Group Structures of Elliptic Curves Over Finite Fields

Vorrapan Chandee[1,2], Chantal David[3], Dimitris Koukoulopoulos[4], and Ethan Smith[5]

[1]Centre de recherches mathématiques, Université de Montréal, PO Box 6128, Centre-ville Station, Montréal, Québec, Canada H3C 3J7, [2]Department of Mathematics, Burapha University, 169 Long-Hard Bangsaen Rd, Chonburi 20131, Thailand, [3]Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve West, Montréal, Québec, Canada H3G 1M8, [4]Département de mathématiques et de statistique, Université de Montréal, CP 6128, Succ. Centre-Ville, Montréal, Québec, Canada H3C 3J7, and [5]Department of Mathematics, Liberty University, 1971 University Blvd, MSC Box 710052, Lynchburg, VA 24502, USA

Correspondence to be sent to: e-mail: cdavid@mathstat.concordia.ca

It is well known that if E is an elliptic curve over the finite field $\mathbb{F}_p$, then $E(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ for some positive integers m, k. Let $S(M, K)$ denote the set of pairs (m, k) with $m \leq M$ and $k \leq K$ for which there exists an elliptic curve over some prime finite field whose group of points is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$. Banks, Pappalardi, and Shparlinski recently conjectured that if $K \leq (\log M)^{2-\epsilon}$, then a density zero proportion of the groups in question actually arises as the group of points on some elliptic curve over some prime finite field. On the other hand, if $K \geq (\log M)^{2+\epsilon}$, they conjectured that a density 1 proportion of the groups in question arises as the group of points on some elliptic curve over some prime finite field. We prove that the first part of their conjecture holds in the full range $K \leq (\log M)^{2-\epsilon}$, and we prove that the second part

of their conjecture holds in the limited range $K \geq M^{4+\epsilon}$. In the wider range $K \geq M^2$, we show that at least a positive density of the groups in question actually occurs.

1   Introduction

Let E be an elliptic curve over $\mathbb{F}_p$, and denote by $E(\mathbb{F}_p)$ its set of points over $\mathbb{F}_p$. It is well known that $E(\mathbb{F}_p)$ admits the structure of an abelian group. It is then natural to ask for a description of the groups that arise this way as p runs through all primes and E through all curves over $\mathbb{F}_p$. This question was first addressed by Banks, Pappalardi, and Shparlinski [2]. Below we reproduce part of the discussion from [2].

   The first relevant property is that the size of $E(\mathbb{F}_p)$ can never be very far from $p+1$. Indeed, if $\#E(\mathbb{F}_p) = p + 1 - a_p$, then Hasse proved that $|a_p| \leq 2\sqrt{p}$. Setting

$$x^- = x + 1 - 2\sqrt{x} = (\sqrt{x} - 1)^2 \quad \text{and} \quad x^+ = x + 1 + 2\sqrt{x} = (\sqrt{x} + 1)^2,$$

for each $x \geq 1$, this is equivalent to saying that $\#E(\mathbb{F}_p) \in (p^-, p^+)$. It follows from the work of Deuring [7] that, for any integer N satisfying $p^- < N < p^+$, there exists an elliptic curve $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = N$. Solving the inequalities for p allows us to conclude that, given a positive integer N, there is a finite field $\mathbb{F}_p$ and an elliptic curve $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = N$ if and only if there is a prime $p \in (N^-, N^+)$. However, this result does not take into account the actual group structure of $E(\mathbb{F}_p)$.

   The second relevant property is that, as an abstract abelian group, $E(\mathbb{F}_p)$ has at most two invariant factors. In other words, we may write

$$E(\mathbb{F}_p) \simeq G_{m,k} := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$$

for some unique positive integers m, k. Refining the ideas already present in the work of Deuring, one can argue that there is an elliptic curve $E/\mathbb{F}_p$ with $E(\mathbb{F}_p) \simeq G_{m,k}$ if and only if $N = m^2 k \in (p^-, p^+)$ and $p \equiv 1 \pmod{m}$. Arguing as before allows us to conclude that, given a group $G_{m,k}$ of order $N = m^2 k$, there is a finite field $\mathbb{F}_p$ and an elliptic curve $E/\mathbb{F}_p$ with $E(\mathbb{F}_p) \simeq G_{m,k}$ if and only if there is a prime $p \equiv 1 \pmod{m}$ in the interval (N^-, N^+). The latter condition is equivalent to the assertion that there is a prime of the form $p = km^2 + jm + 1$ with $|j| < 2\sqrt{k}$; see Corollary 2.2.

   The above characterization gives some interesting consequences. Note that, when k is very small, it is unlikely that there is a finite field $\mathbb{F}_p$ and a curve $E/\mathbb{F}_p$ such that $E(\mathbb{F}_p) \simeq G_{m,k}$ simply because the interval (N^-, N^+) is too short. For example, there is no curve over $\mathbb{F}_p$ such that $E(\mathbb{F}_p) \simeq \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$, since none of the three integers $122 - 11, 122, 122 + 11$ is prime. Other examples of groups not occurring are given by Banks et al. [2].

In order to study the question of which groups $G_{m,k}$ occur as group structures of elliptic curves over $\mathbb{F}_p$ from an average point of view, the authors of [2] defined

$$S(M, K) = \{m \leq M, k \leq K : \text{there is a prime } p \text{ and a curve } E/\mathbb{F}_p \text{ with } E(\mathbb{F}_p) \simeq G_{m,k}\}.$$

They proved the following result for the cardinality of $S(M, K)$.

Theorem 1.1 (Banks et al. [2]).   Let $M \geq 2$ and $K \geq 1$. Then, for every fixed K, we have

$$\#S(M, K) \ll_K \frac{M}{\log M}.$$

If $M \leq K^{43/94-\epsilon}$, then

$$\#S(M, K) \gg \frac{MK}{\log K}.$$

Finally, if $M \leq K^{1/2-\epsilon}$, then

$$\#S(M, K) \gg \frac{MK}{(\log K)^2}. \qquad \square$$

Moreover, the authors of [2] conjectured the following.

Conjecture 1.2 (Banks et al. [2]).

$$\#S(M, K) = \begin{cases} o(MK) & \text{if } K \leq (\log M)^{2-\epsilon}, \\ MK(1 + o(1)) & \text{if } K \geq (\log M)^{2+\epsilon}. \end{cases} \qquad \square$$

The motivation behind the above conjecture can be explained by a simple heuristic. An integer n is prime with probability about $1/\log n$. For $G_{m,k}$ to be the group of a curve E over some finite field, we need at least one of the integers $n = km^2 + jm + 1$ with $|j| < 2\sqrt{k}$ to be prime. If we assume that these events occur independently of each other, the probability that none of the integers $n = km^2 + jm + 1$, $|j| < 2\sqrt{k}$, is prime is about

$$\left(1 - \frac{1}{\log(m^2 k)}\right)^{4\sqrt{k}}.$$

This quantity becomes less than 1 as soon as $\sqrt{k} \gg \log(m^2 k)$. In particular, if $k \geq (\log m)^{2+\epsilon}$, then we expect with probability 1 that $km^2 + jm + 1$ is prime for some $j \in (-2\sqrt{k}, 2\sqrt{k})$. One can make the even bolder guess that if $k \geq (\log m)^{2+\epsilon}$ and k is large enough, then there is always some $j \in (-2\sqrt{k}, 2\sqrt{k})$ for which $km^2 + jm + 1$ is prime. This question is completely out of reach given current techniques, as we do not even know whether there are primes in every interval of the form $(x, x + x^{0.524})$ with x large

enough. (The best result known, due to Baker et al. [1], is that $(x, x + x^{0.525})$ contains primes for every sufficiently large x.)

In this paper, we improve upon Theorem 1.1. Our first result is that the first part of Conjecture 1.2 holds for M, K in the predicted range.

Theorem 1.3. Let $M \geq 2$ and $K \geq 1$. Then we have that

$$\#S(M, K) \ll \frac{MK^{3/2}}{\log M}.$$

In particular, if $K \leq (\log M)^{2-\epsilon}$ for some fixed $\epsilon > 0$, then

$$\#S(M, K) = o_\epsilon(MK) \quad \text{as } M \to \infty. \qquad \Box$$

Remark 1.4. The proof of Theorem 1.3 begins in the same way as the proof given in [2] for the first assertion of Theorem 1.1. The main difference is that we explicitly calculate the dependence on K. Calculation of this dependence relies on the ability to approximate the value of $L(1, \chi)$ by a very short Euler product for most characters χ; see Lemma 3.3. $\qquad \Box$

We also prove that the second part of Conjecture 1.2 holds for a restricted range of M and K.

Theorem 1.5. Fix $A \geq 1$ and $\epsilon \in (0, 1/3]$. If $M \leq K^{1/4-\epsilon}$, then

$$\#S(M, K) = MK + O_{\epsilon, A}\left(\frac{MK}{(\log K)^A}\right).$$

If, in addition, the Riemann hypothesis for Dirichlet L-functions is true, then the above estimate holds for $M \leq K^{1/2-\epsilon}$. $\qquad \Box$

Finally, we show that a lower bound of the correct order of magnitude holds unconditionally in the range $M \leq K^{1/2}$.

Theorem 1.6. For $1 \leq M \leq K^{1/2}$, we have that

$$\#S(M, K) \gg MK. \qquad \Box$$

Notation

Given an integer n, we let $P^+(n)$ and $P^-(n)$ denote its largest and smallest primes factors, respectively, with the notational conventions that $P^+(1) = 1$ and $P^-(1) = \infty$. As usually,

τ, μ, ϕ, and Λ denote the divisor, the Möbius, the totient, and the von Mangoldt function, respectively. Furthermore, we let $\pi(x; q, a)$ be the number of primes up to x that are congruent to $a \pmod q$ and

$$\psi(x; q, a) = \sum_{n \equiv a \pmod q} \Lambda(n).$$

The letters p and ℓ always denote prime numbers. Finally, we write $f \ll_{a,b,\dots} g$ if there is a constant c, depending at most on $a, b, \dots$, such that $|f| \leq cg$, and we write $f \asymp_{a,b,\dots} g$ if $f \ll_{a,b,\dots} g$ and $g \ll_{a,b,\dots} f$.

2 Preliminaries and Cohen–Lenstra Heuristics

In this section, we explain how the existence of an elliptic curve over a prime finite field with a given group structure is equivalent to the existence of a prime in a certain interval with a given congruence condition. Some of the results and arguments of this section are very similar to [2, Section 3], but we reproduce them here for the sake of completeness. The first lemma is a result of Rück [11], who used the work of Deuring, Waterhouse, and Tate–Honda to characterize those groups which actually occur as the group of points on elliptic curves over finite fields.

Lemma 2.1 (Rück).   Let $N = \prod_\ell \ell^{h_\ell}$ be a possible order $\#E(\mathbb{F}_p)$ for an elliptic curve $E/\mathbb{F}_p$, that is, $N \in (p^-, p^+)$. Then all the possible groups $E(\mathbb{F}_p)$ with $\#E(\mathbb{F}_p) = N$ are

$$\mathbb{Z}/p^{h_p}\mathbb{Z} \times \prod_{\ell \neq p}(\mathbb{Z}/\ell^{b_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{h_\ell - b_\ell}\mathbb{Z}),$$

where b_ℓ is an arbitrary integer satisfying $0 \leq b_\ell \leq \min(v_\ell(p-1), \lfloor h_\ell/2 \rfloor)$, and $v_\ell(\alpha)$ is the highest power of ℓ dividing α.   □

As a corollary of the above lemma, we have the following result, which is [2, Lemma 3.5].

Corollary 2.2.   Let m and k be integers. There is a prime p and a curve E over $\mathbb{F}_p$ such that $E(\mathbb{F}_p) \simeq G_{m,k}$ if and only if there is a prime $p \equiv 1 \pmod m$ in the interval

$$I_{m^2 k} := (km^2 - 2m\sqrt{k} + 1, km^2 + 2m\sqrt{k} + 1),$$

or, equivalently, if and only if there is a prime $p = km^2 + jm + 1$ with $|j| < 2\sqrt{k}$.   □

Proof. Suppose that there exists an elliptic curve E over $\mathbb{F}_p$ such that $E(\mathbb{F}_p) \simeq G_{m,k}$. As mentioned in the introduction, we must have that $N = m^2 k = \#E(\mathbb{F}_p) \in (p^-, p^+)$. Solving for p as in the introduction gives that $p \in (N^-, N^+) = I_{mk^2}$. Since the m-torsion points are contained in $E(\mathbb{F}_p)$ and since the Weil pairing is surjective, $\mathbb{F}_p$ must contain the mth roots of unity, which is equivalent to saying that $p \equiv 1 \pmod{m}$.

Conversely, suppose that there is a prime $p \in I_{m^2 k}$ such that $p \equiv 1 \pmod{m}$, and let $N = km^2$. It is easy to check that $|p + 1 - N| \leq 2\sqrt{p}$, that is to say that N is an admissible order. Writing $N = km^2 = \prod_\ell \ell^{h_\ell}$, we immediately see that $v_\ell(m) \leq \lfloor h_\ell/2 \rfloor$. Furthermore, since $p \equiv 1 \pmod{m}$, we also have that $v_\ell(p-1) \geq v_\ell(m)$ for each $\ell \mid m$. Thus, we may take $b_\ell = v_\ell(m)$ in Lemma 2.1 for all $\ell \mid m$. So, in particular, $h_\ell - b_\ell = v_\ell(m) + v_\ell(k)$, and we conclude that

$$G_{m,k} = \prod_\ell (\mathbb{Z}/\ell^{v_\ell(m)}\mathbb{Z} \times \mathbb{Z}/\ell^{v_\ell(m)+v_\ell(k)}\mathbb{Z})$$

is an admissible group. This completes the proof of the corollary. ∎

Remark 2.3. Using Corollary 2.2, we readily find that

$$\#S(M, K) = \sum_{m \leq M} \sum_{k \leq K} \mathbb{I}(m, k),$$

where

$$\mathbb{I}(m, k) := \begin{cases} 1 & \text{if there exists a prime } p \in I_{m^2 k} \text{ such that } p \equiv 1 \pmod{m}, \\ 0 & \text{otherwise.} \end{cases} \qquad \square$$

The fact that the groups $G_{m,k}$ are more likely to occur when m is small is in accordance with the general philosophy of the Cohen–Lenstra heuristics, which predict that random abelian groups "naturally" occur with probability inversely proportional to the size of their automorphism groups. That is, the presence of many automorphisms decreases the frequency of occurrence. In particular, those groups that are "nearly cyclic" (m relatively small) should be the most likely to occur, and those groups that are "very split" (m relatively large) should be the least likely to occur. This is what we observe in Theorems 1.3, 1.5, and 1.6. Indeed, the "very split" groups occur with density zero, and the "nearly cyclic" groups occur with density 1.

In order to see that the probability of occurrence of the groups $G_{m,k}$ is really in correspondence with the weights suggested by the Cohen–Lenstra heuristics, one should count the number of times a given group $G_{m,k}$ occurs as $E(\mathbb{F}_p)$, and not only if it occurs.

More precisely, given a group G of order N and a prime p, let

$$M_p(G) = \#\{E/\mathbb{F}_p : E(\mathbb{F}_p) \simeq G\}.$$

The quantity in question then is the sum

$$M(G) := \sum_{N^- < p < N^+} M_p(G).$$

Using the proper generalization of Deuring's work, $M(G)$ can be related to a certain average of Kronecker class numbers; see [12], for example. It is shown in [6] that, under a suitable hypothesis for the number of primes in short arithmetic progressions,

$$\frac{M(G_{m,k})}{4\sqrt{N}/\log N} \sim_A K(G_{m,k}) \cdot \frac{\#G_{m,k}}{\#\mathrm{Aut}(G_{m,k})} \cdot N^{3/2} \quad (N = m^2 k, m \le (\log k)^A, k \to \infty), \tag{2.1}$$

where $K(G_{m,k})$ is nonzero and uniformly bounded for all integers m and k. So we see that the average frequency of occurrence of groups of elliptic curves over finite fields is compatible with the Cohen–Lenstra heuristics.

As we mentioned above, the results of [6] are conditional under some hypothesis for the number of primes in short arithmetic progressions because the intervals (N^-, N^+) are so short that even the Riemann hypothesis does not guarantee the existence of a prime. Nevertheless, it is possible to obtain unconditional results displaying the Cohen–Lenstra phenomenon, by showing that the asymptotic in (2.1) is an upper bound for all groups G, and a lower bound for most of the groups G (modulo constants). This work is in progress [4]. The proof of the lower bound for most of the groups G has similarities with the proof of Theorem 1.5 of the present paper and, in particular, it requires the generalization of Selberg's theorem about primes in short arithmetic progressions due to the third author [9], but it involves more technical difficulties, as one needs to combine this with the arguments of [6].

3   Auxiliary Results

In this section, we collect some technical results that will be needed to prove the theorems. First, we state the fundamental lemma of the combinatorial sieve (see, e.g., [13, Theorem 3, p. 60]), which will be used in the proof of Theorem 1.3. Given a finite set of integers $\mathcal{A}$ and a number $y \ge 1$, we set

$$S(\mathcal{A}, y) = \#\{a \in \mathcal{A} : P^-(a) > y\}.$$

As is customary, we assume that there is a multiplicative function ρ and a number X such that, for every integer d,

$$\#\{a \in \mathcal{A} : a \equiv 0 \ (\text{mod } d)\} = X \cdot \frac{\rho(d)}{d} + R_d,$$

for some real number R_d, which we think of as an error term. Then we have the following result.

Lemma 3.1. Let $\mathcal{A}$, ρ, X, and $\{R_d : d \in \mathbb{N}\}$ be as above. If $\rho(p) \leq \min\{2, p-1\}$ for all primes p, then we have that

$$S(\mathcal{A}, y) = X \prod_{\ell \leq y} \left(1 - \frac{\rho(\ell)}{\ell}\right) \{1 + O(u^{-u/2})\} + O\left(\sum_{d \leq y^u, \ P^+(d) \leq y} \mu^2(d) |R_d|\right),$$

uniformly for all $y \geq 1$ and $u \geq 1$. $\square$

The next lemma will be used in the proof of Theorem 1.3.

Lemma 3.2. Fix $\epsilon > 0$ and let χ be a nonprincipal character mod q. For every $y \geq 1$, we have that

$$\prod_{\ell \leq y} \left(1 - \frac{\chi(\ell)}{\ell}\right) \ll_\epsilon q^{1/2+\epsilon}.$$ $\square$

Proof.   Mertens's estimate implies that

$$\prod_{\ell \leq y} \left(1 - \frac{\chi(\ell)}{\ell}\right) \ll q^{1/2+\epsilon} \prod_{\exp\{q^{1/2+\epsilon}\} < \ell \leq y} \left(1 - \frac{\chi(\ell)}{\ell}\right).$$

Moreover, by the discussion in [5, p. 123], we have that

$$\sum_{n \leq x} \Lambda(n) \chi(n) \ll_\epsilon \frac{x}{\log x} \quad (x \geq \exp\{q^{1/2+\epsilon}\}), \tag{3.1}$$

using the trivial bound $\beta < 1 - c/(q^{1/2} \log q)$ for the Siegel zero provided by the class number formula. Partial summation then implies that

$$\log \left\{ \prod_{\exp\{q^{1/2+\epsilon}\} < \ell \leq y} \left(1 - \frac{\chi(\ell)}{\ell}\right) \right\} = - \sum_{\substack{n > 1 \\ \ell | n \Rightarrow \exp\{q^{1/2+\epsilon}\} < \ell \leq y}} \frac{\Lambda(n) \chi(n)}{n \log n}$$

$$= - \sum_{\exp\{q^{1/2+\epsilon}\} < n \leq y} \frac{\Lambda(n) \chi(n)}{n \log n} + O(1) \ll 1,$$

which completes the proof of the lemma.   ∎

The next lemma, which is essentially due to Elliott, allows us to bound the value of $L(1, \chi)$ by a very short product for most quadratic characters χ.

Lemma 3.3. Let $\delta \in (0, 1]$ and $Q \geq 3$. There is a set $\mathcal{E}_\delta(Q) \subset \mathbb{Z} \cap [1, Q]$ of size $\ll Q^\delta$ such that if χ is a nonprincipal, quadratic Dirichlet character modulo some $q \leq Q$, whose conductor does not belong to $\mathcal{E}_\delta(Q)$, then

$$\prod_{y < \ell \leq z} \left(1 - \frac{\chi(\ell)}{\ell}\right) \asymp_\delta 1 \quad (z \geq y \geq \sqrt{\log Q}). \qquad \square$$

Proof. We borrow from the proof of [8, Proposition 2.2], which is essentially due to Elliott. Without loss of generality, we may assume that Q is large enough. By Theorem 1 in [10], for every $\sigma_0 \in [\frac{4}{5}, 1]$, $Q \geq 2$, and $T \geq 1$, there are $\ll (Q^2 T)^{2(1-\sigma_0)/\sigma_0} (\log Q)^{14}$ primitive characters of conductor below Q whose L-function has a zero in the region $\{s = \sigma + it \in \mathbb{C} : \sigma \geq \sigma_0, |t| \leq T\}$. Let $\mathcal{E}_\delta(Q)$ be the set of conductors corresponding to these exceptional characters with $\sigma_0 = 1 - \delta/12 \geq 11/12$ and $T = Q^3$. If χ is a Dirichlet character mod $q \in [1, Q]$ whose conductor is not in $\mathcal{E}_\delta(Q)$, then $L(s, \chi)$ has no zeroes in $\{s = \sigma + it \in \mathbb{C} : \sigma \geq 1 - \delta/12, |t| \leq Q^3\}$. So, by [5, Equation (17), p. 120] applied with $T = \min\{Q^3, x\}$, we find that

$$\sum_{n \leq x} \Lambda(n) \chi(n) \ll x^{1-\delta/12} \log^2 x + \frac{x \log^2 x}{Q^3} + \log^2 Q \ll_\delta \frac{x}{\log x} + \log^2 Q \quad (2 \leq x \leq e^Q).$$

The above estimate also holds for $x \geq e^Q$ by (3.1). Together with partial summation, this implies that

$$\log \left\{ \prod_{y < \ell \leq z} \left(1 - \frac{\chi(\ell)}{\ell}\right) \right\} = -\sum_{\ell \mid n \Rightarrow y < \ell \leq z} \frac{\Lambda(n) \chi(n)}{n \log n} = -\sum_{y < n \leq z} \frac{\Lambda(n) \chi(n)}{n \log n} + O(1) \ll_\delta 1, \quad (3.2)$$

for $z \geq y \geq \log^2 Q$, that is to say, the lemma does hold in this range of y and z. Finally, if $\sqrt{\log Q} \leq y < \log^2 Q$, then setting $w = \min\{z, \log^2 Q\}$, we find that

$$\prod_{y < \ell \leq z} \left(1 - \frac{\chi(\ell)}{\ell}\right) = \prod_{y < \ell \leq w} \left(1 - \frac{\chi(\ell)}{\ell}\right) \prod_{w < \ell \leq z} \left(1 - \frac{\chi(\ell)}{\ell}\right) \asymp_\delta 1,$$

by (3.2) and Mertens's estimate, and the lemma follows. ∎

Next, we state the Bombieri–Vinogradov theorem [3, 14, 15], which will be used to prove Theorem 1.6.

Lemma 3.4 (Bombieri–Vinogradov). Let $A > 0$ be fixed. Then there exists a $B = B(A) > 0$, depending on A, such that

$$\sum_{\substack{q \leq x^{1/2}/(\log x)^B \\ (a,q)=1}} \max_{y \leq x} \left| \pi(y; q, a) - \frac{\mathrm{li}(y)}{\phi(q)} \right| \ll \frac{x}{(\log x)^A}.$$

□

Finally, in order to prove Theorem 1.5, we need the following short interval version of the Bombieri–Vinogradov theorem, due to the third author [9].

Lemma 3.5. Fix $\epsilon > 0$ and $A \geq 1$. For $x \geq h \geq 2$ and $1 \leq Q^2 \leq h/x^{1/6+\epsilon}$, we have that

$$\int_x^{2x} \sum_{q \leq Q} \max_{(a,q)=1} \left| \psi(y+h; q, a) - \psi(y; q, a) - \frac{h}{\phi(q)} \right| \, dy \ll \frac{xh}{(\log x)^A}.$$

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

4 Proof of Theorem 1.3

By Remark 2.3, we readily have that

$$\#S(M, K) \leq \sum_{k \leq K} \sum_{|j| < 2\sqrt{k}} S_{k,j}, \tag{4.1}$$

where

$$S_{k,j} := \#\{m \leq M : km^2 + jm + 1 \text{ is prime}\}.$$

Using the combinatorial sieve to bound $S_{k,j}$, one immediately obtains as in [2] that, for any fixed K, $\#S(M, K) \ll_K M/\log M$. Keeping track of the dependence on j and k of the upper bound for $S_{j,k}$, we prove Theorem 1.3.

In the notation of Lemma 3.1, let $\mathcal{A} = \{km^2 + jm + 1 : m \leq M\}$, and note that

$$\#\{a \in \mathcal{A} : a \equiv 0 \pmod{d}\} = \#\{m \leq M : km^2 + jm + 1 \equiv 0 \pmod{d}\}$$

$$= M \cdot \frac{\rho_{k,j}(d)}{d} + O(\rho_{k,j}(d)),$$

where

$$\rho_{k,j}(d) := \#\{c \in \mathbb{Z}/d\mathbb{Z} : kc^2 + jc + 1 \equiv 0 \pmod{d}\}.$$

The Chinese Remainder Theorem implies that $\rho_{j,k}$ is a multiplicative function. Moreover, by a straightforward computation, we find that

$$\rho_{k,j}(\ell) = \begin{cases} \left(\dfrac{k-j}{2}\right)^2 & \text{if } \ell = 2, \\[2mm] 1 + \left(\dfrac{j^2 - 4k}{\ell}\right) & \text{if } \ell \nmid k \text{ and } \ell \neq 2, \\[2mm] \left(\dfrac{j^2}{\ell}\right) & \text{if } \ell \mid k, \end{cases}$$

for all primes ℓ. Since $S_{k,j} \leq S(\mathcal{A}, y) + y$ for all y, applying Lemma 3.1 with $y = M^{1/2}$ and $u = 1$ yields the estimate

$$S_{k,j} \ll M \prod_{\ell \leq Y} \left(1 - \frac{\rho_{k,j}(\ell)}{\ell}\right) + \sum_{d \leq M^{1/2}} \mu^2(d) |\rho_{k,j}(d)| + M^{1/2}$$

$$\ll M \prod_{\ell \mid k, \ell \leq Y} \left(1 - \frac{\left(\dfrac{j^2 - 4k}{\ell}\right)}{\ell}\right) \prod_{\ell \nmid k, \ell \leq Y} \left(1 - \frac{1 + \left(\dfrac{j^2 - 4k}{\ell}\right)}{\ell}\right) + M^{1/2} \log M$$

$$\ll \frac{M}{\log M} \cdot \frac{k}{\phi(k)} \cdot \prod_{\ell \leq Y} \left(1 - \frac{\left(\dfrac{j^2 - 4k}{\ell}\right)}{\ell}\right) + M^{1/2} \log M.$$

This implies that

$$\#S(M, K) \ll \frac{M}{\log M} \sum_{k \leq K, \, j < 2\sqrt{k}} \frac{k}{\phi(k)} \prod_{\ell \leq Y} \left(1 - \frac{\left(\dfrac{j^2 - 4k}{\ell}\right)}{\ell}\right) + M^{1/2} K^{3/2} \log M.$$

Observing that $j^2 - 4k \in [-4K, -1]$ for j and k as above, we fix $d \in [1, 4K]$ and seek a bound for the sum

$$T_d := \sum_{\substack{k \leq K, \, |j| < 2\sqrt{k} \\ j^2 - 4k = -d}} \frac{k}{\phi(k)} \asymp \sum_{\substack{k \leq K, \, |j| < 2\sqrt{k} \\ j^2 - 4k = -d}} \prod_{\ell \mid k} \left(1 + \frac{1}{\ell}\right).$$

First, note that

$$\prod_{\ell \mid k, \, \ell > \sqrt{\log K}} \left(1 + \frac{1}{\ell}\right) \ll \prod_{\ell \mid k, \, \ell > \log K} \left(1 + \frac{1}{\ell}\right) \ll \exp\left\{\sum_{\ell \mid k, \, \ell > \log K} \frac{1}{\ell}\right\} \leq \exp\left\{\frac{\#\{\ell \mid k\}}{\log K}\right\} \ll 1,$$

by Mertens's estimate and the fact that k has at most $\frac{\log k}{\log 2}$ distinct prime factors. Therefore,

$$\prod_{\ell \mid k} \left(1 + \frac{1}{\ell}\right) \ll \prod_{\ell \mid k,\ \ell \le \sqrt{\log K}} \left(1 + \frac{1}{\ell}\right) = \sum_{\substack{a \mid k \\ P^+(a) \le \sqrt{\log K}}} \frac{\mu^2(a)}{a}.$$

So

$$T_d \ll \sum_{P^+(a) \le \sqrt{\log K}} \frac{\mu^2(a)}{a} \sum_{\substack{k \le K,\ |j| < 2\sqrt{k} \\ a \mid k,\ j^2 - 4k = -d}} 1 \le \sum_{P^+(a) \le (\log K)^{1/2}} \frac{\mu^2(a)}{a} \sum_{\substack{|j| < 2\sqrt{K} \\ 4a \mid j^2 + d}} 1$$

$$\ll \sum_{P^+(a) \le (\log K)^{1/2}} \frac{\mu^2(a)}{a} \cdot \tau(a) \left(\frac{\sqrt{K}}{a} + 1\right) \ll \sqrt{K},$$

since $a \le e^{\pi(\sqrt{\log K})} \ll \sqrt{K}$ for all square-free integers a with $P^+(a) \le \sqrt{\log K}$. Consequently,

$$\#S(M, K) \ll \frac{M\sqrt{K}}{\log M} \sum_{d \le 4K} \prod_{\ell \le Y} \left(1 - \frac{\left(\frac{-d}{\ell}\right)}{\ell}\right) + M^{1/2} K^{3/2} \log M.$$

Using Lemma 3.3 on truncated products of L-functions with $\delta = \frac{1}{4}$ and $Q = 4K$, we find that there is a set $\mathcal{E}$ of $O(K^{1/4})$ integers in $[1, 4K]$ such that if $d \in [1, 4K]$ and the conductor of $\left(\frac{-d}{\cdot}\right)$ is not in $\mathcal{E}$, then

$$\prod_{w_1 < \ell \le w_2} \left(1 - \frac{\left(\frac{-d}{\ell}\right)}{\ell}\right) \asymp 1 \quad (w_2 \ge w_1 \ge \sqrt{\log(4K)}).$$

So, for such a d we find that

$$\prod_{\ell \le Y} \left(1 - \frac{\left(\frac{-d}{\ell}\right)}{\ell}\right) \asymp \prod_{\ell \le z} \left(1 - \frac{\left(\frac{-d}{\ell}\right)}{\ell}\right), \tag{4.2}$$

where $z = \min\{y, \sqrt{\log(4K)}\}$. For the exceptional d's, we write $-d = -a^2 d_1$, where d_1 denotes the conductor of $\left(\frac{-d}{\cdot}\right)$, and note that

$$\prod_{\ell \leq Y}\left(1 - \frac{\left(\frac{-d}{\ell}\right)}{\ell}\right) \ll \frac{a}{\phi(a)}\prod_{\ell \leq Y}\left(1 - \frac{\left(\frac{-d_1}{\ell}\right)}{\ell}\right) \ll \frac{a}{\phi(a)}|d_1|^{3/4},$$

by Lemma 3.2. Hence,

$$\sum_{\substack{d \leq 4K \\ \mathrm{cond}\left(\left(\frac{-d}{\cdot}\right)\right) \in \mathcal{E}}} \prod_{\ell \leq Y}\left(1 - \frac{\left(\frac{-d}{\ell}\right)}{\ell}\right) \leq \sum_{d_1 \in \mathcal{E}} \sum_{1 \leq |a| \leq \sqrt{4K/|d_1|}} \prod_{\ell \leq Y}\left(1 - \frac{\left(\frac{-d_1 a^2}{\ell}\right)}{\ell}\right)$$

$$\ll \sum_{d_1 \in \mathcal{E}} \sum_{1 \leq |a| \leq \sqrt{4K/|d_1|}} \frac{a}{\phi(a)}|d_1|^{3/4}$$

$$\ll \sum_{d_1 \in \mathcal{E}} |d_1|^{1/4}\sqrt{K} \ll K^{1/4} \cdot K^{1/4} \cdot \sqrt{K} = K.$$

The above relation and (4.2) then imply that

$$\#S(M, K) \ll \frac{M\sqrt{K}}{\log M} \sum_{d \leq 4K} \prod_{\ell \leq z}\left(1 - \frac{\left(\frac{-d}{\ell}\right)}{\ell}\right) + \frac{MK^{3/2}}{\log M}. \tag{4.3}$$

In order to control the above sum, we proceed by expanding the product to a sum and inverting the order of summation. We have

$$\sum_{d \leq 4K} \prod_{\ell \leq z}\left(1 - \frac{\left(\frac{-d}{\ell}\right)}{\ell}\right) = \sum_{P^+(a) \leq z} \frac{\mu(a)}{a} \sum_{d \leq 4K}\left(\frac{-d}{a}\right).$$

If $a = 1$, the inner sum is $4K + O(1)$; else, it is $\ll a$. So

$$\sum_{d \leq 4K} \prod_{\ell \leq z}\left(1 - \frac{\left(\frac{-d}{\ell}\right)}{\ell}\right) \ll K + \sum_{P^+(a) \leq z} \mu^2(a) = K + 2^{\pi(z)} \leq K + 2^{\pi(\sqrt{\log(4K)})} \ll K.$$

Inserting the last estimate into ([4.3](#)), we obtain the inequality

$$\#S(M, K) \ll \frac{MK^{3/2}}{\log M},$$

which completes the proof of Theorem 1.3.

5   Proof of Theorem 1.3

Define

$$R(M, K) = \{M/2 < m \leq M, \ K/2 < k \leq K : \text{there is no prime } p \equiv 1 \ (\mathrm{mod}\, m) \text{ in } I_{m^2 k}\}.$$

First, we prove an intermediate result for the cardinality of $R(M, K)$.

Theorem 5.1.   Fix $A \geq 1$ and $\epsilon \in (0, 1/6]$. If $M \leq K^{1/4-\epsilon}$, then

$$\#R(M, K) \ll_{\epsilon, A} \frac{MK}{(\log K)^A}.$$

If, in addition, the Riemann hypothesis for Dirichlet L-functions is true, then the above estimate holds when $M \leq K^{1/2-\epsilon}$.   □

Proof.   We prove both parts of the theorem simultaneously. Set $h = M\sqrt{K}$ and

$$E(y, h; q, a) = \left| \psi(y + h; q, a) - \psi(y; q, a) - \frac{h}{\phi(q)} \right|,$$

and note that if the pair $(m, k) \in R(M, K)$, then

$$E((m\sqrt{k} - 1)^2, h; m, 1) \gg \frac{h}{\phi(m)} \geq \frac{h}{m} \asymp \sqrt{K}.$$

Consequently,

$$\#R(M, K) \ll \frac{1}{\sqrt{K}} \sum_{M/2 < m \leq M} \sum_{K/2 < k \leq K} E((m\sqrt{k} - 1)^2, h; m, 1).$$

Next, observe that $(m\sqrt{k} - 1)^2 \in J := [M^2 K/10, M^2 K]$. We cover the interval J by $O((M^2 K)^{1-\lambda})$ subintervals J_r of length $(M^2 K)^\lambda$ each, where $\lambda \in [1/4, 1/2)$ is a fixed parameter to be chosen later. If $(m\sqrt{k} - 1)^2 \in J_r$, then, for every $y \in J_r$, we have that

$$|E(y, h; m, 1) - E((m\sqrt{k} - 1)^2, h; m, 1)| \leq \#\{n \in J_r \cup (J_r + h) : n \equiv 1 \pmod{m}\}$$

$$\ll 1 + \frac{(M^2 K)^\lambda}{m} \asymp \frac{(M^2 K)^\lambda}{M},$$

since $M \leq K^{1/2}$ and $\lambda \geq \frac{1}{4}$. So, if we let $\mathrm{meas}(J_r)$ denote the length of the interval J_r, then

$$E((m\sqrt{k} - 1)^2, h; m, 1) = \frac{1}{\mathrm{meas}(J_r)} \int_{J_r} E(y, h; m, 1) \, \mathrm{d}y + O\left(\frac{(M^2 K)^\lambda}{M}\right)$$

$$\ll \frac{1}{(M^2 K)^\lambda} \int_{J_r} E(y, h; m, 1) \, \mathrm{d}y + \frac{(M^2 K)^\lambda}{M},$$

and consequently

$$\#R(M, K) \ll \frac{1}{\sqrt{K}} \sum_{M/2 < m \leq M} \sum_{J_r} \left(\frac{1}{(M^2 K)^\lambda} \int_{J_r} E(y, h; m, 1) \, \mathrm{d}y + \frac{(M^2 K)^\lambda}{M}\right) \sum_{\substack{K/2 < k \leq K \\ (m\sqrt{k}-1)^2 \in J_r}} 1.$$

For every fixed $m \in [M/2, M]$ and every fixed interval J_r, there are at most $1 + O((M^2 K)^\lambda / M^2)$ values of k with $(m\sqrt{k} - 1)^2 \in J_r$. Since

$$\frac{(M^2 K)^\lambda}{M^2} \gg 1 \iff M \ll K^{\lambda/(2-2\lambda)},$$

by choosing $\lambda \in [1/4, 1/2)$ appropriately in terms of ϵ, we obtain that $M \leq K^{1/2-\epsilon}$ implies that $1 + O((M^2 K)^\lambda / M^2) = O((M^2 K)^\lambda / M^2)$. Therefore, there are at most $O((M^2 K)^\lambda / M^2)$ values of k with $(m\sqrt{k} - 1)^2 \in J_r$, and we deduce that

$$\#R(M, K) \ll \frac{1}{\sqrt{K}} \sum_{M/2 < m \leq M} \sum_{J_r} \left(\frac{1}{(M^2 K)^\lambda} \int_{J_r} E(y, h; m, 1) \, \mathrm{d}y + \frac{(M^2 K)^\lambda}{M}\right) \frac{(M^2 K)^\lambda}{M^2}$$

$$\leq \frac{1}{M^2 \sqrt{K}} \sum_{M/2 < m \leq M} \int_{M^2 K/20}^{M^2 K} E(y, h; m, 1) \, \mathrm{d}y + O(M^{2\lambda} K^{1/2+\lambda}). \tag{5.1}$$

If $M \leq K^{1/4-\epsilon}$, then we have

$$M^2 \leq \frac{M\sqrt{K}}{(M^2 K)^{1/6+\epsilon/2}} = \frac{h}{(M^2 K)^{1/6+\epsilon/2}},$$

and we can apply the Lemma 3.5 to obtain that

$$\sum_{M/2 < m \leq M} \int_{M^2 K/20}^{M^2 K} E(y, h; m, 1) \, \mathrm{d}y \ll \frac{M^2 K h}{(\log K)^A} = \frac{M^3 K^{3/2}}{(\log K)^A}. \tag{5.2}$$

Similarly, if $M \leq K^{1/2-\epsilon}$, then

$$M^2 \leq \frac{M\sqrt{K}}{(M^2 K)^{\epsilon/2}} = \frac{h}{(M^2 K)^{\epsilon/2}}.$$

So, if the Riemann hypothesis for Dirichlet L-functions holds, then Lemma 3.5 implies that (5.2) holds in this case too. Inserting this relation into (5.1), we deduce that

$$\#R(M, K) \ll_{\epsilon, A} \frac{MK}{(\log K)^A} + M^{2\lambda} K^{1/2+\lambda} \ll_{\epsilon, A} \frac{MK}{(\log K)^A},$$

since $\lambda < \frac{1}{2}$ and $M \leq K^{1/2-\epsilon}$. This completes the proof of Theorem 5.1. ∎

Proof of Theorem 1.5.   Let ϵ, M, and K be as in the statement of Theorem 1.5. Clearly,

$$\#\{m \leq M,\, k \leq K : \text{there is no prime } p \equiv 1 \ (\mathrm{mod}\, m) \text{ in } I_{m^2 k}\} \leq \sum_{2^a \leq 2M,\, 2^b \leq 2K} \#R(2^a, 2^b).$$

If $2^b \leq K^{1-\epsilon}$, then we use the trivial bound $\#R(2^a, 2^b) \leq 2^{a+b}$. Otherwise, we have that

$$2^{a-1} \leq M \leq \begin{cases} K^{1/4-\epsilon} \leq 2^{b(1/4-\epsilon/2)} & \text{if } M \leq K^{1/4-\epsilon}, \\ K^{1/2-\epsilon} \leq 2^{b(1/2-\epsilon/2)} & \text{if } M \leq K^{1/2-\epsilon}, \end{cases}$$

and so Theorem 5.1 implies that $\#R(2^a, 2^b) \ll_{\epsilon, A} 2^{a+b}/b^A$. Consequently,

$$\#\{m \leq M,\, k \leq K : \text{there is no prime } p \equiv 1 \ (\mathrm{mod}\, m) \text{ in } I_{m^2 k}\}$$

$$\ll_A \sum_{\substack{2^a \leq 2M \\ 2^b \leq K^{1-\epsilon}}} 2^{a+b} + \sum_{\substack{2^a \leq 2M \\ K^{1-\epsilon} < 2^b \leq 2K}} \frac{2^{a+b}}{b^A} \ll_{\epsilon, A} \frac{MK}{(\log K)^A}.$$

The above estimate and Remark 2.3 complete the proof of Theorem 1.5. ∎

6 Proof of Theorem 1.6

Note that, as a direct consequence of Corollary 2.2 and the fact that $I_1 = (0, 4)$, the primes 2 and 3 are always contained in $S(M, K)$. In particular, $\#S(M, K) \geq 2$ and hence we may assume without loss of generality that K is large enough. Also, we may assume that M is an integer, so that the interval $(3M/4, M]$ always contains integers.

From Remark 2.3, we have that

$$\#S(M, K) = \sum_{m \leq M} \sum_{k \leq K} \mathbb{I}(m, k).$$

Now, note that

$$\mathbb{I}(m, k) \geq \frac{\phi(m) \log(4\sqrt{k})}{8m\sqrt{k}} \cdot \#\{p \in I_{m^2 k} : p \equiv 1 \,(\mathrm{mod}\, m)\},$$

by the Brun–Titchmarsh inequality. Therefore, we deduce that

$$\#S(M, K) \gg \frac{\log K}{\sqrt{K}} \sum_{\substack{3M/4 < m \leq M \\ K/5 < k \leq K}} \frac{\phi(m)}{m} \sum_{\substack{p \in I_{m^2 k} \\ p \equiv 1 \,(\mathrm{mod}\, m)}} 1$$

$$\geq \frac{\log K}{\sqrt{K}} \sum_{\substack{M^2 K/4 < p < M^2 K/3}} \sum_{\substack{3M/4 < m \leq M \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \frac{\phi(m)}{m} \sum_{\substack{K/5 < k \leq K \\ p \in I_{m^2 k}}} 1, \qquad (6.1)$$

by switching the order of summation and restricting p in the interval $(M^2 K/4, M^2 K/3]$. Fix p and m as in (6.1) and note that if k is an integer for which $p \in I_{m^2 k}$, then we necessarily have that $K/5 < k \leq K$. So

$$\sum_{\substack{K/5 < k \leq K \\ p \in I_{m^2 k}}} 1 = \sum_{k \in \mathbb{Z}\,:\, p \in I_{m^2 k}} 1 = \#\left\{ k \in \mathbb{Z} : \frac{p - 2\sqrt{p} + 1}{m^2} < k < \frac{p + 2\sqrt{p} + 1}{m^2} \right\} \gg \frac{\sqrt{p}}{m^2} \asymp \frac{\sqrt{K}}{M},$$

since

$$\frac{4\sqrt{p}}{m^2} > \frac{4\sqrt{M^2 K/4}}{M^2} = \frac{2\sqrt{K}}{M} \geq 2,$$

by our assumption that $M \leq \sqrt{K}$. Consequently,

$$\#S(M, K) \gg \frac{\log K}{M} \sum_{M^2 K/4 < p < M^2 K/3} \sum_{\substack{3M/4 < m \leq M \\ p \equiv 1 \,(\mathrm{mod}\, m)}} \frac{\phi(m)}{m}$$

$$= \frac{\log K}{M} \sum_{3M/4 < m \leq M} \frac{\phi(m)}{m} \left(\pi(M^2 K/3; m, 1) - \pi(M^2 K/4; m, 1) \right)$$

$$= \frac{\log K}{M} \left(\sum_{3M/4 < m \leq M} \frac{\phi(m)}{m} \frac{\mathrm{li}(M^2 K/3) - \mathrm{li}(M^2 K/4)}{\phi(m)} + E \right), \qquad (6.2)$$

where

$$E = \sum_{3M/4 < m \leq M} \frac{\phi(m)}{m} \left(\pi(M^2 K/3; m, 1) - \pi(M^2 K/4; m, 1) - \frac{\mathrm{li}(M^2 K/3) - \mathrm{li}(M^2 K/4)}{\phi(m)} \right).$$

The sum over m in (6.2) is

$$\sum_{3M/4 < m \leq M} \frac{\mathrm{li}(M^2 K/3) - \mathrm{li}(M^2 K/4)}{m} \gg \sum_{3M/4 < m \leq M} \frac{M^2 K}{M \log(M^2 K)} \asymp \frac{M^2 K}{\log K}.$$

It is in this step that we require that the interval $(3M/4, M]$ contains an integer. Furthermore, we have

$$|E| \leq \sum_{3M/4 < m \leq M} \left| \pi(M^2 K/4; m, 1) - \pi(M^2 K/3; m, 1) - \frac{\mathrm{li}(M^2 K/3) - \mathrm{li}(M^2 K/4)}{\phi(m)} \right|$$

$$\ll \frac{M^2 K}{\log^2(M^2 K)},$$

by Lemma 3.4. Combining the above estimates, we find that there is an absolute constant c such that

$$\#S(M, K) \geq cMK + O\left(\frac{MK}{\log K} \right) \geq \frac{cMK}{2},$$

provided that K is large enough. This completes the proof of Theorem 1.6.

Acknowledgements

Funding

References

[1]   Baker, R. C., G. Harman, and J. Pintz. "The difference between consecutive primes. II." *Proceedings of the London Mathematical Society. Third Series* 83, no. 3 (2001): 532–62.

[2]   Banks, W. D., F. Pappalardi, and I. Shparlinski. "On group structures realized by elliptic curves over arbitrary finite fields." *Experimental Mathematics* 21, no. 1 (2012): 11–25.

[3]   Bombieri, E. "On the large sieve." *Mathematika* 12, no. 2 (1965): 201–25.

[4]   Chandee, V., C. David, D. Koukoulopoulos, and E. Smith. "Elliptic curves over $\mathbb{F}_p$ with a given group structure." in preparation.

[5]   Davenport, H. *Multiplicative Number Theory*, 3rd ed. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics 74. New York: Springer, 2000.

[6]   David, C. and E. Smith. "A Cohen–Lenstra phenomenon for elliptic curves." *Journal of the London Mathematical Society* (2012): preprint arXiv:1206.1585.

[7]   Deuring, M. "Die Typen der Multiplikatorenringe elliptischer Funktionenkorper." *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 14, no. 1 (1941): 197–272.

[8]   Granville, A. and K. Soundararajan. "The distribution of values of $L(1, \chi_d)$." *Geometric and Functional Analysis* 13, no. 5 (2003): 992–1028.

[9]   Koukoulopoulos, D. "Primes in short arithmetic progressions." in preparation.

[10]   Montgomery, H. L. "Zeros of L-functions." *Inventiones Mathematicae* 8, no. 4 (1969): 346–54.

[11]   Rück, H.-G. "A note on elliptic curves over finite fields." *Mathematics of Computation* 49, no. 179 (1987): 301–04.

[12]   Schoof, R. "Nonsingular plane cubic curves over finite fields." *Journal of Combinatorial Theory. Series A* 46, no. 2 (1987): 183–211.

[13]   Tenenbaum, G. *Introduction to Analytic and Probabilistic Number Theory*. Cambridge: Cambridge University Press, 1995.

[14]   Vinogradov, A. I. "The density hypothesis for Dirichet L-series." *Izvestiya Akademii Nauk SSSR Seriya Matematika* 29, no. 4 (1965): 903–34 (Russian).

[15]   Vinogradov, A. I. "Correction to the paper of A. I. Vinogradov 'On the density hypothesis for the Dirichlet L-series'." *Izvestiya Akademii Nauk SSSR Seriya Matematika* 30, no. 3 (1966): 719–20 (Russian).