SCIENCE CHINA
Mathematics

• ARTICLES •

October 2025 Vol. 68 No. 10: 2285–2312
https://doi.org/10.1007/s11425-023-2372-1

The Lang-Trotter conjecture for the elliptic curve $y^2 = x^3 + Dx$

Hourong Qin

School of Mathematics, Nanjing University, Nanjing 210093*, China*

Email: hrqin@nju.edu.cn

Received September 27, 2023; accepted December 24, 2024; published online May 23, 2025

Abstract Let E be an elliptic curve over $\mathbb{Q}$. Let a_p denote the trace of the Frobenius endomorphism at a rational prime p. For a fixed integer r, define the prime-counting function as $\pi_{E,r}(x) := \sum_{p\leqslant x, p\nmid \Delta_E, a_p=r} 1$. The Lang-Trotter conjecture predicts that

$$\pi_{E,r}(x) = C_{E,r}\cdot\frac{\sqrt{x}}{\log x} + o\left(\frac{\sqrt{x}}{\log x}\right)$$

as $x\to\infty$, where $C_{E,r}$ is a specific non-negative constant. The Hardy-Littlewood conjecture gives a similar asymptotic formula as above for the number of primes of the form ax^2+bx+c. Assuming that the Hardy-Littlewood conjecture holds, we determine the constant $C_{E_D,r}$ for $E_D: y^2 = x^3 + Dx$. As a consequence, we establish a relationship between the Hardy-Littlewood conjecture and the Lang-Trotter conjecture for the elliptic curve $y^2 = x^3 + Dx$. We show that the Hardy-Littlewood conjecture implies the Lang-Trotter conjecture for $y^2 = x^3 + Dx$. Conversely, if the Lang-Trotter conjecture holds for some D and $2r$ (for $y^2 = x^3 + Dx, p\nmid D, a_p$ is always even) with the positive constant $C_{E_D,r}$, then the polynomial $x^2 + r^2$ represents infinitely many primes. For a prime p, if $a_p = 2r$, then p is necessarily of the form $x^2 + r^2$. Fixing r and D, and assuming that the Hardy-Littlewood conjecture holds, we obtain the density of the primes with $a_p = 2r$ inside the set of primes of the form $x^2 + r^2$. In some cases, the density is $1/4$, which aligns with natural expectations, but this does not hold for all D. In particular, we give a full list of D and r when there is no prime p for $a_p = 2r$.

Keywords the Mazur conjecture, the Lang-Trotter conjecture, the Hardy-Littlewood conjecture, primes represented by a quadratic polynomial

MSC(2020) 11G05, 11G15, 11N32

Citation: Qin H R. The Lang-Trotter conjecture for the elliptic curve $y^2 = x^3 + Dx$. Sci China Math, 2025, 68: 2285–2312, https://doi.org/10.1007/s11425-023-2372-1

1 Introduction

In this paper, we establish a relationship between the Hardy-Littlewood conjecture and the Lang-Trotter conjecture for the elliptic curve $y^2 = x^3 + Dx$. Let us recall these two conjectures first.

Let E be an elliptic curve defined over the rational number field $\mathbb{Q}$ with discriminant Δ_E. For any prime p, we denote the finite field of p elements by $\mathbb{F}_p$. As usual, we use $\tilde{E}_p$ for $E\otimes_{\mathbb{Z}_p}\mathbb{F}_p$ if E has good reduction at p. When E has good reduction at a prime p, we define a_p to be the trace of the Frobenius

automorphism ϕ_p on the first étale cohomology of E_p; it is known that $a_p = 1+p-\#\tilde{E}_p(\mathbb{F}_p)$ is an integer. Then ϕ_p satisfies the equation

$$x^2 - a_p x + p = 0. \tag{1.1}$$

The problem of determining the precise value of a_p is of special interest but is very difficult in general. We only know the necessary and sufficient condition for $a_p = 0$ in the complex multiplication (CM) case. Suppose that K is an imaginary quadratic field and E has CM by an order in K, i.e., $\mathrm{End}_{\bar{\mathbb{Q}}}(E)\otimes\mathbb{Q} \cong K$. Then by Deuring's theorem [5], for any prime number p of good reduction for E, we have

$$a_p = 0 \Leftrightarrow p \text{ is inert in } K.$$

Let E be an elliptic curve defined over K. In 1987, Elkies [6] proved that in the non-CM case, if $[K:\mathbb{Q}]$ is odd, then E has infinitely many supersingular primes.

By the Hasse inequality, $a_p \in (-2\sqrt{p}, 2\sqrt{p})$. Two celebrated theorems describe the distribution of $\frac{a_p}{2\sqrt{p}}$ in $(-1,1)$ as the rational prime p varies. In the CM case, it is Deuring's theorem [5]; in the non-CM case, it is the Sato-Tate conjecture (1960) and proved by Clozel et al. [3], Harris et al. [9] and Taylor [26].

For a fixed integer r, define the prime-counting function

$$\pi_{E,r}(x) := \sum_{p\leqslant x, p\nmid \Delta_E, a_p = r} 1.$$

Observe that $a_p \in (-2\sqrt{p}, 2\sqrt{p})$. If we conceptualize $\mathrm{Prob}(a_p = r)$ having an asymptotic value $\frac{1}{4\sqrt{p}}$, then

$$\pi_{E,r}(x) \approx \sum_{p\leqslant x} \frac{1}{4\sqrt{p}} \sim \frac{1}{2}\frac{\sqrt{x}}{\log x}.$$

By studying a probabilistic model consistent with the Chebotarev density theorem for the division fields of E and the Sato-Tate distribution, Lang and Trotter [16] generalized the Mazur conjecture, as explained below, and formulated the following conjecture.

The Lang-Trotter conjecture (1976). Let E be an elliptic curve over $\mathbb{Q}$ and r be a fixed integer. If $r = 0$, we have to assume additionally that E has no complex multiplication. Then

$$\pi_{E,r}(x) = C_{E,r}\cdot\frac{\sqrt{x}}{\log x} + o\left(\frac{\sqrt{x}}{\log x}\right)$$

as $x\to\infty$, where $C_{E,r}$ is a specific non-negative constant.

This conjecture has not been proved for any single elliptic curve. If the constant $C_{E,r} = 0$, we interpret the asymptotic to mean that there are only finitely many primes p for which $a_p = r$.

The phenomenon of $a_p = 1$ is of special interest and such primes are named anomalous primes by Mazur [17]. By [17], one can see that the anomalous primes are critical in the study of the Shafarevich-Tate group and Iwasawa theory of an abelian variety. Mazur [17] asked the following question:

Can an elliptic curve possess an infinite number of anomalous primes?

Furthermore, Mazur [17] proposed the following conjecture.

The Mazur conjecture (1972). Let D be a rational integer which is neither a square nor a cube in $\mathbb{Q}(\sqrt{-3})$. For the curve $E_D : y^2 = x^3 + D$, there are infinitely many anomalous primes for the elliptic curve E_D. More precisely, let $A.P._D(N)$ denote the number of primes less than N which are anomalous for the elliptic curve E_D. Then we have the asymptotic estimate

$$A.P._D(N) \sim c\frac{\sqrt{N}}{\log N} \quad \text{as } N\to\infty$$

for some positive constant c.

We have proved in [18] the following result.

Theorem 1.1. *The Hardy-Littlewood conjecture implies the Mazur conjecture, except for* $D = 80d^6$, *or* $D = -268912d^6$, *where* $d \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ *with* $d^6 \in \mathbb{Z}$ *is a nonzero integer. Moreover,*

$$A.P._D(N) \sim c\frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty$$

for some positive constant c.

Conversely, if the Mazur conjecture holds for some D, *then the polynomial* $12x^2 + 18x + 7$ *represents infinitely many primes.*

For related discussions and further results, we refer to [1, 4, 12, 14, 15, 19].

Before we state the Hardy-Littlewood conjecture, let us take a look at the polynomial x^2+1, a specific example in degree two. A natural question is the following:

Can $p = x^2 + 1$ represent infinitely many primes ($x \in \mathbb{N}$)?

This question is sometimes called the Euler conjecture in the literature. It is the first one of four basic questions about primes listed by Landau in his talk in ICM1912 in Cambridge. We have no answer to this question yet. However, progress can be found in [11].

When we consider the same question for general quadratic polynomials, we have the well-known Hardy-Littlewood conjecture.

The Hardy-Littlewood conjecture [8]. Let a, b and c be integers subject to the following conditions:

- a is positive;
- $(a, b, c) = 1$;
- $a + b$ and c are not both even;
- $D = b^2 - 4ac$ is not a square.

Let $P(n)$ denote the number of primes less than n which are of the form $ax^2 + bx + c$. Then we have the asymptotic estimate

$$P(n) \sim \delta(a, b, c)\frac{\sqrt{n}}{\log n} \quad \text{as } n \to \infty, \tag{1.2}$$

where

$$\delta(a, b, c) = \frac{\gcd(2, a + b)}{\sqrt{a}} \prod_{\substack{p|a,\, p|b \\ p>2}} \frac{p}{p-1} \prod_{\substack{p\nmid a \\ p>2}} \left(1 - \frac{(\frac{D}{p})}{p-1}\right) \tag{1.3}$$

is a constant. In particular, there are infinitely many primes of the form $ax^2 + bx + c$.

Let us compare this conjecture with a classical result due to Dirichlet.

Dirichlet's theorem. *Let* m *and* a *be relatively prime positive integers. Then there exist infinitely many primes* p *such that*

$$p \equiv a \pmod{m},$$

i.e., $mx + a$ *represents infinitely many primes.*

Let $\pi(n, m, a)$ denote the number of prime numbers $p \leqslant n$ such that $p = mx + a$. Then

$$\pi(n, m, a) \sim \frac{1}{\phi(m)}\frac{n}{\log n} \quad \text{as } n \to \infty.$$

Here, $\phi(\cdot)$ is Euler's totient function.

Therefore, Dirichlet's theorem provides the asymptotic formula for the number of primes represented by polynomials of degree one, and thus establishes the existence of infinitely many such primes. However, when we consider the situation for the polynomials of degree two, the problem becomes exceedingly difficult.

The purpose of this paper is to study the Lang-Trotter conjecture for the elliptic curve $y^2 = x^3 + Dx$. Roughly speaking, we show that in our situation, the validity of the Hardy-Littlewood conjecture and that of the Lang-Trotter conjecture are equivalent.

Let D be a nonzero integer and E_D be the elliptic curve of the affine equation $y^2 = x^3 + Dx$. Then E_D has CM by $\mathbb{Q}(\sqrt{-1})$. By Deuring's theorem, if a prime $p \equiv 3 \pmod 4$, then $a_p(E_D) = 0$. On the other hand, if $p \equiv 1 \pmod 4$, then p is the sum of two squares. It turns out that for $p = r^2 + x^2$, we have $a_p(E_D) = \pm 2r, \pm 2x$. Meanwhile, if $a_p(E_D) = 2r$, then p must be of the form $r^2 + x^2$. Fix r. If a prime p belongs to the quadratic progression $r^2 + x^2$, then there are four possibilities for $a_p(E_D)$. All primes p belonging to $r^2 + x^2$ for which $a_p(E_D) = 2r$ represents, asymptotically, a non-negative fraction of the total number of primes of the form $r^2 + x^2$. We refer to this fraction as density. A natural question is: is this density $1/4$? In some cases, the density is $1/4$, but it fails to be true for all D. It happens that for some D and r, there are no primes p such that $a_p(E_D) = 2r$. We give a full list of such D and r. Furthermore, the Hardy-Littlewood conjecture implies that for any D and even r, it is impossible that the density for $a_p(E_D) = 2r$ is equal to $1/4$. Assuming that the Hardy-Littlewood conjecture holds, we show that this density exists for each D. The explicit values for the density will be given as the main results of this paper. Applying the density results and the Hardy-Littlewood conjecture again, we show that the Lang-Trotter conjecture holds for $y^2 = x^3 + Dx$.

Theorem 1.2. *The Hardy-Littlewood conjecture implies the Lang-Trotter conjecture for $y^2 = x^3 + Dx$. Moreover, for any non-zero integer r,*

$$\pi_{E_D,2r}(x) \sim \delta \cdot \frac{\sqrt{x}}{\log x} \quad \text{as } x \to \infty$$

for some non-negative constant δ.

Conversely, if the Lang-Trotter conjecture holds for some D and r with the positive constant $C_{E_D,2r}$, then the polynomial $x^2 + r^2$ represents infinitely many primes.

The constant δ will be given explicitly in this paper. In particular, we give a full list when the constant $\delta = 0$. Recently, joined with Hu and Lei[1)], we show that the constant δ keeps consistent with the constant suggested by Jones [13]. In this paper, we will directly cite some knowledge about quartic reciprocity and elliptic curves without further explanation. Readers may refer to references such as [7, 10, 20–25].

2 Preliminaries

Let D be a nonzero integer and E_D be the elliptic curve: $y^2 = x^3 + Dx$. For any odd prime $p \nmid D$, $a_p = 1 + p - \#\tilde{E_D}(\mathbb{F}_p)$. The following well-known result is useful for us to compute the values of a_p.

Lemma 2.1 (Gauss)**.** *Let $p = \alpha^2 + \beta^2$ $(\alpha, \beta \in \mathbb{Z})$ with $\alpha \equiv 1 \pmod 4$ be an odd prime. Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2\alpha \pmod p.$$

Proof. See, for example, [2]. □

Lemma 2.2. *Let p be an odd prime. Then for $t \not\equiv 0 \pmod{p-1}$,*

$$\sum_{x=0}^{p-1} x^t \equiv 0 \pmod p$$

and

$$\sum_{x=0}^{p-1} x^{p-1} \equiv -1 \pmod p.$$

[1)] Hu L X, Lei K S, Qin H R. The Lang-Trotter conjecture for CM elliptic curves and the Hardy-Littlewood conjecture. Preprint

Proof. The result follows immediately from a direct computation. □

Lemma 2.3. *Let E be the elliptic curve: $y^2 = x^3 + Dx$, and $p \equiv 1 \pmod 4$ be an odd prime. Then*

$$a_p \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{4}} D^{\frac{p-1}{4}} \pmod p.$$

Assume further that $p = \alpha^2 + \beta^2$ $(\alpha, \beta \in \mathbb{Z})$ with $\alpha \equiv 1 \pmod 4$ is a prime. If $p \nmid D$, then $a_p = \pm 2\alpha, \pm 2\beta$. More precisely,

$$a_p = \begin{cases} 2\alpha, & \text{if } D^{\frac{p-1}{4}} \equiv 1 \pmod p, \\ -2\alpha, & \text{if } D^{\frac{p-1}{4}} \equiv -1 \pmod p, \\ 2\beta, & \text{if } D^{\frac{p-1}{4}} \equiv \dfrac{\beta}{\alpha} \pmod p, \\ -2\beta, & \text{if } D^{\frac{p-1}{4}} \equiv -\dfrac{\beta}{\alpha} \pmod p. \end{cases}$$

Proof. Let $p \nmid D$ be an odd prime. Then

$$\#\tilde{E_D}(\mathbb{F}_p) = 1 + \sum_{x=0}^{p-1} \left(1 + \left(\frac{x^3 + Dx}{p}\right)\right) = 1 + p + \sum_{x=0}^{p-1} \left(\frac{x^3 + Dx}{p}\right).$$

Note that

$$\left(\frac{x^3 + Dx}{p}\right) \equiv (x^3 + Dx)^{\frac{p-1}{2}} \pmod p.$$

Hence, if $p \equiv 1 \pmod 4$ is a prime, then by Lemma 2.2,

$$a_p(E_D) = -\sum_{x=0}^{p-1} \left(\frac{x^3 + Dx}{p}\right) \equiv -\sum_{x=0}^{p-1} (x^3 + Dx)^{\frac{p-1}{2}} \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{4}} D^{\frac{p-1}{4}} \pmod p,$$

and if $p \equiv 3 \pmod 4$ is an odd prime, then $a_p \equiv 0 \pmod p$, and hence $a_p = 0$ by the Hasse inequality.

Now assume that $p = \alpha^2 + \beta^2$, where $\alpha, \beta \in \mathbb{Z}$ with $\alpha \equiv 1 \pmod 4$ is a prime. By the Gauss lemma (see Lemma 2.1),

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2\alpha \pmod p.$$

On the other hand, $D^{\frac{p-1}{4}} \equiv \pm 1, \pm\frac{\beta}{\alpha} \pmod p$, so the result follows by applying the Hasse inequality again. □

Let D be a nonzero integer. Fix an integer r. If $p \nmid D$ with $a_p = 2r \neq 0$, then p must be of the form $r^2 + x^2$. In fact, since $p \nmid D$ and $a_p \neq 0$, p is the sum of two squares. By Lemma 2.3, we can write $p = r^2 + x^2$. On the other hand, if $p = r^2 + x^2$, then $a_p(E_D) = \pm 2r, \pm 2x$. There are four possibilities for $a_p(E_D)$. We are interested in the distribution of such four possibilities for $a_p(E_D)$. To study this distribution, we introduce the following definition.

Definition 2.4. Let $E_D : y^2 = x^3 + Dx$. Put

$$Q(r, N) = \{p \mid p \text{ prime}, p = r^2 + x^2 \leqslant N\}.$$

For any integer r, we put

$$a_p(E_D, 2r) = \lim_{N \to \infty} \frac{\#\{p \mid a_p(E_D) = 2r,\, p \in Q(r, N)\}}{\#Q(r, N)}.$$

We simply write $a_p(2r)$ for $a_p(E_D, 2r)$.

Therefore, $a_p(E_D, 2r)$ represents a natural density for all primes with $a_p = 2r$ inside primes of the form $r^2 + x^2$. We show that $a_p(E_D, 2r)$ exists in the next section.

We now recall some basic facts about the biquadratic residue. By definition, a nonunit $a + b\sqrt{-1} \in \mathbb{Z}[\sqrt{-1}]$ is primary if either $a \equiv 1, b \equiv 0 \pmod 4$ or $a \equiv 3, b \equiv 2 \pmod 4$. Let π be a prime primary element in $\mathbb{Z}[\sqrt{-1}]$ with $\pi \nmid 2$. For any $\lambda \in \mathbb{Z}[\sqrt{-1}]$, relatively prime to π, the biquadratic residue symbol (character) $(\frac{\lambda}{\pi})_4$, which takes values ± 1 and $\pm\sqrt{-1}$, is characterized by the congruence

$$\left(\frac{\lambda}{\pi}\right)_4 \equiv \lambda^{\frac{N\pi-1}{4}} \pmod{\pi}.$$

Theorem 2.5 (The law of biquadratic reciprocity)**.** *Let λ and π be relatively prime primary elements in $\mathbb{Z}[\sqrt{-1}]$ with $\pi \nmid 2$ and $\lambda \nmid 2$. Let $(\frac{\lambda}{\pi})_4$ denote the biquadratic residue character. Then*

$$\left(\frac{\lambda}{\pi}\right)_4 = \left(\frac{\pi}{\lambda}\right)_4 \cdot (-1)^{\frac{N\lambda-1}{4}\cdot\frac{N\pi-1}{4}}.$$

For a rational odd prime $p = \alpha^2 + \beta^2$ with α odd, by a choice of signs, we assume that $\beta > 0$. Suppose that $p = \rho\bar{\rho}$ is its prime factorization in $\mathbb{Z}[\sqrt{-1}]$. Assume that $\rho = \alpha + \beta\sqrt{-1}$ is primary. When D is a nonzero integer with $p \nmid D$, for convenience, we use $(\frac{D}{p})_4$ for $(\frac{D}{\rho})_4$. Under this setting, in $\mathbb{Z}/p\mathbb{Z}$, we have $\sqrt{-1} \equiv \alpha/\beta \pmod p$ and

$$\left(\frac{D}{p}\right)_4 \equiv D^{\frac{p-1}{4}} \pmod{p}.$$

The following lemma gives the precise value $(\frac{D}{p})_4$ for $D = 2$.

Lemma 2.6. *We have the following formula for $2^{\frac{p-1}{4}} \pmod p$:*

$$2^{\frac{p-1}{4}} \equiv \begin{cases} 1 \pmod p, & \text{if } \beta \equiv 0 \pmod 8, \\ -1 \pmod p, & \text{if } \beta \equiv 4 \pmod 8, \\ \dfrac{\beta}{\alpha} \pmod p, & \text{if } \beta \equiv 2\alpha \pmod 8, \\ -\dfrac{\beta}{\alpha} \pmod p, & \text{if } \beta \equiv 6\alpha \pmod 8. \end{cases}$$

Proof. Let $p = \alpha^2 + \beta^2$ with α odd be a prime. Clearly $(\frac{\alpha}{p}) = 1$. Since $(\alpha+\beta)^2 + (\alpha-\beta)^2 = 2p$, we have

$$\left(\frac{\alpha+\beta}{p}\right) = (-1)^{\frac{1}{8}((\alpha+\beta)^2-1)}$$

and

$$\frac{(\alpha+\beta)^2}{\alpha^2} \equiv 2 \cdot \frac{\beta}{\alpha} \pmod{p}.$$

Hence,

$$2^{\frac{p-1}{4}} \cdot \frac{\beta^{\frac{p-1}{4}}}{\alpha^{\frac{p-1}{4}}} \equiv \frac{(\alpha+\beta)^{\frac{p-1}{2}}}{\alpha^{\frac{p-1}{2}}} \pmod{p}.$$

It follows that

$$\begin{aligned} 2^{\frac{p-1}{4}} &\equiv (\alpha+\beta)^{\frac{p-1}{2}} \cdot \frac{\beta^{-\frac{p-1}{4}}}{\alpha^{-\frac{p-1}{4}}} \pmod{p} \\ &\equiv \frac{\beta^{\frac{1}{4}((\alpha+\beta)^2-1)}}{\alpha^{\frac{1}{4}((\alpha+\beta)^2-1)}} \cdot \frac{\beta^{-\frac{p-1}{4}}}{\alpha^{-\frac{p-1}{4}}} \pmod{p} \\ &\equiv \frac{\beta^{\frac{1}{4}(2\alpha\beta)}}{\alpha^{\frac{1}{4}(2\alpha\beta)}} \pmod{p} \\ &\equiv \frac{\beta^{\frac{\alpha\beta}{2}}}{\alpha^{\frac{\alpha\beta}{2}}} \pmod{p}. \end{aligned}$$

Note that $\beta \equiv 2\alpha \pmod 8$ if and only if $\alpha\beta \equiv 2 \pmod 8$, and $\beta \equiv 6\alpha \pmod 8$ if and only if $\alpha\beta \equiv 6 \pmod 8$. Hence, $2^{\frac{p-1}{4}} \equiv 1 \pmod p$ if and only if $\beta \equiv 0 \pmod 8$; $2^{\frac{p-1}{4}} \equiv -1 \pmod p$ if and only if $\beta \equiv 4 \pmod 8$; $2^{\frac{p-1}{4}} \equiv \frac{\beta}{\alpha} \pmod p$ if and only if $\beta \equiv 2 \pmod 8$; $2^{\frac{p-1}{4}} \equiv -\frac{\beta}{\alpha} \pmod p$ if and only if $\beta \equiv 6 \pmod 8$. □

Remark 2.7. Dirichlet gave a beautiful criterion for the solvability of $x^4 \equiv 2 \pmod p$. The proof given above was inspired by his idea.

As an immediate application of the law of biquadratic reciprocity, we have the following lemma.

Lemma 2.8. *Let $p = r^2 + x^2$ and $p' = r^2 + x'^2$ be two primes. Assume that D is an odd integer.*

(i) *If $x \equiv x' \pmod D$, then $(\frac{D}{p}) = (\frac{D}{p'})$.*

(ii) *If $x \equiv x' \pmod{4D}$, then $(\frac{D}{p})_4 = (\frac{D}{p'})_4$.*

(iii) *If $x \equiv x' \pmod{8D}$, then $(\frac{2D}{p})_4 = (\frac{2D}{p'})_4$.*

We conclude this section by giving the following lemma, which is useful in the next two sections.

Lemma 2.9. *Let $l \equiv 3 \pmod 4$ be a prime. If $l > 3$ and $1 \leqslant k < \frac{l+1}{4}$, then*

$$\mathrm{ord}_l \begin{pmatrix} \frac{l^2-1}{4} \\ k(l-1) \end{pmatrix} = 1;$$

in particular,

$$\begin{pmatrix} \frac{l^2-1}{4} \\ k(l-1) \end{pmatrix} \equiv 0 \pmod l.$$

Proof. Assume that m is a positive integer. For a fixed prime l, we write $m = a_0 + a_1 l + \cdots + a_r l^r$, $0 \leqslant a_i < l$. A useful formula for $\mathrm{ord}_l m!$ is the following:

$$\mathrm{ord}_l m! = \frac{1}{l-1}(m - (a_0 + a_1 + \cdots + a_r)).$$

It is easy to see that

$$\begin{aligned} &\frac{l^2-1}{4} = \frac{3l-1}{4} + \frac{l-3}{4}l, \\ &k(l-1) = l - k + (k-1)l, \\ &\frac{l^2-1}{4} - k(l-1) = \left(\frac{l-3}{4} - k\right)l + \frac{3l-1}{4} + k. \end{aligned}$$

Since $l > 3$,

$$\mathrm{ord}_l \begin{pmatrix} \frac{l^2-1}{4} \\ k(l-1) \end{pmatrix} = 1.$$

This completes the proof. □

3 $a_p \equiv 2 \pmod 4$

In this section, we consider the case where $a_p = 2\alpha$ with $\alpha \equiv 1 \pmod 4$ being a fixed integer. Suppose that $p = \alpha^2 + \beta^2$ is a prime. Assume that β takes the values from the arithmetic progression $4Dx + 2k$. Consider the quadratic polynomial in one indeterminate x:

$$p(D, \alpha, k, x) = \alpha^2 + (4Dx + 2k)^2 = 16D^2x^2 + 16kDx + 4k^2 + \alpha^2. \tag{3.1}$$

One can see that $p(D, \alpha, k, x)$ satisfies the assumption in the Hardy-Littlewood conjecture if and only if $(4k^2 + \alpha^2, D) = 1$.

Let

$$H(D,\alpha)=\{k\mid 1\leqslant k\leqslant 2D,(D,4k^2+\alpha^2)=1\}. \tag{3.2}$$

To count the elements in $H(D,\alpha)$, we introduce the following notation.

Notation. Given a prime l, we define

$$\tau(l^r)=\begin{cases} l^r, & \text{if } l\equiv 3 \pmod 4 \text{ or } l=2,\\ l^{r-1}(l-2), & \text{if } l\equiv 1 \pmod 4.\end{cases}$$

Extend this definition to any integer $D\in\mathbb{Z}$ by defining $\tau(\pm 1)=1$ and

$$\tau(D)=\prod_{l\mid D}\tau(l^{v_l(D)}).$$

It is clear that for two nonzero integers D and t, E_D is isomorphic to E_{Dt^4}. Thus we may assume that the general D is of the form as follows:

$$D=\pm 2^{\sigma}p_1\cdots p_r(q_1\cdots q_s)^2(l_1\cdots l_t)^3,$$

where $\sigma=0,1,2,3$ and p_i,q_i and l_i are distinct odd primes. We write $D=d\bar{d}$, where $(d,\bar{d})=1$ and for any odd prime l if $l\mid d$, then $l\mid\alpha$. By this definition, $(D,\alpha)\mid d$, but it is possible that $(D,\alpha)\neq d$. For a non-zero integer n, we define $\mathrm{Rad}(n)=\prod_{l\mid n}l$, where the product is over all odd prime factors of n. Then d and $\bar{d}$ are determined by $D=d\bar{d}$, $d>0$ odd, $\mathrm{Rad}(d)\mid\alpha$ and $(\alpha,\bar{d})=1$. With this notation, we have the following lemma.

Lemma 3.1. *Let $\phi(\cdot)$ be Euler's totient function. Then $\#H(D,\alpha)=2\phi(d)\tau(\bar{d})$. In particular, If $(D,\alpha)=1$, then $\#H(D,\alpha)=2\tau(D)$.*

Proof. By definition, we have

$$H(D,\alpha)=\{k\mid 1\leqslant k\leqslant D,(D,4k^2+\alpha^2)=1\}\cup\{k\mid D+1\leqslant k\leqslant 2D,(D,4k^2+\alpha^2)=1\}.$$

We have

$$\#\{k\mid 1\leqslant k\leqslant D,(D,4k^2+\alpha^2)=1\}=\#\{k\mid D+1\leqslant k\leqslant 2D,(D,4k^2+\alpha^2)=1\}.$$

Write $t(D,\alpha)=\#\{k\mid 1\leqslant k\leqslant D,(D,4k^2+\alpha^2)=1\}$. If $D=D_1D_2$ with $(D_1,D_2)=1$, then

$$t(D,\alpha)=t(D_1,\alpha)t(D_2,\alpha).$$

We see that $t(d,\alpha)=\phi(d)$ and $t((\bar{d},\alpha)=\tau(\bar{d})$. Hence, $\#H(D,\alpha)=2\phi(d)\tau(\bar{d})$.

When $(D,\alpha)=1$, $d=1$ and $D=\bar{d}$, hence $\#H(D,\alpha)=2\tau(D)$. □

It is easy to see that $H(D,\alpha)$ can be partitioned into the following disjoint union of two subsets:

$$H(D,\alpha)=H_I(D,\alpha)\cup H_{II}(D,\alpha), \tag{3.3}$$

where

$$H_I(D,\alpha)=\{k\in H(D,\alpha)\mid k\equiv 1 \pmod 2\}, \tag{3.4}$$

$$H_{II}(D,\alpha)=\{k\in H(D,\alpha)\mid k\equiv 0 \pmod 2\}. \tag{3.5}$$

We use $Q(\alpha,\infty)$ for the set of all primes which are of the form $p=\alpha^2+\beta^2$. For a positive integer N, let

$$Q(\alpha,N)=\{p\leqslant N\mid p\in Q(\alpha,\infty)\}. \tag{3.6}$$

For $k \in H(D,\alpha)$, put

$$P(D,\alpha,k,N) = \{p \in Q(\alpha,N) \mid p = p(D,\alpha,k,x) \text{ for some } x \in \mathbb{Z}\}, \tag{3.7}$$

$$P(D,\alpha,k) = \{p \in Q(\alpha,\infty) \mid p = p(D,\alpha,k,x) \text{ for some } x \in \mathbb{Z}\}. \tag{3.8}$$

So we have a disjoint union

$$Q(\alpha,N) = \bigcup_{k\in H(D,\alpha)} P(D,\alpha,k,N). \tag{3.9}$$

The Hardy-Littlewood conjecture predicts that for the fixed D,α and k,

$$\#P(D,\alpha,k,N) \sim c(D,\alpha,k)\frac{\sqrt{N}}{\log N} \tag{3.10}$$

as $N \to \infty$, where $c(D,\alpha,k) = \delta(16D^2, 16kD, 4k^2+\alpha^2)$ is a constant. Applying the explicit expression of the constant given by the conjecture, we can show that $c(D,\alpha,k)$ does not depend on $k \in H(D,\alpha)$, which enables us to write $c(D,\alpha,k) = c(D,\alpha)$. Therefore,

$$\#Q(\alpha,N) \sim \delta(1,0,\alpha^2)\frac{\sqrt{N}}{\log N} \sim 2\phi(d)\tau(\bar{d})c(D,\alpha)\frac{\sqrt{N}}{\log N}. \tag{3.11}$$

Suppose that $p_{k_1}, p_{k_2}, \ldots, p_{k_{2\tau(D)}} \in Q(\alpha,\infty)$ with $p_{k_i} \in P(D,\alpha,k_i)$ and $p_{k_i} \nmid D$. Put

$$P(D,\alpha) = \{p_{k_1}, p_{k_2}, \ldots, p_{k_{2\tau(D)}}\}. \tag{3.12}$$

Corresponding to the partition of $H(D,\alpha)$, the primes set $P(D,\alpha)$ can be partitioned into

$$P(D,\alpha) = P_I(D,\alpha) \cup P_{II}(D,\alpha), \tag{3.13}$$

where

$$P_I(D,\alpha) = \{p_k \in P(D,\alpha) \mid k \equiv 1 \pmod 2\}, \tag{3.14}$$

$$P_{II}(D,\alpha) = \{p_k \in P(D,\alpha) \mid k \equiv 0 \pmod 2\}. \tag{3.15}$$

Then $\#P(D,\alpha) = \#H(D,\alpha)$.

We introduce the following summations:

$$\sum\nolimits^{(2)}(D) := \sum_{p\in P(D,\alpha)} \left(\frac{D}{p}\right), \quad \sum\nolimits^{(4)}(D) := \sum_{p\in P(D,\alpha)} \left(\frac{D}{p}\right)_4. \tag{3.16}$$

$\sum^{(2)}(D)$ (resp. $\sum^{(4)}(D)$) will be simply denoted by $\sum^{(2)}$ (resp. $\sum^{(4)}$) if no confusion arises. For $\sigma = 2,4$ and $\kappa = I, II$, we put

$$\sum\nolimits_{\kappa}^{(\sigma)} := \sum_{p\in P_\kappa(D,\alpha)} \left(\frac{D}{p}\right)_\sigma. \tag{3.17}$$

Of course, $(\frac{D}{p})_2 = (\frac{D}{p})$ is the Legendre symbol.

It is immediate that

$$\sum\nolimits^{(\sigma)} = \sum\nolimits_{I}^{(\sigma)} + \sum\nolimits_{II}^{(\sigma)}. \tag{3.18}$$

We want to determine the exact number of primes $p \in P(D,\alpha)$, for which $(\frac{D}{p})_4$ equals a fixed value in $\{\pm 1, \pm \mathrm{i}\}$.

Let

$$\begin{aligned}
x_\alpha &= \#\{p \mid a_p = 2\alpha, p \in P(D,\alpha)\},\\
x_{-\alpha} &= \#\{p \mid a_p = -2\alpha, p \in P(D,\alpha)\},\\
x_\beta &= \#\{p \mid a_p = 2\beta, p \in P(D,\alpha)\},\\
x_{-\beta} &= \#\{p \mid a_p = -2\beta, p \in P(D,\alpha)\},
\end{aligned}$$

equivalently,

$$\begin{aligned}
x_\alpha &= \#\{p \mid D^{\frac{p-1}{4}} \equiv 1 \pmod p,\ p \in P(D,\alpha)\},\\
x_{-\alpha} &= \#\{p \mid D^{\frac{p-1}{4}} \equiv -1 \pmod p,\ p \in P(D,\alpha)\},\\
x_\beta &= \#\left\{p \,\middle|\, D^{\frac{p-1}{4}} \equiv \frac{\beta}{\alpha} \pmod p,\ p \in P(D,\alpha)\right\},\\
x_{-\beta} &= \#\left\{p \,\middle|\, D^{\frac{p-1}{4}} \equiv -\frac{\beta}{\alpha} \pmod p,\ p \in P(D,\alpha)\right\}.
\end{aligned}$$

Theorem 3.2. *Assume that the Hardy-Littlewood conjecture holds. Then*

$$a_p(E_D, 2\alpha) = \frac{x_\alpha}{2\phi(d)\tau(\bar{d})}, \quad a_p(E_D, -2\alpha) = \frac{x_{-\alpha}}{2\phi(d)\tau(\bar{d})}. \tag{3.19}$$

Proof. Recall that

$$Q(r,N) = \{p \mid p \text{ prime}, p = r^2 + x^2 \leqslant N\}.$$

By definition,

$$a_p(E_D, 2r) = \lim_{N\to\infty} \frac{\#\{p \mid a_p(E_D) = 2r, p \in Q(r,N)\}}{\#Q(r,N)}.$$

Let $p = \alpha^2 + x^2$ be a prime. By Lemma 2.8, if $p, p' \in P(D,\alpha)$, then $(\frac{D}{p})_4 = (\frac{D}{p'})_4$. With the notation as above, we suppose that $1 \leqslant k_1, \ldots, k_{x_\alpha} \leqslant 2D$ are integers such that

$$\left(\frac{D}{p_{k_j}}\right)_4 = 1.$$

We have

$$\begin{aligned}
a_p(E_D, 2\alpha) &= \lim_{N\to\infty} \frac{\#\{p \mid a_p(E_D) = 2\alpha, p \in Q(\alpha,N)\}}{\#Q(\alpha,N)}\\
&= \lim_{N\to\infty} \frac{\sum_{j=1}^{x_\alpha} \#P(D,\alpha,k_j,N)}{\#Q(\alpha,N)}\\
&= \lim_{N\to\infty} \frac{x_\alpha c(D,\alpha)\frac{\sqrt{N}}{\log N}}{\#H(D,\alpha)c(D,\alpha)\frac{\sqrt{N}}{\log N}}\\
&= \frac{x_\alpha}{2\phi(d)\tau(\bar{d})}.
\end{aligned}$$

The case where $a_p = -2\alpha$ can be checked similarly. □

Lemma 3.3. *Let D and D' with $(D,D') = 1$ be two odd integers. Then for $\kappa = I, II$,*

$$\Sigma_\kappa^{(2)}(DD') = \Sigma_\kappa^{(2)}(D)\Sigma_\kappa^{(2)}(D'), \quad \Sigma_\kappa^{(4)}(DD') = \Sigma_\kappa^{(4)}(D)\Sigma_\kappa^{(4)}(D'). \tag{3.20}$$

Proof. It is sufficient to show that $\Sigma_\kappa^{(4)}(DD') = \Sigma_\kappa^{(4)}(D)\Sigma_\kappa^{(4)}(D')$. By the Chinese remainder theorem, we see that there is a canonical bijection between the set of $\{2k \pmod{4DD'}, k \text{ is odd}\}$ and the set of pairs $\{(2t \pmod{4D}), 2s \pmod{4D'})), t \text{ and } s \text{ are odd}\}$. The same is true if we replace "odd" with "even". With the help of the law of biquadratic reciprocity, we obtain (3.20). □

We set the following notation:

$$\Sigma = \#H(D,\alpha) = 2\phi(d)\tau(\bar{d}). \tag{3.21}$$

Lemma 3.4. *If $\Sigma^{(4)} \in \mathbb{Z}$, then*

$$x_\alpha = \frac{1}{4}(\Sigma + \Sigma^{(2)} + 2\Sigma^{(4)}), \quad x_{-\alpha} = \frac{1}{4}(\Sigma + \Sigma^{(2)} - 2\Sigma^{(4)}).$$

Proof. It follows immediately from the system

$$\begin{cases} x_\alpha + x_{-\alpha} + x_\beta + x_{-\beta} = \Sigma, \\ x_\alpha - x_{-\alpha} + (x_\beta - x_{-\beta})\sqrt{-1} = \Sigma^{(4)}, \\ x_\alpha + x_{-\alpha} - x_\beta - x_{-\beta} = \Sigma^{(2)}. \end{cases} \tag{3.22}$$

This completes the proof. □

In the following, we first establish the density results when D is a prime. The conclusions are applicable for D to be any nonzero integer. In the following lemmas and theorems, except for Lemma 3.12, we assume that the Hardy-Littlewood conjecture holds.

It is immediate that for any odd prime l, $\sum_I^{(2)} = \sum_{II}^{(2)}$.

Lemma 3.5. *For any odd prime l, $\sum_I^{(2)} = \sum_{II}^{(2)} = -1$.*

Proof. Let l be an odd prime. Fix α. Then

$$\sum\nolimits_I^{(2)} = \sum_{y=1}^{l} \left(\frac{\alpha^2 + y^2}{l}\right) \equiv -1 \pmod{l}.$$

Clearly, we have $|\sum_I^{(2)}| \leqslant l$, and hence

$$\sum\nolimits_I^{(2)} = -1 \quad \text{or} \quad \sum\nolimits_I^{(2)} = l - 1.$$

However, $\sum_I^{(2)}$ is odd, and hence $\sum_I^{(2)} = -1$. □

Lemma 3.6. *Let l be an odd prime. Fix an odd integer α. Then*

(1)

$$\sum\nolimits_I^{(4)} = \begin{cases} 1, & \text{if } l \equiv 5,7 \pmod 8, \\ -1, & \text{if } l \equiv 1,3 \pmod 8. \end{cases}$$

(2)

$$\sum\nolimits_{II}^{(4)} = \begin{cases} 1, & \text{if } l \equiv 3,5 \pmod 8, \\ -1, & \text{if } l \equiv 1,7 \pmod 8. \end{cases}$$

(3) *For $p \in P_I(D,\alpha)$, $(\frac{-1}{p})_4 = -1$, and for $p \in P_{II}(D,\alpha)$, $(\frac{-1}{p})_4 = 1$.*

Proof. Assume that $l \equiv 1 \pmod 4$ is a prime. For any prime p of the form $\alpha^2 + (4ly + 2k)^2$, we may assume that $\alpha + (4ly + 2k)\sqrt{-1}$ is primary. Write $l = \rho\bar{\rho}$ for the prime factorization of l in $\mathbb{Z}[\sqrt{-1}]$. By the law of biquadratic reciprocity,

$$\begin{aligned} \left(\frac{l}{\alpha + (4ly+2k)\sqrt{-1}}\right)_4 &= \left(\frac{\rho\bar{\rho}}{\alpha + (4ly+2k)\sqrt{-1}}\right)_4 \\ &= \left(\frac{\alpha + (4ly+2k)\sqrt{-1}}{\rho}\right)_4 \left(\frac{\alpha + (4ly+2k)\sqrt{-1}}{\bar{\rho}}\right)_4 \\ &\equiv (\alpha + 2k\sqrt{-1})^{\frac{l-1}{4}} (\alpha - 2k\sqrt{-1})^{\frac{3}{4}(l-1)} \pmod{\rho}. \end{aligned}$$

Therefore,

$$\begin{aligned}\Sigma_I^{(4)} &\equiv \sum_{k=1}^{l}(\alpha+2k\sqrt{-1})^{\frac{l-1}{4}}(\alpha-2k\sqrt{-1})^{\frac{3}{4}(l-1)} \pmod{\rho}\\ &\equiv \sum_{k=1}^{l}(2k\sqrt{-1})^{\frac{l-1}{4}}(-2k\sqrt{-1})^{\frac{3}{4}(l-1)} \pmod{\rho}\\ &\equiv (l-1)(-1)^{\frac{3}{4}(l-1)} \pmod{\rho}\\ &\equiv \begin{cases}1 \pmod{l}, & \text{if } l\equiv 5 \pmod 8,\\ -1 \pmod{l}, & \text{if } l\equiv 1 \pmod 8.\end{cases}\end{aligned}$$

Since $|\Sigma_I^{(4)}|$ is odd up to l,

$$\Sigma_I^{(4)} = \begin{cases}1, & \text{if } l\equiv 5 \pmod 8,\\ -1, & \text{if } l\equiv 1 \pmod 8.\end{cases}$$

It is easy to see that for a prime $l\equiv 1 \pmod 4$, $\Sigma_I^{(4)}=\Sigma_{II}^{(4)}$.

Assume now that $l\equiv 3 \pmod 4$. If k is odd, then by the law of biquadratic reciprocity,

$$\left(\frac{l}{\alpha+(4ly+2k)\sqrt{-1}}\right)_4 = -\left(\frac{\alpha+(4ly+2k)\sqrt{-1}}{l}\right)_4 = -\left(\frac{\alpha+2k\sqrt{-1}}{l}\right)_4.$$

Hence,

$$\begin{aligned}\Sigma_I^{(4)} &\equiv -\sum_{k=1}^{l}(\alpha+2k\sqrt{-1})^{\frac{l^2-1}{4}} \pmod l\\ &\equiv -\sum_{k=1}^{l}(2k\sqrt{-1})^{\frac{l^2-1}{4}} \pmod l\\ &\equiv -(l-1)(-1)^{\frac{l^2-1}{8}} \pmod l\\ &\equiv (-1)^{\frac{l^2-1}{8}} \pmod l.\end{aligned}$$

Hence, $\Sigma_I^{(4)}=(-1)^{\frac{l^2-1}{8}}$, i.e.,

$$\Sigma_I^{(4)} = (-1)^{\frac{l^2-1}{8}} = \begin{cases}-1, & \text{if } l\equiv 3 \pmod 8,\\ 1, & \text{if } l\equiv 7 \pmod 8.\end{cases}$$

If k is even, then the law of biquadratic reciprocity implies that

$$\left(\frac{l}{\alpha+(4ly+2k)\sqrt{-1}}\right)_4 = \left(\frac{\alpha+2k\sqrt{-1}}{l}\right)_4.$$

A similar computation as above shows that

$$\Sigma_{II}^{(4)} = -(-1)^{\frac{l^2-1}{8}} = \begin{cases}1, & \text{if } l\equiv 3 \pmod 8,\\ -1, & \text{if } l\equiv 7 \pmod 8.\end{cases}$$

This proves (1) and (2).

(3) is immediate. □

Theorem 3.7. *Assume that $D=l$ is an odd prime.*

If $l\equiv 1 \pmod 8$, then

$$a_p(2\alpha)=\frac{l-5}{4(l-2)},\quad a_p(-2\alpha)=\frac{l-1}{4(l-2)}.$$

If $l \equiv 5 \pmod 8$, *then*

$$a_p(2\alpha) = \frac{l-1}{4(l-2)}, \quad a_p(-2\alpha) = \frac{l-5}{4(l-2)}.$$

If $l \equiv 3 \pmod 4$, *then*

$$a_p(2\alpha) = a_p(-2\alpha) = \frac{l-1}{4l}.$$

Proof. We have the following computation for Σ, $\Sigma^{(2)}$ and $\Sigma^{(4)}$.

For $l \equiv 1 \pmod 8$,

$$\Sigma = 2(l-2), \quad \Sigma^{(2)} = -2, \quad \Sigma^{(4)} = -2.$$

For $l \equiv 5 \pmod 8$,

$$\Sigma = 2(l-2), \quad \Sigma^{(2)} = -2, \quad \Sigma^{(4)} = 2.$$

For $l \equiv 3 \pmod 4$

$$\Sigma = 2l, \quad \Sigma^{(2)} = -2, \quad \Sigma^{(4)} = 0.$$

Now the result follows from the formula, i.e.,

$$x_\alpha = \frac{1}{4}(\Sigma + \Sigma^{(2)} + 2\Sigma^{(4)}), \quad x_{-\alpha} = \frac{1}{4}(\Sigma + \Sigma^{(2)} - 2\Sigma^{(4)}).$$

This completes the proof. □

For

$$D = \pm 2^\sigma p_1 \cdots p_r (q_1 \cdots q_s)^2 (l_1 \cdots l_t)^3,$$

where $\sigma = 0, 1, 2, 3$ and p_i, q_i and l_i are distinct odd primes. We define

- $\delta = 0$ if $D > 0$ and $\delta = 1$ if $D < 0$;
- $r_i = \#\{l \mid p_1 \cdots p_r, l \equiv i \pmod 8\}$;
- $t_i = \#\{l \mid l_1 \cdots l_t, l \equiv i \pmod 8\}$.

For a rational odd prime $p = \alpha^2 + \beta^2$ with α odd, replacing α by $-\alpha$ if necessary, we can specify α uniquely by $\alpha \equiv 1 \pmod 4$. This choice is assumed from now on.

Theorem 3.8. *Assume that* $(D, \alpha) = 1$. *If* $D \equiv 1 \pmod 4$, *then*

$$a_p(2\alpha) = \frac{1}{4}\left(1 + \frac{(-1)^{r+t}}{\tau(p_1 \cdots p_r l_1 \cdots l_t)} + \frac{2(-1)^{r_1+r_7+s+t_1+t_7}}{\tau(p_1 \cdots p_r q_1 \cdots q_s l_1 \cdots l_t)}\right),$$
$$a_p(-2\alpha) = \frac{1}{4}\left(1 + \frac{(-1)^{r+t}}{\tau(p_1 \cdots p_r l_1 \cdots l_t)} - \frac{2(-1)^{r_1+r_7+s+t_1+t_7}}{\tau(p_1 \cdots p_r q_1 \cdots q_s l_1 \cdots l_t)}\right).$$

If $D \equiv 3 \pmod 4$, *then*

$$a_p(2\alpha) = a_p(-2\alpha) = \frac{1}{4}\left(1 + \frac{(-1)^{r+t}}{\tau(p_1 \cdots p_r l_1 \cdots l_t)}\right).$$

Proof. We compute Σ, $\Sigma^{(2)}$ and $\Sigma^{(4)}$. First, we have $\Sigma = 2\tau(D)$. We see that

$$\Sigma_I^{(2)} = \Sigma_{II}^{(2)} = (-1)^{r+t}\tau((q_1 \cdots q_s)^2) \cdot (l_1 \cdots l_t)^2.$$

Hence,

$$\Sigma^{(2)} = 2(-1)^{r+t}\tau((q_1 \cdots q_s)^2) \cdot (l_1 \cdots l_t)^2.$$

We have

$$\Sigma_I^{(4)} = (-1)^{r_1+r_3+s+t_1+t_3+\delta} q_1 \cdots q_s l_1^2 \cdots l_t^2, \quad \Sigma_{II}^{(4)} = (-1)^{r_1+r_7+s+t_1+t_7} q_1 \cdots q_s l_1^2 \cdots l_t^2.$$

If $D \equiv 1 \pmod 4$, then $(-1)^{r_1+r_3+s+t_1+t_3+\delta} = (-1)^{r_1+r_7+s+t_1+t_7}$, and if $D \equiv 3 \pmod 4$, then $(-1)^{r_1+r_3+s+t_1+t_3+\delta} = -(-1)^{r_1+r_7+s+t_1+t_7}$, and hence

$$\Sigma^{(4)} = \begin{cases} 2(-1)^{r_1+r_7+s+t_1+t_7} q_1 \cdots q_s l_1^2 \cdots l_t^2, & \text{if } D \equiv 1 \pmod 4, \\ 0, & \text{if } D \equiv 3 \pmod 4. \end{cases}$$

Now the theorem follows from Lemma 3.4.

□

Theorem 3.9. *Assume that* $(D,\alpha)=1$ *and* $4\|D$.

If $\frac{D}{4}\equiv 3 \pmod 4$, *then*

$$a_p(2\alpha)=\frac{1}{4}\bigg(1+\frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)}+\frac{2(-1)^{r_1+r_7+s+t_1+t_7}}{\tau(p_1\cdots p_r q_1\cdots q_s l_1\cdots l_t)}\bigg),$$
$$a_p(-2\alpha)=\frac{1}{4}\bigg(1+\frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)}-\frac{2(-1)^{r_1+r_7+s+t_1+t_7}}{\tau(p_1\cdots p_r q_1\cdots q_s l_1\cdots l_t)}\bigg).$$

If $\frac{D}{4}\equiv 1 \pmod 4$, *then*

$$a_p(2\alpha)=a_p(-2\alpha)=\frac{1}{4}\bigg(1+\frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)}\bigg).$$

Proof. Observe that $\Sigma^{(2)}(D)=4\Sigma^{(2)}(\frac{D}{4})$, $\Sigma_I^{(4)}(D)=-4\Sigma_I^{(4)}(\frac{D}{4})$ and $\Sigma_{II}^{(4)}(D)=4\Sigma_{II}^{(4)}(\frac{D}{4})$. Using the results for $D/4$, we have the following computation for Σ, $\Sigma^{(2)}$ and $\Sigma^{(4)}$:

$$\begin{aligned}&\Sigma=2\tau(D),\\&\Sigma^{(2)}=8(-1)^{r+t}\tau((q_1\cdots q_s)^2)\cdot(l_1\cdots l_t)^2,\\&\Sigma^{(4)}=\begin{cases}8(-1)^{r_1+r_7+s+t_1+t_7}q_1\cdots q_s l_1^2\cdots l_t^2, & \text{if } \frac{D}{4}\equiv 3 \pmod 4,\\ 0, & \text{if } \frac{D}{4}\equiv 1 \pmod 4.\end{cases}\end{aligned}$$

Then the theorem follows from Lemma 3.4. □

Theorem 3.10. *Assume that* $2\|D$ *or* $8\|D$. *Then*

$$a_p(2\alpha)=a(-2\alpha)=\frac{1}{4}.$$

Proof. Assume that $2\|D$. The situation that $8\|D$ is analogous. We claim that $\Sigma^{(2)}=0$ and $\Sigma^{(4)}=0$. In fact, for any prime $p=p(D,\alpha,k,x)$, we have $(\frac{2}{p})=-1$ if $k\in H_I(D,\alpha)$ and $(\frac{2}{p})=1$ if $k\in H_{II}(D,\alpha)$. On the other hand, for $D/2$, $\Sigma_I^{(2)}=\Sigma_{II}^{(2)}$. Hence, $\Sigma^{(2)}=0$.

We introduce a new partition for $H(D,\alpha)$:

$$H(D,\alpha)=H(D,\alpha)_1\cup H(D,\alpha)_2,$$

where for $H(D,\alpha)_1$, $1\leqslant k\leqslant D$, and for $H(D,\alpha)_2$, $D+1\leqslant k\leqslant 2D$. We establish the following one to one correspondence from $H(D,\alpha)_1$ to $H(D,\alpha)_2$ as follows:

$$p_{k_1}=\alpha^2+(4Dy+2k)^2\to p_{k_2}=\alpha^2+(4Dy+2D+2k)^2.$$

Note that

$$\begin{aligned}&\bigg(\frac{D/2}{p_{k_1}}\bigg)_4=\bigg(\frac{D/2}{p_{k_2}}\bigg)_4,\\&\bigg(\frac{2}{p_{k_1}}\bigg)_4=-\bigg(\frac{2}{p_{k_2}}\bigg)_4.\end{aligned}$$

Hence, $\Sigma^{(4)}=0$. Now the theorem follows from Lemma 3.4. □

In particular, taking $\alpha=1$, we have the following corollary, which answers a question proposed to the author by Mazur.

Corollary 3.11. (1) *If* $D \equiv 1 \pmod 4$ *or* $D/4 \equiv 3 \pmod 4$, *then*

$$a_p(2) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)} + \frac{2(-1)^{r_1+r_7+s+t_1+t_7}}{\tau(p_1\cdots p_r q_1\cdots q_s l_1\cdots l_t)}\bigg),$$
$$a_p(-2) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)} - \frac{2(-1)^{r_1+r_7+s+t_1+t_7}}{\tau(p_1\cdots p_r q_1\cdots q_s l_1\cdots l_t)}\bigg).$$

(2) *If* $D \equiv 3 \pmod 4$ *or* $D/4 \equiv 1 \pmod 4$, *then*

$$a_p(2) = a_p(-2) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)}\bigg).$$

(3) *If* $2\|D$ *or* $8\|D$, *then*

$$a_p(2) = a(-2) = \frac{1}{4}.$$

We turn to deal with the general case and thus the case $(D,\alpha) > 1$ is included. We need some notation. Recall the notation above Lemma 3.1 and further assume that

$$d = d_p \cdot d_q^2 \cdot d_l^3, \quad \bar{d} = \pm 2^\sigma \bar{d}_p \cdot \bar{d_q}^2 \cdot \bar{d_l}^3,$$

where d_p, d_q, d_l and $\bar{d_p}, \bar{d_q}, \bar{d_l}$ are all square-free integers. We define

- $r'' = \#\{l \mid l \mid \bar{d_p}\}$;
- $s'' = \#\{l \mid l \mid \bar{d_q}\}$;
- $t'' = \#\{l \mid l \mid \bar{d_l}\}$;
- $r'_i = \#\{l \mid d_p,\, l \equiv i \pmod 8\}$;
- $r''_i = \#\{l \mid \bar{d_p},\, l \equiv i \pmod 8\}$;
- $t'_i = \#\{l \mid d_l,\, l \equiv i \pmod 8\}$;
- $t''_i = \#\{l \mid \bar{d_l},\, l \equiv i \pmod 8\}$.

Lemma 3.12. *Given any nonzero integer* D, *assume that*

$$p = p(D,\alpha,k,x) = \alpha^2 + (4Dx + 2k)^2$$

is a prime. For any odd prime factor l *of* D, *if* $l \mid \alpha$, *then* $(\frac{l}{p}) = 1$ *and*

$$l^{\frac{p-1}{4}} \equiv \begin{cases} 1 \pmod p, & \text{if } l \equiv 1,3 \pmod 8, \\ -1 \pmod p, & \text{if } l \equiv 5,7 \pmod 8, \end{cases}$$

provided that k *is odd*;

$$l^{\frac{p-1}{4}} \equiv \begin{cases} 1 \pmod p, & \text{if } l \equiv 1,7 \pmod 8, \\ -1 \pmod p, & \text{if } l \equiv 5,3 \pmod 8, \end{cases}$$

provided that k *is even.*

Proof. Since $p \equiv 1 \pmod 4$, we have

$$\left(\frac{l}{p}\right) = \left(\frac{p}{l}\right) = \left(\frac{(2k)^2}{l}\right) = 1.$$

On the other hand, by assuming that $\alpha + (4lx + 2k)\sqrt{-1}$ is primary, we see that

$$l^{\frac{p-1}{4}} \equiv \left(\frac{l}{\alpha + (4lx+2k)\sqrt{-1}}\right)_4 \pmod p.$$

If $l \equiv 3 \pmod 4$, then

$$\left(\frac{l}{\alpha + (4lx+2k)\sqrt{-1}}\right)_4 = (-1)^k \left(\frac{\alpha + (4lx+2k)\sqrt{-1}}{l}\right)_4$$

$$\equiv (-1)^k((4lx+2k)\sqrt{-1})^{\frac{l^2-1}{4}}$$
$$\equiv (-1)^{k+\frac{l^2-1}{8}} \pmod{l}.$$

If $l \equiv 1 \pmod 4$ and $l = \rho\bar{\rho}$ is the prime factorization of l in $\mathbb{Z}[\sqrt{-1}]$, then

$$\begin{aligned}\left(\frac{l}{\alpha+(4ly+2k)\sqrt{-1}}\right)_4 &= \left(\frac{\rho\bar{\rho}}{\alpha+(4ly+2k)\sqrt{-1}}\right)_4\\ &= \left(\frac{\alpha+(4ly+2k)\sqrt{-1}}{\rho}\right)_4\left(\frac{\alpha+(4ly+2k)\sqrt{-1}}{\bar{\rho}}\right)_4\\ &\equiv (2k\sqrt{-1})^{\frac{l-1}{4}}(-2k\sqrt{-1})^{\frac{3}{4}(l-1)}\\ &\equiv (-1)^{\frac{l-1}{4}} \pmod{\rho}.\end{aligned}$$

This proves the lemma. □

Theorem 3.13. *Assume that* $\mathrm{Rad}(D) \mid \alpha$, *i.e., for any odd prime factor* l *of* D, $l \mid \alpha$.

(1) *If* $D \equiv 1 \pmod 4$, *then*

$$a_p(2\alpha) = \frac{1}{2}(1+(-1)^{r_3+r_5+t_3+t_5}),$$
$$a_p(-2\alpha) = \frac{1}{2}(1-(-1)^{r_3+r_5+t_3+t_5}).$$

(2) *If* $D \equiv 3 \pmod 4$, *then*

$$a_p(2\alpha) = a_p(-2\alpha) = \frac{1}{2}.$$

(3) *Assume* $4\|D$.
If $\frac{D}{4} \equiv 1 \pmod 4$, *then*

$$a_p(2\alpha) = a_p(-2\alpha) = \frac{1}{2}.$$

If $\frac{D}{4} \equiv 3 \pmod 4$, *then*

$$a_p(2\alpha) = \frac{1}{2}(1+(-1)^{r_3+r_5+t_3+t_5}),$$
$$a_p(-2\alpha) = \frac{1}{2}(1-(-1)^{r_3+r_5+t_3+t_5}).$$

(4) *If* $2\|D$, *or* $8\|D$, *then*

$$a_p(2\alpha) = a_p(-2\alpha) = \frac{1}{4}.$$

Proof. By Lemma 3.12, if $p = p(D,\alpha,k,x) = \alpha^2 + (4Dx+2k)^2$ is a prime, then for odd k,

$$D^{\frac{p-1}{4}} \equiv (-1)^{r_5+r_7+t_5+t_7} \pmod p,$$

and for k even,

$$D^{\frac{p-1}{4}} \equiv (-1)^{r_3+r_5+t_3+t_5} \pmod p.$$

If $D \equiv 1 \pmod 4$, then

$$(-1)^{r_5+r_7+t_5+t_7} = (-1)^{r_3+r_5+t_3+t_5},$$

and if $D \equiv 3 \pmod 4$, then

$$(-1)^{r_5+r_7+t_5+t_7} = -(-1)^{r_3+r_5+t_3+t_5}.$$

Note that $4^{\frac{p-1}{4}} \equiv (\frac{2}{p}) \pmod p$ and $(\frac{2}{p}) = -1$ if k is odd, and 1 if k is even. Hence, the assertions (1)–(3) follow.

If $2\|D$ or $8\|D$, then for odd k, $2^{\frac{p-1}{4}} \not\equiv \pm 1 \pmod p$, and hence $a_p \neq \pm 2\alpha$. On the other hand, if $2\|k$, then $2^{\frac{p-1}{4}} \equiv -1 \pmod p$, and if $4 \mid k$, then $2^{\frac{p-1}{4}} \equiv 1 \pmod p$. Hence, $a_p(2\alpha) = a_p(-2\alpha) = \frac{1}{4}$. □

Remark 3.14. We can make an explicit computation of Σ, $\Sigma^{(2)}$ and $\Sigma^{(4)}$ to give an alternative proof of the above theorem. For example, in the case (4), the proof of Theorem 3.10 works here. Hence, $\Sigma^{(2)}=0$ and $\Sigma^{(4)}=0$, and consequently, $a_p(2\alpha)=a_p(-2\alpha)=\frac{1}{4}$.

Theorem 3.15. (1) *Assume that D is odd.*

If $D\equiv 1 \pmod 4$, then

$$a_p(2\alpha)=\frac{1}{4}\bigg(1+\frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)}+\frac{2(-1)^{r'_3+r'_5+t'_3+t'_5+r''_1+r''_7+t''_1+t''_7+s''}}{\tau(\bar{d}_p\cdot\bar{d}_q\cdot\bar{d}_l)}\bigg),$$
$$a_p(-2\alpha)=\frac{1}{4}\bigg(1+\frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)}-\frac{2(-1)^{r'_3+r'_5+t'_3+t'_5+r''_1+r''_7+t''_1+t''_7+s''}}{\tau(\bar{d}_p\cdot\bar{d}_q\cdot\bar{d}_l)}\bigg).$$

If $D\equiv 3 \pmod 4$, then

$$a_p(2\alpha)=a_p(-2\alpha)=\frac{1}{4}\bigg(1+\frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)}\bigg).$$

(2) *Assume that D is even.*

If $4\|D$ and $\frac{D}{4}\equiv 1 \pmod 4$, then

$$a_p(2\alpha)=a_p(-2\alpha)=\frac{1}{4}\bigg(1+\frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)}\bigg).$$

If $4\|D$ and $\frac{D}{4}\equiv 3 \pmod 4$, then

$$a_p(2\alpha)=\frac{1}{4}\bigg(1+\frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)}+\frac{2(-1)^{r'_3+r'_5+t'_3+t'_5+r''_1+r''_7+t''_1+t''_7+s''}}{\tau(\bar{d}_p\cdot\bar{d}_q\cdot\bar{d}_l)}\bigg),$$
$$a_p(-2\alpha)=\frac{1}{4}\bigg(1+\frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)}-\frac{2(-1)^{r'_3+r'_5+t'_3+t'_5+r''_1+r''_7+t''_1+t''_7+s''}}{\tau(\bar{d}_p\cdot\bar{d}_q\cdot\bar{d}_l)}\bigg).$$

If $2\|D$ or $8\|D$, then

$$a_p(2\alpha)=a_p(-2\alpha)=\frac{1}{4}.$$

Proof. (1) We have

$$\begin{aligned}
&\Sigma=2\phi(d)\Sigma(\bar{d})=2\phi(d)\tau(\bar{d}),\\
&\Sigma^{(2)}=2\phi(d)\Sigma^{(2)}(\bar{d})=2(-1)^{r''+t''}\phi(d)\tau(\bar{d_q}^2\cdot\bar{d_l}^2),\\
&\Sigma^{(4)}_I=(-1)^{r'_5+r'_7+t'_5+t'_7+r''_1+r''_3+t''_1+t''_3+s''+\delta}\phi(d)\cdot\bar{d}_q\cdot\bar{d_l}^2,\\
&\Sigma^{(4)}_{II}=(-1)^{r'_3+r'_5+t'_3+t'_5+r''_1+r''_7+t''_1+t''_7+s''}\phi(d)\cdot\bar{d}_q\cdot\bar{d_l}^2.
\end{aligned}$$

If $D\equiv 1 \pmod 4$, then

$$(-1)^{r'_5+r'_7+t'_5+t'_7+r''_1+r''_3+t''_1+t''_3+s''+\delta}=(-1)^{r'_3+r'_5+t'_3+t'_5+r''_1+r''_7+t''_1+t''_7+s''},$$

and if $D\equiv 3 \pmod 4$, then

$$(-1)^{r'_5+r'_7+t'_5+t'_7+r''_1+r''_3+t''_1+t''_3+s''+\delta}=-(-1)^{r'_3+r'_5+t'_3+t'_5+r''_1+r''_7+t''_1+t''_7+s''}.$$

Hence, if $D\equiv 1 \pmod 4$, then

$$\Sigma^{(4)}=2(-1)^{r'_3+r'_5+t'_3+t'_5+r''_1+r''_7+t''_1+t''_7+s''}\phi(d)\cdot\bar{d}_q\cdot\bar{d_l}^2,$$

and if $D\equiv 3 \pmod 4$, then

$$\Sigma^{(4)}=0.$$

Then the formula in Lemma 3.4 gives the desired results.

(2) For $4\|D$, we can use

$$\Sigma^{(2)}(D)=4\Sigma^{(2)}\left(\frac{D}{4}\right),\quad \Sigma_I^{(4)}(D)=-4\Sigma_I^{(4)}\left(\frac{D}{4}\right),\quad \Sigma_{II}^{(4)}(D)=4\Sigma_{II}^{(4)}\left(\frac{D}{4}\right)$$

to obtain the assertion.

For $2\|D$ or $8\|D$, we have $\Sigma^{(2)}=\Sigma^{(4)}=0$.

This proves the theorem. □

4 $a_p\equiv 0\pmod 4$

Let $\beta>0$ be a fixed even integer. In this section, we consider the case where $a_p=2\beta\equiv 0 \pmod 4$. The idea here is analogous to $a_p\equiv 2 \pmod 4$, but some different technical details are needed. Throughout this section, except for Lemmas 4.5 and 4.7, we assume the Hardy-Littlewood conjecture. Changing α to β, we collect some corresponding, but modified, notations from Section 3. Suppose that $p=\beta^2+\alpha^2$ is a prime. Assume that α takes values from the arithmetic progression $4Dx+2k+1$. Consider the quadratic polynomial in one indeterminate x:

$$p(D,\beta,k,x)=\beta^2+(4Dx+2k+1)^2.$$

Then $p(D,\beta,k,x)$ satisfies the assumption in the Hardy-Littlewood conjecture if and only if $((2k+1)^2+\beta^2,D)=1$.

We have

$$H(D,\beta)=\{k\mid 1\leqslant k\leqslant 2D,(D,(2k+1)^2+\beta^2)=1\} \tag{4.1}$$

and its partition

$$H(D,\beta)=H_I(D,\beta)\cup H_{II}(D,\beta), \tag{4.2}$$

where

$$H_I(D,\beta)=\{k\in H(D,\beta)\mid k\equiv 1 \pmod 2\}, \tag{4.3}$$
$$H_{II}(D,\beta)=\{k\in H(D,\beta)\mid k\equiv 0 \pmod 2\}. \tag{4.4}$$

Then $\#H_I(D,\beta)=\#H_{II}(D,\beta)=\phi(d)\tau(\bar{d})$ and $\#H(D,\beta)=2\phi(d)\tau(\bar{d})$.

In correspondence to $H(D,\beta)$, we have the primes set $P(D,\beta)$ and its partition

$$P(D,\beta)=P_I(D,\beta)\cup P_{II}(D,\beta), \tag{4.5}$$

where

$$P_I(D,\beta)=\{p_k\in P(D,\beta)\mid k\equiv 1 \pmod 2\}, \tag{4.6}$$
$$P_{II}(D,\beta)=\{p_k\in P(D,\beta)\mid k\equiv 0 \pmod 2\}. \tag{4.7}$$

Define

$$\sum\nolimits^{(2)}(D):=\sum_{p\in P(D,\beta)}\left(\frac{D}{p}\right),\quad \sum\nolimits^{(4)}(D):=\sum_{p\in P(D,\beta)}\left(\frac{D}{p}\right)_4. \tag{4.8}$$

Again, we simply write $\sum^{(2)}(D)$ (resp. $\sum^{(4)}(D)$) as $\sum^{(2)}$ (resp. $\sum^{(4)}$).

We also have

$$\sum\nolimits^{(\sigma)}=\sum\nolimits_I^{(\sigma)}+\sum\nolimits_{II}^{(\sigma)}, \tag{4.9}$$

where for $\sigma = 2, 4$ and $\kappa = I, II$,

$$\sum\nolimits_{\kappa}^{(\sigma)} := \sum_{p \in P_\kappa(D,\beta)} \left(\frac{D}{p}\right)_\sigma. \tag{4.10}$$

As in Section 3, we put

$$\begin{aligned} x_\beta &= \#\{p \mid a_p = 2\beta, p \in P(D,\beta)\},\\ x_{-\beta} &= \#\{p \mid a_p = -2\beta, p \in P(D,\beta)\},\\ x_\alpha &= \#\{p \mid a_p = 2\alpha, p \in P(D,\beta)\},\\ x_{-\alpha} &= \#\{p \mid a_p = -2\alpha, p \in P(D,\beta)\}. \end{aligned}$$

Then

$$\begin{cases} x_\beta + x_{-\beta} + x_\alpha + x_{-\alpha} = \Sigma,\\ (x_\beta - x_{-\beta})\sqrt{-1} + x_\alpha - x_{-\alpha} = \Sigma^{(4)},\\ -x_\beta - x_{-\beta} + x_\alpha + x_{-\alpha} = \Sigma^{(2)}. \end{cases} \tag{4.11}$$

This implies the following lemma.

Lemma 4.1. *If $\Sigma^{(4)} \in \mathbb{Z}$, then*

$$x_\beta = x_{-\beta} = \frac{1}{4}(\Sigma - \Sigma^{(2)}).$$

Theorem 4.2. *Assume that the Hardy-Littlewood conjecture holds. Then*

$$a_p(E_D, 2\beta) = \frac{x_\beta}{2\phi(d)\tau(\bar{d})}, \quad a_p(E_D, -2\beta) = \frac{x_{-\beta}}{2\phi(d)\tau(\bar{d})}. \tag{4.12}$$

Proof. See the proof of Theorem 3.2. □

Lemma 4.3. *Let l be an odd prime. Fix an even integer β. Then*

(1) $\Sigma_I^{(2)} = \Sigma_{II}^{(2)} = -1$;

(2) *for $l \equiv 1 \pmod 4$,*

$$\Sigma_I^{(4)} = \Sigma_{II}^{(4)} = -1;$$

for $l \equiv 3 \pmod 4$,

(2a) *if $2\|\beta$, then $\Sigma_I^{(4)} = \Sigma_{II}^{(4)} = 1$;*

(2b) *if $4 \mid \beta$, then $\Sigma_I^{(4)} = \Sigma_{II}^{(4)} = -1$.*

Proof. (1) The proof for the fixed odd α works for the fixed even β.

(2) For any prime of the form $p = (4ly + 2k + 1)^2 + \beta^2$, we may assume that $4ly + 2k + 1 + \beta\sqrt{-1}$ is primary.

Let $l \equiv 1 \pmod 4$ be a prime and $l = \rho\bar{\rho}$ be the prime factorization of l in $\mathbb{Z}[\sqrt{-1}]$. It holds that

$$\begin{aligned} \left(\frac{l}{4ly + 2k + 1 + \beta\sqrt{-1}}\right)_4 &= \left(\frac{\rho\bar{\rho}}{4ly + 2k + 1 + \beta\sqrt{-1}}\right)_4\\ &= \left(\frac{4ly + 2k + 1 + \beta\sqrt{-1}}{\rho}\right)_4 \left(\frac{4ly + 2k + 1 + \beta\sqrt{-1}}{\bar{\rho}}\right)_4\\ &= \left(\frac{2k + 1 + \beta\sqrt{-1}}{\rho}\right)_4 \left(\frac{2k + 1 + \beta\sqrt{-1}}{\bar{\rho}}\right)_4\\ &\equiv (2k + 1 + \beta\sqrt{-1})^{\frac{l-1}{4}} (2k + 1 - \beta\sqrt{-1})^{\frac{3}{4}(l-1)} \pmod{\rho}. \end{aligned}$$

Hence,

$$\Sigma_I^{(4)} \equiv \sum_{k=1}^{l} (2k + 1 + \beta\sqrt{-1})^{\frac{l-1}{4}} (2k + 1 - \beta\sqrt{-1})^{\frac{3}{4}(l-1)} \pmod{\rho}$$

$$\begin{aligned}&\equiv \sum_{k=1}^{l}((2k+1)^{\frac{l-1}{4}}+\cdots+(\beta\sqrt{-1})^{\frac{l-1}{4}})\\&\quad\times((2k+1)^{\frac{3}{4}(l-1)}+\cdots+(-\beta\sqrt{-1})^{\frac{3}{4}(l-1)}) \pmod{\rho}\\&\equiv \sum_{k=1}^{l}(2k+1)^{l-1} \pmod{\rho}\\&\equiv -1 \pmod{\rho}.\end{aligned}$$

Hence, $\Sigma_I^{(4)}=-1$.

Let $l\equiv 3 \pmod 4$ be a prime. Then

$$\begin{aligned}\left(\frac{l}{4ly+2k+1+\beta\sqrt{-1}}\right)_4&=(-1)^{\frac{\beta}{2}}\left(\frac{4ly+2k+1+\beta\sqrt{-1}}{l}\right)_4\\&=(-1)^{\frac{\beta}{2}}\left(\frac{2k+1+\beta\sqrt{-1}}{l}\right)_4.\end{aligned}$$

Hence,

$$\begin{aligned}\Sigma_I^{(4)}&=(-1)^{\frac{\beta}{2}}\sum_{k=1}^{l}\left(\frac{2k+1+\beta\sqrt{-1}}{l}\right)_4\\&\equiv(-1)^{\frac{\beta}{2}}\sum_{k=1}^{l}(2k+1+\beta\sqrt{-1})^{\frac{l^2-1}{4}} \pmod{l}\\&\equiv(-1)^{\frac{\beta}{2}}\sum_{k=1}^{l}((2k+1)^{l-1})^{\frac{l+1}{4}} \pmod{l}\\&\equiv-(-1)^{\frac{\beta}{2}} \pmod{l}.\end{aligned}$$

Therefore, $\Sigma_I^{(4)}=-1$ if $2\|\beta$, and $\Sigma_I^{(4)}=1$ if $4\mid\beta$.

It is clear that $\Sigma_I^{(4)}=\Sigma_{II}^{(4)}$. This proves the lemma. □

Theorem 4.4. *Assume that $D=l$ is an odd prime.*

If $l\equiv 1 \pmod 4$, then

$$a_p(2\beta)=a_p(-2\beta)=\frac{l-1}{4(l-2)}.$$

If $l\equiv 3 \pmod 4$, then

$$a_p(2\beta)=a_p(-2\beta)=\frac{l+1}{4l}.$$

Proof. By Lemma 4.3, $\Sigma^{(4)}\in\mathbb{Z}$. Applying the results on Σ, $\Sigma^{(2)}$ and Lemma 4.1 leads to the formulae. □

Lemma 4.5. *Given any nonzero integer D. Assume that $p=p(D,\beta,k,x)=\beta^2+(4Dx+2k+1)^2$ is a prime. For any odd prime factor l of D, if $l\mid\beta$, then $(\frac{l}{p})=1$ and*

$$l^{\frac{p-1}{4}}\equiv\begin{cases}1 \pmod p, & \text{if } l\equiv 1 \pmod 4,\\ -1 \pmod p, & \text{if } l\equiv 3 \pmod 4,\end{cases}$$

provided that $2\|\beta$;

$$l^{\frac{p-1}{4}}\equiv 1 \pmod p,$$

provided that $4\mid\beta$.

Proof. This proof follows similarly to that of Lemma 3.12. □

As in the case $a_p \equiv 2 \pmod 4$, for any nonzero integer D, we write

$$D = d\bar{d},$$

where $(d, \bar{d}) = 1$, and for any odd prime $l \mid d$, we have $l \mid \beta$, i.e., $\mathrm{Rad}(d) \mid \beta$ and $(\beta, \bar{d}) = 1$. Note that d $(d > 0)$ is odd. We adopt all notations from the case $a_p \equiv 2 \pmod 4$.

Theorem 4.6. *Assume that $D = d\bar{d}$ with D odd or $4 \| D$.*

(1) *If $d = 1$, then*

$$a_p(2\beta) = a_p(-2\beta) = \frac{1}{4}\left(1 - \frac{(-1)^{r+t}}{\tau(p_1 \cdots p_r l_1 \cdots l_t)}\right).$$

(2) *If $\bar{d}$ has no odd prime factor, then*

$$a_p(2\beta) = a_p(-2\beta) = 0.$$

(3) *If $\bar{d}$ has some odd prime factor, then*

$$a_p(2\beta) = a_p(-2\beta) = \frac{1}{4}\left(1 - \frac{(-1)^{r''+t''}}{\tau(\bar{d}_p \cdot \bar{d}_l)}\right).$$

Proof. (1) We always have $\Sigma^{(4)} \in \mathbb{Z}$, so we only need to compute Σ and $\Sigma^{(2)}$. Clearly, $\Sigma = 2\tau(D)$. We see that

$$\Sigma_I^{(2)} = \Sigma_{II}^{(2)} = (-1)^{r+t}\tau((q_1 \cdots q_s)^2) \cdot (l_1 \cdots l_t)^2.$$

Hence,

$$\Sigma^{(2)} = 2(-1)^{r+t}\tau((q_1 \cdots q_s)^2) \cdot (l_1 \cdots l_t)^2,$$

and (1) follows.

(2) By the assumption, for any odd prime $l \mid D$, we have $l \mid \beta$. For any prime $p = \beta^2 + x^2$, by Lemma 4.5, $D^{\frac{p-1}{4}} \equiv \pm 1 \pmod p$. On the other hand, applying the Gauss lemma (see Lemma 2.1) and

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2\alpha \pmod p,$$

we see that

$$a_p \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{4}} D^{\frac{p-1}{4}} \not\equiv \pm 2\beta \pmod p.$$

(3) We have

$$\Sigma = 2\phi(d)\Sigma(\bar{d}) = 2\phi(d)\tau(\bar{d})$$

and

$$\Sigma^{(2)} = 2\phi(d)\Sigma^{(2)}(\bar{d}) = 2(-1)^{r''+t''}\phi(d)\tau(\bar{d}_q{}^2 \cdot \bar{d}_l{}^2).$$

This proves the theorem. □

Lemma 4.7. *Let $p = \alpha^2 + \beta^2$ with $\alpha \equiv 1 \pmod 4$ and $\beta \equiv 2 \pmod 8$ be an odd prime. Then*

$$\left(\frac{2}{p}\right)_4 \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2\beta \pmod p. \tag{4.13}$$

Proof. Since $\beta \equiv 2 \pmod 8$ and $\alpha \equiv 1 \pmod 4$, by Lemma 2.6,

$$\left(\frac{2}{p}\right)_4 \equiv \frac{\beta}{\alpha} \pmod p.$$

However,

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2\alpha \pmod p.$$

This proves the congruence (4.13). □

The lemma above shows that for $2\|D$ and $2\|\beta$, determining the values of $a_p(2\beta, D)$ and $a_p(-2\beta, D)$ is reduced to some computations of the case for $D/2$.

Theorem 4.8. *Assume that* $2\|D$.

(1) *Assume that* $2\|\beta$, *and write* $\beta \equiv 2 \pmod 8$.

(1a) $d = 1$.

For $D = 2p_1 \cdots p_r (q_1 \cdots q_s)^2 (l_1 \cdots l_t)^3$,

$$a_p(2\beta) = \frac{1}{4}\left(1 + \frac{(-1)^{r+t}}{\tau(p_1 \cdots p_r l_1 \cdots l_t)} + \frac{2(-1)^{r_1+r_5+t_1+t_5+s}}{\tau(p_1 \cdots p_r q_1 \cdots q_s l_1 \cdots l_t)}\right),$$
$$a_p(-2\beta) = \frac{1}{4}\left(1 + \frac{(-1)^{r+t}}{\tau(p_1 \cdots p_r l_1 \cdots l_t)} - \frac{2(-1)^{r_1+r_5+t_1+t_5+s}}{\tau(p_1 \cdots p_r q_1 \cdots q_s l_1 \cdots l_t)}\right).$$

For $D = -2p_1 \cdots p_r (q_1 \cdots q_s)^2 (l_1 \cdots l_t)^3$,

$$a_p(2\beta) = \frac{1}{4}\left(1 + \frac{(-1)^{r+t}}{\tau(p_1 \cdots p_r l_1 \cdots l_t)} - \frac{2(-1)^{r_1+r_5+t_1+t_5+s}}{\tau(p_1 \cdots p_r q_1 \cdots q_s l_1 \cdots l_t)}\right),$$
$$a_p(-2\beta) = \frac{1}{4}\left(1 + \frac{(-1)^{r+t}}{\tau(p_1 \cdots p_r l_1 \cdots l_t)} + \frac{2(-1)^{r_1+r_5+t_1+t_5+s}}{\tau(p_1 \cdots p_r q_1 \cdots q_s l_1 \cdots l_t)}\right).$$

(1b) $\bar{d} = \pm 2$ (*equivalently* $\mathrm{Rad}(D) \mid \beta$):

$$a_p(2\beta) = \frac{1}{2}(1 + (-1)^{\frac{1}{2}(\frac{D}{2}-1)}), \quad a_p(-2\beta) = \frac{1}{2}(1 - (-1)^{\frac{1}{2}(\frac{D}{2}-1)}).$$

(2) *Assume* $4|\beta$. *Then*

$$a_p(2\beta) = a_p(-2\beta) = \frac{1}{4}\left(1 - \frac{(-1)^{r+t}}{\tau(p_1 \cdots p_r l_1 \cdots l_t)}\right).$$

Proof. Assume that $2\|D$ and $2\|\beta$. By Lemma 4.7,

$$\left(\frac{2}{p}\right)_4 \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2\beta \pmod p,$$

where $\beta \equiv 2 \pmod 8$. Hence, for a prime $p = \beta^2 + x^2$, we have $a_p \equiv (D/2)^{\frac{p-1}{4}} \pmod p$. It is reduced to calculate

$$\#\left\{p \in P(D/2, \beta) \,\middle|\, \left(\frac{D/2}{p}\right)_4 = 1\right\} \quad \text{and} \quad \#\left\{p \in P(D/2, \beta) \,\middle|\, \left(\frac{D/2}{p}\right)_4 = -1\right\}.$$

We have $\Sigma^{(2)}(D/2) = 2(-1)^{r+t}\tau((q_1 \cdots q_s)^2) \cdot (l_1 \cdots l_t)^2$ and

$$\Sigma_I^{(4)}(D/2) = \Sigma_{II}^{(4)}(D/2) = (-1)^{r_1+r_5+t_1+t_5+s+\delta} q_1 \cdots q_s l_1^2 \cdots l_t^2.$$

One can check that under our assumption,

$$a_p(2\beta) = \frac{1}{4}\left(1 + \frac{\Sigma^{(2)}}{\Sigma} + \frac{2\Sigma^{(4)}}{\Sigma}\right), \quad a_p(-2\beta) = \frac{1}{4}\left(1 + \frac{\Sigma^{(2)}}{\Sigma} - \frac{2\Sigma^{(4)}}{\Sigma}\right),$$

where $\Sigma = \Sigma(D/2)$ and $\Sigma^{(\sigma)} = \Sigma^{(\sigma)}(D/2)$ for $\sigma = 2, 4$. Using the formula, we obtain (1a).

(1b) is a consequence of Lemmas 4.5 and 4.7.

(2) For $4 \mid \beta$, we have $(\frac{2}{p}) = 1$ and $(\frac{2}{p})_4 = \pm 1$, which depends on $4\|\beta$ or $8 \mid \beta$. Hence,

$$\Sigma^4(D) = \pm\Sigma^4(D/2) \in \mathbb{Z},$$

so we only need to apply the known result on Σ and $\Sigma^{(2)}$. Recall that

$$\Sigma_I^{(2)} = \Sigma_{II}^{(2)} = (-1)^{r+t}\tau((q_1 \cdots q_s)^2) \cdot (l_1 \cdots l_t)^2.$$

This proves the theorem. □

Theorem 4.9. *Assume that* $8\|D$.

(1) *Assume that* $2\|\beta$, *and write* $\beta \equiv 2 \pmod 8$.

(1a) $d = 1$.

For $D = 8p_1\cdots p_r(q_1\cdots q_s)^2(l_1\cdots l_t)^3$,

$$a_p(2\beta) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)} - \frac{2(-1)^{r_1+r_5+t_1+t_5+s}}{\tau(p_1\cdots p_r q_1\cdots q_s l_1\cdots l_t)}\bigg),$$
$$a_p(-2\beta) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)} + \frac{2(-1)^{r_1+r_5+t_1+t_5+s}}{\tau(p_1\cdots p_r q_1\cdots q_s l_1\cdots l_t)}\bigg).$$

For $D = -8p_1\cdots p_r(q_1\cdots q_s)^2(l_1\cdots l_t)^3$,

$$a_p(2\beta) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)} + \frac{2(-1)^{r_1+r_5+t_1+t_5+s}}{\tau(p_1\cdots p_r q_1\cdots q_s l_1\cdots l_t)}\bigg),$$
$$a_p(-2\beta) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)} - \frac{2(-1)^{r_1+r_5+t_1+t_5+s}}{\tau(p_1\cdots p_r q_1\cdots q_s l_1\cdots l_t)}\bigg).$$

(1b) $\bar{d} = \pm 2$ (*equivalently* $\mathrm{Rad}(D) \mid \beta$):

$$a_p(2\beta) = \frac{1}{2}(1 - (-1)^{\frac{1}{2}(\frac{D}{8}-1)}), \quad a_p(-2\beta) = \frac{1}{2}(1 + (-1)^{\frac{1}{2}(\frac{D}{8}-1)}).$$

(2) *Assume* $4 \mid \beta$. *Then*

$$a_p(2\beta) = a_p(-2\beta) = \frac{1}{4}\bigg(1 - \frac{(-1)^{r+t}}{\tau(p_1\cdots p_r l_1\cdots l_t)}\bigg).$$

Proof. (1) For $2\|\beta$, we have $(\frac{2}{p}) = -1$, and hence, $(\frac{8}{p})_4 = -(\frac{2}{p})_4$. So the proof is reduced to that of Theorem 4.8. □

Theorem 4.10. *Assume* $2\|D$ *and* $\bar{d}$ *has some odd prime factor.*

(1) *If* $2\|\beta$, *writing* $\beta \equiv 2 \pmod 8$, *then for* $D > 0$,

$$a_p(2\beta) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)} + \frac{2(-1)^{r_1''+r_5''+t_1''+t_5''+s''+\frac{d-1}{2}}}{\tau(\bar{d}_p\cdot\bar{d}_q\cdot\bar{d}_l)}\bigg),$$
$$a_p(-2\beta) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)} - \frac{2(-1)^{r_1''+r_5''+t_1''+t_5''+s''+\frac{d-1}{2}}}{\tau(\bar{d}_p\cdot\bar{d}_q\cdot\bar{d}_l)}\bigg).$$

For $D < 0$,

$$a_p(2\beta) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)} - \frac{2(-1)^{r_1''+r_5''+t_1''+t_5''+s''+\frac{d-1}{2}}}{\tau(\bar{d}_p\cdot\bar{d}_q\cdot\bar{d}_l)}\bigg),$$
$$a_p(-2\beta) = \frac{1}{4}\bigg(1 + \frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)} + \frac{2(-1)^{r_1''+r_5''+t_1''+t_5''+s''+\frac{d-1}{2}}}{\tau(\bar{d}_p\cdot\bar{d}_q\cdot\bar{d}_l)}\bigg).$$

(2) *If* $4 \mid \beta$, *then*

$$a_p(2\beta) = a_p(-2\beta) = \frac{1}{4}\bigg(1 - \frac{(-1)^{r''+t''}}{\tau(\bar{d}_p\cdot\bar{d}_l)}\bigg).$$

Proof. (1) As in the proof of Theorem 4.8, we have

$$a_p(2\beta) = \frac{1}{4}\bigg(1 + \frac{\Sigma^{(2)}}{\Sigma} + \frac{2\Sigma^{(4)}}{\Sigma}\bigg), \quad a_p(-2\beta) = \frac{1}{4}\bigg(1 + \frac{\Sigma^{(2)}}{\Sigma} - \frac{2\Sigma^{(4)}}{\Sigma}\bigg),$$

where $\Sigma = \Sigma(D/2)$ and $\Sigma^{(\sigma)} = \Sigma^{(\sigma)}(D/2)$ for $\sigma = 2, 4$. A computation based on Lemma 4.5 shows that

$$\Sigma = 2\phi(d)\Sigma(\bar{d}) = 2\phi(d)\tau(\bar{d}),$$

$$\Sigma^{(2)} = 2\phi(d)\Sigma^{(2)}(\bar{d}) = 2(-1)^{r''+t''}\phi(d)\tau(\bar{d_q}^2 \cdot \bar{d_l}^2),$$
$$\Sigma^4 = 2\phi(d)\Sigma^{(2)}(\bar{d}) = 2(-1)^{r_1''+r_5''+t_1''+t_5''+s''+\frac{d-1}{2}+\delta}\phi(d)\tau(\bar{d_q}^2 \cdot \bar{d_l}^2).$$

So (1) follows.

(2) For $4 \mid \beta$, we have $\Sigma^4(D) \in \mathbb{Z}$. Now

$$\Sigma = 2\phi(d)\Sigma(\bar{d}) = 2\phi(d)\tau(\bar{d}), \quad \Sigma^{(2)} = 2\phi(d)\Sigma^{(2)}(\bar{d}) = 2(-1)^{r''+t''}\phi(d)\tau(\bar{d_q}^2 \cdot \bar{d_l}^2)$$

give the assertion of (2). □

Theorem 4.11. *Assume $8\|D$ and $\bar{d}$ has some odd prime factor.*

(1) *If $2\|\beta$, writing $\beta \equiv 2 \pmod 8$, then for $D > 0$,*

$$a_p(2\beta) = \frac{1}{4}\left(1 + \frac{(-1)^{r''+t''}}{\tau(\bar{d_p} \cdot \bar{d_l})} - \frac{2(-1)^{r_1''+r_5''+t_1''+t_5''+s''+\frac{d-1}{2}}}{\tau(\bar{d_p} \cdot \bar{d_q} \cdot \bar{d_l})}\right),$$
$$a_p(-2\beta) = \frac{1}{4}\left(1 + \frac{(-1)^{r''+t''}}{\tau(\bar{d_p} \cdot \bar{d_l})} + \frac{2(-1)^{r_1''+r_5''+t_1''+t_5''+s''+\frac{d-1}{2}}}{\tau(\bar{d_p} \cdot \bar{d_q} \cdot \bar{d_l})}\right).$$

For $D < 0$,

$$a_p(2\beta) = \frac{1}{4}\left(1 + \frac{(-1)^{r''+t''}}{\tau(\bar{d_p} \cdot \bar{d_l})} + \frac{2(-1)^{r_1''+r_5''+t_1''+t_5''+s''+\frac{d-1}{2}}}{\tau(\bar{d_p} \cdot \bar{d_q} \cdot \bar{d_l})}\right),$$
$$a_p(-2\beta) = \frac{1}{4}\left(1 + \frac{(-1)^{r''+t''}}{\tau(\bar{d_p} \cdot \bar{d_l})} - \frac{2(-1)^{r_1''+r_5''+t_1''+t_5''+s''+\frac{d-1}{2}}}{\tau(\bar{d_p} \cdot \bar{d_q} \cdot \bar{d_l})}\right).$$

(2) *If $4 \mid \beta$, then*

$$a_p(2\beta) = a_p(-2\beta) = \frac{1}{4}\left(1 - \frac{(-1)^{r''+t''}}{\tau(\bar{d_p} \cdot \bar{d_l})}\right).$$

Proof. The proof follows a similar approach to that of Theorem 4.10. □

5 The Hardy-Littlewood conjecture and the Lang-Trotter conjecture

Let r be a nonzero integer. Let $\rho(r) = 0$ if r is odd and $\rho(r) = 1$ if r is even. We have seen that under the assumption of the Hardy-Littlewood conjecture, the necessary and sufficient condition for

$$p(D, r, k, x) = r^2 + (4Dx + 2k + \rho(r))^2 = 16D^2x^2 + 8(2k + \rho(r))Dx + (2k + \rho(r))^2 + r^2$$

to represent infinitely many primes is $(D, (2k + \rho(r))^2 + r^2) = 1$. If k_1 and k_2 are two integers satisfying $(D, (2k_i + \rho(r))^2 + r^2) = 1$ for $i = 1, 2$, then the constants are the same (see the asymptotic formula (1.2) and the constant expression in the Hardy-Littlewood conjecture (1.3)). This constant is denoted by $\delta(D, r)$.

Lemma 5.1. *Let D and r be two non-zero integer. Then the necessary and sufficient conditions for $a_p(2r) = a_p(E_D, 2r) = 0$ are given in Tables 1 and 2.*

Proof. We see from the formulae for $a_p(2r)$ that the necessary conditions for $a_p(2r) = 0$ are $\tau(\bar{d_p} \cdot \bar{d_l}) = \tau(\bar{d_p} \cdot \bar{d_q} \cdot \bar{d_l}) = 3$. Hence, $\bar{d} = \pm 2^i \cdot 5, \pm 2^j \cdot 5^3, \pm 2^k \cdot 3, \pm 2^l \cdot 3^3$, where $i, j, k, l \in \{0, 1, 2, 3\}$. Then one can check case by case to obtain a full list given by Tables 1 and 2. □

Remark 5.2. For the elliptic curve $E_D : y^2 = x^3 + Dx$, it has bad reduction at a prime p if and only if $p \mid D$, where $a_p \neq 2r$ for any non-zero integer r. Hence, the assertion that there is no prime p with $a_p = 2r$ is equivalent to $a_p(2r) = a_p(E_D, 2r) = 0$.

Table 1 $\alpha \equiv 1 \pmod 4$

$D \equiv 1 \pmod 4$ or $\frac{D}{4} \equiv 3 \pmod 4$	$r_3 + r_5 + t_3 + t_5 \equiv 1 \pmod 2$	$a_p(2\alpha) = 0$
$\bar{d} = \pm 1, \pm 4$	$r_3 + r_5 + t_3 + t_5 \equiv 0 \pmod 2$	$a_p(-2\alpha) = 0$
$D \equiv 1 \pmod 4$	$r'_3 + r'_5 + t'_3 + t'_5 \equiv 1 \pmod 2$	$a_p(2\alpha) = 0$
$\bar{d} = \pm 5, \pm 3, \pm 5^3, \pm 3^3$	$r'_3 + r'_5 + t'_3 + t'_7 \equiv 0 \pmod 2$	$a_p(-2\alpha) = 0$
$\frac{D}{4} \equiv 3 \pmod 4$	$r'_3 + r'_5 + t'_3 + t'_5 \equiv 1 \pmod 2$	$a_p(2\alpha) = 0$
$\bar{d} = \pm 4 \cdot 5, \pm 4 \cdot 3, \pm 4 \cdot 5^3, \pm 4 \cdot 3^3$	$r'_3 + r'_5 + t'_3 + t'_7 \equiv 0 \pmod 2$	$a_p(-2\alpha) = 0$

Table 2 $\beta \equiv 0 \pmod 2$

D odd or $4 \,\|\|\, D$		
$\mathrm{Rad}(D) \mid \beta$	$a_p(2\beta) = a_p(-2\beta) = 0$	
$2 \,\|\|\, D$ or $8 \,\|\|\, D$, $\beta \equiv 2 \pmod 8$		
$\bar{d} = \pm 2$	$\frac{D}{2} \equiv 1 \pmod 4$	$a_p(-2\beta) = 0$
	$\frac{D}{2} \equiv 3 \pmod 4$	$a_p(2\beta) = 0$
$\bar{d} = \pm 8$	$\frac{D}{8} \equiv 1 \pmod 4$	$a_p(2\beta) = 0$
	$\frac{D}{8} \equiv 3 \pmod 4$	$a_p(-2\beta) = 0$
$\bar{d} = 2 \cdot 5, 2 \cdot 5^3, -2 \cdot 3, -2 \cdot 3^3,$ $-8 \cdot 5, -8 \cdot 5^3, 8 \cdot 3, 8 \cdot 3^3$	$d \equiv 1 \pmod 4$	$a_p(2\beta) = 0$
	$d \equiv 3 \pmod 4$	$a_p(-2\beta) = 0$
$\bar{d} = 2 \cdot 3, 2 \cdot 3^3, -2 \cdot 5, -2 \cdot 5^3,$ $-8 \cdot 3, -8 \cdot 3^3, 8 \cdot 5, 8 \cdot 5^3$	$d \equiv 1 \pmod 4$	$a_p(-2\beta) = 0$
	$d \equiv 3 \pmod 4$	$a_p(2\beta) = 0$

Theorem 5.3. *The Hardy-Littlewood conjecture implies the Lang-Trotter conjecture for $y^2 = x^3 + Dx$. Moreover,*

$$\pi_{E_D,2r}(N) \sim \delta(D,r) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty,$$

where the constant $\delta(D,r) = \delta(1,0,r^2)a_p(E_D,2r)$, in which the constant $\delta(1,0,r^2)$ is given by the Hardy-Littlewood conjecture and $a_p(E_D,2r)$, is given explicitly in theorems in Section 3 when r is odd and Section 4 when r is even. In particular, if D and r are not in Table 1 or Table 2, then the constant $\delta(D,r)$ is positive.

Conversely, if the Lang-Trotter conjecture holds for some D and r with the positive constant $C_{E_D,2r}$, then the polynomial $x^2 + r^2$ represents infinitely many primes.

Proof. Since there are only finite primes with $p \mid \Delta_{E_D}$, up to a constant,

$$\begin{aligned}\pi_{E_D,2r}(N) &= \sum_{p \leqslant N, p \nmid \Delta_{E_D}, a_p = 2r} 1 \\ &= \#\{p \mid a_p(E_D) = 2r, p \in Q(r,N)\} \\ &= a_p(E_D,2r)\#Q(r,N) \\ &\sim a_p(E_D,2r)\delta(1,0,r^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty.\end{aligned}$$

Conversely, if $a_p(E_D) = 2r$, then we must have $p = x^2 + r^2$, and hence the assumption that the Lang-Trotter conjecture holds for E_D and r with the positive constant $C_{E_D,2r}$ implies that $x^2 + r^2$ represents infinitely many primes. □

Example 5.4. (1) $D = 1$. We have $a_p = 2\alpha$ if and only if $p = \alpha^2 + x^2$. In particular, $a_p \not\equiv 0 \pmod 4$. Hence,

$$\pi_{E_1,2\alpha}(N) \sim \delta(1,0,\alpha^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty.$$

In addition, for $r \equiv -1 \pmod 4$ or $r \equiv 0 \pmod 2$, we have $\delta(1, 2r) = 0$.

(2) $D = -1$. We have

$$a_p = \begin{cases} 2\alpha, & \text{if } p = \alpha^2 + x^2 \equiv 1 \pmod 8, \\ -2\alpha, & \text{if } p = \alpha^2 + x^2 \equiv 5 \pmod 8. \end{cases}$$

Hence,

$$\pi_{E_{-1},2\alpha}(N) \sim \frac{1}{2}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty$$

and

$$\pi_{E_{-1},-2\alpha}(N) \sim \frac{1}{2}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty.$$

In addition, for $r \equiv 0 \pmod 2$, we have $\delta(1, 2r) = 0$.

(3) $D = 2$. We have

$$a_p = \begin{cases} 2\alpha, & \text{if } p = \alpha^2 + (8x)^2, \\ -2\alpha, & \text{if } p = \alpha^2 + (8x + 4)^2. \end{cases}$$

When $\beta \equiv 2 \pmod 8$, $a_p = 2\beta$ always holds for $p = \beta^2 + x^2$; in particular, $a_p \neq -2\beta$. Hence,

$$\pi_{E_2,2\alpha}(N) \sim \frac{1}{4}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty,$$

$$\pi_{E_2,-2\alpha}(N) \sim \frac{1}{4}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty$$

and

$$\pi_{E_2,2\beta}(N) \sim \delta(1, 0, \beta^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty.$$

Moreover, $\delta(2, -2\beta) = 0$, and for $\beta \equiv 0 \pmod 2$, $\delta(2, 2\beta) = 0$.

(4) $D = -2$. We also have

$$a_p = \begin{cases} 2\alpha, & \text{if } p = \alpha^2 + (8x)^2, \\ -2\alpha, & \text{if } p = \alpha^2 + (8x + 4)^2. \end{cases}$$

Hence,

$$\pi_{E_{-2},2\alpha}(N) \sim \frac{1}{4}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty,$$

$$\pi_{E_{-2},-2\alpha}(N) \sim \frac{1}{4}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty$$

and

$$\pi_{E_{-2},-2\beta}(N) \sim \delta(1, 0, \beta^2) \cdot \frac{\sqrt{N}}{\log N} \quad \text{as } N \to \infty.$$

Moreover, $\delta(-2, 2\beta) = 0$, and for $\beta \equiv 0 \pmod 2$, $\delta(2, 2\beta) = 0$.

(5) $D = -21$. This is the case where $D \equiv 3 \pmod 4$. All eight constants, which appear in the following asymptotic formulae, can be computed by theorems in Sections 3 and 4.

(a) $3 \nmid \alpha, 7 \nmid \alpha$: $\pi_{E_{-21},\pm 2\alpha}(N) \sim \frac{11}{42}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N}$ as $N \to \infty$.

(b) $3 \mid \alpha, 7 \nmid \alpha$: $\pi_{E_{-21},\pm 2\alpha}(N) \sim \frac{3}{14}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N}$ as $N \to \infty$.

(c) $3 \nmid \alpha, 7 \mid \alpha$: $\pi_{E_{-21},\pm 2\alpha}(N) \sim \frac{1}{6}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N}$ as $N \to \infty$.

(d) $3 \mid \alpha, 7 \mid \alpha$: $\pi_{E_{-21},\pm 2\alpha}(N) \sim \frac{1}{2}\delta(1, 0, \alpha^2) \cdot \frac{\sqrt{N}}{\log N}$ as $N \to \infty$.

(e) $3\nmid\beta, 7\nmid\beta$: $\pi_{E_{-21},\pm2\beta}(N)\sim\frac{5}{21}\delta(1,0,\beta^2)\cdot\frac{\sqrt{N}}{\log N}$ as $N\to\infty$.

(f) $3\mid\beta, 7\nmid\beta$: $\pi_{E_{-21},\pm2\beta}(N)\sim\frac{2}{7}\delta(1,0,\beta^2)\cdot\frac{\sqrt{N}}{\log N}$ as $N\to\infty$.

(g) $3\nmid\beta, 7\mid\beta$: $\pi_{E_{-21},\pm2\beta}(N)\sim\frac{1}{3}\delta(1,0,\beta^2)\cdot\frac{\sqrt{N}}{\log N}$ as $N\to\infty$.

(h) $3\mid\beta, 7\mid\beta$: the constant is $\delta(-21,\pm2\beta)=0$. So we omit the asymptotic formula since it is trivial.

(6) $D=-n^2$, where n is a non-zero integer. The curve $y^2=x^3-n^2x$ is called the congruent elliptic curve if n is square-free. Let $p\nmid n$ be an odd prime. Then

$$a_p=\begin{cases}2\alpha, & \text{if } p=\alpha^2+x^2 \text{ with } \left(\dfrac{2n}{p}\right)=1,\\ -2\alpha, & \text{if } p=\alpha^2+x^2 \text{ with } \left(\dfrac{2n}{p}\right)=-1\end{cases}$$

and $a_p\neq 2\beta$, if $2\mid\beta$. Hence, for $(n,\alpha)=1$,

$$\pi_{E_{n^2},2\alpha}(N)\sim\frac{1}{2}\delta(1,0,\alpha^2)\cdot\frac{\sqrt{N}}{\log N}\quad\text{as } N\to\infty$$

and

$$\pi_{E_{n^2},-2\alpha}(N)\sim\frac{1}{2}\delta(1,0,\alpha^2)\cdot\frac{\sqrt{N}}{\log N}\quad\text{as } N\to\infty.$$

The constant is $\delta(n^2,\pm2\beta)=0$ if $(n,\beta)=1$. When $(n,\alpha)>1$ or $(n,\beta)>1$, one can apply theorems in Sections 3 and 4 to calculate the constants, which are omitted here.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 12231009 and 11971224) and the Ministry of Science and Technology of China (Grant No. 2020YFA0713800). The author thanks Professor Barry Mazur, who asked the author about the density of $a_p=2$ for $p=1+x^2$. This problem has motivated the author to write this paper. The author thanks the referees for their helpful suggestions which have been incorporated herein. The author thanks Xia Wu for pointing out $D=-268912=-2^4\cdot7^5$ (in the notation of [18], $a_p(1)=0$) which was missing in [18, Theorem 4.10]. Also, an exception $D=67228=4\cdot7^5$ (in notation of [18], $a_p(\omega^2)=0$) should be added to [18, Theorem 4.10].

References

1 Babinkostova L, Bahr J C, Kim Y H, et al. Anomalous primes and the elliptic Korselt criterion. J Number Theory, 2019, 201: 108–123
2 Berndt B C, Evans R J, Williams K S. Gauss and Jacobi Sums. New York: Wiley, 1998
3 Clozel L, Harris M, Taylor R. Automorphy for some l-adic lifts of automorphic mod l Galois representations. Publ Math Inst Hautes Études Sci, 2008, 108: 1–181
4 Cojocaru A C. Primes, elliptic curves and cyclic groups. In: Analytic Methods in Arithmetic Geometry. Contemporary Mathematics, vol. 740. Providence: Amer Math Soc, 2019, 1–69
5 Deuring M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh Math Semin Univ Hambg, 1941, 14: 197–272
6 Elkies N D. The existence of infinitely many supersingular primes for every elliptic curve over Q. Invent Math, 1987, 89: 561–567
7 Greenberg R. Iwasawa theory for elliptic curves. In: Proceedings of the 3rd Session of the Centro-Internazionale-Matematico-Estivo. Lecture Notes in Mathematics, vol. 1716. Cham: Springer, 1999, 51–144
8 Hardy G H, Littlewood J E. Some problems of partitio numberorum III. Acta Math, 1923, 44: 1–70
9 Harris M, Shepherd-Barron N, Taylor R. A family of Calabi-Yau varieties and potential automorphy. Ann of Math (2), 2010, 171: 779–813
10 Ireland K, Rosen M. A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics, vol. 84. Berlin: Springer-Verlag, 1972
11 Iwaniec H. Almost-primes represented by quadratic polynomials. Invent Math, 1978, 47: 171–188
12 Ji Q, Qin H. CM elliptic curves and primes captured by quadratic polynomials. Asian J Math, 2014, 18: 707–726
13 Jones N. Averages of elliptic curve constants. Math Ann, 2009, 345: 685–710

14 Juyal A, Moody D, Roy B. On ranks of quadratic twists of a Mordell curve. Ramanujan J, 2022, 59: 31–50
15 Kundu D, Ray A. Statistics for Iwasawa invariants of elliptic curves. Trans Amer Math Soc, 2021, 374: 7945–7965
16 Lang S, Trotter H. Frobenius Distributions in GL_2-Extensions. Lecture Notes in Mathematics, vol. 504. Berlin: Springer-Verlag, 1976
17 Mazur B. Rational points of abelian varieties with values in towers of number fields. Invent Math, 1972, 18: 183–266
18 Qin H R. Anomalous primes of the elliptic curve $E_D : y^2 = x^3 + D$. Proc Lond Math Soc (3), 2016, 112: 415–453
19 Qin H R. The Mazur conjecture, the Lang-Trotter conjecture and the Hardy-Littlewood conjecture. In: Forty Years of Algebraic Groups, Algebraic Geometry, and Representation Theory. East China Normal University Scientific Reports, vol. 16. Singapore: World Sci Publ, 2023, 315–329
20 Schmitt S, Zimmer H G. Elliptic Curves. New York: Walter de Gruyter, 2003
21 Serre J P. Quelques applications du theoreme de densite de Chebotarev. Publ Math Inst Hautes Études Sci, 1981, 54: 123–201
22 Serre J P. Abelian l-Adic Representations and Elliptic Curves. New York: CRC Press, 1997
23 Shimura G. Introduction to the Arithmetic Theory of Automorphic Functions. Princeton: Princeton Univ Press, 1971
24 Silverman J H. The Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1986
25 Silverman J H. Advanced Topics in the Arithmetic of Elliptic Curves. New York: Springer-Verlag, 1994
26 Taylor R. Automorphy for some l-adic lifts of automorphic mod l Galois representations. II. Publ Math Inst Hautes Études Sci, 2008, 108: 183–239