Exponential sums on binary quartic forms and their application

Yasuhiro Ishitsuka

Institute of Mathematics for Industry,
Kyushu University

Abstract

This article explains results in [ITTX] by Takashi Taniguchi, Frank Thorne, Stanley Yao Xiao and the author.

1 Introduction

This article is an announcement of the preprint [ITTX] of Takashi Taniguchi, Frank Thorne, Stanley Yao Xiao and the author.

The paper is two-folded. The first goal is to determine the finite Fourier transform $\widehat{\Phi_p}$ of the indicator function Φ_p of degenerate binary quartic forms. The function $\widehat{\Phi_p}$ is what we call *exponential sums on binary quartic forms*. The second goal is to apply the computation to a counting of arithmetic objects; elements in the 2-Selmer groups of elliptic curves over $\mathbf{Q}$. As results, we have a lower bound of the number of elements in those groups whose discriminants are squarefree and have at most four prime factors. This is an analogue of the result in [TT20a], which counts the isomorphism classes of cubic fields with prescribed conditions in the discriminants. Actually, we use the method parallel to [TT20a]; the computation on exponential sums on binary forms, and the weighted sieve in the form of [TT20a]. We will explain these two results devoted one section to each result.

2 Exponential sums on binary quartic forms

In this section, we fix some notion on the space of binary quartic forms, and give a brief account of our first main result.

2.1 The space of binary quartic forms

For a commutative ring R, let $V(R)$ be the space of binary quartics with coefficients in R. Explicitly,

$$V(R) \coloneqq \left\{ f(x,y) = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4 \;\middle|\; a_0, a_1, \ldots, a_4 \in R \right\}.$$

On this space, the group $\mathrm{GL}_1(R) \times \mathrm{GL}_2(R)$ acts as follows. Take an element

$$\left(\lambda, A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \in \mathrm{GL}_1(R) \times \mathrm{GL}_2(R)$$

and $f(x,y) \in V(R)$. Then we define

$$((\lambda, A)f)(x,y) \coloneqq \lambda f(ax+cy, bx+dy).$$

We can modify this action. For $A \in \mathrm{GL}_2(R)$, let us define another action by

$$(A \circ f)(x,y) \coloneqq \frac{1}{\det(A)^2} f(ax+cy, bx+dy). \tag{2.1}$$

This action descends to $\mathrm{PGL}_2(R) = \mathrm{GL}_2(R)/R^\times$. In Section 3, we use the action of $\mathrm{PGL}_2(R)$ to describe the relation between binary quartic forms and Selmer groups of elliptic curves.

Next we define a bilinear form on V. Assume that R is a field k whose characteristic is zero or $p > 3$. For two quartics,

$$f(x,y) = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4$$
$$g(x,y) = b_0x^4 + b_1x^3y + b_2x^2y^2 + b_3xy^3 + b_4y^4,$$

we define $\langle f, g\rangle$ by

$$\langle f, g\rangle \coloneqq a_0b_0 + \frac{a_1b_1}{4} + \frac{a_2b_2}{6} + \frac{a_3b_3}{4} + a_4b_4.$$

By our assumption on $R = k$, it defines an isomorphism between $V(k)$ and its dual $V^*(k)$ as k-linear spaces. Moreover, because the pairing satisfies

$$\langle (\lambda, A)f, g\rangle = \langle f, (\lambda, {}^tA)g\rangle$$

for $(\lambda, A) \in \mathrm{GL}_1(k)\times\mathrm{GL}_2(k)$, the isomorphism is actually an isomorphism as $\mathrm{GL}_1(k)\times\mathrm{GL}_2(k)$-representations, and also as $\mathrm{PGL}_2(k)$-representations.

The representation has some (relative) invariants. Though we can define them over $\mathbf{Z}$, we continue to assume that R is a field k of characteristic not equal to 2 nor 3. Let us define the *fundamental invariants*

$$I(f) \coloneqq 12a_0a_4 - 3a_1a_3 + a_2^2, \qquad I((\lambda, A)f) = \lambda^2 \det(A)^4 I(f),$$
$$J(f) \coloneqq 432 \det \begin{pmatrix} a_0 & a_1/4 & a_2/6 \\ a_1/4 & a_2/6 & a_3/4 \\ a_2/6 & a_3/4 & a_4 \end{pmatrix}, \quad J((\lambda, A)f) = \lambda^3 \det(A)^6 J(f).$$

Then the *discriminant* $\mathrm{Disc}(f)$ is given by

$$\mathrm{Disc}(f) = \frac{4I(f)^3 - J(f)^2}{27}, \quad \mathrm{Disc}((\lambda, A)f) = \lambda^6 \det(A)^{12} \mathrm{Disc}(f).$$

It detects the *degenerate quartics*: $\mathrm{Disc}(f) = 0$ if and only if f is zero or has a multiple factor. Note that the relative invariants are actually invariants with respect to the action of $\mathrm{PGL}_2(k)$.

To describe more detailed information on its factors, we use the *splitting types* as in [BS15]. Let us assume that a nonzero binary form $f(x, y)$ over k is factorized as

$$f(x,y) = cf_1(x,y)^{e_1} f_2(x,y)^{e_2} \dots f_n(x,y)^{e_n}$$

over k with a constant $c \in k^\times$ and irreducible binary forms $f_i(x, y)$ and $e_i \geq 1$. Let $d_i \coloneqq \deg(f_i)$ be the degree of the factor $f_i(x, y)$. Then we say that $f(x, y)$ is of splitting type $(d_1^{e_1}, d_2^{e_2}, \dots, d_n^{e_n})$.

For a binary quartic, there are eleven types; there are five types $(4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)$ for nondegenerate forms, and six types $(1^2, 2), (1^2, 1, 1), (1^2, 1^2), (2^2), (1^3, 1)$ and (1^4) for degenerate forms. We only use the later cases.

2.2 Main result: the explicit value of the exponential sums

In this subsection, we assume that $R = \mathbf{F}_p$ with $p > 3$.

Let $\Phi_p \colon V(\mathbf{F}_p) \to \mathbf{C}$ be the indicator function of degenerate quartics; that is,

$$\Phi_p(f) = \begin{cases} 1 & (\mathrm{Disc}(f) = 0) \\ 0 & (\mathrm{Disc}(f) \neq 0). \end{cases}$$

The *exponential sum on binary quartics* is defined as the finite Fourier transform of Φ_p. Explicitly, it is a function $\widehat{\Phi_p} \colon V(\mathbf{F}_p) \to \mathbf{C}$ defined by

$$\widehat{\Phi_p}(v) \coloneqq \frac{1}{p^5} \sum_{f \in V(\mathbf{F}_p)} \Phi_p(f) \exp\left(\frac{2\pi i\langle v, f\rangle}{p}\right).$$

Our first theorem determines the value of $\widehat{\Phi_p}(v)$ for any $v \in V(\mathbf{F}_p)$.

Theorem 2.1 ([ITTX, Theorem 1.1])**.** For a prime $p > 3$ and $v \in V(\mathbf{F}_p)$, we have

$$\widehat{\Phi}_p(v) = \begin{cases} p^{-1} + p^{-2} - p^{-3} & (v = 0) \\ p^{-2} - p^{-3} & (v : \text{splitting type } (1^3, 1) \text{ or } (1^4)) \\ \chi_{12}(p)(-p^{-3} + p^{-4}) & (v : \text{splitting type } (1^2, 1^2)) \\ \chi_{12}(p)(p^{-3} + p^{-4}) & (v : \text{splitting type } (2^2)) \\ \chi_{12}(p)p^{-4} & (v : \text{splitting type } (1^2, 1, 1) \text{ or } (1^2, 2)) \\ \left(\frac{-3I(v)}{p}\right) p^{-4} & (J(v) = 0, \mathrm{Disc}(v) \neq 0) \\ a(E'_v)p^{-4} & (J(v) \neq 0, \mathrm{Disc}(v) \neq 0). \end{cases}$$

Here, $\chi_{12}(\cdot)$ is the primitive Dirichlet character modulo 12, and $\left(\frac{\cdot}{p}\right)$: the Legendre symbol. The quantity $a(E'_v)$ is $p + 1 - \#E'_v(\mathbf{F}_p)$ for the elliptic curve $E'_v \colon y^2 = x^3 - 3I(v)x^2 + J(v)^2$.

We can consider the corresponding exponential sums of other spaces. In preceding studies [Mor10], [Ish19] and [TT20b], the exponential sums on various *prehomogeneous vector spaces* is obtained. An estimate of the exponential sums on much more general spaces is obtained in [FK01] using a geometric method. In my knowledge, our theorem is the first case that we can determine the value of exponential sums on a non-prehomogeneous *coregular space*, i.e. a linear representation whose ring of invariants is freely generated by two or more invariants.

A brief but enough estimate is obtained by this formula:

$$\widehat{\Phi}_p(v) \ll \begin{cases} p^{-1} & (v = 0) \\ p^{-2} & (v : \text{type } (1^3, 1), (1^4), (1^2, 1^2) \text{ and } (2^2)) \\ p^{-7/2} & (\text{otherwise}). \end{cases} \tag{2.2}$$

This estimate is used in the next section.

2.3 Counting (1): Scalar contraction

We briefly explain how to derive the formula in a generic case.

Let $\mathbf{P}(V(\mathbf{F}_p))$ be the projective space corresponding to the one-dimensional subspaces of $V(\mathbf{F}_p)$. In other words, it is the set of equivalence classes on $V(\mathbf{F}_p) - \{0\}$ defined as $f \sim g$ if $f = \lambda g$ for some $\lambda \in \mathbf{F}_p^\times$. We denote the equivalence class of f as $\overline{f}$. Then, since the scalar multiplication does not change the degeneracy of binary quartics, Φ_p can be interpreted as a function on $\mathbf{P}(V(\mathbf{F}_p))$; we use the same symbol.

Then we can transform the sum defining $\widehat{\Phi_p}$ as

$$\begin{aligned} \sum_{f \in V(\mathbf{F}_p)} \Phi_p(f) \exp\left(\frac{2\pi i \langle v, f\rangle}{p}\right) &= 1 + \sum_{0 \neq f \in V(\mathbf{F}_p)} \Phi_p(f) \exp\left(\frac{2\pi i \langle v, f\rangle}{p}\right) \\ &= 1 + \sum_{\overline{f} \in \mathbf{P}(V(\mathbf{F}_p))} \Phi_p(\overline{f}) \sum_{f \in \overline{f}} \exp\left(\frac{2\pi i \langle v, f\rangle}{p}\right). \end{aligned}$$

The inner sum is easily described as

$$\sum_{f \in \overline{f}} \exp\left(\frac{2\pi i \langle v, f\rangle}{p}\right) = \begin{cases} p - 1 & (\langle v, f\rangle = 0) \\ -1 & (\langle v, f\rangle \neq 0). \end{cases}$$

We introduce the number N_v as

$$N_v := \#\left\{\overline{f} \in \mathbf{P}(V(\mathbf{F}_p)) \;\middle|\; \mathrm{Disc}(\overline{f}) = \langle v, f\rangle = 0\right\}.$$

Since we can write

$$1+\sum_{\overline{f}\in\mathbf{P}(V(\mathbf{F}_p))}\Phi_p(\overline{f})\sum_{f\in\overline{f}}\exp\left(\frac{2\pi i\langle v,f\rangle}{p}\right)=1-N_0+pN_v,$$

it is enough to determine N_v. The special case $N_0=p^3+2p^2+p+1$ is classically known. The remaining task is to determine N_v.

2.4 Counting (2): Geometric decomposition

Our idea is to decompose N_v into three numbers of $\mathbf{F}_p$-rational points in algebraic sets.

On the definition of N_v, we count nonzero degenerate forms $f(x,y)$. The forms have one of the degenerate types $(1^2,1,1),(1^2,2),(1^2,1^2),(2^2),(1^3,1)$ and (1^4). Except the case (2^2), it can be written in the form

$$f(x,y)=\ell_1(x,y)^2q(x,y),$$

where $\ell_1(x,y)$ is a linear form over $\mathbf{F}_p$ and $q(x,y)$ is a quadratic form over $\mathbf{F}_p$. Moreover, the description is unique up to constant except the case $(1^2,1^2)$. Hence we can approximate N_v by the counting of pairs (ℓ_1,q) up to constants such that $\langle v,\ell_1^2q\rangle=0$.

We state this observation explicitly. Let U be the space of linear forms in x,y over $\mathbf{F}_p$. Then Sym^2U is the space of quadratic forms in x,y, and we can identify $V(\mathbf{F}_p)$ with Sym^4U. Consider the morphism

$$\psi_1\colon\mathbf{P}(U)\times\mathbf{P}(\mathrm{Sym}^2U)\to\mathbf{P}(V(\mathbf{F}_p))\quad;\quad\psi_1(\ell_1,q)=\ell_1^2q.$$

Then, the counting N_v is approximated by $\#\psi_1^{-1}(H_v)$, where H_v is the set of $\overline{f}\in\mathbf{P}(V(\mathbf{F}_p))$ with $\langle v,f\rangle=0$. To fix the difference, we prepare other two morphisms:

$$\begin{aligned}\psi_2\colon\mathbf{P}(U)\times\mathbf{P}(U)&\to\mathbf{P}(V(\mathbf{F}_p))\quad;\quad\psi_2(\ell_1,\ell_2)=\ell_1^2\ell_2^2,\\ \psi_3\colon\mathbf{P}(\mathrm{Sym}^2U)&\to\mathbf{P}(V(\mathbf{F}_p))\quad;\quad\psi_2(q)=q^2.\end{aligned}$$

Then we have the following simple formula:

$$N_v=\#\psi_1^{-1}(H_v)-\#\psi_2^{-1}(H_v)+\#\psi_3^{-1}(H_v).$$

This *geometric decomposition* can be extended to the spaces of binary forms of any degree.

Our task is now reduced to compute $\#\psi_i^{-1}(H_v)$. We only treat one case: let $v(x,y)\in V(\mathbf{F}_p)$ be a binary quartic with $J(v)\operatorname{Disc}(v)\neq0$, and consider the value $\#\psi_2^{-1}(H_v)$. It is the number of $\mathbf{F}_p$-rational points $(s_0x+s_1y,t_0x+t_1y)\in\mathbf{P}(U)\times\mathbf{P}(U)$ satisfying

$$\begin{pmatrix}s_0^2 & 2s_0s_1 & s_1^2\end{pmatrix}\begin{pmatrix}a_0 & a_1/4 & a_2/6\\ a_1/4 & a_2/6 & a_3/4\\ a_2/6 & a_3/4 & a_4\end{pmatrix}\begin{pmatrix}t_0^2\\ 2t_0t_1\\ t_1^2\end{pmatrix}=0.$$

According to [BH16], this equation defines a smooth genus one curve over $\mathbf{F}_p$ when $J(v)\operatorname{Disc}(v)\neq0$, and is isomorphic over $\mathbf{F}_p$ to the elliptic curve E'_v. For the remaining cases, see [ITTX].

3 Application: Counting 2-Selmer elemets

In this section, we briefly recall the relation between binary quartics and 2-Selmer groups of elliptic curves. Then we state our application of Theorem 2.1, and explain how to derive it.

3.1 Binary quartic forms and 2-Selmer elements

We recall a fact on binary quartic forms related to 2-Selmer elements.

For each binary quartic $f(x,y) \in V(\mathbf{Q})$, we can associate a subscheme of weighted projective space $\mathbf{P}(1,1,2)$:

$$C_f \coloneqq \left\{(x:y:z) \in \mathbf{P}(1,1,2) \;\middle|\; z^2 = f(x,y)\right\}.$$

This defines a genus one curve over $\mathbf{Q}$ if and only if $\mathrm{Disc}(f) \neq 0$. Its Jacobian variety is isomorphic over $\mathbf{Q}$ to the elliptic curve

$$E_f = E^{I(f),J(f)} \coloneqq \left\{(x:y:z) \in \mathbf{P}^2 \;\middle|\; y^2z = x^3 - \frac{I(f)}{48}xz^2 - \frac{J(f)}{1728}z^3\right\}.$$

If C_f has a rational point over a field K, we say that f is *K-soluble*. Similarly, if C_f is K-soluble for any local field $K = \mathbf{R}, \mathbf{Q}_p$ of $\mathbf{Q}$, we say that f is *locally soluble* over $\mathbf{Q}$.

The following correspondence states that locally soluble binary quartics with fixed invariants I, J gives an interpretation of 2-Selmer groups of $E^{I,J}$. Note that we use the action of $\mathrm{PGL}_2(\mathbf{Q})$ defined in (2.1).

Proposition 3.1 ([BSD63, BS15])**.** Let $E^{I,J}$ be the elliptic curve over $\mathbf{Q}$ defined by $y^2z = x^3 - \frac{I}{48}xz^2 - \frac{J}{1728}z^3$. Then, the $\mathrm{PGL}_2(\mathbf{Q})$-orbits of locally soluble binary quartics over $\mathbf{Q}$ with invariants I, J bijectively correspond to the elements of 2-Selmer group $\mathrm{Sel}_2(E^{I,J})$ of $E^{I,J}$.

Among them, the quartics with a linear factor over $\mathbf{Q}$ consist a single $\mathrm{PGL}_2(\mathbf{Q})$-orbit. The orbit correspond to the identity element of $\mathrm{Sel}_2(E^{I,J})$.

3.2 Main application: Counting 2-Selmer elements

Let E be an elliptic curve over $\mathbf{Q}$. It is uniquely described as a special kind of Weierstrass form:

$$E_{A,B} \colon y^2 = x^3 + Ax + B \quad (A, B \in \mathbf{Z})$$

such that if $p^4 \mid A$ for a prime number p, then $p^6 \nmid B$. The *height* $H(E)$ of E is defined to be

$$H(E) = H(E_{A,B}) \coloneqq \max\{4|A|^3, 27B^2\}.$$

With this quantity and the *discriminant* $\mathrm{Disc}(E)$ of the elliptic curve E, our main theorem is stated as follows:

Theorem 3.2 ([ITTX, Theorem 1.2])**.** For a real number $X > 0$, let $\mathcal{E}(X)$ be the set of isomorphism classes of elliptic curves over $\mathbf{Q}$ satisfying the following conditions:

(i) its *height* $H(E)$ is less than X,

(ii) its *discriminant* $\mathrm{Disc}(E)$ is squarefree, and

(iii) $\mathrm{Disc}(E)$ has at most four prime factors.

Then, we have

$$\sum_{E \in \mathcal{E}(X)} (\#\,\mathrm{Sel}_2(E) - 1) \gg \frac{X^{5/6}}{\log X}.$$

This theorem counts nontrivial 2-Selmer elements with conditions (ii) and (iii). Note that by [BS15], without the conditions (ii) and (iii), the sum is estimated as $\sim cX^{5/6}$ for a constant. This is an analogue of the result in [TT20a] counting cubic and quartic fields with similar conditions.

By Proposition 3.1, it is enough to construct orbits of locally soluble binary quartics satisfying conditions corresponding to (i), (ii) and (iii). In the followings, we illustrate the idea to construct them.

3.3 Weighted sieve

Our main idea is to apply the weighted sieve. To do this, we would like to estimate the number of orbits with $q \mid \mathrm{Disc}(f)$ and $H(f) < X$ for any squarefree q. Fix a fundamental domain[1] $\mathcal{R} \subseteq V(\mathbf{R})$ with respect to $\mathrm{GL}_2(\mathbf{Z})$-action on $V(\mathbf{R})$. Let $r\colon V(\mathbf{R}) \to \{0,1\}$ be the function defined by

$$r(f) = \begin{cases} 1 & (f \in \mathcal{R} \text{ and } 0 < H(f) < 1) \\ 0 & (\text{otherwise}). \end{cases}$$

Additionally, we abuse the notation Φ_q to write the indicator function on $V(\mathbf{Z})$ where $q \mid \mathrm{Disc}(f)$. Note that $\Phi_q = \prod_{p \mid q} \Phi_p$. Then since $H(\alpha f) = \alpha^6 H(f)$ for $\alpha > 0$, the number of orbits with $q \mid \mathrm{Disc}(f)$ and $H(f) < X$ is written as

$$\sum_{f \in V(\mathbf{Z})} \Phi_q(f) r(X^{-1/6} f).$$

With a suitable smooth function $\phi\colon V(\mathbf{R}) \to [0,1]$ such that $0 \le \phi(f) \le r(f)$ for any $f \in V(\mathbf{R})$, we undercount the number by

$$\sum_{f \in V(\mathbf{Z})} \Phi_q(f) \phi(X^{-1/6} f).$$

When we write

$$a(n, X) \coloneqq \sum_{\substack{f \in V(\mathbf{Z}) \\ |\mathrm{Disc}(f)| = n}} \phi(X^{-1/6} f),$$

the sum is written as

$$\sum_{\substack{0 < n < X \\ q \mid n}} a(n, X).$$

The weighted sieve in our context is as follows:

Theorem 3.3 ([TT20a, Theorem 5])**.** Suppose that $(a(n,X))_{n \ge 1}$ be a sequence of nonnegative real numbers depending on X. Assume that the following three conditions:

(1) ([TT20a, (7)]) There is a constant $c > 0$ and a multiplicative function ω with $\omega(1) = 1$ and $0 < \omega(p) < 1$ for any prime p with

$$\sum_{\substack{0 < n < X \\ q \mid n}} a(n, X) = c\omega(q) X^{5/6} + E(X, q).$$

(2) ([TT20a, (11)]) There is a constant $C > 0$ with

$$\left| \omega(p) - \frac{1}{p} \right| < \frac{C}{p^2}.$$

(3) ([TT20a, (9)]) For $\alpha < 1/3$, there is a constant $\delta > 0$ with

$$\sum_{q < X^\alpha} |E(X, q)| \ll X^{5/6 - \delta}.$$

Then, for any positive integer $t > \frac{1}{\alpha} + \frac{\log 4}{\log 3} - 1$, we have

$$\sum_{\substack{n \le X \\ p \mid n \Longrightarrow p > X^{\alpha/4} \\ \Omega(n) \le t}} a(n, X) \gg \frac{X^{5/6}}{\log X}.$$

Here, $\Omega(n)$ be the number of prime factors of n.

[1] Actually we consider a "weighted" fundamental domain in the sense of [BS15].

By Poisson summation formula, the sum is modified to

$$\begin{aligned}\sum_{0<n<X, q|n} a(n,X) &= X^{5/6} \sum_{\substack{v\in V^*(\mathbf{Z}) \\ |\operatorname{Disc}(v)|=n}} \widehat{\Phi_q}(v)\widehat{\phi}(X^{-1/6}v) \\ &= \widehat{\Phi_q}(0)\widehat{\phi}(0)X^{5/6} + E(X,q),\end{aligned} \tag{3.1}$$

where $E(X,q)$ is the error term. In our case, we interpret $c = \widehat{\phi}(0)$ and $\omega(q) = \widehat{\Phi_q}(0)$ in Theorem 3.3. By our estimate (2.2), there is a constant $C > 0$ with

$$\left|\widehat{\Phi_p}(0) - \frac{1}{p}\right| < \frac{C}{p^2} \tag{3.2}$$

for any prime $p > 3$. Then (3.1) and (3.2) are two of three conditions required to apply Theorem 3.3. The third one is the hardest part: it is proved by a variant of Ekedahl–Bhargava geometric sieve [Bha14] and the estimate (2.2) of our exponential sums.

As a result of the weighted sieve, there are $\gg X^{5/6}/\log X$ orbits of irreducbile binary quartics $f \in V(\mathbf{Z})$ with integral coefficients satisfying:

(i) The height $H(f) := \max\{|I(f)|^3/4, J(f)^2\}$ of f is less than X,

(ii) if $p \mid \operatorname{Disc}(f)$, then $p > X^{\alpha/4}$, and

(iii) the discriminant $\operatorname{Disc}(f)$ has at most four prime factors.

Actually, these include enough number of the desired quartics. First, they include reducible quartics, but the number is negligible due to [BS15, Lemma 2.3]. Second, they include quartics with nonsquarefree discriminants. However the number of quartics whose discriminants are divisible by p^2 for some prime $p > X^{\alpha/4}$ is negligible by [SSW21]. With the condition (ii), we may restrict to quartics whose discriminants are squarefree. Then they are automatically $\mathbf{Q}_p$-soluble at odd primes p by [BS15, Proposition 3.18]. We can find that they include a large subset of $\mathbf{R}$-soluble and $\mathbf{Q}_2$-soluble orbits.

The difference between $\mathrm{GL}_2(\mathbf{Z})$-orbits and $\mathrm{PGL}_2(\mathbf{Q})$-orbits can be treated similar to [BS15]. Combining these, we obtain the enough number of desired quartics.

Acknowledgements

The author thanks to the organizers Professor Yu Yasufuku and Professor Maki Nakasuji for giving him an opportunity to give a talk in this wonderful conference. In this study, the author is supported by JSPS KAKENHI Grant Number 20K03747, 21K13773 and 21K18557.

References

[Bha14] M. Bhargava. The geometric sieve and the density of squarefree values of invariant polynomials. Preprint, 2014. Available at `https://arxiv.org/abs/1402.0031`.

[BH16] M. Bhargava and W. Ho, Coregular spaces and genus one curves. Cambridge J. of Math., **4**(1): 1–119, 2016.

[BS15] M. Bhargava and A. Shankar, Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. Ann. of Math. (2), **181**(1): 191–242, 2015.

[BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. J. Reine Angew. Math., **212**: 7–25, 1963.

[FK01] E. Fouvry and N. Katz, A general stratification theorem for exponential sums, and applications. J. Reine Angew. Math., **540**: 115–166, 2001.

[Ish19] K. Ishimoto, O rbital exponential sums for some quadratic prehomogeneous vector spaces. Comment. Math. Univ. St. Pauli, **67**(2): 101–145, 2019.

[Mor10] S. Mori, Orbital Gauss sums associated with the space of binary cubic forms over a finite field. RIMS Kôkyûroku, **1715**: 32–36, 2010.

[SSW21] A. N. Shankar, A. Shankar and X. Wang, Large families of elliptic curves ordered by conductor. Compos. Math., **157**(7): 1538–1583, 2021.

[ITTX] Y. Ishitsuka, T. Taniguchi, F. Thorne and S. Y. Xiao, Exponential sums over singular binary quartic forms and applications, preprint.

[TT20a] T. Taniguchi and F. Thorne, Levels of distribution for sieve problems in prehomogeneous vector spaces. Math. Ann., **376**(3-4):1537–1559, 2020.

[TT20b] T. Taniguchi and F. Thorne, Orbital exponential sums for prehomogeneous vector spaces. Amer. J. Math., **142**(1): 177–213, 2020.