Existence of Rational Points and Integer Points on Certain Algebraic Varieties

February 2024

Yoshinori Kanamura

A Thesis for the Degree of Ph.D. in Science

Existence of Rational Points and Integer Points on Certain Algebraic Varieties

February 2024

Graduate School of Science and Technology
Keio University

Yoshinori Kanamura

Abstract

This thesis is a summary of the works of the author. In arithmetic geometry, one of the fundamental problems is whether a given algebraic variety has a rational point. In this thesis, we examine the proportions in certain families of algebraic varieties that have rational points.

Part 1 concerns the proportion of everywhere locally soluble diagonal hypersurfaces. Bright, Browning, and Loughran showed that the proportion of everywhere locally soluble diagonal hypersurfaces which have fixed degree and dimension is equal to the product of the proportions of $\mathbb{Q}_v$-soluble ones where v runs over all places of $\mathbb{Q}$. We give a strategy for calculating the proportions of $\mathbb{Q}_v$-soluble diagonal hypersurfaces for each degree and dimension. As a corollary, we also obtain approximate values of proportions of soluble ones for each dimension when they are quadratic and cubic under some assumptions. The contents of the first part are based on the joint work [**30**] with Yoshinosuke Hirakawa.

Part 2 concerns the proportion of genus one soluble curves defined by integer binary quartic forms. Bhargava and Bhargava–Ho determined the average sizes of n-Selmer groups in some families of elliptic curves. Consequently, they estimated the proportions of soluble curves defined by binary quartic forms and their subfamilies under the condition of everywhere locally soluble. In this thesis, for smaller subfamilies than that of Bhargava and Bhargava–Ho, we estimate the proportions of soluble curves under the condition of everywhere locally soluble. A part of these results can be regarded as binary quartic analogs of Browning's result that the proportion of soluble genus one curves defined by certain integer ternary cubic forms is positive. The contents of the second part are based on the joint work [**33**] with Yashuhiro Ishitsuka.

Although our main topic in this thesis is rational points on algebraic varieties, we also discuss the integer points on certain varieties called periodic continued fraction (PCF for short) varieties in Part 3. A periodic integer continued fraction (PICF for short) is a generalization of a periodic regular continued fraction. It is classical that a periodic regular continued fraction expansion of $\sqrt{m}$ is unique. On the other hand, a PICF expansion of $\sqrt{m}$ is not unique in general. Brock, Elkies, and Jordan determined all $(1,1)$ and $(1,2)$-type PICF expansions of $\sqrt{2}$. Encouraged by their results, we determined all $(1,l)$-type PICF expansions of $\sqrt{m}$ for $l = 1,2,3$ and positive integers m. To prove our results, it is essential to determine necessary and sufficient conditions for existing non-degenerate integer points on $(1,l)$-type PCF varieties for $\sqrt{m}$. The contents of the third part are based on the joint work with Hyuga Yoshizaki.

Acknowledgments

First of all, I would like to express my sincere gratitude to my supervisor, Professor Kenichi Bannai for his constant encouragements and helpful suggestions. I am deeply grateful to my collaborators, Yoshinosuke Hirakawa, Hyuga Yoshizaki at Tokyo University of Science, and Yasuhiro Ishitsuka at Kyusyu University for being willing to discuss at any time. I am also deeply grateful to Shuji Yamamoto at Keio University for teaching me the proof of Theorem A.1 and many fruitful discussion throughout my doctoral research. I would like to be grateful to Professor Masato Kurihara, Professor Taka-aki Tanaka, Associate Professor Kota Hattori, Yusuke Tanuma, and Takuki Tomita at Keio University for their valuable comments on the manuscript.

I would like to thank every present and former member of Bannai Laboratory, especially Emiko Minato and Maki Morimoto for giving me a great environment to study, and Hohto Bekki, Shinji Chikada, Yuki Goto, Kei Hagihara, Shun Ishii, Kazuna Kanegae, Hideki Matsumura, Tatsuya Ohshita, Masataka Ono, Yosuke Shimizu, Hidetada Wachi, and Kazuki Yamada for helpful discussion.

I also would like to extend my gratitude to Naoto Dainobu, Tomokazu Kashio, Fuyuta Komura, Daichi Takeuchi, Yutaka Takeuchi, Tomoki Uchimura, and other professors, friends and colleagues for their kind help during my graduate career. Finally, I would like to thank my parents and wife for their support and successive encouragement.

I was supported by RIKEN Junior Research Associate Program, by JST project "Support for Pioneering Research Initiated by the Next Generation", and by JSPS Research Fellowship for Young Scientists. This work was supported by the Research Grant of JSPS KAKENHI Grant Number JP22J13607, JST SPRING Grant Number JPMJSP1037, Keio Leading-edge Laboratory of Science and Technology Grant Number 000015 in 2020-2021 and 000027 in 2021-2022, and 2020 Doctoral Student Grant-in-Aid Program by the Ushioda Memorial Fund.

Contents

Part 0

Introduction

1. Hilbert's 10th problem

In number theory, one of the fundamental problems is to determine all rational solutions or all integer solutions of algebraic equations. This problem is sometimes called the Diophantine problem. Here, "Diophantine" comes from Diophantus of Alexandria who was a mathematician of the 3rd century.

As a problem related to the Diophantine problem, Hilbert [**29**] posed the following problem called the Hilbert's 10th problem:

Problem 1.1. Consider a polynomial $f(x_1, \ldots, x_n)$ with integer coefficients. Find an algorithm to determine whether an equation

$$f(x_1, \ldots, x_n) = 0. \tag{1.1}$$

has a solution in $\mathbb{Z}$ or $\mathbb{Q}$.

Matijasevič [**46**] solved Problem 1.1 for $\mathbb{Z}$ negatively. In other words, he proved that there exists no algorithm which decides whether or not an equation (1.1) has a solution in $\mathbb{Z}$. On the other hand, Problem 1.1 for $\mathbb{Q}$ is still an open problem. Hence many researchers have studied this problem for polynomials satisfying some conditions.

Note that Problem 1.1 can be regarded as a problem in algebraic geometry. Let V be a variety defined by $f(x_1, \ldots, x_n) = 0$. Then Problem 1.1 is equivalent to finding an algorithm to determine whether the set of rational points or integer points on V is empty or not. In this thesis, we focus on the problem whether rational points or integer points exist on certain algebraic varieties. More explicitly, we examine the proportions in certain families of algebraic varieties that have rational points.

2. Existing rational points on projective varieties

Let V be a projective variety defined over $\mathbb{Q}$. In this section, we consider the problem whether V has a rational point or not. First, we introduce the local-global principle. If it holds, it gives one of the effective methods for determining whether V has a rational point or not. After that, we consider the arithmetic statistic for the local-global principle which is related to our main theorems in Part 1 and Part 2.

2.1. Local-global principle.

In this subsection, we explain the local-global principle and some examples which satisfy this principle and some examples which do not satisfy this principle. We say that V is everywhere locally soluble if it satisfies $V(\mathbb{R}) \neq \emptyset$ and $V(\mathbb{Q}_p) \neq \emptyset$ for all rational primes p. Then the local-global principle is the following.

Definition 2.1 (local-global principle)**.** We say that V satisfies the local-global principle if

$$V \text{ is everywhere locally soluble } \iff V(\mathbb{Q}) \neq \emptyset$$

holds.

If V satisfies the local-global principle, we can examine the existence of a rational point on V easily. More explicitly, the intermediate value theorem is helpful to check $V(\mathbb{R}) \neq \emptyset$ and Hensel's lemma (see Proposition 6.1) is helpful to check $V(\mathbb{Q}_p) \neq \emptyset$.

The local-global principle holds for some specific classes of varieties. For example, the following theorem holds.

Theorem 2.2 (Hasse and Minkowski, cf. Serre [**59**, Chapter IV, Theorem 8]). Every quadratic hypersurface of $\mathbb{P}^n$ defined over $\mathbb{Q}$ satisfies the local-global principle.

Later, Birch [**7**] proved that complete intersections that have sufficiently large dimensions compared with their degrees satisfy the local-global principle by using a certain analytic method, called the Hardy–Littlewood circle method. Browning and Heath-Brown generalized this theorem to smooth and geometrically integral varieties.

Theorem 2.3 (Browning and Heath-Brown [**14**, Theorem 1.1]). Let $X \subset \mathbb{P}^n$ be a smooth and geometrically integral variety defined over $\mathbb{Q}$. If the condition

$$\dim(X) \geq (\deg(X) - 1)2^{\deg(X)} - 1,$$

holds for X, then X satisfies the local-global principle.

In addition to the above varieties, many varieties satisfy the local-global principle (cf. Skorobogatov [**64**, Theorem 5.1.1]).

On the other hand, many varieties also do not satisfy the local-global principle. For example, we have the following:

Theorem 2.4 (Selmer [**58**]). The curve in $\mathbb{P}^2$ given by $3x^3 + 4y^3 + 5z^3 = 0$ does not satisfy the local-global principle.

Theorem 2.5 (Cassels and Guy [**17**]). The surface in $\mathbb{P}^3$ given by $5x^3 + 12y^3 + 9z^3 + 10w^3 = 0$ does not satisfy the local-global principle.

Theorem 2.6 (Birch and Swinnerton-Dyer [**8**]). The surface in $\mathbb{P}^4$ given by

$$\begin{cases} zw = x^2 - 5y^2 \\ (z+w)(z+2w) = x^2 - 5v^2 \end{cases}$$

does not satisfy the local-global principle.

Theorem 2.7 (Fujiwara [**25**]). The curve in $\mathbb{P}^2$ given by $(x^3+5y^3)(x^2+xy+y^2)-17z^5 = 0$ does not satisfy the local-global principle.

In 1970, Manin [**44**] proposed a criterion called the Brauer–Manin obstruction for verifying the local-global principle geometrically. After that, many researchers have constructed infinitely many counterexamples for the local-global principle which have the Brauer–Manin obstruction (cf. Colliot-Thélène and Skorobogatov [**19**, Section 13.3.3]). Although Skorobogatov [**63**] find a counterexample for the local-global principle which does not have the Brauer–Manin obstruction, it is conjectured by many experts that the Brauer–Manin obstruction explains whether the local-global principle holds or not for quite a lot of varieties (cf. Colliot-Thélène and Swinnerton-Dyer [**20**, p. 49], Manin [**45**, Chapter VI], Poonen [**54**, Chapter 8], Poonen and Voloch [**56**, Conjecture 3.2 and Appendix A]).

2.2. Arithmetic statistic for the local-global principal. In section 2.1, we discussed the local-global principle for each variety. Recently, many researchers studied the local-global principle for a family of algebraic varieties. More explicitly, for a given family of algebraic varieties, we ask how many varieties in its family satisfy the local-global principle. Poonen and Voloch [**56**] gave a philosophy which the proportion of soluble algebraic varieties is equal to the product of the proportions of everywhere locally soluble ones for a family of algebraic varieties satisfying some suitable conditions. In the following, we will explain their philosophy in detail.

Let $n, k \in \mathbb{Z}_{\geq 2}$ and $\mathbb{Z}[x_0, \ldots, x_n]_k$ be the set of homogeneous polynomials in $\mathbb{Z}[x_0, \ldots, x_n]$ of degree k. We set $M_{\mathbb{Q}} = \{p : \text{primes}\} \cup \{\infty\}$ and $\mathbb{Q}_\infty = \mathbb{R}$. For $f \in \mathbb{Z}[x_0, \ldots, x_n]_k$, let V_f be a hypersurface defined by $f = 0$ and the height $h(f)$ be the maximum of the absolute values of the coefficients of f. For $H \in \mathbb{R}_{\geq 0}$, define

$$\delta_{\mathrm{glob}}(H) = \frac{\#\{f \in \mathbb{Z}[x_0, \ldots, x_n]_k \mid h(f) \leq H,\ V_f(\mathbb{Q}) \neq \emptyset\}}{\#\{f \in \mathbb{Z}[x_0, \ldots, x_n]_k \mid h(f) \leq H\}}, \tag{2.1}$$

$$\delta_{\mathrm{loc}}(H) = \frac{\#\{f \in \mathbb{Z}[x_0, \ldots, x_n]_k \mid h(f) \leq H,\ V_f(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in M_{\mathbb{Q}}\}}{\#\{f \in \mathbb{Z}[x_0, \ldots, x_n]_k \mid h(f) \leq H\}}. \tag{2.2}$$

Then Poonen and Voloch conjectured the following.

Conjecture 2.8 (Poonen and Voloch [**56**, Conjecture 2.2])**.**

(1) If $k > n+1$, then $\lim_{H\to\infty} \delta_{\mathrm{glob}}(H) = 0$.

(2) If $k < n+1$ and $(n,k) \neq (2,2)$[a], then $\lim_{H\to\infty} \delta_{\mathrm{glob}}(H) = c$ for some $c \in \mathbb{R}_{>0}$.

Note that (2) in Conjecture 2.8 is proved in 2023 by Browning, Le-Boudec, and Sawin [**15**, Theorem 1.1] except for $(n,k) = (3,3)$. We also note that for $n, k \geq 2$ with $(n,k) \neq (2,2)$, Poonen and Voloch [**56**, Theorem 3.6] showed that $\lim_{H\to\infty} \delta_{\mathrm{loc}}(H)$ exists and is given by

$$\lim_{H\to\infty} \delta_{\mathrm{loc}}(H) = \prod_{v\in M_{\mathbb{Q}}} \delta_v,$$

where δ_v is the proportion of polynomials in $\mathbb{Z}[x_0, \dots, x_n]_k$ with a nontrivial zero over $\mathbb{Q}_v$ (see §3 for the detail of the definition). Hence (2) in Conjecture 2.8 is equivalent to

$$\lim_{H\to\infty} \delta_{\mathrm{glob}}(H) = \prod_{v\in M_{\mathbb{Q}}} \delta_v$$

under the condition on the Brauer–Manin obstruction for the local-global principle.

Although Poonen and Voloch gave the conjecture for certain families of hypersurfaces, many experts predicted or found similar phenomena for other families in e.g. Bhargava [**3**], Browning [**11**], Fisher–Ho–Park [**24**] (see also the table in Loughran, Rome, and Sofos [**43**, pp. 2-3]).

In this thesis, there are two topics about the proportions in certain families of algebraic varieties. The first topic is the proportions of everywhere locally soluble diagonal hypersurfaces. More explicitly, we give the explicit method to calculate the proportions of diagonal hypersurfaces which have $\mathbb{Q}_p$-rational points for all rational primes p. We will explain this topic in §3. The second topic is the proportions of genus one soluble curves defined by certain binary quartic forms. More explicitly, we estimate the proportions of soluble binary quartic forms in locally soluble ones. We will explain this topic in §4.

3. The proportion of everywhere locally soluble diagonal hypersurfaces

In part 1 of this thesis, we consider the proportion of everywhere locally soluble diagonal hypersurfaces.

A family of diagonal hypersurfaces of $\mathbb{P}^n$ is a subfamily of hypersurfaces which appeared in §2.2. Moreover, diagonal hypersurfaces of $\mathbb{P}^n$ have attracted special interests because of their remarkable arithmetic properties. For example, although cubic hypersurfaces of

[a] If $(k,n) = (2,2)$, Serre [**60**] showed that $\lim_{H\to\infty} \delta_{\mathrm{glob}}(H) = \lim_{H\to\infty} \delta_{\mathrm{loc}}(H) = 0$.

$\mathbb{P}^n$ ($n \geq 1$) may not have $\mathbb{Q}_v$-rational points in general, Lewis [**41**, Theorem 2] proved that diagonal cubic hypersurfaces of $\mathbb{P}^n$ ($n \geq 6$) have $\mathbb{Q}_v$-rational points for every $v \in M_{\mathbb{Q}}$. Moreover, Baker [**2**, Theorem 1] proved that diagonal cubic hypersurface of $\mathbb{P}^n$ ($n \geq 6$) also have $\mathbb{Q}$-rational points. For more classical works on $\mathbb{Q}$-rational points on diagonal cubic hypersurfaces of $\mathbb{P}^n$, see e.g. Davenport [**21**, **22**], Hardy and Littlewood [**27**], Hua [**32**].

Before stating our main results, let us explain some simple applications. Fix $n, k \in \mathbb{Z}_{\geq 2}$. For each $\boldsymbol{a} = [a_0 : \cdots : a_n] \in \mathbb{P}^n(\mathbb{Q})$, let $X^k_{\boldsymbol{a}}$ be a diagonal hypersurfaces defined by $\sum_{i=0}^n a'_i x_i^k = 0$ where $a'_0, \ldots, a'_n$ are integers such that

$$[a'_0 : \cdots : a'_n] = [a_0 : \cdots : a_n]$$

and $\gcd(a'_0, \ldots, a'_n) = 1$. We set

$$\overline{h}([a_0 : \cdots : a_n]) = \max_i \{|a'_i|\}$$

with the Euclidean norm $|\cdot|$ on $\mathbb{R}$. We define

$$\rho(n,k) := \lim_{H \to \infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{P}^n(\mathbb{Q}) \;\middle|\; \overline{h}(\boldsymbol{a}) < H \text{ and } X^k_{\boldsymbol{a}}(\mathbb{Q}) \neq \emptyset\right\}}{\#\left\{\boldsymbol{a} \in \mathbb{P}^n(\mathbb{Q}) \;\middle|\; \overline{h}(\boldsymbol{a}) < H\right\}}$$

if the limit exists.

In the following, we refer to hypersurfaces of $\mathbb{P}^n$ as $(n-1)$-folds for $n \geq 2$.

THEOREM 3.1 ([**30**, Theorem 1.1]).

(1) For $k = 2$, we have the following table.

TABLE 1. approximate values of $\rho(n, 2)$

n	2	3	≥ 4
$\rho(n,2)$	0	$0.8268\ldots$	$1 - 2^{-n}$

(2) For $k = 3$, we have the following table under the assumption that if $3 \leq n \leq 5$, then the Brauer-Manin obstruction is the only obstruction to the local-global principle for diagonal cubic $(n-1)$-folds.

TABLE 2. approximate values of $\rho(n, 3)$

n	2	3	4	5	≥ 6
$\rho(n,3)$	0	$0.8964\ldots$	$0.9965\ldots$	$0.9999\ldots$	1

Some values in the above tables have been already known in the literature (e.g. Baker [**2**], Bright, Browning, and Loughran [**9**], Browning and Dietmann [**13**], Serre [**59**]). For example, the results for $\rho(n,3)$ ($n \geq 6$) follow immediately from Baker's result [**2**, Theorem 1] mentioned above. On the other hand, the author could not find any explicit references which contain the values $\rho(3,2), \rho(4,3), \rho(5,3)$. For the last two values, $\rho(4,3)$ and $\rho(5,3)$, it should be remarked that there is no known cubic $(n-1)$-fold ($n = 4,5$) which violates the local-global principle. This fact is contrastive with the fact that there are several counterexamples to the local-global principle for $n = 2,3$ (e.g. Theorems 2.4 and 2.5).

For the proof of Theorem 3.1, we will use diagonal analogy of Poonen and Voloch's philosophy. We define

$$\rho_{\mathrm{loc}}(n,k) = \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{P}^n(\mathbb{Q}) \;\middle|\; \overline{h}(\boldsymbol{a}) < H \text{ and } X^k_{\boldsymbol{a}}(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in M_{\mathbb{Q}}\right\}}{\#\left\{\boldsymbol{a} \in \mathbb{P}^n(\mathbb{Q}) \;\middle|\; \overline{h}(\boldsymbol{a}) < H\right\}}$$

if the limit exists. Then Browning showed the following theorem.

Theorem 3.2 (a special case of Browning [**11**, Theorem 1.4]). *Assume that the Brauer-Manin obstruction is the only obstruction to the local-global principle for $X^k_{\boldsymbol{a}}$. Then we have*

$$\rho(n,k) = \rho_{\mathrm{loc}}(n,k)$$

for each $n,k \in \mathbb{Z}_{\geq 2}$ with $n \geq k$.

Note that Brüdern and Dietmann [**16**, Theorem 1.3] also showed Theorem 3.2 for families of diagonal hypersurfaces $X^k_{\boldsymbol{a}}$ with $k \geq 4$ and $n \geq 3k+2$ without any assumption on the Brauer–Manin obstruction (see also Remark 9.2).

We also note that the proportions $\rho(n,k)$ and $\rho_{\mathrm{loc}}(n,k)$ can be defined by using the height h like (2.1) and (2.2). In other words, we consider the following proportions

$$\rho'(n,k) := \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a} = (a_0,\ldots,a_n) \in \mathbb{Z}^{\oplus n+1} \;\middle|\; h(X^k_{\boldsymbol{a}}) < H \text{ and } X^k_{\boldsymbol{a}}(\mathbb{Q}) \neq \emptyset\right\}}{\#\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \mid h(X^k_{\boldsymbol{a}}) < H\}},$$

$$\rho'_{\mathrm{loc}}(n,k) := \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \;\middle|\; h(X^k_{\boldsymbol{a}}) < H \text{ and } X^k_{\boldsymbol{a}}(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in M_{\mathbb{Q}}\right\}}{\#\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \mid h(X^k_{\boldsymbol{a}}) < H\}}$$

if the limits exist. Here $h(X^k_{\boldsymbol{a}})$ denotes $h(\sum_{i=0}^n a_i x_i^k)$. Then the equalities $\rho(n,k) = \rho'(n,k)$ and $\rho_{\mathrm{loc}}(n,k) = \rho'_{\mathrm{loc}}(n,k)$ hold if the limits $\rho(n,k)$ and $\rho_{\mathrm{loc}}(n,k)$ exist (for more details, see §A in Appendix).

Thanks to Theorem 3.2, under the conditions in this theorem, the value $\rho(n,k)$ coincides with its local avatar $\rho_{\mathrm{loc}}(n,k)$. Moreover, set

$$\rho_v(n,k) := \begin{cases} \mu_p\left(\left\{\boldsymbol{a} \in \mathbb{Z}_p^{\oplus n+1} \mid X_{\boldsymbol{a}}^k(\mathbb{Q}_p) \neq \emptyset\right\}\right) & \text{if } v \text{ is a prime } p, \\ 2^{-n-1}\mu_\infty\left(\left\{\boldsymbol{a} \in [-1,1]^{\oplus n+1} \mid X_{\boldsymbol{a}}^k(\mathbb{R}) \neq \emptyset\right\}\right) & \text{if } v = \infty. \end{cases}$$

Here, μ_p is the Haar measure on $\mathbb{Z}_p$ normalized so that $\mu_p(\mathbb{Z}_p) = 1$ and μ_∞ is the Lebesgue measure on $\mathbb{R}$. We use the same letter μ_p (resp. μ_∞) also for the product measure on $\mathbb{Z}_p^{\oplus n+1}$ (resp. $\mathbb{R}^{\oplus n+1}$). The calculation of $\rho_{\mathrm{loc}}(n,k)$ is reduced to that of $\rho_v(n,k)$ for every $v \in M_{\mathbb{Q}}$ by the following theorem of Bright, Browning, and Loughran.

Theorem 3.3 (a special case of Bright, Browning, and Loughran [**9**, Theorem 1.3]). Assume that $n \neq 2$. Then the limit $\rho_{\mathrm{loc}}(n,k)$ exists [b] and is given by

$$\rho_{\mathrm{loc}}(n,k) = \prod_{v \in M_{\mathbb{Q}}} \rho_v(n,k).$$

Moreover, $\rho_{\mathrm{loc}}(n,k)$ is positive whenever $n \geq 3$.

Let us explain our main results. In this thesis, we establish a strategy to calculate $\rho_v(n,k)$ for all $v \in M_{\mathbb{Q}}$ for each fixed n and k (see Remark 7.4). Our strategy is regarded as a quantitative refinement of the argument in Browning and Dietmann [**13**, §3]. As worked examples, we carry out our strategy in the cases of $k = 2, 3$. In particular, Theorem 3.1 follows from Theorem 3.3 and the following Theorems 3.4 and 3.5.

Theorem 3.4 ([**30**, Theorem 1.3]). Suppose that $k = 2$.

(1) If $n = 2$, then

$$\rho_p(2,2) = \begin{cases} \dfrac{7}{12} & \text{if } p = 2, \\ 1 - \dfrac{3}{2}p^{-1}\left(\dfrac{1-p^{-1}}{1-p^{-2}}\right)^2 & \text{otherwise.} \end{cases}$$

(2) If $n = 3$, then

$$\rho_p(3,2) = \begin{cases} \dfrac{1231}{1296} & \text{if } p = 2, \\ 1 - \dfrac{3}{2}p^{-2}\left(\dfrac{1-p^{-1}}{1-p^{-2}}\right)^4 & \text{otherwise.} \end{cases}$$

[b] Note that $\rho_{\mathrm{loc}}(2,k) = 0$ for every $k \geq 2$ as proven in Browning and Dietmann [**13**, Theorem 1.1]. On the other hand, Proposition 7.3 implies that $\prod_{v \in M_{\mathbb{Q}}} \rho_v(2,k) = 0$ in the sense that $\sum_{v<H} \log \rho_v(2,k) \to -\infty$ $(H \to \infty)$ because $\sum_{p<H, p\equiv 1 \bmod k} p^{-1} \to \infty$ $(H \to \infty)$ (cf. Serre [**59**, p. 75]).

(3) If $n \geq 4$, then $\rho_p(n, 2) = 1$ (cf. Serre [**59**, Corollary 2]).

Note that the value $\rho_\infty(n, 2)$ equals $1 - 2^{-n}$ for every $n \in \mathbb{Z}_{\geq 2}$.

Theorem 3.5 ([**30**, Theorem 1.4]). Suppose that $k = 3$.

(1) If $n = 2$, then

$$\rho_p(2,3) = \begin{cases} \dfrac{13831}{19773} & \text{if } p = 3, \\ 1 - 2p^{-1}\left(\dfrac{1-p^{-1}}{1-p^{-3}}\right) & \text{if } p \equiv 1 \bmod 3, \\ 1 - 6p^{-3}\left(\dfrac{1-p^{-1}}{1-p^{-3}}\right)^3 & \text{if } p \equiv 2 \bmod 3. \end{cases}$$

(2) If $n = 3$, then

$$\rho_p(3,3) = \begin{cases} \dfrac{6391}{6591} & \text{if } p = 3, \\ 1 - \dfrac{8}{3}p^{-2}(1+p^{-1})^2\left(\dfrac{1-p^{-1}}{1-p^{-3}}\right)^3 & \text{if } p \equiv 1 \bmod 3, \\ 1 & \text{if } p \equiv 2 \bmod 3 \end{cases}$$

(Bright, Browning, and Loughran [**9**, Theorem 2.2]).

(3) If $n = 4$, then

$$\rho_p(4,3) = \begin{cases} 1 - \dfrac{40}{3}p^{-4}\left(\dfrac{1-p^{-1}}{1-p^{-3}}\right)^4 & \text{if } p \equiv 1 \bmod 3, \\ 1 & \text{otherwise.} \end{cases}$$

(4) If $n = 5$, then

$$\rho_p(5,3) = \begin{cases} 1 - \dfrac{80}{3}p^{-6}\left(\dfrac{1-p^{-1}}{1-p^{-3}}\right)^6 & \text{if } p \equiv 1 \bmod 3, \\ 1 & \text{otherwise.} \end{cases}$$

(5) If $n \geq 6$, then $\rho_p(n, 3) = 1$ (cf. Lewis [**41**, Theorem 2]).

Note that the value $\rho_\infty(n, 3)$ equals 1 for every $n \in \mathbb{Z}_{\geq 2}$.

When we prove Theorems 3.4 and 3.5, we need to examine whether $X^k_{\boldsymbol{a}}(\mathbb{Q}_p) \neq \emptyset$ or not for infinite many rational primes p and tuples of integers $\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1}$. It seems hard although we can check $X^k_{\boldsymbol{a}}(\mathbb{Q}_p) \neq \emptyset$ easily for each rational prime p and tuple of integers $\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1}$. In order to resolve such difficulty, we introduce an equivalence relation on $\mathbb{Q}_p^{\oplus n+1}$. For more details, see part 1.

4. The proportion of certain genus one curves which have $\mathbb{Q}$-rational points

In part 2 of this thesis, we consider the proportion of certain genus one curves which have $\mathbb{Q}$-rational points.

Let $f(x,y)$ be a binary quartic form over $\mathbb{Q}$, i.e. $f(x,y) = ax^4+bx^3y+cx^2y^2+dxy^3+ey^4$ with $a,b,c,d,e \in \mathbb{Q}$. We call the curve $C_f\colon z^2 = f(x,y)$ *locally soluble* if $C_f(\mathbb{Q}_v) \neq \emptyset$ for all $v \in M_{\mathbb{Q}}$. We also call the curve C_f *soluble* if $C_f(\mathbb{Q}) \neq \emptyset$. In what follows, we also call $f(x,y)$ locally soluble (resp. soluble) when C_f is locally soluble (resp. soluble). For an integral binary quartic form f, the naive height $h(f)$ means the maximum of absolute values of the coefficients of f. Let W be a set of integer binary quartic forms, that is,

$$W = \{f(x,y) = ax^4+bx^3y+cx^2y^2+dxy^3+ey^4 \mid a,b,c,d,e \in \mathbb{Z}\}.$$

Then Bhargava conjectured the following.

Conjecture 4.1 (cf. Bhargava [**3**, Conjecture 7])**.** We have

$$\lim_{X\to\infty} \frac{\#\{f \in W \mid h(f) < H, C_f(\mathbb{Q}) \neq \emptyset\}}{\#\{f \in W \mid h(f) < H, C_f(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in M_{\mathbb{Q}}\}} = \frac{1}{4}.$$

This conjecture is still open, but Bhargava obtained a partial result as follows. Remark that although Bhargava [**3**, Theorem 2] is the result for ternary cubic forms, he also proved the same result for binary quartic forms.

Theorem 4.2 (cf. Bhargava [**3**, Theorem 2 and the last two paragraphs in §1.1]). When locally soluble integral binary quartics $f(x,y)$ are ordered by the naive height, the proportion of soluble forms is positive.

In other words, the above theorem states that

$$\liminf_{H\to\infty} \frac{\#\{f \in W \mid h(f) < H, C_f(\mathbb{Q}) \neq \emptyset\}}{\#\{f \in W \mid h(f) < H,\, C_f(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in M_{\mathbb{Q}}\}} > 0.$$

Note that the proportion of locally soluble forms in integral binary quartic forms is already determined by Poonen–Stoll and Bhargava–Cremona–Fisher.

Theorem 4.3 (Bhargava, Cremona, and Fisher [**4**, Theorem 3], cf. Poonen and Stoll [**55**, Lemma 20]). We have

$$\lim_{H\to\infty} \frac{\#\{f \in W \mid h(f) < H,\, C_f(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in M_{\mathbb{Q}}\}}{\#\{f \in W \mid h(f) < H\}}$$
$$= \frac{23087}{24528} c \prod_{p\,:\,\text{odd prime}} \left(1 - \frac{4p^7+4p^6+2p^5+p^4+3p^3+2p^2+3p+3}{8(p+1)(p^2+p+1)(p^6+p^3+1)}\right),$$

where c is a certain real number satisfying $0.873954 \leq c \leq 0.871424$.

Hence Conjecture 4.1 states that the exact value of the proportion of soluble binary quartic forms is

$$\begin{aligned}&\lim_{H\to\infty} \frac{\#\{f \in W \mid h(f) < H, C_f(\mathbb{Q}) \neq \emptyset\}}{\#\{f \in W \mid h(f) < H\}}\\ &= \frac{1}{4} \times \frac{23087}{24528} c \prod_{p>2} \left(1 - \frac{4p^7 + 4p^6 + 2p^5 + p^4 + 3p^3 + 2p^2 + 3p + 3}{8(p+1)(p^2+p+1)(p^6+p^3+1)}\right).\end{aligned}$$

This can be regarded as the analogy to Conjecture 2.8.

Recently, Bhargava and Ho showed a similar theorem on a subfamily of binary quartics. Before stating their result, we introduce the *Bhargava–Ho height*. For an integral binary quartic $f = ax^4 + Bx^2y^2 + cy^4$, we define the Bhargava–Ho height h_{BH} as

$$h_{\mathrm{BH}}(f) = \max\{B^2, |ac|\}.$$

Then Bhargava–Ho's result is the following.

Theorem 4.4 (Bhargava and Ho [**6**, Theorem 1.6]). When locally soluble integral binary quartic forms $ax^4 + Bx^2y^2 + cy^4$ are ordered by the Bhargava–Ho height, the proportion of soluble forms is 0%.

Comparing the results of Bhargava and Bhargava–Ho, we find that the proportions are different in the two cases. In part 2, we examine the proportion of soluble forms in some other subfamilies. In particular, we find some subfamilies whose proportions of soluble forms are different.

For an integer B and M, we write $W_M^B(\mathbb{Z})$ for the set of binary quartic forms $f(x,y) = ax^4 + Bx^2y^2 + cy^4$ with $a, c \in \mathbb{Z}$ and $ac = M$. We also define

$$\mathcal{F}_M^B = \{ax^4 + Bx^2y^2 + cy^4 \in W_M^B(\mathbb{Z}) \mid 0 \leq \operatorname{ord}_p a \leq 1 \text{ for all primes } p\}.$$

In what follows, we abbreviate squarefree to "sqf.".

Theorem 4.5 ([**33**, Theorem 1.3], see Theorem 11.2). When locally soluble forms $f \in \bigcup_{\substack{n\geq 1\\ n\text{: sqf.}}} \mathcal{F}_{4n^2}^0$ are ordered by the Bhargava–Ho height, the proportion of soluble forms is 100%.

By slightly changing the condition on the coefficients, we obtain the exact opposite result.

Theorem 4.6 ([**33**, Theorem 1.4], see Theorem 12.5). When locally soluble forms $f \in \bigcup_{\substack{n\geq 1\\ n\colon \text{sqf.}}} \mathcal{F}^0_{-n^2}$ are ordered by the Bhargava–Ho height, the proportion of the soluble forms is 0%.

Note that we also obtain similar theorems for four slightly different subfamilies (see Theorem 11.3 and Theorem 12.6).

Bhargava's and Bhargava–Ho's results are related to the average size of the Selmer groups in families of elliptic curves. For example, to prove Theorem 4.2, they first interpret the locally soluble binary quartics as elements of the 2-Selmer group of an elliptic curve. Then Theorem 4.2 is obtained by using the average size of the 2-Selmer groups in all elliptic curves. Similarly, to prove our results, Theorems 4.5 and 4.6, we interpret locally soluble binary quartic forms in $\mathcal{F}^B_M$ as elements of the 2-isogeny or its dual isogeny Selmer groups in the family of elliptic curves $E_n\colon y^2 = x^3 - n^2x$, where n runs over all squarefree positive integers. Then the results follow from the average sizes of those Selmer groups. The average sizes of these Selmer groups in the family have been studied by many researchers. Our results rely on the results of Heath-Brown [**28**] and Xiong–Zaharescu [**68**].

Key facts to prove Theorems 4.5 and 4.6 are the difference in the order between the number of locally soluble quartics and that of soluble quartics. In particular, in the case of Theorem 4.6, there exist much more locally soluble quartics than soluble ones. Hence we next consider whether there are subsets of locally soluble forms comparable to soluble ones in the sense of order. To answer this problem, we introduce the condition which is called *strictly locally soluble*.

Let n be a squarefree integer. A curve $C_f\colon z^2 = f(x,y)$, where $f \in \mathcal{F}^0_{-n^2}$, is called strictly locally soluble if the curve "comes from" 2-Selmer groups of E_n. We will explicitly explain the meaning of "comes from" in §13. In a manner similar to a locally soluble quartic, we call a binary quartic form $f(x,y)$ strictly locally soluble when C_f is strictly locally soluble. Then we answer the above problem of comparable subsets of locally soluble quartics, which is our last theorem.

Theorem 4.7 ([**33**, Theorem 1.5], see Theorem 13.1). The proportion of soluble forms is greater than 42% when strictly locally soluble forms $f \in \bigcup_{\substack{n\geq 1\\ n\colon \text{sqf.}}} \mathcal{F}^0_{-n^2}$ are ordered by the Bhargava–Ho height.

Theorem 4.7 can be considered as the analogy of genus one curves defined by ternary cubic curves. Let $g(x,y,z)$ be a ternary cubic form over $\mathbb{Q}$. For an integer ternary cubic form $g(x,y,z)$, we call $h(x,y,z)$ locally soluble if $D_g(\mathbb{Q}_v) \neq \emptyset$ for all $v \in M_{\mathbb{Q}}$. We also call $h(x, y, z)$ soluble if $D_g(\mathbb{Q}) \neq \emptyset$. As we mentioned, Theorem 4.2 also holds for the ternary cubic forms. In other words, when locally soluble ternary cubics are ordered by the naive height, the proportion of soluble forms is positive. Later, Browning showed a similar theorem for a subfamily of ternary cubic forms:

Theorem 4.8 (cf. Browning [**12**, Theorem 1.3]). When locally soluble integral ternary cubic forms $ax^3 + bx^2y + cxy^2 + dy^3 - z^3$ are ordered by the naive height, the proportion of soluble forms is positive.

The proof of Theorem 4.8 is also similar to Theorem 4.7. More precisely, Browning used Davenport–Heilbronn's result (cf. [**12**, Lemma 3.1]) and Kriz–Li's result ([**40**, Theorem 1.8]) instead of Heath-Brown's result (Lemma 12.3) and Smith's result (Proposition 13.2) respectively.

5. Integer points on PCF varieties

Although our main topic in this thesis is rational points on algebraic varieties, we also discuss the integer points on algebraic varieties.

Let V be an affine variety defined by

$$f_1(x_0, \ldots, x_n) = 0, \ldots, f_r(x_0, \ldots, x_n) = 0$$

where $f_1, \ldots, f_r$ are polynomials with integer coefficients. We say that an integer tuple $(a_1, \ldots, a_n)$ is an integer point on V if the condition

$$f_1(a_1, \ldots, a_n) = 0, \ldots, f_r(a_1, \ldots, a_n) = 0$$

holds. In this section, we consider the problem whether periodic continued fraction varieties have non-degenerate integer points or not. As a consequence, we also determine all $(1, l)$-type periodic integer continued fraction expansions of quadratic irrationals $\sqrt{m}$ for $l = 1, 2, 3$. In the following, we explain more explicitly.

For an integer sequence $\{a_n\}_{n \geq 0}$, let $[a_0, a_1, a_2, \ldots]$ be

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}. \tag{5.1}$$

We say that (5.1) is a regular continued fraction (RCF for short) if $a_n \geq 1$ for all $n \geq 1$. A RCF (5.1) is periodic if there exist $l \in \mathbb{Z}_{\geq 1}$ and $N \in \mathbb{Z}_{\geq 0}$ such that $a_k = a_{l+k}$ for all

$k \geq N$. In the following, we assume that $N = 1$[c] and l is the smallest integer satisfying the periodic condition. We call l the period of a periodic RCF. Let

$$[a_0, \overline{a_1, \ldots, a_l}] := [a_0, a_1, \ldots, a_l, a_1, \ldots, a_l, \ldots]$$

denote a periodic RCF and call it a $(1, l)$-type RCF. It is well-known that every irrational number has a unique RCF expansion. In particular, every quadratic irrational number $\sqrt{m}$ has a $(1, l)$-type RCF expansion for some l.

In this thesis, we consider *periodic integer continued fractions* (PICFs for short). Here, an *integer continued fraction* is (5.1) in which all a_n are integers (not necessarily positive). Of course, the unique periodic RCF expansion of a quadratic irrational number $\sqrt{m}$ is a PICF expansion. However, there are other PICF expansions of $\sqrt{m}$ in general. For example, we obtain

$$\sqrt{2} = [1, \overline{2}] = [-1, \overline{1, -2, 1}].$$

Hence it is natural to consider the following question.

Problem 5.1. For each positive integer l, determine all $(1, l)$-type PICF expansions of a square root of positive nonsquare integer.

In 2021, Brock, Elkies, and Jordan determined all PICF expansion of $\sqrt{2}$ for some types (cf. [**10**, Table 1 in p. 381]). Inspired by their results, we give partial answers to this question for square roots of positive nonsquare integers.

Set

$$\begin{aligned} m_1(t) &:= t^2 + 1, \\ m_2(s, t) &:= s^2 t^2 + t, \\ m_2'(s, t) &:= s^2 t^2 + 2t, \\ m_3(s, t) &:= 16t^2 s^4 + 8ts^3 + (8t^2 + 1)s^2 + 6ts + t^2 + 1. \end{aligned}$$

Then, for each $l = 1, 2, 3$, we give a necessary and sufficient condition for existing PICF expansions of square roots of positive nonsquare integers.

Theorem 5.2. Let m be a positive nonsquare integer.

(1) $\sqrt{m}$ has a $(1, 1)$-type PICF expansion if and only if m is $m_1(t)$ for some $t \in \mathbb{Z}$.

[c] We assume that $N = 1$ since we also consider an application to the solutions of the Pell equations. For details, see §17

(2) $\sqrt{m}$ has a $(1,2)$-type PICF expansion if and only if m is $m_2(s,t)$ or $m_2'(s,t)$ for some $s,t\in\mathbb{Z}$.

(3) $\sqrt{m}$ has a $(1,3)$-type PICF expansion if and only if m is $m_3(s,t)$ for some $s,t\in\mathbb{Z}$.

We also obtain all $(1,l)$-type PICF expansions of square roots of $m_l(s,t)$ for $l=1,2,3$.

Theorem 5.3. For all non-zero integers s, t except for $m_l(s,t)\le 0$, we have $(1,1)$, $(1,2)$, and $(1,3)$-type PICF expansions

$$\operatorname{sgn}(t)\sqrt{m_1(t)}=[t,\overline{2t}], \tag{5.2}$$

$$\operatorname{sgn}(st)\sqrt{m_2(s,t)}=[st,\overline{2s,2st}], \tag{5.3}$$

$$\operatorname{sgn}(st)\sqrt{m_2'(s,t)}=[st,\overline{s,2st}], \tag{5.4}$$

$$\operatorname{sgn}(t)\sqrt{m_3(s,t)}=[s+(4s^2+1)t,\overline{2s,2s,2(s+(4s^2+1)t)}]. \tag{5.5}$$

We further obtain $(1,3)$-type PICF expansions

$$\operatorname{sgn}(t)\sqrt{m_3(0,t)}=[-2+t,\overline{1,-2,-1+2t}]=[-1+t,\overline{2,-1,1+2t}], \tag{5.6}$$

$$\operatorname{sgn}(t)\sqrt{m_3(\pm1,t)}=[2+5t,\overline{-2,3,3+10t}]=[1+5t,\overline{3,-2,3+10t}] \tag{5.7}$$

for $t\in\mathbb{Z}\setminus\{0\}$ and $\sqrt{m_3(\pm1,0)}=\sqrt{2}=[2,\overline{-2,3,3}]=[1,\overline{3,-2,3}]$.

Moreover, these PICFs are all of $(1,1)$, $(1,2)$, and $(1,3)$-type PICF expansions of square roots of positive nonsquare integers.

Note that some of (5.2), (5.3), (5.4) and (5.5) are obtained from classical results. Indeed, we obtain them from Jacobson and Williams [**34**, p. 125, l. 13] if s and t are both positive integers. By using sufficient condition on converging PICFs by Katok and Ugarcovici (see Proposition 16.1), we also check that PICF expansions appeared in RHS of (5.5) converge to $\operatorname{sgn}(t)\sqrt{m_3(s,t)}$ even if s and t are not necessarily positive integers. However, the second part of Theorem 5.3 is not obtained from the above method and we could not find any explicit references which contain (5.6) and (5.7).

To prove Theorems 5.2 and 5.3, we determine all non-degenerate integer points on *periodic continued fraction varieties* (PCF varieties for short). Here, a PCF variety is an algebraic variety such that some integer points on it correspond to PICF expansions of a quadratic irrational number. We will explain the precise definition of PCF varieties in §14.1.

Our main theorem deals with the cases $l=1,2$ and 3. When $l\ge 4$, it seems difficult to obtain a similar result since it may be hard to determine all integer points on PCF varieties. Indeed, the dimensions of PCF varieties grow as l is increased, and simultaneous equations which define PCF varieties become complicated.

Outline of this thesis

In this thesis, our main goal is to prove Theorems 3.1, 3.4, 3.5 and 4.5 to 4.7. We also give the proof of Theorems 5.2 and 5.3 and some applications of them although they are not our main theorems in this thesis.

In part 1, we will prove Theorems 3.1, 3.4 and 3.5. In §6 we introduce an equivalence relation on $\mathbb{Q}_p^{\oplus n+1}$ and recall the Hensel's lemma and the Hasse–Weil bound which we use in the proof. In §7 we give a general upper bound for the value $\rho_p(n,k)$. In fact, $\rho_p(n,k)$ attains this upper bound for a generic p. In §8 we calculate the values $\rho_p(n,k)$ for pathological pairs $(p,k)=(2,2),(3,3)$ and complete the proofs of Theorems 3.4 and 3.5. Our strategy in §8 works also for general n and k in principle. In §9 we prove Theorem 3.1 and discuss a consequence for the proportions of (uni)rationality.

In part 2, we will prove Theorems 4.5 to 4.7. In §10, we prepare some notations or properties which we use in the proof. In §11 (resp. §12, and §13), we state the explicit forms of Theorem 4.5 (resp. Theorem 4.6 and Theorem 4.7) and give their proof.

In part 3, we will prove Theorems 5.2 and 5.3. In §14, we recall fundamental solutions of the Pell equations and PCF varieties. In §15, we determine the set of integer points on some PCF varieties. This is a key ingredient when we prove Theorem 5.3. In §16, we prove Theorems 5.2 and 5.3. In §17, we give some applications of Theorem 5.3 to integer solutions of Pell equations. In §18, instead of $\sqrt{m}$, we consider PCF expansions of certain algebraic integers related to the $\mathbb{Z}_2$-extension over $\mathbb{Q}$. Moreover, we also discuss the relationship between such PCFs and the generalized Pell equations.

Notation

For each abelian group A, let $A^{\oplus n+1}$ denotes the $(n+1)$-th direct sum of A. The following notation is used throughout this thesis. Let $\mathbb{Z}$ be the ring of rational integers and $\mathbb{Q}$, $\mathbb{R}$ be the fields of rational numbers and real numbers respectively. Let $M_{\mathbb{Q}}$ be the set $\{\infty\}\cup\{p : \text{primes}\}$. For each $v\in M_{\mathbb{Q}}$, let $\mathbb{Z}_v$ be the ring of v-adic integers and $\mathbb{Q}_v$ be its field of fractions if v is a prime and $\mathbb{Q}_\infty$ be $\mathbb{R}$. We denote the multiplicative groups of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ by $\mathbb{Z}_p^\times$ and $\mathbb{Q}_p^\times$ respectively. We denote the (additive) p-adic valuation map by $v_p : \mathbb{Q}_p^\times \to \mathbb{Z}$, and we use the same symbol also for its direct sum $v_p : (\mathbb{Q}_p^\times)^{\oplus n+1} \to \mathbb{Z}^{\oplus n+1}$ defined by $v_p(\boldsymbol{a}) := (v_p(a_0),\ldots,v_p(a_n))$ for every $\boldsymbol{a}=(a_0,\ldots,a_n)\in(\mathbb{Q}_p^\times)^{\oplus n+1}$.

Part 1

The proportion of everywhere locally soluble diagonal hypersurfaces

6. Preliminaries

In this section, we introduce a certain equivalence relation on $\mathbb{Q}_p^{\oplus n+1}$. Moreover, we recall the Hensel's lemma and the Hasse–Weil bound.

For every $k, r \in \mathbb{Z}_{\geq 0}$, set $[k] := \{0, 1, \dots, k-1\} \subset \mathbb{Z}$, and let $[k]^{(r)}$ be the set of subsets of $[k]$ consisting of r elements. For every $K = \{k_1, \dots, k_d\} \subset [k]$, set $\boldsymbol{w}(K) := k_1 + \cdots + k_d$. Recall that $X_{\boldsymbol{a}}^k$ is a diagonal hypersurfaces defined by $\sum_{i=0}^n a_i' x_i^k = 0$ where $\boldsymbol{a} \in \mathbb{Q}_p^{\oplus n+1}$.

In a manner similar to Bright, Browning, and Loughran [**9**, §2.1.1], we define an equivalence relation $\simeq$ on $\mathbb{Q}_p^{\oplus n+1}$ as follows. Set $\Gamma_p(n,k) := \mathbb{Q}_p^{\times} \times \big((\mathbb{Q}_p^{\times k})^{\oplus n+1} \rtimes \mathfrak{S}_{n+1}\big)$. Here, the semi-direct product $(\mathbb{Q}_p^{\times k})^{\oplus n+1} \rtimes \mathfrak{S}_{n+1}$ is defined by the natural left permutation action of $\mathfrak{S}_{n+1}$. Define an action of $\Gamma_p(n,k)$ on $\mathbb{Q}_p^{\oplus n+1}$ by

$$(\alpha; \alpha_0^k, \dots, \alpha_n^k; \sigma) \cdot (a_0, \dots, a_n) := (\alpha a_{\sigma(0)} (\alpha_0)^k, \dots, \alpha a_{\sigma(n)} (\alpha_n)^k).$$

Define an equivalence relation $\simeq$ on $\mathbb{Q}_p^{\oplus n+1}$ by $\boldsymbol{a} \simeq \boldsymbol{b}$ if there exists $\gamma \in \Gamma_p(n,k)$ such that $\boldsymbol{a} = \gamma(\boldsymbol{b})$. Then $X_{\boldsymbol{a}}^k$ is isomorphic to $X_{\boldsymbol{b}}^k$ over $\mathbb{Q}_p$ if $\boldsymbol{a} \simeq \boldsymbol{b}$.

Next, we recall the Hensel's lemma and the Hasse–Weil bound.

Proposition 6.1. (Hensel's lemma, cf. Serre [**59**, Chapter II, Theorem 1]) Let $f \in \mathbb{Z}[x_1, \dots, x_m]$, $\alpha = (\alpha_1, \dots, \alpha_m) \in \mathbb{Z}_p^{\oplus m}$, $n, v \in \mathbb{Z}$ and j an integer such that $1 \leq j \leq m$. Suppose that $0 < 2v < n$ and that

$$f(\alpha) \equiv 0 \bmod p^n \text{ and } v_p\left(\frac{\partial f}{\partial x_j}(\alpha)\right) = k.$$

Then there exists $\beta = (\beta_1, \dots, \beta_m) \in \mathbb{Z}_p^{\oplus m}$ such that $\beta_i \equiv \alpha_i \bmod p^{n-v}$ for all $1 \leq i \leq m$ and $f(\beta) = 0$

Proposition 6.2 (Hasse–Weil bound, Weil [**67**])**.** Let p be a prime number and C be a non-singular projective curve of genus g defined over $\mathbb{F}_p$. Then we have

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p}.$$

7. $\rho_p(n,k)$ for generic primes

In this section, we give an explicit formula of $\rho_p(n,k)$ for generic primes p with respect to k. Here, we say that a prime p is *generic with respect to* k if the following conditions hold.

(1) $\gcd(p,k) = 1$.
(2) $p \geq (k-1)^2(k-2)^2$ or $\gcd(p-1,k) = 1$.

Note that for each fixed k almost all but finitely many primes p are generic with respect to k.

Since the set $\mathbb{Q}_p^{\oplus n+1}/\simeq$ is finite, we can calculate $\rho_p(n,k)$ for each fixed n,k,p. In fact, by using the following Proposition 7.3, we can calculate $\rho_p(n,k)$ for many n,k,p uniformly.

In what follows, the measure $\mu_p(\{\boldsymbol{a} \in \mathbb{Z}_p^{\oplus n+1} \mid \cdots\})$ is abbreviated by $\mu_p(\cdots)$. We set

$$\kappa_p(n,k) := \frac{\mu_p\left(v_p(\boldsymbol{a}) \equiv \mathbf{0} \pmod{k}\right)}{\mu_p\left(v_p(\boldsymbol{a}) = \mathbf{0}\right)} = \sum_{e_0,\dots,e_n \geq 0} p^{-ke_0-\cdots-ke_n} = (1-p^{-k})^{-n-1}.$$

Intuitively, this quantity gives the "expansion ratio by $(p^{k\mathbb{Z}_{\geq 0}})^{\oplus n+1}$-action".

Let Δ_n be the set $\left\{\boldsymbol{a} \in \mathbb{Z}_p^{\oplus n+1} \,\middle|\, \prod_{i=0}^{n} a_i = 0\right\}$. Then we have

$$\mu_p(X_{\boldsymbol{a}}^k \text{ is singular}) = \mu_p\left(\Delta_n\right) = 0.$$

Therefore, it is sufficient to consider $\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \setminus \Delta_n$. In the proof of Proposition 7.3, the following Lemma 7.2 is essential. To state Lemma 7.2, we introduce the following definition.

Definition 7.1. Let $n,k \in \mathbb{Z}_{\geq 2}$, p be a prime, and $\boldsymbol{a} \in \mathbb{Z}_p^{\oplus n+1} \setminus \Delta_n$.

(1) If there exist some $u_0,\dots,u_n \in \mathbb{Z}_p^{\times}$ and $k_3,...,k_n \in [k]$ such that

$$\boldsymbol{a} \simeq (u_0, u_1, u_2, p^{k_3}u_3, \dots, p^{k_n}u_n),$$

then we say that $\boldsymbol{a}$ is of type I.

(2) If there exist some $u_1,\dots,u_n,t \in \mathbb{Z}_p^{\times}$, and $k_2,...,k_n \in [k]$ such that

$$\boldsymbol{a} \simeq (u_1, -u_1t^k, p^{k_2}u_2, p^{k_3}u_3, \dots, p^{k_n}u_n),$$

then we say that $\boldsymbol{a}$ is of type II.

(3) If there exist some $r \in \mathbb{Z}_{\geq 0}$, $u_1,\dots,u_{n+1-r} \in \mathbb{Z}_p^{\times}$, $t_1,\dots,t_r \in \mathbb{Z}_p^{\times} \setminus \mathbb{Z}_p^{\times k}$, and distinct $k_1,...,k_{n+1-r} \in [k]$ such that

$$\boldsymbol{a} \simeq (p^{k_1}u_1, -p^{k_1}u_1t_1, \dots, p^{k_r}u_r, -p^{k_r}u_rt_r, p^{k_{r+1}}u_{r+1}, \dots, p^{k_{n+1-r}}u_{n+1-r}), \tag{7.1}$$

then we say that $\boldsymbol{a}$ is of type III.

Note that types I and II are not exclusive.

Lemma 7.2. Let $n,k \in \mathbb{Z}_{\geq 2}$, and p be a prime. Then every $\boldsymbol{a} \in \mathbb{Z}_p^{\oplus n+1} \setminus \Delta_n$ is of type I, II, or III. Moreover the following statements hold.

(1) Suppose that p is generic with respect to k. If $\boldsymbol{a}$ is of type I, then $X_{\boldsymbol{a}}^k(\mathbb{Q}_p) \neq \emptyset$.

(2) If $\boldsymbol{a}$ is of type II, then $X_{\boldsymbol{a}}^k(\mathbb{Q}_p) \neq \emptyset$.

(3) If $\boldsymbol{a}$ is of type III, then $X_{\boldsymbol{a}}^k(\mathbb{Q}_p) = \emptyset$.

Proof. For the former statement, we focus on the p-adic valuations of the components of $\boldsymbol{a}$. We may assume that $0 \leq v_p(a_i) \leq k-1$ for all i. If some three components of $\boldsymbol{a}$ have the same p-adic valuations to each other, then $\boldsymbol{a}$ is of type I. If any two components of $\boldsymbol{a}$ do not have the same p-adic valuations to each other, then $\boldsymbol{a}$ is of type III. In order to treat the remaining cases, by changing the order of the components of $\boldsymbol{a}$, we may assume that $v_p(a_0) = v_p(a_1) < v_p(a_2) = v_p(a_3) < \cdots < v_p(a_{2r}) = v_p(a_{2r+1})$ for some r, and $v_p(a_g) \neq v_p(a_h)$ for every distinct $g \geq 2r+2$ and $h \geq 0$. If at least one of $-a_0/a_1, -a_2/a_3, \ldots, -a_{2r}/a_{2r+1}$ lies in $\mathbb{Z}_p^{\times k}$, then $\boldsymbol{a}$ is of type II. Otherwise, $\boldsymbol{a}$ is of type III. This completes the proof of the former statement.

For the latter statement, we use the same notations in Definition 7.1. More precisely, it is sufficient to consider $\boldsymbol{a} = (a_0, \ldots, a_n)$ such that $\boldsymbol{a} = \ldots$ instead of $\boldsymbol{a} \simeq \ldots$ in Definition 7.1.

(1) If $\gcd(p,k) = 1$ and $p \geq (k-1)^2(k-2)^2$, then by Proposition 6.2, a curve C defined by $u_0x_0^k + u_1x_1^k + u_2x_2^k = 0$ has a smooth $\mathbb{F}_p$-rational point. This $\mathbb{F}_p$-rational point lifts to a $\mathbb{Q}_p$-rational point of C, say $[y_0 : y_1 : y_2]$, by Proposition 6.1. Therefore, $X_{\boldsymbol{a}}^k$ has a $\mathbb{Q}_p$-rational point $[y_0 : y_1 : y_2 : 0 : \cdots : 0]$.

If $\gcd(p,k) = \gcd(p-1,k) = 1$, then we have $\mathbb{Z}_p^{\times} = \mathbb{Z}_p^{\times k}$. In this case, $X_{\boldsymbol{a}}^k$ has a $\mathbb{Q}_p$-rational point $[u_1^{1/k} : (-u_0)^{1/k} : 0 : \cdots : 0]$.

(2) In this case, $X_{\boldsymbol{a}}^k$ has a $\mathbb{Q}_p$-rational point $[t : 1 : 0 : \cdots : 0]$.

(3) We prove the assertion by contradiction. Suppose that $X_{\boldsymbol{a}}^k$ has a $\mathbb{Q}_p$-rational point, say $[x_0 : \cdots : x_n]$ with $x_0, \ldots, x_n \in \mathbb{Z}_p$. Take j so that $v_p(a_jx_j^k) = \min\{v_p(a_lx_l^k) \mid 0 \leq l \leq n\}$. If $0 \leq j \leq 2r-1$, we may assume that j is even. If we divide the defining equation of $X_{\boldsymbol{a}}^k$ by $a_jx_j^k$, then we obtain $1 - t_{j/2+1}(x_{j+1}/x_j)^k \equiv 0 \bmod p$, which contradicts that $t_{j/2+1} \notin \mathbb{Z}_p^{\times k}$. If $2r-1 \leq j \leq n$, then we obtain $1 \equiv 0 \bmod p$, which is a contradiction.

This completes the proof. □

Proposition 7.3. Let $n, k \in \mathbb{Z}_{\geq 2}$, and p be a prime. Then we have

$$\rho_p(n,k) \leq 1 - (n+1)!\left(\frac{1-p^{-1}}{1-p^{-k}}\right)^{n+1} \sum_{r \geq 0} \left(\frac{1}{2} - \frac{1}{2\gcd(p-1,k)}\right)^r \sum_{\substack{K \in [k]^{(r)} \\ L \in [k]^{(n+1-2r)} \\ \text{s.t. } K \cap L = \emptyset}} p^{-2\boldsymbol{w}(K) - \boldsymbol{w}(L)}.$$

Moreover, if p is generic with respect to k, then equality holds. [d]

Here, the sum with respect to r is finite which runs over $\max\{n-k+1,0\} \leq r \leq \min\{[\frac{n+1}{2}],k\}$, where $[x]$ denotes the largest integer not exceeding x.

Proof. The whole statement is a direct consequence of Lemma 7.2. Indeed, since the $\mathfrak{S}_{n+1}$-orbit of $(p^{k_1},p^{k_1},\ldots,p^{k_r},p^{k_r},p^{k_{r+1}},p^{k_{r+2}},\ldots,p^{k_{n+1-r}})$ with distinct $k_i \in [k]$ consists of $(n+1)!/2^r$ vectors, we obtain

$$\begin{aligned}
\rho_p(n,k) &\leq 1-\mu_p\left(\boldsymbol{a} \text{ is of type III}\right)\\
&= 1\\
&-\sum_{r\geq 0}\sum_{\{k_1,\ldots,k_r\}\subset[k]}\sum_{\substack{\{k_{r+1},\ldots,k_{n+1-r}\}\\ \subset[k]\setminus\{k_1,\ldots,k_r\}}} \mu_p\left(\boldsymbol{a} \text{ satisfies (7.1) with some } u_i,t_i\right)\\
&= 1-\sum_{r\geq 0}\sum_{\substack{K=\{k_1,\ldots,k_r\}\in[k]^{(r)}\\ L=\{k_{r+1},\ldots,k_{n+1-r}\}\in[k]^{(n+1-2r)}\\ \text{s.t. } K\cap L=\emptyset}} \frac{(n+1)!}{2^r}p^{-2k_1-\cdots-2k_r-k_{r+1}-\cdots-k_{n+1-r}}\\
&\quad\times \kappa_p(n,k)\\
&\quad\times \mu_p\left(\boldsymbol{a}=(u_1,-u_1t_1,\ldots,u_r,-u_rt_r,u_{r+1},\ldots,u_{n+1-r}) \text{ with some } u_i,t_i\right)\\
&= 1-(n+1)!\sum_{r\geq 0}\frac{1}{2^r}\sum_{\substack{K\in[k]^{(r)}\\ L\in[k]^{(n+1-2r)}\\ \text{s.t. } K\cap L=\emptyset}} p^{-2\,\boldsymbol{w}(K)-\boldsymbol{w}(L)}\\
&\qquad\times (1-p^{-k})^{-(n+1)}\left(1-\frac{1}{\gcd(p-1,k)}\right)^r(1-p^{-1})^{n+1}.
\end{aligned}$$

This completes the claimed inequality. For the last statement, it is sufficient to note that when $p \geq (k-1)^2(k-2)^2$ or $\gcd(p-1,k)=1$, Lemma 7.2 implies that

$$\rho_p(n,k) = 1-\mu_p\left(\boldsymbol{a} \text{ is of type III}\right)$$

in the above argument. □

Remark 7.4. Thanks to Proposition 7.3, in order to determine $\rho_p(n,k)$ for all primes p, it is sufficient to consider the following two kinds of *pathological primes with respect to k*:

[d] In fact, if one of the following conditions holds, then $X^k_{\boldsymbol{a}}(\mathbb{Q}_p) \neq \emptyset$ for all $\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1}\setminus\Delta_n$:

(1) $p \geq (k-1)^2(k-2)^2$ and $n \geq 2k$.
(2) $\gcd(p-1,k)=1$ and $n \geq k$.

In particular, if (1) or (2) holds, then we obtain $\rho_p(n,k)=1$.

(1) $\gcd(p,k) \neq 1$.

(2) $p < (k-1)^2(k-2)^2$ and $\gcd(p-1,k) \neq 1$.

The problems of these cases are as follows:

- In the case (1), every $\mathbb{F}_p$-rational point on a scheme $X^k_{\boldsymbol{a}} \bmod p$ is singular.
- In the case (2), a scheme $X^k_{\boldsymbol{a}} \bmod p$ may not have a $\mathbb{F}_p$-rational point.

Anyway, since the number of pathological primes p with respect to k is finite, we can determine $\rho_p(n,k)$ for all primes p by tour de force and eventually obtain $\rho_{\mathrm{loc}}(n,k)$.

8. $\rho_p(n,k)$ for pathological primes

In this section, we carry out tour de force analysis in order to calculate $\rho_p(n,k)$ for pathological primes p. Although we consider only the cases of $k=2$ and $k=3$, the same method works also for any k in principle.

If $k=2$ (resp. 3), then there is no prime number of second kind in Remark 7.4. Therefore, it is sufficient to calculate $\rho_2(n,2)$ (resp. $\rho_3(n,3)$) as we will do in what follows.

8.1. The case of $k=2$ and $p=2$.

Proposition 8.1 ($p=2$ and $n=2$)**.** Let $u_0,u_1,u_2 \in \mathbb{Z}_2^\times$.

(1) $X^2_{(u_0,u_1,u_2)}$ has a $\mathbb{Q}_2$-rational point if and only if

$$(u_0,u_1,u_2) \simeq (1,1,3),(1,1,7),(1,3,7).$$

(2) $X^2_{(u_0,u_1,2u_2)}$ has a $\mathbb{Q}_2$-rational point if and only if

$$(u_0,u_1,2u_2) \simeq (1,1,6),(1,1,14),(1,5,2),(1,7,2),(1,7,6).$$

In particular, $X^2_{\boldsymbol{a}}$ has a $\mathbb{Q}_2$-rational point if and only if

$$\boldsymbol{a} \simeq (1,1,3),(1,1,7),(1,3,7),(1,1,6),(1,1,14),(1,5,2),(1,7,2),(1,7,6).$$

Proof. (1) We may assume that $u_0=1$ and $u_1,u_2 \in \{1,3,5,7\}$. Moreover, if $u_1=7$ or $u_2=7$, then $X^2_{(1,u_1,u_2)}$ has a rational point. Therefore, it is sufficient to consider the following six cases.

(a) If $(u_1,u_2)=(1,1)$, then we can check that $X^2_{(1,1,1)}$ has no $\mathbb{Q}_2$-rational point. In fact, assume that $X^2_{(1,1,1)}$ has a $\mathbb{Q}_2$-rational point, say $[y_0 : y_1 : y_2]$. Without loss of generality, we may assume that $v_2((y_0,y_1,y_2)) = (0,0,0)$ or $(1,0,0)$. If $v_2((y_0,y_1,y_2)) = (0,0,0)$, then $\sum_{i=0}^2 y_i^2 \equiv 3 \bmod 8$, which is a contradiction. If $v_2((y_0, y_1, y_2)) = (1, 0, 0)$, then $\sum_{i=0}^{2} y_i^2 \equiv 6 \bmod 8$, which is a contradiction.

(b) If $(u_1, u_2) = (1, 3)$, then $X^2_{(1,1,3)}$ has a $\mathbb{Q}_2$-rational point $[\sqrt{-7} : 2 : 1]$.

(c) If $(u_1, u_2) = (1, 5)$, then we can check that $X^2_{(1,1,5)}$ has no $\mathbb{Q}_2$-rational point by an argument similar to (a).

(d) If $(u_1, u_2) = (3, 3)$, then $X^2_{(1,3,3)}$ is isomorphic to $X^2_{(1,1,3)}$ over $\mathbb{Q}_2$ and has a $\mathbb{Q}_2$-rational point.

(e) If $(u_1, u_2) = (3, 5)$, then $X^2_{(1,3,5)}$ is isomorphic to $X^2_{(1,7,3)}$ over $\mathbb{Q}_2$ and has a $\mathbb{Q}_2$-rational point.

(f) If $(u_1, u_2) = (5, 5)$, then $X^2_{(1,5,5)}$ is isomorphic to $X^2_{(1,1,5)}$ over $\mathbb{Q}_2$ and has no $\mathbb{Q}_2$-rational point.

(2) We may assume that $u_2 = 1$ and $u_0, u_1 \in \{1, 3, 5, 7\}$. Note that if $x_0x_1 \equiv 0 \pmod 2$, then $x_0 \equiv x_1 \equiv 0 \pmod 2$ and $x_2 \equiv 0 \pmod 2$. Therefore, it is sufficient to consider rational points such that $x_0, x_1 \in \mathbb{Z}_2^\times$.

(a) If $u_1 \equiv u_0 \pmod 8$, i.e., $u_1 = u_0$, then we have $2u_0 + 2x_3^2 \equiv 0 \pmod 8$, which has a $\mathbb{Z}_2$-solution only if $u_0 \equiv 3 \pmod 4$, i.e., $(u_0, u_1) = (3, 3), (7, 7)$. We can check that $X^2_{(3,3,2)}$ (resp. $X^2_{(7,7,2)}$) has a $\mathbb{Q}_2$-rational point $[x_0 : x_1 : x_2] = [1 : 3 : \sqrt{-15}]$ (resp. $[1 : 1 : \sqrt{-7}]$).

(b) If $u_1 \equiv 3u_0 \pmod 8$, then we have $4u_0 + 2x_3^2 \equiv 0 \pmod 8$, which is impossible.

(c) If $u_1 \equiv 5u_0 \pmod 8$, then we have $6u_0 + 2x_3^2 \equiv 0 \pmod 8$, which has a solution only if $u_0 \equiv 1 \pmod 4$, i.e., $(u_0, u_1) = (1, 5), (5, 1)$. We can check that $X^2_{(1,5,2)}$ has a $\mathbb{Q}_2$-rational point $[x_0 : x_1 : x_2] = [1 : 3 : \sqrt{-23}]$, and $(5, 1, 2) \simeq (1, 5, 2)$.

(d) If $u_1 \equiv 7u_0 \pmod 8$, then $X^2_{(u_0,u_1,u_2)}$ has a $\mathbb{Q}_2$-rational point $[x_0 : x_1 : x_2] = [1 : \sqrt{-7} : 0]$. Note that $(1, 7, 14) \simeq (1, 7, 2)$ and $(1, 7, 10) \simeq (1, 7, 6)$.

This completes the proof. □

Proposition 8.2 ($p = 2$ and $n = 3$)**.** Let $\boldsymbol{a} = (a_0, a_1, a_2, a_3) \in \mathbb{Z}_p^{\oplus 4} \setminus \Delta_3$. Then $X^2_{\boldsymbol{a}}$ has no $\mathbb{Q}_2$-rational point if and only if

$$\boldsymbol{a} \simeq (1, 1, 1, 1), (1, 1, 5, 5), (1, 1, 2, 2), (1, 1, 10, 10), (1, 3, 2, 6), (1, 3, 10, 14), (1, 5, 6, 14).$$

Proof. First of all, we may assume that $a_0 = 1$, $v_2(a_1) = 0$, $0 \le v_2(a_2), v_2(a_3) \le 1$, and $a_i p^{-v_p(a_i)} \in \{1, 3, 5, 7\}$.

(1) Suppose that $v_2(\boldsymbol{a}) = (0,0,0,0)$. If $a_i/a_j \equiv -1 \pmod 8$ for some i,j, then $X^2_{\boldsymbol{a}}$ has a $\mathbb{Q}_2$-rational point such that $(x_i, x_j) = (1, (-a_i/a_j)^{1/2})$. Therefore, it is sufficient to consider the cases $\boldsymbol{a} = (1,1,1,1), (1,1,1,3), (1,1,1,5), (1,1,3,3), (1,1,5,5)$.

  (a) Suppose that $\boldsymbol{a} = (1,1,1,1)$. Then $X^2_{\boldsymbol{a}}$ has no $\mathbb{Q}_2$-rational point.

  (b) Suppose that $\boldsymbol{a} = (1,1,1,3)$. Then $X^2_{\boldsymbol{a}}$ has a $\mathbb{Q}_2$-rational point $[x_0 : x_1 : x_2 : x_3] = [\sqrt{-7} : 2 : 0 : 1]$.

  (c) Suppose that $\boldsymbol{a} = (1,1,1,5), (1,1,3,3)$. Then $X^2_{\boldsymbol{a}}$ has a $\mathbb{Q}_2$-rational point $[x_0 : x_1 : x_2 : x_3] = [\sqrt{-7} : 1 : 1 : 1]$.

  (d) Suppose that $\boldsymbol{a} = (1,1,5,5)$. Then $X^2_{\boldsymbol{a}}$ has no $\mathbb{Q}_2$-rational point.

(2) Suppose that $v_2(\boldsymbol{a}) = (0,0,0,1)$. Then, by the proof of Proposition 8.1 (1), it is sufficient to consider the cases $(a_0, a_1, a_2) = (1,1,1), (1,1,5)$. Moreover, by Proposition 8.1 (2), it is sufficient to consider the cases $(a_0, a_1, a_2, a_3) = (1,1,1,2), (1,1,1,10)$. In each case, $X^2_{\boldsymbol{a}}$ has a $\mathbb{Q}_2$-rational point $[x_0 : x_1 : x_2 : x_3] = [\sqrt{-7} : 1 : 2 : 1], [\sqrt{-15} : 1 : 2 : 1]$ respectively.

(3) Suppose that $v_2(\boldsymbol{a}) = (0,0,1,1)$. Then, by Proposition 8.1 (1), it is sufficient to consider the cases $a_1 \in \{1,3,5\}$.

  (a) Suppose that $a_1 = 1$. Then, by Proposition 8.1 (1), it is sufficient to consider the cases $a_2, a_3 \in \{2, 10\}$. If $(a_2, a_3) = (2, 10)$ (resp. $(10, 2)$), then $X^2_{\boldsymbol{a}}$ has a $\mathbb{Q}_2$-rational point $[x_0 : x_1 : x_2 : x_3] = [2 : 0 : \sqrt{-7} : 1]$ (resp. $[2 : 0 : 1 : \sqrt{-7}]$). If $a_2 = a_3$, then $X^2_{\boldsymbol{a}}$ has no $\mathbb{Q}_2$-rational point.

  (b) Suppose that $a_1 = 3$. Then, by Proposition 8.1 (1), it is sufficient to consider the cases $(a_2, a_3) = (2, 6), (10, 14)$. In both cases, $X^2_{\boldsymbol{a}}$ has no $\mathbb{Q}_2$-rational point.

  (c) Suppose that $a_1 = 5$. Then, by Proposition 8.1 (1), it is sufficient to consider the cases $a_2, a_3 \in \{6, 14\}$. If $a_2 = a_3 = 6$ (resp. $a_2 = a_3 = 14$), then $X^2_{\boldsymbol{a}}$ has a $\mathbb{Q}_2$-rational point $[x_0 : x_1 : x_2 : x_3] = [6 : 0 : \sqrt{-7} : 1]$ (resp. $[14 : 0 : \sqrt{-15} : 1]$). If $a_2 \neq a_3$, then $X^2_{\boldsymbol{a}}$ has no $\mathbb{Q}_2$-rational point.

This completes the proof. □

Remark 8.3. In fact, the $\Gamma_2(3,2)$-orbits of the 7 vectors in the statement of Proposition 8.2 do not intersect each other. We can check it by noting that

- each orbit has a representative whose components lie in $\{1,3,5,7,2,6,10,14\}$,
- in terms of these representatives, the $\Gamma_2(3,2)$-action is reduced to the action of a finite group $2^{\mathbb{Z}}/2^{2\mathbb{Z}} \times \mathbb{Z}_2^{\times}/\mathbb{Z}_2^{\times 2} \times \mathfrak{S}_3$.

Proposition 8.4 ($p = 2$ and $n \geq 4$)**.** Let $n \in \mathbb{Z}_{\geq 4}$ and $\boldsymbol{a} = (a_0, \dots, a_n) \in \mathbb{Z}_2^{\oplus n+1} \setminus \Delta_n$. Then $X_{\boldsymbol{a}}^2$ has a $\mathbb{Q}_2$-rational point.

Proof. First, it is sufficient to consider the case of $n = 4$. By Proposition 8.2, it is sufficient to consider $\boldsymbol{a} = (1, 1, 1, 1, 1)$. In this case, $X_{\boldsymbol{a}}^2$ has a $\mathbb{Q}_2$-rational point $[x_0 : x_1 : x_2 : x_3 : x_4] = [\sqrt{-7} : 2 : 1 : 1 : 1]$. □

Proof of Theorem 3.4. For $p \neq 2$, the statement is immediate from Proposition 7.3. For $p = 2$, the statement is a direct consequence of Propositions 8.1, 8.2 and 8.4 as follows.

(1) For $n = 2$, we have

$$\begin{aligned}
&\rho_2(2,2)\\
&= \mu_2\left(\boldsymbol{a} \simeq (1,1,3), (1,1,7), (1,3,7), (1,1,6), (1,1,14), (1,5,2), (1,7,2), (1,7,6)\right)\\
&= \kappa_2(2,2) \cdot \frac{3 \cdot 4 + 3 \cdot 4 + 3! \cdot 4}{4^3} \cdot \mu_2\left(v_2(\boldsymbol{a}) = (0,0,0), (1,1,1)\right)\\
&\quad + \kappa_2(2,2) \cdot \frac{3 \cdot 4 + 3 \cdot 4 + 3! \cdot 4 + 3! \cdot 4 + 3! \cdot 4}{4^3} \cdot \mu_2\left(v_2(\boldsymbol{a}) = (0,0,1), (1,1,0)\right)\\
&= \frac{2^6}{3^3} \cdot \frac{3}{4} \cdot \left(\frac{1}{2^3} + \frac{1}{2^6}\right) + \frac{2^6}{3^3} \cdot \frac{3}{2} \cdot \left(\frac{1}{2^4} + \frac{1}{2^5}\right)\\
&= \frac{1}{4} + \frac{1}{3}\\
&= \frac{7}{12}.
\end{aligned}$$

Here, in order to obtain the second equality, we use, for example,

$$\{\boldsymbol{a} \in \mathbb{Z}_p^{\oplus 3} \mid \boldsymbol{a} \simeq (1,5,2)\} = \coprod_{k_0,k_1,k_2 \geq 0} (2^{2k_0}, 2^{2k_1}, 2^{2k_2})\mathfrak{S}_3 A$$

and

$$\mu_2(A) = \frac{3! \cdot \#\left(\mathbb{Z}_2/\mathbb{Z}_2^{\times 2}\right)}{\#\left(\mathbb{Z}_2/\mathbb{Z}_2^{\times 2}\right)^3} \mu_2(v_2(\boldsymbol{a}) = (0,0,1), (1,1,0)),$$

where

$$A := \left\{\boldsymbol{a} \in \mathbb{Z}_2^{\oplus 3} \;\middle|\; \boldsymbol{a} = (ut_0, 5ut_1, 2ut_2), (2ut_0, 10ut_1, ut_2) \text{ with } t_i \in \mathbb{Z}_2^{\times 2}, u \in \mathbb{Z}_2^{\times}\right\}.$$

(2) Similarly, for $n = 3$, we have

$$\begin{aligned}
&\rho_2(2,3)\\
&= 1-
\end{aligned}$$

$$
\begin{aligned}
&\mu_2\left(\boldsymbol{a} \simeq (1,1,1,1),(1,1,5,5),(1,1,2,2),(1,1,10,10),(1,3,2,6),(1,3,10,14),(1,5,6,14)\right)\\
&= 1 - \kappa_2(3,2) \cdot \frac{4 + \binom{4}{2} \cdot 2}{4^4} \cdot \mu_2\left(v_2(\boldsymbol{a}) = (0,0,0,0),(1,1,1,1)\right)\\
&\quad - \kappa_2(3,2) \cdot \frac{\binom{4}{2} \cdot 4 + \binom{4}{2} \cdot 4 + 4! \cdot 2 + 4! \cdot 2 + 4! \cdot 2}{4^4} \cdot \mu\left(v_2(\boldsymbol{a}) = (0,0,1,1)\right)\\
&= 1 - \frac{2^8}{3^4} \cdot \frac{4}{4^3} \cdot \left(\frac{1}{2^4} + \frac{1}{2^8}\right) - \frac{2^8}{3^4} \cdot \frac{48}{4^3} \cdot \frac{1}{2^6}\\
&= 1 - \frac{17+48}{2^4 \cdot 3^4}\\
&= \frac{1231}{1296}.
\end{aligned}
$$

(3) For $n \geq 4$, the statement is obvious from Proposition 8.4. □

8.2. The case of $k = 3$ and $p = 3$.

Proposition 8.5 ($p = 3$ and $n = 2$)**.** Let $u_0, u_1, u_2 \in \mathbb{Z}_3^\times$.

(1) $X^3_{(u_0, 3u_1, 9u_2)}$ has no $\mathbb{Q}_3$-rational point.

(2) $X^3_{(u_0, u_1, 9u_2)}$ has a $\mathbb{Q}_3$-rational point if and only if $u_0 \equiv \pm u_1 \pmod 9$.

(3) $X^3_{(u_0, u_1, 3u_2)}$ has a $\mathbb{Q}_3$-rational point.

(4) $X^3_{(u_0, u_1, u_2)}$ has a $\mathbb{Q}_3$-rational point if and only if $\{\pm u_0, \pm u_1, \pm u_2\} \not\equiv \{\pm 1, \pm 2, \pm 4\} \pmod 9$.

Proof. Since $\mathbb{Z}_3^{\times 3} = \pm 1 + 9\mathbb{Z}_3$, we may assume that $u_0, u_1, u_2 \in \{1, 2, 4\}$ by replacing x_i to $w_i x_i$ with some $w_i \in \mathbb{Z}_3^\times$ if necessary.

(1)(2) These are immediate by an argument similar to Proposition 8.1 (1)(a) with calculation of modulo 9 instead of modulo 8.

(3) If $u_0 = u_1$, then our curve has a $\mathbb{Q}_3$-rational point $[x_0 : x_1 : x_2] = [1 : -1 : 0]$. Therefore, it is sufficient to prove that for every $(u_0, u_1) = (1,2), (1,4), (2,4)$

$$u_0 x_0^3 + u_1 x_1^3 + 3 \cdot 1^3 = 0$$

has a $\mathbb{Z}_3$-solution, for instance, $(x_0, x_1) = (-1,-1), (1,-1), ((-7/2)^{1/3}, 1)$ respectively.

(4) By the above argument, it is sufficient to prove that if $(u_0, u_1, u_2) = (1, 2, 4)$, then $X^3_{(1,2,4)}$ has no $\mathbb{Q}_3$-rational point. This can be proven by an argument similar to Proposition 8.1 (1)(a) with calculation of modulo 9 instead of modulo 8.

This completes the proof. □

We define an equivalence relation $\sim$ on the group $\operatorname{Im} v_3 = \mathbb{Z}^{\oplus n+1}$ as the induced equivalence relation by $\simeq$ on $(\mathbb{Q}_3^\times)^{\oplus n+1}$ (cf. Bright, Browning, and Loughran [**9**, §2.2.1]).

Proposition 8.6 ($p = 3$ and $n \geq 3$)**.** Let $n \in \mathbb{Z}_{\geq 3}$ and $\boldsymbol{a} = (a_0, \ldots, a_n) \in \mathbb{Z}_3^{\oplus n+1} \setminus \Delta_n$.

(1) Suppose that $n = 3$. Then $X_{\boldsymbol{a}}^k$ has a $\mathbb{Q}_3$-rational point if and only if one of the following conditions hold:
- $v_3(\boldsymbol{a}) \sim (0,0,0,0)$, $(0,0,0,1)$, $(0,0,1,1)$, or $(0,0,1,2)$.
- $v_3(\boldsymbol{a}) \sim (0,0,0,2)$, and if one normalizes $v_3(\boldsymbol{a})$ so that $v_3(\boldsymbol{a}) = (0,0,0,2)$, then $\{\pm a_0, \pm a_1, \pm a_2\} \not\equiv \{\pm 1, \pm 2, \pm 4\} \pmod 9$.

(2) Suppose that $n \geq 4$. Then $X_{\boldsymbol{a}}^k$ has a $\mathbb{Q}_3$-rational point.

Proof.

(1) For the detail of the case of $n = 3$, see Bright, Browning, and Loughran [**9**, §2.1.2].

(2) For $n \geq 4$, it is sufficient to consider the case of $n = 4$ and $v_3(\boldsymbol{a}) = (0,0,0,2,2)$. In this case, $X^3_{(a_0,a_3,a_4)} \subset X^3_{\boldsymbol{a}}$ has a $\mathbb{Q}_3$-rational point by Proposition 8.5 (3).

This completes the proof. □

Proof of Theorem 3.5. We can prove it in a similar manner to the proof of Theorem 3.4.

(1) Suppose that $n = 2$. By Proposition 7.3, it is sufficient to consider the case of $p = 3$. By Proposition 8.5, we have

$$\begin{aligned}
\rho_3(2,3) &= 1 - \mu_3\left(\boldsymbol{a} \simeq (1,2,4)\right) \\
&\quad - \mu_3\left(\boldsymbol{a} \simeq (u_0, tu_0, 3^2 u_1) \text{ with } u_0, u_1 \in \mathbb{Z}_3^\times, t \in \mathbb{Z}_3^\times \setminus \mathbb{Z}_3^{\times 3}\right) \\
&\quad - \mu_3\left(v_3(\boldsymbol{a}) \sim (0,1,2)\right) \\
&= 1 - \kappa_3(2,3) \cdot \frac{3! \cdot 1}{3^3} \cdot \mu_3\left(v_3(\boldsymbol{a}) = (0,0,0), (1,1,1), (2,2,2)\right) \\
&\quad - \kappa_3(2,3) \cdot \frac{3 \cdot 3^2 \cdot 2}{3^3} \cdot \mu_3\left(v_3(\boldsymbol{a}) = (0,0,2), (1,1,0)\right) \\
&\quad - \kappa_3(2,3) \cdot \frac{3! \cdot 3^3}{3^3} \cdot \mu_3\left(v_3(\boldsymbol{a}) = (0,1,2)\right) \\
&= \frac{13831}{19773}.
\end{aligned}$$

(2) For the detail of the case of $n = 3$, see Bright, Browning, and Loughran [**9**, §2.1].

(3) For $n \geq 4$, the statement is an immediate consequence of Propositions 7.3 and 8.6.

This completes the proof. □

9. Applications

9.1. Proof of Theorem 3.1. Now, we can prove Theorem 3.1.

Proof of Theorem 3.1. Under the assumption with Theorem 3.2 and Theorem 3.3, we have $\rho(n,k) = \rho_{\mathrm{loc}}(n,k) = \prod_{v:\mathrm{place}} \rho_v(n,k)$. Here, note that the local-global principle holds for the case of $k = 2$ (resp. $k = 3$ and $n \geq 6$) due to Serre [**59**, p.48, Theorem 8] (resp. Baker [**2**, Theorem 1]). We can estimate the last infinite product by using the Riemann zeta function $\zeta(s) = \prod_{p:\mathrm{prime}}(1-p^{-s})^{-1}$ $(s \in \mathbb{R}_{>1})$, that is, we obtain the following inequalities which give the desired approximations:

$$\begin{aligned}
\zeta(2)^{-2} \prod_{p<10^6} (1-p^{-2})^{-2} \prod_{p<10^6} \rho_p(3,2) &< \prod_{p:\mathrm{prime}} \rho_p(3,2) < \prod_{p<10^6} \rho_p(3,2),\\
\zeta(2)^{-4} \prod_{p<10^6} (1-p^{-2})^{-4} \prod_{p<10^6} \rho_p(3,3) &< \prod_{p:\mathrm{prime}} \rho_p(3,3) < \prod_{p<10^6} \rho_p(3,3),\\
\zeta(4)^{-15} \prod_{p<10^6} (1-p^{-4})^{-15} \prod_{p<10^6} \rho_p(4,3) &< \prod_{p:\mathrm{prime}} \rho_p(4,3) < \prod_{p<10^6} \rho_p(4,3),\\
\zeta(6)^{-28} \prod_{p<10^6} (1-p^{-6})^{-28} \prod_{p<10^6} \rho_p(5,3) &< \prod_{p:\mathrm{prime}} \rho_p(5,3) < \prod_{p<10^6} \rho_p(5,3). \qquad \square
\end{aligned}$$

Remark 9.1. Bright, Browning, and Loughran [**9**] obtained the formulas of $\rho_p(3,3)$ (σ_p in the notation of [**9**]) correctly. These formulas give the approximation $\rho(3,3) = \rho_{\mathrm{loc}}(3,3) = 0.8964\ldots$. However, they stated that $\rho_{\mathrm{loc}}(3,3)$ (σ in the notation of [**9**]) equals $0.8605\ldots$, which is incorrect.

Remark 9.2. For $k \geq 4$ and $n \geq 3k+2$, Brüdern and Dietmann [**16**, Theorem 1.3] implies that

$$\rho_{\mathrm{loc}}(n,k) - \rho(n,k) \leq \lim_{H\to\infty} \frac{cH^{n+1-\theta}}{(2H+1)^{n+1}} = 0$$

for some $c, \theta \in \mathbb{R}_{>0}$. Hence we obtain $\rho(n,k) = \rho_{\mathrm{loc}}(n,k)$ in these cases without the assumption of the Brauer–Manin obstruction. Since we can express $\rho(n,k)$ by an explicit infinite product, we can approximate $\rho(n,k)$ with arbitrary precision in similar manners to the proof of Theorem 1.1 in principle.

9.2. Rationality and unirationality. In this subsection, we make some remarks on the proportion of $\mathbb{Q}$-rational and $\mathbb{Q}$-unirational hypersurfaces.

Let K be the field of rational numbers $\mathbb{Q}$ or the field of v-adic numbers $\mathbb{Q}_v$ for some place v of $\mathbb{Q}$. Recall that an algebraic variety defined over K is said to be K-rational if it is birationally equivalent to $\mathbb{P}^n$ over K for some n. Set

$$\delta(n,k) := \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \;\middle|\; |\boldsymbol{a}| < H \text{ and } X_{\boldsymbol{a}}^k \text{ is } \mathbb{Q}\text{-rational}\right\}}{\#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \mid |\boldsymbol{a}| < H\right\}}.$$

Proposition 9.3.

$$\delta(n,2) = \rho(n,2) = \begin{cases} 0 & \text{if } n = 2, \\ 0.8268\ldots & \text{if } n = 3, \\ 1 & \text{if } n \geq 4. \end{cases}$$

Proposition 9.3 follows immediately if we apply the following proposition.

Proposition 9.4. Let $Q \subset \mathbb{P}^n$ be a non-singular quadratic hypersurface defined over $\mathbb{Q}$ and $n \in \mathbb{Z}_{\geq 2}$. Then Q is $\mathbb{Q}$-rational if and only if it has a $\mathbb{Q}$-rational point.

Proof. The only if part is trivial. We prove the if part. Indeed, the given non-singular $\mathbb{Q}$-rational point has an open neighborhood isomorphic to an affine quadratic hypersurface $Q' \subset \mathbb{A}^n$ passing through the origin $O = (0, ..., 0)$. Then we can take a Zariski dense subset U of $\mathbb{A}^n$ so that for every $\mathbb{Q}$-rational point A on U the line OA intersects with $Q' \setminus O$ exactly once. This induces a birational (i.e. generically one-to-one and dominant) map of $\mathbb{P}^{n-1}$ to Q', hence Q itself is $\mathbb{Q}$-rational. □

In a similar manner, we can prove a v-adic version of Proposition 9.3. More precisely, if we set $\delta_v(n,2) := \mu_v\left(X_{\boldsymbol{a}}^2 \text{ is } \mathbb{Q}_v\text{-rational}\right)$ for $v \in M_{\mathbb{Q}}$, then we obtain $\delta_v(n,2) = \rho_v(n,2)$ for every $v \in M_{\mathbb{Q}}$. Therefore, combining it with Proposition 9.3, we obtain the product formula

$$\delta(n,2) = \prod_{v \in M_{\mathbb{Q}}} \delta_v(n,2).$$

Moreover, the whole argument works also for the family of all quadratic hypersurfaces of $\mathbb{P}^n$ for every fixed n (cf. Bhargava, Cremona, Fisher, Jones and Keating [**5**]). It is a natural question whether or not similar product formulas hold for other families of geometrically rational algebraic varieties. However, as far as the author knows, there is no reference answering this question for diagonal cubic surfaces.

On the other hand, if we replace "$\mathbb{Q}$-rational" to "$\mathbb{Q}$-unirational", then similar product formulas hold for the families of diagonal cubic hypersurfaces of $\mathbb{P}^n$ ($n \geq 3$). Let K be the field of rational numbers $\mathbb{Q}$ or the field of v-adic numbers $\mathbb{Q}_v$ for some $v \in M_{\mathbb{Q}}$. Recall that an algebraic variety V defined over K is said to be K-unirational if there exists a dominant rational map $\mathbb{P}^n \dashrightarrow V$ over K for some n. Then we obtain the following proposition.

Proposition 9.5. Suppose that the Brauer–Manin obstruction is the only obstruction to the local-global principle for diagonal cubic $(n-1)$-folds if $3 \leq n \leq 5$. Then we obtain

$$\delta'(n,3) = \rho(n,3) = \begin{cases} 0 & \text{if } n = 2, \\ 0.8964\ldots & \text{if } n = 3, \\ 0.9965\ldots & \text{if } n = 4, \\ 0.9999\ldots & \text{if } n = 5, \\ 1 & \text{if } n \geq 6. \end{cases}$$

Moreover, for $n \in \mathbb{Z}_{\geq 2}$, we also obtain $\delta'_v(n,3) = \rho_v(n,3)$ for every $v \in M_{\mathbb{Q}}$ and the product formula

$$\delta'(n,3) = \prod_{v \in M_{\mathbb{Q}}} \delta'_v(n,3).$$

Here, $\delta'(n,3)$ is defined by

$$\delta'(n,3) = \lim_{H \to \infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \mid |\boldsymbol{a}| < H \text{ and } X^3_{\boldsymbol{a}} \text{ is } \mathbb{Q}\text{-unirational}\right\}}{\#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \mid |\boldsymbol{a}| < H\right\}},$$

and $\delta'_v(n,3) := \mu_v(X^3_{\boldsymbol{a}} \text{ is } \mathbb{Q}_v\text{-unirational})$ for $v \in M_{\mathbb{Q}}$.

Note that an analogue of Proposition 9.4 also holds for diagonal cubic hypersurfaces.

Proposition 9.6 (cf. Kollar [**38**, Theorem 1.2], see also Colliot-Thélène, Sansuc and Swinnerton-Dyer [**18**, Remark 2.3.1])**.** Suppose $\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \backslash \Delta_n$. Then $X^3_{\boldsymbol{a}}$ is K-unirational if and only if $X^3_{\boldsymbol{a}}$ has a non-singular K-rational point.

The $\mathbb{Q}$-unirational argument works also for the del Pezzo surfaces defined by

$$\begin{cases} x_0 x_1 = x_2 x_3, \\ \displaystyle\sum_{i=0}^{4} a_i x_i = 0, \end{cases}$$

with $a_i \in \mathbb{Q}$ such that $\prod_{i=0}^{4} a_i(a_0 a_1 - a_2 a_3) \neq 0$ (cf. Mitankin and Salgado [**48**] and Manin [**45**, Theorem 29.4 and Theorem 30.1]).

Part 2

The proportions of soluble binary quartic forms under the everywhere locally soluble ones

10. Preliminaries

In this section, we prepare some notations and recall some properties on certain elliptic curves. We will use them to prove Theorems 4.5 to 4.7.

For integers B and M, we set

$$\begin{aligned} W_M^B(\mathbb{Q}) &= \{f(x,y) = ax^4 + Bx^2y^2 + cy^4 \mid a, c \in \mathbb{Q}, ac = M\}, \\ W_M^B(\mathbb{Z}) &= \{f(x,y) = ax^4 + Bx^2y^2 + cy^4 \mid a, c \in \mathbb{Z}, ac = M\}. \end{aligned}$$

The discriminants and Bhargava–Ho height of $f \in W_M^B(\mathbb{Q})$ is determined by B, M since

$$\mathrm{Disc}(f) = 16M(B^2 - 4M)^2, \tag{10.1}$$

$$h_{\mathrm{BH}}(f) = \max\{B^2, |M|\}. \tag{10.2}$$

In this thesis, we mainly consider the *non-degenerate* quartics, i.e., the quartics with $\mathrm{Disc}(f) \neq 0$. By the above description, the non-degeneracy of $f \in W_M^B(\mathbb{Q})$ only depends on B and M.

A non-degenerate quartic $f(x,y) \in W_M^B(\mathbb{Q})$ defines a genus one curve $C_f \colon z^2 = f(x,y)$ over $\mathbb{Q}$. We write the subsets of $W_M^B(\mathbb{Q})$ of locally soluble (resp. soluble) binary quartic forms as $W_M^B(\mathbb{Q})^{\mathrm{ls}}$ (resp. $W_M^B(\mathbb{Q})^{\mathrm{sol}}$). In concrete terms,

$$\begin{aligned} W_M^B(\mathbb{Q})^{\mathrm{ls}} &= \{f \in W_M^B(\mathbb{Q}) \mid C_f(\mathbb{Q}_v) \neq \emptyset \text{ for all places } v \text{ of } \mathbb{Q}\}, \\ W_M^B(\mathbb{Q})^{\mathrm{sol}} &= \{f \in W_M^B(\mathbb{Q}) \mid C_f(\mathbb{Q}) \neq \emptyset\}. \end{aligned}$$

Similarly we define $W_M^B(\mathbb{Z})^{\mathrm{ls}}$ and $W_M^B(\mathbb{Z})^{\mathrm{sol}}$.

We define an equivalence relation

$$ax^4 + Bx^2y^2 + cy^4 \sim a'x^4 + Bx^2y^2 + c'y^4$$

on $W_M^B(\mathbb{Q})$ if $a' = s^2 a$ and $c' = s^{-2}c$ for some $s \in \mathbb{Q}^\times$. This equivalence preserves solubility and local solubility. We write $[f]$ for the equivalent class of $f \in W_M^B(\mathbb{Q})$. We set

$$\mathcal{F}_M^B(\mathbb{Q}) = \{ax^4 + Bx^2y^2 + cy^4 \in W_M^B(\mathbb{Q}) \mid 0 \leq \mathrm{ord}_p a \leq 1 \text{ for all places } v \text{ in } \mathbb{Q}\}.$$

Then we have $\mathcal{F}_M^B = \mathcal{F}_M^B(\mathbb{Q}) \cap W_M^B(\mathbb{Z})$. The set $\mathcal{F}_M^B(\mathbb{Q})$ (resp. $\mathcal{F}_M^B$) is a complete system of representatives of the equivalence classes in $W_M^B(\mathbb{Q})$ (resp. $W_M^B(\mathbb{Z})$). We also set

$$\begin{aligned} \mathcal{F}_M^{B,\mathrm{sol}} &= \mathcal{F}_M^B \cap W_M^B(\mathbb{Z})^{\mathrm{sol}}, \\ \mathcal{F}_M^{B,\mathrm{ls}} &= \mathcal{F}_M^B \cap W_M^B(\mathbb{Z})^{\mathrm{ls}}. \end{aligned}$$

Next, we recall the definition of the Selmer groups of elliptic curves and some properties of them.

Let E be an elliptic curve and $\varphi\colon E \to E'$ is a nonzero isogeny defined over $\mathbb{Q}$. We write the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as $G_{\overline{\mathbb{Q}}/\mathbb{Q}}$. Then there is an exact sequence of $G_{\overline{\mathbb{Q}}/\mathbb{Q}}$-modules

$$0 \to E[\varphi] \to E \xrightarrow{\varphi} E' \to 0$$

where $E[\varphi]$ denotes the kernel of φ. By taking Galois cohomology, we obtain the long exact sequence

$$0 \to E(\mathbb{Q})[\varphi] \to E(\mathbb{Q}) \xrightarrow{\varphi} E'(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, E[\varphi]) \to H^1(\mathbb{Q}, E) \xrightarrow{\varphi} H^1(\mathbb{Q}, E')$$

and from this we obtain the short exact sequence

$$0 \to E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) \xrightarrow{\delta} H^1(\mathbb{Q}, E[\varphi]) \to H^1(\mathbb{Q}, E)[\varphi] \to 0.$$

Here, we set $H^1(\mathbb{Q}, E[\varphi]) := H^1(G_{\overline{\mathbb{Q}}/\mathbb{Q}}, E[\varphi])$. Repeating the above argument to $\mathbb{Q}_v$ for each $v \in M_{\mathbb{Q}}$, we also obtain

$$0 \to E'(\mathbb{Q}_v)/\varphi(E(\mathbb{Q}_v)) \xrightarrow{\delta} H^1(\mathbb{Q}_v, E[\varphi]) \to H^1(\mathbb{Q}_v, E)[\varphi] \to 0.$$

The natural inclusion $G_{\overline{\mathbb{Q}_v}/\mathbb{Q}_v} \subset G_{\overline{\mathbb{Q}}/\mathbb{Q}}$ and $E(\overline{\mathbb{Q}}) \subset E(\overline{\mathbb{Q}}_v)$ give restriction maps on cohomology. Hence we obtain the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) \arrow[r] \arrow[d] & H^1(\mathbb{Q}, E[\varphi]) \arrow[r] \arrow[d] \arrow[rd, "\beta"] & H^1(\mathbb{Q}, E)[\varphi] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_{v \in M_{\mathbb{Q}}} E'(\mathbb{Q}_v)/\varphi(E(\mathbb{Q}_v)) \arrow[r] & \prod_{v \in M_{\mathbb{Q}}} H^1(\mathbb{Q}_v, E[\varphi]) \arrow[r] & \prod_{v \in M_{\mathbb{Q}}} H^1(\mathbb{Q}_v, E)[\varphi] \arrow[r] & 0.
\end{tikzcd}$$

Then the φ-Selmer group of E is the subgroup of $H^1(\mathbb{Q}, E[\varphi])$ defined by

$$\mathrm{Sel}_{\varphi}(E) = \ker \beta.$$

Note that if we consider the multiplication-by-2 isogeny $[2]\colon E_n \to E_n$ instead of φ, we can define the 2-Selmer group $\mathrm{Sel}_2(E_n)$.

In what follows, we consider the elliptic curves E_n defined by

$$E_n\colon y^2 = x^3 - n^2 x$$

for an integer $n > 0$. We write the point of infinity of E_n as ∞. The curves E_n have three types of isogenies:

$$\begin{aligned}
&\varphi_1 \colon E_n \to E_{1,n} \colon y^2 = x^3 + 4n^2 x, && (x,y) \mapsto \left(\frac{y^2}{x^2}, -\frac{y(n^2+x^2)}{x^2}\right),\\
&\varphi_2 \colon E_n \to E_{2,n} \colon y^2 = x(x^2 - 6nx + n^2), && (x,y) \mapsto \left(\frac{y^2}{(x+n)^2}, \frac{y(2n^2-(x+n)^2)}{(x+n)^2}\right),\\
&\varphi_3 \colon E_n \to E_{3,n} \colon y^2 = x(x^2 + 6nx + n^2), && (x,y) \mapsto \left(\frac{y^2}{(x-n)^2}, \frac{y(2n^2-(x-n)^2)}{(x-n)^2}\right).
\end{aligned}$$

For $i = 1, 2, 3$, we write the dual isogenies of φ_i as $\widehat{\varphi_i}$. We write the weak Mordell–Weil group corresponding to the isogeny φ_i as $E_{i,n}(\mathbb{Q})/\varphi_i(E_n(\mathbb{Q}))$ and similarly for $\widehat{\varphi_i}$. The relation between these isogenies and the set $W_M^B(\mathbb{Q})$ is summarized in the following lemma.

Lemma 10.1 (cf. Silverman [**61**, Proposition X.4.9])**.** For any integer $n \neq 0$, we obtain

$$\begin{aligned}
&\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \cong H^1(\mathbb{Q}, E_n[\varphi_1]) \cong W^0_{4n^2}(\mathbb{Q})/\sim, && d \mapsto \left[dx^4 + \frac{4n^2}{d}y^4\right],\\
&\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \cong H^1(\mathbb{Q}, E_n[\varphi_2]) \cong W^{-6n}_{n^2}(\mathbb{Q})/\sim, && d \mapsto \left[dx^4 - 6nx^2y^2 + (n^2/d)y^4\right],\\
&\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \cong H^1(\mathbb{Q}, E_n[\varphi_3]) \cong W^{6n}_{n^2}(\mathbb{Q})/\sim, && d \mapsto \left[dx^4 + 6nx^2y^2 + (n^2/d)y^4\right],\\
&\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \cong H^1(\mathbb{Q}, E_{1,n}[\widehat{\varphi_1}]) \cong W^0_{-n^2}(\mathbb{Q})/\sim, && d \mapsto \left[dx^4 - \frac{n^2}{d}y^4\right],\\
&\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \cong H^1(\mathbb{Q}, E_{2,n}[\widehat{\varphi_2}]) \cong W^{3n}_{2n^2}(\mathbb{Q})/\sim, && d \mapsto \left[dx^4 + 3nx^2y^2 + 2(n^2/d)y^4\right],\\
&\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \cong H^1(\mathbb{Q}, E_{3,n}[\widehat{\varphi_3}]) \cong W^{-3n}_{2n^2}(\mathbb{Q})/\sim, && d \mapsto \left[dx^4 - 3nx^2y^2 + 2(n^2/d)y^4\right].
\end{aligned}$$

In each case, the set of equivalence classes of locally soluble quartics (resp. soluble quartics) corresponds to the Selmer groups (resp. weak Mordell–Weil groups).

For the quartics in one of six sets appearing in Lemma 10.1, the discriminant and Bhargava–Ho height of the quartics only depend on n by (10.1) and (10.2). In the following, we mainly consider those quartics with $n \neq 0$. In particular, we do not consider degenerate quartics.

In the last part of this section, we cite an integrality lemma analogous to Browning [**12**, Lemma 3.2]. It states that locally soluble quartics in $W_M^B(\mathbb{Q})$ is equivalent to integral ones.

Lemma 10.2 (cf. Silverman and Tate [**62**, Proposition 3.8 (c)])**.** Fix integers $B, M \in \mathbb{Z}$ with $M(B^2 - 4M) \neq 0$. Any equivalence class of $W_M^B(\mathbb{Q})^{\mathrm{ls}}$ contains a unique element of $\mathcal{F}_M^B$.

Proof. The uniqueness follows from the fact that $\mathcal{F}_M^B(\mathbb{Q})$ contains a unique element in each equivalence class of $W_M^B(\mathbb{Q})^{\mathrm{ls}}$. We have to show that for each equivalence class $[f]$ of $W_M^B(\mathbb{Q})$, the unique element in $[f] \cap \mathcal{F}_M^B(\mathbb{Q})$ has integral coefficients.

Take a locally soluble quartic $f(x, y) = ax^4 + Bx^2y^2 + cy^4 \in W_M^B(\mathbb{Q})^{\mathrm{ls}}$. Assume that $f \in \mathcal{F}_M^B(\mathbb{Q})$, or equivalently, that $a \in \mathbb{Z}$ and $0 \leq \operatorname{ord}_p a \leq 1$ for any prime p. Since $a, B \in \mathbb{Z}$, we only have to show that $c \in \mathbb{Z}$. It is enough to prove $\operatorname{ord}_p c \geq 0$ for any prime p.

For a prime p dividing M, we have $\operatorname{ord}_p c \geq 0$ since $ac = M$. Thus, we may assume that $p \nmid M$. Moreover, since $ac = M \in \mathbb{Z}$ and $\operatorname{ord}_p a \leq 1$, we only have to consider the case where $(\operatorname{ord}_p a, \operatorname{ord}_p c) = (1, -1)$.

Since f is locally soluble, we may take a nontrivial solution (Z, X, Y) of $z^2 = f(x, y)$ in $\mathbb{Q}_p$. By scaling, we may assume $X, Y, Z \in \mathbb{Z}_p$. Then we have the following:

- The two values $\operatorname{ord}_p(aX^4), \operatorname{ord}_p(cY^4)$ are odd and distinct because
$$\operatorname{ord}_p(aX^4) \equiv 1 \bmod 4 \ \text{ and } \ \operatorname{ord}_p(cY^4) \equiv -1 \bmod 4.$$
- We would like to compare $\operatorname{ord}_p(nX^2Y^2)$ with $\operatorname{ord}_p(aX^4)$ and $\operatorname{ord}_p(cY^4)$. Since $p \nmid M$, we compute
$$\begin{aligned}\operatorname{ord}_p(aX^4) + \operatorname{ord}_p(cY^4) &= \operatorname{ord}_p(acX^4Y^4)\\ &= \operatorname{ord}_p(M) + \operatorname{ord}_p(X^4Y^4)\\ &= \operatorname{ord}_p(X^4Y^4)\\ &= 2\operatorname{ord}_p(X^2Y^2).\end{aligned}$$
Thus, we obtain $(\operatorname{ord}_p(aX^4) + \operatorname{ord}_p(cY^4))/2 = \operatorname{ord}_p(X^2Y^2)$.

Combining the above two observations, we have
$$\begin{aligned}&\operatorname{ord}_p(aX^4) > \operatorname{ord}_p(X^2Y^2) > \operatorname{ord}_p(cY^4),\\ \text{or } &\operatorname{ord}_p(aX^4) < \operatorname{ord}_p(X^2Y^2) < \operatorname{ord}_p(cY^4).\end{aligned}$$
It is enough to consider the former case. Since $B \in \mathbb{Z}$, we have two inequalities
$$\operatorname{ord}_p(aX^4) > \operatorname{ord}_p(cY^4) \ \text{ and } \ \operatorname{ord}_p(BX^2Y^2) > \operatorname{ord}_p(cY^4).$$
These conclude
$$\operatorname{ord}_p(aX^4 + BX^2Y^2 + cY^4) = \operatorname{ord}_p(cY^4),$$

and the value is odd. However, it contradicts $Z^2 = aX^4 + BX^2Y^2 + cY^4$ since $\mathrm{ord}_p(Z^2)$ is even. $\square$

Applying Lemma 10.2 to six cases in Lemma 10.1, we see that each element in the Selmer groups of the isogenies $\varphi_i, \widehat{\varphi}_i$ has a unique representative of binary quartics in $\mathcal{F}_M^B$ for appropriate B, M. Thus in order to count elements in $\mathcal{F}_M^{B,\mathrm{loc}}$, it is sufficient to count elements of the Selmer groups corresponding to the elements in $\mathcal{F}_M^{B,\mathrm{loc}}$.

11. Proof of Theorem 4.5

Now we prove Theorem 4.5. For $h \in \{\pm 1, \pm 2, \pm 3\}$, define

$$S(X, h) = \{D \in \mathbb{Z} \mid D \equiv h \bmod 8,\ 1 \leq D \leq X,\ \ D : \text{squarefree}\}.$$

The number of elements is estimated as

$$\#S(X, h) = \frac{1}{\pi^2} X + o(X)$$

as $X \to \infty$. For more detailed estimation, see the proof of Xiong and Zaharescu [**68**, Lemma 14].

Lemma 11.1 (Xiong and Zaharescu [**68**, Theorem 6])**.** For $i \in \{1, 2, 3\}$, one has

$$\sum_{n \in S(X,h)} \#\mathrm{Sel}_{\varphi_i}(E_n) = \#S(X, h) + o(X)$$

as $X \to \infty$. In particular, the contribution of nontrivial elements in $\mathrm{Sel}_{\varphi_i}(E_n)$ is estimated as $o(X)$.

Proof. For $h = \pm 1, \pm 3$, see the proof of Xiong and Zaharescu [**68**, Theorem 6].

In the following, we consider the case when $h = \pm 2$ and $i = 1$. In a similar manner, we can treat the other cases when $h = \pm 2$ and $i = 2, 3$. Suppose $p \neq 2$. The conditions on n, d for the existence of $\mathbb{Q}_p$-rational points on $C_{1,d}$ are given by Feng and Xiong [**23**, Lemma 3.1 (1)-(3)]. For the case $h = \pm 1, \pm 3$, we obtain

$$\begin{aligned}\sum_{n \in S(X,h)} \#\mathrm{Sel}_{\varphi_1}(E_n) &\leq \sum_{n = dd'} \prod_{\substack{p \mid d \\ p \neq 2}} \frac{1}{4} \left(\left(\frac{-1}{p} \right) + 1 \right) \left(\left(\frac{d'}{p} \right) + 1 \right) \prod_{\substack{p \mid d' \\ p \neq 2}} \frac{1}{2} \left(\left(\frac{d}{p} \right) + 1 \right) \\ &= \#S(X, h) + o(X)\end{aligned}$$

as $X \to \infty$. Here, $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. Moreover, we obtain

$$\#S(X,h) \le \sum_{n \in S(X,h)} \#\mathrm{Sel}_{\varphi_1}(E_n)$$

by counting the trivial elements of $\mathrm{Sel}_{\varphi_1}(E_n)$. Hence we complete the proof. □

Now, we will prove Theorem 4.5. We can rewrite Theorem 4.5 explicitly as

$$\lim_{X\to\infty} \frac{\#\{f \in \mathcal{F}^{0,\mathrm{sol}}_{4n^2} \mid n\colon \text{sqf. and } h_{\mathrm{BH}}(f) = 4n^2 < X\}}{\#\{f \in \mathcal{F}^{0,\mathrm{ls}}_{4n^2} \mid n\colon \text{sqf. and } h_{\mathrm{BH}}(f) = 4n^2 < X\}} = 1. \tag{11.1}$$

The left hand side quantity is equal to

$$\lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<\sqrt{X}/2 \\ n\colon \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{4n^2}}{\displaystyle\sum_{\substack{0<n<\sqrt{X}/2 \\ n\colon \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{ls}}_{4n^2}},$$

so that by writing X instead of $\sqrt{X}/2$, we only have to show the following theorem.

Theorem 11.2. We obtain

$$\lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{4n^2}}{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{ls}}_{4n^2}} = 1.$$

Proof. Using Lemma 10.2, we can freely interpret elements of the Selmer group $\mathrm{Sel}_{\varphi_1}(E_n)$ as elements in $\mathcal{F}^{0,\mathrm{ls}}_{4n^2}$ under the bijection in Lemma 10.1.

In Lemma 11.1, the main term $\#S(X,h)$ comes from identity elements of the Selmer groups $\mathrm{Sel}_{\varphi_1}(E_n)$, and the other elements are negligible. Since elements of $\mathcal{F}^{0,\mathrm{ls}}_{4n^2}$ which come from identities are soluble, the inequalities

$$\begin{aligned}\sum_{h=\pm1,\pm2,\pm3} \#S(X,h) = \sum_{\substack{0<n<X \\ n\colon \text{sqf.}}} 1 \le \sum_{\substack{0<n<X \\ n\colon \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{4n^2} &\le \sum_{\substack{0<n<X \\ n\colon \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{ls}}_{4n^2} \\ &\le \sum_{h=\pm1,\pm2,\pm3} \#S(X,h) + o(X)\end{aligned}$$

hold as $X \to \infty$. Hence we obtain

$$\frac{\displaystyle\sum_{\substack{0<n<X\\ n\text{: sqf.}}} \#\mathcal{F}_{4n^2}^{0,\mathrm{sol}}}{\displaystyle\sum_{\substack{0<n<X\\ n\text{: sqf.}}} \#\mathcal{F}_{4n^2}^{0,\mathrm{ls}}} \to 1$$

as $X \to \infty$. □

In a similar manner to $\mathrm{Sel}_{\varphi_1}(E_n)$, we also obtain the following theorem for $\mathrm{Sel}_{\varphi_2}(E_n)$ and $\mathrm{Sel}_{\varphi_3}(E_n)$.

Theorem 11.3. We obtain

$$\lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X\\ n\text{: sqf.}}} \#\mathcal{F}_{n^2}^{6n,\mathrm{sol}}}{\displaystyle\sum_{\substack{0<n<X\\ n\text{: sqf.}}} \#\mathcal{F}_{n^2}^{6n,\mathrm{ls}}} = \lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X\\ n\text{: sqf.}}} \#\mathcal{F}_{n^2}^{-6n,\mathrm{sol}}}{\displaystyle\sum_{\substack{0<n<X\\ n\text{: sqf.}}} \#\mathcal{F}_{n^2}^{-6n,\mathrm{ls}}} = 1.$$

12. Proof of Theorem 4.6

In §12.1, we employ results on the 2-Selmer groups to estimate soluble binary quartic forms. Later in §12.2, we prove Theorem 4.6.

12.1. Results on 2-coverings. We set $n = D_1D_2D_3D_4$ for pairwise coprime integers $D_1, D_2, D_3, D_4 > 0$ and $\mathcal{C} = \mathcal{C}(D_1, D_2, D_3, D_4)$ is the genus one curve defined by

$$\mathcal{C}(D_1, D_2, D_3, D_4)\colon \begin{cases} D_1X^2 + D_4W^2 = D_2Y^2, \\ D_1X^2 - D_4W^2 = D_3Z^2. \end{cases}$$

As the following lemma says, this curve represents 2-coverings of E.

Lemma 12.1. (cf. Silverman [**61**, X.4.5.1], Heath-Brown [**28**, Lemma 1]) Let n be a squarefree integer. Then the 2-Selmer group $\mathrm{Sel}_2(E_n)$ is bijective to the set

$$\left\{ (D_1, D_2, D_3, D_4) \;\middle|\; \begin{array}{c} D_1, D_2, D_3, D_4 \in \mathbb{Z}_{>0} \text{ are pairwise coprime,} \\ n = D_1D_2D_3D_4, \\ \mathcal{C}(D_1, D_2, D_3, D_4)(\mathbb{Q}_v) \neq \emptyset \text{ for all places } v \text{ of } \mathbb{Q}. \end{array} \right\}.$$

We quote the following lemma on the existence of local solutions for $\mathcal{C}$. Although Heath-Brown treated only the case when n is odd in [**28**], the following statements are valid when n is even and squarefree.

Lemma 12.2. (Heath-Brown [**28**, pp. 175-176]) Let p be ∞ or an odd prime.

(1) $\mathcal{C}(\mathbb{Q}_\infty) \neq \emptyset$, where $\mathbb{Q}_\infty = \mathbb{R}$.
(2) If $p \nmid 2n$, then $\mathcal{C}(\mathbb{Q}_p) \neq \emptyset$.
(3) If $p \mid D_1$, then $\mathcal{C}(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{D_4 D_2}{p}\right) = \left(\frac{-D_4 D_3}{p}\right) = 1$.
(4) If $p \mid D_2$, then $\mathcal{C}(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{-D_1 D_4}{p}\right) = \left(\frac{2D_1 D_3}{p}\right) = 1$.
(5) If $p \mid D_3$, then $\mathcal{C}(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{D_1 D_4}{p}\right) = \left(\frac{2D_1 D_2}{p}\right) = 1$.
(6) If $p \mid D_4$, then $\mathcal{C}(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{D_1 D_2}{p}\right) = \left(\frac{D_1 D_3}{p}\right) = 1$.

Lemma 12.3. For $h = \pm 1, \pm 2, \pm 3$, we have

$$\sum_{n \in S(X,h)} \#\mathrm{Sel}_2(E_n) \leq 12\#S(X,h) + o(X)$$

as $X \to \infty$.

Proof. For the case where h is odd, more strict estimate is given in Heath-Brown [**28**, Theorem 1]. To consider the case where h is even, we briefly sketch the proof (for the details, see Heath-Brown [**28**]).

By Lemma 12.1, it is enough to count the quadruples of pairwise coprime positive integers (D_1, D_2, D_3, D_4) such that $\mathcal{C}(D_1, D_2, D_3, D_4)$ has $\mathbb{Q}_v$-rational points for any place v of $\mathbb{Q}$.

For odd primes v and $v = \infty$, Lemma 12.2 gives the condition under which the curve $\mathcal{C}(D_1, D_2, D_3, D_4)$ has a $\mathbb{Q}_v$-rational point. When $v = 2$, Heath-Brown [**28**, Lemma 2] states that the existence of $\mathbb{Q}_2$-rational points in $\mathcal{C}(D_1, D_2, D_3, D_4)$ is determined by the existence of $\mathbb{Q}_v$-rational points for every $v \in M_\mathbb{Q} \setminus \{2\}$. By counting coefficients satisfying the local conditions for any odd prime v and $v = \infty$, we obtain the desired estimation.

For the case where h is even, we apply Lemma 12.1 again and reduce to count the quadruples of integers. For odd primes v or $v = \infty$, the conditions for the existence of $\mathbb{Q}_v$-rational points are the same as those of Lemma 12.2. To obtain an estimation from above, we ignore the condition on $v = 2$. □

12.2. Proof of Theorem 4.6. First, we show the following lemma, which is essential when we evaluate the number of locally soluble integral quartics.

Lemma 12.4 (Xiong and Zaharescu [**68**, p. 47. (9)])**.** Define

$$s(n, \widehat{\varphi_i}) := \dim_{\mathbb{F}_2} \mathrm{Sel}_{\widehat{\varphi_i}}(E_{i,n}) - 2.$$

For each $h = \pm 1, \pm 3$ and $i \in \{1, 2, 3\}$, we obtain

$$\sum_{n \in S(X,h)} s(n, \widehat{\varphi}_i) = \frac{\# S(X,h) \log\log X}{2} + O(X)$$

as $X \to \infty$.

Before we begin to prove Theorem 4.6, we show the explicit statement of Theorem 4.6. As a similar manner to (11.1), we can rewrite Theorem 4.6 explicitly as

$$\lim_{X \to \infty} \frac{\#\{f \in \mathcal{F}^{0,\mathrm{sol}}_{-n^2} \mid n\text{: sqf. and } h_{\mathrm{BH}}(f) = n^2 < X\}}{\#\{f \in \mathcal{F}^{0,\mathrm{ls}}_{-n^2} \mid n\text{: sqf. and } h_{\mathrm{BH}}(f) = n^2 < X\}} = 0.$$

Hence, by changing $\sqrt{X}$ to X, it is sufficient to show the following theorem.

Theorem 12.5. We obtain

$$\lim_{X \to \infty} \frac{\displaystyle\sum_{\substack{0<n<X \\ n\text{: sqf.}}} \# \mathcal{F}^{0,\mathrm{sol}}_{-n^2}}{\displaystyle\sum_{\substack{0<n<X \\ n\text{: sqf.}}} \# \mathcal{F}^{0,\mathrm{ls}}_{-n^2}} = 0.$$

Proof. We estimate the denominator and the numerator independently. First, consider the denominator. From Lemmas 10.1 and 12.4, we obtain

$$\begin{aligned}
\sum_{\substack{0<n<X \\ n\text{: sqf.}}} \# \mathcal{F}^{0,\mathrm{ls}}_{-n^2} &\geq \sum_{\substack{0<n<X \\ n\text{: sqf. and odd}}} \# \mathrm{Sel}_{\widehat{\varphi_1}}(E_{1,n}) \\
&= \sum_{\substack{0<n<X \\ n\text{: sqf. and odd}}} 2^{2+s(n,\widehat{\varphi_1})} \\
&= 4 \sum_{\substack{0<n<X \\ n\text{: sqf. and odd}}} (1+1)^{s(n,\widehat{\varphi_1})} \\
&\geq 4 \sum_{\substack{0<n<X \\ n\text{: sqf. and odd}}} (1 + s(n, \widehat{\varphi_1})) \\
&= 4 \times 4 \times \frac{X \log\log X}{2\pi^2} + O(X) \\
&= \frac{8X \log\log X}{\pi^2} + O(X)
\end{aligned}$$

as $X \to \infty$.

Next, we consider the numerator. By Lemma 10.2, the natural map

$$\mathcal{F}^{0,\mathrm{sol}}_{-n^2} \to W^0_{-n^2}(\mathbb{Q})^{\mathrm{sol}}/\!\sim$$

is bijective for each n. By Lemma 10.1, the set $W^0_{-n^2}(\mathbb{Q})^{\mathrm{sol}}/\!\sim$ is bijective to the weak Mordell–Weil group $E_n(\mathbb{Q})/\widehat{\varphi_1}(E_{1,n}(\mathbb{Q}))$. Since there are a surjection

$$E_n(\mathbb{Q})/\widehat{\varphi_1}(E_{1,n}(\mathbb{Q})) \twoheadleftarrow E_n(\mathbb{Q})/2E_n(\mathbb{Q})$$

and an inclusion

$$E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \subseteq \mathrm{Sel}_2(E_n),$$

we can bound $\#\mathcal{F}^{0,\mathrm{sol}}_{-n^2}$ for each n from above as

$$\#\mathcal{F}^{0,\mathrm{sol}}_{-n^2} \leq \#\mathrm{Sel}_2(E_n).$$

Summing this estimate up over sqf. n, we obtain

$$\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{-n^2} \leq \sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathrm{Sel}_2(E_n) \leq O(X)$$

as $X \to \infty$ by Lemma 12.3. Hence we conclude that

$$\frac{\displaystyle\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{-n^2}}{\displaystyle\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{ls}}_{-n^2}} \leq \frac{O(X)}{8X\log\log X/\pi^2 + O(X)} \to 0$$

as $X \to \infty$ and complete the proof. □

In a similar manner to the case of $i = 1$, we can also show the case of $i = 2$ and 3.

Theorem 12.6. We obtain

$$\lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{3n,\mathrm{sol}}_{2n^2}}{\displaystyle\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{3n,\mathrm{ls}}_{2n^2}} = \lim_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{-3n,\mathrm{sol}}_{2n^2}}{\displaystyle\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{-3n,\mathrm{ls}}_{2n^2}} = 0.$$

13. Proof of Theorem 4.7

Since φ_1 maps $E_n[2]$ to $E_{1,n}[\widehat{\varphi_1}]$ (cf. Aoki [**1**, 2nd paragraph in p. 79]), the map φ_1 induces the natural homomorphisms

$$H^1(\mathbb{Q}, E_n[2]) \to H^1(\mathbb{Q}, E_{1,n}[\widehat{\varphi}_1])\ ;\ (\sigma \mapsto P_\sigma) \mapsto (\sigma \mapsto \varphi_1(P_\sigma))$$

and

$$\pi_1 \colon \mathrm{Sel}_2(E_n) \to \mathrm{Sel}_{\widehat{\varphi_1}}(E_{1,n}).$$

We say a binary quartic form $f \in W^0_{-n^2}(\mathbb{Z})^{\mathrm{ls}}$ is *strictly locally soluble* if the element in the Selmer group $\mathrm{Sel}_{\widehat{\varphi_1}}(E_{1,n})$ corresponding to f is in the image of π_1. We write the subset of $W^0_{-n^2}(\mathbb{Z})$ of strictly locally soluble binary quartic forms as $W^0_{-n^2}(\mathbb{Z})^{\mathrm{sls}}$.

The set $W^0_{-n^2}(\mathbb{Z})^{\mathrm{sol}}$ is a subset of $W^0_{-n^2}(\mathbb{Z})^{\mathrm{sls}}$. In fact, this follows from Lemma 10.1 and the following commutative diagram (cf. Aoki [**1**, p. 97]):

$$\begin{tikzcd}
0 \arrow[r] & E_{1,n}(\mathbb{Q})/\varphi_1(E_n(\mathbb{Q})) \arrow[r] \arrow[d] & E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \arrow[r] \arrow[d] & E_n(\mathbb{Q})/\widehat{\varphi_1}(E_{1,n}(\mathbb{Q})) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Sel}_{\varphi_1}(E_n) \arrow[r] & \mathrm{Sel}_2(E_n) \arrow[r, "\pi_1"] & \mathrm{Sel}_{\widehat{\varphi_1}}(E_{1,n}). &
\end{tikzcd}$$

In a similar manner to $\mathcal{F}^{0,\mathrm{sol}}_{-n^2}$ or $\mathcal{F}^{0,\mathrm{ls}}_{-n^2}$, we define $\mathcal{F}^{0,\mathrm{sls}}_{-n^2}$ as $\mathcal{F}^{0}_{-n^2} \cap W^0_{-n^2}(\mathbb{Z})^{\mathrm{sls}}$. Now we restate Theorem 4.7 in a rigorous form. As in Theorems 4.5 and 4.6, it is sufficient to show the following theorem.

Theorem 13.1. We have

$$\liminf_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{-n^2}}{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{0,\mathrm{sls}}_{-n^2}} \geq \frac{2.559}{6}.$$

In the rest of this section, we will prove this theorem. To prove it, we estimate the denominator and the numerator independently. First, consider the denominator.

The number of strictly locally soluble forms are bounded above by the number of elements of the 2-Selmer groups. This leads us to estimate

$$\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{0,\mathrm{sls}}_{-n^2} \leq \sum_{h\in\{\pm1,\pm2,\pm3\}} \sum_{n\in S(X,h)} \#\mathrm{Sel}_2(E_n)$$

$$\leq 6 \times 12 \times \frac{1}{\pi^2} X + o(X) \tag{13.1}$$

as $X \to \infty$. Here, the last inequality follows from Lemma 11.1.

Next, consider the numerator. When we evaluate the number of soluble forms, the following proposition plays an important role.

Proposition 13.2 (Smith [**65**, Theorem 1.5], cf. Li [**42**, Theorem 5.3])**.** Consider the family of elliptic curves $\{E_n \mid n\text{: sqf. and } n \equiv -1, -2, -3 \pmod 8\}$. In this family, the proportion of the curves with $\operatorname{rank}_{\mathbb{Q}}(E_n) = 1$ is at least 55.9%.

Proof. By Smith [**65**, Theorem 1.5], the analytic rank of E_n is equal to one for at least $62.9\%, 41.9\%$ and 62.9% of squarefree integers n with $n \equiv -1, -2$ and $-3 \pmod 8$ respectively. Hence, in the family of elliptic curves $\{E_n \mid n \text{ is sqf. and } n \equiv -1, -2, -3 \pmod 8\}$, the proportion of elliptic curves E_n whose analytic rank is equal to one is at least $(62.9 + 41.9 + 62.9)/3 = 55.9\%$. Combining with the results of Gross and Zagier [**26**] and Kolyvagin [**39**], we deduce that the same is true for the arithmetic rank. □

We need another proposition on the structure of the Mordell–Weil groups of E_n. Recall that the following theorem holds.

Theorem 13.3 (Mordell's theorem, cf. Silverman [**61**, ChapterVIII, Theorem 4.1]). Let E be an elliptic curve defined by $\mathbb{Q}$. Then the group $E(\mathbb{Q})$ is finitely generated.

Thanks to this theorem, a group $E(\mathbb{Q})$ can be written as $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$, where $E(\mathbb{Q})_{\mathrm{tors}}$ is the torsion subgroup of $E(\mathbb{Q})$ and r is a non-negative integer in general. Hence let us write the torsion part of $E_n(\mathbb{Q})$ as T, and the torsion part of $E_{1,n}(\mathbb{Q})$ as T_1. Since $\widehat{\varphi_1}$ is a morphism of degree 2, we have $\widehat{\varphi_1}(T_1) \subseteq T$. Moreover, we can take subgroups $A \subseteq E_n(\mathbb{Q})$ and $A_1 \subseteq E_{1,n}(\mathbb{Q})$ such that

$$E_n(\mathbb{Q}) \cong T \times A, \quad E_{1,n}(\mathbb{Q}) \cong T_1 \times A_1,$$

and $\widehat{\varphi_1}(A_1) \subseteq A$. Note that A, and A_1 are free of rank r. By these, we can consider the decompositions

$$E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \cong T/2T \times A/2A, \tag{13.2}$$

$$E_n(\mathbb{Q})/\widehat{\varphi_1}(E_{1,n}(\mathbb{Q})) \cong T/\widehat{\varphi_1}(T_1) \times A/\widehat{\varphi_1}(A_1). \tag{13.3}$$

The following proposition states that the contribution of the torsion parts does not depend on $n > 1$.

Proposition 13.4. When $n > 1$, we have

$$r = \dim_{\mathbb{F}_2} A/2A = \dim_{\mathbb{F}_2} \frac{E_n(\mathbb{Q})}{2E_n(\mathbb{Q})} - 2,$$
$$\dim_{\mathbb{F}_2} A/\widehat{\varphi_1}(A_1) = \dim_{\mathbb{F}_2} \frac{E_n(\mathbb{Q})}{\widehat{\varphi_1}(E_{1,n}(\mathbb{Q}))} - 2.$$

Proof. The natural inclusion $E_n(\mathbb{Q})[2] \hookrightarrow E_n(\mathbb{Q})$ and the natural surjection $E_n(\mathbb{Q}) \twoheadrightarrow E_n(\mathbb{Q})/2E_n(\mathbb{Q})$ give a composite map

$$E_n(\mathbb{Q})[2] \to \frac{E_n(\mathbb{Q})}{2E_n(\mathbb{Q})}. \tag{13.4}$$

Since $\widehat{\varphi_1} \circ \varphi_1 = [2]$, there is also a natural surjection

$$\frac{E_n(\mathbb{Q})}{2E_n(\mathbb{Q})} \twoheadrightarrow \frac{E_n(\mathbb{Q})}{\widehat{\varphi_1}(E_{1,n}(\mathbb{Q}))}. \tag{13.5}$$

By the decompositions (13.2) and (13.3), the maps (13.4) and (13.5) give two homomorphisms

$$E_n(\mathbb{Q})[2] \to T/2T, \tag{13.6}$$
$$T/2T \twoheadrightarrow T/\widehat{\varphi_1}(T_1). \tag{13.7}$$

Recall that $\#E_n(\mathbb{Q})[2] = 4$. Thus, in order to prove the proposition, it is sufficient to show that $E_n(\mathbb{Q})[2]$, $T/2T$ and $T/\widehat{\varphi_1}(T_1)$ are isomorphic by the homomorphisms (13.6) and (13.7).

We show that the composition map of (13.6) and (13.7) is injective. This amounts to show $\widehat{\varphi_1}(E_{1,n}(\mathbb{Q})) \cap E_n(\mathbb{Q})[2] = \{\infty\}$. Since the degree of $\widehat{\varphi_1}$ is two, we have

$$\widehat{\varphi_1}(E_{1,n}(\mathbb{Q})) \cap E_n(\mathbb{Q})[2] \subseteq \widehat{\varphi_1}(E_{1,n}(\mathbb{Q})[4]) \cap E_n(\mathbb{Q})[2].$$

Since $\mathrm{Ker}(\widehat{\varphi_1}) = E_{1,n}(\mathbb{Q})[2] = E_{1,n}(\mathbb{Q})[4]$, we have

$$\begin{aligned}\widehat{\varphi_1}(E_{1,n}(\mathbb{Q})[4]) \cap E_n(\mathbb{Q})[2] &= \widehat{\varphi_1}(E_{1,n}(\mathbb{Q})[2]) \cap E_n(\mathbb{Q})[2] \\ &= \{\infty\} \cap E_n(\mathbb{Q})[2] = \{\infty\}.\end{aligned}$$

Hence we obtain $\widehat{\varphi_1}(E_{1,n}(\mathbb{Q})) \cap E_n(\mathbb{Q})[2] = \{\infty\}$.

Next, we show that the map (13.6) is an isomorphism. Since the composition map of (13.6) and (13.7) is injective, the map (13.6) is also injective. The groups $E_n(\mathbb{Q})[2] = T[2]$ and $T/2T$ have the same order since they are the kernel and the cokernel of an endomorphism $T \xrightarrow{2} T$ of a finite abelian group T, respectively. Hence the map (13.6) is surjective.

Combining these with the fact that the map (13.7) is surjective, we see that the maps (13.6) and (13.7) are isomorphisms. This completes the proof. □

Remark 13.5. Under the bijection in Lemma 10.1, all 2-torsion points

$$\infty, (0,0), (n,0), (-n,0) \in E_n(\mathbb{Q})[2]$$

correspond to

$$x^4 - n^2y^4, -x^4 + n^2y^4, nx^4 - ny^4, -nx^4 + ny^4 \in \mathcal{F}_{-n^2}^{0,\mathrm{sol}}.$$

For details, see Silverman [**61**, Proposition X.4.9].

Using the above propositions, we can show the following proposition which estimates the numerator.

Proposition 13.6. We have

$$\sum_{\substack{0<n<X \\ n:\ \mathrm{sqf.}}} \#\mathcal{F}_{-n^2}^{0,\mathrm{sol}} \geq \frac{4(6 + 0.559 \times 3)}{\pi^2} X + o(X)$$

as $X \to \infty$.

Proof. First, consider the exact sequence (Silverman [**61**, Remark X.4.7])

$$0 \to \frac{E_{1,n}(\mathbb{Q})[\widehat{\varphi_1}]}{\varphi_1(E_n(\mathbb{Q})[2])} \to \frac{E_{1,n}(\mathbb{Q})}{\varphi_1(E_n(\mathbb{Q}))} \to \frac{E_n(\mathbb{Q})}{2E_n(\mathbb{Q})} \to \frac{E_n(\mathbb{Q})}{\widehat{\varphi_1}(E_{1,n}(\mathbb{Q}))} \to 0.$$

For $n > 1$, we have

$$\frac{E_{1,n}(\mathbb{Q})[\widehat{\varphi_1}]}{\varphi_1(E_n(\mathbb{Q})[2])} = 0.$$

By the above exact sequence, if $n > 1$, we obtain

$$\dim_{\mathbb{F}_2} \frac{E_{1,n}(\mathbb{Q})}{\varphi_1(E_n(\mathbb{Q}))} + \dim_{\mathbb{F}_2} \frac{E_n(\mathbb{Q})}{\widehat{\varphi_1}(E_{1,n}(\mathbb{Q}))} = \dim_{\mathbb{F}_2} \frac{E_n(\mathbb{Q})}{2E_n(\mathbb{Q})}.$$

Recall that $E_{1,n}(\mathbb{Q})/\varphi_1(E_n(\mathbb{Q})) \subseteq \mathrm{Sel}_{\varphi_1}(E_n)$. As stated in Lemma 11.1, we have

$$\sum_{\substack{0<n<X \\ n:\ \mathrm{sqf.}}} \#(\mathrm{Sel}_{\varphi_1}(E_n) \setminus \{0\}) = o(X)$$

as $X \to \infty$. Hence we obtain

$$\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \dim_{\mathbb{F}_2} \frac{E_{1,n}(\mathbb{Q})}{\varphi_1(E_n(\mathbb{Q}))} = o(X)$$

and

$$\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \dim_{\mathbb{F}_2} \frac{E_n(\mathbb{Q})}{\widehat{\varphi_1}(E_{1,n}(\mathbb{Q}))} = \sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \dim_{\mathbb{F}_2} \frac{E_n(\mathbb{Q})}{2E_n(\mathbb{Q})} + o(X) \tag{13.8}$$

as $X \to \infty$.

Since

$$\begin{aligned} \# \frac{E_n(\mathbb{Q})}{\widehat{\varphi_1}(E_n(\mathbb{Q}))} &= \#(E_n(\mathbb{Q})[2] \times A/\widehat{\varphi_1}(A_1)) \\ &= \# E_n(\mathbb{Q})[2] \times 2^{\dim_{\mathbb{F}_2} A/\widehat{\varphi}(A_1)} \\ &\geq 4 \times (1 + \dim_{\mathbb{F}_2} A/\widehat{\varphi_1}(A_1)), \end{aligned}$$

Lemmas 10.1 and 10.2 yields the inequality

$$\begin{aligned} \sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \# \mathcal{F}^{0,\mathrm{sol}}_{-n^2} &= \sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \# \frac{E_n(\mathbb{Q})}{\widehat{\varphi_1}(E_{1,n}(\mathbb{Q}))} \\ &\geq \sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} 4 \times (1 + \dim_{\mathbb{F}_2} A/\widehat{\varphi_1}(A_1)). \end{aligned}$$

Moreover, the inequalities

$$\begin{aligned} \sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} 4 \times (1 + \dim_{\mathbb{F}_2} A/\widehat{\varphi}(A_1)) &= \sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} 4 \times (1 + r) + o(X) \\ &\geq \left(\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} + \sum_{\substack{0<n<X \\ n\colon \text{ sqf.} \\ n \equiv 5,6,7 \bmod 8 \\ \operatorname{rank} E_n(\mathbb{Q}) = 1}} \right) 4 + o(X) \\ &\geq \frac{4(6 + 0.559 \times 3)}{\pi^2} X + o(X) \end{aligned}$$

also hold as $X \to \infty$. Here, the first equality follows from (13.8) and Proposition 13.4 and the second inequality follows from Proposition 13.2. Therefore, we obtain the inequality

$$\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{-n^2} \geq \frac{4(6+0.559\times 3)}{\pi^2} X + o(X)$$

as $X \to \infty$ and we complete the proof. □

Combining with (13.1) and Proposition 13.6, we obtain

$$\liminf_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{-n^2}}{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{0,\mathrm{sls}}_{-n^2}} \geq \frac{4(6+0.559\times 3)/\pi^2}{6\times 12\times (1/\pi^2)} = \frac{2.559}{6} \sim 0.4265,$$

which completes the proof of Theorem 13.1.

In a similar manner to strictly locally soluble quartics in $W^0_{-n^2}(\mathbb{Z})^{\mathrm{ls}}$, we define strictly locally soluble quartics in $W^{\pm 3n}_{2n^2}(\mathbb{Z})^{\mathrm{ls}}$ and consider the subsets $W^{\pm 3n}_{2n^2}(\mathbb{Z})^{\mathrm{sls}} \subseteq W^{\pm 3n}_{2n^2}(\mathbb{Z})^{\mathrm{ls}}$ of all strictly locally soluble quartics. We also define $\mathcal{F}^{3n,\mathrm{sls}}_{2n^2} = \mathcal{F}^{3n}_{2n^2} \cap W^{3n}_{2n^2}(\mathbb{Z})^{\mathrm{sls}}$ and $\mathcal{F}^{-3n,\mathrm{sls}}_{2n^2} = \mathcal{F}^{-3n}_{2n^2} \cap W^{-3n}_{2n^2}(\mathbb{Z})^{\mathrm{sls}}$. The arguments throughout this section also hold when we use φ_2 or φ_3 instead of φ_1. Combining this with Lemmas 10.1 and 10.2, we obtain the following:

Theorem 13.7. We have

$$\liminf_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{3n,\mathrm{sol}}_{2n^2}}{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{3n,\mathrm{sls}}_{2n^2}} \geq \frac{4(6+0.559\times 3)/\pi^2}{6\times 12\times (1/\pi^2)} = \frac{2.559}{6} \sim 0.4265$$

and

$$\liminf_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{-3n,\mathrm{sol}}_{2n^2}}{\displaystyle\sum_{\substack{0<n<X \\ n\colon \text{ sqf.}}} \#\mathcal{F}^{-3n,\mathrm{sls}}_{2n^2}} \geq \frac{4(6+0.559\times 3)/\pi^2}{6\times 12\times (1/\pi^2)} = \frac{2.559}{6} \sim 0.4265.$$

Remark 13.8. Assume that the Goldfeld conjecture holds. Then the proportion of the elliptic curves $\{E_n \mid n\colon \text{ sqf. and } n \equiv -1,-2,-3 \pmod 8\}$ which satisfy $\operatorname{rank} E_n(\mathbb{Q}) = 1$

is 1. Hence we obtain

$$\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{-n^2} \geq \left(\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} + \sum_{\substack{0<n<X\\ n:\ \text{sqf.}\\ n\equiv 5,6,7 \bmod 8\\ \operatorname{rank} E_n(\mathbb{Q})=1}} \right) 4 \geq \frac{4(6+3)}{\pi^2} X + o(X)$$

as $X \to \infty$ and

$$\liminf_{X\to\infty} \frac{\displaystyle\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{sol}}_{-n^2}}{\displaystyle\sum_{\substack{0<n<X\\ n:\ \text{sqf.}}} \#\mathcal{F}^{0,\mathrm{sls}}_{-n^2}} \geq \frac{4(6+3)/\pi^2}{6 \times 12 \times (1/\pi^2)} = \frac{1}{2}.$$

We expect the limit exists, and coincides with 1/2.

Part 3

Non-degenerate integer points on PCF varieties

14. Preliminaries

In this section, we recall the PCF varieties and fundamental solutions of the Pell equations. We will use them in the proof of Theorems 5.2 and 5.3 and Corollary 17.3.

14.1. PCF variety. In this subsection, we introduce the definition of PCF varieties over a number field K. Let $\mathcal{O}$ be a ring of integers of K. Note that we define only (N,l)-type PCF varieties for square roots of $\alpha \in \mathcal{O}$ which are the needed ones in our thesis. See Brock, Elkies, and Jordan [**10**, Section 3] for the definition of general PCF varieties.

Before introducing the definition of PCF varieties, we prepare some notations. For a finite RCF $[c_1, \ldots, c_n]$, define

$$\begin{aligned} M([c_1, c_2 \ldots, c_n]) &= \begin{bmatrix} M([c_1, c_2 \ldots, c_n])_{11} & M([c_1, c_2 \ldots, c_n])_{12} \\ M([c_1, c_2 \ldots, c_n])_{12} & M([c_1, c_2 \ldots, c_n])_{22} \end{bmatrix} \\ &= \begin{bmatrix} c_1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c_2 & 1 \\ 1 & 0 \end{bmatrix} \cdots \begin{bmatrix} c_n & 1 \\ 1 & 0 \end{bmatrix}. \end{aligned}$$

For $N \in \mathbb{Z}_{\geq 0}$ and $l \in \mathbb{Z}_{\geq 1}$, we set

$$\begin{aligned} &E((y_1, \ldots, y_N, x_1, \ldots, x_l)) \\ &= \begin{bmatrix} E((y_1, \ldots, y_N, x_1, \ldots, x_l))_{11} & E((y_1, \ldots, y_N, x_1, \ldots, x_l))_{12} \\ E((y_1, \ldots, y_N, x_1, \ldots, x_l))_{21} & E((y_1, \ldots, y_N, x_1, \ldots, x_l))_{22} \end{bmatrix} \\ &:= \begin{cases} M([y_1, \ldots, y_N, x_1, \ldots, x_l, 0, -y_N, \ldots, -y_1, 0]) & \text{if } N \geq 1, \\ M([x_1, \ldots, x_l]) & \text{if } N = 0. \end{cases} \end{aligned}$$

Note that $E((y_1, \ldots, y_N, x_1, \ldots, x_l)) = E((x_1, \ldots, x_l))$ when $N = 0$.

Definition 14.1. Fix $N \in \mathbb{Z}_{\geq 0}$ and $l \in \mathbb{Z}_{\geq 1}$. For $\alpha \in \mathcal{O}$ with $\sqrt{\alpha} \notin \mathcal{O}$, we define a PCF variety $V(\sqrt{\alpha})_{N,l}$ of (N,l)-type by

$$\begin{cases} E((y_1, \ldots, y_N, x_1, \ldots, x_l))_{22} - E((y_1, \ldots, y_N, x_1, \ldots, x_l))_{11} = 0, \\ E((y_1, \ldots, y_N, x_1, \ldots, x_l))_{12} = \alpha E((y_1, \ldots, y_N, x_1, \ldots, x_l))_{21}, \end{cases}$$

where $y_1, \ldots, y_N, x_1, \ldots, x_l$ are variables. In what follows, $(y_1, \ldots, y_N, x_1, \ldots, x_l)$ denotes the coordinate of $V(\sqrt{\alpha})_{N,l}$.

In what follows, we consider $N = 1$ and $\alpha = m$, where m is a positive nonsquare integer. The following proposition is essential to prove Theorems 5.2 and 5.3

Proposition 14.2. (cf. Brock, Elkies, and Jordan [**10**, (a) in Section 3.1 and Proposition 2.8]) If $\sqrt{m}$ has a $(1,l)$-type PICF expansion $[b_1, \overline{a_1, \ldots, a_l}]$, then a tuple of integers $(b_1, a_1, \ldots, a_l)$ is an integer point on $V(\sqrt{m})_{1,l}$. Moreover, if $(b_1, a_1, \ldots, a_l) \in V(\sqrt{m})_{1,l}$ is an integer point and $[b_1, \overline{a_1, \ldots, a_l}]$ converges, then the value of $[b_1, \overline{a_1, \ldots, a_l}]$ is $\sqrt{m}$ or $-\sqrt{m}$.[e]

Proof. Throughout this proof, we set $P := [b_1, \overline{a_1, \ldots, a_l}]$. Suppose $\sqrt{m}$ has a $(1,l)$-type PICF expansion $P \in \mathbb{C}$. For a matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{C})$, we regard A as the automorphism of the projective line $\mathbb{P}^1$ over $\mathbb{C}$ by

$$z \mapsto \frac{az+b}{cz+d}$$

for $z \in \mathbb{P}^1(\mathbb{C})$. Then we have

$$\begin{aligned} P &= [b_1, a_1, \ldots, a_l, 0, -b_1, 0, b_1, \overline{a_1, \ldots, a_l}] \\ &= M([b_1, a_1, \ldots, a_l, 0, -b_1, 0])P. \end{aligned}$$

Since

$$M([b_1, a_1, \ldots, a_l, 0, -b_1, 0]) = E((b_1, a_1, \ldots, a_l))$$

and $P = \sqrt{m}$, we have

$$\frac{E_{11}((b_1, a_1, \ldots, a_l))P + E_{12}((b_1, a_1, \ldots, a_l))}{E_{21}((b_1, a_1, \ldots, a_l))P + E_{22}((b_1, a_1, \ldots, a_l))} = P \tag{14.1}$$

and

$$\begin{aligned} E_{21}((b_1, a_1, \ldots, a_l))m + [E_{22}((b_1, a_1, \ldots, a_l)) - E_{11}((b_1, a_1, \ldots, a_l))]\sqrt{m} \\ - E_{12}((b_1, a_1, \ldots, a_l)) = 0. \end{aligned}$$

Hence we obtain

$$\begin{cases} E((b_1, a_1, \ldots, a_l))_{22} - E((b_1, a_1, \ldots, a_l))_{11} = 0, \\ E((b_1, a_1, \ldots, a_l))_{12} = mE((b_1, a_1, \ldots, a_l))_{21}, \end{cases} \tag{14.2}$$

which proves $(b_1, a_1, \ldots, a_l) \in V(\sqrt{m})_{1,l}(\mathbb{Z})$.

[e] we can determine the sign of $[b_1, \overline{a_1, \ldots, a_l}]$. For details, see Brock, Elkies, and Jordan [**10**, Theorem 4.3].

Next, suppose that $(b_1, a_1, \ldots, a_l) \in V(\sqrt{m})_{1,l}$ is an integer point and $P = [b_1, \overline{a_1, \ldots, a_l}]$ converges. Then (14.1) and (14.2) hold and we obtain the equation

$$E((b_1, a_1, \ldots, a_l))_{12}(P^2 - m) = 0.$$

Here we have $E((b_1, a_1, \ldots, a_l))_{12} \neq 0$ since $[b_1, \overline{a_1, \ldots, a_l}]$ converges (cf. Brock, Elkies, and Jordan [**10**, Corollary 4.4 and l.12 in p. 392]). Hence we obtain $P = \pm\sqrt{m}$ and we complete the proof. □

From this proposition, it is sufficient to determine all the elements of $V(\sqrt{m})_{1,l}(\mathbb{Z})$ in order to obtain all $(1, l)$-type PICF expansions of $\sqrt{m}$.

We also remark that if $a_1 \cdots a_l = 0$, then the period of $[b_1, \overline{a_1, \ldots, a_l}]$ is less than l (cf. Brock, Elkies, and Jordan [**10**, Lemma 2.2]). Hence we only consider non-degenerate integer points on $V(\sqrt{m})_{1,l}(\mathbb{Z})$ defined as follows.

Definition 14.3. Let $V(\sqrt{m})_{1,l}$ be a PCF variety. An integer point $(b_1, a_1, \ldots, a_l)$ on $V(\sqrt{m})_{1,l}$ is said to be non-degenerate if the condition $a_i \neq 0$ holds for all $1 \leq i \leq l$. We write $V(\sqrt{m})_{1,l}(\mathbb{Z})_{\mathrm{nd}}$ for the set of non-degenerate integer points on $V(\sqrt{m})_{1,l}$.

Remark 14.4. There are some results on geometric properties of PCF varieties (e.g. Jordan–Logan–Zaytman [**35**] and Jordan–Zaytman [**36**]). In particular, $V(\sqrt{m})_{1,l}(\mathbb{Z})_{\mathrm{nd}}$ is a finite set for $l \leq 3$ (see Jordan–Logan–Zaytman [**35**, Proof of Theorem 2.5]).

14.2. Pell equation.

In this subsection, we recall the classical algorithm for finding the fundamental solution of Pell equation. Throughout this subsection, let m be a positive nonsquare integer. We consider all the integer solutions of the Pell equation $x^2 - my^2 = \pm 1$. Set

$$W := \{(u, v) \in \mathbb{Z}^2 \mid u^2 - mv^2 = 1 \text{ or } u^2 - mv^2 = -1\}.$$

There is a natural bijection $(u, v) \mapsto u + v\sqrt{m}$ between W and the group of units of the ring $\mathbb{Z}[\sqrt{m}]$. Moreover the group of units is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$ by Dirichlet's unit theorem. Using these bijections, we define the fundamental solution of the Pell equation $x^2 - my^2 = \pm 1$.

Definition 14.5. We call $(u, v) \in W$ fundamental if (u, v) corresponds to one of

$$(1, 1), (1, -1), (0, 1), (0, -1) \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}.$$

Note that an isomorphism between the group of units $\mathbb{Z}[\sqrt{m}]^\times$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$ is not canonical. However, for any isomorphism, the corresponding elements to $\{(1, \pm 1), (0, \pm 1)\}$ are the same. Thus the fundamental solutions are well-defined.

To find the fundamental solution of the Pell equation $x^2 - my^2 = \pm 1$, we can use the RCF expansion of $\sqrt{m}$. It is well-known that $\sqrt{m}$ has the $(1, l)$-type RCF expansion for some $l \in \mathbb{Z}_{\geq 1}$ (cf. Niven, Zuckerman, and Montgomery [**53**, Theorem 7.21]). Hence we can write $\sqrt{m} = [a_0, \overline{a_1, \ldots, a_l}]$ for some $a_0, a_1, \ldots, a_l \in \mathbb{Z}_{\geq 1}$, where l is the period. To state the relationship between the fundamental solution of the Pell equation $x^2 - my^2 = \pm 1$ and $(1, l)$-type RCF expansion of $\sqrt{m}$, we introduce the convergent of a RCF $[a_0, a_1, a_2, \ldots]$.

Definition 14.6. We define the nth convergent p_n/q_n of the RCF $[a_0, a_1, a_2, \ldots]$ by

$$(p_n, q_n) = (a_n p_{n-1} + p_{n-2}, a_n q_{n-1} + q_{n-2})$$

for each $n \geq 1$. Here, $(p_{-1}, q_{-1}) := (1, 0)$ and $(p_0, q_0) := (a_0, 1)$.

Note that $p_n/q_n = [a_0, \ldots, a_n]$ (cf. Niven, Zuckerman, and Montgomery [**53**, Theorem 7.4]). Under the above preparation, the following holds.

Proposition 14.7. The fundamental solution of the Pell equation $x^2 - my^2 = \pm 1$ is given by

$$(x, y) = (p_{l-1}, q_{l-1}),$$

where l is the period of the RCF expansion of $\sqrt{m}$.

For the proof of Proposition 14.7, see Niven, Zuckerman, and Montgomery [**53**, Theorem 7.25].

15. Non-degenerate integer points on PCF varieties

In this section, we determine all non-degenerate integer points on PCF varieties of $(1, l)$-type for $l = 1, 2, 3$. We recall that

$$\begin{aligned}
m_1(t) &= t^2 + 1, \\
m_2(s, t) &= s^2 t^2 + t, \\
m_2'(s, t) &= s^2 t^2 + 2t, \\
m_3(s, t) &= 16t^2 s^4 + 8ts^3 + (8t^2 + 1)s^2 + 6ts + t^2 + 1.
\end{aligned}$$

15.1. $(1,1)$**-type.** We see that $E((y_1, x_1))$ is

$$\begin{bmatrix} y_1 & x_1y_1 + 1 - y_1^2 \\ 1 & x_1 - y_1 \end{bmatrix}.$$

Hence $V(\sqrt{m})_{1,1}$ is given by

$$\begin{cases} x_1 - 2y_1 = 0, \\ y_1^2 - x_1y_1 - 1 = -m. \end{cases}$$

By easy calculation, $V(\sqrt{m})_{1,1}$ consists of two points $\pm(\sqrt{m-1}, 2\sqrt{m-1})$. Therefore, we immediately obtain the following propositions (cf. Brock, Elkies, and Jordan [**10**, Proposition 5.3]).

Proposition 15.1. A $(1,1)$-type PCF variety $V(\sqrt{m})_{1,1}$ has a non-degenerate integer point if and only if $m = m_1(t)$ for some $t \in \mathbb{Z} \setminus \{0\}$.

Proposition 15.2. Suppose that $m = m_1(t)$ for some $t \in \mathbb{Z} \setminus \{0\}$. We have

$$V(\sqrt{m})_{1,1}(\mathbb{Z})_{\mathrm{nd}} = \{\pm(t, 2t)\}.$$

15.2. $(1,2)$**-type.** We see that $E((y_1, x_1, x_2))$ is

$$\begin{bmatrix} y_1x_1 + 1 & y_1x_1x_2 + x_2 - y_1^2x_1 \\ x_1 & x_1x_2 - y_1x_1 + 1 \end{bmatrix}.$$

Hence $V(\sqrt{m})_{1,2}$ is given by

$$\begin{cases} x_1x_2 - 2y_1x_1 = 0, & (15.1) \\ y_1^2x_1 - y_1x_1x_2 - x_2 = -mx_1. & (15.2) \end{cases}$$

Proposition 15.3. A $(1,2)$-type PCF variety $V(\sqrt{m})_{1,2}$ has a non-degenerate integer point if and only if $m = (st/2)^2 + t$ for some $s, t \in \mathbb{Z} \setminus \{0\}$ with $2 \mid st$.

Proof. Suppose that $m = (st/2)^2 + t$ for some $s, t \in \mathbb{Z} \setminus \{0\}$ with $2 \mid st$. Then we find $(st/2, s, st) \in V(\sqrt{m})_{1,2}(\mathbb{Z})_{\mathrm{nd}}$ and we can check the if part.

Hence it is sufficient to show the only if part. Suppose that $(y_1, x_1, x_2) \in V(\sqrt{m})_{1,2}$ is a non-degenerate integer point. From (15.1), we obtain $x_2 = 2y_1$ since $x_1 \neq 0$. Substituting this into (15.2), we obtain $y_1^2x_1 + 2y_1 - mx_1 = 0$ and $m = y_1^2 + 2y_1/x_1$. Since $m \in \mathbb{Z}$, $2y_1 = tx_1$ for some $t \in \mathbb{Z} \setminus \{0\}$, we obtain $m = (tx_1/2)^2 + t$ and complete the proof by putting $s = x_1$. □

Remark 15.4. Since s or t is even by $2 \mid st$, the condition $m = (st/2)^2 + t$ for some $s, t \in \mathbb{Z} \setminus \{0\}$ with $2 \mid st$ is equivalent to $m = m_2(s,t)$ or $m'_2(s,t)$ for some $s, t \in \mathbb{Z} \setminus \{0\}$.

From the proof of Proposition 15.3 and Remark 15.4, we obtain the following corollary.

Corollary 15.5. We have

$$\begin{aligned}&V(\sqrt{m})_{1,2}(\mathbb{Z})_{\mathrm{nd}}\\ &= \{\pm(st, 2s, 2st) \mid m = m_2(s,t),\ s, t \neq 0\} \cup \{\pm(st, s, 2st) \mid m = m'_2(s,t),\ s, t \neq 0\}.\end{aligned}$$

15.3. $(1,3)$**-type.** We see that $E((y_1, x_1, x_2, x_3))$ is

$$\begin{bmatrix} y_1x_2x_1 + (x_2 + y_1) & ((y_1x_3 - y_1^2)x_2 + y_1)x_1 + (x_3 - y_1)x_2 + y_1x_3 - y_1^2 + 1 \\ x_2x_1 + 1 & ((x_3 - y_1)x_2 + 1)x_1 + x_3 - y_1 \end{bmatrix}.$$

Hence $V(\sqrt{m})_{1,3}$ is given by

$$\begin{cases} 2y_1x_2x_1 + 2y_1 - x_3x_2x_1 + x_2 - x_1 - x_3 = 0, & (15.3) \\ m(x_2x_1 + 1) = y_1(x_3x_2x_1 + x_1 + x_3 - x_2) - y_1^2(x_2x_1 + 1) + x_3x_2 + 1. & (15.4) \end{cases}$$

Before determining the non-degenerate integer points on $V(\sqrt{m})_{1,3}$, we give a necessary and sufficient condition for the existence of a non-degenerate integer point on $V(\sqrt{m})_{1,3}(\mathbb{Z})$.

Proposition 15.6. A $(1,3)$-type PCF variety $V(\sqrt{m})_{1,3}$ has a non-degenerate integer point if and only if $m = m_3(s,t)$ for some $s, t \in \mathbb{Z}$ with $(s,t) \neq (0,0)$.

Proof. Suppose that $m = 16t^2s^4 + 8ts^3 + (8t^2 + 1)s^2 + 6ts + t^2 + 1$ for some $s, t \in \mathbb{Z}$ with $(s,t) \neq (0,0)$. Then we can take non-degenerate integer points such as $(s + (4s^2 + 1)t, 2s, 2s, 2(s + (4s^2 + 1)t))$ and we showed the if part.

Hence it is sufficient to show the only if part. Suppose that (y_1, x_1, x_2, x_3) is a non-degenerate integer point on $\in V(\sqrt{m})_{1,3}$. From (15.3), we obtain

$$|(2y_1 - x_3)(x_2x_1 + 1)| = |x_1 - x_2|. \qquad (15.5)$$

In what follows, we divide the proof into two cases, namely $|x_1 - x_2| > |x_2x_1 + 1|$ and $|x_1 - x_2| \leq |x_2x_1 + 1|$.

(1) If $|x_1 - x_2| > |x_2x_1 + 1|$, we obtain

$$\begin{cases} \frac{-x_1-1}{x_1-1} < x_2 < \frac{x_1-1}{x_1+1} & \text{if } x_1 \neq \pm 1, \\ x_2 > 0 & \text{if } x_1 = -1, \\ x_2 < 0 & \text{if } x_1 = 1. \end{cases}$$

Hence it is sufficient to consider the following five cases:

- $(x_1, x_2) = \pm(2, -2)$,
- $x_1 \geq 2$ and $x_2 = -1$,
- $x_1 \leq -2$ and $x_2 = 1$,
- $x_1 = -1$ and $x_2 > 0$,
- $x_1 = 1$ and $x_2 < 0$.

If $(x_1, x_2) = \pm(2, -2)$, we immediately show that $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} = \emptyset$. Hence we consider the remaining cases.

(a) If $|x_1| \geq 2$, consider the case where $x_1 \geq 2$ and $x_2 = -1$. Substituting $x_2 = -1$ into (15.3), we obtain $(x_1 - 1)(x_3 - 2y_1 - 1) = 2$ and $(x_1, x_3) = (3, 2y_1 + 2), (2, 2y_1 + 3)$ since $x_1 \geq 2$. If $(x_1, x_3) = (3, 2y_1 + 2)$, there are no non-degenerate integer points since $y_1 \notin \mathbb{Z}$. If $(x_1, x_3) = (2, 2y_1 + 3)$, we obtain $y_1^2 + 2y_1 + 2 - m = 0$ by (15.4) and $y_1 = -1 \pm \sqrt{m-1}$. Since $y_1 \in \mathbb{Z}$, the necessary condition for $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \neq \emptyset$ is $m = t^2 + 1$ for some $t \in \mathbb{Z} \setminus \{0\}$.

Similarly, the necessary condition for $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \neq \emptyset$ is $m = t^2 + 1$ for some $t \in \mathbb{Z} \setminus \{0\}$ when $x_1 \leq -2$ and $x_2 = 1$.

(b) If $|x_1| = 1$, consider the case where $x_1 = -1$ and $x_2 > 0$. Substituting $x_1 = -1$ into (15.3), we obtain $(x_2 - 1)(x_3 - 2y_1 + 1) = -2$ and $(x_2, x_3) = (2, 2y_1 - 3), (3, 2y_1 - 2)$ since $x_2 > 0$. If $(x_2, x_3) = (3, 2y_1 - 2)$, there are no non-degenerate integer points since $y_1 \notin \mathbb{Z}$. If $(x_2, x_3) = (2, 2y_1 - 3)$, we obtain $y_1^2 - 4y_1 + 5 - m = 0$ from (15.4) and $y_1 = 2 \pm \sqrt{m-1}$. Since $y_1 \in \mathbb{Z}$, the necessary condition for $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \neq \emptyset$ is $m = t^2 + 1$ for some $t \in \mathbb{Z} \setminus \{0\}$.

Similarly, the necessary condition for $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \neq \emptyset$ is $m = t^2 + 1$ for some $t \in \mathbb{Z} \setminus \{0\}$ when $x_1 = 1$ and $x_2 < 0$.

(2) If $|x_1 - x_2| \leq |x_2x_1 + 1|$, we obtain $(|2y_1 - x_3| - 1)\,|x_2x_1 + 1| \leq 0$. In what follows, we assume $|2y_1 - x_3| - 1 \leq 0$ since we can check that there are no non-degenerate integer points if $|2y_1 - x_3| - 1 > 0$[f].

 (a) If $|2y_1 - x_3| - 1 = 0$, consider the case $2y_1 - x_3 = 1$. From (15.3), we obtain $(x_1+1)(x_2-1) = -2$ and $(x_1, x_2) = (-3, 2), (-2, 3)$. If $(x_1, x_2) = (-3, 2)$, we obtain $5y_1^2 - 4y_1 + 1 - 5m = 0$ from (15.4) and $y_1 = (2 \pm \sqrt{25m-1})/5$. Since $y_1 \in \mathbb{Z}$, the necessary condition for $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \neq \emptyset$ is $m = 25t^2 + 14t + 2$ for some $t \in \mathbb{Z}$. If $(x_1, x_2) = (-2, 3)$, we obtain $5y_1^2 - 6y_1 + 2 - 5m = 0$ from (15.4) and $y_1 = (3 \pm \sqrt{25m-1})/5$. Since $y_1 \in \mathbb{Z}$, the necessary condition for $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \neq \emptyset$ is $m = 25t^2 + 14t + 2$ for some $t \in \mathbb{Z}$.
 Similarly, the necessary condition for $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \neq \emptyset$ is $m = 25t^2+14t+2$ for some $t \in \mathbb{Z}$ when $2y_1 - x_3 = -1$.

 (b) If $|2y_1 - x_3| - 1 < 0$, we obtain $2y_1 = x_3$ from (15.5). Substituting this into (15.3), we obtain $x_1 = x_2$. Combining this and (15.4), we obtain

$$(y_1^2 - m)x_1^2 + 2y_1x_1 + y_1^2 + 1 - m = 0. \tag{15.6}$$

 Hence $2 \mid x_1$ and we can write $x_1 = 2s$ for some $s \in \mathbb{Z} \setminus \{0\}$. Combining (15.6), we have $m = y_1^2 + \frac{4sy_1+1}{4s^2+1} \in \mathbb{Z}$ and $4sy_1 \equiv -1 \bmod 4s^2 + 1$. Thus, we obtain $y_1 = s + (4s^2+1)t$ for some $t \in \mathbb{Z}$ and the necessary condition for $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \neq \emptyset$ is $m = 16t^2s^4 + 8ts^3 + (8t^2+1)s^2 + 6ts + t^2 + 1$ for some $s \in \mathbb{Z} \setminus \{0\}$ and $t \in \mathbb{Z}$.

Therefore, combining the results of (1) and (2), we showed that if $V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \neq \emptyset$ then $m = 16t^2s^4 + 8ts^3 + (8t^2+1)s^2 + 6ts + t^2 + 1 = m_3(s,t)$ for some $s, t \in \mathbb{Z}$ with $(s,t) \neq (0,0)$ since $t^2 + 1 = m_3(0,t)$ and $25t^2 + 14t + 2 = m_3(\pm 1, t)$. □

Tracing the proof of the only if part of Proposition 15.6 and determining (y_1, x_1, x_2, x_3) in each case, we obtain the following:

Corollary 15.7. We have

$$\begin{aligned}
&V(\sqrt{m})_{1,3}(\mathbb{Z})_{\mathrm{nd}} \\
&= \{\pm(s + (4s^2+1)t, 2s, 2s, 2(s + (4s^2+1)t)) \mid m = m_3(s,t), s, t \neq 0\} \\
&\cup \{\pm(-2+t, 1, -2, -1+2t), \pm(-1+t, 2, -1, 1+2t) \mid m = m_3(0,t), t \neq 0\} \\
&\cup \{\pm(2+5t, -2, 3, 3+10t), \pm(1+5t, 3, -2, 3+10t) \mid m = m_3(\pm 1, t)\}.
\end{aligned}$$

[f] In this case, we obtain $x_2x_1 = -1, x_2 = x_1$ but there are no integer x_2, x_1 satisfying the equations.

16. Proof of Theorems 5.2 and 5.3

In this section, we prove Theorems 5.2 and 5.3.

16.1. Convergence to PICF. Before the proof of our theorems, we recall two propositions on the convergence of PICFs.

For a sequence of integers $\{a_n\}_{n\geq 0}$, we define

$$[\![a_0, a_1.a_2, \dots]\!] = a_0 - \cfrac{1}{a_1 - \cfrac{1}{a_2 - \cdots}}.$$

Then Katok and Ugarcovici gave the sufficient condition on the convergence of PICFs.

Proposition 16.1 (Katok and Ugarcovici [**37**, Lemma 1.1])**.** Let $\{a_n\}_{n\geq 0}$ be a sequence of non-zero integers such that $|a_i| = 1$ implies $a_i a_{i+1} < 0$. Then the sequence $[\![a_0, a_1.a_2, \dots]\!]$ converges and it satisfies $a_0 - 1 \leq [\![a_0, a_1.a_2, \dots]\!] \leq a_0 + 1$.

Note that we can regard a PICF $[a_0, a_1, a_2, a_3, \dots]$ as $[\![a_0, -a_1.a_2, -a_3, \dots]\!]$. Hence Proposition 16.1 gives the sufficient condition on the convergence of PICFs satisfying the assumption in this theorem. Moreover, Brock, Elkies, and Jordan obtained necessary and sufficient conditions on the convergence of all the PICFs. In what follows, for a PICF $P = [b_1, \dots, b_N, \overline{a_1, \dots, a_l}]$, we denote $E((b_1, \dots, b_N, a_1, \dots, a_l))$ as $E(P)$ and denote $\lambda(P)_+$ as the eigenvalue of $E(P)$ such that $|\lambda(P)_+| \geq 1$.

Proposition 16.2 (a special case of Brock, Elkies, and Jordan [**10**, Theorem 4.3])**.** Let $P = [b_1, \dots, b_N, \overline{a_1, \dots, a_l}]$ be a PICF. Then P converges if and only if none of the following three conditions is satisfied:

(1) $E(P) = \pm I$, where I is the identity matrix.

(2) $M([a_{j+1}, \dots, a_{l+j}])_{21} = 0$ and $|M([a_{j+1}, \dots, a_{l+j}])_{22}| > 1$ for some $0 \leq j \leq k-1$.

(3) $\mathrm{Tr}(E(P))^2 \in \mathbb{R}$ and $0 \leq (-1)^l \mathrm{Tr}(E(P))^2 < 4$.

Moreover, P converges to $(\lambda(P)_+ - E(P)_{22})/E(P)_{21}$.

We will use these propositions in the proof of Theorems 5.2 and 5.3.

16.2. The proof of Theorem 5.2. First, the only if part follows from Proposition 14.2 and from the only if part of Proposition 15.1 (resp. Proposition 15.3, Proposition 15.6) in $l = 1$(resp. $l = 2$, $l = 3$). To show the if part, it is sufficient to check that $[b_1, \overline{a_1, \dots, a_l}]$ converge for some $(b_1, a_1, \dots, a_l) \in V(\sqrt{m})_{1,l}(\mathbb{Z})_{\mathrm{nd}}$ by Proposition 14.2. Indeed, if a PICF $[b_1, \overline{a_1, \dots, a_l}]$ converges to $-\sqrt{m_l(s,t)}$, we just take $(-b_1, -a_1, ..., -a_l)$

instead of $(b_1, a_1, ..., a_l)$. For the convergence, we can check it easily by Proposition 16.1 except for $[-2+t, \overline{1, -2, -1+2t}]$ and $[-1+t, \overline{2, -1, 1+2t}]$. In what follows, we check the convergence of PICFs corresponding to non-degenerate integer points on $(1,1)$, $(1,2)$ and $(1,3)$-type PCF varieties.

Consider PICFs $[t, \overline{2t}] = [\![t, \overline{-2t, 2t}]\!]$. Then $t \times (-2t) = -2t^2 < 0$ and we can check the convergence.

Consider PICFs $[st, \overline{2s, 2st}] = [\![st, \overline{-2t, 2st}]\!]$. If $t \geq 1$, then $st \times (-2t) = -2s^2t < 0$. If $t < 0$, then $(t, s) = (-1, \pm 1)$ since $|st| = 1$ and $s, t \in \mathbb{Z}$. However, it is a contradiction since $m_2(s,t) = 0$. Hence we can check the convergence. In a similar manner, we can check that PICFs $[st, \overline{s, 2st}]$ converge.

Lastly, consider PICFs $[s+(4s^2+1)t, \overline{2s, 2s, 2(s+(4s^2+1)t)}]$. These PICFs are equivalent to $[\![s+(4s^2+1)t, \overline{-2s, 2s, -2(s+(4s^2+1)t)}]\!]$. By Proposition 16.1, it suffices to check that $[s+(4s^2+1)t, \overline{2s, 2s, 2(s+(4s^2+1)t)}]$ converges when $s+(4s^2+1)t = \pm 1$. If $s+(4s^2+1)t = 1$, we obtain $s > 0$. Indeed, assume $s < 0$. Then we obtain $t = 1$ since $t = (1-s)/(4s^2+1)$ and $t \in \mathbb{Z}$. However, it is a contradiction since s is 0 or 1/4. Hence $(s+(4s^2+1)t) \times (-2s) = -2s < 0$ and

$$[\![s+(4s^2+1)t, \overline{-2s, 2s, -2(s+(4s^2+1)t)}]\!] = [s+(4s^2+1)t, \overline{2s, 2s, 2(s+(4s^2+1)t)}]$$

converges by Proposition 16.1. In a similar manner, we can check that $[s+(4s^2+1)t, \overline{2s, 2s, 2(s+(4s^2+1)t)}]$ converges when $s+(4s^2+1)t = 1$.

For the convergence of $[-2+t, \overline{1, -2, -1+2t}]$ and $[-1+t, \overline{2, -1, 1+2t}]$, we can check it by Proposition 16.2. Consider the case $Q := [-2+t, \overline{1, -2, -1+2t}]$. First, $E(Q) \neq \pm I$ holds for all non-zero integers t since

$$E(Q) = \begin{bmatrix} -t & -t^2-1 \\ -1 & -t \end{bmatrix}.$$

Next, we write down $M([a_{j+1}, a_{j+2}, a_{j+3}])_{21}$ for each $j = 0, 1, 2$. Then we obtain

$$\begin{aligned} M([1, -2, -1+2t])_{21} &= -4t+3, \\ M([-2, -1+2t, 1])_{21} &= 2t, \\ M([-1+2t, 1, -2])_{21} &= -1. \end{aligned}$$

Since all $M([a_{j+1}, a_{j+2}, a_{j+3}])_{21}$ are non-zero, we check that $M([a_{j+1}, ..., a_{j+l}])_{21} \neq 0$ or $|M([a_{j+1}, ..., a_{j+l}])_{22}| \leq 1$ for all $j = 0, \ldots, l-1$.

We also obtain

$$(-1)^3\mathrm{Tr}(E(Q))^2 = -(-2t)^2 < 0$$

for $t \in \mathbb{Z} \setminus \{0\}$, and either $(-1)^l\mathrm{Tr}(E(Q))^2 < 0$ or $4 \geq (-1)^l\mathrm{Tr}(E(Q))^2$ holds. We also check the convergence of $R := [-1+t, \overline{2, -1, 1+2t}]$ in a similar way. Indeed, we obtain

$$E(R) = \begin{bmatrix} -t & -t^2-1 \\ -1 & -t \end{bmatrix},$$

$$\begin{aligned} M([2,-1,1+2t])_{21} &= -2t, \\ M([-1,1+2t,2])_{21} &= 4t+3, \\ M([1+2t,2,-1])_{21} &= -1, \end{aligned}$$

and

$$(-1)^3\mathrm{Tr}(E(R))^2 = -(-2t)^2 < 0$$

for $t \in \mathbb{Z} \setminus \{0\}$.

Combining these results with Proposition 15.2 and Corollaries 15.5 and 15.7, we complete the proof.

16.3. Proof of Theorem 5.3. Recall that we determined all non-degenerate integer points on $V(\sqrt{m_l})_{1,l}(\mathbb{Z})$ for $l = 1, 2, 3$. Then by Proposition 14.2, it is sufficient to consider the convergence of PICFs corresponding to non-degenerating integer points on $V(\sqrt{m_l})_{1,l}(\mathbb{Z})$ in order to prove Theorem 5.3. Since the convergence of PICFs in Theorem 5.3 has already been shown in §16.2, we need only to determine the signs of PICFs. The signs can also be also determined by Proposition 16.1 except for $[-2+t, \overline{1, -2, -1+2t}]$ and $[-1+t, \overline{2, -1, 1+2t}]$, and the signs of $[-2+t, \overline{1, -2, -1+2t}]$ and $[-1+t, \overline{2, -1, 1+2t}]$ by Proposition 16.2. Indeed,

- $[t, \overline{2t}] = \mathrm{sgn}(t)\sqrt{m_1(s,t)}$ since $t-1 \leq [t, \overline{2t}] \leq t+1$,
- $[st, \overline{2s, 2st}] = \mathrm{sgn}(st)\sqrt{m_2(s,t)}$ since $st-1 \leq [st, \overline{2s, 2st}] \leq st+1$,
- $[st, \overline{s, 2st}] = \mathrm{sgn}(st)\sqrt{m_2(s,t)}$ since $st-1 \leq [st, \overline{2s, 2st}] \leq st+1$,
- $[s+(4s^2+1)t, \overline{2s, 2s, 2(s+(4s^2+1)t)}] = \mathrm{sgn}(t)\sqrt{m_3(s,t)}$ since

$$s+(4s^2+1)t-1 > s+(4s^2+1)-1 = 4s^2+s > 0$$

for $s \in \mathbb{Z} \setminus \{0\}$ if $t > 0$ and

$$s + (4s^2 + 1)t + 1 \leq s - 4s^2 - 1 + 1 = -4s^2 + s < 0$$

for $s \in \mathbb{Z} \setminus \{0\}$ if $t < 0$.

Moreover, for $[-2+t, \overline{1, -2, -1+2t}]$ and $[-1+t, \overline{2, -1, 1+2t}]$, it is sufficient to determine $\lambda(P)_+$ for each PICF in Theorem 5.3. Easy calculations show that

$$\lambda((-2+t, 1, -2, -1+2t))_+ = -t - \mathrm{sgn}(t)\sqrt{m_3(0,t)},$$

and

$$\lambda((-1+t, 2, -1, 1+2t))_+ = -t - \mathrm{sgn}(t)\sqrt{m_3(0,t)}.$$

Hence we complete the proof.

17. An application of Theorem 5.3 to the fundamental solutions of the Pell equations

As an application of Theorem 5.3, we obtain the fundamental solutions of some families of the Pell equations from PICF expansions of square roots of positive nonsquare integers. As we seen in Proposition 14.7, we obtain the fundamental solution of the Pell equation $x^2 - my^2 = \pm 1$ from the RCF expansion of $\sqrt{m}$ for a nonsquare positive integer m. On the other hand, the algorithm does not work when we consider PICFs of $\sqrt{m}$ in general. Indeed we obtain a solution $(x, y) = (-7, -5)$ of the Pell equation from $\sqrt{m_3(\pm 1, 0)} = \sqrt{2} = [2, \overline{-2, 3, 3}]$ and this is not the fundamental solution $(x, y) = (1, 1)$. Hence we can consider the following question.

Problem 17.1. For every nonsquare positive integer m and $l \in \mathbb{Z}_{\geq 2}$, when the fundamental solution of the Pell equation $x^2 - my^2 = \pm 1$ is obtained from the $(l-1)$th convergent of a PICF expansion of $\sqrt{m}$?

If $l = 1$, the answer of this question is obtained from a classical result. Indeed, it is a classical result that $(x, y) = (t, 1)$ is the fundamental solution of the Pell equation $x^2 - m_1(t)y^2 = \pm 1$ for every non-zero integer t and we can obtain it from all PICF expansions of $\sqrt{m_1(t)}$ given in Theorem 5.3. In this thesis, we answer this question completely for $l = 2, 3$.

Theorem 17.2. (1) Suppose that s, t are non-zero integers with $m_2(s,t) > 0$. For each s, t, the fundamental solution of the Pell equation $x^2 - m_2(s,t)y^2 = \pm 1$ is obtained from the 1st convergent of the PICF expansion of $\sqrt{m_2(s,t)}$ given in Theorem 5.3 if and only if $|s|=1$ or $t\neq -1$.

(2) Suppose that s,t are non-zero integers with $m_2'(s,t)>0$. For each s,t, the fundamental solution of the Pell equation $x^2-m_2'(s,t)y^2=\pm1$ is obtained from the 1st convergent of the PICF expansion of $\sqrt{m_2'(s,t)}$ given in Theorem 5.3.

(3) Suppose that s,t are non-zero integers with $m_3(s,t)>0$. For each s,t, the fundamental solution of the Pell equation $x^2-m_3(s,t)y^2=\pm1$ is obtained from the 2nd convergent of the PICF expansion of $\sqrt{m_3(s,t)}$ given in Theorem 5.3 except for $\sqrt{m_3(\pm1,0)}=\sqrt{2}=[2,\overline{-2,3,3}]=[1,\overline{3,-2,3}]$.

Note that if $|s|\geq 2$ and $t=-1$, we can obtain the fundamental solution of the Pell equation $x^2-m_2(s,t)y^2=\pm1$ from the 0th convergent of the PICF expansion of $\sqrt{m_2(s,t)}$.

As a by-product of the proof of Theorem 17.2, we also find fundamental solutions of some families of the Pell equations.

Corollary 17.3. Let s,t be non-zero integers.

(1) If s,t satisfy $m_2(s,t)>0$ and $t\neq-1$, then

$$(x_2(s,t),y_2(s,t)):=(2s^2t+1,2s)$$

is the fundamental solution of the Pell equation $x^2-m_2(s,t)y^2=\pm1$.

(2) If s,t satisfy $m_2'(s,t)>0$, then

$$(x_2'(s,t),y_2'(s,t)):=(s^2t+1,s)$$

is the fundamental solution of the Pell equation $x^2-m_2'(s,t)y^2=\pm1$.

(3) $(x_3(s,t),y_3(s,t)):=(16ts^4+4s^3+8ts^2+3s+t,4s^2+1)$ is the fundamental solution of the Pell equation $x^2-m_3(s,t)y^2=\pm1$.

Moreover, $(x_3(s,t),y_3(s,t))$ is also the fundamental solution of the Pell equation $x^2-m_3(s,t)y^2=\pm1$ for each pair of integers (s,t) except for $(s,t)=(\pm1,0),(0,0)$.

Of course, Corollary 17.3 is a classical result when s,t are positive integers. Indeed, we obtain Corollary 17.3 by applying the algorithm of obtaining the fundamental solutions of the Pell equations to the first part of Theorem 5.3. Corollary 17.3 claims that this result also holds when s,t are not necessarily positive.

We also note that Corollary 17.3 can be regarded as the result for fundamental solutions of some families of the Pell equations parametrized by non-zero integers s,t. There are some related results about fundamental solutions of them (e.g. Nathanson [**52**], Mollin [**49**], Ramasamy [**57**]). However, these previous results do not seem to cover our results even if fundamental solutions look like our results since the range of parameter values is different.

Since we obtain Corollary 17.3 by writing down the convergents explicitly in the proof of Theorem 17.2, it is sufficient to show Theorem 17.2. Before proving Theorem 17.2, we give the following lemma which gives the RCF expansion of $m_2(s,t)$, $m_2'(s,t)$ and $m_3(s,t)$.

Lemma 17.4. For $t<0$, we have

$$\sqrt{m_2(s,t)} = \begin{cases} [-st-1, \overline{1, 2s-2, 1, 2(-st-1)}] & \text{if } s \geq 2, \\ [-t-1, \overline{2, -2t-2}] & \text{if } s=1, t \neq -1, \end{cases} \tag{17.1}$$

and

$$\sqrt{m_2'(s,t)} = \begin{cases} [-st-1, \overline{1, s-2, 1, 2(-st-1)}] & \text{if } s \geq 3, \\ [-2t-1, \overline{2, 2(-2t-1)}] & \text{if } s=2, \\ [-t-2, \overline{1, 2(-t-2)}] & \text{if } s=1, t \neq -1, -2. \end{cases} \tag{17.2}$$

If $t>0$ and $s<0$, then we have

$$\sqrt{m_3(s,t)} = [s+(4s^2+1)t-1, \overline{1, -2s-1, -2s-1, 1, 2(s+(4s^2+1)t-1)}]. \tag{17.3}$$

This lemma is proved in a similar way to that of section 16.3. Remark that we except $(s,t)=(1,-1)$ for m_2 and $(s,t)=(1,-1),(1,-2)$ for m_2' since $m_2(1,-1)=0$, $m_2'(1,-1)=-1$, and $m_2'(1,-2)=0$.

Proof of Theorem 17.2. (1) We may assume that $s>0$ since $m_2(s,t)=m_2(-s,t)$. To prove the if part, suppose $s \geq 2$ and $t=-1$. Then we obtain the RCF expansion $\sqrt{m_2(s,-1)} = [s-1, \overline{1, 2s-2}]$ by Lemma 17.4. Since the 1st convergent of $[s-1, \overline{1, 2s-2}]$ is s, the fundamental solution of $x^2 - m_2(s,t)y^2 = 1$ is $(x,y)=(s,1)$ by Proposition 14.7. However, this is not obtained from PICF expansions of $\sqrt{m_2(s,t)} = [st, \overline{2s, 2st}]$ since its 1st convergent is $(-2s^2+1)/(2s)$.

Now we prove the only if part. If $t>0$, a PICF expansion $[st, \overline{2s, 2st}]$ gives the RCF expansion of $\sqrt{m_2(s,t)}$. Hence the fundamental solution is its 1st convergent by Proposition 14.7. If $t<0$, the RCF expansion of $\sqrt{m_2(s,t)}$ is given in Lemma 17.4. Applying Proposition 14.7 to (17.1), we can find the fundamental solution. When $t \neq -1$, the fundamental solution is the 3rd convergent of (17.1) if $s \geq 2$ and is the 1st convergent of (17.1) if $s=1$. When $t=-1$, the fundamental solution is the 1st convergent of (17.1). Hence we check that the fundamental solution coincides with the 1st convergent of $\sqrt{m_2(s,t)} = [-st, \overline{-2s, -2st}]$ up to signs if $s = 1$ or $t \neq -1$.

(2) We may assume that $s > 0$ since $m'_2(s,t) = m'_2(-s,t)$. If $t > 0$, a PICF expansion $[st, \overline{s, 2st}]$ gives the RCF expansion of $\sqrt{m'_2(s,t)}$. Hence the fundamental solution is its 1st convergents by Proposition 14.7. If $t < 0$, the RCF expansion of $\sqrt{m'_2(s,t)}$ is given in Lemma 17.4. Applying Proposition 14.7 to (17.2), we find the fundamental solution. When $s \geq 3$, the fundamental solution is the 3rd convergent of (17.2). When $s = 2$ or $s = 1$, the fundamental solution is the 1st convergent of (17.2). For each case, we can check that the fundamental solution coincides with the 2nd convergent of $\sqrt{m'_2(s,t)} = [-st, \overline{-s, -2st}]$ up to signs.

(3) The proof of the if part is clear since the 2nd convergent of $\sqrt{2} = [2, \overline{-2, 3, 3}]$ does not coincide with the 0th convergent of $\sqrt{2} = [1, \overline{2}]$. Hence it is sufficient to prove the only if part.

Consider the case of

$$\mathrm{sgn}(t)\sqrt{m_3(s,t)} = [s + (4s^2+1)t, \overline{2s, 2s, 2(s + (4s^2+1)t)}]. \tag{17.4}$$

We may assume that

$$s > 0 \quad \text{and} \quad t > 0$$

or

$$s < 0 \quad \text{and} \quad t > 0$$

since $m_3(s,t) = m_3(-s,-t)$. If $s > 0$ and $t > 0$, (17.4) is the RCF expansion of $\sqrt{m_3(s,t)}$ and the fundamental solution is its 2nd convergent. If $s < 0$ and $t > 0$, the 4th convergent of (17.3) in Lemma 17.4 is the fundamental solution by Proposition 14.7 and it coincides with the 2nd convergent of (17.4) up to signs.

Consider the case of

$$\mathrm{sgn}(t)\sqrt{m_3(0,t)} = [-2 + t, \overline{1, -2, -1 + 2t}] = [-1 + t, \overline{2, -1, 1 + 2t}].$$

Then both the 2nd convergents of $[-2+t, \overline{1, -2, -1 + 2t}]$ and $[-1+t, \overline{2, -1, 1 + 2t}]$ are $-t/(-1)$, which give the fundamental solutions of $x^2 - m_3(0,t)y^2 = -1$.

Consider the case of

$$\mathrm{sgn}(t)\sqrt{m_3(\pm 1,t)} = [2 + 5t, \overline{-2, 3, 3 + 10t}] = [1 + 5t, \overline{3, -2, 3 + 10t}].$$

Then both the 2nd convergents of $[2+5t, \overline{-2, 3, 3+10t}]$ and $[1+5t, \overline{3, -2, 3+10t}]$ coincide with the 4th convergent of (17.3) up to signs, which give the fundamental solutions of $x^2 - m_3(\pm 1, t)y^2 = -1$.

□

18. $\mathbb{Z}[X_{n-1}]$-PCF expansions of X_n and the generalized Pell equation

In this section, we consider PCF expansions of certain algebraic integers related to the $\mathbb{Z}_2$-extension over $\mathbb{Q}$. For each non-negative integer n, set $X_n = 2\cos(\pi/2^{n+1})$. For example,

$$X_0 = 0, X_1 = \sqrt{2}, X_2 = \sqrt{2+\sqrt{2}}, \dots.$$

Then $\mathbb{B}_n := \mathbb{Q}(X_n)$ is the Galois extension over $\mathbb{Q}$ with $\mathrm{Gal}(\mathbb{B}_n/\mathbb{Q}) \cong \mathbb{Z}/2^n\mathbb{Z}$ and the ring of integers of $\mathbb{B}_n$ is $\mathbb{Z}[X_n]$ for $n \geq 0$. Note that $\cup_{n\geq 0}\mathbb{B}_n$ is the $\mathbb{Z}_2$-extension over $\mathbb{Q}$.

18.1. $(0,3)$**-type** $\mathbb{Z}[X_{n-1}]$**-PCF expansion of** X_n**.** For $a_i \in \mathbb{Z}[X_{n-1}]$, let $\{a_i\}$ be a sequence satisfying the periodic condition, that is, there exist $l \in \mathbb{Z}_{\geq 1}$, $N \in \mathbb{Z}_{\geq 0}$ such that the condition $a_k = a_{l+k}$ holds for all $k \geq N$. In a similar manner to a PICF, we call $[a_0, \dots, a_{N-1}, \overline{a_N, \dots, a_{N+l-1}}]$ a (N,l)-type $\mathbb{Z}[X_{n-1}]$-PCF. Block, Elkies, and Jordan asked the following question:

Question 18.1 (Brock, Elkies, and Jordan [**10**, Problem 1.1])**.** For each $n \geq 0$, $N \geq 0$ and $l \geq 1$, Find (N,l)-type $\mathbb{Z}[X_{n-1}]$-PCF expansions of X_n.

Block, Elkies, and Jordan [**10**] gave partial answers to Question 18.1. More precisely, for $n = 1, 2$, they determined the all $(0,1)$, $(0,2)$, $(0,3)$, $(1,1)$, $(1,2)$ and $(2,1)$-types $\mathbb{Z}[X_{n-1}]$-PCF expansions of X_n. Moreover, they showed that there are no $(0,1)$, $(0,2)$ and $(1,1)$-types $\mathbb{Z}[X_{n-1}]$-PCF expansions of X_n for all $n \geq 2$. By using a different approach, Yoshizaki also gave partial answers to this question. Indeed, he found $(1,2)$-type $\mathbb{Z}[X_{n-1}]$-PCF expansions of X_n for all $n \geq 1$.

Theorem 18.2 (Yoshizaki [**69**, Theorem 3.4])**.** For all $n \geq 1$, we obtain

$$X_n = \left[1, \overline{\frac{2}{1+X_{n-1}}, 2}\right].$$

In this thesis, we find $(0,3)$-type $\mathbb{Z}[X_{n-1}]$-PCF expansions of X_n for all $n \geq 1$ by considering integer points on PCF varieties. Before stating and proving our result, we prepare some notions and facts. Let $\mathbb{Z}[X_n]^\times$ be the group of units of $\mathbb{Z}[X_n]$ and τ_n is the generator of $\mathrm{Gal}(\mathbb{B}_n/\mathbb{B}_{n-1}) \cong \mathbb{Z}/2\mathbb{Z}$. We define the relative norm of the quadratic extensions

$\mathbb{B}_n/\mathbb{B}_{n-1}$ by $N_{n/n-1} : \mathbb{B}_n \to \mathbb{B}_{n-1}; x \mapsto x\tau_n(x)$. For $x \in \mathbb{Z}[X_n]$, there exists a unique pair $(a, b) \in \mathbb{Z}[X_{n-1}]^{\oplus 2}$ such that $x = a + X_n b$, and the relative norm is of the form $N_{n/n-1}(x) = a^2 - X_n^2 b^2$. Set

$$\eta_n = 1 + \sum_{k=1}^{2^n-1} 2\cos\left(\frac{k\pi}{2^{n+1}}\right).$$

Note that η_n satisfies $N_{n/n-1}(\eta_n) = -1$ (cf. Morisawa and Okazaki [**51**, (6.1)]). In particular, $\eta_n \in \mathbb{Z}[X_n]^\times$ and we call it Horie unit or Weber's normal unit (cf. Horie [**31**], Morisawa and Okazaki [**50**]). Our result is the following:

Theorem 18.3. For every non-negative integer n and $\sigma \in \mathrm{Gal}(\mathbb{B}_n/\mathbb{Q})$, a $\mathbb{Z}[X_{n-1}]$-PCF

$$\left[\overline{\sigma\left(\frac{(\eta_n - \eta_{n-1})X_n - 1}{\eta_{n-1}}\right), \sigma(\eta_{n-1}), \sigma\left(\frac{(\eta_n - \eta_{n-1})/X_n - 1}{\eta_{n-1}}\right)}\right]$$

gives a $(0, 3)$-type $\mathbb{Z}[X_{n-1}]$-PCF expansion of $\sigma(X_n)$ up to signs.

Proof. In a similar manner to Proposition 14.2, we obtain $(0, 3)$-type $\mathbb{Z}[X_{n-1}]$-PCF of X_{n-1} from $(a_1, a_2, a_3) \in V(X_n)_{0,3}(\mathbb{Z}[X_{n-1}])$ if $[\overline{a_1, a_2, a_3}]$ converges. Hence, to prove Theorem 18.3, we find the elements of $V(X_n)_{0,3}(\mathbb{Z}[X_{n-1}])$ and check the convergence for $n \geq 1$.

We see that $E((x_1, x_2, x_3))$ is

$$\begin{bmatrix} x_1x_2x_3 + x_1 + x_3 & x_1x_2 + 1 \\ x_2x_3 + 1 & x_2 \end{bmatrix}$$

.

Hence $V(X_n)_{0,3}$ is given by

$$\begin{cases} x_2 - x_1x_2x_3 - x_1 - x_3 = 0, \\ x_1x_2 + 1 = X_n^2(x_2x_3 + 1). \end{cases} \tag{18.1}$$

By eliminating x_1 from (18.1), we obtain

$$x_2^2 - X_n^2(x_2x_3 + 1)^2 = -1. \tag{18.2}$$

Here, we take

$$x_2 = \eta_{n-1},$$
$$x_3 = \left(-1 + \sum_{\substack{1 \le k \le 2^n - 1, \\ 2 \nmid k}} \epsilon_{k,n} \right) \Bigg/ \eta_{n-1}, \tag{18.3}$$

where $\epsilon_{k,n} = (2\cos(k\pi/2^{n+1}))/(2\cos(\pi/2^{n+1}))$. Then we obtain $\eta_n = x_2 + X_n(x_2 x_3 + 1)$ since

$$\begin{aligned} \eta_n &= 1 + \sum_{k=1}^{2^n-1} 2\cos(k\pi/2^{n+1}) \\ &= \eta_{n-1} + \sum_{\substack{1 \le k \le 2^n - 1, \\ 2 \nmid k}} 2\cos(k\pi/2^{n+1}) \\ &= \eta_{n-1} + 2\cos(\pi/2^{n+1}) \sum_{\substack{1 \le k \le 2^n - 1, \\ 2 \nmid k}} \epsilon_{k,n}. \end{aligned}$$

Combining this with $N_{n/n-1}(\eta_n) = -1$, we see that (18.3) are the solutions of (18.2). We also obtain $\epsilon_{k,n} \in \mathbb{Z}[X_n]^\times$ since $2\cos(k\pi/2^{n+1})$ are prime elements on 2 in $\mathbb{Z}[X_n]$ for each odd integer k and 2 ramifies completely in $\mathbb{B}_n/\mathbb{Q}$ for $n \geq 1$. From $\tau_n(\epsilon_{k,n}) = \epsilon_{k,n}$, we see that $\epsilon_{k,n} \in \mathbb{Z}[X_n]^\times \cap \mathbb{B}_{n-1} = \mathbb{Z}[X_{n-1}]^\times$ for each odd integer k and $n \in \mathbb{Z}_{\geq 1}$. Hence $x_2, x_3 \in \mathbb{Z}[X_{n-1}]$.

By the definition of X_n and η_n, we obtain

$$\sum_{\substack{1 \le k \le 2^n - 1, \\ 2 \nmid k}} \epsilon_{k,n} = \frac{\eta_n - \eta_{n-1}}{X_n}$$

and

$$x_1 = \frac{X_n^2(x_2 x_3 + 1) - 1}{x_2} = \frac{X_n(\eta_n - \eta_{n-1}) - 1}{\eta_{n-1}}.$$

Hence we obtain the elements of $V(X_n)_{0,3}(\mathbb{Z}[X_{n-1}])$ for $n \geq 1$. In a similar way, we also check that

$$\left(\sigma\left(\frac{(\eta_n - \eta_{n-1})X_n - 1}{\eta_{n-1}} \right), \sigma(\eta_{n-1}), \sigma\left(\frac{(\eta_n - \eta_{n-1})/X_n - 1}{\eta_{n-1}} \right) \right) \in V(X_n)_{0,3}(\mathbb{Z}[X_{n-1}])$$

for every $\sigma \in \mathrm{Gal}(\mathbb{B}_n/\mathbb{Q})$.

We can also check the convergence of the PCFs by using Theorem 4.3 in Brock, Elkies, and Jordan [**10**]. Indeed, we obtain

$$
\begin{aligned}
&E((x_1, x_2, x_3)) = \begin{bmatrix} \sigma(\eta_{n-1}) & \sigma((\eta_n - \eta_{n-1})X_n - 1) \\ \sigma((\eta_n - \eta_{n-1})X_n - 1)/X_n^2 & \sigma(\eta_{n-1}) \end{bmatrix} \neq \pm(\sqrt{-1})^3 I, \\
&M([x_1, x_2, x_3])_{21} = x_2x_3 + 1 \neq 0, \\
&M([x_2, x_3, x_1])_{21} = x_3x_1 + 1 \neq 0, \\
&M([x_3, x_1, x_2])_{21} = x_1x_2 + 1 \neq 0, \\
&(-1)^3\mathrm{Tr}(E(x_1, x_2, x_3))^2 = -4\sigma(\eta_{n-1})^2 < 0.
\end{aligned}
$$

Hence we complete the proof. □

Note that we obtain

$$
\begin{aligned}
&\left[\overline{\sigma\left(\frac{(\eta_n - \eta_{n-1})X_n - 1}{\eta_{n-1}}\right), \sigma(\eta_{n-1}), \sigma\left(\frac{(\eta_n - \eta_{n-1})/X_n - 1}{\eta_{n-1}}\right)}\right] \\
&= \begin{cases} \sigma(X_n) & \text{if } |\sigma(\eta_n)| > 1, \\ -\sigma(X_n) & \text{otherwise,} \end{cases}
\end{aligned}
$$

for every $\sigma \in \mathrm{Gal}(\mathbb{B}_n/\mathbb{Q})$.

18.2. An application to the generalized Pell equation. From Theorem 18.3, we obtain $(1, 3)$-type $\mathbb{Z}[X_{n-1}]$-PCF expansions of X_n, that is,

$$
\left[\frac{(\eta_n - \eta_{n-1})X_n - 1}{\eta_{n-1}}, \overline{\eta_{n-1}, \frac{(\eta_n - \eta_{n-1})/X_n - 1}{\eta_{n-1}}, \frac{(\eta_n - \eta_{n-1})X_n - 1}{\eta_{n-1}}}\right]. \tag{18.4}
$$

We will show an application of $\mathbb{Z}[X_{n-1}]$-PCF expansions (18.4) to solutions of the generalized Pell equation $x^2 - X_n^2y^2 = \pm1$ in $\mathbb{Z}[X_{n-1}]$. When $n = 1$, the generalized Pell equation coincides with the Pell equation $x^2 - 2y^2 = \pm1$. In what follows, we will consider the solutions of the generalized Pell equation in $\mathbb{Z}[X_{n-1}]$. Set

$$
W_n := \{(u, v) \in \mathbb{Z}[X_{n-1}]^2 \mid u^2 - X_n^2v^2 = 1 \text{ or } u^2 - X_n^2v^2 = -1\}
$$

and

$$
RE_n = \{\epsilon \in \mathbb{Z}[X_n] \mid N_{n/n-1}(\epsilon) \in \{\pm1\}\} \subset \mathbb{Z}[X_n]^\times.
$$

The RE_n is a subgroup of $\mathbb{Z}[X_n]^\times$ and called the group of relative units. By Dirichlet's unit theorem, we obtain the isomorphism as a $\mathbb{Z}$-module

$$RE_n \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^{2^{n-1}}.$$

In a similar manner to the Pell equation, there is a bijection

$$W_n \cong RE_n;\ (x, y) \mapsto x + X_n y$$

for each $n \geq 1$. The set in W_n corresponding to the generators of RE_n is called a fundamental solution of the generalized Pell equation.

The RE_n is also related to the Weber conjecture. Let h_n be the class number of $\mathbb{B}_n$ for $n \in \mathbb{Z}_{\geq 1}$.

Conjecture 18.4 (cf. Miller [**47**, Section 2])**.** For each $n \in \mathbb{Z}_{\geq 1}$, we have $h_n = 1$.

Assuming Conjecture 18.4, we find that the set of the 2nd convergents of (18.4) gives a fundamental solution of the generalized Pell equation $x^2 - X_n^2 y^2 = \pm 1$ for each n. This is an analogue for Proposition 14.7. Let (p_2, q_2) be the 2nd convergent of (18.4) and set

$$A_n = \langle -1, \sigma(p_2 + X_n q_2) \mid \sigma \in \mathrm{Gal}(\mathbb{B}_n/\mathbb{Q})\rangle_{\mathbb{Z}}.$$

Proposition 18.5. Assuming Conjecture 18.4, we obtain $RE_n = A_n$ for each $n \in \mathbb{Z}_{\geq 1}$.

Proof. Set $X_n = [\overline{a_1, a_2, a_3}]$ as a $(0, 3)$-type $\mathbb{Z}[X_{n-1}]$-PCF in Theorem 18.3. Then

$$\frac{p_2}{q_2} = \frac{a_1 a_2 a_3 + a_1 + a_3}{a_2 a_3 + 1} = \frac{\eta_{n-1}}{(\eta_n - \eta_{n-1})/X_n}$$

and we see that $p_2 X_n + q_2 = \eta_n$. Thus, we obtain

$$A_n = \langle -1, \sigma(\eta_n) \mid \sigma \in \mathrm{Gal}(\mathbb{B}_n/\mathbb{Q})\rangle_{\mathbb{Z}}.$$

In what follows, we will show $(RE_n : A_n) = h_n/h_{n-1}$ for $n \in \mathbb{Z}_{\geq 1}$, where $(RE_n : A_n)$ is the index. Set

$$A_n^+ = \langle -1, \sigma(\eta_n) \mid \sigma \in \mathrm{Gal}(\mathbb{B}_n/\mathbb{Q})\rangle_{\mathbb{Z}} \cap \{\epsilon \in \mathbb{Z}[X_n] \mid N_{n/n-1}(\epsilon) = 1\}.$$

By Morisawa and Okazaki [**51**, Lemma 3.2, (2)], we see that $(RE_n : A_n) = (RE_n^+ : A_n^+)$. Hence it is sufficient to show $(RE_n^+ : A_n^+) = h_n/h_{n-1}$, which is already shown in Yoshizaki [**69**, Section 4]. For convenience, we will recall the outline of the proof.

Let C_n be the group of cyclotomic units in $\mathbb{B}_n$ (cf. Washington [**66**, Chapter 8]). Then $A_n^+ = RE_n^+ \cap C_n$ and the relative norm induces the following exact sequence:

$$1 \to RE_n^+/A_n^+ \to \mathbb{Z}[X_n]^\times/C_n \to \mathbb{Z}[X_{n-1}]^\times/C_{n-1} \to 1.$$

Since $(\mathbb{Z}[X_n]^\times : C_n) = h_n$ (cf. Washington [**66**, Theorem 8.2]), we obtain $(RE_n^+ : A_n^+) = h_n/h_{n-1}$. $\square$

Appendix

A. Comparison of two proportions

In this section, we consider the relationship between the proportion defined by affine points and the proportion defined by projective points. Before stating and proving our theorem, we prepare some notations. Let A be a subset of $\mathbb{Z}^{\oplus n+1}$ such that

- $A \neq \{\mathbf{0}\}$,
- $\boldsymbol{a} \in A \Longrightarrow d\boldsymbol{a} \in A$ for all $d \in \mathbb{Z} \setminus \{0\}$

holds. Here we set $d\boldsymbol{a} = (da_0, \ldots, da_n)$ for $\boldsymbol{a} = (a_0, \ldots, a_n) \in \mathbb{Z}^{\oplus n+1}$ and $d \in \mathbb{Z}$. For $\boldsymbol{a} = (a_0, \ldots, a_n) \in \mathbb{Z}^{\oplus n+1}$, we denote $\gcd(a_0, \ldots, a_n)$ by $\gcd(\boldsymbol{a})$ and the set of $(n+1)$-tuples of integers $\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1}$ with $\gcd(a_0, \ldots, a_n) = 1$ by $\mathbb{Z}^{\oplus n+1}_{\text{prim}}$. For $H \in \mathbb{R}_{\geq 0}$, we define

$$B_A(H) = \#\{\boldsymbol{a} \in A \mid |\boldsymbol{a}| < H\},$$
$$B_{A,\text{prim}}(H) = \#\left\{\boldsymbol{a} \in A \cap \mathbb{Z}^{\oplus n+1}_{\text{prim}} \mid |\boldsymbol{a}| < H\right\},$$

where $|\boldsymbol{a}| = \max_i \{|a_i|\}$ with the Euclidean norm $|\cdot|$ on $\mathbb{R}$. In particular for $A = \mathbb{Z}^{\oplus n+1}$, we have $B_{\mathbb{Z}^{\oplus n+1}}(H)$ and $B_{\mathbb{Z}^{\oplus n+1},\text{prim}}(H)$. Since there is a bijection

$$\left\{\boldsymbol{a} \in A \,\middle|\, \gcd(\boldsymbol{a}) = 1 \text{ and } |\boldsymbol{a}| < \frac{H}{d}\right\} \xrightarrow{\cong} \{\boldsymbol{a} \in A \mid \gcd(\boldsymbol{a}) = d \text{ and } |\boldsymbol{a}| < H\}; \quad \boldsymbol{a} \mapsto d\boldsymbol{a}$$

for $d \in \mathbb{Z} \setminus \{0\}$ and

$$\#\left\{\boldsymbol{a} \in A \,\middle|\, |\boldsymbol{a}| < \frac{H}{d}\right\} = 0$$

for $d \geq H$, we obtain

$$B_A(H) = \sum_{m \in \mathbb{Z}_{\geq 1}} B_{A,\text{prim}}\left(\frac{H}{m}\right). \tag{A.1}$$

Note that $B_{A,\text{prim}}(H)$ is equal to

$$\#\left\{\boldsymbol{a} = [a_0 : \cdots : a_n] \in \mathbb{P}^n(\mathbb{Q}) \,\middle|\, \overline{h}(\boldsymbol{a}) < H \text{ and } \boldsymbol{a}' \in A\right\}.$$

Recall that for $\boldsymbol{a} \in \mathbb{P}^n(\mathbb{Q})$, there exists a tuple of integers $\boldsymbol{a}' = (a'_0, \ldots, a'_n) \in \mathbb{Z}^{\oplus n+1}$ that satisfies

$$[a_0 : \cdots : a_n] = [a'_0 : \cdots : a'_n] \quad \text{and} \quad \gcd(\boldsymbol{a}') = 1.$$

Using $\boldsymbol{a}'$, we define the height $\overline{h}$ by

$$\overline{h}(\boldsymbol{a}) := \max_i \{|a'_i|\}.$$

for $\boldsymbol{a} \in \mathbb{P}^n(\mathbb{Q})$. Then we obtain the following:

THEOREM A.1. Let n be an integer with $n \geq 2$. Suppose that there exists $c \in \mathbb{R}$ such that

$$B_{A,\mathrm{prim}}(H) = cB_{\mathbb{Z}^{\oplus n+1},\mathrm{prim}}(H) + o(H^{n+1}) \tag{A.2}$$

as $H \to \infty$. Then

$$B_A(H) = cB_{\mathbb{Z}^{\oplus n+1}}(H) + o(H^{n+1})$$

holds as $H \to \infty$.

PROOF. By (A.1), we obtain

$$\begin{aligned} B_A(H) &= \sum_{m \in \mathbb{Z}_{\geq 1}} B_{A,\mathrm{prim}}\left(\frac{H}{m}\right) \\ &= \sum_{\substack{m \in \mathbb{Z} \\ 1 \leq m < \sqrt{H}}} B_{A,\mathrm{prim}}\left(\frac{H}{m}\right) + \sum_{\substack{m \in \mathbb{Z} \\ \sqrt{H} \leq m}} B_{A,\mathrm{prim}}\left(\frac{H}{m}\right). \end{aligned}$$

Since

$$\begin{aligned} \sum_{\substack{m \in \mathbb{Z} \\ 1 \leq m < \sqrt{H}}} \left(\frac{H}{m}\right)^{n+1} &= H^{n+1} \sum_{\substack{m \in \mathbb{Z} \\ 1 \leq m < \sqrt{H}}} \left(\frac{1}{m}\right)^{n+1} \\ &\leq H^{n+1}\left(1 + \int_1^{\sqrt{H}} \left(\frac{1}{t}\right)^{n+1} dt\right) \\ &= H^{n+1}\left(1 + \left[\frac{t^{-n}}{n}\right]_{\sqrt{H}}^{1}\right) \\ &= H^{n+1}\left(1 + \frac{1}{n} - \frac{H^{-n/2}}{n}\right) \\ &= O\left(H^{\frac{n}{2}+1}\right), \end{aligned}$$

$n \geq 2$, and (A.2), we obtain

$$\sum_{\substack{m \in \mathbb{Z} \\ 1 \leq m < \sqrt{H}}} B_{A,\mathrm{prim}}\left(\frac{H}{m}\right) = \sum_{\substack{m \in \mathbb{Z} \\ 1 \leq m < \sqrt{H}}} \left(cB_{\mathbb{Z}^{\oplus n+1},\mathrm{prim}}\left(\frac{H}{m}\right) + o\left(\left(\frac{H}{m}\right)^{n+1}\right)\right)$$

$$
\begin{aligned}
&= c \sum_{\substack{m\in\mathbb{Z} \\ 1\le m<\sqrt{H}}} B_{\mathbb{Z}^{\oplus n+1},\mathrm{prim}}\left(\frac{H}{m}\right) + \sum_{\substack{m\in\mathbb{Z} \\ 1\le m<\sqrt{H}}} o\left(\left(\frac{H}{m}\right)^{n+1}\right) \\
&= c \sum_{\substack{m\in\mathbb{Z} \\ 1\le m<\sqrt{H}}} B_{\mathbb{Z}^{\oplus n+1},\mathrm{prim}}\left(\frac{H}{m}\right) + o\left(H^{n+1}\right).
\end{aligned}
$$

Moreover, the inequality

$$
\begin{aligned}
\sum_{\substack{m\in\mathbb{Z} \\ \sqrt{H}\le m<H}} B_{A,\mathrm{prim}}\left(\frac{H}{m}\right) &\le \sum_{\substack{m\in\mathbb{Z} \\ \sqrt{H}\le m<H}} B_{A,\mathrm{prim}}\left(\sqrt{H}\right) \\
&\le \sum_{\substack{m\in\mathbb{Z} \\ \sqrt{H}\le m<H}} B_{\mathbb{Z}^{\oplus n+1}}\left(\sqrt{H}\right) \\
&\le H\left(2\sqrt{H}+1\right)^{n+1} \\
&= O\left(H^{\frac{n+3}{2}}\right)
\end{aligned}
$$

holds. Note that this inequality also holds for $\sum_{\substack{m\in\mathbb{Z} \\ \sqrt{H}\le m<H}} B_{\mathbb{Z}^{\oplus n+1},\mathrm{prim}}(H/m)$. Since $n \ge 2$, we deduce that

$$
\begin{aligned}
B_A(H) &= c \sum_{\substack{m\in\mathbb{Z} \\ 1\le m<\sqrt{H}}} B_{\mathbb{Z}^{\oplus n+1},\mathrm{prim}}\left(\frac{H}{m}\right) + o\left(H^{n+1}\right) \\
&= c \sum_{m\in\mathbb{Z}_{\ge 1}} B_{\mathbb{Z}^{\oplus n+1},\mathrm{prim}}\left(\frac{H}{m}\right) - \sum_{\substack{m\in\mathbb{Z} \\ \sqrt{H}\le m<H}} B_{\mathbb{Z}^{\oplus n+1},\mathrm{prim}}\left(\frac{H}{m}\right) + o\left(H^{n+1}\right) \\
&= cB_{\mathbb{Z}^{\oplus n+1}}(H) + o(H^{n+1})
\end{aligned}
$$

as $H \to \infty$, which completes the proof. □

In what follows, we use the notations in §3. Recall that the proportions

$$
\rho(n,k),\ \rho_{\mathrm{loc}}(n,k),\ \rho'(n,k),\ \rho'_{\mathrm{loc}}(n,k)
$$

are

$$
\rho(n,k) := \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a}\in\mathbb{P}^n(\mathbb{Q}) \;\middle|\; \overline{h}(\boldsymbol{a})<H \text{ and } X_{\boldsymbol{a}}^k(\mathbb{Q})\ne\emptyset\right\}}{\#\left\{\boldsymbol{a}\in\mathbb{P}^n(\mathbb{Q}) \;\middle|\; \overline{h}(\boldsymbol{a})<H\right\}}
$$

$$
\begin{aligned}
&= \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{Z}_{\mathrm{prim}}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H \text{ and } X_{\boldsymbol{a}}^k(\mathbb{Q}) \neq \emptyset\right\}}{\#\left\{\boldsymbol{a} \in \mathbb{Z}_{\mathrm{prim}}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H\right\}},\\
\rho_{\mathrm{loc}}(n,k) &:= \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{P}^n(\mathbb{Q}) \,\middle|\, \overline{h}(\boldsymbol{a}) < H \text{ and } X_{\boldsymbol{a}}^k(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in M_{\mathbb{Q}}\right\}}{\#\left\{\boldsymbol{a} \in \mathbb{P}^n(\mathbb{Q}) \,\middle|\, \overline{h}(\boldsymbol{a}) < H\right\}}\\
&= \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{Z}_{\mathrm{prim}}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H \text{ and } X_{\boldsymbol{a}}^k(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in M_{\mathbb{Q}}\right\}}{\#\left\{\boldsymbol{a} \in \mathbb{Z}_{\mathrm{prim}}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H\right\}},\\
\rho'(n,k) &:= \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H \text{ and } X_{\boldsymbol{a}}^k(\mathbb{Q}) \neq \emptyset\right\}}{\#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \mid |\boldsymbol{a}| < H\right\}},\\
\rho'_{\mathrm{loc}}(n,k) &:= \lim_{H\to\infty} \frac{\#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H \text{ and } X_{\boldsymbol{a}}^k(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in M_{\mathbb{Q}}\right\}}{\#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \mid |\boldsymbol{a}| < H\right\}}
\end{aligned}
$$

if the limit exist. For $H \in \mathbb{R}$, we set

$$
\begin{aligned}
\mathrm{den}(H) &= \#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H\right\} = (2[H]+1)^{n+1},\\
\mathrm{den}_{\mathrm{prim}}(H) &= \#\left\{\boldsymbol{a} \in \mathbb{Z}_{\mathrm{prim}}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H\right\},\\
\mathrm{num}(H) &= \#\left\{\boldsymbol{a} \in \mathbb{Z}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H \text{ and } X_{\boldsymbol{a}}^k(\mathbb{Q}) \neq \emptyset\right\},\\
\mathrm{num}_{\mathrm{prim}}(H) &= \#\left\{\boldsymbol{a} \in \mathbb{Z}_{\mathrm{prim}}^{\oplus n+1} \,\middle|\, |\boldsymbol{a}| < H \text{ and } X_{\boldsymbol{a}}^k(\mathbb{Q}) \neq \emptyset\right\},
\end{aligned}
$$

where $[H]$ is the largest integer that does not exceed H. In a similar manner to the proof of Theorem A.1, we obtain the following:

Lemma A.2. Suppose that $n \geq 2$. Then we obtain

$$
\mathrm{den}(H) = C\mathrm{den}_{\mathrm{prim}}(H) + o(H^{n+1})
$$

for some $C \in \mathbb{R}$ as $H \to \infty$.

Combining Lemma A.2 with Theorem A.1, we obtain the desired result:

Corollary A.3. Fix $n, k \in \mathbb{Z}_{\geq 2}$. Suppose that the limits $\rho(n,k)$ and $\rho_{\mathrm{loc}}(n,k)$ exist. Then the limits $\rho'(n,k)$ and $\rho'_{\mathrm{loc}}(n,k)$ also exist and the equalities

$$
\begin{aligned}
\rho'(n,k) &= \rho(n,k),\\
\rho'_{\mathrm{loc}}(n,k) &= \rho_{\mathrm{loc}}(n,k)
\end{aligned}
$$

hold.

Proof. In the following, we prove $\rho'(n,k) = \rho(n,k)$. In a similar manner, we can prove $\rho'_{\mathrm{loc}}(n,k) = \rho_{\mathrm{loc}}(n,k)$.

If $\mathrm{num}(H) = o(H^{n+1})$ as $H \to \infty$, we obtain $\rho(n,k) = \rho'(n,k) = 0$ by Lemma A.2. Hence it is sufficient to consider the case when $\mathrm{num}(H) = O(H^{n+1})$ as $H \to \infty$. By Lemma A.2 and the assumption of Corollary A.3, we obtain

$$\mathrm{num}_{\mathrm{prim}}(H) = \rho(n,k)\mathrm{den}_{\mathrm{prim}}(H) + o(H^{n+1})$$

for some $C \in \mathbb{R}$ as $H \to \infty$. Applying Theorem A.1, we obtain

$$\mathrm{num}(H) = \rho(n,k)\mathrm{den}(H) + o(H^{n+1}).$$

as $H \to \infty$. Hence we deduce

$$\rho'(n,k) = \lim_{H\to\infty} \frac{\mathrm{num}(H)}{\mathrm{den}(H)} = \lim_{H\to\infty} \frac{\rho(n,k)\mathrm{den}(H) + o(H^{n+1})}{\mathrm{den}(H)} = \rho(n,k),$$

which complete the proof. □

Note that we can prove a similar result for a family of hypersurfaces of degree k in $(n+1)$-variables, which Poonen and Voloch mentioned in [**56**, Remark 2.1 (2)].

Bibliography

[1] N. Aoki, *On the 2-Selmer groups of elliptic curves arising from the congruent number problem*, Comment. Math. Univ. St. Paul. **48** (1999), no. 1, 77–101. MR1684768

[2] R. C. Baker, *Diagonal cubic equations. II*, Acta Arith. **53** (1989), no. 3, 217–250, DOI 10.4064/aa-53-3-217-250. MR1032826

[3] M. Bhargava, *A positive proportion of plane cubics fail the Hasse principle* (2014), available at `arXiv:1402.1131v1`.

[4] M. Bhargava, J. Cremona, and T. Fisher, *The proportion of genus one curves over $\mathbb{Q}$ defined by a binary quartic that everywhere locally have a point*, Int. J. Number Theory **17** (2021), no. 4, 903–923, DOI 10.1142/S1793042121500147. MR4262272

[5] M. Bhargava, J. Cremona, T. Fisher, N. Jones, and J. Keating, *What is the probability that a random integral quadratic form in n variables has an integral zero?*, Int. Math. Res. Not. IMRN **12** (2016), 3828–3848, DOI 10.1093/imrn/rnv251. MR3544620

[6] M. Bhargava and W. Ho, *On average sizes of Selmer groups and ranks in families of elliptic curves having marked points* (2022), available at `arXiv:2207.03309v2`.

[7] B. J. Birch, *Forms in many variables*, Proc. Roy. Soc. London Ser. A **265** (1961/62), 245–263, DOI 10.1098/rspa.1962.0007. MR0150129

[8] B. J. Birch and H. P. F. Swinnerton-Dyer, *The Hasse problem for rational surfaces*, J. Reine Angew. Math. **274/275** (1975), 164–174, DOI 10.1515/crll.1975.274-275.164. MR0429913

[9] M. J. Bright, T. D. Browning, and D. Loughran, *Failures of weak approximation in families*, Compos. Math. **152** (2016), no. 7, 1435–1475, DOI 10.1112/S0010437X16007405. MR3530447

[10] B. W. Brock, N. D. Elkies, and B. W. Jordan, *Periodic continued fractions over S-integers in number fields and Skolem's p-adic method*, Acta Arith. **197** (2021), no. 4, 379–420, DOI 10.4064/aa191001-7-8. MR4201432

[11] T. D. Browning, *How often does the Hasse principle hold?*, Algebraic geometry: Salt Lake City 2015, Proc. Sympos. Pure Math., vol. 97, Amer. Math. Soc., Providence, RI, 2018, pp. 89–102. MR3821168

[12] ———, *Many cubic surfaces contain rational points*, Mathematika **63** (2017), no. 3, 818–839, DOI 10.1112/S0025579317000195. MR3731306

[13] T. D. Browning and R. Dietmann, *Solubility of Fermat equations*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math., vol. 493, Amer. Math. Soc., Providence, RI, 2009, pp. 99–106, DOI 10.1090/conm/493/09666. MR2537095

[14] T. D. Browning and R. Heath-Brown, *Forms in many variables and differing degrees*, J. Eur. Math. Soc. (JEMS) **19** (2017), no. 2, 357–394, DOI 10.4171/JEMS/668. MR3605019

[15] T. D. Browning, P. Le Boudec, and W. Sawin, *The Hasse principle for random Fano hypersurfaces*, Ann. of Math. (2) **197** (2023), no. 3, 1115–1203, DOI 10.4007/annals.2023.197.3.3. MR4564262

[16] J. Brüdern and R. Dietmann, *Random Diophantine equations, I*, Adv. Math. **256** (2014), 18–45, DOI 10.1016/j.aim.2014.01.017. MR3177289

[17] J. W. S. Cassels and M. J. T. Guy, *On the Hasse principle for cubic surfaces*, Mathematika **13** (1966), 111–120, DOI 10.1112/S0025579300003879. MR211966

[18] J.-L. Colliot-Thélène, J.-J. Sansuc, and H. P. F. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces. I*, J. Reine Angew. Math. **373** (1987), 37–107. MR870307

[19] J.-L. Colliot-Thélène and A. N. Skorobogatov, *The Brauer-Grothendieck group*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 71, Springer, Cham, [2021] ©2021. MR4304038

[20] J.-L. Colliot-Thélène and H. P. F. Swinnerton-Dyer, *Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties*, J. Reine Angew. Math. **453** (1994), 49–112, DOI 10.1515/crll.1994.453.49. MR1285781

[21] H. Davenport, *On Waring's problem for cubes*, Acta Math. **71** (1939), 123–143, DOI 10.1007/BF02547752. MR000026

[22] ———, *Cubic forms in thirty-two variables*, Philos. Trans. Roy. Soc. London Ser. A **251** (1959), 193–232, DOI 10.1098/rsta.1959.0002. MR105394

[23] K. Feng and M. Xiong, *On elliptic curves $y^2 = x^3 - n^2x$ with rank zero*, J. Number Theory **109** (2004), no. 1, 1–26, DOI 10.1016/j.jnt.2003.12.015. MR2098473

[24] T. Fisher, W. Ho, and J. Park, *Everywhere local solubility for hypersurfaces in products of projective spaces*, Res. Number Theory **7** (2021), no. 1, Paper No. 6, 27, DOI 10.1007/s40993-020-00223-z. MR4199457

[25] M. Fujiwara, *Hasse principle in algebraic equations*, Acta Arith. **22** (1972/73), 267–276, DOI 10.4064/aa-22-3-267-276. MR0319895

[26] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, DOI 10.1007/BF01388809. MR833192

[27] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum': IV. The singular series in Waring's Problem and the value of the number $G(k)$*, Math. Z. **12** (1922), no. 1, 161–188, DOI 10.1007/BF01482074. MR1544511

[28] R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), no. 1, 171–195, DOI 10.1007/BF01231285. MR1193603

[29] D. Hilbert, *Mathematical problems*, Bull. Amer. Math. Soc. **8** (1902), no. 10, 437–479, DOI 10.1090/S0002-9904-1902-00923-3. MR1557926

[30] Y. Hirakawa and Y. Kanamura, *How to calculate the proportion of everywhere locally soluble diagonal hypersurfaces*, Int. J. Number Theory **17** (2021), no. 10, 2361–2377, DOI 10.1142/S1793042121500925. MR4322838

[31] K. Horie, *The ideal class group of the basic $\mathbb{Z}_p$-extension over an imaginary quadratic field*, Tohoku Math. J. (2) **57** (2005), no. 3, 375–394. MR2154097

[32] L.-K. Hua, *On Waring's problem*, Q. J. Math. **9** (1938), no. 1, 199–202, DOI 10.1093/qmath/os-9.1.199.

[33] Y. Ishitsuka and Y. Kanamura, *On the proportions of soluble forms in some families of locally soluble binary quartic forms* (2023), to appear in Tokyo J. Math., available at `arXiv:2306.15233`.

[34] M. J. Jacobson Jr. and H. C. Williams, *Solving the Pell equation*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, Springer, New York, 2009. MR2466979

[35] B. W. Jordan, A. Logan, and Y. Zaytman, *The Zariski closure of integral points on varieties parametrizing periodic continued fractions* (2021), available at `arXiv:1910.12788v2`.

[36] B. W. Jordan and Y. Zaytman, *Integral points on varieties defined by matrix factorization into elementary matrices*, J. Number Theory **217** (2020), 340–352, DOI 10.1016/j.jnt.2020.05.016. MR4140633

[37] S. Katok and I. Ugarcovici, *Geometrically Markov geodesics on the modular surface*, Mosc. Math. J. **5** (2005), no. 1, 135–155, DOI 10.17323/1609-4514-2005-5-1-135-155 (English, with English and Russian summaries). MR2153471

[38] J. Kollár, *Unirationality of cubic hypersurfaces*, J. Inst. Math. Jussieu **1** (2002), no. 3, 467–476, DOI 10.1017/S1474748002000117. MR1956057

[39] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483. MR1106906

[40] D. Kriz and C. Li, *Goldfeld's conjecture and congruences between Heegner points*, Forum Math. Sigma **7** (2019), Paper No. e15, 80, DOI 10.1017/fms.2019.9. MR3954912

[41] D. J. Lewis, *Cubic congruences*, Michigan Math. J. **4** (1957), 85–95. MR84013

[42] C. Li, *Recent developments on quadratic twists of elliptic curves*, Proceedings of the International Consortium of Chinese Mathematicians 2017, Int. Press, Boston, MA, 2020, pp. 381–399. MR4251120

[43] D. Loughran, N. Rome, and E. Sofos, *The leading constant for rational points in families* (2023), available at `arXiv:2210.13559v4`.

[44] Y. I. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne*, Actes du Congrès International des Mathématiciens (Nice, 1970), Gauthier-Villars Éditeur, Paris, 1971, pp. 401–411. MR0427322

[45] ———, *Cubic forms*, 2nd ed., North-Holland Mathematical Library, vol. 4, North-Holland Publishing Co., Amsterdam, 1986. Algebra, geometry, arithmetic; Translated from the Russian by M. Hazewinkel. MR833513

[46] J. V. Matijasevič, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 (Russian). MR0258744

[47] J. C. Miller, *Class numbers of totally real fields and applications to the Weber class number problem*, Acta Arith. **164** (2014), no. 4, 381–398, DOI 10.4064/aa164-4-4. MR3244941

[48] V. Mitankin and C. Salgado, *Rational points on del Pezzo surfaces of degree four*, Int. J. Number Theory **18** (2022), no. 9, 2099–2127, DOI 10.1142/S179304212250107X. MR4454468

[49] R. A. Mollin, *Polynomial solutions for Pell's equation revisited*, Indian J. Pure Appl. Math. **28** (1997), no. 4, 429–438. MR1448033

[50] T. Morisawa and R. Okazaki, *Height and Weber's class number problem*, J. Théor. Nombres Bordeaux **28** (2016), no. 3, 811–828 (English, with English and French summaries). MR3610699

[51] ______, *Filtrations of units of Viète field*, Int. J. Number Theory **16** (2020), no. 5, 1067–1079, DOI 10.1142/S1793042120500554. MR4101587

[52] M. B. Nathanson, *Polynomial Pell's equations*, Proc. Amer. Math. Soc. **56** (1976), 89–92, DOI 10.2307/2041581. MR401641

[53] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, 5th ed., John Wiley & Sons, Inc., New York, 1991. MR1083765

[54] B. Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. MR3729254

[55] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149, DOI 10.2307/121064. MR1740984

[56] B. Poonen and J. F. Voloch, *Random Diophantine equations*, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, pp. 175–184, DOI 10.1007/978-0-8176-8170-8_11. With appendices by Jean-Louis Colliot-Thélène and Nicholas M. Katz. MR2029869

[57] A. M. S. Ramasamy, *Polynomial solutions for the Pell's equation*, Indian J. Pure Appl. Math. **25** (1994), no. 6, 577–581. MR1285220

[58] E. S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362 (1 plate), DOI 10.1007/BF02395746. MR0041871

[59] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French; Graduate Texts in Mathematics, No. 7. MR0344216

[60] ______, *Spécialisation des éléments de* $\mathrm{Br}_2(\mathbf{Q}(T_1, \cdots, T_n))$, C. R. Acad. Sci. Paris Sér. I Math. **311** (1990), no. 7, 397–402 (French, with English summary). MR1075658

[61] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[62] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves*, 2nd ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015. MR3363545

[63] A. N. Skorobogatov, *Beyond the Manin obstruction*, Invent. Math. **135** (1999), no. 2, 399–424, DOI 10.1007/s002220050291. MR1666779

[64] ______, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, Cambridge, 2001. MR1845760

[65] A. Smith, *The congruent numbers have positive natural density* (2016), available at `arXiv:1603.08479v2`.

[66] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575

[67] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948 (French). MR0027151

[68] M. Xiong and A. Zaharescu, *Selmer groups and Tate-Shafarevich groups for the congruent number problem*, Comment. Math. Helv. **84** (2009), no. 1, 21–56, DOI 10.4171/CMH/151. MR2466074

[69] H. Yoshizaki, *Generalized Pell's equations and Weber's class number problem*, J. Théor. Nombres Bordeaux **35** (2023), no. 2, 373–391 (English, with English and French summaries). MR4655363