma 8.2 *Let $v \geq 0$ with $(2^v, k) = 1$. If m is odd, then*

$$\mathcal{J}(v) = \begin{cases} 1 & \text{if } v = 0 \text{ and } 2|k, \\ \frac{2}{3} & \text{if } v = 0 \text{ and } 2 \nmid k, \\ 0 & \text{if } v \geq 1 \text{ and } 2 \nmid k. \end{cases}$$

Proof The case $v \geq 1$ follows by (8.1). Assume now that $v = 0$. Since m is odd, the condition $jm \equiv 0 \pmod 2$ implies that every $j \in J_r(v)$ is even. Writing $j = 2j'$, we deduce that

$$|J_r(0)| = \#\left\{ j' \pmod 4 : (2j' - mk)^2 \equiv 4k + r \pmod 8 \right\}$$

If k is odd, then we must have that $(2j' - mk)^2 - 4k \equiv -3 \pmod 8$ and thus $r = 5$, in which case $|J_r(0)| = 4$, otherwise $|J_r(0)| = 0$. So

$$\mathcal{J}(0) = \frac{1}{2} \cdot \frac{4}{2 - (-1)} = \frac{2}{3}.$$

Finally, assume that k is even. Writing $z = j' - mk/2$, our task reduces to counting solutions to $4z^2 \equiv r \pmod 8$ with $1 \leq z \leq 4$. If $r \in \{1, 5\}$. Then there are no such solutions. Whereas if $r \in \{0, 4\}$, then there are precisely two such solutions. Consequently, when m is odd and k is even,

$$\mathcal{J}(0) = \frac{1}{2}\left(\frac{2}{2 - 0} + \frac{2}{2 - 0} \right) = 1,$$

and the lemma follows in this case, too. ∎

Lemma 8.3 *Let $v \geq 0$ with $(2^v, k) = 1$, and suppose that $2|m$. If $2|k$, then $\mathcal{J}(0) = \frac{3}{2}$.*

$$\text{If } k \equiv 1 \pmod 8, \text{ then } \mathcal{J}(v) = \begin{cases} \frac{5}{6} & \text{if } v = 0, \\ 1 & \text{if } v = 1, \\ 2 & \text{if } v = 2, \\ \frac{14}{3} & \text{if } v \geq 3. \end{cases}$$

$$\text{If } k \equiv 3, 7 \pmod 8, \text{ then } \mathcal{J}(v) = \begin{cases} \frac{5}{6} & \text{if } v = 0, \\ \frac{4}{3} & \text{if } v = 1, \\ 0 & \text{if } v \geq 2. \end{cases}$$

$$\text{If } k \equiv 5 \pmod 8, \text{ then } \mathcal{J}(v) = \begin{cases} \frac{5}{6} & \text{if } v = 0, \\ 1 & \text{if } v = 1, \\ \frac{8}{3} & \text{if } v = 2, \\ 0 & \text{if } v \geq 3. \end{cases}$$

Proof First, we calculate $|J_r(0)|$. Note that the condition $jm \equiv 0 \pmod 2$ is trivially satisfied now since $2|m$. Therefore, a change of variable and Lemma 8.1 imply that

$$|J_r(0)| = \#\{j \pmod 8 : j^2 \equiv 4k + r \pmod 8\} = \begin{cases} 2 & \text{if } 4k + r \equiv 0, 4 \pmod 8, \\ 4 & \text{if } 4k + r \equiv 1 \pmod 8, \\ 0 & \text{if } 4k + r \equiv 5 \pmod 8. \end{cases}$$

Thus,

$$\mathcal{J}(0) = \begin{cases} \frac{1}{4}\left(\frac{2}{2-0} + \frac{4}{2-1} + \frac{2}{2-0} + \frac{0}{2-(-1)}\right) = \frac{3}{2} & \text{if } 2 \mid k, \\ \frac{1}{4}\left(\frac{2}{2-0} + \frac{0}{2-1} + \frac{2}{2-0} + \frac{4}{2-(-1)}\right) = \frac{5}{6} & \text{if } 2 \nmid k. \end{cases}$$

Next assume that $\nu \geq 1$, and note that the condition $(2^\nu, k) = 1$ means that we only need consider this case when k is odd. By relation (8.1), we have that

$$|J_r(\nu)| = 2 \cdot \#\left\{ j \pmod{2^{2\nu+1}} : j^2 \equiv k + 4^{\nu-1} r \pmod{2^{2\nu+1}} \right\}.$$

Now if $\nu \geq 2$, then Lemma 8.1 implies that $|J_r(\nu)| = 2 \cdot 4 = 8$ or $|J_r(\nu)| = 0$ according to whether $k + 4^{\nu-1} r \equiv 1 \pmod 8$ or not. Therefore, when $\nu \geq 2$,

$$\mathcal{J}(\nu) = \begin{cases} \frac{1}{4}\left(\frac{8}{2-0} + \frac{8}{2-0}\right) = 2 & \text{if } \nu = 2 \text{ and } k \equiv 1 \pmod 8, \\ \frac{1}{4}\left(\frac{8}{2-1} + \frac{8}{2-(-1)}\right) = \frac{8}{3} & \text{if } \nu = 2 \text{ and } k \equiv 5 \pmod 8, \\ \frac{1}{4}\left(\frac{8}{2-0} + \frac{8}{2-1} + \frac{8}{2-0} + \frac{8}{2-(-1)}\right) = \frac{14}{3} & \text{if } \nu \geq 3 \text{ and } k \equiv 1 \pmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

Finally, we consider the case $\nu = 1$. Using Lemma 8.1 again, we have

$$|J_r(1)| = 2 \cdot \#\left\{ j \pmod 8 : j^2 \equiv k + r \pmod 8 \right\} = \begin{cases} 4 & \text{if } k + r \equiv 0, 4 \pmod 8, \\ 8 & \text{if } k + r \equiv 1 \pmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore,

$$\mathcal{J}(1) = \begin{cases} \frac{1}{4} \cdot \frac{8}{2-0} = 1 & \text{if } k \equiv 1, 5 \pmod 8, \\ \frac{1}{4}\left(\frac{4}{2-1} + \frac{4}{2-(-1)}\right) = \frac{4}{3} & \text{if } k \equiv 3, 7 \pmod 8, \end{cases}$$

which completes the proof of the lemma. ∎

Lemma 7.2 now follows as a direct consequence of Lemmas 8.2 and 8.3.

Appendix A by Chantal David, Greg Martin and Ethan Smith

The purpose of this appendix is to give a probabilistic interpretation to the Euler factors arising in $K(G)\frac{|G|}{|\mathrm{Aut}(G)|}$ and $K(N)\frac{N}{\phi(N)}$ where $K(G)$ and $K(N)$ are defined by (1.1) and (1.2), respectively. Given a prime ℓ, we let $v_\ell(\cdot)$ denote the usual ℓ-adic valuation. For each integer $e \geq 1$, we also let $\mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z})$ denote the usual group of invertible 2×2 matrices with entries from $\mathbb{Z}/\ell^e\mathbb{Z}$. The 2×2 identity matrix we denote by I. The main results of this appendix are as follows.

Theorem A.1 *For each positive integer N,*

$$\frac{K(N)\cdot N}{\phi(N)} = \prod_{\ell}\Big(\lim_{e\to\infty}\frac{\ell^e\cdot\#\{\sigma\in \mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z}) : \det(\sigma)+1-\mathrm{tr}(\sigma)\equiv N \pmod{\ell^e}\}}{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z})}\Big),$$

where the product is taken over all primes ℓ. Furthermore, the sequences defining the Euler factors are constant for $e > v_\ell(N)$.

Remark A.2 If μ denotes the Haar measure on the space of 2×2 matrices over the ℓ-adic integers $\mathbb{Z}_\ell$ normalized so that $\mu(\mathrm{GL}_2(\mathbb{Z}_\ell)) = 1$, then the Euler factor of $K(N)\frac{N}{\phi(N)}$ for the prime ℓ may be viewed as the density function for the probability measure on $\mathbb{Z}_\ell$ defined by the pushforward of μ via the map $\det+1-\mathrm{tr}\colon \mathrm{GL}_2(\mathbb{Z}_\ell)\to\mathbb{Z}_\ell$.

Theorem A.3 *For each pair of positive integers m and k, put*

$$G = G_{m,k} = \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/mk\mathbb{Z}.$$

Then

$$\frac{K(G)\cdot|G|}{|\mathrm{Aut}(G)|} = \prod_{\ell}\Big(\lim_{e\to\infty}\frac{\ell^e\cdot(\#C_{N,m}(\ell^e)-\#C_{N,\ell m}(\ell^e))}{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z})}\Big),$$

where $C_{N,n}(\ell^e)$ is defined in equation (A.1), and the product is taken over all primes ℓ. Furthermore, the sequences defining the Euler factors are constant for $e > v_\ell(|G|)$.

For the remainder of this appendix, we assume that e, n, N, and ℓ are positive integers with ℓ prime and $n^2|N$. Later we will also assume that $N = |G| = m^2k$. For convenience, we let

$$C_{N,n}(\ell^e) = \big\{\sigma\in\mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z}) : \det(\sigma)+1-\mathrm{tr}(\sigma)\equiv N \pmod{\ell^e},\ \sigma\equiv I \pmod{\ell^{v_\ell(n)}}\big\}. \tag{A.1}$$

In the case that $\ell\nmid n$, we note that the condition $\sigma\equiv I\pmod{\ell^{v_\ell(n)}}$ is vacuous. As usual, $(\frac{\cdot}{\ell})$ denotes the Kronecker symbol modulo ℓ.

Lemma A.4 *If $\ell\nmid n$, then $\#C_{N,n}(\ell) = \ell\big(\ell^2-\big(\frac{N}{\ell}\big)^2\ell-1-\big(\frac{N-1}{\ell}\big)^2\big)$.*

Proof We first note that $\#C_{N,n}(\ell)$ is equal to the number of quadruples (a,b,c,d) satisfying $0\le a,b,c,d<\ell$ and

$$ad-bc+1-(a+d)\equiv N \pmod{\ell}, \tag{A.2}$$

$$ad-bc\not\equiv 0 \pmod{\ell}. \tag{A.3}$$

The lemma follows by first counting the number of quadruples satisfying (A.2) and then removing the number of quadruples satisfying (A.2) that do not satisfy (A.3).

Rearranging, we see that the condition (A.2) may be rewritten as

$$(a-1)(d-1)-bc\equiv N \pmod{\ell}.$$

It is clear that any choice of a,b,c with $a\neq 1$ uniquely determines d. On the other hand, if $a=1$, then there are ℓ choices for d, and the pair (b,c) must satisfy $bc\equiv -N \pmod{\ell}$. Therefore, there are $\ell^3+(1-(\frac{N}{\ell})^2)\ell^2-\ell$ solutions (a,b,c,d) to (A.2) with $0\le a,b,c,d<\ell$.

We now count the number of quadruples (a,b,c,d) with $0 \le a,b,c,d < \ell$ for which (A.2) holds but (A.3) does not. These are the quadruples that satisfy the system

$$a+d \equiv 1-N \pmod{\ell},$$
$$ad \equiv bc \pmod{\ell}.$$

It is clear that any choice of a uniquely determines d. If $a=0$ or $a=1-N$, then there are $2\ell-1$ choices for the pair (b,c). On the other hand, if $a \neq 0, 1-N$, there are only $\ell-1$ choices for (b,c). Therefore, there are $\ell^2+(\frac{N-1}{\ell})^2\ell$ solutions (a,b,c,d) to (A.2) with $0 \le a,b,c,d < \ell$ for which (A.3) does not hold. ∎

Proposition A.5 *If $\ell \nmid N$, then*

$$\#C_{N,n}(\ell^e) = \ell^{3(e-1)+1}\Big(\ell^2-\ell-1-\Big(\frac{N-1}{\ell}\Big)^2\Big)$$

for every $e \ge 1$.

Proof The case $e=1$ is treated in Lemma A.4, and so we assume that $e \ge 2$. Since any $\sigma \in C_{N,n}(\ell^e)$ must reduce modulo ℓ to a matrix in $C_{N,n}(\ell)$, it suffices to count the number of matrices in $C_{N,n}(\ell^e)$ that reduce to a given matrix in $C_{N,n}(\ell)$. To this end, we assume that $\sigma_0 \in C_{N,n}(\ell)$ and $\sigma \in C_{N,n}(\ell^e)$ is such that $\sigma \equiv \sigma_0 \pmod{\ell}$. Thus, we may write

$$\sigma_0 = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \quad \text{and} \quad \sigma = \begin{pmatrix} a_0+a\ell & b_0+b\ell \\ c_0+c\ell & d_0+d\ell \end{pmatrix}$$

with $0 \le a_0,b_0,c_0,d_0 < \ell$ and $0 \le a,b,c,d < \ell^{e-1}$. Note that the condition $\det\sigma \not\equiv 0 \pmod{\ell}$ is necessarily satisfied since $\det\sigma \equiv \det\sigma_0 \pmod{\ell}$ and $\sigma_0 \in C_{N,n}(\ell)$. Therefore, $\sigma \in C_{N,n}(\ell^e)$ if and only if

$$\text{(A.4)}\quad a_0d_0-b_0c_0+1-a_0-d_0+(a(d_0-1) + d(a_0-1)-b_0c-bc_0)\ell+(ad-bc)\ell^2 \equiv N \pmod{\ell^e}.$$

Since $\sigma_0 \in C_{N,n}(\ell)$, it follows that $a_0d_0-b_0c_0+1-a_0-d_0 = N+k_0\ell$ for some k_0, and hence condition (A.4) reduces to

$$k_0+\big((d_0-1)a-c_0b-b_0c+(a_0-1)d\big)+(ad-bc)\ell \equiv 0 \pmod{\ell^{e-1}}.$$

Since $\ell \nmid N$, σ_0 cannot be the identity matrix modulo ℓ, and the polynomial $(d_0-1)a-c_0b-b_0c+(a_0-1)d$ in the variables a,b,c,d has at least one nonzero coefficient. Say, for example, that d_0-1 is not zero. Then for each triple (b,c,d), there is a unique choice of a satisfying the above congruence. Therefore, there are exactly $\ell^{3(e-1)}$ solutions (a,b,c,d) with $0 \le a,b,c,d < \ell^{e-1}$. ∎

Let $M_2(\mathbb{Z}/\ell^k\mathbb{Z})$ denote the ring of 2×2 matrices with entries from $\mathbb{Z}/\ell^k\mathbb{Z}$. In order to compute $C_{N,n}(\ell^e)$ when $\ell \mid N$ we need to know the number of matrices in $M_2(\mathbb{Z}/\ell^k\mathbb{Z})$ of every individual determinant.

Proposition A.6 *Let M be a positive integer, and let $r = v_\ell(M)$. Then for $r, s \geq 0$, we have*

$$\#\left\{\sigma \in \mathrm{M}_2(\mathbb{Z}/\ell^{r+s}\mathbb{Z}) : \det(\sigma) \equiv M \pmod{\ell^{r+s}}\right\} = \ell^{2(r-1)}\left(\ell^{3s}(\ell+1)(\ell^{r+1}-1) + \delta(s)\right),$$

where $\delta(s)$ is defined by

$$\delta(s) := \begin{cases} 1 & \text{if } s = 0, \\ 0 & \text{otherwise.} \end{cases}$$

For the proof of Proposition A.6, we first make a simple reduction and fix some notation. Given any positive integer M, we write $M = \ell^r M'$ with $r = v_\ell(M)$ and $(M', \ell) = 1$. Since the determinant maps $\mathrm{GL}_2(\mathbb{Z}/\ell^{r+s}\mathbb{Z})$ onto $(\mathbb{Z}/\ell^{r+s}\mathbb{Z})^*$, it follows that there is an $\alpha \in \mathrm{GL}_2(\mathbb{Z}/\ell^{r+s}\mathbb{Z})$ such that $\det(\alpha) \equiv M' \pmod{\ell^{r+s}}$. Since the map $\sigma \mapsto \alpha\sigma$ is a group automorphism of $\mathrm{M}_2(\mathbb{Z}/\ell^{r+s}\mathbb{Z})$ and since $\det(\sigma) = M = \ell^r M'$ if and only if $\det(\alpha^{-1}\sigma) = \ell^r$, it follows that

$$\#\left\{\sigma \in \mathrm{M}_2(\mathbb{Z}/\ell^{r+s}\mathbb{Z}) : \det(\sigma) \equiv M \pmod{\ell^{r+s}}\right\} = \#F(r,s),$$

where

$$F(r,s) := \left\{\sigma \in \mathrm{M}_2(\mathbb{Z}/\ell^{r+s}\mathbb{Z}) : \det(\sigma) \equiv \ell^r \pmod{\ell^{r+s}}\right\}.$$

Thus, we see that $\#\left\{\sigma \in \mathrm{M}_2(\mathbb{Z}/\ell^{r+s}\mathbb{Z}) : \det(\sigma) \equiv M \pmod{\ell^{r+s}}\right\}$ depends on the power of ℓ dividing M and not on the ℓ-free part of M. With this in mind, we define $f(r,s) := \#F(r,s)$ where we adopt the natural convention that $f(0,0) = 1$. Proposition A.6 then follows easily by induction on r using the following lemma.

Lemma A.7 *For every $s \geq 0$, we have*

$$\begin{aligned} f(0,s) &= \ell^{3s-2}(\ell^2-1) + \ell^{-2}\delta(s), \\ f(1,s) &= \ell^{3s}(\ell+1)(\ell^2-1) + \delta(s), \\ f(r,s) &= \ell^{3(r+s-1)}(\ell+1)(\ell^2-1) + \ell^4 f(r-2,s), \quad r \geq 2. \end{aligned}$$

Proof By convention we have $f(0,0) = 1$. For $s \geq 1$,we have the well-known formula

$$f(0,s) = \#\,\mathrm{SL}_2(\mathbb{Z}/\ell^s\mathbb{Z}) = \ell^{3s-2}(\ell^2-1).$$

This proves the first formula given in the statement of the lemma.

Now assume that $r \geq 1$. If $r = 1$ and $s = 0$, then we have

$$f(1,0) = \#\,\mathrm{M}_2(\mathbb{Z}/\ell\mathbb{Z}) - \#\,\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \ell^3 + \ell^2 - \ell.$$

We observe that any $\sigma \in F(r,s)$ must reduce modulo ℓ to some $\sigma_0 \in F(1,0)$. Thus, we assume that $\sigma_0 \in F(1,0)$, and we write

$$\sigma_0 = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \quad \text{and} \quad \sigma = \begin{pmatrix} a_0 + a\ell & b_0 + b\ell \\ c_0 + c\ell & d_0 + d\ell \end{pmatrix},$$

with $0 \leq a_0, b_0, c_0, d_0 < \ell$ and $0 \leq a, b, c, d < \ell^{r+s-1}$. By definition, we see that $\sigma \in F(r,s)$ if and only if

$$a_0 d_0 - b_0 c_0 + (d_0 a - c_0 b - b_0 c + a_0 d)\ell + (ad - bc)\ell^2 \equiv \ell^r \pmod{\ell^{r+s}}.$$

If σ_0 is not the zero matrix modulo ℓ, then there are exactly $\ell^{3(r+s-1)}$ choices of (a,b,c,d) satisfying the above congruence. On the other hand, if σ_0 is the zero matrix (which is always an element of $F(1,0)$), the above congruence condition reduces to

$$(ad-bc)\ell^2 \equiv \ell^r \pmod{\ell^{r+s}}. \tag{A.5}$$

If $r=1$, then there can be no solutions to (A.5) with $s \geq 1$. Therefore,

$$f(1,s) = \ell^{3s}(f(1,0)-1) = \ell^{3s}(\ell^3+\ell^2-\ell-1) = \ell^{3s}(\ell+1)(\ell^2-1)$$

when $s \geq 1$, and this completes the proof of the second formula stated in the lemma. On the other hand, if $r \geq 2$, then condition (A.5) reduces to

$$(ad-bc) \equiv \ell^{r-2} \pmod{\ell^{r-2+s}}.$$

There are $\ell^4 f(r-2,s)$ solutions to this congruence with $0 \leq a,b,c,d < \ell^{r+s-1}$. Whence

$$\begin{aligned} f(r,s) &= \ell^{3(r+s-1)}(f(1,0)-1) + \ell^4 f(r-2,s) \\ &= \ell^{3(r+s-1)}(\ell+1)(\ell^2-1) + \ell^4 f(r-2,s) \end{aligned}$$

for $r \geq 2$, and this completes the proof of the lemma. ∎

Proposition A.8 *If $v = v_\ell(N) \geq 1$ and $\ell \nmid n$, then*

$$\#C_{N,n}(\ell^e) = \ell^{3e-v-2}(\ell+1)\left(\ell^{v+1}-\ell^v-1\right)$$

for every $e > v$.

Proof By Lemma A.4, we have $\#C_{N,n}(\ell) = \ell(\ell^2-2) = \ell^3-2\ell$, and so we may assume that $e \geq 2$. We proceed in a manner similar to the proof of Proposition A.5. In particular, we assume that $\sigma_0 \in C_{N,n}(\ell)$ and count the number of $\sigma \in C_{N,n}(\ell^e)$ that reduce to $C_{N,n}(\ell)$. Writing

$$\sigma_0 = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \quad \text{and} \quad \sigma = \begin{pmatrix} a_0 + a\ell & b_0 + b\ell \\ c_0 + c\ell & d_0 + d\ell \end{pmatrix}$$

with $0 \leq a_0, b_0, c_0, d_0 < \ell$ and $0 \leq a,b,c,d < \ell^{e-1}$, we deduce that the quadruple (a,b,c,d) must satisfy (A.4). As in the proof of Proposition A.5, if σ_0 is not the identity matrix, there are exactly $\ell^{3(e-1)}$ choices for (a,b,c,d).

Now suppose that σ_0 is the identity matrix. (Note that the identity matrix is always an element of $C_{N,n}(\ell)$ when $\ell \mid N$.) Then writing $N = \ell^v N'$ with $v = v_\ell(N) \geq 1$ and $(N',\ell)=1$, we see that condition (A.4) reduces to

$$(ad-bc)\ell^2 \equiv N'\ell^v \pmod{\ell^e}. \tag{A.6}$$

Clearly there are no solutions to this congruence unless $v \geq 2$. Therefore, if $v=1$ and $e \geq 2$, we have that $\#C_{N,n}(\ell^e) = \ell^{3(e-1)}(\ell^3-2\ell-1) = \ell^{3e-3}(\ell+1)(\ell^2-\ell-1)$. Now suppose that $v \geq 2$ and $e \geq 3$. Then (A.6) reduces to $(ad-bc) \equiv N'\ell^{v-2} \pmod{\ell^{e-2}}$. The number of solutions to this congruence with $0 \leq a,b,c,d < \ell^{e-1}$ is equal to

$$\ell^4 \#\left\{\alpha \in \mathrm{M}_2(\mathbb{Z}/\ell^{e-2}\mathbb{Z}) : \det(\alpha) \equiv N'\ell^{v-2} \pmod{\ell^{e-2}}\right\}.$$

Since we are assuming that $v < e$, Proposition A.6 implies that the above count is equal to $\ell^4\ell^{2(v-3)}\ell^{3(e-v)}(\ell+1)(\ell^{v-1}-1) = \ell^{3e-v-2}(\ell+1)(\ell^{v-1}-1)$. Putting everything together, we find that

$$\begin{aligned}\#C_{N,n}(\ell^e) &= \ell^{3(e-1)}(\ell^3-2\ell-1)+\ell^{3e-v-2}(\ell+1)(\ell^{v-1}-1)\\ &= \ell^{3e-v-2}(\ell+1)(\ell^{v+1}-\ell^v-1)\end{aligned}$$

for $v \geq 2$. ∎

Recall our standing assumption that $n^2 \mid N$.

Theorem A.9 *Let $u = v_\ell(n)$ and $v = v_\ell(N)$. Then for every $e > v$, we have*

$$\#C_{N,n}(\ell^e) = \begin{cases} \ell^{3(e-1)+1}\left(\ell^2-\ell-1-\left(\frac{N-1}{\ell}\right)^2\right) & \text{if } u = 0 \text{ and } v = 0,\\ \ell^{3e-v-2}(\ell+1)(\ell^{v+1}-\ell^v-1) & \text{if } u = 0 \text{ and } v \geq 1,\\ \ell^{3e-v-2}(\ell+1)(\ell^{v-2u+1}-1) & \text{if } 1 \leq u \leq v/2,\\ 0 & \text{if } 0 \leq v/2 < u.\end{cases}$$

Therefore, for every $e > v$, we have

$$\frac{\ell^e\#C_{N,n}(\ell^e)}{\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z})} = \begin{cases} \left(1-\frac{\left(\frac{N-1}{\ell}\right)^2\ell+1}{(\ell-1)^2(\ell+1)}\right) & \text{if } u = 0 \text{ and } v = 0,\\ \frac{\ell}{\ell-1}\left(1-\frac{1}{\ell^v(\ell-1)}\right) & \text{if } u = 0 \text{ and } v \geq 1,\\ \frac{\ell}{\ell^{2u}(\ell-1)}\left(\frac{\ell^{v+1}-\ell^{2u}}{\ell^{v+1}-\ell^v-1}\right)\left(1-\frac{1}{\ell^v(\ell-1)}\right) & \text{if } 1 \leq u \leq v/2,\\ 0 & \text{if } 0 \leq v/2 < u.\end{cases}$$

Proof Note that the second assertion of the theorem follows from the first together with the well known formula $\#\,\mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z}) = \ell^{4(e-1)+1}(\ell+1)(\ell-1)^2$, and so it suffices to prove the first assertion of Theorem A.9.

The first two cases have already been addressed by Propositions A.5 and A.8. Therefore, we may assume that $u \geq 1$. Supposing that $\sigma \in C_{N,n}(\ell^e)$, we may write

$$\sigma = \begin{pmatrix} 1+a\ell^u & b\ell^u \\ c\ell^u & 1+d\ell^u \end{pmatrix}$$

with $0 \leq a, b, c, d < \ell^{e-u}$ chosen such that $(ad-bc)\ell^{2u} \equiv N'\ell^v \pmod{\ell^e}$. This congruence clearly has no solutions if $e > v$ and $2u > v$. Therefore, we may assume that $2 \leq 2u \leq v < e$. In this case the above congruence is equivalent to the condition $(ad-bc) \equiv N'\ell^{v-2u} \pmod{\ell^{e-2u}}$ for $0 \leq a, b, c, d < \ell^{e-u}$. Applying Proposition A.6 with $r = v-2u$ and $s = e-v > 0$, we find that

$$\begin{aligned}\#C_{N,n}(\ell^e) &= \ell^{4u}\ell^{2(v-2u-1)}\ell^{3(e-v)}(\ell+1)(\ell^{v-2u+1}-1)\\ &= \ell^{3e-v-2}(\ell+1)(\ell^{v-2u+1}-1).\end{aligned}$$

∎

We are now ready to give the proofs of Theorems A.1 and A.3.

Proof of Theorems A.1 and A.3 Theorem A.1 follows easily from (1.2) and the cases of Theorem A.9 with $v_\ell(n) = u = 0$. For the proof of Theorem A.3, we let $N = m^2k =$

$|G|$, and for each prime ℓ, we put

$$v_\ell(N,n) := \frac{\ell^e \# C_{N,n}(\ell^e)}{\# \mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z})}$$

with $e = e_\ell > v_\ell(N)$. We then compute the absolutely convergent infinite product

$$\prod_\ell \big(v_\ell(N,m) - v_\ell(N,\ell m) \big)$$

in two different ways. On the one hand, by definition of the $v_\ell(N,n)$ the above expression is equal to

$$\prod_\ell \Big(\frac{\ell^e \cdot (\# C_{N,m}(\ell^e) - \# C_{N,\ell m}(\ell^e))}{\# \mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z})} \Big),$$

where $C_{N,n}(\ell^e)$ is defined in equation (A.1). On the other hand, by comparing (1.1) and Lemma 3.1 with Theorem A.9, we see that it is equal to $K(G)\frac{|G|}{|\operatorname{Aut}(G)|}$. ∎

Acknowledgements The work of authors David and Koukoulopoulos was partially supported by the Natural Sciences and Engineering Research Council of Canada. Finally, part of this work was completed while Chandee, Koukoulopoulos, and Smith were postdoctoral fellows at the Centre de recherches mathématiques at Montréal, which they would like to thank for the financial support and the pleasant working environment.

References

[BPS12] W. D. Banks, F. Pappalardi, and I. E. Shparlinski, *On group structures realized by elliptic curves over arbitrary finite fields.* Exp. Math. **21** (2012) no. 1, 11–25. http://dx.doi.org/10.1080/10586458.2011.606075

[BV07] J. Buchmann and U. Vollmer, *Binary quadratic forms. An algorithmic approach.* Algorithms and Computation in Mathematics, 20. Springer, Berlin, 2007.

[CDKS] V. Chandee, C. David, D. Koukoulopoulos, and E. Smith, *Group structures of elliptic curves over finite fields.* Int. Math. Res. Not. **2014**, no. 19, 5230–5248.

[DS13] C. David and E. Smith, *Elliptic curves with a given number of points over finite fields.* Compos. Math. **149**(2013), no. 2, 175–203. http://dx.doi.org/10.1112/S0010437X12000541

[DS14a] ———, *Corrigendum to: Elliptic curves with a given number of points over finite fields.* Compos. Math. **150**(2014), no. 8, 1347–1348. http://dx.doi.org/10.1112/S0010437X14007283

[DS14b] ———, *A Cohen-Lenstra phenomenon for elliptic curves.* J. London Math. Soc. **89**(2014), no. 1, 24–44. http://dx.doi.org/10.1112/jlms/jdt036

[DS14c] ———, *Corrigendum to: A Cohen-Lenstra phenomenon for elliptic curves.* J. London Math. Soc. **89**(2014), no. 1, 45–46. http://dx.doi.org/10.1112/jlms/jdu001

[Deu41] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem. Hansischen Univ. **14**(1941), 197–272, http://dx.doi.org/10.1007/BF02940746

[FI78] J. Friedlander and H. Iwaniec, *On Bombieri's asymptotic sieve.* Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **5**(1978) no. 4, 719–756.

[GS03] A. Granville and K. Soundararajan, *The distribution of values of* $L(1,\chi_d)$. Geom. Funct. Anal. **13**(2003), no. 5, 992–1028. http://dx.doi.org/10.1007/s00039-003-0438-3

[HR74] H. Halberstam and H.-E. Richert, *Sieve methods*. London Mathematical Society Monographs, No. 4. Academic Press, London-New York, 1974.

[Kob88] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field.* Pacific J. Math. **131**(1988), no. 1, 157–165. http://dx.doi.org/10.2140/pjm.1988.131.157

[Kou14] D. Koukoulopoulos, *Prime numbers in short arithmetic progressions.* 2014. arXiv:1405.6592.

[LT76] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*. Lecture Notes in Mathematics 504. Springer-Verlag, Berlin, 1976.

[Sch87] R. Schoof, *Nonsingular plane cubic curves over finite fields*. J. Combin. Theory Ser. A **46**(1987), no. 2, 183–211. http://dx.doi.org/10.1016/0097-3165(87)90003-3

[Ste94] S. A. Stepanov, *Arithmetic of algebraic curves*. Monographs in Contemporary Mathematics. Consultants Bureau, New York, 1994. Translated from the Russian by Irene Aleksanova.

Department of Mathematics, Burapha University, 169 Long-hard Bangsaen rd, Saen suk, Mueang, Chonburi, 20131 Thailand
e-mail: vorrapan@buu.ac.th

Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve West, Montréal, QC, H3G 1M8, Canada
e-mail: cdavid@mathstat.concordia.ca

Département de mathématiques et de statistique, Université de Montréal, CP 6128 succ. Centre-Ville, Montréal, QC H3C 3J7, Canada
e-mail: koukoulo@dms.umontreal.ca

Department of Mathematics, Liberty University, 1971 University Blvd, MSC Box 710052, Lynchburg, VA 24502,, USA
e-mail: ecsmith13@liberty.edu