# Rational Polynomial Pell Equations

by

Zachary L. Scherr

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2013

Doctoral Committee:

        Professor Michael E. Zieve, Chair
        Professor Jeffrey C. Lagarias
        Assistant Professor Dani Neftin
        Associate Professor Kartik Prasanna
        Professor Martin Strauss

To my parents Suanne and David, my sister Alizah and my uncle Mark.

# ACKNOWLEDGEMENTS

I'd like to start by thanking my adviser, Dr. Michael Zieve, for everything he's done for me over the last four years. In addition to helping me with this thesis, he has exposed me to many different interesting problems in number theory and algebra. His energy and enthusiasm for mathematics knows no bounds, and my success in graduate school is due in large part to the effort he put in to mentoring me. I'd also like to thank Dr. Jeffrey Lagarias for his many helpful comments and conversations regarding this thesis. Special thanks go out to my committee members Dr. Danny Neftin, Dr. Kartik Prasanna and Dr. Martin Strauss for helping me with my defense.

To my friends in Ann Arbor, thank you for making the last six years so special. Thank you to my various bridge partners for helping me develop my skills and find an outlet outside of work. I would also like to thank the student arithmetic seminar for being a great forum to learn and discuss various pieces of mathematics.

To my parents, my sister and my uncle, thank you for always being there. Thank you for all of your support and encouragement while I have been away from home.

# TABLE OF CONTENTS

# CHAPTER I

# Introduction and Background

## 1.1 Introduction

Let $d$ be a positive, non-square integer. It is a well known and classical result in elementary number theory that the Pell equation,

$$x^2 - dy^2 = 1$$

has infinitely many solutions $x, y \in \mathbb{Z}$. In the 1760's, Euler [8] discovered several identities for the Pell equation. Among them, he proved that if $d = n^2 + 1$ for some integer $n$ then

$$(2n^2 + 1)^2 - (n^2 + 1)(2n)^2 = 1.$$

Such an identity has the potential for applications to the problem of computing class numbers of real quadratic number fields. If, for example, we know that

$$(2n^2 + 1) + (2n)\sqrt{n^2 + 1}$$

is a fundamental unit in $\mathbb{Q}(\sqrt{n^2 + 1})$ then we may be able to use Dirichlet's class number formula to compute class numbers of real quadratic fields of the form $\mathbb{Q}(\sqrt{n^2 + 1})$. For more on the connection between Pell identities and class numbers we refer the reader to [16].

Motivated by Euler's identity, we consider the following generalization of the Pell equation.

**Question I.1.** *Let $R$ be an integral domain of characteristic different from 2. For which non-constant, non-square $d(x) \in R[x]$ does the Pell equation*

(1.1) $$f(x)^2 - d(x)g(x)^2 = 1$$

*have solutions $f(x), g(x) \in R[x]$ with $g(x)$ non-zero?*

*Remark* I.2. We will call a solution to (1.1) with $g(x)$ non-zero a **non-trivial** solution.

The way to address Question I.1 is to first develop an understanding of when there exist non-trivial solutions in $K[x]$ where $K$ is the fraction field of $R$. Once one knows how to find all of the solutions in $K[x]$, there is hope of picking out those solutions which have coefficients in $R$.

The theory of polynomial Pell equations over $\mathbb{C}$ was developed in the 1800's by Abel [1], Chebyshev [5] and others because of the connection of Equation 1.1 to certain integrals. In particular, they were interested in understanding for which $d(x) \in \mathbb{C}[x]$ do there exist polynomials $F(x) \in \mathbb{C}[x]$ such that the integral

$$\int \frac{F(x)}{\sqrt{d(x)}} dx$$

can be expressed in terms of the logarithm of a function of $\sqrt{d(x)}$. It was proved (for a modern account see [2]) that such $d(x)$ are precisely those for which Equation 1.1 has a non-trivial solution. Furthermore, $F(x)$ must equal $\dfrac{f'(x)}{g(x)}$ where $f(x)$ and $g(x)$ give a non-trivial solution to (1.1). Here, if we let $u = f(x) + \sqrt{d(x)}g(x)$ then we have

$$\int \frac{F(x)}{\sqrt{d(x)}} dx = \int \frac{du}{u}.$$

In this thesis we will study Question I.1 over $\mathbb{Z}$ and $\mathbb{Q}$ in the case that $d(x)$ is a quartic polynomial. The quadratic case was worked on previously in [16, 18, 20, 21], and worked out completely for monic, quadratic $d(x)$ by Webb and Yokota in [31].

When $d(x)$ is square-free and has degree at least 4, equation 1.1 over fields $K$ becomes interesting due to its connection with arithmetic geometry. Namely, (1.1) has non-trivial solutions if and only if a certain explicit $K$-rational point on a certain abelian variety is a torsion point. Furthermore, if (1.1) has a non-trivial solution then the continued fraction of $\sqrt{d(x)}$, when viewed as a Laurent series in $K((x^{-1}))$, will be periodic of period related to the torsion order of said point.

In Chapter II we use the theory of elliptic curves to work out a complete list of all quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which (1.1) has a non-trivial solution in $\mathbb{Q}[x]$. Using our classification, we are able to settle several open problems about polynomial Pell equations for quartic polynomials.

The first conjecture pertains to the period of the continued fraction of $\sqrt{d(x)}$ where $d(x)$ is a quartic, square-free polynomial in $\mathbb{Q}[x]$. In 1962 Schinzel [23] concluded that if $d(x) \in \mathbb{Q}[x]$ is quartic and square-free, and (1.1) has a non-trivial solution, then the period of the continued fraction of $\sqrt{d(x)}$ has value among

$$(1.2) \qquad \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 18, 22\}.$$

After the calculation of the list in (1.2), Schinzel questions whether periods 5, 7, 9 and 11 actually occur for any monic, quartic, square-free polynomials in $\mathbb{Q}[x]$. In Chapter III we answer Schinzel's question for arbitrary quartic, square-free polynomials in $\mathbb{Q}[x]$. We prove

**Theorem I.3.** *There are no quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period $9$ or $11$. Furthermore, we can*

*find infinitely many quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which the period is 5 or 7. The period 7 case can only occur with $d(x)$ non-monic.*

*Remark* I.4. Moreover, for each possible period $n$ we develop a complete list of all quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period $n$.

In Chapter V we discuss what happens if we replace $\mathbb{Q}$ by a number field or allow $d(x)$ to have degree larger than 4. In the case of quartic polynomials over quadratic number fields we are able to determine a list of possible periods which is analogous to Schinzel's list. We get

**Theorem I.5.** *Let $K$ be a quadratic number field and let $d(x) \in K[x]$ be a quartic, square-free polynomial for which the continued fraction of $\sqrt{d(x)}$ is periodic. Then the period is among*

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 22, 26, 30, 34\}.$$

*Furthermore, there do exist quartic polynomials having periods 9 and 11 over quadratic number fields.*

Existence of periods 13, 15 and 17 are still open, although we are able to give ideas on how one might be able to produce examples.

The formulas obtained in Chapter II also allow us to tackle the Pell equation (1.1) in the case $R = \mathbb{Z}$. In this case, Webb and Yokota [29, 30, 31, 32, 33] have been working towards an understanding of which monic, quartic polynomials $d(x) \in \mathbb{Z}[x]$ have a non-trivial solution to (1.1) with $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$. In their work, Webb and Yokota answer this question in the specific case that the period of the continued fraction of $\sqrt{d(x)}$ is either 1 or 2. They conjecture that for higher periods there should never be a non-trivial solution. In Chapter IV we disprove their conjecture

and completely answer Question I.1 for all monic, quartic, square-free polynomials in $\mathbb{Z}[x]$. We prove

**Theorem I.6.** *Aside from Webb and Yokota's list, there exist precisely two infinite families of monic, quartic, square-free polynomials $d(x) \in \mathbb{Z}[x]$ for which the Pell equation has a non-trivial solution in $\mathbb{Z}[x]$. These polynomials are*

$$x^4 + (4c+2)x^3 + (6c^2 + 6c - 7)x^2 + (4c^3 + 6c^2 - 14c - 12)x + c^4 + 2c^3 - 7c^2 - 12c + 6,$$

$$x^4 + (4c+2)x^3 + (6c^2 + 6c - 7)x^2 + (4c^3 + 6c^2 - 14c - 4)x + c^4 + 2c^3 - 7c^2 - 4c + 10.$$

*where $c \in \mathbb{Z}$. Both of these families have the property that the continued fraction of their square root has period 6.*

## 1.2  Background

Let $K$ be a field of characteristic different from 2. Let $d(x) \in K[x]$ be a non-constant, square-free polynomial. We are concerned with studying the following question about the polynomial analogue of the Pell equation.

**Question I.7.** *Does the equation*

$$(1.3) \qquad\qquad f(x)^2 - d(x)g(x)^2 = c$$

*have a solution with $f(x), g(x)$ in $K[x]$ and $c \in K^\times$ where $g(x)$ is non-zero?*

To answer Question I.7 we may make a few observations and simplifications. First, observe that in order for (1.3) to have a non-trivial solution, necessarily we must have that $d(x)$ has even degree and leading coefficient in $(K^\times)^2$. By absorbing the leading coefficient of $d(x)$ into $g(x)$ we may, and often will, assume that $d(x)$ is monic. Observe also that for any $a \in K$, the right hand side of equation (1.3) is invariant under the translation $x \mapsto x + a$. If

$$d(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

then the translation $x \mapsto x - \frac{a_{n-1}}{n}$ allows us to assume without loss of generality that $a_{n-1}$ is zero. We call a polynomial of degree $n$ **centered** if the coefficient of $x^{n-1}$ is zero. Again, we may, and often will, assume that $d(x)$ is centered.

The following lemma guarantees that there is no loss of generality in replacing the right hand side of (1.3) with 1.

**Lemma I.8.** *There exists a solution* $f(x), g(x), c$ *to* (1.3) *if and only if there is a solution* $\widetilde{f}(x), \widetilde{g}(x), 1.$

*Proof.* One implication is clear. For the other one, suppose there exist $c \in K^{\times}$ and polynomials $f(x)$ and $g(x)$ in $K[x]$ for which

$$f(x)^2 - d(x)g(x)^2 = c.$$

Set

$$\widetilde{f}(x) = \frac{1}{c} \cdot (f(x)^2 + d(x)g(x)^2)$$

and

$$\widetilde{g}(x) = \frac{1}{c} \cdot 2f(x)g(x).$$

It is then a simple matter to check that in fact

$$\widetilde{f}(x)^2 - d(x)\widetilde{g}(x)^2 = 1. \qquad \square$$

In view of Lemma I.8, we will restrict ourselves to looking for monic, centered, square-free, even degree polynomials $d(x) \in K[x]$ for which

(1.4) $$f(x)^2 - d(x)g(x)^2 = 1$$

has a solution with $g(x)$ non-zero.

There are two main approaches to detecting and finding solutions to (1.4). The first approach involves the use of continued fractions. We give a brief review of

continued fractions in Laurent series fields. We can expand elements of $K((x^{-1}))$ into continued fractions, which enjoy many of the formal properties possessed by continued fractions in $\mathbb{R}$. For

$$f(x) = \sum_{n \leq M} b_n x^n \in K((x^{-1})),$$

we define

$$\lfloor f(x) \rfloor = \sum_{n=0}^{M} b_n x^n \in K[x].$$

We can then form the continued fraction of $f(x)$ as follows. Set $a_0(x) = \lfloor f(x) \rfloor$ and $\alpha_0(x) = \frac{1}{f(x) - a_0(x)}$. For $i \geq 1$ we recursively define

$$a_i(x) = \lfloor \alpha_{i-1}(x) \rfloor$$

and

$$\alpha_i(x) = \frac{1}{\alpha_{i-1}(x) - a_i(x)}.$$

This yields the continued fraction expansion

$$f(x) = [a_0(x); a_1(x), a_2(x), \ldots]$$

where

$$[a_0(x); a_1(x), a_2(x), \ldots] := a_0(x) + \cfrac{1}{a_1(x) + \cfrac{1}{a_2(x) + \cfrac{1}{\ddots}}}$$

In the above definition for the continued fraction, the $\alpha_i(x)$'s are said to be the **complete quotients** of $f(x)$ and the $a_i(x)$'s are said to be the **partial quotients** of $f(x)$. The truncations of the above continued fraction,

$$\frac{p_i(x)}{q_i(x)} = [a_0(x); a_1(x) \ldots, a_i(x)]$$

periodic and hence that the integer Pell equation always has a non-trivial solution. In our setting, if $K$ has infinite cardinality then it may very well be the case that the continued fraction of $\sqrt{d(x)}$ is not periodic.

It is proved in [24] that if $p(x)$ and $q(x)$ are polynomials in $K[x]$, with $q(x)$ non-zero, such that

$$p(x)^2 - d(x)q(x)^2 \in K^{\times}$$

then necessarily $\gcd(p(x), q(x)) = 1$ and $\dfrac{p(x)}{q(x)}$ is a convergent of $\sqrt{d(x)}$. Thus to actually produce solutions to (1.5), we only need to find convergents $\dfrac{p_i(x)}{q_i(x)}$ of $\sqrt{d(x)}$ for which

$$p_i(x)^2 - d(x)q_i(x)^2 = c^2.$$

If $r$ is the period of the continued fraction of $\sqrt{d(x)}$, then such an $i$ is guaranteed to exist with $i < r$ so that we only need to check finitely many convergents. Before moving on, we make a quick remark on the problem of determining whether or not the continued fraction of $\sqrt{d(x)}$ is periodic. As we have seen above, if $K$ is a finite field then the continued fraction of $\sqrt{d(x)}$ is always periodic. For infinite fields, the question is much more subtle. If $K$ is a number field then Yu [34] gives a deterministic algorithm for deciding whether or not the continued fraction of $\sqrt{d(x)}$ is periodic. His approach involves reducing $d(x)$ modulo several primes for which the reduction $\widetilde{d}(x)$ stays square-free. Piecing together information about the periods of the continued fractions of $\sqrt{\widetilde{d}(x)}$ over the respective finite fields allows one to determine whether the continued fraction of $\sqrt{d(x)}$ is periodic. This is not relevant to the thesis, but the interested reader is encouraged to look at Yu's paper.

## 1.4  Geometry

The second approach to determining whether or not

$$(1.6) \qquad\qquad f(x)^2 - d(x)g(x)^2 = 1$$

has non-trivial solutions involves the geometry of abelian varieties. Consider the function field $K(x,y)$ where $y^2 = d(x)$. Notice that by Lemma I.8, a non-trivial solution to (1.6) exists precisely when the subring $K[x,y]$ contains non-constant units. Because $K(x,y)$ is the function field of the curve $C$ defined by $y^2 = d(x)$, it is reasonable to guess that the problem of determining whether non-trivial solutions exist to (1.6) might be translated into a geometric question about $C$. To translate this problem to geometry we will now assume, and our assumption will remain throughout, that $\deg(d(x)) > 2$.

Because $d(x)$ is monic, square-free and has even degree, the curve $C$ is smooth everywhere except at $\infty$, and the normalization of $C$, denoted by $\widetilde{C}$, has two smooth $K$-points $P$ and $Q$ lying above $\infty$. Let $\gamma$ be the geometric genus of $\widetilde{C}$. Then

$$\gamma = \frac{\deg(d(x))}{2} - 1$$

and the Jacobian of $\widetilde{C}$,

$$J := \operatorname{Pic}^0(\widetilde{C}),$$

is an abelian variety of dimension $\gamma$. Consider the embedding $\phi : \widetilde{C} \hookrightarrow J$ defined by $R \mapsto [R - Q]$. With this setup we get the following nice geometric interpretation for investigating solutions of (1.6).

**Lemma I.10.** *Equation (1.6) has a non-trivial solution in $K[x]$ if and only if $\phi(P)$ is a torsion point on $J$.*

*Proof.* If $\phi(P)$ is a torsion point on $J$ then there exists a positive integer $n$ such that

$$n[P - Q] = [0]$$

in $\mathrm{Pic}^0(\widetilde{C})$. Thus there exists $u \in K(x, y)$ for which

$$\mathrm{div}(u) = nP - nQ.$$

Because the the Galois group $\mathrm{Gal}(K(x, y)/K(x))$ acts transitively on the places above $\infty$, we have that the conjugation automorphism on $K(x, y)$ interchanges $P$ and $Q$, and so the divisor of $\bar{u}$ is

$$\mathrm{div}(\bar{u}) = nQ - nP.$$

write $u = f(x) + g(x)y$ with $f(x), g(x) \in K(x)$. Then because $u$ and $\bar{u} = f(x) - g(x)y$ have poles only at the infinite places, the same is true for

$$2f(x) = u + \bar{u}$$

and

$$2g(x)y = u - \bar{u}.$$

Thus $f(x), g(x) \in K[x]$ are polynomials, and $u \in K[x, y]$. Furthermore,

$$\mathrm{div}(u \cdot \bar{u}) = 0$$

so

$$u \cdot \bar{u} = f(x)^2 - d(x)g(x)^2 \in K^{\times}$$

and by Lemma I.8 we get a solution to the Pell equation.

Conversely, if $f(x), g(x)$ give a solution to

$$f(x)^2 - d(x)g(x)^2 = 1$$

then $u = f(x) + d(x)y$ is a unit in $K[x,y]$ and $u \cdot \overline{u} = 1$. This immediately implies that $u$ and $\overline{u}$ cannot have zeros at the finite places of $K(x,y)$. In view of $\overline{u} = \frac{1}{u}$ we see that $u$ cannot have any poles at the finite places either. Thus there exist integers $r, s$ such that

$$\operatorname{div}(u) = rP - sQ.$$

Since this is a principal divisor, we must have $r = s$ and hence $\phi(P)$ is a torsion point. $\qquad \square$

The above argument can be modified to prove even more. Suppose that there exist non-trivial units in $K[x,y]$, that is there exists $u \in K[x,y]\backslash K$ such that $N(u) := u \cdot \overline{u} \in K^{\times}$. By Lemma I.8 then there exists a unit $\widetilde{u} \in K[x,y]$ with $N(u) = 1$. Among units $u \in K[x,y]$ with $N(u) = 1$, let $u_0$ be such that the degree of $u_0$ is minimal. That is, the divisor $(u_0) = nP - nQ$ is such that $n$ is positive and minimal. We then get the complete description of norm 1 elements in $K[x,y]$ as follows.

**Proposition I.11.** *Let* $v \in K[x,y]\backslash K$. *Then* $N(v) = 1$ *if and only if* $v = \pm u_0^k$ *for some* $k \in \mathbb{Z}$.

*Proof.* Because the norm is multiplicative, it's clear that $N(\pm u_0^k) = 1$ for $k \in \mathbb{Z}$. For the converse, suppose $v \in K[x,y]\backslash K$ is such that $N(v) = 1$. Then the divisor of $v$ is of the form $(v) = mP - mQ$ for some integer $m$. Replacing $v$ with $\overline{v} = \frac{1}{v}$ if necessary, we may assume without loss of generality that $m > 0$. By our choice of $u_0$, we know that $m \geq n$ so there exists an integer $k \geq 1$ such that $nk \leq m < n(k+1)$. Consider

$$w = \frac{v}{u_0^k} = v\overline{u_0}^k \in K[x,y].$$

We have that the divisor of $w$ is

$$(w) = (v) - (u_0^k) = (m - nk)P - (m - nk)Q.$$

Because $0 \leq m - nk < n$ by our choice of $k$, we necessarily have that $w \in K^\times$. Since the norm is multiplicative, we also get that

$$1 = N(w) = w^2$$

so in fact $w = \pm 1$ and the proof is complete. $\qquad\qquad\qquad\qquad\qquad\square$

The construction of $J$ and $\phi(P)$ is of the utmost importance in studying questions regarding (1.6). Since we will refer to this construction often, we say that the pair $(J, \phi(P))$ **corresponds** to $d(x)$. In our construction, we chose $Q$ to be mapped to the identity of $J$, and looked at the image of $P$. Of course geometrically the points $P$ and $Q$ are indistinguishable since the conjugation involution of $K(x, y)$ interchanges $P$ and $Q$. Thus we could have used either $P$ or $Q$ as the origin as long as we study the image of the other point.

Heuristically, Lemma 1.6 says that if $K$ has characteristic 0 then we shouldn't expect a random $d(x)$ to admit a non-trivial solution to (1.6). This is because for a generic pair $(A, p)$, where $A$ is an abelian variety defined over $K$ and $p \in A(K)$, we expect that $p$ is non-torsion. Of course this is only a heuristic since it's not even known which abelian varieties $A$ and points $p \in A(K)$ arise in this construction.

## 1.5 The Connection

Although it is not crucial for our study of quartic polynomials over $\mathbb{Q}$, we briefly digress to discuss the relationship between the geometry of Section 1.4 and the continued fractions of Section 1.3. Let $K$ be a field of characteristic different from 2 and let $f(x) \in K((x^{-1}))$ be a Laurent series. For $i \geq 0$ we define $\alpha_i(x)$ and $a_i(x)$ in accordance with Section 1.2. We then say that the continued fraction of $f(x)$ is

**quasi-periodic** if there exist integers $r \geq 0$ and $s > 1$ such that

$$\alpha_{r+s}(x) = c\alpha_r(x) \tag{1.7}$$

for some $c \in K^{\times}$. The smallest $s > 0$ for which there exist such an $r$ and $c$ is then said to be the **quasi-period** of the continued fraction of $f(x)$. It is clear that if the continued fraction of $f(x)$ is periodic then its quasi-period divides its period.

Repeated application of the formulas for calculating the $\alpha_i$'s gives us the following lemma.

**Lemma I.12.** *Let $f(x) \in K((x^{-1}))$ be a laurent series and let $\alpha_i(x)$ denote the $i$-th complete quotient for the continued fractions expansion of $f(x)$. If*

$$\alpha_{r+s}(x) = c\alpha_r(x)$$

*for $c \in K^{\times}$ and integers $r \geq 0$ and $s > 1$ then for any $n \geq 0$ we have*

$$\alpha_{r+ns}(x) = c^{1+(-1)^s+(-1)^{2s}+...+(-1)^{(n-1)s}}\alpha_r(x). \tag{1.8}$$

*Proof.* We first show by induction that for $i \geq 0$ we have

$$\alpha_{r+s+i}(x) = c^{(-1)^i}\alpha_{r+i}(x). \tag{1.9}$$

This is true by assumption when $i = 0$. Assuming (1.9) is true for some $i \geq 0$, we have

$$
\begin{aligned}
\alpha_{r+s+i+1}(x) &= \frac{1}{\alpha_{r+s+i}(x) - \lfloor \alpha_{r+s+i}(x) \rfloor} \\
&= \frac{1}{c^{(-1)^i}\alpha_{r+i}(x) - \lfloor c^{(-1)^i}\alpha_{r+i}(x) \rfloor} \\
&= c^{(-1)^{i+1}}\frac{1}{\alpha_{r+i}(x) - \lfloor \alpha_{r+i}(x) \rfloor} \\
&= c^{(-1)^{i+1}}\alpha_{r+i+1}(x).
\end{aligned}
$$

Thus

$$\alpha_{r+ns}(x) = \alpha_{r+s+(n-1)s}(x) = c^{(-1)^{(n-1)s}} \alpha_{r+(n-1)s}(x).$$

A simple induction on $n$ then proves (1.8). □

Thus we have the following simple lemmas essentially due to Abel, and proved in Adams-Razar [2].

**Lemma I.13.** *If the continued fraction of $f(x)$ is quasi-periodic of odd quasi-period $s$ then the continued fraction of $f(x)$ is periodic with period either $s$ or $2s$. It will have period $s$ precisely when the value of $c$ in (1.7) is 1.*

**Lemma I.14.** *If the continued fraction of $f(x)$ is quasi-periodic of even quasi-period $s$ then the continued fraction of $f(x)$ is periodic if and only if the constant $c$ in (1.7) is a root of unity. If $c$ is a primitive $m$-th root of unity then the period is $sm$.*

*Proof.* We have that $\alpha_{r+s}(x) = c\alpha_r(x)$ for some $c \in K^\times$. If $s$ is odd then by (1.8) we have that

$$\alpha_{r+2s} = c^{(-1)^s} \alpha_{r+s}(x) = c^{(-1)^s+1} \alpha_r(x)$$

so $\alpha_{r+2s}(x) = \alpha_r(x)$. Thus the period is either $s$ or $2s$ and in fact it can only be $s$ if $c = 1$.

If on the other hand $s$ is even then by (1.8) we see that for any $n \geq 0$ we have

$$\alpha_{r+ns}(x) = c^n \alpha_r(x).$$

This implies that the continued fraction for $f(x)$ will be periodic precisely when $c$ is a root of unity, and furthermore, if $c$ is a primitive $m$-th root of unity then the period will be $sm$. □

We now specialize to the case $f(x) = \sqrt{d(x)}$ where $d(x) \in K[x]$ is a monic, square-free polynomial of even degree at least 4. In this case if $(A, p)$ is the associated abelian

variety and $K$-point then $\sqrt{d(x)}$ will have a periodic continued fraction precisely when $p$ is torsion. The following corollary to a theorem of Berry [3], which is a generalization of Abel's ideas, gives some indication of how to relate the period of the continued fraction with the order of the corresponding torsion point.

**Proposition I.15** (Berry)**.** *Let $d(x)$ have degree $2n$ with $n \geq 2$, let $(A, p)$ be the pair corresponding to $d(x)$, and suppose that $p \in A(K)$ is a torsion point of order $m$. If $s$ is the quasi-period of the continued fraction of $\sqrt{d(x)}$ then $s \leq m - n + 1$. Moreover, equality occurs if $n = 2$.*

Proposition I.15 implies that if $d(x)$ is a quartic polynomial and the corresponding $K$-point is a torsion point of order $m$ then the quasi-period of the continued fraction for $\sqrt{d(x)}$ is $m - 1$. In the case that $m$ is even we have by Lemma I.13 that the period of the continued fraction of $\sqrt{d(x)}$ is either $m - 1$ or $2(m - 1)$. Notice that generically one should expect the period to be $2(m - 1)$. This is because the period will be $m - 1$ precisely when $c = 1$, and *a priori* there is no reason to expect this to be the case. If on the other hand $m$ is odd then it is a theorem of Adams and Razar [2] that $c = 1$ and the period is in fact $m - 1$. In summary, we can relate the period of the continued fraction to order of the torsion point as follows.

**Theorem I.16** (Adams-Razar)**.** *Let $K$ be a field of characteristic different from 2 and let $d(x) \in K[x]$ be a monic, quartic, square-free polynomial. Let $(E, p)$ be the corresponding elliptic curve and $K$-point and suppose that $p$ is a torsion point of order $m$. If $n$ is the period of the continued fraction of $\sqrt{d(x)}$ then either*

$$n = m - 1$$

*or*

$$n = 2(m - 1)$$

*where the second case can only occur if m is even.*

## 1.6 To Come

For the remainder of this document, at least up until Chapter V, we study properties of quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which the Pell equation

$$(1.10) \qquad\qquad f(x)^2 - d(x)g(x)^2 = 1$$

has non-trivial solutions. One reason to study quartic polynomials is that the corresponding abelian variety is an elliptic curve, and over $\mathbb{Q}$, elliptic curves have been very well studied for a long time. In particular, we know precisely which groups arise as the group of rational torsion points on an elliptic curve. We have the following celebrated theorem of Mazur [15].

**Theorem I.17** (Mazur)**.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$. The torsion subgroup of the group of rational points of $E$ is isomorphic to one of the following groups,*

$$\mathbb{Z}/N\mathbb{Z} \text{ where } 1 \le N \le 10 \text{ or } N = 12$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \text{ where } 1 \le N \le 4.$$

In our setting this yields the following important corollary.

**Corollary I.18.** *Let $E$ be an elliptic curve defined over $\mathbb{Q}$. If $p \in E(\mathbb{Q})$ is a torsion point then the order of $p$ is among*

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}.$$

Moreover, if $1 \le N \le 10$ or $N = 12$ then Kubert [13] gave a parametrization of the isomorphism class of pairs $(E, p)$ where $E$ is an elliptic curve defined over $\mathbb{Q}$ and $p \in E(\mathbb{Q})$ is rational torsion point of order $N$.

In chapter II, we will use Kubert's parametrizations, along with explicit formulas from [2], to give a complete description of all monic, centered, square-free, quartic polynomials $d(x) \in \mathbb{Q}[x]$ for which (1.10) has a non-trivial solution. Once we have developed explicit formulas for such $d(x)$, we will be able to settle several open problems in the area of rational polynomial Pell equations.

The first problem we tackle is that of determining all possibilities for the period of the continued fraction of $\sqrt{d(x)}$ for quartic, square-free polynomials $d(x) \in \mathbb{Q}$. Combining Corollary I.18 with Theorem I.16, Schinzel points out in [23] that if the continued fraction of $\sqrt{d(x)}$ is periodic then its period is among

(1.11) $$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 18, 22\}.$$

The list in (1.11) represents the set of possible periods of the continued fraction, but Schinzel questions whether periods 5,7,9 and 11 actually occur. The reason why Schinzel singles out the odd periods goes back to our remarks in Section 1.5. Malyshev partially answered this question in [14]. He asserts that if $d(x)$ is monic then the period of the continued fraction of $\sqrt{d(x)}$ cannot be 7. In Chapter III, we will fully answer Schinzel's question using the formulas of Chapter II. In particular, we will prove that periods 9 and 11 never occur for any $d(x) \in \mathbb{Q}[x]$. We will also expand on Malyshev's result by proving that there are infinitely many non-monic $d(x) \in \mathbb{Q}[x]$ for which the period is 7.

In another direction, several authors [29, 30, 31, 33] have specialized to the case of looking at $d(x) \in \mathbb{Z}[x]$. In this setting, they have been interested in obtaining some sort of classification of monic, square-free, quartic polynomials $d(x) \in \mathbb{Z}[x]$ for which there exists a non-trivial solution to (1.10) with $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ as well. We will use the formulas obtained in Chapter II to give a complete answer to this question in the case that $d(x)$ is monic, quartic and square-free.

# CHAPTER II

# Parametrizations

## 2.1 Synopsis

In this chapter we will obtain parametrizations of all monic, square-free quartics $d(x) \in \mathbb{Q}[x]$ for which the equation

$$(2.1) \qquad\qquad f(x)^2 - d(x)g(x)^2 = 1$$

has a non-trivial solution $f(x), g(x) \in \mathbb{Q}[x]$. Notice that equation (2.1) is invariant under the substitution $x \mapsto x + c$ for any $c \in \mathbb{Q}$. Thus by choosing $c \in \mathbb{Q}$ appropriately, we may assume that $d(x)$ contains no cubic term.

Let $C$ denote the normalization of the curve $y^2 = d(x)$. Since $d(x)$ is monic, square-free and has degree 4, the curve $C$ has genus 1 and has two points, $P$ and $Q$, above $\infty$. Consider the map

$$\varphi : C \to \operatorname{Pic}^0(C)$$

defined by $\varphi(R) = [R - Q]$. We've already seen in Chapter I that equation (2.1) has a non-constant solution if and only if $\varphi(P)$ is a torsion point on the elliptic curve $\operatorname{Pic}^0(C)$. Further, Adams and Razar [2] give an explicit embedding of $\operatorname{Pic}^0(C)$ and $\varphi(P)$ in $\mathbb{P}^2$. Namely,

**Lemma II.1.** *The polynomial*

$$d(x) = x^4 - 6ax^2 - 8bx + c$$

*corresponds to the curve*

$$v^2 = u^3 + Au + B$$

*and the point $(a, b)$ where*

$$A = \frac{-1}{4}(c + 3a^2)$$
$$B = b^2 - a^3 - Aa.$$

Thus to parametrize all monic, square-free quartics $d(x) \in \mathbb{Q}[x]$ for which (2.1) has a non-constant solution, it suffices to be able to write down all elliptic curves in short Weierstrass form with a $\mathbb{Q}$-rational torsion point.

The methods in this chapter work only when the torsion point in question has order at least 4. Thus in accordance with Theorem I.16 we will be able to parametrize all quartic polynomials for which the continued fraction of their square root is periodic of period at least 3. For periods 1 and 2 we can just use brute force to write down a parametrization.

**Proposition II.2.** *Let $d(x) \in \mathbb{Q}[x]$ be a monic, centered, quartic, square-free polynomial. The continued fraction of $\sqrt{d(x)}$ will be periodic of period 1 if and only if $d(x) = (x^2 + c)^2 + 1$ for some $c \in \mathbb{Q}$.*

**Proposition II.3.** *Let $d(x) \in \mathbb{Q}[x]$ be a monic, centered, quartic, square-free polynomial. Then the continued fraction of $\sqrt{d(x)}$ will be periodic of period 2 if and only if $d(x) = (x^2 - c^2)^2 + a(x - c)$ for some $a, c \in \mathbb{Q}$ with $a \neq 0$ or $d(x) = (x^2 + c)^2 + a$ for some $a, c \in \mathbb{Q}$ with $a \neq 0, 1$.*

## 2.2   Tate Normal Form

While our goal is to write down all elliptic curves in short Weierstrass form with a $\mathbb{Q}$-rational torsion point, it is convenient to deal with curves in Tate normal form.

**Definition II.4.** A non-singular plane cubic of the form

$$y^2 + a_2 xy + a_4 y = x^3 + a_1 x^2 + a_3 x + x_5$$

is said to be in **Tate normal form** if $a_3 = a_5 = 0$ and $a_4 = a_1$. For consistency with the literature, we will typically write such a cubic as

$$y^2 + (1 - c)xy - by = x^3 - bx^2.$$

*Remark* II.5. The reason one works with Tate normal form is as follows. For $n \in \{4, 5, 6, 7, 8, 9, 10, 12\}$ Kubert [13] writes down explicit formulas for $b$ and $c$ so that the point $(0, 0)$ on $E$ is a torsion point of order $n$.

Because we would like to be able to write our curves in short Weierstrass form, we need to know how to convert from one form to another. The following lemma works over any field of characteristic not equal to 2. It essentially follows a procedure of [12], which details how to convert an elliptic curve in Weierstrass form to Tate normal form.

**Lemma II.6.** *Let $E/K$ be in short Weierstrass form, $y^2 = x^3 + Ax + B$. For $(r, s) = P \in E(K)$, a point of order neither 2 nor 3, there exist constants $c_{E,P}$ and $b_{E,P}$ in $K$ such that $E$ is isomorphic to the curve*

$$y^2 + (1 - c_{E,P})xy - b_{E,P}y = x^3 - b_{E,P}x^2$$

*for which maps $P$ to $(0, 0)$. Furthermore, if in our construction a curve $E'/K$ of the form $y^2 = x^3 + A'x + B'$ with $P' \in E(K)$ is such that $c_{E',P'} = c_{E,P}$ and $b_{E',P'} = b_{E,P}$ then necessarily there exists $u \in K$ such that $A' = A/u^4$, $B' = B/u^6$, and $P' = (r/u^2, s/u^3)$.*

*Proof.* We first start out by transforming our curve in short Weierstrass form to a curve in Tate Normal Form by a series of invertible isomorphisms. By making the

substitution $(x, y) \mapsto (x + r, y + s)$ we get the curve

$$y^2 + 2sy = x^3 + 3rx^2 + (3r^2 + A)x.$$

It is easy to check that since $(r, s)$ doesn't have order 2 then necessarily $s \neq 0$. Thus we can make the substitution $(x, y) \mapsto (x, y + Qx)$ where $Q = \dfrac{3r^2 + A}{2s}$ to get

$$y^2 + 2Qxy + 2sy = x^3 + (3r - Q^2)x^2.$$

It is also easy to check that since $(0, 0)$, the image of $(r, s)$ on this curve, doesn't have order 3 then the coefficient of $x^2$ is non-zero. Hence we may make the substitution $(x, y) \mapsto (t^2 x, t^3 y)$, where $t = \dfrac{2s}{3r - Q^2}$, to transform our curve into

$$y^2 + \frac{2Q}{t}xy + \frac{2s}{t^3}y = x^3 + \frac{3r - Q^2}{t^2}x^2.$$

By our choice of $t$ we have that $\dfrac{2s}{t^3} = \dfrac{3r - Q^2}{t^2}$ so letting $b_{E,P} = -\dfrac{2s}{t^3}$ and $c_{E,P} = 1 - \dfrac{2Q}{t}$ we have

$$y^2 + (1 - c_{E,P})xy - b_{E,P}y = x^3 - b_{E,P}x^2.$$

All of our transformations are invertible, and $(r, s)$ maps to $(0, 0)$ so we have our desired isomorphism. This is *a priori* just an isomorphism of varieties. But since our isomorphism fixes the point $[0, 1, 0]$, which is the identity element in the group of $K$ points in the projective closure of both of these plane cubics, our map is also an isogeny and hence a group isomorphism as well.

If $E'/K$ is another curve in the form $y^2 = x^3 + A'x + B'$ with $c_{E',P'} = c_{E,P}$ and $b_{E',P'} = b_{E,P}$ then we can compose isomorphisms to see that $E \cong E'$ over $\overline{K}$. Furthermore, this isomorphism fixes the identity element $[0, 1, 0]$ so it is an isogeny as well. It is proved in [25, p. 45] that the only isomorphisms of elliptic curves which preserve short Weierstrass form are of the type $(x, y) \mapsto (x/u^2, y/u^3)$ with $u \in \overline{K}^\times$.

To see that $u \in K$, note that we have

$$A, B, r, s, \frac{A}{u^4}, \frac{B}{u^6}, \frac{r}{u^2}, \frac{s}{u^3} \in K.$$

We know that $s$ is non-zero. If either $r$ or $A$ is also non-zero then it is clear that $u \in K$. Otherwise, we have the point $(0, s)$ on $y^2 = x^3 + s^2$. It is easy to check that $(0, s)$ has order 3, which contradicts the hypotheses of the lemma. $\qquad\square$

If we follow the proof of Lemma II.6 then we can write out explicitly which curves in short Weierstrass form correspond to a given curve in Tate Normal Form.

**Proposition II.7.** *Let $E$ be an elliptic curve over $K$ defined by $y^2 + (1-c)xy - by = x^3 - bx^2$. Then an elliptic curve $y^2 = x^3 + Ax + B$ with $K$-rational point $(r, s)$ is isomorphic to $E$ (in the sense of Lemma II.6) if and only if there exists $u \in K^{\times}$ with*

$$
\begin{aligned}
u^4 A &= -\frac{1}{3}b^2 + \frac{1}{6}bc^2 + \frac{1}{6}bc - \frac{1}{3}b - \frac{1}{48}c^4 \\
&\quad + \frac{1}{12}c^3 - \frac{1}{8}c^2 + \frac{1}{12}c - \frac{1}{48} \\
u^6 B &= -\frac{2}{27}b^3 + \frac{1}{18}b^2c^2 + \frac{1}{18}b^2c + \frac{5}{36}b^2 \\
&\quad - \frac{1}{72}bc^4 + \frac{1}{72}bc^3 + \frac{1}{24}bc^2 - \frac{5}{72}bc \\
&\quad + \frac{1}{36}b + \frac{1}{864}c^6 - \frac{1}{144}c^5 + \frac{5}{288}c^4 \\
&\quad - \frac{5}{216}c^3 + \frac{5}{288}c^2 - \frac{1}{144}c + \frac{1}{864} \\
u^2 r &= -\frac{1}{3}b + \frac{1}{12}c^2 - \frac{1}{6}c + \frac{1}{12} \\
u^3 s &= -\frac{b}{2}.
\end{aligned}
$$

## 2.3  Parametrizing Quartics

Now that we know how to convert from Tate normal form to short Weierstrass form, we can use Kubert's parametrizations in order to write down all monic, square-free, centered, rational quartic polynomials for which (2.1) has a non-constant solu-

tion. We do this by writing down conditions on the coefficients of a curve in Tate normal form for the point $(0, 0)$ to have a given torsion order. Then we can combine the formulas from Proposition II.7 and Lemma II.1 in order to write down the corresponding quartics.

We begin by recording Kubert's parametrizations [13]. For $b, c \in \mathbb{Q}$ let $E(b, c)$ denote the elliptic curve

$$y^2 + (1 - c)xy - by = x^3 - bx^2.$$

The discriminant of this curve is given by

$$(2.2) \qquad \Delta(b, c) = b^3(16b^2 - 8bc^2 - 20bc + b + c^4 - 3c^3 + 3c^2 - c).$$

In the list below $n$ corresponds to the order of $(0, 0)$. All of the parametrizations are valid so long as $\Delta(b, c) \neq 0$. Each parametrization will be in terms of one variable $t$.

| $n$ | $b$ | $c$ |
|---|---|---|
| 4 | $t$ | $0$ |
| 5 | $t$ | $t$ |
| 6 | $t(t + 1)$ | $t$ |
| 7 | $t^2(t - 1)$ | $t(t - 1)$ |
| 8 | $(2t - 1)(t - 1)$ | $\frac{(2t-1)(t-1)}{t}$ |
| 9 | $t^2(t - 1)(t^2 - t + 1)$ | $t^2(t - 1)$ |
| 10 | $\frac{t^3(t-1)(2t-1)}{(t^2-3t+1)^2}$ | $\frac{-t(t-1)(2t-1)}{t^2-3t+1}$ |
| 12 | $\frac{t(2t-1)(3t^2-3t+1)(2t^2-2t+1)}{(t-1)^4}$ | $\frac{-t(2t-1)(3t^2-3t+1)}{(t-1)^2}$ |

We are now ready to give our parametrizations. Write

$$d(x) = x^4 + r_2 x^2 + r_1 x + r_0.$$

The formulas below will parametrize $r_2, r_1, r_0$ in terms of two rational parameters $a$ and $b$. They are valid so long as the resulting quartic is square-free, which is equivalent to the condition of the discriminant (2.2) being non-zero. The parametrizations are organized by the corresponding order of the torsion point on the Jacobian.

**Theorem II.8.** *The following list gives a complete parametrization of all monic, centered, square-free, quartic polynomials*

$$d(x) = x^4 + r_2 x^2 + r_1 x + r_0 \in \mathbb{Q}[x]$$

*for which the equation*

$$f(x)^2 - d(x)g(x)^2 = 1$$

*has a non-trivial solution $f(x), g(x) \in \mathbb{Q}[x]$. The formulas below are valid for any $a, b \in \mathbb{Q}$ provided $r_2, r_1, r_0$ are defined and $d(x)$ is square-free. The square-free condition can be checked by ensuring the discriminant of $d(x)$ is nonzero. This discriminant is given by*

$$\Delta(r_2, r_1, r_0) = 16 r_2^4 r_0 - 4 r_2^3 r_1^2 - 128 r_2^2 r_0^2 + 144 r_2 r_1^2 r_0 - 27 r_1^4 + 256 r_0^3.$$

Order 4:

$r_2 = (8a - 2)/b^2$

$r_1 = 32a/b^3$

$r_0 = (16a^2 + 24a + 1)/b^4$

where $b \neq 0$ and $a \neq 0, -\dfrac{1}{16}$.

Order 5:

$$r_2 = (-2a^2 + 12a - 2)/b^2$$

$$r_1 = 32a/b^3$$

$$r_0 = (a^4 - 12a^3 + 6a^2 + 20a + 1)/b^4$$

where $b \neq 0$ and $a \neq 0$.

Order 6:

$$r_2 = (6a^2 + 12a - 2)/b^2$$

$$r_1 = (32a^2 + 32a)/b^3$$

$$r_0 = (9a^4 + 4a^3 + 30a^2 + 20a + 1)/b^4$$

where $b \neq 0$ and $a \neq 0, -1, -\dfrac{1}{9}$.

Order 7:

$$r_2 = (-2a^4 + 12a^3 - 6a^2 - 4a - 2)/b^2$$

$$r_1 = (32a^3 - 32a^2)/b^3$$

$$r_0 = (a^8 - 12a^7 + 42a^6 - 64a^5 + 51a^4 - 22a^2 + 4a + 1)/b^4$$

where $b \neq 0$ and $a \neq 0, 1$.

Order 8:

$$r_2 = (8a^4 + 8a^3 - 32a^2 + 16a - 2)/(a^2 b^2)$$

$$r_1 = (64a^2 - 96a + 32)/b^3$$

$$r_0 = (16a^8 - 96a^7 + 336a^6 - 576a^5 + 536a^4 - 296a^3 + 96a^2 - 16a + 1)/(a^4 b^4)$$

where $b \neq 0$ and $a \neq 0, 1, \dfrac{1}{2}$.

Order 9:

$$r_2 = (-2a^6 + 12a^5 - 18a^4 + 20a^3 - 12a^2 - 2)/b^2$$

$$r_1 = (32a^5 - 64a^4 + 64a^3 - 32a^2)/b^3$$

$$r_0 = (a^{12} - 12a^{11} + 54a^{10} - 128a^9 + 181a^8 - 156a^7 + 82a^6 - 4a^5 - 42a^4 + 44a^3$$
$$- 20a^2 + 1)/b^4$$

where $b \neq 0$ and $a \neq 0, 1$.

Order 10:

$$r_2 = (-8a^6 + 32a^5 - 16a^4 - 16a^3 + 8a - 2)/(a^4b^2 - 6a^3b^2 + 11a^2b^2 - 6ab^2 + b^2)$$

$$r_1 = (64a^5 - 96a^4 + 32a^3)/(a^4b^3 - 6a^3b^3 + 11a^2b^3 - 6ab^3 + b^3)$$

$$r_0 = (16a^{12} - 128a^{11} + 448a^{10} - 896a^9 + 1024a^8 - 416a^7 - 408a^6 + 608a^5 - 304a^4$$
$$+ 48a^3 + 16a^2 - 8a + 1)/(a^8b^4 - 12a^7b^4 + 58a^6b^4 - 144a^5b^4 + 195a^4b^4$$
$$- 144a^3b^4 + 58a^2b^4 - 12ab^4 + b^4)$$

where $b \neq 0$ and $a \neq 0, 1, \dfrac{1}{2}$.

Order 12:

$$r_2 = (24a^8 - 240a^7 + 672a^6 - 936a^5 + 744a^4 - 336a^3 + 72a^2 - 2)/(a^6b^2 - 6a^5b^2$$
$$+ 15a^4b^2 - 20a^3b^2 + 15a^2b^2 - 6ab^2 + b^2)$$

$$r_1 = (384a^6 - 960a^5 + 1088a^4 - 672a^3 + 224a^2 - 32a)/(a^4b^3 - 4a^3b^3 + 6a^2b^3$$
$$- 4ab^3 + b^3)$$

$$r_0 = (144a^{16} - 576a^{15} + 2112a^{14} - 9696a^{13} + 34016a^{12} - 82176a^{11} + 141936a^{10}$$
$$- 181984a^9 + 177240a^8 - 132528a^7 + 76096a^6 - 33208a^5 + 10760a^4 - 2480a^3$$
$$+ 376a^2 - 32a + 1)/(a^{12}b^4 - 12a^{11}b^4 + 66a^{10}b^4 - 220a^9b^4 + 495a^8b^4 - 792a^7b^4$$
$$+ 924a^6b^4 - 792a^5b^4 + 495a^4b^4 - 220a^3b^4 + 66a^2b^4 - 12ab^4 + b^4)$$

where $b \neq 0$ and $a \neq 0, 1, \dfrac{1}{2}$.

*Remark* II.9. The parameters $a$ and $b$ have been rescaled by rational numbers in order to make the formulas above more presentable.

## 2.4 Continued Fractions

As a consequence of equation (2.1) having a non-constant solution, the continued fraction of $\sqrt{d(x)}$ is periodic. Thus we can use the formulas developed in Section 2.3 in order to write down the corresponding continued fractions. To do so, we employ an algorithm of Berry [3] in order to compute the partial quotients in the continued fraction.

Let $K$ be a field of characteristic not 2, and let $d(x) \in K[x]$ be a monic, square-free, even degree polynomial. Let $B(x) \in K[x]$ be the unique monic polynomial for which the degree of $d - B^2$ is positive and minimal. If

$$\sqrt{d(x)} = [a_0(x); a_1(x), a_2(x), a_3(x), a_4(x), \ldots]$$

is the continued fraction for $\sqrt{d(x)}$ then the partial quotients $a_i(x) \in K[x]$ are computed by the following algorithm.

---
**Algorithm 1** Calculate The Continued Fraction of $\sqrt{d(x)}$
---

$L_0 \Leftarrow 0$
$M_0 \Leftarrow 1$
**for** $i \geq 0$ **do**
    $r_i \Leftarrow L_i + B \mod M_i$
    $a_i \Leftarrow (L_i + B - r_i)/M_i$
    $L_{i+1} \Leftarrow B - r_i$
    **if** $i = 1$ **then**
        $M_1 \Leftarrow d - L_1^2$
    **else**
        $M_{i+1} \Leftarrow M_{i-1} + a_i(r_i - r_{i-1})$
    **end if**
**end for**

---

We can use Algorithm 1 to compute the continued fractions of $\sqrt{d(x)}$ corresponding to the parametrizations given in Theorem II.8. We already know that if the torsion

order is $m$ then the period is at most $2(m-1)$ so we only need to run our algorithm for at most $2(m-1)$ steps.

**Theorem II.10.** *The complementary list of continued fractions of $\sqrt{d(x)}$ to the formulas of Theorem II.8 is given below.*

Order 4:

$$\sqrt{d(x)} = [a_0; \overline{a_1, a_2, a_3, a_2, a_1, 2a_0}]$$

where

$$a_0 = x^2 + (4a - 1)/b^2$$

$$16a_1 = (b^3/a) \cdot x - b^2/a$$

$$a_2 = (4/b) \cdot x - 4/b^2$$

$$32a_3 = (b^4/a) \cdot x^2 + (4ab^2 - b^2)/a$$

Order 5:

$$\sqrt{d(x)} = [a_0; \overline{a_1, a_2, a_1, 2a_0}]$$

where

$$a_0 = x^2 + (-a^2 + 6a - 1)/b^2$$

$$16a_1 = (b^3/a) \cdot x + (ab^2 - b^2)/a$$

$$a_2 = (4/b) \cdot x + (-4a - 4)/b^2$$

Order 6:

$$\sqrt{d(x)} = [a_0; \overline{a_1, a_2, a_3, a_4, a_5, a_4, a_3, a_2, a_1, 2a_0}]$$

where

$$a_0 = x^2 + (3a^2 + 6a - 1)/b^2$$

$$16a_1 = (b^3/(a^2 + a)) \cdot x + (ab^2 - b^2)/(a^2 + a)$$

$$a_2 = (4/b) \cdot x + (-4a - 4)/b^2$$

$$16a_3 = (b^3/a) \cdot x + (-ab^2 - b^2)/a$$

$$a_4 = (4/(ab + b)) \cdot x + (4a - 4)/(ab^2 + b^2)$$

$$32a_5 = (b^4/a) \cdot x^2 + (3a^2b^2 + 6ab^2 - b^2)/a$$

Order 7:

$$\sqrt{d(x)} = [a_0; \overline{a_1, a_2, a_3, a_2, a_1, 2a_0}]$$

where

$$a_0 = x^2 + (-a^4 + 6a^3 - 3a^2 - 2a - 1)/b^2$$

$$16a_1 = (b^3/(a^3 - a^2)) \cdot x + (a^2b^2 - ab^2 - b^2)/(a^3 - a^2)$$

$$a_2 = (4/b) \cdot x + (-4a^2 + 4a - 4)/b^2$$

$$16a_3 = (b^3/(a^2 - a)) \cdot x + (a^2b^2 - 3ab^2 + b^2)/(a^2 - a)$$

Order 8:

$$\sqrt{d(x)} = [a_0; \overline{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_6, a_5, a_4, a_3, a_2, a_1, 2a_0}]$$

where

$$a_0 = x^2 + (4a^4 + 4a^3 - 16a^2 + 8a - 1)/(a^2b^2)$$

$$32a_1 = (b^3/(a^2 - (3/2)a + 1/2)) \cdot x + (2a^2b^2 - 4ab^2 + b^2)/(a^3 - (3/2)a^2 + (1/2)a)$$

$$a_2 = (4/b) \cdot x + (-8a^2 + 8a - 4)/(ab^2)$$

$$32a_3 = (ab^3/(a^2 - (3/2)a + 1/2)) \cdot x - 2b^2/(a - 1)$$

$$a_4 = ((8a - 4)/(a^2b)) \cdot x + (-16a^2 + 16a - 4)/(a^3b^2)$$

$$64a_5 = (a^3b^3/(a^3 - 2a^2 + (5/4)a - 1/4) \cdot x + (-2a^4b^2 + 2a^3b^2 - a^2b^2)/(a^3 - 2a^2$$
$$+ (5/4)a - 1/4)$$

$$a_6 = ((8a - 4)/(a^3b)) \cdot x + (16a^3 - 40a^2 + 24a - 4)/(a^4b^2)$$

$$128a_7 = (a^3b^4/(a^3 - 2a^2 + (5/4)a - 1/4)) \cdot x^2 + (4a^5b^2 + 4a^4b^2 - 16a^3b^2 + 8a^2b^2$$
$$- ab^2)/(a^3 - 2a^2 + (5/4)a - 1/4)$$

Order 9:

$$\sqrt{d(x)} = [a_0; \overline{a_1, a_2, a_3, a_4, a_3, a_2, a_1, 2a_0}]$$

where

$$a_0 = x^2 + (-a^6 + 6a^5 - 9a^4 + 10a^3 - 6a^2 - 1)/b^2$$

$$16a_1 = (b^3/(a^5 - 2a^4 + 2a^3 - a^2)) \cdot x + (a^3b^2 - a^2b^2 - b^2)/(a^5 - 2a^4 + 2a^3 - a^2)$$

$$a_2 = (4/b) \cdot x + (-4a^3 + 4a^2 - 4)/b^2$$

$$16a_3 = (b^3/(a^3 - a^2)) \cdot x + (a^3b^2 - 3a^2b^2 + 2ab^2 - b^2)/(a^3 - a^2)$$

$$a_4 = (4a/(a^2b - ab + b)) \cdot x + (-4a^4 + 12a^3 - 16a^2 + 4a)/(a^2b^2 - ab^2 + b^2)$$

Order 10:

$$\sqrt{d(x)} = [a_0; \overline{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_8, a_7, a_6, a_5, a_4, a_3, a_2, a_1, 2a_0}]$$

where

$$a_0 = x^2 + (-4a^6 + 16a^5 - 8a^4 - 8a^3 + 4a - 1)/(a^4b^2 - 6a^3b^2 + 11a^2b^2 - 6ab^2 + b^2)$$

$$32a_1 = ((a^4b^3 - 6a^3b^3 + 11a^2b^3 - 6ab^3 + b^3)/(a^5 - (3/2)a^4 + (1/2)a^3) \cdot x + (-2a^5b^2 + 8a^4b^2 - 6a^3b^2 - 5a^2b^2 + 5ab^2 - 1b^2)/(a^5 - (3/2)a^4 + (1/2)a^3)$$

$$a_2 = (4/b) \cdot x + (8a^3 - 16a^2 + 16a - 4)/(a^2b^2 - 3ab^2 + b^2)$$

$$32a_3 = ((-a^2b^3 + 3ab^3 - 1b^3)/(a^3 - (3/2)a^2 + (1/2)a)) \cdot x + (2a^3b^2 - 6a^2b^2 + 4ab^2 - b^2)/(a^3 - (3/2)a^2 + (1/2)a)$$

$$a_4 = ((-4a^2 + 12a - 4)/(ab)) \cdot x + (-8a + 4)/(ab^2)$$

$$16a_5 = (b^3/(a^3 - a^2)) \cdot x + (2ab^2 - b^2)/(a^5 - 4a^4 + 4a^3 - a^2)$$

$$a_6 = ((2a^4 - 12a^3 + 22a^2 - 12a + 2)/(ab - (1/2)b)) \cdot x + (-4a^5 + 24a^4 - 48a^3 + 38a^2 - 14a + 2)/(ab^2 - (1/2)b^2)$$

$$16a_7 = (-b^3/(a^4 - 4a^3 + 4a^2 - a)) \cdot x + (-2a^3b^2 + 4a^2b^2 - 4ab^2 + b^2)/(a^6 - 7a^5 + 17a^4 - 17a^3 + 7a^2 - a)$$

$$a_8 = ((-2a^6 + 18a^5 - 60a^4 + 90a^3 - 60a^2 + 18a - 2)/(a^3b - (1/2)a^2b) \cdot x + (4a^7 - 28a^6 + 64a^5 - 42a^4 - 28a^3 + 42a^2 - 16a + 2)/(a^3b^2 - (1/2)a^2b^2)$$

$$32a_9 = (-b^4/(a^4 - 4a^3 + 4a^2 - a)) \cdot x^2 + (4a^6b^2 - 16a^5b^2 + 8a^4b^2 + 8a^3b^2 - 4ab^2 + b^2)/(a^8 - 10a^7 + 39a^6 - 75a^5 + 75a^4 - 39a^3 + 10a^2 - a)$$

Order 12:

$$\sqrt{d(x)} = [a_0; \overline{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{10}, a_9, a_8, a_7, a_6, a_5, a_4, a_3, a_2, a_1, 2a_0}]$$

where

$$a_0 = x^2 + (12a^8 - 120a^7 + 336a^6 - 468a^5 + 372a^4 - 168a^3 + 36a^2 - 1)/(a^6 b^2$$

$$- 6a^5 b^2 + 15a^4 b^2 - 20a^3 b^2 + 15a^2 b^2 - 6ab^2 + b^2)$$

$$192a_1 = ((a^4 b^3 - 4a^3 b^3 + 6a^2 b^3 - 4ab^3 + b^3)/(a^6 - (5/2)a^5 + (17/6)a^4 - (7/4)a^3$$

$$+ (7/12)a^2 - (1/12)a)) \cdot x + (-6a^5 b^2 + 14a^4 b^2 - 10a^3 b^2 + 3ab^2 - b^2)/(a^6$$

$$- (5/2)a^5 + (17/6)a^4 - (7/4)a^3 + (7/12)a^2 - (1/12)a)$$

$$a_2 = (4/b) \cdot x + (24a^4 - 40a^3 + 32a^2 - 16a + 4)/(a^3 b^2 - 3a^2 b^2 + 3ab^2 - b^2)$$

$$96a_3 = ((-a^3 b^3 + 3a^2 b^3 - 3ab^3 + b^3)/(a^4 - (3/2)a^3 + (5/6)a^2 - (1/6)a)) \cdot x$$

$$+ (2a^4 b^2 + 2a^3 b^2 - 6a^2 b^2 + 4ab^2 - b^2)/(a^4 - (3/2)a^3 + (5/6)a^2 - (1/6)a)$$

$$a_4 = ((-6a^2 + 6a - 2)/(a^3 b - 2a^2 b + (3/2)ab - (1/2)b)) \cdot x + (-12a^6 + 36a^5$$

$$- 64a^4 + 68a^3 - 42a^2 + 14a - 2)/(a^6 b^2 - 5a^5 b^2 + (21/2)a^4 b^2 - 12a^3 b^2$$

$$+ 8a^2 b^2 - 3ab^2 + (1/2)b^2)$$

$$288a_5 = ((a^6 b^3 - 6a^5 b^3 + 15a^4 b^3 - 20a^3 b^3 + 15a^2 b^3 - 6ab^3 + b^3)/(a^6 - (5/2)a^5$$

$$+ (8/3)a^4 - (3/2)a^3 + (4/9)a^2 - (1/18)a)) \cdot x + (-4a^5 b^2 + 16a^4 b^2 - 26a^3 b^2$$

$$+ 22a^2 b^2 - 10ab^2 + 2b^2)/(a^5 - 2a^4 + (5/3)a^3 - (2/3)a^2 + (1/9)a)$$

$$a_6 = ((24a^3 - 36a^2 + 20a - 4)/(a^5b - 5a^4b + 10a^3b - 10a^2b + 5ab - b)) \cdot x$$

$$+ (-96a^6 + 288a^5 - 392a^4 + 304a^3 - 140a^2 + 36a - 4)/(a^8b^2 - 8a^7b^2$$

$$+ 28a^6b^2 - 56a^5b^2 + 70a^4b^2 - 56a^3b^2 + 28a^2b^2 - 8ab^2 + b^2)$$

$$1152a_7 = ((-a^{10}b^3 + 10a^9b^3 - 45a^8b^3 + 120a^7b^3 - 210a^6b^3 + 252a^5b^3 - 210a^4b^3$$

$$+ 120a^3b^3 - 45a^2b^3 + 10ab^3 - b^3)/(a^9 - 4a^8 + (89/12)a^7 - (33/4)a^6$$

$$+ (431/72)a^5 - (26/9)a^4 + (65/72)a^3 - (1/6)a^2 + (1/72)a)) \cdot x + (-2a^{11}b^2$$

$$+ 18a^{10}b^2 - 76a^9b^2 + 200a^8b^2 - 365a^7b^2 + 483a^6b^2 - 469a^5b^2 + 331a^4b^2$$

$$- 165a^3b^2 + 55a^2b^2 - 11ab^2 + b^2)/(a^9 - 4a^8 + (89/12)a^7 - (33/4)a^6$$

$$+ (431/72)a^5 - (26/9)a^4 + (65/72)a^3 - (1/6)a^2 + (1/72)a)$$

$$a_8 = ((-72a^5 + 180a^4 - 192a^3 + 108a^2 - 32a + 4)/(a^8b - 8a^7b + 28a^6b - 56a^5b$$

$$+ 70a^4b - 56a^3b + 28a^2b - 8ab + b)) \cdot x + (144a^9 - 216a^8 - 408a^7 + 1536a^6$$

$$- 2096a^5 + 1652a^4 - 824a^3 + 260a^2 - 48a + 4)/(a^{11}b^2 - 11a^{10}b^2 + 55a^9b^2$$

$$- 165a^8b^2 + 330a^7b^2 - 462a^6b^2 + 462a^5b^2 - 330a^4b^2 + 165a^3b^2 - 55a^2b^2$$

$$+ 11ab^2 - b^2)$$

$$1728a_9 = ((a^{11}b^3 - 11a^{10}b^3 + 55a^9b^3 - 165a^8b^3 + 330a^7b^3 - 462a^6b^3 + 462a^5b^3$$

$$- 330a^4b^3 + 165a^3b^3 - 55a^2b^3 + 11ab^3 - b^3)/(a^9 - 4a^8 + (29/4)a^7$$

$$- (31/4)a^6 + (16/3)a^5 - (29/12)a^4 + (19/27)a^3 - (13/108)a^2$$

$$+ (1/108)a)) \cdot x + (6a^{12}b^2 - 58a^{11}b^2 + 256a^{10}b^2 - 684a^9b^2 + 1237a^8b^2$$

$$- 1604a^7b^2 + 1540a^6b^2 - 1112a^5b^2 + 604a^4b^2 - 242a^3b^2 + 68a^2b^2 - 12ab^2$$

$$+ b^2)/(a^9 - 4a^8 + (29/4)a^7 - (31/4)a^6 + (16/3)a^5 - (29/12)a^4 + (19/27)a^3$$

$$- (13/108)a^2 + (1/108)a)$$

$$a_{10} = ((36a^5 - 90a^4 + 96a^3 - 54a^2 + 16a - 2)/(a^9 b - 8a^8 b + (57/2)a^7 b$$

$$- (119/2)a^6 b + (161/2)a^5 b - (147/2)a^4 b + (91/2)a^3 b - (37/2)a^2 b$$

$$+ (9/2)ab - (1/2)b)) \cdot x + (-216a^9 + 828a^8 - 1368a^7 + 1200a^6 - 504a^5$$

$$- 34a^4 + 156a^3 - 82a^2 + 20a - 2)/(a^{12}b^2 - 11a^{11}b^2 + (111/2)a^{10}b^2$$

$$- 170a^9 b^2 + (705/2)a^8 b^2 - 522a^7 b^2 + 567a^6 b^2 - 456a^5 b^2 + 270a^4 b^2$$

$$- 115a^3 b^2 + (67/2)a^2 b^2 - 6ab^2 + (1/2)b^2)$$

$$3456a_{11} = ((a^{11}b^4 - 11a^{10}b^4 + 55a^9 b^4 - 165a^8 b^4 + 330a^7 b^4 - 462a^6 b^4 + 462a^5 b^4$$

$$- 330a^4 b^4 + 165a^3 b^4 - 55a^2 b^4 + 11ab^4 - b^4)/(a^9 - 4a^8 + (29/4)a^7$$

$$- (31/4)a^6 + (16/3)a^5 - (29/12)a^4 + (19/27)a^3 - (13/108)a^2$$

$$+ (1/108)a)) \cdot x^2 + (12a^{13}b^2 - 180a^{12}b^2 + 1056a^{11}b^2 - 3468a^{10}b^2$$

$$+ 7332a^9 b^2 - 10680a^8 b^2 + 11076a^7 b^2 - 8256a^6 b^2 + 4367a^5 b^2 - 1567a^4 b^2$$

$$+ 338a^3 b^2 - 26a^2 b^2 - 5ab^2 + b^2)/(a^9 - 4a^8 + (29/4)a^7 - (31/4)a^6$$

$$+ (16/3)a^5 - (29/12)a^4 + (19/27)a^3 - (13/108)a^2 + (1/108)a).$$

# CHAPTER III

# Periods

## 3.1 Synopsis

Now that we have explicit formulas for monic, centered, quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which (2.1) has a solution, we can begin to use them. In this chapter we will analyze the integers which occur as the period of the continued fraction of $\sqrt{d(x)}$.

Recall that Mazur's theorem [15] implies that a rational torsion point on an elliptic curve defined over $\mathbb{Q}$ can only have order among $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$. Thus Theorem I.16 yields that if the continued fraction of $\sqrt{d(x)}$ is period then its period is one of

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 18, 22\}.$$

One of the deficiencies of Theorem I.16 is that if $d(x)$ corresponds to a point on the Jacobian of $y^2 = d(x)$ of order $n$, where $n$ is even, then there is no nice criterion for determining whether the period of the continued fraction of $\sqrt{d(x)}$ is $n-1$ or $2(n-1)$. In fact, the next proposition shows that the period of the continued fraction is not an isomorphism invariant of the pair $(E, p)$ where $E$ is the Jacobian of $y^2 = d(x)$ and $p$ is the corresponding point of interest.

**Proposition III.1.** *There exist monic, quartic, square-free polynomials $d_1(x)$ and $d_2(x)$ in $\mathbb{Q}[x]$ with corresponding isomorphic pairs $(E_1, p_1)$ and $(E_2, p_2)$ such that the periods of the continued fractions of $\sqrt{d_1(x)}$ and $\sqrt{d_2(x)}$ are different.*

*Proof.* Let

$$d_1(x) = x^4 - \frac{1295}{72}x^2 + \frac{1}{6}x + \frac{1687393}{20736}$$

and

$$d_2(x) = x^4 - \frac{1295}{648}x^2 + \frac{1}{162}x + \frac{1687393}{1679616}.$$

For $i \in \{1, 2\}$, Lemma II.1 gives that $d_i(x)$ corresponds to the pair $(E_i, p_i)$ where $E_1$ is the elliptic curve

$$y^2 = x^3 - \frac{1684801}{62208}x + \frac{2186869751}{40310784}$$

and $p_1$ is the point

$$\left( \frac{1295}{432}, -\frac{1}{48} \right),$$

and $E_2$ is the curve

$$y^2 = x^3 - \frac{1684801}{5038848}x + \frac{2186869751}{29386561536}$$

and $p_2$ is the point

$$\left( \frac{1295}{3888}, -\frac{1}{1296} \right).$$

The map $\phi : E_1 \to E_2$ given by

$$(x, y) \mapsto \left( \frac{1}{9}x, \frac{1}{27}y \right)$$

is an isomorphism with $\phi(p_1) = p_2$. On the other hand, applying Algorithm 1 shows that the continued fraction of $\sqrt{d_1(x)}$ is

$$[a_0; \overline{a_1, a_1, 2a_0}]$$

with

$$a_0 = x^2 - \frac{1295}{144}$$

$$a_1 = 12x - 36$$

whereas the continued fraction of $\sqrt{d_2(x)}$ is

$$[b_0; \overline{b_1, b_2, b_3, b_2, b_1, 2b_0}]$$

with

$$b_0 = x^2 - \frac{1295}{1296}$$

$$b_1 = 324x - 324$$

$$b_2 = 4x - 4$$

$$b_3 = 162x^2 - \frac{1295}{8}.$$

In particular, the continued fractions of $\sqrt{d_1(x)}$ and $\sqrt{d_2(x)}$ have different periods despite their corresponding Jacobians being isomorphic. □

In view of Proposition III.1, we must take care when trying to prove properties of the periods showing up in the expansions of continued fractions. It is worth remarking that in the formulas from Section 2.3 and Section 2.4, the parameter $a$ determines the isomorphism class of the Jacobian, while the parameter $b$ determines the embedding in $\mathbb{P}^2$. Because the period is not determined by the isomorphism class alone, we must take into account both parameters when proving theorems about periods.

One major open problem in the area of quartic $d(x) \in \mathbb{Q}[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic is an understanding of which odd periods can actually occur. In [23], Schinzel asks whether periods 5, 7, 9 or 11 actually occur for any such $d(x)$. Several authors have worked on this problem since. In [14], Malyshev proves

that there are no monic $d(x)$ for which the period is 7. In [28], van der Poorten and Tran find examples of periods 1, 3 and 5, and also construct an example of a non-monic polynomial $d(x)$ for which the period is 7. Through parametrizations similar to those found in Chapter II, van der Poorten and Tran also claim to prove that periods 9 and 11 never occur. Unfortunately, in light of Proposition III.1, their methods don't solve the problem since they fail to take into account the embedding of the corresponding elliptic curve.

In this chapter, we will completely solve the problem of understanding which odd periods occur. Using the parametrizations found in Chapter II, we will first write down complete parametrizations of all quartic, square-free, polynomials $d(x) \in \mathbb{Q}[x]$ for which the period of $\sqrt{d(x)}$ is 3, 5 or 7. We will then furnish correct proofs that periods 9 and 11 never occur.

The strategies of these proofs are as follows. Suppose we want to write down all $d(x)$ for which the continued fraction of $\sqrt{d(x)}$ has odd period $r$, where $r > 1$. First, we note that it suffices to assume without loss of generality that $d(x)$ is centered. This is because of the following observation. If $f(x) \in K((x^{-1}))$ is a Laurent series with continued fraction expansion

$$f(x) = [a_0(x); a_1(x), a_2(x), \ldots]$$

where $a_i(x) \in K[x]$, then for any $c \in K^\times$ for which $f(x + c)$ is well-defined, we have

$$f(x + c) = [a_0(x + c); a_1(x + c), a_2(x + c), \ldots].$$

Thus the continued fraction of $f(x)$ is periodic if and only if the continued fraction of $f(x + c)$ is periodic, and moreover the two periods must be the same.

Next, write our centered, square-free, quartic polynomial $d(x)$ as $\alpha^2 \widetilde{d}(x)$ where

$\alpha \in K^{\times}$ and $\widetilde{d}(x)$ is monic. If the continued fraction of $\sqrt{\widetilde{d}(x)}$ is

$$\sqrt{\widetilde{d}(x)} = [a_0(x); a_1(x), a_2(x), \ldots],$$

then a formula of Schmidt [24] says that

(3.1) $$\alpha\sqrt{\widetilde{d}(x)} = [\alpha a_0(x); \alpha^{-1} a_1(x), \alpha a_2(x), \ldots].$$

By Theorem I.16 we know that $\widetilde{d}(x)$ corresponds to a pair $(E, p)$ where $p \in E(\mathbb{Q})$ is a torsion point of order $r + 1$. Thus the continued fraction of $\sqrt{\widetilde{d}(x)}$ is of the form

$$\sqrt{\widetilde{d}(x)} = [a_0(x); \overline{a_1(x), \ldots, a_{r-1}(x), a_r(x), a_{r-1}(x), \ldots, a_1(x), 2a_0(x)}].$$

Notice that $r$ is the quasi-period of this continued fraction and from the formulas of Chapter II we notice that $a_r(x)$ is a constant multiple of $a_0(x)$. Coupling this fact with (3.1), we see that $\sqrt{d(x)}$ will have period $r$ precisely when

$$\alpha^{-1} a_r(x) = 2\alpha a_0(x)$$

or

$$\frac{a_r(x)}{a_0(x)} = 2\alpha^2.$$

This will allow us to write down all $d(x)$ corresponding to a given odd period. We summarize all of this in the following proposition.

**Proposition III.2.** *Let* $d(x) = c^2 \widetilde{d}(x)$ *where* $\widetilde{d}(x) \in \mathbb{Q}[x]$ *is a monic, centered, quartic and square-free polynomial. If the continued fraction of* $\sqrt{\widetilde{d}(x)}$ *is of the form*

$$\sqrt{\widetilde{d}(x)} = [a_0(x); \overline{a_1(x), \ldots, a_{r-1}(x), a_r(x), a_{r-1}(x), \ldots, a_1(x), 2a_0(x)}],$$

*with* $r > 1$ *odd, then the continued fraction of* $\sqrt{d(x)}$ *will have period* $r$ *precisely when*

$$\frac{a_r(x)}{a_0(x)} = 2c^2.$$

## 3.2 Period 3

From the formulas found in Theorem II.10, we have that if $\widetilde{d}(x) \in \mathbb{Q}[x]$ is monic, centered, square-free and quartic, and corresponds to a torsion point of order 4, then

$$(3.2) \qquad \frac{a_3(x)}{a_0(x)} = \frac{b^4}{32a}.$$

Thus finding all centered, quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which $\sqrt{d(x)}$ has period 3, by Proposition III.2, amounts to solving in $\mathbb{Q}$, with $b$ and $c$ non-zero, the equation

$$(3.3) \qquad b^4 = 64ac^2.$$

Obviously, (3.3) has as solutions the triples

$$\left( \frac{b^4}{64c^2}, b, c \right)$$

where $b, c \in \mathbb{Q}^\times$ are arbitrary.

Plugging this into the formula from Theorem II.8 gives the following result.

**Proposition III.3.** *The square-free, quartic polynomial*

$$d(x) = c^2 x^4 + r_2 x^2 + r_1 x + r_0 \in \mathbb{Q}[x]$$

*has the property that the continued fraction of $\sqrt{d(x)}$ has period 3 if and only if there exists $b \in \mathbb{Q}$ such that*

$$
\begin{aligned}
8r_2 &= \frac{b^4 - 16c^2}{b^2} \\
2r_1 &= b \\
256r_0 &= \frac{b^8 + 96b^4 c^2 + 256 c^4}{b^4 c^2}.
\end{aligned}
$$

*where $b \neq 0$, $c \neq 0$ and $b^4 \neq -4c^2$.*

## 3.3 Period 5

From the formulas found in Theorem II.10, we have that if $\widetilde{d}(x) \in \mathbb{Q}[x]$ is monic, centered, square-free and quartic, and corresponds to a torsion point of order 6, then

$$(3.4) \qquad \frac{a_5(x)}{a_0(x)} = \frac{b^4}{32a}.$$

Thus finding all centered, quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which $\sqrt{d(x)}$ has period 5, by Proposition III.2, amounts to solving in $\mathbb{Q}$, with $b$ and $c$ non-zero, the equation

$$(3.5) \qquad b^4 = 64ac^2.$$

Obviously, (3.5) has as solutions the triples

$$\left( \frac{b^4}{64c^2}, b, c \right)$$

where $b, c \in \mathbb{Q}^\times$ are arbitrary.

Plugging this into the formula from Theorem II.8 gives the following result.

**Proposition III.4.** *The square-free, quartic polynomial*

$$d(x) = c^2 x^4 + r_2 x^2 + r_1 x + r_0 \in \mathbb{Q}[x]$$

*has the property that the continued fraction of $\sqrt{d(x)}$ has period 5 if and only if there exists $b \in \mathbb{Q}$ such that*

$$
\begin{aligned}
2048 r_2 &= \frac{3b^8 + 384 b^4 c^2 - 4096 c^4}{b^2 c^2} \\
128 r_1 &= \frac{b^5 + 64 b c^2}{c^2} \\
2^{24} r_0 &= \frac{9 b^{16} + 256 b^{12} c^2 + 2^{13} \cdot 15 \cdot b^8 c^4 + 2^{20} \cdot 5 \cdot b^4 c^6 + 2^{24} c^8}{b^4 c^8}.
\end{aligned}
$$

*where $b \neq 0$, $c \neq 0$, $b^4 \neq -64c^2$ and $9b^4 \neq -64c^2$.*

## 3.4   Period 7

From the formulas found in Theorem II.10, we have that if $\widetilde{d}(x) \in \mathbb{Q}[x]$ is monic, centered, square-free and quartic, and corresponds to a torsion point of order 8, then

$$(3.6) \qquad \frac{a_7(x)}{a_0(x)} = \frac{1}{128} \cdot \frac{a^3 b^4}{a^3 - 2a^2 + \frac{5a}{4} - \frac{1}{4}}.$$

Thus finding all centered, quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which $\sqrt{d(x)}$ has period 7, by Proposition III.2, amounts to solving in $\mathbb{Q}$, with $b$ and $c$ non-zero, the equation (obtained after factoring)

$$(3.7) \qquad b^4 a^3 = 256 c^2 (a - 1) \left( a - \frac{1}{2} \right)^2.$$

To solve (3.7) we make the substitution

$$(a, b, c) = \left( A, B, \frac{B^2 C A}{16 \left( A - \frac{1}{2} \right)} \right)$$

which is valid since we are not interested in solutions with $a = \frac{1}{2}$. With this change of variables we are reduced to solving the equation

$$(3.8) \qquad B^4 A^2 (A - C^2 (A - 1)) = 0.$$

Because we are looking for solutions with $b$ and $c$ non-zero, we can divide both sides of (3.8) by $B^4 A^2$, and we are left with

$$A = \frac{C^2}{C^2 - 1}.$$

Thus, after simplifying, all solutions to (3.7) are given by

$$\begin{aligned}
a &= \frac{C^2}{C^2 - 1} \\
b &= B \\
c &= \frac{B^2 C^3}{8(C^2 + 1)}
\end{aligned}$$

where $B \neq 0$ and $C \neq 0, \pm 1$. Combining this with the formula from Theorem II.8 gives the following parametrization.

**Proposition III.5.**

$$d(x) = c^2 x^4 + r_2 x^2 + r_1 x + r_0 \in \mathbb{Q}[x]$$

*has the property that the continued fraction of $\sqrt{d(x)}$ has period 7 if and only if there exists $B, C \in \mathbb{Q}$ such that*

$$8c = \frac{B^2 C^3}{C^2 + 1}$$

$$32 r_2 = \frac{-B^2 C^2 (C^8 - 8C^6 - 2C^4 + 4C^2 + 1)}{(C-1)^2 (C+1)^2 (C^2+1)^2}$$

$$2 r_1 = \frac{BC^6}{(C-1)^2 (C+1)^2 (C^2+1)}$$

$$64 r_0 = \frac{C^{16} + 16C^{14} - 4C^{12} - 24C^{10} + 6C^8 + 12C^4 + 8C^2 + 1}{(C-1)^4 (C+1)^4 (C^2+1)^2 C^2}.$$

*where $B \neq 0$ and $C \neq 0, \pm 1$.*

Using our parametrization, we are in a position to give a new proof of Malyshev's theorem, [14]. We can reduce his theorem to a question about rational points on certain elliptic curves.

**Theorem III.6** (Malyshev)**.** *There do not exist monic, quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which the continued fraction of $\sqrt{d(x)}$ has period 7.*

*Proof.* By Proposition III.5, it suffices to prove that there do not exist $B, C \in \mathbb{Q}^\times$, with $C \neq \pm 1$, for which

(3.9) $$\pm 8(C^2 + 1) = C^3 B^2.$$

Changing $C$ to $-C$, if necessary, and making the substitution

$$(B, C) = \left( \frac{y}{x^2}, x \right)$$

leaves us with

$$(3.10) \qquad\qquad y^2 = 8x(x^2 + 1).$$

Equation (3.10) defines an elliptic curve over $\mathbb{Q}$. This is curve *32a1* in Cremona's tables [7]. He computes that the rank of this curve is zero and that its torsion subgroup contains exactly four rational points. Besides the point at infinity, these points are

$$(0,0), (1,\pm 4).$$

Therefore we see that (3.9) contains no rational points with $C \neq 0, \pm 1$ and hence the theorem is complete. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

## 3.5   Period 9

From the formulas found in Theorem II.10, we have that if $\widetilde{d}(x) \in \mathbb{Q}[x]$ is monic, centered, square-free and quartic, and corresponds to a torsion point of order 10, then

$$(3.11) \qquad\qquad \frac{a_9(x)}{a_0(x)} = \frac{-1}{32} \cdot \frac{b^4}{a^4 - 4a^3 + 4a^2 - a}.$$

Thus finding all centered, quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which $\sqrt{d(x)}$ has period 9, by Proposition III.2, amounts to solving in $\mathbb{Q}$, with $b$ and $c$ non-zero, the equation (after factoring)

$$(3.12) \qquad\qquad b^4 = -64(a-1)a(a^2 - 3a + 1)c^2.$$

**Theorem III.7.** *There are no quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which the continued fraction of $\sqrt{d(x)}$ has period 9.*

*Proof.* As noted above, this theorem is equivalent to proving that (3.12) has no rational solutions with $b$ and $c$ non-zero, which means that certainly $a \neq 0, 1$. We

then make the change of variables

$$(a, b, c) = \left( x, z, \frac{yz^2}{8(x-1)x(x^2-3x+1)} \right)$$

to arrive at

(3.13)
$$z^4((x-1)x(x^2-3x+1)+y^2) = 0.$$

Because we want solutions with $b$ non-zero, we may divide both sides of (3.13) by $z^4$ to arrive at

(3.14)
$$y^2 = -(x-1)x(x^2-3x+1).$$

The right hand side of (3.14) is a square-free quartic, and since this curve contains the smooth point $(0,0)$, Equation (3.14) defines an elliptic curve over $\mathbb{Q}$. This is curve *80b2* in Cremona's tables [7]. This curve has rank zero and that its torsion subgroup contains exactly two rational points. These are the obvious points

$$(0,0), (1,0).$$

Thus we see that our original equation, (3.12), has no rational solutions with $b$ and $c$ non-zero, and therefore there do not exist quartic, square-free polynomials over $\mathbb{Q}$ for which the period of the continued fraction of their square root is nine. ☐

## 3.6 Period 11

From the formulas found in Theorem II.10, we have that if $\widetilde{d}(x) \in \mathbb{Q}[x]$ is monic, centered, square-free and quartic, and corresponds to a torsion point of order 12, then (after factoring)

(3.15)
$$\frac{a_{11}(x)}{a_0(x)} = \frac{1}{3456} \cdot \frac{b^4(a-1)^{11}}{a\left(a-\frac{1}{2}\right)^2\left(a^2-a+\frac{1}{3}\right)^3}.$$

Thus finding all centered, quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which $\sqrt{d(x)}$ has period 11, by Proposition III.2, amounts to solving in $\mathbb{Q}$, with $b$ and $c$ non-zero, the equation (after factoring)

$$(3.16) \qquad b^4(a-1)^{11} = 6912c^2a\left(a - \frac{1}{2}\right)^2\left(a^2 - a + \frac{1}{3}\right)^3.$$

**Theorem III.8.** *There are no quartic, square-free polynomials $d(x) \in \mathbb{Q}[x]$ for which the continued fraction of $\sqrt{d(x)}$ has period 11.*

*Proof.* As noted above, this theorem is equivalent to proving that (3.16) has no rational solutions with $b$ and $c$ non-zero, which means that certainly $a \neq 0, 1, \frac{1}{2}$. Making the change of variables

$$(a, b, c) = \left(x, z, \frac{yz^2(x-1)^5}{48x\left(x - \frac{1}{2}\right)\left(x^2 - x + \frac{1}{3}\right)^2}\right)$$

changes (3.16) into

$$(3.17) \qquad z^4(x-1)^{10}(x(x-1)\left(x^2 - x + \frac{1}{3}\right) - 3y^2) = 0.$$

Because we are looking for solutions with $b \neq 0$ and $a \neq 1$ we may divide both sides of (3.17) by $z^4(x-1)^{10}$ to arrive at

$$(3.18) \qquad y^2 = \frac{1}{3}\left(x(x-1)\left(x^2 - x + \frac{1}{3}\right)\right).$$

The right hand side of (3.18) is a square-free quartic, and since this curve contains the smooth point $(0, 0)$, Equation (3.18) defines an elliptic curve over $\mathbb{Q}$. This is curve *48a4* in Cremona's tables [7]. The rank of this elliptic curve is zero and its torsion subgroup contains exactly two rational points. These are the obvious points

$$(0, 0), (1, 0).$$

Thus we see that our original equation, (3.16), has no rational solutions with $b$ and $c$ non-zero, and therefore there do not exist quartic, square-free polynomials over $\mathbb{Q}$ for which the period of the continued fraction of their square root is eleven. $\qquad \square$

# Integral Polynomial Pell Equations

## 4.1 Synopsis

In this chapter we shift our focus to monic, square-free, even degree polynomials $d(x) \in \mathbb{Z}[x]$. A fundamental problem in this area is as follows.

**Problem IV.1.** *Classify all monic, square-free, even degree polynomials $d(x) \in \mathbb{Z}[x]$ for which there exists a non-trivial solution to the Pell equation*

$$(4.1) \qquad\qquad f(x)^2 - d(x)g(x)^2 = 1$$

*with $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$.*

This problem essentially goes back to Euler [8], who produced several identities for the continued fractions of square roots of certain positive integers. Among his formulas is the following example. For any positive integer $n > 1$, we have

$$\sqrt{n^2 + 1} = [n; \overline{2n}].$$

By computing the convergents of this continued fraction, we also obtain the identity

$$(2n^2 + 1)^2 - (n^2 + 1)(2n)^2 = 1$$

which gives a solution to a family of Pell equations. Although Euler didn't think

about continued fractions over any fields other than $\mathbb{R}$, he is essentially just comput-
ing the continued fraction of the polynomial $\sqrt{x^2 + 1}$ in $\mathbb{Q}((x^{-1}))$ which is

$$\sqrt{x^2 + 1} = [x; \overline{2x}].$$

This example naturally leads to studying Problem IV.1, for if we have a polynomial
identity

$$f(x)^2 - d(x)g(x)^2 = 1$$

with $f(x), g(x), d(x)$ in $\mathbb{Z}[x]$ and $g(x)$ non-constant, then by specializing at various
positive integers, we would obtain families of solutions to integral Pell equations.

Since the time of Euler, there has been much study of polynomial identities for the
Pell equation. Included in this history is Nathanson's resolution [20] of Problem IV.1
in the case that $d(x)$ is centered and quadratic. Ramasamy [21], Mollin [18] and
McLaughlin [16] have obtained many families of polynomial Pell identities, with
McLaughlin using his identities to construct the fundamental unit in a variety of real
quadratic number fields. In [22, 23], Schinzel studies the problem of determining
which polynomials will give rise to continued fractions of arbitrary large period by
specializing at various integers.

In this chapter, we will use the formulas of Chapter II to study Problem IV.1
when $d(x)$ is a quartic polynomial. In a series of papers, Webb and Yokota lay the
groundwork for studying this instance of Problem IV.1. In [32], Yokota proves that if
$d(x) \in \mathbb{Z}[x]$ is monic and quartic, then if the continued fraction of $\sqrt{d(x)}$ is periodic
then the period must be either 1 or even. In Section 4.2 we will use our formulas
to reprove this result. In [29, 31], Webb and Yokota completely classify the monic,
quartic $d(x) \in \mathbb{Z}[x]$ for which (4.1) has a non-trivial solution with integer coefficients
and for which the continued fraction of $\sqrt{d(x)}$ has period 1 or 2. Most recently,

Yokota proves in [33] that if $\sqrt{d(x)}$ has period 4 then (4.1) will have no non-trivial solutions with integer coefficients.

Yokota conjectures in [33] that there shouldn't be any non-trivial integral polynomial solutions to (4.1) whenever the period of the continued fraction of $\sqrt{d(x)}$ is larger than 2. In Section 4.3 we will disprove Yokota's conjecture. Moreover, we will prove the following result

**Theorem IV.2.** *Let*

$$d(x) = x^4 + r_3 x^3 + r_2 x^2 + r_1 x + r_0$$

*be a monic, quartic, square-free polynomial in $\mathbb{Z}[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period at least 6. Then the equation*

$$f(x)^2 - d(x)g(x)^2 = 1$$

*has a non-trivial solution with $f(x), g(x)$ in $\mathbb{Z}[x]$ if and only if $(r_3, r_2, r_1, r_0)$ is one of*

$$(4a + 2, 6a^2 + 6a - 7, 4a^3 + 6a^2 - 14a - 12, a^4 + 2a^3 - 7a^2 - 12a + 6)$$

$$(4a + 2, 6a^2 + 6a - 7, 4a^3 + 6a^2 - 14a - 4, a^4 + 2a^3 - 7a^2 - 4a + 10)$$

*where $a \in \mathbb{Z}$ is arbitrary.*

In conjunction with Webb and Yokota's work on periods 1, 2 and 4, Theorem IV.2 completely solves Problem IV.1 for quartic polynomials.

The formulas of Chapter II all assume that the quartic we have is centered. When dealing with quartic polynomials in $\mathbb{Z}[x]$, the substitution required to center the polynomial may introduce denominators to the coefficients. Thus there is a loss of generality in assuming a given quartic is centered. Even so, we make the following

observation about what types of denominators can be introduced in the process of centering.

**Lemma IV.3.** *Let $d(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 \in \mathbb{Z}[x]$. If we write the centered version of $d(x)$ as*

$$d_c(x) = d\left(x - \frac{a_3}{4}\right) = x^4 + b_2 x^2 + b_1 x + b_0$$

*then $8b_2, 8b_1, 256b_0$ are integers.*

## 4.2   Odd Periods

As a warmup to the types of arguments we will use repeatedly throughout this chapter, we first use our explicit parametrizations to recover a theorem of Yokota [32].

**Theorem IV.4** (Yokota). *Let $d(x) \in \mathbb{Z}[x]$ be a quartic, monic, square-free polynomial. If the continued fraction of $\sqrt{d(x)}$ is periodic of period at least $2$ then its period must be even.*

In light of Theorems III.6, III.7 and III.8, we already know that if the continued fraction of $\sqrt{d(x)}$ is periodic with odd period, then its period must be either 3 or 5. Thus we split the proof of Theorem IV.4 into two propositions.

**Proposition IV.5.** *If $d(x) \in \mathbb{Q}[x]$ is a monic, quartic, square-free polynomial for which the continued fraction of $\sqrt{d(x)}$ is periodic of period $3$ then $d(x) \notin \mathbb{Z}[x]$.*

*Proof.* Assume for the sake of contradiction that there exists a monic, quartic, square-free polynomial $d(x) \in \mathbb{Z}[x]$ such that the continued fraction of $\sqrt{d(x)}$ is periodic of period 3. Because $\sqrt{d_c(x)}$ will also have period 3, Proposition III.3 implies that there exists $b \in \mathbb{Q}$ such that

$$d_c(x) = x^4 + \frac{b^4 - 16}{8b^2} x^2 + \frac{b}{2} x + \frac{b^8 + 96b^4 + 256}{256b^4}.$$

In light of Lemma IV.3 we must have

$$\frac{b^4 - 16}{b^2}, 4b, \frac{b^8 + 96b^4 + 256}{b^4} \in \mathbb{Z}.$$

It's then clear that $b \in \mathbb{Z}$ and $b^2 \mid 16$, so $b$ must be among $\{\pm 1, \pm 2, \pm 4\}$. Thus $d_c(x)$ is one of

$$x^4 + \frac{15}{8}x^2 \pm 2x + \frac{353}{256},$$

$$x^4 - \frac{15}{8}x^2 \pm \frac{1}{2}x + \frac{353}{256},$$

$$x^4 \pm x + \frac{1}{2}.$$

Our original polynomial, $d(x)$, equals $d_c\left(x + \frac{a}{4}\right)$ for some $a \in \mathbb{Z}$. Thus $d(x)$ is one of

$$x^4 + ax^3 + \frac{3a^2 + 15}{8} \cdot x^2 + \frac{a^3 + 15a - 32}{16} \cdot x + \frac{a^4 + 30a^2 - 128a + 353}{256},$$

$$x^4 + ax^3 + \frac{3a^2}{8} \cdot x^2 + \frac{a^3 - 16}{16} \cdot x + \frac{a^4 - 64a + 128}{256},$$

$$x^4 + ax^3 + \frac{3a^2 - 15}{8} \cdot x^2 + \frac{a^3 - 15a - 8}{16} \cdot x + \frac{a^4 - 30a^2 - 32a + 353}{256},$$

$$x^4 + ax^3 + \frac{3a^2 - 15}{8} \cdot x^2 + \frac{a^3 - 15a + 8}{16} \cdot x + \frac{a^4 - 30a^2 + 32a + 353}{256},$$

$$x^4 + ax^3 + \frac{3a^2}{8} \cdot x^2 + \frac{a^3 + 16}{16} \cdot x + \frac{a^4 + 64a + 128}{256},$$

$$x^4 + ax^3 + \frac{3a^2 + 15}{8} \cdot x^2 + \frac{a^3 + 15a + 32}{16} \cdot x + \frac{a^4 + 30a^2 + 128a + 353}{256}.$$

It is now a finite, but tedious computation to check that there is no $a \in \mathbb{Z}$ for which any of these polynomials is in $\mathbb{Z}[x]$. Since all the denominators are divisors of 256, one only needs to check $a$ in residue classes modulo 256. This gives our contradiction, and we see that there is no monic $d(x) \in \mathbb{Z}[x]$ for which the period of the continued fraction of $\sqrt{d(x)}$ is 3.

$\square$

**Proposition IV.6.** *If $d(x) \in \mathbb{Q}[x]$ is a monic, quartic, square-free polynomial for which the continued fraction of $\sqrt{d(x)}$ is periodic of period 5 then $d(x) \notin \mathbb{Z}[x]$.*

*Proof.* The proof of non-existence of period 5 follows the same strategy as the proof of Proposition IV.5. We assume for the sake of contradiction that there exists a monic, quartic, square-free polynomial $d(x) \in \mathbb{Z}[x]$ such that the continued fraction of $\sqrt{d(x)}$ is periodic of period 5. The centered square root, $\sqrt{d_c(x)}$, will also have period 5 so Proposition III.4 implies that there exists $b \in \mathbb{Q}$ such that

$$d_c(x) \;=\; x^4 + \frac{3b^8 + 384b^4 - 4096}{2048b^2}x^2 + \frac{b^5 + 64b}{128}x$$
$$+ \frac{9b^{16} + 256b^{12} + 122880b^8 + 5242880b^4 + 16777216}{16777216b^4}.$$

By Lemma IV.3 we know that
$$\frac{b^5 + 64b}{16} \in \mathbb{Z}$$

and from this its easy to see that $b \in \mathbb{Z}$. Furthermore, since

$$\frac{3b^8 + 384b^4 - 4096}{256b^2} \in \mathbb{Z},$$

we can conclude that $b^2 \mid 4096$, but then checking all such $b$ shows that $b$ must be $\pm 4$. Thus we see that $d_c(x)$ must be of the form

$$d_c(x) = x^4 + \frac{71}{8}x^2 \pm 10x + \frac{3121}{256}.$$

There exists an $a \in \mathbb{Z}$ such that $d(x) = d_c\left(x + \frac{a}{4}\right)$, so there two possibilities for $d(x)$. Again, we may iterate through the residue classes modulo 256 for $a$, and check if any of these $d(x) \in \mathbb{Z}[x]$. We suppress the computation, but doing the iteration yields no $d(x) \in \mathbb{Z}[x]$. This gives our contradiction, and we see that there is no monic $d(x) \in \mathbb{Z}[x]$ for which the period of the continued fraction of $\sqrt{d(x)}$ is 5. $\qquad\square$

## 4.3 A Classification

In this section we will use elementary number theoretic arguments, coupled with our parametrizations from Chapter II in order to prove Theorem IV.2. Before embarking on the proof of Theorem IV.2 we collect several observations and lemmas which will be most useful for us.

Ultimately we would like to understand when we get solutions to the Pell equation in $\mathbb{Z}[x]$. We begin by trying to understand when we get solutions whose leading coefficients are integers. This simplification of the problem will turn out to be enough to get us the result in Theorem IV.2. We first observe that if there is a solution to the Pell equation with integral leading coefficient then every solution to the same Pell equation will also have integral leading coefficient.

**Lemma IV.7.** *Let $d(x) \in \mathbb{Q}[x]$ be a monic, quartic, square-free polynomial. Suppose there exists a non-trivial solution to*

$$(4.2) \qquad\qquad f(x)^2 - d(x)g(x)^2 = 1$$

*with leading coefficient in $\mathbb{Z}$. Then every solution to (4.2) will also have leading coefficient in $\mathbb{Z}$.*

*Proof.* If (4.2) has a solution, then it has a minimal solution (*cf.* Proposition I.11) $u = p(x) + \sqrt{d(x)}q(x)$. Let $a$ denote the leading coefficient of $p(x)$, which after changing $q(x)$ to $-q(x)$ if necessary, is then also the leading coefficient of $q(x)$. By Proposition I.11 we know that every non-trivial solution to (4.2) is of the form $\pm u^k$ for $k \geq 1$. Let

$$u^k = p_k(x) + \sqrt{d(x)}q_k(x).$$

Because we have the identity

$$(r(x) + \sqrt{d(x)}s(x))(w(x) + \sqrt{d(x)}t(x)) =$$

$$(r(x)s(x) + d(x)s(x)t(x)) + \sqrt{d(x)}(s(x)w(x) + r(x)t(x)),$$

a simple induction proves that the leading coefficient of $q_k(x)$ is $2^{k-1}a^k$. By the hypotheses of the lemma, there is some $k_0 \geq 1$ such that $2^{k_0-1}a^{k_0} \in \mathbb{Z}$. Write $a = \frac{m}{n}$ with $n > 0$ and $\gcd(m, n) = 1$. If $p$ is a prime dividing $n$, then we must have $p^{k_0} \mid 2^{k_0-1}$ which is absurd. Thus $n = 1$ and $a \in \mathbb{Z}$ so $\pm 2^{k-1}a^k \in \mathbb{Z}$ for all $k \geq 1$ and lemma is proved. $\square$

Lemma IV.7 is useful because if there will exist a solution to the Pell equation with integral coefficients then necessarily the leading coefficient of any solution must be integral. Our parametrizations from Chapter II contain the assumption that the quartic is centered. While we would like to prove results about arbitrary monic, square-free, quartics, the following lemma allows us to pass off certain properties to the centered version of the arbitrary polynomial.

**Lemma IV.8.** *Let $d(x) \in \mathbb{Q}[x]$ be a monic, quartic, square-free polynomial, and let $d_c(x)$ denote the centered version of $d(x)$. Suppose there exists a non-trivial solution to*

$$f(x)^2 - d(x)g(x)^2 = 1$$

*with the leading coefficient of $f(x)$ an integer. Then every non-trivial solution to*

$$f(x)^2 - d_c(x)g(x)^2 = 1$$

*has integral leading coefficient.*

*Proof.* Let $d(x) = x^4 + rx^3 + sx^2 + tx + u$, and suppose there exist $p(x), q(x) \in \mathbb{Q}[x]$ such that

(4.3)
$$p(x)^2 - d(x)q(x)^2 = 1$$

with $p(x)$ non-constant and having integral leading coefficient. Put $\tilde{p}(x) = p\left(x - \frac{r}{4}\right)$ and $\tilde{q}(x) = q\left(x - \frac{r}{4}\right)$. If in (4.3) we make the change of variables $x \mapsto x - \frac{r}{4}$ then we get

$$\tilde{p}(x)^2 - d_c(x)\tilde{q}(x)^2 = 1.$$

Note that the leading coefficient of $\tilde{p}(x)$ is integral since it is the same as the leading coefficient of $p(x)$. Thus by Lemma IV.7 we have that every non-trivial solution to the Pell equation

$$f(x)^2 - d_c(x)g(x)^2$$

will have integral leading coefficient. $\qquad\square$

We are now in a position to be able to prove Theorem IV.2, and we briefly detail the strategy of proof. Let $d(x) \in \mathbb{Z}[x]$ be a monic, square-free, quartic polynomial, and suppose there exists a non-trivial solution to

$$f(x)^2 - d(x)g(x)^2 = 1$$

with $f(x), g(x) \in \mathbb{Z}[x]$. Because $d(x) \in \mathbb{Z}[x]$, Lemma IV.3 guarantees that if we write the centered version of $d(x)$ as $d_c(x) = x^4 + rx^2 + sx + t$, then $8r$, $8s$ and $256t$ are integers. Furthermore, Lemma IV.8 guarantees that any non-trivial solution to the Pell equation

$$f(x)^2 - d_c(x)g(x)^2 = 1$$

will have an integral leading coefficient. In Chapter II we wrote down a complete list of monic, centered, square-free, quartic polynomials in $\mathbb{Q}[x]$ which allow for a

non-trivial solution to the Pell equation. We've also already seen in Chapter I that any non-trivial solution to

$$f(x)^2 - d_c(x)g(x)^2 = 1$$

has that $\frac{f(x)}{g(x)}$ arises as a convergent to $\sqrt{d_c(x)}$. Thus we may also use the parametrizations found in Chapter II of the continued fractions in order to produce a solution to the Pell equation. Thus we must figure out conditions on the parameters $a$ and $b$ so that the leading coefficient of a solution is an integer, and that the coefficients of the centered quartic have at worst appropriate powers of 2 showing up in their denominators.

We perform our calculations by filtering based on the torsion order of the corresponding point on the Jacobian. Recall from Section 4.2 we need only consider polynomials for which the continued fraction of their square root has even order. Also, since periods 1, 2 and 4 have already been done by Webb and Yokota, we assume that the torsion order is not 5.

It is proven in [27] that if the period of the continued fraction of $\sqrt{d_c(x)}$ is $r$, and $\frac{p_k(x)}{q_k(x)}$ denotes the $k$-th convergent of $\sqrt{d_c(x)}$, then

$$p_{r-1}(x)^2 - d_c(x)q_{r-1}(x)^2 = (-1)^r.$$

We've already seen in Section 4.2 that we only need to consider continued fractions with even periods. Thus if $n$ is the order of the torsion element we are considering, then we will use the leading coefficient of $p_{r-1}(x)$ where

$$r = \begin{cases} n - 1, & n \text{ odd} \\ \\ 2(n - 1), & n \text{ even} \end{cases}$$

Throughout our computations, we will rely heavily on a formula for the leading coefficient of a solution to the Pell equation. By our remarks above, we must compute the leading coefficient of $p_{r-1}(x)$ for appropriate values of $r$. The next lemma allows us to easily compute this leading coefficient.

**Lemma IV.9.** *Let $K$ be a field and let $[a_0(x); a_1(x), a_2(x), \ldots]$ be a continued fraction with all $a_i(x)$ being non-constant polynomials in $K[x]$. Consider the $r$-th convergent*

$$\frac{p_r(x)}{q_r(x)} = [a_0(x); a_1(x), \ldots, a_r(x)].$$

*If $a_i(x)$ has leading coefficient $\alpha_i$ then the leading coefficient of $p_r(x)$ is*

$$\prod_{i=0}^{r} \alpha_i.$$

*Proof.* If we set $p_{-2}(x) = 0$, $p_{-1}(x) = 1$, $q_{-2}(x) = 1$ and $q_{-1}(x) = 0$ then it is a classical fact about continued fractions that for $i \geq 0$ we have

$$
\begin{aligned}
p_i(x) &= a_i(x)p_{i-1}(x) + p_{i-2}(x) \\
q_i(x) &= a_i(x)q_{i-1}(x) + q_{i-2}(x)
\end{aligned}
$$

(for a discussion of this, see Schmidt [24]). Notice that $p_0(x) = a_0(x)$ so the leading coefficient of $p_0(x)$ is $\alpha_0$. Furthermore, since $a_0(x)$ is assumed to be non-constant, we have that $\deg p_0(x)$ is strictly larger than $\deg p_{-1}(x)$. Because all $a_i(x)$'s are assumed to be non-constant, a simple induction shows that the sequence $(\deg p_i(x))_{i \geq -1}$ is increasing. Thus the recursive formula defining $p_i(x)$ implies that for $i \geq 0$, the leading coefficient of $p_i(x)$ is just the product of the leading coefficient of $p_{i-1}(x)$ with $\alpha_i$. Another simple induction yields the conclusion of the lemma. $\square$

As mentioned above, we will try to find rational values of the parameters $a$ and $b$ for which various rational functions in $a$ and $b$ are integer valued. By taking

appropriate products of these rational functions, we will be able to kill off one of the parameters, and only need to deal with rational functions in one variable. The following two lemmas will be used repeatedly to get a handle on which values of the parameter ensure that the value of our rational function is an integer.

**Lemma IV.10.** *Let $f(x), g(x) \in \mathbb{Z}[x]$ with $\gcd(f(x), g(x)) = 1$, $\deg(f(x)) > \deg(g(x))$, $f(0) \neq 0$ and $g(0) = 0$. Then the set of $\alpha \in \mathbb{Q}$ for which*

$$\frac{f(\alpha)}{g(\alpha)} \in \mathbb{Z}$$

*is finite. Moreover, there is an effective algorithm for computing this set of $\alpha$'s.*

*Proof.* Write

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

with $a_n a_0 \neq 0$, and write

$$g(x) = x^r (b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + b_0)$$

with $r > 0$ and $b_m b_0 \neq 0$. If $\alpha \in \mathbb{Q}^\times$ is such that

$$\frac{f(\alpha)}{g(\alpha)} = c \in \mathbb{Z},$$

then $\alpha$ will be a rational root of the polynomial

(4.4)  $$f(x) - cg(x).$$

If we write $\alpha = \dfrac{p}{q}$ with $q \neq 0$ and $\gcd(p, q) = 1$ then the rational root theorem says that $p$ must divide the constant term of (4.4) and $q$ must divide the leading coefficient of (4.4).

Thus we see that $p \mid a_0$ and $q \mid a_n$ by the conditions imposed on $f(x)$ and $g(x)$. This immediately implies that the set of $\alpha$'s for which $\dfrac{f(x)}{g(x)} \in \mathbb{Z}$ is finite. Moreover,

we can effectively compute this set of $\alpha$'s since we know that the numerator of $\alpha$ divides $a_0$ and the denominator divides $a_n$. □

**Lemma IV.11.** *For $n$ and $m$ positive integers, and $r, s \in \mathbb{Q}^\times$, the set*

$$\{\beta \in \mathbb{Q} : r\beta^n, s\beta^{-m} \in \mathbb{Z}\},$$

*is finite. Moreover, there is an effective algorithm for computing the set of $\beta$'s.*

*Proof.* The condition that $r\beta^n$ and $s\beta^{-m}$ are integers implies that

$$r\beta^n - s\beta^{-m} = \frac{r\beta^{n+m} - s}{\beta^m}$$

is an integer. Thus we may invoke Lemma IV.10 to reach the desired conclusion. □

We now prove Theorem IV.2 one torsion order at a time. The proofs in all orders are nearly identical, and where convenient, we sacrifice some computation (most of which is done using MAGMA [4]) for the sake of presentation.

**Order 4**

Here we are dealing with period 6. Put

$$
\begin{aligned}
A &= \frac{8a - 2}{b^2} \\
B &= \frac{32a}{b^3} \\
C &= \frac{16a^2 + 24a + 1}{b^4}.
\end{aligned}
$$

These are the coefficients arising in Theorem II.8, so we require that $8A, 8B, 256C \in \mathbb{Z}$. By Lemma IV.9 and Theorem II.10, the leading coefficient of $p_5(x)$ is

$$D = \frac{1}{512} \cdot \frac{b^8}{a^3}$$

which must be an integer as well. Hence the product

$$(8A)^4 D = \frac{2^{14}a^4 - 2^{15}a^3 + 3 \cdot 2^{12}a^2 - 2^{11}a + 2^7}{a^3}$$

is also an integer. Thus by Lemma IV.10 we see that for $(8A)^4 D$ to be an integer, certainly $a$ must be of the form $\pm 2^k$ where $-14 \le k \le 7$. For each such value of $a$, if we plug this number into the expressions for $8B$ and $D$, Lemma IV.11 gives us a finite list of values of $b$ for which both of these expressions can be integers. In total, there are 60 pairs $(a, b)$ for which $8A, 8B, 256C$ and $D$ are all integers. These pairs are

$$(\pm 2^{-14}, \pm 2^{-4}), (\pm 2^{-12}, \pm 2^{-3}), (\pm 2^{-11}, \pm 2^{-3}), (\pm 2^{-10}, \pm 2^{-2}), (\pm 2^{-9}, 2^{-2}),$$

$$(\pm 2^{-8}, \pm 2^{-1}), (\pm 2^{-7}, \pm 2^{-1}), (\pm 2^{-6}, \pm 2^{-1}), (\pm 2^{-5}, \pm 1), (\pm 2^{-4}, \pm 1),$$

$$(\pm 2^{-3}, \pm 1), (\pm 2^{-2}, \pm 2), (\pm 2^{-1}, \pm 2), (\pm 2, \pm 4), (\pm 4, \pm 4).$$

For each such pair $(a, b)$, we form the polynomial $f_{(a,b)}(x) = x^4 + Ax^2 + Bx + C$. In order for this polynomial to be the centered version of some polynomial with integer coefficients, there must exist $c \in \mathbb{Z}$ for which

$$f_{(a,b)}\left(x + \frac{c}{4}\right) \in \mathbb{Z}[x].$$

For example, if we look at the pair $(-2, -4)$ then we get the polynomial

$$x^4 + cx^3 + \frac{3c^2 - 9}{8}x^2 + \frac{c^3 - 9c + 16}{16}x + \frac{c^4 - 18c^2 + 64c + 17}{256}.$$

If we check all residue classes of $c$ modulo 8, we notice that there is no residue class for which $2c^2 - 9 \equiv 0 \pmod 8$. Thus there is no integer $c$ for which the polynomial $f_{(-2,-4)}\left(x + \frac{c}{4}\right)$ is in $\mathbb{Z}[x]$. For each of the 60 polynomials corresponding to our 60 pairs, we can check residue classes to see if there is a value of $c \in \mathbb{Z}$ for which the corresponding polynomial has integer coefficients. Surprisingly, among our list of 60 polynomials there are only 4 for which we can simultaneously make the coefficients integers. They are:

$$x^4 + cx^3 + \frac{3c^2 - 68}{8}x^2 + \frac{c^3 - 68c + \epsilon \cdot 64}{16}x + \frac{c^4 - 136c^2 + \epsilon \cdot 256c + 2576}{256},$$

$$x^4 + cx^3 + \frac{3c^2 - 20}{8}x^2 + \frac{c^3 - 20c + \epsilon \cdot 32}{16}x + \frac{c^4 - 50c^2 + \epsilon \cdot 128c - 112}{256}$$

where $\epsilon = \pm 1$. One can check that the second polynomial is not square-free! In fact, it is divisible by

$$\left(x + \frac{c - 2\epsilon}{4}\right)^2.$$

Since we are only dealing with square-free polynomials, we see that the only possibility for a monic, quartic, square-free polynomial in $\mathbb{Z}[x]$, which corresponds to a torsion point of order 4, for which there is a solution of the Pell equation with integer coefficients is

$$x^4 + cx^3 + \frac{3c^2 - 68}{8}x^2 + \frac{c^3 - 68c + \epsilon \cdot 64}{16}x + \frac{c^4 - 136c^2 + \epsilon \cdot 256c + 2576}{256}$$

for $\epsilon = \pm 1$. By looking at the coefficient of the $x^2$ term, we see that the only hope of this coefficient being integral is when $c \equiv 2 \pmod 4$. Substituting $c = 4d + 2$ gives the polynomials

$$x^4 + (4d+2)x^3 + (6d^2 + 6d - 7)x^2 + (4d^3 + 6d^2 - 14d - 12)x + d^4 + 2d^3 - 7d^2 - 12d + 6$$

$$x^4 + (4d+2)x^3 + (6d^2 + 6d - 7)x^2 + (4d^3 + 6d^2 - 14d - 4)x + d^4 + 2d^3 - 7d^2 - 4d + 10$$

which are obviously in $\mathbb{Z}[x]$ for any integer $d$. Thus it only remains to check if these polynomials actually have a non-trivial solution to the Pell equation with integer coefficients. In fact it is easy to check that the minimal degree solutions in these two cases are already in $\mathbb{Z}[x]$. The minimal solution to the Pell equation for the first polynomial (found by checking convergents) is

$$
\begin{aligned}
f(x) &= 4x^4 + (16d - 8)x^3 + (24d^2 - 24d - 20)x^2 + (16d^3 - 24d^2 - 40d + 48)x \\
&\quad + 4d^4 - 8d^3 - 20d^2 + 48d - 20 \\
g(x) &= 4x^2 + (8d - 12)x + 4d^2 + 12d - 8,
\end{aligned}
$$

and the minimal solution to the Pell equation for the second polynomial is

$$
\begin{aligned}
f(x) \;=\;& 4x^4 + (16d + 24)x^3 + (24d^2 + 72d + 28)x^2 + (16d^3 + 72d^2 + 56d - 48)x \\
& + 4d^4 + 24d^3 + 28d^2 - 48d - 76 \\
g(x) \;=\;& 4x^2 + (8d + 20)x + 4d^2 + 20d + 24.
\end{aligned}
$$

## Order 6

In this case, we are looking at period 10 and the coefficients arising in Theorem II.8 are

$$
\begin{aligned}
A \;&=\; \frac{6a^2 + 12a - 2}{b^2} \\
B \;&=\; \frac{32a^2 + 32a}{b^3} \\
C \;&=\; \frac{9a^4 + 4a^3 + 30a^2 + 20a + 1}{b^4}.
\end{aligned}
$$

The leading coefficient of $p_9(x)$ is

$$
D = \frac{1}{8192} \cdot \frac{b^{12}}{a^5(a + 1)^4}.
$$

Hence the product

$$
(8A)^6 D = \frac{2^{11} 3^6 \left(a^2 + 2a - \frac{1}{3}\right)^6}{a^5(a + 1)^4}
$$

is an integer. Using Lemma IV.10, we find that the only values of $a$ for which this expression is an integer are

$$
\left\{ -2, -\frac{4}{3}, -\frac{2}{3}, -\frac{1}{2}, -\frac{1}{3}, -\frac{1}{9}, \frac{1}{3}, 1 \right\}.
$$

If, for each $a$, we use Lemma IV.11 with $8A$ and $D$ we find that the only pairs $(a, b)$ for which $8A, 8B, 256C$ and $D$ are all integers are

$$
(-2, \pm 4) \left( -\frac{1}{2}, \pm 2 \right), (1, \pm 4), (1, \pm 8).
$$

For each pair $(a, b)$ we look at the polynomial $f_{(a,b)}\left(x + \frac{c}{4}\right)$ where

$$f_{(a,b)} = x^4 + Ax^2 + Bx + C.$$

For example, the pair $(1, -4)$ gives rise to the polynomial

$$x^4 + cx^3 + \frac{3c^2 + 8}{8}x^2 + \frac{c^3 + 8c - 16}{16}x + \frac{c^4 + 16c^2 - 64c + 64}{256}.$$

It is easy to check that there is no value of $c$ for which $c^4 + 16c^2 - 64c + 64 \equiv 0$ (mod 256). Thus there is no value of $c \in \mathbb{Z}$ for which this polynomial has integer coefficients. Repeating this argument for each $f_{(a,b)}\left(x + \frac{c}{4}\right)$ shows, somewhat surprisingly, that there is no $c \in \mathbb{Z}$ for which any of these polynomials have all integer coefficients. Thus there is no monic, quartic, square-free polynomial $d(x) \in \mathbb{Z}[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period 10 and the Pell equation has a solution with integral leading coefficient.

**Order 7**

This corresponds to the case of period 6. Letting $A, B$ and $C$ be the coefficients arising in Theorem II.8, we require that $8A, 8B, 256C \in \mathbb{Z}$. By Lemma IV.9 we compute the leading coefficient of $p_5(x)$ as

$$D = \frac{1}{256} \cdot \frac{b^7}{a^5(a-1)^3}.$$

Hence the product

$$(8A)^2(8B)D = \frac{256(a^4 - 6a^3 + 3a^2 + 2a + 1)^2}{a^3(a-1)^2}$$

is an integer. Lemma IV.10 gives that the only values of $a$ for which this expression is an integer are

$$\left\{-1, \frac{1}{2}, 2\right\}.$$

For each value of $a$ we can use Lemma IV.11 with $8A$ and $D$. The pairs $(a, b)$ for which $8A, 8B, 256C$ and $D$ are integers are

$$(-1, \pm 4), \left(\frac{1}{2}, \pm 1\right), (2, \pm 4).$$

Again, we look at the polynomials $f_{(a,b)}\left(x + \frac{c}{4}\right)$ for each pair $(a, b)$. For example, the pair $(2, 4)$ gives rise to the polynomial

$$x^4 + cx^3 + \frac{3c^2 + 15}{8}x^2 + \frac{c^3 + 15c + 32}{16}x + \frac{c^4 + 30c^2 + 128c + 97}{256}.$$

Notice that there is no $c$ for which $3c^2 + 15 \equiv 0 \pmod 8$, so there is no $c \in \mathbb{Z}$ for which this polynomial has integer coefficients. Looking at the quadratic term on each of the polynomials that arise shows that there is no $c \in \mathbb{Z}$ for which any of these polynomials has integer coefficients. Thus there are no other polynomials in period 6 which give an integral solution to the Pell equation.

**Order 8**

This corresponds to the case of period 14. Letting $A, B$ and $C$ be the coefficients arising in Theorem II.8, we require that $8A, 8B, 256C \in \mathbb{Z}$. By Lemma IV.9 we compute the leading coefficient of $p_{13}(x)$ as

$$D = \frac{1}{2^{23}} \cdot \frac{ab^{16}}{(a-1)^7 \left(a - \frac{1}{2}\right)^6}.$$

Hence the product

$$(8A)^8 D = \frac{2^{25}\left(a^4 + a^3 - 4a^2 + 2a - \frac{1}{4}\right)^8}{a^{15}(a-1)^7 \left(a - \frac{1}{2}\right)^6}$$

is an integer. If we appeal to Lemma IV.10 we find that there are no values of $a$ for which this expression is an integer. Thus there is no monic, quartic, square-free polynomial $d(x) \in \mathbb{Z}[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period 14 and the Pell equation has a solution with integral leading coefficient.

**Order 9**

This corresponds to the case of period 8. Letting $A, B$ and $C$ be the coefficients arising in Theorem II.8, we require that $8A, 8B, 256C \in \mathbb{Z}$. By Lemma IV.9 we compute the leading coefficient of $p_7(x)$ as

$$D = \frac{1}{1024} \cdot \frac{b^9}{a^7(a-1)^4(a^2-a+1)^3}.$$

Hence the product

$$(8A)(8B)(256C)D$$

is an integer. Lemma IV.10 gives that the only values of $a$ for which this expression is an integer are

$$\left\{-1, \frac{1}{2}, 2\right\}.$$

If for each $a$ we use Lemma IV.11 on $8A$ and $D$, we actually get that there are no values of $b$ for which $8A$ and $D$ are integers. Thus there is no monic, quartic, square-free polynomial $d(x) \in \mathbb{Z}[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period 8 and the Pell equation has a solution with integral leading coefficient.

**Order 10**

This corresponds to the case of period 18. Letting $A, B$ and $C$ be the coefficients arising in Theorem II.8, we require that $8A, 8B, 256C \in \mathbb{Z}$. By Lemma IV.9 we compute the leading coefficient of $p_{17}(x)$ as

$$D = \frac{-1}{2^{29}} \cdot \frac{b^{20}(a^2-3a+1)^{15}}{a^{21}(a-1)^9 \left(a-\frac{1}{2}\right)^8}.$$

Hence the product

$$(8A)^{10}D$$

is an integer. If we appeal to Lemma IV.10 we find that there are no values of $a$ for which this expression is an integer. Thus there is no monic, quartic, square-free

polynomial $d(x) \in \mathbb{Z}[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period 18 and the Pell equation has a solution with integral leading coefficient.

## Order 12

This corresponds to the case of period 22. Letting $A, B$ and $C$ be the coefficients arising in Theorem II.8, we require that $8A, 8B, 256C \in \mathbb{Z}$. By Lemma IV.9 we compute the leading coefficient of $p_{21}(x)$ as

$$D = \frac{1}{2^{43}3^9} \cdot \frac{(a-1)^{37}b^{24}}{a^{11}\left(a-\frac{1}{2}\right)^{10}\left(a^2-a+\frac{1}{2}\right)^8\left(a^2-a+\frac{1}{3}\right)^9}.$$

Hence the product

$$(8A)^{12}D$$

is an integer. If we appeal to Lemma IV.10 we find that there are no values of $a$ for which this expression is an integer. Thus there is no monic, quartic, square-free polynomial $d(x) \in \mathbb{Z}[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period 22 and the Pell equation has a solution with integral leading coefficient.

Combining our results with Webb and Yokota's results, we obtain the following theorems.

**Theorem IV.12.** *Let $d(x) \in \mathbb{Z}[x]$ be a monic, quartic, square-free polynomial. If the Pell equation*

$$f(x)^2 - d(x)g(x)^2 = 1$$

*has a non-trivial solution $f(x), g(x) \in \mathbb{Z}[x]$ then the period of the continued fraction of $\sqrt{d(x)}$ is either 1, 2 or 6.*

**Theorem IV.13.** *Let $d(x) \in \mathbb{Z}[x]$ be a monic, quartic, square-free polynomial for which the period of the continued fraction of $\sqrt{d(x)}$ is 6. Then the Pell equation*

$$f(x)^2 - d(x)g(x)^2 = 1$$

has a non-trivial solution $f(x), g(x) \in \mathbb{Z}[x]$ if and only if there exists $c \in \mathbb{Z}$ for which $d(x)$ is one of:

$$x^4 + (4c+2)x^3 + (6c^2 + 6c - 7)x^2 + (4c^3 + 6c^2 - 14c - 12)x + c^4 + 2c^3 - 7c^2 - 12c + 6,$$

$$x^4 + (4c+2)x^3 + (6c^2 + 6c - 7)x^2 + (4c^3 + 6c^2 - 14c - 4)x + c^4 + 2c^3 - 7c^2 - 4c + 10.$$

**Theorem IV.14** (Webb-Yokota). *Let $d(x) \in \mathbb{Z}[x]$ be a monic, quartic polynomial such that the continued fraction of $\sqrt{d(x)}$ is periodic of period 1 or 2. Then there exist polynomials $a(x), c(x) \in \mathbb{Q}[x]$ for which $d(x) = a(x)^2 + 2c(x)$ and $b(x) = \dfrac{a(x)}{c(x)} \in \mathbb{Q}[x]$ and either $a(x) \in \mathbb{Z}[x]$ or $2a(x) \in \mathbb{Z}[x]$. The Pell equation*

$$f(x)^2 - d(x)g(x)^2 = 1$$

*has a non-trivial solution $f(x), g(x) \in \mathbb{Z}[x]$ if and only if one of the following holds*

- $b(x), c(x) \in \mathbb{Z}[x]$

- $a(x) \in \mathbb{Z}[x]$ and $2c(x) = 1$

- $a(x), \frac{1}{2}b(x), 2c(x) \in \mathbb{Z}[x]$, $\deg c(x) > 0$ and the leading coefficient of $c(x)$ is $\pm\frac{1}{2}$.

*Moreover, in this case the minimal degree solution to the Pell equation has integer coefficients.*

## 4.4   Remarks

We conclude this chapter with some remarks on our classification of Section 4.3. The crucial idea in the proof of Theorem IV.14 of Webb and Yokota comes from the following proposition.

**Proposition IV.15** (Webb-Yokota). *Let $d(x) = a(x)^2 + 2c(x)$ be a monic polynomial in $\mathbb{Z}[x]$, where $\deg c(x) < \deg a(x)$ and $\dfrac{a(x)}{c(x)} \in \mathbb{Q}[x]$ and $2a(x) \in \mathbb{Z}[x]$. Then the Pell*

*equation*

$$f(x)^2 - d(x)g(x)^2 = 1$$

*has a non-trivial solution $f(x), g(x) \in \mathbb{Z}[x]$ if and only if the minimal degree solution already has integral coefficients.*

*Remark* IV.16. The condition $\dfrac{a(x)}{c(x)} \in \mathbb{Q}[x]$ is equivalent to the condition that the continued fraction of $\sqrt{d(x)}$ is periodic of period 1 or 2. Furthermore, the condition $2a(x) \in \mathbb{Z}[x]$ is automatically satisfied whenever $d(x)$ is quartic. This proposition allows Webb and Yokota to solve the corresponding classification problem for monic, quadratic $d(x)$. This is because if $d(x) = x^2 + ax + b$ is square-free and in $\mathbb{Z}[x]$ then one can write $d(x) = \left(x + \frac{a}{2}\right)^2 + \left(b - \frac{a^2}{4}\right)$.

Theorem IV.14 follows easily from this Proposition because one may easily compute the minimal degree solution of the Pell equation using the continued fraction of $\sqrt{d(x)}$, and then check what conditions must be satisfied for this minimal solution to have integer coefficients.

As a corollary of our proofs of Theorem IV.12 and Theorem IV.13, we observe

**Corollary IV.17.** *Let $d(x) \in \mathbb{Z}[x]$ be a monic, quartic, square-free polynomial. If the Pell equation*

$$f(x)^2 - d(x)g(x)^2 = 1$$

*has a non-trivial solution $f(x), g(x) \in \mathbb{Z}[x]$ then already the minimal degree solution to the Pell equation has integer coefficients.*

One can hope that Corollary IV.17 applies more generally. We may ask the following question, for which there is no known counter-example.

**Question IV.18.** *Let $d(x) \in \mathbb{Z}[x]$ be a monic polynomial of even degree. If the Pell equation has a non-trivial solution with integer coefficients then is it necessarily the*

*case that the minimal degree solution must also have integer coefficients?*

An affirmative answer to Question IV.18 would greatly help the study of polynomial Pell equation over $\mathbb{Z}[x]$. This is because one can hope to explicitly write out the continued fraction of $\sqrt{d(x)}$, use its convergents to find a minimal degree to solution to the Pell equation, and then check if the minimal solution has integer coefficients.

At this time we are also not able to analyze the case that $d(x)$ is non-square free. This is because if $d(x)$ is divisible by the square of a non-constant polynomial then the curve $y^2 = d(x)$ will not have geometric genus 1, and we cannot use results about elliptic curves. In the course of our proof of Theorem IV.13, we did exhibit a non square-free polynomial for which the Pell equation has a non-trivial solution. For example, for $a \in \mathbb{Z}$ the polynomials

$$d_1(x) = x^4 + (4a+2)x^3 + (6a^2 + 6a - 1)x^2 + (4a^3 + 6a^2 - 2a)x + a^4 + 2a^3 - a^2$$

$$d_2(x) = x^4 + (4a+2)x^3 + (6a^2 + 6a - 1)x^2 + (4a^3 + 6a^2 - 2a - 4)x + (a+1)^2(a^2 - 2)$$

are both non square-free, both have the property that $\sqrt{d_i(x)}$ has a continued fraction of period 6, and both have a minimal solution to the Pell equation which has integer coefficients. It would be great to have an answer to the following question.

**Question IV.19.** *Outside of periods 1 and 2, are these the only examples of monic, quartic, non square-free polynomials in $\mathbb{Z}[x]$ for which the Pell equation has a non-trivial solution with integer coefficients?*

Most generally, it would be interesting to try to solve the problem of which quartic polynomials in $\mathbb{Z}[x]$ have a non-trivial solution to the Pell equation with integer coefficients, where we don't require our polynomial to be monic. At this time we do not have an answer for the most general problem, but there is hope that some of the techniques in this chapter may lead to a resolution of this problem.

# CHAPTER V

# Generalizations and Questions

## 5.1 Synopsis

We conclude our discussion of polynomial Pell equations with a brief discussion of potential directions, generalizations and conjectures pertaining to the material in this thesis. First we will look at some of the challenges of working with quartic polynomial Pell equations over number fields other than $\mathbb{Q}$. Then we will examine the difficulties of working with polynomials whose degree is larger than four.

## 5.2 Number Fields

Throughout our work we repeatedly made use of Mazur's theorem to bound the torsion order of a rational point on an elliptic curve defined over $\mathbb{Q}$, and subsequently we used this to conclude facts about the periods of certain continued fractions. There is a generalization of Mazur's theorem due to Merel [17].

**Theorem V.1** (Merel). *For all positive integers $n$ there exists a positive constant $B_n$ such that for all elliptic curves $E$ over a number field $K$ with $[K : \mathbb{Q}] = n$ then*

$$|E(K)_{tors}| \leq B_n.$$

Combining Theorem V.1 with Theorem I.16 gives the following corollary about quartic polynomials over number fields.

**Corollary V.2.** *For all positive integers $n$ there exists a positive constant $C_n$ such that the following holds. If $K$ is a number field with $[K : \mathbb{Q}] = n$ and $d(x) \in K[x]$ is a quartic, square-free polynomial for which the Pell equation*

$$f(x)^2 - d(x)g(x)^2 = 1$$

*has a non-trivial solution $f(x), g(x) \in K[x]$, then the period of the continued fraction of $\sqrt{d(x)}$ is bounded by $C_n$.*

For values of $n > 2$ it is not known how small $B_n$ can be taken in Theorem V.1. The constant $B_2$, however, is known for quadratic number fields. Kenku and Momose [11], and Kamienny [9] prove exactly which finite groups can occur for $E(K)_{tors}$ when $K$ is a quadratic number field. We have as a corollary of their result

**Theorem V.3** (Kamienny, Kenku, Momose). *Let $K$ be a quadratic number field, $E$ an elliptic curve defined over $K$ and $p \in E(K)$ a torsion point. If $m$ denotes the order of $p$ in $E(K)$ then $m$ is one of*

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18\}.$$

Thus Theorem V.3 and Theorem I.16 allow us to conclude that if $K$ is a quadratic number field and $d(x) \in K[x]$ is a quartic, square-free polynomial for which the continued fraction of $\sqrt{d(x)}$ is periodic then the period of the continued fraction is among

(5.1) $\qquad \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 22, 26, 30, 34\}.$

It is then natural to ask the following questions about this list of possible periods.

**Question V.4.** *Let $K$ be a quadratic number field. For which values $n$ in (5.1) does there exist a quartic, square-free polynomial $d(x) \in K[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period $n$?*

**Question V.5.** *For which odd n in (5.1) does there exist a quadratic number field K and a quartic, square-free polynomial $d(x) \in K[x]$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period n?*

The formulas of Chapter II remain valid over arbitrary number fields. Thus to study periods 7, 9 and 11 over quadratic number fields $K$ we only need to look for $K$-points of the curves defined in Chapter III. By naively searching for points on equations (3.10), (3.14), (3.18) over quadratic number fields of small discriminant, we can find examples of periods 9 and 11, and an example of a monic polynomial having period 7.

**Example V.6.** Consider the curve (3.10) defined by $y^2 = 8x(x^2 + 1)$. Over $\mathbb{Q}(\sqrt{5})$ this curve has in addition to the solutions in Theorem III.6 the solution $(2, 4\sqrt{5})$. Thus the polynomial

$$d_7(x) = x^4 + \frac{271}{360}x^2 + \frac{32\sqrt{5}}{45}x + \frac{288481}{518400} \in \mathbb{Q}(\sqrt{5})$$

has the property that the period of the continued fraction of $\sqrt{d_7(x)}$ is 7.

**Example V.7.** Consider the curve (3.14) defined by $y^2 = -(x - 1)x(x^2 - 3x + 1)$. Over $\mathbb{Q}(\sqrt{2})$ this curve has the solution $\left(\frac{\sqrt{2}+2}{2}, \frac{\sqrt{2}+1}{2}\right)$. By taking $z = 2$ in (3.13) we get that the polynomial

$$d_9(x) = (-2\sqrt{2} + 3)x^4 + (2\sqrt{2} - 1)x^2 + 4x + \frac{-2\sqrt{2} + 11}{4} \in \mathbb{Q}(\sqrt{2})[x]$$

has the property that the period of the continued fraction of $\sqrt{d_9(x)}$ is 9.

**Example V.8.** Consider the curve (3.14) defined by $y^2 = \frac{1}{3}(x - 1)x\left(x^2 - x + \frac{1}{3}\right)$. Over $\mathbb{Q}(\sqrt{5})$ this curve has the solution $\left(\frac{\sqrt{5}+1}{2}, -\frac{2}{3}\right)$. By taking $z = 4$ in (3.17) we get that the $\mathbb{Q}(\sqrt{5})[x]$ polynomial

$$d_{11}(x) = \frac{-72\sqrt{5} + 161}{45}x^4 + \frac{-1384\sqrt{5} + 3078}{45}x^2 + \frac{-1856\sqrt{5} + 4160}{15}x + \frac{528\sqrt{5} + 23161}{45}$$

has the property that the period of the continued fraction of $\sqrt{d_{11}(x)}$ is 11.

For torsion orders other than the ones given in Mazur's theorem we can no longer obtain parametrizations. This is because Mazur [15] showed that for $N$ not among

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\},$$

the compactification of the moduli space parametrizring isomorphism classes of elliptic curves with a point of order $N$, denoted by $X_1(N)$, is no longer a genus 0 curve. There is still some hope to get information in other cases, though, since we do have explicit equations for $X_1(N)$ for higher values of $N$. In [10], Kamienny and Najman give equations for $X_1(N)$ for $11 \leq N \leq 18$ excluding 17. Given a quadratic number field $K$ one could hope to find all the $K$-points on the $X_1(N)$, thereby finding all elliptic curves over $K$ with a point of order $N$, and then use the methods of Chapter II and Chapter III in order to reduce the existence question of certain periods of continued fractions to a question about $K$-points on certain varieties.

In [10], the authors also tackle the the question of determining, for each $N \in \{11, 13, 14, 15, 16, 18\}$, the minimal discriminant field $\mathbb{Q}(\sqrt{r})$ such that there exists an elliptic curve defined over $\mathbb{Q}(\sqrt{r})$ and a torsion $\mathbb{Q}(\sqrt{r})$-point of order $N$. For 14, 16, and 18 these fields are $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-15})$ and $\mathbb{Q}(\sqrt{33})$ respectively. Thus to look for polynomials whose square roots have periodic continued fraction of period 13, 15 or 17, one must work over quadratic fields of sufficiently large discriminant.

The problem of finding all the $K$-points on a smooth, projective variety defined over $K$ is in general open and very difficult. There have been lots of advances of finding all the $K$-points on curves, but even this case is open for genus greater than 0. Even so, there is some hope that if the equations produced are sufficiently nice, then one could prove or disprove the existence of periods 13, 15, and 17 over various

quadratic number fields.

## 5.3    Higher Degrees

Another direction for this research to go would be to look at the case where the degree of $d(x)$ is at least 6. Now, if $K$ is a field and $d(x) \in K[x]$ is a monic, square-free polynomial of even degree at least 6, then the normalization of the curve

$$y^2 = d(x)$$

has genus at least 2. Thus studying the existence of non-trivial solutions to the Pell equation

$$f(x)^2 - d(x)g(x)^2 = 1$$

is equivalent to the assertion that a particular $K$-point on an abelian variety of dimension at least 2 is a torsion point. For abelian varieties of dimension at least 2, there is no known analogue of Merel's theorem, Theorem V.1. There are, however, a couple of conjectures in this direction. Both of these are taken from Alice Silverberg's lectures found in [6].

**Conjecture V.9** (Torsion Conjecture for Abelian Varieties)**.** *If $A$ is an abelian variety of dimension $d$ defined over a number field $K$ of degree $m$, then $|A(K)_{tors}|$ is bounded above by a constant depending only on $d$ and $K$.*

**Conjecture V.10** (Strong Torsion Conjecture for Abelian Varieties)**.** *If $A$ is an abelian variety of dimension $d$ defined over a number field $K$ of degree $m$, then $|A(K)_{tors}|$ is bounded above by a constant depending only on $d$ and $m$.*

In addition to it being open as to whether or not there is a uniform bound on how large the torsion order of a $K$-point can be (which is a slightly weaker condition than asserting that $|A(K)_{tors}|$ is uniformly bounded), there is another difficulty. Namely

if $(A, p)$ is the abelian variety and point at infinity associated with $d(x)$, then there is no known formula relating the period of the continued fraction of $\sqrt{d(x)}$ and the torsion order of $p$. We do however have an upper bound on the quasi-period of the continued fraction of $\sqrt{d(x)}$ in terms of the torsion order due to Berry [3]

**Theorem V.11** (Berry). *Let $K$ be a field of characteristic different from 2 and let $d(x) \in K[x]$ be a monic, square-free polynomial of degree $2m$ where $m > 4$. If $d(x)$ corresponds to the pair $(A, p)$ where $A$ is an abelian variety defined over $K$ and $p \in A(K)$ is a torsion point of order $n$, then the quasi-period of the continued fraction of $\sqrt{d(x)}$ is at most $n - m + 1$.*

Using Theorem V.11 we can show that a finiteness result on the set of periods of continued fractions corresponding to fixed degree follows from Conjectures V.9 and V.10.

**Proposition V.12.** *Let $m > 2$ be an integer and $K$ a number field. If Conjecture V.9 is true then there exists a positive constant $C(m, K)$, depending only on $m$ and $K$, such that if $d(x) \in K[x]$ is a monic, square-free polynomial of degree $2m$ for which the continued fraction of $\sqrt{d(x)}$ is periodic, then the period is bounded above by $C(m, K)$.*

*Proof.* Assume Conjecture V.9 and let $B(m-1, K)$ be an upper bound for the torsion order of a $K$-point on an abelian variety of dimension $m - 1$ defined over $K$. Let $d(x) \in K[x]$ be a monic, square-free polynomial of degree $2m$ for which the continued fraction of $\sqrt{d(x)}$ is periodic of period $n$. In this case, $d(x)$ corresponds to an abelian variety $A$ of dimension $m - 1$ and a torsion point $p \in A(K)$. Thus the order of $p$ is bounded above by $B(m-1, K)$, and by Theorem V.11, we know that the quasi-period $q$ of the continued fraction of $\sqrt{d(x)}$ is at most $B(m - 1, K) - m + 1$.

We've already seen in Chapter I that $q$ divides $n$ and that if $q$ is odd then neces-

sarily $n \leq 2q$. If on the other hand $q$ is even then in the continued fraction expansion for $\sqrt{d(x)}$ we will have $\alpha_q(x) = \mu\alpha_0(x)$ for some primitive $r$-th root of unity $\mu \in K$ in which case $n = rq$. The field $K$ contains only finitely many roots of unity so let $r(K)$ be the maximal order among the roots of unity in $K$. Then $n$ is bounded above by $r(K)q$ which is at most $r(K)(B(m-1,K) - m + 1)$. Thus we have an upper bound $C(m, K)$, depending only on $m$ and $K$, for the period of the continued fraction of $\sqrt{d(x)}$. $\qquad\square$

**Proposition V.13.** *Let $r$ and $m$ be nonnegative integers with $m > 2$. If Conjecture V.10 is true then there exists a positive constant $C(m, r)$, depending only on $m$ and $r$, such that if $K$ is a numbr field of degree $r$ and $d(x) \in K[x]$ is a monic, square-free polynomial of degree $2m$ for which the continued fraction of $\sqrt{d(x)}$ is periodic, then the period is bounded above by $C(m, r)$.*

*Proof.* The proof is identical to that of Proposition V.12 except now we can bound the maximal order of a root of unity in terms of the degree of the number field. $\qquad\square$

The hypothetical bounds given in Proposition V.12 and Proposition V.13 may or may not be optimal. In the quartic case, we've already seen that if the quasi-period is even then the root of unity showing up is just 1, and the quasi-period is also the period. This is independent of the field we are working over, so it would be interesting to understand which other roots of unity, if any, may arise in the case of polynomials of higher degree. There are very few examples known of sextic polynomials for which the continued fraction of their square-root is periodic. It would be useful to try to find several examples over number fields and compute the continued fractions and the constants arising.

Another interesting question in the higher degree case is to understand which pairs

$(A, p)$ correspond to polynomials. In the elliptic case, we saw that Adams and Razar [2] proved that, given any elliptic curve $E$ defined over $\mathbb{Q}$ and any $\mathbb{Q}$-rational point $p$ on $E$, there exists a monic, square-free, quartic polynomial $d(x) \in \mathbb{Q}[x]$ corresponding to $(E, p)$. There is currently no analogue of this result to higher dimensional varieties. Obviously one cannot expect to get every abelian variety because not every abelian variety occurs as the Jacobian of some curve. Even so, it would be interesting to consider the following analogue of Adams and Razar.

**Question V.14.** *Let $A$ be an abelian variety defined over $\mathbb{Q}$ for which $A$ is isomorphic to the jacobian of some hyperelliptic curve. For which points $p \in A(\mathbb{Q})$ do there exist $d(x) \in \mathbb{Q}[x]$ such that $(A, p)$ corresponds to $d(x)$?*

This question seems a bit ambitious yet an answer to it would be useful since it would allow one to construct many examples of polynomials in higher degree for which we can test the periods of the corresponding continued fractions.

# BIBLIOGRAPHY

# BIBLIOGRAPHY

[1] N. H Abel. Ueber die integration der differential-formel $\rho dx/\sqrt{R}$, wenn $r$ und $\rho$ ganze functionen sind. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1826(1):185–221, 1826.

[2] William W. Adams and Michael J. Razar. Multiples of points on elliptic curves and continued fractions. *Proc. London Math. Soc. (3)*, 41(3):481–498, 1980.

[3] T. G. Berry. On periodicity of continued fractions in hyperelliptic function fields. *Arch. Math. (Basel)*, 55(3):259–266, 1990.

[4] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[5] P.L Chebyshev. Sur l'intégration de la differential $\frac{x+A}{\sqrt{(x^4+\alpha x^3+\beta x^2+\gamma)}}dx$. *J. Math. Pures Appl.*, 9(1):225–46, 1864.

[6] Brian Conrad and Karl Rubin, editors. *Arithmetic algebraic geometry*, volume 9 of *IAS/Park City Mathematics Series*. American Mathematical Society, Providence, RI, 2001. Including papers from the Graduate Summer School of the Institute for Advanced Study/Park City Mathematics Institute held in Park City, UT, June 20–July 10, 1999.

[7] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[8] L. Euler. usu novi algorithmi in problemate pelliano solvendo. *Novi Commentarii academiae scientiarum Petropolitanae*, 11:29–66, 1767.

[9] S. Kamienny. Torsion points on elliptic curves and $q$-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

[10] Sheldon Kamienny and Filip Najman. Torsion groups of elliptic curves over quadratic fields. *Acta Arith.*, 152(3):291–305, 2012.

[11] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988.

[12] Anthony W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[13] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc. (3)*, 33(2):193–237, 1976.

[14] V. A. Malyshev. Periods of quadratic irrationalities, and torsion of elliptic curves. *Algebra i Analiz*, 15(4):177–203, 2003.

[15] B. Mazur. Rational points on modular curves. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 107–148. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[16] J. McLaughlin. Polynomial solutions of Pell's equation and fundamental units in real quadratic fields. *J. London Math. Soc. (2)*, 67(1):16–28, 2003.

[17] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[18] R. A. Mollin. Polynomial solutions for Pell's equation revisited. *Indian J. Pure Appl. Math.*, 28(4):429–438, 1997.

[19] Richard A. Mollin. *Quadratics*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1996.

[20] Melvyn B. Nathanson. Polynomial Pell's equations. *Proc. Amer. Math. Soc.*, 56:89–92, 1976.

[21] A. M. S. Ramasamy. Polynomial solutions for the Pell's equation. *Indian J. Pure Appl. Math.*, 25(6):577–581, 1994.

[22] A. Schinzel. On some problems of the arithmetical theory of continued fractions. *Acta Arith.*, 6:393–413, 1960/1961.

[23] A. Schinzel. On some problems of the arithmetical theory of continued fractions. II. *Acta Arith.*, 7:287–298, 1961/1962.

[24] Wolfgang M. Schmidt. On continued fractions and Diophantine approximation in power series fields. *Acta Arith.*, 95(2):139–166, 2000.

[25] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[26] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

[27] Alfred J. van der Poorten and Xuan Chuong Tran. Quasi-elliptic integrals and periodic continued fractions. *Monatsh. Math.*, 131(2):155–169, 2000.

[28] Alfred J. van der Poorten and Xuan Chuong Tran. Periodic continued fractions in elliptic function fields. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 390–404. Springer, Berlin, 2002.

[29] W. A. Webb and H. Yokota. Polynomial Pell's equation. II. *J. Number Theory*, 106(1):128–141, 2004.

[30] W. A. Webb and H. Yokota. On the period of continued fractions. *JP J. Algebra Number Theory Appl.*, 6(3):551–559, 2006.

[31] William A. Webb and Hisashi Yokota. Polynomial Pell's equation. *Proc. Amer. Math. Soc.*, 131(4):993–1006 (electronic), 2003.

[32] H. Yokota. Polynomial Pell's equation and periods of quadratic irrationals. *JP J. Algebra Number Theory Appl.*, 8(1):135–144, 2007.

[33] H. Yokota. Solutions of polynomial Pell's equation. *J. Number Theory*, 130(9):2003–2010, 2010.

[34] Jing Yu. On arithmetic of hyper elliptic curves. *Aspects of Mathematics*, pages 395–415, 2001.