

AVERAGE TWIN PRIME CONJECTURE FOR ELLIPTIC CURVES

ANTAL BALOG, ALINA-CARMEN COJOCARU AND CHANTAL DAVID

ABSTRACT. Let E be an elliptic curve over \mathbb{Q} . In 1988, N. Koblitz conjectured a precise asymptotic for the number of primes p up to x such that the order of the group of points of E over \mathbb{F}_p is prime. This is an analogue of the Hardy–Littlewood twin prime conjecture in the case of elliptic curves.

Koblitz’s Conjecture is still widely open. In this paper we prove that Koblitz’s Conjecture is true on average over a two-parameter family of elliptic curves. One of the key ingredients in the proof is a short average distribution result of primes in the style of Barban–Davenport–Halberstam, where the average is taken over prime differences and over arithmetic progressions.

CONTENTS

1. Introduction	1
2. Average of Koblitz’s Conjecture and the conjectural constant	5
3. Reduction of Theorem 1 and Corollary 2 to Theorem 3	6
3.1. Reduction of Theorem 1 to Theorem 3	6
3.2. Proof of Corollary 2	8
3.3. Character sums	9
4. Reduction of Theorem 3 to an average of Kronecker class numbers	14
5. Reduction of Proposition 12 to an average twin prime conjecture	15
6. Average of the twin prime conjecture and proof of Theorem 4	18
7. Proof of Proposition 13	24
7.1. Estimate of the error term in Proposition 13	25
7.2. Computation of the constant in Proposition 13	26
7.3. The average constant	30
References	33

1. INTRODUCTION

A well-known open problem in number theory is *the twin prime conjecture*, which states that there exist infinitely many primes p such that $p + 2$ is also a prime. This conjecture was generalized by A. de Polignac in 1849 to the statement that, for any even integer $r \neq 0$, there exist infinitely many primes p such that $p + r$ is also a prime. In 1922, G.H. Hardy and J. Littlewood [HaLi] made this statement precise, predicting that, as $x \rightarrow \infty$,

$$\#\{p \leq x : p + r \text{ is prime}\} \sim \mathfrak{S}(r) \frac{x}{\log^2 x},$$

where

$$(1) \quad \mathfrak{S}(r) := \begin{cases} 2 \prod_{\ell \neq 2} \frac{\ell(\ell-2)}{(\ell-1)^2} \prod_{\ell | r, \ell \neq 2} \frac{\ell-1}{\ell-2} & \text{if } 2 \mid r, \\ 0 & \text{otherwise.} \end{cases}$$

Here and everywhere in the paper, p and ℓ are used to denote primes.

A. Balog was supported by Hungarian OTKA grants K49693 and K72731. A.C. Cojocaru was partially supported by NSF grants DMS-0636750 and DMS-0747724. C. David was partially supported by an NSERC Discovery Grant 155635-2008.

Even though still inaccessible by current methods, the twin prime conjecture has generated tremendous advances in number theory. In particular, in 1915-1919, V. Brun developed what is now known as the theory of the Brun sieve to prove that $\sum_{\substack{p \\ p+2 \text{ prime}}} \frac{1}{p} < \infty$, as well as upper bounds of the right order of magnitude for

the number of twin primes $p \leq x$. Brun's methods opened the way to sieve theory, leading to the important achievement of J. Chen from 1966 that $\#\{p \leq x : p+r = P_2\} \gg \frac{x}{\log^2 x}$, where, for an integer k , P_k denotes the product of at most k primes. This result relies on other major achievements of sieve theory, such as applications of the large sieve to averages of primes in an arithmetic progression. Subsequently, further important work has been done concerning average versions of the twin prime conjecture, the size of the set of exceptions to the twin prime conjecture, and the size of small gaps between consecutive primes.

The twin prime conjecture can be generalized in many directions. For instance, the Hardy-Littlewood heuristic can be used to predict the (same) asymptotic formula for the number of primes $p \leq x$ such that $\frac{p-1}{2}$ is also a prime. This question may be reformulated as counting the number of primes $p \leq x$ such that the group $\mathbb{F}_p^*/\{\pm 1\}$ is of prime order. Such a reformulation may then be easily generalized to other groups, such as the group of points of an elliptic curve: given an elliptic curve E/\mathbb{Q} over the field of rational numbers, count the number of primes $p \leq x$ of good reduction for E such that the group $E(\mathbb{F}_p)/E(\mathbb{Q})_{\text{tors}}$ is of prime order, where $E(\mathbb{F}_p)$ denotes the reduction of E modulo p and $E(\mathbb{Q})_{\text{tors}}$ denotes the torsion subgroup of E/\mathbb{Q} . This question has theoretical relevance to elliptic curve cryptography and was first considered by N. Koblitz in 1988:

Koblitz's Conjecture [Ko]

Let E/\mathbb{Q} be an elliptic curve without complex multiplication defined over the field of rational numbers. Then there exists a constant $C(E)$ such that, as $x \rightarrow \infty$,

$$\pi_E^{\text{twin}}(x) := \#\{p \leq x : |E(\mathbb{F}_p)| \text{ is prime}\} \sim C(E) \frac{x}{\log^2 x}.$$

We remark that the constant $C(E)$ in Koblitz's Conjecture can be zero, and the asymptotic relation is then interpreted to mean that there are only finitely many primes p such that $|E(\mathbb{F}_p)|$ is prime. This happens for curves isogenous to a curve with non-trivial rational torsion, but not exclusively. It also happens, for example, for the curve with Weierstrass equation $Y^2 = X^3 + 9X + 18$ which is not isogenous to a curve with rational torsion, but has the property that $(|E(\mathbb{F}_p)|, 6) > 1$ for any prime p . This example is due to N. Jones and is discussed in [Zy2]; for other examples, see [Jo3].

A candidate for the explicit constant $C(E)$ was given by Koblitz in his paper and was later corrected by D. Zywna [Zy2] in the generic case of an elliptic curve E/\mathbb{Q} without complex multiplication; in this case, it will also be described in detail in Section 2. For the case of an elliptic curve E/\mathbb{Q} with complex multiplication, we refer the reader to [Ko], [Jo2], and [Zy2].

To investigate Koblitz's Conjecture, it is useful to write the number of points of E over \mathbb{F}_p as

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

where $a_p(E)$ satisfies the Hasse bound $|a_p(E)| \leq 2\sqrt{p}$. In particular, this makes the analogy between Koblitz's Conjecture and the twin prime conjecture more apparent.

Based on this analogy, one can employ sieve methods to find partial results towards Koblitz's Conjecture. This approach was initiated by S.A. Miri and V.K. Murty [MiMu] and further refined by A. Steuding and J. Weng [StWe], the second author [Co], H. Iwaniec and J. Jiménez Urroz [IwJU], [JU], and the third author and J. Wu [DaWu]. Consequently, we currently know: upper bounds of the right order of magnitude for $\pi_E^{\text{twin}}(x)$, provided a Generalized quasi-Riemann Hypothesis holds if E/\mathbb{Q} is without complex multiplication and unconditional otherwise [Co], [Zy1]; various lower bounds in the style of Chen's result [MiMu], [StWe], [Co], [IwJU], [JU], [DaWu], again conditional if E/\mathbb{Q} is without complex multiplication and unconditional otherwise. Regarding lower bounds, the best result was obtained in [JU] for elliptic curves with complex multiplication; namely,

$$\#\left\{p \leq x : \frac{1}{t_E} |E(\mathbb{F}_p)| = P_2\right\} \gg \frac{x}{\log^2 x},$$

where t_E is the least common multiple of $|E'(\mathbb{Q})_{\text{tors}}|$, with E' varying over all elliptic curves over \mathbb{Q} which are \mathbb{Q} -isogenous to E .

The main purpose of our paper is to prove the validity of Koblitz's Conjecture on average over a set of elliptic curves E/\mathbb{Q} :

Theorem 1. *Let $x > 0$ be a variable and let $\varepsilon > 0$. Let $A = A(x), B = B(x)$ be parameters such that $A, B > x^\varepsilon$ and $AB > x \log^{10} x$. Let $\mathcal{C} = \mathcal{C}(A, B)$ be the set of elliptic curves $E(a, b) : Y^2 = X^3 + aX + b$, where $a, b \in \mathbb{Z}$ with $|a| \leq A, |b| \leq B$. Then, as $x \rightarrow \infty$,*

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) = \mathfrak{C} \frac{x}{\log^2 x} + O\left(\frac{x}{\log^3 x}\right),$$

where \mathfrak{C} is the non-zero constant

$$\mathfrak{C} := \frac{2}{3} \prod_{\ell \neq 2} \frac{\ell^4 - 2\ell^3 - \ell^2 + 3\ell}{(\ell - 1)^3(\ell + 1)} = \prod_{\ell} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\right) \approx 0.505166168239435774.$$

As will be explained in Section 2, the average constant \mathfrak{C} gives further evidence for the conjectural constant of Koblitz's Conjecture. In particular, it leads to the following "almost all" result:

Corollary 2. *We keep the above notation and consider a family $\mathcal{C} = \mathcal{C}(A, B)$ of elliptic curves for which $A, B > x^\varepsilon$, $AB > x^2 \log^{14} x$ and $\lim_{A, B \rightarrow \infty} \frac{\log B \cdot \log^7 A}{B} = 0$. Then, for any real positive function $f(x) = o(\log x)$, with at most*

$$O_\varepsilon\left(\frac{f(x)^2}{\log^2 x} |\mathcal{C}|\right)$$

exceptions, the curves $E \in \mathcal{C}$ satisfy the refined Koblitz conjecture

$$\left| \pi_E^{\text{twin}}(x) - C(E) \frac{x}{\log^2 x} \right| \ll \frac{x}{f(x) \log^2 x}.$$

Thus, even though we do not construct any particular elliptic curve E/\mathbb{Q} for which Koblitz's Conjecture holds, we provide strong evidence that the conjecture is indeed true.

Theorem 1 is the consequence of two key ingredients of independent interest, which we state below. The first one is concerned with the distribution of elliptic curves over a fixed finite field and having a prime number of points:

Theorem 3. *Let p be a prime and let*

$$\pi^*(p) := \#\{E/\mathbb{F}_p \text{ elliptic curve} : |E(\mathbb{F}_p)| \text{ is prime}\}.$$

Then, as $x \rightarrow \infty$,

$$\sum_{p \leq x} \pi^*(p) = \frac{\mathfrak{C} x^3}{3 \log^2 x} + O\left(\frac{x^3}{\log^3 x}\right),$$

where \mathfrak{C} is the constant of Theorem 1.

The second ingredient is an average of the standard twin prime conjecture. Such averages were first considered by N.G. Chudakov [Chu] and A.F. Lavrik [Lav], and then, among others, by A. Balog [Bal], who added distribution in residue classes, and by A. Perelli and J. Pintz [PePi], who shortened the average. The length of the average needed for our application to elliptic curves is dictated by Hasse's bound and is *short* (\sqrt{x} compared to x); additionally, we also need distribution in *residue classes*. Such a mixture of additional features is not in the literature and is proven here:

Theorem 4. *Let $x > 0$ and let $\varepsilon, M > 0$. Then there exists an integer $N(M) > 0$ such that, for any $x^{\frac{1}{3}+\varepsilon} \leq R \leq x$, $N > N(M)$, $Q \leq x \log^{-N} x$, and X, Y satisfying $2 \leq X + Y \leq x$, we have*

$$\sum_{0 < |r| \leq R} \sum_{q \leq Q} \sum_{a \pmod{q}} \left| \sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q} \\ p-p'=r}} \log p \cdot \log p' - \mathfrak{S}(r, q, a) Y \right|^2 \ll \frac{Rx^2}{\log^M x},$$

where

$$\mathfrak{S}(r, q, a) := \begin{cases} \frac{1}{\phi(q)} \mathfrak{S}(rq) & \text{if } 2 \mid r, (a, q) = (a-r, q) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

$\mathfrak{S}(rq)$ is as in (1) and $\phi(q)$ is the Euler function of q . Here (and in what follows), q denotes a positive integer, and p, p' and ℓ denote rational primes.

Remarks

- (1) There are several open questions about the reductions of an elliptic curve E/\mathbb{Q} modulo primes. In particular, for a fixed integer $a \neq 0$, a conjecture of Lang and Trotter [LaTr] predicts that, as $x \rightarrow \infty$,

$$\#\{p \leq x : a_p(E) = a\} \sim C'(E) \frac{\sqrt{x}}{\log x}$$

for some constant $C'(E)$. This conjecture is known to hold on average over elliptic curves E/\mathbb{Q} in a two-parameter family $\mathcal{C} = \mathcal{C}(A, B)$ [DaPa1]. The size of this family was further reduced from $A, B > x^{1+\varepsilon}$ [DaPa1] to $A, B > x^\varepsilon, AB > x^{\frac{3}{2}+\varepsilon}$ [Bai] by following the techniques of [FoMu].

- (2) The size of the family \mathcal{C} in Theorem 1 is substantially smaller than that in the afore-mentioned average of the Lang-Trotter Conjecture of [Bai]. This is because the set of elliptic curves over E/\mathbb{F}_p with a fixed trace $a_p(E)$ is far thinner (among all elliptic curves over \mathbb{F}_p) than the set of elliptic curves over \mathbb{F}_p for which the group of points has prime order.
- (3) Theorem 1 and Corollary 2 may be viewed as GL_2 -generalizations of the various existing average results for the twin prime conjecture, in particular of Theorem 4. Similarly, the average results for the Lang-Trotter Conjecture above may be viewed as GL_2 -generalizations of the Barban-Davenport-Halberstam Theorem on averages of primes in an arithmetic progression. While we do not compare the orders of difficulty of the Lang-Trotter and Koblitz's Conjectures, our work shows that the average of Koblitz's Conjecture requires a finer analysis than the average of the Lang-Trotter Conjecture.
- (4) Similarly to the work on the exceptional set in the twin prime conjecture (see [MoVa] and [PePi]), it would be interesting to investigate further the size of the exceptional set in Koblitz's Conjecture and thus improve on Corollary 2.
- (5) Theorem 3 is only concerned with the distribution of elliptic curves over \mathbb{F}_p having a prime number of points. More properties of this distribution could be obtained by considering the higher moments

$$M_k(x) := \sum_{p \leq x} (\pi^*(p))^k \quad \text{for } k \geq 1.$$

- (6) Finally, we remark that Koblitz's Conjecture has a version stated over number fields in [Zy2], and it would be interesting to see if one can obtain evidence for this more general conjecture by averaging over curves over number fields. Some averages of the Lang-Trotter Conjecture over number fields were considered for $K = \mathbb{Q}(i)$ in [DaPa2], and, very recently, for abelian extensions of \mathbb{Q} in [Wa]. It would be interesting to do a similar analysis for Koblitz's Conjecture.

The structure of the paper is as follows. In Section 2, we present the heuristic reasoning behind Koblitz's Conjecture and discuss the constant \mathfrak{C} . In Section 3, we reduce Theorem 1 to Theorem 3 and we prove Corollary 2. In Section 4, we reduce the statement of Theorem 3 to an average of Kronecker class numbers (Proposition 12). In Section 5, we show how an average of the twin prime conjecture (Proposition 13) implies Proposition 12. Finally, in Sections 6-7, we give the proofs of the afore-mentioned Proposition 13 and of Theorem 4.

2. AVERAGE OF KOBLITZ'S CONJECTURE AND THE CONJECTURAL CONSTANT

The constant $C(E)$ in Koblitz's Conjecture is based on the following heuristic argument, which is reminiscent of the argument leading to the classical twin prime constant of Hardy and Littlewood (as explained, for example, in [So]).

Let E/\mathbb{Q} be an elliptic curve without complex multiplication. We want to count the number of primes p such that $|E(\mathbb{F}_p)| = p + 1 - a_p(E)$ is also a prime. We need to ensure that, for each prime ℓ , the number $p + 1 - a_p(E)$ is not divisible by ℓ . Clearly, for a fixed prime ℓ , the probability that a random integer n is not divisible by ℓ is $(\ell - 1)/\ell$. To compute the probability that $\ell \nmid p + 1 - a_p(E)$, we consider the action of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the torsion points of E , which leads to the absolute Galois representation

$$\rho_E : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_2(\hat{\mathbb{Z}})$$

attached to E , and, in particular, for any integer m , to the injection

$$\rho_{E,m} : \text{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \hookrightarrow \text{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

where $\mathbb{Q}(E[m])$ is the field obtained by adjoining to \mathbb{Q} the coordinates of the m -division points $E[m]$. By studying the action of the Frobenius map σ_p on the torsion points of E , it follows that

$$\begin{aligned} \text{tr}(\rho_{E,m}(\sigma_p)) &\equiv a_p(E) \pmod{m}, \\ \det(\rho_{E,m}(\sigma_p)) &\equiv p \pmod{m}, \end{aligned}$$

for all primes $p \nmid m$ of good reduction for E . Then, for a prime ℓ , the probability that $\ell \nmid p + 1 - a_p(E)$ may be evaluated by counting matrices g in $\text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that $\det(g) + 1 - \text{tr}(g) \not\equiv 0 \pmod{\ell}$.

Let $G(m)$ be the image of $\rho_{E,m}$ in $\text{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and let

$$\Omega(m) := \{g \in G(m) : (\det(g) + 1 - \text{tr}(g), m) \neq 1\}.$$

In particular, if $m = \ell$,

$$\Omega(\ell) = \{g \in G(\ell) : \det(g) + 1 - \text{tr}(g) \equiv 0 \pmod{\ell}\}.$$

Then, at each prime ℓ , the correcting probability factor is the quotient

$$\frac{1 - \frac{|\Omega(\ell)|}{|G(\ell)|}}{1 - \frac{1}{\ell}},$$

where the numerator is the probability that $p + 1 - a_p(E)$ is not divisible by ℓ and the denominator is the probability that a random integer is not divisible by ℓ .

If $G(\ell) = \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then we have

$$\frac{1 - \frac{|\Omega(\ell)|}{|G(\ell)|}}{1 - \frac{1}{\ell}} = 1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}.$$

If E/\mathbb{Q} is without complex multiplication, the constant $C(E)$ of [Ko] is defined as the product over all primes ℓ of the local factors above. But the probabilities are not necessarily independent from one prime to another, as observed by Serre [Se]; Zywinia [Zy2] refined the constant $C(E)$ by including this observation.

The dependence of the probabilities can be quantified: there is an integer m_E which has the property that the probabilities are independent for primes $\ell \nmid m_E$; more precisely, m_E is the smallest positive integer such that the image of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ under the absolute Galois representation of E is $\pi^{-1}(G(m_E))$, where $\pi : \text{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \text{GL}_2(\mathbb{Z}/m_E\mathbb{Z})$ is the natural projection. For each elliptic curve E/\mathbb{Q} without complex multiplication, the constant $C(E)$ in Koblitz's Conjecture is then expected to be

$$(2) \quad C(E) = \frac{1 - \frac{|\Omega(m_E)|}{|G(m_E)|}}{\prod_{\ell|m_E} \left(1 - \frac{1}{\ell}\right)} \times \prod_{\ell \nmid m_E} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}\right).$$

Some numerical evidence for this constant can be found in [Zy2].

We remark that, even though m_E is never 1 [Se], it is possible for some elliptic curves E/\mathbb{Q} to have

$$C(E) = \prod_{\ell} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)} \right) = \mathfrak{C}.$$

Indeed, as shown in [Jo2, Proposition 14], if E/\mathbb{Q} is a Serre curve such that the squarefree part of its minimal discriminant is $\equiv 2, 3 \pmod{4}$, then $C(E) = \mathfrak{C}$; moreover, it was shown by Jones in a previous work [Jo1] that, in an average sense, most curves E/\mathbb{Q} are Serre curves.¹

The average constant \mathfrak{C} of Theorem 1 should not be thought of, however, as the constant of *any* given curve over \mathbb{Q} , but as the *average* of all the constants $C(E)$. Indeed, in [Jo2], Jones shows that if one assumes a positive answer to a well-known question of Serre, then the average of the conjectural constants $C(E)$ of (2) is indeed the average constant of Theorem 1. This result is now known to hold unconditionally [Zy2]. Our result then gives evidence for both the asymptotic of Koblitz's Conjecture and the constant appearing in the conjecture.

Theorem 5. (*Jones [Jo2, Theorem 6], Zywinina [Zy2, Proposition 9.1]*)

For any positive integer k , we have that, as $A, B \rightarrow \infty$,

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} |C(E) - \mathfrak{C}|^k \ll_k \max \left\{ \left(\frac{\log B \cdot (\log A)^7}{B} \right)^{\frac{k}{k+1}}, \frac{\log^\gamma(\min\{A, B\})}{\sqrt{\min\{A, B\}}} \right\}$$

for some explicit constant γ . In particular, if $\lim_{A, B \rightarrow \infty} \frac{\log B \cdot \log^7 A}{B} = 0$, then $\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} C(E) \sim \mathfrak{C}$.

3. REDUCTION OF THEOREM 1 AND COROLLARY 2 TO THEOREM 3

In this section we show how Theorem 1 and its Corollary 2 reduce to Theorem 3. We will place a special emphasis on the length of the average in Theorem 1, which, as we mentioned, is shorter than what can be obtained for the average of the Lang-Trotter Conjecture.

3.1. Reduction of Theorem 1 to Theorem 3. Let $x > 0$ and let \mathcal{C} be the family of elliptic curves introduced in Theorem 1. In this section we show how the average of $\pi_E^{\text{twin}}(x)$ over E/\mathbb{Q} reduces to an average of $\pi^*(p)$, which is estimated in Theorem 3.

As a start, let us write

$$\begin{aligned} \frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) &= \frac{1}{|\mathcal{C}|} \sum_{p \leq x} \sum_{s, t \in \mathbb{F}_p} \#\{a \leq A, b \leq B : a \equiv s \pmod{p}, b \equiv t \pmod{p}, |E(a, b)(\mathbb{F}_p)| \text{ prime}\} \\ &= \frac{1}{|\mathcal{C}|} \sum_{p \leq x} \sum_{\substack{s, t \in \mathbb{F}_p \\ |E(s, t)| \text{ prime}}} \sum_{\substack{|a| \leq A, |b| \leq B \\ a \equiv s \pmod{p} \\ b \equiv t \pmod{p}}} 1, \end{aligned}$$

where $E(s, t)$ is the elliptic curve over \mathbb{F}_p with model $Y^2 = X^3 + sX + t$ and $|E(s, t)|$ is the number of its \mathbb{F}_p -rational points. Thus we partitioned the elliptic curves in \mathcal{C} according to their models over \mathbb{F}_p .

Note that the number of terms in the middle sum above is $\pi^*(p)$. The innermost sum is simply

$$\left(\frac{2A}{p} + O(1) \right) \left(\frac{2B}{p} + O(1) \right) \sim \frac{4AB}{p^2},$$

provided A, B are large enough with respect to x . This leads to the asymptotic

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) \sim \sum_{p \leq x} \frac{\pi^*(p)}{p^2}.$$

We remark that this approach leads to a poor average, since we need to take $AB > x^{2+\varepsilon}$ in order to obtain the asymptotic formula above. A substantial improvement can be obtained from a better use of the

¹We recall that an elliptic curve E/\mathbb{Q} is called a Serre curve if, for each positive integer m , one has $[\text{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \text{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})] \leq 2$.

uniform distribution of isomorphic elliptic curves. More precisely, instead of partitioning the elliptic curves in \mathcal{C} according to their models over \mathbb{F}_p , we partition them according to their isomorphism classes over \mathbb{F}_p , as follows.

After fixing an elliptic curve $E(s, t)$ over \mathbb{F}_p , we enumerate the curves $E(a, b) \in \mathcal{C}$ whose reduction modulo p is isomorphic to $E(s, t)$ over \mathbb{F}_p . It is well known that, if $s, t, a, b \in \mathbb{F}_p$, then the two elliptic curves $E(s, t)$ and $E(a, b)$ are isomorphic over \mathbb{F}_p if and only if $a = su^4$ and $b = tu^6$ for some $u \in \mathbb{F}_p^*$; moreover, there are $(p-1)/|\text{Aut}(E(s, t))|$ elliptic curves over \mathbb{F}_p which are \mathbb{F}_p -isomorphic to $E(s, t)$. Here, $\text{Aut}(E)$ is the automorphism group of the elliptic curve E . This approach leads to

$$(3) \quad \frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) = \frac{1}{|\mathcal{C}|} \sum_{p \leq x} \sum_{\substack{s, t \in \mathbb{F}_p \\ |E(s, t)| \text{ prime}}} \frac{|\text{Aut}(E(s, t))|}{p-1} \sum_{\substack{|a| \leq A, |b| \leq B, \exists 1 \leq u < p: \\ a \equiv su^4 \pmod{p} \\ b \equiv tu^6 \pmod{p}}} 1,$$

where, for each fixed $s, t \in \mathbb{F}_p$, the innermost sum is over all integers $|a| \leq A, |b| \leq B$ such that there exists $u \in \mathbb{F}_p^*$ with $a \equiv su^4 \pmod{p}$ and $b \equiv tu^6 \pmod{p}$.

We calculate the innermost sum (on average over p, s , and t) using a character sum method borrowed from Banks and Shparlinski [BaSh] with their kind permission. The resulting tool of this method is the following lemma, which we prove at the end of the section:

Lemma 6. *For a fixed prime p and fixed $s, t \in \mathbb{F}_p^*$, let $w_{p,s,t} \in \mathbb{C}$ be such that $|w_{p,s,t}| \leq 1$. Let $A, B > 0$. Then, for any positive integer k , we have that, as $x \rightarrow \infty$,*

$$\sum_{p \leq x} \frac{1}{p} \sum_{1 \leq s, t < p} w_{p,s,t} \left| \sum_{\substack{|a| \leq A, |b| \leq B, \exists 1 \leq u < p: \\ a \equiv su^4 \pmod{p} \\ b \equiv tu^6 \pmod{p}}} 1 - \frac{2AB}{p} \right| \ll_k ABx^{1-\frac{1}{2k}} \log^{\frac{k}{2}-1} x + (A\sqrt{B} + B\sqrt{A})x^{1+\frac{1}{2k}} \log^{\frac{k}{2}-1} x + \sqrt{AB}x^{\frac{3}{2}} \log^2 x.$$

In our application, the weights $w_{p,s,t}$ are 1 or 0, according to whether $|E(s, t)|$ is prime or not. Since

$$|\text{Aut}(E(s, t))| = \begin{cases} 6 & \text{if } s = 0 \text{ and } p \equiv 1 \pmod{3}, \\ 4 & \text{if } t = 0 \text{ and } p \equiv 1 \pmod{4}, \\ 2 & \text{otherwise,} \end{cases}$$

and

$$|\mathcal{C}| = 4AB + O(A + B),$$

we can rewrite (3) as

$$(4) \quad \begin{aligned} & \frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) \\ &= \frac{1}{|\mathcal{C}|} \sum_{p \leq x} \sum_{\substack{s, t \in \mathbb{F}_p \\ |E(s, t)| \text{ prime}}} \frac{2}{p-1} \sum_{\substack{|a| \leq A, |b| \leq B, \exists 1 \leq u < p: \\ a \equiv su^4 \pmod{p}, \\ b \equiv tu^6 \pmod{p}}} 1 + O\left(\frac{1}{|\mathcal{C}|} \sum_{p \leq x} \sum_{\substack{|a| \leq A \\ |b| \leq B \\ ab \equiv 0 \pmod{p}}} 1\right) \\ &= \frac{2}{|\mathcal{C}|} \sum_{p \leq x} \frac{1}{p-1} \sum_{s, t \in \mathbb{F}_p} w_{p,s,t} \sum_{\substack{|a| \leq A, |b| \leq B, \exists 1 \leq u < p: \\ a \equiv su^4 \pmod{p}, \\ b \equiv tu^6 \pmod{p}}} 1 + O\left(\log \log x + \frac{x}{A \log x} + \frac{x}{B \log x}\right). \end{aligned}$$

Then, using Lemma 6 to estimate the first term in (4), and observing that the error term in (4) is smaller than the error term in Lemma 6, we obtain

$$(5) \quad \frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) = \sum_{p \leq x} \frac{\pi^*(p)}{p(p-1)} + O_k \left(x^{1-\frac{1}{2k}} \log^{\frac{k}{2}-1} x + \left(\frac{1}{\sqrt{A}} + \frac{1}{\sqrt{B}} \right) x^{1+\frac{1}{2k}} \log^{\frac{k}{2}-1} x + \frac{1}{\sqrt{AB}} x^{\frac{3}{2}} \log^2 x \right)$$

for any positive integer k . Choosing A, B such that $A, B > x^\varepsilon$ and $AB > x \log^{10} x$, Theorem 1 now follows easily from (5), Theorem 3, partial summation, and from choosing the integer k large enough to have that $\varepsilon k > 1$.

3.2. Proof of Corollary 2. Let

$$\mu := \frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x).$$

We consider

$$(6) \quad \begin{aligned} \frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \left| \pi_E^{\text{twin}}(x) - \mathfrak{C} \frac{x}{\log^2 x} \right|^2 &= \left(\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x)^2 \right) + \left(\mu - \mathfrak{C} \frac{x}{\log^2 x} \right)^2 - \mu^2 \\ &= \left(\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \sum_{\substack{p, p' \leq x \\ p \neq p' \\ |E(\mathbb{F}_p)|, |E(\mathbb{F}_{p'})| \text{ prime}}} 1 \right) + \mu - \mu^2 + \left(\mu - \mathfrak{C} \frac{x}{\log^2 x} \right)^2, \end{aligned}$$

where p, p' denote primes. For μ and the last term above, we will use the estimates given by Theorem 1 provided that the family \mathcal{C} is large enough (i.e. provided that $A, B > x^\varepsilon$ and $AB > x \log^{10} x$). For the first term on the right hand side of (6) we will obtain an exact formula with main term μ^2 . We proceed as follows.

As in our deduction of formula (3), by partitioning the elliptic curves in \mathcal{C} according to their isomorphism classes over \mathbb{F}_p and $\mathbb{F}_{p'}$, we obtain

$$\begin{aligned} &\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \sum_{\substack{p, p' \leq x \\ p \neq p' \\ |E(\mathbb{F}_p)|, |E(\mathbb{F}_{p'})| \text{ prime}}} 1 \\ &= \frac{1}{|\mathcal{C}|} \sum_{\substack{p, p' \leq x \\ p \neq p'}} \frac{1}{(p-1)(p'-1)} \sum_{\substack{s, t \in \mathbb{F}_p \\ s', t' \in \mathbb{F}_{p'}}} w_{p, s, t} w_{p', s', t'} |\text{Aut}(E(s, t))| \cdot |\text{Aut}(E(s', t'))| \cdot S(p, p', s, t, s', t'), \end{aligned}$$

where $w_{p, s, t}, w_{p', s', t'}$ are 1 or 0 according to whether $|E(s, t)|, |E(s', t')|$, respectively, are prime or not, and

$$S(p, p', s, t, s', t')$$

is the number of integers $|a| \leq A, |b| \leq B$ such that there exist $1 \leq u < p, 1 \leq u' < p'$ satisfying

$$a \equiv su^4 \pmod{p}, a \equiv s'u'^4 \pmod{p'}, b \equiv tu^6 \pmod{p}, b \equiv t'u'^6 \pmod{p'}.$$

We now use the following generalization of Lemma 6, which will be proved at the end of the section:

Lemma 7. *For fixed primes p, p' and fixed $s, t \in \mathbb{F}_p^*, s', t' \in \mathbb{F}_{p'}^*$, let $w_{p, s, t}, w_{p', s', t'} \in \mathbb{C}$ be such that $|w_{p, s, t}|, |w_{p', s', t'}| \leq 1$. Let $A, B > 0$. Then, for any positive integer k , we have that, as $x \rightarrow \infty$,*

$$\begin{aligned} &\sum_{\substack{p, p' \leq x \\ p \neq p'}} \frac{1}{pp'} \sum_{\substack{1 \leq s, t < p \\ 1 \leq s', t' < p'}} w_{p, s, t} w_{p', s', t'} \left| S(p, p', s, t, s', t') - \frac{AB}{pp'} \right| \\ &\ll_k AB x^{2-\frac{1}{2k}} \log^{\frac{k}{2}-1} x + (A\sqrt{B} + B\sqrt{A}) x^{2+\frac{1}{k}} \log^{\frac{k}{2}+\frac{1}{2k}-2} x + \sqrt{AB} x^3 \log x. \end{aligned}$$

Similarly to our deduction of (5), we obtain that

$$(7) \quad \frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \sum_{\substack{p, p' \leq x \\ p \neq p' \\ |E(\mathbb{F}_p)|, |E(\mathbb{F}_{p'})| \text{ prime}}} 1 = \sum_{\substack{p, p' \leq x \\ p \neq p'}} \frac{\pi^*(p)\pi^*(p')}{p(p-1)p'(p'-1)} + O_k \left(x^{2-\frac{1}{2k}} \log^{\frac{k}{2}-1} x + \left(\frac{1}{\sqrt{A}} + \frac{1}{\sqrt{B}} \right) x^{2+\frac{1}{k}} \log^{\frac{k}{2}+\frac{1}{2k}-2} x + \frac{1}{\sqrt{AB}} x^3 \log x \right).$$

By using the trivial bound $\pi^*(p) \ll p^2$, we see that

$$(8) \quad \sum_{\substack{p, p' \leq x \\ p \neq p'}} \frac{\pi^*(p)\pi^*(p')}{p(p-1)p'(p'-1)} = \left(\sum_{p \leq x} \frac{\pi^*(p)}{p(p-1)} \right)^2 - \sum_{p \leq x} \frac{\pi^*(p)^2}{p^2(p-1)^2} = \left(\sum_{p \leq x} \frac{\pi^*(p)}{p(p-1)} \right)^2 + O \left(\frac{x}{\log x} \right).$$

Moreover, by appealing to formula (5) and the upper bound $\mu \ll \frac{x}{\log^2 x}$ resulting from Theorem 1, we obtain

$$(9) \quad \left(\sum_{p \leq x} \frac{\pi^*(p)}{p(p-1)} \right)^2 = \mu^2 + O_k \left(x^{2-\frac{1}{2k}} \log^{\frac{k}{2}-3} x + \left(\frac{1}{\sqrt{A}} + \frac{1}{\sqrt{B}} \right) x^{2+\frac{1}{2k}} \log^{\frac{k}{2}-3} x + \frac{1}{\sqrt{AB}} x^{\frac{5}{2}} \right) + O_k \left(x^{2-\frac{1}{k}} \log^{k-2} x + \left(\frac{1}{A} + \frac{1}{B} \right) x^{2+\frac{1}{k}} \log^{k-2} x + \frac{1}{AB} x^3 \log^4 x \right).$$

By plugging (7)-(9) back into (6), we obtain

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \left| \pi_E^{\text{twin}}(x) - \mathfrak{C} \frac{x}{\log^2 x} \right|^2 \ll_k \frac{x^2}{\log^6 x} + \frac{1}{\sqrt{AB}} x^3 \log x + \left(\frac{1}{\sqrt{A}} + \frac{1}{\sqrt{B}} \right) x^{2+\frac{1}{k}} \log^{\frac{k}{2}+\frac{1}{2k}-2} x \ll_\varepsilon \frac{x^2}{\log^6 x},$$

provided that $k = \frac{2}{\varepsilon}$, $A, B > x^\varepsilon$, and $AB > x^2 \log^{14} x$, where $\varepsilon > 0$ is fixed and arbitrarily small.

Now we apply Theorem 5 to deduce

$$(10) \quad \frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \left| \pi_E^{\text{twin}}(x) - C(E) \frac{x}{\log^2 x} \right|^2 \ll_\varepsilon \frac{x^2}{\log^6 x},$$

provided that $A, B > x^\varepsilon$, $AB > x^2 \log^{14} x$, and $\lim_{A, B \rightarrow \infty} \frac{\log B \cdot \log^7 A}{B} = 0$.

Finally, let $f(x)$ be any real function such that $f(x) = o(\log x)$. Then (10) implies that

$$\# \left\{ E \in \mathcal{C} : \left| \pi_E^{\text{twin}}(x) - C(E) \frac{x}{\log^2 x} \right| \gg \frac{x}{f(x) \log^2 x} \right\} \ll \frac{f(x)^2 \log^4 x}{x^2} \sum_{E \in \mathcal{C}} \left| \pi_E^{\text{twin}}(x) - C(E) \frac{x}{\log^2 x} \right|^2 \ll_\varepsilon \frac{f(x)^2}{\log^2 x} |\mathcal{C}|.$$

This completes the proof of Corollary 2. □

3.3. Character sums. The rest of this section consists of proving Lemmas 6 and 7. Let us note that we make no effort to write the error term in terms of the weights $w_{p,s,t}$, as we will use the trivial bound

$|w_{p,s,t}| \leq 1$ for our application.² Our proofs will rely on two important analytic results, which we state below.

Theorem 8. (*The large sieve inequality*)

Let M, N, Q be positive integers and $(a_n)_n$ a sequence of complex numbers. For a fixed $q \leq Q$, we denote by χ Dirichlet characters modulo q . Then

$$\sum_{q \leq Q} \frac{q}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi \text{ primitive}}} \left| \sum_{M < n \leq M+N} a_n \chi(n) \right|^2 \leq (N + 3Q^2) \sum_{M < n \leq M+N} |a_n|^2.$$

Proof. For a proof, see [Da, p.160]. □

Theorem 9. (*The fourth power moment of Dirichlet L-functions; J. Friedlander and H. Iwaniec [FrIw]*)

Let p be a prime and N a positive integer. Let χ denote Dirichlet characters modulo p , with χ_0 denoting the principal character. Then

$$\sum_{\chi \neq \chi_0} \left| \sum_{n \leq N} \chi(n) \right|^4 \ll N^2 p \log^6 p.$$

Proof of Lemma 6. Let p be a prime and let $1 \leq s, t < p$. In what follows, χ, χ_1, χ_2 will denote Dirichlet characters modulo p , and χ_0 the principal Dirichlet character modulo p . As usual, $\bar{\chi}$ will denote the complex conjugate of χ . We first rewrite the sum over a and b by means of characters. Note that, for fixed s, t, a, b , if there exists one $u \pmod{p}$ such that $a \equiv su^4 \pmod{p}$ and $b \equiv tu^6 \pmod{p}$, then there exist exactly two such u , namely $\pm u$. By the orthogonality of characters, we obtain that

$$\begin{aligned} \sum_{\substack{|a| \leq A, |b| \leq B, \exists 1 \leq u < p: \\ a \equiv su^4 \pmod{p} \\ b \equiv tu^6 \pmod{p}}} 1 &= \frac{1}{2} \sum_{1 \leq u \leq p-1} \sum_{|a| \leq A} \sum_{|b| \leq B} \left(\frac{1}{p-1} \sum_{\chi_1} \chi_1(su^4) \bar{\chi}_1(a) \right) \left(\frac{1}{p-1} \sum_{\chi_2} \chi_2(tu^6) \bar{\chi}_2(b) \right) \\ &= \frac{1}{2(p-1)^2} \sum_{\chi_1, \chi_2} \chi_1(s) \chi_2(t) \mathcal{U}(\chi_1^4 \chi_2^6) \mathcal{A}(\bar{\chi}_1) \mathcal{B}(\bar{\chi}_2), \end{aligned}$$

where

$$(11) \quad \mathcal{U}(\chi) := \sum_{1 \leq u \leq p-1} \chi(u) = \begin{cases} p-1 & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0, \end{cases}$$

and

$$\mathcal{A}(\chi) := \sum_{|a| \leq A} \chi(a), \quad \mathcal{B}(\chi) := \sum_{|b| \leq B} \chi(b).$$

Using (11), we obtain further that

$$(12) \quad \sum_{\substack{|a| \leq A, |b| \leq B, \exists 1 \leq u < p: \\ a \equiv su^4 \pmod{p} \\ b \equiv tu^6 \pmod{p}}} 1 = \frac{1}{2(p-1)} \sum_{\chi_1^4 \chi_2^6 = \chi_0} \chi_1(s) \chi_2(t) \mathcal{A}(\bar{\chi}_1) \mathcal{B}(\bar{\chi}_2).$$

The contribution of $\chi_1 = \chi_2 = \chi_0$ to (12) is

$$\frac{1}{2(p-1)} \sum_{\substack{|a| \leq A \\ p \nmid a}} \sum_{\substack{|b| \leq B \\ p \nmid b}} 1 = \frac{2AB}{p} + O\left(\frac{AB}{p^2} + \frac{A}{p} + \frac{B}{p}\right).$$

²The present method using the trivial bound on the weights also works in the case when the weight function $w_{p,s,t}$ is supported on a sparse set. However, in that case the result is less satisfactory: the method recovers the results of Baier [Bai] and Fouvry-Murty [FoMu] about the average Lang–Trotter conjecture on Frobenius traces, but does not seem to improve upon them, even after a careful analysis of the contribution of the weights to the error term.

The contribution of $\chi_1 = \chi_0, \chi_2 \neq \chi_0$ to (12) is

$$\ll \frac{A}{p} \sum_{\substack{\chi_2^6 = \chi_0 \\ \chi_2 \neq \chi_0}} |\mathcal{B}(\chi_2)|;$$

similarly, the contribution of $\chi_1 \neq \chi_0, \chi_2 = \chi_0$ to (12) is

$$\ll \frac{B}{p} \sum_{\substack{\chi_1^4 = \chi_0 \\ \chi_1 \neq \chi_0}} |\mathcal{A}(\chi_1)|.$$

We note that these estimates are independent of s and t .

Replacing these three contributions in (12) and using the trivial bound for the weights, $|w_{p,s,t}| \leq 1$, we infer that

$$(13) \quad \sum_{p \leq x} \frac{1}{p} \sum_{1 \leq s, t < p} w_{p,s,t} \left(\sum_{\substack{|a| \leq A, |b| \leq B, \exists 1 \leq u < p: \\ a \equiv su^4 \pmod{p} \\ b \equiv tu^6 \pmod{p}}} 1 - \frac{2AB}{p} \right)$$

$$= \sum_{p \leq x} \frac{1}{2p(p-1)} \sum_{1 \leq s, t < p} w_{p,s,t} \sum_{\substack{\chi_1^4 \chi_2^6 = \chi_0 \\ \chi_1 \neq \chi_0, \chi_2 \neq \chi_0}} \chi_1(s) \chi_2(t) \mathcal{A}(\bar{\chi}_1) \mathcal{B}(\bar{\chi}_2)$$

$$(14) \quad + O \left(\sum_{p \leq x} \left(\frac{AB}{p} + A + B \right) + A \sum_{p \leq x} \sum_{\substack{\chi_2^6 = \chi_0 \\ \chi_2 \neq \chi_0}} |\mathcal{B}(\chi_2)| + B \sum_{p \leq x} \sum_{\substack{\chi_1^4 = \chi_0 \\ \chi_1 \neq \chi_0}} |\mathcal{A}(\chi_1)| \right).$$

The contribution of the first sum in the error term (14) is smaller than that of the first two terms on the right hand side of Lemma 6. For the contribution of the second (and third) sum in the error term (14), we note that there are at most 6 (at most 4) characters satisfying $\chi_2^6 = \chi_0$ ($\chi_1^4 = \chi_0$). By Hölder's inequality, we have that, for any $k \geq 1$,

$$A \sum_{p \leq x} \sum_{\substack{\chi_2^6 = \chi_0 \\ \chi_2 \neq \chi_0}} |\mathcal{B}(\chi_2)| \leq 2A \sum_{p \leq x} \sum_{\substack{\chi_2^6 = \chi_0 \\ \chi_2 \neq \chi_0}} \left| \sum_{b \leq B} \chi_2(b) \right| \leq 2A \left(\sum_{p \leq x} \sum_{\substack{\chi_2^6 = \chi_0 \\ \chi_2 \neq \chi_0}} 1 \right)^{1 - \frac{1}{2k}} \left(\sum_{p \leq x} \sum_{\chi_2 \neq \chi_0} \left| \sum_{b \leq B} \chi_2(b) \right|^{2k} \right)^{\frac{1}{2k}}.$$

Rewriting

$$\left| \sum_{b \leq B} \chi_2(b) \right|^{2k} = \left| \sum_{b \leq B^k} \tau_k(b) \chi_2(b) \right|^2,$$

where $\tau_k(b)$ is the number of ways of writing b as the product of k positive integers at most B , and using the large sieve, we then obtain that

$$(15) \quad A \sum_{p \leq x} \sum_{\substack{\chi_2^6 = \chi_0 \\ \chi_2 \neq \chi_0}} |\mathcal{B}(\chi_2)| \ll_k A \left(\frac{x}{\log x} \right)^{1 - \frac{1}{2k}} \left((x^2 + B^k) B^k \log^{k^2 - 1} B^k \right)^{\frac{1}{2k}}.$$

We may assume that $B \leq x^2$ and then replace $\log B$ by $\log x$ in (15). Indeed, if $B > x^2$, using $k = 1$, the right hand side of (15) is bounded by $AB(x/\log x)^{1/2}$, which is smaller than the error term of Lemma 6 for any positive integer k .

Similarly, we deduce that

$$B \sum_{p \leq x} \sum_{\substack{\chi_1^4 = \chi_0 \\ \chi_1 \neq \chi_0}} |\mathcal{A}(\chi_1)| \ll_k B \left(\frac{x}{\log x} \right)^{1 - \frac{1}{2k}} \left((x^2 + A^k) A^k \log^{k^2 - 1} x \right)^{\frac{1}{2k}}.$$

Using these last two estimates in (13), we arrive at

$$\begin{aligned}
(16) \quad & \sum_{p \leq x} \frac{1}{p} \sum_{1 \leq s, t < p} w_{p,s,t} \left(\sum_{\substack{|a| \leq A, |b| \leq B, \exists 1 \leq u < p: \\ a \equiv su^4 \pmod{p} \\ b \equiv tu^6 \pmod{p}}} 1 - \frac{2AB}{p} \right) \\
&= \sum_{p \leq x} \frac{1}{2p(p-1)} \sum_{\substack{\chi_1^4 \chi_2^6 = \chi_0 \\ \chi_1 \neq \chi_0, \chi_2 \neq \chi_0}} \mathcal{W}_p(\chi_1, \chi_2) \mathcal{A}(\bar{\chi}_1) \mathcal{B}(\bar{\chi}_2) \\
&+ O_k \left(ABx^{1-\frac{1}{2k}} \log^{\frac{k}{2}-1} x + (A\sqrt{B} + B\sqrt{A})x^{1+\frac{1}{2k}} \log^{\frac{k}{2}-1} x \right),
\end{aligned}$$

where

$$\mathcal{W}_p(\chi_1, \chi_2) := \sum_{1 \leq s, t < p} w_{p,s,t} \chi_1(s) \chi_2(t).$$

Two uses of the Cauchy–Schwarz inequality lead to

$$\begin{aligned}
(17) \quad & \left| \sum_{\substack{\chi_1^4 \chi_2^6 = \chi_0 \\ \chi_1 \neq \chi_0, \chi_2 \neq \chi_0}} \mathcal{W}_p(\chi_1, \chi_2) \mathcal{A}(\bar{\chi}_1) \mathcal{B}(\bar{\chi}_2) \right|^4 \\
&\leq \left(\sum_{\substack{\chi_1^4 \chi_2^6 = \chi_0 \\ \chi_1 \neq \chi_0, \chi_2 \neq \chi_0}} |\mathcal{W}_p(\chi_1, \chi_2)|^2 \right)^2 \sum_{\substack{\chi_1^4 \chi_2^6 = \chi_0 \\ \chi_1 \neq \chi_0, \chi_2 \neq \chi_0}} |\mathcal{A}(\chi_1)|^4 \sum_{\substack{\chi_1^4 \chi_2^6 = \chi_0 \\ \chi_1 \neq \chi_0, \chi_2 \neq \chi_0}} |\mathcal{B}(\chi_2)|^4.
\end{aligned}$$

We can now apply Theorem 9 to the second and third character sums above, using the fact that for any fixed character χ_1 there are at most 6 characters χ_2 (or for any fixed character χ_2 there are at most 4 characters χ_1) satisfying the condition $\chi_1^4 \chi_2^6 = \chi_0$. This implies that

$$(18) \quad \sum_{\substack{\chi_1^4 \chi_2^6 = \chi_0 \\ \chi_1 \neq \chi_0, \chi_2 \neq \chi_0}} |\mathcal{A}(\chi_1)|^4 \sum_{\substack{\chi_1^4 \chi_2^6 = \chi_0 \\ \chi_1 \neq \chi_0, \chi_2 \neq \chi_0}} |\mathcal{B}(\chi_2)|^4 \ll A^2 B^2 p^2 \log^{12} p.$$

For the first character sum, we extend the sum over all pairs of characters modulo p (including the trivial character) to get that

$$\begin{aligned}
(19) \quad & \sum_{\chi_1} \sum_{\chi_2} |\mathcal{W}_p(\chi_1, \chi_2)|^2 = \sum_{1 \leq s, t < p} \sum_{1 \leq s', t' < p} w_{p,s,t} \overline{w_{p,s',t'}} \sum_{\chi_1} \chi_1(s) \overline{\chi_1(s')} \sum_{\chi_2} \chi_2(t) \overline{\chi_2(t')} \\
&= (p-1)^2 \sum_{1 \leq s, t < p} |w_{p,s,t}|^2 \leq (p-1)^4.
\end{aligned}$$

Replacing (18) and (19) in (17) and then in (16), we finally obtain

$$\begin{aligned}
& \sum_{p \leq x} \frac{1}{p} \sum_{1 \leq s, t < p} w_{p,s,t} \left(\sum_{\substack{|a| \leq A, |b| \leq B, \exists 1 \leq u < p: \\ a \equiv su^4 \pmod{p} \\ b \equiv tu^6 \pmod{p}}} 1 - \frac{2AB}{p} \right) \\
&\ll_k ABx^{1-\frac{1}{2k}} \log^{\frac{k}{2}-1} x + (A\sqrt{B} + B\sqrt{A})x^{1+\frac{1}{2k}} \log^{\frac{k}{2}-1} x + \sqrt{AB}x^{\frac{3}{2}} \log^2 x,
\end{aligned}$$

which finishes the proof of Lemma 6. \square

Proof of Lemma 7. The proof of Lemma 7 is a generalization of that of Lemma 6 and thus will only be outlined.

Let p, p' be distinct primes and let $1 \leq s, t < p, 1 \leq s', t' < p'$. As before, we denote by χ_1, χ_2 Dirichlet characters modulo p and by χ'_1, χ'_2 Dirichlet characters modulo p' . The principal characters modulo p and p' are denoted by χ_0 and χ'_0 , respectively; thus $\chi_0 \chi'_0$ is the principal character modulo pp' .

With the same notation as in the proof of Lemma 6, we write

$$\begin{aligned} S(p, p', s, t, s', t') &= \frac{1}{4(p-1)(p'-1)} \sum_{\chi_1^4 \chi_2^6 = \chi_0} \chi_1(s) \chi_2(t) \sum_{\chi_1^4 \chi_2^6 = \chi'_0} \chi'_1(s) \chi'_2(t) \mathcal{A}(\overline{\chi_1 \chi_1}) \mathcal{B}(\overline{\chi_2 \chi_2}) \\ &=: \sum_{1 \leq j \leq 16} S_j(p, p', s, t, s', t'), \end{aligned}$$

where the sixteen character sums $S_j(p, p', s, t, s', t')$, $1 \leq j \leq 16$, correspond to the cases arising from

$$\begin{aligned} \chi_1 &= \chi_2 = \chi_0; \\ \chi_1 &= \chi_0, \chi_2 \neq \chi_0, \chi_2^6 = \chi_0; \\ \chi_1 &\neq \chi_0, \chi_2 = \chi_0, \chi_1^4 = \chi_0; \\ \chi_1 &\neq \chi_0, \chi_2 \neq \chi_0, \chi_1^4 \chi_2^6 = \chi_0; \\ \chi'_1 &= \chi'_2 = \chi'_0; \\ \chi'_1 &= \chi'_0, \chi'_2 \neq \chi'_0, \chi'^6_2 = \chi'_0; \\ \chi'_1 &\neq \chi'_0, \chi'_2 = \chi'_0, \chi'^4_1 = \chi'_0; \\ \chi'_1 &\neq \chi'_0, \chi'_2 \neq \chi'_0, \chi'^4_1 \chi'^6_2 = \chi'_0. \end{aligned}$$

Let us note that the sixteen cases monitor whether any of the characters $\chi_1, \chi'_1, \chi_2, \chi'_2$ is principal or not; this, in turn, allows us to determine the main term, to determine whether $\chi_1 \chi'_1$ is primitive modulo pp' or not, and so on.

We remark that the first case $\chi_1 = \chi_2 = \chi_0, \chi'_1 = \chi'_2 = \chi'_0$ gives

$$S_1(p, p', s, t, s', t') = \frac{AB}{pp'} + O\left(\frac{AB}{p^2 p'} + \frac{AB}{pp'^2} + \frac{A+B}{pp'}\right).$$

Thus

$$\begin{aligned} &\sum_{\substack{p, p' \leq x \\ p \neq p'}} \frac{1}{pp'} \sum_{\substack{1 \leq s, t < p \\ 1 \leq s', t' < p'}} w_{p, s, t} w_{p', s', t'} \left(S(p, p', s, t, s', t') - \frac{AB}{pp'} \right) \\ &= \sum_{\substack{p, p' \leq x \\ p \neq p'}} \frac{1}{pp'} \sum_{\substack{1 \leq s, t < p \\ 1 \leq s', t' < p'}} w_{p, s, t} w_{p', s', t'} \sum_{2 \leq j \leq 16} S_j(p, p', s, t, s', t') + O\left(AB \frac{x \log \log x}{\log x} + (A+B) \frac{x^2}{\log^2 x} \right). \end{aligned}$$

The remaining fifteen averages arising from the character sums $S_j(p, p', s, t, s', t')$, $2 \leq j \leq 16$, are estimated similarly to their analogues in the proof of Lemma 6, by appealing to the large sieve and the fourth power moment of Friedlander and Iwaniec. In particular, for any positive integer k , we obtain

$$\begin{aligned} &\sum_{\substack{p, p' \leq x \\ p \neq p'}} \frac{1}{pp'} \sum_{\substack{1 \leq s, t < p \\ 1 \leq s', t' \leq p'}} w_{p, s, t} w_{p', s', t'} \sum_{2 \leq j \leq 16} S_j(p, p', s, t, s', t') \\ &\ll_k \sqrt{AB} x^3 \log x \\ &+ A \left(\frac{x}{\log x} \right)^{1 - \frac{1}{2k}} \left((x^2 + B^k) B^k \log^{k^2-1} B \right)^{\frac{1}{2k}} \\ &+ B \left(\frac{x}{\log x} \right)^{1 - \frac{1}{2k}} \left((x^2 + A^k) A^k \log^{k^2-1} A \right)^{\frac{1}{2k}} \\ &+ A \left(\frac{x}{\log x} \right)^{2 - \frac{1}{k}} \left((x^4 + B^k) B^k \log^{k^2-1} B \right)^{\frac{1}{2k}} \\ &+ B \left(\frac{x}{\log x} \right)^{2 - \frac{1}{k}} \left((x^4 + A^k) A^k \log^{k^2-1} A \right)^{\frac{1}{2k}} \\ &\ll_k \sqrt{AB} x^3 \log x + \left(A\sqrt{B} + B\sqrt{A} \right) x^{2 + \frac{1}{k}} \log^{\frac{k}{2} + \frac{1}{2k} - 2} x + AB x^{2 - \frac{1}{2k}} \log^{\frac{k}{2} - 2} x. \end{aligned}$$

This completes the proof of Lemma 7. \square

4. REDUCTION OF THEOREM 3 TO AN AVERAGE OF KRONECKER CLASS NUMBERS

In this section we reduce Theorem 3 to an average of Kronecker class numbers. We do this by essentially following the standard method of partitioning our curves according to their Frobenius trace and by relying on Deuring's formula (see below). More explicitly, we first write

$$\pi^*(p) = \sum_{\substack{|r| \leq 2\sqrt{p} \\ p+1-r \text{ prime}}} \#\{s, t \in \mathbb{F}_p : a_p(E(s, t)) = r\}.$$

In order to evaluate this sum, we start by counting Weierstrass models $Y^2 = X^3 + aX + b$ of elliptic curves over \mathbb{F}_p with $p + 1 - r$ points for each given r , which can be done using the following two results.

Theorem 10. (*Deuring's Theorem* [De])

For any discriminant $d < 0$, let $h(d)$ and $w(d)$ be, respectively, the class number and the number of units of the order of discriminant d . Let $p > 3$ be a prime and let r be an integer such that $r^2 - 4p < 0$. Let $\mathcal{E}_r(p)$ be the set of \mathbb{F}_p -isomorphism classes of elliptic curves over \mathbb{F}_p having $p + 1 - r$ \mathbb{F}_p -rational points. Then

$$\sum_{E \in \mathcal{E}_r(p)} \frac{1}{|\text{Aut}(E)|} = H(r^2 - 4p),$$

where, for any $D < 0$, $H(D)$ is the Kronecker class number

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

In particular, for any fixed $-2\sqrt{p} \leq r \leq 2\sqrt{p}$, there are exactly $(p - 1)H(r^2 - 4p)$ Weierstrass models of elliptic curves over \mathbb{F}_p with $p + 1 - r$ points.

Lemma 11. Let D be a positive integer such that $-D \equiv 0, 1 \pmod{4}$. Then, as $D \rightarrow \infty$,

$$H(-D) \ll \sqrt{D} \log^2 D.$$

Proof. This follows from the class number formula and from standard bounds on special values of Dirichlet L-functions; see for example [DaPa1]. □

Using Deuring's Theorem and Lemma 11, we write

$$(20) \quad \sum_{p \leq x} \pi^*(p) = \sum_{\substack{p \leq x, |r| \leq 2\sqrt{p} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) + O(x^2 \log^2 x).$$

Thus it remains to evaluate an average of class numbers.

Let us remark that the above average of Kronecker class numbers, without the extra condition that $p + 1 - r$ be prime, is basically the content of the papers [DaPa1] and [FoMu]. This extra condition complicates the problem considerably and leads to the main contributions of our paper. More precisely, we will show:

Proposition 12. Let x, X, Y be positive real numbers such that $2 \leq X + Y \leq x$. Then, for any $M > 0$,

$$\sum_{X < p \leq X+Y} \sum_{\substack{|r| \leq 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) = \frac{\mathfrak{C} X^2 Y}{\log^2(X + Y)} + O(XY^2 \log^2 x) + O\left(\frac{x^3}{\log^M x}\right),$$

where \mathfrak{C} is the constant defined in Theorem 1.

The proof of this result will be explained in Section 5. Provided Proposition 12 holds, we can now complete the proof of Theorem 3, and hence also of Theorem 1.

Proof of Theorem 3. Let $x > 0$. We fix an integer $M \geq 10$ and let

$$K := \lceil \log \frac{M}{2} x \rceil, \quad Y := \frac{x}{K}.$$

For $0 \leq k \leq K - 1$, let

$$X = X_k := kY.$$

We partition the interval $p \leq x$ into K intervals of length Y and rewrite the main term of (20) as

$$\sum_{\substack{p \leq x \\ |r| \leq 2\sqrt{p} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) = \sum_{1 \leq k \leq K-1} \sum_{\substack{X < p \leq X+Y \\ |r| \leq 2\sqrt{p} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) + O\left(Y^{\frac{5}{2}} \log Y\right),$$

where the O -term comes from $k = 0$ and an application of Lemma 11. One more application of Lemma 11 gives us that the above equals

$$(21) \quad \begin{aligned} & \sum_{1 \leq k \leq K-1} \sum_{\substack{X < p \leq X+Y \\ |r| \leq 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) + O\left(Y^{\frac{5}{2}} \log Y\right) + O\left(\sum_{1 \leq k \leq K-1} XY^2 \log^2 x\right) \\ &= \sum_{1 \leq k \leq K-1} \sum_{\substack{X < p \leq X+Y \\ |r| \leq 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) + O\left(\frac{x^3}{\log^{\frac{M}{2}-2} x}\right). \end{aligned}$$

For the main term of (21) we use Proposition 12 (with the same M) and obtain:

$$(22) \quad \begin{aligned} \sum_{1 \leq k \leq K-1} \sum_{\substack{X < p \leq X+Y \\ |r| \leq 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) &= \mathfrak{C}Y^3 \sum_{1 \leq k \leq K-1} \frac{k^2}{\log^2(kY)} + O\left(\sum_{1 \leq k \leq K-1} XY^2 \log^2 x\right) \\ &+ O\left(\sum_{1 \leq k \leq K-1} \frac{x^3}{\log^M x}\right) + O\left(Y^{\frac{5}{2}} \log^2 Y\right) \\ &= \mathfrak{C}Y^3 \int_1^{K-1} \frac{t^2}{\log^2(tY)} dt + O\left(\frac{x^3}{\log^{\frac{M}{2}-2} x}\right) \\ &= \mathfrak{C} \int_Y^x \frac{u^2}{\log^2(u)} du + O\left(\frac{x^3}{\log^{\frac{M}{2}-2} x}\right) \\ &= \frac{\mathfrak{C}x^3}{3 \log^2 x} + O\left(\frac{x^3}{\log^3 x}\right). \end{aligned}$$

Replacing (21) and (22) in (20), the proof of Theorem 3 is completed. \square

5. REDUCTION OF PROPOSITION 12 TO AN AVERAGE TWIN PRIME CONJECTURE

In this section we show how Proposition 12 reduces to an average of the twin prime conjecture, which, in turn, will be proved completely in Sections 6-7. To be precise, our proof of Proposition 12 relies on the validity of the following result:

Proposition 13. *Let $x, M, \varepsilon > 0$. If $N \geq M + 3$, then, for any parameters X, Y, R, U, V satisfying*

$$2 \leq X + Y \leq x, \quad R \leq x, \quad x^{\frac{1}{2}} \log^N x \leq U, \quad \log^N x \leq V, \quad UV^2 \leq x \log^{-N} x,$$

and as $x \rightarrow \infty$,

$$(23) \quad \begin{aligned} & \sum_{\substack{|r| \leq R \\ f \leq V \\ n \leq U}} \frac{1}{nf} \sum_{a \pmod{4n}} \left(\frac{a}{n}\right) \sum_{\substack{X < p \leq X+Y \\ p+1-r \text{ prime} \\ p \equiv (r^2 - af^2)/4 \pmod{nf^2}}} \log p \cdot \log(p + 1 - r) \\ &= 2\mathfrak{C}RY + O\left(\frac{Rx}{\log^M x}\right) + O_\varepsilon\left(x^{\frac{4}{3}+\varepsilon}\right), \end{aligned}$$

where \mathfrak{C} is the constant defined in Theorem 1.

We assume this result as true and proceed to proving Proposition 12.

Proof of Proposition 12. Let x, X, Y, M be as in the statement of Proposition 12. Using the class number formula, we write

$$(24) \quad \sum_{X < p \leq X+Y} \sum_{\substack{|r| \leq 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) = \frac{1}{2\pi} \sum_{\substack{|r| \leq 2\sqrt{X} \\ f \leq 2\sqrt{X+Y}}} \frac{1}{f} \sum_{X < p \leq X+Y}^* p\sqrt{4p - r^2} L(1, \chi_d),$$

where

$$d = d(r, p, f) := \frac{r^2 - 4p}{f^2}$$

and the $*$ on the summation over p indicates that we are summing over primes $X < p \leq X + Y$ such that

$$p + 1 - r \text{ prime, } f^2 \mid r^2 - 4p, \text{ and } d \equiv 0, 1 \pmod{4}.$$

Here, χ_d denotes the Kronecker symbol of discriminant d (see for example [Hu, Section 12.3]), and $L(s, \chi_d)$ denotes its Dirichlet L-function.

Using the Pólya-Vinogradov inequality, we write the special value $L(1, \chi_d)$ as

$$\begin{aligned} L(1, \chi_d) &= \sum_{n \leq U} \frac{\chi_d(n)}{n} + \sum_{n > U} \frac{\chi_d(n)}{n} \\ &= \sum_{n \leq U} \frac{\chi_d(n)}{n} + O\left(\frac{\sqrt{|d|} \log |d|}{U}\right), \end{aligned}$$

where $U = U(x, M)$ is a parameter to be chosen soon. By using the above in (24), we obtain that

$$(25) \quad \sum_{X < p \leq X+Y} \sum_{\substack{|r| \leq 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) = \frac{1}{2\pi} \sum_{\substack{|r| \leq 2\sqrt{X} \\ f \leq 2\sqrt{X+Y} \\ n \leq U}} \frac{1}{nf} \sum_{X < p \leq X+Y}^* p\sqrt{4p - r^2} \chi_d(n) + O\left(\frac{X^{\frac{1}{2}} Y^3 \log Y}{U}\right).$$

Thus, by taking

$$(26) \quad x^{\frac{1}{2}} \log^{M+1} x \leq U \leq x,$$

the O-term above becomes $O\left(\frac{x^3}{\log^M x}\right)$.

Now we change the weights of the sum on the right hand side of (25) from $p\sqrt{4p - r^2}$ to

$$\frac{X\sqrt{4X - r^2}}{\log^2(X + Y)} \log p \cdot \log(p + 1 - r).$$

Since $p = X + O(Y)$, we have that

$$p\sqrt{4p - r^2} = \frac{X\sqrt{4X - r^2}}{\log^2(X + Y)} \log p \cdot \log(p + 1 - r) + O\left(Y\sqrt{X} + \frac{XY}{\sqrt{4p - r^2}}\right).$$

Then the right hand side of (25) becomes

$$(27) \quad \begin{aligned} &\frac{X}{2\pi \log^2(X + Y)} \sum_{\substack{|r| \leq 2\sqrt{X} \\ f \leq 2\sqrt{X+Y} \\ n \leq U}} \frac{\sqrt{4X - r^2}}{nf} \sum_{X < p \leq X+Y}^* \log p \cdot \log(p + 1 - r) \chi_d(n) \\ &+ O\left(\sum_{\substack{f \leq 2\sqrt{X+Y} \\ n \leq U}} \frac{1}{nf} \sum_{\substack{|r| \leq 2\sqrt{X} \\ X < p \leq X+Y}} \frac{XY}{\sqrt{4p - r^2}}\right) + O\left(XY^2 \log^2 x + \frac{x^3}{\log^M x}\right). \end{aligned}$$

For the first error term of (27), we remark that, by the conditions on p and r , we have $4p - r^2 \geq 1$. Thus, for any p , the innermost sum satisfies

$$\sum_{|r| \leq 2\sqrt{X}} \frac{1}{\sqrt{4p - r^2}} \leq 2 + 2 \int_0^{2\sqrt{X}} \frac{dr}{\sqrt{4p - r^2}} \leq 2 + \pi,$$

which gives a bound of $XY^2 \log^2 x$ for the first error term of (27). Then

$$\begin{aligned} \sum_{X < p \leq X+Y} \sum_{\substack{|r| \leq 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) &= \frac{X}{2\pi \log^2(X+Y)} \sum_{\substack{|r| \leq 2\sqrt{X} \\ f \leq 2\sqrt{X+Y} \\ n \leq U}} \frac{\sqrt{4X - r^2}}{nf} \sum_{X < p \leq X+Y}^* \log p \cdot \log(p+1-r) \chi_d(n) \\ &+ O(XY^2 \log^2 x) + O\left(\frac{x^3}{\log^M x}\right). \end{aligned}$$

We now truncate the sum over f with respect to a parameter $V = V(x, M)$, to be chosen soon. We write

$$\begin{aligned} &\frac{X}{2\pi \log^2(X+Y)} \sum_{\substack{|r| \leq 2\sqrt{X} \\ f \leq 2\sqrt{X+Y} \\ n \leq U}} \frac{\sqrt{4X - r^2}}{nf} \sum_{X < p \leq X+Y}^* \log p \cdot \log(p+1-r) \chi_d(n) \\ &= \frac{X}{2\pi \log^2(X+Y)} \sum_{\substack{|r| \leq 2\sqrt{X} \\ f \leq V \\ n \leq U}} \frac{\sqrt{4X - r^2}}{nf} \sum_{X < p \leq X+Y}^* \log p \cdot \log(p+1-r) \chi_d(n) \\ (28) \quad &+ O\left(X^{\frac{3}{2}} \sum_{\substack{|r| \leq 2\sqrt{X} \\ V < f \leq 2\sqrt{X+Y} \\ n \leq U}} \frac{1}{nf} \sum_{\substack{X < p \leq X+Y \\ p \equiv \frac{r^2}{4} \pmod{f^2}}} 1\right). \end{aligned}$$

For the error term we used that, since r is odd and $f^2|r^2 - 4p$, we must have that f is odd; hence the condition in the sum over p that $4p \equiv r^2 \pmod{f^2}$ becomes $p \equiv \bar{4}r^2 \pmod{f^2}$. Here, $\bar{4}$ is the inverse of 4 modulo f^2 .

It is easy to see that the error term in (28) reduces to

$$O\left(\frac{X^2 Y \log U}{V^2}\right).$$

Choosing V such that

$$(29) \quad V \geq (\log x)^{\frac{M+1}{2}},$$

the error term becomes $O\left(\frac{x^3}{\log^M x}\right)$.

Thus we have shown that

$$\begin{aligned} (30) \quad &\sum_{X < p \leq X+Y} \sum_{\substack{|r| \leq 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2 - 4p) \\ &= \frac{X}{2\pi \log^2(X+Y)} \sum_{\substack{|r| \leq 2\sqrt{X} \\ f \leq V \\ n \leq U}} \frac{\sqrt{4X - r^2}}{nf} \sum_{X < p \leq X+Y}^* \log p \cdot \log(p+1-r) \chi_d(n) \\ &+ O(XY^2 \log^2 x) + O\left(\frac{x^3}{\log^M x}\right), \end{aligned}$$

provided conditions (26) and (29) hold.

Now we use quadratic reciprocity and consider $\chi_d(n)$ as a character modulo $4n$. In other words, we rewrite the main term of (30) as

$$(31) \quad \frac{X}{2\pi \log^2(X+Y)} \sum_{\substack{|r| \leq 2\sqrt{X} \\ f \leq V \\ n \leq U}} \frac{1}{nf} \sqrt{4X-r^2} \sum_{a \pmod{4n}} \left(\frac{a}{n}\right) \sum_{X < p \leq X+Y}^{**} \log p \cdot \log(p+1-r),$$

where the $**$ on the summation over p indicates that we are summing over primes $X < p \leq X+Y$ such that

$$p+1-r \text{ prime, } f^2 \mid r^2 - 4p, \ d \equiv 0, 1 \pmod{4}, \text{ and } \frac{r^2 - 4p}{f^2} \equiv a \pmod{4n}.$$

Since r and f must be odd, we necessarily have $d \equiv 1 \pmod{4}$; thus $**$ is equivalent to the conditions

$$p+1-r \text{ prime and } p \equiv \frac{r^2 - af^2}{4} \pmod{nf^2}.$$

Consequently, we have reduced our question to an average of the standard twin prime conjecture, twisted by some Kronecker symbols. This average is evaluated using Proposition 13 stated in the beginning of the section; the details follow.

Let us write the left hand side of Proposition 13 as $\sum_{|r| \leq R} F(r)$. With this notation, (31) becomes

$$\frac{X}{2\pi \log^2(X+Y)} \sum_{|r| \leq 2\sqrt{X}} F(r) \sqrt{4X-r^2},$$

which we can compute from Proposition 13 by partial summation. Evaluating the integral

$$\int_0^{2\sqrt{X}} t^2(4X-t^2)^{-\frac{1}{2}} dt = 4X \int_0^1 t^2(1-t^2)^{-\frac{1}{2}} dt = \pi X$$

and letting

$$U := x^{\frac{1}{2}} \log^{M+3} x, \quad V := \log^{M+3} x,$$

we obtain:

$$\begin{aligned} & \frac{X}{2\pi \log^2(X+Y)} \sum_{|r| \leq 2\sqrt{X}} F(r) \sqrt{4X-r^2} \\ &= \frac{X}{2\pi \log^2(X+Y)} \int_0^{2\sqrt{X}} \left(2\mathfrak{C}tY + O\left(\frac{tx}{\log^M x} + x^{\frac{4}{3}+\varepsilon}\right) \right) (t(4X-t^2)^{-\frac{1}{2}}) dt \\ &= \frac{\mathfrak{C}}{\pi} \cdot \frac{XY}{\log^2(X+Y)} \int_0^{2\sqrt{X}} t^2(4X-t^2)^{-\frac{1}{2}} dt + O\left(\frac{(Xx)^{\frac{3}{2}}}{(\log^2(X+Y))(\log^M x)}\right). \\ &= \frac{\mathfrak{C}X^2Y}{\log^2(X+Y)} + O\left(\frac{(Xx)^{\frac{3}{2}}}{(\log^2(X+Y))(\log^M x)}\right). \end{aligned}$$

Combining this with (30), the proof of Proposition 12 is now completed (provided that Proposition 13 holds). Proposition 13 will be proved in Sections 6 and 7, which contain the main novel contributions of our paper. \square

6. AVERAGE OF THE TWIN PRIME CONJECTURE AND PROOF OF THEOREM 4

In this section we shall prove Theorem 4. The statement is a Barban-Davenport-Halberstam type distribution result for twin primes, where the average is over the twin prime differences. The main (and difficult) part of the proof is the case $Q = 1$ of Theorem 4. A version of this was proven by Perelli and Pintz in [PePi]. Beside minor cosmetics, their result differs from what we need in two aspects: (i) rather than a Goldbach type problem, we have a twin prime problem; (ii) more importantly, our result requires a Siegel-Walfisz type analogue, namely:

Proposition 14. *Let $\varepsilon, M, N > 0$ be fixed. Then there exists $x(\varepsilon, M, N) > 0$ such that, for any $x > x(\varepsilon, M, N)$, $x^{\frac{1}{3}+\varepsilon} \leq R \leq x$, $q \leq \log^N x$, $(a, q) = 1$, and $2 \leq X + Y \leq x$, we have*

$$\sum_{0 < r \leq R} \left| \sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q} \\ p-p'=r}} \log p \cdot \log p' - \mathfrak{S}(r, q, a)Y \right|^2 \ll \frac{Rx^2}{\log^M x}.$$

The proof of Proposition 14 is similar to the proof of [PePi, Theorem 1] and, for this reason, we will only indicate the major steps; this will enable the interested reader to modify [PePi] accordingly. After we complete the proof of Proposition 14, we proceed to proving Theorem 4.

Proof of Proposition 14. We use the following notation (which is, unfortunately, not exactly the same as the one in [PePi], since our $S_1(\alpha)$ should reflect the extra conditions on the running variable p):

$$S_1(\alpha) := \sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q}}} \log p \cdot e(p\alpha), \quad S_2(\alpha) := \sum_{p \leq x} \log p \cdot e(p\alpha), \quad e(y) := e^{2\pi i y},$$

$$C := C(\varepsilon, M, N), \quad I_{s,b} := \text{the Farey arc around } \frac{b}{s} = \left\{ \frac{b}{s} + \eta : |\eta| < \frac{\log^{2C} x}{sx} \right\},$$

$$\mathfrak{M} := \bigcup_{s \leq \log^C x} \bigcup_{(b,s)=1} I_{s,b}, \quad \mathfrak{m} := [0, 1] \setminus \mathfrak{M}.$$

By the circle method, we have

$$\sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q} \\ p-p'=r}} \log p \cdot \log p' = \int_0^1 S_1(\alpha) S_2(-\alpha) e(-r\alpha) d\alpha,$$

and so

$$(32) \quad \sum_{0 < r \leq R} \left| \sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q} \\ p-p'=r}} \log p \cdot \log p' - \mathfrak{S}(r, q, a)Y \right|^2 \ll \sum_{0 < r \leq R} \left| \int_{\mathfrak{m}} S_1(\alpha) S_2(-\alpha) e(-r\alpha) d\alpha \right|^2$$

$$+ \sum_{0 < r \leq R} \left| \int_{\mathfrak{M}} S_1(\alpha) S_2(-\alpha) e(-r\alpha) d\alpha - \mathfrak{S}(r, q, a)Y \right|^2.$$

The estimate for the contribution of the minor arcs (the first term in formula (32)) is identical to the one in [PePi]. To start, we remark that the Cauchy-Schwarz inequality and the well-known estimate $\sum_{0 < r \leq R} e(ry) \ll \min(R, 1/|y|)$ reduce this term to

$$\begin{aligned} & \sum_{0 < r \leq R} \left| \int_{\mathfrak{m}} S_1(\alpha) S_2(-\alpha) e(-r\alpha) d\alpha \right|^2 \\ &= \sum_{0 < r \leq R} \int_{\mathfrak{m}} S_1(\alpha) S_2(-\alpha) e(-r\alpha) d\alpha \int_{\mathfrak{m}} \overline{S_1(\beta) S_2(-\beta)} e(r\beta) d\beta \\ &\ll \int_{\mathfrak{m}} |S_1(\beta) S_2(\beta)| \int_{\mathfrak{m}} |S_1(\alpha) S_2(\alpha)| \min\left(R, \frac{1}{\|\alpha - \beta\|}\right) d\alpha d\beta \\ &\ll \sup_{\beta \in \mathfrak{m}} \left(\int_{\mathfrak{m}} |S_2(\alpha)|^2 \min\left(R, \frac{1}{\|\alpha - \beta\|}\right)^2 d\alpha \right)^{\frac{1}{2}} \\ &\times \left(\int_{\mathfrak{m}} |S_1(\alpha)|^2 d\alpha \right)^{\frac{1}{2}} \left(\int_{\mathfrak{m}} |S_1(\beta)|^2 d\beta \right)^{\frac{1}{2}} \left(\int_{\mathfrak{m}} |S_2(\beta)|^2 d\beta \right)^{\frac{1}{2}}, \end{aligned}$$

where $\|\cdot\|$ denotes the distance to the nearest integer. Now let us observe that our $S_2(\alpha)$ is essentially the same as the one in [PePi], thus the third integral above can be estimated as in [PePi, Section 5]. Note that the function $S_2(\alpha)$ plays the crucial role, while the somewhat different $S_1(\alpha)$ only appears in Parseval's identity. Since our $S_1(\alpha)$ has smaller L^2 -norm than its analogue in [PePi], the arguments in [PePi, Section 3] provide the necessary bound in our case as well.

For the calculation of the major arcs (the second term in (32)) we follow the exact steps of [PePi, Section 4]. First, for $\alpha = \frac{b}{s} + \eta \in I_{s,b}$, we use the Siegel-Walfisz theorem to approximate the function

$$S_1(\alpha) = \sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q}}} \log p \cdot e\left(p\left(\frac{b}{s} + \eta\right)\right) = \sum_{1 \leq c \leq s} e\left(\frac{bc}{s}\right) \sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q} \\ p \equiv c \pmod{s}}} \log p \cdot e(p\eta)$$

by

$$\frac{1}{\phi([q, s])} \sum_{\substack{1 \leq c \leq s \\ (c, s) = 1 \\ (q, s) | c - a}} e\left(\frac{bc}{s}\right) \sum_{X < n \leq X+Y} e(n\eta),$$

and the function $S_2(\alpha)$ by

$$\frac{1}{\phi(s)} \sum_{\substack{1 \leq c \leq s \\ (c, s) = 1}} e\left(\frac{bc}{s}\right) \sum_{n \leq x} e(n\eta) = \frac{\mu(s)}{\phi(s)} \sum_{n \leq x} e(n\eta).$$

Here, $\mu(\cdot)$ denotes the Möbius function.

The estimates for the error terms in our resulting analogue of [PePi, (7)] are identical to the ones described in [PePi, Section 4]. For the main term, the only difference is in the singular series, which now originates in

$$(33) \quad \sum_{s \leq \log^C x} \frac{\mu(s)}{\phi(s)\phi([s, q])} \sum_{\substack{1 \leq b \leq s \\ (b, s) = 1}} e\left(\frac{-rb}{s}\right) \sum_{\substack{1 \leq c \leq s \\ (c, s) = 1 \\ (q, s) | c - a}} e\left(\frac{bc}{s}\right).$$

We proceed as follows. The standard argument via the Chinese Remainder Theorem shows that the function

$$F(s; r; q, a) := \sum_{\substack{1 \leq b \leq s \\ (b, s) = 1}} e\left(\frac{-rb}{s}\right) \sum_{\substack{1 \leq c \leq s \\ (c, s) = 1 \\ (q, s) | c - a}} e\left(\frac{bc}{s}\right)$$

is multiplicative in s . Indeed, for $s = uv$, $(u, v) = 1$, $u\bar{u} \equiv 1 \pmod{v}$ and $v\bar{v} \equiv 1 \pmod{u}$, we note that the relation $c = gu\bar{u} + hv\bar{v}$ establishes a bijection between the reduced residue classes c modulo uv and the pairs of reduced residue classes g modulo v , h modulo u . Similarly, the relation $b = du + fv$ establishes a bijection between the reduced residue classes b modulo uv and the pairs of reduced residue classes d modulo v , f modulo u . Thus

$$e\left(\frac{bc - rb}{s}\right) = e\left(\frac{(du + fv)(gu\bar{u} + hv\bar{v}) - r(du + fv)}{uv}\right) = e\left(\frac{dg - rd}{v}\right) e\left(\frac{fh - rf}{u}\right).$$

Moreover, $(q, uv) | c - a$ if and only if $(q, u) | h - a$ and $(q, v) | g - a$.

Observe that we are only interested in square-free s , thus it is enough to know $F(p; r; q; a)$ for a prime p . A routine computation shows that

$$F(p; r; q, a) = \sum_{1 \leq b \leq p-1} \sum_{\substack{1 \leq c \leq p-1 \\ (q, p) | c - a}} e\left(\frac{bc - br}{p}\right) = \begin{cases} p-1 & \text{if } p|q, p|a-r, \\ -1 & \text{if } p|q, p \nmid a-r, \\ -p+1 & \text{if } p \nmid q, p|r, \\ 1 & \text{if } p \nmid q, p \nmid r. \end{cases}$$

Now one can easily check that, after extending the sum over s in (33) up to infinity, we have

$$\frac{1}{\phi(q)} \sum_{s \geq 1} \frac{\mu(s)}{\phi(s)} \cdot \frac{\phi(q)}{\phi([s, q])} F(s; r; q, a) = \frac{1}{\phi(q)} \prod_p \left(1 - \frac{\phi(q)F(p; r; q, a)}{(p-1)\phi([p, q])}\right) = \mathfrak{S}(r, q, a).$$

Proposition 14 then follows. \square

Proof of Theorem 4. Let us observe that the expected density of twin primes of distance r is $\mathfrak{S}(r)$. If $a \pmod{q}$ is an admissible residue class, that is, $(a, q) = (a - r, q) = 1$, then the expected density of twin primes of distance r in the residue class $a \pmod{q}$ should satisfy

$$\mathfrak{S}(r, q, a) = \frac{\mathfrak{S}(r)}{\rho(r, q)},$$

where

$$\rho(r, q) := \#\{a \pmod{q} : (a, q) = (a - r, q) = 1\}.$$

To see this, let us evaluate $\rho(r, q)$. On one hand, we have that this function is multiplicative in the second variable q . Indeed, let $q = uv$ with $(u, v) = 1$ and note that by the Chinese Remainder Theorem, the relation $b = cu\bar{u} + dv\bar{v}$ establishes a bijection between the reduced residue classes b modulo uv and the pairs of reduced residue classes c modulo v , d modulo u . Here, $u\bar{u} \equiv 1 \pmod{v}$ and $v\bar{v} \equiv 1 \pmod{u}$. The multiplicativity then follows from the fact that $(b - r, uv) = 1$ if and only if $(c - r, v) = (d - r, u) = 1$. On the other hand, we have that

$$\rho(r, p^\alpha) = \sum_{\substack{1 \leq b \leq p^\alpha \\ p \nmid b \\ p \nmid b-r}} 1 = \begin{cases} p^\alpha - p^{\alpha-1} & \text{if } p \mid r, \\ p^\alpha - 2p^{\alpha-1} & \text{if } p \nmid r. \end{cases}$$

Then our claim follows from the equations

$$(34) \quad \rho(r, q) = \prod_{p^\alpha \parallel q, p \mid r} (p^\alpha - p^{\alpha-1}) \cdot \prod_{p^\alpha \parallel q, p \nmid r} (p^\alpha - 2p^{\alpha-1}) = \phi(q) \prod_{p \mid q, p \nmid r} \frac{p-2}{p-1},$$

$$\frac{\mathfrak{S}(r)}{\rho(r, q)} = \frac{\mathfrak{S}(r)}{\phi(q)} \prod_{p \mid q, p \nmid r} \frac{p-1}{p-2} = \frac{2}{\phi(q)} \prod_{p \neq 2} \frac{p(p-2)}{(p-1)^2} \cdot \prod_{p \mid r} \frac{p-1}{p-2} \cdot \prod_{p \mid q, p \nmid r} \frac{p-1}{p-2} = \mathfrak{S}(r, q, a).$$

Now let us extend the definition of $\rho(r, q)$ to characters modulo q : if χ is any character modulo q , let

$$\rho(r, \chi) := \sum_{\substack{1 \leq b \leq q \\ (b-r, q)=1}} \chi(b) = \sum_{1 \leq b \leq q} \chi(b) \chi_0(b-r).$$

Note that $\rho(r, \chi_0) = \rho(r, q)$ when χ_0 is the trivial character modulo q .

By the orthogonality of characters, we obtain that

$$(35) \quad \mathfrak{S}(r, q, a) = \frac{\mathfrak{S}(r)}{\rho(r, q)} = \frac{\mathfrak{S}(r)}{\phi(q)} \sum_{\chi} \bar{\chi}(a) \frac{\rho(r, \chi)}{\rho(r, q)},$$

where this formula also incorporates all the conditions that $2 \mid r$ and $(a, q) = (a - r, q) = 1$. This simple representation plays a crucial role in the following computation.

Let $\varepsilon, M > 0, N \geq M + 3, x > x(\varepsilon, M), x^{\frac{1}{3} + \varepsilon} \leq R \leq x, Q \leq x \log^{-N} x$, and $0 \leq X < X + Y \leq x$ be fixed, as in the statement of Theorem 4.

For any (even) integer r and character χ , we define

$$F(r, \chi) := \sum_{\substack{X < p \leq X+Y \\ p-p'=r}} \chi(p) \log p \cdot \log p'.$$

By the orthogonality of characters we obtain that

$$\sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q} \\ p-p'=r}} \log p \cdot \log p' = \frac{1}{\phi(q)} \sum_{\chi} \bar{\chi}(a) F(r, \chi).$$

Usually, the main term comes from the trivial character and the contribution of the rest is small due to the oscillation of the characters. Unfortunately, our situation above is more complex and we need to compute a dispersion over *all* characters, as follows.

The left hand side of Theorem 4 can be transformed (using (35) and orthogonality) into:

$$\begin{aligned}
S &:= \sum_{0 < r \leq R} \sum_{q \leq Q} \sum_{1 \leq a \leq q} \left| \sum_{\substack{X < p \leq X+Y \\ p \equiv a \pmod{q} \\ p-p'=r}} \log p \cdot \log p' - \mathfrak{S}(r, q, a)Y \right|^2 \\
&= \sum_{0 < r \leq R} \sum_{q \leq Q} \sum_{1 \leq a \leq q} \left| \frac{1}{\phi(q)} \sum_{\chi} \bar{\chi}(a) \left(F(r, \chi) - \frac{\mathfrak{S}(r)\rho(r, \chi)Y}{\rho(r, q)} \right) \right|^2 \\
&= \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{1}{\phi(q)} \sum_{\chi} \left| F(r, \chi) - \frac{\mathfrak{S}(r)\rho(r, \chi)Y}{\rho(r, q)} \right|^2 \\
&= \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{1}{\phi(q)} \sum_{\chi} |F(r, \chi)|^2 \\
&\quad - \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{1}{\phi(q)} \sum_{\chi} \frac{\mathfrak{S}(r)Y}{\rho(r, q)} 2\Re(F(r, \chi)\rho(r, \bar{\chi})) \\
&\quad + \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{1}{\phi(q)} \sum_{\chi} \frac{\mathfrak{S}(r)^2 |\rho(r, \chi)|^2 Y^2}{\rho(r, q)^2}.
\end{aligned}$$

By the orthogonality of characters,

$$\frac{1}{\phi(q)} \sum_{\chi} |\rho(r, \chi)|^2 = \sum_{\substack{1 \leq b \leq q \\ (b-r, q)=1}} \sum_{\substack{1 \leq c \leq q \\ (c-r, q)=1}} \frac{1}{\phi(q)} \sum_{\chi} \chi(b)\bar{\chi}(c) = \rho(r, q),$$

and then the last term in S simplifies to

$$\sum_{0 < r \leq R} \sum_{q \leq Q} \frac{1}{\phi(q)} \sum_{\chi} \frac{\mathfrak{S}(r)^2 |\rho(r, \chi)|^2 Y^2}{\rho(r, q)^2} = Y^2 \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{\mathfrak{S}(r)^2}{\rho(r, q)}.$$

More importantly,

$$\begin{aligned}
&\frac{1}{\phi(q)} \sum_{\chi} F(r, \chi)\rho(r, \bar{\chi}) \\
&= \sum_{\substack{X < p \leq X+Y \\ p-p'=r}} \sum_{\substack{1 \leq b \leq q \\ (b-r, q)=1}} \log p \cdot \log p' \frac{1}{\phi(q)} \sum_{\chi} \chi(p)\bar{\chi}(b) \\
&= \sum_{\substack{X < p \leq X+Y \\ p-p'=r \\ (pp', q)=1}} \log p \cdot \log p' = \sum_{\substack{X < p \leq X+Y \\ p-p'=r}} \log p \cdot \log p' + O(\log^2 x).
\end{aligned}$$

The expected asymptotic for this last sum is $\mathfrak{S}(r)Y$, which is indeed true on average over r from the case of $a = q = 1$ of Proposition 14.

We remark that, if r and q are even, then $\mathfrak{S}(rq) \ll \mathfrak{S}(r)\mathfrak{S}(q)$. Moreover, by using standard methods to estimate the average of a multiplicative function having a value of $1 + O\left(\frac{1}{p}\right)$ at any p prime power (see, for example, [Te]), we obtain that $\mathfrak{S}(r)$ is bounded on average, that is,

$$\sum_{r \leq R} \mathfrak{S}(r) = O(R)$$

and

$$\sum_{r \leq R} \mathfrak{S}(r)^2 = O(R).$$

Using these remarks, we deduce that

$$\begin{aligned}
& \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{1}{\phi(q)} \sum_{\chi} \frac{\mathfrak{S}(r)Y}{\rho(r, q)} 2\Re(F(r, \chi)\rho(r, \bar{\chi})) \\
&= 2 \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{\mathfrak{S}(r)Y}{\rho(r, q)} (\mathfrak{S}(r)Y + O(\log^2 x)) + O\left(\frac{Rx^2}{\log^M x}\right) \\
&= 2Y^2 \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{\mathfrak{S}(r)^2}{\rho(r, q)} + O\left(\frac{Rx^2}{\log^M x}\right).
\end{aligned}$$

Putting everything together, we obtain that

$$S = \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{1}{\phi(q)} \sum_{\chi} |F(r, \chi)|^2 - Y^2 \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{\mathfrak{S}(r)^2}{\rho(r, q)} + O\left(\frac{Rx^2}{\log^M x}\right).$$

Note that nothing deep has happened so far beside the one application of Proposition 14 – we have utilized only the basic properties of Dirichlet characters. Now we need to show that the first and the second terms are asymptotically equal, that is, we need to be exact in our computation.

As a first step we define

$$(36) \quad C(f, Q) := \sum_{\substack{q \leq Q \\ f|q}} \frac{1}{\phi(q)},$$

which satisfies

$$(37) \quad C(f, Q) \ll \frac{1}{\phi(f)} \log Q.$$

We also observe that, if $\chi \pmod{q}$ is induced by the primitive character $\chi^* \pmod{f}$, then, due to the fact that $F(r, \chi)$ is a sum over primes, we have

$$F(r, \chi) = F(r, \chi^*) + O(\log^2 x).$$

By rearranging the first sum in S according to primitive characters and using the above, we see that

$$S = \sum_{0 < r \leq R} \sum_{f \leq Q} C(f, Q) \sum_{\chi}^* |F(r, \chi)|^2 - Y^2 \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{\mathfrak{S}(r)^2}{\rho(r, q)} + O\left(\frac{Rx^2}{\log^M x}\right),$$

where \sum_{χ}^* is a sum over all primitive characters modulo f .

Now for any fixed (even) $0 < r \leq R$, we use the large sieve inequality to estimate

$$\sum_{Q_0 < f \leq Q} C(f, Q) \sum_{\chi}^* |F(r, \chi)|^2 \ll \left(\frac{Y}{Q_0} + Q\right) Y \log^3 x \ll \frac{x^2}{\log^M x},$$

where $Q_0 := \log^{M+3} x$ and (recall) $N \geq M + 3$. This implies that

$$S = \sum_{0 < r \leq R} \sum_{f \leq Q_0} C(f, Q) \sum_{\chi}^* |F(r, \chi)|^2 - Y^2 \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{\mathfrak{S}(r)^2}{\rho(r, q)} + O\left(\frac{Rx^2}{\log^M x}\right).$$

Using the notation

$$(38) \quad \psi(X, Y; r, f, b) := \sum_{\substack{X < p \leq X+Y \\ p \equiv b \pmod{f} \\ p-p'=r}} \log p \cdot \log p',$$

$$(39) \quad E(X, Y; r, f, b) := \psi(X, Y; r, f, b) - \mathfrak{S}(r, f, b)Y,$$

we see that

$$\begin{aligned}
F(r, \chi) &= \sum_{1 \leq b \leq f} \chi(b) \psi(X, Y; r, f, b) \\
&= \sum_{\substack{1 \leq b \leq f \\ (b-r, f)=1}} \chi(b) \mathfrak{S}(r, f, b) Y + \sum_{1 \leq b \leq f} \chi(b) E(X, Y; r, f, b) \\
&= \frac{\mathfrak{S}(r) Y}{\rho(r, f)} \rho(r, \chi) + O\left(f \max_{(b, f)=1} |E(X, Y; r, f, b)|\right).
\end{aligned}$$

For any small f and b , the sum of $|E(X, Y; r, f, b)|$ over r is sufficiently small by Proposition 14; consequently, the same is also true for the sum over f .

Additionally, we can evaluate $\rho(r, \chi)$ for a primitive character. It is well-known that for a primitive character χ modulo f and for all $d|f$, $d \neq f$, we have $\sum_{1 \leq c \leq f/d} \chi(r + cd) = 0$ (see [Da, Chapter 9]). Using this, we quickly infer that

$$\rho(r, \chi) = \sum_{1 \leq b \leq f} \chi(b) \sum_{d|(b-r, f)} \mu(d) = \sum_{d|f} \mu(d) \sum_{\substack{1 \leq b \leq f \\ b \equiv r \pmod{d}}} \chi(b) = \mu(f) \chi(r).$$

Putting everything together, we arrive at the equation

$$S = \sum_{0 < r \leq R} \sum_{\substack{f \leq Q_0 \\ (r, f)=1 \\ f \text{ is square-free}}} C(f, Q) \frac{\mathfrak{S}(r)^2 Y^2}{\rho(r, f)^2} \sum_{\chi}^* 1 - Y^2 \sum_{0 < r \leq R} \sum_{q \leq Q} \frac{\mathfrak{S}(r)^2}{\rho(r, q)} + O\left(\frac{Rx^2}{\log^M x}\right).$$

Let us denote the number of primitive characters modulo f by $\phi^*(f)$. We note that this is a multiplicative function for which $\phi^*(p) = p - 2$. The sum over f is a quickly converging sum by (34) and (37), so we can drop the condition $f \leq Q_0$ for a price already paid by the error term. Writing back the definition of $C(f, Q)$, we obtain, after a little rearrangement, that

$$S = Y^2 \sum_{0 < r \leq R} \mathfrak{S}(r)^2 \sum_{q \leq Q} \frac{1}{\phi(q)} \left(\sum_{\substack{f|q \\ (r, f)=1 \\ f \text{ is square-free}}} \frac{\phi^*(f)}{\rho(r, f)^2} - \frac{\phi(q)}{\rho(r, q)} \right) + O\left(\frac{Rx^2}{\log^M x}\right).$$

Finally, let us notice that by (34) we actually have 0 inside the big parentheses, as everything is multiplicative and

$$\sum_{\substack{f|q \\ (r, f)=1 \\ f \text{ is square-free}}} \frac{\phi^*(f)}{\rho(r, f)^2} = \prod_{\substack{p|q \\ p \nmid r}} \left(1 + \frac{\phi^*(p)}{\rho(r, p)^2}\right) = \prod_{\substack{p|q \\ p \nmid r}} \left(1 + \frac{1}{p-2}\right) = \frac{\phi(q)}{\rho(r, q)}.$$

This completes the proof of Theorem 4. \square

7. PROOF OF PROPOSITION 13

This section consists of a proof of Proposition 13. This is done in two parts: an estimate of the error term in Proposition 13, which relies on Theorem 4, and an estimate of the main term, which consists mainly of the computation of the constant \mathfrak{C} . Note that in the course of proving Proposition 13 we can always assume $R \geq x^{\frac{1}{3}+\varepsilon}$ and $Y \geq \sqrt{X}$, as otherwise the error term is an obvious upper bound for all the other terms in (23). Note also that the term $r = 1$ behaves differently, as $p + 1 - r$ is always prime in this case. However, any trivial bound (obtained by dropping the primality of p and by bounding the character by 1) shows that this term is much smaller than the error term in Proposition 13; therefore, it can comfortably be excluded from any further investigation.

Note that, using notation (39), Theorem 4 can be formulated as

$$\sum_{0 < |r| \leq R} \sum_{q \leq Q} \sum_{a \pmod{q}} |E(X, Y; r, q, a)|^2 \ll \frac{Rx^2}{\log^M x},$$

whenever $x^{\frac{1}{3}+\varepsilon} \leq R \leq x$, $Q \leq x \log^{-N} x$, and $X + Y \leq x$.

Using the same notation, as well as (38), we rewrite the left hand side of (23) as

$$(40) \quad \sum_{\substack{|r| \leq R, r \neq 1 \\ f \leq V \\ n \leq U}} \frac{1}{nf} \sum_{a \pmod{4n}} \left(\frac{a}{n}\right) \psi \left(X, Y; r-1, nf^2, \frac{r^2 - af^2}{4} \right)$$

$$(41) \quad = Y \sum_{\substack{|r| \leq R, r \neq 1 \\ f \leq V \\ n \leq U}} \frac{1}{nf} \sum_{a \pmod{4n}} \left(\frac{a}{n}\right) \mathfrak{S} \left(r-1, nf^2, \frac{r^2 - af^2}{4} \right)$$

$$(42) \quad + \sum_{\substack{|r| \leq R, r \neq 1 \\ f \leq V \\ n \leq U}} \frac{1}{nf} \sum_{a \pmod{4n}} \left(\frac{a}{n}\right) E \left(X, Y; r-1, nf^2, \frac{r^2 - af^2}{4} \right).$$

7.1. Estimate of the error term in Proposition 13. In what follows, we will show how Theorem 4 allows us to control the error term (42). First, using the Cauchy-Schwarz inequality, we obtain

$$(43) \quad \sum_{\substack{|r| \leq R, r \neq 1 \\ f \leq V \\ n \leq U}} \frac{1}{nf} \sum_{a \pmod{4n}} \left(\frac{a}{n}\right) E \left(X, Y; r-1, nf^2, \frac{r^2 - af^2}{4} \right) \\ \leq \sum_{f \leq V} \frac{1}{f} \left(\sum_{\substack{|r| \leq R \\ n \leq U \\ a \pmod{4n}}} \frac{1}{n^2} \right)^{\frac{1}{2}} \left(\sum_{\substack{|r| \leq R, r \neq 1 \\ n \leq U \\ a \pmod{4n}}} E^2 \left(X, Y; r-1, nf^2, \frac{r^2 - af^2}{4} \right) \right)^{\frac{1}{2}}.$$

The first inner sum above is estimated trivially as

$$(44) \quad \left(\sum_{\substack{|r| \leq R \\ n \leq U \\ a \pmod{4n}}} \frac{1}{n^2} \right)^{\frac{1}{2}} \ll R^{\frac{1}{2}} \log^{\frac{1}{2}} U.$$

For the second inner sum we observe that

$$\sum_{\substack{|r| \leq R, r \neq 1 \\ n \leq U \\ a \pmod{4n}}} E^2 \left(X, Y; r-1, nf^2, \frac{r^2 - af^2}{4} \right) \leq \sum_{\substack{|r| \leq R \\ r \neq 1}} \sum_{q \leq 4Uf^2} \sum_{b \pmod{q}} E^2(X, Y; r-1, q, b),$$

as, for each fixed f, r, n , the residue classes

$$\left\{ b = \frac{r^2 - af^2}{4} : a \pmod{4nf^2} \right\}$$

cover each residue class modulo $4nf^2$ at most once. Then, using Theorem 4, we obtain

$$(45) \quad \sum_{\substack{|r| \leq R, r \neq 1 \\ n \leq U \\ a \pmod{4n}}} E^2 \left(X, Y; r-1, nf^2, \frac{r^2 - af^2}{4} \right) \ll \frac{Rx^2}{\log^M x}$$

for any $M > 0$, provided that

$$(46) \quad 4UV^2 \leq x \log^{-N} x.$$

Using the estimates (44) and (45) in (43), we finally obtain that

$$(47) \quad \sum_{\substack{|r| \leq R, r \neq 1 \\ f \leq V \\ n \leq U}} \frac{1}{nf} \sum_{a \pmod{4n}} \left(\frac{a}{n}\right) E \left(X, Y; r-1, nf^2, \frac{r^2 - af^2}{4} \right) \ll \frac{Rx \log^{\frac{1}{2}} U}{\log^{\frac{M}{2}} x} \sum_{f \leq V} \frac{1}{f} \\ \ll \frac{Rx}{\log^{\frac{M-3}{2}} x}$$

for any $M > 0$. This estimates the error term (42), and thus the error term of Proposition 13 (after renaming M).

7.2. Computation of the constant in Proposition 13. We now treat the main term (41) in (40), which is essentially a computation of the constant \mathfrak{C} in Theorem 1. We first analyze the sum over n and f of (41) when r is a *fixed* integer. We remark that the sum is zero if r is even, thus we can assume that r is odd. We also take $r \neq 1$.

Our goal in this section is to prove:

Proposition 15. *Let $r \neq 1$ be an odd integer. Then*

$$\sum_{\substack{f \leq V \\ n \leq U}} \frac{1}{nf} \sum_{a \pmod{4n}} \left(\frac{a}{n}\right) \mathfrak{S}\left(r-1, nf^2, \frac{r^2 - af^2}{4}\right) = C_r + O\left(\frac{1}{V^2} + \frac{1}{\sqrt{U}}\right),$$

where C_r is the positive constant

$$\begin{aligned} C_r &:= \sum_{f=1}^{\infty} \sum_{n=1}^{\infty} \frac{1}{nf} \sum_{a \pmod{4n}} \left(\frac{a}{n}\right) \mathfrak{S}\left(r-1, nf^2, \frac{r^2 - af^2}{4}\right) \\ &= \frac{4}{3} \prod_{\ell \neq 2} \frac{\ell^2(\ell^2 - 2\ell - 2)}{(\ell-1)^3(\ell+1)} \cdot \prod_{\substack{\ell \mid (r-1) \\ \ell \neq 2}} \left(1 + \frac{\ell+1}{\ell^2 - 2\ell - 2}\right) \cdot \prod_{\substack{\ell \mid r(r-2) \\ \ell \neq 2}} \left(1 + \frac{1}{\ell^2 - 2\ell - 2}\right). \end{aligned}$$

Proof of Proposition 15. Using the definition of $\mathfrak{S}(\cdot, \cdot, \cdot)$, we rewrite the left hand side of the desired equation in Proposition 15 as

$$(48) \quad 2 \left(\prod_{\ell \neq 2} \frac{\ell(\ell-2)}{(\ell-1)^2} \right) \sum_{\substack{f \leq V \\ f \text{ odd}}} \sum_{n \leq U} \frac{1}{nf\phi(nf^2)} \left(\prod_{\substack{\ell \mid nf^2(r-1) \\ \ell \neq 2}} \frac{\ell-1}{\ell-2} \right) c_f^r(n),$$

where

$$c_f^r(n) := \sum'_{a \pmod{4n}} \left(\frac{a}{n}\right)$$

and \sum' indicates that the sum is taken over the invertible residues a modulo $4n$ such that

$$\begin{aligned} &\left(\frac{r^2 - af^2}{4}, nf^2\right) = 1 \quad \text{and} \quad \left(\frac{r^2 - af^2}{4} - (r-1), nf^2\right) = 1 \\ \iff &\left(r^2 - af^2, 4nf^2\right) = 4 \quad \text{and} \quad \left(r^2 - af^2 - 4(r-1), 4nf^2\right) = 4. \end{aligned}$$

As r, f are odd and (r, f) divides $(r^2 - af^2, 4nf^2)$, we must have that $(r, f) = 1$; in this case,

$$\left(r^2 - af^2, 4nf^2\right) = 4 \iff \left(r^2 - af^2, 4n\right) = 4.$$

Similarly, as $(r-2, f)$ divides $(r^2 - af^2 - 4(r-1), nf^2) = ((r-2)^2 - af^2, nf^2)$, we must have $(r-2, f) = 1$; in this case,

$$\left((r-2)^2 - af^2, 4nf^2\right) = 4 \iff \left((r-2)^2 - af^2, 4n\right) = 4.$$

Thus

$$c_f^r(n) = \begin{cases} \sum_{\substack{a \pmod{4n}^* \\ (r^2 - af^2, 4n) = 4 \\ ((r-2)^2 - af^2, 4n) = 4}} \left(\frac{a}{n}\right) & \text{if } (r, f) = (r-2, f) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where $a \pmod{4n}^*$ denotes invertible residue classes a modulo $4n$.

To continue the proof, we need some properties of the function $c_f^r(n)$:

Lemma 16. *Let $r \neq 1$ be an odd integer and let f be a positive odd integer such that $(r, f) = (r-2, f) = 1$. Let $c_f^r(n)$ be as defined above. The following statements hold:*

(1) if n is odd, then

$$c_f^r(n) = \sum_{\substack{a(\bmod n)^* \\ (r^2 - af^2, n) = 1 \\ ((r-2)^2 - af^2, n) = 1}} \left(\frac{a}{n}\right),$$

where $a(\bmod n)^*$ denotes invertible residue classes a modulo n ;

(2) $c_f^r(n)$ is a multiplicative function of n ;

(3) if ℓ is an odd prime and $(\ell, f) = 1$, then

$$\frac{c_f^r(\ell^\alpha)}{\ell^{\alpha-1}} = \begin{cases} \ell - 2 & \text{if } \alpha \text{ is even and } \ell \mid r(r-2)(r-1), \\ \ell - 3 & \text{if } \alpha \text{ is even and } \ell \nmid r(r-2)(r-1), \\ -1 & \text{if } \alpha \text{ is odd and } \ell \mid r(r-2)(r-1), \\ -2 & \text{if } \alpha \text{ is odd and } \ell \nmid r(r-2)(r-1); \end{cases}$$

(4) if ℓ is an odd prime and $\ell \mid f$ (which implies that $(\ell, r) = (\ell, r-2) = 1$ by the hypotheses on f), then

$$\frac{c_f^r(\ell^\alpha)}{\ell^{\alpha-1}} = \begin{cases} 0 & \text{if } \alpha \text{ is odd,} \\ \ell - 1 & \text{if } \alpha \text{ is even;} \end{cases}$$

$$(5) \frac{c_f^r(2^\alpha)}{2^{\alpha-1}} = (-1)^\alpha.$$

Proof.

1. If n is odd, then

$$c_f^r(n) = \sum_{\substack{a(\bmod 4n)^*, a \equiv 1(\bmod 4) \\ (r^2 - af^2, n) = 1 \\ ((r-2)^2 - af^2, n) = 1}} \left(\frac{a}{n}\right) = \sum_{\substack{a(\bmod n)^* \\ (r^2 - af^2, n) = 1 \\ ((r-2)^2 - af^2, n) = 1}} \left(\frac{a}{n}\right),$$

where the last equality follows from the Chinese Remainder Theorem and the fact that $\left(\frac{a_1}{n}\right) = \left(\frac{a_2}{n}\right)$ when $a_1 \equiv a_2(\bmod n)$ for n odd.

2. Let n_1, n_2 be two co-prime positive integers with n_1 odd, and let $n = n_1 n_2$. Then, using the Chinese Remainder Theorem, we obtain

$$\begin{aligned} c_f^r(n_1)c_f^r(n_2) &= \sum_{\substack{a_1(\bmod n_1)^* \\ (r^2 - a_1 f^2, n_1) = 1 \\ ((r-2)^2 - a_1 f^2, n_1) = 1}} \left(\frac{a_1}{n_1}\right) \times \sum_{\substack{a_2(\bmod 4n_2)^* \\ (r^2 - a_2 f^2, 4n_2) = 4 \\ ((r-2)^2 - a_2 f^2, 4n_2) = 4}} \left(\frac{a_2}{n_2}\right) \\ &= \sum_{\substack{a(\bmod 4n_1 n_2)^* \\ (r^2 - af^2, 4n_1 n_2) = 4 \\ ((r-2)^2 - af^2, 4n_1 n_2) = 4}} \left(\frac{a}{n_1}\right) \left(\frac{a}{n_2}\right) = c_f^r(n_1 n_2). \end{aligned}$$

3. We have that

$$(49) \quad c_f^r(\ell^\alpha) = \ell^{\alpha-1} \sum_{\substack{a(\bmod \ell)^* \\ (r^2 - af^2, \ell) = 1 \\ ((r-2)^2 - af^2, \ell) = 1}} \left(\frac{a}{\ell}\right)^\alpha = \ell^{\alpha-1} \left(\sum_{a(\bmod \ell)^*} \left(\frac{a}{\ell}\right)^\alpha - \sum_{\substack{a(\bmod \ell)^* \\ a \equiv \bar{f}^{-2} r^2(\bmod \ell) \text{ or} \\ a \equiv \bar{f}^{-2} (r-2)^2(\bmod \ell)}} \left(\frac{a}{\ell}\right)^\alpha \right),$$

where \bar{f} denotes the inverse of f modulo ℓ . We then need to count the number of invertible residues a modulo ℓ which are eliminated by the two congruence conditions of the second sum. If $r \equiv 0, 1, 2(\bmod 4)$, there is exactly one such residue (notice that $r^2 \equiv (r-2)^2(\bmod \ell) \iff r \equiv 1(\bmod \ell)$). In all three cases, this residue is an invertible square modulo ℓ , and the second sum on the right hand side of (49) has value $+1$. The result follows immediately when α is even, and follows from the orthogonality relations when α is odd. If $r \not\equiv 0, 1, 2(\bmod \ell)$, there are two invertible residues which are eliminated by the two congruence conditions on a , and the second sum on the right hand side of (49) has value $+2$. The result follows as above.

4. We have that

$$c_f^r(\ell^\alpha) = \ell^{\alpha-1} \sum_{\substack{a \pmod{\ell}^* \\ (r^2 - af^2, \ell) = 1 \\ ((r-2)^2 - af^2, \ell) = 1}} \left(\frac{a}{\ell}\right)^\alpha = \ell^{\alpha-1} \sum_{a \pmod{\ell}^*} \left(\frac{a}{\ell}\right)^\alpha$$

since $(r^2 - af^2, \ell) = ((r-2)^2 - af^2, \ell) = 1$ for all a when $\ell \mid f$ and $(r, f) = (r-2, f) = 1$. The result follows immediately when α is even, and using the orthogonality relations when α is odd.

5. Let $\alpha \geq 1$. Since $\left(\frac{a}{2}\right)$ is a character modulo 8, we write

$$c_f^r(2^\alpha) = 2^{\alpha-1} \sum_{\substack{a \pmod{8}^* \\ (r^2 - af^2, 2^{\alpha+2}) = 4 \\ ((r-2)^2 - af^2, 2^{\alpha+2}) = 4}} \left(\frac{a}{2}\right)^\alpha = 2^{\alpha-1} \left(\frac{5}{2}\right)^\alpha = 2^{\alpha-1}(-1)^\alpha.$$

□

Using parts 3 and 4 of Lemma 16, we write

$$\begin{aligned} & \sum_{\substack{f \leq V \\ f \text{ odd}}} \sum_{n \leq U} \frac{1}{nf\phi(nf^2)} \left(\prod_{\substack{\ell \mid nf^2(r-1) \\ \ell \neq 2}} \frac{\ell-1}{\ell-2} \right) c_f^r(n) \\ &= \sum_{\substack{f=1 \\ (2, f) = (r, f) = (r-2, f) = 1}}^{\infty} \sum_{n=1}^{\infty} \frac{1}{nf\phi(nf^2)} \left(\prod_{\substack{\ell \mid nf^2(r-1) \\ \ell \neq 2}} \frac{\ell-1}{\ell-2} \right) c_f^r(n) + O\left(\frac{1}{V^2} + \frac{1}{\sqrt{U}}\right) \\ &=: D_r + O\left(\frac{1}{V^2} + \frac{1}{\sqrt{U}}\right). \end{aligned}$$

Note that

$$C_r = 2 \prod_{\ell \neq 2} \frac{\ell(\ell-2)}{(\ell-1)^2} D_r.$$

The rest of this section consists of writing D_r as an Euler product. We first write the sum over n as a product. In order to have multiplicative functions of n , we use the formulas

$$\begin{aligned} \phi(nf^2) &= \frac{\phi(n)\phi(f^2)(n, f^2)}{\phi((n, f^2))}, \\ \prod_{\substack{\ell \mid nf^2(r-1) \\ \ell \neq 2}} \frac{\ell-1}{\ell-2} &= \left(\prod_{\substack{\ell \mid n \\ \ell \neq 2}} \frac{\ell-1}{\ell-2} \right) \left(\prod_{\substack{\ell \mid f^2(r-1) \\ \ell \neq 2}} \frac{\ell-1}{\ell-2} \right) \left(\prod_{\substack{\ell \mid (n, f^2(r-1)) \\ \ell \neq 2}} \frac{\ell-2}{\ell-1} \right). \end{aligned}$$

Now we rewrite D_r as

$$\left(\sum_{\substack{f \geq 1 \\ f \text{ odd} \\ (r, f) = (r-2, f) = 1}} \frac{1}{f\phi(f^2)} \prod_{\substack{\ell \mid f^2(r-1) \\ \ell \neq 2}} \frac{\ell-1}{\ell-2} \right) \sum_{n \geq 1} \frac{c_f^r(n)}{n\phi(n)} \frac{\phi((f^2, n))}{(f^2, n)} \left(\prod_{\substack{\ell \mid n \\ \ell \neq 2}} \frac{\ell-1}{\ell-2} \right) \left(\prod_{\substack{\ell \mid (n, f^2(r-1)) \\ \ell \neq 2}} \frac{\ell-2}{\ell-1} \right).$$

The sum over n is the sum of a multiplicative function of n whose factors at prime powers ℓ^α depend on the divisibilities of $f, r, r-1$ and $r-2$ by ℓ . Using Lemma 16, we write the n -sum as

$$\left(\prod_{\ell \mid f} \sum_{\alpha \geq 0} a_r(\ell^\alpha) \right) \left(\prod_{\ell \mid f} \sum_{\alpha \geq 0} b_r(\ell^\alpha) \right) = \left(\prod_{\ell} \sum_{\alpha \geq 0} b_r(\ell^\alpha) \right) \left(\prod_{\ell \mid f} \frac{\sum_{\alpha \geq 0} a_r(\ell^\alpha)}{\sum_{\alpha \geq 0} b_r(\ell^\alpha)} \right),$$

where $a_r(1) = b_r(1) = 1$ and for $\ell \neq 2$ and $\alpha \geq 1$,

$$a_r(\ell^\alpha) = \begin{cases} 0 & \text{if } \alpha \text{ odd,} \\ (\ell - 1)/(\ell^{\alpha+1}) & \text{if } \alpha \text{ even;} \end{cases}$$

$$b_r(\ell^\alpha) = \begin{cases} -2/\ell^\alpha(\ell - 2) & \text{if } \alpha \text{ odd and } \ell \nmid r(r-1)(r-2), \\ (\ell - 3)/\ell^\alpha(\ell - 2) & \text{if } \alpha \text{ even and } \ell \nmid r(r-1)(r-2), \\ -1/\ell^\alpha(\ell - 2) & \text{if } \alpha \text{ odd and } \ell \mid r(r-2), \\ 1/\ell^\alpha & \text{if } \alpha \text{ even and } \ell \mid r(r-2), \\ -1/\ell^\alpha(\ell - 1) & \text{if } \alpha \text{ odd and } \ell \mid r-1, \\ (\ell - 2)/\ell^\alpha(\ell - 1) & \text{if } \alpha \text{ even and } \ell \mid r-1. \end{cases}$$

Replacing in D_r , this gives

$$\begin{aligned} D_r &= \left(\prod_{\ell} \sum_{\alpha \geq 0} b_r(\ell^\alpha) \right) \sum_{\substack{f \geq 1 \\ f \text{ odd} \\ (r,f)=(r-2,f)=1}} \frac{1}{f\phi(f^2)} \left(\prod_{\substack{\ell \mid f^{2(r-1)} \\ \ell \neq 2}} \frac{\ell - 1}{\ell - 2} \right) \left(\prod_{\substack{\ell \mid f \\ \alpha \geq 0}} \frac{\sum_{\alpha \geq 0} a_r(\ell^\alpha)}{\sum_{\alpha \geq 0} b_r(\ell^\alpha)} \right) \\ &= \left(\prod_{\ell} \sum_{\alpha \geq 0} b_r(\ell^\alpha) \right) \left(\prod_{\substack{\ell \mid (r-1) \\ \ell \neq 2}} \frac{\ell - 1}{\ell - 2} \right) \times \\ &\quad \times \sum_{\substack{f \geq 1 \\ f \text{ odd} \\ (r,f)=(r-2,f)=1}} \frac{1}{f\phi(f^2)} \left(\prod_{\substack{\ell \mid f^2 \\ \ell \neq 2}} \frac{\ell - 1}{\ell - 2} \right) \left(\prod_{\substack{\ell \mid (f^2, r-1) \\ \ell \neq 2}} \frac{\ell - 2}{\ell - 1} \right) \left(\prod_{\substack{\ell \mid f \\ \alpha \geq 0}} \frac{\sum_{\alpha \geq 0} a_r(\ell^\alpha)}{\sum_{\alpha \geq 0} b_r(\ell^\alpha)} \right). \end{aligned}$$

The sum over f in the last expression is a sum of multiplicative functions of f , which we write as

$$\prod_{\ell \nmid 2r(r-2)} \sum_{\alpha \geq 0} c_r(\ell^\alpha).$$

Here $c_r(1) = 1$ and for any prime ℓ with $\ell \nmid 2r(r-2)$ and any $\alpha \geq 1$, we have

$$c_r(\ell^\alpha) = \begin{cases} \frac{1}{\ell^{3\alpha-1}(\ell - 2)} \cdot \frac{\sum_{\beta \geq 0} a_r(\ell^\beta)}{\sum_{\beta \geq 0} b_r(\ell^\beta)} & \text{if } \ell \nmid r-1, \\ \frac{1}{\ell^{3\alpha-1}(\ell - 1)} \cdot \frac{\sum_{\beta \geq 0} a_r(\ell^\beta)}{\sum_{\beta \geq 0} b_r(\ell^\beta)} & \text{if } \ell \mid r-1. \end{cases}$$

Then

$$(50) \quad D_r = \left(\prod_{\ell} \sum_{\alpha \geq 0} b_r(\ell^\alpha) \right) \left(\prod_{\substack{\ell \mid (r-1) \\ \ell \neq 2}} \frac{\ell - 1}{\ell - 2} \right) \left(\prod_{\ell \nmid 2r(r-2)} \sum_{\alpha \geq 0} c_r(\ell^\alpha) \right).$$

We now compute the sums appearing in (50), using the formulas for $a_r(\ell)$ and $b_r(\ell)$ listed above:

Lemma 17. *Let ℓ be an odd prime and $\alpha \geq 1$. Let $a_r(\ell^\alpha)$, $b_r(\ell^\alpha)$ and $c_r(\ell^\alpha)$ be as defined above. We have:*

- (1) $A(\ell) := \sum_{\alpha \geq 0} a_r(\ell^\alpha) = \frac{\ell^2 + \ell + 1}{\ell(\ell + 1)}$;
- (2) if $\ell \nmid r(r-1)(r-2)$, then $B^{(1)}(\ell) := \sum_{\alpha \geq 0} b_r(\ell^\alpha) = \frac{\ell^3 - 2\ell^2 - 2\ell - 1}{(\ell - 2)(\ell^2 - 1)}$;

- (3) if $\ell \mid r-1$, then $B^{(2)}(\ell) := \sum_{\alpha \geq 0} b_r(\ell^\alpha) = \frac{\ell^3 - \ell^2 - \ell - 1}{(\ell-1)^2(\ell+1)}$;
- (4) if $\ell \nmid r-1$, but $\ell \mid r(r-2)$, then $B^{(3)}(\ell) := \sum_{\alpha \geq 0} b_r(\ell^\alpha) = \frac{\ell(\ell^2 - 2\ell - 1)}{(\ell-2)(\ell^2-1)}$;
- (5) if $\ell \nmid 2r(r-2)(r-1)$, then $C^{(1)}(\ell) := \sum_{\alpha \geq 0} c_r(\ell^\alpha) = \frac{\ell^3 - 2\ell^2 - 2\ell}{\ell^3 - 2\ell^2 - 2\ell - 1}$;
- (6) if $\ell \mid r-1$, then $C^{(2)}(\ell) := \sum_{\alpha \geq 0} c_r(\ell^\alpha) = \frac{\ell(\ell^2 - \ell - 1)}{\ell^3 - \ell^2 - \ell - 1}$;
- (7) if $\ell = 2$, then $B(2) := \sum_{\alpha \geq 0} b_r(\ell^\alpha) = \frac{2}{3}$.

Proof. All the computations are straightforward, following from the formula for the sum of the geometric series. \square

We extend the definitions of $A(\ell), B^{(1)}(\ell), B^{(2)}(\ell), B^{(3)}(\ell), C^{(1)}(\ell), C^{(2)}(\ell)$ introduced in Lemma 17 to any odd prime ℓ (independently of the relation between ℓ and r). Then we rewrite D_r as

$$\begin{aligned} D_r &= B(2) \left(\prod_{\ell \neq 2} \sum_{\alpha \geq 0} b_r(\ell^\alpha) \right) \left(\prod_{\substack{\ell \mid r-1 \\ \ell \neq 2}} \frac{\ell-1}{\ell-2} \right) \left(\prod_{\ell \nmid 2r(r-2)} \sum_{\alpha \geq 0} c_r(\ell^\alpha) \right) \\ &= B(2) \left(\prod_{\ell \neq 2} B^{(1)}(\ell) C^{(1)}(\ell) \right) \left(\prod_{\substack{\ell \mid r(r-2) \\ \ell \neq 2}} B^{(1)}(\ell)^{-1} C^{(1)}(\ell)^{-1} B^{(3)}(\ell) \right) \times \\ &\quad \times \left(\prod_{\substack{\ell \mid r-1 \\ \ell \neq 2}} B^{(1)}(\ell)^{-1} C^{(1)}(\ell)^{-1} B^{(2)}(\ell) \frac{\ell-1}{\ell-2} C^{(2)}(\ell) \right). \end{aligned}$$

Using Lemma 17, we compute

$$\begin{aligned} B^{(1)}(\ell) C^{(1)}(\ell) &= \frac{\ell^3 - 2\ell^2 - 2\ell}{\ell^3 - 2\ell^2 - \ell + 2} = \frac{\ell(\ell^2 - 2\ell - 2)}{(\ell-2)(\ell^2-1)}, \\ B^{(1)}(\ell)^{-1} C^{(1)}(\ell)^{-1} B^{(3)}(\ell) &= \frac{\ell^2 - 2\ell - 1}{\ell^2 - 2\ell - 2} = 1 + \frac{1}{\ell^2 - 2\ell - 2}, \\ B^{(1)}(\ell)^{-1} C^{(1)}(\ell)^{-1} B^{(2)}(\ell) C^{(2)}(\ell) \frac{\ell-1}{\ell-2} &= \frac{\ell^2 - \ell - 1}{\ell^2 - 2\ell - 2} = 1 + \frac{\ell+1}{\ell^2 - 2\ell - 2}. \end{aligned}$$

Finally, replacing all the above in (48), we obtain

$$\begin{aligned} C_r &= \frac{4}{3} \left(\prod_{\ell \neq 2} \frac{\ell(\ell-2)}{(\ell-1)^2} \cdot \frac{\ell(\ell^2 - 2\ell - 2)}{(\ell-2)(\ell^2-1)} \right) \cdot \prod_{\substack{\ell \mid r-1 \\ \ell \neq 2}} \left(1 + \frac{\ell+1}{\ell^2 - 2\ell - 2} \right) \cdot \prod_{\substack{\ell \mid r(r-2) \\ \ell \neq 2}} \left(1 + \frac{1}{\ell^2 - 2\ell - 2} \right) \\ &= \frac{4}{3} \prod_{\ell \neq 2} \frac{\ell^2(\ell^2 - 2\ell - 2)}{(\ell-1)^3(\ell+1)} \cdot \prod_{\substack{\ell \mid (r-1) \\ \ell \neq 2}} \left(1 + \frac{\ell+1}{\ell^2 - 2\ell - 2} \right) \cdot \prod_{\substack{\ell \mid r(r-2) \\ \ell \neq 2}} \left(1 + \frac{1}{\ell^2 - 2\ell - 2} \right). \end{aligned}$$

This completes the proof of Proposition 15. \square

7.3. The average constant. Using Proposition 15, the main term (41) of (40) is $Y \sum_{|r| \leq R, r \neq 1 \text{ odd}} C_r$; thus now we need to average the constant C_r over r . This calculation has similarities with the one done by Gallagher in [Gal] for the average of the standard twin prime constant. As such, we will follow the notation used in [Gal].

The main result of this section is:

Lemma 18. As $R \rightarrow \infty$,

$$\sum_{\substack{|r| \leq R \\ r \neq 1 \text{ odd}}} C_r = 2\mathfrak{C}R + O(\log^2 R).$$

Proof. Let us write

$$(51) \quad C_r = \frac{4}{3} \prod_{\ell \neq 2} \frac{\ell^2(\ell^2 - 2\ell - 2)}{(\ell - 1)^3(\ell + 1)} \cdot \prod_{\substack{\ell \neq 2 \\ \ell | r(r-1)(r-2)}} (1 + e_r(\ell)),$$

where

$$e_r(\ell) := \begin{cases} e^{(1)}(\ell) & \text{if } \ell \mid r - 1 \\ e^{(2)}(\ell) & \text{if } \ell \mid r(r - 2) \\ 0 & \text{otherwise} \end{cases} = \begin{cases} \frac{\ell + 1}{\ell^2 - \ell - 2} & \text{if } \ell \mid r - 1, \\ \frac{1}{\ell^2 - 2\ell - 2} & \text{if } \ell \mid r(r - 2), \\ 0 & \text{otherwise.} \end{cases}$$

Let us also fix the following notation: for $r \neq 1$ odd, we take

$$\begin{aligned} \mathcal{P}(r) &:= \{\ell \text{ odd prime} : \ell \mid r(r - 1)(r - 2)\}, \\ \mathcal{F}(r) &:= \{q \text{ positive square-free integer} : \ell \mid q \Rightarrow \ell \in \mathcal{P}(r)\}, \\ \mathcal{D}(R) &:= \bigcup_{\substack{|r| \leq R \\ r \neq 1 \text{ odd}}} \mathcal{F}(r). \end{aligned}$$

We want to evaluate

$$(52) \quad \mathcal{S} := \sum_{\substack{|r| \leq R \\ r \neq 1 \text{ odd}}} \prod_{\substack{\ell \neq 2 \\ \ell | r(r-1)(r-2)}} (1 + e_r(\ell)) = \sum_{\substack{|r| \leq R \\ r \neq 1 \text{ odd}}} \sum_{q \in \mathcal{F}(r)} e_r(q),$$

where $e_r(1) = 1$ and, for $q \neq 1$, $e_r(q) = \prod_{\ell | q} e_r(\ell)$. We write

$$\begin{aligned} \mathcal{S} &= \sum_{q \in \mathcal{D}(R)} \sum_{\substack{|r| \leq R \\ r \neq 1 \text{ odd}}} e_r(q) = \sum_{q \in \mathcal{D}(R)} \sum_{\substack{\text{all possible} \\ e = e(q)}} \sum_{\substack{|r| \leq R \\ r \neq 1 \text{ odd} \\ e_r(q) = e}} e_r(q) \\ &= \sum_{q \in \mathcal{D}(R)} \sum_{\substack{\text{all possible} \\ e = e(q)}} \#\{|r| \leq R : r \neq 1 \text{ odd}, e_r(q) = e\} \\ &= \sum_{q \in \mathcal{D}(R)} \sum_{v = v(q)} \prod_{\ell | q} e^{v(\ell)}(\ell) N(q, v), \end{aligned}$$

where the sum $\sum_{v = v(q)}$ is over all maps $v : \{\ell : \ell | q\} \rightarrow \{1, 2\}$ and where

$$N(q, v) := \#\{|r| \leq R : r \neq 1 \text{ odd}, e_r(\ell) = e^{v(\ell)}(\ell) \forall \ell | q\}.$$

By looking at the conditions imposed on ℓ when defining $e^{(1)}(\ell)$ and $e^{(2)}(\ell)$, we see that $N(q, v)$ is the number of integers $|r| \leq R$ with $r \neq 1$ odd such that

$$\begin{aligned} r &\equiv 1 \pmod{2}, \\ r &\equiv 1 \pmod{\ell} \quad \forall \ell | q \text{ with } v(\ell) = 1, \\ r &\equiv 0 \text{ or } 2 \pmod{\ell} \quad \forall \ell | q \text{ with } v(\ell) = 2. \end{aligned}$$

Therefore, by using the Chinese Remainder Theorem, r as above lies in one of $\prod_{\ell|q} 2^{v(\ell)-1}$ distinct residue classes modulo $2q$. Consequently,

$$\begin{aligned} N(q, v) &= \left(\prod_{\ell|q} 2^{v(\ell)-1} \right) \left(\frac{2R+1}{2q} + O(1) \right) \\ &= \frac{R}{q} \prod_{\ell|q} 2^{v(\ell)-1} + O\left(2^{\omega(q)}\right), \end{aligned}$$

where $\omega(q)$ denotes the number of distinct prime factors of q . We plug this in the formula for \mathcal{S} and obtain

$$\begin{aligned} \mathcal{S} &= R \sum_{q \in \mathcal{D}(R)} \frac{1}{q} \sum_{v=v(q)} \prod_{\ell|q} e^{v(\ell)}(\ell) 2^{v(\ell)-1} + O\left(\sum_{q \in \mathcal{D}(R)} 2^{\omega(q)} \sum_{v=v(q)} \prod_{\ell|q} e^{v(\ell)}(\ell) \right) \\ &=: \mathcal{S}_{\text{main}} + \mathcal{S}_{\text{error}}. \end{aligned}$$

To estimate $\mathcal{S}_{\text{main}}$, we observe that we have

$$\mathcal{S}_{\text{main}} = R \sum_{q \in \mathcal{D}(R)} G(q)$$

for some multiplicative function $G(q)$. Therefore

$$\begin{aligned} \mathcal{S}_{\text{main}} &= R \prod_{\substack{\ell \leq R \\ \ell \neq 2}} (1 + G(\ell)) = R \prod_{\substack{\ell \leq R \\ \ell \neq 2}} \left(1 + \frac{e^{(1)}(\ell) + 2e^{(2)}(\ell)}{\ell} \right) \\ &= R \prod_{\substack{\ell \leq R \\ \ell \neq 2}} \frac{\ell^3 - 2\ell^2 - \ell + 3}{\ell(\ell^2 - 2\ell - 2)} = R \prod_{\ell \neq 2} \frac{\ell^3 - 2\ell^2 - \ell + 3}{\ell(\ell^2 - 2\ell - 2)} + O(1). \end{aligned}$$

Now let us estimate $\mathcal{S}_{\text{error}}$. As for $\mathcal{S}_{\text{main}}$, we observe that we have

$$\mathcal{S}_{\text{error}} = O\left(\sum_{q \in \mathcal{D}(R)} F(q) \right)$$

for some multiplicative function $F(q)$. Therefore

$$\begin{aligned} \mathcal{S}_{\text{error}} &= O\left(\prod_{\substack{\ell \leq R \\ \ell \neq 2}} [1 + 2(e^{(1)}(\ell) + e^{(2)}(\ell))] \right) \\ &= O\left(\prod_{\substack{\ell \leq R \\ \ell \neq 2}} \left(1 + \frac{2(\ell^2 + \ell - 1)}{\ell(\ell^2 - 2\ell - 2)} \right) \right) = O((\log R)^2). \end{aligned}$$

We put the two estimates together and obtain

$$\mathcal{S} = R \prod_{\substack{\ell \leq R \\ \ell \neq 2}} \frac{\ell^3 - 2\ell^2 - \ell + 3}{\ell(\ell^2 - 2\ell - 2)} + O((\log R)^2).$$

By replacing (52) in (51), this gives

$$\begin{aligned} \sum_{\substack{|r| \leq R \\ r \neq 1 \text{ odd}}} C_r &= \frac{4R}{3} \prod_{\ell \neq 2} \frac{\ell^2(\ell^2 - 2\ell - 2)}{(\ell - 1)^3(\ell + 1)} \cdot \frac{\ell^3 - 2\ell^2 - \ell + 3}{\ell(\ell^2 - 2\ell - 2)} + O(\log^2 R) \\ &= \frac{4R}{3} \prod_{\ell \neq 2} \frac{\ell^4 - 2\ell^3 - \ell^2 + 3\ell}{(\ell - 1)^3(\ell + 1)} + O(\log^2 R), \end{aligned}$$

which completes the proof of Lemma 18. □

Replacing Proposition 15 and Lemma 18 in (41), this concludes the proof of Proposition 13. \square

Acknowledgements: The authors thank Andrew Granville, Nathan Jones and Igor Shparlinski for helpful comments, and the referees for their careful reading of the paper and useful suggestions. Part of this work was done while (some of) the authors visited the American Institute for Mathematics (Palo Alto, USA), the Fields Institute for Research in Mathematical Sciences (Toronto, Canada), and the Max Plank Institute for Mathematics (Bonn, Germany); the authors thank these institutes for the financial support and work facilities provided.

REFERENCES

- [Bal] A. Balog, *The prime k -tuples conjecture on average*, in Analytic Number Theory (Allerton Park, IL, 1989), Progr. Math. **85**, Birkhäuser, 1990, 47–75.
- [BaSh] B. Banks and I. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics for elliptic curves of small height*, Israel J. Math. **173**, 2009, 253–277.
- [Bai] S. Baier, *A remark on the Lang-Trotter Conjecture*, to appear in Proceedings of the Conference “New Directions in the Theory of Universal Zeta- and L-Functions”, Würzburg, October 2008.
- [Chu] N.G. Chudakov, *On Goldbach-Vinogradov’s theorem*, Annals of Math. **48**, 1947, 515–545.
- [Co] A.C. Cojocaru, *Reductions of an elliptic curve with almost prime orders*, Acta Arithmetica **119** no. 3, 2005, 265–289.
- [Da] H. Davenport, *Multiplicative Number Theory*, third edition, Springer Verlag, 1980.
- [DaPa1] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, International Mathematics Research Notices **4**, 1999, 165–183.
- [DaPa2] C. David and F. Pappalardi, *Average Frobenius distribution for inerts in $\mathbb{Q}(i)$* , Journal of the Ramanujan Mathematical Society **19**, 2004, 1–21.
- [DaWu] C. David and J. Wu, *Almost prime values of the order of elliptic curves over finite fields*, to appear in Forum Mathematicum.
- [De] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Hamb. Abh., 1941, 197–272.
- [FoMu] E. Fouvry and R. Murty, *On the distribution of supersingular primes*, Canadian Journal of Mathematics **48**, 1996, 81–104.
- [FrIw] J. B. Friedlander and H. Iwaniec, *The divisor problem for arithmetic progressions*, Acta Arithmetica **45**, 1985, 273–277.
- [Gal] P.X. Gallagher, *On the distribution of primes in short intervals*, Mathematika **23** no. 1, 1976, 4–9.
- [HaLi] G.H. Hardy and J.E. Littlewood, *Some problems of ‘partitio numerorum’; III: on the expression of a number as a sum of primes*, Acta Mathematica **44**, 1922, 1–70.
- [Hu] L. K. Hua, *Introduction to number theory*, Springer-Verlag, Heidelberg, 1982.
- [IwJU] H. Iwaniec and J. Jiménez Urroz, *Almost prime orders of elliptic curves with CM modulo p* , to appear in Annali della Scuola Normale Superiore di Pisa, issue 4, vol. IX/2010, series V.
- [JU] J. Jiménez Urroz, *Almost prime orders of CM elliptic curves modulo p* , Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, 74–87.
- [Jo1] N. Jones, *Almost all elliptic curves are Serre curves*, Transactions of the AMS **36** no. 3, 2010, 1547–1570.
- [Jo2] N. Jones, *Averages of elliptic curve constants*, Mathematische Annalen **345** no. 3, 2009, 685–710.
- [Jo3] N. Jones, *Primes p for which $\#E(\mathbb{F}_p)$ has only large prime factors*, appendix to “Geometry and arithmetic of verbal dynamical systems on simple groups” by T. Bandman, F. Grunewald and B. Kunyavskii, preprint.
- [Ko] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific Journal of Mathematics **131** no. 1, 1988, 157–165.
- [LaTr] S. Lang and H. Trotter, *Frobenius distribution in GL_2 -extensions*, Lecture Notes in Mathematics **504**, Springer, Heidelberg, 1976.
- [Lav] A. F. Lavrik, *The number of k -twin primes lying on an interval of given length*, Dokl. Acad. Nauk. SSSR **136**, 1961, 281–283 (Russian), translated as Soviet Math. Dokl. **2**, 1961, 52–55.
- [MaPo] H. Maier and C. Pomerance, *Unusually large gaps between consecutive primes*, Trans. of the AMS **322**, 1990, 201–237.
- [MiMu] S.A. Miri and V.K. Murty, *An application of sieve methods to elliptic curves*, Indocrypt 2001, Springer Lecture Notes **2247**, 2001, 91–98.
- [MoVa] H.L. Montgomery and R.C. Vaughan, *The exceptional set in Goldbach’s problem*, Acta Arithmetica **27**, 1975, 353–370.
- [PePi] A. Perelli and J. Pintz, *On the exceptional set for Goldbach’s problem in short intervals*, J. London Math. Soc. (2) **47**, 1993, 41–49.
- [Se] J.-P. Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Inventiones Mathematicae **15**, 1972, 259–331.

- [So] K. Soundararajan, *The distribution of prime numbers*, in *Equidistribution in Number Theory, an Introduction*, NATO Science Series II. Mathematics, Physics and Chemistry **237**, Springer, 2007, 59–83.
- [StWe] J. Steuding and A. Weng, *On the number of prime divisors of the order of elliptic curves modulo p* , *Acta Arithmetica* **117** no. 4, 2005, 341–352; erratum in *Acta Arithmetica* **119** no. 4, 2005, 407–408.
- [Te] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics 46, Cambridge University Press, 2004.
- [Wa] N. Walji, *Supersingular distribution on average for congruence classes of primes*, to appear in *Acta Arithmetica*.
- [Zy1] D. Zywna, *The large sieve and Galois representations*, preprint.
- [Zy2] D. Zywna, *A refinement of Koblitz’s conjecture*, preprint.

(Antal Balog) ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, H-1053 BUDAPEST, REÁLTANODA U. 13-15, HUNGARY.

E-mail address, Antal Balog: balog@renyi.hu

(Alina-Carmen Cojocaru) DEPARTMENT OF MATHEMATICS, STATISTICS AND COMPUTER SCIENCE, UNIVERSITY OF ILLINOIS AT CHICAGO, 851 S MORGAN ST, 322 SEO, CHICAGO, 60607, IL, USA; INSTITUTE OF MATHEMATICS “SIMION STOILOW” OF THE ROMANIAN ACADEMY, 21 CALEA GRIVITEI ST, BUCHAREST, 010702, SECTOR 1, ROMANIA.

E-mail address, Alina-Carmen Cojocaru: cojocaru@math.uic.edu

(Chantal David) DEPARTMENT OF MATHEMATICS AND STATISTICS, CONCORDIA UNIVERSITY, 1455 DE MAISONNEUVE WEST, MONTRÉAL, QC, H3G 1M8, CANADA; INSTITUTE FOR ADVANCED STUDY, EINSTEIN DRIVE, PRINCETON, NJ, 08540, USA.

E-mail address, Chantal David: cdavid@mathstat.concordia.ca