Uniform construction of non-singular ternary and quaternary homogeneous forms violating the local-global principle

August 2020

Yoshinosuke Hirakawa

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

Uniform construction of non-singular ternary and quaternary homogeneous forms violating the local-global principle

August 2020

Graduate School of Science and Technology
Keio University

Yoshinosuke Hirakawa

Contents

Thesis Summary

In number theory, rational points on algebraic varieties have been studied by many people from the time of Diophantus of Alexandria. In particular, it is an important problem to determine whether a given algebraic variety has a rational point or not. It is obvious that an algebraic variety has no rational points if it has no local points. However, it is a very deep problem to determine whether an algebraic variety with local points has a rational point or not. In fact, many SPORADIC examples of algebraic varieties are known to have local points but no rational points, i.e., violate the local-global principle. In this thesis, we give two kinds of conjectural but UNIFORM constructions of algebraic varieties which violate the local-global principle. More precisely, our UNIFORM construction of algebraic varieties of specified dimension means an algorithm to obtain a non-singular projective hypersurface of the projective space $\mathbb{P}^N$ of every sufficiently large degree $n \gg 1$ which violates the local-global principle ($N = 3$ or 4 in this thesis).

In the first part of this thesis, we construct a family of non-singular curves of odd degree $n > 3$ which violate the local-global principle under a certain mild hypothesis on the degree n. In fact, we conjecture that EVERY odd integer $n > 3$ satisfies our hypothesis, and we prove that our construction actually produces non-singular curves which violate the local-global principle for at least 90% (if ordered by heights) of the odd degrees $n > 3$. Moreover, for each fixed n, our construction gives infinitely many algebraic curves of degree n which are not geometrically isomorphic to each other. Our construction gives a vast generalization of Fujiwara's quintic curve (1972).

The contents of the first part are based on the joint work [**28**] with Yosuke Shimizu, and the author contributed to the major part including the formulations of the theorems and the details of their proofs.

In the second part of this thesis, for every odd prime number $p > 3$ such that $p \equiv 3 \pmod 4$, we construct a family of non-singular projective surfaces of degrees $n = (p-1)/2$ which violate the local-global principle. In fact, we construct non-singular projective surfaces of both GENERAL odd and even degrees $n \geq 3$ which violate the local-global principle under a certain mild hypothesis that the arithmetic progression $\{1 + nr\}_{r \in \mathbb{N}}$ contains a sufficiently small prime number. Our construction gives a vast generalization of (modified) Swinnerton-Dyer's cubic surface (1962). The contents of the second part is based on [**26**] and its generalization.

Although there is a vast literature on the violation of the local-global principle, there is no known such a uniform construction of non-singular homogeneous forms violating the local-global principle before the results in this thesis.

Acknowledgement

First, the author would like to express his sincere gratitude to his family, especially his parents, for their mental and financial support constantly throughout his life. Without their constant support, any researches by the author cannot be realized. The author would like to thank every member of Bannai Laboratory and every staff of Keio University for her/his support of the research by the author from various directions. Among them, the author would like to express his sincere gratitude to his supervisor Prof. Ken-ichi Bannai for his encouragement of the whole of the graduate research by the author, for reading carefully many drafts of articles including this thesis, and for giving many valuable and suggestive comments in every time. Additionally, the author would like to express his sincere gratitude to Yoshinori Kanamura and Yosuke Shimizu for valuable discussions on the local-global principle, which gave the author a motivation of the whole of the research of this thesis. Finally but not least, the author would like to also thank Prof. Hiroyasu Izeki, Prof. Masato Kurihara, Prof. Takaaki Tanaka, and Dr. Yusuke Tanuma for careful reading of the draft of this thesis and giving many valuable comments. All of their comments were very helpful for the author to improve the contents of this thesis.

Part 0. Introduction

1. The local-global principle

In number theory, rational points on algebraic varieties have been studied by many people from the time of Diophantus of Alexandria. More precise terminologies, it is one of the most classical problems to determine the set of (usually tuples of) rational numbers which satisfy given algebraic equations. In terms of algebraic geometry, this problem is equivalent to determine the set of rational points on given algebraic varieties. In particular, it is important as the first step to determine whether this set is empty or not.

Since the linear equations are trivial objects in this aspect, the first non-trivial objects are quadratic equations, i.e., quadratic hypersurfaces of the projective space $\mathbb{P}^n$. For this class of algebraic varieties, a classical theorem of Minkowski and Hasse is formulated as follows:

Theorem 1.1 (Hasse-Minkowski (cf. [**60**, Theorem 8, Ch. IV])). *Let $X \subset \mathbb{P}^n$ be a quadratic hypersurface. Then, X has a $\mathbb{Q}$-rational point if (and only if) X has a $\mathbb{Q}_v$-rational point for the completion $\mathbb{Q}_v$ of $\mathbb{Q}$ with respect to every finite and infinite place v of $\mathbb{Q}$, namely the field of p-adic numbers $\mathbb{Q}_p$ for every prime number p* [1] *and the field of real numbers $\mathbb{R} = \mathbb{Q}_\infty$.*

This is the so called local-global principle of quadratic hypersurfaces (or quadratic forms). Since Theorem 1.1 is quite strong and useful in the study of the set of rational points on quadratic hypersurfaces, it is natural to study possible generalizations of this property. In this view point, we introduce the following terminology.

Definition 1.2 (local-global principle)**.** Let X be an algebraic variety. Then, we say that **the local-global principle holds for** X if it has a $\mathbb{Q}$-rational point if and only if it has a $\mathbb{Q}_v$-rational point with respect to every finite and infinite place v of $\mathbb{Q}$. Contrarily, we say that X **violates the local-global principle** if the local-global principle does not hold for X.

By using certain analytic methods, for example the Hardy-Littlewood circle method, we can prove that the local-global principle holds if the dimension of an algebraic variety is sufficiently larger than the degree of its defining equation. For instance, the following result was obtained by Browning and Heath-Brown [**11**].

[1] For the basic properties of $\mathbb{Q}_p$, we refer the reader to [**23**, **60**, **61**]. See also §19.

THEOREM 1.3 (a part of [**11**, Theorem 1.1]). *Let $X \subset \mathbb{P}^n$ be a geometrically integral and non-singular variety defined over $\mathbb{Q}$. Then, the local-global principle holds for X whenever*

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

If $X \subset \mathbb{P}^n$ is a hypersurface, i,e., the case $\dim(X) = n - 1$, then the above result had been already obtained by Birch [**5**].

On the other hand, the most natural targets next to quadratic hypersurfaces treated in Theorem 1.1 is cubic hypersurfaces of $\mathbb{P}^n$. If we restrict our attention to them, then we can prove more precise unconditional/conditional results.

THEOREM 1.4 ([**35**, **36**], see also [**29**]). *Let $X \subset \mathbb{P}^n$ be a non-singular cubic hypersurface defined over $\mathbb{Q}$. Then, the local-global principle holds for X whenever*

$$n \geq 8, \ \textit{i.e.,} \ \dim(X) \geq 7.$$

Moreover, under the Riemann hypothesis for certain Hasse-Weil L-functions, the same conclusion holds whenever

$$n \geq 7, \ \textit{i.e.,} \ \dim(X) \geq 6.$$

In [**45**], a similar unconditional result is obtained for non-singular quartic hypersurfaces of dimension larger than or equal to 28. In fact, it is conjectured by several specialists that, more generally, if $d, n \in \mathbb{Z}_{\geq 2}$, $d \leq n$, and $(d, n) \neq (3, 3)$, then the local-global principle holds for every non-singular hypersurface $X \subset \mathbb{P}^n$ of degree d. An explicit reference is [**54**, Conjecture 3.2]. See also [**18**] and [**54**, Remark 3.3 and Appendix A] for the background in view of the Brauer-Manin obstruction.

Besides above deterministic results, there are also many probabilistic or statistical results. Among them, the following conjecture by Poonen and Voloch [**54**] has motivated many researchers. In order to state their conjecture precisely, we introduce some notation.

For every $d, n \in \mathbb{Z}_{\geq 2}$, let $\mathbb{Z}[x_0, \ldots, x_n]_d$ denote the set of homogeneous polynomials of degree d in $\mathbb{Z}[x_0, \ldots, x_n]$. Define the height $h(f)$ of a non-zero polynomial $f \in \mathbb{Z}[x_0, \ldots, x_n]$

as the maximum of the absolute values of its coefficients. For every $H \in \mathbb{R}_{>0}$, set

$$\begin{aligned}
&\mathbb{V}^{\mathrm{tot}}_{d,n}(H) := \{f \in \mathbb{Z}[x_0, \dots, x_n]_d \mid h(f) \leq H\},\\
&\mathbb{V}^{\mathrm{glo}}_{d,n}(H) := \left\{f \in \mathbb{V}^{\mathrm{tot}}_{d,n}(H) \;\middle|\; \exists x \in \mathbb{Q}^{\oplus n+1} \setminus \{0\} \text{ such that } f(x) = 0\right\},\\
&\mathbb{V}^{\mathrm{loc}}_{d,n}(H) := \left\{f \in \mathbb{V}^{\mathrm{tot}}_{d,n}(H) \;\middle|\; \exists x \in \mathbb{Q}_v^{\oplus n+1} \setminus \{0\} \text{ such that } f(x) = 0 \text{ for every place } v\right\},\\
&\rho_{d,n}(H) := \frac{\#\mathbb{V}^{\mathrm{glo}}_{d,n}(H)}{\#\mathbb{V}^{\mathrm{tot}}_{d,n}(H)},\\
&\rho^{\mathrm{loc}}_{d,n}(H) := \frac{\#\mathbb{V}^{\mathrm{loc}}_{d,n}(H)}{\#\mathbb{V}^{\mathrm{tot}}_{d,n}(H)}.
\end{aligned}$$

In this setting, Poonen and Voloch [**54**, Theorem 3.6] showed that $\rho^{\mathrm{loc}}_{d,n}(H) \to c_{d,n}$ for some $c_{d,n} \in \mathbb{R}_{>0}$ whenever $(d, n) \neq (2, 2)$, and they formulated the following conjecture.

Conjecture 1.5 ([**54**, Conjecture 2.2])**.**

(1) *If $d \geq n + 2$, then $\rho_{d,n}(H) \to 0$. In particular, the local-global principle does not hold for 100% of hypersurfaces of $\mathbb{P}^n$ of degree d which have $\mathbb{Q}_v$-rational points for every place v.*

(2) *If $d \leq n$ and $(d, n) \neq (2, 2)$, then $\rho^{\mathrm{loc}}_{d,n}(H) - \rho_{d,n}(H) \to 0$. In particular, the local-global principle holds for 100% of hypersurfaces of $\mathbb{P}^n$ of degree d.*

Recently, Browning, Le Boudec, and Sawin [**12**] succeeded in proving the second part of Conjecture 1.5 under the condition that $(d, n) \neq (3, 3)$. For related results, see a nice survey article [**10**].

On the other hand, the first part of Conjecture 1.5 is based on the long-standing folklore that *most* algebraic varieties (especially of general type) violate the local-global principle. In this thesis, we study this direction by constructing in certain uniform manners non-singular ternary and quaternary forms, i.e., non-singular hypersurfaces of $\mathbb{P}^2$ and $\mathbb{P}^3$ which violate the local-global principle.

2. Violation of the local-global principle in ternary forms

In the Part I of this thesis, we treat ternary forms, i.e., homogeneous polynomials in the ring $\mathbb{Z}[X, Y, Z]$, which violate the local-global principle.

The first example of algebraic variety which violates the local-global principle is the following curves of genus one, which was found first by Lind in his thesis [**42**] and independently by Reichardt [**55**] shortly after that. The expository article [**1**] by Aitken and Lemmermeyer is one of the best introduction papers to the violation of the local-global principle, which also contains some generalizations of the following example by Lind and Reichardt.

THEOREM 2.1 ([**1**, **42**, **55**]). *The weighted homogeneous equation*

$$X^4 - 17Y^4 = 2Z^2,$$

or equivalently the homogeneous equation

$$\begin{cases} X^2 - 17Y^2 = 2Z^2 \\ XY = W^2 \end{cases}$$

defines a non-singular curve over $\mathbb{Q}$ *which violates the local-global principle.*

PROOF. See [**1**]. □

For hypersurface of $\mathbb{P}^n$, the following example by Selmer is the most classical one.

THEOREM 2.2 ([**59**]). *The equation*

$$3X^3 + 4Y^3 + 5Z^5 = 0,$$

or equivalently

$$X^3 + 6Y^3 = 10Z^3$$

defines a non-singular curve of degree 3 *over* $\mathbb{Q}$ *which violates the local-global principle.*

PROOF. See [**59**] or [**19**]. □

By combining these examples in small degrees, we can construct many reducible examples in higher degree case, but the first example of (absolutely) irreducible curves of higher odd degree is given by Fujiwara [**24**] as follows.

THEOREM 2.3 ([**24**, Theorem 2]). *The equation*

$$(X^3 + 5Y^3)(X^2 + XY + Y^2) = 17Z^5$$

defines a non-singular curve of degree 5 *over* $\mathbb{Q}$ *which violates the local-global principle.*

PROOF. See [**24**]. □

For examples in higher degree but with singularities, see [**25**]. After [**24**, **25**], several examples of non-singular curves of degree 4 are discovered. For example, the following equations are known to violate the local-global principle, which were found by Bremner-Lewis-Morton, Schinzel, and Cassels respectively.

Theorem 2.4 ([**9**, II (a)]). *The equation*

$$3X^4 + 4Y^4 = 19Z^4$$

defines a non-singular curve of degree 4 *over* $\mathbb{Q}$ *which violates the local-global principle.*

Proof. See [**9**, II (a)]. □

Theorem 2.5 ([**57**, Theorem 2]). *The equation*

$$X^4 - 2Y^4 - 16Y^2Z^2 - 49Z^4 = 0$$

defines a non-singular curve of degree 4 *over* $\mathbb{Q}$ *which violates the local-global principle.*

Proof. See [**57**, Theorem 2]. □

Theorem 2.6 ([**13**]). *The equation*

$$-158711X^4 + 100Y^4 + 29641Z^4 + 4028X^2Y^2 - 212014X^2Z^2 - 1732Y^2Z^2 = 0$$

defines a non-singular curve of degree 4 *over* $\mathbb{Q}$ *which violates the local-global principle.*

Proof. See [**13**]. □

More recently, Cohen [**16**, Corollary 6.4.11] gave several equations of the form $X^p + bY^p + cZ^p = 0$ of degree $p = 3, 5, 7, 11$ with $b, c \in \mathbb{Z}$ which violate the local-global principle. However, all of examples so far are sporadic, and we need a new idea to obtain infinitely many examples at the same time.

Around the end of the last century, some people have studied infinite families of non-singular plane curves which violate the local-global principle. In [**17**], the existence of such a family of cubic curves was proven, and an explicit example was constructed first by Poonen [**53**].

Theorem 2.7 ([**53**]). *For any* $t \in \mathbb{Q}$*, the equation*

$$5X^3 + 9Y^3 + 10Z^3 + 12\left(\frac{t^2+82}{t^2+22}\right)(X+Y+Z)^3 = 0$$

defines a plane curve $C = C_t$ *of degree* 3 *defined over* $\mathbb{Q}$ *which violates the local-global principle. Moreover, there exists a set of* $t \in \mathbb{Q}$ *which gives infinitely many geometrically non-isomorphic classes of such curves.*

Proof. See [**53**]. □

Motivated by the above result by Poonen, Nguyen obtained many examples in higher genus cases. In particular, by using such examples of hyperelliptic curves, he obtained many plane curves of even degree which violate the local-global principle as follows.

THEOREM 2.8 ([**49**, Theorem 1.1]). *Let p, d, m be integers satisfying the following conditions.*

1. *p be a prime number such that $p \equiv 1 \pmod{16}$.*
2. *$q := d^2 - pm^2$ is a prime number.*
3. *d is a quadratic non-residue in $\mathbb{F}_p^\times$ and $d \equiv 0, \pm 2 \pmod 5$.*
4. *$m \equiv 1 \pmod 2$, $m \equiv 0, \pm 2 \pmod 5$, $m \equiv \pm 3 \pmod{13}$, $m \equiv \pm 3, \pm 6, \pm 7, \pm 8 \pmod{17}$, $m \equiv 0, \pm 1, \pm 2, \pm 3, \pm 7, \pm 9, \pm 13, \pm 14 \pmod{29}$, and $m \not\equiv d \pmod 5$,*

Then, the equation

$$X^4 - pY^4 = q(Y^2 + qZ^2)^2$$

defines a plane curve $C = C_{p,d,m}$ of degree 4 defined over $\mathbb{Q}$ which violates the local-global principle. Moreover, this violation is explained by the Brauer-Manin obstruction.

PROOF. See [**49**]. □

THEOREM 2.9 ([**50**, Theorem 1.4]). *Let $n = 2k$ with $k \geq 1$. Take $p, d, m,$ and α as follows:*

1. *p is a prime number such that $p \equiv 1 \pmod 8$.*
2. *d is an integer which is a quadratic non-residue in $\mathbb{F}_p^\times$ and prime to $2n$.*
3. *m is an even integer such that $q := d^2 + pm^2$ is a prime number.*
4. *α is a rational number such that $\alpha \in \mathbb{Z}_l$ for every prime divisor l of dp and $\alpha \neq 0, qp^{-k}, qd^{-k}, (m(d+p) - 2q)((dp)^k - d^k - p^k)^{-1}$.*

Set $A = q - \alpha p^k$, $B = q - \alpha d^k$, and $C = m(d+p) - 2q - \alpha((dp)^k - d^k - p^k)$. Then, the equation

$$\begin{aligned} pq^2X^{4k+2} + Y^{4k-2}(d(d+p)X^2 - qY^2)(pm^2(d+p)X^2 - dqY^2) \\ - Z^2(AX^{2k} + BY^{2k} + CX^kY^k + \alpha Z^{2k})^2 = 0 \end{aligned}$$

defines a plane curve $C = C_{p,d,m,\alpha}$ of degree $4k+2$ defined over $\mathbb{Q}$ which violates the local-global principle. Moreover, this violation is explained by the Brauer-Manin obstruction.

PROOF. See [**50**]. □

Theorem 2.10 (a special case of [**51**, Theorem 3.1]). *Let $m, n \in \mathbb{Z}_{\geq 1}$ such that $m < n$. Let p be a prime number and $\alpha, \beta \in \mathbb{Z}$. Define a homogeneous polynomial $d(X, Y) \in \mathbb{Z}[X, Y]$ by*

$$d(X,Y) = X^m(p(X+Y))^n - (-Y)^m(p(X+Y)+Y)^n.$$

Suppose that

(1) $p \equiv 1 \pmod 8$.
(2) $\gcd(\alpha\beta, p) = 1$.
(3) *l is a quadratic residue in $\mathbb{F}_p^\times$ for any odd prime divisor of $\alpha d(\alpha, \beta)$.*
(4) *β is a quadratic non-residue in $\mathbb{F}_p^\times$.*
(5) *$n - m \not\equiv 0 \pmod l$ for any odd prime divisor l of $\beta^2 + p(\alpha+\beta)^2$.*

Then, there exists a family of explicit homogeneous polynomials $Q_\zeta = Q_\zeta(X, Y, Z) \in \mathbb{Q}[X, Y, Z]$ of degree $2n-1$ parametrized by a rational number $\zeta \in \mathbb{Q}$ such that the equation

$$Q_\zeta(X,Y,Z)^2 Z^2 = p(\alpha X^{2n} + \beta Y^{2n})^2 + Y^{4n-4m}((p\alpha + (p+1)\beta)X^{2m} - p(\alpha+\beta)Y^{2m})^2$$

defines a plane curve $C = C_{p,\alpha,\beta,\zeta}$ of degree $4n$ defined over $\mathbb{Q}$ which violates the local-global principle. Moreover, this violation is explained by the Brauer-Manin obstruction.

Proof. See [**51**]. □

A remarkable character which the families obtained by Nguyen share is that each member of these families covers a hyperelliptic curve which violates the local-global principle, and the latter violation of the local-global principle is explained by the Brauer-Manin obstruction by a certain Brauer class of degree 2. Note also that the recipe in Theorems 2.8 and 2.9 actually give infinitely many explicit counterexamples of degree 4 and $4k + 2$ for every $k \geq 1$ respectively. On the other hand, Nguyen [**51**] claimed only for $k \neq 1, 2, 4$ that the recipe in Theorem 2.10 actually gives explicit counterexamples of degree $4k$.

On the other hand, Nguyen's method via hyperelliptic curves seems to have a drawback that it gives no non-singular plane curves of odd degree which violate the local-global principle. In this aspect, our first main result of the Part I of this thesis is striking, which gives a UNIFORM construction of non-singular plane curves of ODD degree which violate the local-global principle under a certain condition on the cubic fields $\mathbb{Q}(p^{1/3})$ and $\mathbb{Q}((2p)^{1/3})$ with an odd prime number p. Here, a uniform construction for a specified dimension (now 1-dimension) means an algorithm to obtain a non-singular projective hypersurface of the projective space $\mathbb{P}^N$ (now $N = 2$) of every sufficiently large degree $n \gg 1$ which violates the local-global principle.

Theorem 2.11 (Theorem 4.1, [**28**, Theorem 1.1]). *Let p be an odd prime number. Set $P = p$ or $2p$ so that $P \not\equiv \pm 1 \pmod 9$. Let $\epsilon = \alpha + \beta P^{1/3} + \gamma P^{2/3} \in \mathbb{R}_{>1}$ be the fundamental unit of $\mathbb{Q}(P^{1/3})$ with $\alpha, \beta, \gamma \in \mathbb{Z}$. Set*

$$\iota = \begin{cases} 1 & \textit{except if } \beta \equiv 0 \pmod p \textit{ and } \gamma \not\equiv 0 \pmod p \\ 2 & \textit{if } \beta \equiv 0 \pmod p \textit{ and } \gamma \not\equiv 0 \pmod p \end{cases}.$$

Let $n \in \mathbb{Z}_{\geq 5}$ be an odd integer divisible by p^ι. Then, there exist infinitely many $(n-3)/2$-tuples of pairs of integers (b_j, c_j) $(1 \leq j \leq (n-3)/2)$ satisfying the following condition:

For every j, the integer $P^\iota b_j^3 + c_j^3$ is a prime number congruent to $2 \pmod 3$, and there exist infinitely many integers L such that every prime divisor l of L satisfies $l \equiv 2 \pmod 3$ and the equation

$$(X^3 + P^\iota Y^3) \prod_{j=1}^{\frac{n-3}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = LZ^n \tag{1}$$

define non-singular plane curves of degree n which violate the local-global principle.

Moreover, for each $n \geq 5$ divisible by p^ι, there exists a set of such $(n-3)/2$-tuples $((b_j, c_j))_{1 \leq j \leq (n-3)/2}$ which gives infinitely many geometrically non-isomorphic classes of such curves of degree n.

In view of eq. (1), it is fair to say that our construction in Theorem 2.11 gives a vast generalization of Theorems 2.2 and 2.3. For more detailed properties satisfied by (b_j, c_j) and L, see Proposition 5.1 in §5 and the proof of Theorem 2.11 in §7.

In fact, as claimed before Theorem 2.11, our construction ensures that for every odd degree $n \geq 5$ divisible by p^ι with a prime number p, we have an algorithm to obtain arbitrarily many explicit parameters (b_j, c_j) and L for which eq. (1) define non-singular plane curves which violate the local-global principle. In this sense, we obtain a UNIFORM construction of non-singular plane curves of odd degree $n \geq 5$ which works well under the hyposethis that $\iota = 1$ for every odd prime number p (cf. Theorem 2.7 for $n = 3$). As a consequence of the proof of Theorem 2.11, we can produce as many as we want explicit examples of many odd degrees $n \geq 5$ as explicit examples of degree 3 and 5 obtained by Selmer (cf. Theorem 2.2) and Fujiwara (cf. Theorem 2.3) respectively. For example, we obtain the following new example (cf. §8)

$$(X^3 + 7Y^3)(X^2 + 4XY + 16Y^2)(16X^2 + 4XY + Y^2) = 262193^4 Z^7$$

which defines a non-singular curve of degree 7 which violate the local-global principle. Note also that the proof of the infinitude of the geometric isomorphy classes in Theorem 2.11 is based on the infinitude of prime numbers of the form $P^{\iota}b^3 + c^3$ with $b, c \in \mathbb{Z}$ satisfying some additional conditions, where the latter is a consequence of a theorem of Heath-Brwon and Moroz [**33**] (cf. Theorem 4.4).

Furthermore, we verified numerically the condition $\iota = 1$ for all prime numbers $p < 10^5$ with a help of Magma [**7**] (cf. §23). This numerical verification ensures that, for at least 90% (if ordered by height) of the odd integers $n \geq 5$, there exist infinitely many non-singular plane curves of degree n which are defined by eq. (1) and violate the local-global principle. In fact, we conjecture that $\iota = 1$ for EVERY prime number $p \neq 3$ (and $P = 6$), hence we actually have a UNIFORM construction of non-singular plane curves of EVERY odd degree $n \geq 5$. For more precise Conjecture 4.2 and its background, see §4.

Secondly, we obtain a similar result for non-singular plane curves of even degree. In this case, however, we obtain the following unconditional construction. Note also that Nguyen's construction in Theorems 2.9 and 2.10 have already given many families of non-singular plane curves of degree $4n + 2$ and $4n$ respectively. However, our construction has an advantage that we can treat all even degrees $n \geq 8$ in a uniform manner.

THEOREM 2.12 (Theorem 9.1 (cf. [**27**, Theorem 1.7])). *Let $n \in \mathbb{Z}_{\geq 8}$ be an even integer, and $m \in \mathbb{Z}_{\geq 3}$ be an odd integer such that $m < n$. Then, there exist infinitely many $(n-6)/2$-tuples of pairs of integers (b_j, c_j) $(1 \leq j \leq (n-6)/2)$ satisfying the following condition:*

For every $j \geq 1$, the integer $158^2 b_j^3 + c_j^3$ is a prime number, and there exist infinitely many prime numbers l and infinitely many pairs of integers (b_0, c_0) such that $l \equiv 2 \pmod 3$ and the equation

$$(X^3 + 158^2 Y^3)(b_0 X^3 - l c_0 Y^3) \prod_{j=1}^{(n-6)/2} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = l^m Z^n \tag{2}$$

define non-singular plane curves of degree n which violate the local-global principle.

Moreover, for each even $n \geq 8$, there exists a set of such $(n-4)/2$-tuples $((b_j, c_j))_{0 \leq j \leq (n-6)/2}$ which gives infinitely many geometrically non-isomorphic classes of such curves of degree n.

For more detailed properties satisfied by (b_j, c_j) and l, see Proposition 10.1 in §10 and the proof of Theorem 2.12 in §11.

As its visual suggested, the family in Theorem 2.12 is a variant of the family of Theorem 2.11. In fact, their proofs are quite similar. Moreover, for every even degree $n \geq 8$, we have an algorithm to obtain arbitrarily many explicit parameters (b_j, c_j) and l for which eq. (2) define non-singular plane curves which violate the local-global principle. In this sense, we again obtain a UNIFORM construction of non-singular plane curves of even degree, but in this time our algorithm works unconditionally. As a consequence of the proof of Theorem 2.12, we can produce as many as we want explicit examples of every even degree $n \geq 8$ as the above examples of degree 4 which were obtained by Bremner-Lewis-Morton (cf. Theorem 2.4), Schinzel (cf. Theorem 2.5), and Cassels (cf. Theorem 2.6). For example, we obtain the following new examples (cf. §12)

$$(X^3 + 158^2Y^3)(671X^3 - 7583 \cdot (-47^2) \cdot Y^3)(X^2 + 7XY + 7^2Y^2) = 7583^m Z^8 \quad (m = 3, 5, 7)$$

each of which defines a non-singular plane curve of degree 8 which violates the local-global principle. Note also that the proof of the infinitude of the geometric isomorphy classes in Theorem 2.12 is again based on the infinitude of prime numbers of the form $P^{\iota}b^3 + c^3$ with $b, c \in \mathbb{Z}$ satisfying some additional conditions.

3. Violation of the local-global principle in quaternary forms

In the Part II of this thesis, we treat quaternary forms, i.e., homogeneous polynomials in the ring $\mathbb{Z}[t, x_0, x_1, x_2]$, which violate the local-global principle.

The first example of non-singular algebraic surface which violates the local-global principle was discovered by Swinnerton-Dyer.

Theorem 3.1 ([**62**]). *Let $\theta = \theta_{7,3} = \cos(2\pi/7)$. Then, the equation*

$$t(t + x_0)(2t + x_0) = N_{\mathbb{Q}(\theta)/\mathbb{Q}}(x_0 + \theta x_1 + \theta^2 x_2)$$

defines a non-singular cubic surface over $\mathbb{Q}$ which violates the local-global principle.

Proof. See [**62**]. □

In his paper [**62**], Swinnerton-Dyer said that

> *"I guess that there are plenty of such examples: however, my arguments depends on a series of lucky coincidences and I can find no surfaces other than the one given here for which an argument of this type would work."* [**62**]

After the above examples, many cubic surfaces and more general del Pezzo surfaces have been found to violate the local-global principle. For example, see e.g. [**8**, **14**, **38**, **39**,

46]. Among them, Jahnel [**39**] gave a huge generalization as a certain axiomatization of Theorem 3.1.

THEOREM 3.2 ([**39**, Theorem 1.1]). *Let p be a prime number such that $p \equiv 1 \pmod 3$, $K_{p,3}$ be the unique subfield of $\mathbb{Q}(\zeta_p)$ such that $[K_{p,3} : \mathbb{Q}] = 3$, and $\tau_{p,3} := \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K_{p,3}}(1-\zeta_p)$. For $a_1, a_2, d_1, d_2 \in \mathbb{Z}$, define the cubic surface $S = S_{a_1,a_2,d_1,d_2} \subset \mathbb{P}^3_{\mathbb{Q}}$ by*

$$t(a_1x_0 + d_1t)(a_2x_0 + d_2t) = N_{K_{p,3}/\mathbb{Q}}(t + \tau_{p,3}x_1 + \tau_{p,3}^2 x_2).$$

Let $s_i \in \overline{\mathbb{F}_p}$ be the roots of the polynomial $T(a_1 + d_1T)(a_2 + d_2T) - 1 \in \mathbb{F}_p[T]$. Then, the following hold.

(1) *Suppose that $d_1d_2 \not\equiv 0 \pmod p$ and $\gcd(d_1, d_2) = 1$. If $(a_1 + d_1s_i)/s_i \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 3}$ for every $i = 1, 2, 3$ such that $s_i \in \mathbb{F}_p$, then X has no $\mathbb{Q}$-rational points.*

(2) *Suppose that $d_1d_2 \not\equiv 0 \pmod p$ and that $\gcd(a_1, d_1)$ and $\gcd(a_2, d_2)$ contain only prime divisors that completely split in $K_{p,3}$. Suppose further that $T(a_1+d_1T)(a_2+d_2T) - 1 \in \mathbb{F}_p[T]$ has at least one simple zero in $\mathbb{F}_p$. Then, X has $\mathbb{Q}_v$-rational points for every place.*

However, explicit examples of non-singular surfaces of higher degree, especially those of general type, are poor. In this point of view, we obtain the following results on uniform construction of non-singular surfaces which violate the local-global principle. It is a generalization of the main result of an article [**26**] by the author himself.

In order to state our results, let $N_{K/F} : K \to F$ denotes the norm map for every field extension K/F of finite degree. For every odd prime number p, we fix a primitive p-th root of unity in the field $\mathbb{C}$ of complex numbers and denote it by ζ_p. Moreover, for every integer d such that $p \equiv 1 \pmod d$, $K_{p,d}$ denotes the unique subfield of $\mathbb{Q}(\zeta_p)$ such that $[K_{p,d} : \mathbb{Q}] = d$, and set $\theta_{p,d} = N_{\mathbb{Q}(\zeta_p)/K_{p,d}}(1 - \zeta_p)$.

THEOREM 3.3 (Theorem 13.1 (cf. [**26**, Theorem 1])). *Let $d \in \mathbb{Z}_{\geq 3}$ be an integer. Then, the following statements hold.*

(1) *Suppose that d is odd. If there exists a prime number p such that $p \equiv 1 \pmod d$ and $p < (d + 1)^2$, then there exist infinitely many integers $\beta \in \mathbb{Z}$ and infinitely many homogeneous polynomials $g(t, x_0) \in \mathbb{Z}[t, x_0]$ of degree $k = (d - 1)/2$ such that, for each of them, the equation*

$$tg(t, x_0)(g(t, x_0) + \beta t^k) = N_{K_{p,d}/\mathbb{Q}}(x_0 + \theta_{p,d}x_1 + \theta_{p,d}^2 x_2) \tag{3}$$

defines a non-singular surface of degree d which violates the local-global principle.

(2) *Suppose that d is even. If there exists a prime number p such that $p \equiv 1 \pmod{d}$ and $p < (d/2+1)^2$, then there exist infinitely many integers $\beta \in \mathbb{Z}$ and infinitely many homogeneous polynomials $g(t, x_0) \in \mathbb{Z}[t, x_0]$ of degree $k = d/2$ such that, for each of them, the equation*

$$g(t, x_0)(g(t, x_0) + \beta t^k) = N_{K_{p,d}/\mathbb{Q}}(x_0 + \theta_{p,d}x_1 + \theta_{p,d}^2 x_2) \tag{4}$$

defines a non-singular surface of degree d which violates the local-global principle.

For more detailed properties satisfied by β and $g(t, x_0)$, see Corollaries 16.3 and 16.6 and the proofs of Theorems 17.1 and 17.2.

In fact, our construction ensures that for every degree $d \geq 3$ satisfies the condition in Theorem 3.3, we have an algorithm to obtain arbitrarily many explicit integers β and polynomials $g(t, x_0)$ for which eqs. (3) and (4) define non-singular hypersurfaces of $\mathbb{P}^3$ which violate the local-global principle. In this sense, we obtain a UNIFORM construction of non-singular plane curves of even degree which works well under a hypothesis that the arithmetic progressions $\{1 + dr\}_{r \in \mathbb{N}}$ or $\{1 + (d/2)r\}_{r \in \mathbb{N}}$ contains a prime number p such that $p < (d+1)^2$ or $p < (d/2+1)^2$ according to whether d is odd or even (cf. Remark 3.5). As a consequence of the proof of Theorem 3.3, especially the proofs of Theorems 17.1 and 17.2, we can produce as many as we want explicit examples of many degree $n \geq 3$ as the above Swinnerton-Dyer's cubic surface. For example, we obtain the following new example of degree 4

$$(3N_1t^2 + 5tx + 5x^2)((3N_1 + 1)t^2 + 5tx + 5x^2) = N_{\mathbb{Q}(\zeta_5)/\mathbb{Q}}(x + (1 - \zeta_5)y + (1 - \zeta_5)^2 z)$$

which violates the local-global principle, where N_1 is the product of prime numbers $l < 36$ except for 5. Similarly, we also obtain the following new examples of degree 5

$$t(9N_2t^2+11tx+11x^2)((9N_2+1)t^2+11tx+11x^2) = N_{\mathbb{Q}(\cos(2\pi/11))/\mathbb{Q}}(x+\cos(2\pi/11)y+\cos(2\pi/11)^2 z)$$

which again violates the local-global principle, where N_2 is the product of prime numbers $l < 144$ except for 11.

On the other hand, by applying Theorem 3.3 iteratively, we can prove the existence of non-singular surface which violate the local-global principle for many degrees: For instance, the followings are parts of immediate corollaries of Theorem 3.3. These corollaries show how Theorem 3.3 actually works well unconditionally for many degrees.

Corollary 3.4. *Let p be a prime number.*

(1) *Suppose that $p > 3$. Then, there exist non-singular surfaces of degree $p-1$ which violate the local-global principle.*

(2) *Suppose that $p > 5$. Then, there exist non-singular surfaces of degree $(p-1)/2$ which violate the local-global principle.*

(3) *Suppose that $p > 7$ and $p \equiv 1 \pmod 3$. Then, there exist non-singular surfaces of degree $(p-1)/3$ which violate the local-global principle.*

(4) *Suppose that $p > 9$ and $p \equiv 1 \pmod 4$. Then, there exist non-singular surfaces of degree $(p-1)/4$ which violate the local-global principle.*

Proof of Corollary 3.4. (1) In this case, we have $p = d+1 < (d/2+1)^2$, hence the assertion follows from Theorem 3.3.

(2) In this case, we have $p = 2d+1 < (d+1)^2$, hence the assertion for $p \equiv 3 \pmod 4$ follows from Theorem 3.3. On the other hand, the assertion for $p \equiv 1 \pmod 4$ also follows from Theorem 3.3 because the inequality $2d+1 < (d/2+1)^2$ holds if $d > 4$.

(3) In this case, we have $p = 3d+1$ with even $d \in \mathbb{Z}$. On the other hand, the inequality $3d+1 < (d/2+1)^2$ follows for $d > 8$. Therefore, by Theorem 3.3, it is sufficient to consider the cases $d = 4, 6$. Indeed, the assertions for these cases are the first assertion for $p = 5, 7$, which we have already proven.

(4) In this case, we have $p = 4d+1 < (d+1)^2$ for $d > 2$, hence the assertion for $p \equiv 5 \pmod 8$ follows from Theorem 3.3. On the other hand, the assertion for $p \equiv 1 \pmod 8$ with $p > 49$ also follows from Theorem 3.3 because the inequality $4d+1 < (d/2+1)^2$ holds if $d > 12$. Therefore, it is sufficient to consider the cases $d = 4, 10$. Indeed, the assertions for these cases are the first assertion for $p = 5, 11$, which we have already proven.

□

Remark 3.5. From the above proof of Corollary 3.4, it is natural to expect that we can prove the following statement for every given integer $r \geq 1$ in a similar manner:

"Suppose that $p > 2r+1$ and $p \equiv 1 \pmod r$, i.e., $d := (p-1)/r$ is an integer such that $d > 2$. Then, there exist non-singular surfaces of degree d which violate the local-global principle."

If this is the case, by Dirichlet's theorem on arithmetic progression (cf. Theorem 21.3), we obtain unconditionally non-singular surfaces of degree d which violate the local-global principle for EVERY $d \geq 3$, i.e., we obtain a UNIFORM construction! In fact, as we have seen in the proof of Corollary 3.4, the expected proof works in the case $d \gg r$. However, there is an obstruction in the case where d is small, that is, we need to find sufficiently small p such that $p \equiv 1 \bmod d$. This obstructing assumption is essentially equivalent to the inequalities

$$p < (d+1)^2 \quad \text{and} \quad p < (d/2+1)^2$$

assumed in Theorem 2.12, and we cannot drop these assumptions at least by a technical reason (cf. the proofs of Theorems 17.1 and 17.2). Here, note that, even under the Generalized Riemann Hypothesis for Dirichlet L-functions, it is best possible to deduce the well-known upper bound $p = O(d^{2+\epsilon})$ for the least prime number p in the arithmetic progression $\{1 + dr\}_{r \in \mathbb{N}}$ (cf. [**15**]), but even this conjectural estimate is strictly weaker than the desired inequalities in Theorem 2.12. On the other hand, a stronger estimate $p = O(d^{1+\epsilon})$ based on the prime number theorem with a heuristic argument is widely believed since Chowla's article [**15**]. For more information on these topics, see e.g. [**30**], [**41**], and their references.

Outline of this thesis

In this thesis, we give proofs of Theorems 2.11, 2.12 and 3.3.

In the Part I, we treat non-singular ternary forms which violate the local-global principle. A key ingredient of our construction is prime numbers of the form $q = X^3 + P^\iota Y^3$ where $P = p$ or $2p$ with a prime number p and $\iota = 1$ or 2. The infinitude of such prime numbers is a consequence of the monumental works by Heath-Brown and Moroz [**32**,**33**]. Under the assumption that we have many such prime numbers, we start from an axiomatization of Fujiwara's example in Theorem 2.3 whose proof is based on Fujiwara's original argument in [**24**] and Hensel's lemma. This reduces the problem to the study of primitive integral solutions of the inhomogeneous equations of the form $X^3 + P^\iota Y^3 = l^m Z^{p^\iota}$ with a prime number l and an integer $m \in \mathbb{Z}_{\geq 1}$. After that, we prove that the primitive solutions of these equations satisfy $X \equiv Y \equiv 0 \pmod{l}$ under certain conditions on l, which assures that the above axiomatic construction actually works well. The proof of the last step is a combination of the argument of Fujiwara [**24**] and the analytic estimate of the class number of $\mathbb{Q}(p^{1/3})$ and $\mathbb{Q}((2p)^{1/3})$, where the latter we also use a part of the cubic analogue of Gauss' genus theory.

In the Part II, we treat non-singular quaternary forms which violate the local-global principle. We start from investigations of the condition for which our hypersurfaces are non-singular. After that, we study local solubility and global unsolubility under certain technical conditions. The proofs in these steps are based on Swinnerton-Dyer's original proof of Theorem 3.1 given in [**62**], the Hasse-Weil bound on the number of rational points on a non-singular projective curve defined over the finite field $\mathbb{F}_q$ with a prime number q, and consideration on certain exponential equations modulo p. The last one is a new contribution of this thesis and may be interesting itself. In the last section, we reduce these technical conditions to the estimate of the size of a prime number in the given arithmetic progression given by the congruent condition $\equiv 1 \pmod{n}$.

Notation

The following notation is used in the whole of this thesis.

Let $\mathbb{Z}$ be the ring of integers and $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ be the fields of rational numbers, real numbers, and complex numbers respectively. For every prime number l, $\mathbb{Q}_l$ denotes the field of l-adic numbers and $v_l : \mathbb{Q}_l^\times \to \mathbb{Z}$ be the additive l-adic valuation map normalized so that $v_l(l) = 1$. $v_l(1) = 0$, and $v_l(0) = +\infty$.

For every commutative ring R, $R^\times$ denotes the group of invertible elements.

Part I

Construction of ternary forms which violate the local-global principle

In the Part I, we exhibit how to construct non-singular plane curves which violate the local-global principle in a uniform manner both in odd and even degree cases.

In §§4–7, we prove Theorem 2.11 (Theorem 4.1). After that, we give a concrete example of degree 7 in §8.

In the sections 9–11, we prove Theorem 2.12 (Theorem 9.1). After that, we give a concrete example of degree 8 in §12.

4. Main theorem in odd degree case and conjecture

The goal of §§4–7 is to prove the following Theorem 4.1. We should emphasize that although it is unclear from the statement, our proof of Theorem 4.1 ensures that for every odd degree $n \geq 5$ divisible by p^ι with a prime number p, we have an algorithm to obtain arbitrarily many explicit parameters (b_j, c_j) and L for which eq. (5) define non-singular plane curves which violate the local-global principle. For detailed properties satisfied by (b_j, c_j) and L, see Proposition 5.1 in §5 and the proof of Theorem 4.1 in §7. Note also that the proof of the infinitude of the geometric isomorphy classes in Theorem 2.11 is based on the infinitude of prime numbers of the form $P^\iota b^3 + c^3$ with $b, c \in \mathbb{Z}$ satisfying some additional conditions (cf. Theorem 4.4, Proposition 5.1, and Lemma 7.1).

Theorem 4.1 (= [**28**, Theorem 1.1]). *Let p be an odd prime number. Set $P = p$ or $2p$ so that $P \not\equiv \pm 1 \pmod 9$. Let $\epsilon = \alpha + \beta P^{1/3} + \gamma P^{2/3} \in \mathbb{R}_{>1}$ be the fundamental unit of $\mathbb{Q}(P^{1/3})$ with $\alpha, \beta, \gamma \in \mathbb{Z}$. Set*

$$\iota = \begin{cases} 1 & \textit{except if } \beta \equiv 0 \pmod p \textit{ and } \gamma \not\equiv 0 \pmod p \\ 2 & \textit{if } \beta \equiv 0 \pmod p \textit{ and } \gamma \not\equiv 0 \pmod p \end{cases}.$$

Let $n \in \mathbb{Z}_{\geq 5}$ be an odd integer divisible by p^ι. Then, there exist infinitely many $(n-3)/2$-tuples of pairs of integers (b_j, c_j) $(1 \leq j \leq (n-3)/2)$ satisfying the following condition:

For every j, the integer $P^\iota b_j^3 + c_j^3$ is a prime number congruent to $2 \pmod 3$, and there exist infinitely many integers L such that every prime divisor l of L satisfies $l \equiv 2 \pmod 3$ and the equation

$$(X^3 + P^\iota Y^3) \prod_{j=1}^{\frac{n-3}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = LZ^n \tag{5}$$

define non-singular plane curves of degree n which violate the local-global principle.

Moreover, for each $n \geq 5$ divisible by p^{ι}, there exists a set of such $(n-3)/2$-tuples $((b_j, c_j))_{1 \leq j \leq (n-3)/2}$ which gives infinitely many geometrically non-isomorphic classes of such curves of degree n.

As a consequence of the proof of Theorem 4.1, we can produce as many as we want explicit examples of many odd degrees $n \geq 5$ as Selmer's example (cf. Theorem 2.2)

$$X^3 + 6Y^3 = 10Z^3$$

and Fujiwara's example (cf. Theorem 2.3)

$$(X^3 + 5Y^3)(X^2 + XY + Y^2) = 17Z^5.$$

For example, we obtain the following new example (cf. §8)

$$(X^3 + 7Y^3)(X^2 + 4XY + 16Y^2)(16X^2 + 4XY + Y^2) = 262193^4 Z^7$$

which defines a non-singular curve of degree 7 which violate the local-global principle.

Here, note that since we assume that $P \not\equiv \pm 1 \pmod 9$ in Theorem 4.1, the ring of integers of $K = \mathbb{Q}(P^{1/3})$ coincides with $\mathbb{Z}[\pi]$. Hence, we see that $\alpha, \beta, \gamma \in \mathbb{Z}$ (cf. Conjecture 4.2).

For example, if $p = 3$, then we take $P = 6$. In this case, since $\epsilon = 109 + 60 \cdot 6^{1/3} + 33 \cdot 6^{2/3}$, we see that $\iota = 1$. Therefore, Theorem 4.1 implies that, for every odd $n \equiv 0 \pmod 3$ satisfying $n \geq 9$, there exist infinitely many plane curves of degree n which violate the local-global principle. This is a vast generalization of the case of cubic curves which was established by Selmer (cf. Theorem 2.2).

Another example is the case of $p = 5$. Then, we take $P = 5$. In this case, since $\epsilon = 41 + 24 \cdot 5^{1/3} + 14 \cdot 5^{2/3}$, we see that $\iota = 1$. Therefore, Theorem 4.1 implies that, for every odd $n \equiv 0 \pmod 5$ satisfying $n \geq 5$, there exist infinitely many plane curves of degree n which violate the local-global principle. This is a vast generalization of the case of quintic curves which was established by Fujiwara (cf. Theorem 2.3).

More generally, if $\beta \not\equiv 0 \pmod p$ for an odd prime number $p \geq 5$, then we can produce infinite family of explicit counterexamples for every odd degree $n \equiv 0 \pmod p$. The authors conjecture that this hypothesis is always true whenever $p \neq 3$: [2]

[2] Note that Conjecture 4.2 holds if and only if $\mathbb{Q}(P^{1/3})$ has a unit $\alpha_0 + \beta_0 P^{1/3} + \gamma_0 P^{2/3}$ with $\alpha_0, \beta_0, \gamma_0 \in (1/3)\mathbb{Z}$ such that $\beta_0 \not\equiv 0 \pmod p$. The authors verified Conjecture 4.2 for all $p < 10^5$ by Magma [**7**]. For the detail, see Appendix B.

Conjecture 4.2. *Let $p \neq 3$ be a prime number, $P = p$ or $2p$, and $\epsilon = \alpha + \beta p^{1/3} + \gamma p^{2/3} \in \mathbb{R}_{>1}$ be the fundamental unit of $\mathbb{Q}(P^{1/3})$ with $\alpha, \beta, \gamma \in (1/3)\mathbb{Z}$. Then, we have $\beta \not\equiv 0 \pmod{p}$.*

In fact, Conjecture 4.2 is a natural cubic field analogue of the following more classical conjecture for the real quadratic field $\mathbb{Q}(p^{1/2})$, [3] whose origin goes back to Ankeny-Artin-Chowla [**2**] for $p \equiv 1 \pmod 4$ and Mordell [**47**] for $p \equiv 3 \pmod 4$ respectively:

Conjecture 4.3. *Let $p \neq 2$ be a prime number, and $\epsilon = \alpha + \beta p^{1/2} \in \mathbb{R}_{>1}$ be the fundamental unit of $\mathbb{Q}(p^{1/2})$ with $\alpha, \beta \in (1/2)\mathbb{Z}$. Then, we have $\beta \not\equiv 0 \pmod{p}$.*

A key ingredient of our construction is the following theorem on the distribution of prime numbers represented by binary cubic polynomials:

Theorem 4.4 ([**33**, Theorem 1]). *Let $f_0 \in \mathbb{Z}[X, Y]$ be an irreducible binary cubic form, $\rho \in \mathbb{Z}$, $(\gamma_1, \gamma_2) \in \mathbb{Z}^{\oplus 2}$, and γ_0 be the greatest common divisor of the coefficients of $f_0(\rho x + \gamma_1, \rho y + \gamma_2)$. Set $f(x, y) := \gamma_0^{-1} f_0(\rho x + \gamma_1, \rho y + \gamma_2)$. Suppose that $\gcd(f(\mathbb{Z}^{\oplus 2})) = 1$. Then, the set $f(\mathbb{Z}^{\oplus 2})$ contains infinitely many prime numbers.*

In §5, we give a recipe which exhibits how to construct counterexamples to the local-global principle as in eq. (5) from certain Fermat type equations and prime numbers. These objects are constructed in completely explicit manners via Theorem 4.4 in §6 and §7 respectively. In §7, the proofs of Theorem 4.1 is done by combining these arithmetic objects with a geometric argument (Lemma 7.1) on the non-isomorphy of complex algebraic curves defined by eq. (5). It should be emphasized that the infinitude in Theorem 4.1 is a striking advantage of our construction based on analytic number theory and complex algebraic geometry, which is contrast to those based on algebraic and computational tools in e.g. [**16, 24, 25**]. In §8, we demonstrate how our construction works for each given degree by exhibiting a concrete example of degree 7. [4]

It is fair to say that thanks to Theorem 4.4 (and Lemma 6.4), which is one of the culminations of highly sophisticated modern analytic number theory, our proof of Theorem 4.1 is relatively elementary and almost covered by a standard first course of algebraic number theory (as in e.g. [**16**, Part I], [**34**, Ch. I – Ch. V], [**44**, Ch. I – Ch. V], and [**56**]). Moreover, after one admits Theorem 4.1, it is quite easy to produce as many as we want explicit counterexamples to the local-global principle.

[3] For numerical verification of Conjecture 4.3, see e.g. [**64, 65**].

[4] For more examples, see [**28**, §5].

Remark 4.5. Recently, the author [**27**, Theorem 1.8] succeeded in generalizing Theorem 4.1 to the case where the degree n is divisible by p but not necessarily by p^2. As a consequence, we are released from the mysterious Conjecture 4.2, and we obtain an unconditional algorithm to produce infinitely many counterexamples to the local-global principle for non-singular plane curves of every odd degree $n \geq 5$.

Notation for §§4–8

For every prime number p, P denotes p or $2p$ and $\iota = 1$ or 2. In §5, the choice of P and ι is arbitrary. However, in §6, the choice is restricted so that $P \not\equiv \pm 1 \pmod 9$. For the detail, see the top of each section.

We say that a triple $(x, y, z) \in \mathbb{Z}^{\oplus 3}$ is primitive if $\gcd(x, y, z) = 1$.

5. Construction from prime numbers and Fermat type equations

Let p be an odd prime number, $P = p$ or $2p$, and $\iota = 1$ or 2. Here, we can take P and ι independently of p. In this section, we prove the following proposition, which gives explicit counterexamples to the local-global principle of degree n under the assumption that we have

- sufficiently many prime numbers of the form $P^\iota b^3 + c^3$ with $b, c \in \mathbb{Z}$ and
- integers L such that the equation $x^3 + P^\iota y^3 = Lz^n$ has a specific property.

Proposition 5.1 (Recipe for odd degrees)**.** *Let $n \in \mathbb{Z}_{\geq 5}$ be an odd integer, p be a prime number, $P = p$ or $2p$, $\iota = 1$ or 2, and $b_1, \ldots, b_{(n-3)/2}, c_1, \ldots, c_{(n-3)/2}, L \in \mathbb{Z}$ satisfying the following conditions:*

(1) *For every j, the integer $P^\iota b_j^3 + c_j^3$ is a prime number such that $P^\iota b_j^3 + c_j^3 \equiv 2 \pmod 3$.*

(2) *For every prime divisor l of L, we have $l \equiv 2 \pmod 3$, $v_l(L) < n$, and $\gcd(l, b_j c_j) = 1$ for every j.*

(3) *If $P \equiv 0 \pmod 2$, then $L \equiv \prod_j b_j^2 \equiv 1 \pmod 2$.*

(4) *If $P \not\equiv \pm 1 \pmod 9$, then $L \equiv \prod_j b_j^2 \not\equiv 0 \pmod 3$ and $\sum_j b_j^{-1} c_j \not\equiv 0 \pmod 3$.*

(5) *If $p \equiv 2 \pmod 3$, then $L \equiv \prod_j b_j^2 \not\equiv 0 \pmod p$ and $\sum_j b_j^{-1} c_j \not\equiv 0 \pmod p$.*

(6) *For every primitive triple $(x, y, z) \in \mathbb{Z}^{\oplus 3}$ satisfying $x^3 + P^\iota y^3 = Lz^n$, there exists a prime divisor l of L such that $x \equiv y \equiv 0 \pmod l$.*

Then, the equation

$$(X^3 + P^\iota Y^3)\prod_{j=1}^{\frac{n-3}{2}}(b_j^2X^2 + b_jc_jXY + c_j^2Y^2) = LZ^n$$

violates the local-global principle.

This is a consequence of the following two lemmas.

Lemma 5.2 (local solubility for odd degrees)**.** *Let $n \in \mathbb{Z}_{\geq 5}$ be an odd integer, p be a prime number, $P = p$ or $2p$, $\iota = 1$ or 2, and $b_1, \ldots, b_{(n-3)/2}, c_1, \ldots, c_{(n-3)/2}, L \in \mathbb{Z}$ satisfying the following conditions:*

(1) *If $P \equiv 0 \pmod 2$, then $L \equiv \prod_j b_j^2 \equiv 1 \pmod 2$.*
(2) *If $P \not\equiv \pm 1 \pmod 9$, $L \equiv \prod_j b_j^2 \not\equiv 0 \pmod 3$ and $\sum_j b_j^{-1}c_j \not\equiv 0 \pmod 3$.*
(3) *If $p \equiv 2 \pmod 3$, $L \equiv \prod_j b_j^2 \not\equiv 0 \pmod p$ and $\sum_j b_j^{-1}c_j \not\equiv 0 \pmod p$.*

Then, the equation

$$F(X,Y,Z) := (X^3 + P^\iota Y^3)\prod_{j=1}^{\frac{n-3}{2}}(b_j^2X^2 + b_jc_jXY + c_j^2Y^2) - LZ^n = 0$$

has non-trivial solutions over $\mathbb{R}$ and $\mathbb{Q}_l$ for every prime number l.

Proof. By Fujiwara's argument (cf. Proposition 22.4), it is sufficient to consider the solubility over $\mathbb{Q}_l$ for $l = 2, 3, p$.

(1) If $P \equiv 1 \pmod 2$, then $X^3 + P^\iota Y^3$ is decomposed in $\mathbb{Z}_2[X,Y]$. On the other hand, if $P \equiv 0 \pmod 2$, then since $F(1,0,1) \equiv \prod_j b_j^2 - L \equiv 0 \pmod 2$, and $(\partial F/\partial Z)(1,0,1) = nL \not\equiv 0 \pmod 2$, we obtain a 2-adic lift of mod 2 solution $(1,0,1)$ by Hensel's lemma.
(2) If $P \equiv \pm 1 \pmod 9$, then $X^3 + P^\iota Y^3$ is decomposed in $\mathbb{Z}_3[X,Y]$. On the other hand, if $P \not\equiv \pm 1 \pmod 9$, then since $F(1,0,1) \equiv \prod_j b_j^2 - L \equiv 0 \pmod 3$, and $(\partial F/\partial Y)(1,0,1) \equiv (\prod_j b_j^2) \cdot (\sum_j b_j^{-1}c_j) \not\equiv 0 \pmod 3$, we obtain a 3-adic lift of mod 3 solution $(1,0,1)$ by Hensel's lemma.
(3) If $p \equiv 1 \pmod 3$, then $b_j^2X^2 + b_jc_jXY + c_j^2Y^2$ is decomposed in $\mathbb{Z}_p[X,Y]$. On the other hand, if $p \equiv 2 \pmod 3$, then since $F(1,0,1) \equiv \prod_j b_j^2 - L \equiv 0 \pmod p$ and $(\partial F/\partial Y)(1,0,1) \equiv (\prod_j b_j^2) \cdot (\sum_j b_j^{-1}c_j) \not\equiv 0 \pmod p$, we obtain a p-adic lift of mod p solution $(1,0,1)$ by Hensel's lemma.

This completes the proof. □

Lemma 5.3 (global unsolubility for odd degrees)**.** *Let $n \in \mathbb{Z}_{\geq 3}$ be an odd integer, and a, $b_1, \ldots, b_{(n-3)/2}$, $c_1, \ldots, c_{(n-3)/2}$, $L \in \mathbb{Z}$ satisfying the following conditions:*

(1) *For every j, the integer $ab_j^3 + c_j^3$ is a prime number such that $ab_j^3 + c_j^3 \equiv 2 \pmod 3$ and $\gcd(a, c_j) = 1$.*

(2) *For every prime divisor l of L, we have $l \equiv 2 \pmod 3$, $v_l(L) < n$, and $\gcd(l, b_j c_j) = 1$ for every j.*

(3) *For every primitive triple $(x, y, z) \in \mathbb{Z}^{\oplus 3} \setminus \{(0,0,0)\}$ satisfying $x^3 + ay^3 = Lz^n$, there exists a prime divisor l of L such that $x \equiv y \equiv 0 \pmod l$.*

Then, there is no triple $(X, Y, Z) \in \mathbb{Z}^{\oplus 3}$ satisfying

$$(X^3 + aY^3) \prod_{j=1}^{\frac{n-3}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = LZ^n. \tag{6}$$

Proof. We prove the assertion by contradiction. Let $(X, Y, Z) \in \mathbb{Z}^{\oplus 3}$ be a triple satisfying eq. (6). We may assume that it is primitive. It is sufficient to deduce that

$$\gcd((X^3 + aY^3)L, b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = 1 \quad \text{for every } j. \tag{7}$$

Indeed, if eq. (7) holds, then we have some divisor z of Z satisfying $X^3 + aY^3 = Lz^n$. Hence, the fourth assumption implies that $X \equiv Y \equiv 0 \pmod l$ for some prime divisor l of L. However, since $v_l(L) < n$, we have $Z \equiv 0 \pmod l$, which contradicts that $\gcd(X, Y, Z) = 1$. In what follows, we deduce eq. (7).

First, suppose that a prime divisor q of $X^3 + aY^3$ divides $b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2$ for some j. Then, q divides

$$b_j^3(X^3 + aY^3) - (b_j X - c_j Y)(b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = (ab_j^3 + c_j^3)Y^3.$$

Since $\gcd(X, Y, Z) = 1$ and $v_q(L) < n$, we see that $Y \not\equiv 0 \pmod q$. Hence, by the first assumption, we have $q = ab_j^3 + c_j^3 \equiv 2 \pmod 3$. In particular, the polynomial $b_j^2 T^2 + b_j c_j T + c_j^2$ is irreducible in $\mathbb{Z}_q[T]$. Since $b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2 \equiv 0 \pmod q$ and $Y \not\equiv 0 \pmod q$, we have $c_j \equiv 0 \pmod q$. However, $q = ab_j^3 + c_j^3$ implies that a must be divisible by q, a contradiction.

Secondly, suppose that a prime divisor $l \equiv 2 \pmod 3$ of L divides $b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2$ for some j. Then, since $T^2 + T + 1$ is irreducible in $\mathbb{F}_l[T]$, we have $b_j X \equiv c_j Y \equiv 0 \pmod l$. On the other hand, since $\gcd(X, Y, Z) = 1$ and $v_l(L) < n$, we see that $X \not\equiv 0 \pmod l$ or $Y \not\equiv 0 \pmod l$. However, if $X \not\equiv 0 \pmod l$ (resp. $Y \not\equiv 0 \pmod l$), then $b_j \equiv 0 \pmod l$ (resp. $c_j \equiv 0 \pmod l$), which contradicts that $\gcd(L, b_j c_j) = 1$.

This completes the proof. □

6. Fermat type equations of the form $X^3 + P^\iota Y^3 = LZ^{p^\iota}$

In this section, we take an odd prime number p and $P = 2p$ or p so that $P \not\equiv \pm 1 \pmod 9$. We fix them through the whole of this section. Let $\pi = P^{1/3} \in \mathbb{R}$ be the real cubic root of P, $K = \mathbb{Q}(\pi) \subset \mathbb{R}$, and $\mathcal{O}_K$ denotes the ring of integers in K. Since $P \not\equiv \pm 1 \pmod 9$, we see that $\mathcal{O}_K = \mathbb{Z}[\pi]$. Let $\epsilon = \alpha + \beta\pi + \gamma\pi^2 > 1$ be the fundamental unit of K with $\alpha, \beta, \gamma \in \mathbb{Z}$. Note that the Galois closure of K in $\mathbb{C}$ is $K(\zeta_3)$, where $\zeta_3 \in \mathbb{C}$ is a fixed primitive cubic root of unity. For basic properties of these objects, see §22 (cf. [**3**], [**22**], and their references).

Set

$$\iota = \begin{cases} 1 & \text{if } \beta \not\equiv 0 \pmod p \text{ or } \beta \equiv \gamma \equiv 0 \pmod p \\ 2 & \text{otherwise} \end{cases}.$$

For example, if $P = 3$ or 6, then we have $(\alpha, \beta, \gamma) = (4, 3, 2)$ or $(109, 60, 33)$, hence $\iota = 2$ or 1 respectively. On the other hand, if Conjecture 4.2 holds for $p \geq 5$, then we have $\iota = 1$ for $P = p$ and $2p$.

In this section, we prove the following theorem.

THEOREM 6.1. *Let p be an odd prime number. Then, there exist infinitely many prime numbers l and a positive even integer $m < p$ satisfying the following conditions:*

(1) $l \equiv 2 \pmod 3$.
(2) $l^m \equiv 1 \pmod p$.
(3) *Every primitive solution of* $x^3 + P^\iota y^3 = l^m z^{p^\iota}$ *satisfies* $x \equiv y \equiv 0 \pmod l$.

In order to prove Theorem 6.1, we use Theorem 4.4. Suppose that $p \neq 3$. Let $h(A, C) = (3P^\iota A + 1)^3 + P^{2\iota}(3P^\iota C + 1)^3$. Then, since $\gcd(f(\mathbb{Z}^{\oplus 2})) = 1$, [5] Theorem 4.4 implies that there exist infinitely many prime numbers l of the form

$$l = a^3 + P^{2\iota}c^3 \quad \text{with} \quad (a, c) = (3P^\iota A + 1, 3P^\iota C + 1) \in \mathbb{Z}^{\oplus 2}.$$

[5] Note that

$$\begin{aligned} \gcd(h(0,0), h(1,0), h(-1,0)) &= \gcd(1 + P^{2\iota}, 27P^{3\iota} + 28P^{2\iota} + 9P^\iota + 1, -27P^{3\iota} + 28P^{2\iota} - 9P^\iota + 1) \\ &= \gcd(1 + P^{2\iota}, -18P^\iota - 27, 18P^\iota - 27) = \gcd(4 + 4P^{2\iota}, 2P^\iota + 3, 2P^\iota - 3) \\ &= \gcd(13, 6) = 1. \end{aligned}$$

On the other hand, if $p = 3$, we can use $h(A, C) = (3A-1)^3 + P^{2\iota}(3C+1)^3$. [6] Thus, Theorem 6.1 is reduced to the following proposition.

Proposition 6.2. *Let p be an odd prime number and $l \equiv 2 \pmod 3$ be a prime number prime to P. Suppose that there exist $a, b, c \in \mathbb{Z}$ satisfying the following conditions:*

(1) *$l = a^3 + P^\iota b^3 + P^{2\iota}c^3 - 3P^\iota abc$.*

(2) *$a \equiv \pm 1 \pmod p$, $b \equiv 0 \pmod p$, and $c \not\equiv 0 \pmod p$.*

(3) *If $p = 5$, then additionally $c \not\equiv -a \pmod 5$.*

(4) *If $P = 3$, then additionally $c \equiv -a \pmod 3$.*

Then, there exists a positive even integer $m < p$ such that every primitive solution of $x^3 + P^\iota y^3 = l^m z^{p^\iota}$ satisfies $x \equiv y \equiv 0 \pmod l$.

First, we prove the following proposition as an intermediate step.

Proposition 6.3. *Let p be a prime number, l be a prime number such that l is prime to P and $l \equiv 2 \pmod 3$, and $m \in \mathbb{Z}_{\geq 1}$. Assume that there exist $a + b\pi^\iota + c\pi^{2\iota} \in \mathcal{O}_K$ with $a, b, c \in \mathbb{Z}$ satisfying the following conditions:*

(1) *$l = a^3 + b^3 P^\iota + c^3 P^{2\iota} - 3abcP^\iota$.* [7]

(2) *If we define $A_k, B_k, C_k \in \mathbb{Z}$ by*

$$A_k + B_k\pi^\iota + C_k\pi^{2\iota} = \epsilon^k(a + b\pi^\iota + c\pi^{2\iota})^m \quad (k \in \mathbb{Z}),$$

then we have $C_k \not\equiv 0 \pmod p$ for every $k \in \mathbb{Z}$.

Then, every primitive solution of $x^3 + P^\iota y^3 = l^m z^{p^\iota}$ satisfies $x \equiv y \equiv 0 \pmod l$.

We prove Proposition 6.3 along a classical idea as given in [**24**], where Fujiwara proved that the Fermat type equation $x^3 + 5y^3 = 17z^5$ has no primitive solutions. We use the following lemma.

Lemma 6.4 (Lemma 22.5)**.** *Let p be a prime number.*

(1) *The class number of $K = \mathbb{Q}(p^{1/3})$ is smaller than p.*

(2) *The class number of $K = \mathbb{Q}((2p)^{1/3})$ is prime to p.*

For the proof, see Lemma 22.5 in Appendix A.

[6] Note that

$$\gcd(h(0,0), h(1,0)) = \gcd(-1 + P^{2\iota}, 8 + P^{2\iota}) = \gcd(-1 + P^{2\iota}, 9) = 1.$$

[7] Since $l \equiv 2 \pmod 3$, $\mathcal{O}_K$ has prime ideals $\mathfrak{p}_l$ and $\mathfrak{p}_{l^2}$ of norms of degree 1 and 2 respectively. Therefore, the first condition holds (up to signature) if and only if $\mathfrak{p}_l$ is generated by $a + b\pi + c\pi^2$.

Proof of Proposition 6.3. We prove the assertion by contradiction. Suppose that there exists a primitive triple $(x, y, z) \in \mathbb{Z}^{\oplus 3}$ such that $x^3 + P^\iota y^3 = l^m z^{p^\iota}$, and either x or y is prime to l.

First, note that since either x or y is prime to l and $\gcd(l, 3P) = 1$, $x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ cannot be divisible by l. Moreover, $l \equiv 2 \pmod 3$ splits to the product of two prime ideals $\mathfrak{p}_l$ and $\mathfrak{p}_{l^2}$ of degree 1 and 2 respectively. Suppose that $x + y\pi^\iota$ is divisible by $\mathfrak{p}_{l^2}$. Then, the product of its conjugates $(x + \zeta_3 y\pi^\iota)(x + \zeta_3^2 y\pi^\iota) = x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ is divisible by l, a contradiction (cf. the following argument for $q \equiv 2 \pmod 3$). Therefore, $x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ is divisible by $\mathfrak{p}_{l^2}^m$ but not divisible by $\mathfrak{p}_l$. Accordingly, $x + y\pi^\iota$ is divisible by $\mathfrak{p}_l^m$ but not divisible by $\mathfrak{p}_{l^2}$.

Next, suppose that $x + y\pi^\iota$ is divisible by a prime ideal above a prime divisor q of z. Then, since (x, y, z) is primitive, neither $x + y\pi^\iota$ nor $x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ is divisible by q itself. Therefore, by the definition of $P \not\equiv \pm 1 \pmod 9$, the possible decomposition types of q in K are as follows:

(1) $(q) = \mathfrak{p}_{q,1}\mathfrak{p}_{q,2}\mathfrak{p}_{q,3}$, i.e., $q \equiv 1 \pmod 3$ and $P \pmod q \in \mathbb{F}_q^{\times 3}$

(2) $(q) = \mathfrak{p}_q\mathfrak{p}_{q^2}$, i.e., $q \equiv 2 \pmod 3$ and $P \not\equiv 0 \pmod q$

(3) $(q) = \mathfrak{p}_q^3$, i.e., $P \equiv 0 \pmod q$, or $q = 3$ and $P \not\equiv \pm 1 \pmod 9$.

In each case, we have the following conclusion:

(1) If $x + y\pi^\iota$ is divisible by distinct two prime ideals above q, say $\mathfrak{p}_{q,1}$ and $\mathfrak{p}_{q,2}$, then $x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ is divisible by $(\mathfrak{p}_{q,1}\mathfrak{p}_{q,3}) \cdot (\mathfrak{p}_{q,2}\mathfrak{p}_{q,3})$, hence by q, a contradiction. Therefore, $x + y\pi^\iota$ is divisible by $\mathfrak{p}_{q,1}^{p^\iota v_q(z)}$ but not by $\mathfrak{p}_{q,2}$ nor $\mathfrak{p}_{q,3}$ if we replace $\mathfrak{p}_{q,1}, \mathfrak{p}_{q,2}, \mathfrak{p}_{q,3}$ to each other if necessary.

(2) In this case, q is decomposed in $K(\zeta_3)$ so that $\mathfrak{p}_q = \mathfrak{P}_{q^2,1}$ and $\mathfrak{p}_{q^2} = \mathfrak{P}_{q^2,2}\mathfrak{P}_{q^2,3}$. If $x + y\pi^\iota$ is divisible by $\mathfrak{p}_{q^2}$, then $x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ is divisible by $(\mathfrak{P}_{q^2,1}\mathfrak{P}_{q^2,2}) \cdot (\mathfrak{P}_{q^2,1}\mathfrak{P}_{q^2,3})$, hence by q, a contradiction. Therefore, $x + y\pi^\iota$ is divisible by $\mathfrak{p}_q^{p^\iota v_q(z)}$ but not by $\mathfrak{p}_{q^2}$.

(3) In this case, since $x^3 + P^\iota y^3$ is divisible by $\mathfrak{p}_q^{3p^\iota}$, $x + y\pi^\iota$ is divisible by $\mathfrak{p}_q^{p^\iota}$. Since $p^\iota \geq 3$, and π^ι cannot be divisible by q, both x and y are divisible by q. It contradicts that (x, y, z) is primitive.

As a consequence, we see that there exists an integral ideal $\mathfrak{w}$ of $\mathcal{O}_K$ such that

$$(x + y\pi^\iota) = \mathfrak{p}_l^m \mathfrak{w}^{p^\iota} \quad \text{and} \quad (p, \mathfrak{w}) = 1.$$

Since the first assumption implies that $\mathfrak{p}_l$ is generated by $a + b\pi^\iota + c\pi^{2\iota}$, $\mathfrak{w}^{p^\iota}$ is a principal ideal. Moreover, Lemma 6.4 implies that $\mathfrak{w}$ is also generated by a single element $w_0 +$

$w_1\pi + w_2\pi^2 \in \mathcal{O}_K$ with $w_0, w_1, w_2 \in \mathbb{Z}$. [8] Therefore, there exists $k \in \mathbb{Z}$ such that

$$x + y\pi^\iota = \epsilon^k(a + b\pi^\iota + c\pi^{2\iota})^m(w_0 + w_1\pi + w_2\pi^2)^{p^\iota}.$$

Hence, by applying Lemma 11.3 and the definition of A_k, B_k, C_k, we have

$$x + y\pi^\iota \equiv A_k w_0 + B_k w_0 \pi^\iota + C_k w_0 \pi^{2\iota} \pmod{\pi^{2\iota+1}}.$$

In particular, we have $C_k w_0 \equiv 0 \pmod p$. On the other hand, since $(p, \mathfrak{w}) = 1$, we have $w_0 \not\equiv 0 \pmod p$. Therefore, $C_k \equiv 0 \pmod p$ for some k, which contradicts the assumption. This completes the proof for odd p. □

Now, we can prove Proposition 6.2. In what follows, suppose that p is odd. Set

$$\rho(X, Y, Z) := Y/2X - Z/Y \in \mathbb{Q}(X, Y, Z)$$

and

$$\delta(X, Z) := \begin{cases} \rho(\alpha, \beta, \gamma)^2 - 2Z/X & \text{if } \beta \not\equiv 0 \pmod p \\ \rho(\alpha, \gamma, p^{-1}\beta)^2 - 2Z/X & \text{if } \beta \equiv 0 \pmod p \text{ and } \gamma \not\equiv 0 \pmod p \end{cases}$$
$$\in \mathbb{Q}(X, Z).$$

In what follows, let $\mathfrak{p} = \mathfrak{p}_p$ be the unique prime ideal of K above p. Then, we see that $\mathfrak{p}^3 = p\mathcal{O}_K$, and π is a uniformizer of the $\mathfrak{p}$-adic completion of $\mathcal{O}_K$.

Lemma 6.5. *Let $a, c \in \mathbb{Z}$. Let $(A_k, B_k, C_k) \in \mathbb{Z}^{\oplus 3}$ ($k \in \mathbb{Z}$) such that*

$$A_k + B_k\pi^\iota + C_k\pi^{2\iota} \equiv \epsilon^k(a + c\pi^{2\iota}) \pmod{p^\iota}.$$

(1) *Suppose that $\beta \not\equiv 0 \pmod p$ or $\beta \equiv 0 \pmod p$ and $\gamma \not\equiv 0 \pmod p$. Then, $C_k \not\equiv 0 \pmod p$ for every k if and only if $\delta(a, c)$ is not a quadratic residue modulo p.*

(2) *Suppose that $\beta \equiv \gamma \equiv 0 \pmod p$. Then, $C_k \not\equiv 0 \pmod p$ for every k if and only if $c \not\equiv 0 \pmod p$.*

Proof. First, note that π is divisible by $\mathfrak{p}$, and α is prime to $\mathfrak{p}$ because $\epsilon = \alpha + \beta\pi + \gamma\pi^2$ is the fundamental unit of K. Therefore, by a simple induction on $k \in \mathbb{Z}$, we have

$$\frac{\epsilon^k}{\alpha^k} \equiv \begin{cases} 1 + k \cdot \dfrac{\beta}{\alpha}\pi + k \cdot \left(\dfrac{k-1}{2} \cdot \dfrac{\beta^2}{\alpha^2} + \dfrac{\gamma}{\alpha}\right)\pi^2 \pmod{\mathfrak{p}^3} & \text{if } \iota = 1 \\ 1 + k \cdot \dfrac{\gamma}{\alpha}\pi^2 + k \cdot \left(\dfrac{k-1}{2} \cdot \dfrac{\gamma^2}{\alpha^2} + \dfrac{p^{-1}\beta}{\alpha}\right)\pi^4 \pmod{\mathfrak{p}^6} & \text{if } \iota = 2 \end{cases}$$

[8] Note that if $p = 3$, then we can take $w_0, w_1, w_2 \in \mathbb{Z}$.

for every $k \in \mathbb{Z}$. This implies that

$$\frac{C_k}{\alpha^k} \equiv \begin{cases} \dfrac{\beta^2}{2\alpha^2}ak^2 - \left(\dfrac{\beta^2}{2\alpha^2} - \dfrac{\gamma}{\alpha}\right)ak + c \pmod{p} & \text{if } \iota = 1 \\ \dfrac{\gamma^2}{2\alpha^2}ak^2 - \left(\dfrac{\gamma^2}{2\alpha^2} - \dfrac{p^{-1}\beta}{\alpha}\right)ak + c \pmod{p} & \text{if } \iota = 2 \end{cases}$$

for every $k \in \mathbb{Z}$. Therefore, $C_k \not\equiv 0 \pmod{p}$ for every k if and only if the above quadratic polynomial of k has no zeros in $\mathbb{F}_p$. This implies the assertion. □

Proof of Proposition 6.2. First, note that Lemma 6.5 shows that the assertion holds if $\beta \equiv \gamma \equiv 0 \pmod{p}$.

Suppose that $\beta \not\equiv 0 \pmod{p}$, or $\beta \equiv 0 \pmod{p}$ and $\gamma \not\equiv 0 \pmod{p}$. For every $m \in \mathbb{Z}$, define $(a^{(m)}, b^{(m)}, c^{(m)}) \in \mathbb{Z}^{\oplus 3}$ by

$$a^{(m)} + b^{(m)}\pi^{\iota} + c^{(m)}\pi^{2\iota} = (a + c\pi^{2\iota})^m.$$

Then, by the assumption, we have $(a, b, c) \equiv (\pm 1 + pA, pB, c) \pmod{p^2}$ with some $A, B \in \mathbb{Z}$, hence $(a^{(m)}, b^{(m)}, c^{(m)}) \equiv ((\pm 1)^m, 0, \pm c) \pmod{p}$. Therefore, for every positive even integer $m < p$, we have

$$\delta(a^{(m)}, c^{(m)}) \equiv \begin{cases} \rho(\alpha, \beta, \gamma)^2 \mp 2cm \pmod{p} & \text{if } \beta \not\equiv 0 \pmod{p} \\ \rho(\alpha, \gamma, p^{-1}\beta)^2 \mp 2cm \pmod{p} & \text{if } \beta \equiv 0 \pmod{p} \text{ and } \gamma \not\equiv 0 \pmod{p} \end{cases}.$$

Suppose that $p \geq 7$ and $\beta \not\equiv 0 \pmod{p}$. Then, by taking into account of Proposition 6.3 and Lemma 6.5, what we have to prove is that

$$\left\{ \rho(\alpha, \beta, \gamma)^2 - 4cm' \pmod{p} \,\middle|\, 1 \leq m' \leq \frac{p-1}{2} \right\}$$

contains a quadratic non-residue. In particular, it is sufficient to prove that

$$B := \left\{ -\frac{1}{4c}\rho(\alpha, \beta, \gamma)^2 + m' \pmod{p} \,\middle|\, 1 \leq m' \leq \frac{p-1}{2} \right\}$$

contains both quadratic residues and non-residues, i.e.,

$$\left| \sum_{n \in B} \left(\frac{n}{p}\right) \right| < \frac{p-3}{2},$$

where (n/p) is the quadratic residue symbol. If $p = 19, 23, 31$ or $p \geq 37$, then the above inequality follows from an explicit version of the Pólya-Vinogradov inequality, e.g. the following one due to Pomerance [**52**]:

$$\left|\sum_{M\leq n\leq N}\left(\frac{n}{p}\right)\right|\leq\begin{cases}\left(\dfrac{2}{\pi^2}\log p+\dfrac{4}{\pi^2}\log\log p+\dfrac{3}{2}\right)p^{1/2} & \text{if } p\equiv 1 \pmod 4\\ \left(\dfrac{1}{2\pi}\log p+\dfrac{1}{\pi}\log\log p+1\right)p^{1/2} & \text{if } p\equiv 3 \pmod 4),\end{cases}$$

For $p = 11, 13, 17, 29$, we can check that B contains both quadratic residues and non-residues. In fact, we have the following table, which implies the desired inequality. Here, note that $(-n/p) \equiv (-1)^{(p-1)/2}(n/p)$.

n	0	1	2	3	4	5	6	7	8	9	10
$\left(\frac{n}{11}\right)$	0	1	-1	1	1	1	-1	-1	-1	1	-1

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$\left(\frac{n}{13}\right)$	0	1	-1	-1	1	-1	1	1	-1	1	-1	-1	1

n	0	1	2	3	4	5	6	7	8	9	$\ldots$	16
$\left(\frac{n}{17}\right)$	0	1	1	-1	1	-1	-1	-1	1	1	$\ldots$	1

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	$\ldots$	29
$\left(\frac{n}{29}\right)$	0	1	-1	-1	1	1	1	1	-1	1	-1	-1	-1	1	-1	-1	$\ldots$	1

If $P = 7$, then we have $\epsilon = 4 + 2 \cdot 7^{1/3} + 7^{2/3}$, so $\beta \not\equiv 0 \pmod 7$ and $\rho(\alpha, \beta, \gamma) \equiv 1 \pmod 7$. Therefore, we have $\delta(a^{(m)}, c^{(m)}) \equiv 1 - 2acm \pmod 7$. Suppose that $a \equiv 1 \pmod 7$. In this case, if $c \equiv 1, 2, 3, 4, 5, 6 \pmod 7$, then we can take $m = 6, 4, 2, 2, 4, 2$ respectively. Suppose that $a \equiv -1 \pmod 7$. In this case, if $c \equiv 1, 2, 3, 4, 5, 6 \pmod 7$, then we can take $m = 2, 4, 2, 2, 4, 6$ respectively according to the case of $a \equiv 1 \pmod 7$.

If $P = 14$, then we have $\epsilon = 1 + 2 \cdot 7^{1/3} - 7^{2/3}$, so $\beta \not\equiv 0 \pmod 7$ and $\rho(\alpha, \beta, \gamma) \equiv 5 \pmod 7$. Therefore, we have $\delta(a^{(m)}, c^{(m)}) \equiv 4 - 2acm \pmod 7$. Suppose that $a \equiv 1 \pmod 7$. In this case, if $c \equiv 1, 2, 3, 4, 5, 6 \pmod 7$, then we can take $m = 4, 2, 2, 6, 2, 4$ respectively. The case of $a \equiv -1 \pmod 7$ is similar.

If $P = 5$, then we have $\epsilon = 41 + 24 \cdot 5^{1/3} + 14 \cdot 5^{2/3}$, so $\beta \not\equiv 0 \pmod 5$ and $\rho(\alpha, \beta, \gamma) \equiv 1 \pmod 5$. Suppose that $a \equiv 1 \pmod 7$. In this case, if $c \equiv 1, 2, 3 \pmod 5$, then we can take $m = 2, 2, 4$. (Note, however, that if $c \equiv 4 \pmod 5$, then we cannot take even m.) The case of $a \equiv -1 \pmod 5$ is similar.

If $P = 6$, then since $\beta \equiv \gamma \equiv 0 \pmod 3$ we obtain the conclusion. If $P = 3$, then by assumption, we have $a \equiv 2 \pmod 3$, hence $(a^{(2)}, c^{(2)}) \equiv (1, c) \pmod 3$. Since $\epsilon = 2 - 3^{2/3}$, we have $\beta = 0$ and $\rho(\alpha, \gamma, 3^{-1}\beta) \equiv 2 \pmod 3$. Therefore, we have

$$\delta(a^{(2)}, c^{(2)}) \equiv 1 - 2c \pmod 3,$$

which is quadratic non-residue if and only if $c \equiv 1 \pmod 3$. The case of $a \equiv -1 \pmod 3$ is similar. This completes the proof in the case of $\beta \not\equiv 0 \pmod p$. The case where $\beta \equiv 0 \pmod p$ and $\gamma \not\equiv 0 \pmod p$ is similar. $\square$

7. Proof of the main theorem

Proof of Theorem 4.1. First, suppose that $p \neq 3$ and $\iota = 1$. Let $f(X, Y) = P(3PX \pm 1)^3 + (3PY + 1)^3$ and $g(X, Y) = P(3PX \mp 1)^3 + (3PY + 3)^3$ according to $P \equiv \pm 1 \pmod 3$. [9] Then, since $\gcd(f(0,0), f(0,1), f(0,-1)) = \gcd(g(0,0), g(0,1), g(0,-1)) = 1$, we have $\gcd(f(x,y) \mid (x,y) \in \mathbb{Z}^{\oplus 2}) = \gcd(g(x,y) \mid (x,y) \in \mathbb{Z}^{\oplus 2}) = 1$. Therefore, by Theorem 4.4, there exist infinitely many distinct prime numbers of the form $q = f(B, C)$ or $g(B, C)$ with $(B, C) \in \mathbb{Z}^{\oplus 2}$ such that $q \equiv 2 \pmod 3$. Among them, we can take distinct $(n-3)/2$ prime numbers $q_j = f(B_j, C_j)$ or $g(B_j, C_j)$ $(1 \leq j \leq (n-3)/2)$ so that $\gcd(3P, \sum_j b_j^{-1} c_j) = 1$, where $(b_j, c_j) := (3PB_j + 1, 3PC_j + 1)$ or $(3PB_j + 1, 3PC_j + 3)$ according to whether $q_j = f(B_j, C_j)$ or $g(B_j, C_j)$. Note that if $P \equiv 0 \pmod 2$, then the condition $\prod_j b_j \equiv 1 \pmod 2$ in Proposition 5.1 holds for arbitrary $(n-3)/2$-tuple $((b_j, c_j))_{1 \leq j \leq (n-3)/2}$ taken as above.

For each $(n-3)/2$-tuple $((b_j, c_j))_{1 \leq j \leq (n-3)/2}$ taken as above, by Theorem 6.1, there exist infinitely many prime numbers $l \equiv 2 \pmod 3$ and a positive even integer $m < p$ such that $l > \max\{p, b_j, c_j \mid j = 1, 2, \ldots, (n-3)/2\}$ and every primitive solution of $x^3 + P^\iota y^3 = l^m z^n$ satisfies $x \equiv y \equiv 0 \pmod l$. Therefore, Proposition 5.1 implies that the equation

$$(X^3 + P^\iota Y^3) \prod_{j=1}^{\frac{n-3}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = l^m Z^n$$

violates the local-global principle. The non-singularity follows from the fact that q_j and q_k are distinct prime numbers, hence $[b_j : c_j] \neq [b_k : c_k]$ for any $j \neq k$. The infinitude of the non-isomorphy classes follows from the following Lemma 7.1.

Next, suppose that $p \neq 3$ and $\iota = 2$. Let $f(X, Y) = P^2(3PX + 1)^3 + (3PY + 1)^3$ and $g(X, Y) = P^2(3PX - 1)^3 + (3PY + 3)^3$. Then, since $\gcd(f(0,0), f(0, \pm 1)) = \gcd(g(0,0), g(0, \pm 1)) = 1$, we have $\gcd(f(x,y) \mid (x,y) \in \mathbb{Z}^{\oplus 2}) = \gcd(g(x,y) \mid (x,y) \in \mathbb{Z}^{\oplus 2}) = 1$. The rest part is the same as the above argument.

[9] In fact, we can use more general polynomials to produce b_j, c_j with small absolute values. Here, we take f and g so that the proof of the infinitude gets simple.

Finally, suppose that $p = 3$. Then, we combine $f_{\pm}(X, Y) = P^{\iota}(PX \pm 1)^3 + (PY - 1)^3$ to produce (b_j, c_j) so that we can apply Proposition 5.1 with a help of Theorem 6.1. This completes the proof. □

Lemma 7.1. *Let $n \in \mathbb{Z}_{\geq 5}$ be an odd integer, $a \in \mathbb{Z} \setminus \{0\}$. Let $\mathcal{P} \subset \mathbb{Z}^{\oplus 2}$ be an infinite set of 2-dimensional integral vectors (b, c) such that $[b : c] \neq [b' : c']$ as a rational point of the projective line $\mathbb{P}^1$ for each distinct $(b, c), (b', c') \in \mathcal{P}$. For each $(n-3)/2$-tuple $\boldsymbol{v} = (b_j, c_j)_{1 \leq j \leq (n-3)/2} \in \mathcal{P}^{\frac{n-3}{2}}$, let $C(a, \boldsymbol{v})$ be the plane curve defined by*

$$(X^3 + aY^3) \prod_{j=1}^{\frac{n-3}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = Z^n.$$

Then, the set

$$\mathcal{C}_{a,n} := \left\{ C(a, \boldsymbol{v}) \,\middle|\, \boldsymbol{v} \in \mathcal{P}^{\frac{n-3}{2}} \right\}$$

contains infinitely many non-singular curves non-isomorphic to each other over $\mathbb{C}$.

Proof. Let C be a non-singular curve in $\mathcal{C}_{a,n}$. Then, since its genus $\frac{(n-2)(n-1)}{2} > 1$, Schwarz' theorem [**58**] ensures that the automorphism group $\mathrm{Aut}(C)$ of C is a finite group. [10] In particular, the set

$$\mathrm{Quot}(C) := \left\{ (C/\langle \varphi \rangle)^{\mathrm{nb}} \,\middle|\, \varphi \in \mathrm{Aut}(C) \right\}$$

contains finitely many n-punctured lines (i.e., $\mathbb{P}^1$ minus n points). Here, $C/\langle \varphi \rangle$ denotes the quotient of C by the cyclic group $\langle \varphi \rangle$ generated by φ, and $(C/\langle \varphi \rangle)^{\mathrm{nb}}$ denotes its non-branched locus, i.e., the image of the points each of whose φ-orbit consists of exactly $\# \langle \varphi \rangle$ distinct points.

On the other hand, for each $(n-3)/2$-tuple $\boldsymbol{v} = (b_j, c_j)_{1 \leq j \leq (n-3)/2} \in \mathcal{P}^{\frac{n-3}{2}}$, let $L(a, \boldsymbol{v})$ be a punctured line defined by

$$(X^3 + aY^3) \prod_{i=1}^{\frac{n-3}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) \neq 0.$$

Then, we can prove that the set consisting of them

$$\mathcal{L}_a^{\leq n} := \left\{ L(a, \boldsymbol{v}) \,\middle|\, \boldsymbol{v} \in \mathcal{P}^{\frac{n-3}{2}} \right\}$$

contains infinitely many non-isomorphic n-punctured lines. Indeed, for each $\boldsymbol{v} \in \mathcal{P}^{\frac{n-3}{2}}$, there exist at most $n(n-1)(n-2)$ tuples $\boldsymbol{v}' \in \mathcal{P}^{\frac{n-3}{2}}$ such that $L(a, \boldsymbol{v}')$ is isomorphic

[10] In fact, Hurwitz' theorem [**37**] gives an explicit bound $\# \mathrm{Aut}(C) \leq 84(g-1)$.

to $L(a, \boldsymbol{v})$ because such an isomorphism is extended to an element of $\mathrm{Aut}(\mathbb{P}^1)$, which is uniquely determined from the images of three points, say those satisfying $X^3 + aY^3 = 0$. As a consequence, we see that the set $\mathcal{L}_a^{\leq n}/\simeq_{\mathbb{C}}$ contains infinitely many isomorphism classes of n-punctured lines over $\mathbb{C}$.

Finally, note that we have a natural injection

$$\mathcal{L}_a^{\leq n}/\simeq_{\mathbb{C}} \hookrightarrow \left(\bigcup_{C \in \mathcal{C}_{a,n}} \mathrm{Quot}(C) \right) \Big/ \simeq_{\mathbb{C}}$$

induced by $L(a, \boldsymbol{v}) \mapsto (C(a, \boldsymbol{v})/\langle \varphi \rangle)^{\mathrm{nb}}$, where $\varphi([X : Y : Z]) = [X : Y : \zeta_n Z]$ with a fixed primitive n-th root of unity $\zeta_n \in \mathbb{C}$. Therefore, $\mathcal{C}_{a,n}$ contains infinitely many isomorphism classes of non-singular curves over $\mathbb{C}$ as claimed. □

8. A concrete example of degree 7

In this section, we demonstrate that the proof of Theorem 4.1 actually gives explicit parameters $(b_1, c_1; b_2, c_2; L)$ for which the equation

$$(X^3 + 7Y^3)(b_1^2X^2 + b_1c_1XY + c_1^2Y^2)(b_2^2X^2 + b_2c_2XY + c_2^2Y^2) = LZ^7$$

defines a non-singular plane curve which violates the local-global principle.

First of all, since the fundamental unit of $\mathbb{Q}(7^{1/3})$ is $\epsilon = 4 + 2 \cdot 7^{1/3} + 7^{2/3}$, Conjecture 4.2 is verified for $p = 7$. Hence, we have $\iota = 1$, and so we can actually take $n = 7$ in Theorem 4.1.

In order to produce the coefficients $(b_1, c_1; b_2, c_2)$, we can use the cubic polynomial $f(X, Y) = 7(3X + 1)^3 + (3Y + 1)^3$ in the proof of Theorem 4.1. Indeed, by Theorem 4.4, the set $f(\mathbb{Z}^{\oplus 2})$ contains infinitely many prime numbers, for example,

$$\begin{aligned} 71 &= 7 \cdot (3 \cdot 0 + 1)^3 + (3 \cdot 1 + 1)^3, \\ 449 &= 7 \cdot (3 \cdot 1 + 1)^3 + (3 \cdot 0 + 1)^3, \\ 503 &= 7 \cdot (3 \cdot 11 + 1)^3 + (3 \cdot (-22) + 1)^3, \\ &\ \vdots \quad \text{etc.} \end{aligned}$$

Among such $(b_j, c_j) = (3X + 1, 3Y + 1)$, we can take, for example, $(b_1, c_1) = (1, 4)$ and $(b_2, c_2) = (4, 1)$.

For each choice of the above coefficients, we can take $L = l^m$ with a prime number $l > \max\{p, b_1, c_1, b_2, c_2\}(= 7)$ and even integer $m \in \mathbb{Z}_{\geq 2}$ so that every primitive solution of $x^3+7y^3=l^mz^7$ satisfies $x\equiv y\equiv 0 \pmod{l}$ (cf. condition (6) in Proposition 5.1). In fact, as in the proof of Theorem 6.1, we can produce such l as integral values of another cubic polynomial $g(A,C)=(21A+1)^3+49(21C+1)^3$. For example,

$$\begin{aligned}
262193 &= (21\cdot 3+1)^3+49(21\cdot 0+1)^3,\\
452831 &= (21\cdot(-2)+1)^3+49(21\cdot 1+1)^3,\\
521753 &= (21\cdot 0+1)^3+49(21\cdot 1+1)^3,\\
&\ \ \vdots \quad \text{etc.}
\end{aligned}$$

Here, we take $l=262193$ with $(a,c):=(21A+1,21C+1)=(64,1)$.

Finally, to produce the exponent m, we use Proposition 6.3 and Lemma 6.5. They ensure that every primitive solution of $x^3+7y^3=262193^mz^7$ satisfies $x\equiv y\equiv 0 \pmod{262193}$ whenever $\delta(a,mc)\equiv\delta(1,m)\equiv 4-2m \pmod{7}$ is a non-quadratic residue. Thus, we can take $m=4$.

As a consequence, we obtain an explicit counterexample to the local-global principle:

$$(X^3+7Y^3)(X^2+4XY+16Y^2)(16X^2+4XY+Y^2)=262193^4Z^7.$$

9. Main theorem in even degree case

The goal of §§9–11 is to prove the following Theorem 9.1. Similarly to Theorem 4.1, we should emphasize the following point: Although it is unclear from the statement, our proof of Theorem 9.1 ensures that for every even degree $n\geq 8$, we have an algorithm to obtain arbitrarily many explicit parameters (b_j,c_j) and l for which eq. (8) define non-singular plane curves which violate the local-global principle. For detailed properties satisfied by (b_j,c_j) and l, see Proposition 10.1 in §10 and the proof of Theorem 9.1 in §11. Note also that the proof of the infinitude of the geometric isomorphy classes in Theorem 9.1 is based on the infinitude of prime numbers of the form $158b^3+c^3$ with $b,c\in Z$ satisfying some additional conditions (cf. Theorem 4.4, Lemma 7.1, and Proposition 10.1).

Theorem 9.1. *Let $n\in\mathbb{Z}_{\geq 8}$ be an even integer, and $m\in\mathbb{Z}_{\geq 3}$ be an odd integer such that $m<n$. Then, there exist infinitely many $(n-6)/2$-tuples of pairs of integers (b_j,c_j) $(1\leq j\leq(n-6)/2)$ satisfying the following condition:*

For every $j\geq 1$, the integer $158^2b_j^3+c_j^3$ is a prime number, and there exist infinitely many prime numbers l and infinitely many pairs of integers (b_0,c_0) such that $l\equiv 2 \pmod{3}$ and *the equation*

$$(8) \qquad (X^3+158^2Y^3)(b_0X^3-lc_0Y^3)\prod_{j=1}^{(n-6)/2}(b_j^2X^2+b_jc_jXY+c_j^2Y^2)=l^mZ^n$$

define non-singular plane curves of degree n which violate the local-global principle.

Moreover, for each even $n \geq 8$, there exists a set of such $(n-4)/2$-tuples $((b_j, c_j))_{0\leq j\leq (n-6)/2}$ which gives infinitely many geometrically non-isomorphic classes of such curves of degree n.

As a consequence of the proof of Theorem 9.1, we can produce as many as we want explicit examples as Bremner-Lewis-Morton's example (cf. Theorem 2.4)

$$3X^4+4Y^4=19Z^4$$

and Schinzel's example (cf. Theorem 2.5)

$$X^4-2Y^4-16Y^2Z^2-49Z^4=0.$$

For example, we obtain the following new examples (cf. §12)

$$(X^3+158^2Y^3)(671X^3-7583\cdot(-47^2)\cdot Y^3)(X^2+7XY+7^2Y^2)=7583^mZ^8 \quad (m=3,5,7)$$

each of which defines a non-singular plane curve of degree 8 which violates the local-global principle.

A key ingredient of our construction is again Theorem 4.4. However, the construction in §§4–7 does not work for $p=2$. One of the major obstructions is the fact that the congruence

$$(a+bp^{1/3}+cp^{2/3})^p\equiv a \pmod p \quad (a,b,c\in\mathbb{Z})$$

does not hold for $p=2$. In these setting, a standard compromise method in number theory is to use "$p=4$" in place of $p=2$, that is,

$$(a+b\cdot 2^{1/3}+c\cdot 2^{2/3})^4\equiv a \pmod 2 \quad (a,b,c\in\mathbb{Z}).$$

If one avoids the above obstruction by this compromise method, however, the crucial obstruction arises from the fundamental unit of $K=\mathbb{Q}(2^{1/3})$ if one uses the cubic form $X^3+2^\iota Y^3$ in place of $X^3+P^\iota Y^3$ ($\iota=1,2$), that is, there is no prime numbers l satisfying the conditions in Proposition 6.3 for $p=2$.

In order to avoid these obstructions at the same time, we use an auxiliary odd prime number p and the associated nice cubic field $\mathbb{Q}((2p)^{1/3})$. In some sense, we reverse the roles of odd prime numbers p and the even prime number 2 in the case of $p \equiv \pm 1 \pmod 9$ in Theorem 4.1. In fact, we take $p = 79$ in Theorem 9.1 here, but there are possible other choices. For the arithmetic background of this subtlety, see Theorem 11.1.

In §10, we give a recipe which exhibits how to construct counterexamples to the local-global principle as in eq. (8) from certain Fermat type equations and prime numbers. These objects are constructed in completely explicit manners via Theorem 4.4 in §11. The proofs of Theorem 9.1 is done in §11 by combining these arithmetic objects with a geometric argument on the non-isomorphy of complex algebraic curves defined by eq. (8), where the latter we can prove exactly in a similar manner to Lemma 7.1. In §12, we demonstrate how our construction works well by exhibiting a concrete example of degree 8.

Remark 9.2. Recently, the author [**27**, Theorem 1.7] succeeded in generalizing Theorem 9.1. For the detail, see the cited article.

Notation for §§9–12

For every prime number p, P denotes $2p$ and $\iota = 1$ or 2. We use these notation for the comparison of the contents of §§9–12 with those of §§4–8. However, in order to prove Theorem 9.1, $\iota = 2$ is sufficient.

We say that a triple $(x, y, z) \in \mathbb{Z}^{\oplus 3}$ is primitive if $\gcd(x, y, z) = 1$.

10. Construction from prime numbers and Fermat type equations

Let p be an odd prime number, $P = 2p$, and $\iota = 1$ or 2. For simplicity, we assume that $p \not\equiv \pm 4 \pmod 9$, i.e., $P \not\equiv \pm 1 \pmod 9$. In this section, we prove the following proposition, which gives explicit counterexamples to the local-global principle of even degree n under the assumption that we have

- sufficiently many prime numbers of the form $P^\iota b^3 + c^3$ with $b, c \in \mathbb{Z}$ and
- integers L such that the equation $x^3 + P^\iota y^3 = Lz^n$ has a specific property.

In what follows, for each prime number l, $v_l(n)$ denotes the additive l-adic valuation of $n \in \mathbb{Z}$.

Proposition 10.1 (Recipe for even degree)**.** *Let $n \in \mathbb{Z}_{\geq 8}$ be an even integer, p be a prime number, $P = 2p$, and $\iota = 1$ or 2. Let $b_0, \ldots, b_{(n-6)/2}, c_0, \ldots, c_{(n-6)/2}, m \in \mathbb{Z}$ and l be a prime number satisfying the following conditions:*

(1) $P^\iota b_0 - lc_0 = \pm 3^k$ *for some* $k \geq 0$. *Moreover, if* $P \not\equiv \pm 2, \pm 4 \bmod 9$ *(i.e.,* $p = 3$*), then* $k = 0$.

(2) *For every* $j \geq 1$, *the integer* $P^\iota b_j^3 + c_j^3$ *is a prime number such that* $P^\iota b_j^3 + c_j^3 \equiv 2 \pmod 3$ *and* $\gcd(P, c_j) = 1$.

(3) $l \equiv 2 \pmod 3$ *and* $\gcd(l, b_j c_j) = 1$ *for every* $j \geq 0$.

(4) $b_0 \equiv 1 \pmod 2$.

(5) *If* $P \not\equiv \pm 1 \pmod 9$, $l^m \equiv b_0 \prod_{j\geq 1} b_j^2 \not\equiv 0 \pmod 3$ *and* $\sum_{j\geq 1} b_j^{-1} c_j \not\equiv 0 \pmod 3$.

(6) *If* $p \equiv 2 \pmod 3$, $l^m \equiv b_0 \prod_{j\geq 1} b_j^2 \not\equiv 0 \pmod p$ *and* $\sum_{j\geq 1} b_j^{-1} c_j \not\equiv 0 \pmod p$.

(7) $2 \leq m < n$.

(8) *For every primitive triple* $(x, y, z) \in \mathbb{Z}^{\oplus 3}$ *satisfying* $x^3 + P^\iota y^3 = l^m z^n$, *we have* $x \equiv y \equiv 0 \pmod l$.

Then, the equation

$$(X^3 + P^\iota Y^3)(b_0 X^3 + lc_0 Y^3) \prod_{j=1}^{\frac{n-6}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = l^m Z^n$$

violates the local-global principle.

Lemma 10.2 (local solubility for even degrees)**.** *Let* $n \in \mathbb{Z}_{\geq 8}$ *be an even integer,* p *be a prime number,* $P = 2p$, *and* $\iota = 1$ *or* 2. *Let* $a, b_0, \ldots, b_{(n-6)/2}, c_0, \ldots, c_{(n-6)/2}, L \in \mathbb{Z}$ *satisfying the following conditions:*

(1) $b_0, c_0 \equiv 1 \pmod 2$.

(2) *If* $P \not\equiv \pm 1 \pmod 9$, $L \equiv b_0 \prod_{j\geq 1} b_j^2 \not\equiv 0 \pmod 3$ *and* $\sum_{j\geq 1} b_j^{-1} c_j \not\equiv 0 \pmod 3$.

(3) *If* $p \equiv 2 \pmod 3$, $L \equiv b_0 \prod_{j\geq 1} b_j^2 \not\equiv 0 \pmod p$ *and* $\sum_{j\geq 1} b_j^{-1} c_j \not\equiv 0 \pmod p$.

Then, the equation

$$F(X, Y, Z) := (X^3 + P^\iota Y^3)(b_0 X^3 + c_0 Y^3) \prod_{j=1}^{\frac{n-6}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) - LZ^n = 0$$

has non-trivial solutions over $\mathbb{R}$ *and* $\mathbb{Q}_l$ *for every prime number* l.

Proof. By Fujiwara's argument (cf. Proposition 22.4), it is sufficient to consider the solubility over $\mathbb{Q}_l$ for $l = 2, 3, p$.

(1) $b_0 X^3 + c_0 Y^3$ is decomposed in $\mathbb{Z}_2[X, Y]$.

(2) If $P \equiv \pm 1 \pmod 9$, then $X^3 + P^\iota Y^3$ is decomposed in $\mathbb{Z}_3[X, Y]$. On the other hand, if $P \not\equiv \pm 1 \pmod 9$, then since $F(1, 0, 1) \equiv b_0 \prod_{j\geq 1} b_j^2 - L \equiv 0 \pmod 3$,

and $(\partial F/\partial Y)(1,0,1) \equiv (b_0 \prod_{j\geq 1} b_j^2) \cdot (\sum_{j \geq 1} b_j^{-1} c_j) \not\equiv 0 \pmod 3$, we obtain a 3-adic lift of mod 3 solution $(1,0,1)$ by Hensel's lemma.

(3) If $p \equiv 1 \pmod 3$, then $b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2$ is decomposed in $\mathbb{Z}_p[X,Y]$. On the other hand, if $p \equiv 2 \pmod 3$, then since $F(1,0,1) \equiv b_0 \prod_{j \geq 1} b_j^2 - L \equiv 0 \pmod p$ and $(\partial F/\partial Y)(1,0,1) \equiv (b_0 \prod_{j\geq 1} b_j^2) \cdot (\sum_{j \geq 1} b_j^{-1} c_j) \not\equiv 0 \pmod p$, we obtain a p-adic lift of mod p solution $(1,0,1)$ by Hensel's lemma.

This completes the proof. □

Lemma 10.3 (global unsolubility for even degrees). *Let $n \in \mathbb{Z}_{\geq 8}$ be an even integer, a, $b_0, \ldots, b_{(n-6)/2}$, $c_0, \ldots, c_{(n-6)/2}$, $m \in \mathbb{Z}$, and l be a prime number satisfying the following conditions:*

(1) *$ab_0 - lc_0 = \pm 3^k$ with some $k \geq 0$. Moreover, if $a \not\equiv \pm 2, \pm 4 \bmod 9$, then $k = 0$.*

(2) *For every $j \geq 1$, the integer $ab_j^3 + c_j^3$ is a prime number such that $ab_j^3 + c_j^3 \equiv 2 \pmod 3$ and $\gcd(a, c_j) = 1$.*

(3) *$l \equiv 2 \pmod 3$ and $\gcd(l, b_j c_j) = 1$ for every $j \geq 0$.*

(4) *$2 \leq m < n$.*

(5) *For every primitive triple $(x,y,z) \in \mathbb{Z}^{\oplus 3}$ satisfying $x^3 + P^\iota y^3 = l^m z^n$, we have $x \equiv y \equiv 0 \pmod l$.*

Then, there exist no triples $(X,Y,Z) \in \mathbb{Z}^{\oplus 3} \setminus \{(0,0,0)\}$ satisfying

$$(X^3 + aY^3)(b_0 X^3 + lc_0 Y^3) \prod_{j=1}^{\frac{n-6}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = l^m Z^n. \tag{9}$$

Proof. We prove the assertion by contradiction. Let $(X,Y,Z) \in \mathbb{Z}^{\oplus 3}$ be a triple satisfying eq. (9). We may assume that it is primitive. It is sufficient to prove that

$$\gcd((X^3 + aY^3)l, (b_0 X^3 + lc_0 Y^3)(b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2)) = 1 \quad \text{for every } j \geq 1. \tag{10}$$

Indeed, if eq. (10) hold, then we have some divisor z of Z satisfying $X^3 + aY^3 = l^m z^n$, hence $X \equiv Y \equiv 0 \pmod l$. However, since $m < n$, we also have $Z \equiv 0 \pmod l$, which contradicts that $\gcd(X,Y,Z) = 1$. In what follows, we prove eq. (10) by contradiction.

First, suppose that a prime divisor q of $X^3 + aY^3$ divides $b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2$ for some $j \geq 1$. Then, q divides

$$b_j^3 (X^3 + aY^3) - (b_j X - c_j Y)(b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = (ab_j^3 + c_j^3) Y^3.$$

Since $\gcd(X,Y,Z) = 1$ and $m < n$, we see that $Y \not\equiv 0 \pmod q$. Hence, we have $q = ab_j^3 + c_j^3 \equiv 2 \pmod 3$. In particular, the polynomial $b_j^2 T^2 + b_j c_j T + c_j^2$ is irreducible in

$\mathbb{Z}_q[T]$. Since $b_j^2X^2 + b_jc_jXY + c_j^2Y^2 \equiv 0 \pmod q$ and $Y \not\equiv 0 \pmod q$, we have $c_j \equiv 0 \pmod q$. However, the equality $q = ab_j^3 + c_j^3$ implies that a must be divisible by q, which contradicts the assumption that $\gcd(a, c_j) = 1$.

Secondly, suppose that l divides $b_j^2X^2 + b_jc_jXY + c_j^2Y^2$ for some $j \geq 1$. Then, since $l \equiv 2 \bmod 3$ and $\gcd(l, b_jc_j) = 1$, we have $X \equiv Y \equiv 0 \bmod l$. However, since $v_l(L) < n$, we see that $Z \equiv 0 \bmod l$, which contradicts that $\gcd(X, Y, Z) = 1$.

Thirdly, suppose that a prime divisor q of $X^3 + aY^3$ divides $b_0X^3 + lc_0Y^3$. Then, since $\gcd(X, Y, Z) = 1$ and $m < n$, we see that $Y \not\equiv 0 \pmod q$. On the other hand, since q divides

$$b_0(X^3 + aY^3) - (b_0X^3 + lc_0Y^3) = (ab_0 - lc_0)Y^3 = \pm 3^kY^3,$$

we have $q = 3$ and $k \geq 1$, hence $a \equiv \pm 2, \pm 4 \bmod 9$. However, $X^3 + aY^3 \equiv 0 \bmod 3$ implies that $X \equiv aY \equiv 0 \bmod 3$, which contradicts that $Y \not\equiv 0 \bmod 3$ and $a \equiv \pm 2, \pm 4 \bmod 9$.

Finally, suppose that l divides $b_0X^3 + lc_0Y^3$. Then, we have $X \equiv 0 \pmod l$. Since $m \geq 2$, we have $(a \cdot lc_0 \prod_{j \geq 1} c_j^2)Y^n \equiv 0 \bmod l^2$. On the other hand, since $ab_0 - lc_0 = \pm 3^k$, we have $\gcd(l, a) = 1$. Moreover, since $\gcd(l, c_j) = 1$ for every $j \geq 0$, we have $\gcd(l, ac_0 \prod_{j \geq 1} c_j^2) = 1$ for every $j \geq 0$, hence $Y \equiv 0 \bmod l$. However, since $m < n$, we have $Z \equiv 0 \bmod l$, which contradicts that $\gcd(X, Y, Z) = 1$. This completes the proof.

□

11. Reduction to the Fermat type equations $X^3 + P^\iota Y^3 = l^m Z^n$

In this section, let p be an odd prime number, $P = 2p$, $\pi = P^{1/3} \in \mathbb{R}$ be the real cubic root of P, $K = \mathbb{Q}(\pi) \subset \mathbb{R}$, and $\mathcal{O}_K$ denotes the ring of integers in K. Suppose that $p \not\equiv \pm 4 \pmod 9$ so that $\mathcal{O}_K = \mathbb{Z}[\pi]$. Let $\epsilon = \alpha + \beta\pi + \gamma\pi^2 > 1$ be the fundamental unit of K with $\alpha, \beta, \gamma \in \mathbb{Z}$. Note that the Galois closure of K in $\mathbb{C}$ is $K(\zeta_3)$, where $\zeta_3 \in \mathbb{C}$ is a fixed primitive cubic root of unity. For basic properties of these objects, see §22 (cf. [**3**], [**22**], and their references).

In this section, we prove Theorem 9.1 by using the following theorem.

Theorem 11.1. *In the above setting, further suppose that* $\beta \equiv \gamma \equiv 0 \pmod 2$*, and the class number of* K *is odd. Then, for every even integer* $n \in \mathbb{Z}_{\geq 4}$ *and every odd integer* $m \in \mathbb{Z}_{\geq 1}$*, there exist infinitely many odd prime numbers* $l \equiv 2 \pmod 3$ *such that for every primitive triple* $(x, y, z) \in \mathbb{Z}^{\oplus 3}$ *satisfying* $x^3 + P^2y^3 = l^mz^n$*, we have* $x \equiv y \equiv 0 \pmod l$*.*

Proof of Theorem 9.1 under Theorem 11.1. Let $p = 79$ and $P = 2p = 158$. Then, we can check directly the conditions in Theorem 11.1. Let $f(X, Y) = P^2(3X+1)^3 +$

$(3Y+1)^3$ and $g(X,Y) = P^2(3X-1)^3+(3Y)^3$. Then, since $\gcd(f(0,0), f(0,1)) = 1$ and $\gcd(g(0,0), g(0,1)) = 1$, we have $\gcd(f(x,y) \mid (x,y) \in \mathbb{Z}^{\oplus 2}) = 1$ and $\gcd(g(x,y) \mid (x,y) \in \mathbb{Z}^{\oplus 2}) = 1$ respectively. Therefore, by Theorem 4.4, there exist infinitely many distinct prime numbers of the forms $q = f(B,C)$ (resp. $q = g(B,C)$) with $(B,C) \in \mathbb{Z}^{\oplus 2}$. Among such prime numbers q, take distinct $(n-6)/2$ prime numbers $q_j = f(B_j, C_j)$ or $g(B_j, C_j)$ with $(B_j, C_j) \in \mathbb{Z}^{\oplus 2}$ $(1 \leq j \leq (n-6)/2)$ so that $\sum_j b_j^{-1} c_j \not\equiv 0 \pmod 3$, where $(b_j, c_j) := (3B_j+1, 3C_j+1)$ or $(3B_j-1, 3C_j)$ according to whether $q_j = f(B_j, C_j)$ or $g(B_j, C_j)$.

For each $(n-6)/2$-tuple $((b_j, c_j))_{1 \leq j \leq (n-6)/2}$ taken as above, we have infinitely many prime numbers $l > \max\{p, b_j, c_j \mid j = 1, 2, \ldots, (n-6)/2\}$ satisfying the properties claimed in Theorem 11.1. We fix such l arbitrarily. Then, we have $l^m \equiv 2 \pmod 3$. Since $\gcd(l, 3P) = 1$, there exist infinitely many pairs $(b, c_0) \in \mathbb{Z}^{\oplus 2}$ such that $6P^2 b - lc_0 = 1 - P^2 l$ and $\gcd(l, c_0) = 1$. Take such a pair (b, c_0) and set $b_0 = l + 6b$. Then, we see that b_0 is odd, $l^m \equiv b_0 \prod_{j \geq 1} b_j^2 \equiv 2 \pmod 3$, and $\gcd(l, b_0 c_0) = 1$. Therefore, Proposition 10.1 implies that the equation

$$(X^3 + P^2 Y^3)(b_0 X^3 + lc_0 Y^3) \prod_{j=1}^{\frac{n-6}{2}} (b_j^2 X^2 + b_j c_j XY + c_j^2 Y^2) = l^m Z^n$$

violates the local-global principle. The non-singularity follows from the following two facts:

(1) q_j and q_k are distinct prime numbers, hence $[b_j : c_j] \neq [b_k : c_k]$ for any distinct $j, k \geq 1$.
(2) Since all of l, b_0, c_0 are odd, $X^3 + 158^2 Y^3$ and $b_0 X^3 + lc_0 Y^3$ cannot have a common root in $\mathbb{C}$.

The non-isomorphy follows from the same argument as in the proof of Lemma 7.1. This completes the proof. □

In order to prove Theorem 11.1, we use Theorem 4.4. Let p $(\neq 3)$ be a prime number satisfying the conditions in Theorem 11.1. Let $h(A,B) = (6A+1)^3 + P(6B \mp 1)^3$ according to $p \equiv \pm 1 \pmod 3$. Then, since $\gcd(h(0,0), h(1,0), h(-1,0)) = 1$, we have $\gcd(h(\mathbb{Z}^{\oplus 2})) = 1$. Therefore, Theorem 4.4 implies that there exist infinitely many prime numbers l of the form

$$l = a^3 + Pb^3 \equiv 2 \pmod 3 \quad \text{with} \quad (a,b) = (6A+1, 6B \mp 1) \in \mathbb{Z}^{\oplus 2}.$$

Thus, Theorem 11.1 is obtained from the case of $(\iota, \nu) = (2, 1)$ in the following proposition.

Proposition 11.2. *Let p be a prime number satisfying the conditions in Theorem 11.1 and $(\iota, \nu) = (1, 2)$ or $(2, 1)$. Let $l \neq 2, p$ be a prime number such that $l \equiv 2 \pmod 3$. Assume that there exist $a + b\pi + c\pi^2 \in \mathcal{O}_K$ with $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}_{\geq 1}$ satisfying the following conditions:*

(1) $l = a^3 + b^3P + c^3P^2 - 3abcP$. [11]

(2) (a) *If $\iota = 1$, then $m \not\equiv 0 \pmod 4$. Moreover, if $m \equiv 1$ (resp. $2, 3$) $\pmod 4$, then c (resp. $b, b + c$) is odd.*

(b) *If $\iota = 2$, then both m and b are odd.*

Then, for every integer $n \in \mathbb{Z}_{\geq 3}$ divisible by 2^ν and every primitive triple $(x, y, z) \in \mathbb{Z}^{\oplus 3}$ satisfying $x^3 + P^\iota y^3 = l^m z^n$, we have $x \equiv y \equiv 0 \pmod l$.

Proof of Proposition 11.2. We prove the assertion by contradiction. Suppose that there exists a primitive triple $(x, y, z) \in \mathbb{Z}^{\oplus 3}$ such that $x^3 + P^\iota y^3 = l^m z^n$, and either x or y is prime to l.

First, note that since either x or y is prime to l and $\gcd(l, 3P) = 1$, $x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ cannot be divisible by l. Moreover, $l \equiv 2 \pmod 3$ splits to the product of two prime ideals $\mathfrak{p}_l$ and $\mathfrak{p}_{l^2}$ of degree 1 and 2 respectively. Suppose that $x + y\pi$ is divisible by $\mathfrak{p}_{l^2}$. Then, the product of its conjugates $(x + \zeta_3 y\pi^\iota)(x + \zeta_3^2 y\pi^\iota) = x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ is divisible by l, a contradiction (cf. the following argument for $q \equiv 2 \pmod 3$). Therefore, $x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ is divisible by $\mathfrak{p}_{l^2}^m$ but not divisible by $\mathfrak{p}_l$. Accordingly, $x + y\pi^\iota$ is divisible by $\mathfrak{p}_l^m$ but not divisible by $\mathfrak{p}_{l^2}$.

Next, suppose that $x + y\pi^\iota$ is divisible by a prime ideal above a prime divisor q of z. Then, note that if $\gcd(q, P) = 1$ and $x + y\pi^\iota$ or $x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ is divisible by q itself, then we have $x \equiv y \equiv 0 \pmod q$, which contradicts that (x, y, z) is primitive. On the other hand, since $P \not\equiv \pm 1 \pmod 9$, the possible decomposition types of q in K are as follows:

(1) $(q) = \mathfrak{p}_{q,1}\mathfrak{p}_{q,2}\mathfrak{p}_{q,3}$, i.e., $q \equiv 1 \pmod 3$ and $P \pmod q \in \mathbb{F}_q^{\times 3}$

(2) $(q) = \mathfrak{p}_q\mathfrak{p}_{q^2}$, i.e., $q \equiv 2 \pmod 3$ and $P \not\equiv 0 \pmod q$

(3) $(q) = \mathfrak{p}_q^3$, i.e., $P \equiv 0 \pmod q$, or $q = 3$ and $P \not\equiv \pm 1 \pmod 9$.

In each case, we have the following conclusion:

(1) If $x + y\pi^\iota$ is divisible by distinct two prime ideals above q, say $\mathfrak{p}_{q,1}$ and $\mathfrak{p}_{q,2}$, then $x^2 - xy\pi^\iota + y^2\pi^{2\iota}$ is divisible by $(\mathfrak{p}_{q,1}\mathfrak{p}_{q,3}) \cdot (\mathfrak{p}_{q,2}\mathfrak{p}_{q,3})$, hence by q, a contradiction.

[11] Since $l \equiv 2 \pmod 3$, $\mathcal{O}_K$ has prime ideals $\mathfrak{p}_l$ and $\mathfrak{p}_{l^2}$ of norms of degree 1 and 2 respectively. Therefore, the first condition holds up to signature if and only if $\mathfrak{p}_l$ is generated by $a + b\pi + c\pi^2$.

Therefore, $x + y\pi^{\iota}$ is divisible by $\mathfrak{p}_{q,1}^{nv_q(z)}$ but not by $\mathfrak{p}_{q,2}$ nor $\mathfrak{p}_{q,3}$ if we replace $\mathfrak{p}_{q,1}, \mathfrak{p}_{q,2}, \mathfrak{p}_{q,3}$ to each other if necessary.

(2) In this case, q is decomposed in $K(\zeta_3)$ so that $\mathfrak{p}_q = \mathfrak{P}_{q^2,1}$ and $\mathfrak{p}_{q^2} = \mathfrak{P}_{q^2,2}\mathfrak{P}_{q^2,3}$. If $x + y\pi^{\iota}$ is divisible by $\mathfrak{p}_{q^2}$, then $x^2 - xy\pi^{\iota} + y^2\pi^{2\iota}$ is divisible by $(\mathfrak{P}_{q^2,1}\mathfrak{P}_{q^2,2}) \cdot (\mathfrak{P}_{q^2,1}\mathfrak{P}_{q^2,3})$, hence by q, a contradiction. Therefore, $x + y\pi^{\iota}$ is divisible by $\mathfrak{p}_q^{nv_q(z)}$ but not by $\mathfrak{p}_{q^2}$.

(3) In this case, since $x^3 + P^{\iota}y^3$ is divisible by $\mathfrak{p}_q^{3n}$, $x + y\pi^{\iota}$ is divisible by $\mathfrak{p}_q^{n}$. Since $n \geq 3$, and π^{ι} cannot be divisible by q, both x and y are divisible by q. It contradicts that (x, y, z) is primitive.

As a consequence, we see that there exists an integral ideal $\mathfrak{w}$ of $\mathcal{O}_K$ such that

$$(x + y\pi^{\iota}) = \mathfrak{p}_l^m \mathfrak{w}^n \quad \text{and} \quad (P, \mathfrak{w}) = 1.$$

Then, since the first assumption implies that $\mathfrak{p}_l$ is generated by $a + b\pi + c\pi^2$, $\mathfrak{w}^n$ is a principal ideal. Moreover, since we assume that the class number of K is odd, the ideal $\mathfrak{w}^{n/2^{\nu}}$ is also generated by a single element $w_0 + w_1\pi + w_2\pi^2 \in \mathcal{O}_K$ with $w_0, w_1, w_2 \in \mathbb{Z}$. [12] Therefore, there exists $k \in \mathbb{Z}$ such that

$$x + y\pi^{\iota} = \epsilon^k (a + b\pi + c\pi^2)^m (w_0 + w_1\pi + w_2\pi^2)^{2^{\nu}}.$$

Since we assume that $\beta \equiv \gamma \equiv 0 \pmod 2$, and $\gcd(l, P) = 1$ implies that $a \equiv 1 \pmod 2$, by using Lemma 11.3, we have

$$x + y\pi^{\iota} \equiv \left(1 + mb\pi + \left(\binom{m}{2}b^2 + mc\right)\pi^2\right)(w_0 + w_1\pi^{2^{\nu}}) \pmod 2.$$

Here, note that since $\gcd(P, \mathfrak{w}) = 1$, we see that $w_0 \not\equiv 0 \pmod 2$.

If $\iota = 1$, then since we assume that $\nu = 2$, the above congruence between the coefficients of π^2 contradicts the assumption on the parities of $b, c, b + c$.

If $\iota = 2$, then the above congruence between the coefficients of π contradicts the assumption that both m and b are odd. This completes the proof. □

Lemma 11.3. *Let p be a prime number, d be a cube-free integer such that $d \equiv 0 \pmod p$, $\pi = d^{1/3} \in \mathbb{R}_{\geq 1}$ be the real cubic root of d, and $K = \mathbb{Q}(\pi) \subset \mathbb{R}$ be the number field generated by π. Let $\mathfrak{p}$ be the (unique) prime ideal of K above p. Then, for every $w_0+w_1\pi+w_2\pi^2 \in \mathcal{O}_K$ with $w_0, w_1, w_2 \in (1/3)\mathbb{Z}$, we have*

$$(w_0 + w_1\pi + w_2\pi^2)^p \equiv w_0 + w_1\pi^p \pmod p$$

[12] Note that if $p = 3$, then we can take $w_0, w_1, w_2 \in \mathbb{Z}$.

and

$$(w_0 + w_1\pi + w_2\pi^2)^{p^2} \equiv w_0 + w_1\pi^{p^2} \pmod{\mathfrak{p}^5}.$$

Proof. First, note that $\pi^3 \equiv 0 \pmod{p}$.

Suppose that p is odd. Then, the first congruence follows from $p \geq 3$, $\binom{p}{1} \equiv \binom{p}{2} \equiv 0 \pmod{p}$, and $w_0^p \equiv w_0 \pmod{p}$. The second congruence follows from $p^2 \geq 6$, $\binom{p^2}{1} \equiv \binom{p^2}{2} \equiv 0 \pmod{p^2}$, $\binom{p^2}{3} \equiv \binom{p^2}{4} \equiv 0 \pmod{p}$, and $w_0^{p^2} \equiv w_0 \pmod{p^2}$.

Next, suppose that $p = 2$. Then, the first congruence follows from $\binom{2}{1} \equiv 0 \pmod{2}$ and $w_i^2 \equiv w_0 \pmod{2}$. The second congruence follows from $4 \geq 3$, $\binom{4}{1} \equiv \binom{4}{3} \equiv 0 \pmod{4}$, $\binom{4}{2} \equiv 0 \pmod{2}$, and $w_i^4 \equiv w_0 \pmod{4}$. □

It is obvious that we obtain a counterpart of Theorem 11.1 from the case of $(\iota, \nu) = (1, 2)$ in Proposition 11.2. For instance, we obtain the following corollary by applying the exactly same argument as the proof of Theorem 11.1 (with the exactly same polynomial $h(A, B)$).

Corollary 11.4. *Let $p \not\equiv \pm 4 \pmod{9}$ be a prime number. Suppose that $\beta \equiv \gamma \equiv 0 \pmod{2}$, and the class number of K is odd. Then, there exist infinitely many odd prime numbers $l \equiv 2 \pmod{3}$ such that there exist no primitive solution of $x^3 + Py^3 = l^2z^4$.*

Moreover, it is also obvious that we obtain a variant of Theorem 11.5 by combining Corollary 11.4 and appropriate prime generating polynomials. For instance, if $p \equiv \pm 1 \pmod{3}$, then by taking $f(X, Y) = P(3PX \mp 1)^3 + (3PY + 1)^3$ and $g(X, Y) = P(3PX \pm 1)^3 + (3PY + 3)^3$ in place of f and g in the proof of Theorem 9.1, and $b_0 = l^2 + 3Pb$ in place of $b_0 = l + 6b$, we obtain the following. [13]

Theorem 11.5. *Let $n \in \mathbb{Z}_{\geq 8}$ be an integer such that $n \equiv 0 \pmod{4}$, and p be as in Corollary 11.4. Then, there exist infinitely many $(n-6)/2$-tuples of pairs of integers (b_j, c_j) $(1 \leq j \leq (n-6)/2)$ such that for each tuple there exist infinitely many prime numbers l and infinitely many pairs of integers (b_0, c_0) such that the equation*

$$(X^3 + PY^3)(b_0X^3 - lc_0Y^3) \prod_{j=1}^{(n-6)/2} (b_j^2X^2 + b_jc_jXY + c_j^2Y^2) = l^2Z^n \tag{11}$$

define non-singular plane curves which violate the local-global principle. Moreover, for each n, there exist infinitely many such curves geometrically non-isomorphic to each other.

[13] In fact, if $p \equiv 1 \pmod{3}$, then the original f and g, namely $f(X, Y) = P(3X - 1)^3 + (3Y + 1)^3$ and $g(X, Y) = P(3X + 1)^3 + (3Y + 3)^3$ with $b_0 = l^2 + 6b$ also work well. Moreover, since $b_0 = l^2 + 6b$ is odd, it is sufficient to search b_0 of the form $b_0 = 1 + 6b$ with $b \in \mathbb{Z}$, where the latter saves the cost of calculation.

12. Concrete examples of degree 8

In this section, we demonstrate that the proofs of Theorems 9.1 and 11.5 actually gives explicit equations for non-singular plane curve which violates the local-global principle. We emphasize that our construction has a character contrasted with examples obtained by Nguyen in [**50**, **51**] (cf. Theorems 2.9 and 2.10). Recall that Nguyen constructed infinitely many plane curves of even degree which violate the local-global principle but explained by the Brauer-Manin obstruction on certain hyperelliptic curves covered by the plane curves. Here, we give two concrete examples for Theorems 9.1 and 11.5 respectively, both of which are $\mathbb{Z}/4\mathbb{Z}$-coverings of hyperellitpic curves with $\mathbb{Q}$-rational points. Therefore, the violation of the local-global principle for the former plane curves cannot be explained by the Brauer-Manin obstruction on the latter hyperelliptic curves. On the other hand, we should note that Nguyen's construction in [**50**, **51**] actually gives an algebraic family of such plane curves of even degree, which has an advantage over our purely arithmetic construction.

12.1. Example for Theorem 9.1. First, we construct an example for Theorem 9.1 in the case of $n = 8$. By using $f(X, Y) = 158^2(3X + 1)^3 + (3Y + 1)^3$, we obtain a prime number $25307 = f(0, 2) = 158^2 \cdot 1^3 + 7^3$, hence $(b_1, c_1) = (1, 7)$. Note that $\gcd(P, c_1) = 1$. Moreover, by using $h(A, B) = (6A + 1)^3 + 158(6B - 1)^3$, we obtain a prime number $l = 7583 = h(-4, 1) = (-23)^3 + 158 \cdot 5^3 > \max\{79, 1, 7\}$. Finally, in order to produce the coefficients $b_0 = 7583 + 6b$ and c_0, we solve the equation

$$158^2(7583 + 6b) - 7583c_0 = \pm 3^k.$$

It has a solution $(b_0, c_0, \pm 3^k) = (671, 47^2, -3)$. Therefore, for every $m = 3, 5, 7$, the equation

$$(X^3 + 158^2Y^3)(671X^3 + 7583 \cdot 47^2Y^3)(X^2 + 7XY + 7^2Y^2) = 7583^m Z^8$$

defines a non-singular plane curve which violates the local-global principle. However, its quotient by the automorphism $Z \to \zeta_4 Z$ gives a hyperelliptic curve defined by

$$(X^3 + 158^2Y^3)(671X^3 + 7583 \cdot 47^2Y^3)(X^2 + 7XY + 7^2Y^2) = 7583^m Z^2,$$

which has a $\mathbb{Q}$-rational point $[X : Y : Z] = [0 : 1 : 7 \cdot 158 \cdot 47/7583^{(m-1)/2}]$.

12.2. Example for Theorem 11.5. Next, we construct an example for Theorem 11.5 again for $n = 8$ and $p = 79$. By using $f(X, Y) = 158(3X - 1)^3 + (3Y + 1)^3$, we obtain a prime number 19751 $= f(2,0) = 158 \cdot 5^3 + 1^3$, hence $(b_1, c_1) = (5, 1)$. Note that $\gcd(P, c_1) = 1$. Moreover, by using $h(A,B) = (6A+1)^3 + 158(6B-1)^3$, we obtain a prime number $l = 4919 = h(-10, 2) = (-59)^3 + 158 \cdot 11^3 > \max\{79, 1, 5\}$. Then, by solving the equation

$$158(4919^2 + 6b) - 4919c_0 = \pm 3^k$$

with $b_0 = 4919^2 + 6b$, we obtain a solution $(b_0, c_0, \pm 3^k) = (271^2, 2359, -3^5)$. Therefore, the equation

$$(X^3 + 158Y^3)(271^2X^3 + 4919 \cdot 2359Y^3)(5^2X^2 + 5XY + Y^2) = 4919^2Z^8$$

defines a non-singular plane curve which violates the local-global principle. However, its quotient by the automorphism $Z \to \zeta_4 Z$ gives a hyperelliptic curve defined by

$$(X^3 + 158Y^3)(271^2X^3 + 4919 \cdot 2359Y^3)(5^2X^2 + 5XY + Y^2) = 4919^2Z^2,$$

which again has a $\mathbb{Q}$-rational point $[X : Y : Z] = [1 : 0 : 5 \cdot 271/4919]$.

Part II

Construction of quaternary forms which violate the local-global principle

13. Main theorem

The goal of §§13–18 is to prove the following theorem. As in the Part I, we should emphasize that although it is unclear from the statement, in the proof, we shall exhibit how to produce parameters in the following equations. In other words, we obtain an algorithm to produce as many as we want explicit counterexample to the local-global principle for non-singular hypersurface of $\mathbb{P}^3$ of degree d under the hypothesis that the arithmetic progression $\{1+dr\}_{r\in\mathbb{N}}$ contains a sufficiently small prime number p.

Recall that $N_{K/F} : K \to F$ denotes the norm map for every field extension K/F of finite degree. For every odd prime number p, we fix a primitive p-th root of unity in the field $\mathbb{C}$ of complex numbers and denote it by ζ_p. Moreover, for every integer d such that $p \equiv 1 \pmod{d}$, $K_{p,d}$ denotes the unique subfield of $\mathbb{Q}(\zeta_p)$ such that $[K_{p,d} : \mathbb{Q}] = d$, and set $\theta_{p,d} = N_{\mathbb{Q}(\zeta_p)/K_{p,d}}(1-\zeta_p)$. The following is our main result in the Part II.

THEOREM 13.1. *Let $d \in \mathbb{Z}_{\geq 3}$ be an integer. Then, the following statements hold.*

(1) *Suppose that d is odd. If there exists a prime number p such that $p \equiv 1 \pmod{d}$ and $p < (d+1)^2$, then there exist infinitely many integers $\beta \in \mathbb{Z}$ and infinitely many homogeneous polynomials $g(t, x_0) \in \mathbb{Z}[t, x_0]$ of degree $k = (d-1)/2$ such that, for each of them, the equation*

$$tg(t,x_0)(g(t,x_0)+\beta t^k) = N_{K_{p,d}/\mathbb{Q}}(x_0 + \theta_{p,d}x_1 + \theta_{p,d}^2 x_2)$$

defines a non-singular surface of degree d which violates the local-global principle.

(2) *Suppose that d is even. If there exists a prime number p such that $p \equiv 1 \pmod{d}$ and $p < (d/2+1)^2$, then there exist infinitely many integers $\beta \in \mathbb{Z}$ and infinitely many homogeneous polynomials $g(t, x_0) \in \mathbb{Z}[t, x_0]$ of degree $k = d/2$ such that, for each of them, the equation*

$$g(t,x_0)(g(t,x_0)+\beta t^k) = N_{K_{p,d}/\mathbb{Q}}(x_0 + \theta_{p,d}x_1 + \theta_{p,d}^2 x_2)$$

defines a non-singular surface of degree d which violates the local-global principle.

Remark 13.2. In fact, for every integer d with a prime number p satisfying the assumption, by taking a polynomial g appropriately, we can obtain non-singular curves of degree d as the hyperplane section of the above surface along $x_2 = 0$ which violate the local-global principle. This gives another conjectural uniform construction of non-singular curves which violate the local-global principle (cf. the Part I).

Remark 13.3. It is plausible that our counterexamples may be explained by the Brauer-Manin obstruction (cf. [**39**]).

The Part II is organized as follows: In the next section §14, we study the singularities on our surface or more general hypersurfaces of higher dimensions. The argument is standard one in projective algebraic geometry. In §15, we prove that our surfaces have local points by using the Hasse-Weil bound on the number of $\mathbb{F}_l$-rational points on a non-singular curve over $\mathbb{F}_l$. In §16, we construct hypersurfaces of degree d having no global points under the assumption that we have a prime number p, an integer β, and a polynomials $g = g(t, x_0)$ satisfying certain technical conditions. Our construction is based on Swinnerton-Dyer's original proof for cubic surfaces in Theorem 3.1 with a new observation on certain modulo p exponential equations. Finally, in the fourth section, we prove that the existence of desired β is reduced to the upper bound of the least prime number p in a given arithmetic progression, hence we complete the proof of Theorem 13.1.
[14]

Notation for §§13–18

For every field extension K/F of finite degree, $N_{K/F} : K \to F$ denotes the norm map. For every odd prime number p, we fix a primitive p-th root of unity in the field $\mathbb{C}$ of complex numbers and denote it by ζ_p. Moreover, for every integer d such that $p \equiv 1 \pmod{d}$, $K_{p,d}$ denotes the unique subfield of $\mathbb{Q}(\zeta_p)$ such that $[K_{p,d} : \mathbb{Q}] = d$, and set $\theta_{p,d} = N_{\mathbb{Q}(\zeta_p)/K_{p,d}}(1 - \zeta_p)$. We often abbreviate $K_{p,d}$ and $\theta_{p,d}$ to K and θ respectively if there is no fear of confusion.

14. Singularities

In this section, we consider the condition under which our hypersurface is non-singular.

Let $f(t, x_0) \in \mathbb{C}[t, x_0]$ be a polynomial such that $d := \deg(f) \geq 2$ and $f(t, 0) \neq 0$, $\theta_1, \ldots, \theta_d \in \mathbb{C}$ be non-zero distinct numbers, and $\gamma \in \mathbb{Z}_{\geq 1}$. Define a hypersurface $X_f^\gamma = X_f^\gamma(\theta_1, \ldots, \theta_d)$ of $\mathbb{P}^{\gamma+1}$ by

$$f(t, x_0) - \prod_{m=1}^{d} \sum_{i=0}^{\gamma} \theta_m^i x_i = 0.$$

Proposition 14.1. *The hypersurface X_f^γ is irreducible over $\mathbb{C}$. Moreover, the following hold.*

[14] The core of our proof of the global unsolubility is exactly the same as that given by Swinnerton-Dyer (cf. §2) although our counterexamples do not contain his counterexample itself. [15]

(1) *Suppose that $f(t,1)$ has no multiple roots. Then, X_f^γ is non-singular if $\gamma = 1, 2$, but singular on a codimension 3 locus if $\gamma \geq 3$.*

(2) *Suppose that $f(t,1)$ has a multiple root. Then, X_f^γ is non-singular if $\gamma = 1$, but singular on a codimension 2 locus for every $\gamma \geq 2$.*

Proof. First, note that since the irreducibility of X_f^γ follows from the latter statements on singularities because a reducible hypersurface of $\mathbb{P}^{\gamma+1}$ has a singular locus of codimension 2 in $\mathbb{P}^{\gamma+1}$. Therefore, it is sufficient to prove the statements on singularities.

If we set

$$M_k := \prod_{\substack{1 \leq m \leq d \\ m \neq k}} \sum_{i=0}^{\gamma} \theta_m^i x_i$$

for every k such that $1 \leq k \leq d$, then the simultaneous vanishing condition of the x_i-derivatives ($1 \leq i \leq \gamma$) of the defining polynomial of X_f^γ is given by the following linear equation of M_i:

$$\begin{pmatrix} \theta_1 & \theta_2 & \dots & \theta_d \\ \theta_1^2 & \theta_2^2 & \dots & \theta_d^2 \\ \vdots & \vdots & & \vdots \\ \theta_1^d & \theta_2^d & \dots & \theta_d^d \end{pmatrix} \begin{pmatrix} M_1 \\ M_2 \\ \vdots \\ M_d \end{pmatrix} = 0. \tag{12}$$

On the other hand, since we assume that θ_m ($1 \leq m \leq d$) are non-zero complex numbers distinct to each other, the Vandermonde determinant (up to the non-zero factor $\theta_1 \cdots \theta_d$)

$$\det \begin{pmatrix} \theta_1 & \theta_2 & \dots & \theta_d \\ \theta_1^2 & \theta_2^2 & \dots & \theta_d^2 \\ \vdots & \vdots & & \vdots \\ \theta_1^d & \theta_2^d & \dots & \theta_d^d \end{pmatrix} = \theta_1 \cdots \theta_d \cdot (-1)^{\frac{d(d-1)}{2}} \prod_{1 \leq l < m \leq d} (\theta_l - \theta_m)$$

does not vanish. Therefore, eq. (12) implies that $M_k = 0$ for every k and that X_f^γ is non-singular outside the linear subspaces of $\mathbb{P}^{\gamma+1}$ of codimension 2 defined by

$$\sum_{i=0}^{\gamma} \theta_l^i x_i = \sum_{i=0}^{\gamma} \theta_m^i x_i = 0 \quad (1 \leq l < m \leq d).$$

In particular, X_f^γ is non-singular outside the locus where $f(t, x_0) = 0$.

If $f(t,1)$ has no multiple root, then the only intersection of $(\partial f/\partial t)(t, x_0) = 0$ and $f(t, x_0) = 0$ is the locus where $t = x_0 = 0$. Hence, X_f^γ is non-singular outside the following codimensional 3 loci:

$$t = x_0 = \sum_{i=1}^{\gamma} \theta_l^i x_i = \sum_{i=1}^{\gamma} \theta_m^i x_i = 0 \quad (1 \leq l < m \leq d).$$

Conversely, these codimension 3 loci on X_f^γ are exactly its singular loci.

On the other hand, if $f(t,1)$ has a multiple root which defines a hyperplane $t + \alpha x_0 = 0$, then the above argument works if we replace $t = x_0 = 0$ to $t + \alpha x_0 = 0$. In particular, the singular loci of X_f^γ are codimension 2 loci given by

$$t + \alpha x_0 = \sum_{i=0}^{\gamma} \theta_l^i x_i = \sum_{i=0}^{\gamma} \theta_m^i x_i = 0 \quad (1 \leq l < m \leq d).$$

This completes the proof. □

Remark 14.2. As a consequence of Proposition 14.1, the hypersurface X_f^γ is singular whenever $\gamma \geq 3$. On the other hand, it is known (cf. [**54**, Proposition A.1]) that there is no Brauer-Manin obstruction on every non-singular complete intersection X of dimension ≥ 3 of a projective space because the natural morphism $H^2_{et}(\mathrm{Spec}(\mathbb{Q}), \mathbb{G}_m) \to H^2_{et}(X, \mathbb{G}_m)$ is isomorphic (especially surjective). This difficulty for construction of higher dimensional non-singular (Fano) hypersurface associated with norm form may be explained by the conjecture that the violation of the local-global principle for rationally connected varieties of dimension larger than or equal to 3 are explained only by the Brauer-Manin obstruction. For this topic, see e.g. [**18**] and [**54**, Remark 3.3 and Appendix A].

Remark 14.3. If f has a multiple root of multiplicity m, then the local analytic model corresponding this multiple root is given

$$x^m = (w_1^2 + w_2^2) \prod_{i=3}^{\gamma} w_i$$

In particular, if $\gamma = 2$, then this is the rational double singularity of type A_{m-1}.

15. Local solubility

In this section, we prove the following theorem, which implies that our surfaces in Theorem 13.1 have $\mathbb{R}$- and $\mathbb{Q}_l$-rational points for every prime number l.

Proposition 15.1. *Let $d \in \mathbb{Z}_{\geq 2}$ and p be a prime number such that $p \equiv 1 \pmod{d}$. Let $k, n \in \mathbb{Z}_{\geq 1}$ and $m \in \mathbb{Z}_{\geq 0}$ such that $d = m + k(n+1)$. Let $\beta \in \mathbb{Z}$ and $g = \sum_{i=0}^{k} \alpha_i t^{k-i} x_0^i \in \mathbb{Z}[t, x_0]$ be homogeneous polynomials of degrees k. Let S be the algebraic surface defined* *by*

$$f(t,x_0,x_1,x_2) := t^m g(t,x_0)(g(t,x_0)^n + \beta t^{kn}) - N_{K_{p,d}/\mathbb{Q}}(x_0 + \theta_{p,d}x_1 + \theta_{p,d}^2 x_2) = 0.$$

Assume that

(1) $\alpha_0(\alpha_0^n + \beta)$ *is divisible by every prime number smaller than* $(d-1)^2(d-2)^2$ *except for* p.

(2) *The polynomial* $f(t,1,0,0) - 1 \pmod{p}$ *has a simple root in* $\mathbb{F}_p$.

(3) $\gcd(\alpha_0, \beta) = \gcd(\alpha_1, \alpha_0(\alpha_0^n + \beta)) = 1$.

Then, S *has a* $\mathbb{Q}_l$*-rational point for every prime number* l*. Moreover, if* $\alpha_0(\alpha_0^n + \beta) > 0$*, then* S *has an* $\mathbb{R}$*-rational point.*

Proof. First, note that S has a $\mathbb{Q}_l$-rational point whenever l satisfies $l \geq (d-1)^2(d-2)^2$ and $\gcd(l, p\alpha_0(\alpha_0^n+\beta)) = 1$: Indeed, since the hyperplane section of S by $x_0 = 0$ defines a non-singular curve of genus $(1/2)(d-1)(d-2)$ over $\mathbb{F}_l$ (cf. Proposition 14.1), the Hasse-Weil bound (cf. [**6**], [**66**]) ensures that it has an $\mathbb{F}_l$-rational point. Therefore, Hensel's lemma (Theorem 19.1) ensures that S has a $\mathbb{Q}_l$-rational point. Thus, it is sufficient to consider the cases where $l < (d-1)^2(d-2)^2$ or l divides $p\alpha_0(\alpha_0^n + \beta)$. The first case is included in the second case by our assumption.

Suppose that $l \neq p$ divides α_0. Then, since $\gcd(l, \alpha_1) = \gcd(\alpha_0, \alpha_1) = 1$, $\gcd(l, \beta) = \gcd(\alpha_0, \beta) = 1$, and $d \geq 2$, the polynomial

$$f(1, x_0, 0, 0) \equiv \alpha_1 \beta x_0 + (\text{higher degree terms}) \pmod{l}$$

in $\mathbb{F}_l[x_0]$ has a simple root $x_0 = 0$. Therefore, Hensel's lemma ensures that S has a $\mathbb{Q}_l$-rational point. The case where l divides $\alpha_0^n + \beta$ is similar.

Suppose that $l = p$. Then, by the assumption, the polynomial $f(t,1,0,0) - 1 \pmod{p}$ has a simple root. Therefore, by Hensel's lemma, S has a $\mathbb{Q}_p$-rational point.

Finally, for $\mathbb{R}$-rational points, it is sufficient to note that S has an $\mathbb{R}$-point $[t : x_0 : x_1 : x_2] = [1 : 0 : (\alpha_0(\alpha_0^n + \beta)p^{-1})^{1/d} : 0]$. This completes the proof. □

We can also prove the following refinement to the hyperplane section of the above surface S along $x_2 = 0$, which is helpful when we construct non-singular plane curves which violate the local-global principle.

Proposition 15.2. *Let* $d \in \mathbb{Z}_{\geq 2}$ *and* p *be a prime number such that* $p \equiv 1 \pmod{d}$*. Let* $k, m, n \in \mathbb{Z}_{\geq 1}$ *such that* $d = m + k(n+1)$*. Let* $\beta \in \mathbb{Z}$ *and* $g = \sum_{i=0}^{k} \alpha_i t^{k-i} x_0^i \in \mathbb{Z}[t, x_0]$ *be homogeneous polynomials of degrees* k *such that* $t^m g(t,1)(g(t,1)^n + \beta t^{kn})$ *has no multiple* *roots. Let C be the algebraic curve defined by*

$$f(t,x_0,x_1) := t^m g(t,x_0)(g(t,x_0)^n + \beta t^{kn}) - N_{K_{p,d}/\mathbb{Q}}(x_0 + \theta_{p,d}x_1) = 0.$$

Assume that

(1) *$\alpha_0(\alpha_0^n + \beta)$ is divisible by every prime number smaller than $(d-1)^2(d-2)^2$ except for p and every prime number at which C has bad reduction except for p.*

(2) *The polynomial $f(t,1,0) \pmod p$ has a simple root in $\mathbb{F}_p$.*

(3) *$\gcd(\alpha_0, \beta) = \gcd(\alpha_1, \alpha_0(\alpha_0^n + \beta)) = 1$.*

Then, C has a $\mathbb{Q}_l$-rational point for every prime number l. Moreover, if $\alpha_0(\alpha_0^n + \beta) > 0$, then C has an $\mathbb{R}$-rational point.

Since we can apply the Hasse-Weil bound for prime numbers prime to $\alpha_0(\alpha_0^n+\beta)$, we can prove Proposition 15.2 by a completely parallel manner to the proof of Proposition 15.1.

16. Global unsolubility

In this section, we prove the following theorem, which implies that our hypersurface in Theorem 13.1 have no $\mathbb{Q}$-rational points if the degree d of our hypersurface is even and the defining polynomial satisfies certain technical conditions. These technical conditions are reduced to the size of a prime number p in the next section.

Theorem 16.1. *Let $d \in \mathbb{Z}_{\geq 2}$ and p be a prime number such that $p \equiv 1 \pmod d$. Let $k, n \in \mathbb{Z}_{\geq 1}$ such that $d = k(n+1)$, and take a generator ξ of $(\mathbb{Z}/p\mathbb{Z})^\times$. Let $\beta \in \mathbb{Z}$ and $g = \sum_{i=0}^{k} \alpha_i t^{k-i} x_0^i \in \mathbb{Z}[t, x_0]$ be a homogeneous polynomial of degree k satisfying the following properties:*

(1) $\gcd(p, \alpha_0(\alpha_0^n + \beta)) = 1$. [16]

(2) *Every prime divisor of β is totally inert in $K_{p,d}/\mathbb{Q}$ and prime to α_0.*

(3) *α_k is divisible by p and every prime divisor of α_k except for p is totally inert in $K_{p,d}/\mathbb{Q}$.*

(4) *There exist no integers $a, b, c \in \mathbb{Z}$ such that $(\pm\xi^d)^a - (\pm\xi^d)^b \equiv \beta\xi^{kc} \pmod p$.*

Then, the projective hypersurface of degree d defined by

$$g(t,x_0)(g(t,x_0)^n + \beta t^{kn}) - N_{K_{p,d}/\mathbb{Q}}\left(\sum_{i=0}^{d-1} \theta_{p,d}^i x_i\right) = 0$$

has no $\mathbb{Q}$-rational points.

[16] In fact, the condition $v_p(\alpha(\alpha^n + 1)) \equiv 0 \pmod d$ is sufficient.

Proof. We prove our assertion by contradiction. Suppose that our hypersurface has a $\mathbb{Q}$-rational point $[t : x_0 : \cdots : x_{d-1}] \neq [0 : 0 : \cdots : 0]$.

First, we prove that $t \neq 0$ by contradiction. Suppose that $t = 0$. Then, since we assume that α_k is divisible by p, we have

$$p^2 M x_0^d = N_{K/\mathbb{Q}} \left(x_0 + \theta \sum_{i=1}^{d-1} \theta^{i-1} x_i \right)$$

with some non-zero integer M. We may assume that $x_i \in \mathbb{Z}$ $(0 \leq i \leq d-1)$ and $\gcd(x_0, \ldots, x_{d-1}) = 1$. Then, since

$$N_{K/\mathbb{Q}}(\theta) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 - \zeta_p) = p,$$

we can check that each x_i $(i \geq 0)$ is divisible by p by induction on i. However, it contradicts that $\gcd(x_0, \ldots, x_{d-1}) = 1$. Therefore, $t \neq 0$ as claimed.

Moreover, we can prove also that $x_0 \neq 0$ by a similar manner by noting the assumption that $\gcd(p, \alpha_0(\alpha_0^n + \beta)) = 1$. Therefore, we may assume that t and x_0 are coprime integers by multiplying simultaneously $t, x_0, ..., x_{d-1}$ by a suitable rational number. Here, note that $x_1, ..., x_{d-1}$ are not necessarily integers, but $\sum_{i=0}^{d-1} \theta^i x_i$ is an algebraic integer in K.

Next, we prove that $\sum_{i=0}^{d-1} \theta^i x_i$ is prime to p by contradiction. Suppose that it is divisible by p. Then, since $\sum_{i=0}^{d-1} \theta^i x_i$ is an algebraic integer in K, we see that the (additive) θ-adic valuation of $\sum_{i=0}^{d-1} \theta^i x_i$ is non-negative. In particular, $x_1, ..., x_{d-1}$ are θ-adic integers, and x_0 is divisible by p. Moreover, since we assume that $\gcd(p, \alpha_0(\alpha_0^n + \beta)) = 1$, we see that t is also divisible by p. However, it contradicts that $\gcd(t, x_0) = 1$. Therefore, $\sum_{i=0}^{d-1} \theta^i x_i$ is prime to p as claimed.

Moreover, we can prove that $\gcd(g(t, x_0), \beta) = 1$ by contradiction. Suppose that a prime divisor q of β divides $g(t, x_0)$. Set $v = \min_{0 \leq i \leq d-1}(v_q(x_i))$. If $v \geq 0$, then we have $N_{K/\mathbb{Q}}(\sum_{i=0}^{d-1} \theta^i x_i) \equiv 0 \pmod{q}$ with q-adic integers $x_0, \ldots, x_{d-1}$. Since we assume that q is totally inert in $K/\mathbb{Q}$, $(\theta^i \pmod{q})_{0 \leq i \leq d-1}$ forms an $\mathbb{F}_q$-basis of $\mathbb{F}_q(\theta \pmod{q})$. Therefore, we have $x_0 \equiv \cdots \equiv x_{d-1} \equiv 0 \pmod{q}$, hence $\alpha_0^2 t^d \equiv 0 \pmod{q}$. On the other hand, we know that $\gcd(\alpha_0, \beta) = 1$ and $\gcd(t, x_0) = 1$, a contradiction. If $v < 0$, then we have $\sum_{i \geq 0} \theta^i (q^{-v} x_i) \equiv 0 \pmod{q^{1-v}}$ with q-adic integers $q^{-v}x_0, \ldots, q^{-v}x_{d-1}$. Therefore, we have $q^{-v}x_i \equiv 0 \pmod{q}$, i.e., $v_q(x_i) \geq v + 1$ for each i, a contradiction.

In exactly similar manner, we can prove also that $\gcd(t, \alpha_k) = 1$ by contradiction. As a consequence, we have

$$\gcd(g(t, x_0), g(t, x_0)^n + \beta t^{kn}) = \gcd(g(t, x_0), \beta t^{kn}) = \gcd(g(t, x_0), \beta) \gcd(\alpha_k x_0, t) = 1.$$

On the other hand, since the product of $g(t,x_0)$ and $g(t,x_0)^n+\beta t^{kn}$ is a norm of an algebraic integer $\sum_{i=0}^{d-1}\theta^i x_i$ prime to p, each of themselves is the absolute value of the norm of an integral ideal of K prime to p up to signature. By Corollary 21.2, we have

$$g(t,x_0), g(t,x_0)^n+\beta t^{kn}\equiv\pm 1 \quad \text{in } (\mathbb{Z}/p\mathbb{Z})^\times/\langle\xi^d\rangle.$$

Therefore, we see that there exist some $a,b,c\in\mathbb{Z}$ such that

$$(\pm\xi^d)^a-(\pm\xi^d)^{bn}\equiv(g(t,x_0)^n+\beta t^{kn})-g(t,x_0)^n=\beta t^{kn}\equiv\beta(\xi^c)^{kn}\pmod p,$$

which contradicts the assumption. This completes the proof. □

Remark 16.2. We use the condition $\gcd(\alpha_0,\beta)=1$ for the validity of $\gcd(g(t,x_0),\beta)=1$. On the other hand, we have also used the same condition in the proof of Proposition 15.1 for the validity of $\pmod l$-solubility of our hypersurface for small prime numbers l.

In the setting of Theorem 16.1, assume further that $(p-1)/k$ is even. For example, this is the case when $n=1$. Then, we see that $-1\pmod p\in\langle\xi^k\rangle$, hence $\pm\xi^d\pmod p\in\langle\xi^k\rangle$. In particular, there exist no integers $a,b,c\in\mathbb{Z}$ such that

$$(\pm\xi^d)^a-(\pm\xi^d)^b\equiv\beta\xi^{kc}\pmod p$$

if there exist no integers $a,b\in\mathbb{Z}$ such that

$$\xi^{ka}+\xi^{kb}\equiv\beta\pmod p.$$

By noting this fact and Proposition 15.1, we obtain the following:

Corollary 16.3. *Let $d=2k\in\mathbb{Z}_{\geq 4}$ and p be a prime number such that $p\equiv 1\pmod d$. Take a generator ξ of $(\mathbb{Z}/p\mathbb{Z})^\times$. Let $\beta\in\mathbb{Z}$ and $g=\sum_{i=0}^k\alpha_i t^{k-i}x_0^i\in\mathbb{Z}[t,x_0]$ be a homogeneous polynomial of degree k satisfying the following properties:*

(1) *Every prime divisor of β is larger than $(d-1)^2(d-2)^2$ and totally inert in $K_{p,d}/\mathbb{Q}$.*
(2) *α_0 is divisible by every prime number $q<(d-1)^2(d-2)^2$ except for p, and α_0 is prime to β.*
(3) *$\alpha_0(\alpha_0+\beta)$ is positive and prime to α_1.*
(4) *α_k is divisible by p and every prime divisor of α_k except for p is totally inert in $K_{p,d}/\mathbb{Q}$.*
(5) *$g(t,1)(g(t,1)+\beta t^k)-1\pmod p$ has a simple root in $\mathbb{F}_p$.*
(6) *There exist no integers $a,b\in\mathbb{Z}$ such that $\xi^{ka}+\xi^{kb}\equiv\beta\pmod p$.*

Then, the projective hypersurface of degree d defined by

$$g(t,x_0)(g(t,x_0)+\beta t^k) - N_{K_{p,d}/\mathbb{Q}}\left(\sum_{i=0}^{d-1}\theta_{p,d}^i x_i\right) = 0$$

has local points but no $\mathbb{Q}$-rational points, i.e., violates the local-global principle.

Remark 16.4. In fact, the above corollary is TRUE also for $d=2$. In this case, we must take $k=1$, however, we cannot find β such that there exist no integers $a,b\in\mathbb{Z}$ such that $\xi^a+\xi^b\equiv\beta \pmod{p}$. More precisely, there exist no integers $a,b,c\in\mathbb{Z}$ such that $(\pm\xi^2)^a-(\pm\xi^2)^b\equiv\beta\xi^c \pmod{p}$ because $\beta\xi^c \pmod{p}$ attains arbitrary values in $\mathbb{F}_p^\times$.

On the other hand, we can prove also the following theorem, which implies that our hypersurface in Theorem 13.1 have no $\mathbb{Q}$-rational points if the degree d of our hypersurface is even and the defining polynomial satisfies certain technical conditions.

Theorem 16.5. *Let $d\in\mathbb{Z}_{\geq 3}$ and p be a prime number such that $p\equiv 1 \pmod{d}$. Let $k,n\in\mathbb{Z}_{\geq 1}$ such that $d=1+k(n+1)$, and take a generator ξ of $(\mathbb{Z}/p\mathbb{Z})^\times$. Let $\beta\in\mathbb{Z}$ and $g=\sum_{i=0}^k\alpha_i t^{k-i}x_i\in\mathbb{Z}[t,x_0]$ be a homogeneous polynomial of degree k satisfying the following properties:*

1. $\gcd(p,\alpha_0(\alpha_0^n+\beta))=1$. [17]
2. *Every prime divisor of β is totally inert in $K_{p,d}/\mathbb{Q}$ and prime to α_0.*
3. *Every prime divisor of α_k is equal to p or totally inert in $K_{p,d}/\mathbb{Q}$.*
4. *There exist no integers $a,b\in\mathbb{Z}$ such that $(\pm\xi^d)^a-(\pm\xi^d)^b\equiv\beta \pmod{p}$.*

Then, the projective hypersurface defined by

$$tg(t,x_0)(g(t,x_0)^n+\beta t^{kn}) - N_{K_{p,d}/\mathbb{Q}}\left(\sum_{i=0}^{d-1}\theta_{p,d}^i x_i\right)$$

has no $\mathbb{Q}$-rational points.

Proof. The proof is completely parallel except for the last step. In this time, we do not need to assume that α_k is divisible by p thanks to the factor t in the first summand of the defining polynomial of our hypersurface.

We prove our assertion by contradiction. Suppose that our hypersurface has a $\mathbb{Q}$-rational point $[t:x_0:\cdots:x_{d-1}]\neq[0:0:\cdots:0]$.

[17] Again, the condition $v_p(\alpha(\alpha^n+1))\equiv 0 \pmod{d}$ is sufficient.

First, we prove that $t \neq 0$ by contradiction. Suppose that $t = 0$. Then, we have

$$0 = N_{K/\mathbb{Q}}\left(\sum_{i=0}^{d-1} \theta^i x_i\right).$$

Since $(\theta^i)_{0 \leq i \leq d-1}$ forms a $\mathbb{Q}$-basis of K, we see that $x_0 = \cdots = x_{d-1} = 0$, a contradiction.

Moreover, we can prove also that $x_0 \neq 0$ again by contradiction. Suppose that $x_0 = 0$. Then, we have

$$\alpha_0(\alpha_0^n + \beta)t^d = N_{K/\mathbb{Q}}\left(\theta \sum_{i=1}^{d-1} \theta^{i-1} x_i\right).$$

We may assume that $t, x_i \in \mathbb{Z}$ $(1 \leq i \leq d-1)$ and $\gcd(t, x_1, \ldots, x_{d-1}) = 1$. Then, since

$$N_{K/\mathbb{Q}}(\theta) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1 - \zeta_p) = p,$$

and we assume that $\gcd(p, \alpha_0(\alpha_0^n + \beta)) = 1$, we see that t is divisible by p. Hence, we can check that each x_i $(i \geq 1)$ is divisible by p by induction on i. However, it contradicts that $\gcd(t, x_0, \ldots, x_{d-1}) = 1$.

Therefore, we may assume that t and x_0 are coprime integers by multiplying simultaneously $t, x_0, ..., x_{d-1}$ by a suitable rational number. Here, note that $x_1, ..., x_{d-1}$ are not necessarily integers, but $\sum_{i=0}^{d-1} \theta^i x_i$ is an algebraic integer in K.

Next, we prove that $\sum_{i=0}^{d-1} \theta^i x_i$ is prime to p by contradiction. Suppose that it is divisible by p. Then, since $\sum_{i=0}^{d-1} \theta^i x_i$ is an algebraic integer in K,, we see that the (additive) θ-adic valuation of $\sum_{i=0}^{d-1} \theta^i x_i$ is non-negative. In particular, $x_1, ..., x_{d-1}$ are θ-adic integers, and x_0 is divisible by p. Moreover, since we assume that $\gcd(p, \alpha_0(\alpha_0^n + \beta)) = 1$, we see that t is also divisible by p. However, it contradicts that $\gcd(t, x_0) = 1$. Therefore, $\sum_{i=0}^{d-1} \theta^i x_i$ is prime to p as claimed.

Moreover, we can prove that $\gcd(g(t, x_0), \beta) = 1$ by contradiction. Suppose that a prime divisor q of β divides $g(t, x_0)$. Set $v = \min_{0 \leq i \leq d-1}(v_q(x_i))$. If $v \geq 0$, then we have $N_{K/\mathbb{Q}}(\sum_{i=0}^{d-1} \theta^i x_i) \equiv 0 \pmod{q}$ with q-adic integers $x_0, \ldots, x_{d-1}$. Since we assume that q is totally inert in $K/\mathbb{Q}$, $(\theta^i \pmod{q})_{0 \leq i \leq d-1}$ forms an $\mathbb{F}_q$-basis of $\mathbb{F}_q(\theta \pmod{q})$. Therefore, we have $x_0 \equiv \cdots \equiv x_{d-1} \equiv 0 \pmod{q}$, hence $\alpha_0^2 t^d \equiv 0 \pmod{q}$. On the other hand, we know that $\gcd(\alpha_0, \beta) = 1$ and $\gcd(t, x_0) = 1$, a contradiction. If $v < 0$, then we have $\sum_{i \geq 0} \theta^i (q^{-v} x_i) \equiv 0 \pmod{q^{1-v}}$ with q-adic integers $q^{-v}x_0, \ldots, q^{-v}x_{d-1}$. Therefore, we have $q^{-v}x_i \equiv 0 \pmod{q}$, i.e., $v_q(x_i) \geq v + 1$ for each i, a contradiction.

In exactly similar manner, we can prove also that $\gcd(t, \alpha_k) = 1$. As a consequence, we have

$$\gcd(t, g(t, x_0)^n + \beta t^{kn}) = \gcd(t, g(t, x_0)) = \gcd(t, \alpha_k) = 1,$$

and

$$\gcd(g(t, x_0), g(t, x_0)^n + \beta t^{kn}) = \gcd(g(t, x_0), \beta t) = \gcd(g(t, x_0), \beta) \gcd(\alpha_k x_0, t) = 1.$$

On the other hand, since the product of t, $g(t, x_0)$, and $g(t, x_0)^n + \beta t^{kn}$ is a norm of an algebraic integer $\sum_{i=0}^{d-1} \theta^i x_i$ prime to p, each of themselves is the (absolute) norm of an integral ideal of K prime to p up to signature. By Corollary 21.2, we have

$$t, g(t, x_0), g(t, x_0)^n + \beta t^{kn} \equiv \pm 1 \quad \text{in } (\mathbb{Z}/p\mathbb{Z})^\times / \langle \xi^d \rangle.$$

Therefore, we see that there exist some $a, b, c \in \mathbb{Z}$ such that

$$(\pm \xi^d)^a - (\pm \xi^d)^{bn} \equiv (g(t, x_0)^n + \beta t^{kn}) - g(t, x_0)^n = \beta t^{kn} \equiv \beta (\pm \xi^d)^{knc} \pmod{p},$$

which contradicts the assumption. This completes the proof. □

In the setting of Theorem 16.5, assume further that $(p-1)/d$ is even. For example, this is the case when d is odd. Then, we see that $-1 \pmod{p} \in \langle \xi^d \rangle$. In particular, there exist no integers $a, b, c \in \mathbb{Z}$ such that

$$(\pm \xi^d)^a - (\pm \xi^d)^b \equiv \beta \pmod{p}$$

if there exist no integers $a, b \in \mathbb{Z}$ such that

$$\xi^{da} + \xi^{db} \equiv \beta \pmod{p}.$$

By noting this fact and Proposition 15.1, we obtain the following:

Corollary 16.6. *Let $d = 2k + 1 \in \mathbb{Z}_{\geq 3}$ and p be a prime number such that $p \equiv 1 \pmod{d}$. Take a generator ξ of $(\mathbb{Z}/p\mathbb{Z})^\times$. Let $\beta \in \mathbb{Z}$ and $g = \sum_{i=0}^{k} \alpha_i t^{k-i} x_0^i \in \mathbb{Z}[t, x_0]$ be a homogeneous polynomial of degree k satisfying the following properties:*

1. *Every prime divisor of β is larger than $(d-1)^2(d-2)^2$ and totally inert in $K_{p,d}/\mathbb{Q}$.*
2. *α_0 is divisible by every prime number $q < (d-1)^2(d-2)^2$ except for p, and α_0 is prime to β.*
3. *$\alpha_0(\alpha_0 + \beta)$ is positive and prime to α_1.*
4. *Every prime divisor of α_k is equal to p or totally inert in $K_{p,d}/\mathbb{Q}$.*
5. *$tg(t, 1)(g(t, 1) + \beta t^k) - 1 \pmod{p}$ has a simple root in $\mathbb{F}_p$.*
6. *There exist no integers $a, b \in \mathbb{Z}$ such that $\xi^{da} + \xi^{db} \equiv \beta \pmod{p}$.*

Then, the projective hypersurface of degree d defined by

$$tg(t,x_0)(g(t,x_0)+\beta t^k) - N_{K_{p,d}/\mathbb{Q}}\left(\sum_{i=0}^{d-1}\theta_{p,d}^i x_i\right) = 0$$

has local points but no $\mathbb{Q}$-rational points, i.e., violates the local-global principle.

Remark 16.7. In fact, the whole of the arguments in this section works also if we replace p to its power p^r with $r \geq 1$ and take d as a positive divisor of $(p-1)p^{r-1}$.

17. Reduction to small prime numbers in arithmetic progressions

In this section, we reduce the technical conditions in Theorems 16.1 and 16.5 to the estimate of the prime numbers of the form $p \equiv 1 \pmod{d}$. For this purpose for even d, it is sufficient to prove the following theorem. For odd d, see Theorem 17.2.

Theorem 17.1. *Let $k \in \mathbb{Z}_{\geq 2}$. Suppose that there exists a prime number p and an integer β satisfying the following conditions:*

(1) $p \equiv 1 \pmod{2k}$.

(2) *Every prime divisor of β is larger than $(2k-1)^2(2k-2)^2$ and totally inert in $K_{2k}/\mathbb{Q}$.*

(3) *β^2+4 is a quadratic residue modulo p.*

(4) *There exist no integers $a, b \in \mathbb{Z}$ such that $\xi^{ka}+\xi^{kb} \equiv \beta \pmod{p}$.*

Then, there exist infinitely many homogeneous polynomials $g(t,x_0) \in \mathbb{Z}[t,x_0]$ of degree k such that the equation

$$g(t,x_0)(g(t,x_0)+\beta t^k) = N_{K_{2k}/\mathbb{Q}}(x_0+\theta x_1+\theta^2 x_2)$$

defines a non-singular surface of degree $2k$ over $\mathbb{Q}$ which violates the local-global principle. In particular, the above conclusion holds if there exists a prime number p such that $p \equiv 1 \pmod{2k}$ and $p < (k+1)^2$.

Proof. For the given β, define

$$\tilde{A} := \left\{\alpha \in \mathbb{Z}\setminus p\mathbb{Z} \mid \alpha \equiv 0 \pmod{l} \text{ for every prime number } l < (2k-1)^2(2k-2)^2 \text{ except for } p\right\},$$

$$A_\beta := \left\{\alpha \in \tilde{A} \;\middle|\; \gcd(\alpha,\beta)=1 \text{ and } \alpha \not\equiv -\beta \pmod{p}\right\}.$$

Then, since $p < (d-1)^2(d-2)^2$, there is a prime number l which is smaller than $(d-1)^2(d-2)^2$ totally inert in $K_{p,d}/\mathbb{Q}$. Hence, we see that $A_\beta \pmod{p} = \mathbb{F}_p^\times \setminus \{-\beta \pmod{p}\}$. For arbitrary $\alpha_0 \in A_\beta$, we can take $\alpha_1, \alpha_k \in \mathbb{Z}$ so that $\alpha_0(\alpha_0+\beta) > 0$, $\gcd(\alpha_1, \alpha_0(\alpha_0+\beta)) = 1$, and α_k is a power of the prime number p. Conversely, every such triple $(\alpha_0, \alpha_1, \alpha_k)$ with the given β satisfies the conditions (1), (2), (3), (4), and (6) in Corollary 16.3.

For the validity the condition (5), we take $\alpha_1, \ldots, \alpha_k$ from $p\mathbb{Z}$. This is possible because the only constraint for $\alpha_0, \alpha_1, \ldots, \alpha_k \pmod p$ is that $\alpha_0(\alpha_0 + \beta) \not\equiv 0 \pmod p$, which follows from the definition of A_β. For every $\alpha_1, \ldots, \alpha_k \in p\mathbb{Z}$ satisfying the conditions so far, we can check that, for every $\alpha_0 \in A_\beta$ such that $\alpha_0 \equiv (-\beta \pm \sqrt{\beta^2 + 4})/2 \pmod p$, the polynomial $g(t, 1)(g(t, 1) + \beta t^k) - 1 \equiv \alpha_0(\alpha_0 + \beta)t^d - 1 \pmod p$ has a simple root $t = 1$ in $\mathbb{F}_p$. Since p is odd, we have $(-\beta \pm \sqrt{\beta^2 + 4})/2 \not\equiv -\beta \pmod p$. Therefore, the above choice of $\alpha_0 \in A_\beta$ is actually possible.

Finally, we consider the condition on the non-singularity of our surface. In view of Proposition 14.1, it is sufficient to take $\alpha_0, \ldots, \alpha_k$ so that for some sufficiently large prime numbers q_1 and q_2, the two polynomials $g(t, x_0) \pmod{q_1}$ and $g(t, x_0) + \beta t^k \pmod{q_2}$ are separable. In fact, this is possible by the Chinese remainder theorem, and the fact that $g(t, x_0)$ and $g(t, x_0) + \beta t^k$ has no common roots in $\mathbb{C}$ because $\alpha_k, \beta \neq 0$. This completes the proof of the former statement.

For the latter statement, set

$$\tilde{B} := \left\{ \beta \in \mathbb{Z} \;\middle|\; \begin{array}{c}\text{every prime divisor of } \beta \text{ is larger than } (2k-1)^2(2k-2)^2 \\ \text{and totally inert in } K_{p,d}/\mathbb{Q}\end{array} \right\},$$
$$B := \left\{ \beta \in \tilde{B} \;\middle|\; \text{there exist no } a, b \in \mathbb{Z} \text{ such that } \xi^{ka} + \xi^{kb} \equiv \beta \pmod p \right\}.$$

Then, it is sufficient to prove that

$$\#\left(\left\{ \overline{\beta} \in \mathbb{F}_p^\times \;\middle|\; \overline{\beta}^2 + 4 \in \mathbb{F}_p^{\times 2} \cup \{0\} \right\} \cap (B \pmod p) \right) > 0.$$

Since $p < (k+1)^2$, we have $\tilde{B} \pmod p = \mathbb{F}_p^\times$, hence

$$\#(\mathbb{F}_p^\times \setminus B \pmod p) \leq \frac{1}{2} \cdot \frac{p-1}{k} \cdot \left(\frac{p-1}{k} - 1 \right).$$

On the other hand, since $(p-1)/k$ is even, and $\beta \notin B \pmod p$ if and only if $\xi^k \beta \notin B \pmod p$, the above estimate can be refined to

$$\#(\mathbb{F}_p^\times \setminus B \pmod p) \leq \frac{1}{2} \cdot \frac{p-1}{k} \cdot \left(\frac{p-1}{k} - 2 \right).$$

Since

$$\#\left\{ \overline{\beta} \in \mathbb{F}_p^\times \;\middle|\; \overline{\beta}^2 + 4 \in \mathbb{F}_p^{\times 2} \cup \{0\} \right\} = \begin{cases} \dfrac{p-1}{2} & p \equiv 1 \pmod 4 \\ \dfrac{p-3}{2} & p \equiv 3 \pmod 4 \end{cases},$$

we have an estimate

$$\#\left(\left\{\overline{\beta} \in \mathbb{F}_p^\times \;\middle|\; \overline{\beta}^2 + 4 \in \mathbb{F}_p^{\times 2} \cup \{0\}\right\} \cap \left(B \pmod p\right)\right) \geq \frac{p-3}{2} - \frac{1}{2} \cdot \frac{p-1}{k} \cdot \left(\frac{p-1}{k} - 2\right).$$

The right hand side is positive, for instance, if $k \geq 4$ and $p < k^2 + 2k - 5$. By considering another condition $p \equiv 1 \pmod{2k}$, the above condition $p < k^2 + 2k - 5$ follows from the given condition $p < (k+1)^2$ for every $k \geq 7$. Therefore, by direct calculations for $k \leq 6$, [18] we obtain the assertion for every $k \geq 2$. □

Theorem 17.2. *Let $d = 2k + 1 \in \mathbb{Z}_{\geq 5}$ with $k \in \mathbb{Z}_{\geq 2}$. Suppose that there exists a prime number p and an integer β satisfying the following conditions:*

1. *$p \equiv 1 \pmod d$.*
2. *Every prime divisor of β is larger than $(d-1)^2(d-2)^2$ and totally inert in $K_{p,d}/\mathbb{Q}$.*
3. *$\beta^2 + 4$ or $\beta^2 - 4$ is a quadratic residue modulo p.*
4. *There exist no integers $a, b \in \mathbb{Z}$ such that $\xi^{da} + \xi^{db} \equiv \beta \pmod p$.*

Then, there exist infinitely many homogeneous polynomials $g(t, x_0) \in \mathbb{Z}[t, x_0]$ of degree k such that the equation

$$tg(t, x_0)(g(t, x_0) + \beta t^k) = N_{K_{p,d}/\mathbb{Q}}(x_0 + \theta x_1 + \theta^2 x_2)$$

defines a non-singular surface of degree $d = 2k + 1$ over $\mathbb{Q}$ which violates the local-global principle. In particular, the above conclusion holds if there exists a prime number p such that $p \equiv 1 \pmod d$ and $p < (d+1)^2$.

Proof. The proof is completely parallel to the proof of Theorem 17.2.

For the given β, define

$$\tilde{A} := \left\{\alpha \in \mathbb{Z} \setminus p\mathbb{Z} \;\middle|\; \alpha \equiv 0 \pmod p \text{ for every prime number } l < (d-1)^2(d-2)^2 \text{ except for } p\right\},$$

$$A_\beta := \left\{\alpha \in \tilde{A} \;\middle|\; \gcd(\alpha, \beta) = 1 \text{ and } \alpha \not\equiv -\beta \pmod p\right\},$$

Then, since $p < (d-1)^2(d-2)^2$, there is a prime number l which is smaller than $(d-1)^2(d-2)^2$ totally inert in $K_{p,d}/\mathbb{Q}$. Hence, we see that $A_\beta \pmod p = \mathbb{F}_p^\times \setminus \{-\beta \pmod p\}$. For arbitrary $\alpha_0 \in A_\beta$, we can take $\alpha_1, \alpha_k \in \mathbb{Z}$ so that $\gcd(\alpha_1, \alpha_0(\alpha_0 + \beta)) = 1$ and α_k is a power of the prime number p. Conversely, every such triple $(\alpha_0, \alpha_1, \alpha_k)$ with the given β satisfies the conditions (1), (2), (3), (4), and (6) in Corollary 16.6.

For the validity the condition (5), we take $\alpha_1, \ldots, \alpha_k$ from $p\mathbb{Z}$. This is possible because the only constraint for $\alpha_0, \alpha_1, \ldots, \alpha_k \pmod p$ is that $\alpha_0(\alpha_0 + \beta) \not\equiv 0 \pmod p$, which

[18] For $k = 2, 3, 4, 5, 6$, we can use e.g. $(p, \beta \pmod p) = (5, 1), (13, 5), (17, 4), (11, 1), (13, 3)$ respectively.

follows from the definition of A_β. For every $\alpha_1, \dots, \alpha_k \in p\mathbb{Z}$ satisfying the conditions so far, we can check the following: Suppose that β^2+4 is a quadratic residue modulo p. Then, for every $\alpha_0 \in A_\beta$ such that $\alpha_0 \equiv (-\beta \pm \sqrt{\beta^2+4})/2 \pmod{p}$, the polynomial $tg(t,1)(g(t,1)+\beta t^k)-1 \equiv \alpha_0(\alpha_0+\beta)t^d - 1 \pmod{p}$ has a simple root $t=1$ in $\mathbb{F}_p$. Since p is odd, we have $(-\beta \pm \sqrt{\beta^2+4})/2 \not\equiv -\beta \pmod{p}$. Therefore, the above choice of $\alpha_0 \in A_\beta$ is actually possible.

The case where β^2-4 is a quadratic residue modulo p is exactly similar if we consider $t=-1$ in place of $t=1$. Here, note that d is odd.

Finally, we consider the condition on the non-singularity of our surface. In view of Proposition 14.1, it is sufficient to take $\alpha_0, \dots, \alpha_k$ so that for some sufficiently large prime numbers q_1 and q_2, the two polynomials $g(t,x_0) \pmod{q_1}$ and $g(t,x_0)+\beta t^k \pmod{q_2}$ are separable. In fact, this is possible by the Chinese remainder theorem, and the fact that $g(t,x_0)$ and $g(t,x_0)+\beta t^k$ has no common roots in $\mathbb{C}$ because $\alpha_k, \beta \neq 0$. This completes the proof of the former statement.

This completes the proof of the former statement.

For the last statement, set

$$\tilde{B} := \left\{\beta \in \mathbb{Z} \;\middle|\; \text{every prime divisor of } \beta \text{ is larger than } (d-1)^2(d-2)^2 \text{ and totally inert in } K_{p,d}/\mathbb{Q}\right\},$$
$$B := \left\{\beta \in \tilde{B} \;\middle|\; \text{there exist no } a, b \in \mathbb{Z} \text{ such that } \xi^{da}+\xi^{db} \equiv \beta \pmod{p}\right\}.$$

Then, it is sufficient to prove that

$$\#\left(\left\{\overline{\beta} \in \mathbb{F}_p^\times \;\middle|\; \overline{\beta}^2+4 \in \mathbb{F}_p^{\times 2} \cup \{0\}\right\} \cap (B \pmod{p})\right) > 0.$$

Since $p < (d+1)^2$, we have $\tilde{B} \pmod{p} = \mathbb{F}_p^\times$, hence

$$\#(\mathbb{F}_p^\times \setminus B \pmod{p}) \leq \frac{1}{2} \cdot \frac{p-1}{d} \cdot \left(\frac{p-1}{d} - 1\right).$$

On the other hand, since $(p-1)/d$ is even, and $\beta \notin B \pmod{p}$ if and only if $\xi^d\beta \notin B \pmod{p}$, the above estimate can be refined to

$$\#(\mathbb{F}_p^\times \setminus B \pmod{p}) \leq \frac{1}{2} \cdot \frac{p-1}{d} \cdot \left(\frac{p-1}{d} - 2\right).$$

Since

$$\#\left\{\overline{\beta} \in \mathbb{F}_p^\times \;\middle|\; \overline{\beta}^2+4 \in \mathbb{F}_p^{\times 2} \cup \{0\}\right\} = \begin{cases} \dfrac{p-1}{2} & p \equiv 1 \pmod{4} \\ \dfrac{p-3}{2} & p \equiv 3 \pmod{4} \end{cases},$$

we have an estimate

$$\#\left(\left\{\overline{\beta} \in \mathbb{F}_p^\times \;\middle|\; \overline{\beta}^2 + 4 \in \mathbb{F}_p^{\times 2} \cup \{0\}\right\} \cap (B \pmod p)\right) \geq \frac{p-3}{2} - \frac{1}{2} \cdot \frac{p-1}{d} \cdot \left(\frac{p-1}{d} - 2\right).$$

The right hand side is positive, for instance, if $p < d^2 + 2d - 5$. By considering another condition $p \equiv 1 \pmod d$, the above condition $p < d^2 + 2d - 5$ follows from the given condition $p < (d+1)^2$ for every $d \geq 7$. Therefore, by direct calculations for $d = 5$, [19] we obtain the assertion for every $d = 2k + 1 \geq 5$. □

18. Concrete examples of Theorem 13.1

In this section, we demonstrate that the proof of Theorem 13.1 actually gives explicit equations for non-singular plane curves which violates the local-global principle. As a demonstration, we focus on the cases of degree 4 and 5.

18.1. Example of degree 4. In this subsection, we consider the case of degree $d = 4$. In this case, we have $k = 2$.

First, we search prime numbers $p < (4/2 + 1)^2 = 9$ such that $p \equiv 1 \pmod 4$. There is only one such prime number, that is, $p = 5$. Hence, we consider the norm with respect to $K_{5,4}/\mathbb{Q} = \mathbb{Q}(\theta_{5,4})/\mathbb{Q}$ with $\theta_{5,4} = \zeta_5 = \exp(2\pi i/5)$. Moreover, we can take $\xi = 2$ as a generator of $\mathbb{F}_5^\times$.

Next, we search integers β such that $\beta^2 + 4$ is square modulo 5. This is the case if and only if $\beta \equiv 0, \pm 1 \pmod 5$. However, in order to verify the condition that there exist no integers $a, b \in \mathbb{Z}$ such that $2^{2a} + 2^{2b} \equiv \beta \pmod 5$, we should take β so that $\beta \equiv \pm 1$ $\pmod 5$. Conversely, if $\beta \equiv \pm 1 \pmod 5$, then there exist no integers $a, b \in \mathbb{Z}$ such that $2^{2a} + 2^{2b} \equiv \beta \pmod 5$. For simplicity, we take $\beta = 1$, which obviously ensures that every prime divisor of β is totally inert in $K_{5,4}/\mathbb{Q}$.

Finally, we take a polynomial $g(t, x) = \alpha_0 t^2 + \alpha_1 tx + \alpha_2 x^2 \in \mathbb{Z}[t, x]$ satisfying the following conditions:

(1) $\alpha_0 \equiv (-\beta \pm \sqrt{\beta^2 + 4})/2 \equiv 2 \pmod 5$.

(2) α_0 is divisible by every prime number $l < (4-1)^2(4-2)^2 = 36$ except for $p = 5$, i.e., divisible by $l = 2, 3, 7, 9, 11, 13, 17, 19, 23, 29, 31$.

(3) $\gcd(\alpha_1, \alpha_0(\alpha_0 + 1)) = 1$.

(4) Both of α_1 and α_2 are divisible by $p = 5$ and α_2 is a power of $p = 5$.

(5) Both of $g(t, x)$ and $g(t, , x) + t^2$ have no multiple roots.

[19] For $d = 5$, i.e., $k = 2$, we can use e.g. $(p, \beta \pmod p) = (11, 1)$.

Here, if we set N as the product of prime numbers $l < 36$ except for $p = 5$, then we have $N \equiv 4 \pmod 5$. Hence, for example, we can take $\alpha_0 = 3N \equiv 2 \pmod 5$, $\alpha_1 = \alpha_2 = 5$. Indeed, for the last condition, it is sufficient to note that both of $g(t,x)$ and $g(t,,x) + t^2$ are 5-adic Eisenstein polynomials up to 5-adic unit factor α_0. Therefore, then the quartic surface defined by the following equation violates the local-global principle:

$$(3Nt^2 + 5tx + 5x^2)((3N+1)t^2 + 5tx + 5x^2) = N_{\mathbb{Q}(\zeta_5)/\mathbb{Q}}(x + (1-\zeta_5)y + (1-\zeta_5)^2 z).$$

18.2. Example of degree 5. Next, we consider the case of degree $d = 5$.

First, we search prime numbers $p < (5+1)^2 = 36$ such that $p \equiv 1 \pmod 5$. There are two such prime numbers, that is, $p = 11, 31$. We take $p = 11$. Hence, we consider the norm with respect to $K_{11,5}/\mathbb{Q} = \mathbb{Q}(\theta_{11,5})/\mathbb{Q}$ with $\theta_{11,5} = N_{\mathbb{Q}(\zeta_{11})/K_{11,5}}(1 - \zeta_{11}) = \cos(2\pi/11)$. Moreover, we can take $\xi = 2$ as a generator of $\mathbb{F}_{11}^{\times}$.

Next, we search integers β such that $\beta^2 + 4$ is square modulo 11. This is the case if and only if $\beta \equiv 0, \pm 1, \pm 4 \pmod{11}$. However, in order to verify the condition that there exist no integers $a, b \in \mathbb{Z}$ such that $2^{5a} + 2^{5b} \equiv \beta \pmod{11}$, we should take β so that $\beta \equiv \pm 1, \pm 4 \pmod{11}$. Conversely, if $\beta \equiv \pm 1, \pm 4 \pmod{11}$, then there exist no integers $a, b \in \mathbb{Z}$ such that $2^{5a} + 2^{5b} \equiv \beta \pmod{11}$. For simplicity, we take $\beta = 1$, which obviously ensures that every prime divisor of β is totally inert in $K_{11,5}/\mathbb{Q}$.

Finally, we take a polynomial $g(t,x) = \alpha_0 t^2 + \alpha_1 tx + \alpha_2 x^2 \in \mathbb{Z}[t,x]$ satisfying the following conditions:

1. $\alpha_0 \equiv (-\beta \pm \sqrt{\beta^2 + 4})/2 \equiv 3, 7 \pmod{11}$.
2. α_0 is divisible by every prime number $l < (5-1)^2(5-2)^2 = 144$ except for $p = 11$.
3. $\gcd(\alpha_1, \alpha_0(\alpha_0 + 1)) = 1$.
4. Both of α_1 and α_2 are divisible by $p = 11$ and α_2 is a power of $p = 11$.
5. Both of $g(t,x)$ and $g(t,,x) + t^2$ have no multiple roots.

Here, if we set N as the product of prime numbers $l < 144$ except for $p = 11$, then we have $N \equiv 4 \pmod{11}$. Hence, for example, we can take $\alpha_0 = 9N \equiv 3 \pmod{11}$, $\alpha_1 = \alpha_2 = 11$. Indeed, for the last condition, it is sufficient to note that both of $g(t,x)$ and $g(t,,x) + t^2$ are 11-adic Eisenstein polynomials up to 11-adic unit factor α_0. Therefore, the quintic surface defined by the following equation violates the local-global principle:

$$t(9Nt^2+11tx+11x^2)((9N+1)t^2+11tx+11x^2) = N_{\mathbb{Q}(\cos(2\pi/11))/\mathbb{Q}}(x+\cos(2\pi/11)y+\cos(2\pi/11)^2 z).$$

Appendix A : Basic tools

Notation

We call an extension field of $\mathbb{Q}$ of finite degree as a number field. For every number field K, we denote the group of roots of unity in K by $\mu(K)$. The ring of integers in K is the subring of K consisting of elements whose monic minimal polynomial over $\mathbb{Q}$ have coefficients in $\mathbb{Z}$. In other words, it is the integral closure of $\mathbb{Z}$ in K. We denote this ring by $\mathcal{O}_K$. In what follows, we often call an ideal of $\mathcal{O}_K$ just as an ideal of K. Accordingly, we often call the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ of $\mathcal{O}_K$ just as the ideal class group of K and denote it by $\mathrm{Cl}(K)$.

For every maximal ideal $\mathfrak{p}$ of K, we denote the (additive) $\mathfrak{p}$-adic valuation map by $v_{\mathfrak{p}} : K^{\times} \to \mathbb{Z}$, and for every fractional ideal $\mathfrak{a}$ of K, we abbreviate $\min\{v_{\mathfrak{p}}(x) \mid x \in \mathfrak{a} \setminus \{0\}\}$ to $v_{\mathfrak{p}}(\mathfrak{a})$. We assume that every $\mathfrak{p}$-adic valuation map is normalized so that $v_{\mathfrak{p}}(\mathfrak{p}) = 1$. We denote the completion of K by $v_{\mathfrak{p}}$ by $K_{\mathfrak{p}}$ and the residue field $\mathcal{O}_K/\mathfrak{p}$ by $k(\mathfrak{p})$. The field $k(\mathfrak{p})$ is a finite field of cardinality $N_{K/\mathbb{Q}}(\mathfrak{p})$. Here and after, for evert finite extension L/K of number fields, $N_{L/K} : L \to K$ denotes the norm map, and for every ideal $\mathfrak{A}$ of L, $N_{L/K}(\mathfrak{A})$ denotes the ideal $\{N_{L/K}(a) \in K \mid a \in \mathfrak{A}\}$ of K. Moreover, for every ideal $\mathfrak{a}$ of K, we often abbreviate the ideal $\mathfrak{a}\mathcal{O}_L$ to $\mathfrak{a}$ if there is no fear of confusion.

If there is unique field homomorphism from K to $\mathbb{R}$, we denote it by ∞_K or ∞ if there is no confusion.

Finally, we often abbreviate an ideal $m\mathbb{Z}$ of $\mathbb{Z}$ to m for simplicity.

19. Basic properties of p-adic and finite fields

In this appendix, we recall some basic theorems around p-adic numbers which we use in the body of this thesis.

19.1. Hensel's lemma.

First, recall that a discrete valuation ring $R = (R, v)$ is an integral domain with a surjective homomorphism $v : (Q(R), \cdot) \to (\mathbb{Z} \cup \{+\infty\}, \times)$ of multiplicative monoids, where $Q(R)$ is the quotient field of R, such that

$$v(x+y) \geq \min\{v(x), v(y)\} \quad (\forall x, y \in Q(R)).$$

Hence, a discrete valuation ring (R, v) has a canonical topological ring structure defined by a metric, say $d(x, y) := e^{-v(x-y)}$ with some $e \in \mathbb{R}_{>1}$, and is said to be complete if it is complete with respect to such a metric. A unifromizer u of discrete valuation ring (R, v) is an element of R such that $v(u) = 1$, i.e., a generator of the unique maximal ideal $\{x \in R \mid v(x) \geq 1\}$ of R.

The ring $\mathbb{Z}_p$ of p-adic integers is defined by the completion of the ring $\mathbb{Z}$ of rational integers with respect to the p-adic valuation $v_p(x) := \sup\{v \in \mathbb{Z} \mid x/p^v \in \mathbb{Z}\} \in \mathbb{Z} \cup \{+\infty\}$. Equivalently, this ring is constructed as the projective limit $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ of the finite rings $\mathbb{Z}/p^n\mathbb{Z}$. Anyway, the ring $\mathbb{Z}_p$ is a complete discrete valuation ring with a uniformizer p, and the field $\mathbb{Q}_p$ of p-adic numbers is defined as the quotient field of $\mathbb{Z}_p$.

The following theorem is the most fundamental analytic property of complete discrete valuation rings, which has many arithmetic applications.

Theorem 19.1 (Hensel's lemma (cf. [**60**, Corollary 1, Ch. II])). *Let $\mathcal{O}$ be a complete discrete valuation ring such that $\mathcal{O} \supset \mathbb{Z}$, π be its uniformizer, and $f(x)$ be a polynomial in $\mathcal{O}[x]$. Suppose that there exist $v \in \mathbb{Z}_{\geq 1}$ and $x_0 \in \mathcal{O}$ such that*

$$f(x_0) \equiv 0 \pmod{\pi^{2v-1}} \quad \textit{and} \quad \frac{df}{dx}(x_0) \not\equiv 0 \pmod{\pi^v}.$$

Then, there exists $x_1 \in \mathcal{O}$ such that $x_1 \equiv x_0 \pmod{\pi^v}$ and $f(x_1) = 0$.

Since we assume that $\mathcal{O}$ is complete, Theorem 19.1 is obtained by applying the following lemma for more general discrete valuation rings iteratively.

Lemma 19.2. *Let $\mathcal{O}$ be a discrete valuation ring such that $\mathcal{O} \supset \mathbb{Z}$, π be its uniformizer, and $f(x)$ be a polynomial in $\mathcal{O}[x]$. Suppose that there exists $x_0 \in \mathcal{O}$ such that*

$$f(x_0) \equiv 0 \pmod{\pi^{2v-1}} \quad \textit{and} \quad \frac{df}{dx}(x_0) \not\equiv 0 \pmod{\pi^v}.$$

Then, there exists $x_1 \in \mathcal{O}$ such that

$$x_1 \equiv x_0 \pmod{\pi^v}, \quad f(x_1) \equiv 0 \pmod{\pi^{2v+1}}, \quad \textit{and} \quad \frac{df}{dx}(x_1) \not\equiv \pmod{\pi^{v+1}}.$$

Proof of Lemma 19.2. First, note that for every $n \in \mathbb{Z}_{\geq 0}$, we have

$$\frac{1}{n!}\frac{d^n f}{dx^n}(x) \in \mathcal{O}[x].$$

Therefore, there exists a (unique) polynomial $y(x) \in \mathcal{O}[x]$ such that

$$f(x) = f(x_0) + \frac{df}{dx}(x_0) \cdot (x - x_0) + (x - x_0)^2 y(x). \tag{13}$$

In particular, for every $x \in \mathcal{O}$ such that $x \equiv x_0 \pmod{\pi^v}$, the following congruence holds:

$$f(x) \equiv f(x_0) + \frac{df}{dx}(x_0) \cdot (x - x_0) \pmod{\pi^{2v}}. \tag{14}$$

On the other hand, since we assume that $f(x_0) \equiv 0 \pmod{\pi^{2v-1}}$ and $(df/dx)(x_0) \not\equiv 0 \pmod{\pi^v}$, by setting $x_0' = x_0 - (df/dx)(x_0)^{-1} f(x_0) \in \mathcal{O}$, we have

$$x_0' \equiv x_0 \pmod{\pi^v},$$

hence

$$f(x_0') \equiv 0 \pmod{\pi^{2v}}.$$

Moreover, by considering the differentials of the both sides of eq. (13), we see that the following congruence holds:

$$\frac{df}{dx}(x_0') \equiv \frac{df}{dx}(x_0) \not\equiv 0 \pmod{\pi^v}.$$

Set $x_1 := x_0' - (df/dx)(x_0')^{-1} f(x_0') \in \mathcal{O}$. Then, by the above arguments, we have

$$x_1 \equiv x_0' \pmod{\pi^{v+1}}.$$

Therefore, by applying eq. (14) to $(x_1, x_0', v+1)$ in place of (x, x_0, v), we obtain the congruence

$$f(x_1) \equiv 0 \pmod{\pi^{2v+2}}.$$

In particular, we obtain the desired congruences

$$x_1 \equiv x_0 \pmod{\pi^v}, \quad f(x_1) \equiv 0 \pmod{\pi^{2v+1}}, \quad \text{and} \quad \frac{df}{dx}(x_1) \not\equiv \pmod{\pi^{v+1}}.$$

□

By applying Theorem 19.1 to polynomials $f(x) = x^3 - u$ ($u \in \mathbb{Z}_p$) and $f(x) = x^2 + x + 1$, we obtain the following corollary.

Corollary 19.3. *Let p be a prime number.*

(1) *Let $\mu_{(p-1)/3} \subset \mathbb{Z}_p^\times$ be the group of $(p-1)/3$-th roots of unity. Then, we have*

$$\mathbb{Z}_p^{\times 3} = \begin{cases} \mu_{(p-1)/3} \times p\mathbb{Z}_p & \text{if } p \equiv 1 \pmod 3 \\ \mathbb{Z}_p^\times & \text{if } p \equiv 2 \pmod 3 \\ \pm 1 + 9\mathbb{Z}_3 & \text{if } p = 3 \end{cases}.$$

(2) *The polynomial x^2+x+1 is irreducible in $\mathbb{Z}_p[x]$ if and only if $p \equiv 0, -1 \pmod 3$. In other words, the ring $\mathbb{Z}_p$ contains a primitive third root of unity if and only if $p \equiv 1 \pmod 3$.*

19.2. Hasse-Weil bound for curves and its application to p-adic solubility.

THEOREM 19.4 (Hasse-Weil bound [**66**]). *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*

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

PROOF. See [**66**] or [**6**]. □

Corollary 19.5. *Let p be a prime number and C be a non-singular projective curve of genus g defined over $\mathbb{Q}$. Suppose that $p \geq (2g)^2$ and C has a good reduction at p. Then, $C \pmod{p}$ has an $\mathbb{F}_p$-rational point. In particular, C has a $\mathbb{Q}_p$-rational point.*

PROOF. The former statement is a consequence of the following estimate of $\#C(\mathbb{F}_p)$:

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

The latter statement is a consequence of Theorem 19.1: In order to describe the detailed argument, we assume for simplicity that C is a plane curve defined by $F(x, y, z) = 0$ with some homogeneous polynomial $F \in \mathbb{Z}[x, y, z]$ and the good reduction model of C (mod p) is defined by $F(x, y, z) \equiv 0 \pmod{p}$. [20] Then, by the former statement, C (mod p) has an $\mathbb{F}_p$-rational point $[X : Y : Z] = [x_0 : y_0 : z_0]$ with some $x_0, y_0, z_0 \in \mathbb{F}_p$. Moreover, since $C \pmod{p}$ is non-singular, one of X, Y, Z-derivatives of F does not vanish at $[X : Y : Z] = [x_0 : y_0 : z_0]$. We may assume that $(\partial F/\partial X)(x_0, y_0, z_0) \neq 0$ in $\mathbb{F}_p$. Then, by fixing some $y_1, z_1 \in \mathbb{Z}_p$ so that $y_1 \equiv y_0 \pmod{p}$ and $z_1 \equiv z_0 \pmod{p}$ and by applying Theorem 19.1 to the polynomial $f(x) = F(x, y_1, z_1) \in \mathbb{Z}_p[x]$, we see that there exists some $x_1 \in \mathbb{Z}_p$ such that $F(x_1, y_1, z_1) = 0$, i.e., C has a $\mathbb{Q}_p$-rational point $[X : Y : Z] = [x_1 : y_1 : z_1]$. □

[20] This special case is sufficient for the application to the body of this thesis.

20. Arithmetic of global fields

In this section, we give a summary of arithmetic of number fields. We especially focus on the ideal theory of number fields, which plays a central role in the body of this thesis.

20.1. Decomposition of prime ideals and Artin symbols.

In this subsection, we give a summary on the decomposition of prime ideals in finite extension of number fields and define the Artin symbols associated with prime ideals. The contents of this subsection is based on [**40**, Ch. III], [**56**, Ch. V], and [**61**, Part I].

Let L/K be a finite extension of number fields and $\mathfrak{p}$ be a prime ideal of K. Then, since $\mathcal{O}_L$ is a Dedekind domain, there exist distinct prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_{g(\mathfrak{p})}$ of L and integers $e(\mathfrak{P}_i/\mathfrak{p})$ such that

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g(\mathfrak{p})} \mathfrak{P}_i^{e(\mathfrak{P}_i/\mathfrak{p})}.$$

In this situation, we say that each prime ideal $\mathfrak{P}_i$ lies above $\mathfrak{p}$, and we call the integer $e(\mathfrak{P}_i/\mathfrak{p})$ as the ramification index of $\mathfrak{P}_i$ in L/K. If $e(\mathfrak{P}_i/\mathfrak{p}) = 1$ (resp. > 1), we say that $\mathfrak{P}_i$ is unramified (resp. ramified) in L/K. For the integer $g(\mathfrak{p})$, we have another equality

$$[L : K] = \sum_{i=1}^{g(\mathfrak{p})} [L_{\mathfrak{P}_i} : K_{\mathfrak{p}}].$$

On the other hand, if we define the integer $f(\mathfrak{P}_i/\mathfrak{p}) = [k(\mathfrak{P}_i) : k(\mathfrak{p})]$, then we have an equality

$$[L_{\mathfrak{P}_i} : K_{\mathfrak{p}}] = e(\mathfrak{P}_i/\mathfrak{p})f(\mathfrak{P}_i/\mathfrak{p}),$$

hence

$$[L : K] = \sum_{i=1}^{g(\mathfrak{p})} e(\mathfrak{P}_i/\mathfrak{p})f(\mathfrak{P}_i/\mathfrak{p}).$$

We call the integer $f(\mathfrak{P}_i/\mathfrak{p})$ as the residual degree of $\mathfrak{P}_i$ in L/K.

In what follows, we assume that L/K is a Galois extension. Then, the prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_{g(\mathfrak{p})}$ of L above $\mathfrak{p}$ are $\mathrm{Gal}(L/K)$-conjugate to each other. Therefore, both $e(\mathfrak{P}_i/\mathfrak{p})$ and $f(\mathfrak{P}_i/\mathfrak{p})$ are independent of i and determined by $\mathfrak{p}$. In this situation, we denote them by $e(\mathfrak{p})$ and $f(\mathfrak{p})$, which we call as the ramification index and the residual degree of $\mathfrak{p}$ in L/K respectively. Moreover, we say that $\mathfrak{p}$ is uniamified (resp. ramified) in L/K if $e(\mathfrak{p}) = 1$ (resp. > 1). As a consequence, we have a simplified equality

$$[L : K] = e(\mathfrak{p})f(\mathfrak{p})g(\mathfrak{p}).$$

Furthermore, for each prime ideal $\mathfrak{P}_i$ above $\mathfrak{p}$, we obtain a distinguished subgroup of $\mathrm{Gal}(L/K)$ consisting of the elements preserving $\mathfrak{P}_i$, which we call the decomposition group of $\mathfrak{P}_i$ in L/K and denote it by $D(\mathfrak{P}_i) = D(L/K; \mathfrak{P}_i)$. Note that the groups $D(\mathfrak{P}_i)$ $(1 \leq i \leq g(\mathfrak{p}))$ are $\mathrm{Gal}(L/K)$-conjugate to each other, and the $\mathfrak{P}_i$-adic completion $L \hookrightarrow L_{\mathfrak{P}_i}$ induces a canonical isomorphism

$$\mathrm{Gal}(L_{\mathfrak{P}_i}/K_{\mathfrak{p}}) \simeq D(\mathfrak{P}_i)(\subset \mathrm{Gal}(L/K)).$$

On the other hand, the modulo $\mathfrak{P}_i$ operation $\mathcal{O}_L \to k(\mathfrak{P}_i)$ induces a canonical group homomorphism

$$D(\mathfrak{P}_i) \to \mathrm{Gal}(k(\mathfrak{P}_i)/k(\mathfrak{p})).$$

By Hensel's lemma, it is surjective. The kernel of this homomorphism is called the inertia group of $\mathfrak{P}_i$, which we denote by $T(\mathfrak{P}_i)$. Note that $\#T(\mathfrak{P}_i) = e(\mathfrak{P}_i/\mathfrak{p}) = e(\mathfrak{p})$.

If $\mathfrak{P}_i$ is untamified in L/K, then the above homomorphism $D(\mathfrak{P}_i) \to \mathrm{Gal}(k(\mathfrak{P}_i)/k(\mathfrak{p}))$ is bijective. If this is the case, $D(\mathfrak{P}_i)$ is cyclic, and there exists a unique element $\left(\frac{L/K}{\mathfrak{P}_i}\right) \in D(\mathfrak{P}_i)$ such that

$$\left(\frac{L/K}{\mathfrak{P}_i}\right) x \equiv x^{\#k(\mathfrak{p})} \pmod{\mathfrak{P}_i}$$

for every $x \in \mathcal{O}_L$. We call this element as the Artin symbol of $\mathfrak{P}_i$ with respect to L/K.

Finally, note that if L/K is abelian, then the decomposition group $D(\mathfrak{P}_i) \subset \mathrm{Gal}(L/K)$ is independent of i. In particular, the Artin symbol $\left(\frac{L/K}{\mathfrak{P}_i}\right)$ is independent of i and determined by $\mathfrak{p}$. In this situation, we denote it by $\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$, which we call as the Artin symbol of $\mathfrak{p}$ with respect to L/K.

20.2. Class field theory. In this subsection, we summarize a part of main theorems of class field theory which we use in this thesis. The contents of this subsection are based on [**40**, Ch. III and Ch. V] and [**63**]

Let K be a number field. A modulus of K is the formal product of a non-zero fractional ideal $\mathfrak{m}_0$ of K and the formal product $\mathfrak{m}_\infty = \sigma_1 \cdots \sigma_s$ of some distinct embeddings $\sigma_i : K \to \mathbb{R}$ of K into the field $\mathbb{R}$ of real numbers (i.e., real embeddings of K). Therefore, we may regard moduli of K are generalizations of ideals of K enhanced with additional data on Archimedean valuations.

Let $\mathfrak{m}$ be a modulus of K and L/K be a finite extension. Then, we identify the modulus $\mathfrak{M}$ of L with $\mathfrak{m}$, where $\mathfrak{M}_0 = \mathfrak{m}_0\mathcal{O}_K$ and σ divides $\mathfrak{M}_\infty$ if and only if $\sigma|_K$ divides $\mathfrak{m}_\infty$. Further, we say that a real embedding $\sigma : K \to \mathbb{R}$ is ramified in L/K if there exists an embedding $\tilde{\sigma} : L \to \mathbb{C}$ such that $\tilde{\sigma}|_K = \sigma$ and $\tilde{\sigma}(L) \not\subset \mathbb{R}$.

Suppose further that L/K is abelian and $\mathfrak{m}$ is divisible by all prime ideals and real embeddings of K ramified in L/K. Let $I_K^{\mathfrak{m}}$ be the free abelian group generated by all non-zero prime ideals of K prime to $\mathfrak{m}_0$. Then, by means of Artin symbols, we can define a map

$$\mathrm{Art}_{L/K} : I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K); \quad \mathfrak{a} \mapsto \prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}} \right)^{v_{\mathfrak{p}}(\mathfrak{a})}.$$

We call this map as the Artin reciprocity map with respect to L/K. By the definition of Artin symbols, this map is characterized as the unique group homomorphism such that the following congruence holds for every prime ideal $\mathfrak{p} \in I_K^{\mathfrak{m}}$ and every $x \in \mathcal{O}_L$:

$$\mathrm{Art}_{L/K}(\mathfrak{p})(x) \equiv x^{\#k(\mathfrak{p})} \pmod{\mathfrak{p}}.$$

Therefore, the Artin reciprocity map has the following functorial property:

Theorem 20.1. *Let L/K and be a finite abelian extension of number fields and E be a finite extension of K. Let $\mathfrak{m}$ be a modulus of Kdivisible by all prime ideals ramified in L/K. Then, the following diagram is commutative.*

$$\begin{tikzcd} I_E^{\mathfrak{m}} \arrow[r, "\mathrm{Art}_{EL/E}"] \arrow[d, "N_{E/K}"'] & \mathrm{Gal}(EL/E) \arrow[d, "\mathrm{Res}_{EL/L}"] \\ I_K^{\mathfrak{m}} \arrow[r, "\mathrm{Art}_{L/K}"] & \mathrm{Gal}(L/K) \end{tikzcd}$$

Here, $\mathrm{Res}_{EL/L}$ is the natural map defined by the restriction to L. In particular, the map $\mathrm{Art}_{L/K}$ induces a homomorphism $I_K^{\mathfrak{m}}/N_{L/K}(I_L^{\mathfrak{m}}) \to \mathrm{Gal}(L/K)$.

Proof. By the definition of the Artin reciprocity map, it is sufficient to prove that

$$\left. \left(\frac{EL/E}{\mathfrak{P}} \right) \right|_L x \equiv \left(\frac{L/K}{N_{E/K}(\mathfrak{P})} \right) x \pmod{\mathfrak{P}}$$

for every prime ideal $\mathfrak{P} \in I_E^{\mathfrak{m}}$ and every $x \in \mathcal{O}_L$. Let $\mathfrak{p} = \mathfrak{P} \cap K$. Then, we have

$$N_{E/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})},$$

hence the above congruence is equivalent to

$$x^{\#k(\mathfrak{P})} \equiv x^{\#k(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})}} \pmod{\mathfrak{P}},$$

which follows from the definition of the residual degree $f(\mathfrak{P}/\mathfrak{p}) = [k(\mathfrak{P}) : k(\mathfrak{p})]$. □

Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus of K. Then, we obtain the subgroup $K_{\mathfrak{m},1}$ of $K^\times$ consisting of the element $a/b \in K^\times$ with $a, b \in \mathcal{O}_K$ satisfying the following conditions:

- ab is prime to $\mathfrak{m}_0$ and $v_\mathfrak{p}(a/b - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$ for every prime ideal $\mathfrak{p}$ dividing $\mathfrak{m}_0$.
- $\sigma(a/b) > 0$ for every real place $\sigma : K \to \mathbb{R}$ dividing $\mathfrak{m}_\infty$.

We denote the image of the natural map $K_{\mathfrak{m},1} \to I_K^\mathfrak{m}; x \mapsto x\mathcal{O}_K$ by $P_K^\mathfrak{m}$ and call the quotient group $I_K^\mathfrak{m}/P_K^\mathfrak{m}$ as the ray class group of modulus $\mathfrak{m}$. Note that I_K^1/P_K^1 is nothing but the ideal class group $\mathrm{Cl}(K)$, and if $\mathfrak{m} \subset \mathfrak{n}$, we have a natural surjective map $I_K^\mathfrak{m}/P_K^\mathfrak{m} \to I_K^\mathfrak{n}/P_K^\mathfrak{n}$ as a consequence of the approximation theorem (cf. [**40**, §1, Ch. IV]). The following theorem states that the Galois group $\mathrm{Gal}(L/K)$ of a given abelian extension L/K is completely described by the ray class group $I_K^\mathfrak{m}/P_K^\mathfrak{m}$ (purely intrinsic data) with a modification by the image $N_{L/K}(I_L^\mathfrak{m})$ of the norm map (auxiliary extrinsic data).

Theorem 20.2 (Reciprocity law). *Let L/K be a finite abelian extension of number fields and $\mathfrak{m}$ be a modulus of K divisible by all prime ideals and real embeddings which are ramified in L/K. Suppose that the ideal $\mathfrak{m}_0$ is sufficiently small. Then, the map* $\mathrm{Art}_{L/K} : I_K^\mathfrak{m} \to \mathrm{Gal}(L/K)$ *induces an isomorphism*

$$I_K^\mathfrak{m}/P_K^\mathfrak{m} N_{L/K}(I_L^\mathfrak{m}) \simeq \mathrm{Gal}(L/K).$$

Proof. See [**40**, Theorem 5.8, Ch. V]. □

Remark 20.3. The assumption on the size of $\mathfrak{m}$ is necessary to ensure the well-definedness of the (induced) isomorphism map. This well-definedness is the core of the proof of Theorem 20.2, which is reduced to the so called fundamental equality

$$[I_K^\mathfrak{m} : P_K^\mathfrak{m} N_{L/K}(I_L^\mathfrak{m})] = [L : K]$$

(cf. [**40**, Theorems 3.10 and 4.4, Ch. V]). We can describe some sufficient conditions for the validity of this equality in more explicit manner. For instance, Janusz [**40**, Corollary 3.7] gave such an explicit condition, that is, the following inequality holds for every prime ideal $\mathfrak{p}$ ramified in L/K which lies above a prime number p:

$$v_\mathfrak{p}(\mathfrak{m}_0) > v_\mathfrak{p}(e(\mathfrak{p})) + v_\mathfrak{p}(f(\mathfrak{p})) + \frac{v_\mathfrak{p}(p)}{p-1}.$$

In particular, if $[L : K]$ is prime to $\mathfrak{m}_0$, then the above condition is simplified to

$$v_\mathfrak{p}(\mathfrak{m}_0) > \frac{v_\mathfrak{p}(p)}{p-1}.$$

On the other hand, if one formulates the class field theory in terms of the idèle (class) group, such an algebraic ambiguity arising from the choice of the modulus disappears due to the *hugeness* of the idèle group or its sufficiently fine topology. (See [**63**].)

We conclude this subsection with the following existence theorem in class filed theory.

Theorem 20.4 (Existence theorem). *Let K be a number field, $\mathfrak{m}$ be a modulus of K, and H be a subgroup of $I_K^{\mathfrak{m}}$ containing $P_K^{\mathfrak{m}}$. Then, there exists a unique abelian extension L/K such that all prime ideals and real embeddings ramified in L/K divides $\mathfrak{m}$ and the Artin reciprocity map $\mathrm{Art}_{L/K} : I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ indues an isomorphism $I_K^{\mathfrak{m}}/H \to \mathrm{Gal}(L/K)$.*

Proof. See [**40**, Theorems 9.9 and 11.11, Ch. V]. □

20.3. Ring class fields. Let K be a number field. In this subsection, we recall the ring class filed theory, which gives an isomorphism between the Picard groups of certain subrings of the ring $\mathcal{O}_K$ of integers in K and the Galois groups of special abelian extensions of K. The contents of this subsection is based on [**43**] and [**48**, §12, Ch. I].

A subring of K whose $\mathbb{Z}$-rank is $[K : \mathbb{Q}]$ is called an order of K. An order $\mathcal{O}$ of K is a Dedekind domain if and only if $\mathcal{O} = \mathcal{O}_K$, however, we can associate an arbitrary order to the Picard group which is a generalization of the ideal class group $\mathrm{Cl}(K) = \mathrm{Cl}(\mathcal{O}_K)$ of K. In order to define the Picard group $\mathrm{Pic}(\mathcal{O})$ of $\mathcal{O}$, we introduce some terminologies. A finitely generated $\mathcal{O}$-supmodule $\mathfrak{a}$ of K is called as a fractional ideal of $\mathcal{O}$, and it is said to be invertible if there exists another fractional ideal $\mathfrak{b}$ of $\mathcal{O}$ such that $\mathfrak{a}\mathfrak{b} = \mathcal{O}$. We denote the group of invertible fractional ideals of $\mathcal{O}$ by $I_{\mathcal{O}}$, which includes the subgroup $P_{\mathcal{O}}$ consisting of (principal) fractional ideals $x\mathcal{O}$ with $x \in K^\times$. Then, the Picard group $\mathrm{Pic}(\mathcal{O})$ of $\mathcal{O}$ is defined as the quotient group $\mathrm{Pic}(\mathcal{O}) := I_{\mathcal{O}}/P_{\mathcal{O}}$. Note that the Picard group $\mathrm{Pic}(\mathcal{O}_K)$ of the ring $\mathcal{O}_K$ of integers in K is nothing but the ideal class group $\mathrm{Cl}(\mathcal{O}_K)$ of $\mathcal{O}_K$.

On the other hand, every order $\mathcal{O}$ of K has another important invariant $\mathfrak{f} = \mathfrak{f}(\mathcal{O})$, the so called conductor, which is defined by $\mathfrak{f} := \{f \in \mathcal{O}_K \mid f\mathcal{O}_K \subset \mathcal{O}\}$. Note that since the conductor $\mathfrak{f}$ of $\mathcal{O}$ is a non-zero hence invertible ideal of $\mathcal{O}_K$, the group $I_K^{\mathfrak{f}}$ is well-defined. Let $P_{\mathcal{O}}^{\mathfrak{f}}$ be the subgroup of $I_K^{\mathfrak{f}}$ generated by principal ideals $x\mathcal{O}_K$ of K with $x \in \mathcal{O}$ such that $x\mathcal{O} + \mathfrak{f} = \mathcal{O}$ (i.e., “x is prime to $\mathfrak{f}$” in this sense). Then, we can describe the Picard group $\mathrm{Pic}(\mathcal{O})$ of each order $\mathcal{O}$ as a modified ideal class group of the Dedekind domain $\mathcal{O}_K$.

Theorem 20.5. *Let $\mathcal{O}$ be an order of K with conductor $\mathfrak{f}$. Then, the scalar extension induces a natural isomorphism $\mathrm{Pic}(\mathcal{O}) \simeq I_K^{\mathfrak{f}}/P_{\mathcal{O}}^{\mathfrak{f}}$.*

PROOF. See [**43**, Theorems 3.8 and 3.11]. □

Since $P_{\mathcal{O}}^{\mathfrak{f}}$ contains the group $P_K^{\mathfrak{f}}$, Theorem 20.4 implies the following theorem.

THEOREM 20.6 ([**43**, Theorem 4.2]). *Let K be a number field and $\mathcal{O}$ be an order of K with conductor $\mathfrak{f}$. Then, there exists a unique abelian extension $H_{\mathcal{O}}$ of K such that all prime ideals of K ramified in $H_{\mathcal{O}}/K$ divide $\mathfrak{f}$ and the Artin reciprocity map $\mathrm{Art}_{H_{\mathcal{O}}/K} : I_K^{\mathfrak{f}} \to \mathrm{Gal}(H_{\mathcal{O}}/K)$ induces an isomorphism $I_K^{\mathfrak{f}}/P_{\mathcal{O}}^{\mathfrak{f}} \simeq \mathrm{Gal}(H_{\mathcal{O}}/K)$, hence $\mathrm{Pic}(\mathcal{O}) \simeq \mathrm{Gal}(H_{\mathcal{O}}/K)$.*

The last isomorphism is useful in the study of certain Diophantine problems related with prime ideals of special form. For example, Cox [**21**] studied prime numbers of the form

$$l = x^2 + ny^2$$

with $x, y, n \in \mathbb{Z}_{\geq 1}$, and Lv and Deng generalized this study by Cox to the case $x, y \in \mathcal{O}_K$ with an imaginary quadratic field K. In section 22, we apply the above isomorphism in the study of prime numbers of the form

$$l = a^3 + pb^3 + p^2c^3 - 3pabc$$

with a prime number p and $a, b, c \in (1/3)\mathbb{Z}$ such that $b \equiv 0 \pmod{p}$ and $c \not\equiv 0 \pmod{p}$.

20.4. Analytic class number formula. In this subsection, we recall the analytic class number formula, which reduce the estimate of the class numbers of number fields to the estimate of certain analytic objects. The contents of this subsection are based on [**40**, Ch. I, IV, and V] and [**56**, Ch. IV and V].

Let L/K be finite extension of number fields of degree $[L : K] = r$. First, we introduce the discriminant ideals of L/K, which is useful to determine the prime ideals ramified in L/K.

Definition 20.7. For every K-basis $(x_i)_{1\leq i\leq r}$ of L, we define the discriminant of L/K with respect to $(x_i)_{1\leq i\leq r}$ as $\det(\mathrm{Tr}_{L/K}(x_ix_j)_{1\leq i,j\leq r})$. Moreover, we define the discriminant ideal $\mathfrak{D}_{L/K}$ of L/K as the ideal of $\mathcal{O}_K$ generated by the discriminants with respect to all K-basis of L consisting of elements of $\mathcal{O}_L$. If $K = \mathbb{Q}$, the unique positive generator of the discriminant ideal $\mathfrak{D}_{L/\mathbb{Q}}$ is called the (absolute) discriminant of L and denoted by $\mathrm{Disc}(L)$.

THEOREM 20.8 (Dedekind's criterion). *A prime ideal $\mathfrak{p}$ of K is ramified in L/K if and only if $\mathfrak{p}$ divides $\mathfrak{D}_{L/K}$.*

PROOF. See [**40**, Theorem 7.3, Ch. I] or [**56**, Theorem 1, §5.3, Ch. V]. □

Next, we recall the finiteness of the ideal class group, which we have already encountered in Theorem 20.4 in more general setting.

THEOREM 20.9 (Finiteness of ideal class group). *For every number field K, the ideal class group* $\mathrm{Cl}(K)$ *is a finite abelian group.*

PROOF. See [**56**, Theorem 2, §4.3, Ch. IV]. For a generalization to ray class groups, see [**40**, Corollary 1.6, Ch. III]. □

We call the order of $\mathrm{Cl}(K)$ as the class number of K.

Besides the above finiteness of the ideal class group, the following unit theorem of Dirichlet is also a distinguished property of number fields. This theorem states that the group $\mathcal{O}_K^\times$ of invertible elements of $\mathcal{O}_K$ is a finitely generated abelian group, and the rank of this abelian group is explicitly described by means of the fields of real and complex numbers. Let $\sigma : K \to \mathbb{C}$ be a homomorphism of fields. Then, we say that σ is real or complex according to whether its image $\mathrm{Im}(\sigma)$ is contained in the field $\mathbb{R}$ of real numbers or not. Since we have the canonical involution ρ on $\mathbb{C}$, namely the complex conjugation automorphism, we see that there exist even number of complex embeddings for every number field K. Let r_1 be the number of real embeddings $K \to \mathbb{R}$ and $2r_2$ be the number of complex embeddings $K \to \mathbb{C}$. Then, Dirichlet's unit theorem states as follows:

THEOREM 20.10 (Dirichlet's unit theorem). *For every number field K, we have the following isomorphism:*

$$\mathcal{O}_K^\times \simeq \mu(K) \times \mathbb{Z}^{\oplus r_1 + r_2 - 1}.$$

PROOF. See [**56**, Theorem 1, §4.4, Ch. IV]. For a generalization with moduli (i.e., S-units), see [**40**, Theorem 8.2, Ch. V]. □

From Theorem 20.10, we can further define an interesting analytic invariant, the so called regulator of a number field K, which is defined as follows. Let $\sigma_i : K \to \mathbb{C}$ $(i = 1, \dots, r_1 + 2r_2)$ be distinct $r_1 + 2r_2$ homomorphisms of fields labeled so that $\sigma_1, \dots, \sigma_{r_1}$ are real and $\sigma_{r_1+r_2+j} = \rho \circ \sigma_{r_1+j}$ for $j = 1, \dots, r_2$. Then, the regulator $\mathrm{Reg}(K)$ of K is defined as the volume of the fundamental domain of the $r_1 + r_2 - 1$-dimensional lattice obtained as the image of the group homomorphism

$$\mathcal{O}_K^\times \to \mathbb{R}^{r_1+r_2}; x \mapsto (\log|\sigma_1(x)|, \dots, \log|\sigma_{r_1}(x)|, \log|\sigma_{r_1+1}(x)|^2, \dots, \log|\sigma_{r_1+r_2}(x)|^2).$$

More explicitly, if we take a system $(\epsilon_i)_{1\leq i\leq r_1+r_2-1}$ of elements of $\mathcal{O}_K^\times$ so that their images in the quotient group $\mathcal{O}_K^\times/\mu(K)$ span the whole of the latter group, then we can express $\operatorname{Reg}(K)$ as follows:

$$\operatorname{Reg}(K) = \left|\det\left((N_i \log|\sigma_i(\epsilon_j)|)_{1\leq i,j\leq r_1+r_2-1}\right)\right|,$$

where $N_i = 1$ or 2 according to whether $1 \leq i \leq r_1$ or not.

In order to describe the connection of the above number theoretic invariants of K, namely

- the discriminant $\operatorname{Disc}(K)$,
- the class number $\#\operatorname{Cl}(K)$, and
- the regulator $\operatorname{Reg}(K)$,

we introduce the Dedekind zeta function $\zeta_K(s)$ of K. This function is defined by the Dirichlet series

$$\zeta_K(s) = \sum_{0\neq\mathfrak{a}\subset\mathcal{O}_K} N_{K/\mathbb{Q}}(\mathfrak{a})^{-s} \quad (s \in \mathbb{C} \text{ and } \Re(s) > 1).$$

Here, $\mathfrak{a}$ in the summation runs over all non-zero ideals of $\mathcal{O}_K$. Since $\mathcal{O}_K$ is a Dedekind domain, $\zeta_K(s)$ has the following product representation of Euler-type

$$\zeta_K(s) = \prod_{\mathfrak{p}\subset\mathcal{O}_K} (1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s})^{-1} \quad (s \in \mathbb{C} \text{ and } \Re(s) > 1),$$

which converges uniformly (cf. [**40**, Theorem 4.2, Ch. IV]). Here, $\mathfrak{p}$ in the product runs over all maximal ideals of $\mathcal{O}_K$. Through this complex analytic function ζ_K, the above number-theoretic characters of K are connected to each other as follows:

Theorem 20.11 (analytic class number formula). *For every number field K, the Dedekind zeta function $\zeta_K(s)$ has a meromorphic extension on $\mathbb{C}$ with a simple pole at $s = 1$. Moreover, the residue of $\zeta_K(s)$ at $s = 1$ is given by*

$$\operatorname{Res}_{s=1}\zeta_K(s) = \frac{\#\operatorname{Cl}(K)}{\#\mu(K)} \cdot \frac{2^{r_1}(2\pi)^{r_2}\operatorname{Reg}(K)}{\sqrt{\operatorname{Disc}(K)}}.$$

Proof. For the equality, see [**40**, Theorem 2.12, Ch. IV]. For the meromorphic continuation to the whole cimplex plane $\mathbb{C}$, see [**48**, Corollary 5.11, Ch. VII]. □

In the study of Diophantine equations, we often encounter with the problem to estimate $\#\operatorname{Cl}(K)$ for a certain number field K of special form. In particular, we are interested in the p-divisibility of $\#\operatorname{Cl}(K)$ for a certain prime number p, hence an explicit upper bound of $\#\,\mathrm{Cl}(K)$ is desirable in many case. For instance, one of the long-standing obstructions against the proof of Fermat's Last Theorem was the p-divisibility of $\#\,\mathrm{Cl}(\mathbb{Q}(\zeta_p))$ for some "irregular" prime numbers.

Since the discriminants $\mathrm{Disc}(K)$ often has an explicit formula convenient for the calculation, the equality in Theorem 20.11 shows that in order to obtain an upper bound of the class number $\#\,\mathrm{Cl}(K)$, it is sufficient to give an upper bound of the residue $\mathrm{Res}_{s=1}\,\zeta_K(s)$ and a lower bound of the regulator $\mathrm{Reg}(K)$. In section 22, we carry out this task for pure cubic fields $K = \mathbb{Q}(p^{1/3}), \mathbb{Q}((2p)^{1/3})$ with a prime number p and prove that $\#\,\mathrm{Cl}(K)$ is prime to p. This is a key ingredient of the study of Diophantine equations of the form $X^3 + P^\iota Y^3 = LZ^{p^\iota}$, where $P = p$ or $2p$, $\iota = 1, 2$, and $L \in \mathbb{Z}$.

21. Cyclotomic fields

In this section, we recall some basic theorems around cyclotomic fields, which we use in the body of the thesis. Let $m \in \mathbb{Z}_{\geq 1}$ be an integer and $\zeta_m = \exp(2\pi i/m) \in \mathbb{C}$ be the fixed primitive m-th root of unity.

21.1. Galois groups of cylclotomic extensions. First, we give an elementary description of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ by using class field theory.

Theorem 21.1. *The Artin reciprocity map* $\mathrm{Art}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}$ *induces an isomorphism* $\psi_m : (\mathbb{Z}/m\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, *which maps the class* $(p \pmod m)$ *to the Artin symbol* $\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right)$ *for every prime number* p *prime to* m.

Proof. Since $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is unramified outside $m\infty$, we have a surjective map $\mathrm{Art}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} : I_{\mathbb{Q}}^{m\infty} = I_{\mathbb{Q}}^{m} \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Suppose that an ideal $(a/b)\mathbb{Z} \in I_{\mathbb{Q}}^{m\infty}$ lies in the kernel of this map. We may assume that $\gcd(m, ab) = 1$. Then, we have an equality of the Artin symbols

$$\prod_p \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right)^{v_p(a)} = \prod_p \left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right)^{v_p(b)},$$

where p runs over all prime numbers prime to m. Here, note that since the Artin symbol $\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right)$ is characterized by the congruence

$$\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right) x \equiv x^p \pmod{\mathfrak{p}}$$

for every $x \in \mathcal{O}_{\mathbb{Q}(\zeta_m)}$ and every prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_m)$ above p, and the $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$-conjugates of ζ_m has the form ζ_m^k with some $k \in \mathbb{Z}$, we have an equality

$$\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right) \zeta_m = \zeta_m^p,$$

which holds in $\mathbb{Q}(\zeta_m)$. Hence, we have

$$\zeta_m^{|a|} = \zeta_m^{|b|}.$$

Since we take $a, b \in \mathbb{Z}$ so that $a, b > 0$, the above equality shows that $\mathrm{Ker}\,\mathrm{Art}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} \subset P_{\mathbb{Q}}^{m\infty}$.

On the other hand, since each element of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is determined by its action on ζ_m, we see that $\mathrm{Ker}\,\mathrm{Art}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}$ consists of non-zero fractional ideals $(a/b)\mathbb{Z} = (|a|/|b|)\mathbb{Z}$ with some integers $a, b \in \mathbb{Z}$ such that $\gcd(m, ab) = 1$ and $|a| \equiv |b| \pmod m$. Hence, we obtain an equality $\operatorname{Ker}\operatorname{Art}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} = P_{\mathbb{Q}}^{m\infty}$. Since $I_{\mathbb{Q}}^{m\infty}/P_{\mathbb{Q}}^{m\infty} \simeq (\mathbb{Z}/m\mathbb{Z})^{\times}$, we complete the proof. □

The above description gives an interesting Diophantine consequence as follows.

Corollary 21.2. *Let $m \geq 2$ be an integer and $H \subset (\mathbb{Z}/m\mathbb{Z})^{\times}$ be a subgroup. Let $\psi_m : (\mathbb{Z}/m\mathbb{Z})^{\times} \simeq \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ be the isomorphism in Theorem 21.1 and K^H be the subfield of $\mathbb{Q}(\zeta_m)$ fixed by $\psi_m(H)$. Then, for every integer x such that $x\mathbb{Z} \in N_{K^H/\mathbb{Q}}(I_{K^H}^{m\infty})$, there exists some $h \in H$ such that $x \equiv \pm h \pmod m$.*

Proof. By Theorems 20.1 and 21.1, we obtain the following commutative diagram, which implies that there exists some $h \in H$ such that $|x| \equiv h \pmod m$ as claimed.

$$\begin{tikzcd}
I_{K^H}^{m\infty} \arrow[rr] \arrow[d, "N_{K^H/\mathbb{Q}}"'] & & H \arrow[r, "\psi_m", "\simeq"'] \arrow[d, hook] & \operatorname{Gal}(\mathbb{Q}(\zeta_m)/K^H) \arrow[d, hook] \\
I_{\mathbb{Q}}^{m\infty} \arrow[r] & I_{\mathbb{Q}}^{m\infty}/P_{\mathbb{Q}}^{m\infty} \arrow[r, "\simeq"'] & (\mathbb{Z}/m\mathbb{Z})^{\times} \arrow[r, "\psi_m", "\simeq"'] & \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})
\end{tikzcd}$$

□

The above result is used in the proof of Theorems 16.1 and 16.5.

21.2. Prime numbers in arithmetic progressions. We start from the following one of the most classical results in the theory of distribution of prime numbers.

Theorem 21.3 (Dirichlet's theorem on arithmetic progressions). *Let a, m be positive integers such that* $\gcd(a, m) = 1$. *Then, there exist infinitely many prime numbers p such that $p = mx + a$ with some $x \in \mathbb{Z}$.*

Proof. See [**40**, Theorem 5.9, Ch. IV] or [**60**, Theorem 2, Ch. VI]. □

For a more precise quantitative statement by means of the density of prime numbers, see e.g. [**40**, Theorem 5.8, Ch. IV] or [**60**, Ch. VI].

Corollary 21.4. *Let m be a positive integer such that the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^{\times}$ is cyclic. Then, there exist infinitely many prime numbers p such that the residual degree $f(p)$ coincides with the degree $[\mathbb{Q}(\zeta_m) : \mathbb{Q}]$, i.e., p is totally inert in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.*

Proof. By definition, a prime number p is totally inert in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ if and only if it is unramified in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ and the order of the Artin symbol $\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{p}\right) \in \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ coincides with the degree $[\mathbb{Q}(\zeta_m) : \mathbb{Q}]$. By Theorem 21.1, p is totally inert in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ if and only if the order of $(p \pmod{m})$ coincides with $\#(\mathbb{Z}/m\mathbb{Z})^\times = \phi(m)$. On the other hand, since we assume that $(\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic, there exists an integer a whose image in $(\mathbb{Z}/m\mathbb{Z})^\times$ has order $\phi(m)$. By Theorem 21.3, there exist infinitely many prime numbers p such that $p \equiv a \pmod{m}$. This implies the desired conclusion. □

For more general abelian extensions, see [**40**, Corollary 5.4, Ch. IV].

22. Pure cubic fields

In this section, we recall some basic theorems around pure cubic fields, which we use in the body of the thesis.

22.1. Integer rings of pure cubic fields. First, we recall the structure of the ring of integers in a pure cubic field. The main reference is [**22**].

Let $d = d_1 d_2^2$ be a positive cube-free integer with square-free integer $d_1, d_2 \in \mathbb{Z}$, $\pi_1 := d^{1/3} \in \mathbb{R}_{>0}$ be the real cubic root of d, $K = \mathbb{Q}(\pi_1)$ be the associated pure cubic field, and $\mathcal{O}_K$ be the ring of integers in K. We also set $\pi_2 := d_1 d_2/\pi_1$, which is a cubic root of $d_1^2 d_2$, and $\pi_3 := (1 + d_1\pi_1 + d_2\pi_2)/3$. Recall that the discriminant $\mathrm{Disc}(K)$ of K is the unique positive generator of the ideal $\mathfrak{D}_{K/\mathbb{Q}}$ (cf. Definition 20.7).

Definition 22.1. The cubic field K is called a pure cubic field of the first or second kind according to whether $d_1^2 - d_2^2$ is not divisible by 9 or divisible by 9.

Here, note that since $\gcd(d_1, d_2) = 1$, $d_1^2 - d_2^2$ is divisible by 9 if and only if $\gcd(3, d_1 d_2) = 1$ and $d_1^2 d_2 \equiv d_2^3 \pmod 9$, i.e., $d \equiv \pm 1 \pmod 9$.

Proposition 22.2.
(1) *Suppose that K is of the first kind. Then, we have $\mathcal{O}_K = \mathbb{Z}[\pi_1, \pi_2]$, and there exists a unique prime ideal $\mathfrak{p}_3$ of K such that $3\mathcal{O}_K = \mathfrak{p}_3^3$. Moreover, we have* $\mathrm{Disc}(K) = 27 d_1^2 d_2^2$.
(2) *Suppose that K is of the second kind. Then, we have $\mathcal{O}_K = \mathbb{Z}[\pi_1, \pi_3]$. Moreover, there exist two prime ideals $\mathfrak{p}_{3,1}$ and $\mathfrak{p}_{3,2}$ of K such that $3\mathcal{O}_K = \mathfrak{p}_{3,1}\mathfrak{p}_{3,2}^2$. Moreover, we have* $\mathrm{Disc}(K) = 3 d_1^2 d_2^2$.

Proof. See [**22**, §§3–4]. □

As a consequence, the analytic class number formula (Theorem 20.11) for pure cubic fields can be reduced to the following simple form:

Corollary 22.3. *Let ϵ be the fundamental unit of $\mathcal{O}_K$. Then, the following formulae hold:*

$$\mathrm{Res}_{s=1}\,\zeta_K(s) = \begin{cases} \#\,\mathrm{Cl}(K) \cdot \dfrac{2\pi \log \epsilon}{d_1 d_2 \sqrt{3}} & \text{if } d \equiv \pm 1 \pmod 9 \\ \#\,\mathrm{Cl}(K) \cdot \dfrac{2\pi \log \epsilon}{3 d_1 d_2 \sqrt{3}} & \text{if } d \not\equiv \pm 1 \pmod 9 \end{cases}.$$

Turning to the algebraic side, in view of the local-global principle, the following theorem is interesting.

Proposition 22.4 (Fujiwara's trick (cf. [**24**]))**.** *Let $d \in \mathbb{Z}$ be a cube-free integer. Then, the polynomial $f_d(x) := (x^3 - d)(x^2 + x + 1)$ has a linear factor over $\mathbb{Q}_p$ if p is prime to $3d$. In particular, if $d \equiv 1 \pmod 9$ and every prime divisor l of d satisfies $l \equiv 1 \pmod 3$, then the polynomial $f_d(x)$ violates the local-global principle over $\mathbb{Q}$.*

Proof. First, recall that the minimal splitting field K_d of f_d is a Galois extension of $\mathbb{Q}$ whose Galois group is isomorphic to the symmetric group of order 3. Since the residual degree of every prime number is $1, 2,$ or 3, we see that f_d has a linear factor in $\mathbb{Q}_l[x]$ if l is unramified in $K_d/\mathbb{Q}$. Therefore, the former statement holds from Theorem 20.8 and Proposition 22.2. The latter statement is a consequence of the former and Corollary 19.3. □

22.2. Estimate of the class numbers of $\mathbb{Q}(p^{1/3})$ and $\mathbb{Q}((2p)^{1/3})$. In this subsection, we prove the following lemma, which is a key ingredient of the proof of Theorem 4.1.

Lemma 22.5. *Let p be a prime number.*

(1) *The class number of $K = \mathbb{Q}(p^{1/3})$ is smaller than p.*
(2) *The class number of $K = \mathbb{Q}((2p)^{1/3})$ is prime to p.*

For this purpose, we combine an upper bound of the residue $\mathrm{Res}_{s=1}\,\zeta_K(s)$ and a lower bound of the regulator $\mathrm{Reg}(K) = \log \epsilon$, both of which are known as follows.

Theorem 22.6 ([**4**, Théorème 1 and Corollarie 2]). *Let p be a prime number, $k = \mathbb{Q}(\zeta_p)$. Let $d \geq 2$ be a positive p-th power free integer and $K = \mathbb{Q}(d^{1/p})$ be the associated number field of degree p. Then, there exists an explicit constant B_p determined by p such that*

$$\mathrm{Res}_{s=1}\,\zeta_K(s) \leq \frac{1}{2}(\mathrm{Res}_{s=1}\,\zeta_k(s))\,(\log \mathrm{Disc}(K) + B_p)$$

and $\exp B_p \leq p^{4-2p}\,\mathrm{Disc}(K)$. As a consequence, for $p = 3$, the following explicit inequality holds:

$$\#\,\mathrm{Cl}(K) \leq \frac{\sqrt{\mathrm{Disc}(K)}\log \mathrm{Disc}(K)}{12\sqrt{3}\,\mathrm{Reg}(K)}.$$

Theorem 22.7 ([**20**, Theorem 3]). *Let K be a cubic field such that $r_1 = r_2 = 1$. Then, the following inequality holds:*

$$\mathrm{Reg}(K) \geq \frac{1}{3}\log\left(\frac{\mathrm{Disc}(K)}{27}\right).$$

By combining above estimates, we obtain an explicit upper bound of the class number of pure cubic fields.

Corollary 22.8. *Let $d \geq 2$ be a positive cube-free integer and $K = \mathbb{Q}(d^{1/3})$ be the associated cubic field. Then, the following inequality holds:*

$$\#\operatorname{Cl}(K) \leq \frac{\sqrt{\operatorname{Disc}(K)} \log \operatorname{Disc}(K)}{4\sqrt{3}\,(\log \operatorname{Disc}(K) - 3\log 3)}.$$

The above upper bound of the class number of a pure cubic field $K = \mathbb{Q}(d^{1/3})$ is sufficiently strong so that the proof of the first part of Lemma 22.5 is reduced to a small computer calculation. However, we *cannot* deduce a similar upper bound

$$\#\operatorname{Cl}(\mathbb{Q}(2p)^{1/3}) < p$$

for the second part in general. Thus, we have to combine the above upper bound in Corollary 22.8 and the following 3-divisibility result, where the latter is a consequence of the rational cubic genus theory in [**3**].

Lemma 22.9 ([**3**, Corollary 4.2.1])**.** *Let m be a cube-free integer and $K = \mathbb{Q}(m^{1/3})$ be the associated pure cubic field. Then, the class number $\#\operatorname{Cl}(K)$ of K is divisible by 3 except for possibly when*

$$m = 3, 9, p_1, p_1^2, 3p_1, 9p_1^2, 9p_1, 3p_1^2, p_1p_2, p_1^2p_2^2, p_3^2p_4, p_3p_4^2,$$

where the prime numbers $p_i \equiv 2 \pmod 3$ and $p_1p_2 \equiv 1 \pmod 9$ or $p_3 \equiv p_4 \pmod 9$.

Proof of Lemma 22.5. (1) If $p \equiv \pm 1 \pmod p$ (resp. $\not\equiv \pm 1 \pmod 9$), then we have $\operatorname{Disc} K = 3p^2$ (resp. $27p^2$). Therefore, by applying Theorems 22.6 and 22.7, we obtain the following upper bound for $\#\operatorname{Cl}(K)$

$$\#\operatorname{Cl}(K) \leq \frac{1}{4}p \cdot \frac{2\log p + \log 3}{2\log p - \log 9} \quad \left(\text{resp.} \quad \frac{3}{4}p \cdot \frac{2\log p + \log 27}{2\log p}\right),$$

from which we can deduce the desired upper bound for $p \geq 16$. [21] For $p < 140$, we can check the desired upper bound directly (e.g. by using Magma [**7**]).

[21] In order to deduce

$$\frac{2\log p + \log 3}{2\log p - \log 9} < 4,$$

it is sufficient to assume that $\log(3^9) < \log p^6$, i.e., $p \geq 6$. On the other hand, in order to deduce

$$\frac{2\log p + \log 27}{2\log p} < \frac{4}{3},$$

it is sufficient to assume that $\log(3^9) < \log p^2$, i.e., $p \geq 141$.

(2) If $p \equiv \pm 4 \pmod 9$ (resp. $\not\equiv \pm 4 \pmod 9$), then we have $\operatorname{Disc} K = 12p^2$ (resp. $108p^2$). Therefore, by applying Theorems 22.6 and 22.7, we obtain the following upper bound for $\#\operatorname{Cl}(K)$

$$\#\operatorname{Cl}(K) \leq \frac{1}{2}p \cdot \frac{2\log p + \log 12}{2\log p - \log(9/4)} \quad \left(\text{resp.} \quad \frac{3}{2}p \cdot \frac{2\log p + \log 108}{2\log p + \log 4}\right).$$

If $p \equiv \pm 4 \pmod 9$ and $p \geq 8$, the above upper bound implies that $\#\operatorname{Cl}(K) < p$. [22] For $p = 5$, we can check that $\#\operatorname{Cl}(K) = 1$ directly (e.g. by using Magma [**7**]). On the other hand, if $p \not\equiv \pm 4 \pmod 9$ and $p \neq 2, 3$, Lemma 22.9 implies thet $\#\operatorname{Cl}(K)$ is divisible by 3. Thus, we have

$$\frac{\#\operatorname{Cl}(K)}{3} \leq \frac{1}{2}p \cdot \frac{2\log p + \log 108}{2\log p + \log 4}.$$

from which we can deduce that $\#\operatorname{Cl}(K)/3 < p$, hence $\#\operatorname{Cl}(K)$ is prime to p. [23] For $p = 2, 3$, we can check that $\#\operatorname{Cl}(K) = 1$ directly (e.g. by using Magma [**7**]). □

The following is the program which we used in the proof of Lemma 22.5.

```
P<x> := PolynomialRing(Rationals());
for p in [1..140] do;
    if IsPrime(p) then
    K1 := NumberField(x^3-p);
        if ClassNumber(K1) gt p-1 then
        > <p, K1>;
        end if;
    end if;
end for;


>>
```

```
P<x> := PolynomialRing(Rationals());
for p in [1..8] do;
```

[22] In order to deduce

$$\frac{2\log p + \log 12}{2\log p - \log(9/4)} < 2,$$

it is sufficient to assume that $\log(243/4) < \log p^2$, i.e., $p \geq 8$.

[23] In order to deduce

$$\frac{2\log p + \log 108}{2\log p + \log 4} < 2,$$

it is sufficient to assume that $\log(27/4) < \log p^2$, i.e., $p \geq 3$.

```
    if IsPrime(p) then
    K2 := NumberField(x^3-2*p);
    > <p, ClassNumber(K2)>;
    end if;
end for;

>>
<2, 1>
<3, 1>
<5, 1>
<7, 3>
```

22.3. More plane curves of odd degrees. Let p be a prime number and $P = p$ or $2p$ such that $P \not\equiv \pm 1 \pmod 9$. In this subsection, we discuss how to obtain more plane curves which violate the local-global principle as stated in Theorem 4.1. More precisely, we discuss on how to produce relatively small L for every fixed odd degree $n \geq 5$ divisible by p and for every fixed $(n-3)/2$-tuples $(b_1, c_1), \ldots, (b_{(n-3)/2}, c_{(n-3)/2}) \in \mathbb{Z}^{\oplus 2}$.

For simplicity, suppose that $\iota = 1$. In view of the proof of Theorem 4.1, in order to obtain sufficiently many desired plane curves it is sufficient to find sufficiently many integers L satisfying the following condition gives

- L is prime to b_j and c_j $(1 \leq j \leq (n-3)/2)$.
- $L \equiv 1 \pmod p$ and L is a product of an even number $m < n$ of (possibly same) prime numbers $l_1, \ldots, l_m$ such that $l_i \equiv 2 \pmod 3$.
- There exists no $(x, y, z) \in \mathbb{Z}^{\oplus 3}$ such that $\gcd(x, y, z) = 1$ and $x^3 + Py^3 = Lz^n$.

The following Proposition 22.10, which is a generalization of Proposition 6.2, reduce the above problem to another problem of finding prime numbers associated with norms and satisfying some congruences. The proof of the original Proposition 6.2 works also in this generalized form in the exactly same manner because its proof depends only on the assumption $l_i \equiv 2 \pmod 3$ and the property of $(a_i, b_i, c_i) \in (\mathbb{Z}/p\mathbb{Z})^{\oplus 3}$.

Proposition 22.10. *In the above setting, further suppose that there exist (possibly same) $p-1$ prime numbers $l_1, \ldots, l_{n-1} \equiv 2 \pmod 3$ such that there exist $a_i, b_i, c_i \in \mathbb{Z}$ satisfying the following conditions:*

(1) *$l_i = a_i^3 + Pb_i^3 + P^2c_i^3 - 3Pa_ib_ic_i$.*

(2) *$(a_i, b_i, c_i) \in (\mathbb{Z}/p\mathbb{Z})^{\oplus 3}$ is independent of i, and $a_i \equiv \pm 1 \pmod p$, $b_i \equiv 0 \pmod p$, and $c_i \not\equiv 0 \pmod p$.*

(3) *If $p = 5$, then additionally $c \not\equiv -a \pmod{5}$.*

Then, there exist a positive even integer $m < n$ such that if we set $L = \prod_{i=1}^{m} l_i$, then every primitive solution of $x^3 + Py^3 = Lz^n$ satisfies $x \equiv y \equiv 0 \pmod{l_i}$ for some $1 \leq i \leq m$.

In the proof of Theorem 4.1, we restricted us to the special case $l_1 = \cdots = l_{n-1} = l$ with a prime number l produced by *Theorem* 4.4. This restriction made the proof of the infinitude of L simpler, however, the resulting L should be quite large in principle. As a consequence, such L forms a quite small set of integers.

The goal of this subsection is to prove the following Proposition 22.11. It gives relatively small prime numbers l of positive density (cf. the last of the proof of Proposition 22.12), to some of which we can apply Proposition 22.10. As a consequence, we can expect that these integers L form a relatively large set of integers.

More precisely, in order to apply Proposition 22.10 to the prime numbers l in Proposition 22.11, it is sufficient to check that $a \equiv \pm 1 \pmod{p}$ or not and classify the prime numbers l associated with $a \equiv \pm 1 \pmod{p}$ by the modulo p equivalence class of (a, c). Here, note that for any given infinite subset S of $\mathbb{Z}^{\oplus 3}$, at least one of the equivalence classes in $(\mathbb{Z}/p\mathbb{Z})^{\oplus 3}$ contains infinitely many triples in S by the pigeon hole principle.

In what follows, let $\pi = P^{1/3} \in \mathbb{R}_{>1}$ be the real cubic root, $K = \mathbb{Q}(\pi)$, $\mathcal{O}_K$ be the ring of integers in K, and $\epsilon = \alpha + \beta\pi + \gamma\pi^2$ be the fundamental unit of K with $\alpha, \beta, \gamma \in (1/3)\mathbb{Z}$.

Proposition 22.11. *Suppose that $\beta \not\equiv 0 \pmod{p}$. Then, there exist infinitely many principal prime ideals of $\mathcal{O}_K$ generated by some elements of the form $\lambda = a + b\pi + c\pi^2 \in \mathcal{O}_K$ with $a, b, c \in (1/3)\mathbb{Z}$ such that*

$$b \equiv 0 \pmod{p}, \quad c \not\equiv 0 \pmod{p}, \quad \textit{and} \quad l := N_{K/\mathbb{Q}}(\lambda) \equiv 2 \pmod{3}.$$

Here, note that since $\lambda\mathcal{O}_K$ is a prime ideal, the congruence $N_{K/\mathbb{Q}}(\lambda) \equiv 2 \pmod{3}$ implies that $N_{K/\mathbb{Q}}(\lambda)$ is a prime number. We should emphasize that the prime ideals $\lambda\mathcal{O}_K$ in Proposition 22.11 form a set of prime ideals of K with positive density (cf. the last of the proof of Proposition 22.12). This fact ensures that we can obtain sufficiently small and many prime numbers $l = N_{K/\mathbb{Q}}(\lambda)$.

Let $\mathcal{O} = \mathbb{Z} + p\mathcal{O}_K$. In principle, the whole of the following arguments can be easily generalized to more general orders, but we restrict us to $\mathcal{O} = \mathbb{Z} + p\mathcal{O}_K$ for simplicity of description.

Since $p\mathcal{O}_K \subset \mathcal{O}$ but $\pi^2 \notin \mathcal{O}[1/2]$, the conductor $\mathfrak{f} := \{a \in \mathcal{O}_K \mid a\mathcal{O}_K \subset \mathcal{O}\}$ of $\mathcal{O}$ coincides with $p\mathcal{O}_K$. Let $\lambda \in \mathcal{O}$ prime to $\mathfrak{f} = p\mathcal{O}_K$. Then, we see that $\mu \in \mathcal{O}_K$ satisfies $\lambda\mu \in \mathcal{O}$ only if $\mu \in \mathcal{O}$. Indeed, if we take $a, b, c \in (1/3)\mathbb{Z}$ so that $\lambda = a + b\pi + c\pi^2 \in \mathcal{O}$, then we have $a \not\equiv 0 \pmod{p}$ and $b \equiv c \equiv 0 \pmod{p}$, hence $\lambda\mu \equiv a\mu \pmod{p}$. Thus, we have $\lambda\mathcal{O}_K \cap \mathcal{O} \subset \lambda\mathcal{O}$, hence $\lambda\mathcal{O}_K \cap \mathcal{O} = \lambda\mathcal{O}$.

We have a natural group homomorphism $\mathrm{Pic}(\mathcal{O}) \to \mathrm{Pic}(\mathcal{O}_K) = \mathrm{Cl}(K)$ associated with the scalar extension of ideals. Then, it is surjective by the approximation theorem (cf. [**40**, §1, Ch. IV]). The following proposition is a key step of the proof of Proposition 22.11.

Proposition 22.12. *There exist infinitely many prime ideals Λ of $\mathcal{O}_K$ such that*

(1) $\Lambda \cap \mathbb{Z} = N_{K/\mathbb{Q}}(\Lambda)$ *is generated by a prime number* $l \equiv 2 \pmod 3$ *and*

(2) Λ *is a principal ideal of* $\mathcal{O}_K$ *prime to* p *but* $\Lambda \cap \mathcal{O}$ *is not a principal ideal of* $\mathcal{O}$.

Proof. First, note that a prime number l satisfies $l \equiv 2 \pmod 3$ if and only if the Artin symbol $\left(\frac{\mathbb{Q}(\zeta_3)/\mathbb{Q}}{l}\right)$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ is non-trivial. Moreover, a prime number l prime to P satisfies $l \equiv 2 \pmod 3$ if and only if there exist two prime ideals $\Lambda_{l,1}$ and $\Lambda_{l,2}$ of K whose norms are l and l^2 respectively. By the functoriality of the Artin reciprocity maps (Theorem 20.1), we see that $\left(\frac{K(\zeta_3)/K}{\Lambda_{l,1}}\right)$ is non-trivial and $\left(\frac{K(\zeta_3)/K}{\Lambda_{l,2}}\right)$ is trivial. Since each prime ideal Λ above a prime number $l \equiv 1 \pmod 3$ has norm l, we see that $\left(\frac{K(\zeta_3)/K}{\Lambda}\right)$ is trivial. As a consequence, we see that a prime ideal Λ of $\mathcal{O}_K$ satisfies the first condition in the statement if its Artin symbol $\left(\frac{K(\zeta_3)/K}{\Lambda}\right)$ defines a non-trivial element of $\mathrm{Gal}(K(\zeta_3)/K)$.

Next, let H_K be the maximal unramified abelian extension of K, and $H_{\mathcal{O}}$ be the ring class field associated with $\mathcal{O}$. Then, the Artin reciprocity map induces an isomorphism

$$\mathrm{Ker}(\mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}(K)) \simeq \mathrm{Ker}(\mathrm{Gal}(H_{\mathcal{O}}/K) \to \mathrm{Gal}(H_K/K)) \simeq \mathrm{Gal}(H_{\mathcal{O}}/H_K)$$

(cf. Theorems 20.1 and 20.6). Here, note that the second condition in the statement holds if and only if the ideal $\Lambda \cap \mathcal{O}$ of $\mathcal{O}$ defines a non-trivial class of $\mathrm{Ker}(\mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}(K))$.

By combining the above arguments, every prime ideal of K whose Artin symbol in $\mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/K)$ lies in the following subset S satisfy the desired conditions:

$$\begin{aligned} S &:= \mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/K(\zeta_3))^c \cap \mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/H_K) \cap \mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/H_{\mathcal{O}})^c \\ &= \mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/H_K) \cap \mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/H_K(\zeta_3))^c \cap \mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/H_{\mathcal{O}})^c \\ &= \mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/H_K) \setminus \left(\mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/H_K(\zeta_3)) \cup \mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/H_{\mathcal{O}})\right). \end{aligned}$$

Here, note that $\zeta_3 \notin H_K$ because $K(\zeta_3)/K$ is ramified at a prime ideal above 3 (which is unique if $P \not\equiv \pm 1 \pmod 9$) but H_K/K is unramified at every prime ideal. Therefore, if we set $\delta = 0$ or 1 according to whether $\zeta_3 \in H_{\mathcal{O}}$ or not, we can calculate the above three subgroups of $\mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/\mathbb{Q})$ as follows:

- $\#\,\mathrm{Gal}(H_{\mathcal{O}}(\zeta_3)/H_K) = 2^{\delta}\#\,\mathrm{Ker}(\mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}(K))$.

- $\#\operatorname{Gal}(H_{\mathcal{O}}(\zeta_3)/H_K(\zeta_3)) = (1/2)\#\operatorname{Gal}(H_{\mathcal{O}}(\zeta_3)/H_K)$.
- $\#\operatorname{Gal}(H_{\mathcal{O}}(\zeta_3)/H_{\mathcal{O}}) = 2^{\delta}$.

Thus, we can conclude that $S \neq \emptyset$ whenever $\operatorname{Pic}(\mathcal{O}) \not\simeq \operatorname{Cl}(K)$, which follows from the following Lemma 22.13. Therefore, the assertion follows from Chebotarev's density theorem (cf. [**40**, Theorem 10.4, Ch. V]), which actually ensures that such prime ideals Λ form a set of prime ideals of K with positive density $\#S/2^{\delta}\#\operatorname{Pic}(\mathcal{O})$. □

Lemma 22.13. *We have $\mathcal{O}_K^{\times}/\mathcal{O}^{\times} \simeq 1$ or $\mathbb{Z}/p\mathbb{Z}$ according to whether $\mathcal{O}^{\times} = \mathcal{O}_K^{\times}$ or not. Moreover, if we set r so that $(\mathcal{O}_K^{\times}/\mathcal{O}^{\times}) \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus r}$, then we have*

$$\operatorname{Ker}(\operatorname{Pic}(\mathcal{O}) \to \operatorname{Cl}(K)) \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus 2-r}.$$

Proof. The fist statement is an immediate consequence of Dirichlet's unit theorem (Theorem 20.10): Indeed, we see that $\mathcal{O}_K^{\times}/\{\pm 1\}$ is cyclic, and $\eta^p \in \mathcal{O}$ for every $\eta \in \mathcal{O}_K$ because $p \geq 3$.

For the second statement, we start from the exact sequence

$$1 \to \mathcal{O}_K^{\times}/\mathcal{O}^{\times} \to (\mathcal{O}_K/\mathfrak{f})^{\times}/(\mathcal{O}/\mathfrak{f})^{\times} \to \operatorname{Pic}(\mathcal{O}) \to \operatorname{Cl}(K) \to 1$$

induced by natural homomorphisms (cf. [**48**, Theorem 12.12, Ch. I]).

Since $\eta = a + b\pi + c\pi^2 \in \mathcal{O}_K$ with $a, b, c \in (1/3)\mathbb{Z}$ [24] is prime to p if and only if a is prime to p, we have

$$(\mathcal{O}_K/p\mathcal{O}_K)^{\times} \simeq (\mathbb{Z}/p\mathbb{Z})^{\times} \times (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$$

Similarly, we have $(\mathcal{O}/p\mathcal{O}_K)^{\times} \simeq (\mathbb{Z}/p\mathbb{Z})^{\times}$, hence

$$(\mathcal{O}_K/p\mathcal{O}_K)^{\times}/(\mathcal{O}/p\mathcal{O}_K)^{\times} \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}.$$

This implies the desired conclusion. □

Example 22.14. If $P = 3$, then since $\epsilon = 4 + 3\pi + 2\pi^2 \notin \mathcal{O}^{\times}$, we have $\mathcal{O}^{\times} = \mathcal{O}_K^{\times 3}$, hence $\operatorname{Ker}(\operatorname{Pic}(\mathcal{O}) \to \operatorname{Cl}(K)) \simeq \mathbb{Z}/3\mathbb{Z}$. If $P = 6$, then since $\epsilon = 109 + 60\pi + 33\pi^2 \in \mathcal{O}^{\times}$, we have $\mathcal{O}^{\times} = \mathcal{O}_K^{\times}$, hence $\operatorname{Ker}(\operatorname{Pic}(\mathcal{O}) \to \operatorname{Cl}(K)) = (\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$. For more general $p \geq 3$, see Corollary 22.16.

Remark 22.15. On the other hand, if $P = p = 2$, then we have$\epsilon = 1 + \pi + \pi^2$, $\mathfrak{f} = 2\mathcal{O}_K$, $\mathcal{O}_K^{\times}/\mathcal{O}^{\times} \simeq \mathbb{Z}/4\mathbb{Z}$, and $(\mathcal{O}_K/p\mathcal{O}_K)^{\times}/(\mathcal{O}/p\mathcal{O}_K)^{\times} \simeq (\mathcal{O}_K/p\mathcal{O}_K)^{\times} \simeq \mathbb{Z}/4\mathbb{Z}$. As a consequence, we have $\operatorname{Pic}(\mathcal{O}) \simeq \operatorname{Cl}(K) \simeq 1$.

[24] If $p = 3$, then $a.b, c \in \mathbb{Z}$.

Proof of Proposition 22.11. By Proposition 22.12, there exist infinitely many prime ideals of $\mathcal{O}_K$ generated by some $\lambda = a + b\pi + c\pi^2 \in \mathcal{O}_K$ with $a, b, c \in (1/3)\mathbb{Z}$ such that $N_{K/\mathbb{Q}}(\lambda) = 2$, [25] λ is prime to p (i.e., $a \not\equiv 0 \pmod{p}$), and $\lambda\mathcal{O}_K \cap \mathcal{O}$ is not a principal ideal of $\mathcal{O}$. For such λ, define $(a_k, b_k, c_k) \in (1/3)\mathbb{Z}^{\oplus 3}$ $(k \in \mathbb{Z})$ by $a_k + b_k\pi + c_k\pi^2 = \epsilon^k\lambda$. Then, we have $b_k \equiv \alpha^{k-1}\beta ak + \alpha^k b \pmod{p}$ inductively. Since we assume that $\beta \not\equiv 0 \pmod{p}$, if we take an integer $K \in \mathbb{Z}$ such that $K \equiv -b\alpha/a\beta \pmod{p}$, then we have $b_K \equiv 0 \pmod{p}$. On the other hand, if $b_K \equiv c_K \equiv 0 \pmod{p}$, then $\epsilon^K\lambda \in \mathcal{O}$, hence $\lambda\mathcal{O}_K \cap \mathcal{O} = \epsilon^K\lambda\mathcal{O}$ is a principal ideal of $\mathcal{O}$, a contradiction. Therefore, by replacing λ to $\epsilon^K\lambda$ if necessary, we obtain the desired conclusion. □

By the way, Lemma 22.13 gives the following purely ideal/Galois theoretic consequence of Conjecture 4.2 which states that $\beta \not\equiv 0 \pmod{p}$.

Corollary 22.16. *Suppose that* $\beta \not\equiv 0 \pmod{p}$ *or* $\gamma \not\equiv 0 \pmod{p}$. *Then, we have* $\mathrm{Pic}(\mathcal{O}) \otimes \mathbb{Z}_p \simeq \mathrm{Gal}(H_{\mathcal{O}}/K) \otimes \mathbb{Z}_p \simeq \mathbb{Z}/p\mathbb{Z}$.

Proof. First, recall that by Lemma 22.5 $\#\,\mathrm{Cl}(K)$ is prime to p. Hence, we have a natural isomorphism

$$\mathrm{Ker}(\mathrm{Pic}(\mathcal{O}) \to \mathrm{Cl}(K)) \otimes \mathbb{Z}_p \simeq \mathrm{Pic}(\mathcal{O}) \otimes \mathbb{Z}_p.$$

On the other hand, the fundamental unit $\epsilon = \alpha + \beta\pi + \gamma\pi^2$ belongs to $\mathcal{O}$ if and only if $\beta \equiv \gamma \equiv 0 \pmod{p}$. Therefore, Lemma 22.13 implies the desired conclusion. □

22.4. Prime numbers represented by cubic polynomials. In the previous subsection, we have proven that there are infinitely many prime numbers which arise as norms of special element of a pure cubic field. Its proof is almost algebraic and reduced to the problem of counting Artin symbols of the associated prime ideals due to Chebotarev density theorem. However, if we want to obtain prime numbers which arise as norms of more special elements in a cubic field, we encounter highly hard analytic problems. The following theorems due to Heath-Brown and Moroz are the break through in this direction.

Theorem 22.17 ([**31**, Theorem] for $X^3 + 2Y^3$, [**32**, Theorem 1.1] in general). *Let* $f(X, Y) \in \mathbb{Z}[X, Y]$ *be a binary cubic form which is irreducible in* $\mathbb{Z}[X, Y]$. *Then, there are infinitely many prime numbers* p *of the form* $p = f(x, y)$ *with some* $(x, y) \in \mathbb{Z}^{\oplus 2}$ *unless*

[25] Recall that a prime number $l \equiv 2 \pmod{3}$ is decomposed to $l\mathcal{O}_K = \Lambda_{l,1}\Lambda_{l,2}$ so that $N_{K/\mathbb{Q}}(\Lambda_{l,i}) = l^i$. Therefore, $\Lambda_{l,1}$ is principal if and only if $\Lambda_{l,2}$ is so.

$f(x,y)$ us divisible by 2 for each $(x,y) \in \mathbb{Z}^{\oplus 2}$, in which case there are infinitely many prime numbers p of the form $p = (1/2)f(x,y)$ with some $(x,y) \in \mathbb{Z}^{\oplus 2}$.

PROOF. See [**31**,**32**]. □

For more precise quantitative statement, see the original articles [**31**, Theorem] and [**32**, Theorem 2.1 and Corollary 2.2].

Heath-Brown and Moroz generalized Theorem 22.17 on cubic forms to more general cubic polynomials as follows.

THEOREM 22.18 ([**33**, Theorem 1]). *Let $f_0(X,Y) \in \mathbb{Z}[X,Y]$ be a binary cubic form which is irreducible in $\mathbb{Z}[X,Y]$. For every $d \in \mathbb{Z}$ and $\gamma = (\gamma_1, \gamma_2) \in \mathbb{Z}^{\oplus 2}$, let the positive integer γ_0 be the greatest common divisor of the coefficients of f_0 and set the polynomial $f(x,y) := \gamma_0^{-1} f_0(dx + \gamma_1, dy + \gamma_2)$. Suppose, moreover, that $\gcd f(\mathbb{Z}^{\oplus 2}) = 1$. Then, the set $f(\mathbb{Z}^{\oplus 2})$ contains infinitely many prime numbers.*

PROOF. See [**33**]. □

Appendix B : Numerical examinations

23. A cubic analogue of the Ankeny-Artin-Chowla-Mordell conjecture

In this appendix, we summarize the results of numerical examinations around Conjecture 4.2. Recall that this conjecture states as follows:

Conjecture 23.1. *(Conjecture 4.2) Let $p \neq 3$ be a prime number and $P = p$ or2p. Let $\pi = P^{1/3} \in \mathbb{R}$ be the real cubic root of P, $K = \mathbb{Q}(\pi)$ be the associated pure cubic field, and $\epsilon = \alpha + \beta\pi + \gamma\pi^2 \in \mathbb{R}_{>1}$ with $\alpha, \beta, \gamma \in (1/3)\mathbb{Z}$ be the fundamental unit of K. Then, $\beta \not\equiv 0 \pmod{p}$.*

We can easily verify this conjecture numerically. In fact, by using Magma [**7**], we have verified this conjecture for both $P = p$ and $2p$ in the range $p < 10^5$. For example, the following program returns that there exist no counterexamples of the above conjecture for $P = p$ in the range $p < 10^4$. Here, recall that Conjecture 23.1 holds for P if the order $\mathbb{Z}[\pi] \subset \mathcal{O}_K$ has a unit $\alpha + \beta\pi + \gamma\pi^2$ with $\alpha, \beta, \gamma \in (1/3)\mathbb{Z}$ such that $\beta \not\equiv 0 \pmod{p}$. In fact, for every element $\epsilon_1 \in \mathbb{Z}[\pi]^\times$, we have $\epsilon_1 = \epsilon$ or ϵ^3. The latter case may happen only if $P \equiv \pm 1 \pmod{9}$ and if this is the case, we have $\epsilon_1 \equiv \alpha^3 + 3\alpha\beta\pi \pmod{\pi^2}$.

```
Zx<x> := PolynomialRing(Integers());
for p in [1..10^4] do;  // the range for search
   if IsPrime(p) then
   O := EquationOrder(x^3-p);   // create the order O := Z[p^{1/3}]
   U,phi := UnitGroup(O);
        // U.1 := -1 and U.2 := another generator of the unit group of O;
   Fpy<y> := PolynomialRing(FiniteField(p));
        // y is a formal parameter in place of π
   h := hom< O -> Fpy | y >;
        // represent each element of O mod pO
        // as a polynomial of y = p^{1/3}
      if Coefficient(h(phi(U.2)), 1) eq 0 then;
         // if the coefficient of p^{1/3} for U.2 is 0 mod p, then
      > <p, h(phi(U.2))>;
        // return such a prime number p and the corresponding U.2
      end if;
   end if;
end for;

>>
<3, 2*y^2 + 2>
```

Note that the return $p = 3$ is the conjectural unique exception.

Moreover, the above numerical experiment implies that there exist non-singular plane curves of degree n which violate the local-global principle for "most" odd integers n in the sense of natural density: Let $\mathbb{N} := \mathbb{Z}_{\geq 1}$, and $\mathbb{N}^{\mathrm{odd}}$ be the set of positive odd integers. Set

$$\begin{aligned}
P &:= \{p : \text{prime number}\}, \\
BP &:= \left\{p \in P \mid p < 10^5\right\}, \\
M &:= \left\{n \in \mathbb{N} \mid n \not\equiv 0 \pmod{p} \text{ for all } p \in BP \text{ and } n \not\equiv 0 \pmod{p^2} \text{ for all } p \in P\right\}, \\
N &:= \mathbb{N} \setminus (M \cup \{1\}), \\
\mathbb{N}^{\mathrm{odd}} &:= \{n \in \mathbb{N} \mid n \text{ is an odd integer}\}, \\
N^{\mathrm{odd}} &:= N \cap \mathbb{N}^{\mathrm{odd}},
\end{aligned}$$

then Theorem 4.1 and the above numerical verification of Conjecture 23.1 (with Poonen's construction Theorem 2.7 for $n = 3$) ensures that we can construct infinitely many explicit non-singular plane curves of degree n which violates the local-global principle for each $n \in N^{\mathrm{odd}}$. Moreover, if we denote the natural density of $S \subset \mathbb{N}$ by $d(S)$ (if it exists), then we have

$$\begin{aligned}
d(M) &= \prod_{p \in BP} (1 - p^{-1}) \times \prod_{p \in P \setminus BP} (1 - p^{-2}) = \prod_{p \in BP} (1 + p^{-1})^{-1} \times \zeta(2)^{-1} \\
&< 0.0487529
\end{aligned}$$

and

$$d(\mathbb{N}^{\mathrm{odd}}) = \frac{1}{2},$$

hence

$$\frac{d(N^{\mathrm{odd}})}{d(\mathbb{N}^{\mathrm{odd}})} = 1 - \frac{d(M)}{d(\mathbb{N}^{\mathrm{odd}})} > 0.90249$$

Therefore, at least 90% of odd integers lie in N^{odd}. For the above numerical estimate, we use the following program carried out by Magma:

```
function g(p)
if IsPrime(p) then
return 1/(1+1/p);
```

```
else
return 1;
end if;
end function;

function G(k, n)
if n eq 0 then
return 1;
else
return G(k, n-1)*g(5*(k-1)*10^3+n);
end if;
end function;

function F(k)
if k eq 0 then
return 1;
else
return F(k-1)*G(k, 5*10^3);
end if;
end function;

R := RealField(6);

Zeta2 := (1/6)*Pi(R)^2;

> R!F(20);
> R!(1/Zeta2);
> R!(F(20)/Zeta2);
> R!(1-2*F(20)/Zeta2);

>>
0.0801953
0.607926
0.0487528
0.902494
```

On the other hand, Conjecture 23.1 has the following obvious cousins.

Question 23.2. *Let n be a positive integer and p be a prime number. Suppose that $P = np$ is not a cubic. Let $\pi = P^{1/3} \in \mathbb{R}$ be the real cubic root of P and $\epsilon = \alpha + \beta\pi + \gamma\pi^2 \in \mathbb{R}_{>1}$*

with $\alpha, \beta, \gamma \in \mathbb{Z}$ be the fundamental unit of the order $\mathbb{Z}[\pi]$. Then, is it true that $\beta \not\equiv 0 \pmod{p}$?

However, the above question is negative in general. For the search of such counterexamples for $n \leq 24$, we carried out the similar program to the above numerical examination by Magma. In this time, we searched such counterexamples in the range $p < 10^4$. The following table is the summary of this numerical examination.

n	Small p for which $\beta \equiv 0 \pmod{p}$ holds
1	3
2	3
3	2, 5, 13, 9377
4	3, 37
5	2, 3, 5, 17, 59
6	2, 3, 7
7	2, 3, 5, 7, 71
8	2, 3
9	67, 1303
10	3, 5
11	3, 11
12	3, 313, 701, 4273
13	3, 53
14	3, 7, 4079
15	3, 5, 11, 31, 79, 4229
16	2, 3
17	2, 3, 17, 101
18	3, 107, 389, 647
19	3, 19, 61
20	2, 3, 5, 3529
21	2, 7, 13, 479, 2239
22	3, 5, 11
23	2, 3, 5, 23, 7043
24	2, 3, 5, 13, 19, 9377

The above table suggests the following conjectures.

Conjecture 23.3. *Let $p \geq 5$ be a prime number, $\pi = p^{1/3} \in \mathbb{R}$ be the real cubic root of p, and $\epsilon = \alpha + \beta\pi^2 + \gamma\pi^4 \in \mathbb{R}_{>1}$ with $\alpha, \beta, \gamma \in \mathbb{Z}$ be the fundamental unit of the order $\mathbb{Z}[\pi^2]$. Then, the congruence $\beta \equiv 0 \pmod{p}$ holds.*

We verified Conjecture 23.3 in the range $p < 2000$ by a similar program carried out by Magma. Although this range is quite shorter than the range $p < 10^5$ where Conjecture 23.1

is verified, it should be noted that under the uniform distribution the probability that a randomly taken integer is divisible by p, is just $1/p$. Hence, our numerical verification for Conjecture 23.3 in the range $p < 2000$ suggests that Conjecture 23.3 itself is plausibile more strongly than our numerical verification of Conjecture 23.1 in the range $p < 10^5$ does.

Recall that we proved in Lemma 22.13 and Corollary 22.16 (cf. Lemma 22.5) that $\mathrm{Pic}(\mathbb{Z} + p\mathcal{O}_K) \otimes \mathbb{Z}_p \simeq (\mathbb{Z}/p\mathbb{Z})^{2-r}$ with $r = v_p([\mathcal{O}_K^\times : (\mathbb{Z} + p\mathcal{O}_K)^\times]) \in \{0, 1\}$. Moreover, note that Conjecture 23.1 implies that $r = 1$. By the same argument as Lemma 22.13 and Corollary 22.16, we can prove also the following: If we set $s = v_p([\mathcal{O}_K^\times : \mathbb{Z}[\pi^2]^\times]) \in \{0, 1\}$, then $\mathrm{Pic}(\mathbb{Z}[\pi^2]) \otimes \mathbb{Z}_p \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus 1-s}$, i.e., $s = 1$ if and only if the abelian extension of $K = \mathbb{Q}(p^{1/3})$ of conductor $p^{2/3}$ is trivial. Here, note that the conductor of $\mathbb{Z}[\pi^2]$ is $\mathfrak{p}_3^i \cdot \pi^2\mathcal{O}_K$ or $\pi^2\mathcal{O}_K$ according to whether $p \equiv \pm 1 \pmod 9$ or not, where $\mathfrak{p}_3$ is a prime ideal above 3 and does not affect on $\mathrm{Pic}(\mathbb{Z}[\pi^2]) \otimes \mathbb{Z}_p$ because we assume that $p \geq 5$.

Proposition 23.4. *If $s = 1$, then Conjecture 23.3 holds. Moreover, Conjecture 23.1 implies that $s = 1$. As a consequence, Conjecture 23.1 implies Conjecture 23.3.*

Besides the above p-adic property for every prime number p, the following 3-adic property is also plausible in view of the above table.

Conjecture 23.5. *Let $n \neq 3$ be a positive cube-free integer prime to 3, $P = 3n$, $\pi = P^{1/3} \in \mathbb{R}$ be the real cubic root of P, and $\epsilon = \alpha + \beta\pi + \gamma\pi^2 \in \mathbb{R}_{>1}$ with $\alpha, \beta, \gamma \in \mathbb{Z}$ be the fundamental unit of the order $\mathbb{Z}[\pi]$. Then, the congruence $\beta \equiv 0 \pmod 3$ holds.*

Bibliography

[1] W. Aitken and F. Lemmermeyer, *Counterexamples to the Hasse principle*, Amer. Math. Monthly **118** (2011), no. 7, 610–628, DOI 10.4169/amer.math.monthly.118.07.610. MR2826452

[2] N. C. Ankeny, E. Artin, and S. Chowla, *The class-number of real quadratic number fields*, Ann. of Math. (2) **56** (1952), 479–493, DOI 10.2307/1969656. MR0049948

[3] P. Barrucand and H. Cohn, *A rational genus, class number divisibility, and unit theory for pure cubic fields*, J. Number Theory **2** (1970), 7–21, DOI 10.1016/0022-314X(70)90003-X. MR249398

[4] P. Barrucand and S. Louboutin, *Majoration et minoration du nombre de classes d'idéaux des corps réels purs de degré premier*, Bull. London Math. Soc. **25** (1993), no. 6, 533–540, DOI 10.1112/blms/25.6.533 (French, with French summary). MR1245078

[5] B. J. Birch, *Forms in many variables*, Proc. Roy. Soc. London Ser. A **265** (1961/62), 245–263, DOI 10.1098/rspa.1962.0007. MR150129

[6] E. Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, Springer, Berlin, 1974, pp. 234–241. Lecture Notes in Math., Vol. 383. MR0429903

[7] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[8] A. Bremner, *Some cubic surfaces with no rational points*, Math. Proc. Cambridge Philos. Soc. **84** (1978), no. 2, 219–223, DOI 10.1017/S0305004100055055. MR0485683

[9] A. Bremner, D. J. Lewis, and P. Morton, *Some varieties with points only in a field extension*, Arch. Math. (Basel) **43** (1984), no. 4, 344–350, DOI 10.1007/BF01196658. MR802310

[10] 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

[11] T. 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

[12] T. Browning, P. Le Boudec, and Will Sawin, *The Hasse principle for random Fano hypersurfaces* (2020), available at `arXiv:2006.02356`.

[13] J. W. S. Cassels, *The arithmetic of certain quartic curves*, Proc. Roy. Soc. Edinburgh Sect. A **100** (1985), no. 3-4, 201–218, DOI 10.1017/S0308210500013779. MR807702

[14] 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. MR0211966

[15] S. Chowla, *On the least prime in an arithmetical progression*, J. Indian Math. Soc. **1** (1934), no. 2, 1–3.

[16] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, vol. 239, Springer, New York, 2007. MR2312337

[17] J.-L. Colliot-Thélène and B. Poonen, *Algebraic families of nonzero elements of Shafarevich-Tate groups*, J. Amer. Math. Soc. **13** (2000), no. 1, 83–99, DOI 10.1090/S0894-0347-99-00315-X. MR1697093

[18] J.-L. Colliot-Thélène and P. 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

[19] K. Conrad, *Selmer's example*, available at `https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf`.

[20] T. W. Cusick, *Lower bounds for regulators*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 63–73, DOI 10.1007/BFb0099441. MR756083

[21] D. A. Cox, *Primes of the form $x^2 + ny^2$*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013. Fermat, class field theory, and complex multiplication. MR3236783

[22] R. Dedekind, *Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. **121** (1900), 40–123, DOI 10.1515/crll.1900.121.40 (German). MR1580516

[23] A. Fröhlich, *Local fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 1–41. MR0236145

[24] M. Fujiwara, *Hasse principle in algebraic equations*, Acta Arith. **22** (1972/73), 267–276, DOI 10.4064/aa-22-3-267-276. MR0319895

[25] M. Fujiwara and M. Sudo, *Some forms of odd degree for which the Hasse principle fails*, Pacific J. Math. **67** (1976), no. 1, 161–169. MR0429737

[26] Y. Hirakawa, *Counterexamples to the local-global principle associated with Swinnerton-Dyer's cubic form* (2019), to appear in Rocky Mountain J. Math., available at `arXiv:1912.04620`.

[27] ———, *Primes of the form $X^3 + NY^3$ and a family of non-singular plane curves which violate the local-global principle* (2020), available at `arXiv:2007.11425`.

[28] Y. Hirakawa and Y. Shimizu, *Counterexamples to the local-global principle for non-singular plane curves and a cubic analogue of Ankeny-Artin-Chowla-Mordell conjecture* (2019), to appear in Proc. Amer. Math. Soc.

[29] D. R. Heath-Brown, *Cubic forms in ten variables*, Proc. London Math. Soc. (3) **47** (1983), no. 2, 225–257, DOI 10.1112/plms/s3-47.2.225. MR703978

[30] ———, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), no. 2, 265–338, DOI 10.1112/plms/s3-64.2.265. MR1143227

[31] ———, *Primes represented by $x^3 + 2y^3$*, Acta Math. **186** (2001), no. 1, 1–84, DOI 10.1007/BF02392715. MR1828372

[32] D. R. Heath-Brown and B. Z. Moroz, *Primes represented by binary cubic forms*, Proc. London Math. Soc. (3) **84** (2002), no. 2, 257–288, DOI 10.1112/plms/84.2.257. MR1881392

[33] ———, *On the representation of primes by cubic polynomials in two variables*, Proc. London Math. Soc. (3) **88** (2004), no. 2, 289–312, DOI 10.1112/S0024611503014497. MR2032509

[34] E. Hecke, *Lectures on the theory of algebraic numbers*, Graduate Texts in Mathematics, vol. 77, Springer-Verlag, New York-Berlin, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. MR638719

[35] C. Hooley, *On nonary cubic forms*, J. Reine Angew. Math. **386** (1988), 32–98, DOI 10.1515/crll.1988.386.32. MR936992

[36] ———, *On octonary cubic forms*, Proc. Lond. Math. Soc. (3) **109** (2014), no. 1, 241–281, DOI 10.1112/plms/pdt066. MR3237742

[37] A. Hurwitz, *Ueber algebraische Gebilde mit eindeutigen Transformationen in sich*, Math. Ann. **41** (1892), no. 3, 403–442, DOI 10.1007/BF01443420 (German). MR1510753

[38] V. A. Iskovskih, *A counterexample to the Hasse principle for systems of two quadratic forms in five variables*, Mat. Zametki **10** (1971), 253–257 (Russian). MR286743

[39] J. Jahnel, *More cubic surfaces violating the Hasse principle*, J. Théor. Nombres Bordeaux **23** (2011), no. 2, 471–477 (English, with English and French summaries). MR2817940

[40] G. J. Janusz, *Algebraic number fields*, 2nd ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996. MR1362545

[41] J. Li, *On primes in arithmetic progressions*, Automorphic forms and related topics, Contemp. Math., vol. 732, Amer. Math. Soc., Providence, RI, 2019, pp. 165–167, DOI 10.1090/conm/732/14789. MR3973290

[42] C. E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, Thesis, University of Uppsala, 1940 (German). MR0022563

[43] C. Lv and Y. P. Deng, *On orders in number fields: Picard groups, ring class fields and applications*, Sci. China Math. **58** (2015), no. 8, 1627–1638, DOI 10.1007/s11425-015-4979-3. MR3368170

[44] D. A. Marcus, *Number fields*, Springer-Verlag, New York-Heidelberg, 1977. Universitext. MR0457396

[45] O. Marmon and P. Vishe, *On the Hasse principle for quartic hypersurfaces*, Duke Math. J. **168** (2019), no. 14, 2727–2799, DOI 10.1215/00127094-2019-0025. MR4012347

[46] L. J. Mordell, *On the conjecture for the rational points on a cubic surface*, J. London Math. Soc. **40** (1965), 149–158, DOI 10.1112/jlms/s1-40.1.149. MR0169815

[47] ———, *On a Pellian equation conjecture. II*, J. London Math. Soc. **36** (1961), 282–288, DOI 10.1112/jlms/s1-36.1.282. MR0126411

[48] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder. MR1697859

[49] D. Q. N. Nguyen, *On the Hasse principle for certain quartic hypersurfaces*, Proc. Amer. Math. Soc. **139** (2011), no. 12, 4293–4305, DOI 10.1090/S0002-9939-2011-10936-5. MR2823075

[50] ______, *The Hasse principle for certain hyperelliptic curves and forms*, Q. J. Math. **64** (2013), no. 1, 253–268, DOI 10.1093/qmath/har041. MR3032098

[51] ______, *Certain forms violate the Hasse principle*, Tokyo J. Math. **40** (2017), no. 1, 277–299, DOI 10.3836/tjm/1502179228. MR3689991

[52] C. Pomerance, *Remarks on the Pólya-Vinogradov inequality*, Integers **11** (2011), no. 4, 531–542, DOI 10.1515/integ.2011.039. MR2988079

[53] B. Poonen, *An explicit algebraic family of genus-one curves violating the Hasse principle*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 263–274 (English, with English and French summaries). 21st Journées Arithmétiques (Rome, 2001). MR1838086

[54] B. Poonen and José Felipe 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

[55] H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*, J. Reine Angew. Math. **184** (1942), 12–18, DOI 10.1515/crll.1942.184.12 (German). MR9381

[56] P. Samuel, *Algebraic theory of numbers*, Translated from the French by Allan J. Silberger, Houghton Mifflin Co., Boston, Mass., 1970. MR0265266

[57] A. Schinzel, *Hasse's principle for systems of ternary quadratic forms and for one biquadratic form*, Studia Math. **77** (1984), no. 2, 103–109, DOI 10.4064/sm-77-2-103-109. MR743067

[58] H. A. Schwarz, *Ueber diejenigen algebraischen Gleichungen zwischen zwei veränderlichen Grössen, welche eine Schaar rationaler eindeutig umkehrbarer Transformationen in sich selbst zulassen*, J. Reine Angew. Math. **87** (1879), 139–145, DOI 10.1515/crll.1879.87.139 (German). MR1579787

[59] 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

[60] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French; Graduate Texts in Mathematics, No. 7. MR0344216

[61] ______, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237

[62] H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika **9** (1962), 54–56, DOI 10.1112/S0025579300003090. MR0139989

[63] J. T. Tate, *Global class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 162–203. MR0220697

[64] A. J. van der Poorten, H. J. J. te Riele, and H. C. Williams, *Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than* 100 000 000 000, Math. Comp. **70** (2001), no. 235, 1311–1328, DOI 10.1090/S0025-5718-00-01234-5. MR1709160

[65] A. J. Van Der Poorten, H. J. J. te Riele, and H. C. Williams, *Corrigenda and addition to: "Computer verification of the Ankeny-Artin-Chowla conjecture for all primes less than* 100 000 000 000*" [Math. Comp.* **70** *(2001), no. 235, 1311–1328; MR1709160 (2001j:11125)]*, Math. Comp. **72** (2003), no. 241, 521–523, DOI 10.1090/S0025-5718-02-01527-2. MR1933835

[66] 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