2023-08

The Negative Pell's Equation in Positive Characteri

Fujikawa, Shohei

UNIVERSITY OF CALGARY

The Negative Pell's Equation in Positive Characteristic

by

Shohei Fujikawa

A THESIS
SUBMITTED TO THE FACULTY OF GRADUATE STUDIES
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF MASTER OF SCIENCE

GRADUATE PROGRAM IN MATHEMATICS AND STATISTICS

CALGARY, ALBERTA
AUGUST, 2023

Abstract

The Pell's equation and the negative Pell's equation are two of the most well-studied topics in number theory. While the solvability of the Pell's equation over the integers is well known for centuries, the solvability problem of the negative Pell's equation over the integers, especially the density problem of how likely the negative Pell's equation is solvable, was not fully answered until recently. In this thesis, we consider these equations over the polynomial ring $\mathbb{F}[t]$ where $\mathbb{F}$ is a finite field whose characteristic is greater than 2. In Chapter 3 of this thesis, two different well-known proofs of the solvability of the Pell's equation over $\mathbb{F}[t]$ are presented. In Chapter 4, we present conditions and examples of when the negative Pell's equation is solvable and the function field analogue of the density problem on the negative Pell's equation.

Preface

Both proofs of the solvability of the Pell's equation are well known: the first proof uses the Dirichlet's unit theorem over function fields and the second proof uses the continued fraction of the formal Laurent series as in Schmidt's paper [23]. The asymptotic expression in Theorem 4.18 and Theorem 4.19 and the function field analogue of the Stevenhagen problem are original works by the author.

Acknowledgements

I would like to thank my MSc supervisor, Dr. Dang Khoa Nguyen, for his support and advice during my mathematical journey at the University of Calgary. Without his help, it is not possible to understand and appreciate the topic at the level I do. I would also like to thank Dr. Erik Thomas Holmes, a postdoctoral fellow under Dr. Nguyen, for providing frequent feedback on my writing process of this thesis. In addition, I would like to thank Dr. Mark Bauer and Dr. Renate Scheidler for joining my MSc thesis examination committee.

I would like to dedicate this thesis to my parents, Chikako and Kosei Fujikawa. Without your support, I have never been able to pursue my passion and curiosity throughout my life. Thank you for their love and support to achieve goals in my life and move me forward.

Last but not least, I would like to dedicate to this thesis my grandmother, Ryoko Kashima, who passed away during the writing process of this thesis. I remember all the fond memories with you during my time in your home. You will be missed forever.

To my parents and my grandmother.

Table of Contents

Chapter 1

Introduction

From the ancient times, a Diophantine equation, an equation with indeterminates in integers or in rational numbers, has been one of the most well studied objects in the history of mathematics [13]. In this thesis, we investigate one particular type of Diophantine equation and its variant which were well studied both in the East and the West: the Pell's equation

$$X^2 - dY^2 = 1.$$

In ancient Greece, this equation was studied using a recurrence relation to obtain an approximation of the square root of an integer, especially the square root of 2. On the other hand, Indian mathematicians, most notably Brahmagupta and Bhâskara II, discovered systematic and recursive methods to solve the Pell's equation. Despite the fact that this equation was studied for hundreds of years, it was not until the 17th and 18th century that Lagrange and other European mathematicians provided rigorous proofs about the solvability of the equation [25]. Regardless of the era, one of the central questions about an equation is whether or not it admits a solution. For the Pell's equation over the integers, this question is precisely given as follows.

Question. *Let $d > 1$ be a squarefree integer. Is there a solution to*

$$X^2 - dY^2 = 1$$

with $X, Y \in \mathbb{Z}$ and $Y \neq 0$?

Lagrange is known to give a first affirmative answer this question [13]. The techniques used to solve this equation involve ideas from elementary number theory to modern mathematical notions such as the use of continued fractions, as in [9] Chapter XIV, the consideration of real quadratic number fields and the unit

groups, as in [1] Chapter 6, and class groups and class numbers as summarized in [13]. Not only that, the Pell's equation is known to have a connection to interesting topics in modern mathematics, for example, the study of cryptography as seen in cryptographic techniques utilize the fact that the unit group of the integral closure of $\mathbb{Q}$ in quadratic number field is generated by the fundamental unit to construct a two-key cryptosystem as seen in [13].

In this thesis, we are interested in one particular variation of the Pell's equation. In particular, consider the following equation

$$X^2 - dY^2 = -1.$$

In contrast to the previous equation, this particular variation, which is often referred to as the "negative" Pell's equation [24], does not always admit a solution. It is known that the solvability depends on the prime factorization of the discriminant of the maximal order in $\mathbb{Q}(\sqrt{d})$, the norm of a fundamental unit in $\mathbb{Z}[\sqrt{d}]$, and the period length of the continued fraction expansion of $\sqrt{d}$ as documented in [24]. While there is a known case when it is not solvable, for example, d has a prime factor congruent to 3 modulo 4, the likelihood of d providing a solution to the equation was not known until recently. More precisely, the following question was not fully answered until 2022.

Question 1.1. *Let $\mathcal{D}_{\leq X}$ and $\mathcal{D}^{-}_{\leq X}$ be the set of discriminants that are not divisible by a prime congruent to 3 modulo 4 up to X of a real quadratic number field and the subset of $\mathcal{D}_{\leq X}$ with norm -1 fundamental units, respectively. Does the limit*

$$\lim_{X\to\infty} \frac{\left|\mathcal{D}^{-}_{\leq X}\right|}{\left|\mathcal{D}_{\leq X}\right|}$$

exist? If it exists, what is the limit?

This question has been studied for decades by mathematicians. Nagell confirmed that the limit inferior and the limit superior of the fraction are in the open interval $(0, 1)$ [17]. The asymptotic expression of $\left|\mathcal{D}_{\leq X}\right|$ was given as $\dfrac{cX}{\sqrt{\log(X)}}$ where

$$c = \frac{9}{8\pi} \prod_{\substack{p \text{ prime} \\ p\equiv 1 \mod 4}} \left(1 - p^{-2}\right)^{\frac{1}{2}}$$

by Rieger [20]. In addition, the asymptotic bounds of $\left|\mathcal{D}^{-}_{\leq X}\right|$ and $\left|\mathcal{D}_{\leq X} \setminus \mathcal{D}^{-}_{\leq X}\right|$ were known to satisfy

$$\left|\mathcal{D}^{-}_{\leq X}\right| \gg \frac{X}{\log(X)}$$
$$\left|\mathcal{D}_{\leq X} \setminus \mathcal{D}^{-}_{\leq X}\right| \gg \frac{X\log(\log(X))}{\log(X)}$$

as $X \to \infty$ according to Stevenhagen [24] and Dirichlet [6]. Later, Bloomer improved the asymptotic bound of $\left|\mathcal{D}^-_{\leq X}\right|$ to be

$$\left|\mathcal{D}^-_{\leq X}\right| \gg \frac{X}{(\log(X))^{0.62}}$$

[3]. While the asymptotic bounds of $\dfrac{\left|\mathcal{D}^-_{\leq X}\right|}{\left|\mathcal{D}_{\leq X}\right|}$ was shown by Fouvry and Klüners as

$$\alpha = \prod_{\substack{j \geq 1 \\ j \text{ odd}}} \left(1 - 2^{-j}\right) \leq \liminf_{X \to \infty} \frac{\left|\mathcal{D}^-_{\leq X}\right|}{\left|\mathcal{D}_{\leq X}\right|} \leq \limsup_{X \to \infty} \frac{\left|\mathcal{D}^-_{\leq X}\right|}{\left|\mathcal{D}_{\leq X}\right|} \leq \frac{2}{3}$$

[8], the limit value of the fraction was finally proven by Koymans and Pagano [14] to the value Stevenhagen has conjectured:

$$\lim_{X \to \infty} \frac{\left|\mathcal{D}^-_{\leq X}\right|}{\left|\mathcal{D}_{\leq X}\right|} = 1 - \alpha \approx 0.58058$$

Analogous to the Pell's equation and the negative Pell's equation over integers, we may consider the problems of these equations over the other kind of global field, a function field over a finite field. As Poonen summarized in Chapter 2 of [19], there are some analogies between algebraic number fields and function fields and some of the results in one class are thought to be transferable to the other. As in classical number theory over the integers, we may consider the Pell's equation over the polynomial ring $\mathbb{F}[t]$ where the finite field $\mathbb{F}$ has characteristic greater than 2; more precisely, we may consider the equation

$$X^2 - dY^2 = a^2$$

where $a \in \mathbb{F}^*$ and $d \in \mathbb{F}[t] \setminus \mathbb{F}$ is a monic squarefree polynomial. Clearly, the equation admits at least one solution regardless of the choice of d: $(X, Y) = (a, 0)$. Similar to the Pell's equation over integers, this certainly provides "trivial" solution to the Pell's equation and the next question is whether the existence of a "nontrivial" solution is guaranteed or not. In this thesis, we begin with the following question.

Question. *Let $d \in \mathbb{F}[t] \setminus \mathbb{F}$ be a monic squarefree polynomial and let $a \in \mathbb{F}^*$. Is there a solution to*

$$X^2 - dY^2 = a^2$$

with $X, Y \in \mathbb{F}[t]$ and $Y \neq 0$?

It is well known that it has an affirmative answer as documented by, for example, Schmidt [23]. The

techniques to prove the existence of a nontrivial solution are similar to how the equation over integers have nontrivial solutions; two examples of such techniques are the use of continued fractions and units in the integral closure of $\mathbb{F}[t]$ in quadratic field extension $\mathbb{F}(t)(\sqrt{d})$ and the function field analogue of the Dirichlet's unit theorem. Despite the fact that there is a nontrivial solution to the equation, we include the proofs of this fact to show some properties of the unit group of the integral closure of $\mathbb{F}[t]$ in $\mathbb{F}(t)(\sqrt{d})$ and examples of the negative Pell's equation over $\mathbb{F}[t]$, which is the next major topic of this thesis.

In addition to this "polynomial version" of the Pell's equation, this thesis explores the polynomial version of the negative Pell's equation: the equation

$$X^2 - dY^2 = c \tag{1.1}$$

where $c \in \mathbb{F}^* \setminus (\mathbb{F}^*)^2$, $(\mathbb{F}^*)^2 := \{a^2 : a \in \mathbb{F}^*\}$, and $d \in \mathbb{F}[t]$ is a non constant polynomial. Similar to the negative Pell's equation over integers, this negative Pell's equation does not always have a solution. When the squarefree polynomial d has an odd degree irreducible factor, for example, we can deduce that the negative Pell's equation does not have a solution as in Proposition 4.4. However, excluding such choice of d does not guarantee the solvability of the equation. This poses a similar question as we saw previously; how likely is the polynomial version of the negative Pell's equation solvable? More precisely, we may ask the following question.

Question 1.2. *Let $\mathbb{F}$, $\mathcal{D}_{\mathbb{F},\leq N}$ and $\mathcal{D}^-_{\mathbb{F},\leq N}$ be a finite field with characteristic greater than 2, and the sets consists of polynomials up to degree N which are the function field analogue of $\mathcal{D}_{\leq X}$ and $\mathcal{D}^-_{\leq X}$ in Question 1.1, respectively. Does the limit*

$$\lim_{N\to\infty} \frac{\left|\mathcal{D}^-_{\mathbb{F},\leq N}\right|}{\left|\mathcal{D}_{\mathbb{F},\leq N}\right|}$$

exist? If it exists, what is the limit?

In this thesis, we aim to make a step towards answering this question. In particular, we show that there are infinite sets of monic even degree polynomials with no odd degree irreducible factors, for which the negative Pell's equation is solvable, and for which it is not solvable. Additionally, we present the asymptotic expression of $|\mathcal{D}_{\mathbb{F},\leq N}|$. After this, we compare this and the cardinality of these infinite sets.

This thesis consists of 4 chapters including this introduction. Chapter 2 provides preliminary knowledge for this thesis. In particular, we introduce algebraic objects such as Dedekind domains and the residue symbol, the completion of a function field, S-units, infinite products and their convergence, and useful functions and formulae such as the Möbius inversion formula and the Gamma functions.

In Chapter 3, we explore the solvability of the polynomial version of the Pell's equation over $\mathbb{F}[t]$ where $\mathbb{F}$ is a finite field. In particular, we will see that Pell's equation given by a non constant squarefree monic even degree polynomial has a nontrivial solution. The proof of this fact is presented in two different ways. One proof involves a technique using S-units and the other involves a technique using continued fractions. Many of the techniques and facts about continued fractions introduced in this chapter are similar to the ones for continued fractions over integers as seen in a classical number theory text book such as Hardy and Wright [9].

The final chapter, Chapter 4, of this thesis focuses on the topic of the polynomial version of the negative Pell's equation. In this chapter, we first explore some of the conditions for which the negative Pell's equation is solvable, for which the equation is not solvable, and some examples. The second topic of this chapter is to give an asymptotic expression of the function field analogue of $|\mathcal{D}_{\mathbb{F},\leq N}|$; then, we compare this to the cardinality of two infinite sets, one consists of polynomials that make the equation solvable and the other consists of polynomials that make the equation not solvable. The new results by the author are presented in this section. The new results are Theorem 4.18, Theorem 4.19, Problem 4.21, Proposition 4.22, Proposition 4.24, Proposition 4.25, and its discussion.

Chapter 2

Preliminaries

The second chapter of this thesis introduces basic knowledge of algebraic number theory. In particular, this chapter covers materials related to Dedekind domains, the completion of a function field $\mathbb{F}(t)$ over a finite field $\mathbb{F}$, residue symbols in function fields, S-units, infinite products and their convergence, and some useful formulae such as the Möbius inversion formula and the Gamma function. Throughout, the characteristic of the finite field $\mathbb{F}$ is assumed to be greater than 2. The definitions and properties introduced here are taken from [1], [2], [5], [7], [10], [16], [18], [21], and [26]. Throughout this chapter, a ring always has a mutliplicative identity 1.

2.1 Dedekind domains and factorization of ideals

The materials introduced in this section are from [1], [2], [7], and [26].

Definition 2.1 (Noetherian ring)**.** *Let R be a commutative ring. R is a Noetherian ring if for every ascending chain of proper ideals*

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq ...$$

there is a natural number k such that for all $m \geq k$, $I_k = I_m$.

Proposition 2.2. *Let R be a commutative ring. Then the following are equivalent.*

1. *R is Noetherian.*
2. *Every ideal of R is finitely generated.*

3. Every nonempty set of ideals of R has its maximal element with respect to inclusion.

Proof. See [2] Chapter 6. □

Example 2.3. *Every principal ideal domain is a Noetherian ring. However, not all unique factorization domains are Noetherian rings. For example, a ring $\mathbb{F}[x_1, x_2, ...]$ with countably infinite variables is not a Noetherian ring. Indeed, there is a ascending chain of proper ideals*

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \dots.$$

Theorem 2.4 (Hilbert's basis theorem)**.** *If R is a Noetherian ring, then the polynomial ring $R[x]$ is Noetherian.*

Proof. See [2] Chapter 7. □

Definition 2.5 (Norms, traces, and characteristic polynomials)**.** *Let L/K be a finite field extension of degreee n. Fix an element $a \in L$ and a basis of L as an n dimensional K-vector space. We have the K-linear transformation $m(a)$ on L defined by $m(a)(b) = ab$ and its matrix representation $M(a)$ with respect to the fixed basis. Define the norm $N_{L/K}(a)$,the trace $T_{L/K}(a)$, and the characteristic polynomial $\operatorname{char}_{L/K}(a)$ of a relative to this field extension by*

$$N_{L/K}(a) = \det M(a)$$
$$T_{L/K}(a) = \operatorname{Tr} M(a)$$
$$\operatorname{char}_{L/K}(a) = \det(xI - M(a))$$

where I is the $n \times n$ identity matrix. Note that this definition is independent of the choice of basis since choosing another basis yields a similar matrix representation of the linear transformation. If the field extension is understood from the context, the subscript L/K is omitted from the notations of norm, trace, and characteristic polynomial.

Proposition 2.6. *Let L/K be a finite field extension of degree n. Fix an element $a \in L$. The trace $-T(a)$ and the norm $(-1)^n N(a)$ are coefficients of degree $n-1$ term and the constant term of $\operatorname{char}(a)$, respectively. Further, $\operatorname{char}(a) = (\min(a, K))^d$ where $\min(a, K)$ is the minimal polynomial of a over K and $d = [L : K(a)]$.*

Proof. See [1] Chapter 2. □

Remark 2.7. *If the field extension L/K is a degree n separable extension and $a \in L$, then $N(a)$, $T(a)$, and*

$\text{char}(a)$ *are given by*

$$N(a) = \prod_{i=1}^{n} \sigma_i(a)$$
$$T(a) = \sum_{i=1}^{n} \sigma_i(a)$$
$$\text{char}(a) = \prod_{i=1}^{n} (x - \sigma_i(a))$$

where each σ_i *is a* K*-embedding of* L *into the algebraic closure of* L*.*

Definition 2.8 (Integral extension)**.** *Let* R *and* S *be commutative rings with* $S \subseteq R$*. An element* $r \in R$ *is integral over* S *if it is a root of a monic polynomial over* S*. If all elements of* R *are integral over* S*, we say* R *is an integral extension of* S*. If* $T \subseteq R$ *is exactly the set of all intergral elements over* S*, we say* T *is the integral closure of* S *in* R*. We say* S *is integrally closed in* R *if* $S = T$*. When we simply say* S *is integrally closed, it is assumed that* S *is an integral domain with its field of fractions* K *such that* S *is integrally closed in* K*.*

Example 2.9. *Every unique factorization domain, UFD, is integrally closed. To see this, suppose that* R *is a UFD with its field of fractions* K *and* $\alpha = \frac{p}{q} \in K$ *is integral over* R *where* p *and* q *are in* R *and both* p *and* q *do not have common factors other than units in* R*. Then there is a monic irreducible polynomial*

$$f(x) = x^{n+1} + a_n x^n + ... + a_0$$

in $R[x]$ *with a root* α*. From this, we have*

$$q^{n+1} f(\alpha) = p^{n+1} + a_n p^n q + ... + a_1 p q^n + a_0 q^{n+1} = 0,$$

which implies

$$p^{n+1} = -q(a_n p^n + ... + a_1 p q^{n-1} + q^n).$$

However, this implies that p *must divide* $a_n p^n + ... + a_1 p q^{n-1} + q^n$ *since* p *and* q *are relatively prime and*

$$a_n p^n + ... + a_1 p q^{n-1} + q^n = up$$

for some $u \in R$*. It follows that* $p^{n+1} = -upq$ *and* $p^n = -uq$*. As a result,* q *must divide* p *so that* $p = vq$ *for some* $v \in R$*. But then, by the definition of* p *and* q*, such* v *must be a unit in* R*, forcing* $\alpha \in R$*.*

Example 2.10. *$\mathbb{F}[t]$ and $\mathbb{F}[t^{-1}]$ are integrally closed where t is an indeterminate. They have the common field of fractions $\mathbb{F}(t)$.*

Definition 2.11 ("AKLB" setup)**.** *An AKLB setup consists of an integral domain A with its field of fractions K, a finite separable extension L, and the integral closure B of A in L. This is summarized in the diagram below.*

$$\begin{array}{ccc} B & \text{——} & L \\ | & & | \\ A & \text{——} & K \end{array}$$

Note that this is a generalized definition of AKLB setup typically used in number theory as seen in Chapter 3 and 4 of [1] and the notes on Dedekind extension (Lecture #5) in [26]; a typical definition involves A to be a Dedekind domain, which will be introduced later in this section. Before we define a Dedekind domain, the following is one of the properties of this setup.

Proposition 2.12. *In an AKLB setup, if $x \in B$, then the coefficients of $\mathrm{char}(x)$ and $\min(x, K)$ are integral over A. If A is integrally closed, then the coefficients are in A. Moreover, if A is integrally closed and $x \in L$, $x \in B$ if and only if $\min(x, K)$ has a coefficients in A.*

Proof. See [1] Chapter 2. □

Remark 2.13. *In an AKLB setup, if A is integrally closed, then for all $a \in L$, $N(a) \in A$ and $T(a) \in A$.*

Example 2.14. *The ring $\mathbb{F}[t][\sqrt{d}]$ is the integral closure of $\mathbb{F}[t]$ in $\mathbb{F}(t)(\sqrt{d})$ where d is a squarefree polynomial in $\mathbb{F}[t] \setminus \mathbb{F}$. To see this, for every $f(t), g(t) \in \mathbb{F}[t]$, an element $f(t) + g(t)\sqrt{d} \in \mathbb{F}(t)(\sqrt{d})$ is a root of*

$$X^2 - 2f(t)X + f(t)^2 - g(t)^2 d = 0.$$

From this, $\mathbb{F}[t][\sqrt{d}] \subseteq \mathbb{F}(t)(\sqrt{d})$ is an integral extension of $\mathbb{F}[t]$ in $\mathbb{F}(t)(\sqrt{d})$. On the other hand, if we have an element $\alpha = p(t) + q(t)\sqrt{d} \in \mathbb{F}(t)(\sqrt{d})$ integral over $\mathbb{F}[t]$ where $p(t), q(t) \in \mathbb{F}(t)$, then by taking the trace of α, we know that $T(\alpha) = 2p(t) \in \mathbb{F}[t]$ and, therefore, $p(t) \in \mathbb{F}[t]$ because $\mathbb{F}$ has its characteristic not equal to 2. Because $\mathbb{F}[t]$ is integrally closed, we know that the norm $N(\alpha)$ of α is

$$N(\alpha) = p(t)^2 - dq(t)^2 \in \mathbb{F}[t]$$

by Proposition 2.12. This implies that $q_0 := dq(t)^2 \in \mathbb{F}[t]$ since $p(t) \in \mathbb{F}[t]$. If we let two relatively prime $u(t), v(t) \in \mathbb{F}[t]$ satisfy $q(t) = \dfrac{u(t)}{v(t)}$, we have

$$q_0(t)v(t)^2 = du(t)^2$$

and $v(t)^2|d$ must hold which is not possible for squarefree d, unless $v(t) \in \mathbb{F}^*$. As a result, all elements in $\mathbb{F}(t)(\sqrt{d})$ that are integral over $\mathbb{F}[t]$ are precisely in $\mathbb{F}[t][\sqrt{d}]$.

Remark 2.15. *By a similar argument and setting $x = t^{-1}$, we have $\mathbb{F}[t^{-1}][\sqrt{d}]$ is the integral closure of $\mathbb{F}[t^{-1}]$ in $\mathbb{F}(t)(\sqrt{d})$ where d is a squarefree polynomial in $\mathbb{F}[t^{-1}] \setminus \mathbb{F}$.*

Example 2.16. *Consider a degree 2 separable extension $\mathbb{F}(t)(\sqrt{d})$ over $\mathbb{F}(t)$, where d is a squarefree polynomial not in $\mathbb{F}$. Let $\alpha = (t+1) + \sqrt{d}$. Then an $\mathbb{F}(t)$-linear transformation given by $m(\alpha)(x) = \alpha x$ corresponds to the matrix M given as*

$$M = \begin{pmatrix} t+1 & d \\ 1 & t+1 \end{pmatrix}$$

in $\mathbb{F}(t)$. This implies that

$$\begin{aligned} N(\alpha) &= \det M = (t+1)^2 - d \\ T(\alpha) &= \operatorname{Tr} M = 2(t+1) \\ \operatorname{char}(\alpha) &= \det(xI - M) = (x - (t+1))^2 - d = x^2 - 2(t+1)x + (t+1)^2 - d. \end{aligned}$$

On the other hand, we know that there are two distinct $\mathbb{F}(t)$-embeddings σ_1 and σ_2 of $\mathbb{F}(t)(\sqrt{d})$ into the algebraic closure of $\mathbb{F}(t)(\sqrt{d})$ which are

$$\begin{aligned} \sigma_1(a + b\sqrt{d}) &= a + b\sqrt{d} \\ \sigma_2(a + b\sqrt{d}) &= a - b\sqrt{d}. \end{aligned}$$

This shows that

$$\begin{aligned} N(\alpha) &= \sigma_1(\alpha)\sigma_2(\alpha) = (t+1)^2 - d \\ T(\alpha) &= \sigma_1(\alpha) + \sigma_2(\alpha) = 2(t+1) \\ \operatorname{char}(\alpha) &= (x - \sigma_1(\alpha))(x - \sigma_2(\alpha)) = x^2 - 2(t+1)x + (t+1)^2 - d. \end{aligned}$$

Definition 2.17 (Dedekind domain)**.** *An integral domain R is a Dedekind domain if R is integrally closed Noetherian ring such that its nonzero prime ideals are all maximal ideals.*

Notation 2.18. *For the remainder of this section, an AKLB setup consists of a Dedekind domain A with its field of fractions K, a finite separable extension L, and the integral closure B of A in L.*

Proposition 2.19 (Prime factorization in Dedekind domain)**.** *Let R be a commutative ring. Then R is a*

Dedekind domain if and only if every nonzero proper ideal of R has a unique factorization into primes ideals of R.

Proof. See [7] Chapter 16. □

Proposition 2.20. *Consider an AKLB setup. Then B is a Dedekind domain.*

Proof. See [1] Chapter 3. □

Definition 2.21 (Lifting of an ideal)**.** *Consider an AKLB setup. Let P be a nonzero prime ideal of A. We say that the ideal PB is the lifting or the lift of P from A into B. If Q is a nonzero prime ideal of B such that $Q \cap A = P$, we say Q lies over P and P is the contraction of Q to A.*

Definition 2.22 (Ramification index and relative degree)**.** *Consider an AKLB set up. Given the factorization*

$$PS = \prod_{i=1}^{g} P_i^{e_i}$$

of the lifting of an ideal P in A to the integral closure B, we call each e_i the ramification index of P_i over P and we call $f_i = [B/P_iB : A/P]$ the relative degree of P_i over P. If there is at least one i such that $e_i > 1$, we say P ramifies. If $e_i = 1$ for all i and $g > 1$, we say P splits.

Proposition 2.23. *Consider an AKLB setup. If a nonzero prime ideal Q of B appears in the prime factorization of PB, where P is a nonzero prime ideal of A, then Q lies over P.*

Proof. See [1] Chapter 4. □

Proposition 2.24 (Dedekind-Kummer theorem)**.** *Consider an AKLB setup with $L = K(\alpha)$ for some $\alpha \in B$. Let P be a prime ideal of A and let $f \in A[t]$ be the minimal polynomial of α. Suppose we have the factorization*

$$\overline{f} \equiv u\overline{h}_1^{e_1}\overline{h}_2^{e_2}...\overline{h}_n^{e_n} \pmod{P}$$

of the reduction modulo P of f. Let Q_i be an ideal of B given by $Q_i = (P, h_i(\alpha))$ where $h_i \in A[t]$ satisfies $h_i \equiv \overline{h}_i \pmod{P}$. If $B = A[\alpha]$, then the lift PB has the prime factorization

$$PB = \prod_{i=1}^{n} Q_i^{e_i}$$

and the relative degree of Q_i is $\deg(\overline{h}_i)$

Proof. See [26] Lecture #6. □

Remark 2.25. *By the same reasoning, we have the similar result for* $A = \mathbb{F}[t^{-1}]$, $K = \mathbb{F}(t)$, $L = \mathbb{F}(t)(\sqrt{d})$, *and* $B = \mathbb{F}[t^{-1}][\sqrt{d}]$ *by setting* $x = t^{-1}$ *and* d *to be a squarefree polynomial in* $\mathbb{F}[t^{-1}] \setminus \mathbb{F}$.

Example 2.26. *Let* P *be a prime ideal of* $\mathbb{F}[t]$ *generated by* $t+1$ *and let* $d = t^2 + 2t + 2 \in \mathbb{F}[t]$ *where* $\mathbb{F} = \mathbb{F}_3$. *By the definition,* d *is irreducible in* $\mathbb{F}[t]$ *and squarefree. To compute the lifting of* P, *notice first that* $x^2 - d \in \mathbb{F}[t][x]$ *can be factored into*

$$x^2 - d \equiv x^2 - 1 \equiv x^2 - 1 \equiv (x+1)(x-1) \pmod{p}$$

As a result, by Proposition 2.24, we have

$$P\mathbb{F}[t][\sqrt{d}] = (t+1, \sqrt{d}+1)\mathbb{F}[t][\sqrt{d}](t+1, \sqrt{d}-1)\mathbb{F}[t][\sqrt{d}].$$

Proposition 2.27 (The fundamental identity of ramification index and relative degree)**.** *Consider an AKLB setup. Let* P *be a prime ideal of* A. *Suppose that we have the factorization of the lifting of* P

$$PB = \prod_{i=1}^{g} P_i^{e_i}.$$

Then

$$\sum_{i=1}^{g} e_i f_i = [B/PB : A/P] = n$$

where $[B/PB : A/P]$ *denotes the dimension of* B/PB *as an* A/P*-vector space.*

Proof. See [1] Chapter 4. □

Example 2.28. *Let* P *be a prime ideal of* $\mathbb{F}[t]$ *generated by* $t+1$ *and let* $d = t^2 + t + 2 \in \mathbb{F}[t]$ *where* $\mathbb{F} = \mathbb{F}_3$. *By the definition,* d *is irreducible in* $\mathbb{F}[t]$ *and squarefree. To compute the lifting of* P, *notice first that* $x^2 - d \in \mathbb{F}[t][x]$ *can be factored into*

$$x^2 - d \equiv x^2 - 2 \pmod{p}$$

Since 2 *is not a square in* $\mathbb{F}$, *by Proposition 2.24, we have*

$$P\mathbb{F}[t][\sqrt{d}] = (t+1, \sqrt{d}-2)\mathbb{F}[t][\sqrt{d}].$$

Now, note that $(t+1, \sqrt{d}-2)\mathbb{F}[t][\sqrt{d}]$ *has the ramification index* $e = 1$*. This implies that*

$$ef = f = [\mathbb{F}[t][\sqrt{d}]/P\mathbb{F}[t][\sqrt{d}] : \mathbb{F}[t]/(t+1)\mathbb{F}[t]] = 2$$

forcing the relative degree of $(t+1, \sqrt{d}-2)\mathbb{F}[t][\sqrt{d}]$ *to be 2.*

2.2 Completion of $\mathbb{F}(t)$

The materials introduced in this section are from [5], [16], and [18].

Definition 2.29 (Absolute value)**.** *Let* K *be a field. An absolute value* $|\cdot|$ *of* K *is a map from* K *to* $\mathbb{R}$ *satisfying the following conditions.*

1. *For all* $x \in K$, $|x| \geq 0$ *and* $|x| = 0 \iff x = 0$.
2. *For all* $x, y \in K$, $|xy| = |x||y|$.
3. *For all* $x, y \in K$, $|x + y| \leq |x| + |y|$.

If an absolute value $|\cdot|$ *satisfies the next condition, we call* $|\cdot|$ *a nonarchimedean absolute value. Otherwise, we call* $|\cdot|$ *an archimedean absolute value.*

4. *For all* $x, y \in K$, $|x + y| \leq \max\{|x|, |y|\}$.

The absolute value of a field K *defined by* $|x| = 1$ *for all nonzero* $x \in K$ *is called the trivial absolute value of* K*.*

Proposition 2.30. *An absolute value* $|\cdot|$ *of a field* K *is nonarchimedean if and only if every element in the set* $\{m \cdot 1_K : m \in \mathbb{Z}\}$ *is bounded where* 1_K *is the multiplicative identity of* K*.*

Proof. See [16] Chapter 7. □

Definition 2.31 (Valuation)**.** *Let* $|\cdot|$ *be a nontrivial nonarchimedean absolute value of a field* K*. A valuation* v *associated to* $|\cdot|$ *is a map from* K *to* $\mathbb{R} \cup \{\infty\}$ *given by the following.*

$$\text{For all nonzero } x \in K, v(x) = -\log_c |x|, \text{ and } v(0) = \infty$$

where the logarithm is taken with respect to a fixed real constant $c > 1$*.*

Remark 2.32. *Direct verification shows the following properties of a valuation* v *of a field* K*.*

1. $v(x) = \infty \iff x = 0$.

2. *For all* $x, y \in K$, $v(xy) = v(x) + v(y)$.

3. *For all nonzero* $x, y \in K$ *satisfies* $v(x+y) \geq \min\{v(x), v(y)\}$.

Definition 2.33 (P-adic and infinite valuations and absolute values on function field)**.** *Let* F *and* P *be a nonzero element in* $\mathbb{F}(t)$ *and an irreducible polynomial in* $\mathbb{F}[t]$*, respectively. Suppose that* n *is the largest possible integer such that* $F = P^n\left(\frac{f}{g}\right)$ *with* f *and* g *in* $\mathbb{F}[t]$ *and* fg *and* P *are relatively prime. The maps* $v_p : \mathbb{F}(t) \to \mathbb{Z} \cup \{\infty\}$ *and* $|\cdot|_p : \mathbb{F}(t) \to \mathbb{R}$ *given by*

$$v_p(F) = n \text{ for nonzero } F \text{ and } v_P(0) = \infty$$

and

$$|F|_P = \left(\frac{1}{q^{\deg(P)}}\right)^{v_P(F)} \text{ for nonzero } F \text{ and } |0|_P = 0$$

are called the P*-adic valuation and the* P*-adic absolute value, respectively. If the context is clear,* P *in the the subscript will be omitted. Moreover, define the infinite valuation* v_∞ *and the infinite absolute value* $|\cdot|_\infty$ *of* $\mathbb{F}(t)$ *by*

$$v_\infty\left(\frac{f}{g}\right) = \deg(g) - \deg(f) \text{ and } \left|\frac{f}{g}\right|_\infty = \left(\frac{1}{q}\right)^{v_\infty\left(\frac{f}{g}\right)}.$$

In addition, define $|0|_\infty = 0$

Remark 2.34. *By* $d(f, g) = |f - g|$*, we may consider the function field* $\mathbb{F}(t)$ *as a metric space given by an absolute value* $|\cdot|$.

Remark 2.35. *This allows the notion of Cauchy sequence with respect to an absolute value. Using this, we may construct the completion with respect to this absolute value.*

Notice that for each irreducible polynomial P, we may define valuations and absolute values. However, the equivalence of those maps allows us to restrict to one particular valuation and absolute values. To see this, we first need the notion of equivalent absolute values.

Definition 2.36 (Equivalence of absolute values)**.** *Let* $|\cdot|$ *and* $|\cdot|'$ *be two absolute values on* $\mathbb{F}(t)$*.* $|\cdot|$ *and* $|\cdot|'$ *are equivalent if they define the same topology.*

Proposition 2.37. *Let* $|\cdot|$ *and* $|\cdot|'$ *be two absolute values on* $\mathbb{F}(t)$*. They are equivalent if and only if*

$$|F| = (|F|')^s$$

for some positive real number s for all $F \in \mathbb{F}(t)$

Proof. See [18] Chapter II §3. □

Proposition 2.38 (Absolute values of $\mathbb{F}(t)$)**.** *A nontrivial absolute value of $\mathbb{F}(t)$ is equivalent to a P-adic absolute value or the infinte absolute value.*

Proof. See [5] □

Remark 2.39. *All the absolute values $|\cdot|_1$ equivalent to the P-adic absolute value $|\cdot|_P$ for $P \in \mathbb{F}[t]$ have the form*

$$|F|_1 = c_1^{v_P(F)}$$

for a fixed number $c_1 \in (0,1)$ where $F \in \mathbb{F}[t]$. Moreover, all the absolute values $|\cdot|_2$ equivalent to the infinite absolute value $|\cdot|_\infty$ have the form

$$|F|_2 = c_2^{v_\infty(F)}$$

for a fixed number $c_2 \in (0,1)$ where $F \in \mathbb{F}[t]$. This follows from Proposition 2.37.

For each P-adic absolute value $|\cdot|$ and corresponding valuation v of $\mathbb{F}(t)$ defined for a fixed irreducible polynomial, we may consider the following ring and its ideal, and its group of units.

Proposition 2.40. *Let v and $|\cdot|$ be a P-adic valuation and its corresponding absolute value, respectively. Let $\mathcal{O}$, $\mathcal{O}^*$, and $\mathfrak{m}$ be defined as*

$$\mathcal{O} = \{F \in \mathbb{F}(t) : v(F) \geq 0\} = \{F \in \mathbb{F}(t) : |F| \leq 1\}$$
$$\mathcal{O}^* = \{F \in \mathbb{F}(t) : v(F) = 0\} = \{F \in \mathbb{F}(t) : |F| = 1\}$$
$$\mathfrak{m} = \{F \in \mathbb{F}(t) : v(F) > 0\} = \{F \in \mathbb{F}(t) : |F| < 1\}.$$

Then $\mathcal{O}$, $\mathcal{O}^*$, and $\mathfrak{m}$ are a ring, the group of units of $\mathcal{O}$, and the unique maximal ideal of $\mathcal{O}$, respectively.

Proof. Direct verification using the properties of the absolute value will yield $\mathcal{O}$ is a ring and $\mathcal{O}^*$ is the group of units in $\mathcal{O}$. To see $\mathfrak{m}$ is the unique maximal ideal, note that all the elements that are not unit must have their valuation greater than 1. This implies that the set of such elements form a maximal ideal. This proves that $\mathfrak{m}$ is the unique maximal ideal. □

Definition 2.41 (Complete field)**.** *Let K be a field with an absolute value $|\cdot|$. A Cauchy sequence $\{x_n\}$ in K is a sequence from K such that for every $\epsilon > 0$, there is $N \in \mathbb{N}$ such that for all $n, m \geq N$*

$$|x_n - x_m| < \epsilon.$$

K is complete if every Cauchy sequence in $\{x_n\}$ satisfies

$$\lim_{n\to\infty} |x_n - x| = 0$$

for some $x \in K$. Such x is called the limit of $\{x_n\}$ with respect to $|\cdot|$.

Remark 2.42. *The set of Cauchy sequences in a field K forms a ring under*

$$\{x_n\} + \{y_n\} = \{x_n + y_n\}$$
$$\{x_n\}\{y_n\} = \{x_n y_n\}$$

with the additive identity $\{0\}$, the constant sequence of 0s, and the unity $\{1\}$, the constant sequence of 1s.

Definition 2.43 (Completion of a field)**.** *Let K be a field with an absolute value $|\cdot|$. Consider the set of all Cauchy sequence in K and the equivalence relation $\sim$ defined by*

$$\{x_n\} \sim \{y_n\} \iff \lim_{n\to\infty} |x_n - y_n| = 0.$$

A completion $\hat{K}$ of K is the quotient set obtained under the equivalence relation $\sim$.

Remark 2.44. *For a field K, we may consider the canonical map*

$$K \to \hat{K}$$
$$x \mapsto [\{x\}] = [\{x_n = x : n \in \mathbb{N}\}]$$

where the equivalence class of a Cauchy sequence $\{a_n\}$ is denoted by $[\{a_n\}]$.

Remark 2.45. *We may extend the absolute value $|\cdot|$ and the corresponding valuation v for K to $\hat{K}$ by*

$$|x| = \lim_{n\to\infty} |x_n|$$
$$v(x) = \lim_{n\to\infty} v(x_n)$$

where $x = \{x_n\} \in \hat{K}$. $|x|$ exists since $\{|x_n|\}$ is a convergent Cauchy sequence in $\mathbb{R}$ by

$$||x_n| - |x_m|| \leq |x_m - x_n|$$

and $\{v(x_n)\}$ is convergent by this. Moreover, $\hat{K}$ has the ring structure given by

$$[\{x_n\}] + [\{y_n\}] = [\{x_n + y_n\}]$$
$$[\{x_n\}][\{y_n\}] = [\{x_n y_n\}]$$

with the additive identity $[\{0\}]$ and the unity $[\{1\}]$, where $[\{x_n\}]$ denotes the equivalence class of $\{x_n\}$.

Proposition 2.46 (Completion has the unique maximal ideal)**.** *Let K, $|\cdot|$, and v be a field, an absolute value defined on K, and the corresponding valuation, respectively. Let R be the ring of all Cauchy sequences of a field K. Then R has the unique maximal ideal*

$$m = \{x = \{x_n\} \in R : \{|x_n|\} \text{ is a Cauchy sequence in } \mathbb{R} \text{ converging to 0.}\}.$$

Moreover,

$$\hat{K} \cong R/m.$$

Proof. First, we show m is a maximal ideal. This is because for $\{x_n\} \in R$ and $\{y_n\}, \{z_n\} \in m$, we know that

$$\lim_{n\to\infty} |x_n y_n| = \lim_{n\to\infty} |x_n||y_n| = 0$$
$$\lim_{n\to\infty} |y_n + z_n| \leq \lim_{n\to\infty} \max\{|y_n|, |z_n|\} \leq 0$$

making m an ideal. This ideal m is a maximal ideal since if there is an ideal I with $m \subsetneq I$, then there is a Cauchy sequence $\{x_n\} \in I$ converging to a non zero constant c. But then, $\{x_n^{-1}\}$ is a Cauchy sequence because of

$$|x_n^{-1} - x_m^{-1}| = |(x_m - x_n)x_n^{-1}x_m^{-1}| = |x_m - x_n||x_n^{-1}||x_m^{-1}|$$

and it converges to c^{-1} by a property of the absolute value. The uniqueness follows from the fact every element in $R \setminus m$ has its inverse given by the argument above. As a result, we know that R/m is a field. Note that this coincide with $\hat{K}$ because given two elements $\{x_n\}m$ and $\{y_n\}m$ of R/m,

$$\{x_n\}m - \{y_n\}m = 0 \iff \{x_n - y_n\}m = 0 \iff \lim_{n\to\infty} |x_n - y_n| = 0 \iff \{x_n\} \sim \{y_n\}$$

making the elements in R/m given by equivalence classes under $\sim$. □

Proposition 2.47.

$$\hat{\mathcal{O}}/\hat{\mathfrak{m}}^n \cong \mathcal{O}/\mathfrak{m}^n$$

for every positive integer n where $\hat{\mathcal{O}}$ and $\hat{\mathfrak{m}}$ are defined analogous to $\mathcal{O}$ and $\mathfrak{m}$ as in Proposition 2.40 with respect to the extended absolute value and valuations for the completion of $\mathbb{F}(t)$.

Proof. See [18] Chapter II §4. □

Proposition 2.48. *Let R be the subset of $\mathcal{O}$ consisting of representatives for $\mathcal{O}/\mathfrak{m}$. Let $\pi \in \mathcal{O}$ satisfy $v(\pi) = 1$. Then every nonzero element in the completion of $\mathbb{F}(t)$ has a unique representation in the form of*

$$\pi^n(a_0 + a_1\pi + a_2\pi^2 + ...)$$

where $a_i \in R$ for each $i \in \mathbb{N}$ and a_0 is nonzero.

Proof. See [18] Chapter II §4. □

Corollary 2.49. *The completion of $\mathbb{F}(t)$ is given by $\mathbb{F}((t^{-1}))$ with respect to $|\cdot|_\infty$. The completion of $\mathbb{F}(t)$ is given by $\mathbb{F}((t))$ with respect to $|\cdot|_t$.*

Proof. Note that the element π such that $v_\infty(\pi) = 1$ has the form $t^{-1}(a_0 + a_1t^{-1} + ... + a_nt^{-n})$ where each a_i is in $\mathbb{F}$ and $n \in \mathbb{N}$ by construction. This shows that the completion of $\mathbb{F}(t)$ is

$$\mathbb{F}((t^{-1})) = \{t^m(a_0 + a_1t^{-1} + a_2t^{-2} + ...) : m \in \mathbb{Z}, a_i \in \mathbb{F} \text{ for each } i\}.$$

By the similar argument, the element π such that $v_\infty(\pi) = 1$ has $t(a_0 + a_1t + ... + a_nt^n)$. This shows that the completion of $\mathbb{F}(t)$ with respect to v_t is

$$\mathbb{F}((t)) = \{t^m(a_0 + a_1t + a_2t^2 + ...) : m \in \mathbb{Z}, a_i \in \mathbb{F} \text{ for each } i\}.$$

□

2.3 Residue symbol

Similar to the number field case, we may define a residue symbol for a function field. Throughout, $\mathbb{F}$ is a finite field with q elements and n is a natural number dividing $q-1$. The materials introduced in this section are taken from [21].

Definition 2.50 (nth power residue symbol)**.** *Let P be an irreducible polynomial in $\mathbb{F}[t]$. The nth power residue symbol of $f \in \mathbb{F}[t]$ is*

$$\left(\frac{f}{P}\right)_n \equiv \begin{cases} f^{\frac{|P|-1}{n}} \pmod{P} & \text{if } P \nmid f \\ 0 & \text{otherwise} \end{cases}$$

where $|\cdot|$ is the infinite absolute value as defined in Definition 2.33. If n is understood from the context, it will be omitted in this thesis.

Proposition 2.51. *Let P be an irreducible polynomial in $\mathbb{F}[t]$. Suppose that $P \nmid f$. Then*

1. *The congruence $x^n \equiv f \pmod{P}$ is solvable if and only if $\left(\frac{f}{P}\right)_n = 1$,*
2. *The number of nth power in $(\mathbb{F}[t]/(P))^*$ is $\frac{|P|-1}{n}$, and*
3. *There is a unique element $\alpha \in \mathbb{F}$ such that it is congruent to $f^{\frac{|P|-1}{n}}$ modulo P so that $\left(\frac{f}{P}\right)_n$ takes on values in $\mathbb{F}$.*

Proof. See [21] Chapter 3. □

Proposition 2.52. *Let P be an irreducible polynomial in $\mathbb{F}[t]$. Then, for $f, g \in \mathbb{F}[t]$, we have the following.*

1. *If $f \equiv g \pmod{P}$, then $\left(\frac{f}{P}\right)_n = \left(\frac{g}{P}\right)_n$.*
2. *$\left(\frac{fg}{P}\right)_n = \left(\frac{f}{P}\right)_n \left(\frac{g}{P}\right)_n$.*
3. *$\left(\frac{f}{P}\right)_n = 1$ if and only if $x^n \equiv f \pmod{P}$ is solvable in $\mathbb{F}[t]$,*
4. *If $\alpha \in \mathbb{F}^*$ has multiplicative order dividing n, then there is $x \in \mathbb{F}[t]$ such that $\left(\frac{x}{P}\right)_n = \alpha$.*
5. *If $\alpha \in \mathbb{F}$, then $\left(\frac{\alpha}{P}\right)_n = \alpha^{\frac{q-1}{n} \deg P}$*

Proof. See [21] Chapter 3. □

The nth power residue symbol can be extended as in the following definition. This extended residue symbol satisfies the similar properties.

Definition 2.53. *Let $f, g \in \mathbb{F}[t]$ with $g \neq 0$. If g has the prime factorization given by $g = uP_1^{e_1} P_2^{e_2} \dots P_r^{e_r}$ where the P_i are monic irreducible polynomials and $u \in \mathbb{F}^*$, then define*

$$\left(\frac{f}{g}\right)_n = \prod_{i=1}^{r} \left(\frac{f}{P_i}\right)_n.$$

Proposition 2.54. *Let $f, g, h \in \mathbb{F}[t]$. Then we have the following.*

1. *If* $f \equiv g \pmod{h}$, *then* $\left(\frac{f}{h}\right)_n = \left(\frac{g}{h}\right)_n$.

2. $\left(\frac{fg}{h}\right)_n = \left(\frac{f}{h}\right)_n \left(\frac{g}{h}\right)_n$.

3. $\left(\frac{f}{gh}\right)_n = \left(\frac{f}{g}\right)_n \left(\frac{f}{h}\right)_n$.

4. $\left(\frac{f}{g}\right)_n \neq 0$ *if and only if* f *and* g *are relatively prime.*

5. *Given* f *and* g *are relatively prime, if there is* x *such that* $x^n \equiv f$, *then* $\left(\frac{f}{g}\right)_n = 1$.

Proof. See [21] Chapter 3. □

It is known that the following statement hold for residue symbols.

Proposition 2.55 (Reciprocity law)**.** *Let* $f, g \in \mathbb{F}[t] \setminus \{0\}$ *be relatively prime. Then*

$$\left(\frac{f}{g}\right)_n \left(\frac{g}{f}\right)_n^{-1} = (-1)^{\frac{q-1}{n} \deg(f) \deg(g)} \operatorname{sgn}_n(f)^{\deg(g)} \operatorname{sgn}_n(g)^{-\deg(f)}$$

where $\operatorname{sgn}_n(f)$ *is the leading coefficient of* f *raised to* $\frac{q-1}{n}$*th power. In particular, if* f *and* g *are monic irreducible polynomials, then we have*

$$\left(\frac{f}{g}\right)_n \left(\frac{g}{f}\right)_n^{-1} = (-1)^{\frac{q-1}{n} \deg(f) \deg(g)}.$$

Proof. See [21] Chapter 3. □

Example 2.56. *Consider the irreducible polynomial* $P = t^2 + t + 2 \in \mathbb{F}[t]$ *over* $\mathbb{F} = \mathbb{F}_3$. *Then the quadratic residue symbol of* $t^3 + 2t + 1$ *over* P *is*

$$\left(\frac{t^3 + 2t + 1}{P}\right)_2 \equiv (t^3 + 2t + 1)^{\frac{9-1}{2}} \equiv -1 \pmod{P}.$$

Meanwhile, from the properties of residue symbol, we know that

$$\left(\frac{(t^3 + 2t + 1)^2}{P}\right)_2 \equiv 1.$$

This is certainly equivalent to the fact that there is a root of

$$x^2 \equiv t^6 + t^4 + 2t^3 + t^2 + t + 1 \pmod{P}$$

in $\mathbb{F}[t]$ *since* $t^6 + t^4 + 2t^3 + t^2 + t + 1 = (t^3 + 2t + 1)^2$.

On the other hand, the reciprocity law states that

$$\begin{aligned}\left(\frac{t^3+2t+1}{P}\right)_2\left(\frac{P}{t^3+2t+1}\right)_2^{-1} &= (-1)^{\frac{3-1}{2}\cdot 3\cdot 2}\cdot 1^2\cdot 1^{-2}\\ &= 1.\end{aligned}$$

As a result,

$$\left(\frac{t^3+2t+1}{P}\right)_2 = \left(\frac{P}{t^3+2t+1}\right)_2 = -1.$$

2.4 S-units

In this section, we provide the function field analogue of the Dirichlet's unit theorem. In particular, we are interested in the unit group of the integral closure of $\mathbb{F}[t]$ in $K := \mathbb{F}(t)(\sqrt{d})$. In general, the function field analogue of the Dirichlet's unit theorem is given by the notion of S-units. Throughout this section, let d and S be a nonconstant monic squarefree even degree polynomial in $\mathbb{F}[t]$ and the set of inequivalent valuations of $\mathbb{F}(t)(\sqrt{d})$ such that their restrictions to $\mathbb{F}(t)$ are v_∞, respectively.

Proposition 2.57. *Let P_∞ be the ideal generated by t^{-1} in $\mathbb{F}[t^{-1}]$ and let $B = \mathbb{F}[t^{-1}][\sqrt{d}]$. Then*

$$P_\infty B = P_1 P_2$$

where P_1 and P_2 are distinct prime ideals in B.

Proof. See [21] Chapter 14. □

Remark 2.58. *For us, Proposition 2.24 and Proposition 2.57 imply that there are only two valuations in K whose restrictions to $\mathbb{F}(t)$ are v_∞ and each of them bijectively corresponds to one of P_1 or P_2. As a result of this, we have*

$$S = \{v_{P_1}, v_{P_2}\}.$$

Proposition 2.59. *Let $E(S)$ be given by*

$$E(S) = \{\alpha \in K : v(\alpha) = 0 \text{ for all valuation } v \notin S \text{ in } K\}.$$

Then the unit group $\mathcal{U}$ of the integral closure $\mathbb{F}[t][\sqrt{d}]$ of $\mathbb{F}[t]$ in K is $E(S)$.

Proof. See [21] Chapter 14. □

Proposition 2.60. *There exists an element* $u \in \left(\mathbb{F}[t][\sqrt{d}]^* \setminus \mathbb{F}\right)^*$ *such that for all* $x \in \mathbb{F}[t][\sqrt{d}]^*$*, there are unique* $c \in \mathbb{F}^*$ *and* $n \in \mathbb{Z}$ *such that* $x = cu^n$*.*

Proof. From Corollary 1 in Chapter 14 of [21], we know that

$$\mathbb{F}[t][\sqrt{d}]^* \cong G \times F$$

where G is an abelian group whose elements have finite order and F is a free group of rank 1. From this, for all $x \in \mathbb{F}[t][\sqrt{d}]^*$, there are c, $u \in \mathbb{F}[t][\sqrt{d}]^* \setminus \mathbb{F}^*$, and $n \in \mathbb{Z}$ such that $x = cu^n$. We claim that $c \in \mathbb{F}^*$. To see this, suppose that $x = a + b\sqrt{d} \in \mathbb{F}[t][\sqrt{d}]^*$ has a finite order m. Then we know that

$$x^m = (a + b\sqrt{d})^m = 1$$

must happen and this implies x is algebraic over $\mathbb{F}$ and it is an element in $\mathbb{F}(x)$ whose order is q^r where $q = |\mathbb{F}|$. Then, since $\mathbb{F}$ has the characteristic greater than 2 making q odd, we have

$$x^{q^r} = x \iff (a + b\sqrt{d})^{q^r} = a^{q^r} + b^{q^r} d^{\frac{q^r-1}{2}} \sqrt{d} = a + b\sqrt{d}.$$

Since $\deg(b^{q^r} d^{\frac{q^r-1}{2}}) > \deg(b)$ for nonzero b, $b = 0$ must happen. Similarly, $\deg(a^{q^r}) > \deg(a)$ for $a \notin \mathbb{F}$ and $x \in \mathbb{F}[t][\sqrt{d}]^*$, we have $a \in \mathbb{F}^*$. As a result, we have

$$\mathbb{F}[t][\sqrt{d}]^* \cong \mathbb{F}^* \times F$$

where F is a free abelian group of rank 1. The uniqueness follows from the isomorphism

$$\mathbb{F}[t][\sqrt{d}]^* \cong G \times F.$$

□

2.5 Complex analysis

The major complex analytic tools used in this thesis is the convergence of infinite products. The materials here are taken from [10] Chapter 8.

Definition 2.61 (Infinite products)**.** *Let* $\{a_n\}$ *be a sequence of nonzero complex numbers. An infinite*

product of $\{a_n\}$ *is an ordered pair of sequences* $[\{a_n\}, \{p_n\}]$ *where for each* n,

$$p_n = \prod_{i=1}^{n} a_i.$$

For each n, *the element* a_n *of the sequence* $\{a_n\}$ *is called the* n*th factor and the element* p_n *of the sequence* $\{p_n\}$ *is called the* n*th partial product. When we consider the infinite product* $[\{a_n\}, \{p_n\}]$, *we often denote this by*

$$\prod_{n=1}^{\infty} a_n.$$

We say the infinite product $[\{a_n\}, \{p_n\}]$ *converges if there are at most finitely many zeros in the sequence* $\{a_n\}$ *and the sequence of partial products of nonzero factors of* $\{a_n\}$ *converges to a nonzero constant.*

Remark 2.62. *Let* $\prod_{n=1}^{\infty} a_n$ *be a convergent infinte product and let* $\{p_n\}$ *be its sequence of nonzero partial products. Then*

$$\lim_{n\to\infty} \frac{p_n}{p_{n-1}} = 1$$

and therefore,

$$\lim_{n\to\infty} a_n = 1.$$

As a result, the convergent infinte product is also often denoted as

$$\prod_{n=1}^{\infty} (1 + b_n)$$

where $\{b_n\}$ *is a sequence converging to* 0.

Definition 2.63 (Absolute convergence of infinite products)**.** *An infinite product* $\prod_{n=1}^{\infty} (1 + a_n)$ *converges absolutely if the series* $\sum_{n=1}^{\infty} \log(1 + a_n)$ *converges absolutely.*

Proposition 2.64. *Consider an infinite product*

$$\prod_{n=1}^{\infty} (1 + a_n)$$

with nonzero factors. Then the following hold.

1. *The infinite product converges if and only if the series* $\sum_{n=1}^{\infty} \log(1 + a_n)$ *converges,*
2. *The series* $\sum_{n=1}^{\infty} \log(1 + a_n)$ *absolutely converges if and only if the series* $\sum_{n=1}^{\infty} a_n$ *converges absolutely*

where $\log(x)$ *denotes the principal value of* x.

Proof. See [10] Chapter 8. □

Proposition 2.65. *Given a nonzero sequence $\{a_n\}$ with $|a_n| < 1$ converging to 0 and a sequence of nonzero numbers $\{c_n\}$, if the series*

$$\sum_{n=1}^{\infty} c_n a_n$$

converges absolutely, then the infinite product

$$\prod_{n=1}^{\infty} (1 + a_n)^{c_n}$$

converges. Moreover, we may rearrange the order of the factors in the infinite product.

Proof. The proof is analogous to the argument seen in Chapter IV of [4] but is included for convenience for the readers. Since $\{a_n\}$ is a converging sequence with limit 0, we know that for a positive real number $M < \frac{1}{2}$, there is N such that for all $n \geq N$, $|a_n| < M$. This implies that $|c_n a_n| < M|c_n|$. Now, using the power series expression of the logarithm

$$\log(1 + x) = \sum_{n=1} \frac{(-1)^{n+1} x^n}{n},$$

for $n \geq N$, we have

$$\begin{aligned} |\log(1 + a_n)| &\leq \sum_{k=1}^{\infty} \frac{|a_n|^k}{k} \\ &\leq |a_n| + \sum_{k=2}^{\infty} \frac{|a_n|^k}{k} \\ &\leq |a_n| + \sum_{k=2}^{\infty} \frac{|a_n|^k}{2} \\ &= |a_n| + \frac{1}{2} \cdot \frac{|a_n|^2}{1 - |a_n|} \\ &< 2|a_n| \end{aligned}$$

since $\frac{|a_n|}{1-|a_n|} < 1$ by $|a_n| < \frac{1}{2}$. As a result, we have

$$0 \leq |c_n||\log(1 + a_n)| = |c_n \log(1 + a_n)| < 2|c_n||a_n| = 2|c_n a_n|$$

But then, by the assumption that the series $\sum_{n=1}^{\infty} c_n a_n$ converges absolutely, the series $\sum_{n=1}^{\infty} c_n \log(1 + a_n)$

converges absolutely. From this, we know that the infinite product $\prod_{n=1}^{\infty}(1+a_n)^{c_n}$ converges since

$$\prod_{n=1}^{\infty}(1+a_n)^{c_n} = e^{\sum_{n=1}^{\infty} c_n \log(1+a_n)}.$$

Reordering of each factor has no effect on what value the infinite product takes since $\sum_{n=1}^{\infty} c_n \log(1+a_n)$ converges absolutely and we may rearrange each term without changing the value of the series. □

Example 2.66. *Consider the infinite product*

$$\prod_{n=1}^{\infty}\frac{n^3+2n}{n^3+1} = \prod_{n=1}^{\infty}\left(1+\frac{2n-1}{n^3+1}\right).$$

Then we know that $\frac{2n-1}{n^3+1}$ *converges to 0 as* $n \to \infty$ *and the sum*

$$\sum_{n=1}^{\infty}\frac{2n-1}{n^3+1} \leq \sum_{n=1}^{\infty}\frac{2n-1}{n^3} \leq \sum_{n=1}^{\infty}\frac{2}{n^2}$$

converges absolutely since $\left|\frac{2n-1}{n^3+1}\right| = \frac{2n-1}{n^3+1}$. *Therefore,*

$$\sum_{n=1}^{\infty}\log\left(1+\frac{2n-1}{n^3+1}\right)$$

converges absolutely and the infinite product converges.

2.6 Useful Formulas

In this thesis, two functions, the Möbius function and the Gamma function, are used. This section provides the definitions and some formulae about them. The materials in this section are taken from [10] and [12].

Definition 2.67 (Möbius function)**.** *The Möbius function* μ *is a function from* $\mathbb{Z}^+$ *to* $\{-1,0,1\}$ *such that*

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n \text{ is not squarefree} \\ (-1)^l \text{ if } l \text{ is the number of distinct prime factors of squarefree } n \end{cases}$$

Remark 2.68. *Notice that when two positive integers* m *and* n *are relatively prime, then* $\mu(mn) = \mu(m)\mu(n)$. *This is because if one of them, say* m*, is 1, then* $\mu(mn) = \mu(n) = \mu(m)\mu(n)$*; if neither of them is 1, then*

mn has no square prime factors since m and n are coprime, so we have $\mu(mn) = \mu(m)\mu(n)$ by the prime factorizations of m, n, and mn.

Proposition 2.69 (Möbius inversion formula)**.** *Let n be a positive integer, f be a complex valued function, and*

$$F(n) = \sum_{d|n} f(d).$$

Then

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

where μ is the Möbius function.

Proof. See [12] Chapter 2 §2. □

Definition 2.70 (Gamma function)**.** *The Gamma function $\Gamma(z)$ on $\mathbb{C}$ is defined as*

$$\Gamma(z) = \frac{e^{-\gamma z}}{z} \prod_{n=1}^{\infty} \left(1 + \frac{z}{n}\right)^{-1} e^{\frac{z}{n}}$$

where γ is the limit

$$\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} - \log(n)\right).$$

The Gamma function has important basic properties, one of which is similar to the factorial function defined on positive integers.

Proposition 2.71 (Properties of gamma function)**.** *For a complex number z, the following statements hold.*

1. $\Gamma(z+1) = z\Gamma(z)$. *In particular, for a positive integer n,* $\Gamma(n) = n!$.
2. $\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}$
3. $\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}$
4. $\left(\frac{\Gamma'(z)}{\Gamma(z)}\right)' = \sum_{n=0}^{\infty} \frac{1}{(z+n)^2}$

Proof. See [10] Chapter 8 §8.4. □

Proposition 2.72 (Equivalent definition of gamma function)**.**

$$\Gamma(z) = \lim_{n\to\infty} \frac{n^z n!}{(z)_{n+1}} = \int_0^{\infty} e^{-\sigma} \sigma^{x-1} d\sigma$$

where $(z)_m = \prod_{k=0}^{m}(z+k)$.

Proof. See [10] Chapter 8 §8.4. □

Proposition 2.73 (Legendre duplication formula)**.**

$$\frac{\Gamma(z)\Gamma(z+\frac{1}{2})}{\Gamma(2z)} = 2^{1-2z}\sqrt{\pi}$$

Proof. See [10] Chapter 8 §8.4. □

Chapter 3

The Solvability of the Pell's Equation

Throughout this chapter, $\mathbb{F}$ is a finite field with characteristic greater than 2. The Pell's equation over the polynomial ring $\mathbb{F}[t]$ is a Diophantine equation

$$X^2 - dY^2 = c^2$$

where $c \in \mathbb{F}^*$ and $d \in \mathbb{F}[t] \setminus \mathbb{F}$. Notice that, by $X = cX'$ and $Y = cY'$, we may assume the Pell's equation is given by

$$X^2 - dY^2 = 1.$$

We can see that it always has at least one solution, the trivial solution $(X, Y) = (\pm 1, 0)$. This poses a question about whether a nontrivial solution, a solution with $Y \neq 0$, exists or not.

Question. *Given a polynomial $d \in \mathbb{F}[t] \setminus \mathbb{F}$, is there a nontrivial solution to the Pell's equation over $\mathbb{F}[t]$?*

In this chapter, we provide a complete answer to this question. When the polynomial d has odd degree and Y is nonzero, then

$$\deg(X^2 - dY^2) = \max\{\deg(X^2), \deg(dY^2)\} > 0.$$

This means that there is at least one non-constant term. As a result, $X^2 - dY^2$ cannot be in $\mathbb{F}^*$ and the Pell's equation does not have a nontrivial solution. This implies that d must be an even degree polynomial to give a nontrivial solution. Furthermore, the polynomial d must have a square leading coefficient. Otherwise, the degree of $X^2 - dY^2$ is at least that of dY^2 since the leading term of dY^2 is not cancelled out. If d has a square leading coefficient c_d^2 for some $c_d \in \mathbb{F}^*$, by setting $Y = c_d^{-1}Y'$, we may assume d to be monic. For

this reason, we may assume $d \in \mathbb{F}[t]$ is a nonconstant monic even degree squarefree polynomial.

It is well known that the Pell's equation over the integers has a nontrivial solution as in, for example, [13]. Using the analogous techniques for the integers, we may prove that the Pell's equation over $\mathbb{F}[t]$ for d above has a nontrivial solution, as in, for example, [23]. In this chapter, we explore the solvability of the Pell's equation. Precisely, we are interested in the following statement.

Theorem 3.1. *Let d be a nonconstant monic even degree squarefree polynomial. The Pell's equation*

$$X^2 - dY^2 = 1$$

has a nontrivial solution (X, Y) (i.e., $Y \neq 0$) in $\mathbb{F}[t]$.

We prove this statement in two different ways. In the first section 3.1, a proof by S-units is presented. Then, in the following sections, a proof by continued fractions is presented. The motivation behind to prove in two ways is that this allows us to construct tools and examples in Chapter 4.

3.1 The existence of nontrivial solutions by S-Units

This section provides a proof of Theorem 3.1 using S-units.

Proof. Let S be the set of primes lying above the place at infinity in $\mathbb{F}(t)(\sqrt{d})$. Notice first that the existence of a nontrivial solution to $X^2 - dY^2 = 1$ is equivalent to the existence of a unit $a + b\sqrt{d}$ with norm 1 in the integral closure of $\mathbb{F}[t]$ in $\mathbb{F}(t)(\sqrt{d})$ and $b \neq 0$. Since the polynomial d is a monic squarefree even degree polynomial, the unit group of this integral closure of $\mathbb{F}[t]$ in $\mathbb{F}(t)(\sqrt{d})$ is $E(S)$ from Proposition 2.59. Moreover, by Proposition 2.60, we have

$$E(S) = \mathbb{F}^* \times \langle a + b\sqrt{d} \rangle$$

for some nonzero $a, b \in \mathbb{F}[t]$. By

$$N(a + b\sqrt{d})^2 = N((a + b\sqrt{d})^2),$$

$N\left((a + b\sqrt{d})^2\right)$ is a square in $\mathbb{F}^*$. If we set $u = N(a + b\sqrt{d})$, we have an element

$$u^{-1}(a + b\sqrt{d})^2 = u^{-1}\left((a^2 + db^2) + 2ab\sqrt{d}\right)$$

in the unit group. This element certainly satisfies

$$N(u^{-1}(a+b\sqrt{d})^2) = u^{-2}((a^2+db^2)^2 - (2ab\sqrt{d})^2) = u^{-2}(a^2+db^2)^2 - du^{-2}(2ab)^2 = 1$$

From this, we have a norm 1 element in the unit group and, therefore, we now have a nontrivial solution $(X,Y) = (u^{-1}(a^2+db^2), 2u^{-1}ab)$ to Pell's equation. □

3.2 Continued fractions in a function field

While we have already established Theorem 3.1, we aim to show the same result using continued fractions. By a similar argument used in classical number theory over the integers as in [9], we may characterize elements in $\mathbb{F}((t^{-1}))$ in terms of the length of their continued fraction expansion. In particular, we show an element in $\mathbb{F}((t^{-1}))$ has an infinite continued fraction expansion if and only if it is not in $\mathbb{F}(t)$. This and the following section mainly refer to a book by Hardy and Wright [9], a dissertation by Malagoli [15], and a paper by Schmidt [23].

Notation 3.2. *For the remainder, let the absolute value $|\cdot|$ and v denote the infinite absolute value $|\cdot|_\infty$ and the infinite valuation v_∞ as defined in Definition 2.33. Recall that completion of $\mathbb{F}(t)$ with respect to $|\cdot|$ is $\mathbb{F}((t^{-1}))$ which is given in Proposition 2.49.*

3.2.1 Finite continued fractions

In order to define an infinite continued fraction, we first need the notion of a finite continued fraction. This is because an infinite continued fraction is defined as the limit of a converging sequence of finite continued fractions.

Definition 3.3 (Finite Continued fractions)**.** *Let $p_0, p_1, ..., p_n$ be in $\mathbb{F}((t^{-1}))$ where each p_i is nonzero for $i \geq 1$. A finite continued fraction or a finite continued fraction expansion is*

$$[p_0, p_1, ..., p_n] = \begin{cases} p_0 & \text{if } n = 0 \\ p_0 + \frac{1}{p_1} & \text{if } n = 1 \\ [p_0, p_1, ..., p_{n-1} + \frac{1}{p_n}] & \text{if } n \geq 2. \end{cases}$$

In particular, if all of the p_i are polynomials in $\mathbb{F}[t]$ with $|p_i| > 1$ for each $i > 0$, $[p_0, p_1, ..., p_n]$ is a finite regular continued fraction.

Remark 3.4. *By the definition, for* $1 \leq m \leq n$, $[p_0, p_1, ..., p_n] = [p_0, p_1, ..., p_m, [p_{m+1}, ..., p_n]]$.

A finite regular continued fraction plays an important role because it provides another expression for the elements in $\mathbb{F}(t)$.

Proposition 3.5 ($\mathbb{F}(t)$ is the field of finite regular continued fractions)**.** *An element in* $\mathbb{F}(t)$ *has a unique finite regular continued fraction expansion.*

Proof. This is well-known but we include a proof for the convenience for readers.

Let $x = \dfrac{h_0}{k_0} \in \mathbb{F}(t)$ with h_0 and nonzero k_0 are in $\mathbb{F}[t]$. Notice first that by the definition of x, we know that we may express x as the following:

$$x = a_0 + \epsilon_0 = \frac{h_0}{k_0}$$

where $a_0 \in \mathbb{F}[t]$ is the quotient of the Euclidean division $\frac{h_0}{k_0}$ and $\epsilon_0 \in \mathbb{F}(t)$ is defined so that $k_0\epsilon_0$ is the remainder. Note that $|\epsilon| < 1$. If $\epsilon_0 = 0$, then we have $x = [a_0]$. Otherwise, by $\alpha_0 = \frac{1}{\epsilon_0}$,

$$x = a_0 + \frac{1}{\alpha_0}.$$

Now, since $\epsilon_0 = x - a_0 \in \mathbb{F}(t)$, we may consider $a_1 \in \mathbb{F}[t]$ and $\epsilon_1 \in \mathbb{F}(t)$, analogous to a_0 and ϵ_0 with $|a_1| > 1$ and $|\epsilon_1| < 1$. If $\epsilon_1 = 0$, then x has a finite regular continued fraction expansion $x = [a_0, a_1]$. Otherwise, repeat this process and define k_{n+1} for $n \geq 0$ by $k_{n+1} = \epsilon_n k_n$. Then we obtain the following sequence.

$$\begin{aligned}
\frac{h_0}{k_0} &= a_0 + \epsilon_0 \\
\frac{k_0}{k_1} &= a_1 + \epsilon_1 \\
\frac{k_1}{k_2} &= a_2 + \epsilon_2 \\
&\vdots
\end{aligned}$$

By construction, notice that $\{|k_n|\}$ is a strictly decreasing sequence by the recursive definition of k_n and the multiplicative property of $|\cdot|$. Moreover, from the sequence above, we have

$$\begin{aligned}
h_0 &= a_0k_0 + \epsilon_0k_0 \\
k_0 &= a_1k_1 + \epsilon_1k_1 \\
k_1 &= a_2k_2 + \epsilon_2k_2 \\
&\vdots
\end{aligned}$$

and, because of $k_{n+1} = \epsilon_n k_n$, $k_0 \in \mathbb{F}[t]$, and $h_0 \in \mathbb{F}[t]$, we have each of k_n to be in $\mathbb{F}[t]$. This implies that $\{|k_n|\}$ is a strictly decreasing sequence and, therefore, $\{\deg(k_n)\}$ is a strictly decreasing sequence of positive integers. So, this process terminates after at most finitely many steps. As a result, we have

$$\begin{aligned} h_0 &= a_0 k_0 + \epsilon_0 k_0 \\ k_0 &= a_1 k_1 + \epsilon_1 k_1 \\ k_1 &= a_2 k_2 + \epsilon_2 k_2 \\ &\vdots \\ k_N &= a_{N+1} k_{N+1}. \end{aligned}$$

From this, we have a finite continued fraction

$$x = [a_0, a_1, ..., a_{N+1}].$$

Furthermore, the choice of each a_n is unique because each of them is chosen so that $|a_n| > 1$ for $n \geq 1$ and $|\epsilon_n| < 1$ for all n by their definitions. □

By this proposition, given an element in $\mathbb{F}(t)$, we may construct two sequences $\{P_n\}$ and $\{Q_n\}$ of polynomials in $\mathbb{F}[t]$ from its finite continued fraction expansion. These sequences have the following important properties.

Proposition 3.6. *Let $[a_0, ..., a_n] \in \mathbb{F}(t)$ be a finite regular continued fraction expansion. Define the sequences $\{P_n\}$ and $\{Q_n\}$ starting from $n = -2$ as*

- $P_{-2} = 0,\ Q_{-2} = 1,\ P_{-1} = 1,\ Q_{-1} = 0$
- $P_n = a_n P_{n-1} + P_{n-2},\ Q_n = a_n Q_{n-1} + Q_{n-2}$.

Then

1. $Q_n P_{n-1} - P_n Q_{n-1} = (-1)^n$ *for* $n \geq -1$.
2. $[a_0, ..., a_n] = \dfrac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}} = \dfrac{P_n}{Q_n}$ *for* $n \geq 0$.
3. $|P_n| = |a_n||P_{n-1}|$ *and* $|Q_n| = |a_n||Q_{n-1}|$ *for* $n \geq 1$.
4. P_n *and* Q_n *are relatively prime for* $n \geq -1$.

Proof. The proof is analogous to the integer case. See [9] Chapter X and use properties of the absolute value $|\cdot|$. □

Using the same notation as in the preceding proposition, we have the following corollary.

Corollary 3.7. *For a finite regular continued fraction $x = [a_0, a_1, ..., a_n]$, we have the following.*

1. $P_kQ_{k-2} - Q_kP_{k-2} = (-1)^k a_k$ *and* $\dfrac{P_k}{Q_k} - \dfrac{P_{k-2}}{Q_{k-2}} = \dfrac{(-1)^k a_k}{Q_kQ_{k-2}}$ *for* $k \geq 0$.
2. $\dfrac{P_{k+1}}{Q_{k+1}} - \dfrac{P_k}{Q_k} = \dfrac{(-1)^{k+1}}{Q_{k+1}Q_k}$.
3. *If* $\alpha_k = [a_k, a_{k+1}, ..., a_n]$, *then* $x = \dfrac{\alpha_k P_{k-1} + P_{k-2}}{\alpha_k Q_{k-1} + Q_{k-2}}$ *for* $k \geq 0$.
4. *If* $\alpha_k = [a_k, a_{k+1}, ..., a_n]$ *for* $1 \leq k \leq n$, *then for* $|\alpha_k| = |a_k|$.
5. *If* $\alpha_k = [a_k, a_{k+1}, ..., a_n]$ *for* $1 \leq k \leq n$, *then* $|P_n| = |\alpha_n||P_{n-1}|$ *and* $|Q_n| = |\alpha_n||Q_{n-1}|$ *for* $n \geq 1$.
6. $\left|[a_0, a_1, ..., a_n, \alpha_{n+1}] - \dfrac{P_n}{Q_n}\right| = \dfrac{1}{|Q_n||Q_{n+1}|} = \dfrac{1}{|a_{n+1}||Q_n|^2}$ *for* $n \geq 0$.

Proof. The proof is analogous to the integer case. See [9] Chapter X and apply properties of absolute value $|\cdot|$. □

Example 3.8. *Let* $\mathbb{F} = \mathbb{F}_3$ *and consider an element* $\dfrac{t^3 + 2t + 2}{t^2 + t + 2}$ *in* $\mathbb{F}(t)$. *Applying polynomial long division, we have*

$$\begin{aligned} \frac{t^3 + 2t + 2}{t^2 + t + 2} &= t + 2 + \frac{t + 1}{t^2 + t + 2}, \\ \frac{t^2 + t + 2}{t + 1} &= t + \frac{2}{t + 1}, \\ \frac{t + 1}{2} &= 2t + 2 \end{aligned}$$

From this, we obtain a finite continued fraction expansion $\dfrac{t^3 + 2t + 2}{t^2 + t + 2} = [t + 2, t, 2t + 2]$. *In addition, we have the sequences* $\{P_n\}$ *and* $\{Q_n\}$ *as:*

$$\begin{aligned} &P_{-2} = 0, \quad P_{-1} = 1, \quad P_0 = t + 2, \quad P_1 = t^2 + 2t + 1, \quad P_2 = 2t^3 + t + 1, \\ &Q_{-2} = 1, \quad Q_{-1} = 0, \quad Q_0 = 1, \quad Q_1 = t, \quad Q_2 = 2t^2 + 2t + 1. \end{aligned}$$

If we let $\alpha_1 = [t, 2t + 2]$ *and* $\alpha_2 = [2t + 2]$, *then*

$$\frac{\alpha_1 P_0 + P_{-1}}{\alpha_1 Q_0 + Q_{-1}} = \frac{\frac{t(2t+2)+1}{2t+2}(t + 2) + 1}{\frac{t(2t+2)+1}{2t+2} + 0} = \frac{t^3 + 2t + 2}{t^2 + t + 2}$$

and

$$\frac{\alpha_2 P_1 + P_0}{\alpha_2 Q_1 + Q_0} = \frac{(2t + 2)(t^2 + 2t + 1) + t + 2}{(2t + 2)t + 1} = \frac{t^3 + 2t + 2}{t^2 + t + 2}.$$

Moreover,

$$\begin{aligned}\left|[t+2,\alpha_1]-\frac{P_0}{Q_0}\right| &= \left|\frac{\alpha_1 P_0+P_{-1}}{\alpha_1 Q_0+Q_1}-\frac{P_0}{Q_0}\right| \\ &= \left|\frac{P_{-1}Q_0-P_0Q_{-1}}{(\alpha_1 Q_0+Q_{-1})Q_0}\right| \\ &= \left|\frac{(-1)^1}{Q_1Q_0}\right| = \frac{1}{|Q_1||Q_0|} \\ &= \frac{1}{|(\alpha_1 Q_0+Q_{-1})||Q_0|} = \frac{1}{|\alpha_1||Q_0|^2}\end{aligned}$$

3.2.2 Infinite continued fractions

In the previous section, we defined finite continued fractions in $\mathbb{F}((t^{-1}))$ and their properties. We may extend the definition of finite continued fractions to infinite continued fractions using the notion of limit with respect to $|\cdot|$. In particular, we are interested in infinite regular continued fractions.

Definition 3.9 (Infinite regular continued fraction)**.** *Let $a_0, a_1, a_2, ...$ be polynomials in $\mathbb{F}[t]$ such that $|a_i| > 1$ for $i \geq 1$. Let $\{x_n\}$ be a sequence in $\mathbb{F}[t]$ where each term is a finite regular continued fraction expansion given by*

$$x_n = [a_0, a_1, a_2, ..., a_n].$$

An infinite regular continued fraction expansion $x = [a_0, a_1, ...]$ is the limit of $\{x_n\}$ with respect to $|\cdot|$, if it exists. If such limit exists, we call each a_n the n-th partial quotient and $\alpha_n = [a_n, a_{n+1}, ...]$ the n-th complete quotient. Moreover, we call each $[a_0, a_1, ..., a_n]$ the n-th convergent.

Remark 3.10. *Because each x_n is an element in $\mathbb{F}(t)$ in the above definition, the infinite sequences $\{P_n\}$ and $\{Q_n\}$ analogously defined in Proposition 3.6 are well-defined.*

Remark 3.11. *Notice that direct verification yields that for $\alpha = [a_0, a_1, ...] \in \mathbb{F}((t^{-1}))$ and for $a \in \mathbb{F}^\times$, $a\alpha = [aa_0, a^{-1}a_1, aa_2, ...]$.*

Similar to how a finite regular continued fraction provides another expression for an element in $\mathbb{F}(t)$, an infinite regular continued fraction provides a new expression for an element in $\mathbb{F}((t^{-1})) \setminus \mathbb{F}(t)$.

Proposition 3.12. *An element $x \in \mathbb{F}((t^{-1}))$ can be expressed as a unique regular infinite continued expansion of polynomials in $\mathbb{F}[t]$ if and only if it is not in $\mathbb{F}(t)$.*

Proof. This is well-known as pointed out in [23] but the proof is included for the readers' convenience. Define

a function $G : \mathfrak{M} \to \mathfrak{M}$ such that

$$x \mapsto \begin{cases} 0 & \text{if } x = 0 \\ \frac{1}{x} - \left\lfloor \frac{1}{x} \right\rfloor & \text{otherwise.} \end{cases}$$

where $\mathfrak{M}$ is the set of elements in $\mathbb{F}((t^{-1}))$ with absolute value strictly less than 1 and $\lfloor x \rfloor$ is the polynomial $x' \in \mathbb{F}[t]$ with the largest possible degree so that $|x - x'| < 1$.

Now, suppose $x \in \mathbb{F}((t^{-1})) \setminus \mathbb{F}(t)$ with $|x| < 1$ and define a sequence $\{a_n\}$ starting from $n = 1$ as

$$a_1 = \left\lfloor \frac{1}{x} \right\rfloor$$
$$a_n = \left\lfloor \frac{1}{G^{n-1}(x)} \right\rfloor \text{ for } n > 1$$

Notice that since $x \notin \mathbb{F}(t)$, we know that this definition enumerates infinitely many nonzero terms for the sequence. This is because if it only enumerates finitely many nonzero terms, say $N+1$ gives the last nonzero term in the sequence, then we know that, by the definition of G,

$$G^{k+1}(x) = \frac{1}{G^k(x)} - \left\lfloor \frac{1}{G^k(x)} \right\rfloor \Longrightarrow G^k(x) = \frac{1}{G^{k+1}(x) - \left\lfloor \frac{1}{G^k(x)} \right\rfloor}$$

for each $1 \leq k \leq N$ and applying this repeatedly up to $k = N$ implies $G(x) \in \mathbb{F}(t)$. This further implies that $x \in \mathbb{F}(t)$ which is a contradiction to $x \notin \mathbb{F}(t)$. We claim and prove $|x - [0, a_1, a_2, ..., a_n]| \leq c^n$ by induction where $|t^{-1}| = c < 1$. To see this, notice first that $|x| \leq c$ by $|x| < 1$ and $|a_1| \geq \frac{1}{c} > 1$ since $a_1 \in \mathbb{F}[t]$. Then we have

$$|x - \frac{1}{a_1}| \leq c$$

For the induction, suppose that for $k \geq 1$, we have

$$|x - [0, a_1, a_2, ..., a_k]| \leq c^k.$$

Then notice that we have

$$\frac{1}{[0, a_1, a_2, ..., a_{k+1}]} = a_1 + [0, a_2, ..., a_{k+1}]$$

and

$$\left| \frac{1}{x} - \frac{1}{[0, a_1, a_2, ..., a_{k+1}]} \right| = \left| \frac{1}{x} - a_1 - [0, a_2, ..., a_{k+1}] \right| \leq c^k$$

by applying the induction hypothesis for $\frac{1}{x} - a_1$. At the same time, since

$$\left|\frac{1}{x} - \frac{1}{[0, a_1, a_2, ..., a_{k+1}]}\right| = \left|\frac{[0, a_1, a_2, ..., a_{k+1}] - x}{x[0, a_1, a_2, ..., a_{k+1}]}\right|,$$

we have

$$\left|\frac{[0, a_1, a_2, ..., a_{k+1}] - x}{x[0, a_1, a_2, ..., a_{k+1}]}\right| \leq c^k.$$

This implies that

$$|[0, a_1, a_2, ..., a_{k+1}] - x| \leq c^k \, |x| \, |[0, a_1, a_2, ..., a_{k+1}]| \leq c^{k+2} < c^{k+1}$$

because $c < 1$, $|x| \leq c$, and $|[0, a_1, a_2, ..., a_{k+1}]| \leq c$. By induction, we have $|x - [0, a_1, a_2, ..., a_n]| \leq c^n$ for each n, and this gives

$$\lim_{n \to \infty} |x - [0, a_1, a_2, ..., a_n]| = 0$$

concluding that x has the infinite regular continued fractions expansion $[0, a_0, a_1, ...]$. For $x \notin \mathbb{F}(t)$ with $|x| \geq 1$, consider $x' = x - \lfloor x \rfloor$. Suppose that after applying the argument above, we have $x' = [0, b_1, b_2, ...]$. Then, with $b_0 = \lfloor x \rfloor$,

$$\lim_{n \to \infty} |x - [b_0, b_1, b_2, ..., b_n]| = \lim_{n \to \infty} |x' - [0, b_1, b_2, ..., b_n]| = 0$$

holds so that $x = [b_0, b_1, b_2, ...]$. The uniqueness follows from the definition of G since $\lfloor y \rfloor$ is the polynomial in $\mathbb{F}[t]$ with the largest possible degree so that $|y - \lfloor y \rfloor| < 1$ for each $y \in \mathbb{F}((t^{-1}))$.

For the other direction, this is the contrapositive of Proposition 3.5. □

Remark 3.13. *As a result of Proposition 3.12, we know that for every squarefree polynomial d in $\mathbb{F}[t]$, the roots of*

$$x^2 - d = 0$$

must have an infinite continued fraction expansion if they exist in $\mathbb{F}((t^{-1}))$.

One of the important classes of infinite continued fraction expansions are the pseudoperiodic continued fraction expansions:

Definition 3.14 (Pseudoperiodic infinite continued fraction by [15])**.** *Let $x \in \mathbb{F}((t^{-1}))$ have an infinite continued fraction expansion and let α_k be the k-th complete quotient. If there are natural numbers $n \geq 0$ and $m \geq 1$ and $c \in \mathbb{F}^*$ such that $\alpha_{n+m} = c\alpha_n$, then we say x has a pseudoperiodic continued fraction*

expansion; if $c = 1$, we say x has a periodic continued fraction expansion. The smallest m satisfying this is called the pseudoperiod of x if $c \neq 1$, and period of x if $c = 1$. In particular, if there are n and m such that for every natural number k, $\alpha_{n+m+k} = c\alpha_{n+k}$ holds, we have

$$\left[a_0, a_1, ..., a_{n-1}, cb_1, c^{-1}b_2, cb_3, ..., c^{(-1)^m}b_m, c^2b_1, c^{-2}b_2..., c^{(-2)^m}b_m, c^3b_1, ...\right]$$

where each a_i and b_j are in $\mathbb{F}[t]$ with positive degree for $i, j > 0$ and $\alpha \in \mathbb{F}$. We denote the above pseudoperiodic continued fraction as

$$\left[a_0, a_1, ..., a_{n-1}, \overline{b_1, b_2, ..., b_m}^c\right]$$

and, in particular, if it is periodic

$$\left[a_0, a_1, ..., a_{n-1}, \overline{b_1, b_2, ..., b_m}\right]$$

This is significant since it implies an important result used to prove Theorem 3.1.

Theorem 3.15 (Lagrange's theorem on continued fractions)**.** *Let $x \in \mathbb{F}((t^{-1})) \setminus \mathbb{F}(t)$ be quadratic over $\mathbb{F}(t)$. Then x has a periodic continued fraction expansion.*

Proof. For the convenience of readers, the proof is included in this section.

Let $x \in \mathbb{F}((t^{-1})) \setminus \mathbb{F}(t)$ be a root of

$$AX^2 + BX + C = 0$$

A, B, and C are in $\mathbb{F}(t)$ and $A \neq 0$. Without loss of generality, we may assume they are in $\mathbb{F}[t]$ by multiplying by common denominator on both sides. Let $x = [a_0, a_1, ...]$ be its infinite regular continued fraction expansion. Then for $n > 0$, the n-th complete quotient α_n of x satisfies

$$x = \frac{\alpha_n P_{n-1} + P_{n-2}}{\alpha_n Q_{n-1} + Q_{n-2}}.$$

This implies that we have $A_n\alpha_n^2 + B_n\alpha_n + C_n = 0$ where

$$\begin{aligned}
A_n &= AP_{n-1}^2 + BP_{n-1}Q_{n-1} + CQ_{n-1}^2 \\
B_n &= 2AP_{n-1}P_{n-2} + B(P_{n-1}Q_{n-2} + P_{n-2}Q_{n-1}) + 2CQ_{n-1}Q_{n-2} \\
C_n &= A_{n-1}
\end{aligned}$$

Notice that A_n must be non zero because if $A_n = 0$, then this allows for $At^2 + Bt + C = 0$ to have at least

two solutions, the n-th convergent $\dfrac{P_n}{Q_n}$ of x and x. But then, by the Vieta's formula yields

$$x + \frac{P_n}{Q_n} = -\frac{B}{A}$$

which clearly contradicts to our choice of $x \notin \mathbb{F}(t)$. Now, notice that

$$\begin{aligned}
x - \frac{P_{n-1}}{Q_{n-1}} &= \frac{(-1)^n}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})}, \\
A_n &= -\frac{(-1)^n(2Ax+B)Q_{n-1}}{\alpha_n Q_{n-1} + Q_{n-2}} + \frac{A}{(\alpha_n Q_{n-1} + Q_{n-2})^2}, \\
B_n^2 - 4A_nC_n &= B^2 - 4AC.
\end{aligned}$$

This implies that

$$A_n = -\frac{(-1)^n(2Ax+B)Q_{n-1}}{\alpha_n Q_{n-1} + Q_{n-2}} + \frac{A}{(\alpha_n Q_{n-1} + Q_{n-2})^2}$$

by $P_{n-1} = Q_{n-1}x - \dfrac{(-1)^n}{\alpha_n Q_{n-1} + Q_{n-2}}$. As a result,

$$\begin{aligned}
|A_n| &\le \left|\frac{(-1)^n(2Ax+B)Q_{n-1}}{\alpha_n Q_{n-1} + Q_{n-2}}\right| + \left|\frac{A}{(\alpha_n Q_{n-1} + Q_{n-2})^2}\right| \\
&= \frac{|2Ax+B||Q_{n-1}|}{|\alpha_n Q_{n-1} + Q_{n-2}|} + \frac{|A|}{|\alpha_n Q_{n-1} + Q_{n-2}|^2} \\
&\le \frac{(|A||x|+|B|)|Q_{n-1}|}{|\alpha_n Q_{n-1}|} + \frac{|A|}{(|\alpha_n Q_{n-1}|)^2} \\
&< |A|(|x|+1|) + |B| \\
|B_n|^2 &= |B^2 - 4AC + 4A_nC_n| \\
&\le |B^2 - 4AC| + |4A_nC_n| \\
&< |B^2 - 4AC| + (|A|(|x|+1|) + |B|)^2 \\
|C_n| &= |A_{n-1}| \\
&< |A|(|x|+1|) + |B|.
\end{aligned}$$

As a result, we may have at most finitely many choices for a triplet A_n, B_n, and C_n since they are in $\mathbb{F}[t]$.

Because the choice of n is countably infinite, we have distinct n_1, n_2, and n_3 such that

$$A_{n_1} = A_{n_2} = A_{n_3}$$
$$B_{n_1} = B_{n_2} = B_{n_3}$$
$$C_{n_1} = C_{n_2} = C_{n_3}$$

by the pigeonhole principle. This implies that if there is a root of

$$A_{n_i}X^2 + B_{n_i}X + C_{n_i} = 0$$

for any of $i = 1, 2$, or 3, it must also be a root of the other two equations as well. Since $A_n\alpha_n^2 + B_n\alpha_n + C_n = 0$ for each $n > 0$, this shows that at least two of $\alpha_{n_1}, \alpha_{n_2}$, and α_{n_3} are equal. This shows the periodicity. □

Example 3.16. *In the polynomial ring $\mathbb{F}[t]$ over the field $\mathbb{F} = \mathbb{F}_3$, we know that $d = t^2 + t + 2$ is a monic irreducible polynomial. To obtain the infinite continued fraction expansion for α where $\alpha^2 - d = 0$, notice first that*

$$\alpha = t\left(1 + \frac{1}{t} + \frac{2}{t^2}\right)^{\frac{1}{2}}$$

in the completion $\mathbb{F}((t^{-1}))$. Expanding $\left(1 + \frac{1}{t} + \frac{2}{t^2}\right)^{\frac{1}{2}}$ as a binomial series, we have

$$\alpha = t\left(1 + \frac{2}{t} + \frac{2}{t^2} + \frac{1}{t^3} + ...\right) = t + 2 + O\left(t^{-1}\right)$$

Now, notice that if we let $\beta = \dfrac{1}{\alpha - (t+2)}$, then this β is a root of

$$X^2 - (2t+1)X - 1 = 0$$

and $|\beta| > 1$ while the other root has absolute value strictly less than 1. At the same time, the infinite continued fraction $\left[\overline{2t+1}\right]$ is a solution to the same equation with $\left|\left[\overline{2t+1}\right]\right| > 1$. This implies that $\beta = \left[\overline{2t+1}\right]$. As a result, we have the periodic continued fraction expansion

$$\alpha = \left[t + 2, \overline{2t+1}\right]$$

3.3 The existence of nontrivial solutions by continued fractions

Finally, after all the necessary materials are presented in this section, the proof of Theorem 3.1 is given. We begin with an equivalence relation on $\mathbb{F}((t^{-1}))$.

Proposition 3.17 (Equivalence relation on $\mathbb{F}((t^{-1}))$)**.** *The binary relation $\sim$ on $\mathbb{F}((t^{-1}))$ defined by*

$$\alpha \sim \beta \iff \beta = \frac{R\alpha + S}{T\alpha + U}$$

for some $R, S, T, U \in \mathbb{F}[t]$ with $RU - ST \in \mathbb{F}^*$ is an equivalence relation.

Proof. See [23]. □

Remark 3.18. *For the rest of this chapter, when we use $\sim$, it means this equivalence relation.*

The equivalence $\sim$ has useful properties. In particular, these properties imply Proposition 3.23 which is important for the solvability of the Pell's equation.

Proposition 3.19 (Properties of the equivalence relation $\sim$)**.** *The equivalence relation $\sim$ satisfies the following properties.*

1. *If α_n is the n-th complete quotient of $\alpha \in \mathbb{F}((t^{-1}))$, then $\alpha \sim \alpha_n$.*
2. *If $\beta \in \mathbb{F}(t)$ and $\alpha \sim \beta$, then $\alpha \in \mathbb{F}(t)$.*
3. *Any two elements in $\mathbb{F}(t)$ are equivalent under $\sim$.*

Proof. 1. The statement follows from Proposition 3.6 for infinite regular continued fraction expansions if $\alpha \in \mathbb{F}(t)$ and the analogous statement to this proposition if $\alpha \notin \mathbb{F}(t)$.

2. By Definition 3.17, we have
$$\beta = \frac{R\alpha + S}{T\alpha + U}$$
with $RU - ST \in \mathbb{F}^*$. The statement follows since
$$\alpha = \frac{(-U)\beta + S}{T\beta + (-R)}.$$
Note that $T\beta + (-R)$ must be non zero; otherwise, if $T \neq 0$, then we have $\beta = \dfrac{R}{T} = \dfrac{S}{U}$ making $RU - ST = 0 \notin \mathbb{F}^*$; if $T = 0$, then $R = 0$ making $RU - ST \notin \mathbb{F}^*$.

3. Recall that an element in $\mathbb{F}(t)$ is given by a finite continued fraction expansion of polynomials and an element in $\mathbb{F}(t)$ is equivalent to a polynomial in $\mathbb{F}[t]$ by Proposition 3.6. Note that for every $f \in \mathbb{F}[t]$, we have
$$f = \frac{1 \cdot 1 + 1 - f}{0 \cdot f + 1}.$$
Since $\sim$ is an equivalence relation, we have the desired result.

4. Direct verification yields the statement we want.

□

The equivalence relation $\sim$ has two important properties that are used in the proof of Proposition 3.23.

Proposition 3.20 (Lemma 1 in [23]). *Suppose that for α and β in $\mathbb{F}((t^{-1}))\backslash\mathbb{F}(t)$ we have*
$$\alpha = \frac{A\beta + B}{C\beta + D}$$
where all of A, B, C, and D are in $\mathbb{F}[t]$ satisfying $|D| < |C|$, $a = AD - BC \in \mathbb{F}^*$, and $|\beta| > 1$. Let $\frac{P_n}{Q_n}$ and α_n be the convergents and the complete quotients of α for $n \geq 0$. Then there exist n such that
$$\frac{A}{C} = \frac{P_n}{Q_n},$$
$$\frac{B}{D} = \frac{P_{n-1}}{Q_{n-1}}$$
and $\beta = b\alpha_{n+1}$ where $b \in (-1)^{n+1}a(\mathbb{F}^*)^2$ and $a(\mathbb{F}^*)^2$ denotes the coset of $(\mathbb{F}^*)^2 = \{c^2 : c \in \mathbb{F}^*\}$ in $\mathbb{F}^*$ by a.

Proof. See [23, Lemma 1]. □

Proposition 3.21 (Lemma 2 in [23]). *Let $x \in \mathbb{F}((t^{-1}))\backslash\mathbb{F}(t)$. Then x is pseudoperiodic if and only if there is $M \in \mathcal{M}$ such that M is not a multiple of the identity matrix and*
$$x = Mx,$$
where $\mathcal{M}$ is the multiplicative group of 2×2 matrices of $\mathbb{F}[t]$ whose determinants are in $\mathbb{F}^*$ and the group action by $\mathcal{M}$ on $\mathbb{F}((t^{-1}))$ is given by
$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} x := \frac{Ax + B}{Cx + D}.$$

Proof. See [23, Lemma 2]. □

Example 3.22. *In the previous section, we saw that the infinite continued fraction expansion of α satisfying $\alpha^2 - (t^2 + t + 2) = 0$ is $\left[t + 2, \overline{2t + 1}\right]$ as in Example 3.16. Since it is periodic, there is a matrix M, which is not a multiple of the identity such that $\alpha = M\alpha$ from Proposition 3.23. In particular, such a matrix M is given by*

$$M = \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} P_{n-1} & P_{n-2} \\ Q_{n-1} & Q_{n-2} \end{pmatrix}^{-1}$$

where $n \geq 0$ since $\alpha_{n+1} = 1\alpha_n$. This matrix is obtained through the proof of Lemma 2 which is in [23]. For example, we have

$$\begin{aligned} M &= \begin{pmatrix} P_1 & P_0 \\ Q_1 & Q_0 \end{pmatrix} \begin{pmatrix} P_0 & P_{-1} \\ Q_0 & Q_{-1} \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 2t^2 + 2t & t + 2 \\ 2t + 1 & 1 \end{pmatrix} \begin{pmatrix} t + 2 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} t + 2 & t^2 + t + 2 \\ 1 & t + 2 \end{pmatrix} \end{aligned}$$

Proposition 3.23 (Theorem 2 in [23])**.** *Suppose that $\alpha \in \mathbb{F}((t^{-1}))$ quadratic over $\mathbb{F}(t)$ satisfies*

$$A\alpha^2 + B\alpha + C = 0$$

where A, B, C are relatively prime and A is nonzero. Then, for $d = B^2 - 4AC$,

$$X^2 - dY^2 \in \mathbb{F}^\times$$

has a nontrivial solution, a solution with $Y \neq 0$ in $\mathbb{F}[t]$.

Proof. By Theorem 3.15, we know that α has a periodic continued fraction expansion. This, together with the fact that $B^2 - 4AC$ is a square and the arguments in [23, Theorem 2] prove the result. □

Example 3.24. *In the preceding example 3.22, for α satisfying $\alpha^2 - (t^2 + t + 2) = 0$, there is a matrix*

$$\begin{pmatrix} R & S \\ T & U \end{pmatrix} = \begin{pmatrix} t+2 & t^2+t+2 \\ 1 & t+2 \end{pmatrix}$$

whose determinant is in $\mathbb{F}^* = \mathbb{F}_3^*$ such that

$$\alpha = \begin{pmatrix} R & S \\ T & U \end{pmatrix} \alpha.$$

After rearranging, we have

$$T\alpha^2 + (U - R)\alpha - S = 0.$$

This implies that

$$RU - ST = (t+2)^2 - (t^2 + t + 2) \cdot 1 = 2 \in \mathbb{F}^*$$

which is the norm of $(t + 2) + \alpha$ relative to the quadratic extension $\mathbb{F}(t)(\alpha)/\mathbb{F}(t)$. Since the norm is multiplicative, we have

$$N\left((t+2)+\alpha)^2\right) = N\left((2t^2+2t)+(2t+1)\alpha\right) = \left(2t^2+2t\right)^2 - (t^2+t+2)(2t+1)^2 = 1.$$

As a result, the Pell's equation

$$X^2 - (t^2 + t + 2)Y^2 = 1$$

has a nontrivial solution $(2t^2 + 2t, 2t + 1)$.

In order to show the existence of a solution for Pell's equation using continued fractions, the Hensel's lemma is useful. The major reason for this is that given a squarefree polynomial d, the Hensel's lemma assures the existence of an element $\alpha \in \mathbb{F}((t^{-1}))$ with $\alpha^2 - d = 0$. Since such α has a periodic infinite continued fraction expansion, this allows us to use 3.23.

Proposition 3.25 (Hensel's lemma)**.** *Let R, m, and k be a complete discrete valuation ring with respect to $|\cdot|$, a maximal ideal of R, and the field $k = R/m$, respectively. Let*

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \ldots a_0 \in R[t]$$

be a polynomial such that f is not congruent to 0 modulo m, $f'(t)$ is the formal derivative of f, and $\overline{g}(t) \in k[t]$ be the reduction of the polynomial $g(t) \in R[t]$ modulo m. If $\overline{f}(t)$ has a solution $\overline{a}$ such that $\overline{f'}(a) \neq 0$, then

there is a lift a in R such that $f(a) = 0$. In other words, there is a in R such that

$$a \equiv \overline{a} \,(mod\, m) \text{ and } f(a) = 0.$$

Proof. See [18] Chapter II. □

We have the immediate consequence of the existence of an element $\alpha \in \mathbb{F}((t^{-1}))$ such that $\alpha^2 - d = 0$. This eventually allows us to apply Proposition 3.23 in the proof of Theorem 3.1.

Corollary 3.26. *Let $d \in \mathbb{F}[t]$ be a squarefree even degree polynomial. Suppose that the leading coefficient of d is a square in $\mathbb{F}^*$. Then there is $\alpha \in \mathbb{F}((t^{-1}))$ such that*

$$\alpha^2 - d = 0.$$

Proof. Let

$$d = a_{2n}^2 t^{2n} + a_{2n-1} t^{2n-1} + ... + a_0$$

and let $R = \mathbb{F}[[t^{-1}]]$. Note that

$$d = a_{2n}^2 t^{2n} \left(1 + \frac{a_{2n-1}}{a_{2n}^2 t} + \frac{a_{2n-2}}{a_{2n}^2 t^2} + ... + \frac{a_0}{a_{2n}^2 t^{2n}}\right).$$

Now, consider the polynomial

$$p = x^2 - \left(1 + \frac{a_{2n-1}}{a_{2n}^2 t} + \frac{a_{2n-2}}{a_{2n}^2 t^2} + ... + \frac{a_0}{a_{2n}^2 t^{2n}}\right) \in R[x].$$

Then, by the maximality of the ideal $m = t^{-1}R$, we know that $p(1) = 0$ in $R/m[x]$ but $p'(1) \neq 0$ in $R/m[x]$. By Proposition 3.25, we know that there exists $\beta \in R \subseteq \mathbb{F}((t^{-1}))$ such that $p(\beta) = 0$ in $R[x]$. Thus, by letting $\alpha = a_{2n} t^n \beta \in \mathbb{F}((t^{-1}))$, we have $\alpha^2 - d = 0$. □

Finally, we have the existence of a nontrivial solution of Pell's equation.

Theorem 3.27. *The Pell equation*

$$X^2 - dY^2 = 1$$

has a nontrivial solution (x, y), a solution with $y \neq 0$ and $x, y \in \mathbb{F}[t]$.

Proof. By Corollary 3.26, we know that there is $\alpha \in \mathbb{F}((t^{-1})) \setminus \mathbb{F}(t)$ which is quadratic over $\mathbb{F}(t)$ such that

$$\alpha^2 - \frac{d}{4} = 0.$$

Since α has an infinite periodic continued fraction expansion from Theorem 3.15, we have

$$x^2 - dy^2 = a$$

for some $x, y \in \mathbb{F}[t]$ with $y \neq 0$ and $a \in \mathbb{F}^*$ from Proposition 3.23. If a is a square, then we have a nontrivial solution. Otherwise, notice that

$$(x^2 - dy^2)^2 = (x^2 + dy^2)^2 - d(2xy)^2 = a^2.$$

Since $x^2 - dy^2 = a$, $y \neq 0$, and d is a nonconstant polynomial, x must be nonzero. This implies that there is a nontrivial solution to the equation. As a result, in both cases of a is a square or not, we now know that there is always a nontrivial solution to the Pell equation. □

Remark 3.28. *For the classical Pell's equation over integers, the existence of a nontrivial solution can be proven analogously.*

Chapter 4

The Solvability of the Negative Pell's Equation

As in the previous chapter, let $\mathbb{F}$ and d be a finite field with characteristic different from 2 and a monic squarefree even degree polynomial in $\mathbb{F}[t]$ throughout this chapter, respectively. In the previous chapter, we observed that over a function field $\mathbb{F}(t)$ the Pell's equation

$$X^2 - dY^2 = c^2 \tag{4.1}$$

has a nontrivial solution (x, y), a solution with $y \neq 0$, given $c \in \mathbb{F}^*$. This poses a question which we will examine in the second half of this thesis. The question we investigate is *the existence of a solution of*

$$X^2 - dY^2 = a \tag{4.2}$$

where $a \in \mathbb{F}^* \setminus (\mathbb{F}^*)^2$ *and* $(\mathbb{F}^*)^2 := \{c^2 : c \in \mathbb{F}^*\}$. We refer to this Equation 4.2 as the "negative" Pell's equation.

Question. *Given a monic squarefree even degree polynomial* $d \in \mathbb{F}[t]$*, does a solution for the negative Pell's equation exist?*

It is known that the negative Pell's equation does not have a solution in general. For example, consider the following.

Example 4.1. *Let* $\mathbb{F} = \mathbb{F}_3$*. Then* $d = t^2 - 1$ *gives a nontrivial solution* $(X, Y) = (\pm t, \pm 1)$ *for the Pell's equation* (4.1) *but no solutions for the negative Pell's equation* (4.2)*. The reason will be provided later in*

Proposition 4.4.

In the classical case, consider this equation over integers. Peter Stevenhagen proposed the following conjecture on the negative Pell's equation in 1993 [24].

Conjecture 4.2 (Stevenhagen conjecture)**.** *The number of squarefree integers up to N for which the negative Pell equation is solvable is asymptotically equal to $\frac{cN}{\sqrt{\log(N)}}$ where*

$$c = \frac{3}{2\pi}\left(1 - \prod_{\substack{j\geq 1\\ j\ odd}}\left(1-2^{-j}\right)\right)\prod_{\substack{p\ prime\\ p\equiv 1 mod 4}}\left(1-p^{-2}\right)^{\frac{1}{2}} \approx 0.2697.$$

Furthermore,

$$\lim_{N\to\infty}\frac{\left|\mathcal{D}^{-}_{\leq N}\right|}{\left|\mathcal{D}_{\leq N}\right|} = 1 - \prod_{\substack{j\geq 1\\ j:odd}}\left(1-2^{-j}\right) \approx 0.58058$$

where $\mathcal{D}_{\leq N}$ and $\mathcal{D}^{-}_{\leq N}$ are the set of discriminants up to N of real quadratic fields that are not divisible by any prime congruent to 3 mod 4 and the subset of $\mathcal{D}_{\leq N}$ whose elements are discriminants for which the norm of the fundamental units is -1, respectively.

Over the integers, Stevenhagen reports that the denominator of the limit

$$\lim_{N\to\infty}\frac{\left|\mathcal{D}^{-}_{\leq N}\right|}{\left|\mathcal{D}_{\leq N}\right|}$$

has the asymptotic formula given by Rieger [20] as

$$|\mathcal{D}_{\leq N}| \sim \frac{cN}{\sqrt{\log(N)}}$$

where

$$c = \frac{9}{8\pi}\prod_{\substack{p \text{ prime}\\ p\equiv 1 \pmod 4}}(1-p^{-2})^{\frac{1}{2}},$$

while Nagell was the first mathematician to conjecture the limit converges within $(0,1)$ [17]. Moreover, Blomer determined that the numerator of the limit satisfies $\left|\mathcal{D}^{-}_{\leq (N)}\right| \gg \frac{N}{(\log(N))^{0.62}}$ as $N\to\infty$ in [3]; on the other hand, however, one of Dirichlet's results imply that $\left|\mathcal{D}_{\leq N}\setminus\mathcal{D}^{-}_{\leq N}\right| \gg \frac{N\log(\log(N))}{\log(N)}$ as $X\to\infty$ in [24]. In 2022, the Stevenhagen conjecture was proven by Koymans and Pagano [14].

The first goal of this chapter is to explore some conditions for the negative Pell's equation to be solvable or not with some examples. To present those conditions and examples, we consider the unit group of $\mathbb{F}[t][\sqrt{d}]$

and continued fraction of $\sqrt{d}$. As a result, this section allows us to construct the function field analogue of $\mathcal{D}_{\leq X}$. However, the conditions we explore here are not sufficient to fully answer the problem of solvability. To see this, we introduce two infinite classes of d, one admits a solution and the other does not.

The second goal of this chapter is to provide the asymptotic expression of the function field analogue of $|\mathcal{D}_{\leq X}|$. In the end of this chapter, we formulate a problem of the solvability of the negative Pell's equation. More precisely, we aim to propose the function field analogue of the question whether

$$\lim_{X\to\infty} \frac{\left|\mathcal{D}^{-}_{\leq X}\right|}{\left|\mathcal{D}_{\leq X}\right|}$$

exists as in the Stevenhagen's paper [24]. We refer this question as the Stevenhagen's limit problem.

4.1 Solutions of the negative Pell's equation

In the previous chapter, we have observed that for a monic polynomial d in $\mathbb{F}[t]$ with even degree, the Pell's equation (4.1) has a nontrivial solution. However, it is not true that the negative Pell's equation (4.2) has a solution for the same d.

Example 4.3. *Over the finite field $\mathbb{F} = \mathbb{F}_3$, let $d = t^2 + t = t(t+1)$, then there is a nontrivial solution $(2t+1, 1)$ to the Pell's equation. On the other hand, $X^2 - dY^2 = -1$ does not have a solution to the negative Pell's equation. Indeed, if there is a solution $x, y \in \mathbb{F}[t]$, then we have $x^2 = dy^2 - 1$. However, this is not possible since x^2 must have the square constant term while it is not. In general, it is known that if d has an odd degree irreducible factor, there is no solution to $X^2 - dY^2 = -1$. The proof of this result will be given in Proposition 4.4.*

To see whether a negative Pell's equation has a solution, we may rule out several classes of polynomials d. One class of polynomials making the equation not solvable is the class of odd degree polynomials by the same reason that there is no nontrivial solution to the Pell's equation. This implies that for the negative Pell's equation to be solvable, d must have an even positive degree. However, even if this even degree criteria is met, there is at least one class of polynomials that makes the negative Pell's equation not solvable.

4.1.1 Conditions for the existence of solutions to the negative Pell's equation

A class of monic even degree polynomials that does not allow a solution for the negative Pell's equation is the class of polynomials with an odd degree irreducible factor.

Proposition 4.4. *Let $d \in \mathbb{F}[t]$ have an odd degree irreducible factor. Then there is no solution (X, Y) in $\mathbb{F}[t]$ for*

$$X^2 - dY^2 = a$$

where $a \in \mathbb{F}^* \setminus (\mathbb{F}^*)^2$.

Proof. For the sake of contradiction, suppose there is a solution (x_0, y_0) to

$$X^2 - dY^2 = a$$

where $a \in \mathbb{F}$ is not square. Notice first that y_0 must be non zero and

$$2\deg(x_0) = \deg(d) + 2\deg(y_0) \geq 2$$

forcing $\deg(x_0) \geq 1$. Let d_0 be an odd degree irreducible factor of d. Then we have

$$x_0^2 \equiv a \pmod{d_0}.$$

This implies that, by the quadratic residue symbol, we have

$$\left(\frac{x_0^2}{d_0}\right)_2 = \left(\frac{a}{d_0}\right)_2 = 1.$$

But then, because

$$\left(\frac{x_0}{d_0}\right)_2 = x_0^{\frac{|d_0|-1}{2}}$$

by Proposition 2.50, we have

$$\left(\frac{x_0^2}{d_0}\right)_2 = \left(\frac{x_0}{d_0}\right)_2^2 = x_0^{|d_0|-1} = 1$$

So, we have $x_0^{|d_0|} = x_0$ implying x_0 is necessarily in $\mathbb{F}^*$ since $|d_0| > 1$. Hence, we have a contradiction. □

Proposition 4.4 reduces the solvability of the negative Pell's equation to the problem of a class of monic even degree polynomials with no odd degree irreducible factors. However, as we will see later in Example 4.10, this condition alone does not guarantee the solvability of the negative Pell's equation.

In general, whether the negative Pell's equation has a solution can be identified by looking at the unit group in $\mathbb{F}[t][\sqrt{d}]$. For the remainder of this chapter, let $\mathcal{U}$ and $\mathcal{U}^+$ be the set of all units in the integral closure $\mathbb{F}[t][\sqrt{d}]$ of $\mathbb{F}[t]$ in $\mathbb{F}(t)(\sqrt{d})$ and the subset of $\mathcal{U}$ with square norm, respectively.

Proposition 4.5. *Let* $\mathcal{U} = \langle a + b\sqrt{d} \rangle \times \mathbb{F}^*$.

1. *There is a generator* $a + b\sqrt{d}$ *of* $\mathcal{U}$ *such that both* a *and* b *are monic.*

2. *There is an element* $x + y\sqrt{d} \in \mathcal{U}$ *where the degree of* $x \in \mathbb{F}[t]$ *is the smallest among the elements in* $\mathcal{U}$*. In addition, for this element, the degree of* $y \in \mathbb{F}[t]$ *is the smallest among the elements in* $\mathcal{U}$*.*

Proof. 1. To begin with, recall that by Proposition 2.60, the unit group $\mathcal{U}$ is given by $\mathcal{U} = \langle a + b\sqrt{d} \rangle \times \mathbb{F}^*$ for some $a, b \in \mathbb{F}[t]$ with $b \neq 0$. Since $b \neq 0$ and d is monic, if a has leading coefficient c, then b must have the leading coefficient $\pm c$ since $a^2 - db^2 \in \mathbb{F}^*$. If b has leading coefficient $-c$, then

$$a + b\sqrt{d} = (a^2 - db^2)(a - b\sqrt{d})^{-1}$$

implies that

$$\mathcal{U} = \langle a - b\sqrt{d} \rangle \times \mathbb{F}^* = \langle a + b\sqrt{d} \rangle \times \mathbb{F}^*.$$

As a result, we may pick a generator $a + b\sqrt{d}$ of $\mathcal{U}$ to have both a and b to have the same leading coefficient. By factoring out the coefficients of a and b, we may pick a generator $a + b\sqrt{d}$ where both a and b are monic.

2. Since $x \in \mathbb{F}[t]$ is a polynomial and the degree of polynomials is a non negative integer or $-\infty$ for $x = 0$, we may order an element in $\mathcal{U}$ based on the degree of x as in $x + y\sqrt{d}$. Moreover, because $x^2 - dy^2 \in \mathbb{F}^*$ for $x + y\sqrt{d} \in \mathcal{U}$, we know that

$$2\deg(x) = \deg(d) + 2\deg(y)$$

must hold. Given the polynomial d, this implies that once we have x with the smallest degree, y must also have the smallest degree. Note that by a similar argument, we may order $x + y\sqrt{d}$ based on the degree of y and the smallest degree of y forces the polynomial x to have the smallest degree.

□

As an immediate consequence of this proposition above, we have the following definition.

Definition 4.6 (Minimal units)**.** *An element* $x + y\sqrt{d} \in \mathcal{U}$ *is a minimal element if* $\deg(x)$ *and* $\deg(y)$ *are the smallest among elements in* $\mathcal{U}$*. Similarly, we have the notion of a minimal element in* $\mathcal{U}^+$*.*

The following proposition shows conditions on $\mathcal{U}$ and $\mathcal{U}^+$ when the negative Pell's equation is solvable.

Proposition 4.7. *Let* $x + y\sqrt{d} \in \mathcal{U} = \langle a + b\sqrt{d} \rangle \times \mathbb{F}^*$ *with* $y \neq 0$ *a minimal element of* $\mathcal{U}$ *and* $a, b \in \mathbb{F}[t]$ *monic.*

1. $\mathcal{U} = \langle x + y\sqrt{d} \rangle \times \mathbb{F}^*$.

2. $[\mathcal{U} : \mathcal{U}^+] \leq 2$.

3. *The followings are equivalent*

   (a) $x + y\sqrt{d} \in \mathcal{U}^+$.

   (b) $\mathcal{U} = \mathcal{U}^+$.

   (c) *The negative Pell's equation* $x^2 - dy^2 \in \mathbb{F}^* \setminus (\mathbb{F}^*)^2$ *has no solution.*

Proof. 1. Consider a sequence $\{a_n\}$ and $\{b_n\}$ of $\mathbb{F}[t]$ defined by

$$a_n + b_n\sqrt{d} = (a + b\sqrt{d})^n$$

where a and b are monic and n is a positive integer. Notice that, by induction, a_n and b_n have the same leading coefficient for each n and $\{\deg(a_n)\}$ and $\{\deg(b_n)\}$ are strictly increasing sequences of integers. Indeed, sicne a and b are monic,

$$(a + b\sqrt{d})^2 = (a^2 + db^2) + 2ab\sqrt{d}$$

so that the leading coefficients of a_2 and b_2 are the same, and we have $\deg(a_2) > \deg(a_1)$ and $\deg(b_2) > \deg(b_1)$. For the inductive step, suppose that $\deg(a_{k+1}) > \deg(a_k)$ and $\deg(b_{k+1}) > \deg(b_k)$, and a_{k+1} and b_{k+1} have the same leading coefficient for some positive integer k. Then we have

$$\begin{aligned} a_{k+2} + b_{k+2}\sqrt{d} &= (a + b\sqrt{d})^{k+2} \\ &= (a_{k+1} + b_{k+1})(a + b\sqrt{d}) \\ &= (a_{k+1}a + b_{k+1}bd) + (a_{k+1}b + b_{k+1}a)\sqrt{d}. \end{aligned}$$

This shows that a_{k+2} and b_{k+2} have the same leading coefficient and $\deg(a_{k+2}) > \deg(a_{k+1})$ and $\deg(b_{k+2}) > \deg(b_{k+1})$. By a similar argument, we know that $a'_n + b'_n\sqrt{d} = (a + b\sqrt{d})^{-n} = (a^2 - db^2)^{-1}(a - b\sqrt{d})$ gives strictly increasing sequences $\{\deg(a'_n)\}$ and $\{\deg(b'_n)\}$.

Now, consider a minimal element $x + y\sqrt{d} \in \mathcal{U}$. Then there are $n \in \mathbb{Z}$ and $c \in \mathbb{F}^*$ such that

$$x + y\sqrt{d} = c(a + b\sqrt{d})^n.$$

This implies that $\langle x + y\sqrt{d} \rangle \times \mathbb{F}^* \subseteq \mathcal{U}$. Moreover, this forces $n = 1$ or -1 by the minimality of $x + y\sqrt{d}$.

As a result, we have

$$x + y\sqrt{d} = c(a + b\sqrt{d}) \text{ or } x + y\sqrt{d} = c(a + b\sqrt{d})^{-1}.$$

In either case, this implies that $\mathcal{U} \subseteq \langle x + y\sqrt{d} \rangle \times \mathbb{F}^*$ as desired.

2. Notice first that $\mathcal{U}^+ \subseteq \mathcal{U}$ by the definition. Notice that we have $\langle (a + b\sqrt{d})^2 \rangle \times \mathbb{F}^* \subseteq \mathcal{U}^+$ regardless of $[\mathcal{U} : \mathcal{U}^+]$ since the norm N is multiplicative. If $a + b\sqrt{d}$ has a square norm, we have $[\mathcal{U} : \mathcal{U}^+] = 1$. Now, suppose $a + b\sqrt{d}$ does not have a square norm. Note that for all $x + y\sqrt{d} \in \mathcal{U}^+$, there are $c \in \mathbb{F}^*$ and $k \in \mathbb{Z}$ such that

$$x + y\sqrt{d} = c(a + b\sqrt{d})^k.$$

Pick $x + y\sqrt{d}$ to be a minimal element in $\mathcal{U}^+$. This implies that

$$N\left(x + y\sqrt{d}\right) = N\left(c(a + b\sqrt{d})^k\right) = c^2 N\left(a + b\sqrt{d}\right)^k$$

is a square. This shows that k must be an even number and the minimality of $x + y\sqrt{d}$ forces $k = \pm 2$. This implies

$$\mathcal{U}^+ = \left\langle \left(a + b\sqrt{d}\right)^2 \right\rangle \times \mathbb{F}^*$$

forcing

$$[\mathcal{U} : \mathcal{U}^+] = 2.$$

3. 3a$\Longrightarrow$3b is given because the generator $x + y\sqrt{d}$ has a square norm and this forces all elements in $\mathcal{U}$ to have square norm.

   3b$\Longrightarrow$3c is given since every element in the unit group has a square norm.

   3c$\Longrightarrow$3a is given as a result of $N(x + y\sqrt{d}) \in (\mathbb{F}^*)^2$ obtained from the assumption.

□

Remark 4.8. *By a similar argument to the proof in Proposition 4.7, we know that if $x_0 + y_0\sqrt{d} \in \mathcal{U}^+$ is a minimal element of $\mathcal{U}^+$ with $y_0 \neq 0$,*

$$\mathcal{U}^+ = \langle x_0 + y_0\sqrt{d} \rangle \times \mathbb{F}^*.$$

Remark 4.9. *If $[\mathcal{U} : \mathcal{U}^+] = 2$ and $\mathcal{U} = \langle a + b\sqrt{d} \rangle \times \mathbb{F}^*$, then $\mathcal{U}^+ = \left\langle \left(a + b\sqrt{d}\right)^2 \right\rangle \times \mathbb{F}^*$*

The following example illustrates the conditions above.

Example 4.10. *Let $\mathbb{F} = \mathbb{F}_7$. Consider the unit group $\mathcal{U}$ of $\mathbb{F}[t][\sqrt{d}]$ where $d = t^2 + t + 4$. Notice that this*

polynomial is irreducible and squarefree. Notice that the Pell's equation

$$X^2 - (t^2 + t + 4)Y^2 = 1$$

has a nontrivial solution $(X, Y) = (t^2 + t + 3, t + 4)$*. Notice further that this nontrivial solution is minimal in* $\mathcal{U}^+ \setminus \mathbb{F}^*$*. This is because if there is another nontrivial solution* $(X, Y) = (\alpha t + \beta, \gamma)$ *for some* $\alpha, \beta, \gamma \in \mathbb{F}$ *with* $\gamma \neq 0$*,*

$$(\alpha t + \beta)^2 - (t^2 + t + 4)\gamma^2 = 1$$

must happen and finding such α, β*, and* γ *gives a contradiction; in particular,* $\alpha = 0$ *or* $\alpha = 2\beta$ *must happen and the former implies* $\gamma = 0$ *and the latter implies* $\beta^2 = -1 \notin (\mathbb{F}^*)^2$*. As a result,* $\mathcal{U}^+ = \langle (t^2 + t + 3) + (t + 4)\sqrt{d} \rangle \times \mathbb{F}^*$ *as in Remark 4.8*

On the other hand, recall that for

$$a_n + b_n\sqrt{d} = \left(a + b\sqrt{d}\right)^n$$
$$a'_n + b'_n\sqrt{d} = \left(a + b\sqrt{d}\right)^{-n}$$

where n *is a positive integer and* $a, b \in \mathbb{F}[t]$ *with* $b \neq 0$*,* $\{\deg(b_n)\}$ *and* $\{\deg(b'_n)\}$ *are strictly increasing sequences as in the argument in the proof of Proposition 4.7. This implies that* $(2t + 1) + 2\sqrt{d}$ *is a minimal element in* $\mathcal{U}$ *up to the multiplication by an element in* $\mathbb{F}^*$*. Moreover,* $(2t+1)+2\sqrt{d}$ *is not in* $\mathcal{U}^+$*. Therefore, there is no solution to the negative Pell's equation for this polynomial* d*.*

4.1.2 Continued fractions and the negative Pell's equation

In the previous section, we have covered some criteria that would provide polynomials d such that the negative Pell's equation does not have a nontrivial solution. In this section, we aim to provide some examples of d that admit a nontrivial solution to the negative Pell's equation. For such purpose, continued fraction expansions could be useful. One example that may be useful is the following proposition in the thesis of Malagoli [15, Lemma 2.1.16.].

Proposition 4.11 (Period length and Pell's equation)**.** *Let* $\alpha = \sqrt{d} \in \mathbb{F}((t^{-1}))$ *have a pseudoperiodic continued fraction expansion* $[a_0, a_1, a_2, ...]$ *with period* n *and pseudoperiod* m *such that* $a_m = 2ca_0$ *for some* $c \in \mathbb{F}^*$*. Then the solutions to the Pell's equation* $X^2 - dY^2$ *are given up to multiplicative constants as follows:*

1. *if* $n = m$ *and it is even, then* $c = 1$ *and* $P_{jm-1}^2 - dQ_{jm-1}^2 = 1$ *for every* $j \in \mathbb{N}$

2. if $n = m$ and it is odd, then $c = 1$ and $P_{jm-1}^2 - dQ_{jm-1}^2 = (-1)^j$ for every $j \in \mathbb{N}$

3. if $n = 2m$ and m is odd, then $P_{jm-1}^2 - dQ_{jm-1}^2 = \begin{cases} 1 & \text{if } j \text{ is even} \\ -c^{-1} & \text{if } j \text{ is odd} \end{cases}$

where $\dfrac{P_n}{Q_n} = [a_0, a_1, ..., a_n]$ *is n-th convergent of α.*

Proof. See [15, Lemma 2.1.16.]. □

Remark 4.12. *The preceding proposition implies that the convergents of $\sqrt{d}$ can give the solutions to Pell's equation. Moreover, in certain cases, this proposition above can be used to conclude the negative Pell's equation has a solution. In addition, we may be able to find a solution to the negative Pell's equation from the convergents of $\sqrt{d}$.*

Using the preceding proposition, we have the following example.

Example 4.13. *Let $\mathbb{F} = \mathbb{F}_3$ and $d = t^2 + t + 2 \in \mathbb{F}[t]$. Then we know that α such that $\alpha^2 - d = 0$ has a periodic continued fraction expansion*

$$\sqrt{d} = [t + 2, \overline{2t + 1}]$$

from Example 3.16. Because it has an odd period length, we expect to have a non-trivial solution to the negative Pell's equation from Proposition 4.11. Notice that we have

$$P_{-2} = 0, P_{-1} = 1, P_0 = t + 2, P_1 = 2t^2 + 2t, Q_{-2} = 1, Q_{-1} = 0, Q_0 = 1, Q_1 = 2t + 1.$$

Then we have

$$\begin{aligned} P_{0\cdot 1-1}^2 - dQ_{0\cdot 1-1}^2 &= 1^2 - (t^2 + t + 2) \cdot 0^2 = 1 \\ P_{1\cdot 1-1}^2 - dQ_{1\cdot 1-1}^2 &= (t + 2)^2 - (t^2 + t + 2) \cdot 1^2 = -1 \\ P_{2\cdot 1-1}^2 - dQ_{2\cdot 1-1}^2 &= (2t(t + 1))^2 - (t^2 + t + 2) \cdot (2t + 1)^2 = 1 \end{aligned}$$

From this, we know that

$$\mathcal{U} = \left\langle (t + 2) + \sqrt{d} \right\rangle \times \mathbb{F}^*$$

$$\mathcal{U}^+ = \left\langle 2t(t + 1) + (2t + 1)\sqrt{d} \right\rangle \times \mathbb{F}^* = \left\langle \left((t + 2) + \sqrt{d} \right)^2 \right\rangle \times \mathbb{F}^*$$

4.2 Asymptotics of certain squarefree polynomials

In this section, we aim to find the asymptotic expression for the number of monic squarefree polynomials without odd degree irreducible factors. Finding such expression corresponds to $|\mathcal{D}_{\leq X}|$ in the Stevenhagen conjecture 4.2.

To do so, we need Corollary 4.15 and Proposition 4.16 which are given below.

Proposition 4.14 (Darboux's theorem)**.** *Let t_0 and v be in $\mathbb{C}$ with $t_0 \neq 0$ and $v \notin \mathbb{Z}$. For $\left|arg\left(1 - tt_0^{-1}\right)\right| < \pi$, let*

$$p(t) = \left(1 - \frac{t}{t_0}\right)^{-\nu} r(t)$$

where $r(t)$ is an analytic function in $|t| < \rho$ for some $\rho > |t_0|$ and the power has its principal value. For $|t - t_0| < \rho - |t_0|$, let

$$r(t) = \sum_{k=0}^{\infty} b_k \left(t - t_0\right)^k .$$

Then the sequence of coefficients $\{p_n\}$ of $p(t)$ has the following asymptotic expression as $n \to \infty$:

$$p_n \sim t_0^{-n} \sum_{k=0}^{\infty} (-1)^k b_k t_0^k \frac{(\nu - k)_n}{n!}$$

where $(z)_m = z(z+1)\cdots(z+m-1)$.

Proof. See [10] Chapter 11. □

Hunter and Guerrieri obtained a simpler formula for the asymptotic of the sequence $\{p_n\}$:

Corollary 4.15. *Let $p(t)$, $r(t)$, $\{p_n\}$, and t_0 are given as in Proposition 4.14. Then we have*

$$p_n \sim \frac{b_0 n^{\nu-1}}{t_0^n \Gamma(\nu)}$$

Proof. See [11]. □

Proposition 4.16. *Let $c_{K,n}$ be the number of degree n monic irreducible polynomials in $K[t]$ where K is a finite field with $q_0 > 2$ elements. Then*

$$c_{K,n} = \frac{1}{n} \sum_{d|n} \mu(d) q_0^{\frac{n}{d}} = \frac{q_0^n}{n} + O\left(\frac{q_0^{\frac{n}{2}}}{n}\right)$$

where μ is the Möbius function. Moreover, the series

$$\mathcal{Z}_K(t) = \sum_g t^{\deg(g)},$$

where the sum is taken over monic even degree polynomials, converges absolutely for $|t| < \frac{1}{q_0}$ and is equal to an infinite product

$$\prod_p \left(1 + t^{\deg(p)} + t^{\deg(p^2)} + \ldots\right) = \prod_{k=1}^{\infty} \left(1 + t^k + t^{2k} + \ldots\right)^{c_K,k}.$$

Proof. See [21] Chapter 2 for the proof. For convenience for the readers, the proof for the second claim is included. Let $g = p_{1,g}^{e_{1,g}} p_2^{e_{2,g}} ... p_{r,g}^{e_{r,g}}$ be the factorization of a monic polynomial g in irreducibles into $K[t]$. Then

$$\begin{aligned}
\mathcal{Z}_K(t) &= \sum_g t^{\deg g} \\
&= \sum_g t^{\deg\left(p_{1,g}^{e_{1,g}} p_2^{e_{2,g}} \ldots p_{r,g}^{e_{r,g}}\right)} \\
&= \sum_g t^{\deg\left(p_{1,g}^{e_{1,g}}\right)} t^{\deg\left(p_{2,g}^{e_{2,g}}\right)} \ldots t^{\deg\left(p_{r,g}^{e_{r,g}}\right)} \\
&= \prod_p \left(1 + t^{\deg(p)} + t^{\deg(p^2)} + \ldots\right) \\
&= \prod_{k=1}^{\infty} (1 + t^k + t^{2k} + ...)^{c_{K,k}}.
\end{aligned}$$

where g in the sum is taken over monic polynomials in $K[t]$ and p in the product is taken over monic irreducible polynomials in $K[t]$. To see the absolute convergence, we want

$$\sum_{k=1}^{\infty} c_{K,k}(t^k + t^{2k} + \ldots)$$

to be absolutely convergent because of Proposition 2.65. Notice that if $|t| < \frac{1}{q_0}$, then

$$\begin{aligned}
\sum_{k=1}^{\infty} \left|c_{K,k}(t^k + t^{2k} + \ldots)\right| &\leq \sum_{k=1}^{\infty} |c_{K,k}|(|t|^k + |t|^{2k} + \ldots) \\
&= \sum_{k=1}^{\infty} |c_{K,k}| \frac{|t|^k}{1 - |t|^k} \\
&\leq 2 \sum_{k=1}^{\infty} |c_{K,k}||t|^k
\end{aligned}$$

since $\frac{1}{1-|t|^k}$ is strictly decreasing for positive real number k and $\frac{1}{1-|t|^k} \leq 2$. By the definition, we know that there are positive M and $N \in \mathbb{Z}$ such that for $k \geq N$

$$|c_{K,k}| \leq \frac{q_0^k}{k} + \frac{Mq_0^{\frac{k}{2}}}{k} \leq \frac{(M+1)q_0^k}{k}.$$

As a result,

$$\begin{aligned}\sum_{k=1}^{\infty} |c_{K,k}||t|^k &\leq \sum_{k=1}^{N} |c_{K,k}||t|^k + \sum_{k=N+1}^{\infty} \left|\frac{(M+1)q_0^k}{k}\right| |t|^k \\ &\leq \sum_{k=1}^{N} |c_{K,k}||t|^k + \sum_{k=N+1}^{\infty} (M+1)q_0^k|t|^k\end{aligned}$$

Since $\sum_{k=N+1}^{\infty} (M+1)q_0^k|t|^k \leq \sum_{k=0}^{\infty}(M+1)q_0^k|t|^k = \frac{M+1}{1-q_0|t|}$ by $|t| < \frac{1}{q_0}$, the series $\sum_{k=1}^{\infty} c_{K,k}(t^k + t^{2k} + \ldots)$ is absolutely convergent. From this, $\mathcal{Z}_K(t)$ converges absolutely. □

The next lemma provides the convergence of the infinite product appearing in the asymptotics which we will see in Theorem 4.19.

Lemma 4.17. *The series*

$$\sum_{k=0}^{\infty} -\frac{c_{\mathbb{F},2k+1}}{2}(t^{2k+1} + t^{2(2k+1)} + \ldots)$$

converges absolutely for $|t| < \frac{1}{q}$*, and therefore, the infinite product*

$$\prod_{k=0}^{\infty}(1 + t^{2k+1} + t^{2(2k+1)} + \ldots)^{-\frac{c_{\mathbb{F},2k+1}}{2}}$$

converges absolutely where $\mathbb{F}$ *is a finite field of* q *elements.*

Proof. The proof is analogous to Proposition 4.16. □

Finally, we have the following results.

Theorem 4.18. *Let* s_n *denote the number of monic polynomials of degree* n *without odd degree irreducible factors over the finite field* $\mathbb{F}$ *with* q *elements. Then*

$$s_{2n} \sim \frac{cq^{4n}}{\sqrt{2n}}$$

where

$$c = \left(\Gamma\left(\frac{1}{2}\right)\right)^{-1} \prod_{k=0}^{\infty}\left(\frac{1}{1-q^{-2(2k+1)}}\right)^{-\frac{c_{\mathbb{F},2k+1}}{2}}.$$

Proof. For the finite field $\mathbb{F}$, define a function f from the set of monic polynomials in $\mathbb{F}[t]$ to $\mathbb{C}$ by

$$f(g) = \begin{cases} 1 & \text{if } g \text{ has no odd degree irreducible factors} \\ 0 & \text{otherwise} \end{cases}.$$

Now, let a series $\mathcal{F}(t)$ be given by

$$\mathcal{F}(t) = \sum_g f(g) t^{\frac{\deg(g)}{2}}$$

where the sum is taken over even degree monic polynomials in $\mathbb{F}[t]$. Then notice that

$$\mathcal{F}(t) = \sum_g f(g) t^{\frac{\deg(g)}{2}} = \sum_{k=0}^{\infty} s_{2k} t^k$$

by the definition of $\mathcal{F}(t)$. Moreover, by a similar argument as in the proof of Proposition 4.16, we have

$$\begin{aligned} \mathcal{F}(t) &= \sum_g f(g) t^{\frac{\deg(g)}{2}} \\ &= \prod_p (1 + t^{\frac{\deg(p)}{2}} + t^{\frac{\deg(p^2)}{2}} + \ldots) \\ &= \prod_{k=1}^{\infty} (1 + t^k + t^{2k} + \ldots)^{c_{\mathbb{F},2k}} \end{aligned}$$

which is nonzero and converges absolutely for $|t| < \frac{1}{q^2}$ by applying the analogous method as in Proposition 4.16 where the p appearing in the infinite product above is taken over the set of monic even degree irreducible polynomials in $\mathbb{F}[t]$. Let K be the finite field with q^2 elements and consider

$$Z_K(t) = \sum_g t^{\deg g} = \prod_{k=1}^{\infty} (1 + t^k + t^{2k} + ...)^{c_{K,k}}$$

as in Proposition 4.16. Note that if $|t| < \frac{1}{q^2}$, then we have

$$\mathcal{Z}_K(t) = \sum_{k=0}^{\infty} q^{2k} t^k = \frac{1}{1 - q^2 t}.$$

In order to get the asymptotic expression of s_{2k}, we aim to compare and express $\mathcal{F}(t)$ using $\mathcal{Z}_K(t)$. To do

this, define

$$c'_{\mathbb{F},n} = c_{\mathbb{F},n} - \frac{q^n}{n}$$
$$c'_{K,n} = c_{K,n} - \frac{q^{2n}}{n}$$

Using them, we may express $\mathcal{F}(t)$ and $\mathcal{Z}_K(t)$ as

$$\mathcal{F}(t) = \prod_{k=1}^{\infty}(1+t^k+t^{2k}+\ldots)^{\frac{q^{2k}}{2k}} \prod_{k=1}^{\infty}(1+t^k+t^{2k}+\ldots)^{c'_{\mathbb{F},2k}}$$
$$\mathcal{Z}_K(t) = \prod_{k=1}^{\infty}(1+t^k+t^{2k}+\ldots)^{\frac{q^{2k}}{k}} \prod_{k=1}^{\infty}(1+t^k+t^{2k}+\ldots)^{c'_{K,k}}.$$

because of the absolute convergence. As a result, for $|t| < \dfrac{1}{q^2}$, we have

$$\begin{aligned}\mathcal{F}(t) &= \sqrt{\mathcal{Z}_K(t)\cdot\frac{1}{\prod_{k=1}^{\infty}(1+t^k+t^{2k}+\ldots)^{c'_{K,k}}}} \prod_{k=1}^{\infty}(1+t^k+t^{2k}+\ldots)^{c'_{\mathbb{F},2k}} \\ &= \sqrt{\mathcal{Z}_K(t)} \prod_{k=1}^{\infty}(1+t^k+t^{2k}+\ldots)^{c'_{\mathbb{F},2k}-\frac{c'_{K,k}}{2}} \\ &= (1-q^2t)^{-\frac{1}{2}} \prod_{k=1}^{\infty}(1+t^k+t^{2k}+\ldots)^{c'_{\mathbb{F},2k}-\frac{c'_{K,k}}{2}}\end{aligned}$$

Because of the definition of $c'_{\mathbb{F},2k}$ and $c'_{K,k}$, together with Proposition 4.16,

$$\begin{aligned}c'_{\mathbb{F},2k} - \frac{c'_{K,k}}{2} &= c_{\mathbb{F},2k} - \frac{c_{K,k}}{2} \\ &= \frac{1}{2k}\sum_{d|2k}\mu(d)q^{\frac{2k}{d}} - \frac{1}{2k}\sum_{d|k}\mu(d)q^{\frac{2k}{d}} \\ &= \frac{1}{2k}\sum_{\substack{d|2k \\ d\nmid k}}\mu(d)q^{\frac{2k}{d}}\end{aligned}$$

Now, note that if d is a divisor of $2k$ and k is given by $k = 2^{e_0}p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r}$ where each p_i is an odd prime number and each e_i is a nonnegative integer, d has the form

$$d = 2^{l_0}p_1^{l_1}p_2^{l_2}\ldots p_r^{l_r}$$

where each l_i is a nonnegative integer and $l_i \le e_i$. If this d does not divide k, this forces $l_0 = e_0 + 1$ and

$l_i \leq e_i$ for each positive i. This implies that

$$c'_{\mathbb{F},2k} - \frac{c'_{K,k}}{2} = \frac{1}{2k} \sum_{\substack{d|k \\ d \text{ odd}}} \mu(2^{e_0+1}d) q^{\frac{2k}{2^{e_0+1}d}}.$$

If k is an even number, then $\mu(2^{e_0+1}d) = 0$ for d in the sum above since $2^{e_0+1}d$ is not squarefree and by Definition 2.67 of the Möbius function. As a result, we have

$$c'_{\mathbb{F},2k} - \frac{c'_{K,k}}{2} = \begin{cases} 0 \text{ if } k \text{ is even} \\ -\frac{1}{2k} \sum_{d|k} \mu(d) q^{\frac{k}{d}} = -\frac{c_{\mathbb{F},k}}{2} \text{ if } k \text{ is odd} \end{cases}$$

$$\mathcal{F}(t) = (1-q^2t)^{-\frac{1}{2}} \prod_{k=0}^{\infty} (1 + t^{2k+1} + t^{2(2k+1)} + \ldots)^{-\frac{c_{\mathbb{F},2k+1}}{2}}$$

The infinite product appearing in the above expression is analytic for $|t| < \frac{1}{q}$ because of a similar argument in Proposition 4.16 and by Lemma 4.17. As a result, we may express this infinite product as

$$s(t) = \sum_{k=0}^{\infty} b_k \left(t - \left(\frac{1}{q^2} \right) \right)^k$$

using some sequence $\{b_k\}$. This sequence $\{b_k\}$ is given by taking the Taylor series representation of the infinite product. In particular, b_0 is

$$b_0 = \prod_{k=0}^{\infty} (1 + q^{-2(2k+1)} + q^{-4(2k+1)} + \ldots)^{-\frac{c_{\mathbb{F},2k+1}}{2}} = \prod_{k=0}^{\infty} \left(\frac{1}{1 - q^{-2(2k+1)}} \right)^{-\frac{c_{\mathbb{F},2k+1}}{2}}.$$

By Corollary 4.15, we have

$$s_{2k} \sim \frac{c(2k)^{-\frac{1}{2}}}{(\frac{1}{q^2})^{2k}} = \frac{cq^{4k}}{\sqrt{2k}}$$

where

$$c = \left(\Gamma\left(\frac{1}{2} \right) \right)^{-1} \prod_{k=0}^{\infty} \left(\frac{1}{1 - q^{-2(2k+1)}} \right)^{-\frac{c_{\mathbb{F},2k+1}}{2}}.$$

□

Using this theorem, we have the asymptotic expression of the number of monic even degree squarefree polynomials with no odd degree irreducible factors.

Theorem 4.19. *Let s_n^* denote the number of monic squarefree polynomials of degree n with no odd degree*

irreducible factor over the finite field $\mathbb{F}$ of q elements. Then

$$s^*_{2n} \sim \frac{c^* q^{4n}}{\sqrt{2n}}$$

where c^* is

$$c^* = \left(\Gamma\left(\frac{1}{2}\right)\right)^{-1} \prod_{k=0}^{\infty} \left(\frac{1}{1-q^{-2(2k+1)}}\right)^{-\frac{c_{\mathbb{F},2k+1}}{2}} \prod_{k=1}^{\infty} \left(\frac{1}{1-q^{-4k}}\right)^{-c_{\mathbb{F},2k}}.$$

Proof. Let $\mathcal{F}^*(t)$ denote the infinite product given by

$$\mathcal{F}^*(t) = \prod_{k=1}^{\infty} (1+t^k)^{c_{\mathbb{F},2k}}$$

which converges absolutely for $|t| < \frac{1}{q^2}$ by a similar argument to Proposition 2.65. Notice that, by a similar argument to Proposition 4.16 and Theorem 4.18, $\mathcal{F}^*(t)$ can be expressed as

$$\mathcal{F}^*(t) = \sum_g f^*(g) t^{\frac{\deg(g)}{2}} = \sum_{k=0}^{\infty} s^*_{2k} t^k$$

where g in the sum above is taken over the set of monic even degree polynomials in $\mathbb{F}[t]$ and f^* is a function from the set of monic polynomials in $\mathbb{F}[t]$ to $\mathbb{C}$ by

$$f^*(g) = \begin{cases} 1 & \text{if } g \text{ is squarefree and has no odd degree irreducible factors} \\ 0 & \text{otherwise.} \end{cases}$$

Notice that every monic polynomial $g \in \mathbb{F}[t]$ can be uniquely written as a product $g = g_1^2 g_2$ where $g_1 \in \mathbb{F}[t]$ and a squarefree polynomial $g_2 \in \mathbb{F}[t]$. Moreover, g has no odd degree irreducible factors if and only if both g_1 and g_2 have no odd degree irreducible factors. Using the notations we see in the proof of Theorem 4.18, we have

$$\mathcal{F}(t) = \left(\sum_{g_1} t^{\frac{\deg(g_1^2)}{2}}\right)\left(\sum_{g_2} t^{\frac{\deg(g_2)}{2}}\right) = \mathcal{F}(t^2)\mathcal{F}^*(t),$$

where the polynomial $g_1 \in \mathbb{F}[t]$ in the sum is a monic even degree polynomial with no odd degree irreducible factors and the polynomial $g_2 \in \mathbb{F}[t]$ in the sum is a monic squarefree even degree polynomial with no odd degree irreducible factors. Since $\mathcal{F}(t)$ and, therefore, $\mathcal{F}(t^2)$ are nonzero, we know that

$$\mathcal{F}^*(t) = \mathcal{F}(t)\left(\mathcal{F}(t^2)\right)^{-1} = (1-q^2t)^{-\frac{1}{2}} \prod_{k=0}^{\infty} (1+t^{2k+1}+t^{2(2k+1)}+\ldots)^{-\frac{c_{\mathbb{F},2k+1}}{2}} \left(\mathcal{F}(t^2)\right)^{-1}.$$

Since

$$\mathcal{F}(t^2) = \prod_{k=1}^{\infty}(1 + t^{2k} + t^{4k} + \ldots)^{c_{\mathbb{F},2k}},$$

is nonzero and absolutely convergent for $|t| < \frac{1}{q}$ as in the argument in Proposition 4.16, we know that

$$\prod_{k=0}^{\infty}(1 + t^{2k+1} + t^{2(2k+1)} + \ldots)^{-\frac{c_{\mathbb{F},2k+1}}{2}} \left(\mathcal{F}(t^2)\right)^{-1}$$

is nonzero, analytic, and absolutely convergent for $|t| < \frac{1}{q}$. Applying Corollary 4.15, we have

$$s_{2k}^* \sim \frac{c^* q^{4n}}{\sqrt{2n}}$$

where c^* is

$$c^* = \left(\Gamma\left(\frac{1}{2}\right)\right)^{-1} \prod_{k=0}^{\infty}\left(\frac{1}{1-q^{-2(2k+1)}}\right)^{-\frac{c_{\mathbb{F},2k+1}}{2}} \prod_{k=1}^{\infty}\left(\frac{1}{1-q^{-4k}}\right)^{-c_{\mathbb{F},2k}}.$$

□

4.3 Function Field Analogue of the Stevenhagen Problem

In the previous sections of this chapter, we have explored some examples and conditions when the negative Pell's equation is solvable. Moreover, we found the asymptotic expression of the function field analogue of $|\mathcal{D}_{\leq X}|$ in the Stevenhagen conjecture. As in one of the statement in the Stevenhagen conjecture 4.2, the next question to ask is how likely even degree polynomials without odd degree irreducible factors would give a solution to the negative Pell's equation. More precisely, the next question is to formulate and find a solution to the function field analogue of the Stevenhagen's limit problem:

Problem 4.20 (Stevenhagen limit problem)**.** *Let $\mathcal{D}_{\leq X}$ and $\mathcal{D}^-_{\leq X}$ be the set of discriminants of real quadratic field that are not divisible by any prime up to X congruent to 3 mod 4 and the subset of $\mathcal{D}_{\leq X}$ whose elements are discriminants for which the norm of the fundamental units is -1, respectively. Does the limit*

$$\lim_{X\to\infty} \frac{\left|\mathcal{D}^-_{\leq X}\right|}{\left|\mathcal{D}_{\leq X}\right|}$$

exists? If it exists, determine its value.

Over integers, notice that if $d \in \mathbb{N}$ has a prime factor congruent to 3 modulo 4, then we have $x^2 - dy^2$ mod 4 is one of 0, 1, and 2, for $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$. As a result, the negative Pell's equation over integers has no solution. In addition, when d is a negative integer so that $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is an imaginary quadratic extension,

then we know that the units of algebraic integers in $\mathbb{Q}(\sqrt{d})$ are 1 and -1. In this case, there is no solution to negative Pell's equation.

As a result, in the Stevenhagen's limit problem, the only quadratic extensions $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ we are considering are the ones with $d > 0$ and discriminants not divisible by primes congruent to 3 mod 4. However, this condition alone does not guarantee the solvability of the negative Pell's equation.

This arguments provide the analogues of d in $\mathbb{F}[t]$ and the analogue of d in $\mathbb{Z}$. If we denote a monic polyomial in $\mathbb{F}[t]$ and a square free integer by $d(t)$ and d, respectively, then an odd degree polynomial d corresponds to a negative d; an even degree $d(t)$ with an odd degree irreducible factor corresponds to a positive d with a prime factor congruent to 3 under modulo 4; an even degree $d(t)$ without an odd degree irreducible factor corresponds to a positive d without a prime factor congruent to 3 under modulo 4. Since we are interested in units in quadratic extension of $\mathbb{F}(t)$ with the norm in $\mathbb{F}^* \setminus (\mathbb{F}^*)^2$, which corresponds to units in the extension of $\mathbb{Q}$ with squarefree norm -1, we may formulate the function field analogue of the limit problem:

Problem 4.21 (Function field analogue of Stevenhagen's limit problem)**.** *Let $d \in \mathbb{F}[t]$ be a monic positive even degree polynomial with no odd degree irreducible factor. Let $\mathcal{D}_{\mathbb{F},\leq N}$ be the set of polynomials d up to degree N and let $\mathcal{D}^-_{\mathbb{F},\leq N}$ be the subset $\mathcal{D}_{\mathbb{F},\leq N}$ where the negative Pell's equation has a nontrivial solution. Does the following limit exists?*

$$\lim_{N\to\infty} \frac{|\mathcal{D}^-_{\mathbb{F},\leq N}|}{|\mathcal{D}_{\mathbb{F},\leq N}|}$$

Notice that from our result for the asymptotics in Theorem 4.19, we know that the asymptotic expression of $|\mathcal{D}_{\mathbb{F},\leq N}|$ is given by

$$|\mathcal{D}_{\mathbb{F},\leq N}| \sim \frac{cq^{4N}}{\sqrt{2N}}$$

where

$$c = \left(\Gamma\left(\frac{1}{2}\right)\right)^{-1} \prod_{k=0}^{\infty} \left(\frac{1}{1-q^{-2(2k+1)}}\right)^{-\frac{c_{\mathbb{F},2k+1}}{2}} \prod_{k=1}^{\infty} \left(\frac{1}{1-q^{-4k}}\right)^{-c_{\mathbb{F},2k}}.$$

In the final section of this thesis, we explore this problem through two infinite classes of even degree polynomials, one of which guarantees the solvability and the other does not. The first class we consider is the function field analogue of twin primes with constant gap and the second class is the polynomials in the form of $f^2 - c$ where $c \in \mathbb{F}^*$ is not a square.

Over the integers, there is a notion of twin primes, a pair of prime numbers with difference 2. Analogous to this, we may consider a pair of irreducible polynomials (p_1, p_2) of $\mathbb{F}[t]$ such that $p_1 - p_2 = \pm c$ for some $c \in \mathbb{F}^*$. We call such pair as a twin prime pair in $\mathbb{F}[t]$. For such pairs, we have the following result.

Proposition 4.22. *Let $d = f^2 - c$ where $f \in \mathbb{F}[t]$ and $c \in (\mathbb{F}^*)^2$. Then there is no solution to the negative Pell's equation.*

Proof. Since $f + \sqrt{d}$ is minimal in both $\mathcal{U}$ and $\mathcal{U}^+$, we know that

$$\mathcal{U} = \mathcal{U}^+ = \langle f + \sqrt{d} \rangle \times \mathbb{F}^*$$

by Proposition 4.7, forcing that there is no solution to the negative Pell's equation.

□

Proposition 4.22 provides some polynomials d that make the negative Pell's equation not solvable and, in particular, if d is given by a product of function field analogue of twin prime pairs, then the negative Pell's equation is not solvable. In the paper by Sawin and Shusterman [22], the asymptotics of such d is given by the following result.

Proposition 4.23 (Asymptotics of Twin Prime Polynomials)**.** *Let p be an odd prime and let q be a positive integer such that $q > 68509p^2$. Let $|\cdot|$ denote the infinite absolute value on the finite field $\mathbb{F}$ where $q = |\mathbb{F}|$ is a prime power. Let $h \in \mathbb{F}[t]$ be nonzero. Define the set $\mathcal{T}(n)$ by*

$$\mathcal{T}(n) = \{f \in \mathbb{F}[t] : |f| = n \text{ and both } f \text{ and } f + h \text{ are primes}\}$$

Then for all non zero polynomial h over $\mathbb{F}$, the asymptotic expression $\mathfrak{T}(n)$ of $|\mathcal{T}(n)|$ satisfies

$$\mathfrak{T}(n) \sim \frac{n}{(\log(n))^2} \left(\prod_P \left(1 - |P|^{-1}\right)^{-2} \left(1 - |P|^{-1} - |P|^{-1} \mathbf{1}_{P \nmid h}\right) \right)$$

as $n \to \infty$ through powers of q where the infinite product is taken over monic irreducibles P in $\mathbb{F}[t]$ and $\mathbf{1}_{P \nmid h}$ returns 1 if $P \nmid h$ and 0 otherwise. In particular, if $h \in \mathbb{F}^*$, we have

$$\mathfrak{T}(n) \sim \frac{n}{(\log(n))^2} \left(\prod_P \left(1 - |P|^{-1}\right)^{-1} \right)$$

Proof. See [22]. □

As a result, we have an infinite class of polynomials d where the negative Pell's equation is not solvable.

As we have an infinite class of polynomials d that does not allow the existence of nontrivial solutions to negative Pell's equation $X^2 - dY^2 = c \in \mathbb{F}^* \setminus (\mathbb{F}^*)^2$, there is an infinite class of polynomials d that makes the equation solvable.

Proposition 4.24. *Let $d \in \mathbb{F}[t]$ be given by $d = f^2 - c$ where $f \in \mathbb{F}[t]$ is a monic polynomial and $c \in \mathbb{F}^* \setminus (\mathbb{F}^*)^2$. Then there is a solution to*

$$X^2 - dY^2 = c.$$

Proof. A solution is given by $f^2 - d \cdot (\pm 1)^2 = c$. □

Note that number $\mathfrak{F}(n)$ of degree $2n$ polynomials $d \in \mathbb{F}[t]$ of the form of $d = f^2 - c$ for some degree n polynomial $f \in \mathbb{F}[t]$ and squarefree $c \in \mathbb{F}^*$ is given by

$$\mathfrak{F}(n) = \frac{q^n(q-1)}{2}$$

where $q = |\mathbb{F}|$.

Despite the fact there are infinite sets that makes the negative Pell's equation solvable and not solvable, they still fail to show whether lim sup and lim inf of the fraction $\dfrac{|\mathcal{D}^-_{\mathbb{F},\leq N}|}{|\mathcal{D}_{\mathbb{F},\leq N}|}$ in Problem 4.21 is within the open interval $(0,1)$. This is because when we compare the asymptotics of the denominator

$$|\mathcal{D}_{\mathbb{F},\leq N}| \sim \frac{cq^{4N}}{\sqrt{2N}}$$

where

$$c = \left(\Gamma\left(\frac{1}{2}\right)\right)^{-1} \prod_{k=0}^{\infty} \left(\frac{1}{1-q^{-2(2k+1)}}\right)^{-\frac{c_{\mathbb{F},2k+1}}{2}} \prod_{k=1}^{\infty} \left(\frac{1}{1-q^{-4k}}\right)^{-c_{\mathbb{F},2k}}$$

to those of the examples, we have the following.

Proposition 4.25.

$$\lim_{N\to\infty} \frac{\mathfrak{T}(N)}{|\mathcal{D}_{\mathbb{F},\leq q^N}|} = 0$$
$$\lim_{n\to\infty} \frac{\mathfrak{F}(N)}{|\mathcal{D}_{\mathbb{F},\leq N}|} = 0.$$

Recall that over the integers, Rieger showed that the asymptotic expression of $\left|\mathcal{D}_{\mathbb{F},\leq X}\right|$ is $\dfrac{cX}{\sqrt{\log(X)}}$ where

$$c = \frac{9}{8\pi} \prod_{\substack{p:\text{prime} \\ p\equiv 1 \pmod 4}} (1-p^{-2})^{\frac{1}{2}}$$

[20] while Nagell conjectured the limit converges within $(0,1)$. Moreover, Bloomer showed the asymptotic bound of $\left|\mathcal{D}^-_{\leq X}\right|$ to be $\left|\mathcal{D}^-_{\leq X}\right| \gg \frac{X}{(\log(X))^{0.62}}$ as $X \to \infty$; on the other hand, however, one of Dirichlet's results implies that the density $\left|\mathcal{D}_{\leq X} \setminus \mathcal{D}^-_{\leq X}\right| \gg \frac{X\log(\log(X))}{\log(X)}$ as $X \to \infty$ [24]. Moreover, Koymans and Pagano

proved in [14] that the limit of $\frac{|\mathcal{D}^-_{\leq X}|}{|\mathcal{D}_{\leq X}|}$ is

$$\lim_{X\to\infty} \frac{\left|\mathcal{D}^-_{\leq X}\right|}{\left|\mathcal{D}_{\leq X}\right|} = 1 - \left(\prod_{\substack{j\geq 1 \\ j \text{ odd}}} \left(1 - 2^{-j}\right) \right).$$

Similar to the negative Pell's equation over integers, we believe it is possible that analogous results would hold for the polynomial negative Pell's equation. In other words, we believe that the limit

$$\lim_{N\to\infty} \frac{|\mathcal{D}^-_{\mathbb{F},\leq N}|}{|\mathcal{D}_{\mathbb{F},\leq N}|}$$

converges to a constant in $(0, 1)$, as shown in the negative Pell's equation over integers. In addition, we believe there are asymptotic bounds for $\left|\mathcal{D}^-_{\mathbb{F},\leq N}\right|$ and $\left|\mathcal{D}^-_{\mathbb{F},\leq N} \setminus \mathcal{D}^-_{\mathbb{F},\leq N}\right|$ as Bloomer and Dirichlet showed. However, to support this claim, this thesis alone could not provide sufficient reasoning for this. The current result of this thesis presents the function field analogue of the result by Rieger, the asymptotic expression of $|\mathcal{D}_{\mathbb{F},\leq N}|$. Therefore, future research on the negative Pell's equation over function field would involve finding the asymptotic expressions and bounds of $\left|\mathcal{D}^-_{\mathbb{F},\leq N}\right|$ and $\left|\mathcal{D}_{\mathbb{F},\leq N} \setminus \mathcal{D}^-_{\mathbb{F},\leq N}\right|$. Ultimately, the major goal of research on the negative Pell's equation over function field is to determine the convergence and the limit of

$$\lim_{N\to\infty} \frac{|\mathcal{D}^-_{\mathbb{F},\leq N}|}{|\mathcal{D}_{\mathbb{F},\leq N}|}.$$

Bibliography

[1] R.B. Ash. *A Course In Algebraic Number Theory*. Available at `https://faculty.math.illinois.edu/~r-ash/ANT.html`.

[2] M. Atiyah. *Introduction To Commutative Algebra, Student Economy Edition*. First edition. Boca Raton, FL: CRC Press, 2018.

[3] V. Blomer. "A Note on the Negative Pell Equation". In: *From Arithmetic to Zeta-Functions: Number Theory in Memory of Wolfgang Schwarz*. Ed. by J. Sander, J. Steuding, and R. Steuding. Cham: Springer International Publishing, 2016, pp. 31–40.

[4] R. Busam and E. Freitag. *Complex analysis*. eng. Universitext. Springer, 2009.

[5] K. Conrad. *Ostrowki's Theorem on F(T)*. URL: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskiF(T).pdf`.

[6] P. G. L. Dirichlet. "Einige neue Sätze über unbestimmte Gleichungen". In: *Abh. K. Preuss. Akad. d. Wiss.* (1836), pp. 649–664.

[7] D. S. Dummit and R. M. Foote. *Abstract algebra*. 3rd ed. New York: Wiley, 2004.

[8] E. Fouvry and J. Klüner. "On the negative Pell equation". eng. In: *Annals of mathematics* 172.3 (2010), pp. 2035–2104.

[9] G. H. Hardy. *An introduction to the theory of numbers*. 6th ed./ by G.H. Hardy and E.M. Wright; [revised by D.R. Heath-Brown and J.H. Silverman]. Oxford Mathematics. Oxford: Oxford University Press, 2008.

[10] P. Henrici. *Applied and computational complex analysis*. Pure and Applied Mathematics (John Wiley & Sons: Unnumbered). New York: Wiley, 1974 - 1986.

[11] C. Hunter and B. Guerrieri. "Deducing the Properties of Singularities of Functions from their Taylor Series Coefficients". In: *Siam Journal on Applied Mathematics* 39 (1980), pp. 203–203.

[12] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. 2nd ed. Vol. 84. Graduate Texts in Mathematics. New York: Springer, 1990.

[13] M. Jacobson and H. Williams. *Solving the Pell equation*. CMS Books in Mathematics. New York: Springer, 2009.

[14] P. Koymans and C. Pagano. "On Stevenhagen's conjecture". arXiv:2201.13424. 2022.

[15] F. Malagoli. "Continued fractions in function fields: polynomial analogues of McMullen's and Zaremba's conjectures". arXiv:1704.02640. 2017.

[16] J. S. Milne. "Algebraic Number Theory (v3.08)". Available at `www.jmilne.org/math/`, 2020.

[17] T. Nagell. "Über die Lösbarkeit der Gleichung $x^2 - Dy^2 = -1$". In: *Arkiv för Mat. Astr. Fysik* (1932).

[18] J. Neukirch. *Algebraic number theory*. eng. Vol. 323. Grundlehren der Mathematischen Wissenschaften. Berlin: Springer, 1999.

[19] B. Poonen. "Lectures on rationalpoints on curves". Available at `https://math.mit.edu/~poonen/papers/curves.pdf`, 2006.

[20] G.J. Rieger. "Über die Anzahl der als Summe von zwei Quadraten darstellbaren und in einer primen Restklasse gelegenen Zahlen unterhalb einer positiven Schranke. II." In: *Journal für die reine und angewandte Mathematik* 217 (1965), pp. 200–216.

[21] M. I. Rosen. *Number theory in function fields*. Vol. 210. Graduate Texts in Mathematics. New York: Springer, 2002.

[22] W. Sawin and M. Shusterman. "On the Chowla and twin primes conjectures over $\mathbb{F}_q[T]$". In: *Annals of Mathematics* 196.2 (2022), pp. 457–506.

[23] W. M. Schmidt. "On continued fractions and Diophantine approximation in power series fields". In: *Acta Arithmetica* 95.2 (2000), pp. 139–166.

[24] P. Stevenhagen. "The Number of Real Quadratic Fields Having Units of Negative Norm". In: *Experimental Mathematics* 2.2 (1993), pp. 121–136.

[25] J. Stillwell. *Mathematics and its history: a concise edition*. eng. 1st ed. 2020. Undergraduate Texts in Mathematics. Cham, Switzerland: Springer, 2020.

[26] A. Sutherland. "Lecture Notes on Number Theory I". 2017. URL: `https://dspace.mit.edu/bitstream/handle/1721.1/124987/18-785-fall-2017/contents/index.htm`.