Average twin prime conjecture for elliptic curves

Antal Balog (Alfréd Rényi Institute of Mathematics)
balog@renyi.hu
Alina-Carmen Cojocaru (University of Illinois at Chicago) [*]
cojocaru@math.uic.edu
Chantal David (Concordia University) [†]
cdavid@mathstat.concordia.ca

February 1, 2008

Abstract

Let E be an elliptic curve over $\mathbb{Q}$. In 1988, 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 and 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 in the style of Barban-Davenport-Halberstam, where the average is taken over twin primes and their differences.

Contents

1 Introduction

A well-known open problem in number theory is *the twin prime conjecture*, which states that that there exist infinitely many primes p such that $p+2$ is also a prime. This conjecture

[*]Research supported in part by NSF grant DMS-0636750.

[†]Research supported in part by NSERC.

was generalized by Alphonse 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 made this statement precise, predicting that, as $x \to \infty$,

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

where

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

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

Even though still inaccessible by current methods, the twin prime conjecture has generated tremendous advances in number theory. Indeed, in 1919 Viggo Brun [Br] developed what is now known as the Brun sieve to prove the surprising result that $\sum\limits_{\substack{p \\ p+2 \text{ prime}}} \frac{1}{p} < \infty$. Brun's methods opened the way to sieve theory, leading to upper bounds of the right order of magnitude for the number of twin primes $p \leq x$ and to the important achievement of Jingrun Chen [Che] 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 another important application of sieve theory, the Bombieri-Vinogradov theorem on averages of primes in an arithmetic progression, obtained independently by E. Bombieri and A.I. Vinogradov in the mid 1960s. In the late 1980s, H. Maier and C. Pomerance, and, subsequently, the first author of this paper, obtained similar Bombieri-Vinogradov type results concerning averages of twin primes (see [MaPo], [Ba]), by building on previous work of N.G. Chudakov, A.F. Lavrik, H.L. Montgomery and R.C. Vaughan.

The twin prime conjecture can be generalized in many directions. For instance, the Hardy-Littlewood heuristics 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 $\mathbb{F}_p^* \backslash \{\pm 1\}$ is of prime order. Such a reformulation may then be easily generalized to other groups, say to 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 Neal Koblitz in 1988:

Koblitz's Conjecture [Ko]

Let $E/\mathbb{Q}$ be an elliptic curve defined over the field of rational numbers. We assume that E is not $\mathbb{Q}$-isogenous to an elliptic curve with non-trivial $\mathbb{Q}$-torsion subgroup. Then there exists a positive constant $C(E)$ such that, as $x \to \infty$,

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

A candidate for the explicit constant $C(E)$ was given by Koblitz in his paper and was later corrected by D. Zywina [Zy]. It is described in detail in Section 2 in the generic case that $E/\mathbb{Q}$ is without complex multiplication.

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 $|a_p(E)| \leq 2\sqrt{p}$. This also makes the analogy between Koblitz's Conjecture and the twin prime conjecture more apparent. Exploiting 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], and H. Iwaniec and J. Jimenez Urroz [IwUr]. We currently know upper bounds of the right order of magnitude for $\pi_E^{\text{twin}}(x)$ ([Co]), provided the Generalized Riemann Hypothesis holds if $E/\mathbb{Q}$ is without complex multiplication, and various lower bounds in the style of Chen's result ([MiMu], [StWe], [Co], [IwUr]). Regarding lower bounds, the best result that one may hope to achieve by sieve technology was obtained by [IwUr] for the complex multiplication elliptic curve $E : y^2 = x^3 - x$. They showed that

$$\#\left\{p \leq x : p \equiv 1 (\operatorname{mod} 4), \frac{1}{8}\left|E(\mathbb{F}_p)\right| = P_2\right\} \gg \frac{x}{\log^2 x}.$$

The main purpose of this 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 $A = A(x), B = B(x)$ be parameters such that $A, B > x^{1/2+\varepsilon}$ and $AB > x^{3/2+\varepsilon}$ for any fixed $\varepsilon > 0$. Let $\mathcal{C}$ 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 $x \to \infty$,*

$$\frac{1}{|\mathcal{C}|}\sum_{E \in \mathcal{C}} \pi_E^{\text{twin}}(x) \sim \mathfrak{C}\frac{x}{\log^2 x},$$

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

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

As will be shown in Section 2, the average constant $\mathfrak{C}$ gives further evidence for the conjectural constant of Koblitz's Conjecture.

The first steps in the proof of Theorem 1 follow the ones in the proof of the average Lang-Trotter Conjecture on Frobenius traces obtained by the third author and F. Pappalardi in [DaPa], with an improvement due to S. Baier [Bai] to shorten the average in terms of A and B (in [DaPa], one needed to take $A, B > x^{1+\varepsilon}$). More precisely, we first reduce the average of Koblitz's Conjecture given in Theorem 1 to an average involving only elliptic curves over the finite field $\mathbb{F}_p$; we then use Deuring's Theorem to rewrite this as an average of Kronecker class numbers. These steps are described in detail in Section 3.

As corollaries, we obtain the average result of Theorem 1, as well as:

Theorem 2 *Let*

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

Then, as $x \to \infty$,

$$\sum_{p \leq x} \pi^*(p) \sim \frac{\mathfrak{C}x^3}{3\log^2 x},$$

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

One remarks that Theorem 2 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

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

One of the key ingredients in the proof of Theorems 1-2 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 [Ba], 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 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 in our paper:

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

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

where

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

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

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 the statements of Theorems 1-2 to an average of Kronecker class numbers (Proposition 7). In Section 4, we show how an average of the twin prime conjecture implies Proposition 7. Finally, in Sections 5-6, we give the proofs of the afore-mentioned average of the twin prime conjecture and of Theorem 3.

2 Average of Koblitz's Conjecture and the conjectural constant

The constant $C(E)$ of 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 (see, for example, [So]).

We want to count the number of primes p such that $p + 1 - a_p(E)$ is also a prime. For each prime ℓ, this means that $p + 1 - a_p(E)$ is not divisible by ℓ. For a random integer n, the probability that $\ell \nmid n$ would be $(\ell - 1)/\ell$. To compute the probability that $\ell \nmid p + 1 - a_p(E)$ we consider the action of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the group $E[\ell]$ of ℓ-torsion points of E, which leads to the injection

$$\rho_\ell : \operatorname{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \hookrightarrow \operatorname{GL}_2(\mathbb{Z}/\ell\mathbb{Z});$$

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

$$\begin{aligned} \operatorname{tr}(\rho_\ell(\sigma_p)) &\equiv a_p(E) (\operatorname{mod} \ell), \\ \det(\rho_\ell(\sigma_p)) &\equiv p (\operatorname{mod} \ell), \end{aligned}$$

for all primes $p \neq \ell$ of good reduction for E. Then the probability that $\ell \nmid p + 1 - a_p(E)$ can be evaluated by counting matrices g in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that $\det(g) + 1 - \operatorname{tr}(g) \not\equiv 0 (\operatorname{mod} \ell)$.

Let $G(\ell)$ be the image of ρ_ℓ in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and let

$$\begin{aligned} \Omega(\ell) &:= \{g \in G(\ell) : \det(g) + 1 - \operatorname{tr}(g) \equiv 0 (\operatorname{mod} \ell)\}, \\ \Omega'(\ell) &:= \{g \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \det(g) + 1 - \operatorname{tr}(g) \equiv 0 (\operatorname{mod} \ell)\}. \end{aligned}$$

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

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

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

$$\frac{1 - \dfrac{|\Omega(\ell)|}{|G(\ell)|}}{1 - \dfrac{1}{\ell}} = \frac{1 - \dfrac{|\Omega'(\ell)|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|}}{1 - \dfrac{1}{\ell}} = 1 - \frac{\ell^2 - \ell - 1}{(\ell - 1)^3(\ell + 1)}.$$

The constant $C(E)$ of [Ko] is defined as the product over all primes ℓ of the local factors above. In [Zy], Zywina made the observation that the probabilities are not independent from one prime to another, because the fields $\mathbb{Q}(E[\ell])$ are never independent for all primes ℓ, as already observed by Serre in [Se]. Their dependence can be quantified: for each elliptic curve $E/\mathbb{Q}$, there is an integer M_E which has the property that the probabilities are independent for primes $\ell \nmid M_E$ (see [Zy] for a precise definition).

Now let $G(M_E) \subseteq \mathrm{GL}_2(\mathbb{Z}/M_E\mathbb{Z})$ be the Galois group of $\mathbb{Q}(E[M_E])/\mathbb{Q}$ and let

$$\Omega(M_E) := \{g \in G(M_E) : \det(g) + 1 - \operatorname{tr}(g) \equiv 0 (\operatorname{mod} M_E)\}.$$

For each elliptic curve E, the constant $C(E)$ of Koblitz's Conjecture is then expected to be

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

We remark that even if M_E is never 1, it is possible for some elliptic curves $E/\mathbb{Q}$ to have

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

as shown in [Jo] and [Zy] (it is shown in [Jo] that $C(E) = \mathfrak{C}$ when the square-free part of the discriminant of E is congruent to 2 or 3 modulo 4). However, the average constant $\mathfrak{C}$ of Theorem

1 should not be thought of as the constant of *any* given curve over $\mathbb{Q}$, but as the *average* of all the constants $C(E)$. Indeed, in [Jo], N. Jones shows that if one assumes a positive answer to a well-known question of Serre regarding the open image theorem for elliptic curves proven in [Se], then the average of the conjectural constants $C(E)$ of (2) is indeed the average constant of Theorem 1. Our result then gives evidence for both the asymptotic of Koblitz's Conjecture and the constant appearing in the conjecture.

3 Reduction to an average of Kronecker class numbers and proofs of Theorems 1-2

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 $\pi_E^{\rm twin}(x)$ over $E/\mathbb{Q}$ reduces to an average of Kronecker class numbers, which is Proposition 7 of the present section.

First we write

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\pi_E^{\rm twin}(x) \quad = \quad \frac{1}{|\mathcal{C}|}\sum_{\substack{p\le x,\ |r|\le 2\sqrt{p} \\ p+1-r \text{ prime}}} N_{A,B,r}(p), \tag{3}$$

where

$$N_{A,B,r}(p) := \#\left\{|a|\le A, |b|\le B : a_p(E(a,b)) = r\right\}.$$

As the value of $a_p(E(a,b))$ depends only on a and b modulo p, $N_{A,B,r}(p)$ can be evaluated by counting elliptic curves over the finite field $\mathbb{F}_p$ and having $p+1-r$ points for each given r. In turn, this can be done using the following results:

Theorem 4 *(Deuring's Theorem [De])*
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

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

where $\mathrm{Aut}(E)$ *is the automorphism group of E and for any $D < 0$, $H(D)$ is the Kronecker class number*

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

defined in terms of the class number $h(D/f^2)$ and number of units $w(D/f^2)$ of $\mathbb{Q}(\sqrt{D/f^2})$. Then, for any fixed $-2\sqrt{p}\le r\le 2\sqrt{p}$, there are exactly $(p-1)H(r^2-4p)$ elliptic curves defined over $\mathbb{F}_p$ with $p+1-r$ points.

Lemma 5 *Let D be a positive integer such that $-D \equiv 0, 1 (\mathrm{mod}\, 4)$. Then, as $D\to\infty$,*

$$H(-D) \ll D^{1/2}\log^2 D. \tag{4}$$

Proof. This follows from the class number formula and from standard bounds on special values of Dirichlet L-functions.□

By reducing modulo p and counting curves over $\mathbb{F}_p$, it follows that

$$N_{A,B,r}(p) \quad = \quad \left(\frac{2A}{p} + \mathrm{O}(1)\right)\left(\frac{2B}{p} + \mathrm{O}(1)\right)\left(pH(r^2-4p) + \mathrm{O}\left(\sqrt{p}\log^2 p\right)\right). \tag{5}$$

This is the approach of [DaPa] which gives an average of size $A, B > x^{1+\varepsilon}$ when one replaces (5) in (3). In order to get the shorter average of Theorem 1, one needs to count $N_{A,B,r}(p)$ in a more subtle way, using character sums. This was done by Baier, who proved the following lemma:

Lemma 6 *Let $N_{A,B,r}(p)$ be the number of curves $E(a,b) \in \mathcal{C}$ such that $a_p(E(a,b)) = r$. Then,*

$$\begin{aligned} N_{A,B,r}(p) \quad &= \quad \frac{4AB \cdot H(r^2-4p)}{p} + \mathrm{O}\left(\frac{AB}{p} + \frac{AB \cdot H(r^2-4p)}{p^2} + A + B\right. \\ &\qquad \left. + (AB \cdot H(r^2-4p))^{1/2}\log^3 p + \frac{(A+B)H(r^2-4p)}{p^{1/2}}\log p\right). \end{aligned}$$

Proof. See [Bai]. □

Replacing Lemma 6 in (3) and using Lemma 5 to bound the Kronecker class numbers, we obtain that

$$\begin{aligned} \frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}} \pi_E^{\mathrm{twin}}(x) \quad &= \sum_{\substack{p\le x,\ |r|\le 2\sqrt{p} \\ p+1-r \text{ prime}}} \frac{H(r^2-4p)}{p} + \mathrm{O}\left(x^{1/2} + \frac{x^{3/2}\log^3 x}{A} + \frac{x^{3/2}\log^3 x}{A} + \frac{x^{7/4}\log^4 x}{(AB)^{1/2}}\right) \\ &= \sum_{\substack{p\le x,\ |r|\le 2\sqrt{p} \\ p+1-r \text{ prime}}} \frac{H(r^2-4p)}{p} + \mathrm{O}(x^{1-\varepsilon}), \end{aligned} \tag{6}$$

provided we take A, B such that $A, B > x^{1/2+2\varepsilon}$ and $AB > x^{3/2+2\varepsilon}$.

In a similar way, using Deuring's Theorem and the bound of Lemma 5, we can write

$$\sum_{p\le x} \pi^*(p) \quad = \sum_{\substack{p\le x,\ |r|\le 2\sqrt{p} \\ p+1-r \text{ prime}}} pH(r^2-4p) + \mathrm{O}\left(x^2\log^2 x\right). \tag{7}$$

Thus, once again, we need to evaluate an average of class numbers. Then, Theorems 1 and 2 will follow from:

Proposition 7 *Let x, X, Y be positive real numbers such that $X + Y \le x$, $Y \ge \sqrt{X}$. Then, for any $M > 0$,*

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

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

Now let us indicate in detail how Proposition 7 implies Theorems 1 and 2.

Proof of Theorems 1-2. Comparing (6) and (7), we see that the two asymptotics to prove are equivalent by partial summation; we will only prove the second one.

Let M be any positive integer (e.g. $M = 10$ suffices) and $K := [\log^{M/2} x]$. Let

$$Y := \frac{x}{K} \text{ and } X := kY \text{ for } 0 \le k \le K-1.$$

We partition the interval $p \leq x$ into K intervals of length Y and rewrite the main term of (7) as

$$\begin{aligned}
\sum_{\substack{p\leq x \\ |r|\leq 2\sqrt{p} \\ p+1-r \text{ prime}}} pH(r^2-4p) &= \sum_{0\leq k\leq K-1} \sum_{\substack{X<p\leq X+Y \\ |r|\leq 2\sqrt{p} \\ p+1-r \text{ prime}}} pH(r^2-4p) \\
&= \sum_{0\leq k\leq K-1} \sum_{\substack{X<p\leq X+Y \\ |r|\leq 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2-4p) + \mathrm{O}\left(\sum_{0\leq k\leq K-1} XY^2 \log^2 x \right), \quad (8)
\end{aligned}$$

where the O-term comes from the bound (4) on the Kronecker class number $H(r^2-4p)$ for r in the interval $2\sqrt{X} < r \leq 2\sqrt{p}$ and is bounded by $K^2Y^3\log^2 x \leq x \log^{2-M/2} x$. For the main term we use Propostion 7 with the same M, and obtain:

$$\begin{aligned}
\sum_{0\leq k\leq K-1} \sum_{\substack{X<p\leq X+Y \\ p+1-r \text{ prime} \\ |r|\leq 2\sqrt{X}}} pH(r^2-4p) &= \mathfrak{C}Y^3 \sum_{1\leq k\leq K-1} \frac{k^2}{\log^2(kY)} + \mathrm{O}\left(\sum_{1\leq k\leq K-1} XY^2 \log X \right) \\
&\quad + \mathrm{O}\left(\sum_{1\leq k\leq K-1} \frac{x^3}{\log^M x} \right) + \mathrm{O}\left(Y^{5/2} \log^2 Y \right) \\
&= \mathfrak{C}Y^3 \int_1^{K-1} \frac{t^2}{\log^2(tY)}\, dt + \mathrm{O}\left(\frac{x^3}{\log^{M/2-1} x} \right) \\
&= \mathfrak{C} \int_Y^x \frac{u^2}{\log^2(u)}\, du + \mathrm{O}\left(\frac{x^3}{\log^{M/2-1} x} \right) \\
&= \frac{\mathfrak{C}x^3}{3\log^2 x} + \mathrm{O}\left(\frac{x^3}{\log^3 x} \right). \quad (9)
\end{aligned}$$

Replacing(8) and (9) in (7), the proof of Theorem 2 is completed. The proof of Theorem 1 follows by partial summation. □

4 Reduction to an average twin prime conjecture and proof of Proposition 7

In this section we show how Proposition 7 reduces to an average of the twin prime conjecture which, in turn, will be proved completely in Sections 5-6. To be precise, our proof of Proposition 7 relies on the validity of the following result:

Proposition 8 *Let $x > 0$ and let $M > 0$. Let X, Y, R, U, V be parameters depending on x and satisfying*

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

There exists an integer $N(M) > 0$ such that, if $N > N(M)$, then, as $x \to \infty$,

$$\begin{aligned}
&\sum_{\substack{|r|\leq R \\ f\leq V \\ n\leq U}} \frac{1}{nf} \sum_{a (\mathrm{mod}\, 4n)} \left(\frac{a}{n}\right) \sum_{\substack{X<p\leq X+Y \\ p+1-r \text{ prime} \\ p\equiv(r^2-af^2)/4\, (\mathrm{mod}\, nf^2)}} \log p \cdot \log(p+1-r) \\
&= 2\mathfrak{C}RY + \mathrm{O}\left(\frac{Rx}{\log^M x} + x^{4/3+\varepsilon} \right), \quad (10)
\end{aligned}$$

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

We assume this result as true and proceed to proving Proposition 7.

Proof of Proposition 7. Let x, X, Y be as in the statement of Proposition 7. Using the class number formula, we write

$$\sum_{X<p\le X+Y} \sum_{\substack{|r|\le 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2-4p) = \frac{1}{2\pi} \sum_{\substack{|r|\le 2\sqrt{X} \\ f\le 2\sqrt{x}}} \frac{1}{f} \sum_{X<p\le X+Y}{}^{*} p\sqrt{4p-r^2} L(1,\chi_d), \tag{11}$$

where $d = d(r,p,f) := (r^2-4p)/f^2$ and the $*$ on the summation over p indicates that we are summing over primes $X < p \le X+Y$ such that

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

Here, χ_d denotes the Dirichlet character modulo d defined by the Kronecker symbol 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

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

where $U = U(x)$ is a parameter to be chosen soon. By plugging this into (11), we obtain that

$$\begin{aligned} &\sum_{X<p\le X+Y} \sum_{\substack{|r|\le 2\sqrt{X} \\ p+1-r \text{ prime}}} pH(r^2-4p) \\ &= \frac{1}{2\pi} \sum_{\substack{|r|\le 2\sqrt{X} \\ f\le 2\sqrt{x} \\ n\le U}} \frac{1}{nf} \sum_{X<p\le X+Y}{}^{*} p\sqrt{4p-r^2}\chi_d(n) + \mathrm{O}\left(\frac{x^{7/2}}{U} \right). \end{aligned} \tag{12}$$

Thus, by taking

$$x^{1/2} \log^{M+1} x \le U \le x, \tag{13}$$

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

Now let us also truncate the sum over f. We write

$$\begin{aligned} &\frac{1}{2\pi} \sum_{\substack{|r|\le 2\sqrt{X} \\ f\le 2\sqrt{x} \\ n\le U}} \frac{1}{nf} \sum_{X<p\le X+Y}{}^{*} p\sqrt{4p-r^2}\chi_d(n) \\ &= \frac{1}{2\pi} \sum_{\substack{|r|\le 2\sqrt{X} \\ f\le V \\ n\le U}} \frac{1}{nf} \sum_{X<p\le X+Y}{}^{*} p\sqrt{4p-r^2}\chi_d(n) + \mathrm{O}\left(\sum_{\substack{|r|\le 2\sqrt{X} \\ V<f\le 2\sqrt{x} \\ n\le U}} \frac{1}{nf} \sum_{\substack{X<p\le X+Y \\ p\equiv \frac{r^2}{4} (\operatorname{mod} f^2)}} p^{3/2} \right) \\ &= \frac{1}{2\pi} \sum_{\substack{|r|\le 2\sqrt{X} \\ f\le V \\ n\le U}} \frac{1}{nf} \sum_{X<p\le X+Y}{}^{*} p\sqrt{4p-r^2}\chi_d(n) + \mathrm{O}\left(\frac{x^3 \log U}{V^2} \right). \end{aligned} \tag{14}$$

On the second line 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 $4p \equiv r^2 (\operatorname{mod} f^2)$ becomes $p \equiv \bar{4}r^2 (\operatorname{mod} f^2)$, where $\bar{4}$ is the inverse of 4 modulo f^2. The other estimates used for the O-term are elementary.

We choose V such that

$$V \geq (\log x)^{(M+1)/2} \tag{15}$$

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

Now we use quadratic reciprocity and consider $\chi_d(n)$ as a character modulo $4n$. Hence we rewrite the main term of (14) as

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

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

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

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

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

We now change the weight of the primes p from $p\sqrt{4p-r^2}$ to

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

Then the main term of (14) becomes

$$\frac{X}{2\pi \log^2 X} \sum_{\substack{|r|\leq 2\sqrt{X} \\ f\leq V \\ n\leq U}} \frac{1}{nf}\sqrt{4X-r^2} \sum_{a (\operatorname{mod} 4n)} \left(\frac{a}{n}\right) \sum_{X<p\leq X+Y}{}^{**} \log p \cdot \log{(p+1-r)} \tag{16}$$
$$+ \mathrm{O}\left(XY^2 \log X\right)$$

and so we reduced our question to an average of the standard twin prime conjecture, twisted by some Kronecker symbols. This average is evaluated using Proposition 8 stated in the beginning of this section; the details follow.

Let us write the left hand side of Proposition 8 as $\sum_{|r|\leq R} F(r)$. With this notation, the main term of (16) becomes

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

which we can compute from Proposition 8 by partial summation. We obtain:

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

Evaluating the integral

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

and replacing in the above, we obtain

$$\frac{X}{2\pi\log^2 X}\sum_{|r|\le 2\sqrt{X}} F(r)\sqrt{4X-r^2} \;=\; \frac{\mathfrak{C}X^2Y}{\log^2 X} + \mathrm{O}\left(\frac{(Xx)^{3/2}}{(\log^2 X)(\log^M x)}\right).$$

Using this together with (16), the proof of Proposition 7 is now completed (provided that Proposition 8 holds). □

5 Average of the twin prime conjecture and proof of Theorem 3

In this section we shall prove Theorem 3. 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 3. 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: rather than a Goldbach type problem, we have a twin prime problem; more importantly, we need a Siegel-Walfisz type analogue, namely:

Proposition 9 *Let $\varepsilon, M, N > 0$ be fixed. Then there exists $x(\varepsilon, M, N) > 0$ such that, for any $x > x(\varepsilon, M, N)$, $x^{1/3+\varepsilon} \le R \le x$, $q \le \log^N x$, $(a,q)=1$ and $0 < X < X+Y \le x$, we have*

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

The proof of Proposition 9 is similar to the proof of [PePi, Theorem 1]. For this reason, we will only indicate the major steps that should enable the interested reader to modify [PePi] accordingly. After we complete the proof of Proposition 9, we proceed to proving Theorem 3.

Proof of Proposition 9. We use the following notation (which is, unfortunately, not exactly the same as in [PePi]):

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

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

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

By the circle method, we have

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

and so

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

$$+\sum_{0<r\leq R}\left|\int_{\mathfrak{M}} S_1(\alpha)S_2(-\alpha)e(-r\alpha)\,d\alpha - \mathfrak{S}(r,q,a)Y\right|^2. \tag{17}$$

The estimate for the contribution of the minor arcs – the first term in formula (17) – 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

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

where $\|\|$ denotes the distance to the nearest integer. Now let us observe that our $S_2(\alpha)$ is exactly 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 (17) – 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

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

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

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

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

$$\sum_{s\le \log^C x} \frac{\mu(s)}{\phi(s)\phi([s,q])} \sum_{\substack{1\le b\le s\\(b,s)=1}} e\left(\frac{-rb}{s}\right) \sum_{\substack{1\le c\le s\\(c,s)=1\\(q,s)|c-a}} e\left(\frac{bc}{s}\right). \tag{18}$$

We proceed as follows.

The standard argument via the Chinese Remainder Theorem shows that the function

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

is multiplicative in s. Indeed, for $s = uv$, $(u,v) = 1$, $u\overline{u} \equiv 1(\operatorname{mod} v)$ and $v\overline{v} \equiv 1(\operatorname{mod} u)$, note that the relation $c = gu\overline{u} + hv\overline{v}$ 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

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

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

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

Now one can easily check that, after extending the sum over s in (18) up to infinity, we have

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

Proposition 9 then follows. □

Proof of Theorem 3. Let us observe that the expected density of twin primes of distance r is $\mathfrak{S}(r)$. If $a(\operatorname{mod} q)$ is an admissible residue class, then the expected density of twin primes of distance r in the residue class $a(\operatorname{mod} q)$ should satisfy

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

whenever $(a, q) = (a - r, q) = 1$, where

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

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 $b = cu\overline{u} + dv\overline{v}$ 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, $u\overline{u} \equiv 1 (\operatorname{mod} v)$ and $v\overline{v} \equiv 1 (\operatorname{mod} u)$. 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

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

Then our claim follows from the equations

$$\rho(r, q) = \prod_{p^\alpha \| q, p | r} (p^\alpha - p^{\alpha-1}) \cdot \prod_{p^\alpha \| q, p \nmid r} (p^\alpha - 2p^{\alpha-1}) = \phi(q) \prod_{p | q, p \nmid r} \frac{p-2}{p-1}, \tag{19}$$

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

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

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

if χ_0 denotes the principal character modulo q, let

$$\rho(r, \chi_0) := \rho(r, q).$$

By the orthogonality of characters, we obtain that

$$\mathfrak{S}(r, q, a) = \frac{\mathfrak{S}(r)}{\rho(r, q)} = \frac{\mathfrak{S}(r)}{\phi(q)} \sum_{\chi} \overline{\chi}(a) \frac{\rho(r, \chi)}{\rho(r, q)}, \tag{20}$$

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

Let $\varepsilon, M > 0$, $N > N(M)$, $x > x(\varepsilon, M)$, $x^{1/3+\varepsilon} \le R \le x$, $Q \le x \log^{-N} x$ and $0 \le X < X + Y \le x$ be fixed, as in the statement of Theorem 3. We define, for any (even) integer r and character χ,

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

Then, from the orthogonality of characters we obtain that

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

Usually, the main term comes from the principal 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 3 can be transformed (using (20) and orthogonality) into:

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

By the orthogonality of characters,

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

and then the last term in S simplifies to

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

More importantly,

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

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 9.

Also, from $\mathfrak{S}(rq)\ll\mathfrak{S}(r)\mathfrak{S}(q)$ and from the fact that $\mathfrak{S}(r)$ is 1 on average, that is,

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

and

$$\sum_{r\le R}\mathfrak{S}(r)^2=\mathrm{O}(R),$$

we deduce that

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

Putting everything together, we obtain that

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

Note that nothing deep has happened so far beside the one application of Proposition 9; 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

$$C(f,Q):=\sum_{\substack{q\le Q\\ f|q}}\frac{1}{\phi(q)},\tag{21}$$

which satisfies

$$C(f,Q)\ll\frac{1}{\phi(f)}\log Q.\tag{22}$$

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

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

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

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

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

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

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

where $Q_0:=\log^{-M-3}x$ and $N\ge M+3$. This implies that

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

Using the notation

$$\begin{aligned}
\psi(X,Y;r,f,b) \quad &:= \quad \sum_{\substack{X<p\le X+Y \\ p\equiv b (\mathrm{mod}\, f) \\ p-p'=r}} \log p \cdot \log p', && (23)\\
E(X,Y;r,f,b) \quad &:= \quad \psi(X,Y;r,f,b) - \mathfrak{S}(r,f,b)Y, && (24)
\end{aligned}$$

we see that

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

For any small f and b, the sum of $|E(X,Y;r,f,b)|$ over r is sufficiently small by Proposition 9; 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 $d|f$, $d\ne f$, we have $\sum_{1\le c\le f/d} \chi(r+cd) = 0$ (see [Da, Chapter 9]). Using this, we quickly infer that

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

Putting everything together, we arrive at the equation

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

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 (19) and (22), so we can drop the condition $f\le Q_0$ for a price already paid by the error term. Writing back the definition of $C(f,Q)$, we obtain, after a little rearrangement, that

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

Finally, let us notice that by (19) we actually have 0 inside the big parantheses, 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 3. □

6 Proof of Proposition 8

This section consists of a proof of Proposition 8. This is done in two parts: an estimate of the error term in Proposition 8, which relies on Theorem 3, and an estimate of the main term, which consists mainly in the computation of the constant $\mathfrak{C}$. Note that in the course of proving Proposition 8 we can always assume $R \geq x^{1/3+\epsilon}$ and $Y \geq \sqrt{X}$, as otherwise the error term is an obvious upper bound for all the other terms in (10). 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, or by bounding the character by 1) shows that this term is much smaller than the error term in Proposition 8; therefore it can comfortably be excluded from any further investigation.

Note that, using notation (24), Theorem 3 can be formulated as

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

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

Using the same notation, as well as (23), we rewrite the left hand side of (10) as

$$\sum_{\substack{|r|\leq R,\, r\neq 1\\ f\leq V\\ n\leq U}} \frac{1}{nf} \sum_{a(\mathrm{mod}\, 4n)} \left(\frac{a}{n}\right) \psi(X,Y;r-1,nf^2,(r^2-af^2)/4) \tag{25}$$

$$= Y \sum_{\substack{|r|\leq R,\, r\neq 1\\ f\leq V\\ n\leq U}} \frac{1}{nf} \sum_{a(\mathrm{mod}\, 4n)} \left(\frac{a}{n}\right) \mathfrak{S}(r-1,nf^2,(r^2-af^2)/4) \tag{26}$$

$$+ \sum_{\substack{|r|\leq R,\, r\neq 1\\ f\leq V\\ n\leq U}} \frac{1}{nf} \sum_{a(\mathrm{mod}\, 4n)} \left(\frac{a}{n}\right) E(X,Y;r-1,nf^2,(r^2-af^2)/4). \tag{27}$$

6.1 Estimate of the error term in Proposition 8

In what follows, we will show how Theorem 3 allows us to control the error term (27). First, using the Cauchy-Schwarz inequality, we obtain

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

$$\leq \sum_{f\leq V}\frac{1}{f}\left(\sum_{\substack{|r|\leq R\\ n\leq U\\ a(\mathrm{mod}\, 4n)}} \frac{1}{n^2}\right)^{1/2} \left(\sum_{\substack{|r|\leq R,\, r\neq 1\\ n\leq U\\ a(\mathrm{mod}\, 4n)}} E^2(X,Y;r-1,nf^2,(r^2-af^2)/4)\right)^{1/2}. \tag{28}$$

The first inner sum above is estimated trivially as

$$\left(\sum_{\substack{|r|\leq R\\ n\leq U\\ a(\mathrm{mod}\, 4n)}} \frac{1}{n^2}\right)^{1/2} \ll R^{1/2}\log^{1/2} U. \tag{29}$$

For the second inner sum we observe that

$$\sum_{\substack{|r|\le R,\, r\neq 1\\ n\le U\\ a(\mathrm{mod}\, 4n)}} E^2(X,Y;r-1,nf^2,(r^2-af^2)/4) \le \sum_{\substack{|r|\le R\\ r\neq 1}} \sum_{q\le 4Uf^2} \sum_{b(\mathrm{mod}\, q)} E^2(X,Y;r-1,q,b),$$

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

$$\left\{ b = \frac{r^2-af^2}{4} \;:\; a(\mathrm{mod}\, 4n) \right\}$$

cover each residue class modulo $4n$ at most once. Then, using Theorem 3, we obtain

$$\sum_{\substack{|r|\le R,\, r\neq 1\\ n\le U\\ a(\mathrm{mod}\, 4n)}} E^2(X,Y;r-1,nf^2,(r^2-af^2)/4) \;\ll\; \frac{Rx^2}{\log^M x} \tag{30}$$

for any $M>0$, provided that

$$4UV^2 \le x\log^{-N} x. \tag{31}$$

Using the estimates (29) and (30) in (28), we finally obtain that

$$\begin{aligned}\sum_{\substack{|r|\le R,\, r\neq 1\\ f\le V\\ n\le U}} \frac{1}{nf} \sum_{a(\mathrm{mod}\, 4n)} \left(\frac{a}{n}\right) E(X,Y;r-1,nf^2,(r^2-af^2)/4) &\ll \frac{Rx\log^{1/2} U}{\log^{M/2} x} \sum_{f\le V} \frac{1}{f}\\ &\ll \frac{Rx}{\log^{(M-3)/2} x} \end{aligned} \tag{32}$$

for any $M>0$. This estimates the error term (27), and thus the error term of Proposition 8 (after renaming M).

6.2 Computation of the constant in Proposition 8

We now treat the main term (26) in (25), which is essentially a computation of the constant $\mathfrak{C}$ in Theorem 1. We first analyse the sum over n and f of (26) 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 10 *Let $r\neq 1$ be an odd integer. Then,*

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

where C_r is the positive constant

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

Proof of Proposition 10. Using the definition of $\mathfrak{S}(\cdot,\cdot,\cdot)$, we rewrite the left hand side of the desired equation in Proposition 10 as

$$2\left(\prod_{\ell\neq 2}\frac{\ell(\ell-2)}{(\ell-1)^2}\right)\sum_{\substack{f\leq V\\ f\text{ odd}}}\sum_{n\leq U}\frac{1}{nf\phi(nf^2)}\left(\prod_{\substack{\ell\mid nf^2(r-1)\\ \ell\neq 2}}\frac{\ell-1}{\ell-2}\right)\ c_f^r(n), \tag{33}$$

where

$$c_f^r(n):=\sum_{a(\operatorname{mod}4n)}{}'\left(\frac{a}{n}\right)$$

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

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

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,

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

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,

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

Then

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

where $a(4n)^*$ denotes invertible residue classes a modulo $4n$.

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

Lemma 11 *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*

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

where $a(\operatorname{mod}n)^*$ 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*
$$\frac{c_f^r(\ell^\alpha)}{\ell^{\alpha-1}} = \begin{cases} 0 & \textit{if } \alpha \textit{ is odd,} \\ \ell - 1 & \textit{if } \alpha \textit{ is even;} \end{cases}$$

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

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
$$\begin{aligned} c_f^r(n_1) c_f^r(n_2) \;\; &= \sum_{\substack{a_1 (\bmod n_1)^* \\ (r^2-a_1f^2,n_1)=1 \\ ((r-2)^2-a_1f^2,n_1)=1}} \left(\frac{a_1}{n_1}\right) \times \sum_{\substack{a_2 (\bmod 4n_2)^* \\ (r^2-a_2f^2,4n_2)=4 \\ ((r-2)^2-a_2f^2,4n_2)=4}} \left(\frac{a_2}{n_2}\right) \\ &= \sum_{\substack{a (\bmod 4n_1n_2)^* \\ (r^2-af^2,4n_1n_2)=4 \\ ((r-2)^2-af^2,4n_1n_2)=4}} \left(\frac{a}{n_1}\right) \left(\frac{a}{n_2}\right) = c_f^r(n_1 n_2). \end{aligned}$$

3. We have that
$$c_f^r(\ell^\alpha) = \ell^{\alpha-1} \sum_{\substack{a (\bmod \ell)^* \\ (r^2-af^2,\ell)=1 \\ ((r-2)^2-af^2,\ell)=1}} \left(\frac{a}{\ell}\right)^\alpha = \ell^{\alpha-1} \left(\sum_{a (\bmod \ell)^*} \left(\frac{a}{\ell}\right)^\alpha - \sum_{\substack{a (\bmod \ell)^* \\ a \equiv \bar{f}^{-2} r^2 (\bmod \ell) \text{ or} \\ a \equiv \bar{f}^{-2} (r-2)^2 (\bmod \ell)}} \left(\frac{a}{\ell}\right)^\alpha \right), \quad (34)$$
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 (34) has value $+1$. The result follows immediately when α is even, and follows from the orthogonality relations when α is odd. If $r \not\equiv 0, 1, 2 (\bmod 4)$, 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 (34) has value $+2$. The result follows as above.

4. We have that
$$c_f^r(\ell^\alpha) = \ell^{\alpha-1} \sum_{\substack{a (\bmod \ell)^* \\ (r^2-af^2,\ell)=1 \\ ((r-2)^2-af^2,\ell)=1}} \left(\frac{a}{\ell}\right)^\alpha = \ell^{\alpha-1} \sum_{a (\bmod \ell)^*} \left(\frac{a}{\ell}\right)^\alpha$$

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

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

□

Using parts 3. and 4. of Lemma 11, we can write

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

as in [DaPa]. 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

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

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 11, we can then write the n-sum as

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

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

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

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

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

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

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

Then,

$$D_r \;=\; \left(\prod_\ell \sum_{\alpha=0}^\infty b_r(\ell^\alpha)\right) \left(\prod_{\substack{\ell \mid (r-1) \\ \ell \neq 2}} \frac{\ell-1}{\ell-2}\right) \left(\prod_{\ell \nmid 2r(r-2)} \sum_{\alpha=0}^\infty c_r(\ell^\alpha)\right). \tag{35}$$

We now compute the sums appearing in (35), using the formulas for $a_r(\ell)$ and $b_r(\ell)$ listed above:

Lemma 12 *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. $A(\ell) := \sum_{\alpha=0}^{\infty} a_r(\ell^\alpha) = \dfrac{\ell^2+\ell+1}{\ell(\ell+1)}$;
2. *if* $\ell \nmid r(r-1)(r-2)$, *then* $B^{(1)}(\ell) := \sum_{\alpha=0}^{\infty} b_r(\ell^\alpha) = \dfrac{\ell^3-2\ell^2-2\ell-1}{(\ell-2)(\ell^2-1)}$;
3. *if* $\ell \mid r-1$, *then* $B^{(2)}(\ell) := \sum_{\alpha=0}^{\infty} b_r(\ell^\alpha) = \dfrac{\ell^3-\ell^2-\ell-1}{(\ell-1)^2(\ell+1)}$;
4. *if* $\ell \nmid r-1$, *but* $\ell \mid r(r-2)$, *then* $B^{(3)}(\ell) := \sum_{\alpha=0}^{\infty} b_r(\ell^\alpha) = \dfrac{\ell(\ell^2-2\ell-1)}{(\ell-2)(\ell^2-1)}$;
5. *if* $\ell \nmid 2r(r-2)(r-1)$, *then* $C^{(1)}(\ell) := \sum_{\alpha=0}^{\infty} c_r(\ell^\alpha) = \dfrac{\ell^3-2\ell^2-2\ell}{\ell^3-2\ell^2-2\ell-1}$;
6. *if* $\ell \mid r-1$, *then* $C^{(2)}(\ell) := \sum_{\alpha=0}^{\infty} c_r(\ell^\alpha) = \dfrac{\ell(\ell^2-\ell-1}{\ell^3-\ell^2-\ell-1}$;
7. *if* $\ell = 2$, *then* $B(2) := \sum_{\alpha=0}^{\infty} b_r(\ell^\alpha) = \dfrac{2}{3}$.

Proof. All the computations are straightforward, following in one line from the formula for the sum of the geometric series. □

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 12 to any odd prime ℓ (independently of the relation between ℓ and r). Then we rewrite D_r as

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

Using Lemma 12, 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 (33), 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 10. □

6.3 The average constant

Using Proposition 10, the main term (26) of (25) 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 [Ga] for the average of the standard twin prime constant. As such, we will follow the notation used in [Ga].

The main result of this section is:

Lemma 13 *As $R\to\infty$,*

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

Proof. Let us write

$$C_r = \frac{4}{3}\prod_{\ell\neq 2}\frac{\ell^2(\ell^2-2\ell-2)}{(\ell-1)^3(\ell+1)}\cdot\prod_{\substack{\ell\neq 2\\ \ell\mid r(r-1)(r-2)}}\left(1+e_r(\ell)\right), \tag{36}$$

where

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

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

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

We want to evaluate

$$\mathcal{S} := \sum_{\substack{|r|\leq R\\ r\neq 1 \text{ odd}}}\ \prod_{\substack{\ell\neq 2\\ \ell\mid r(r-1)(r-2)}}\left(1+e_r(\ell)\right) = \sum_{\substack{|r|\leq R\\ r\neq 1 \text{ odd}}}\ \sum_{q\in\mathcal{F}(r)} e_r(q), \tag{37}$$

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

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

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

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

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 $|r| \le R$ with $r \neq 1$ odd such that

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

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,

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

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

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

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

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

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

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

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

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

We put the two estimates together and obtain

$$\mathcal{S} = R \prod_{\ell \neq 2} \left[\frac{\ell^3 - 2\ell^2 - \ell + 3}{\ell(\ell^2 - 2\ell - 2)}\right] + \mathrm{O}\left((\log R)^2\right).$$

By replacing (37) in (36), this gives

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

which completes the proof of Lemma 13. □

Replacing Proposition 10 and Lemma 13 in (26), this concludes the proof of Proposition 8.

References

[Ba] A. Balog, *The prime k-tuples conjecture on average*, in Analytic Number Theory (Allerton Park, IL, 1989), Progr. Math. **85**, Birkhäuser, 1990, 47–75.

[Bai] S. Baier, *The Lang-Trotter Conjecture in average*, J. of the Ramanujan Math. Soc, to appear.

[Br] V. Brun, *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}+\dots$ *ou les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie*, Bull. Sci. Math. (2) **43**, 1919, 100–104, 124–128.

[Che] J. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16**, 1973, 157–176.

[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.

[DaPa] C. David and F. Pappalardi, *Average Frobenius distributions of elliptic curves*, International Mathematics Research Notices **4**, 1999, 165–183.

[De] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Hamb. Abh., 1941, 197–272.

[Ga] P.X. Gallagher, *On the distribution of primes in short intervals*, Mathematika **23**, 1976 (no. 1), 4–9.

[IwUr] H. Iwaniec and J. Jimenez Urroz, *Almost prime orders of elliptic curves with CM modulo p*, preprint, 2006.

[Jo] N. Jones, *The square-free sieve and averages of elliptic curve constants*, preprint 2007.

[Ko] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific Journal of Mathematics **131**, 1988 (no. 1), 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.

[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, 2005, no. 4, 341–352; erratum in Acta Arithmetica **119**, 2005 (no. 4), 407–408.

[Zy] D. Zywina, *On Koblitz's constant*, preprint 2006.