COMPOSITIO MATHEMATICA

Elliptic curves with a given number of points over finite fields

Chantal David and Ethan Smith

Compositio Math. **149** (2013), 175–203.

doi:10.1112/S0010437X12000541

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY

Compositio Math. 149 (2013) 175–203
doi:10.1112/S0010437X12000541

Elliptic curves with a given number of points over finite fields

Chantal David and Ethan Smith

Abstract

Given an elliptic curve E and a positive integer N, we consider the problem of counting the number of primes p for which the reduction of E modulo p possesses exactly N points over $\mathbb{F}_p$. On average (over a family of elliptic curves), we show bounds that are significantly better than what is trivially obtained by the Hasse bound. Under some additional hypotheses, including a conjecture concerning the short-interval distribution of primes in arithmetic progressions, we obtain an asymptotic formula for the average.

1. Introduction

Let E be an elliptic curve defined over the rational field $\mathbb{Q}$. For a prime p where E has good reduction, we let E_p denote the reduced curve modulo p and $\#E_p(\mathbb{F}_p)$ the number of $\mathbb{F}_p$-rational points. Then the trace of the Frobenius morphism at p, $a_p(E)$, satisfies the well-known identity $\#E_p(\mathbb{F}_p) = p + 1 - a_p(E)$ and the Hasse bound $|a_p(E)| < 2\sqrt{p}$.

Let N be a positive integer. We are interested in the number of primes for which $\#E_p(\mathbb{F}_p) = N$. In particular, we are interested in the behavior of the prime counting function

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

Note that if $\#E_p(\mathbb{F}_p) = N$, then the Hasse bound implies $(\sqrt{p} - 1)^2 < N < (\sqrt{p} + 1)^2$, which in turn implies that

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

Hence, $M_E(N)$ is a finite number, and we have the trivial bound

$$M_E(N) \ll \frac{\sqrt{N}}{\log(N+1)}. \tag{1}$$

In [Kow06], Kowalski shows that if E possesses complex multiplication (CM), then

$$M_E(N) \ll_{E,\varepsilon} N^{\varepsilon} \tag{2}$$

for any $\varepsilon > 0$. He asks if the same might be true for curves without CM. However, no bound between (1) and (2) is known for curves without CM.

Given an integer N, it is always possible through a Chinese remainder theorem argument to find an elliptic curve E that achieves the upper bound (1), i.e., such that $\#E_p(\mathbb{F}_p) = N$ for every prime p in the interval (N^-, N^+). Yet, for a fixed curve, one expects $M_E(N)$ to be quite small.

Received 22 August 2011, accepted in final form 8 May 2012, published online 1 November 2012.
2010 Mathematics Subject Classification 11G05 (primary), 11N13 (secondary).
Keywords: average order, elliptic curves, primes in short intervals, Barban–Davenport–Halberstam theorem, Cohen–Lenstra heuristics.

Consider the following naïve probabilistic model for $M_E(N)$. If we suppose that the values of $\#E(\mathbb{F}_p)$ are uniformly distributed, i.e., that

$$\mathrm{Prob}(\#E(\mathbb{F}_p) = N) = \begin{cases} \dfrac{1}{4\sqrt{p}} & \text{if } N^- < p < N^+, \\ 0 & \text{otherwise,} \end{cases} \tag{3}$$

then we expect that

$$\begin{aligned} M_E(N) &\approx \sum_p \mathrm{Prob}(\#E(\mathbb{F}_p) = N) = \sum_{N^- < p < N^+} \frac{1}{4\sqrt{p}} \\ &\approx \frac{1}{4\sqrt{N}} \int_{N^-}^{N^+} \frac{dt}{\log t} \sim \frac{1}{\log N}. \end{aligned} \tag{4}$$

Moreover, it is quite easy to show (see [Kow06] for example) that

$$\sum_{N \leqslant X} M_E(N) = \pi(X) + O(\sqrt{X}) \sim \frac{X}{\log X}, \tag{5}$$

where, as usual, $\pi(X) := \#\{p \leqslant X : p \text{ is prime}\}$. Therefore, the average order of $M_E(N)$ is $1/\log N$ in accordance with the above model. Perhaps the correct way to interpret these statements is to say that $M_E(N)$ must be equal to zero on a density-one subset of the integers for the mere reason that the primes are a subset of the integers of density zero. Finally, we note that, while it is not difficult to see that $\liminf M_E(N) = 0$, numerical computations [Kow06] are consistent with the possibility that $\limsup M_E(N) = \infty$. In fact, using the model (3) as in [Kow06], it is possible to predict this.

2. Statement of results

In this paper, we study the average for $M_E(N)$ over all elliptic curves over $\mathbb{Q}$ (and not over N as in (5)). Given integers a and b, let $E_{a,b}$ be the elliptic curve defined by the Weierstrass equation

$$E_{a,b} : y^2 = x^3 + ax + b.$$

For $A, B > 0$, we define a set of Weierstrass equations by

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

The following is our first main result.

Theorem 1. *If $A, B \geqslant \sqrt{N} \log N$ and $AB \geqslant N^{3/2}(\log N)^2$, then*

$$\frac{1}{\#\mathscr{C}(A, B)} \sum_{E \in \mathscr{C}(A,B)} M_E(N) \ll \frac{\log\log N}{\log N}$$

holds uniformly for $N \geqslant 3$.

Remark. We refer to the expression on the left-hand side of the above inequality as the average order of $M_E(N)$ taken over the family $\mathscr{C}(A, B)$.

Under an additional hypothesis concerning the short-interval distribution of primes in arithmetic progressions, we can prove an asymptotic formula for the average order of $M_E(N)$ over $\mathscr{C}(A, B)$. In particular, we note that all of the primes counted by $M_E(N)$ are of size N

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

lying in an interval of length $4\sqrt{N}$. Therefore, we require an appropriate short-interval version of the Barban–Davenport–Halberstam theorem.

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

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

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

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

Conjecture 2 (Barban–Davenport–Halberstam for intervals of length X^η). Let $0 < \eta \leqslant 1$, and let $\beta > 0$ be arbitrary. Suppose that $X^\eta \leqslant Y \leqslant X$, and that $Y/(\log X)^\beta \leqslant Q \leqslant Y$. Then

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

Remark. If $\eta = 1$, this is essentially the classical Barban–Davenport–Halberstam theorem. See for example [Dav80, p. 196]. The best results known are due to Languasco *et al.* [LPZ10], who show that, for any $\epsilon > 0$, Conjecture 2 holds unconditionally for $\eta = 7/12 + \epsilon$ and for $\eta = 1/2 + \epsilon$ under the generalized Riemann hypothesis. For our application, we essentially need $\eta = 1/2 - \epsilon$.

Theorem 3. *Let $\gamma > 0$, and assume that Conjecture 2 holds with*

$$\eta = \frac{1}{2} - (\gamma + 2)\frac{\log\log N}{\log N}.$$

Suppose further that $A, B \geqslant \sqrt{N}(\log N)^{1+\gamma} \log\log N$ and that $AB \geqslant N^{3/2}(\log N)^{2+\gamma} \log\log N$. Then, for any odd integer N, we have

$$\frac{1}{\#\mathscr{C}(A, B)} \sum_{E \in \mathscr{C}(A,B)} M_E(N) = K(N)\frac{N}{\varphi(N)\log N} + O\left(\frac{1}{(\log N)^{1+\gamma}}\right),$$

where

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

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

Remark. We note that $K(N)$ is uniformly bounded as a function of N. We also note that $N/\varphi(N) \ll \log\log N$ (see [HW79, Theorem 328] for example), which gives the upper bound of Theorem 1. Working with V. Chandee and D. Koukoulopoulos, the authors have recently shown that the upper bound implicit in Theorem 3 holds unconditionally. That is, Theorem 1 holds with $\log\log N$ replaced by $N/\varphi(N)$.

The average of Theorem 3 displays some interesting characteristics that are not present in the average order (5). In particular, the main term of the average in Theorem 3 does not depend solely on the size of the integer N but also on some arithmetic properties of N as it involves the factor $K(N)N/\varphi(N)$. The occurrence of the weight $\varphi(N)$ appearing in the denominator seems

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

to suggest that this is another example of the Cohen–Lenstra heuristics [CL84a, CL84b], which predict that random groups G occur with probability weighted by $1/\#\mathrm{Aut}(G)$. Notice that if as an additive group $E(\mathbb{F}_p) \simeq \mathbb{Z}/N\mathbb{Z}$, then $\#\mathrm{Aut}(E(\mathbb{F}_p)) = \varphi(N)$. Indeed, the Cohen–Lenstra heuristics predict that, relative to other groups of same size, the cyclic groups are the most likely to occur since they have the fewest number of automorphisms.

In some recent work, the authors explored this connection further by considering the average of

$$M_E(G) := \#\{p : E(\mathbb{F}_p) \simeq G\}$$

for those Abelian groups G which may arise as the group of $\mathbb{F}_p$-rational points of an elliptic curve. This is the subject of paper [DS12]. Given an elliptic curve E, it is well known that

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z},$$

for some positive integers N_1, N_2 satisfying the Hasse bound: $|p+1-N_1^2N_2| \leqslant 2\sqrt{p}$. Under Conjecture 2, it is shown in [DS12] that, for every odd order group $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$, we have that

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

provided that A, B, and the exponent of G (the size of the largest cyclic subgroup) are large enough with respect to $\#G = N_1^2N_2$. The function $K(G)$ is explicitly computed and shown to be non-zero and absolutely bounded as a function of G.

We can express the results of Theorem 3 as stating that, for a 'random curve' $E/\mathbb{Q}$ and a 'random prime' $p \in (N^-, N^+)$,

$$\mathrm{Prob}(\#E(\mathbb{F}_p) = N) \approx \frac{K(N)(N/\varphi(N)\log(N))}{4\sqrt{N}/\log N} = \frac{K(N)N}{\varphi(N)} \frac{1}{4\sqrt{N}},$$

refining the naïve model given by (3). Here, as in (3), we make the assumption that there are about $4\sqrt{N}/\log N$ primes in the interval (N^-, N^+) though we cannot justify such an assumption even under the Riemann hypothesis.

There are many open conjectures about the distributions of invariants associated with the reductions of a fixed elliptic curve over the finite fields $\mathbb{F}_p$ such as the famous conjectures of Koblitz [Kob88] and of Lang and Trotter [LT76]. 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 K.

These conjectures are all completely open. To gain evidence, it is natural to consider the averages for these conjectures over some family of elliptic curves. This has been done by various authors originating with the work of Fouvry and Murty [FR96] for the number of supersingular primes (i.e., the fixed trace Lang–Trotter conjecture for $t = 0$). See [BBIJ05, CFJKP11, DP99, DP04, Jam04, JS11] for other averages regarding the fixed trace Lang–Trotter conjecture. The average order for the Koblitz conjecture was considered in [BCD11]. Very recently, the average has been successfully carried out for the Lang–Trotter conjecture on Frobenius fields [CIJ]. The average order that we consider in this paper displays a very different character than the above averages. This is primarily because the size of primes considered varies with the parameter N.

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

Moreover, they all must lie in a very short interval. This necessitates the use of a short-interval version of the Barban–Davenport–Halberstam theorem (Conjecture 2 above). This is also the first time that one observes a Cohen–Lenstra phenomenon governing the distribution of the average.

3. Reduction to an average of class numbers

Given a (not necessarily fundamental) discriminant $D<0$, we follow Lenstra [Len87] in defining the *Kronecker class number* of discriminant D by

$$H(D) := \sum_{\substack{f^2|D \\ D/f^2\equiv 0,1 \pmod 4}} \frac{h(D/f^2)}{w(D/f^2)}, \tag{6}$$

where $h(d)$ denotes the (ordinary) class number of the unique imaginary quadratic order of discriminant $d<0$ and $w(d)$ denotes the cardinality of its unit group.

Theorem 4 (Deuring). *Let $p>3$ be a prime and t an integer such that $t^2-4p<0$. Then*

$$\sum_{\substack{\tilde{E}/\mathbb{F}_p \\ a_p(\tilde{E})=t}} \frac{1}{\#\mathrm{Aut}(\tilde{E})} = H(t^2-4p),$$

where the sum is over the $\mathbb{F}_p$-isomorphism classes of elliptic curves.

Proof. See [Len87, p. 654]. □

The first step in computing the average order of $M_E(N)$ over $\mathscr{C}(A,B)$ is to reduce to an average of class numbers by using Deuring's theorem. The following estimate will then be crucial to obtain the upper bound of Theorem 1, and is also used in getting an optimal average length in Theorem 3.

Proposition 5. *For primes p in the range $N^-<p<N^+$, we define the quadratic polynomial*

$$D_N(p) := (p+1-N)^2-4p = p^2-2(N+1)p+(N-1)^2. \tag{7}$$

Then

$$\sum_{N^-<p<N^+} H(D_N(p)) \ll \frac{N\log\log N}{\log N}. \tag{8}$$

Before giving the proof of this result, we define some notation that we will use throughout the remainder of the article. Given a negative discriminant d, we write χ_d for the Kronecker symbol $(d/\cdot)$. Since d is not a perfect square, the Dirichlet L-series defined by

$$L(s,\chi_d) := \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s}$$

converges at $s=1$. Finally, given a positive integer f, we let

$$d_{N,f}(p) := \frac{D_N(p)}{f^2}, \tag{9}$$

where $D_N(p)$ is defined by (7).

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

Proof of Proposition 5. The definition of the Kronecker class number (6) and the class number formula [IK04, p. 515]

$$\frac{h(d)}{w(d)} = \frac{\sqrt{|d|}}{2\pi} L(1, \chi_d) \tag{10}$$

give us the identity

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

Since $|D_N(p)| \leqslant 4N$, this yields

$$\sum_{N^-<p<N^+} H(D_N(p)) \ll \sqrt{N} \sum_{N^-<p<N^+} \sum_{\substack{f^2 | D_N(p) \\ D_N(p)/f^2 \equiv 0,1 \pmod 4}} \frac{L(1, \chi_{d_{N,f}(p)})}{f}. \tag{11}$$

In order to obtain an optimal bound for this expression, we will use the fact that, for almost all primitive Dirichlet characters ψ, $L(1, \psi)$ is well approximated by a very short Euler product. More precisely, fix any integer $\alpha \geqslant 1$. Then, by [GS03, Proposition 2.2], we know that

$$L(1, \psi) = \prod_{\ell \leqslant (\log Q)^\alpha} \left(1 - \frac{\psi(\ell)}{\ell}\right)^{-1} (1 + \underline{o}(1)) \tag{12}$$

for all but at most $Q^{2/\alpha + 5 \log\log\log Q / \log\log Q}$ of the primitive characters of conductor less than Q. We remark that this gives a good upper bound for $L(1, \chi)$ whenever χ is a Dirichlet character modulo $q \leqslant Q$ which is induced by a primitive character ψ satisfying (12). Indeed, let χ be such a Dirichlet character, and let ψ be the primitive character that induces χ. Then by (12), we have

$$\begin{aligned}
L(1, \chi) &= \prod_{\ell | q} \left(1 - \frac{\psi(\ell)}{\ell}\right) \prod_{\ell \leqslant (\log Q)^\alpha} \left(1 - \frac{\psi(\ell)}{\ell}\right)^{-1} (1 + \underline{o}(1)) \\
&= \prod_{\substack{\ell | q \\ \ell > (\log Q)^\alpha}} \left(1 - \frac{\psi(\ell)}{\ell}\right) \prod_{\ell \leqslant (\log Q)^\alpha} \left(1 - \frac{\chi(\ell)}{\ell}\right)^{-1} (1 + \underline{o}(1)) \\
&\ll \prod_{\substack{\ell | q \\ \ell > (\log Q)^\alpha}} \left(1 + \frac{1}{\ell}\right) \prod_{\ell \leqslant (\log Q)^\alpha} \left(1 - \frac{1}{\ell}\right)^{-1} \\
&\ll \prod_{\substack{\ell | q \\ \ell > (\log Q)^\alpha}} \left(1 + \frac{1}{\ell}\right) \log\log Q,
\end{aligned}$$

where the last line follows by Mertens' formula [IK04, p. 34] since α is fixed. For the remaining product, we observe that

$$\prod_{\substack{\ell | q \\ \ell > (\log Q)^\alpha}} \left(1 + \frac{1}{\ell}\right) \leqslant \exp\left\{ \sum_{\substack{\ell | q \\ \ell > (\log Q)^\alpha}} \frac{1}{\ell} \right\} \leqslant \exp\left\{ \frac{\omega(q)}{(\log Q)^\alpha} \right\} \leqslant \exp\left\{ \frac{(\log q)^{1-\alpha}}{\log 2} \right\},$$

where $\omega(q)$ denotes the number of distinct prime factors of q. Therefore, since $\alpha \geqslant 1$, we may conclude that if χ is a character of modulus $q \leqslant Q$ and (12) holds for the primitive character

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

inducing χ, then

$$L(1,\chi) \ll \log\log Q. \tag{13}$$

We make use of this fact in (11) as follows. Let $d_N^*(p)$ be the discriminant of the imaginary quadratic field $\mathbb{Q}(\sqrt{D_N(p)})$. Then $d_N^*(p)$ is a fundamental discriminant, and $\chi_{d_N^*(p)}$ is the primitive character inducing every character of the set $\{\chi_{d_{N,f}(p)} : f^2 \mid D_N(p)\}$. Furthermore, $|d_N^*(p)|$ is the conductor of each of these characters, and $3 \leqslant |d_N^*(p)| \leqslant 4N$. Now fix some $\alpha > 100$, and let $\mathscr{E}(Q)$ be the set of primitive characters of conductor less than or equal to Q for which (12) does not hold. Then $\#\mathscr{E}(4N) \ll N^{1/50}$. We now divide the outer sum over p on the right-hand side of (11) according to whether or not the primitive character $\chi_{d_N^*(p)}$ is in the exceptional set $\mathscr{E}(4N)$. For those p for which $\chi_{d_N^*(p)}$ is not exceptional, we use (13), writing

$$\sum_{\substack{N^-<p<N^+\\ \chi_{d_N^*(p)}\notin\mathscr{E}(4N)}} \sum_{\substack{f^2\mid D_N(p)\\ D_N(p)/f^2\equiv 0,1 \pmod 4}} \frac{L(1,\chi_{d_{N,f}(p)})}{f} \ll \log\log N \sum_{f\leqslant 2\sqrt{N}} \frac{1}{f} \sum_{\substack{N^-<p<N^+\\ f^2\mid D_N(p)}} 1.$$

To bound the sum over p, we apply the Brun–Titchmarsh inequality [IK04, p. 167], which gives that

$$\#\{N^- < p < N^+ : p \equiv a \pmod f\} \ll \frac{\sqrt{N}}{\varphi(f)\log(4\sqrt{N}/f)}.$$

For the sum over a, we use the bound

$$\#\{a \in \mathbb{Z}/f\mathbb{Z} : D_N(a) \equiv 0 \pmod f\} \ll \sqrt{f},$$

which is Lemma 12 of § 7. Combining these two estimates, we have that

$$\begin{aligned}\sum_{\substack{N^-<p<N^+\\ \chi_{d_N^*(p)}\notin\mathscr{E}(4N)}} \sum_{\substack{f^2\mid D_N(p)\\ D_N(p)/f^2\equiv 0,1 \pmod 4}} \frac{L(1,\chi_{d_{N,f}(p)})}{f} &\ll \frac{\sqrt{N}\log\log N}{\log N} \sum_{f\geqslant 1} \frac{\log f}{f^{1/2}\varphi(f)}\\ &\ll \frac{\sqrt{N}\log\log N}{\log N}.\end{aligned} \tag{14}$$

It remains to estimate the sum over primes p such that $\chi_{d_N^*(p)} \in \mathscr{E}(4N)$. In that case, we simply need the standard bound

$$L(1,\chi) \ll \log q,$$

which is valid for all Dirichlet characters of conductor q (see [Dav80, p. 96] for example). We note that

$$\#\{N^- < p < N^+ : \chi_{d_N^*(p)} \in \mathscr{E}(4N)\} \leqslant \#\mathscr{E}(4N)\tau(4N),$$

where $\tau(n)$ denotes the number of positive divisors of n. Therefore, we obtain the bound

$$\begin{aligned}\sum_{\substack{N^-<p<N^+\\ \chi_{d_N^*(p)}\in\mathscr{E}(4N)}} \sum_{\substack{f^2\mid D_N(p)\\ D_N(p)/f^2\equiv 0,1 \pmod 4}} \frac{L(1,\chi_{d_{N,f}(p)})}{f} &\ll \log N \sum_{\substack{N^-<p<N^+\\ \chi_{d_N^*(p)}\in\mathscr{E}(4N)}} \sum_{f^2\mid D_N(p)} \frac{1}{f}\\ &\ll N^{1/50+\varepsilon}\end{aligned} \tag{15}$$

for any $\varepsilon > 0$. Combining (11), (14), and (15) completes the proof of Proposition 5. □

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

Proposition 6. *Let $D_N(p)$ be as defined by (7). Then*

$$\frac{1}{\#\mathscr{C}(A,B)}\sum_{E\in\mathscr{C}(A,B)} M_E(N) = \sum_{N^-<p<N^+}\frac{H(D_N(p))}{p} + \mathcal{E}(N;A,B),$$

where

$$\mathcal{E}(N;A,B) \ll \frac{\log\log N}{N\log N} + \left(\frac{1}{A}+\frac{1}{B}\right)\sqrt{N}\log\log N + \frac{N^{3/2}\log N\log\log N}{AB}$$

uniformly for $A, B > 0$.

Remark. The above holds without assuming that N is odd.

Proof of Proposition 6. First, we write $M_E(N)$ as a sum over primes and interchange sums to obtain

$$\frac{1}{\#\mathscr{C}(A,B)}\sum_{E\in\mathscr{C}(A,B)} M_E(N) = \frac{1}{\#\mathscr{C}(A,B)}\sum_{N^-<p<N^+}\sum_{\substack{E\in\mathscr{C}(A,B)\\ \#E_p(\mathbb{F}_p)=N}} 1.$$

For each prime p, we group the $E\in\mathscr{C}(A,B)$ according to which isomorphism class they reduce modulo p, writing

$$\sum_{\substack{E\in\mathscr{C}(A,B)\\ \#E_p(\mathbb{F}_p)=N}} 1 = \sum_{\substack{\tilde{E}/\mathbb{F}_p\\ \#\tilde{E}(\mathbb{F}_p)=N}} \#\{E\in\mathscr{C}(A,B) : E_p\cong\tilde{E}\}.$$

For N large enough ($N\geqslant 8$), the primes 2 and 3 will not enter into the sum over p. Thus, we will assume that $p>3$ throughout the remainder of the article. Therefore, given an elliptic curve defined over $\mathbb{F}_p$, we may associate a Weierstrass equation, say $E_{s,t}: y^2 = x^3+sx+t$ with $s,t\in\mathbb{F}_p$. Using a character sum argument as in [FR96, pp. 93–95], we have

$$\begin{aligned}\#\{E\in\mathscr{C}(A,B) : E_p\cong E_{s,t}\} = \frac{4AB}{\#\mathrm{Aut}(E_{s,t})p} &+ O\left(\frac{AB}{p^2}+\sqrt{p}(\log p)^2\right)\\ &+\begin{cases} O\left(\dfrac{A\log p}{\sqrt{p}}+\dfrac{B\log p}{\sqrt{p}}\right) & \text{if } st\neq 0,\\ O\left(\dfrac{A\log p}{\sqrt{p}}+B\log p\right) & \text{if } s=0,\\ O\left(A\log p+\dfrac{B\log p}{\sqrt{p}}\right) & \text{if } t=0.\end{cases}\end{aligned}$$

Here $\mathrm{Aut}(E_{s,t})$ denotes the size of the automorphism group of $E_{s,t}$ over $\mathbb{F}_p$. Substituting this estimate and applying Theorem 4, we find that

$$\frac{1}{\#\mathscr{C}(A,B)}\sum_{E\in\mathscr{C}(A,B)} M_E(N) = \sum_{N^-<p<N^+}\frac{H(D_N(p))}{p} + \mathcal{E}(N;A,B),$$

where

$$\begin{aligned}\mathcal{E}(N;A,B) \ll \left\{\frac{1}{N^2}+\frac{\log N}{\sqrt{N}}\left(\frac{1}{A}+\frac{1}{B}\right)+\frac{\sqrt{N}(\log N)^2}{AB}\right\}\sum_{N^-<p<N^+}H(D_N(p))\\ +\left(\frac{1}{A}+\frac{1}{B}\right)\log N\sum_{N^-<p<N^+}1.\end{aligned}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

In estimating the error, we have used the facts that $\#\mathscr{C}(A,B) = 4AB + O(A+B)$, $p = N + O(\sqrt{N})$ for every prime p in the interval (N^-, N^+), and there are at most 10 isomorphism classes $E_{s,t}$ over $\mathbb{F}_p$ with $st = 0$. The result now follows by applying Proposition 5 and the upper bound $\{N^- < p < N^+\} \ll \sqrt{N}/\log N$. □

Theorem 1 now follows immediately upon combining Propositions 5 and 6, and noting again that $p = N + O(\sqrt{N})$ for every prime p in the interval (N^-, N^+). Furthermore, we have reduced the proof of Theorem 3 to computing the sum

$$\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p}.$$

This computation requires several intermediate results. Therefore, we delay it until § 6.

4. A short average of special values of Dirichlet L-functions

Since Theorem 3 holds only for odd N, we assume for the the remainder of the article that N is an odd integer except during the proof of Lemma 12. Recall that Lemma 12 was used in the proof of Proposition 5, which holds for all positive integers N.

In this section, we prove a short-average result for special values of Dirichlet L-functions that is needed to compute our average over elliptic curves. As the average is very short, we need the equivalent of the Barban–Davenport–Halberstam theorem to hold for intervals of that size.

Theorem 7. *Let $\gamma > 0$. Suppose that $N^- \leqslant X < X + Y \leqslant N^+$ with $Y \gg \sqrt{N}/(\log N)^{\upsilon}$ for some choice of $\upsilon \geqslant 0$. Assume that Conjecture 2 holds for intervals of length Y. Then, for odd integers N,*

$$\sum_{\substack{f \leqslant 2\sqrt{X+Y} \\ (f,2)=1}} \frac{1}{f} \sum_{\substack{X < p \leqslant X+Y \\ f^2 \mid D_N(p)}} L(1, \chi_{d_{N,f}(p)}) \log p = K_0(N)Y + O\left(\frac{Y}{(\log N)^{\gamma}}\right),$$

where

$$K_0(N) := \sum_{\substack{f=1 \\ (f,2)=1}}^{\infty} \frac{1}{f} \sum_{n=1}^{\infty} \frac{1}{n\varphi(4nf^2)} \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ a \equiv 1 \pmod 4}} \left(\frac{a}{n}\right) \#C_N(a,n,f), \tag{16}$$

and

$$C_N(a,n,f) := \{z \in (\mathbb{Z}/4nf^2\mathbb{Z})^* : D_N(z) \equiv af^2 \pmod{4nf^2}\}. \tag{17}$$

Proof. Let U be a real parameter to be determined. Using partial summation and Burgess' bound for character sums [Bur63, Theorem 2] to bound the tail of the L-series, we have

$$L(1, \chi_{d_{N,f}(p)}) = \sum_{n \geqslant 1} \left(\frac{d_{N,f}(p)}{n}\right) \frac{1}{n} = \sum_{n \leqslant U} \left(\frac{d_{N,f}(p)}{n}\right) \frac{1}{n} + O\left(\frac{|d_{N,f}(p)|^{7/32}}{\sqrt{U}}\right).$$

For $N^- < p < N^+$, we have $|d_{N,f}(p)| \leqslant 4N/f^2$, and hence

$$\sum_{\substack{f \leqslant 2\sqrt{X+Y} \\ (f,2)=1}} \frac{1}{f} \sum_{\substack{X < p \leqslant X+Y \\ f^2 \mid D_N(p)}} \log p \sum_{n > U} \frac{1}{n} \left(\frac{d_{N,f}(p)}{n}\right) \ll \frac{YN^{7/32}}{\sqrt{U}}.$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

Now let V be a real parameter to be determined. Using Lemma 12, we obtain

$$\begin{aligned}
&\sum_{\substack{V<f\leqslant 2\sqrt{X+Y}\\(f,2)=1}}\frac{1}{f}\sum_{n\leqslant U}\frac{1}{n}\sum_{\substack{X<p\leqslant X+Y\\f^2\mid D_N(p)}}\left(\frac{d_{N,f}(p)}{n}\right)\log p\\
&\ll \log U\log N\sum_{\substack{V<f\leqslant 2\sqrt{X+Y}\\(f,2)=1}}\frac{1}{f}\sum_{\substack{X<k\leqslant X+4\sqrt{N}\\f\mid D_N(p)}}1\\
&\ll \log U\log N\sum_{\substack{V<f\leqslant 2\sqrt{X+Y}\\(f,2)=1}}\frac{\sqrt{N}\#\{z\in\mathbb{Z}/f\mathbb{Z}:D_N(z)\equiv 0\pmod f\}}{f^2}\\
&\ll \sqrt{N}\log U\log N\sum_{f>V}\frac{1}{f^{3/2}}\\
&\ll \frac{\sqrt{N}\log U\log N}{\sqrt{V}},
\end{aligned}$$

and, therefore,

$$\begin{aligned}
\sum_{\substack{f\leqslant 2\sqrt{X+Y}\\(f,2)=1}}\frac{1}{f}\sum_{\substack{X<p\leqslant X+Y\\f^2\mid D_N(p)}}L(1,\chi_{d_{N,f}(p)})\log p=&\sum_{\substack{f\leqslant V\\(f,2)=1}}\frac{1}{f}\sum_{n\leqslant U}\frac{1}{n}\sum_{\substack{X<p\leqslant X+Y\\f^2\mid D_N(p)}}\left(\frac{d_{N,f}(p)}{n}\right)\log p\\
&+O\left(\frac{YN^{7/32}}{\sqrt{U}}+\frac{\sqrt{N}\log U\log N}{\sqrt{V}}\right).
\end{aligned}$$

With $C_N(a,n,f)$ as defined by (17), we regroup terms on the right-hand side above, writing

$$\begin{aligned}
&\sum_{\substack{f\leqslant V,n\leqslant U\\(f,2)=1}}\frac{1}{fn}\sum_{\substack{X<p\leqslant X+Y\\f^2\mid D_N(p)}}\left(\frac{d_{N,f}(p)}{n}\right)\log p\\
&=\sum_{\substack{f\leqslant V,n\leqslant U\\(f,2)=1}}\frac{1}{fn}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\a\equiv 1\pmod 4}}\left(\frac{a}{n}\right)\sum_{b\in C_N(a,n,f)}\theta(X,Y;4nf^2,b)\\
&\quad+O\left(\sum_{\substack{f\leqslant V,n\leqslant U\\(f,2)=1}}\frac{1}{fn}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\a\equiv 1\pmod 4}}\left(\frac{a}{n}\right)\sum_{\substack{X<p\leqslant X+Y\\f^2\mid D_N(p)\\D_N(p)\equiv af^2\\p\mid 4nf^2}}\log p\right).
\end{aligned}$$

If p satisfies the congruence $D_N(p)\equiv af^2\pmod{4nf^2}$ and p divides $4nf^2$, then p divides $(4nf^2,(N-1)^2-af^2)$. It follows that such a p must divide $n(N-1)$. Hence, the error term

$$\sum_{\substack{f\leqslant V,n\leqslant U\\(f,2)=1}}\frac{1}{fn}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\a\equiv 1\pmod 4}}\left(\frac{a}{n}\right)\sum_{\substack{X<p\leqslant X+Y\\f^2\mid D_N(p)\\D_N(p)\equiv af^2\\p\mid 4nf^2}}\log p\ll U\log N\log V+U\log U\log V,$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

and

$$\sum_{\substack{f\leqslant 2\sqrt{X+Y}\\(f,2)=1}}\frac{1}{f}\sum_{\substack{X<p\leqslant X+Y\\f^2\mid D_N(p)}}L(1,\chi_{d_{N,f}(p)})\log p$$
$$=\sum_{\substack{f\leqslant V,n\leqslant U\\(f,2)=1}}\frac{1}{fn}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\a\equiv 1\pmod 4}}\left(\frac{a}{n}\right)\sum_{b\in C_N(a,n,f)}\theta(X,Y;4nf^2,b)$$
$$+O\left(\frac{YN^{7/32}}{\sqrt{U}}+\frac{\sqrt{N}\log U\log N}{\sqrt{V}}+U\log(UN)\log V\right).$$

We approximate $\theta(X,Y;4nf^2,b)$ by $Y/\varphi(4nf^2)$, incurring an error of

$$\sum_{\substack{f\leqslant V,n\leqslant U\\(f,2)=1}}\frac{1}{fn}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\a\equiv 1\pmod 4}}\left(\frac{a}{n}\right)\sum_{b\in C_N(a,n,f)}E(X,Y;4nf^2,b). \tag{18}$$

For any given value of $b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*$, there is at most one value of $a\in\mathbb{Z}/4n\mathbb{Z}$ satisfying the congruence $D_N(b)\equiv af^2 \pmod{4nf^2}$. Hence, interchanging the two inner sums shows that

$$\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\a\equiv 1\pmod 4}}\left(\frac{a}{n}\right)\sum_{b\in C_N(a,n,f)}E(X,Y;4nf^2,b)\ll\sum_{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*}|E(X,Y;4nf^2,b)|.$$

By Cauchy–Schwarz, the error term (18) is

$$\ll\sum_{f\leqslant V}\frac{1}{f}\sum_{n\leqslant U}\frac{1}{n}\sum_{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*}|E(X,Y;4nf^2,b)|$$
$$\leqslant\sum_{f\leqslant V}\frac{1}{f}\left[\sum_{n\leqslant U}\frac{\varphi(4nf^2)}{n^2}\right]^{1/2}\left[\sum_{n\leqslant U}\sum_{b\in(\mathbb{Z}/4nf^2\mathbb{Z})^*}|E(X,Y;4nf^2,b)|^2\right]^{1/2}$$
$$\ll V\sqrt{\log U}\left[\sum_{q\leqslant 4UV^2}\sum_{\substack{a=1\\(a,q)=1}}^{q}|E(X,Y;q,a)|^2\right]^{1/2}.$$

Assuming Conjecture 2 for an appropriate value of η, we obtain the bound

$$V\sqrt{\log U}\left[\sum_{q\leqslant 4UV^2}\sum_{\substack{a=1\\(a,q)=1}}^{q}|E(X,Y;q,a)|^2\right]^{1/2}\ll\frac{YV\sqrt{\log U\log N}}{(\log N)^{2\upsilon+3\gamma+5}}$$

whenever

$$UV^2\leqslant\frac{Y}{(\log N)^{4\upsilon+6\gamma+10}}. \tag{19}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

Thus, we have

$$\begin{aligned}&\sum_{\substack{f\leqslant 2\sqrt{X+Y}\\(f,2)=1}}\frac{1}{f}\sum_{\substack{X<p\leqslant X+Y\\f^2\mid D_N(p)}}L(1,\chi_{d_{N,f}(p)})\log p\\&\quad=Y\sum_{\substack{f\leqslant V,n\leqslant U\\(f,2)=1}}\frac{1}{fn\varphi(4nf^2)}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\a\equiv 1 \pmod 4}}\left(\frac{a}{n}\right)\#C_N(a,n,f)\\&\qquad+O\left(\frac{YN^{7/32}}{\sqrt{U}}+\frac{\sqrt{N}\log U\log N}{\sqrt{V}}+U\log(UN)\log V\right)\\&\qquad+O\left(\frac{YV\sqrt{\log U\log N}}{(\log N)^{2\upsilon+3\gamma+5}}\right).\end{aligned}$$

Lemma 8. *For any $U,V,\epsilon>0$, we have*

$$K_0(N)=\sum_{\substack{f\leqslant V,n\leqslant U\\(f,2)=1}}\frac{1}{fn\varphi(4nf^2)}\sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\a\equiv 1 \pmod 4}}\left(\frac{a}{n}\right)\#C_N(a,n,f)+O\left(\frac{N^{\epsilon}}{\sqrt{U}}+\frac{\log\log N}{V}\right).$$

We delay the proof of Lemma 8 until § 7. Applying the lemma and choosing

$$U=\frac{Y}{(\log N)^{4\upsilon+10\gamma+18}},\quad V=(\log N)^{2\upsilon+2\gamma+4},$$

we have

$$\sum_{\substack{f\leqslant 2\sqrt{X+Y}\\(f,2)=1}}\frac{1}{f}\sum_{\substack{X<p\leqslant X+Y\\f^2\mid D_N(p)}}L(1,\chi_{d_{N,f}(p)})\log p=K_0(N)Y+O\left(\frac{Y}{(\log N)^{\gamma}}\right)$$

provided that $Y\gg\sqrt{N}/(\log N)^{\upsilon}$. Note that our choice of U,V satisfies the condition (19). □

5. Computing the 'almost constant'

Recall that $C_N(a,n,f)$ was defined by

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

where $D_N(z)=z^2-2(N+1)z+(N-1)^2$. The following is the main result of this section.

Proposition 9. *With $K(N)$ as defined in Theorem 3 and $K_0(N)$ as defined in Theorem 7, we have*

$$\frac{N}{\varphi(N)}K(N)=K_0(N).$$

Proof. By the Chinese remainder theorem and the definition of $C_N(a,n,f)$,

$$\#C_N(a,n,f)=\prod_{\ell\mid 4nf^2}\#C_N^{(\ell)}(a,n,f),$$

where

$$C_N^{(\ell)}(a,n,f):=\{z\in(\mathbb{Z}/\ell^{\nu_\ell(4nf^2)}\mathbb{Z})^*:D_N(z)\equiv af^2 \pmod{\ell^{\nu_\ell(4nf^2)}}\}.\tag{20}$$

We require the following lemma, whose proof we delay until § 7.

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

Lemma 10. *Suppose that N and f are odd and that $a \equiv 1 \pmod 4$. Let ℓ be any odd prime dividing nf, and let $e = \nu_\ell(4nf^2) = \nu_\ell(nf^2)$. If $\ell \nmid 4N + af^2$, then*

$$\#C_N^{(\ell)}(a,n,f) = \begin{cases} 1 + \left(\dfrac{4N+af^2}{\ell}\right) & \text{if } \ell \nmid (N-1)^2 - af^2, \\ 1 & \text{if } \ell \mid (N-1)^2 - af^2. \end{cases}$$

If $\ell \mid 4N + af^2$, then, with $s = \nu_\ell(4N+af^2)$, we have

$$\#C_N^{(\ell)}(a,n,f) = \begin{cases} 2\left(\dfrac{N+1}{\ell}\right)^2 \ell^{s/2} & \text{if } 1 \leqslant s < e,\ 2 \mid s,\ \text{and } \left(\dfrac{(4N+af^2)/\ell^s}{\ell}\right) = 1, \\ \left(\dfrac{N+1}{\ell}\right)^2 \ell^{\lfloor e/2 \rfloor} & \text{if } s \geqslant e, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, if $\ell \mid f$, then

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

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

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

By Lemma 10, we may write

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

where

$$\mathcal{S}_2(n,a) := \begin{cases} 1 & \text{if } 2 \nmid n, \\ 2 & \text{if } 2 \mid n \text{ and } a \equiv 5 \pmod 8, \\ 0 & \text{otherwise.} \end{cases} \tag{21}$$

Note that if ℓ is a prime dividing f and not dividing n, then $af^2 \equiv 0 \pmod{\ell^{\nu_\ell(4nf^2)}}$ as $\nu_\ell(4nf^2) = \nu_\ell(f^2)$. Hence, in this case, $\#C_N^{(\ell)}(a,n,f)$ does not depend on the value of a, and so we write $\#C_N^{(\ell)}(a,n,f) = \#C_N^{(\ell)}(1,1,f)$ if $\ell \mid f$ and $\ell \nmid n$. Therefore, letting n' denote the odd part of n and

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

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

we may write

$$\begin{aligned} K_0(N) &= \sum_{\substack{f=1\\(f,2)=1}}^{\infty} \frac{1}{f} \sum_{n=1}^{\infty} \frac{1}{n\varphi(4nf^2)} \sum_{\substack{a\in\mathbb{Z}/4n\mathbb{Z}\\ a\equiv 1 \pmod 4}} \left(\frac{a}{n}\right) \#C_N(a,n,f) \\ &= \sum_{\substack{f=1\\(f,2)=1}}^{\infty} \frac{1}{f^2\varphi(f)} \sum_{n=1}^{\infty} \frac{2\varphi((n,f))}{(n,f)n\varphi(4n)} \left[\prod_{\substack{\ell\mid f\\ \ell\nmid n}} \#C_N^{(\ell)}(1,1,f)\right] c_{N,f}(n) \\ &= \sum_{f=1}^{\infty}{}' \frac{\prod_{\ell\mid f} \#C_N^{(\ell)}(1,1,f)}{f^2\varphi(f)} \sum_{n=1}^{\infty} \frac{2\varphi((n,f))}{(n,f)n\varphi(4n)} \left[\prod_{\ell\mid (f,n)} \#C_N^{(\ell)}(1,1,f)\right]^{-1} c_{N,f}(n), \quad (22) \end{aligned}$$

where the prime on the outer sum indicates that the sum is to be restricted to those f which are odd and are not divisible by any prime for which $\#C_N^{(\ell)}(1,1,f) = 0$.

In order to proceed further, we must show how to compute the function $c_{N,f}(n)$. We summarize the computation in the following lemma, whose proof we also delay until § 7.

Lemma 11. *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 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

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

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

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

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

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. Furthermore, for any n, we have the bound

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

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

$$\kappa_m(\ell^\alpha) := \begin{cases} \ell & \text{if } 2 \nmid \alpha \text{ and } \ell \nmid m, \\ 1 & \text{otherwise.} \end{cases} \tag{23}$$

Recalling the restrictions on f in (22) and applying Lemma 11, the sum over n in (22) may be factored as

$$\begin{aligned} &\sum_{n=1}^{\infty} \frac{2\varphi((n,f))}{(n,f)n\varphi(4n)} \left[\prod_{\ell \mid (f,n)} \#C_N^{(\ell)}(1,1,f)\right]^{-1} c_{N,f}(n) \\ &\quad = \left\{\sum_{\alpha \geqslant 0} \frac{2c_{N,f}(2^\alpha)}{2^\alpha \varphi(2^{\alpha+2})}\right\} \prod_{\substack{\ell \nmid f \\ \ell \neq 2}} \left\{\sum_{\alpha \geqslant 0} \frac{c_{N,f}(\ell^\alpha)}{\ell^\alpha \varphi(\ell^\alpha)}\right\} \prod_{\ell \mid f} \left\{1 + \sum_{\alpha \geqslant 1} \frac{\varphi((\ell^\alpha, f)) c_{N,f}(\ell^\alpha)}{(\ell^\alpha, f)\ell^\alpha \varphi(\ell^\alpha) \#C_N^{(\ell)}(1,1,f)}\right\} \\ &\quad = \frac{2}{3} \prod_{\substack{\ell \nmid f \\ \ell \mid N}} F_0(\ell) \prod_{\substack{\ell \nmid f \\ \ell \nmid N \\ \ell \neq 2}} F_1(\ell) \prod_{\ell \mid f} F_2(\ell, f), \end{aligned}$$

where, for any odd prime ℓ, we make the definitions

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

Substituting this back into (22), we have

$$K_0(N) = \frac{2}{3} \prod_{\ell \mid N} F_0(\ell) \prod_{\substack{\ell \nmid N \\ \ell \neq 2}} F_1(\ell) \sideset{}{'}\sum_{\substack{f=1 \\ (f,2)=1}}^{\infty} \frac{\prod_{\ell \mid f} \#C_N^{(\ell)}(1,1,f)}{\varphi(f) f^2} \prod_{\substack{\ell \mid f \\ \ell \mid N}} \frac{F_2(\ell, f)}{F_0(\ell)} \prod_{\substack{\ell \mid f \\ \ell \nmid N}} \frac{F_2(\ell, f)}{F_1(\ell)}. \tag{24}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

The sum over f may be factored as

$$\sum_{\substack{f=1\\(f,2)=1}}^{\infty}{}' \frac{\prod_{\ell\mid f}\#C_N^{(\ell)}(1,1,f)}{\varphi(f)f^2}\prod_{\substack{\ell\mid f\\ \ell\mid N}}\frac{F_2(\ell,f)}{F_0(\ell)}\prod_{\substack{\ell\mid f\\ \ell\nmid N}}\frac{F_2(\ell,f)}{F_1(\ell)}$$
$$=\prod_{\ell\mid N}\Bigg\{1+\sum_{\alpha\geqslant 1}\frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\varphi(\ell^\alpha)\ell^{2\alpha}F_0(\ell)}\Bigg\}\prod_{\substack{\ell\nmid N\\ \ell\neq 2}}\Bigg\{1+\sum_{\alpha\geqslant 1}\frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\varphi(\ell^\alpha)\ell^{2\alpha}F_1(\ell)}\Bigg\}.$$

When $\ell\nmid 2N$, the factor simplifies as

$$\begin{aligned}1+\sum_{\alpha\geqslant 1}\frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\varphi(\ell^\alpha)\ell^{2\alpha}F_1(\ell)}&=1+\frac{\ell C_N^{(\ell)}(1,1,\ell)F_2(\ell,\ell)}{F_1(\ell)(\ell-1)}\sum_{\alpha\geqslant 1}\frac{1}{\ell^{3\alpha}}\\&=1+\frac{\left(1+\left(\frac{N(N-1)^2}{\ell}\right)\right)(\ell^2+\ell+1)}{(\ell^2-1)(\ell^3-1)F_1(\ell)}\\&=1+\frac{1+\left(\frac{N(N-1)^2}{\ell}\right)}{(\ell^2-1)(\ell-1)F_1(\ell)}.\end{aligned}$$

When $\nu_\ell(N)$ is odd, the factor simplifies as

$$\begin{aligned}1+\sum_{\alpha\geqslant 1}\frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\varphi(\ell^\alpha)\ell^{2\alpha}F_0(\ell)}&=1+\frac{\ell}{F_0(\ell)(\ell-1)}\sum_{\alpha\geqslant 1}\frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\ell^{3\alpha}}\\&=1+\frac{\ell}{F_0(\ell)(\ell-1)}\sum_{\alpha=1}^{\lfloor\nu_\ell(N)/2\rfloor}\frac{\ell^\alpha(1+1/\ell)}{\ell^{3\alpha}}\\&=1+\frac{(\ell+1)(1-\ell^{1-\nu_\ell(N)})}{F_0(\ell)(\ell-1)(\ell^2-1)}\\&=1+\frac{1-\ell^{1-\nu_\ell(N)}}{F_0(\ell)(\ell-1)^2}\\&=1+\frac{\ell^{\nu_\ell(N)}-\ell}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2}.\end{aligned}$$

When $\nu_\ell(N)$ positive, even, and $\left(\frac{N_\ell}{\ell}\right)=-1$, the factor simplifies as

$$\begin{aligned}&1+\sum_{\alpha\geqslant 1}\frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\varphi(\ell^\alpha)\ell^{2\alpha}F_0(\ell)}\\&\quad=1+\frac{\ell}{F_0(\ell)(\ell-1)}\sum_{\alpha\geqslant 1}\frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\ell^{3\alpha}}\\&\quad=1+\frac{\ell^{\nu_\ell(N)}-\ell^2}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2}+\frac{\ell\#C_N^{(\ell)}(1,1,\ell^{\nu_\ell(N)/2})F_2(\ell,\ell^{\nu_\ell(N)/2})}{F_0(\ell)(\ell-1)\ell^{3\nu_\ell(N)/2}}\end{aligned}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

$$
\begin{aligned}
&= 1 + \frac{\ell^{\nu_\ell(N)} - \ell^2}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2} + \frac{\ell^2 - \ell - \left(\frac{-1}{\ell}\right)}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2} \\
&= 1 + \frac{\ell^{\nu_\ell(N)} - \ell - \left(\frac{-1}{\ell}\right)}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2} \\
&= 1 + \frac{\ell^{\nu_\ell(N)} - \ell + \left(\frac{-N_\ell}{\ell}\right)}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2}.
\end{aligned}
$$

When $\nu_\ell(N)$ positive, even, and $\left(\frac{N_\ell}{\ell}\right) = 1$, the factor simplifies as

$$
\begin{aligned}
1 + \sum_{\alpha \geqslant 1} \frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\varphi(\ell^\alpha)\ell^{2\alpha}F_0(\ell)} &= 1 + \frac{\ell}{F_0(\ell)(\ell-1)} \sum_{\alpha \geqslant 1} \frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\ell^{3\alpha}} \\
&= 1 + \frac{\ell^{\nu_\ell(N)} - \ell}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2} + \frac{\ell \#C_N^{(\ell)}(1,1,\ell^{\nu_\ell(N)/2})F_2(\ell,\ell^{\nu_\ell(N)/2})}{F_0(\ell)(\ell-1)\ell^{3\nu_\ell(N)/2}} \\
&\quad + \frac{\ell}{F_0(\ell)(\ell-1)} \sum_{\alpha=\nu_\ell(N)/2+1}^{\infty} \frac{\#C_N^{(\ell)}(1,1,\ell^\alpha)F_2(\ell,\ell^\alpha)}{\ell^{3\alpha}} \\
&= 1 + \frac{\ell^{\nu_\ell(N)} - \ell^2}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2} + \frac{\ell(\ell^2-1) + \left(\frac{-1}{\ell}\right)\ell + \left(\frac{-1}{\ell}\right) - 2}{F_0(\ell)(\ell-1)(\ell^2-1)\ell^{\nu_\ell(N)}} \\
&\quad + \frac{\ell}{F_0(\ell)(\ell-1)} \sum_{\alpha=\nu_\ell(N)/2+1}^{\infty} \frac{2\ell^{\nu_\ell(N)/2}(1 + 1/\ell(\ell+1))}{\ell^{3\alpha}} \\
&= 1 + \frac{\ell^{\nu_\ell(N)} - \ell^2}{F_0(\ell)\ell^{\nu_\ell(N)}(\ell-1)^2} + \frac{\ell^2 - \ell + \left(\frac{-1}{\ell}\right)}{F_0(\ell)(\ell-1)^2\ell^{\nu_\ell(N)}} \\
&= 1 + \frac{\ell^{\nu_\ell(N)} - \ell + \left(\frac{-N_\ell}{\ell}\right)}{F_0(\ell)(\ell-1)^2\ell^{\nu_\ell(N)}}.
\end{aligned}
$$

Substituting this back into (24), we find that

$$
\begin{aligned}
K_0(N) &= \frac{2}{3} \prod_{\ell \nmid 2N} \left(F_1(\ell) + \frac{1 + \left(\frac{N(N-1)^2}{\ell}\right)}{(\ell^2-1)(\ell-1)} \right) \prod_{\substack{\ell \mid N \\ 2 \nmid \nu_\ell(N)}} \left(F_0(\ell) + \frac{(\ell^{\nu_\ell(N)} - \ell)}{\ell^{\nu_\ell(N)}(\ell-1)^2} \right) \\
&\quad \times \prod_{\substack{\ell \mid N \\ 2 \mid \nu_\ell(N)}} \left(F_0(\ell) + \frac{\ell^{\nu_\ell(N)} - \ell + \left(\frac{-N_\ell}{\ell}\right)}{\ell^{\nu_\ell(N)}(\ell-1)^2} \right) \\
&= \frac{2}{3} \prod_{\ell \nmid 2N} \left(1 - \frac{\left(\frac{N-1}{\ell}\right)^2 \left[\ell + 1 - \left(\frac{N}{\ell}\right)\right] + \left(\frac{N}{\ell}\right)}{(\ell-1)(\ell^2-1)} \right) \prod_{\substack{\ell \mid N \\ 2 \nmid \nu_\ell(N)}} \left(1 + \frac{\ell^{\nu_\ell(N)+1} - \ell^{\nu_\ell(N)} - \ell}{\ell^{\nu_\ell(N)}(\ell-1)^2} \right) \\
&\quad \times \prod_{\substack{\ell \mid N \\ 2 \mid \nu_\ell(N)}} \left(1 + \frac{\ell^{\nu_\ell(N)+1} - \ell^{\nu_\ell(N)} - \ell + \left(\frac{-N_\ell}{\ell}\right)}{\ell^{\nu_\ell(N)}(\ell-1)^2} \right)
\end{aligned}
$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

$$= \frac{N}{\varphi(N)} \prod_{\ell \nmid N} \left(1 - \frac{\left(\frac{N-1}{\ell}\right)^2 \ell + 1}{(\ell-1)(\ell^2-1)}\right) \prod_{\substack{\ell \mid N \\ 2 \nmid \nu_\ell(N)}} \left(1 - \frac{1}{\ell^{\nu_\ell(N)}(\ell-1)}\right)$$

$$\times \prod_{\substack{\ell \mid N \\ 2 \mid \nu_\ell(N)}} \left(1 - \frac{\ell - \left(\frac{-N_\ell}{\ell}\right)}{\ell^{\nu_\ell(N)+1}(\ell-1)}\right). \qquad \square$$

6. Proof of Theorem 3

We are now ready to give the proof of our main result.

Proof of Theorem 3. By Proposition 6, we see that Theorem 3 follows if we show that

$$\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} = K(N) \frac{N}{\varphi(N) \log N} + O\left(\frac{1}{(\log N)^{1+\gamma}}\right).$$

We begin by dividing the interval (N^-, N^+) into intervals of length $Y := \sqrt{N}/\lfloor (\log N)^{\gamma+2} \rfloor$. For each integer k in $I := [-2\sqrt{N}/Y, 2\sqrt{N}/Y) \cap \mathbb{Z}$, we write $X = X_k := N + 1 + kY$. Thus,

$$\sum_{N^- < p < N^+} \frac{H(D_N(p))}{p} = \sum_{k \in I} \sum_{X_k < p \leqslant X_k + Y} \frac{H(D_N(p))}{p}. \tag{25}$$

Recalling the definition of the Kronecker class number, the definition of $d_{N,f}(p)$, and the class number formula (see (6), (9), and (10)), we have the identity

$$H(D_N(p)) = \frac{1}{2\pi} \sum_{\substack{f^2 \mid D_N(p) \\ d_{N,f}(p) \equiv 0,1 \pmod 4}} \sqrt{|d_{N,f}(p)|} L(1, \chi_{d_{N,f}(p)}). \tag{26}$$

We assume that N is large enough so that there are only odd primes p satisfying the condition $N^- < p < N^+$. Therefore, since we assumed that N is odd,

$$D_N(p) = (p + 1 - N)^2 - 4p \equiv 1 \pmod 4,$$

and it follows that there are only odd f in the above sum and that $d_{N,f}(p) \equiv 1 \pmod 4$ for each such f. Hence, summing (26) over all primes p in the range $X < p \leqslant X + Y$ and switching the order of summation, we have

$$\begin{aligned} \sum_{X < p \leqslant X+Y} \frac{H(D_N(p))}{p} &= \frac{1}{2\pi} \sum_{X < p \leqslant X+Y} \frac{1}{p} \sum_{f^2 \mid D_N(p)} \sqrt{|d_{N,f}(p)|} L(1, \chi_{d_{N,f}(p)}) \\ &= \frac{1}{2\pi} \sum_{\substack{f \leqslant 2\sqrt{X+Y} \\ (f,2)=1}} \frac{1}{f} \sum_{\substack{X < p \leqslant X+Y \\ f^2 \mid D_N(p)}} \frac{\sqrt{|D_N(p)|}}{p} L(1, \chi_{d_{N,f}(p)}). \end{aligned} \tag{27}$$

We now change 'weights', approximating $\sqrt{|D_N(p)|}/p$ by $\sqrt{|D_N(X)|} \log p/(N \log N)$. If p is a prime in the interval $(X, X+Y]$, then $p = X + O(Y)$, and hence

$$D_N(p) = D_N(X) + O(Y\sqrt{N}).$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

Let X^* be the value minimizing the function $\sqrt{|D_N(t)|}$ on the interval $[X, X+Y]$. Since it is also true that $p = N + O(\sqrt{N})$, we have that

$$\left|\frac{\sqrt{|D_N(p)|}}{p} - \frac{\sqrt{|D_N(X)|}\log p}{N\log N}\right| \ll \begin{cases} \dfrac{\sqrt{|D_N(X)|}}{N^{3/2}} + \dfrac{\sqrt{Y}}{N^{3/4}} & \text{if } N^{\pm} \in [X, X+Y], \\ \dfrac{\sqrt{|D_N(X)|}}{N^{3/2}} + \dfrac{Y}{N^{1/2}\sqrt{|D_N(X^*)|}} & \text{otherwise.} \end{cases}$$

Hence, by Theorem 7 and Proposition 9, the right-hand side of (27) is equal to

$$\frac{K(N)Y\sqrt{|D_N(X)|}}{2\pi\varphi(N)\log N} + \begin{cases} O\left(\dfrac{Y\sqrt{|D_N(X)|}}{N(\log N)^{\gamma+1}} + \dfrac{Y\sqrt{|D_N(X)|}\log N}{N^{3/2}} + \dfrac{Y^{3/2}\log N}{N^{3/4}}\right) \\ \quad \text{if } N^{\pm} \in [X, X+Y], \\ O\left(\dfrac{Y\sqrt{|D_N(X)|}}{N(\log N)^{\gamma+1}} + \dfrac{Y\sqrt{|D_N(X)|}\log N}{N^{3/2}} + \dfrac{Y^2\log N}{N^{1/2}\sqrt{|D_N(X^*)|}}\right) \\ \quad \text{otherwise.} \end{cases} \tag{28}$$

Since $D_N(X_k) = 0$ for k on the endpoints of the interval $[-2\sqrt{N}/Y, 2\sqrt{N}/Y] \supset I$, by the Euler–Maclaurin summation formula, we have

$$\begin{aligned} \sum_{k\in I}\sqrt{|D_N(X_k)|} &= \int_{-2\sqrt{N}/Y}^{2\sqrt{N}/Y}\sqrt{4N-(tY)^2}\,dt + O\left(\int_{-2\sqrt{N}/Y}^{2\sqrt{N}/Y}\frac{|tY^2|}{\sqrt{4N-(tY)^2}}\,dt\right) \\ &= \frac{2\pi N}{Y} + O(\sqrt{N}), \end{aligned}$$

and, furthermore,

$$\sum_{k\in I}\frac{1}{\sqrt{|D_N(X_k^*)|}} \ll \int_{-2\sqrt{N}/Y}^{2\sqrt{N}/Y}\frac{dt}{\sqrt{4N-(tY)^2}} = \frac{1}{Y}\int_{-2\sqrt{N}}^{2\sqrt{N}}\frac{du}{\sqrt{4N-u^2}} = \frac{\pi}{Y}.$$

Whence, summing (28) over $k \in I$, we have

$$\sum_{N^-<p<N^+}\frac{H(D_N(p))}{p} = K(N)\frac{N}{\varphi(N)\log N} + O\left(\frac{1}{(\log N)^{\gamma+1}} + \frac{Y\log N}{\sqrt{N}}\right). \qquad \square$$

7. Proofs of lemmas

In this section, we give the proofs of the technical lemmas needed in the rest of the paper.

LEMMA 12. *For every positive integer f,*

$$\#\{a \in \mathbb{Z}/f\mathbb{Z} : D_N(a) \equiv 0 \pmod f\} \ll \sqrt{f}.$$

Remark. Recall that since this lemma was used in the proof of Proposition 5, we do not assume that N is odd here.

Proof of Lemma 12. First, we use the Chinese remainder theorem to write

$$\#\{a \in \mathbb{Z}/f\mathbb{Z} : D_N(a) \equiv 0 \pmod f\} = \prod_{\ell\mid f}\#\{a \in \mathbb{Z}/\ell^{\nu_\ell(f)}\mathbb{Z} : D_N(a) \equiv 0 \pmod{\ell^{\nu_\ell(f)}}\}.$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

We will show that

$$\#\{a \in \mathbb{Z}/\ell^e\mathbb{Z} : D_N(a) \equiv 0 \pmod{\ell^e}\} \leqslant \begin{cases} \max\{\ell^{\lfloor e/2 \rfloor}, 2\ell^{(e-1)/2}\} & \text{if } \ell > 2, \\ \max\{\ell^{\lfloor e/2 \rfloor}, 4\ell^{(e-1)/2}\} & \text{if } \ell = 2. \end{cases} \tag{29}$$

From this, we readily deduce that

$$\#\{a \in \mathbb{Z}/f\mathbb{Z} : D_N(a) \equiv 0 \pmod{f}\} \leqslant 8\sqrt{f},$$

which is a more precise result than that stated in the lemma.

We now give the proof of (29). Since

$$D_N(a) = a^2 - 2(N+1)a + (N-1)^2 = (a - N - 1)^2 - 4N,$$

it suffices to consider the number of solutions to the congruence

$$Z^2 \equiv 4N \pmod{\ell^e}. \tag{30}$$

Suppose z is an integer solution to (30) and write $4N = \ell^s N_0$ with $(\ell, N_0) = 1$. If $s \geqslant e$, it follows that $z \equiv 0 \pmod{\ell^{\lceil e/2 \rceil}}$, and hence there are at most $\ell^{\lfloor e/2 \rfloor}$ solutions to (30). Thus, we may assume that $s < e$ and write

$$z^2 = \ell^s(N_0 + \ell^{e-s}k)$$

for some integer k. Since $(\ell, N_0) = 1$, it follows that s must be even. Writing $s = 2s_0$, we see that $z = \ell^{s_0}x$, where x is an integer solution to the congruence

$$X^2 \equiv N_0 \pmod{\ell^{e-s}}. \tag{31}$$

So, in particular, $z \equiv \ell^{s_0}x \pmod{\ell^{e-s_0}}$. Since $(\ell, N_0) = 1$, it is a classical exercise as in [HW79, p. 98] to show that

$$\#\{X \in \mathbb{Z}/\ell^{e-s}\mathbb{Z} : X^2 \equiv N_0 \pmod{\ell^{e-s}}\} \leqslant \begin{cases} 2 & \text{if } \ell > 2, \\ 4 & \text{if } \ell = 2. \end{cases}$$

Therefore, there are at most $2\ell^{e-(e-s_0)} = 2\ell^{s/2} \leqslant 2\ell^{(e-1)/2}$ solutions to (30) when ℓ is odd, and there are at most $4\ell^{e-(e-s_0)} = 4\ell^{s/2} \leqslant 4\ell^{(e-1)/2}$ solutions when $\ell = 2$. □

Proof of Lemma 8. By Lemma 11, $c_{N,f}(n) \ll n \prod_{\ell \mid (f,n)} \#C_N^{(\ell)}(1,1,f)/\kappa_{2N}(n)$, where, for any positive integer m, $\kappa_m(n)$ is the multiplicative function defined on the prime powers by (23). Therefore,

$$\begin{aligned} K_0(N) &- \sum_{\substack{f \leqslant V \\ (f,2)=1}} \frac{1}{f} \sum_{n \leqslant U} \frac{1}{n\varphi(4nf^2)} \sum_{\substack{a \in \mathbb{Z}/4n\mathbb{Z} \\ a \equiv 1 \pmod 4}} \left(\frac{a}{n}\right) \#C_N(a,n,f) \\ &\ll \sum_{f \leqslant V}{}' \frac{\prod_{\ell \mid f} \#C_N^{(\ell)}(1,1,f)}{f^2\varphi(f)} \sum_{n > U} \frac{2\varphi((n,f))c_{N,f}(n)}{(n,f)n\varphi(4n)\prod_{\ell \mid (n,f)} \#C_N^{(\ell)}(1,1,f)} \\ &\quad + \sum_{f > V}{}' \frac{\prod_{\ell \mid f} \#C_N^{(\ell)}(1,1,f)}{f^2\varphi(f)} \sum_{n \geqslant 1} \frac{2\varphi((n,f))c_{N,f}(n)}{(n,f)n\varphi(4n)\prod_{\ell \mid (n,f)} \#C_N^{(\ell)}(1,1,f)} \end{aligned}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

$$\ll \sum_{\substack{f\leqslant V\\(f,2)=1}} \frac{\prod_{\ell\mid f}\#C_N^{(\ell)}(1,1,f)}{f^2\varphi(f)} \sum_{n>U} \frac{1}{\kappa_{2N}(n)\varphi(n)}$$

$$+ \sum_{\substack{f>V\\(f,2)=1}} \frac{\prod_{\ell\mid f}\#C_N^{(\ell)}(1,1,f)}{f^2\varphi(f)} \sum_{n\geqslant 1} \frac{1}{\kappa_{2N}(n)\varphi(n)}, \tag{32}$$

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 [DP99, Lemma 3.4], we find that

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

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

$$\sum_{n>U} \frac{1}{\kappa_{2N}(n)\varphi(n)} = \sum_{\substack{km>U\\(m,2N)=1\\ \ell\mid k\Rightarrow \ell\mid 2N}} \frac{1}{\kappa_1(m)\varphi(m)\varphi(k)} = \sum_{\substack{k\geqslant 1\\ \ell\mid k\Rightarrow \ell\mid 2N}} \frac{1}{\varphi(k)} \sum_{\substack{m>U/k\\(m,2N)=1}} \frac{1}{\kappa_1(m)\varphi(m)}$$

$$\ll \sum_{\substack{k\geqslant 1\\ \ell\mid k\Rightarrow \ell\mid 2N}} \frac{1}{\varphi(k)}\frac{\sqrt{k}}{\sqrt{U}} \ll \frac{1}{\sqrt{U}} \prod_{\ell\mid N}\left(1+\frac{\ell}{(\ell-1)(\sqrt{\ell}-1)}\right)$$

$$= \frac{1}{\sqrt{U}}\frac{N}{\varphi(N)} \prod_{\ell\mid N}\left(1+\frac{1}{\sqrt{\ell}(\ell-1)}\right)\left(1+\frac{1}{\sqrt{\ell}}\right)$$

$$\ll \frac{1}{\sqrt{U}}\frac{N}{\varphi(N)} \prod_{\ell\mid N}\left(1+\frac{1}{\sqrt{\ell}}\right).$$

We have already noted that $N/\varphi(N)\ll \log\log N$. It is a straightforward exercise as in [MV07, p. 63] to show that

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

Thus, we conclude that

$$\sum_{n>U} \frac{1}{\kappa_{2N}(n)\varphi(n)} \ll \frac{N^\epsilon}{\sqrt{U}} \tag{33}$$

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

$$\sum_{n\geqslant 1} \frac{1}{\kappa_{2N}(n)\varphi(n)} = \prod_{\ell\mid 2N}\left(1+\frac{\ell}{(\ell-1)^2}\right) \sum_{\substack{n\geqslant 1\\(n,2N)=1}} \frac{1}{\kappa_{2N}(n)\varphi(n)}$$

$$\leqslant \frac{2N}{\varphi(2N)} \prod_{\ell\mid 2N}\left(1+\frac{1}{\ell(\ell-1)}\right) \sum_{n\geqslant 1} \frac{1}{\kappa_1(n)\varphi(n)}$$

$$\ll \log\log N. \tag{34}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

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 Lemma 10. However, if $\nu_\ell(f) > \nu_\ell(N)/2$ and $2 \mid \nu_\ell(N)$, it follows that $\nu_\ell(f) \geqslant 1 + \nu_\ell(N)/2$, and hence

$$2\ell^{\nu_\ell(N)/2} \leqslant \ell^{1+\nu_\ell(N)/2} \leqslant \ell^{\nu_\ell(f)}$$

since $\ell > 2$. Therefore, for every odd integer f, we have that

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

and hence

$$\sum_{\substack{f>V \\ (f,2)=1}} \frac{\prod_{\ell \mid f} \#C_N^{(\ell)}(1,1,f)}{f^2\varphi(f)} < \sum_{f>V} \frac{1}{f\varphi(f)} \ll \frac{1}{V}. \tag{35}$$

Substituting the bounds (33)–(35) into (32), the lemma follows. □

Proof of Lemma 10. Upon completing the square, we have that

$$z^2 - 2(N+1)z + (N-1)^2 - af^2 = (z-N-1)^2 - (4N + af^2).$$

Since N is odd, the number of invertible solutions to the congruence

$$(z-N-1)^2 \equiv 4N + af^2 \pmod{2^\alpha}$$

is the same as the number of invertible solutions to the congruence $Z^2 \equiv 4N + af^2 \pmod{2^\alpha}$. Since $4N + af^2 \equiv 4 + a \pmod 8$, the computation of $C_N^{(2)}(a,n,f)$ is thus reduced to a standard exercise. See [HW79, p. 98] for example.

If $\ell \nmid 4N + af^2$, then there are exactly $1 + \left(\frac{4N+af^2}{\ell}\right)$ solutions to the congruence

$$(z-N-1)^2 \equiv 4N + af^2 \pmod{\ell^\alpha}. \tag{36}$$

However, if ℓ divides the constant term, $(N-1)^2 - af^2$, then we have exactly one invertible solution and exactly one noninvertible solution.

It remains to treat the case when $\ell \mid 4N + af^2$. We write $4N + af^2 = \ell^s m$ with $(m,\ell) = 1$. First, we observe that any solution z to (36) must satisfy $z \equiv N+1 \pmod \ell$. Therefore, if $\ell \mid N+1$, then there are no invertible solutions; if $\ell \nmid N+1$, then every solution is invertible. Hence, we assume that $\ell \nmid N+1$. Now, the number of invertible solutions to (36) is equal to the number of (noninvertible) solutions to

$$Z^2 \equiv \ell^s m \pmod{\ell^e}. \tag{37}$$

If $s \geqslant e$, then Z is a solution if and only if $Z \equiv 0 \pmod{\ell^{\lceil e/2 \rceil}}$. There are exactly $\ell^{e-\lceil e/2 \rceil} = \ell^{\lfloor e/2 \rfloor}$ such values for Z modulo ℓ^e. Now, suppose that $0 < s < e$. Then Z is a solution to (37) if and only if

$$Z^2 = \ell^s m + \ell^e k = \ell^s(m + \ell^{e-s})$$

for some integer k. Since $\ell \nmid m$ and $s < e$, we see that there can be no such Z if s is odd or if $\left(\frac{m}{\ell}\right) = -1$. Thus, we assume that $s = 2s_0$, $\left(\frac{m}{\ell}\right) = 1$, and we write $r^2 = m + \ell^{e-s}$. Under this assumption, there are exactly two (distinct modulo ℓ^{e-s}) solutions, say r_1 and r_2, to the

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

congruence $r^2 \equiv m \pmod{\ell^{e-2s_0}}$. Therefore, if Z is a solution to (37), then either $Z = \ell^{s_0}(r_1 + k_1\ell^{e-s})$ for some integer k_1 or $Z = \ell^{s_0}(r_2 + k_2\ell^{e-s})$ for some integer k_2. In other words, $Z \equiv \ell^{s_0} r_1 \pmod{\ell^{e-s_0}}$ or $Z \equiv \ell^{s_0} r_2 \pmod{\ell^{e-s_0}}$. It is not hard to check that if Z satisfies either of these two conditions, then Z is a solution to (37). There are exactly $2\ell^{e-(e-s_0)} = 2\ell^{s_0}$ such values for Z modulo ℓ^e. □

Proof of Lemma 11. It is easily checked that $c_{N,f}(1) = 1$. If n is odd, we observe that

$$c_{N,f}(n) = \sum_{a \in (\mathbb{Z}/n\mathbb{Z})^*} \left(\frac{a}{n}\right) \prod_{\ell \mid n} \#C_N^{(\ell)}(a, n, f).$$

Now, suppose that $(m, n) = 1$. It follows that at least one of m and n must be odd. Without loss of generality, we assume that n is odd. Choose integers m_0 and n_0 so that $4mm_0 + nn_0 = 1$. Then

$$\begin{aligned} c_{N,f}(n)c_{N,f}(m) &= \sum_{a_1 \in (\mathbb{Z}/n\mathbb{Z})^*} \left(\frac{a_1}{n}\right) \prod_{\ell \mid n} \#C_N^{(\ell)}(a_1, n, f) \\ &\quad \times \sum_{\substack{a_2 \in (\mathbb{Z}/4m\mathbb{Z})^* \\ a_2 \equiv 1 \pmod 4}} \left(\frac{a_2}{m}\right) \mathcal{S}_2(m, a_2) \prod_{\ell \mid m'} \#C_N^{(\ell)}(a_2, m, f) \\ &= \sum_{\substack{a_1 \in (\mathbb{Z}/n\mathbb{Z})^*, \\ a_2 \in (\mathbb{Z}/4m\mathbb{Z})^* \\ a_2 \equiv 1 \pmod 4}} \left(\frac{a_1 4mm_0 + a_2 nn_0}{nm}\right) \mathcal{S}_2(nm, a_1 4mm_0 + a_2 nn_0) \\ &\quad \times \prod_{\ell \mid nm'} \#C_N^{(\ell)}(a_1 4mm_0 + a_2 nn_0, nm, f) \\ &= c_{N,f}(nm). \end{aligned}$$

Hence $c_{N,f}(n)$ is multiplicative in n.

By (21), we find that

$$c_{N,f}(2^\alpha) = \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ a \equiv 1 \pmod 4}} \left(\frac{a}{2^\alpha}\right) \mathcal{S}_2(2^\alpha, a) = 2 \sum_{\substack{a \in (\mathbb{Z}/2^{\alpha+2}\mathbb{Z})^* \\ a \equiv 5 \pmod 8}} \left(\frac{a}{2}\right)^\alpha = (-1)^\alpha 2^\alpha$$

for $\alpha \geqslant 1$.

We now consider the case when ℓ^α is an odd prime power. In view of Lemma 10, it is natural to split $c_{N,f}(\ell^\alpha)$ into two parts, writing

$$\begin{aligned} c_{N,f}^{(1)}(\ell^\alpha) &:= \sum_{\substack{a \in (\mathbb{Z}/\ell^\alpha\mathbb{Z})^* \\ \ell \mid 4N + af^2}} \left(\frac{a}{\ell}\right)^\alpha \#C_N^{(\ell)}(a, \ell^\alpha, f), \\ c_{N,f}^{(0)}(\ell^\alpha) &:= \sum_{\substack{a \in (\mathbb{Z}/\ell^\alpha\mathbb{Z})^* \\ \ell \mid 4N + af^2}} \left(\frac{a}{\ell}\right)^\alpha \#C_N^{(\ell)}(a, \ell^\alpha, f) \end{aligned}$$

so that

$$c_{N,f}(\ell^\alpha) = c_{N,f}^{(1)}(\ell^\alpha) + c_{N,f}^{(0)}(\ell^\alpha). \tag{38}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

We concentrate on $c^{(1)}_{N,f}(\ell^\alpha)$ first. Applying Lemma 10, we have

$$\begin{aligned} c^{(1)}_{N,f}(\ell^\alpha) &= \sum_{\substack{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^*\\ \ell\nmid 4N+af^2\\ \ell\nmid (N-1)^2-af^2}} \left(\frac{a}{\ell}\right)^\alpha \#C_N^{(\ell)}(a,\ell^\alpha,f) + \sum_{\substack{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^*\\ \ell\nmid 4N+af^2\\ \ell\mid (N-1)^2-af^2}} \left(\frac{a}{\ell}\right)^\alpha \#C_N^{(\ell)}(a,\ell^\alpha,f) \\ &= \sum_{\substack{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^*\\ \ell\nmid 4N+af^2\\ \ell\nmid (N-1)^2-af^2}} \left(\frac{a}{\ell}\right)^\alpha \left[1+\left(\frac{4N+af^2}{\ell}\right)\right] + \sum_{\substack{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^*\\ \ell\nmid 4N+af^2\\ \ell\mid (N-1)^2-af^2}} \left(\frac{a}{\ell}\right)^\alpha \\ &= \ell^{\alpha-1}\Bigg\{ \sum_{\substack{a\in(\mathbb{Z}/\ell\mathbb{Z})^*\\ \ell\nmid 4N+af^2\\ \ell\nmid (N-1)^2-af^2}} \left(\frac{a}{\ell}\right)^\alpha \left[1+\left(\frac{4N+af^2}{\ell}\right)\right] + \sum_{\substack{a\in(\mathbb{Z}/\ell\mathbb{Z})^*\\ \ell\nmid 4N+af^2\\ \ell\mid (N-1)^2-af^2}} \left(\frac{a}{\ell}\right)^\alpha \Bigg\}. \end{aligned} \tag{39}$$

In order to finish evaluating this sum, we split into cases. First, assume that $\ell \mid f$. Then the sum defining $c^{(1)}_{N,f}(\ell^\alpha)$ is empty unless $\ell \nmid N$. In this case, $\ell \mid (N-1)^2 - af^2$ if and only if $\ell \mid N-1$. Therefore, if $\ell \mid f$ and $\ell \nmid N$, then

$$\begin{aligned} \frac{c^{(1)}_{N,f}(\ell^\alpha)}{\ell^{\alpha-1}} &= \begin{cases} \left[1+\left(\frac{N}{\ell}\right)\right] \displaystyle\sum_{a\in(\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{a}{\ell}\right)^\alpha & \text{if } \ell\nmid N-1, \\ \displaystyle\sum_{a\in(\mathbb{Z}/\ell\mathbb{Z})^*} \left(\frac{a}{\ell}\right)^\alpha & \text{if } \ell\mid N-1 \end{cases} \\ &= \begin{cases} (\ell-1)\left[1+\left(\frac{N}{\ell}\right)\right] & \text{if } 2\mid\alpha \text{ and } \ell\nmid N-1, \\ \ell-1 & \text{if } 2\mid\alpha \text{ and } \ell\mid N-1, \\ 0 & \text{if } 2\nmid\alpha \end{cases} \\ &= \begin{cases} (\ell-1)\left(1+\left(\frac{N}{\ell}\right)\left(\frac{N-1}{\ell}\right)^2\right) & \text{if } 2\mid\alpha, \\ 0 & \text{if } 2\nmid\alpha \end{cases} \\ &= \#C_N^{(\ell)}(1,1,f)\begin{cases} (\ell-1) & \text{if } 2\mid\alpha, \\ 0 & \text{if } 2\nmid\alpha \end{cases} \end{aligned} \tag{40}$$

as $\#C_N^{(\ell)}(1,1,f) = \left(1+\left(\frac{N}{\ell}\right)\left(\frac{N-1}{\ell}\right)^2\right)$ in this case.

Now, suppose that $\ell \nmid f$. Under this assumption, we note that $\left(\frac{a}{\ell}\right) = \left(\frac{af^2}{\ell}\right)$. Picking up with (39) and dividing through by $\ell^{\alpha-1}$, we have

$$\begin{aligned} \frac{c^{(1)}_{N,f}(\ell^\alpha)}{\ell^{\alpha-1}} &= \sum_{\substack{a\in(\mathbb{Z}/\ell\mathbb{Z})^*\\ \ell\nmid 4N+af^2\\ \ell\nmid (N-1)^2-af^2}} \left(\frac{af^2}{\ell}\right)^\alpha \left[1+\left(\frac{4N+af^2}{\ell}\right)\right] + \sum_{\substack{a\in(\mathbb{Z}/\ell\mathbb{Z})^*\\ \ell\nmid 4N+af^2\\ \ell\mid (N-1)^2-af^2}} \left(\frac{af^2}{\ell}\right)^\alpha \\ &= \sum_{\substack{a\in(\mathbb{Z}/\ell\mathbb{Z})^*\\ \ell\nmid 4N+a\\ \ell\nmid (N-1)^2-a}} \left(\frac{a}{\ell}\right)^\alpha \left[1+\left(\frac{4N+a}{\ell}\right)\right] + \sum_{\substack{a\in(\mathbb{Z}/\ell\mathbb{Z})^*\\ \ell\nmid 4N+a\\ \ell\mid (N-1)^2-a}} \left(\frac{a}{\ell}\right)^\alpha \end{aligned}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

$$= \sum_{\substack{a\in\mathbb{Z}/\ell\mathbb{Z}\\ a\not\equiv -4N \pmod{\ell}}} \left(\frac{a}{\ell}\right)^{\alpha} + \sum_{\substack{a\in\mathbb{Z}/\ell\mathbb{Z}\\ a\not\equiv (N-1)^2 \pmod{\ell}}} \left(\frac{a}{\ell}\right)^{\alpha}\left(\frac{4N+a}{\ell}\right)$$

$$= \left[\sum_{b=1}^{\ell}\left(1+\left(\frac{b}{\ell}\right)\right)\left(\frac{b-4N}{\ell}\right)^{\alpha}\right] - \left(\frac{-N}{\ell}\right)^{\alpha} - \left(\frac{N^2-1}{\ell}\right)^{2} \tag{41}$$

upon completing the sums and making the change of variables $b = 4N + a$. One easily computes that

$$\sum_{b=1}^{\ell}\left(1+\left(\frac{b}{\ell}\right)\right)\left(\frac{b-4N}{\ell}\right)^{\alpha} = \begin{cases} \ell-1 & \text{if } \ell \mid N,\\ \ell-1-\left(\frac{N}{\ell}\right) & \text{if } \ell\nmid N \text{ and } 2\mid\alpha,\\ -1 & \text{if } \ell\nmid N \text{ and } 2\nmid\alpha. \end{cases}$$

For example, the third case is [MV07, Exercise 1(b), p. 301]. Therefore,

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

It remains to compute $c_{N,f}^{(0)}(\ell^{\alpha})$. We first consider the case when $\ell\nmid f$. Note that the sum defining $c_{N,f}^{(0)}(\ell^{\alpha})$ is empty unless $\ell\nmid N$ as well. Thus, under this assumption, we have that

$$\begin{aligned} c_{N,f}^{(0)}(\ell^{\alpha}) &= \sum_{\substack{a\in(\mathbb{Z}/\ell^{\alpha}\mathbb{Z})^{*}\\ \ell\mid 4N+af^2}} \left(\frac{af^2}{\ell}\right)^{\alpha} \#C_N^{(\ell)}(a,\ell^{\alpha},f)\\ &= \sum_{\substack{a\in(\mathbb{Z}/\ell^{\alpha}\mathbb{Z})^{*}\\ \ell\mid 4N+a}} \left(\frac{a}{\ell}\right)^{\alpha} \#C_N^{(\ell)}(a,\ell^{\alpha},1)\\ &= \left(\frac{-4N}{\ell}\right)^{\alpha} \sum_{\substack{a\in(\mathbb{Z}/\ell^{\alpha}\mathbb{Z})^{*}\\ \ell\mid 4N+a}} \#C_N^{(\ell)}(a,\ell^{\alpha},1). \end{aligned}$$

In order to evaluate this last sum, for each $a\in(\mathbb{Z}/\ell^{\alpha}\mathbb{Z})^{*}$, we choose an integer representative in the range $-4N < a \leqslant \ell^{\alpha} - 4N$. This ensures that $0\leqslant \nu_{\ell}(4N+a)\leqslant\alpha$. There is exactly one such choice of a so that $\nu_{\ell}(4N+a)=\alpha$, namely $a=\ell^{\alpha}-4N$. For $1\leqslant t\leqslant\alpha-1$, the number of such a with $\nu_{\ell}(4N+a)=t$ is $(\ell-1)\ell^{\alpha-t-1}$, but for only half of those values is $\left(\frac{(4N+a)/\ell^{t}}{\ell}\right)=1$. Perhaps, the easiest way to see this is to consider the base-ℓ expansion of $4N+a$ for each a in this range.

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

Therefore, applying Lemma 10 again, we have

$$\begin{aligned}\sum_{t=1}^{\alpha}\sum_{\substack{0<4N+a\leqslant \ell^\alpha\\ \nu_\ell(4N+a)=t}} \#C_N^{(\ell)}(a,\ell^\alpha,1) &= \left(\frac{N+1}{\ell}\right)^2 \ell^{\lfloor \alpha/2\rfloor} + \sum_{t=1}^{\lfloor(\alpha-1)/2\rfloor}\sum_{\substack{0<4N+a<\ell^\alpha\\ \nu_\ell(4N+a)=2t}} \#C_N^{(\ell)}(a,\ell^\alpha,1)\\ &= \left(\frac{N+1}{\ell}\right)^2 \ell^{\lfloor \alpha/2\rfloor} + \sum_{t=1}^{\lfloor(\alpha-1)/2\rfloor} \frac{(\ell-1)\ell^{\alpha-2t-1}}{2} 2\left(\frac{N+1}{\ell}\right)^2 \ell^t\\ &= \left(\frac{N+1}{\ell}\right)^2 \ell^{\lfloor \alpha/2\rfloor} + \left(\frac{N+1}{\ell}\right)^2 \ell^{\alpha-1}(1-\ell^{-\lfloor(\alpha-1)/2\rfloor})\\ &= \left(\frac{N+1}{\ell}\right)^2 (\ell^{\lfloor \alpha/2\rfloor} + \ell^{\alpha-1}(1-\ell^{-\lfloor(\alpha-1)/2\rfloor}))\\ &= \left(\frac{N+1}{\ell}\right)^2 \ell^{\alpha-1}.\end{aligned}$$

Therefore, if $\ell \nmid fN$, then

$$c_{N,f}^{(0)}(\ell^\alpha) = \left(\frac{-N}{\ell}\right)^\alpha \left(\frac{N+1}{\ell}\right)^2 \ell^{\alpha-1}.$$

We now compute $c_{N,f}^{(0)}(\ell^\alpha)$ in the case that $\ell \mid f$. Note that, in this case, the sum defining $c_{N,f}^{(0)}(\ell^\alpha)$ is empty unless $\ell \mid N$. Note that $\nu_\ell(4N+af^2) \geqslant \min\{\nu_\ell(N), 2\nu_\ell(f)\}$ with equality holding if $\nu_\ell(N) \neq 2\nu_\ell(f)$.

First, suppose that $2\nu_\ell(f) < \nu_\ell(N)$. Noting that $e = \nu_\ell(4\ell^\alpha f^2) > 2\nu_\ell(f)$, by Lemma 10 we have that

$$\#C_N^{(\ell)}(a,\ell^\alpha,f) = 2\ell^{\nu_\ell(f)} = 2\#C_N^{(\ell)}(1,1,f)$$

if and only if $\left(\frac{a}{\ell}\right) = \left(\frac{(4N+af^2)/\ell^{2\nu_\ell(f)}}{\ell}\right) = 1$. Hence,

$$\begin{aligned}c_{N,f}^{(0)}(\ell^\alpha) &= \sum_{\substack{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^*\\ \ell\mid 4N+af^2}} \left(\frac{a}{\ell}\right)^\alpha \#C_N^{(\ell)}(a,\ell^\alpha,f)\\ &= 2\#C_N^{(\ell)}(1,1,f) \sum_{\substack{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^*\\ (a/\ell)=1}} \left(\frac{a}{\ell}\right)^\alpha\\ &= \#C_N^{(\ell)}(1,1,f)\ell^{\alpha-1}(\ell-1)\end{aligned}$$

if $1 < 2\nu_\ell(f) < \nu_\ell(N)$.

Now, suppose that $\nu_\ell(N) < 2\nu_\ell(f)$. Since $e = \nu_\ell(4\ell^\alpha f^2) > \nu_\ell(N)$, by Lemma 10, we have that

$$\begin{aligned}\#C_N^{(\ell)}(a,\ell^\alpha,f) &= \begin{cases} 2\ell^{\nu_\ell(N)/2} & \text{if } 2\mid \nu_\ell(N) \text{ and } \left(\frac{N_\ell}{\ell}\right)=1,\\ 0 & \text{otherwise}\end{cases}\\ &= \#C_N^{(\ell)}(1,1,f)\end{aligned}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

for every $a \in (\mathbb{Z}/\ell^\alpha\mathbb{Z})^*$. Hence,

$$\begin{aligned} c_{N,f}^{(0)}(\ell^\alpha) &= \sum_{\substack{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^* \\ \ell\mid 4N+af^2}} \left(\frac{a}{\ell}\right)^\alpha \#C_N^{(\ell)}(a,\ell^\alpha,f) \\ &= \#C_N^{(\ell)}(1,1,f) \sum_{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^*} \left(\frac{a}{\ell}\right)^\alpha \\ &= \#C_N^{(\ell)}(1,1,f) \begin{cases} \ell^{\alpha-1}(\ell-1) & \text{if } 2 \mid \alpha, \\ 0 & \text{if } 2 \nmid \alpha \end{cases} \end{aligned}$$

if $1 \leqslant \nu_\ell(N) < 2\nu_\ell(f)$.

Finally, consider the case when $2\nu_\ell(f) = \nu_\ell(N)$. Let $r = \nu_\ell(f)$ and $s = \nu_\ell(N)$, and write $f = \ell^r f_\ell$ and $N = \ell^s N_\ell$ with $(\ell, f_\ell N_\ell) = 1$. Then

$$\begin{aligned} c_{N,f}^{(0)}(\ell^\alpha) &= \sum_{\substack{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^* \\ \ell\mid 4N+af^2}} \left(\frac{a}{\ell}\right)^\alpha \#C_N^{(\ell)}(a,\ell^\alpha,f) = \sum_{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^*} \left(\frac{af_\ell^2}{\ell}\right)^\alpha \#C_N^{(\ell)}(a,\ell^\alpha,\ell^r f_\ell) \\ &= \sum_{a\in(\mathbb{Z}/\ell^\alpha\mathbb{Z})^*} \left(\frac{a}{\ell}\right)^\alpha \#C_N^{(\ell)}(a,\ell^\alpha,\ell^r). \end{aligned}$$

To evaluate this last sum, for each $a \in (\mathbb{Z}/\ell^\alpha\mathbb{Z})^*$, we choose an integer representative in the range $-4N_\ell < a \leqslant \ell^\alpha - 4N_\ell$. This ensures that $0 \leqslant \nu_\ell(4N_\ell + a) \leqslant \alpha$, and hence that $2r \leqslant \nu_\ell(4N + a\ell^{2r}) \leqslant 2r + \alpha$. Similarly to before, there is exactly one choice of a such that $\nu_\ell(4N_\ell + a) = \alpha$, namely $a = \ell^\alpha - 4N_\ell$. For $1 \leqslant t \leqslant \alpha - 1$, there are $(\ell-1)\ell^{\alpha-t-1}$ choices with $\nu_\ell(4N_\ell + a) = t$, but for only half of those values is $\left(\frac{(4N_\ell+a)/\ell^t}{\ell}\right) = 1$. Note that if $\ell \mid 4N_\ell + a$, then $\left(\frac{a}{\ell}\right) = \left(\frac{-N_\ell}{\ell}\right)$. Therefore, if $1 < \nu_\ell(N) = 2\nu_\ell(f)$, then

$$\begin{aligned} c_{N,f}^{(0)}(\ell^\alpha) &= \sum_{t=0}^{\alpha} \sum_{\substack{0<4N_\ell+a\leqslant\ell^\alpha \\ \nu_\ell(4N_\ell+a)=t}} \left(\frac{a}{\ell}\right)^\alpha \#C_N^{(\ell)}(a,\ell^\alpha,\ell^r) \\ &= \left(\frac{-N_\ell}{\ell}\right)^\alpha \ell^{\lfloor(2r+\alpha)/2\rfloor} + \sum_{t=1}^{\lfloor(\alpha-1)/2\rfloor} \left(\frac{-N_\ell}{\ell}\right)^\alpha \frac{(\ell-1)\ell^{\alpha-2t-1}}{2} 2\ell^{r+t} \\ &\quad + \sum_{\substack{0<4N_\ell+a<\ell^\alpha \\ \left(\frac{4N_\ell+a}{\ell}\right)=1}} \left(\frac{a}{\ell}\right)^\alpha 2\ell^r \\ &= \left(\frac{-N_\ell}{\ell}\right)^\alpha \ell^{r+\lfloor\alpha/2\rfloor} + \left(\frac{-N_\ell}{\ell}\right)^\alpha \ell^{\alpha-1+r}\left(1-\ell^{-\lfloor(\alpha-1)/2\rfloor}\right) \\ &\quad + \ell^{r+\alpha-1} \sum_{a\in\mathbb{Z}/\ell\mathbb{Z}} \left(\frac{a}{\ell}\right)^\alpha \left(1+\left(\frac{4N_\ell+a}{\ell}\right)\right) \\ &= \left(\frac{-N_\ell}{\ell}\right) \ell^r [\ell^{\lfloor\alpha/2\rfloor} + \ell^{\alpha-1}(1-\ell^{-\lfloor(\alpha-1)/2\rfloor})] \end{aligned}$$

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press

$$
\begin{aligned}
&+ \ell^{r+\alpha-1} \sum_{b \in \mathbb{Z}/\ell\mathbb{Z}} \left(1 + \left(\frac{b}{\ell}\right)\right) \left(\frac{b - 4N_\ell}{\ell}\right)^\alpha \\
&= \ell^{r+\alpha-1} \begin{cases} \left(\dfrac{-N_\ell}{\ell}\right) + \ell - 1 - \left(\dfrac{N_\ell}{\ell}\right) & \text{if } 2 \mid \alpha, \\ \left(\dfrac{-N_\ell}{\ell}\right) - 1 & \text{if } 2 \nmid \alpha \end{cases} \\
&= \#C_N^{(\ell)}(1,1,f) \ell^{\alpha-1} \begin{cases} \left(\dfrac{-N_\ell}{\ell}\right) + \ell - 1 - \left(\dfrac{N_\ell}{\ell}\right) & \text{if } 2 \mid \alpha, \\ \left(\dfrac{-N_\ell}{\ell}\right) - 1 & \text{if } 2 \nmid \alpha. \end{cases}
\end{aligned}
$$

The lemma now follows by combining our computations for $c_{N,f}^{(0)}(\ell^\alpha)$ and $c_{N,f}^{(1)}(\ell^\alpha)$. □

Acknowledgements

The authors would like to thank K. Soundararajan for pointing out how to improve the average upper bound of Theorem 1 by using short Euler products holding for almost all characters. They also thank Henri Cohen, Andrew Granville and Dimitris Koukoulopoulos for useful discussions related to this work and Andrea Smith for a careful reading of the manuscript.

References

BCD11 A. Balog, A.-C. Cojocaru and C. David, *Average twin prime conjecture for elliptic curves*, Amer. J. Math. **133** (2011), 1179–1229.

BBIJ05 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.

Bur63 D. A. Burgess, *On character sums and L-series. II*, Proc. Lond. Math. Soc. (3) **13** (1963), 524–536.

CFJKP11 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.

CL84a H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups*, in *Number theory (New York, 1982)*, Lecture Notes in Mathematics, vol. 1052 (Springer, Berlin, 1984), 26–36.

CL84b H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, in *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, Lecture Notes in Mathematics, vol. 1068 (Springer, Berlin, 1984), 33–62.

CIJ A. C. Cojocaru, H. Iwaniec and N. Jones, *The Lang–Trotter conjecture on Frobenius fields*, Preprint.

Dav80 H. Davenport, *Multiplicative number theory*, Graduate Texts in Mathematics, vol. 74, second edition (Springer, New York, 1980).

DP99 C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, Int. Math. Res. Not. IMRN **1999** (1999), 165–183.

DP04 C. David and F. Pappalardi, *Average Frobenius distribution for inerts in* $\mathbb{Q}(i)$, J. Ramanujan Math. Soc. **19** (2004), 181–201.

DS12 C. David and E. Smith, A *Cohen–Lenstra phenomenon for elliptic curves*, Preprint (2012), arXiv:1206.1585.

FR96 E. Fouvry and M. Ram Murty, *On the distribution of supersingular primes*, Canad. J. Math. **48** (1996), 81–104.

GS03 A. Granville and K. Soundararajan, *The distribution of values of* $L(1, \chi_d)$, Geom. Funct. Anal. **13** (2003), 992–1028.

HW79 G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth edition (The Clarendon Press, Oxford University Press, New York, NY, 1979).

IK04 H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53 (American Mathematical Society, Providence, RI, 2004).

Jam04 K. James, *Average Frobenius distributions for elliptic curves with 3-torsion*, J. Number Theory **109** (2004), 278–298.

JS11 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.

Kob88 N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), 157–165.

Kow06 E. Kowalski, *Analytic problems for elliptic curves*, J. Ramanujan Math. Soc. **21** (2006), 19–114.

LT76 S. Lang and H. Trotter, *Distribution of Frobenius automorphisms in* GL_2*-extensions of the rational numbers*, in *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics, vol. 504 (Springer, Berlin, 1976).

LPZ10 A. Languasco, A. Perelli and A. Zaccagnini, *On the Montgomery–Hooley theorem in short intervals*, Mathematika **56** (2010), 231–243.

Len87 H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) **126** (1987), 649–673.

MV07 H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97 (Cambridge University Press, Cambridge, 2007).

Chantal David cdavid@mathstat.concordia.ca
Department of Mathematics and Statistics, Concordia University,
1455 de Maisonneuve West, Montréal, Québec H3G 1M8, Canada

Ethan Smith ethans@mtu.edu
Centre de recherches mathématiques, Université de Montréal, P.O. Box 6128,
Centre-ville Station, Montréal, Québec H3C 3J7, Canada
and
Department of Mathematical Sciences, Michigan Technological University,
1400 Townsend Drive, Houghton, MI, 49931-1295, USA

https://doi.org/10.1112/S0010437X12000541 Published online by Cambridge University Press