ASIAN J. MATH.
Vol. 18, No. 4, pp. 707–726, September 2014

007

CM ELLIPTIC CURVES AND PRIMES CAPTURED BY QUADRATIC POLYNOMIALS*

QINGZHONG JI† AND HOURONG QIN†‡

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication. For a prime p, some formulas for $a_p = p + 1 - \sharp E(\mathbb{F}_p)$ are given in terms of the binomial coefficients. We show that the equality $a_p = r$ holds for some fixed integer r if and only if a certain quadratic polynomial represents the prime p. In particular, for $E : y^2 = x^3 + x$, $a_p = 2$ holding for an odd prime p if and only if p is of the form $n^2 + 1$ and for $E : y^2 = x^3 - 11x + 14$, $a_p = 2$ holding for an odd prime p if and only if p is of the form $(4n)^2 + 1$; $a_p = -2$ holding for an odd prime p if and only if p is of the form $(4n + 2)^2 + 1$. In some CM cases the Lang-Trotter conjecture and the Hardy-Littlewood conjecture are equivalent.

Key words. CM elliptic curve, anomalous prime, Hardy-Littlewood conjecture.

AMS subject classifications. 11G05, 11G15, 11N32.

1. Introduction. Let E be an elliptic curve defined over a number field K and let v be a prime of K, k_v the residue field of K at v. We use $\tilde{E_v}$ for the reductive curve of E if E has good reduction at v. If the characteristic of k_v divides $|\tilde{E_v}(k_v)|$, then v is called an anomalous prime for E ([6]). Hence v is an anomalous prime if and only if E has good reduction at v and the trace of the Frobenius automorphism associated to $\tilde{E_v}$ is congruent to 1 mod p, where p is the characteristic of k_v.

Assume that E has good ordinary reduction at all primes dividing p. Let L/K be a $\mathbb{Z}_p$-extension with Galois group $\Gamma = \mathrm{Gal}(L/K)$ and with the sequence of subfields

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty = L = \bigcup_{n=0}^{\infty} K_n.$$

Mazur ([6]) constructed a Γ-module $H = H_{(L/K,E)}$ for any admissible pair $(L/K, E)$ and established the following exact sequence (modulo finite groups whose orders are bounded, independent of n):

$$0 \longrightarrow E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^{\Gamma_n} \longrightarrow Ш_E(K_n)(p^\infty) \longrightarrow 0 \ \ (n \geq 0)$$

where $Ш_E(K_n)(p^\infty)$ is the p-primary component of the Shafarevich-Tate group of E over K_n.

For the anomalous primes of E, Mazur ([6]) proved that the Γ-module H is necessarily of infinite order. We refer to ([3], [6]) for extensive discussion of anomalous primes. Denote by $\Sigma_E(K)$ the set of anomalous primes v for E over a number field K. Mazur proved the following result.

THEOREM 1.1. ([6]) (1) *If $E(\mathbb{Q})$ has nontrivial torsion points, then the set $\sum_E(\mathbb{Q})$ consists either of a single element, or none, or else is contained in the set* $\{2, 3, 5\}$.

*Received April 14, 2013; accepted for publication June 18, 2013. Supported by NSFC (Nos. 11171141, 11471154, 11271177), NSFJ (Nos. BK2010007, BK2010362), PAPD and the Cultivation Fund of the Key Scientific and Technical Innovation Project, Ministry of Education of China (No.708044).
†Department of Mathematics, Nanjing University, Nanjing 210093, P. R. China ({qingzhji; hrqin}@nju.edu.cn).
‡Corresponding author.

(2) *Given any finite set of primes P, there is an elliptic curve E defined over $\mathbb{Q}$, such that $\Sigma_E(\mathbb{Q})$ contains P.*

Further, Mazur ([6]) asked the following question:

Q1: *Can an elliptic curve possess an infinite number of anomalous primes?*

Let D be a rational integer which is neither a square nor a cube in $\mathbb{Q}(\sqrt{-3})$. There is a good discussion of this question for the curve $E_D: \ y^2 = x^3 + D$ in the introduction of [6]. Mazur conjectured that 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. Mazur proposed the following conjecture.

Mazur Conjecture ([6])

$$A.P._D(N) \sim c\frac{\sqrt{N}}{\log N}, \ \text{ as } N \longrightarrow \infty, \tag{1}$$

for some positive constant c.

Later, Lang and Trotter ([5]) generalized this conjecture. Let E be an elliptic curve over $\mathbb{Q}$ and $r \in \mathbb{Z}$ a fixed integer. Define the prime-counting function

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

If $r = 0$ then assume additionally that E has no complex multiplication.

Lang-Trotter Conjecture ([5])

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

as $x \longrightarrow \infty$, where $C_{E,r}$ is a specific non-negative constant. If the constant $C_{E,r} = 0$, we interpret the asymptotic to mean that there are only finitely many primes p for which $a_p = r$.

Note that both the Mazur conjecture and the Lang-Trotter conjecture have the same asymptotic shape. The well-known Hardy-Littlewood Conjecture, below, predicts that the number of primes of the form $ax^2 + bx + c$ also has the same asymptotic shape.

Suppose that a, b, c are integers and a is positive; that $(a, b, c) = 1$; that $a + b$ and c are not both even; and that $D = b^2 - 4ac$ is not a square. Let $P(n)$ denote the number of primes less than n which are of the form $ax^2 + bx + c$.

Hardy-Littlewood Conjecture ([4])

$$P(n) \sim \delta\frac{\sqrt{n}}{\log n}, \ \text{ as } n \longrightarrow \infty,$$

where $\delta = \delta(a, b, c)$ is a positive constant. In particular, there are infinitely many primes of the form $ax^2 + bx + c$.

The Hardy-Littlewood Conjecture has not been proved even for a single polynomial. For example, at present, we do not know whether the polynomial $x^2 + 1$ represents infinitely many primes. Qin[8] establishes a connection between the Mazur conjecture and the Hardy-Littlewood conjecture.

Let E be an elliptic curve defined over $\mathbb{Q}$. As usual, for a prime p where E has good reduction, we use a_p for the trace of the Frobenius automorphism ϕ_p, *i.e.*, $a_p = 1 + p - \sharp\tilde{E}_p(\mathbb{F}_p)$. Then ϕ_p satisfies the equation

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

The polynomial $L_p(E/\mathbb{Q}, T) = 1 - a_p T + pT^2$ is called the *local L-series* of E at p. By the Hasse inequality, $|a_p| \leq 2\sqrt{p}$.

In the complex multiplication case, the distribution of $\frac{a_p}{2\sqrt{p}} \in (-1, 1)$ is described by Deuring ([2]), and in the non-complex multiplication case, it is described by the Sato-Tate Conjecture which is proved by L. Clozel, M. Harris, N. Shepherd-Barron and R. Taylor.

We find that in some CM cases the Lang-Trotter conjecture and the Hardy-Littlewood conjecture are equivalent.

Let E be an elliptic curve defined over a number field K and let $0 \neq r \in \mathbb{Z}$ be an integer. Denote by $\Sigma_E^{(r)}(K)$ the set of all primes v where E has good reduction such that $a_v(E/K) \equiv r \pmod{p}$, where p is the characteristic of k_v. We may ask the following question:

Q2: *Let r be any nonzero integer. Is there an elliptic curve E defined over $\mathbb{Q}$ such that the set $\Sigma_E^{(r)}(\mathbb{Q})$ is an infinite set?*

In this paper we consider this question for elliptic curves over $\mathbb{Q}$ with complex multiplication by an order $R = \mathbb{Z} + fR_K$ of conductor f in a quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$ of discriminant D. For a given CM elliptic curve $E/\mathbb{Q}$, we obtain some formulas for a_p in terms of the binomial coefficients, which enable us to prove the equality $a_p(E/\mathbb{Q}) = r$ holds if and only if a certain quadratic polynomial represents the prime p. In particular, for $E : y^2 = x^3 + x$, $a_p = 2$ holds for an odd prime p if and only if p is of the form $n^2 + 1$. Obviously, for an odd prime $p = n^2 + 1$, then n is even, which we may characterize as being exactly divisible by 2. More precisely, we show that for $E : y^2 = x^3 - 11x + 14$, $a_p = 2$ holds for an odd prime p if and only if p is of the form $(4n)^2 + 1$; $a_p = -2$ holds for an odd prime p if and only if p is of the form $(4n + 2)^2 + 1$.

2. Twist elliptic curves. Let E be an elliptic curve defined over $\mathbb{Q}$ and choose a model of E of the form:

$$y^2 = f(x) \tag{3}$$

with a monic cubic polynomial $f(x) \in \mathbb{Z}[x]$. Then the (quadratic) *twist* of E by a nonzero rational number d is

$$E_{(d)} : \ \ y^2 = d^3 f(x/d).$$

For a discussion on the twist of elliptic curves defined over an arbitrary perfect field, see [16].

The following two lemmas are useful for us to compute a_p.

LEMMA 2.1. ([14] Proposition 3.21) *Let E be an ordinary elliptic curve defined over a finite field $\mathbb{F}_q$ with q elements and let E' be a twist of E. Then*

$$\sharp E(\mathbb{F}_q) + \sharp E'(\mathbb{F}_q) = 2q + 2. \tag{4}$$

LEMMA 2.2. ([2]) *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by an imaginary quadratic field K. Let p be a prime where E has good reduction. Then*

$$a_p = \begin{cases} 0, & \text{if } p \text{ is not a norm,} \\ \pi + \bar{\pi}, & \text{if } p = \pi\bar{\pi} \text{ is a norm,} \end{cases}$$

where the endomorphism $[\pi]$ has the same effect as does the Frobenius automorphism

$$\phi_p : (x, y) \longrightarrow (x^p, y^p) \pmod p.$$

The foregoing results allow us to give a preliminary criterion to determine $\Sigma_E^{(r)}(K)$.

LEMMA 2.3. *Let E be an elliptic curve defined over $\mathbb{Q}$. For a square-free integer d, let $\mathfrak{p}$ be a prime of $K = \mathbb{Q}(\sqrt{d})$ where E has good ordinary reduction. Assume that $\mathfrak{p}|p$ and $p \geq 3$. Then for a given integer $r \in \mathbb{Z}$, $\mathfrak{p} \in \Sigma_E^{(r)}(K)$ if and only if one of the following conditions holds*:

(1) $p|d$ *and* $p \in \Sigma_E^{(r)}(\mathbb{Q})$;
(2) $(\frac{d}{p}) = 1$ *and* $p \in \Sigma_E^{(r)}(\mathbb{Q})$;
(3) $(\frac{d}{p}) = -1$ *and* $a_p^2 \equiv r \pmod p$.

Proof. (i) Assume that $p|d$ or $(\frac{d}{p}) = 1$. Then $O_K/\mathfrak{p} = \mathbb{F}_p$. Hence $\tilde{E}(\mathbb{F}_p) = \tilde{E}(O_K/\mathfrak{p})$, and

$$p \in \Sigma_E^{(r)}(\mathbb{Q}) \Leftrightarrow \mathfrak{p} \in \Sigma_E^{(r)}(K).$$

(ii) Assume that $(\frac{d}{p}) = -1$. Then p is inertia in K. Hence $\mathfrak{p} = pO_K$ is a prime and $O_K/\mathfrak{p} \cong \mathbb{F}_{p^2}$.

Let α and β be the roots of the equation (2). Then

$$a_p = a_p(E/\mathbb{Q}) = 1 + p - \sharp\tilde{E}(\mathbb{F}_p) = \alpha + \beta, \ \ p = \alpha\beta.$$

Hence

$$a_\mathfrak{p} = a_\mathfrak{p}(E/K) = \alpha^2 + \beta^2 = a_p^2 - 2p.$$

Therefore

$$\mathfrak{p} \in \Sigma_E^{(r)}(K) \Leftrightarrow a_\mathfrak{p} \equiv r \pmod p \Leftrightarrow a_p^2 \equiv r \pmod p.$$

□

COROLLARY 2.4. *Under assumptions in Lemma 2.3, $\mathfrak{p} \in \Sigma_E(K)$ if and only if one of the following conditions holds*:

(1) $p \in \Sigma_E(\mathbb{Q})$;
(2) $(\frac{d}{p}) = -1$ *and*

$$a_p = a_p(E/\mathbb{Q}) = \begin{cases} -1, & \text{if } p \geq 7; \\ -1 \text{ or } p - 1, & \text{if } p = 3, 5. \end{cases}$$

Proof. Note that

$$a_p^2 \equiv 1 \pmod p \Leftrightarrow a_p \equiv \pm 1 \pmod p.$$

Hence $p \in \Sigma_E(\mathbb{Q})$ if $a_p \equiv 1 \pmod p$.

On the other hand, since $|a_p| \leq 2\sqrt{p}$,

$$a_p \equiv -1 \pmod p \Leftrightarrow a_p = \begin{cases} -1, & \text{if } p \geq 7; \\ -1 \text{ or } p-1, & \text{if } p = 3, 5. \end{cases}$$

This completes the proof. □

LEMMA 2.5. *Let E be an elliptic curve defined over $\mathbb{Q}$ of the form (3), $E_{(d)}$ the twist curve of E by a square-free integer d. Let p be an odd prime where both E and $E_{(d)}$ have good ordinary reduction. Then*

(1) $a_p(E_{(d)}) \equiv (\frac{d}{p})a_p(E) \pmod p$, *i.e., for any $r \in \mathbb{Z}$, we have $p \in \Sigma^{(r)}_{E_{(d)}}(\mathbb{Q})$ if and only if one of the following conditions holds*:

(i) $(\frac{d}{p}) = 1$ *and* $p \in \Sigma^{(r)}_E(\mathbb{Q})$.

(ii) $(\frac{d}{p}) = -1$ *and* $p \in \Sigma^{(-r)}_E(\mathbb{Q})$.

(2) *Assume that E has complex multiplication by $K = \mathbb{Q}(\sqrt{d})$. Then*

$$a_p(E_{(d)}) \equiv a_p(E) \pmod p,$$

i.e., for any $r \in \mathbb{Z}$, we have

$$\Sigma^{(r)}_E(\mathbb{Q}) = \Sigma^{(r)}_{E_{(d)}}(\mathbb{Q}).$$

Proof. (1) (i) If $(\frac{d}{p}) = 1$, then $\tilde{E} \cong \tilde{E}_{(d)}$ over $\mathbb{F}_p$. Hence $a_p(E/\mathbb{Q}) = r$ if and only if $a_p(E_{(d)}/\mathbb{Q}) = r$.

(ii) If $(\frac{d}{p}) = -1$, then $\tilde{E}_{(d)}$ is a twist of $\tilde{E}$ over $\mathbb{F}_p$. By Lemma 2.1, we have

$$a_p(E/\mathbb{Q}) + a_p(E_{(d)}/\mathbb{Q}) = 0.$$

Hence

$$a_p(E_{(d)}/\mathbb{Q}) \equiv r \pmod p \iff a_p(E/\mathbb{Q}) \equiv -r \pmod p.$$

(2) Both E and $E_{(d)}$ have complex multiplication by $K = \mathbb{Q}(\sqrt{d})$, hence $a_p(E) = a_p(E_{(d)}) = 0$ for all primes p with $(\frac{d}{p}) = -1$. Therefore the result $\Sigma^{(r)}_E(\mathbb{Q}) = \Sigma^{(r)}_{E_{(d)}}(\mathbb{Q})$ follows from (1). □

COROLLARY 2.6. *Assume that $\Sigma_E(\mathbb{Q})$ is finite and $\Sigma_E(\mathbb{Q}(\sqrt{d}))$ is infinite for some square-free integer d. Then $\Sigma_{E_{(d)}}(\mathbb{Q})$ is infinite.*

Proof. By the assumption and Corollary 2.4,

$$\{p \text{ is an odd prime} \mid (\frac{d}{p}) = -1 \text{ and } a_p(E/\mathbb{Q}) \equiv -1 \pmod p\}$$

is infinite. Hence $\Sigma_{E_{(d)}}(\mathbb{Q})$ is infinite by Lemma 2.5. □

THEOREM 2.7. *The following statements are equivalent*:

(1) *There is an elliptic curve E defined over $\mathbb{Q}$ such that the set $\Sigma_E(\mathbb{Q})$ is infinite.*

(2) *There is an elliptic curve E defined over $\mathbb{Q}$ such that the set $\Sigma_E(\mathbb{Q}(\sqrt{d}))$ is infinite for some nonzero rational number d.*

Proof. Indeed, that (1) implies (2) is trivial. By Corollary 2.4 and Lemma 2.5, (2) also implies (1). □

3. Main results. Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication. Write $R = \mathrm{End}(E)$. Then R is an order of some imaginary quadratic field K. The theory of complex multiplication tells us that the j-invariant $j(E)$ is in $\mathbb{Q}$ if and only if K has class number 1. It is well known that there are nine imaginary quadratic fields with class number 1. Let R_K be the ring of integers of K. Then the orders of K are precisely the rings $\mathbb{Z} + fR_K$ for integers $f > 0$. The integer f is called the conductor of the order. The following lemma describes all elliptic curves defined over $\mathbb{Q}$ with complex multiplication up to isomorphism over $\bar{\mathbb{Q}}$.

LEMMA 3.1. ([15], [16]) *There are exactly thirteen isomorphism classes of elliptic curves over $\bar{\mathbb{Q}}$ with complex multiplication and with the j-invariant $j(E)$ in $\mathbb{Q}$. The following table 3.1 gives the j-invariant and a representative elliptic curve E over $\mathbb{Q}$ for each isomorphism class, together with the minimal discriminant Δ_E and conductor N_E of E.*

Discriminant $-D$ of K	conductor f of R	j-invariant of E	Minimal Weierstrass equation of E over $\mathbb{Q}$	Δ_E	N_E
-3	1	0	$y^2+y=x^3$	-3^3	3^3
	2	$2^4 3^3 5^3$	$y^2=x^3-15x+22$	$2^8 3^3$	$2^2 3^3$
	3	$-2^{15} 3\cdot 5^3$	$y^2+y=x^3-30x+63$	-3^5	3^3
-4	1	$2^6 3^3$	$y^2=x^3+x$	2^6	2^6
	2	$2^3 3^3 11^3$	$y^2=x^3-11x+14$	2^9	2^5
-7	1	$-3^3 5^3$	$y^2+xy=x^3-x^2-2x-1$	7^3	7^2
	2	$3^3 5^3 17^3$	$y^2=x^3-595x+5586$	$2^{12} 7^3$	$2^4 7^2$
-8	1	$2^6 5^3$	$y^2=x^3+4x^2+2x$	2^9	2^8
-11	1	-2^{15}	$y^2+y=x^3-x^2-7x+10$	11^3	11^2
-19	1	$-2^{15} 3^3$	$y^2+y=x^3-38x+90$	19^3	19^2
-43	1	$-2^{18} 3^3 5^3$	$y^2+y=x^3-860x+9707$	43^3	43^2
-67	1	$-2^{15} 3^3 5^3 11^3$	$y^2+y=x^3-7370x+243528$	67^3	67^2
-163	1	$-2^{18} 3^3 5^3 23^3 29^3$	$y^2+y=x^3-2174420x+1234136692$	163^3	163^2

TABLE 3.1

It is easy to see that $E: y^2+y=x^3$ is isomorphic to $E': \ y^2 = x^3 + \frac{1}{4}$ and the twist of E' by 2 will be $E'': y^2 = x^3 + 2$. Mazur's conjecture suggests a formulation for anomalous primes of E'' (See [8]). In the rest of the paper, we shall discuss the remaining twelve elliptic curves listed in the above table. For convenience, we label these as follows.

$$\begin{aligned}
&E_1: \ y^2 = x^3 + x \text{ (Theorem 3.11, Corollary 3.12, Corollary 3.13)},\\
&E_2: \ y^2 = x^3 - 11x + 14 \text{ (Theorem 3.14, Corollary 3.15)},\\
&E_3: \ y^2 = x^3 + 4x^2 + 2x \text{ (Theorem 3.18, Corollary 3.19)},\\
&E_4: \ y^2 = x^3 - 15x + 22 \text{ (Theorem 3.21, Corollary 3.22)},\\
&E_5: \ y^2 + xy = x^3 - x^2 - 2x - 1 \text{ (Theorem 3.25, Corollary 3.26, Corollary 3.27)},\\
&E_6: \ y^2 = x^3 - 595x + 5586 \text{ (Theorem 3.28, Corollary 3.29, Corollary 3.30)},\\
&E^{(1)}: \ y^2 + y = x^3 - 30x + 63 \text{ (Theorem 3.2, Corollary 3.3)},\\
&E^{(2)}: \ y^2 + y = x^3 - x^2 - 7x + 10 \text{ (Theorem 3.4, Corollary 3.5)},\\
&E^{(3)}: \ y^2 + y = x^3 - 38x + 90 \text{ (Theorem 3.6, Corollary 3.7)},\\
&E^{(4)}: \ y^2 + y = x^3 - 860x + 9707 \text{ (Theorem 3.6, Corollary 3.7)},\\
&E^{(5)}: \ y^2 + y = x^3 - 7370x + 243528 \text{ (Theorem 3.6, Corollary 3.7)},\\
&E^{(6)}: \ y^2 + y = x^3 - 2174420x + 1234136692 \text{ (Theorem 3.6, Corollary 3.7)}.
\end{aligned}$$

We consider the anomalous primes for the twist of $E^{(i)} (1 \le i \le 6)$, and look for all possible values of a_p of $E_i (1 \le i \le 6)$. Some formulas for a_p in terms of the binomial coefficients are given.

We introduce the following notation.

$$\begin{aligned}
&q_1(x) = 27x^2 + 27x + 7,\\
&q_2(x) = 11x^2 + 11x + 3,\\
&q_3(x) = 19x^2 + 19x + 5,\\
&q_4(x) = 43x^2 + 43x + 11,\\
&q_5(x) = 67x^2 + 67x + 17,\\
&q_6(x) = 163x^2 + 163x + 41,\\
&d_1 = 27,\ d_2 = 11,\ d_3 = 19,\ d_4 = 43,\ d_5 = 67,\ d_6 = 163.
\end{aligned}$$

THEOREM 3.2. *Let p be a prime. Then*

(i) $\sum_{E^{(1)}}(\mathbb{Q}) = \emptyset$, *i.e.,* $E^{(1)}$ *has no anomalous primes.*

(ii) $a_p(E^{(1)}) = -1$ *if and only if* $p = q_1(x)$ *for some* $x \in \mathbb{Z}$. *In particular, the polynomial* $27x^2 + 27x + 7$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p(E^{(1)}) = -1$.

Proof. Since $E^{(1)}(\mathbb{Q})_{\text{tors}}$ is a cyclic group of order 3 and $a_2 = a_3 = a_5 = 0$, by Theorem 1.1, we have $\sum_{E^{(1)}}(\mathbb{Q}) = \emptyset$. Hence, we see that

$$a_p(E^{(1)}) = -1 \Leftrightarrow a_p(E^{(1)})^2 = 1 \Leftrightarrow p = q_1(h) \text{ for some } h \in \mathbb{Z}.$$

This completes the proof of Theorem 3.2. ∎

COROLLARY 3.3. *Let d be a square-free integer. Then a prime p is an anomalous prime for* $E^{(1)}_{(d)}$ *(the twist of $E^{(1)}$ by d) if and only if* $(\frac{d}{p}) = -1$ *and* $p = q_1(x)$ *for some* $x \in \mathbb{Z}$.

THEOREM 3.4. *Let p be a prime. Then*

(i) $\sum_{E^{(2)}}(\mathbb{Q}) = \emptyset$, *i.e.,* $E^{(2)}$ *has no anomalous primes.*

(ii) $a_p(E^{(2)}) = -1$ *if and only if* $p = q_2(x)$ *for some* $x \in \mathbb{Z}$. *In particular, the polynomial* $11x^2 + 11x + 3$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p(E^{(2)}) = -1$.

Proof. Consider the following two elliptic curves:

$$\begin{aligned}
C_1:&\quad y^2 = x^3 - \tfrac{22}{3}x + \tfrac{847}{108},\\
C_2:&\quad y^2 = x^3 - 8\cdot 33x + 14\cdot 11^2.
\end{aligned}$$

One can check that the morphism $E \longrightarrow C_1,\ \ (x,y) \longrightarrow (x - \frac{1}{3}, y + \frac{1}{2})$ is an isomorphism and C_2 is the twist of C_1 by $d = 6$. Let $p \geq 7$. By the Hasse inequality and (1) of Lemma 2.5, we have $a_p(E^{(2)}) = a_p(C_1) = (\frac{6}{p})a_p(C_2)$. On the other hand, by Theorem 1 of [13]

$$\sum_{x \bmod p} \left(\frac{x^3 - 8\cdot 33x + 14\cdot 11^2}{p}\right) = \begin{cases} 0, & \text{if } p \equiv 2,6,7,8,10 \pmod{11},\\ c, & \text{otherwise, where } 4p = c^2 + 11d^2 \text{ with}\\ & c \text{ determined uniquely by } (\frac{c}{11}) = (\frac{6}{p}). \end{cases}$$

Hence we obtain that $p = q_2(x) = 11x^2 + 11x + 3$ for some $x \in \mathbb{Z}$ if and only if

$$a_p(E^{(2)}) = a_p(C_1) = (\frac{6}{p})a_p(C_2) = -(\frac{6}{p})c = -1.$$

Note that $a_5(E^{(2)}) = -3$, $a_3(E^{(2)}) = -1, a_2(E^{(2)}) = 0$ and $3 = q_2(0)$. This completes the proof. □

Corollary 3.5. *Let d be a square-free integer. Then a prime p is an anomalous prime for $E^{(2)}_{(d)}$ (the twist of $E^{(2)}$ by d) if and only if $(\frac{d}{p}) = -1$ and $p = q_2(x)$ for some $x \in \mathbb{Z}$.*

Theorem 3.6. *Let p be a prime and $E = E^{(i)}$, $i = 3, 4, 5, 6$. Then we have*
(i) $\sum_E(\mathbb{Q}) = \emptyset$, *i.e., E has no anomalous primes.*
(ii) *For $i = 3, 4, 5, 6$, $a_p(E^{(i)}) = -1$ if and only if $p = q_i(x)$ for some $x \in \mathbb{Z}$. In particular, the polynomial $q_i(x)$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E^{(i)}) = -1$.*

Proof. Assume $3 \le i \le 6$. Let C_i and C'_i be the elliptic curves defined as follows:

$$C_i : \ y^2 = \begin{cases} x^3 - 38x + 90 + \frac{1}{4}, & \text{if } i = 3,\\ x^3 - 860x + 9707 + \frac{1}{4}, & \text{if } i = 4,\\ x^3 - 7370x + 243528 + \frac{1}{4}, & \text{if } i = 5,\\ x^3 - 2174420x + 1234136692 + \frac{1}{4}, & \text{if } i = 6, \end{cases}$$

$$C'_i : \ y^2 = g_i(x) = \begin{cases} x^3 - 2^3 \cdot 19x + 2 \cdot 19^2, & \text{if } i = 3,\\ x^3 - 2^4 \cdot 5 \cdot 43x + 2 \cdot 3 \cdot 7 \cdot 43^2, & \text{if } i = 4,\\ x^3 - 2^3 \cdot 5 \cdot 11 \cdot 67x + 2 \cdot 7 \cdot 31 \cdot 67^2, & \text{if } i = 5,\\ x^3 - 2^4 \cdot 5 \cdot 23 \cdot 29 \cdot 163x + 2 \cdot 7 \cdot 11 \cdot 19 \cdot 127 \cdot 163^2, & \text{if } i = 6. \end{cases}$$

It is clear that the morphism $E^{(i)} \longrightarrow C_i,\ (x, y) \longrightarrow (x, y + \frac{1}{2})$ is an isomorphism and C'_i is the twist of C_i by $d = 2$. By [7], we have

$$\sum_{x \bmod p} \left(\frac{g_i(x)}{p}\right) = \begin{cases} 0, & \text{if } (\frac{d_i}{p}) = -1,\\ c, & \text{if } 4p = c^2 + d_i d^2 \text{ with } (\frac{c}{d_i}) = (\frac{2}{p}). \end{cases}$$

Let $p \ge 7$ be a prime. By the Hasse inequality and (1) of Lemma 2.5, we obtain that $p = q_i(x)$ for some $x \in \mathbb{Z}$ if and only if

$$a_p(E^{(i)}) = (\frac{2}{p}) a_p(C'_i) = -(\frac{2}{p})c = -1.$$

Note that

$$\begin{aligned} &a_2(E^{(3)}) = a_3(E^{(3)}) = 0,\ a_5(E^{(3)}) = -1 \text{ and } 5 = q_3(0),\\ &a_2(E^{(4)}) = a_3(E^{(4)}) = a_5(E^{(4)}) = 0,\\ &a_2(E^{(5)}) = a_3(E^{(5)}) = a_5(E^{(5)}) = 0,\\ &a_2(E^{(6)}) = a_3(E^{(6)}) = a_5(E^{(6)}) = 0. \end{aligned}$$

This completes the proof. □

Corollary 3.7. *Assume $3 \le i \le 6$. Let d be a square-free integer. Then a prime p is an anomalous prime for $E^{(i)}_{(d)}$ (the twist of $E^{(i)}$ by d) if and only if $(\frac{d}{p}) = -1$ and $p = q_i(x)$ for some $x \in \mathbb{Z}$.*

Lemma 3.8. *Let p be a prime. The following assertions hold:*

(1) ([15], Exercises 2.33) E_1 *(resp. E_2) has good ordinary reduction at p if and only if* $p \equiv 1 \pmod 4$. *Factor p in $\mathbb{Z}[i]$ as*

$$p = \pi\bar{\pi}, \quad \text{with} \quad \pi \equiv 1 \pmod{2+2i}.$$

Then $a_p(E_1) = \pi + \bar{\pi}$. Hence $a_p(E_1)$ is even and $\frac{a_p(E_1)}{2}$ is odd.

(2) E_3 *has good ordinary reduction at p if and only if* $p \equiv 1, 3 \pmod 8$.

(3) E_4 *has good ordinary reduction at p if and only if* $p \equiv 1 \pmod 3$.

(4) E_5 (resp. E_6) *has good ordinary reduction at p if and only if* $p \equiv 1, 2, 4 \pmod 7$.

Proof. It follows easily from the criterion of supersingular primes for elliptic curves with complex multiplication ([2]) or Lemma 2.2. ☐

The following criterion to determine the good ordinary reduction primes of $E_j (1 \leq j \leq 6)$ is an immediate consequence of [2] and Lemma 2.2.

PROPOSITION 3.9. *Let $r > 0$ be an integer and let p be a prime where $E = E_j (1 \leq j \leq 6)$ has good reduction. The following assertions hold*:

(1) *The integer a_p happens to be odd only when $E = E_5$, $p = 2$, where $a_2 = 1$.*

(2) *If $r = 2k > 0$ is an even integer, then $|a_p| = r$ if and only if one of the following conditions holds:*

(i) $E = E_1$ (or E_2) *and the prime p is of the form $k^2 + n^2$ with k being odd.*

(ii) $E = E_3$ *and the prime p is of the form $k^2 + 2n^2$.*

(iii) $E = E_4$ *and the prime p is of the form $k^2 + 3n^2$.*

(iv) $E = E_5$ or E_6 *and the prime p is of the form $k^2 + 7n^2$.*

Proof. (1) Let $p \geq 7$ be a prime where the elliptic curve E has good ordinary reduction. Note that the Frobenius automorphism ϕ_p satisfies the equation (2). Hence we have:

(a) $a_p^2 - 4p = -4h^2$ for some $h \in \mathbb{Z}$ if $\mathrm{End}(E) = \mathbb{Z}[i]$.

(b) $a_p^2 - 4p = -16h^2$ for some $h \in \mathbb{Z}$ if $\mathrm{End}(E) = \mathbb{Z} + 2\mathbb{Z}[i]$.

(c) $a_p^2 - 4p = -8h^2$ for some $h \in \mathbb{Z}$ if $\mathrm{End}(E) = \mathbb{Z}[\sqrt{-2}]$.

(d) $a_p^2 - 4p = -12h^2$ for some $h \in \mathbb{Z}$ if $\mathrm{End}(E) = \mathbb{Z}[\sqrt{-3}]$.

(e) $a_p^2 - 4p = -28h^2$ for some $h \in \mathbb{Z}$ if $\mathrm{End}(E) = \mathbb{Z}[\sqrt{-7}]$.

(f) $a_p^2 - 4p = -7h^2$ for some $h \in \mathbb{Z}$ if $\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-7}}{2}$.

It is clear that a_p is always even in each case.

For $p \in \{2, 3, 5\}$, one can verify easily that a_p is odd if and only if $E = E_5$, $p = 2$, $a_2 = 1$.

(2) (i) Assume that $E = E_1$. Then $\mathrm{End}(E) = \mathbb{Z}[i]$. Let $p \in \sum_E^{(2k)}(\mathbb{Q})$ or $p \in \sum_E^{(-2k)}(\mathbb{Q})$. By (1) of Lemma 3.8, the equality $|a_p| = 2k$ implies that $p = k^2 + m^2$ for some $m \in \mathbb{Z}$ and k is odd. Conversely, let $p = k^2 + m^2 \geq 7$ be a prime with $k > 0$ being odd. Then E has good ordinary reduction at p by (1) of Lemma 3.8. Hence $4p = a_p^2 + n^2$ for some $n \in \mathbb{Z}$. By (1) of Lemma 3.8, we have that a_p is even and $\frac{a_p}{2}$ is odd. Hence $p = (\frac{a_p}{2})^2 + (\frac{n}{2})^2 = k^2 + m^2$. Since $\mathbb{Z}[i]$ is a UFD, we obtain that $|a_p| = 2k$.

Assume that $E = E_2$. Then $\mathrm{End}(E) = \mathbb{Z} + 2\mathbb{Z}[i]$. Let p be a prime where E_2 has good ordinary reduction and $|a_p| = 2k$. Then $p = k^2 + 4m^2$ for some integer m. Conversely, let $p = k^2 + 4m^2 \geq 7$ be a prime. Then E has good ordinary reduction at p by (1) of Lemma 3.8. Hence $4p = a_p^2 + 16n^2$ for some $n \in \mathbb{Z}$. It follows that $p = k^2 + 4m^2 = (\frac{a_p}{2})^2 + 4n^2$. Therefore $|a_p| = 2k$.

The proofs of (ii), (iii), (iv) are analogous. □

LEMMA 3.10. (**Gauss**) *Let $p = 4n+1$ be a prime. Hence the prime p is of the form $p = k^2 + m^2$ with $k \equiv 1 \pmod 4$. Then*

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

where $\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$ is the binomial coefficient.

THEOREM 3.11. *Let p be an odd prime. The following assertions hold:*
(1) $a_p(E_1) = 0$ *if and only if* $p \equiv 3 \pmod 4$.
(2) $a_p(E_1) \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod p$ *if* $p \equiv 1 \pmod 4$.
(3) *Let* $p \equiv 1 \pmod 4$. *Write* $p = m^2+k^2$ *with* $k \equiv 1 \pmod 4$. *Then* $a_p(E_1) = 2k$.

Proof. The discriminant $\Delta(E_1) = -2^6$, hence E_1 has bad reduction at prime 2.
(1) and (2). See [16], Example 4.5.
(3) Assume the prime $p \equiv 1 \pmod 4$. Then there exist integers m, k with $k \equiv 1 \pmod 4$ such that $p = m^2 + k^2$. By (2) and Lemma 3.10, $a_p(E_1) \equiv 2k \pmod p$. Hence, for any prime $p \geq 17$, we have $a_p(E_1) = 2k$ since $|k| < \sqrt{p}$. On the other hand, for $p = 5$ and 13, we have a computation:

$$a_{13}(E_1) = -6: \quad 13 = (-3)^2 + 2^2 (k = -3),$$

$$a_5(E_1) = 2: \quad 5 = 1^2 + 2^2 (k = 1).$$

This completes the proof of (3). □

COROLLARY 3.12. (1) *Let $0 \neq r \in \mathbb{Z}$. If there exists a prime p such that $a_p(E_1) = r$, then, for any prime q, $a_q(E_1) \neq -r$.*
(2) *For a prime p, $a_p(E_1) = 2$ if and only if $p = x^2 + 1$ for some $x \in \mathbb{Z}$. In particular, the polynomial x^2+1 represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E_1) = 2$. Similarly, $a_p(E_1) = -6$ if and only if $p = x^2+9$ for some $x \in \mathbb{Z}$. The polynomial x^2+9 represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E_1) = -6$.*

REMARK. By computing the $(1+i)^n$ division points for $n = 1, 2, 3, 4, 5$ on the elliptic curve $E_D: y^2 = x^3 - Dx$, Rajwade ([9]) obtained $a_p(E_D)$ as follows:

$$a_p(E_D) = \begin{cases} 0, & \text{if } p \equiv 3 \pmod 4, \\ \left(\frac{D}{\pi}\right)_4 \bar{\pi} + \left(\frac{D}{\bar{\pi}}\right)_4 \pi, & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

where $p = \pi\bar{\pi}$ is the decomposition of p in $\mathbb{Z}[i]$, where π and $\bar{\pi}$ are normalized so that each is congruent to $1 \pmod{2+2i}$ and where $(\div)_4$ is the biquadratic residue symbol.

Let $f(x) \in \mathbb{Z}[x]$ be a cubic polynomial with distinct roots in $\bar{\mathbb{Q}}$. Then $E: \ y^2 = f(x)$ is an elliptic curve defined over $\mathbb{Q}$. Let p be a prime where E has good reduction. We have

$$\sharp\tilde{E}(\mathbb{F}_p) = 1 + \sum_{x=0}^{p-1}(1 + \left(\frac{f(x)}{p}\right)) = 1 + p + \sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right),$$

i.e., $a_p(E) = -\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)$. Hence we have

Corollary 3.13. *Let p be an odd prime. Then*

$$\sum_{x=0}^{p-1}\left(\frac{x^3+x}{p}\right) = \begin{cases} 0, & \text{if } p\equiv 3 \pmod 4, \\ 2k, & \text{if } p\equiv 1 \pmod 4, \end{cases}$$

where $p = m^2 + k^2$ with $k \equiv 3 \pmod 4$.

Theorem 3.14. *Let p be an odd prime. The following assertions hold:*

(1) *$a_p(E_2) = 0$ if and only if $p \equiv 3 \pmod 4$.*

(2) *$a_p(E_2) \equiv (-1)^{\frac{p-1}{4}}\begin{pmatrix}\frac{p-1}{2}\\ \frac{p-1}{4}\end{pmatrix} \pmod p$ if $p \equiv 1 \pmod 4$.*

(3) *Let $p \equiv 1 \pmod 4$ be a prime. Write $p = (2n)^2 + k^2$, and fix the sign of k by the following congruence:*

$$k \equiv \begin{cases} 1 \pmod 4 & \text{if } n \text{ is even;} \\ 3 \pmod 4 & \text{if } n \text{ is odd.} \end{cases} \tag{5}$$

Then $a_p(E_2) = 2k$.

(4) *Let $k \equiv 1 \pmod 4$. Then the Hardy-Littlewood Conjecture holds for $16x^2+k^2$ with the constant $\delta = \delta(16, 0, k^2) > 0$ if and only if the Lang-Trotter Conjecture holds for $\pi_{E_2,2k}(x)$ with the constant $C_{E_2,2k} = \delta > 0$.*

(5) *Let $k \equiv 3 \pmod 4$. Then the Hardy-Littlewood Conjecture holds for $16x^2 + 16x+4+k^2$ with the constant $\delta = \delta(16, 16, 4+k^2) > 0$ if and only if the Lang-Trotter Conjecture holds for $\pi_{E_2,2k}(x)$ with the constant $C_{E_2,2k} = \delta > 0$.*

Proof. Since the discriminant $\Delta(E_2) = 2^9$, E_2 has bad reduction at prime 2.

(1) The assertion is a consequence of Lemma 2.2.

(2) Set

$$\begin{aligned} E_{(2,1)}:&\quad y^2 = x^3 - x, \\ E_{(2,2)}:&\quad y^2 = x^3 + 3x^2 + 2x, \\ E_{(2,3)}:&\quad y^2 = x^3 - 3x^2 + 2x, \\ E_{(2,4)}:&\quad y^2 = x^3 + 6x^2 + x. \end{aligned}$$

Then one may check that

$\phi_1 : E_{(2,1)} \longrightarrow E_{(2,2)},\ (x, y) \longrightarrow (x-1, y)$, is an isomorphism;
$E_{(2,3)}$ is the twist of $E_{(2,2)}$ by $d = -1$;
$\phi_2 : E_{(2,3)} \longrightarrow E_{(2,4)},\ (x, y) \longrightarrow (\frac{y^2}{x^2}, \frac{y(2-x^2)}{x^2})$, is an isogeny of degree 2;
$\phi_3 : E_2 \longrightarrow E_{(2,4)},\ (x, y) \longrightarrow (x-2, y)$, is an isomorphism.

Since $E_{(2,2)}$ and $E_{(2,3)}$ have complex multiplication by $\mathbb{Q}(\sqrt{-1})$, by (2) of Lemma 2.5, we have $a_p(E_{(2,3)}) = a_p(E_{(2,2)})$. Hence we obtain

$$a_p(E_2) = a_p(E_{(2,4)}) = a_p(E_{(2,3)}) = a_p(E_{(2,2)}) = a_p(E_{(2,1)}).$$

Note that

$$a_p(E_2) = a_p(E_{(2,1)}) \equiv (-1)^{\frac{p-1}{4}}\begin{pmatrix}\frac{p-1}{2}\\ \frac{p-1}{4}\end{pmatrix} \pmod p, \quad \text{if } p\equiv 1 \pmod 4.$$

Therefore, we complete the proof of (2).

(3) Let $p \equiv 1 \pmod 4$. If $p = (4n)^2 + k^2$ with $k \equiv 1 \pmod 4$, then, by (2) and Lemma 3.10, we have

$$a_p(E_2) \equiv (-1)^{\frac{p-1}{4}} \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2k \pmod p.$$

If $p = (4n+2)^2 + k^2$ with $k \equiv 3 \pmod 4$, then, by (2) and Lemma 3.10, we have

$$a_p(E_2) \equiv (-1)^{\frac{p-1}{4}} \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv -(-1)^{\frac{p-1}{4}} 2k = 2k \pmod p.$$

In both cases, we have $a_p(E_2) \equiv 2k \pmod p$. Hence, for any prime $p \geq 17$, we have $a_p(E_2) = 2k$ since $|k| < \sqrt{p}$. On the other hand,

$$a_{13}(E_2) = 6: \quad 13 = 3^2 + 2^2 (k = 3),$$

$$a_5(E_2) = -2: \quad 5 = (-1)^2 + 2^2 (k = -1).$$

This completes the proof of (3).

The assertions (4) and (5) are consequences of (3). $\square$

Corollary 3.15. *Let p be an odd prime. The following assertions hold.*

(1) *For a prime p, $a_p(E_2) = 2$ if and only if $p = (4x)^2 + 1$ for some $x \in \mathbb{Z}$. In particular, the polynomial $(4x)^2 + 1$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E_2) = 2$. Similarly, $a_p(E_2) = -2$ if and only if $p = (4x+2)^2 + 1$ for some $x \in \mathbb{Z}$. The polynomial $(4x+2)^2 + 1$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E_2) = -2$.*

(2) $\sum_{x=0}^{p-1} \left(\frac{x^3 - 11x + 14}{p}\right) = \begin{cases} 0, & \text{if } p \equiv 3 \pmod 4, \\ -2k, & \text{if } p \equiv 1 \pmod 4, \end{cases}$ *where the integer k is determined by* (5).

(3) $$\sum_{\frac{p-1}{3} \leq i \leq \frac{p-1}{2}, i \text{ even}} \binom{\frac{p-1}{2}}{i} \binom{i}{\frac{p-1-i}{2}} (-11)^{\frac{3i-(p-1)}{2}} 14^{\frac{p-1-2i}{2}}$$
$$\equiv \begin{cases} (-1)^{\frac{p-1}{4}} \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod p, & \text{if } p \equiv 1 \pmod 4, \\ 0 \pmod p, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Remark. The assertion (1) of Corollary 3.15 extends the assertion in Corollary 3.12. When $x^2 + 1$ is an odd prime, x is necessarily even. We may ask when x is exactly divisible by 2. The assertion (1) of Corollary 3.15 gives a criterion for this.

Lemma 3.16. (1) ([1], Theorem 9.2.8) *Let $p \equiv 1 \pmod 8$ be a prime. Write $p = \alpha_8^2 + 2\beta_8^2$ with $\alpha_8 \equiv -1 \pmod 4$. Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{8}} \equiv (-1)^{\frac{p+7}{8}} 2\alpha_8 \pmod p.$$

(2) ([1], Theorem 12.9.7) *Let $p \equiv 3 \pmod 8$ be a prime. Write $p = \alpha_8^2 + 2\beta_8^2$ with $\alpha_8 \equiv (-1)^{\frac{p-3}{8}} \pmod 4$. Then*

$$\binom{\frac{p-1}{2}}{\frac{p-3}{8}} \equiv -2\alpha_8 \pmod p.$$

LEMMA 3.17. ([10]) *Let* $E : y^2 = x(x^2 - 4Dx + 2D^2)$, $(D \in \mathbb{Z})$ *be an elliptic curve. Then*

$$a_p(E) = \begin{cases} 0, & \text{if } p \equiv -1, -3 \pmod 8, \\ \pi + \bar{\pi}, & \text{if } p \equiv 1, 3 \pmod 8, \end{cases}$$

where $p = \pi\bar{\pi}$ *and* $\pi(\bar{\pi})$ *can be determined uniquely by the following congruence*

$$\pi(\bar{\pi}) \equiv \left(\frac{D}{p}\right)\lambda \pmod{4\sqrt{-2}}$$

with $\lambda \in \Lambda$, *where*

$$\Lambda = \{1, 3, 1 + \sqrt{-2}, 3 + \sqrt{-2}, 1 + 3\sqrt{-2}, 3 + 3\sqrt{-2}, 5 + 2\sqrt{-2}, 7 + 2\sqrt{-2}\}.$$

THEOREM 3.18. *Let p be an odd prime. The following assertions hold:*
(1) $a_p(E_3) = 0$ *if and only if* $p \equiv -1, -3 \pmod 8$.

(2) $$a_p(E_3) \equiv \begin{cases} \begin{pmatrix} \frac{p-1}{2} \\ \frac{p-1}{8} \end{pmatrix} \pmod p, & \text{if } p \equiv 1 \pmod 8, \\ \begin{pmatrix} \frac{p-1}{2} \\ \frac{p-3}{8} \end{pmatrix} \pmod p, & \text{if } p \equiv 3 \pmod 8. \end{cases}$$

(3) *Let* $p \equiv 1, 3 \pmod 8$. *Write* $p = 2n^2 + k^2$, *and fix the sign of k by the following congruence:*

$$k \equiv \begin{cases} 1, \quad 3 \pmod 8, & \text{if } 4|n, \\ -1, \ -3 \pmod 8, & \text{if } 4 \nmid n. \end{cases} \tag{6}$$

Then $a_p(E_3) = 2k$.

(4) *Let* $k \equiv 1, 3 \pmod 8$. *Then the Hardy-Littlewood Conjecture holds for* $32x^2 + k^2$ *with the constant* $\delta = \delta(32, 0, k^2) > 0$ *if and only if the Lang-Trotter Conjecture holds for* $\pi_{E_3,2k}(x)$ *with the constant* $C_{E_3,2k} = \delta > 0$.

Proof. Since the discriminant $\Delta(E_3) = 2^9$, E_3 has bad reduction at prime 2.

The assertion (1) is a consequence of Lemma 2.2. We first prove the assertion (3). Taking $D = -1$ in Lemma 3.17, we have $a_p(E_3) = \pi + \bar{\pi}$, where $p = \pi\bar{\pi}$ and $\pi(\bar{\pi})$ can be determined uniquely by the following congruence

$$\pi(\bar{\pi}) \equiv \left(\frac{-1}{p}\right)\lambda \pmod{4\sqrt{-2}}$$

with $\lambda \in \{1, 3, 1 + \sqrt{-2}, 3 + \sqrt{-2}, 1 + 3\sqrt{-2}, 3 + 3\sqrt{-2}, 5 + 2\sqrt{-2}, 7 + 2\sqrt{-2}\}$.

Assume that $p \equiv 1$ or $3 \pmod 8$. Then

$$p = 2n^2 + k^2 = (k + n\sqrt{-2})(k - n\sqrt{-2}) = (-k + n\sqrt{-2})(-k - n\sqrt{-2}).$$

If $2|n$, then $p \equiv 1 \pmod 8$ and so $\left(\frac{-1}{p}\right) = 1$.

If $4|n$, then $\pi \equiv \bar{\pi} \equiv 1$ or $3 \pmod{4\sqrt{-2}}$; if $2||n$, then $\pi \equiv \bar{\pi} \equiv 5 + 2\sqrt{-2}$ or $7 + 2\sqrt{-2} \pmod{4\sqrt{-2}}$. In both cases, by our choice of k we have $a_p(E_3) = \pi + \bar{\pi} = 2k$.

If n is odd, then $p \equiv 3 \pmod 8$ and so $\left(\frac{-1}{p}\right) = -1$. Hence

$$-\pi \equiv 1 + \sqrt{-2} \text{ or } 3 + \sqrt{-2} \text{ or } 1 + 3\sqrt{-2} \text{ or } 3 + 3\sqrt{-2} \pmod{4\sqrt{-2}}$$

and correspondingly,

$$-\bar{\pi} \equiv 1+3\sqrt{-2} \text{ or } 3+3\sqrt{-2} \text{ or } 1+\sqrt{-2} \text{ or } 3+\sqrt{-2} \pmod{4\sqrt{-2}}.$$

Therefore, by our choice, $k \equiv -1, -3 \pmod 8$, we have $a_p(E_3) = \pi + \bar{\pi} = 2k$. This completes the proof of assertion (3).

Now we prove the assertion (2). From (1), we get that $a_p(E_3) \neq 0$ if and only if $p = 2n^2 + k^2 \equiv 1, 3 \pmod 8$. Assume that $p \equiv 3 \pmod 8$. Then n is odd. If $k \equiv -1 \pmod 8$, then $-k \equiv 1 \equiv (-1)^{\frac{p-3}{8}} \pmod 4$. If $k \equiv -3 \pmod 8$, then $-k \equiv -1 \equiv (-1)^{\frac{p-3}{8}} \pmod 4$. In both cases, we have $\alpha_8 = -k \equiv (-1)^{\frac{p-3}{8}} \pmod 4$. By the assertion (3) and Lemma 3.16, we have

$$a_p(E_3) = 2k = -2\alpha_8 \equiv \binom{\frac{p-1}{2}}{\frac{p-3}{8}} \pmod p.$$

Assume that $p \equiv 1 \pmod 8$. Then n is even. By the choice of k and α_8, one can check that $k = (-1)^{\frac{p+7}{8}}\alpha_8$. Hence, by the assertion (3) and Lemma 3.16, we have

$$a_p(E_3) = 2k = (-1)^{\frac{p+7}{8}} 2\alpha_8 \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{8}} \pmod p.$$

The assertion (4) is a consequence of (3). □

Corollary 3.19. *Let the notation be the same as in Theorem* 3.18.

(1) *For a prime p, $a_p(E_3) = 2$ if and only if $p = 32x^2 + 1$ for some $x \in \mathbb{Z}$. In particular, the polynomial $32x^2 + 1$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E_3) = 2$. Similarly, $a_p(E_3) = 6$ if and only if $p = 32x^2 + 9$ for some $x \in \mathbb{Z}$. The polynomial $32x^2 + 9$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E_3) = 6$.*

(2) $\sum_{x=0}^{p-1} \left(\frac{x^3+4x^2+2x}{p}\right) = \begin{cases} 0, & \text{if } p \equiv -1, -3 \pmod 8, \\ -2k, & \text{if } p \equiv 1, 3 \pmod 8, \end{cases}$ *where k is defined by* (6).

(3) $$\sum_{\frac{p-1}{4} \le k \le \frac{p-1}{2}} 2^{3k - \frac{p-1}{2}} \binom{\frac{p-1}{2}}{k} \binom{k}{\frac{p-1}{2} - k}$$
$$\equiv \begin{cases} \binom{\frac{p-1}{2}}{\frac{p-1}{8}} \pmod p, & \text{if } p \equiv 1 \pmod 8, \\ \binom{\frac{p-1}{2}}{\frac{p-3}{8}} \pmod p, & \text{if } p \equiv 3 \pmod 8, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 3.20. ([1], Theorem 6.4.3) *Let $p \equiv 1 \pmod 3$ be a prime. Write $p = \alpha_3^2 + 3\beta_3^2$ with $\alpha_3 \equiv -1 \pmod 3$. Then*

$$2\alpha_3 \equiv -\binom{\frac{p-1}{2}}{\frac{p-1}{6}} \pmod p.$$

Theorem 3.21. *Let p be an odd prime. The following assertions hold.*

(1) $a_p(E_4) = 0$ *if and only if* $p \equiv 2 \pmod 3$.

(2) $a_p(E_4) \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{3}} \pmod p$ *if* $p \equiv 1 \pmod 3$.

(3) *Let* $p \equiv 1 \pmod 3$. *Write* $p = k^2 + 3m^2$ *with* $k \equiv 1 \pmod 3$. *Then* $a_p(E_4) = 2k$.

(4) *Let* $k \equiv 1 \pmod 3$. *Then the Hardy-Littlewood conjecture holds for* $3x^2 + k^2$ *with the constant* $\delta = \delta(3, 0, k^2) > 0$ *if and only if the Lang-Trotter conjecture holds for* $\pi_{E_4,2k}(x)$ *with the constant* $C_{E_4,2k} = \delta > 0$.

Proof. Since the discriminant $\Delta(E_4) = 2^8 3^3$, E_4 has bad reduction at primes 2 and 3.

(1) By Lemma 2.2, $a_p(E_4) = 0$ if and only if $p \equiv 2 \pmod 3$.

(2) Set $E: \ y^2 = x^3 + 1$. We see that

$$\phi: \ E_4 \longrightarrow E, \ \ (x, y) \longrightarrow \left(\frac{y^2 - 4(x-2)^2}{4(x-2)^2}, -\frac{y(x^2 - 4x + 7)}{8(x-2)^2} \right)$$

is an isogeny. Hence for any odd prime p,

$$a_p(E_4) = a_p(E) \equiv \text{coefficient of } x^{p-1} \text{ in } (x^3+1)^{\frac{p-1}{2}} \pmod p.$$

Therefore we obtain

$$a_p(E_4) \equiv \begin{pmatrix} \frac{p-1}{2} \\ \frac{p-1}{3} \end{pmatrix} \pmod p, \ \ \text{if } p \equiv 1 \pmod 3.$$

(3) Assume that $p \equiv 1 \pmod 3$ is a prime. Write $p = k^2 + 3m^2$ with $k \equiv 1 \pmod 3$. Then, by (2) and Lemma 3.20, we have

$$a_p(E_4) \equiv \begin{pmatrix} \frac{p-1}{2} \\ \frac{p-1}{3} \end{pmatrix} \equiv \begin{pmatrix} \frac{p-1}{2} \\ \frac{p-1}{6} \end{pmatrix} \equiv 2k \pmod p.$$

Hence, for any prime $p \geq 17$, $a_p(E_4) = 2k$. On the other hand, for $p < 17$, we have

$$a_{13}(E_4) = 2: \ \ 13 = 1^2 + 3 \cdot 2^2 (k = 1),$$

$$a_7(E_4) = -4: \ \ 7 = (-2)^2 + 3 \cdot 1^2 (k = -2).$$

This proves (3).

(4) is a consequence of (3). ∎

Corollary 3.22. (1) *Let* $0 \neq r \in \mathbb{Z}$. *If there exists a prime* p *such that* $a_p(E_4) = r$, *then, for any prime* q, $a_q(E_4) \neq -r$.

(2) *For a prime* p, $a_p = 2$ *if and only if* $p = 3x^2 + 1$ *for some* $x \in \mathbb{Z}$. *In particular, the polynomial* $3x^2 + 1$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p = 2$. *Similarly,* $a_p = -4$ *if and only if* $p = 3x^2 + 4$ *for some* $x \in \mathbb{Z}$. *The polynomial* $3x^2 + 4$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p = -4$.

(3) $\sum_{\frac{p-1}{3} \leq i \leq \frac{p-1}{2}, i \text{ even}} \begin{pmatrix} \frac{p-1}{2} \\ i \end{pmatrix} \begin{pmatrix} i \\ \frac{p-1-i}{2} \end{pmatrix} (-15)^{\frac{3i-(p-1)}{2}} 22^{\frac{p-1-2i}{2}}$

$$\equiv \begin{cases} \begin{pmatrix} \frac{p-1}{2} \\ \frac{p-1}{3} \end{pmatrix} \pmod p, & \text{if } \ p \equiv 1 \pmod 3, \\ 0 \pmod p, & \text{if } \ p \equiv 2 \pmod 3. \end{cases}$$

(4) $\sum_{x=0}^{p-1} \left(\frac{x^3 - 15x + 22}{p} \right)$

$$= \begin{cases} 0, & \text{if } p \equiv 2 \pmod 3, \\ 2k, & \text{if } p \equiv 1 \pmod 3, \text{where } p = k^2 + 3m^2 \ \text{ with } k \equiv 2 \pmod 3. \end{cases}$$

LEMMA 3.23. *Let p be an odd prime with $\left(\frac{p}{7}\right)=1$. Write $p=\alpha_7^2+2\beta_7^2$ with $\left(\frac{\alpha_7}{7}\right)=1$.*

(1) ([1], Theorems 9.2.6) *If $p\equiv 1 \pmod 7$, then*

$$\binom{\frac{3(p-1)}{7}}{\frac{p-1}{7}}\equiv 2\alpha_7 \pmod p.$$

(2) ([1], Theorems 12.9.8) *If $p\equiv 2 \pmod 7$, then*

$$\binom{\frac{3(p-2)}{7}}{\frac{p-2}{7}}\equiv -2\alpha_7 \pmod p.$$

(3) ([1], Theorems 12.9.9) *If $p\equiv 4 \pmod 7$, then*

$$\binom{\frac{3(p-4)}{7}}{\frac{p-4}{7}}\equiv 2\alpha_7 \pmod p.$$

LEMMA 3.24. ([12]) *Let $K=\mathbb{Q}(\sqrt{-7})$ and let $E:\ y^2=x^3+21Dx^2+112D^2x$ $(x\in\mathbb{Z})$ be an elliptic curve. Then*

$$a_p(E)=\begin{cases}0, & \text{if } p\equiv 3,5,13 \pmod{14},\\ \pi+\bar\pi, & \text{if } p\equiv 1,9,11 \pmod{14},\end{cases}$$

where $p=\pi\bar\pi$ and $\pi(\bar\pi)$ can be determined uniquely by the following congruence

$$\pi(\bar\pi)\equiv\left(\frac{D}{p}\right)\lambda \pmod{\sqrt{-7}},\quad \lambda\in\{1,2,4\}.$$

We now consider the elliptic curve $E_5:\ y^2+xy=x^3-x^2-2x-1$.

THEOREM 3.25. *Let p be an odd prime. The following assertions hold.*

(1) *$a_p(E_5)=0$ if and only if $p\equiv 3,5,6 \pmod 7$.*

(2) $$a_p(E_5)\equiv\begin{cases}\binom{\frac{3(p-1)}{7}}{\frac{p-1}{7}} \pmod p, & \text{if } p\equiv 1 \pmod 7,\\ -\binom{\frac{3(p-2)}{7}}{\frac{p-2}{7}} \pmod p, & \text{if } p\equiv 2 \pmod 7,\\ \binom{\frac{3(p+3)}{7}}{\frac{p+3}{7}} \pmod p, & \text{if } p\equiv 4 \pmod 7.\end{cases}$$

(3) *Let $p\equiv 1,2,4 \pmod 7$. Write $p=7n^2+k^2$. We fix the sign of k by $\left(\frac{k}{7}\right)=1$, i.e.,*

$$\begin{cases}k\equiv 1 \pmod 7, & \text{if } p\equiv 1 \pmod 7,\\ k\equiv 4 \pmod 7, & \text{if } p\equiv 2 \pmod 7,\\ k\equiv 2 \pmod 7, & \text{if } p\equiv 4 \pmod 7.\end{cases}$$

Then $a_p(E_5)=2k$.

(4) *Let k be an integer such that $\left(\frac{k}{7}\right)=1$. Then the Hardy-Littlewood Conjecture holds for $7x^2+k^2$ with the constant $\delta=\delta(7,0,k^2)>0$ if and only if the Lang-Trotter Conjecture holds for $\pi_{E_5,2k}(x)$ with the constant $C_{E_5,2k}=\delta>0$.*

Proof. Since the discriminant $\Delta(E_5) = -7^3$, E_5 has bad reduction at prime 7.

(1) By Lemma 2.2, $a_p(E_5) = 0$ if and only if $p \equiv 3, 5, 6 \pmod 7$.

(2) It is a consequence of Lemma 3.23 and (3). Hence it suffices to prove the assertion (3).

(3) Take $D = 1$ in Lemma 3.24. Set $E: \ Y^2 = X^3 + 21X^2 + 112X$. Then

$$\phi: \ E_5 \longrightarrow E, \ (x, y) \longrightarrow (4(x-2), 4(x+2y))$$

is an isomorphism defined over $\mathbb{Q}$. For any odd prime p, we have

$$a_p(E_5) = a_p(E) = \begin{cases} 0, & \text{if } p \equiv 3, 5, 13 \pmod{14}, \\ \pi + \bar{\pi}, & \text{if } p \equiv 1, 9, 11 \pmod{14}, \end{cases}$$

where $p = \pi\bar{\pi}$ and $\pi(\bar{\pi})$ can be determined by the following congruence

$$\pi(\bar{\pi}) \equiv 1, 2, 4 \pmod{\sqrt{-7}}.$$

Note that

$$p \equiv 1, 2, 4 \pmod 7 \ \text{ if and only if } p \equiv 1, 9, 11 \pmod{14}.$$

And

$$p \equiv 3, 5, 6 \pmod 7 \ \text{ if and only if } p \equiv 3, 5, 13 \pmod{14}.$$

By our choices of k, we have $a_p(E_5) = \pi + \bar{\pi} = 2k$. ∎

Corollary 3.26. (1) *Let* $0 \neq r \in \mathbb{Z}$. *If there exists a prime* p *such that* $a_p(E_5) = r$, *then, for any prime* q, $a_q(E_5) \neq -r$.

(2) *Let* p *be a prime. Then the following statements hold:*

(i) $a_p(E_5) = 2$ *if and only if* $p = 7x^2 + 1$ *for some* $x \in \mathbb{Z}$. *In particular, the polynomial* $7x^2 + 1$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p(E_5) = 2$.

(ii) $a_p(E_5) = 4$ *if and only if* $p = 7x^2 + 4$ *for some* $x \in \mathbb{Z}$. *In particular, the polynomial* $7x^2 + 4$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p(E_5) = 4$.

(iii) $a_p(E_5) = 8$ *if and only if* $p = 7x^2 + 16$ *for some* $x \in \mathbb{Z}$. *In particular, the polynomial* $7x^2 + 16$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p(E_5) = 8$.

Corollary 3.27. *Let* p *be an odd prime. Then*

(1) $\sum_{x=0}^{p-1} \left(\frac{x^3 - \frac{3}{4}x^2 - 2x - 1}{p}\right) = \begin{cases} 0, & \text{if } p \equiv 3, 5, 6 \pmod 7, \\ -2k, & \text{if } p \equiv 1, 2, 4 \pmod 7, \end{cases}$ *where* k *is determined by* (3) *of Theorem* 3.25.

(2) $\sum_{\frac{p-1}{4} \leq k \leq \frac{p-1}{2}} 2^{2(p-1)-4k} 3^{2k - \frac{p-1}{2}} 7^k \begin{pmatrix} \frac{p-1}{2} \\ k \end{pmatrix} \begin{pmatrix} k \\ \frac{p-1}{2} - k \end{pmatrix}$

$$\equiv \begin{cases} \begin{pmatrix} \frac{3(p-1)}{7} \\ \frac{p-1}{7} \end{pmatrix} \pmod p, & \text{if } p \equiv 1 \pmod 7, \\ -\begin{pmatrix} \frac{3(p-2)}{7} \\ \frac{p-2}{7} \end{pmatrix} \pmod p, & \text{if } p \equiv 2 \pmod 7, \\ \begin{pmatrix} \frac{3(p+3)}{7} \\ \frac{p+3}{7} \end{pmatrix} \pmod p, & \text{if } p \equiv 4 \pmod 7, \\ \quad 0 \pmod p, & \text{otherwise.} \end{cases}$$

Finally, we consider the elliptic curve $E_6 : \ y^2 = x^3 - 595x + 5586$.

THEOREM 3.28. *Let p be an odd prime. The following assertions hold.*
(1) $a_p(E_6) = 0$ *if and only if* $p \equiv 3, 5, 6 \pmod 7$.

$$(2)\ a_p(E_6) \equiv \begin{cases} \left(\frac{-1}{p}\right)\begin{pmatrix} 3\frac{p-1}{7} \\ \frac{p-1}{7}\end{pmatrix} \pmod p, & \text{if } p \equiv 1 \pmod 7, \\ -\left(\frac{-1}{p}\right)\begin{pmatrix} 3\frac{p-2}{7} \\ \frac{p-2}{7}\end{pmatrix} \pmod p, & \text{if } p \equiv 2 \pmod 7, \\ \left(\frac{-1}{p}\right)\begin{pmatrix} 3\frac{p+3}{7} \\ \frac{p+3}{7}\end{pmatrix} \pmod p, & \text{if } p \equiv 4 \pmod 7. \end{cases}$$

(3) *Let $p \equiv 1, 2, 4 \pmod 7$. Write $p = 7n^2 + k^2$, and fix the sign of k by $\left(\frac{k}{7}\right) = \left(\frac{-1}{p}\right)$. Then $a_p(E_6) = 2k$.*

(4) *Let k be an integer such that $\left(\frac{k}{7}\right) = \left(\frac{-1}{p}\right)$. Then the Hardy-Littlewood Conjecture holds for $7x^2 + k^2$ with the constant $\delta = \delta(7, 0, k^2) > 0$ if and only if the Lang-Trotter Conjecture holds for $\pi_{E_6,2k}(x)$ with the constant $C_{E_6,2k} = \delta > 0$.*

Proof. Since the discriminant $\Delta(E_6) = 2^{12}7^3$, E_6 has bad reduction at primes 2 and 7.

Set

$$\begin{aligned} E_{(6,1)} :&\quad y^2 = x^3 + 42x^2 - 7x, \\ E_{(6,2)} :&\quad y^2 = x^3 - 84x^2 + 1792x, \\ E_{(6,3)} :&\quad y^2 = x^3 - 21x^2 + 112x, \\ E_{(6,4)} :&\quad y^2 = x^3 + 21x^2 + 112x. \end{aligned}$$

Then one can check that

$\phi_1 : E_6 \longrightarrow E_{(6,1)}$, $(x, y) \longrightarrow (x - 14, y)$, is an isomorphism;
$\phi_2 : E_{(6,1)} \longrightarrow E_{(6,2)}$, $(x, y) \longrightarrow (\frac{y^2}{x^2}, -\frac{y(7+x^2)}{x^2})$, is an isogeny of degree 2;
$\phi_3 : E_{(6,2)} \longrightarrow E_{(6,3)}$, $(x, y) \longrightarrow (x/4, y/8)$, is an isomorphism;
$E_{(6,3)}$ is a twist of $E_{(6,4)}$ by -1.

Hence, for any odd prime p, we have

$$a_p(E_6) = a_p(E_{(6,1)}) = a_p(E_{(6,2)}) = a_p(E_{(6,3)}) = \left(\frac{-1}{p}\right) a_p(E_{(6,4)}).$$

It follows from the proof of Theorem 3.25 that E_5 is isomorphic to $E_{(6,4)}$ over $\mathbb{Q}$, hence $a_p(E_{(6,4)}) = a_p(E_5)$. Therefore the result follows. □

COROLLARY 3.29. (1) *Let $0 \neq r \in \mathbb{Z}$. If there exists a prime p such that $a_p(E_6) = r$, then, for all prime q, $a_q(E_6) \neq -r$.*

(2) *Let p be a prime. The following statements hold:*

(i) $a_p(E_6) = 2$ *if and only if $p = 28x^2 + 1$ for some $x \in \mathbb{Z}$. In particular, the polynomial $28x^2+1$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E_6) = 2$.*

(ii) $a_p(E_6) = 12$ *if and only if $p = 7(2x+1)^2+36$ for some $x \in \mathbb{Z}$. In particular, the polynomial $7(2x + 1)^2 + 36$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E_6) = 12$.*

(iii) $a_p(E_6) = 18$ *if and only if $p = 28x^2 + 81$ for some $x \in \mathbb{Z}$. In particular, the polynomial $28x^2 + 81$ represents infinitely many primes if and only if there are infinitely many primes p such that $a_p(E_6) = 18$.*

(iv) $a_p(E_6) = -4$ *if and only if* $p = 7(2x+1)^2+4$ *for some* $x \in \mathbb{Z}$. *In particular, the polynomial* $7(2x+1)^2+4$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p(E_6) = -4$.

(v) $a_p(E_6) = 22$ *if and only if* $p = 28x^2+121$ *for some* $x \in \mathbb{Z}$. *In particular, the polynomial* $28x^2+121$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p(E_6) = 22$.

(vi) $a_p(E_6) = -8$ *if and only if* $p = 7(2x+1)^2+16$ *for some* $x \in \mathbb{Z}$. *In particular, the polynomial* $7(2x+1)^2+16$ *represents infinitely many primes if and only if there are infinitely many primes* p *such that* $a_p(E_6) = -8$.

COROLLARY 3.30. *Let* p *be an odd prime. Then*

(1) $\sum_{x=0}^{p-1}\left(\frac{x^3-595x+5586}{p}\right) = \begin{cases} 0, & \text{if } p \equiv 3,5,6 \pmod 7, \\ -2k, & \text{if } p \equiv 1,2,4 \pmod 7, \end{cases}$ *where* k *is determined by* (3) *of Theorem* 3.28.

(2) $$\sum_{\frac{p-1}{3}\le i\le \frac{p-1}{2}, i \text{ even}} \binom{\frac{p-1}{2}}{i}\binom{i}{\frac{p-1-i}{2}}(-595)^{\frac{3i-(p-1)}{2}}5586^{\frac{p-1-2i}{2}}$$
$$\equiv \begin{cases} \left(\frac{-1}{p}\right)\binom{3\frac{p-1}{7}}{\frac{p-1}{7}} \pmod p, & \text{if } p \equiv 1 \pmod 7, \\ -\left(\frac{-1}{p}\right)\binom{3\frac{p-2}{7}}{\frac{p-2}{7}} \pmod p, & \text{if } p \equiv 2 \pmod 7, \\ \left(\frac{-1}{p}\right)\binom{3\frac{p+3}{7}}{\frac{p+3}{7}} \pmod p, & \text{if } p \equiv 4 \pmod 7, \\ 0 \pmod p, & \text{otherwise.} \end{cases}$$

REFERENCES

[1] B. C. BERNDT, R. J. EVANS AND K. S. WILLIAMS, *Gauss and Jacobi sums*, Wiley, New York, 1998.

[2] M. DEURING, *Die Typen der Multiplikatorenringe elliptischer Funktonenkörper*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, 14 (1941), pp. 197–272.

[3] R. GREENBERG, *Iwasawa theory for elliptic curves*, Lecture Notes in Math., 1716 (1999), pp. 51–144.

[4] G. H. HARDY AND J. E. LITTLEWOOD, *Some problems of partitio numberorum III*, Acta Math., 44 (1923), pp. 1–70.

[5] S. LANG AND H. TROTTER, *Frobenius distributions in GL_2-extensions*, Lecture notes in Math., 504, Springer-Verlag, Berlin, 1976.

[6] B. MAZUR, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math., 18 (1972), pp. 183–266.

[7] R. PADMA AND S. VENKATARAMAN, *Elliptic curves with complex multiplication and a character sum*, J. Number Theory, 61 (1996), pp. 274–282.

[8] H. QIN, *Anomalous primes of the elliptic curve $E_D : y^2 = x^3 + D$*, to appear.

[9] A. R. RAJWADE, *A note on the number of solutions N_p of the congruence $y^2 \equiv x^3 - Dx (\mathrm{mod} p)$*, Proc. Camb. Phil. Soc., 67 (1970), pp. 603–605.

[10] A. R. RAJWADE, *Arithmetic on curves with complex multiplication by $\sqrt{-2}$,* Proc. Camb. Phil. Soc., 64 (1968), pp. 659–672.

[11] A. R. RAJWADE, *On rational primes p congruent to 1 (mod 3 or 5)*, Proc. Camb. Phil. Soc., 66 (1969), pp. 61–70.

[12] A. R. RAJWADE, *The Diophantine equation $y^2 = x(x^2 + 21Dx + 112D^2)$ and the conjectures of Birch and Swinnerton-Dyer*, J. Australian Math. Soc., 24 (1977), pp. 286–295.

[13] A. R. RAJWADE AND J. C. PARNAMI, *A new cubic charater sum*, Acta Arithmetica, 40 (1982), pp. 347–356.

[14] S. SCHMITT AND H. G. ZIMMER, *Elliptic Curves*, Walter de Gruyter, Berlin, New York, 2003.

[15] J. H. SILVERMAN, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

[16] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[17] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, New Jersey, 1971.