Journal of the London Mathematical Society Advance Access published September 5, 2013

J. London Math. Soc. Page 1 of 21
doi:10.1112/jlms/jdt036

A Cohen–Lenstra phenomenon for elliptic curves

Chantal David and Ethan Smith

Abstract

Given an elliptic curve E and a finite Abelian group G, we consider the problem of counting the number of primes p for which the group of points modulo p is isomorphic to G. Under a certain conjecture concerning the distribution of primes in short intervals, we obtain an asymptotic formula for this problem on average over a family of elliptic curves.

1. *Introduction*

Let E be an elliptic curve defined over the rational field $\mathbb{Q}$. Given a prime p where E has good reduction, we consider the reduced curve, which we denote by E_p. In previous work [**13**], we studied the arithmetic function

$$M_E(N) := \#\{p : \#E_p(\mathbb{F}_p) = N\},$$

where $\#E_p(\mathbb{F}_p)$ denotes the number of $\mathbb{F}_p$-rational points on the reduction. Despite being such a natural object to study, it seems that the recent paper of Kowalski [**21**] is the first to introduce the function $M_E(N)$ and ask interesting questions about its behavior. Kowalski's motivation for studying $M_E(N)$ stems from its relation with what he calls 'elliptic twins'. A prime p is called an E-twin prime if there exists a prime $q \neq p$ such that $\#E_p(\mathbb{F}_p) = \#E_p(\mathbb{F}_q)$. Then p is an E-twin prime if and only if $M_E(\#E_p(\mathbb{F}_p)) > 1$.

The Hasse bound states that $\#E_p(\mathbb{F}_p)$ is never very far from $p+1$. In particular, $|p+1-\#E_p(\mathbb{F}_p)| < 2\sqrt{p}$. It follows that if $\#E_p(\mathbb{F}_p) = N$, then

$$N^- := (\sqrt{N}-1)^2 < p < (\sqrt{N}+1)^2 =: N^+. \tag{1}$$

Hence, $M_E(N)$ is a finite number, satisfying the trivial bound $M_E(N) \ll \sqrt{N}/\log(N+1)$. In [**21**], the author shows that if E possesses complex multiplication, then $M_E(N) \ll_{E,\varepsilon} N^\varepsilon$ for any $\varepsilon > 0$, and asks whether the same might be true for general elliptic curves, but up to now, no bound better than the trivial bound is known for curves without complex multiplication.

In [**13**], we studied the average behavior of $M_E(N)$ taken over a family of elliptic curves. More precisely, given integers a, b, we let $E_{a,b}$ denote the elliptic curve given by the Weierstrass equation $y^2 = x^3 + ax + b$; we let $\mathscr{C}$ denote the multiset defined by

$$\mathscr{C} = \mathscr{C}(A,B) := \{E_{a,b} : |a| \leqslant A, |b| \leqslant B, \Delta(E_{a,b}) \neq 0\}.$$

Under a suitable conjecture (specifically Conjecture 17 with any $\eta < \frac{1}{2}$), we showed that there exists an absolutely bounded function $K(N)$ (see equation (20)) such that if A, B are large enough with respect to N, then

$$\frac{1}{\#\mathscr{C}} \sum_{E \in \mathscr{C}} M_E(N) \sim K(N) \frac{N}{\varphi(N)\log N} \tag{2}$$

as $N \to \infty$.

Received 13 June 2012; revised 22 March 2013.

2010 *Mathematics Subject Classification* 11G05 (primary), 11N13 (secondary).

The first author was supported by the Natural Sciences and Engineering Research Council of Canada [Discovery Grant 155635-2008] and the Fonds de recherche du Québec - Nature et technologies [Octroi 166534].

Apart from the 'arithmetic factor' $K(N)N/\varphi(N)$, the above result agrees with a naïve probabilistic model for $M_E(N)$ where one supposes that the values $\#E_p(\mathbb{F}_p)$ are uniformly distributed in the interval (N^-, N^+). This is explained in detail in [**13**]. The occurrence of the weight $\varphi(N)$ appearing in the denominator on the right-hand side of (2) suggested to the authors that perhaps this is another example of phenomena which are governed by the Cohen–Lenstra Heuristics [**7**, **8**], which predict that random groups occur with probability inversely proportional to the size of their automorphism groups. The purpose of this paper is to explore this connection further by studying the function

$$M_E(G) := \#\{p : E_p(\mathbb{F}_p) \cong G\},$$

where G is a finite Abelian group. Given an elliptic curve E, it is well known that

$$E_p(\mathbb{F}_p) \cong \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$$

for some positive integers N_1, N_2 satisfying the Hasse bound $|p + 1 - N_1^2N_2| < 2\sqrt{p}$. For much of this work, we will restrict to the case when N_1 and N_2 are both odd as this reduces the number of special cases to consider.

As with our study of $M_E(N)$ in [**13**], the restriction imposed by the Hasse bound means that any prime counted by $M_E(G)$ must lie in a very short interval near $N = \#G = N_1^2N_2$. In particular, all of the primes are of size N, lying in an interval of length $4\sqrt{N}$. Even the Riemann Hypothesis does not guarantee the existence of a prime in such a short interval. Thus, our work here, as in [**13**], requires a conjecture (Conjecture 17) concerning the distribution of primes of size X in intervals of length X^η. The case $\eta = 1$ corresponds to the classical Barban–Davenport–Halberstam Theorem. The precise statement of this conjecture can be found in Section 6.

Recall that the *exponent* of a finite Abelian group is the size of its largest cyclic subgroup. In particular, for groups of the form $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$, the exponent of G is given by $\exp(G) = N_1N_2$. The following is our main result.

THEOREM 1. *Assume that Conjecture* 17 *holds for some $\eta < \frac{1}{2}$. Let $\alpha, \beta > 0$ and be fixed. Then there exists a non-zero and absolutely bounded function $K(G)$ such that for every non-trivial, odd order group $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$, we have*

$$\frac{1}{\#\mathscr{C}} \sum_{E \in \mathscr{C}} M_E(G) = \left(K(G) + O\left(\frac{1}{(\log \#G)^\beta}\right)\right) \frac{\#G}{\#\mathrm{Aut}(G)\log(\#G)}$$

as $\#G \to \infty$, provided that $A, B \geqslant (\#G)^{1/2}(\log \#G)^{\beta+1}$, $AB \geqslant (\#G)^{3/2}(\log \#G)^{\beta+2}$, and the exponent of G satisfies $\#G/(\log \#G)^\alpha \leqslant \exp(G) \leqslant \#G$. Furthermore, the function $K(G)$ is given as a product over primes ℓ by

$$K(G) := \prod_{\ell \nmid N}\left(1 - \frac{((N-1)/\ell)^2\ell + 1}{(\ell-1)^2(\ell+1)}\right) \prod_{\ell \mid N}\left(1 - \frac{1}{\ell(\ell-1)}\right)$$
$$\times \prod_{\ell \mid N_1}\left(1 + \frac{1}{\ell(\ell^2 - \ell - 1)}\right) \prod_{\substack{\ell \mid N_1 \\ \ell \nmid N_2}}\left(1 + \frac{(-N_2/\ell)}{\ell(\ell-1)}\right), \tag{3}$$

where $N = \#G = N_1^2N_2$ and $\left(\frac{\cdot}{\ell}\right)$ is the usual Kronecker symbol.

Many results similar to Theorem 1 may be equivalently (and perhaps more naturally) stated as results about counting isomorphism classes of elliptic curves over finite fields which possess some desired property. In this case, the desired property is having a group of $\mathbb{F}_p$-points isomorphic to G. We now restate Theorem 1 in such an equivalent form.

Let $M_p(G)$ denote the weighted number of isomorphism classes of elliptic curves defined over $\mathbb{F}_p$ with group isomorphic to G. That is,

$$M_p(G) := \sum_{\substack{E/\mathbb{F}_p \\ E(\mathbb{F}_p)\cong G}} \frac{1}{\#\mathrm{Aut}(E)}, \tag{4}$$

where the sum is taken over all isomorphism classes of elliptic curves E defined over $\mathbb{F}_p$ and $\#\mathrm{Aut}(E)$ is the number of automorphisms of E as a curve over $\mathbb{F}_p$. It is important to distinguish between the similar notation $\mathrm{Aut}(E)$ and $\mathrm{Aut}(E(\mathbb{F}_p))$. The former refers to the $\mathbb{F}_p$-automorphisms of E as a curve, while the latter refers to the automorphisms of $E(\mathbb{F}_p)$ as a group. Now let

$$M(G) := \sum_p M_p(G).$$

With this notation, Theorem 1 is equivalent to the following estimate for $M(G)$, the weighted number of isomorphism classes of elliptic curves defined over any prime finite field with group of points isomorphic to G.

THEOREM 2. *Assume that Conjecture* 17 *holds for some* $\eta < \frac{1}{2}$. *Let* $\alpha, \beta > 0$ *and be fixed. Then for every non-trivial, odd order group* $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$, *we have*

$$M(G) = \left(K(G) + O\left(\frac{1}{(\log \#G)^{\beta}}\right)\right) \frac{(\#G)^2}{\#\mathrm{Aut}(G)\log(\#G)}$$

as $\#G \to \infty$, *provided that the exponent of* G *satisfies* $\#G/(\log \#G)^{\alpha} \leqslant \exp(G) \leqslant \#G$.

REMARK 3. The proofs of Theorems 1 and 2 do not really require that Conjecture 17 holds for a fixed $\eta < \frac{1}{2}$. It is sufficient that it holds for intervals of length $Y = \sqrt{X}/(\log X)^{\beta+1}$.

The restriction that $\#G/(\log \#G)^{\alpha} \leqslant \exp(G) \leqslant \#G$ may seem a bit severe. We believe that our results should hold in the range $(\#G)^{1/2+\epsilon} \leqslant \exp(G) \leqslant \#G$ for any fixed $\epsilon > 0$. Proving this would require that we assume a conjecture similar to Conjecture 17 for primes in short intervals *and* in a fixed arithmetic progression. Unconditionally, it is possible to obtain upper bounds of the correct order of magnitude in this larger range. This is the subject of a forthcoming paper with Chandee and Koukoulopoulos in which we show

$$M(G) \ll \frac{(\#G)^2}{\#\mathrm{Aut}(G)\log(\#G)},$$

or equivalently,

$$\frac{1}{\#\mathscr{C}} \sum_{E\in\mathscr{C}} M_E(G) \ll \frac{\#G}{\#\mathrm{Aut}(G)\log(\#G)},$$

both holding for $(\#G)^{1/2+\epsilon} \leqslant \exp(G) \leqslant \#G$. However, lower bounds are impossible without hypothesis.

One should not expect our results to hold without some restriction on the size of the exponent. In particular, not all groups of the form $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$ occur as the group of points on an elliptic curve over a finite field. For example, the authors of [**2**] have noted that the group $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ never occurs. This is perhaps surprising at first since given a positive integer N and a prime p in the range (1), a theorem of Deuring [**14**] ensures that there is always an elliptic curve $E/\mathbb{F}_p$ possessing N points. Given a positive integer N, we believe that there should always be a prime close enough, but as we noted earlier, this is not provable even under the Riemann Hypothesis. A refinement of the Deuring result (see Theorem 5) implies that given an order N group $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$ and a prime $p \equiv 1 \pmod{N_1}$

in the range (1), there is always an elliptic curve with $E(\mathbb{F}_p) \cong G$. However, in the extreme case when $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1\mathbb{Z}$, we are looking for a prime $p \equiv 1 \pmod{N_1}$ in the interval $(N_1^2 - 2N_1 + 1, N_1^2 + 2N_1 + 1)$, and we should not expect this to happen very often as this interval contains exactly *three* integers congruent to 1 modulo N_1. In fact, letting N_1 and N_2 vary, it would seem very unlikely (though not impossible) to find an elliptic curve $E/\mathbb{F}_p$ with $E(\mathbb{F}_p) \cong \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$ unless N_1 grows slower than an arbitrarily large (but fixed) power of N_2. Note that this condition is equivalent to assuming $\sqrt{N}/N_1 \geqslant N^\epsilon$, which is equivalent to assuming $(\#G)^{1/2+\epsilon} \leqslant \exp(G)$.

The remainder of the article is organized as follows. We show in Section 2 how the proof of Theorem 1 is reduced to proving Theorem 2, and in turn, how the proof of Theorem 2 is reduced to the computation of a certain average of class numbers. The computation of this average of class numbers occupies Section 3 (see Theorem 10) and Section 4 (see Proposition 12). In Section 5, we gather together all of our intermediate results to complete the proof of Theorem 2. Section 6 contains the precise statement of Conjecture 17 as well as the proofs of a couple of auxiliary lemmas which are used in Section 3. Finally, in Section 7 we close with some concluding remarks concerning the arithmetic factors $K(G)$ and $K(N)$, which are defined by (3) and (20), respectively.

2. *Reduction to an average of class numbers*

In this section, we show how the proof of Theorem 1 is reduced to proving Theorem 2. We then show how the proof of Theorem 2 is reduced to computing a certain average of class numbers.

Proof that Theorem 2 *implies Theorem* 1. For notational convenience, we let $N = \#G$. The Hasse bound implies that any prime p counted by $M_E(G)$ must fall in the range (1). Hence, interchanging the order of summation yields

$$\frac{1}{\#\mathscr{C}} \sum_{E \in \mathscr{C}} M_E(G) = \frac{1}{\#\mathscr{C}} \sum_{N^- < p < N^+} \#\{E \in \mathscr{C} : E_p(\mathbb{F}_p) \cong G\}. \tag{5}$$

To estimate the above, we group the E in $\mathscr{C}$ according to which $\mathbb{F}_p$-isomorphism class they reduce modulo p. That is, we write

$$\#\{E \in \mathscr{C} : E_p(\mathbb{F}_p) \cong G\} = \sum_{\substack{\tilde{E}/\mathbb{F}_p \\ \tilde{E}(\mathbb{F}_p) \cong G}} \#\{E \in \mathscr{C} : E_p(\mathbb{F}_p) \simeq_p \tilde{E}\}, \tag{6}$$

where the sum is over the $\mathbb{F}_p$-isomorphism classes of elliptic curves $\tilde{E}$ whose group of $\mathbb{F}_p$-points is isomorphic to G. We may assume $N \geqslant 8$ so that $N^- = (\sqrt{N} - 1)^2 > 3$ and only primes greater than 3 enter into the sum over p above. Therefore, we may choose a model for each $\tilde{E}$ of the form $y^2 = x^3 + \alpha x + \beta$, and a character sum argument as in [**15**, pp. 93–96] yields the estimate

$$\begin{aligned} \#\{E \in \mathscr{C} : E_p(\mathbb{F}_p) \cong \tilde{E}\} &= \frac{4AB}{\#\mathrm{Aut}(\tilde{E})N} + O\left(\frac{AB}{N^2} + \sqrt{N}(\log N)^2\right) \\ &\quad + \begin{cases} O\left(\dfrac{A\log N}{\sqrt{N}} + \dfrac{B\log N}{\sqrt{N}}\right) & \text{if } \alpha\beta \neq 0, \\ O\left(\dfrac{A\log N}{\sqrt{N}} + B\log N\right) & \text{if } \alpha = 0, \\ O\left(A\log N + \dfrac{B\log N}{\sqrt{N}}\right) & \text{if } \beta = 0, \end{cases} \end{aligned} \tag{7}$$

for $N^- < p < N^+$.

We now recall the definition of $M_p(G)$ as given by (4). Then equations (5)–(7) imply

$$\frac{1}{\#\mathscr{C}}\sum_{E\in\mathscr{C}} M_E(G) = \left[\frac{1}{N} + O\left(\frac{1}{N^2} + \frac{\log N}{\sqrt{N}}\left(\frac{1}{A}+\frac{1}{B}\right) + \frac{\sqrt{N}(\log N)^2}{AB}\right)\right]\sum_{N^-<p<N^+} M_p(G)$$
$$+ O\left(\left(\frac{1}{A}+\frac{1}{B}\right)\log N \sum_{N^-<p<N^+} 1\right),$$

since $\#\mathscr{C} = 4AB + O(A+B)$ and there are at most ten isomorphism classes of elliptic curves $\tilde{E}/\mathbb{F}_p$ with $\alpha\beta = 0$. Recalling that $M(G) = \sum_p M_p(G)$ and $\#\{N^- < p < N^+\} \ll \sqrt{N}/\log N$, we see that Theorem 1 follows from Theorem 2 provided that $A, B \geqslant \sqrt{N}(\log N)^{\beta+1}$ and $AB \geqslant N^{3/2}(\log N)^{\beta+2}$. □

Now let N and m be positive integers with m^2 dividing N, and define

$$M_p(N;m) := \sum_{\substack{E/\mathbb{F}_p \\ \#E(\mathbb{F}_p)=N \\ E(\mathbb{F}_p)[m]\cong\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}}} \frac{1}{\#\mathrm{Aut}(E)},$$

the weighted number of isomorphism classes of elliptic curves defined over $\mathbb{F}_p$ which have exactly N points over $\mathbb{F}_p$ and whose $\mathbb{F}_p$-rational m-torsion subgroup is isomorphic to $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. We also define

$$M(N;m) := \sum_p M_p(N;m),$$

the weighted number of isomorphism classes of elliptic curves defined over any prime finite field which have exactly N points over $\mathbb{F}_p$ and whose $\mathbb{F}_p$-rational m-torsion subgroup is isomorphic to $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. The following lemma, which follows by the principle of inclusion-exclusion, reduces the task of estimating $M(G)$ to that of estimating $M(N;m)$.

Lemma 4. *Let $G = \mathbb{Z}/N_1\mathbb{Z}\times\mathbb{Z}/N_1N_2\mathbb{Z}$. Then*

$$M(G) = \sum_{k^2|N_2} \mu(k) M(N_1^2N_2; kN_1),$$

where $\mu(k)$ denotes the usual Möbius function.

We now explain how computing $M(N;m)$ is equivalent to computing a certain average of class numbers. Given a negative discriminant d, we let $h(d)$ denote the class number of the unique imaginary quadratic order of discriminant d, and we let $w(d)$ denote the cardinality of its unit group. The *Kronecker class number* of discriminant D is defined by

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

Given a positive integer N and a prime p, we define the 'discriminant polynomial' $D_N(p)$ by

$$D_N(p) := (p+1-N)^2 - 4p. \tag{8}$$

Adapting the proofs in [27, Lemma 4.8 and Theorem 4.9] to count isomorphism classes of elliptic curves weighted by the size of their automorphism groups, we obtain the following.

THEOREM 5. *Let p be a prime, N be a positive integer such that $|p+1-N| < 2\sqrt{p}$, and m be a positive integer such that $m^2 \mid N$. Then the weighted number of $\mathbb{F}_p$-isomorphism classes of elliptic curves having exactly N points and $E(\mathbb{F}_p)[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is given by*

$$M_p(N;m) = \begin{cases} H\left(\frac{D_N(p)}{m^2}\right) & \text{if } m \mid p-1 \text{ and } m^2 \mid N, \\ 0 & \text{otherwise.} \end{cases}$$

REMARK 6. It is easy to check that the conditions $m \mid p-1$ and $m^2 \mid N$ imply $m^2 \mid D_N(p)$ in the above theorem.

REMARK 7. The corresponding results in [27] are more general as Schoof does not restrict to finite fields of prime order.

As an immediate corollary, we have the following.

COROLLARY 8. *Let N and m be positive integers with m^2 dividing N. Then*

$$M(N;m) = \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \ (\mathrm{mod}\, m)}} H\left(\frac{D_N(p)}{m^2}\right).$$

3. *Conditional estimates for the average of class numbers*

The following lemma will be useful for bounding various sums that appear in this section. We postpone its proof until Section 6.

LEMMA 9. *Suppose that N, u, and v are positive integers with $u^2 \mid N$. Let $D_N(p)$ be as defined by equation (8). If $(X, X+Y] \subseteq (N^-, N^+)$, then uniformly for $uv < Y$,*

$$\#\left\{ X < p \leqslant X+Y : \begin{array}{l} p \equiv 1 \ (\mathrm{mod}\, u) \\ D_N(p) \equiv 0 \ (\mathrm{mod}\, u^2 v) \\ (p,v) = 1 \end{array} \right\} \ll \frac{\sqrt{v}}{\varphi(uv)} \frac{Y}{\log(Y/uv)}.$$

The main result of this section is the following conditional (under Conjecture 17) estimate for $M(N;m)$, the weighted number of isomorphism classes of elliptic curves E defined over any prime finite field which have exactly N points over $\mathbb{F}_p$ and such that $E(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

THEOREM 10. *Let $\alpha, \beta > 0$ be fixed, and assume that Conjecture 17 holds for $\eta < \frac{1}{2}$. Then there exists a function $K_0(N,m)$ such that for every pair of odd positive integers N and m with $m^2 \mid N$,*

$$M(N;m) = \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \ (\mathrm{mod}\, m)}} H\left(\frac{D_N(p)}{m^2}\right) = K_0(N,m)\frac{N}{\log N} + O\left(\frac{N}{\varphi(m^2)(\log N)^{\beta+1}}\right),$$

provided that $m \leqslant (\log N)^\alpha$. Furthermore, the function $K_0(N,m)$ is given by the absolutely convergent sum

$$K_0(N,m) := \sum_{\substack{f=1\\ m\mid f\\ (f,2)=1}}^{\infty} \frac{1}{f} \sum_{n=1}^{\infty} \frac{1}{n\varphi(4nf^2)} \sum_{\substack{a=1\\ a\equiv 1 \pmod 4}}^{4n} \left(\frac{a}{n}\right) \#C_N(a,n,f), \tag{9}$$

where

$$C_N(a,n,f) := \{b \in (\mathbb{Z}/4nf^2\mathbb{Z})^\times : D_N(b) \equiv af^2 \pmod{4nf^2}\}. \tag{10}$$

Proof. We begin by using the definition of the Kronecker class number and the class number formula to write

$$\sum_{\substack{N^-<p<N^+\\ p\equiv 1 \pmod m}} H\left(\frac{D_N(p)}{m^2}\right) = \frac{1}{2\pi} \sum_{\substack{N^-<p<N^+\\ p\equiv 1 \pmod m}} \sum_{\substack{f^2\mid D_N(p)/m^2\\ d_{N,fm}(p)\equiv 0,1 \pmod 4}} \frac{\sqrt{|D_N(p)|}}{fm} L\left(1, \chi_{d_{N,fm}(p)}\right),$$

where $\chi_d := (d/\cdot)$ is the Kronecker symbol associated to the discriminant d,

$$L(1,\chi_d) = \sum_{n\geqslant 1} \frac{\chi_d(n)}{n},$$

and we write $d_{N,f}(p) := D_N(p)/f^2$ whenever $f^2 \mid D_N(p)$. We may assume $N > 5$. As a result, the prime 2 does not enter into the sum over p above. Since N is odd, we have $D_N(p) = (p+1-N)^2 - 4p \equiv 1 \pmod 4$, and hence it follows that each f above is odd and $d_{N,fm}(p) \equiv 1 \pmod 4$. Therefore, we may omit the congruence condition under the sum over f above. Furthermore, if $p \mid f$ and $f^2 \mid D_N(p)$, then it follows that $p = 2$, but this is contrary to our assumption that $N > 5$. Since -3 is the largest discriminant possible for an imaginary quadratic order, we have $d_{N,fm}(p) \leqslant -3$, and it follows that if $(fm)^2 \mid D_N(p)$, then $fm \leqslant 2\sqrt{N/3}$. Therefore, after rearranging the order of summation, we have

$$\sum_{\substack{N^-<p<N^+\\ p\equiv 1 \pmod m}} H\left(\frac{D_N(p)}{m^2}\right) = \frac{1}{2\pi} \sum_{\substack{f\leqslant (2/m)\sqrt{N/3}\\ (f,2)=1}} \frac{1}{fm} \sum_{\substack{N^-<p<N^+\\ p\equiv 1 \pmod m\\ (fm)^2\mid D_N(p)\\ p\nmid f}} \sqrt{|D_N(p)|} L(1, \chi_{d_{N,fm}(p)}). \tag{11}$$

Let V be a positive parameter to be chosen. Using Lemma 9 (with $u = m$ and $v = f$), we see that the contribution made to the above by the values of f which are larger than V is bounded (up to a constant) by

$$\sqrt{N} \sum_{\substack{V<f\leqslant (2/m)\sqrt{N/3}\\ (f,2)=1}} \frac{\log(4N/(fm)^2)}{fm} \sum_{\substack{N^-<p<N^+\\ p\equiv 1 \pmod m\\ fm^2\mid D_N(p)\\ p\nmid f}} 1 \ll N \sum_{f>V} \frac{1}{\sqrt{f}\varphi(fm^2)} \ll \frac{N}{\varphi(m^2)\sqrt{V}}.$$

Choosing $V = (\log N)^{2(\beta+1)}$, we have

$$\sum_{\substack{N^-<p<N^+\\ p\equiv 1 \pmod m}} H\left(\frac{D_N(p)}{m^2}\right) = \frac{1}{2\pi} \sum_{\substack{f\leqslant V\\ (f,2)=1}} \frac{1}{fm} \sum_{\substack{N^-<p<N^+\\ p\equiv 1 \pmod m\\ (fm)^2\mid D_N(p)\\ p\nmid f}} \sqrt{|D_N(p)|} L(1, \chi_{d_{N,fm}(p)}) + O\left(\frac{N}{\varphi(m^2)(\log N)^{\beta+1}}\right). \tag{12}$$

If $U > 0$ and d is a discriminant, then Burgess' bound for character sums [**5**, Theorem 2] and partial summation imply

$$L(1,\chi_d) = \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n} = \sum_{n \leqslant U} \frac{\chi_d(n)}{n} + O\left(\frac{|d|^{7/32}}{\sqrt{U}}\right).$$

Thus, if we truncate the L-series in (12) at U and use the Brun–Titchmarsh inequality [**17**, p. 167], then we see that the contribution made by the tail of the L-series is bounded (up to a constant) by

$$\frac{N^{23/32}}{\sqrt{U}} \sum_{f \leqslant V} \frac{1}{(fm)^{1+7/16}} \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod{m}}} 1 \ll \frac{N^{39/32}}{\varphi(m^2) m^{7/16} \log(4\sqrt{N}/m)},$$

uniformly for $m \leqslant \sqrt{N}$. Choosing $U = N^{7/16}(\log N)^{2\beta}$, we have

$$\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod{m}}} H\left(\frac{D_N(p)}{m^2}\right) = \frac{1}{2\pi} \sum_{\substack{f \leqslant V \\ (f,2)=1}} \frac{1}{fm} \sum_{n \leqslant U} \frac{1}{n} \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod{m} \\ (fm)^2 \mid D_N(p) \\ p \nmid f}} \left(\frac{d_{N,fm}(p)}{n}\right) \sqrt{|D_N(p)|}$$
$$+ O\left(\frac{N}{\varphi(m^2)(\log N)^{\beta+1}}\right). \tag{13}$$

At this point, it is convenient to break the interval (N^-, N^+) into subintervals of length $Y = \sqrt{N}/\lfloor (\log N)^{\gamma} \rfloor$, where γ is some fixed positive parameter to be chosen. For each integer $k \in I := [-2\sqrt{N}/Y, 2\sqrt{N}/Y) \cap \mathbb{Z}$, we write $X = X_k := N + 1 + kY$ so that

$$\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod{m} \\ (fm)^2 \mid D_N(p) \\ p \nmid f}} \left(\frac{d_{N,fm}(p)}{n}\right) \sqrt{|D_N(p)|} = \sum_{k \in I} \sum_{\substack{X_k < p < X_k + Y \\ p \equiv 1 \pmod{m} \\ (fm)^2 \mid D_N(p) \\ p \nmid f}} \left(\frac{d_{N,fm}(p)}{n}\right) \sqrt{|D_N(p)|}. \tag{14}$$

On the interval $(X, X+Y]$, we approximate $\sqrt{|D_N(p)|}$ by $\sqrt{|D_N(X)|}\log p/\log N$. Letting X^* be the value of t minimizing the function $\sqrt{|D_N(t)|}$ on the interval $[X, X+Y]$, we find

$$\left| \sqrt{|D_N(p)|} - \frac{\sqrt{|D_N(X)|}\log p}{\log N} \right| \ll \begin{cases} N^{1/4}\sqrt{Y} + \dfrac{\sqrt{|D_N(X)|}}{\sqrt{N}\log N} & \text{if } N^{\pm} \in [X, X+Y], \\ \dfrac{Y\sqrt{N}}{\sqrt{|D_N(X^*)|}} + \dfrac{\sqrt{|D_N(X)|}}{\sqrt{N}\log N} & \text{otherwise.} \end{cases}$$

Using Euler–Maclaurin summation as in [**13**], it is easy to show

$$\sum_{k \in I} \sqrt{|D_N(X_k)|} = \frac{2\pi N}{Y} + O(\sqrt{N}) \tag{15}$$

and

$$\sum_{k \in I} \frac{1}{\sqrt{|D_N(X_k^*)|}} \ll \frac{1}{Y}.$$

Employing these estimates and Lemma 9 (with $u = m$ and $v = f^2$), we find

$$\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m \\ (fm)^2 \mid D_N(p) \\ p \nmid f}} \left(\frac{d_{N,fm}(p)}{n}\right) \sqrt{|D_N(p)|} = \frac{1}{\log N} \sum_{k \in I} \sqrt{|D_N(X_k)|} \sum_{\substack{X_k < p \leqslant X_k + Y \\ p \equiv 1 \pmod m \\ (fm)^2 \mid D_N(p) \\ p \nmid f}} \left(\frac{d_{N,fm}(p)}{n}\right) \log p$$
$$+ O\left(\frac{Y\sqrt{N}}{\varphi(mf)\log(Y/mf^2)}\right),$$

provided that $mf < Y$. Summing this error over n and f, we find that the total error is $O(Y\sqrt{N}\log U/\varphi(m^2)(\log(Y/m)))$ provided $m < Y$. Therefore, if $\gamma = \beta + 1$, then

$$\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} H\left(\frac{D_N(p)}{m^2}\right)$$
$$= \frac{1}{2\pi \log N} \sum_{k \in I} \sqrt{|D_N(X_k)|} \sum_{\substack{f \leqslant V \\ (f,2)=1, \\ n \leqslant U}} \frac{1}{fmn} \sum_{\substack{X_k < p \leqslant X_k + Y \\ p \equiv 1 \pmod m \\ (fm)^2 \mid D_N(p) \\ p \nmid f}} \left(\frac{d_{N,fm}(p)}{n}\right) \log p$$
$$+ O\left(\frac{N}{\varphi(m^2)(\log N)^{\beta+1}}\right)$$

for m as large as $N^{1/2-\epsilon}$ (for any fixed $\epsilon > 0$). It is also convenient to remove those primes p which divide n from the innermost sum above. Doing this introduces an error which is $O(m^{-1}\sqrt{N}(\log V)(\log U)^2)$. Given our choice of U and V, this can easily be absorbed into the error term for m as large as $N^{1/2-\epsilon}$.

Now let

$$S_k(N, m; U, V) := \sum_{\substack{f \leqslant V \\ (f,2)=1, \\ n \leqslant U}} \frac{1}{fmn} \sum_{\substack{X_k < p \leqslant X_k + Y \\ p \equiv 1 \pmod m \\ (fm)^2 \mid D_N(p) \\ p \nmid fn}} \left(\frac{d_{N,fm}(p)}{n}\right) \log p,$$

so that

$$\sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod m}} H\left(\frac{D_N(p)}{m^2}\right) = \frac{1}{2\pi \log N} \sum_{k \in I} \sqrt{|D_N(X_k)|} S_k(N, m; U, V) + O\left(\frac{N}{\varphi(m^2)(\log N)^{\beta+1}}\right).$$

Using the fact that the Kronecker symbol $(\cdot/n)$ is periodic modulo $4n$, we may write

$$S_k(N, m; U, V) = \sum_{\substack{f \leqslant V \\ (f,2)=1, \\ n \leqslant U}} \frac{1}{fmn} \sum_{\substack{a=1 \\ a \equiv 1 \pmod 4}}^{4n} \left(\frac{a}{n}\right) \sum_{\substack{X_k < p \leqslant X_k + Y \\ p \equiv 1 \pmod m \\ (fm)^2 \mid D_N(p) \\ d_{N,fm}(p) \equiv a \pmod{4n} \\ p \nmid nf}} \log p. \tag{16}$$

We now note that since $m^2 \mid N$, the condition $(fm)^2 \mid D_N(p)$ implies $p \equiv 1 \pmod m$. Therefore, making the change of variables $mf \mapsto f$ and reorganizing the innermost sum over p, we obtain the identity

$$S_k(N,m;U,V) = \sum_{\substack{f\leqslant mV\\ m\mid f\\ (f,2)=1,\\ n\leqslant U}} \frac{1}{fn} \sum_{\substack{a=1\\ a\equiv 1 \pmod 4}}^{4n} \left(\frac{a}{n}\right) \sum_{b\in C_N(a,n,f)} \sum_{\substack{X_k<p\leqslant X_k+Y\\ p\equiv b \pmod{4nf^2}}} \log p, \tag{17}$$

where

$$C_N(a,n,f) := \{b \in (\mathbb{Z}/4nf^2\mathbb{Z})^\times : D_N(b) \equiv af^2 \pmod{4nf^2}\}.$$

We choose to approximate $S_k(N,m;U,V)$ by

$$\tilde{S}_k(N,m;U,V) := \sum_{\substack{f\leqslant mV\\ m\mid f\\ (f,2)=1,\\ n\leqslant U}} \frac{1}{fn} \sum_{\substack{a=1\\ a\equiv 1 \pmod 4}}^{4n} \left(\frac{a}{n}\right) \#C_N(a,n,f) \frac{Y}{\varphi(4nf^2)}.$$

It is at this point that we must impose the condition $m \leqslant (\log N)^\alpha$. To bound the error in the above approximation, we use Cauchy–Schwarz and Conjecture 17 to see that

$$\begin{aligned}
|S-\tilde{S}| &\leqslant \sum_{\substack{f\leqslant mV\\ m\mid f,\\ n\leqslant U}} \frac{1}{fn} \sum_{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^\times} \left|\theta(X_k,Y;4nf^2,b) - \frac{Y}{\varphi(4nf^2)}\right| \\
&\leqslant \sum_{\substack{f\leqslant mV\\ m\mid f}} \frac{1}{f} \left[\sum_{n\leqslant U} \frac{\varphi(4nf^2)}{n^2}\right]^{1/2} \left[\sum_{n\leqslant U} \sum_{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^\times} \left|E(X_k,Y;4nf^2,b)\right|^2\right]^{1/2} \\
&\ll \frac{Y}{(\log N)^\upsilon}
\end{aligned}$$

for any choice of $\upsilon > 0$ since $4Um^2V^2 \leqslant 4N^{7/16}(\log N)^{2\alpha+6\beta+4} \ll Y/(\log N)^{\upsilon+1}$. Summing this error over $k \in I$ and choosing $\upsilon = 2\alpha+\beta$, we have

$$\sum_{\substack{N^-<p<N^+\\ p\equiv 1 \pmod m}} H\left(\frac{D_N(p)}{m^2}\right) = \frac{1}{2\pi\log N} \sum_{k\in I} \sqrt{|D_N(X_k)|}\,\tilde{S}_k(N,m;U,V) + O\left(\frac{N}{\varphi(m^2)(\log N)^{\beta+1}}\right)$$

since $m \leqslant (\log N)^\alpha$. Now, let

$$K_0(N,m;U,V) := \sum_{\substack{f\leqslant mV\\ m\mid f\\ (f,2)=1}} \frac{1}{f} \sum_{n\leqslant U} \frac{1}{n\varphi(4nf^2)} \sum_{\substack{a=1\\ a\equiv 1 \pmod 4}}^{4n} \left(\frac{a}{n}\right) \#C_N(a,n,f). \tag{18}$$

With this notation, we may rewrite the above as

$$\sum_{\substack{N^-<p<N^+\\ p\equiv 1 \pmod m}} H\left(\frac{D_N(p)}{m^2}\right) = \frac{Y}{2\pi\log N} \sum_{k\in I} \sqrt{|D_N(X_k)|}\,K_0(N,m;U,V) + O\left(\frac{N}{\varphi(m^2)(\log N)^{\beta+1}}\right). \tag{19}$$

We now require the following lemma whose proof we postpone until Section 6.

Lemma 11. *For $\epsilon, U, V > 0$,*

$$K_0(N,m) = K_0(N,m;U,V) + O\left(\frac{N^\epsilon}{\varphi(m^2)\sqrt{U}} + \frac{\log\log N}{\varphi(m^2)V}\right).$$

Given our choice of U and V, this lemma together with (15) and (19) is sufficient to complete the proof of the theorem. □

4. *Computing the arithmetic factor $K_0(N,m)$*

The main result of this section is the following factorization of $K_0(N,m)$ as an Euler product.

Proposition 12. *Let m and N be odd positive integers with $m^2 \mid N$, and let $K_0(N,m)$ be as defined in Theorem 10. Then*

$$K_0(N,m) = \frac{N}{\varphi(N)m^2} K(N)K(N,m),$$

where

$$K(N,m) := \prod_{\substack{\ell\mid m\\ 2\nmid\nu_\ell(N)}} \left(\frac{\ell^{\nu_\ell(N)+1} - \ell^{2\nu_\ell(m)}}{\ell^{\nu_\ell(N)+1} - \ell^{\nu_\ell(N)} - 1}\right) \prod_{\substack{\ell\mid m\\ 2\mid\nu_\ell(N)}} \left(\frac{\ell^{\nu_\ell(N)+2} - \ell^{2\nu_\ell(m)+1} + (-N_{(\ell)}/\ell)\ell^{2\nu_\ell(m)}}{\ell^{\nu_\ell(N)+2} - \ell^{\nu_\ell(N)+1} - \ell + (-N_{(\ell)}/\ell)}\right)$$

and

$$K(N) := \prod_{\ell\nmid N}\left(1 - \frac{((N-1)/\ell)^2\ell + 1}{(\ell+1)(\ell-1)^2}\right) \prod_{\substack{\ell\mid N\\ 2\nmid\nu_\ell(N)}} \left(1 - \frac{1}{\ell^{\nu_\ell(N)}(\ell-1)}\right) \prod_{\substack{\ell\mid N\\ 2\mid\nu_\ell(N)}} \left(1 - \frac{\ell - (-N_{(\ell)}/\ell)}{\ell^{\nu_\ell(N)+1}(\ell-1)}\right). \tag{20}$$

Here $\nu_\ell(N)$ is the usual ℓ-adic valuation, $N_{(\ell)} := N/\ell^{\nu_\ell(N)}$ denotes the ℓ-free part of N, and $(\cdot/\ell)$ is the usual Kronecker symbol.

Remark 13. It will be convenient in the next section to note that $K(N)$ is absolutely bounded as a function of N, $N/\varphi(N) \ll \log\log N$, and $K(N,m) \ll m/\varphi(m) \ll \log\log m$.

We note that $K_0(N) = K_0(N,1)$ was computed in [**13**]. We will appeal often to results from [**13**] in our computation of $K_0(N,m)$.

Proof of Proposition 12. We begin by using the Chinese Remainder Theorem to write

$$K_0(N,m) := \sum_{\substack{f=1\\ m\mid f\\ (f,2)=1}}^\infty \frac{1}{f}\sum_{n=1}^\infty \frac{1}{n\varphi(4nf^2)} \sum_{\substack{a\in(\mathbb{Z}/4n\mathbb{Z})^*\\ a\equiv 1 \pmod 4}} \left(\frac{a}{n}\right) \prod_{\ell\mid 4nf} \#C_N^{(\ell)}(a,n,f),$$

where for each prime ℓ dividing $4nf$ we write

$$C_N^{(\ell)}(a,n,f) := \{z \in (\mathbb{Z}/\ell^{\nu_\ell(4nf^2)}\mathbb{Z})^* : D_N(z) \equiv af^2 \pmod{\ell^{\nu_\ell(4nf^2)}}\}.$$

We note that if ℓ is a prime dividing f but not n, then $af^2 \equiv 0 \pmod{\ell^{\nu_\ell(4nf^2)}}$. Hence, it is clear that $\#C_N^{(\ell)}(a,n,f) = \#C_N^{(\ell)}(1,1,f)$ if $\ell \mid f$ but $\ell \nmid n$. In [**13**, Lemma 10], it was shown that

$$\#C_N^{(2)}(a,n,f) = 2\mathcal{S}_2(n,a),$$

where

$$\mathcal{S}_2(n,a) = \begin{cases} 2 & \text{if } \nu_2(4nf^2) = 2 + \nu_2(n) = 2, \\ 4 & \text{if } \nu_2(4nf^2) = 2 + \nu_2(n) \geqslant 3 \text{ and } a \equiv 5 \pmod 8, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, letting n' denote the odd part of n and

$$c_{N,f}(n) := \sum_{\substack{a \in (\mathbb{Z}/4n\mathbb{Z})^* \\ a \equiv 1 \pmod 4}} \left(\frac{a}{n}\right) \mathcal{S}_2(n,a) \prod_{\ell \mid n'} \#C_N^{(\ell)}(a,n,f),$$

we may write

$$\begin{aligned} K_0(N,m) &= \sum_{\substack{f=1 \\ m \mid f \\ (f,2)=1}}^{\infty} \frac{1}{f^2} \sum_{n=1}^{\infty} \frac{2}{n\varphi(4nf)} \left[\prod_{\substack{\ell \mid f \\ \ell \nmid n}} \#C_N^{(\ell)}(a,n,f) \right] c_{N,f}(n) \\ &= \sideset{}{'}\sum_{\substack{f=1 \\ m \mid f \\ (f,2)=1}}^{\infty} \frac{\prod_{\ell \mid f} \#C_N^{(\ell)}(1,1,f)}{f^2 \varphi(f)} \sum_{n=1}^{\infty} \frac{2\varphi((n,f))}{(n,f) n \varphi(4n)} \left[\prod_{\ell \mid (f,n)} \#C_N^{(\ell)}(1,1,f) \right]^{-1} c_{N,f}(n), \end{aligned} \tag{21}$$

where the $'$ on the sum over f is meant to indicate that the sum is to be restricted to those f that are not divisible by any prime ℓ for which $\#C_N^{(\ell)}(1,1,f) = 0$. The following was shown in [13], and we state it here without proof.

Lemma 14. *Suppose that N and f are odd. The function $c_{N,f}(n)$ is multiplicative in n. Let α be a positive integer and ℓ be an odd prime. Then*

$$\frac{c_{N,f}(2^\alpha)}{2^{\alpha-1}} = (-1)^\alpha 2.$$

If $\ell \mid f$ and $\ell \nmid N$, then

$$\frac{c_{N,f}(\ell^\alpha)}{\ell^{\alpha-1}} = \#C_N^{(\ell)}(1,1,f) \begin{cases} \ell - 1 & \text{if } 2 \mid \alpha, \\ 0 & \text{if } 2 \nmid \alpha. \end{cases}$$

If $\ell \mid N$ and $\ell \nmid f$, then

$$\frac{c_{N,f}(\ell^\alpha)}{\ell^{\alpha-1}} = \ell - 2.$$

If $\ell \nmid Nf$, then

$$\frac{c_{N,f}(\ell^\alpha)}{\ell^{\alpha-1}} = \begin{cases} \ell - 1 - \left(\frac{N}{\ell}\right) - \left(\frac{N-1}{\ell}\right)^2 & \text{if } 2 \mid \alpha, \\ -1 - \left(\frac{N-1}{\ell}\right)^2 & \text{if } 2 \nmid \alpha. \end{cases}$$

If $\ell \mid (f,N)$ and $2\nu_\ell(f) < \nu_\ell(N)$, then

$$\frac{c_{N,f}(\ell^\alpha)}{\ell^{\alpha-1}} = \#C_N^{(\ell)}(1,1,f)(\ell - 1).$$

If $\ell \mid (f,N)$ *and* $\nu_\ell(N) < 2\nu_\ell(f)$*, then*

$$\frac{c_{N,f}(\ell^\alpha)}{\ell^{\alpha-1}} = \#C_N^{(\ell)}(1,1,f)\begin{cases} \ell-1 & \text{if } 2\mid\alpha, \\ 0 & \text{if } 2\nmid\alpha. \end{cases}$$

If $\ell \mid (f,N)$ *and* $\nu_\ell(N) = 2\nu_\ell(f)$*, then*

$$\frac{c_{N,f}(\ell^\alpha)}{\ell^{\alpha-1}} = \#C_N^{(\ell)}(1,1,f)\begin{cases} \left(\ell-1-\left(\frac{N_{(\ell)}}{\ell}\right)+\left(\frac{-N_{(\ell)}}{\ell}\right)\right) & \text{if } 2\mid\alpha, \\ \left(\left(\frac{-N_{(\ell)}}{\ell}\right)-1\right) & \text{if } 2\nmid\alpha, \end{cases}$$

where $N_{(\ell)} = N/\ell^{\nu_\ell(N)}$ *denotes the* ℓ*-free part of* N*.*

Using this result, the sum over n in equation (21) may be factored as

$$\sum_{n=1}^\infty \frac{2\varphi((n,f))}{(n,f)n\varphi(4n)}\left[\prod_{\ell\mid(f,n)}\#C_N^{(\ell)}(1,1,f)\right]^{-1} c_{N,f}(n) = \frac{2}{3}\prod_{\substack{\ell\nmid f\\ \ell\mid N}}F_0(\ell)\prod_{\ell\nmid 2fN}F_1(\ell)\prod_{\ell\mid f}F_2(\ell,f),$$

where for any odd prime ℓ, we make the definitions

$$\begin{aligned} F_0(\ell) &:= \left(1+\frac{\ell-2}{(\ell-1)^2}\right), \\ F_1(\ell) &:= \left(1-\frac{((N-1)/\ell)^2\ell+(N/\ell)+((N-1)/\ell)^2+1}{(\ell-1)(\ell^2-1)}\right), \\ F_2(\ell,f) &:= \begin{cases} \left(1+\frac{1}{\ell(\ell+1)}\right) & \text{if } \nu_\ell(N)<2\nu_\ell(f), \\ \left(1+\frac{1}{\ell}\right) & \text{if } \nu_\ell(N)>2\nu_\ell(f), \\ \left(1+\frac{(-N_{(\ell)}/\ell)\ell+(-N_{(\ell)}/\ell)-(N_{(\ell)}/\ell)-1}{\ell(\ell^2-1)}\right) & \text{if } \nu_\ell(N)=2\nu_\ell(f). \end{cases} \end{aligned}$$

Substituting this back into equation (21) and rearranging slightly, we have

$$K_0(N,m) = \frac{2}{3}\prod_{\ell\mid N}F_0(\ell)\prod_{\ell\nmid 2N}F_1(\ell)\sum_{\substack{f=1\\ m\mid f\\ (f,2)=1}}^{\infty}{}' \frac{\prod_{\ell\mid f}\#C_N^{(\ell)}(1,1,f)}{\varphi(f)f^2}\prod_{\ell\mid(f,N)}\frac{F_2(\ell,f)}{F_0(\ell)}\prod_{\substack{\ell\mid f\\ \ell\nmid N}}\frac{F_2(\ell,f)}{F_1(\ell)}. \quad (22)$$

In [**13**], we showed that for any odd prime power ℓ^α,

$$\#C_N^{(\ell)}(1,1,\ell^\alpha) = \begin{cases} 1+\left(\frac{N(N-1)^2}{\ell}\right) & \text{if } \ell\nmid N, \\ 2\ell^{\nu_\ell(N)/2} & \text{if } 1\leqslant\nu_\ell(N)<2\alpha,\ 2\mid\nu_\ell(N) \text{ and } \left(\frac{N_{(\ell)}}{\ell}\right)=1, \\ \ell^\alpha & \text{if } 2\alpha\leqslant\nu_\ell(N), \\ 0 & \text{otherwise.} \end{cases} \quad (23)$$

Hence, the sum over f in equation (22) may be factored as

$$\sum_{\substack{f=1\\ m|f\\ (f,2)=1}}^{\infty}{}' \frac{\prod_{\ell|f} \#C_N^{(\ell)}(1,1,f)}{\varphi(f)f^2} \prod_{\ell|(f,N)} \frac{F_2(\ell,f)}{F_0(\ell)} \prod_{\substack{\ell|f\\ \ell\nmid N}} \frac{F_2(\ell,f)}{F_1(\ell)} = \prod_{\ell\nmid 2N} F_3(\ell) \prod_{\substack{\ell|N\\ \ell\nmid m}} F_4(\ell) \prod_{\ell|m} F_5(\ell),$$

where for any odd prime ℓ, we make the definitions

$$F_3(\ell) := 1 + \frac{1+(N(N-1)^2/\ell)}{F_1(\ell)(\ell+1)(\ell-1)^2},$$
$$F_4(\ell) := \begin{cases} 1 + \dfrac{\ell^{\nu_\ell(N)} - \ell}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2} & \text{if } 2 \nmid \nu_\ell(N), \\ 1 + \dfrac{\ell^{\nu_\ell(N)} - \ell + (-N_{(\ell)}/\ell)}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2} & \text{if } 2 \mid \nu_\ell(N), \end{cases}$$
$$F_5(\ell) := \frac{1}{F_0(\ell)\ell^{2\nu_\ell(m)}} \begin{cases} \dfrac{\ell(\ell^{\nu_\ell(N)} - \ell^{2\nu_\ell(m)})}{\ell^{\nu_\ell(N)}(\ell-1)^2} & \text{if } 2 \nmid \nu_\ell(N), \\ \dfrac{\ell^{\nu_\ell(N)+2} - \ell^{2\nu_\ell(m)+1} + (-N_{(\ell)}/\ell)\ell^{2\nu_\ell(m)}}{\ell^{\nu_\ell(N)}(\ell-1)^2} & \text{if } 2 \mid \nu_\ell(N). \end{cases}$$

Substituting this back into equation (22), we have

$$\begin{aligned} K_0(N,m) &= \frac{2}{3} \prod_{\ell\nmid 2N} F_1(\ell)F_3(\ell) \prod_{\substack{\ell|N\\ \ell\nmid m}} F_0(\ell)F_4(\ell) \prod_{\ell|m} F_0(\ell)F_5(\ell) \\ &= \frac{2}{3} \prod_{\ell\nmid 2N} F_1(\ell)F_3(\ell) \prod_{\ell|N} F_0(\ell)F_4(\ell) \prod_{\ell|m} \frac{F_5(\ell)}{F_4(\ell)}. \end{aligned} \tag{24}$$

The result now follows by simplifying the factors. □

5. *Removing the larger group structures*

In this section, we complete the proof of Theorem 2. Before doing so, we require the following lemma.

LEMMA 15. *Let $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$, and write $N = \#G = N_1^2N_2$. Then*

$$\frac{\#G}{\#\mathrm{Aut}(G)} = \frac{N}{\varphi(N)N_1^2} \prod_{\substack{\ell|N_1\\ \ell\nmid N_2}} \frac{\ell^2}{\ell^2-1} \prod_{\ell|(N_1,N_2)} \frac{\ell}{\ell-1}.$$

Proof. For the proof, see [**16**, Lemma 2.1 and Theorem 4.1]. □

REMARK 16. From the above factorization, it is easy to see that $\#G/\#\mathrm{Aut}(G) > 1/\varphi(N_1^2)$.

We now combine all of our intermediate results to give the proof of Theorem 2.

Proof of Theorem 2. Let $N = N_1^2 N_2 = \#G$. Then the condition $\exp(G) \geqslant \#G/(\log \#G)^\alpha$ is equivalent to $N_1 \leqslant (\log N)^\alpha$. Now choose any $\gamma > \beta + 1$. By Lemma 4, we have

$$M(G) = \sum_{\substack{k^2 \mid N_2 \\ k \leqslant (\log N)^\gamma}} \mu(k) M(N; kN_1) + \sum_{\substack{k^2 \mid N_2 \\ k > (\log N)^\gamma}} \mu(k) M(N; kN_1).$$

In [24, p. 656], we find the standard bound $H(D) \ll \sqrt{|D|} \log |D| (\log\log |D|)^2$. Using this, Corollary 8, and the Brun–Titchmarsh inequality [17, p. 167], we have

$$\begin{aligned}\sum_{\substack{k^2 \mid N_2 \\ k > (\log N)^\gamma}} \mu(k) M(N; kN_1) &\ll \sum_{\substack{k^2 \mid N_2 \\ k > (\log N)^\gamma}} \sum_{\substack{N^- < p < N^+ \\ p \equiv 1 \pmod{kN_1}}} \frac{\sqrt{N} \log N (\log\log N)^2}{kN_1} \\ &\ll \frac{N \log N (\log\log N)^2}{\varphi(N_1^2)} \sum_{k > (\log N)^\gamma} \frac{1}{\varphi(k^2) \log(\sqrt{N}/kN_1)} \\ &\ll \frac{N}{\varphi(N_1^2)(\log N)^{\beta+1}}.\end{aligned}$$

Applying Theorem 10 for small k, we find

$$M(G) = \frac{N}{\log N} \sum_{\substack{k^2 \mid N_2 \\ k \leqslant (\log N)^\gamma}} \mu(k) K_0(N, kN_1) + O\left(\frac{N}{\varphi(N_1^2)(\log N)^{\beta+1}} \right).$$

By the remark following the statement of Proposition 12,

$$\sum_{\substack{k^2 \mid N_2 \\ k > (\log N)^\gamma}} \mu(k) K_0(N, kN_1) \ll \sum_{k > (\log N)^\gamma} \frac{(\log\log N)^2}{k^2 N_1^2} \ll \frac{1}{\varphi(N_1^2)(\log N)^{\beta+1}},$$

and therefore,

$$M(G) = \frac{N}{\log N} \sum_{k^2 \mid N_2} \mu(k) K_0(N, kN_1) + O\left(\frac{N}{\varphi(N_1^2)(\log N)^{\beta+1}} \right). \tag{25}$$

Using Proposition 12, we have

$$\sum_{k^2 \mid N_2} \mu(k) K_0(N, kN_1) = \frac{N}{\varphi(N) N_1^2} K(N) \sum_{k^2 \mid N_2} \frac{\mu(k)}{k^2} K(N, kN_1). \tag{26}$$

Now let $K^{(\ell)}(N, m)$ stand for the factor of $K(N, m)$ coming from the prime ℓ, that is,

$$K^{(\ell)}(N, m) := \begin{cases} \dfrac{\ell^{\nu_\ell(N)+1} - \ell^{2\nu_\ell(m)}}{\ell^{\nu_\ell(N)+1} - \ell^{\nu_\ell(N)} - 1} & \text{if } \ell \mid m \text{ and } 2 \nmid \nu_\ell(N), \\[2ex] \dfrac{\ell^{\nu_\ell(N)+2} - \ell^{2\nu_\ell(m)+1} + (-N_{(\ell)}/\ell)\ell^{2\nu_\ell(m)}}{\ell^{\nu_\ell(N)+2} - \ell^{\nu_\ell(N)+1} - \ell + (-N_{(\ell)}/\ell)} & \text{if } \ell \mid m \text{ and } 2 \mid \nu_\ell(N). \end{cases}$$

Then by multiplicativity, we have

$$\begin{aligned}\sum_{k^2|N_2}\frac{\mu(k)}{k^2}K(N,kN_1) &= \prod_{\ell|N_1}K^{(\ell)}(N,N_1)\sum_{k^2|N_2}\frac{\mu(k)}{k^2}\frac{\prod_{\ell|k}K^{(\ell)}(N,kN_1)}{\prod_{\ell|(k,N_1)}K^{(\ell)}(N,N_1)}\\ &= \prod_{\ell|N_1}K^{(\ell)}(N,N_1)\prod_{\substack{\ell^2|N_2\\ \ell\nmid N_1}}\left(1-\frac{K^{(\ell)}(N,\ell N_1)}{\ell^2}\right)\prod_{\substack{\ell^2|N_2\\ \ell|N_1}}\left(1-\frac{K^{(\ell)}(N,\ell N_1)}{\ell^2 K^{(\ell)}(N,N_1)}\right)\\ &= \prod_{\substack{\ell|N_1\\ \ell^2\nmid N_2}}K^{(\ell)}(N,N_1)\prod_{\substack{\ell^2|N_2\\ \ell\nmid N_1}}\left(1-\frac{K^{(\ell)}(N,\ell)}{\ell^2}\right)\\ &\quad\times\prod_{\substack{\ell^2|N_2\\ \ell|N_1}}\left(K^{(\ell)}(N,N_1)-\frac{K^{(\ell)}(N,\ell N_1)}{\ell^2}\right).\end{aligned}$$

Recalling the definition of $K(N)$ as given by equation (20), we find

$$\begin{aligned}&K(N)\sum_{k^2|N_2}\frac{\mu(k)}{k^2}K(N,kN_1)\\ &\quad=\prod_{\ell\nmid N}\left(1-\frac{((N-1)/\ell)^2\ell+1}{(\ell+1)(\ell-2)^2}\right)\prod_{\substack{\ell|N_1\\ \ell\nmid N_2}}\frac{\ell^2}{\ell^2-1}F_6(\ell)\prod_{\substack{\ell|N_1\\ \ell|N_2}}\frac{\ell}{\ell-1}F_7(\ell)\prod_{\substack{\ell\nmid N_1\\ \ell|N_2}}F_8(\ell),\end{aligned}$$

where for each odd prime ℓ, we make the definitions

$$\begin{aligned}F_6(\ell) &:= 1+\frac{((-N_{(\ell)}/\ell)-1)\ell+(-N_{(\ell)}/\ell)}{\ell^3},\\ F_7(\ell) &:= 1-\frac{1}{\ell^2},\\ F_8(\ell) &:= 1-\frac{1}{\ell(\ell-1)}.\end{aligned}$$

Substituting the above into equation (26) and using Lemma 15, we find (after some slight rearrangement of the factors) that

$$\sum_{k^2|N_2}\mu(k)K_0(N,kN_1)=K(G)\frac{\#G}{\#\mathrm{Aut}(G)},$$

where $K(G)$ is defined by equation (3). The result now follows by substituting this into equation (25) and using the remark following the statement of Lemma 15. □

6. *Conjecture* 17 *and proofs of Lemmas* 9 *and* 11

In this section, we give the precise statement of the conjecture for the distribution of primes in short intervals that is needed to prove Theorems 1 and 2. We also present the proofs of Lemmas 9 and 11.

Given real parameters $X, Y > 0$ and integers q and a, we let $\theta(X,Y;q,a)$ denote the logarithmic weighted prime counting function

$$\theta(X,Y;q,a):=\sum_{\substack{X<p<X+Y\\ p\equiv a \pmod q}}\log p,$$

and we let $E(X,Y;q,a)$ be the error in approximating $\theta(X,Y;q,a)$ by $Y/\varphi(q)$. That is,

$$E(X,Y;q,a) := \theta(X,Y;q,a) - Y/\varphi(q).$$

Conjecture 17 (Barban–Davenport–Halberstam for intervals of length X^η). Let $0<\eta\leqslant 1$, and let $\beta>0$ be arbitrary. Suppose $X^\eta \leqslant Y \leqslant X$, and $Y/(\log X)^\beta \leqslant Q \leqslant Y$. Then

$$\sum_{q\leqslant Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} |E(X,Y;q,a)|^2 \ll YQ\log X.$$

Remark 18. If $\eta = 1$, then this is essentially the classical Barban–Davenport–Halberstam Theorem; see, for example, [10, p. 196]. The best results known are due to Languasco, Perelli, and Zaccagnini [22], who show that Conjecture 17 holds unconditionally for any $\eta > \frac{7}{12}$ and for any $\eta > \frac{1}{2}$ under the Generalized Riemann Hypothesis. For the proofs of Theorems 1 and 2, we essentially need to assume that it holds for some $\eta < \frac{1}{2}$.

Proof of Lemma 9. First, we make the definition

$$\Delta_{N,u}(l) := (l - N/u)^2 - 4N/u^2, \tag{27}$$

and note that this is a quadratic polynomial in l with integer coefficients since $u^2 \mid N$. We also note that if $p = 1 + lu$, then $\Delta_{N,u}(l) = D_N(p)/u^2$. Therefore,

$$\begin{aligned}
\#\left\{ X < p \leqslant X+Y : \begin{array}{l} p\equiv 1 \pmod u \\ D_N(p)\equiv 0 \pmod{u^2v} \\ (p,v)=1 \end{array} \right\}
&= \#\left\{ X < p \leqslant X+Y : \begin{array}{c} p\equiv 1 \pmod u \\ \Delta_{N,u}\left(\dfrac{p-1}{u}\right) \equiv 0 \pmod v \\ (p,v)=1 \end{array} \right\} \\
&= \sum_{\substack{1\leqslant l\leqslant v\\ (1+lu,v)=1\\ \Delta_{N,u}(l)\equiv 0 \pmod v}} \#\{X<p<X+Y : p\equiv 1+lu \pmod{uv}\}.
\end{aligned}$$

Using the Chinese Remainder Theorem, it is easy (though perhaps a bit tedious) to show

$$\#\{l \in \mathbb{Z}/v\mathbb{Z} : \Delta_{N,u}(l) \equiv 0 \pmod v\} \leqslant 8\sqrt{v}.$$

We refer the reader to [13, Lemma 12] where the same bound is shown for the polynomial $D_N(p)$. However, the same proof goes through for any monic quadratic with integer coefficients. The above inequality together with the Brun–Titchmarsh inequality [17, p. 167] implies

$$\#\left\{ X < p \leqslant X+Y : \begin{array}{l} p\equiv 1 \pmod u \\ D_N(p)\equiv 0 \pmod{u^2v} \\ (p,v)=1 \end{array} \right\} \ll \frac{\sqrt{v}}{\varphi(uv)} \frac{Y}{\log(Y/uv)}, \tag{28}$$

uniformly for $uv \leqslant Y$. □

Proof of Lemma 11. In [13], we showed

$$c_{N,f}(n) \ll \frac{n\prod_{\ell\mid(f,n)} \#C_N(1,1,f)}{\kappa_{2N}(n)},$$

where for any integer m, $\kappa_m(n)$ is the multiplicative function defined on prime powers by

$$\kappa_m(\ell^\alpha) := \begin{cases} \ell & \text{if } 2 \nmid \alpha \text{ and } \ell \nmid m, \\ 1 & \text{otherwise.} \end{cases} \tag{29}$$

Therefore,

$$\begin{aligned} &K_0(N,m) - K_0(N,m;U,V) \\ &\ll \sum_{\substack{f \leqslant mV \\ m \mid f}}{}' \frac{\prod_{\ell \mid f} \#C_N^{(\ell)}(1,1,f)}{f^2 \varphi(f)} \sum_{n > U} \frac{2\varphi((n,f)) c_{N,f}(n)}{(n,f) n \varphi(4n) \prod_{\ell \mid (n,f)} \#C_N^{(\ell)}(1,1,f)} \\ &\quad + \sum_{\substack{f > mV \\ m \mid f}}{}' \frac{\prod_{\ell \mid f} \#C_N^{(\ell)}(1,1,f)}{f^2 \varphi(f)} \sum_{n \geqslant 1} \frac{2\varphi((n,f)) c_{N,f}(n)}{(n,f) n \varphi(4n) \prod_{\ell \mid (n,f)} \#C_N^{(\ell)}(1,1,f)} \\ &\ll \sum_{\substack{f \leqslant mV \\ m \mid f \\ (f,2)=1}} \frac{\prod_{\ell \mid f} \#C_N^{(\ell)}(1,1,f)}{f^2 \varphi(f)} \sum_{n > U} \frac{1}{\kappa_{2N}(n) \varphi(n)} \\ &\quad + \sum_{\substack{f > mV \\ m \mid f \\ (f,2)=1}} \frac{\prod_{\ell \mid f} \#C_N^{(\ell)}(1,1,f)}{f^2 \varphi(f)} \sum_{n \geqslant 1} \frac{1}{\kappa_{2N}(n) \varphi(n)}, \end{aligned} \tag{30}$$

where the primes on the sums on f are meant to indicate that the sums are to be restricted to odd f such that $\#C_N^{(\ell)}(1,1,f) \neq 0$ for all primes ℓ dividing f.

In [**11**, Lemma 3.4], we find

$$\sum_{n > U} \frac{1}{\kappa_1(n) \varphi(n)} \sim \frac{c_0}{\sqrt{U}}$$

for some positive constant c_0. In particular, this implies that the full sum converges. From this, we obtain a crude bound for the tail of the sum over n:

$$\begin{aligned} \sum_{n > U} \frac{1}{\kappa_{2N}(n) \varphi(n)} &= \sum_{\substack{kl > U \\ (l,2N)=1 \\ \ell \mid k \Rightarrow \ell \mid 2N}} \frac{1}{\kappa_1(l) \varphi(l) \varphi(k)} = \sum_{\substack{k \geqslant 1 \\ \ell \mid k \Rightarrow \ell \mid 2N}} \frac{1}{\varphi(k)} \sum_{\substack{l > U/k \\ (l,2N)=1}} \frac{1}{\kappa_1(l) \varphi(l)} \\ &\ll \sum_{\substack{k \geqslant 1 \\ \ell \mid k \Rightarrow \ell \mid 2N}} \frac{1}{\varphi(k)} \frac{\sqrt{k}}{\sqrt{U}} \ll \frac{1}{\sqrt{U}} \prod_{\ell \mid N} \left(1 + \frac{\ell}{(\ell-1)(\sqrt{\ell}-1)}\right) \\ &= \frac{1}{\sqrt{U}} \frac{N}{\varphi(N)} \prod_{\ell \mid N} \left(1 + \frac{1}{\sqrt{\ell}(\ell-1)}\right) \left(1 + \frac{1}{\sqrt{\ell}}\right) \\ &\ll \frac{1}{\sqrt{U}} \frac{N}{\varphi(N)} \prod_{\ell \mid N} \left(1 + \frac{1}{\sqrt{\ell}}\right). \end{aligned}$$

We have already noted that $N/\varphi(N) \ll \log\log N$. It is a straightforward exercise as in [**26**, p. 63] to show

$$\prod_{\ell \mid N} \left(1 + \frac{1}{\sqrt{\ell}}\right) < \exp\left\{O\left(\frac{\sqrt{\log N}}{\log\log N}\right)\right\}.$$

Thus, we conclude

$$\sum_{n>U} \frac{1}{\kappa_{2N}(n)\varphi(n)} \ll \frac{N^\epsilon}{\sqrt{U}}, \tag{31}$$

for any $\epsilon > 0$. For the full sum over n, we need a sharper bound in the N-aspect, which we obtain by writing

$$\begin{aligned}\sum_{n\geqslant 1} \frac{1}{\kappa_{2N}(n)\varphi(n)} &= \prod_{\ell\mid 2N}\left(1+\frac{\ell}{(\ell-1)^2}\right) \sum_{\substack{n\geqslant 1\\(n,2N)=1}} \frac{1}{\kappa_{2N}(n)\varphi(n)}\\ &\leqslant \frac{2N}{\varphi(2N)} \prod_{\ell\mid 2N}\left(1+\frac{1}{\ell(\ell-1)}\right)\sum_{n\geqslant 1}\frac{1}{\kappa_1(n)\varphi(n)}\\ &\ll \log\log N. \end{aligned} \tag{32}$$

For any odd prime ℓ dividing f, we obtain the bounds

$$\#C_N^{(\ell)}(1,1,f) \leqslant \begin{cases} 2\ell^{\nu_\ell(N)/2} & \text{if } \nu_\ell(f) > \nu_\ell(N)/2 \text{ and } 2 \mid \nu_\ell(N),\\ \ell^{\nu_\ell(f)} & \text{otherwise,}\end{cases}$$

from equation (23). Therefore, for every odd integer f, we have

$$\prod_{\ell\mid f} \#C_N^{(\ell)}(1,1,f) \leqslant f,$$

and hence

$$\sum_{\substack{f>mV\\ m\mid f\\ (f,2)=1}} \frac{\prod_{\ell\mid f}\#C_N^{(\ell)}(1,1,f)}{f^2\varphi(f)} < \sum_{\substack{f>mV\\ m\mid f}} \frac{1}{f\varphi(f)} \ll \frac{1}{\varphi(m^2)V}. \tag{33}$$

Substituting the bounds (31)–(33) into (30), the lemma follows. □

7. *Concluding remarks*

There are many open conjectures about the distribution of local invariants associated with the reductions modulo p of a fixed elliptic curve defined over $\mathbb{Q}$ as p varies over the primes. Perhaps the most famous examples are the conjectures of Koblitz [**20**] and of Lang and Trotter [**23**]. The Koblitz Conjecture concerns the number of primes $p \leqslant X$ such that $\#E(\mathbb{F}_p)$ is prime. The fixed trace Lang–Trotter Conjecture concerns the number of primes $p \leqslant X$ such that the trace of Frobenius $a_p(E)$ is equal to a fixed integer t. Another conjecture of Lang and Trotter (also called the Lang–Trotter Conjecture) concerns the number of primes $p \leqslant X$ such that the Frobenius field $\mathbb{Q}(\sqrt{a_p(E)^2 - 4p})$ is a fixed imaginary quadratic field.

These conjectures are all completely open. In order to gain evidence, it is natural to consider the averages for these problems over some family of elliptic curves. This has been done by various authors originating with the work of Fouvry and Murty [**15**] for the number of supersingular primes (that is, the fixed trace Lang–Trotter Conjecture for $t = 0$). See [**4**, **6**, **11**, **12**, **18**, **19**] for other averages regarding the fixed trace Lang–Trotter Conjecture. The average order for the Koblitz Conjecture was considered in [**1**]. Very recently, the average was successfully carried out for the Lang–Trotter Conjecture on Frobenius fields [**9**]. The average order problems that we consider here and in [**13**] have very different features than the above averages. This is primarily because both $M_E(G)$ and $M_E(N)$ count finite sets of primes whose sizes vary with the parameters G and N, whereas the above problems seek estimates for the densities of (what are believed to be) infinite sets of primes.

Much like the conjectural constants appearing in the Twin Prime Conjecture and the more general Bateman–Horn Conjectures [3], the constants in the conjectural asymptotics for the Lang–Trotter Conjectures and the Koblitz Conjecture can be written as Euler products in which the local Euler factors at each prime ℓ can be understood in terms of the probability that p satisfies the desired property modulo ℓ. Thus, for those conjectures, the constant from the average asymptotic gave strong evidence for the original conjectures as one retrieves the local Euler factors of the conjectural constants (forgetting about a finite number of 'exceptional primes' for each elliptic curve).

In the questions considered in [13] and the present paper, it does not seem very likely that there should be an asymptotic for a fixed elliptic curve. Moreover, the 'constants' $K(G)$ and $K(N)$ (defined by (3) and (20), respectively) are much more peculiar. In the first place, they are not truly constant. In the second place, it is not completely clear how to understand them in terms of local probabilities. However, there are some parts of $K(N)$ which do seem to fit those local probabilities. More precisely, given an elliptic curve $E/\mathbb{Q}$ without complex multiplication, for all but finitely many primes ℓ, we have an isomorphism $\mathrm{Gal}(\mathbb{Q}(E[\ell])) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, where $\mathbb{Q}(E[\ell])$ denotes the field obtained by adjoining to $\mathbb{Q}$ the coordinates of the ℓ-division torsion points $E[\ell]$. Furthermore, $\#E_p(\mathbb{F}_p) = p + 1 - a_p(E) \equiv \det(\sigma_p) + 1 - \mathrm{tr}(\sigma_p) \pmod{\ell}$, where σ_p denotes any element of the image of the Frobenius class at p in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Letting

$$C_N(\ell) := \{g \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(g) + 1 - \mathrm{tr}(g) \equiv N \pmod{\ell}\},$$

one readily finds in the case that $\ell \nmid N$,

$$\begin{aligned}\frac{\mathrm{Prob}(p + 1 - a_p(E) \equiv N \pmod{\ell})}{\mathrm{Prob}(n \equiv N \mod \ell)} &= \frac{\#C_N(\ell)/\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}{1/\ell} \\ &= \left(1 - \frac{((N-1)/\ell)^2\ell + 1}{(\ell-1)^2(\ell+1)}\right),\end{aligned}$$

where the denominator is the probability that a random integer n is congruent to N modulo ℓ. That is, we find agreement with the Euler factors of $K(N)$ at the primes ℓ not dividing N. It should be noted that Euler factors of $K(N)$ and $K(G)$ agree at the primes ℓ not dividing $N = \#G$. The local factors of $K(N)$ at the primes ℓ dividing N are more subtle. Some of the issues appearing in the analysis of those local factors are addressed in [25], where a statistical analysis of the function $K(N)N/\varphi(N)$ has been carried out. Employing a new technique to address moments of functions which are 'almost but not quite multiplicative', the authors show

$$\sum_{\substack{N \leqslant x \\ 2\nmid N}} K(N) \frac{N}{\varphi(N) \log N} \sim \frac{1}{3} \frac{x}{\log x}.$$

Note that this is what one should expect as exactly $\frac{1}{3}$ of the elements of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ have odd trace (that is, satisfy the condition $\det(g) + 1 - \mathrm{tr}(g) \equiv 1 \pmod{2}$). In collaboration with the authors of [25], the authors of the present paper are studying further properties of the function $K(N)$ which could lead to a probabilistic model for the local factors at the primes ℓ dividing N. It seems that those could eventually be understood by looking at probabilities on the group $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

As far as we know, no statistical analysis similar to [25] has been made for $K(G)$, but this could certainly be an interesting avenue of research.

Acknowledgements. The authors would like to thank Andrew Granville and Dimitris Koukoulopoulos for helpful discussions while working on this project, and the anonymous referee for useful suggestions. The first author also thanks Henri Cohen for enlightening discussions about the Cohen–Lenstra Heuristics during the MSRI Program 'Arithmetic Statistics' in 2011. This work was completed while the second author was a postdoctoral fellow at Centre de recherches mathématiques in Montreal, Canada. He is grateful for their support.

References

1. A. Balog, A. Cojocaru and C. David, 'Average twin prime conjecture for elliptic curves', *Amer. J. Math.* 133 (2011) 1179–1229.
2. W. D. Banks, F. Pappalardi and I. E. Shparlinski, 'On group structures realized by elliptic curves over arbitrary finite fields', *Experiment. Math.* 21 (2012) 11–25.
3. P. T. Bateman and R. A. Horn, 'A heuristic asymptotic formula concerning the distribution of prime numbers', *Math. Comp.* 16 (1962) 363–367.
4. J. Battista, J. Bayless, D. Ivanov and K. James, 'Average Frobenius distributions for elliptic curves with nontrivial rational torsion', *Acta Arith.* 119 (2005) 81–91.
5. D. A. Burgess, 'On character sums and L-series. II', *Proc. London Math. Soc.* (3) 13 (1963) 524–536.
6. N. Calkin, B. Faulkner, K. James, M. King and D. Penniston, 'Average Frobenius distributions for elliptic curves over abelian extensions', *Acta Arith.* 149 (2011) 215–244.
7. H. Cohen and H. W. Lenstra, Jr., 'Heuristics on class groups', *Number theory (New York, 1982)*, Lecture Notes in Mathematics 1052 (Springer, Berlin, 1984) 26–36.
8. H. Cohen and H. W. Lenstra, Jr., 'Heuristics on class groups of number fields', *Number theory, (Noordwijkerhout, 1983)*, Lecture Notes in Mathematics 1068 (Springer, Berlin, 1984) 33–62.
9. A. C. Cojocaru, H. Iwaniec and N. Jones, 'The average asymptotic behaviour of the Frobenius fields of an elliptic curve', Preprint.
10. H. Davenport, *Multiplicative number theory*, 2nd edn, Graduate Texts in Mathematics 74 (Springer, New York, 1980). Revised by Hugh L. Montgomery.
11. C. David and F. Pappalardi, 'Average Frobenius distributions of elliptic curves', *Int. Math. Res. Not.* 1999 (1999) 165–183.
12. C. David and F. Pappalardi, 'Average Frobenius distribution for inerts in $\mathbb{Q}(i)$', *J. Ramanujan Math. Soc.* 19 (2004) 181–201.
13. C. David and E. Smith, 'Elliptic curves with a given number of points over finite fields', *Compos. Math.* 149 (2013) 175–203.
14. M. Deuring, 'Die Typen der Multiplikatorenringe elliptischer Funktionenkörper', *Abh. Math. Sem. Hansischen Univ.* 14 (1941) 197–272.
15. E. Fouvry and M. R. Murty, 'On the distribution of supersingular primes', *Canad. J. Math.* 48 (1996) 81–104.
16. C. J. Hillar and D. L. Rhea, 'Automorphisms of finite abelian groups', *Amer. Math. Monthly* 114 (2007) 917–923.
17. H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications 33 (American Mathematical Society, Providence, RI, 2004).
18. K. James, 'Average Frobenius distributions for elliptic curves with 3-torsion', *J. Number Theory* 109 (2004) 278–298.
19. K. James and E. Smith, 'Average Frobenius distribution for elliptic curves defined over finite Galois extensions of the rationals', *Math. Proc. Cambridge Philos. Soc.* 150 (2011) 439–458.
20. N. Koblitz, 'Primality of the number of points on an elliptic curve over a finite field', *Pacific J. Math.* 131 (1988) 157–165.
21. E. Kowalski, 'Analytic problems for elliptic curves', *J. Ramanujan Math. Soc.* 21 (2006) 19–114.
22. A. Languasco, A. Perelli and A. Zaccagnini, 'On the Montgomery–Hooley theorem in short intervals', *Mathematika* 56 (2010) 231–243.
23. S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics 504 (Springer, Berlin, 1976). Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.
24. H. W. Lenstra, Jr., 'Factoring integers with elliptic curves', *Ann. of Math.* (2) 126 (1987) 649–673.
25. G. Martin, P. Pollack and E. Smith. 'Averages of the number of points on elliptic curves', Preprint, http://arxiv.org/abs/1208.0919.
26. H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics 97 (Cambridge University Press, Cambridge, 2007).
27. R. Schoof, 'Nonsingular plane cubic curves over finite fields', *J. Combin. Theory Ser. A* 46 (1987) 183–211.

Chantal David
Department of Mathematics and Statistics
Concordia University
1455 de Maisonneuve West
Montreal
Canada QC H3G 1M8

cdavid@mathstat.concordia.ca

Ethan Smith
Department of Mathematics
Liberty University
1971 University Blvd
MSC Box 710052
Lynchburg, VA 24502
USA

ecsmith13@liberty.edu