Chapter 3

Hyperelliptic continued fractions and generalized Jacobians (minicourse given by Umberto Zannier)

Laura Capuano, Peter Jossen, Christina Karolus, Francesco Veneziano

These are notes from the minicourse given by Umberto Zannier (Scuola Normale Superiore di Pisa). The notes were worked out by Laura Capuano, Peter Jossen[1], Christina Karolus, and Francesco Veneziano. Most of the material of these lectures, except for the numerical examples which were added by us, is already available in [Zan16]. The authors wish to thank Umberto Zannier for the lively discussions in Alpbach, and Olaf Merkert for providing computations of the examples 3.17, 3.28, 3.29, 3.33 and 3.25.

3.1 Introduction and some history

Let d be an integer. The Pell equation, bearing John Pell's (1611-1685) name somewhat by mistake, is the Diophantine equation

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

to be solved in integers x and y. This equation was studied by Indian, and later by Arabic and Greek mathematicians (see for example [Len02] for some history on the problem). From a modern point of view, solutions (x, y) of the Pell equation correspond to units $x + y\sqrt{d}$ of norm 1 in the ring $\mathbb{Z}[\sqrt{d}]$. One reason why ancient mathematicians were interested in the Pell equation is that a solution (x, y) of the Pell equation with large x and y provides a good rational

[1] P. Jossen served as group leader of the working group "Minicourse Zannier".

approximation to the square root of d, as

$$d = \frac{x^2-1}{y^2} \simeq \left(\frac{x}{y}\right)^2.$$

For instance, Baudhayana (a vedic priest who lived around the 800 BC) discovered that $(x, y) = (17, 12)$ and $(x, y) = (577, 408)$ are solutions for the Pell equation with $d = 2$, and that 17/12 and 577/408 are close approximations to $\sqrt{2}$. In fact,

$$\frac{577}{408} = 1.41421568627 \qquad \text{and} \qquad \sqrt{2} = 1.41421356237.$$

Methods to construct new, larger solutions of the Pell equation from a given solution were already known to the Indian mathematician and astronomer Bramagupta in the 7th century. The fact that for every nonsquare $d > 0$ the Pell equation has one (hence infinitely many) nontrivial solutions is a result attributed to Lagrange. Long before him, Wallis and Euler described methods finding solutions of the Pell equation, although Lagrange was the first to show that the method actually works in any case. Euler's method involves continued fractions. For example, to solve the equation $x^2 - 3y^2 = 1$, we can write

$$\sqrt{3} = 1 + \frac{1}{1+\frac{1}{2+\sqrt{3}}} = 1 + \frac{1}{1+\frac{1}{2+\frac{1}{1+\frac{1}{2+\cdots}}}},$$

and notice that the continued fraction of $\sqrt{3}$ is periodic. Stopping the continued fraction at various stages yields a sequence of rational approximations to $\sqrt{3}$. These are:

$$1, \frac{2}{1}, \frac{5}{3}, \frac{7}{4}, \frac{19}{11}, \frac{26}{15}, \frac{71}{41}, \frac{97}{56}, \frac{265}{153}, \frac{362}{209}, \frac{989}{571}, \frac{1351}{780}, \frac{3691}{2131}, \frac{5042}{2911}, \frac{13775}{7953}, \frac{18817}{10864}, \frac{51409}{29681}, \frac{70226}{40545}, \ldots$$

In this sequence, solutions (x, y) of the Pell equation $x^2 - 3y^2 = 1$ occur as numerators and denominators, as one stops the continued fraction at even stages:

$$1 = 2^2 - 3 \cdot 1^2 = 7^2 - 3 \cdot 4^2 = 26^2 - 3 \cdot 15^2 = \cdots = 70226^2 - 3 \cdot 40545^2.$$

If we stop at odd stages we solve the equation $x^2 - 3y^2 = -2$. Lagrange's contribution is the statement that for every nonsquare integer $d > 1$, the continued fraction expansion of $\sqrt{d}$ is periodic.

In the 1760's, Euler discovered several polynomial identities for the Pell equation. Among them, for example, the following equality ([Eu1767]):

$$(2n^2+1)^2 - (n^2+1)(2n)^2 = 1. \tag{3.1}$$

More generally, if T_k and U_k denote the Chebyshev polynomials of the first and second kind, the relation

$$T_k(n)^2 - (n^2-1)U_{k-1}(n)^2 = 1$$

holds. Euler's identity is the case $k = 2$. Such polynomial solutions to Pell equation have interesting applications to the problem of computing class numbers of real quadratic number fields, see [McL03], but also qualify as interesting for their own sake.

In these notes, we study the polynomial interpretation of the Pell equation

$$x(t)^2 - D(t)y(t)^2 = 1,$$

where $D \in \mathbb{C}[t]$ is a given polynomial with complex coefficients of even degree, to be solved in polynomials $x(t), y(t) \in \mathbb{C}[t]$. This topic was already studied by Abel in 1826, later also by Chebyshev and, more recently, among others by Hellegouarch, van der Poorten, Platonov, Akhiezer, Krichever, McMullen, Masser, Bertrand and Zannier. Abel was interested in expressing certain integrals in 'finite terms'. He observed that, if $x(t), y(t) \in \mathbb{C}[t]$ form a nontrivial solution of the Pell equation, then the equality

$$\int \frac{x'(t)}{y(t)\sqrt{D(t)}}dt \;=\; \log\left(x(t) + y(t)\sqrt{D(t)}\right)$$

holds. As in the arithmetic case, there is a close connection between continued fractions and the solutions of the Pell equation. Namely, if we expand $\sqrt{D(t)}$ as a Laurent series around ∞ and determine its continued fraction expansion (a procedure we shall explain in more details later), then the following holds.

Theorem 3.1 (Abel, 1826). *Let $D(t) \in \mathbb{C}[t]$ be a polynomial of even degree, which is not a perfect square. The Pell equation $x(t)^2 - D(t)y(t)^2 = 1$ has a nontrivial solution if and only if the continued fraction expansion of $\sqrt{D(t)}$ is eventually periodic.*

Among the myriad of interesting questions that one may ask about continued fraction expansions of algebraic functions such as $\sqrt{D(t)}$, or of Laurent series in general, we will focus on two. The first concerns the behaviour of the solvability of the polynomial Pell equation for families of polynomials. Consider the a family of polynomials $D_\lambda(t) \in \mathbb{C}(\lambda)[t]$ depending on a parameter λ, for example, $D_\lambda(t) = t^4 + \lambda t^2 + t + 1$. We may ask for which specializations of the parameter $\lambda \in \mathbb{C}$ the equation

$$x(t)^2 - D_\lambda(t)y(t)^2 = 1$$

has a nontrivial solution. These problems for different pencils of polynomials have been studied by several authors (see [MZ15] for $D_\lambda(t) = t^6 + t + \lambda$, and [Ber13] and [Sch15] for some non-squarefree families of $D_\lambda(t)$). We also point out that these questions are related to problems of *Unlikely Intersections* in families of Jacobians of hyperelliptic curves (or *Generalized Jacobians*, as they are called in the non-squarefree case). For a survey on this, see also [Zan14]. We will discuss this matter in Section 3.6.

The second question concerns the behaviour of the partial quotients in the continued fraction expansion of $\sqrt{D(t)}$ in the non-periodic case. Here we will prove that at least the sequence of degrees of the partial quotients is periodic, which is a recent result of Zannier (Theorem 3.30). We will give a proof of this result in Section 3.9.

3.2 The continued fraction expansion of real numbers

In this section we review several classical definitions and results related to the continued fraction expansion of real numbers, and illustrate them by examples. A good general reference is Khinchin's book [Khi97].

— **3.2.** Let r be a real number. The continued fraction expansion of r is an expression, either finite or not, of the form

$$r = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \cdots}}}$$

where the a_n are integers, and are positive for $n \geq 1$. The continued fraction expansion of a given real number r can be obtained as follows. Denote by $\lfloor r \rfloor$ the integral part of r, that is, the largest integer which is smaller or equal to r, so that $0 \leq r - \lfloor r \rfloor < 1$ holds. Set $a_0 = \lfloor r \rfloor$ and $r_0 = r - a_0$, then $a_{n+1} = \lfloor r_n^{-1} \rfloor$ and $r_{n+1} = r_n^{-1} - a_{n+1}$. If ever $r_n = 0$, which happens if and only if r is a rational number, the procedure stops. The integers $a_0, a_1, \ldots$ are called *partial quotients*. As a matter of notation, we usually denote the continued fraction by

$$r = [a_0; a_1, a_2, a_3, \ldots]. \tag{3.2}$$

Given any finite or infinite sequence of integers $a_0, a_1, a_2 \ldots$, we define two new sequences $\{p_n\}$ and $\{q_n\}$ by setting[2]

$$\begin{cases} p_{n+1} = a_n p_n + p_{n-1}, & p_{-1} = 0 \quad \text{and} \quad p_0 = 1 \\ q_{n+1} = a_n q_n + q_{n-1}, & q_{-1} = 1 \quad \text{and} \quad q_0 = 0. \end{cases} \tag{3.3}$$

An elegant way of rewriting (3.3) is

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix}$$

from which we obtain the relation $p_n q_{n-1} - q_n p_{n-1} = (-1)^n$. In particular, p_n and q_n are coprime. We have for instance

$$\begin{array}{lll} p_0 = a_0 & p_1 = a_0 a_1 + 1 & p_2 = a_0 a_1 a_2 + a_0 + a_2 \\ q_0 = 1 & q_1 = a_1 & q_2 = a_1 a_2 + 1 \end{array}$$

We may look at p_n and q_n as elements of the ring of polynomials $\mathbb{Z}[a_0, a_1, \ldots]$. The equality

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_{n-1}] = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots \frac{\cdots}{\frac{1}{a_{n-1}}}}}$$

holds in the fraction field of $\mathbb{Z}[a_0, a_1, \ldots]$. In our concrete situation, the ratios p_n/q_n are just rational numbers, called *convergents*, and the meaning of equality (3.2) is that

$$\lim_{n \to \infty} \frac{p_n}{q_n} = r \tag{3.4}$$

holds.

[2]Several authors use shifted indices, so that their p_n are our p_{n+1}.

— **3.3.** The convergents p_n/q_n obtained from the continued fraction expansion of a real number r are the "best" rational approximations of r; this statement can be made precise in several different ways.

The convergents approximate r better than any other rational number with a smaller denominator: If p_n/q_n is a convergent (so it is automatically a reduced fraction), then the inequality

$$|p_n - q_n r| < |p - qr|$$

holds for all rational numbers p/q with $q \leq q_n$ and $p/q \neq p_n/q_n$. And viceversa if p/q is a rational number with the property that the inequality $|p - qr| < |p' - q'r|$ holds for all rational numbers p'/q' with $q' \leq q$ and $p'/q' \neq p/q$, then p/q is a convergent.

The convergents have also the property that they approximate the number r with an error very small compared to the denominator q_n:

$$\left| \frac{p_n}{q_n} - r \right| < \frac{1}{q_n^2}.$$

The converse of this statement holds up to a factor 2: If p/q is a rational number such that

$$\left| \frac{p}{q} - r \right| < \frac{1}{2q^2},$$

then p/q is a convergent of the continued fraction expansion of r.

Example 3.4. Let us compute the continued fraction expansion of $\sqrt{13}$. We have $3 < \sqrt{13} < 4$, so $a_0 = 3$ and $r_0 = \sqrt{13} - 3$. We continue with the algorithm, where at each step we rationalize the denominators:

$$\begin{aligned}
a_1 &= \left\lfloor \tfrac{1}{\sqrt{13}-3} \right\rfloor = \left\lfloor \tfrac{1}{4}(\sqrt{13}+3) \right\rfloor = 1 & \qquad r_1 &= \tfrac{1}{4}(\sqrt{13}+3) - 1 = \tfrac{1}{4}(\sqrt{13}-1) \\
a_2 &= \left\lfloor \tfrac{4}{\sqrt{13}-1} \right\rfloor = \left\lfloor \tfrac{1}{3}(\sqrt{13}+1) \right\rfloor = 1 & \qquad r_2 &= \tfrac{1}{3}(\sqrt{13}+1) - 1 = \tfrac{1}{3}(\sqrt{13}-2) \\
a_3 &= \left\lfloor \tfrac{3}{\sqrt{13}-2} \right\rfloor = \left\lfloor \tfrac{1}{3}(\sqrt{13}+2) \right\rfloor = 1 & \qquad r_3 &= \tfrac{1}{3}(\sqrt{13}+2) - 1 = \tfrac{1}{3}(\sqrt{13}-1) \\
a_4 &= \left\lfloor \tfrac{3}{\sqrt{13}-1} \right\rfloor = \left\lfloor \tfrac{1}{4}(\sqrt{13}+1) \right\rfloor = 1 & \qquad r_4 &= \tfrac{1}{4}(\sqrt{13}+1) - 1 = \tfrac{1}{4}(\sqrt{13}-3) \\
a_5 &= \left\lfloor \tfrac{4}{\sqrt{13}-3} \right\rfloor = \left\lfloor (\sqrt{13}+3) \right\rfloor = 6 & \qquad r_5 &= (\sqrt{13}+3) - 6 = \sqrt{13} - 3
\end{aligned}$$

We find $r_5 = r_0$, hence $a_6 = a_1$ and $r_6 = r_1$, and the pattern repeats. The continued fraction expansion of $\sqrt{13}$ is therefore given by

$$\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}]$$

where the bar indicates that the pattern of partial quotients $1, 1, 1, 1, 6$ repeats periodically. We compute a few convergents. Starting with $p_0 = a_0 = 3$ and $q_0 = 1$, we find

$$\frac{p_1}{q_1} = \frac{3}{1}, \quad \frac{p_2}{q_2} = \frac{4}{1}, \quad \frac{p_3}{q_3} = \frac{7}{2}, \quad \frac{p_4}{q_4} = \frac{11}{3}, \quad \frac{p_5}{q_5} = \frac{18}{5}, \quad \frac{p_6}{q_6} = \frac{119}{33}, \quad \frac{p_7}{q_7} = \frac{137}{38}, \quad \ldots$$

and, with the help of a machine

$$\frac{p_{101}}{q_{101}} = \frac{678757046537523807507515706001}{188253333451810715517247220820 0}$$

which yields about $65 \simeq \log_{10}(p_{101}) + \log_{10}(q_{101})$ correct decimals of $\sqrt{13}$. We point out that, from a computational point of view, continued fractions are not the optimal tool to approximate square roots (Newton's method for example is much faster).

Theorem 3.5 (Euler, Lagrange)**.** *Let r be a real number. The continued fraction expansion of r is eventually periodic if and only if r is an irrational algebraic number of degree* 2*.*

It was Euler's observation that real numbers with an eventually periodic continued fraction expansion satisfy a quadratic equation with integer coefficients, and Lagrange proved the converse by showing that there are only finitely many possible inner terms r_n – in Example 3.4 it is clear that inner terms are of the shape $\frac{1}{P}(\sqrt{13}+Q)$ for integers P, Q of bounded size. Determining the length of the period of the continued fraction expansion of a quadratic algebraic number is a difficult problem. Denoting by $l(d)$ the length of the period of the continued fraction expansion of $\sqrt{d}$ for a nonsquare integer $d > 0$, estimates such as

$$l(d) \leq \frac{7}{2\pi^2}\sqrt{d} \cdot \log(d) + O(\sqrt{d})$$

as $d \to \infty$ can be proven by making Lagrange's finiteness result effective, as done in [Coh77].

— **3.6.** We have explained in 3.3 how convergents of the continued fraction expansion of a real number r are the best possible approximations of r by rational numbers as one imposes an upper bound for the denominator. How well a real number r can be approximated by rational numbers with bounded denominator is measured by the *irrationality measure* $\mu(r)$ of r, also called *Liouville-Roth constant* of r, which is defined as follows. Let $M(r)$ be the set of those real numbers $\mu \in \mathbb{R}$ for which the inequality

$$0 < \left| r - \frac{p}{q} \right| < \frac{1}{q^\mu}$$

has infinitely many solutions in rational numbers p/q, where p and $q > 0$ are integers. The set $M(r)$ is not empty, for it contains the whole interval $(-\infty, 1)$. The irrationality measure of r is defined by $\mu(r) := \sup M(r)$ which is either a real number or the symbol $+\infty$. The most important theorem about irrationality measures is Roth's Theorem.

Theorem 3.7 (Roth, 1955)**.** *Let $r \in \mathbb{R}$ be an irrational, algebraic number. The irrationality measure of r is* 2*.*

— **3.8.** Roth's Theorem, also called the Thue-Siegel-Roth theorem, has a long history, starting with Dirichlet and Liouville. For a real number r, there are two possible regimes for $\mu(r)$:

$$\mu(r) = \begin{cases} = 1 & \text{if and only if } r \text{ is rational} \\ \geq 2 & \text{if } r \text{ is irrational (exactly equal to 2 if } r \text{ is algebraic).} \end{cases}$$

All algebraic irrational numbers satisfy $\mu(r) = 2$, but there exist also transcendental numbers with irrationality measure equal to two; this can be shown by a simple counting argument, but it is also known that $\mu(e) = 2$ holds. The numbers for which $\mu(r) = \infty$ are called *Liouville numbers*; an example of a Liouville number is Liouville's constant

$$L = \sum_{n=1}^{\infty} 10^{-n!} = 1.100010000000000000000000100\dots$$

which served as an explicit example of a transcendental number in 1850, about 40 years before Cantor's diagonal argument. The relation between continued fractions and irrationality measures, already established in Paragraph 3.3, is further illustrated by the following proposition ([Son04], Theorem 1).

Proposition 3.9. *Let r be a real number with continued fraction expansion $r = [a_0; a_1, a_2, \dots]$. The irrationality measure $\mu(r)$ of r is given by*

$$\mu(r) \;=\; 1 + \limsup_{n\to\infty} \frac{\log(q_{n+1})}{\log(q_n)} \;=\; 2 + \limsup_{n\to\infty} \frac{\log(a_n)}{\log(q_n)}$$

where p_n/q_n are the convergents of the continued fraction expansion of r.

Example 3.10. The continued fraction expansion of Liouville's constant starts with

$$\begin{aligned} L = [&0, 9, 11, 99, 1, 10, 9, 999999999999, 1, 8, 10, 1, 99, 11, 9,\\ &999999999999999999999999999999999999999999999999999999999999999999999999, \dots] \end{aligned}$$

and these extremely large terms continue to appear. For infinitely many n, the partial quotient a_{n+1} is much larger than q_n, which is a polynomial expression in $a_0, a_1, \dots a_n$.

3.3 Continued fractions in more general settings

One may think of several variants of continued fraction expansions, for real or complex numbers, or even in other fields such as the p-adic numbers. Continued fractions in p-adic numbers were studied by Mahler in [Mah34].

— **3.11.** Let us sum up what we needed in 3.2 in order to create a theory of continued fractions. First of all we need a topological field k, so that the limit of convergents (3.4) makes sense. Then we also need a notion of integral part and fractional part of elements of k. What we want is two subsets I and F of k, which satisfy the following properties:

1. For every $r \in k$ there exists a unique $i \in I$ satisfying $r - i \in F$.

2. The subfield $k_0 \subseteq k$ generated by elements of I is dense in k.

3. $r \in F, r \neq 0 \implies r^{-1} \notin F$.

We call integral part of r and denote by $\lfloor r \rfloor$ the unique element $i \in I$ satisfying $r - i \in F$. A sequence of partial quotients for $r \in k$ with respect to the chosen pair of sets (I, F) can be obtained in the usual way. Set $a_0 = \lfloor r \rfloor$ and $r_0 = r - a_0$, then $a_{n+1} = \lfloor r_n^{-1} \rfloor$ and $r_{n+1} = r_n^{-1} - a_{n+1}$. If some $r_n = 0$, then r belongs to the subfield of k generated by I, and the procedure stops. The sequence of partial quotients

$$[a_0; a_1, a_2, \dots]$$

satisfies $a_0 \in I$ and $a_n \in I_0 := \{\lfloor f^{-1} \rfloor \mid f \in F, f \neq 0\}$ for $n \geq 1$. Conditions (2) and (3) are necessary for the sequence of convergents of the so constructed continued fraction expansion to converge to r, but not sufficient. Condition (3) states that 0 is not an element of I_0. In order to guarantee continued fraction expansions to converge, one should probably replace (3) by a stronger condition which states that elements of I_0 are sufficiently far away from 0.

Example 3.12. Consider the field $k = \mathbb{R}$ with set of integral parts $I = \mathbb{Z}$, but with set of fractional parts $F = [-\frac{1}{2}, \frac{1}{2})$. The continued fraction expansion with respect to this choice will have positive or negative partial quotients $a_n \in \mathbb{Z}$ of absolute value ≥ 2. The reader may compute the continued fraction expansion of $\sqrt{13}$ with respect to this choice of fractional parts. Interestingly enough, one finds a periodic pattern, with period length 3, different from the period length 5 in the standard expansion that was given in Example 3.4.

$$\sqrt{13} = [4; \overline{-3, 2, 7}]$$

Here is a list of convergents:

$$4, \frac{11}{3}, \frac{18}{5}, \frac{137}{38}, \frac{393}{109}, \frac{649}{180}, \frac{4936}{1369}, \frac{14159}{3927}, \frac{23382}{6485}, \frac{177833}{49322}, \frac{510117}{141481}, \frac{842401}{233640}, \frac{6406924}{1776961}, \frac{18378371}{5097243}.$$

The numerators and denominators of the convergents p_n/q_n are solutions to $p_n^2 - 13q_n^2 = c$ where c is $3, 4, -1, -3, -4, 1$, depending on the congruence class of n modulo 6. In particular, we find the solutions

$$649^2 - 13 \cdot 180^2 = 1 \qquad 842401^2 - 13 \cdot 233640^2 = 1$$

of the Pell equation.

Example 3.13. Consider the field $k = \mathbb{C}$ with set of integral parts $I = \mathbb{Z}[i]$ and set of fractional parts $F = [-\frac{1}{2}, \frac{1}{2}) \times [-\frac{1}{2}, \frac{1}{2})i$. This choice yields a theory of continued fractions for complex numbers which extends the continued fractions for real numbers given in example 3.12. For example we have

$$\sqrt{2 + 3i} = [2 + i; \overline{-3 + i, 4 + 2i}]$$

where the square root is the one which is about $1.67415 + 0.895977i$. The first few convergents are

$$2 + i, \frac{17 + 9i}{10}, \frac{290 + 155i}{173}, \frac{1239663i}{740}, \frac{42358 + 22669i}{25301}, \frac{72407 + 38751i}{43250}, \frac{6188662 + 3312071i}{3696601},$$

but, somewhat disappointingly, numerators and denominators of these convergents do not solve the Pell equation for $d = 2 + 3i$. It was rather important that we chose F as we did, and not

$F = [0,1) \times [0,1)i$. With the latter choice, reciprocals of elements of F may have too small norms for continued fractions to converge. To see what goes wrong, consider with the latter choice for F the expansion of the 12-th root of unity $\exp(2\pi i/12)$. It is $[0; i, i, i, i, \ldots]$ and does not converge.

Example 3.14. Let $\mathbb{Q}_p$ denote the field of p-adic numbers. There is no canonical way to define the continued fractions in this context, as we do not have a canonical definition of "integral part". Our setup here is the same as Ruban's in [Rub70]. Declare the set of fractional parts to be $F = p\mathbb{Z}_p$, and the set of integral parts I to be the set of all sums

$$c_0 + c_1 p^{-1} + c_2 p^{-2} + \cdots + c_n p^{-n},$$

with $c_i \in \{0, 1, 2, \ldots, p-1\}$. Notice that also rational numbers may have infinite continued fraction expansions, for instance for $p = 3$ we find

$$\tfrac{1}{7} = [1; \tfrac{1}{3}, \tfrac{7}{3}, \tfrac{8}{3}, \tfrac{8}{3}, \tfrac{8}{3}, \tfrac{8}{3}, \ldots].$$

As a more elaborate example, let us compute the continued fraction expansion of $\sqrt{13}$ in $\mathbb{Q}_3$, where $\sqrt{13}$ is the unique element of $\mathbb{Z}_3$ whose square is 13 and whose class modulo 3 is 1 (and not 2). From $16^2 = 256 \equiv 13 \bmod 243 = 3^5$ we get

$$\sqrt{13} = 1 \cdot 3^0 + 2 \cdot 3^1 + 1 \cdot 3^2 + 0 \cdot 3^3 + 0 \cdot 3^4 + \cdots, \tag{3.5}$$

for some remainder in $3^5\mathbb{Z}_3$. So $a_0 = 1$ and $r_0 = \sqrt{13} - 1$. To compute the 3-adic expansion of r_0^{-1} we complete the square and use $4 \cdot 61 \equiv 1 \bmod 243$:

$$r_0^{-1} = \tfrac{1}{12}(\sqrt{13} + 1) = 2 \cdot 3^{-1} + 0 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 + 0 \cdot 3^3 + \cdots$$

From this expansion we read off $a_1 = 2 \cdot 3^{-1}$ and $r_1 = \frac{1}{12}(\sqrt{13} - 7)$, and proceed with calculating the 3-adic expansion of r_1^{-1} in the same fashion

$$r_1^{-1} = \tfrac{-1}{3}(\sqrt{13} + 7) = 1 \cdot 3^{-1} + 1 \cdot 3^0 + 0 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + \cdots$$

hence get $a_2 = \frac{4}{3}$. Next up we find

$$r_2^{-1} = \tfrac{1}{36}(\sqrt{13} - 11) = 2 \cdot 3^{-2} + 2 \cdot 3^{-1} + 0 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2 + \cdots$$

hence $a_3 = \frac{8}{9}$. So far we have computed

$$\sqrt{13} = [1; \tfrac{2}{3}, \tfrac{4}{3}, \tfrac{8}{9}, \ldots]$$

by hand. Here is a machine computation using Sage [S+09]. We start with

```
(1) sage: R=Zp(3, prec = 1000, print_mode = 'series')
(2) sage: A=sqrt(R(13))
```

so `A` is the square root of 13 in $\mathbb{Z}_3$ up to precision 3^{1000}. Printing `A` yields the first 999 terms of the series representation (3.5). To compute the first 100 terms in the continued fraction expansion, we use the following algorithm:

```
 (3) sage: n=100
 (4) sage: fraction=[]
 (5) sage: for i in range(n):
 (6) sage:     v=A.valuation()
 (7) sage:     B=A/3^v
 (8) sage:     C=B.residue(1-v)
 (9) sage:     D=int(C)
(10) sage:     DD=D*3^v
(11) sage:     print DD
(12) sage:     fraction = fraction + [[D , v]]
(13) sage:     A=1/(A-R(D)*3^v)
```

It works as follows. In lines (3) and (4) we choose the number `n=100` of iteration steps, and create an empty list named `fraction`. We need this list only later to compute convergents. Lines (6) to (13) are then repeated `n` times. In line (6) we assign to `v` the 3-adic valuation of `A`, which is zero or a negative integer, and in line (7) scale `A` to a 3-adic integer `B` of valuation 0. Then we define `C` to be the residue modulo 3^{-v+1}, which encodes the first $-v+1$ coefficients in the series expansion of `A`. Sage [S$^+$09] sees `C` as an element of $\mathbb{Z}/3^{-v+1}\mathbb{Z}$, and we need to reconvert `C` to an integer `D` and scale back by the power of 3 we divided in line (7). Now `DD` is the integral part of the series expansion of `A`, and we print it. In line (12) we add the pair (`D,V`) to the list `fraction` for later use. Finally, in line (13) we subtract from `A` its integral part and invert. Here is the output:

$$\begin{array}{cccccccccccccccccccc}
1 & \frac{2}{3} & \frac{4}{3} & \frac{8}{9} & \frac{5}{3} & \frac{4}{3} & \frac{5}{9} & \frac{2}{3} & \frac{5}{3} & \frac{8}{3} & \frac{16}{9} & \frac{7}{3} & \frac{5}{9} & \frac{76}{27} & \frac{8}{3} & \frac{8}{3} & \frac{1}{3} & \frac{7}{3} & \frac{43}{27} & \frac{7}{3} \\
\frac{64}{27} & \frac{536}{243} & \frac{8}{3} & \frac{5}{3} & \frac{8}{3} & \frac{4}{3} & \frac{4}{9} & \frac{26}{9} & \frac{4}{3} & \frac{25}{9} & \frac{50}{243} & \frac{1}{3} & \frac{5}{3} & \frac{1}{9} & \frac{5}{3} & \frac{25}{9} & \frac{8}{3} & \frac{7}{3} & \frac{1}{3} & \frac{1}{3} \\
\frac{4}{3} & \frac{2}{3} & \frac{7}{3} & \frac{58}{27} & \frac{8}{3} & \frac{5}{3} & \frac{4}{3} & \frac{2}{3} & \frac{1}{27} & \frac{7}{9} & \frac{4}{9} & \frac{4}{3} & \frac{5}{3} & \frac{34}{27} & \frac{2}{3} & \frac{5}{3} & \frac{5}{3} & \frac{7}{3} & \frac{16}{9} & \frac{4}{9} \\
\frac{2}{3} & \frac{73}{27} & \frac{8}{3} & \frac{4}{3} & \frac{43}{27} & \frac{7}{3} & \frac{2}{3} & \frac{7}{3} & \frac{2}{3} & \frac{203}{81} & \frac{5}{3} & \frac{10}{9} & \frac{10}{9} & \frac{7}{3} & \frac{5}{3} & \frac{8}{9} & \frac{59}{27} & \frac{2}{3} & \frac{5}{3} & \frac{8}{3} \\
\frac{8}{3} & \frac{14}{9} & \frac{2}{3} & \frac{23}{9} & \frac{23}{9} & \frac{2}{3} & \frac{7}{3} & \frac{20}{9} & \frac{2}{3} & \frac{2}{3} & \frac{8}{3} & \frac{4}{3} & \frac{5}{9} & \frac{2}{3} & \frac{7}{3} & \frac{1}{3} & \frac{20}{9} & \frac{5}{3} & \frac{4}{3} & \frac{569}{243}
\end{array}$$

The first fourteen convergents we get from our computation are:

$$1, \tfrac{5}{2}, \tfrac{29}{17}, \tfrac{367}{190}, \tfrac{2618}{1409}, \tfrac{13775}{7346}, \tfrac{139561}{74773}, \tfrac{651047}{347888}, \tfrac{4511284}{2412397}, \tfrac{41949695}{22430168}, \tfrac{792999788}{424017407}, \tfrac{6683640281}{3573736385}, \tfrac{54829195681}{29317151914}, \tfrac{5791143460039}{3096521487019}$$

The last error term here is

$$\sqrt{13} - \tfrac{5791143460039}{3096521487019} = 1 \cdot 3^{39} + 2 \cdot 3^{41} + 2 \cdot 3^{42} + 2 \cdot 3^{43} + 2 \cdot 3^{44} + 1 \cdot 3^{45} + 1 \cdot 3^{46} + \cdots$$

which is very close to $\sqrt{13}$ in $\mathbb{Z}_3$. To compute the convergents, we used the following algorithm in Sage [S$^+$09]: After resetting the correct value for `A` in line (14), it computes the convergents using the Euler-Wallis formulas (3.3), and prints the valuation of the difference $\sqrt{13} - p_n/q_n$.

```
sage: A=sqrt(R(13))
sage: p0=R(fraction[0][0])*3^fraction[0][1]
sage: q0=1
sage: q1=R(fraction[1][0])*3^fraction[1][1]
sage: p1=p0*q1+1
sage: for i in range(2,n):
sage:     an=R(fraction[i][0])*3^fraction[i][1]
sage:     pn=an*p1+p0
sage:     qn=an*q1+q0
sage:     p0=p1
sage:     q0=q1
sage:     p1=pn
sage:     q1=qn
sage:     error= A-pn/qn
sage:     print error.valuation()
```

The output reads

$$6, 9, 11, 14, 17, 19, 21, 24, 27, 30, 35, 39, \dots, 309$$

which gives us a pretty good idea of what the speed of convergence might be. However the matter of the convergence of Ruban's continued fraction in $\mathbb{Q}_p$ is not a simple one: unlike the real case, it is not true in general that the convergents always provide good approximations.

It is clear that if $r \in \mathbb{Q}_p$ admits a periodic continued fraction expansion, then r must be a quadratic algebraic number over $\mathbb{Q}$. It is easy to engineer examples in which the continued fraction expansion is periodic. For instance

$$\tfrac{1}{2p}(-1 + \sqrt{4p^2 + 1}) = [0; \tfrac{1}{p}, \tfrac{1}{p}, \tfrac{1}{p}, \tfrac{1}{p}, \dots]$$

in $\mathbb{Q}_p$ is periodic and indeed the right hand side solves the following quadratic equation

$$r = \frac{1}{\frac{1}{p} + r}.$$

In a very recent work [CVZ18], Capuano, Veneziano and Zannier found an effective criterion to detect periodicity of Ruban's continued fraction of quadratic irrational numbers. In particular, their criterion shows that $\sqrt{13}$ has not periodic continued fraction in $\mathbb{Q}_3$.

Example 3.15. Let $k((s))$ be the field of Laurent series in the variable s and coefficients in a field k. Let us declare the set of fractional parts to be Taylor series with zero constant term, and the set of integral parts to be polynomials in s^{-1}. This choice yields a theory of continued fractions for Laurent series. It is the topic of the next section, except that we shall prefer to work with the variable t^{-1} in place of s, so that integral parts become polynomials in t.

3.4 The continued fraction expansion of Laurent series

In this section we describe the continued fraction expansion of Laurent series, and show some analogies with continued fraction expansions of real numbers. Later we will be interested in the continued fraction expansion of square roots of polynomials.

— **3.16.** Let k be a field, and write $k(\!(t^{-1})\!)$ for the field of Laurent series in the variable t^{-1} and coefficients in k. An element of $k(\!(t^{-1})\!)$ is a formal series

$$f(t) = \sum_{n=-\infty}^{n_0} c_n t^n$$

with $c_{n_0} \neq 0$, and we call $\nu(f) := -n_0 \in \mathbb{Z}$ the valuation of f. For $f = 0$ we set $\nu(f) = \infty$. The sets $\{f \in k(\!(t^{-1})\!) \mid \nu(f) \geq n\}$ form a fundamental system of neighbourhoods for a topology on $k(\!(t^{-1})\!)$. Let us write

$$\lfloor f \rfloor = \sum_{n=0}^{n_0} c_n t^n$$

for the *integral* or *polynomial part* of f. We obtain the continued fraction expansion of a Laurent series $f \in k(\!(t)\!)$ as follows. Set $a_0 = \lfloor f \rfloor$ and $f_0(t) = f(t) - a_0(t)$, and then

$$a_{n+1}(t) = \lfloor f_n(t)^{-1} \rfloor \qquad \text{and} \qquad f_{n+1}(t) = f_n(t)^{-1} - a_{n+1}(t)$$

recursively for $n \geq 1$. We obtain the obtain the continued fraction of f

$$f(t) = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots}} = [a_0; a_1, a_2, \ldots] \tag{3.6}$$

with $a_n \in k[t]$ for every n. The *convergents* p_n/q_n of the sequence of polynomials $a_0, a_1, \ldots$ are given, as in the real case, by the recurrence formula (3.3). The meaning of equation (3.6) is that

$$f(t) = \lim_{n \to \infty} \frac{p_n(t)}{q_n(t)}$$

holds, for the topology on $k(\!(t^{-1})\!)$ induced by the valuation ν.

Example 3.17. Let us compute a few terms of the continued fraction expansion of the exponential function. The polynomial part of

$$\exp(t^{-1}) = 1 + t^{-1} + \tfrac{1}{2}t^{-2} + \tfrac{1}{3!}t^{-3} + \tfrac{1}{4!}t^{-4} + \cdots$$

is the constant polynomial $a_0 = 1$. Subtract a_0 from $\exp(t^{-1})$, invert and write the resulting Laurent series:

$$\frac{1}{\exp(t^{-1}) - 1} = t - \frac{1}{2} + \frac{t^{-1}}{12} - \frac{t^{-3}}{720} + \frac{t^{-5}}{30240} - \frac{t^{-7}}{1209600} + \cdots$$

The polynomial part is $a_1 = t - \frac{1}{2}$. Again, subtract a_1, invert and write the Laurent series:

$$\frac{1}{\frac{1}{\exp(t^{-1})-1} - t + \frac{1}{2}} = \frac{\exp(t^{-1}) - 1}{\frac{1}{2} + t - (t - \frac{1}{2})\exp(t^{-1})} = 12t + \frac{t^{-1}}{5} - \frac{t^{-3}}{700} + \frac{t^{-5}}{63000} - \frac{37t^{-7}}{194040000} + \cdots$$

The integral part, which is the next partial quotient, is thus $a_2 = 12t$. The following table was calculated for us by Olaf Merkert:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$a_n(t)$	1	$t - \frac{1}{2}$	$12t$	$5t$	$28t$	$9t$	$44t$	$13t$	$60t$	$17t$	$76t$	$21t$	$92t$
	13	14	15	16	17	18	19	20	21	22	23	24	25
	$25t$	$108t$	$29t$	$124t$	$33t$	$140t$	$37t$	$156t$	$41t$	$172t$	$45t$	$188t$	$49t$
	26	27	28	29	30								
	$204t$	$53t$	$220t$	$57t$	$236t$								

We observe, and once we know what we are looking for, it is not hard to prove either, that for $n \geq 2$ the partial fraction a_n is equal to $(2n-1)t$ for odd n, and $4(2n-1)t$ for even n. Let us compute a few convergents:

$$1, \quad \frac{\frac{1}{2} + t}{-\frac{1}{2} + t}, \quad \frac{1 + 6t + 12t^2}{1 - 6t + 12t^2}, \quad \frac{\frac{1}{2} + 6t + 30t^2 + 60t^3}{-\frac{1}{2} + 6t - 30t^2 + 60t^3}, \quad \frac{1 + 20t + 180t^2 + 840t^3 + 1680t^4}{1 - 20t + 180t^2 - 840t^3 + 1680t^4}$$

The Taylor series expansion at infinity of the convergent of degree 2 reads

$$1 + t^{-1} + \frac{t^{-2}}{2} + \frac{t^{-3}}{6} + \frac{t^{-4}}{24} + \frac{t^{-5}}{144} - \frac{t^{-7}}{1728} - \frac{t^{-8}}{3456} - \frac{t^{-9}}{10368} - \frac{t^{-10}}{41472} + \cdots$$

hence agrees with $\exp(t^{-1})$ up to order $O(t^{-5})$. These are the so called *Padé-approximations* of the function $\exp(t^{-1})$.

— **3.18.** We may try to link the irrationality measure of a Laurent series $f \in k(\!(t^{-1})\!)$ with the degrees of the partial quotients a_n in the continued fraction expansion

$$f = [a_0; a_1, a_2, a_3, \ldots]$$

as we did in Proposition 3.9. In view of the recurrence (3.3) and the fact that $\deg(a_n) > 0$ for all $n > 0$, the equalities

$$\begin{aligned} \deg p_{n+1} &= \deg a_n + \deg p_n \\ \deg q_{n+1} &= \deg a_n + \deg q_n \end{aligned}$$

hold, which make it easy to compute the degrees of convergents. The degrees of the partial quotients a_n are connected to the ranks of the so-called *Hankel matrices*, which are associated to the Laurent coefficients of f. In fact, a partial quotient of large degree amounts to the vanishing of several determinants in these matrices. The convergents provide *Padé-approximations* to f, which are of importance in transcendence theory and Diophantine approximation.

— **3.19.** Let us recapitulate briefly what Padé-approximations are. In a standard setup, Padé-approximations are associated with power series in a variable t instead of Laurent series in t^{-1}. Let

$$f(t) = \sum_{n=0}^{\infty} c_n t^n \qquad \in k[\![t]\!]$$

be a formal power series, and pick two integers $m \geq 0$ and $n \geq 1$. The Padé-approximant of f of order (m, n) is the rational function

$$R(t) = \frac{p(t)}{q(t)} = \frac{a_0 + a_1 t + a_2 t^2 + \cdots + a_m t^m}{1 + b_1 t + b_2 t^2 + \cdots + b_n t^n}$$

which agrees with f up to order $m + n$. The requirement $q(0) = 1$ determines p and q uniquely. There exist several efficient algorithms to compute Padé-approximants. From an elementary point of view, one has to solve the linear system of $m + n + 1$ equations

$$k\text{-th Taylor coefficient of } q(t)f(t) = k\text{-th Taylor coefficient of } p(t)$$

for $0 \leq k \leq m + n$ in the $m + n + 1$ variables $a_0, \ldots, a_m, b_1, \ldots, b_n$, but this is computationally not very efficient. Now if f is a Laurent series in t^{-1} rather than a Taylor series in t, say

$$f(t) = \sum_{n=-\infty}^{n_0} c_n t^n \qquad \in k(\!(t)\!)$$

we can still look for rational functions $R = p/q$ with $\deg p \leq m$ and $\deg q \leq n$ such that $\nu(f - R)$ is as large as possible. Comparing to the Taylor series case, the difference is that we don't need to prescribe a bound on the degree of the nominator p anymore - there is only so much one can do if $\deg q \leq n$ is imposed. We may thus define the n-th Padé-approximant of $f \in k(\!(t)\!)$ as the rational function $R = p/q$ with $\deg q \leq n$ such that $\nu(f - R)$ is maximal. The next proposition is an analogue of the statements in 3.3.

Proposition 3.20. *Let $f \in k(\!(t^{-1})\!)$ be a Laurent series in the variable t^{-1}, and let $p(t)$ and $q(t)$ be coprime polynomials. Then $p(t) - q(t)f(t) = O(t^{-\deg q - 1})$ holds if and only if p/q is a convergent of the continued fraction expansion of f.*

Proof. See [PT00], Proposition 2.1. □

— **3.21.** The classical theorem of Roth, which we recalled in 3.7, has a function field analogue, due to Saburô Uchiyama. For a Laurent series $f \in k(\!(t^{-1})\!)$ we may consider the set $M(f)$ of those real numbers μ for which the inequality

$$\nu\Big(f - \frac{p}{q}\Big) > \mu \cdot \deg(q)$$

has infinitely many solutions in rational functions $p/q \in k(t)$, where p and q are polynomials. If we define, as Uchiyama does, an absolute value for Laurent series by setting $|f| := c^{-\nu(f)}$ for some fixed real constant $c > 1$, then the above inequality becomes

$$\Big| f - \frac{p}{q} \Big| < \frac{1}{|q|^{\mu}},$$

similar to the inequality in 3.6. Again, $M(f)$ contains $(-\infty, 1)$, and we define the irrationality measure of f to be $\mu(f) := \sup M(f)$. Then [Uch61a, Theorem 3(i)] states that if f is not rational, then $\mu(f) \geq 2$ holds, while [Uch61a, Theorem 2(i)] is an analogue of Roth's theorem.

Theorem 3.22 (Uchiyama)**.** *Let k be a field of characteristic zero and let $f \in k(\!(t^{-1})\!)$ be algebraic but not rational over $k(t)$. Then the irrationality measure of f is 2.*

— **3.23.** Let k be a field of characteristic zero and let $f \in k(\!(t^{-1})\!)$ be algebraic but not rational over $k(t)$. Uchiyama's Theorem states that for any $\epsilon > 0$, the inequality

$$\nu\Big(f - \frac{p}{q}\Big) > (2+\epsilon) \cdot \deg(q)$$

has only finitely many solutions $p/q \in k(t)$. The possible periodic behaviour of the degrees of the partial quotients in the continued fraction expansion of f is related to a stronger version of Uchiyama's theorem, namely a uniform version with $2\deg q + O(1)$ in place of $(2+\epsilon)\deg q$. Such an estimate should follow for algebraic functions of degree ≤ 3 over $\mathbb{C}(t)$ from Min Ru's effective version of Uchiyama's theorem (see [Ru00] extending work of J. Wang [Wan96]).

— **3.24.** Analogously to the irrationality measure for real numbers, we can express the irrationality measure of a Laurent series in terms of its continued fraction expansion. With notations of 3.18, the equalities

$$\mu(f) = 1 + \limsup_{n\to\infty} \frac{\deg q_{n+1}}{\deg q_n} = 2 + \limsup_{n\to\infty} \frac{\deg a_{n+1}}{\deg q_n}$$

hold when f has an infinite continued fraction expansion.

Example 3.25. Let us look at the function field analogue of Liouville's constant, which we introduced in Example 3.10. Set

$$L(t) = \sum_{n=1}^{\infty} t^{-n!} = t^{-1} + t^{-2} + t^{-6} + t^{-24} + t^{-120} + t^{-720} + \cdots$$

Power series like this go under the name of *lacunary series*, of which Jacobi's theta series is another example. The continued fraction expansion of L, again computed by Merkert, reads

$$\begin{array}{lllllllllll}
a_0 & = & 0 & & & & & & & & \\
a_1 & = & t-1 & a_{11} & = & -t+1 & a_{21} & = & -t^2 & a_{31} & = & t-1 \\
a_2 & = & t+1 & a_{12} & = & -t^{72} & a_{22} & = & -t-1 & a_{32} & = & t+1 \\
a_3 & = & t^2 & a_{13} & = & t-1 & a_{23} & = & -t+1 & a_{33} & = & -t^2 \\
a_4 & = & -t-1 & a_{14} & = & t+1 & a_{24} & = & -t^{480} & a_{34} & = & -t-1 \\
a_5 & = & -t+1 & a_{15} & = & t^2 & a_{25} & = & t-1 & a_{35} & = & -t+1 \\
a_6 & = & -t^{12} & a_{16} & = & -t-1 & a_{26} & = & t+1 & a_{36} & = & t^{72} \\
a_7 & = & t-1 & a_{17} & = & -t+1 & a_{27} & = & t^2 & a_{37} & = & t-1 \\
a_8 & = & t+1 & a_{18} & = & t^{12} & a_{28} & = & -t-1 & a_{38} & = & t+1 \\
a_9 & = & -t^2 & a_{19} & = & t-1 & a_{29} & = & -t+1 & a_{39} & = & t^2 \\
a_{10} & = & -t-1 & a_{20} & = & t+1 & a_{30} & = & -t^{12} & a_{40} & = & -t-1
\end{array}$$

and we observe the sporadic large terms a_6, a_{24} whose degree is much larger than the degrees of all previous terms combined. It seems safe to conjecture that $\mu(L) = \infty$.

3.5 Pell equation in polynomials

In this section we take a closer look at the continued fraction expansion of $f(t) = \sqrt{D(t)}$, viewed as a Laurent series in $s = t^{-1}$. As in the case of continued fraction expansions of real numbers, the behaviour of the continued fraction expansion of $\sqrt{D(t)}$ is related to the solvability of the Pell equation $x(t)^2 - D(t)y(t)^2 = 1$.

Definition 3.26. Let k be a field, and let $D(t) \in k[t]$ be a nonconstant polynomial. We say that D is *Pellian* if the Pell equation

$$x(t)^2 - D(t)y(t)^2 = 1 \tag{3.7}$$

has a solution $x(t), y(t) \in k[t]$, with $y \neq 0$.

— **3.27.** The Pell equation is solved by $x = \pm 1$ and $y = 0$. We call this the trivial solution. The notion of Pellianity may depend on the arithmetic of the ground field k. We will often stick to algebraically closed fields, or just to $k = \mathbb{C}$. A polynomial $D(t) \in k[t]$ is Pellian if and only if the polynomial $cD(at+b)$ is Pellian for some $a, c \in k^*$ and $b \in k$. Polynomials of odd degree are never Pellian. The link between the polynomial Pell equation and continued fractions is given by Abel's Theorem 3.1, stated in the introduction. It says that D is Pellian if and only if the continued fraction expansion of $\sqrt{D(t)}$ is eventually periodic.

Example 3.28. Let us compute the continued fraction expansion of the square root of the polynomial $D(t) = t^2 + 1$. Set $s = \frac{1}{t}$. The Laurent series[3]

$$\sqrt{D(s)} = s^{-1}\sqrt{1+s^2} = s^{-1} + \frac{s}{2} - \frac{s^3}{8} + \frac{s^5}{16} - \frac{5s^7}{128} + \frac{7s^9}{256} - \frac{21s^{11}}{1024} + \cdots$$

has polynomial part $a_0 = s^{-1} = t$. For the next step, we have to compute the Laurent expansion of $(\sqrt{D(s)} - a_0)^{-1}$:

$$(\sqrt{D(s)} - s^{-1})^{-1} = 2s^{-1} + \frac{s}{2} - \frac{s^3}{8} + \frac{s^5}{16} - \frac{5s^7}{128} + \frac{7s^9}{256} - \frac{21s^{11}}{1024} + \cdots .$$

We find $a_1 = 2t$. The remainder $(\sqrt{D(s)} - s^{-1})^{-1} - 2s^{-2}$ is the same as the one obtained in the previous step, and the continued fraction expansion of $\sqrt{D(t)}$ is thus periodic.

$$\sqrt{D(t)} = [t; 2t, 2t, 2t, \ldots]$$

To justify this properly, set $h(t) = \sqrt{D(t)} - t$. We need to show that $h(t)^{-1} - 2t = h(t)$ holds, but this is immediate: complete the square in the denominator in the left hand side

$$\frac{1}{\sqrt{t^2+1} - t} - 2t = \sqrt{t^2+1} - t,$$

[3]Such a Laurent expansion would not exist if D had an odd degree, because then the two roots of $D(t)$ would be interchanged by monodromy around ∞. In other words, if $D(t)$ has odd degree $< 2d-1$, then the polynomial $s^{2d}D(s)$ has a simple zero at $s = 0$, hence $s^d\sqrt{D(s)}$ does not define an analytic continuation around $s = 0$.

and notice that the fact that both sides are equal is all but Euler's identity (3.1). Therefore, this example is an illustration of Abel's Theorem 3.1. As a corollary, we find the continued fraction expansion of $\sqrt{n^2+1}$ for all integers (or even that of $\frac{1}{2}+\sqrt{n^2+1}$ for half-integers) n; for example:

$$\sqrt{101} = 10 + \cfrac{1}{20 + \cfrac{1}{20+\cfrac{1}{20+\cfrac{1}{20+\cdots}}}}$$

Example 3.29. To give a nonexample to Abel's Theorem 3.1, let us examine the continued fraction expansion of the square root of the polynomial $D(t) = t^6 + 2t^3 + t + 1$. The Laurent series of $\sqrt{D(t)}$ around $t = \infty$ (same procedure as in the previous example) reads

$$t^3+1+\frac{t^{-2}}{2}-\frac{t^{-5}}{2}-\frac{t^{-7}}{8}+\frac{t^{-8}}{2}+\frac{3t^{-10}}{8}-\frac{t^{-11}}{2}+\frac{t^{-12}}{16}-\frac{3t^{-13}}{4}+\frac{t^{-14}}{2}-\frac{5t^{-15}}{16}+\frac{5t^{-16}}{4}-\frac{69t^{-17}}{128}+\cdots$$

and we calculate $a_0, a_1, \ldots$ just as before. Here is the list $a_0, a_1, \ldots a_{13}$ provided by Merkert:

$$\begin{aligned}
a_0 &= t^3+1\\
a_1 &= 2t^2\\
a_2 &= \tfrac{1}{2}t\\
a_3 &= -8t\\
a_4 &= \tfrac{-1}{2}t+2\\
a_5 &= \tfrac{-1}{8}t-\tfrac{65}{128}\\
a_6 &= -2048t-8064\\
a_7 &= \tfrac{-1}{65536}t+\tfrac{3}{32768}\\
a_8 &= \tfrac{524288}{33}t+\tfrac{35651584}{1089}\\
a_9 &= \tfrac{35937}{4259840}t-\tfrac{4886343}{138444800}\\
a_{10} &= \tfrac{562432000}{81828549}t+\tfrac{52597667200}{1882056627}\\
a_{11} &= \tfrac{-129861907263}{204068345000}t-\tfrac{161124749894097}{4665818640080000}\\
a_{12} &= \tfrac{52089490911518125}{8659797998530734}t+\tfrac{740122772124315125 0}{18830730747805081083}\\
a_{13} &= \tfrac{727954204641815978933 04}{21921367399948743484062 5}t-\tfrac{4354274674005459232096488 96}{6455842699284904956056406 25}
\end{aligned}$$

This suggests that a_n is of degree 1, but that the height of the coefficients of a_n tends to $+\infty$ as $n \to \infty$. In particular, the sequence of polynomials $a_1, a_0, a_2, \ldots$ is not periodic. How to show directly that the Pell equation

$$x(t)^2 - (t^6 + 2t^3 + t + 1)y(t)^2 = 1$$

has no nontrivial solution? See exercise 3.44, 2. below.

Although the periodicity of the continued fraction for $\sqrt{D(t)}$ is a very "rare" phenomenon, some periodicity survives in full generality. Indeed, we have the following:

Theorem 3.30 (Theorem 1.1 [Zan16])**.** *Let k be an algebraically closed field of characteristic 0. Let $D \in k(t)$ be a polynomial of even degree, and let*

$$\sqrt{D(t)} = [a_0; a_1, a_2, a_3, \ldots]$$

be its continued fraction expansion. The sequence $\deg(a_0), \deg(a_1), \deg(a_2), \deg(a_3), \ldots$ *is eventually periodic.*

This analogue of Lagrange's theorem for the polynomial case seems not to have been noticed until now, as the most common behaviour, which can be seen in many examples, is that all the degrees are equal to 1 or eventually constant. In particular, when $d \leq 3$ (or when the genus of the curve given by $u^2 = D(t)$ is 0), it may be seen that $\deg a_n$ is eventually constant in the non-Pellian case. More specifically, one can prove the following:

Proposition 3.31. *If $d \leq 3$ or the geometric genus is 0 (even if D is non-squarefree), either $D(t)$ is Pellian or there are only finitely many partial quotients with* $\deg a_n > 1$.

A proof of this, in the special case $D(t) = t^2(t^2 - 1)$, can be found in [Zan16, Example 4.2]. We also point out that, if $d \geq 4$, this is not true anymore, as the following example (found by Merkert, see [Mer16]) shows.

Example 3.32. The polynomial $D(t) = t^8 - t^7 - (3/4)t^6 + (7/2)t^5 - (21/4)t^4 + (7/2)t^3 - (3/4)t^2 - t + 1$ yields infinitely many partial quotients of degrees 1 and 2, with the periodic pattern of degrees $4, 1, 1, 2, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1, 1, 1, 1, 1, 1, 1, 1, 2, 1, \ldots$.

— **3.33.** We shall prove Theorem 3.30 in Section 3.9. It is not clear for which algebraic functions the sequence of degrees of partial quotients is periodic. The phenomenon seems not to be limited to square roots, for example the convergents of the continued fraction expansion at infinity of $\sqrt[4]{t^4 + 3}$ are

$$\begin{array}{rclrclrclrcl}
a_0 & = & t & & & & & & & & & \\
a_1 & = & \frac{4}{3}t^3 & a_{11} & = & \frac{9196}{1989}t^3 & a_{21} & = & \frac{23896908}{3739405}t^3 & a_{31} & = & \frac{115963743148}{14934083745}t^3 \\
a_2 & = & \frac{2}{3}t & a_{12} & = & \frac{1326}{4807}t & a_{22} & = & \frac{7478810}{36698823}t & a_{32} & = & \frac{1422293690}{8416723293}t \\
a_3 & = & \frac{12}{5}t^3 & a_{13} & = & \frac{19228}{3825}t^3 & a_{23} & = & \frac{375143524}{56091075}t^3 & a_{33} & = & \frac{370335824892}{46224544925}t^3 \\
a_4 & = & \frac{10}{21}t & a_{14} & = & \frac{11050}{43263}t & a_{24} & = & \frac{37394050}{191649409}t & a_{34} & = & \frac{92449089850}{563920460631}t \\
a_5 & = & \frac{28}{9}t^3 & a_{15} & = & \frac{173052}{32045}t^3 & a_{25} & = & \frac{109513948}{15705501}t^3 & a_{35} & = & \frac{76279096124}{9244908985}t^3 \\
a_6 & = & \frac{30}{77}t & a_{16} & = & \frac{320450}{1341153}t & a_{26} & = & \frac{15397550}{82135461}t & a_{36} & = & \frac{92449089850}{580265981229}t \\
a_7 & = & \frac{2156}{585}t^3 & a_{17} & = & \frac{54188}{9425}t^3 & a_{27} & = & \frac{2956876596}{408035075}t^3 & a_{37} & = & \frac{773687974972}{91199777825}t^3 \\
a_8 & = & \frac{26}{77}t & a_{18} & = & \frac{64090}{284487}t & a_{28} & = & \frac{163214030}{903490071}t & a_{38} & = & \frac{269951342362}{1740797943687}t \\
a_9 & = & \frac{924}{221}t^3 & a_{19} & = & \frac{7207004}{1185665}t^3 & a_{29} & = & \frac{63402812}{8442105}t^3 & a_{39} & = & \frac{633017434068}{72679207559}t^3 \\
a_{10} & = & \frac{442}{1463}t & a_{20} & = & \frac{182410}{853461}t & a_{30} & = & \frac{163214030}{935191477}t & a_{40} & = & \frac{1889659396534}{12502094322843}t
\end{array}$$

and their degrees clearly show a periodic pattern.

— **3.34.** As in the arithmetic situation, the solutions of the polynomial Pell equation form a group. We can identify it with a subgroup of the multiplicative group of the field $k(t)[u]/\langle u^2-D\rangle$ by associating $(x,y)\mapsto x+yu$. It can be shown that the group of solutions of the Pell equation is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ in the non-Pellian case, and to $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}$ in the Pellian case. To check this, show that all solutions are generated by a solution of minimal degree.

— **3.35.** Let D be a nonsquare polynomial of even degree $2d$, and set $\sqrt{D}=[a_0;a_1,a_2,\ldots]$. It can be shown that $1\le \deg a_n\le d$ holds for all n. The upper bound $\deg a_n = d$ holds for some $n>0$ if and only if D is Pellian; if this is the case, then such values of n form an arithmetic progression. On the other hand, if D is squarefree and not Pellian then the tighter upper bound $\deg a_n\le d/2$ holds for all n big enough (see [Zan16], Theorem 1.3 and the paragraph above it for details and a more precise statement).

— **3.36.** Another interesting line of inquiry concerns the heights of $a_n(t)$, $p_n(t)$, $q_n(t)$ over $\overline{\mathbb{Q}}$. The height of a nonzero polynomial $f\in\overline{\mathbb{Q}}[t]$, denoted $h(f)$, is the usual projective absolute (logarithmic) height of the vector of the coefficients. The affine height of f is the affine height of the same vector; it is denoted by $h_a(f)$. It can be shown that when D is not Pellian then the heights of the q_n grow quadratically in terms of n: $h(q_n)\gg n^2$; this follows from a more general theorem of Bombieri-Cohen [BC97], but can also be proved directly. For the partial quotients the following theorem ([Zan16, Theorem 1.5]) holds.

Theorem 3.37. *Suppose that $D(t)\in\overline{\mathbb{Q}}\,[t]$ is squarefree and non-Pellian. Then $h(a_n)\ll n^2$. Also, there exists an integer $M=M_D$ such that*

$$\max\{h_a(a_{n-s})\mid\ 0\le s\le M\}\ \gg n^2$$

holds for large n.

We remark that this theorem cannot be recovered easily from the bounds on q_n and the recurrence relation satisfied by the q_n and the a_n and requires and independent proof.

— **3.38.** A question of McMullen [McM09] asks whether every real quadratic field $\mathbb{Q}(\sqrt{d})$ contains infinitely many periodic continued fractions $x=[\overline{a_0,a_1,\ldots}]$ such that $a_i\in\{1,2\}$ for all $i=1,2,\ldots$. In her PhD thesis [Mal16], Malagoli proved a function field analogue of this question:

Theorem 3.39 (Theorem 7 [Mal16])**.** *Let k be a number field; then, for every non-square polynomial $D\in k(t)$ of even degree, not a square in $k[t]$ and with leading coefficient which is a square in k, there exists a polynomial $f\in k[t]$ such that the partial quotients of $f\sqrt{D}$ (except possibly for finitely many of them) have degree ≤ 1.*

The proof of this theorem relies on the study of zeroes of the denominators $q_n(t)$ of the partial quotients, which appear infinitely often. This is of interest if we want to specialise t to an element of $\overline{\mathbb{Q}}$. In this context, Zannier proved the following result:

Theorem 3.40 (Theorem 1.7 [Zan16]). *Let k be a number field and let $D \in k[t]$ be a polynomial of even degree. Then, for each $l \in \mathbb{R}$ there are only finitely many $\theta \in \overline{\mathbb{Q}}$ of degree $\leq l$ over k which are common zeros of infinitely many $q_n(t)$.*

We point out that the proof of Malagoli's theorem deals also with the case of non-squarefree $D(t)$ which complicates (also conceptually) the proofs.

— **3.41.** Another question which can be investigated regards how prime factors arise in denominators of polynomial continued fractions. This is strongly related to the problem of reducing polynomial continued fractions modulo a prime. In his thesis [Mer16], Merkert studied this problem for the continued fraction of $\sqrt{D} \in \mathbb{Q}[t]$, in the nontrivial case that the continued fraction is not periodic (i.e. $D(t)$ is not Pellian). More precisely, he proved the following result:

Theorem 3.42 (Theorem 1, [Mer16]). *If $D(t)$ is not Pellian, then for all primes p except finitely many, p appears in infinitely many polynomials a_n in a denominator of the coefficients.*

Notice that the primes excluded by the theorem are exactly the prime 2, any prime appearing already in the denominators of the coefficients of D and those such that D_p (the reduction modulo p of D) is a square. The proof of this result is based on the comparison between the continued fractions of $\sqrt{D}$ and $\sqrt{D_p}$. This question was already studied in a series of papers [vdP98], [vdP99], [vdP99] by van der Poorten, which analyzed whether the reduction of the convergents of $\sqrt{D}$ gives the convergents of $\sqrt{D_p}$ giving a theorem whose proof seems incomplete. In his thesis, Merkert completes the proof of van der Porten's theorem to prove his result (see [Mer16, Theorem 7.2]). We also point out that these questions are related to the problem of reducing minimal solutions of the polynomial Pell equation, and has recently been used by Platonov [Pla12] to construct hyperelliptic curves over $\mathbb{Q}$ of genus 2, where the Jacobian contains a torsion point of a specific order. These examples are relevant for the uniform boundedness conjecture for torsion points of abelian varieties.

— **3.43.** We present here to the interested reader three exercises about Pellian polynomials. The solutions are collected in Appendix 3.10.

Exercise 3.44.

1. Show that if $D \in \mathbb{Z}[t]$ is monic and irreducible over any quadratic extension of $\mathbb{Q}$, then D is not Pellian.
2. Show that, if $D \in \mathbb{Z}[t]$ is a monic polynomial, irreducible over $\mathbb{Q}$ and, for every prime p, not a square modulo p, then D is not Pellian.
3. Show that, if $D \in \mathbb{Z}[t]$ is monic, irreducible over $\mathbb{Q}_2(\sqrt{5})$ and not a square modulo 2, then D is not Pellian.

3.6 Distribution of Pellian polynomials

In this section we give a criterion for the solvability of the Pell equation $x(t)^2 - Dy(t)^2 = 1$ in terms of a special point on the Jacobian of the hyperelliptic curve $u^2 = D(t)$, in the case where

D is squarefree. This will allow us to study the solvability of the Pell equation for families of polynomials, and links the problem to the topic of Unlikely Intersections.

— **3.45.** Let k be an algebraically closed field, and let us denote by $(t : u : v)$ homogeneous coordinates of the projective plane $\mathbb{P}^2_k$, and call *line at infinity* the line defined by $v = 0$. Let $D(t) \in k[t]$ be a squarefree polynomial of even degree $\deg D = 2d > 0$. As D is squarefree, the affine curve given by the equation

$$u^2 = D(t)$$

is smooth. We denote by C the corresponding smooth projective curve. We may cover C by two affine charts, one given by the affine curve above, and the other by the affine curve $v^2 = s^{2d}D(s^{-1})$, the glueing map between charts given by $(v, s) = (ut^{-d}, t^{-1})$ whenever it is defined. The genus of C is $g = d - 1 > 0$. Such a curve is called a *hyperelliptic curve*, the elliptic curves being those where $d = 2$. We may view C as a $2:1$ cover of $\mathbb{P}^1$ ramified at the $2d$ distinct zeroes of D. In particular $C \to \mathbb{P}^1$ is unramified at infinity. The projective curve C has thus two distinct points at infinity, corresponding to the two distinct roots of $s^{2d}D(s^{-1})$ around $s = 0$. We denote[4] these two points by ∞_+ and ∞_-. Let J be the Jacobian variety of C. We embed C into J via

$$j : x \mapsto \text{ class of the divisor } (x) - (\infty_+) =: [(x) - (\infty_+)]$$

and write

$$\delta := j(\infty_-) = [(\infty_-) - (\infty_+)].$$

Notice that if the ground field k is not algebraically closed, then the points ∞_+ and ∞_- might not be defined over k. In this case they are conjugate points of degree two over k. With these notations, the following holds:

Theorem 3.46. *Let $D(t) \in k[t]$ be a polynomial of even degree and nonzero discriminant. With the notation from above, the polynomial D is Pellian if and only if $\delta \in J(k)$ is a torsion point.*

Proof. Suppose first that D is Pellian, so there exist polynomials $x(t)$ and $y(t) \neq 0$ satisfying $x^2 - Dy^2 = 1$. The nonconstant rational functions

$$\varphi_+ = x(t) + y(t)u \qquad \text{and} \qquad \varphi_- = x(t) - y(t)u$$

on C are regular on the affine part of C, so their divisors of poles are supported on $\{+\infty, -\infty\}$. Since $\varphi_+ \cdot \varphi_- = 1$, also their divisors of zeroes are supported at $\{+\infty, -\infty\}$, so we have

$$\operatorname{div}(\varphi_+) = a(\infty_+) + b(\infty_-)$$

for integers a, b which are not both zero. The degree of $\operatorname{div}(\varphi_+)$ is zero, hence $b = -a$ and thus $a\delta = \operatorname{div}(\varphi_+)$. This shows that δ is a torsion point of order dividing a. Conversely, suppose

[4] After fixing the equation $u^2 = D(t) = d_0t^{2d} + d_1t^{2d-1} + \cdots$ it is possible to identify the two points by stipulating that $u \pm d_0^{1/2}t^d$ has a zero at $\infty_\pm$.

that δ is torsion, so $a\delta$ is a principal divisor for some $a \neq 0$. Set $a\delta = \mathrm{div}(\psi)$. We may write ψ as $x(t) + y(t)u$ on the affine part of C, where x and y are polynomials in t. The function $(x + yu)(x - yu) = x^2 - Dy^2$ is then a rational function on $\mathbb{P}^1$ whose divisor is supported at infinity, hence must be constant. Scaling x and y by a square root of this constant yields a solution of the Pell equation. $\square$

— **3.47.** Let k be an algebraically closed field. A polynomial $D(t) \in k[t]$ is Pellian if and only if the polynomial $cD(at + b)$ is Pellian for some $a, c \in k^*$ and $b \in k$. A suitable substitution will bring a general polynomial $D(t)$ of even degree $2d$ into the form

$$D(t) = t^{2d} + t^m + a_1 t^{m-1} + \cdots + a_m$$

for some $m \leq 2d - 2$. We may consider the affine spaces $\mathbb{A}_k^m$ for $0 \leq m \leq 2d - 2$ as moduli for polynomials of degree $2d$ up to substitutions $D(t) \rightsquigarrow cD(at + b)$. As such, $\mathbb{A}_k^m$ contains a nonempty open subvariety $U \subseteq \mathbb{A}_k^m$ where the discriminant

$$\mathrm{disc}(t^{2d} + t^m + a_1 t^{m-1} + \cdots + a_m)$$

as a polynomial in $(a_1, \ldots, a_m)$ is nonzero. Over this open subvariety, the curves $u^2 = D(t)$ are smooth, and their Jacobians define a principally polarised abelian scheme J over U. On the boundary of U, the abelian scheme J degenerates. The abelian scheme J comes equipped with a section $\sigma : U \to J$ given by the divisor of points at infinity $(\infty_-) - (\infty_+)$. We may regard σ as a group homomorphism $\mathbb{Z} \to J$, hence as a peculiar 1-motive $M = [\mathbb{Z} \to J]$ over U. We want to understand the set

$$\{\lambda \in U \mid \sigma_\lambda \text{ is torsion in } J_\lambda\} \tag{3.8}$$

that is, the set of those $\lambda \in U$ for which the 1-motive M_λ splits up to isogeny.

— **3.48.** Let us take an analytic viewpoint on the exceptional set (3.8). Let U be a simply connected complex manifold, and let $A \to U$ be a holomorphic family of complex tori of dimension g on U. We obtain a vector bundle $\mathrm{Lie}(A)$ of rank g over U. The kernel of the exponential map $\mathrm{Lie}(A) \to A$ is a local system of free $\mathbb{Z}$-modules of rank $2g$, which we may identify with the homology $H_1(A/U)$. Let $\omega_1, \ldots, \omega_{2g}$ be a basis of sections of this local system. We now may describe sections $\sigma : U \to A$ as functions $\beta : U \to \mathbb{R}^{2g}$ via the following correspondence.

$$\beta : U \to \mathbb{R}^{2g} \qquad\qquad \sigma(u) = \exp \sum_{i=1}^{2g} \beta_i(u)\omega_i(u)$$

We refer to β as *Betti map.* Notice that $\sigma(u_0)$ is a torsion point in the fibre A_{u_0} if and only if all coordinates of $\beta(u_0)$ are rational.

Let us consider the situation of 3.47, taking for simplicity as U a simply connected open subset of $\mathbb{C}^m$ where the discriminant $\mathrm{disc}(t^{2d} + a_1 t^{m-1} + \cdots + a_m)$ is nonzero. In this case, $2g = 2d - 2$ so the scheme J over U (given by the Jacobians) has relative dimension $d - 1$. The rank of the Betti map is defined as the rank of the jacobian matrix of these Betti coordinates, at a certain point of U, with respect to any choice of real-coordinates x_j, y_j, where we can assume for example $z_j = x_j + iy_j$ on U are holomorphic coordinates on U and x_j and y_j are the corresponding real and imaginary parts. For a general U the Betti map may be defined passing to the universal cover (as done in [ACZ18]). We call generic rank the maximal rank of this differential on S. The set where the rank decreases is a (proper) closed real-analytic subvariety; hence the set where the rank is the generic one is open and dense (since U is simply connected). Let u_0 be a point of U where the rank r is maximal (i.e. $= d-1$). By the implicit function theorem, the fiber $\beta^{-1}(\beta(u))$ is, in a neighbourhood of u_0, a real analytic variety of dimension $2d-r$.

The rank of the Betti map has been intensively studied in [ACZ18] (see also [CMZ16, Section 1.2] for some general proofs in the case $d \leq 2$). In this case, the expectation is that the Betti map $\beta : U \to \mathbb{R}^{2d-2}$ has full rank almost everywhere, so we expect the fibres of β to be of complex dimension $d-1$. In particular, $\beta^{-1}(\mathbb{Q}^{2d-2})$ is a countable union of subvarieties of complex dimension $m-d-1$ (empty if $m < d-1$) in the ambient space U which has dimension m.

Suppose now that we are given a one parameter family $D_\lambda(t)$ describing a curve L in U. Solely for dimension reasons, we expect $L \cap \beta^{-1}(x) = \varnothing$ for general $x \in \mathbb{R}^{2d-2}$. According to the philosophy of *unlikely intersections*, it is reasonable to expect that

$$L \cap \beta^{-1}(\mathbb{Q}^{2d-2}) = \{\lambda \in L \mid D_\lambda(t) \text{ is Pellian}\}$$

is a finite set, unless L has a very special shape. Indeed this has been proven in full generality by Masser and Zannier (see [MZ15] for the special family $D_\lambda(t) = t^6 + t + \lambda$).

Example 3.49. In the case $d = 1$, the set U is a single point corresponding to the polynomial $t^2 - 1$, which is Pellian. The case $d = 1$ becomes interesting if we add an arithmetic constraint and ask for the integers $n \neq 0$ such that the Pell equation

$$x(t)^2 - (t^2 + n)y(t)^2 = 1$$

has a nontrivial solution with $x(t), y(t) \in \mathbb{Z}[t]$. The answer was given by Nathanson in [Nat76]: there is a nontrivial solution if and only if $n \in \{-2, -1, 1, 2\}$, and we can moreover describe all solutions.

Example 3.50. Consider the family of polynomials $D_\lambda(t) = t^4 + t + \lambda$. With the notation of 3.47, we are in the case $d = 2$ and $m = 1$. The discriminant of $D_\lambda(t)$ is $2^8\lambda^3 - 3^3$, so we will take for U the complex plane minus the three points $\frac{3}{8}\sqrt[3]{2}e^{2\pi i p/3}$ for $p = 0, 1, 2$. One can show that in this example, the Betti map $\mathbb{C} \supseteq U \to \mathbb{R}^2$ is locally surjective, so we expect countably many $\lambda \in U$ for which $D_\lambda(t)$ is Pellian. As a consequence of a theorem of Silverman-Tate, algebraic points $\lambda \in U$ for which $D_\lambda(t)$ is Pellian have bounded height. In particular, given any number field k, there are only finitely many $\lambda \in k$ for which $t^4 + t + \lambda$ is Pellian.

Example 3.51. Consider the family of polynomials $D_\lambda(t) = t^6 + t + \lambda$. With the notation of 3.47, we are in the case $d = 3$ and $m = 1$. The discriminant is $5^5 - 6^6\lambda^5$. In this case the Betti map $\mathbb{C} \supseteq U \to \mathbb{R}^4$ cannot be surjective, so it is unlikely that $\beta(u)$ has only rational coordinates. Let us compute a few terms of the continued fraction expansion of the square root of the polynomial $D_\lambda(t)$. We may think for the moment that the field of coefficients is $\mathbb{Q}(\lambda)$. The Laurent series expansion of $\sqrt{D}$ at infinity reads

$$\sqrt{D(s)} = t^3 + \frac{t^{-2}}{2} + \frac{\lambda t^{-1}}{2} - \frac{t^{-7}}{8} - \frac{\lambda t^{-8}}{4} - \frac{\lambda^2 t^{-9}}{8} + \frac{t^{-12}}{16} + \frac{3\lambda t^{-13}}{16} + \frac{3\lambda^2 t^{-14}}{16} + \frac{\lambda^3 t^{-15}}{16} - \frac{5t^{-17}}{128} + \cdots$$

and has polynomial part t^3. We find

$$\begin{aligned}
a_0 &= t^3 \\
a_1 &= 2t^2 - 2\lambda t + 2\lambda^2 \\
a_2 &= -\frac{t}{2\lambda^3} - \frac{1}{2\lambda^2} \\
a_3 &= -8\lambda^6 t + 16\lambda^7 \\
a_4 &= -\frac{t}{24\lambda^8 - 2\lambda^3} - \frac{16\lambda^5 - 1}{288\lambda^{12} - 48\lambda^7 + 2\lambda^2} \\
a_5 &= -\frac{(1-12\lambda^5)^3 t}{8\lambda^9} - \frac{18432\lambda^{25} + 15360\lambda^{20} - 6400\lambda^{15} + 848\lambda^{10} - 48\lambda^5 + 1}{128\lambda^{18}}
\end{aligned}$$

and the expressions keep growing. According to Abel's Theorem, $D_{\lambda_0}(t)$ is Pellian if and only if the specialized sequence of the a_i is periodic. Already from these few terms this periodicity seems unlikely. Indeed, it has been shown by Masser and Zannier that there are only finitely many $\lambda_0 \in U$ for which $D_{\lambda_0}(t)$ is Pellian (see [MZ15]).

3.7 The Pell equation in the non-squarefree case

In this section, we analyze some examples of polynomial Pell equations with non-squarefree D. These can be interesting for certain applications, and involve the study of so-called *generalised Jacobians*. Consider, for example the, family

$$D_\lambda(t) = t^2(t^4 + t^2 + \lambda t)$$

where λ varies over complex numbers such that $\mathrm{disc}(t^4 + t^2 + \lambda t) \neq 0$. The corresponding curves

$$u^2 = D_\lambda(t)$$

have a cusp at $(u,t) = (0,0)$. The criterion in Theorem 3.46 is still valid when instead of the Jacobian of a smooth curve we consider the generalised Jacobian of a possibly singular projective curve (see Theorem 3.54 below). The theory of generalised Jacobians goes back to Rosenlicht [Ros54], a standard reference is Chapter V in Serre's *Groupes algébriques et corps de classes*, [Ser75]. For the curves above, the generalised Jacobian is an algebraic group G_λ for which the short exact sequence

$$0 \to \mathbb{G}_a \to G_\lambda \to E_\lambda \to 0$$

holds. It turns out that the extension is non-split (for a proof, see [Ser88, p. 188] or [CMZ13, p.249]) We can then recover a finiteness result analogously to the case of squarefree D; this has been done by H. Schmidt, a student of Masser, in his PhD thesis [Sch15], using again the Betti maps and involving in this case the Weierstrass $\wp$ and ζ functions.

— **3.52.** Let us give a short résumé on generalised Jacobians. Let C be a smooth projective curve of genus $g \geq 0$ over a field k, and let

$$\mathfrak{m} = \sum_{i=1}^{d} n_i P_i \tag{3.9}$$

be an effective divisor on C. We suppose that in (3.9) the P_i are distinct, so that d is the degree of the reduced divisor underlying $\mathfrak{m}$. We call $\mathfrak{m}$ a *modulus*. For a given rational function f on C, write $f \equiv 1 \bmod \mathfrak{m}$ if $\mathrm{ord}_{P_i}(1-f) \geq n_i$ holds for each i. Given two divisors D and D' on C whose support is disjoint from the support of $\mathfrak{m}$, we say that D and D' are $\mathfrak{m}$-*equivalent* and write

$$D \sim_{\mathfrak{m}} D'$$

if there exists a rational function f such that $D - D' = \mathrm{div}(f)$ and $f \equiv 1 \bmod \mathfrak{m}$. The zealous reader may check that $\sim_{\mathfrak{m}}$ is indeed an equivalence relation. Set

$$\mathrm{Pic}^0_{\mathfrak{m}}(C) := \frac{\text{Divisors on } C \text{ of degree 0 and support disjoint from } \mathfrak{m}}{\text{Divisors } \mathrm{div}(f) \text{ with } f \equiv 1 \bmod \mathfrak{m}}.$$

A first theorem of Rosenlicht ([Ser88], Chap.V, Prop. 2 and Thm 1(b)) states that the functor $k' \mapsto \mathrm{Pic}^0_{\mathfrak{m}}(C \times_k k')$ is representable by a commutative connected algebraic group $G_{\mathfrak{m}}$ over k. We call $G_{\mathfrak{m}}$ the generalised Jacobian of the pair $(C, \mathfrak{m})$. Its dimension is g if $\mathfrak{m} = 0$ and $g + \deg(\mathfrak{m}) - 1$ if $\mathfrak{m} \neq 0$. If $\mathfrak{m} = 0$, we recover the usual Jacobian of C. If $\mathfrak{m}'$ divides $\mathfrak{m}$, there is a canonical surjective morphism $G_{\mathfrak{m}} \to G_{\mathfrak{m}'}$. In particular, there is a canonical short exact sequence

$$0 \to L_{\mathfrak{m}} \to G_{\mathfrak{m}} \to A \to 0$$

where $A = G_0$ is the Jacobian of C. A second theorem of Rosenlicht ([Ser88], V.13-V.17) concerns the structure of $L_{\mathfrak{m}}$. It states that $L_{\mathfrak{m}}$ is an affine algebraic group, isomorphic to the product of a torus T of dimension $d-1$ (and gives its precise structure), and an additive group of dimension $\deg(\mathfrak{m}) - d$. As in (3.9), d is the degree of the reduced divisor underlying $\mathfrak{m}$, hence if $\mathfrak{m}$ is already reduced, $G_{\mathfrak{m}}$ is a semiabelian variety.

Definition 3.53. Let C be a proper, but not necessarily smooth curve over a field k. We call *generalised Jacobian* of C the generalised Jacobian $G_{\mathfrak{m}}$ of the pair $(\widetilde{C}, \mathfrak{m})$ as introduced in 3.52, where $\widetilde{C}$ is the normalisation of C and $\mathfrak{m}$ the exceptional divisor on $\widetilde{C}$.

Theorem 3.54. *Let $D(t) \in \mathbb{C}[t]$ be a polynomial of even degree, and denote by $C \subseteq \mathbb{P}^2$ the projective curve given by the equation $u^2 = D(t)$. Let G be the generalised Jacobian of C, and let $\delta := [(\infty_-) - (\infty_+)]$ be the divisor of points at infinity on C. The polynomial D is Pellian if and only if $\delta \in G(\mathbb{C})$ is a torsion point.*

Proof. The proof is essentially the same as that of Theorem 3.46, and left as an exercise. □

Example 3.55. Consider the polynomial Pell equation $x(t)^2 - D_\lambda(t)y(t)^2 = 1$, where D_λ is the following pencil of non-squarefree polynomials

$$D_\lambda(t) = t^2(t^4 + t^2 + \lambda t)$$

where λ varies over the complex numbers such that $\operatorname{disc}(t^4+t^2+\lambda t) \neq 0$. As already mentioned, the affine curve given by the equation $u^2 = D_\lambda(t)$ is singular at ∞ and at 0, and its generalised Jacobian is a nonsplit extension

$$0 \to \mathbb{G}_a \to G \to E_\lambda \to 0$$

where E_λ is the elliptic curve given by $u^2 = \widetilde{D}_\lambda := t^4 + t^2 + \lambda t$. If (x, y) is a solution of the Pell equation $x^2 - D_\lambda y^2 = 1$, then (x, ty) is a solution of $x^2 - \widetilde{D}_\lambda y^2 = 1$. This way, solutions of the Pell equation $x^2 - D_\lambda y^2 = 1$ are in one-to-one correspondence with those solutions $(\widetilde{x}, \widetilde{y})$ of $\widetilde{x}^2 + \widetilde{D}_\lambda \widetilde{y}^2 = 1$ where $t|\widetilde{y}$. From the viewpoint of Theorem 3.54, this reflects the evident fact that any torsion point of G maps to a torsion point on E_λ. A point $g \in G(\mathbb{C})$ is torsion if and only if it maps to a torsion point in $E_\lambda(\mathbb{C})$ and moreover satisfies a "linear" condition.

Example 3.56. Consider the family of polynomials $D_\lambda(t) = (t-\lambda)^2(t^2-1)$ for λ varying in $\mathbb{C}\setminus\{0\}$. In this case, the solvability of the associated Pell equation is related to the study of some special torsion points on $\mathbb{G}_m$. Let us consider the projective curve H defined by the equation $u^2 = t^2 - 1$: its normalisation has genus zero, so its Jacobian is trivial. Consider the two points $\xi_\lambda^\pm = (\lambda, \pm\sqrt{\lambda^2-1})$ of H with first coordinate equal to λ. A divisor A of degree 0 on H is always principal, so $A = \operatorname{div}(f)$ for some function f on H; hence, we have an homomorphism from divisors on H to $\mathbb{G}_m$ sending $A \mapsto \frac{f(\xi_\lambda^+)}{f(\xi_\lambda^-)}$. This yields indeed an isomorphism from the generalised Jacobian of H to $\mathbb{G}_m$. The divisor $\infty_- - \infty_+$ is equal to $\operatorname{div}(z)$, where $z = t + u$. Here, as before, we denote by ∞_+ the pole of the function $t + u$ and by ∞_- the pole of $t - u$. The image of $\operatorname{div}(z)$ under the described isomorphism is equal to $\frac{z(\xi_\lambda^+)}{z(\xi_\lambda^-)} = (\lambda + \sqrt{\lambda^2-1})^2$. This means that the polynomial $D_\lambda(t)$ is Pellian if and only if $\lambda + \sqrt{\lambda^2-1}$ is a root of unity in $\mathbb{G}_m$. Hence there are countably infinitely many $\lambda \in \mathbb{C}$ such that the polynomial D_λ is Pellian.

Example 3.57. Consider the family of polynomials $D_\lambda(t) = (t-\lambda)^2(t-\lambda-1)^2(t^2-1)$. We can generalise the construction of the previous example. This time, we consider the two pairs of points $\xi_\lambda^\pm = (\lambda, \pm\sqrt{\lambda^2-1})$ and $\xi_{\lambda+1}^\pm = (\lambda+1, \pm\sqrt{\lambda^2+2\lambda})$, and obtain an isomorphism from the generalized Jacobian to $\mathbb{G}_m^2$ by sending $\operatorname{div}(f)$ to $\left(\frac{f(\xi_\lambda^+)}{f(\xi_\lambda^-)}, \frac{f(\xi_{\lambda+1}^+)}{f(\xi_{\lambda+1}^-)}\right)$. Arguing as in the previous case, we conclude that $D_\lambda(t)$ is Pellian if and only if $\lambda + \sqrt{\lambda^2-1}$ and $\lambda + 1 + \sqrt{\lambda^2+2\lambda}$ are both roots of unity. This is equivalent to study the torsion points on a curve in $\mathbb{G}_m^2$, that in our case is the curve of equation $x + x^{-1} = 2 + y + y^{-1}$. In general, these questions are related to Manin-Mumford type questions for $\mathbb{G}_m$, already asked by Lang, and proved by Ihara, Serre, Tate in the case of curves (see [Lan65]) and then generalised by Laurent [Lau94] and independently by Sarnak-Adams [SA94] to higher dimension. For a survey on this questions, see also Zannier's book [Zan12].

Example 3.58. Consider the family of polynomials $D_\lambda(t) = (t-1)^2(t^4+t+\lambda)$. In this case, the generalized Jacobian G is an extension by $\mathbb{G}_m$ of an elliptic curve E. This elliptic curve E is the Jacobian of the relative quartic with equation $u^2 = t^4 + t^2 + \lambda$, and the extension is non split in general. Also in this case we can apply Pellian criterion to the section s of G defined by the class of the relative divisor $(\infty_-) - (\infty_+)$ on the quartic, for the strict linear equivalence attached to the node of the sextic $u^2 = D_\lambda(t)$ at $t = 1$ (see [Ser88]). This case was studied in [BMPZ11]: applying the Main Theorem to the generalized Jacobian, we have again a result of finiteness.

Exercise 3.59. Prove that there are countably infinitely many $\lambda \in \mathbb{C}$ such that the Pell equation $x^2 - (t^4 + t^2 + \lambda t)y^2 = 1$ has a nontrivial solution, but that there are only finitely many λ for which there is a solution (x, y) where x is monic.

3.8 A Skolem-Mahler-Lech theorem for algebraic groups

The key ingredient in the proof of Theorem 3.30 is a theorem on algebraic groups reminiscent of the classical Skolem-Mahler-Lech theorem. This theorem states that for a sequence of elements in a field of characteristic zero $u_1, u_2, \ldots$ which is generated by a linear recurrence relation, there exist an integer N and a subset $R \subseteq \mathbb{Z}/N\mathbb{Z}$ such that

$$u_n = 0 \iff (n \bmod N) \in R$$

holds, with finitely many exceptions. For sequences of rational numbers, this theorem is due to Skolem (1933). Subsequent generalisations are due to Mahler for the case of number fields (1935), and to Lech for general fields of characteristic zero (1953).

— **3.60.** A subset $A \subseteq \mathbb{Z}$ is called a *full arithmetic progression* if there exist integers a, $b \neq 0$ such that $A = \{a + bn \mid n \in \mathbb{Z}\}$ holds. Subsets of $\mathbb{Z}$ which are the union of a finite set and finitely many full arithmetic progressions form the closed sets of a topology on $\mathbb{Z}$.

Theorem 3.61 (Skolem-Mahler-Lech)**.** *Let k be a field of characteristic zero. Let $c_1, \ldots, c_r$ and $u_1, \ldots, u_r$ be elements of k with $c_r \neq 0$, and recursively define $u_n \in k$ by*

$$u_n = c_1 u_{n-1} + \cdots + c_r u_{n-r}$$

for all $n \in \mathbb{Z}$. The set $\{n \in \mathbb{Z} \mid u_n = 0\}$ is the union of a finite set and finitely many full arithmetic progressions.

We shall deduce this theorem as a corollary of Theorem 3.63 below.

Classical proofs of this theorem use p-adic methods in one way or another. The corresponding statement in characteristic $p > 0$ is wrong. The question was studied by Derksen (2005), but there are already counterexamples by Lech (1953).

Example 3.62. The sequence $u_1, u_2, \ldots$ in $\mathbb{F}_p(t)$ defined by $u_1 = 0$, $u_2 = 2t$, $u_3 = 3t^3 + 3t^2$ and

$$u_n = (2t+2)u_{n-1} - (t^2+3t+1)u_{n-2} + (t^2+t)u_{n-3}$$

has the closed expression $u_n = (t+1)^n - t^n - 1$. The set $\{n \mid u_n = 0\}$ is the set of all powers of p, which cannot be written as the union of a finite set and finitely many arithmetic progressions.

For the proof of Theorem 3.30 we will need the following result:

Theorem 3.63 (Corollary 3.3 [Zan16]). *Let k be a field of characteristic zero and let G be an algebraic group over k. Let $X \subseteq G$ be a closed subvariety of G, and let $g \in G(k)$ be a rational point. The set*

$$\{n \in \mathbb{Z} \mid \ g^n \in X(k)\}$$

is the union of a finite set and finitely many full arithmetic progressions.

Proof of Theorem 3.63. The proof of the main statement consists of a series of reductions to particular cases, until we are in the situation where G is commutative, defined over a p-adic field, and g is sufficiently close to the identity so that g lies in the image of the p-adic exponential map. The final argument is then an application of elementary of p-adic analysis.

By replacing G by the Zariski closure of $\{g^n \mid \ n \geq 1\}$ we may without loss of generality assume that G is commutative and that $\{g^n \mid \ n \geq 1\}$ is Zariski dense in G. Let $G_0, \ldots, G_n$ be the connected components of G, where G_m is the component of g^m. The group G/G_0 is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, generated by the class of $g \in G_1(k)$. If the statement of the theorem holds for the closed subvarieties $g^{-m}(X \cap G_m)$ of G_0 and the element $g^n \in G_0(k)$, then it holds for $X \subseteq G$ and $g \in G(k)$, hence we also may suppose that G is connected.

We are now in the situation where G is commutative and connected, and $\{g^n \mid \ n \geq 1\}$ is dense in G. If $X = G$, then the set $\{n \in \mathbb{N} \mid \ g^n \in X\}$ is all of $\mathbb{Z}$ and we are done. Suppose then that $X \neq G$, and let us show that the set $\{n \in \mathbb{N} \mid \ g^n \in X\}$ is indeed finite. In other words, we show that for any infinite subset $A \subseteq \mathbb{N}$ the set of points $\{g^a \mid \ a \in A\}$ is dense in G. Fix an infinite subset $A \subseteq \mathbb{N}$ and a rational function f on G such that $f(g^a) = 0$ for all $a \in A$. We must show that f is zero, and we will do so by using properties of p-adic analytic maps. In order to move to a p-adic setting, let us choose and still denote by G a model of G over $\mathrm{spec}(R)$ for some finitely generated integral ring R, such that the point $g \in G(k)$ extends to a point $g \in G(R)$. For some sufficiently big prime number p, there exists a finite extension K of $\mathbb{Q}_p$ and an embedding R into the ring $\mathcal{O}_K$ of integers of K. We may also assume that f has good reduction modulo p. It suffices to show that the set of points $\{g^a \mid \ a \in A\} \subseteq G(K)$ is dense in G viewed as an algebraic group over K.

We are now in the situation where G is defined over finite extension K of $\mathbb{Q}_p$ with a model over $\mathcal{O}_K$, and g is an integral point of G, that is, $g \in G(\mathcal{O}_K) \subseteq G(K)$. With its p-adic topology the group $G(K)$ is a topological group, and $G(\mathcal{O}_K) \subseteq G(K)$ is a compact open subgroup. There exists a p-adic analytic group homomorphism $e : \mathcal{O}_K^d \to G(\mathcal{O}_K)$ which is a homeomorphism of $\mathcal{O}_K^d$ onto its image (the map e is the p-adic exponential map, see [Hoo42] for an elementary treatment). The integer d is the dimension of G as an algebraic group. Since $G(\mathcal{O}_K)$ is compact we have $g^n \in e(\mathcal{O}_K)$ for some sufficiently big $n \geq 1$. Let us write $\xi = e^{-1}(g^n)$. By partitioning A into congruence classes modulo n and passing to one of these subsets, we may assume that all elements of A are pairwise congruent modulo n, and so we write $a = a'n + r$ with a fixed r for all elements $a \in A$.

Let us now consider the map $\phi : \mathcal{O}_K \to \mathcal{O}_K$ given by $\phi(z\xi) = f(g^{nz+r})$. For every $a \in A$ we have that a' is a zero of the locally analytic function $z \mapsto \phi(z\xi)$, but this is only possible if the function is identically zero, which implies that also f is identically zero as we wished to show. □

We show now how the classical Skolem-Mahler-Lech theorem can be derived from the more general Theorem 3.63.

Proof of Theorem 3.61. Let $u_1, u_2, \ldots$ be a sequence of elements of k defined by its initial terms $u_1, \ldots, u_r \in k$ and a linear recurrence relation, say

$$u_n = c_1 u_{n-1} + \cdots + c_r u_{n-r}$$

for all $n > r$. In order to study the nature of the set $\{n \in \mathbb{N} \mid u_n = 0\}$ we may assume that k is algebraically closed, hence we may suppose that there exist $\alpha_1, \ldots, \alpha_r \in k$ and polynomials $P_1, \ldots P_r \in k[t]$ such that

$$u_n = \sum_{i=1}^{r} P_i(n)\alpha_i^n$$

holds for all $n \geq 0$. We can consider the closed algebraic group $G := \mathbb{G}_a \times \mathbb{G}_m^r$ over k, the subvariety $X \subseteq G$ defined by

$$X = \{(y, z_1, \ldots, z_r) \mid P_1(y)z_1 + \cdots + P_r(y)z_r = 0\}$$

and the point $g = (1, \alpha_1, \ldots, \alpha_r) \in G(k)$. We have $g^n \in X(k) \iff u_n = 0$, hence Theorem 3.61 is indeed a consequence of Theorem 3.63. □

3.9 Periodicity of the degrees of the partial quotients

In this section we prove Theorem 3.30, stating that given a polynomial $D(t) \in K[t]$ where k is an algebraically closed field of characteristic zero, the sequence of degrees of the partial quotients in the continued fraction expansion of $\sqrt{D(t)}$ is periodic. If $D(t)$ is a square, the assertion holds trivially, so we will assume not to be in this case. Moreover, for simplicity of exposition we will only consider the case where D is squarefree, even if the reduction to this case is not immediate. The general case, which involves the use of generalized Jacobians, is treated in [Zan16].

— **3.64.** We call a sequence $(x_n)_{n\geq 0}$ *eventually periodic* if there exist integers $N \geq 1$ and $L \geq 1$ such that $x_{n+L} = x_n$ holds for all $n > N$. We call a subset $X \subseteq \mathbb{N}$ *eventually periodic* if its characteristic function, viewed as a sequence, is eventually periodic. In other words, a subset $X \subseteq \mathbb{N}$ is eventually periodic if, up to a finite set, it is a finite union of arithmetic progressions.

— **3.65.** We fix once and for all a squarefree complex polynomial $D(t) \in K[t]$ of even degree $2d > 2$, and denote by

$$\sqrt{D(t)} = [a_0; a_1, a_2, a_3, \ldots]$$

the continued fraction expansion of $\sqrt{D}$. We denote by p_n/q_n the convergents, where p_n and q_n are the polynomials obtained from the recurrence relations (3.3). We set

$$l_n := \deg a_n$$

to ease notations. Let us denote by $\mathcal{C}$ the non-singular model of the curve given by the equation $u^2 = D(t)$ as introduced in Section 3.6, and let J be the Jacobian variety of $\mathcal{C}$. The curve $\mathcal{C}$ has genus $g = d - 1$, so J is an abelian variety of dimension g. As done before, let us call ∞_+ and ∞_- the two points at infinity of $\mathcal{C}$. The canonical embedding $j : \mathcal{C} \to J$ sends $y \in \mathcal{C}$ to the class of $(y) - (\infty_+)$. Define

$$\delta := j(\infty_-) = [(\infty_-) - (\infty_+)].$$

and, for $0 \leq m \leq g$ the closed, irreducible subvariety $W_m \subseteq J$ given by

$$W_m = \{j(y_1) + j(y_2) + \cdots + j(y_m) \mid y_1, \ldots, y_m \in \mathcal{C}\},$$

which has dimension m. In particular $W_g = J$.

— **3.66.** We will work with rational functions on the hyperelliptic curve $\mathcal{C}$ of the form $f = p - qu$, where p and q are polynomials in the variable t. Such a function is regular on the affine part of $\mathcal{C}$, i.e. on the affine curve given by the equation $u^2 = D(t)$. An affine neighbourhood of the points ∞_+ and ∞_- is given by the curve with equation

$$v^2 = s^{2d} D(s^{-1}) \tag{3.10}$$

as we have already seen in 3.45. Using the substitution rule $(u, t) = (vs^{-d}, s^{-1})$, the rational function $f(u, t) = p(t) - q(t)u$ transforms to $g(v, s) = p(s^{-1}) - q(s^{-1})vs^{-d}$. Denoting by $c \in \mathbb{C}$ the leading coefficient of $D(t)$, the points ∞_+ and ∞_- correspond to the solutions $(v, s) = (\pm\sqrt{c}, 0)$ of (3.10). We can understand the behaviour of f at the two points at infinity as follows: write $v = s^{-d}\sqrt{D(s^{-1})}$ around $s = 0$ as a Laurent series:

$$v = s^{-d}\sqrt{D(s^{-1})} = \pm \sum_{n \geq -d} c_n s^n$$

The behaviour of f at the two points at infinity is then the one of the series

$$p(s) \pm q(s)v = p(s) \pm q(s) \sum_{n \geq -d} c_n s^n$$

around $s = 0$, the sign depending on the choice of the signs for ∞_+ and which ∞_-. In particular, if p_n/q_n is a convergent in the continued fraction expansion of $\sqrt{D}$, then $p_n - q_n u$ has a pole of order $\deg p_n + d$ at one point, and a zero of order $\deg q_n + \deg a_n$ at the other point at infinity.

— **3.67.** Our goal is to prove that the sequence $(\deg a_n)_n$ is eventually periodic. By (3.3), we have $\deg(p_{n+1}) = \deg(p_n)+\deg(a_n)$, hence to show that $(\deg a_n)_n$ is eventually periodic amounts to show that the set

$$B := \{\deg p_n \mid n \geq 1\}$$

is, up to a finite set, a union of finitely many arithmetic progressions. Let us introduce for $l \geq 1$ the following three sets

$$\begin{aligned}
A(l) &:= \{k \geq 1 \mid k \cdot \delta \in W_{d-l}\}; \\
B(l) &:= \{k \geq 1 \mid \exists n \geq 1 \text{ with } \deg(p_n) = k,\ \deg(a_n) = l\}; \\
C(l) &:= \{k \geq 1 \mid \exists n \geq 1, h \geq 1 \text{ with } \deg(p_n) = k - h,\ \deg(a_n) = l + h\}.
\end{aligned}$$

Notice that $A(d) = \varnothing$, $A(1) = \mathbb{N}\backslash\{0\}$ and, for every $i = 1, \ldots, d-1$ we have that $A(i+1) \subseteq A(i)$. Furthermore, as the sequence of the degrees of the p_n is strictly increasing, the sets $B(l)$ are all disjoint.

Theorem 3.63 states that for any integer $l \geq 0$, the set $A(l)$ is eventually periodic. We have

$$B = \bigcup_{l=1}^{d} B(l),$$

so it suffices to show for each l individually that $B(l)$ is eventually periodic. We will do this essentially by a "downward" induction on l, noting that $B(l)$ is empty for $l > d$. The bulk of the work consists of relating the sets $A(l)$, $B(l)$ and $C(l)$, which we will do in the following lemmas.

Lemma 3.68. *The inclusion $B(l) \subseteq A(l)$ holds for all $l \geq 1$.*

Proof. To show this, we consider the rational functions $\varphi_n := p_n - uq_n$ on the curve $\mathcal{C}$. After choosing signs suitably, φ_n has a zero at ∞_+ of order $\deg q_n + l_n$, and a pole at ∞_- of order $\deg q_n + d$, which is in fact the only pole. We then have

$$\begin{aligned}
\operatorname{div}(\varphi_n) &= (\deg q_n + l_n)(\infty_+) - (\deg q_n + d)(\infty_-) + \sigma_n \\
&= -(\deg p_n)((\infty_-) - (\infty_+)) - (d - l_n)(\infty_+) + \sigma_n,
\end{aligned}$$

where σ_n is an effective divisor of degree $d - l_n$ of the form

$$\sigma = \sum_{i=1}^{d-l_n} (x_i)$$

with $x_i \neq \infty_\pm$, and we have used that $\deg p_n = \deg q_n + d$. Considering the corresponding linear equivalence classes, we have that

$$(\deg p_n)\delta = [\sigma - (d - l_n)(\infty_+)] = \sum_{i=1}^{d-l_n} [(x_i) - (\infty_+)] = \sum_{i=1}^{d-l_n} j(x_i),$$

hence $(\deg p_n)\delta \in W_{d-l_n}$ as wanted. $\square$

On a side note, using the fact that $W_{d-l_n} = W_{g-l_n-1}$, we can observe that in some sense we "usually" have $l_n = \deg a_n = 1$, since otherwise we would have $(\deg p_n)\delta \in W_{g-1}$, and $W_{g-1} \subseteq J$ is a subvariety of codimension 1.

We also remark that a similar argument combined with a more general version of Theorem 3.63 implies for instance that if the Jacobian is simple, then either $\deg a_n = 1$ for all large n or δ is a torsion point, i.e. we are in the Pellian case. Since a generic curve has a simple Jacobian, this justifies the assertion that *"usually, almost all the a_n have degree 1"*.

Lemma 3.69. *Let us consider the set $C := \bigcup_{i\geq 1} C(i)$. Then, for every $l \geq 1$, the sets $B(l)$ and C are disjoint.*

Proof. We argue by contradiction. Let $k \geq 1$ be an element of C and also of $B(l)$. As C is the union of the $C(i)$ for all $i \geq 0$ (and $C(i) = \emptyset$ for all $i \geq d$), then there exists $1 \leq r \leq d-1$ such that $k \in C(r)$. hence, there exist by definition integers $n, m, h \geq 1$ such that

$$\deg p_m = k - h \qquad \deg a_m = r + h \qquad \deg p_n = k \qquad \deg a_n = l$$

holds. Moreover, notice that $\deg q_n - \deg q_m = \deg p_n - \deg p_m = h$. Consider now the rational function

$$q_n p_m - p_n q_m = q_n(p_m - uq_m) - q_m(p_n - uq_n);$$

then, on $\mathcal{C}$ it has a zero at ∞_+ of order at least the minimum of $\deg q_m + \deg a_m - \deg q_n = r$ and $\deg q_n + \deg a_n - \deg q_m = l + h$. We conclude that $q_n p_m - p_n q_m$ has a zero of order at least 1 at ∞_+, hence is identically zero since it is a polynomial in t which we just considered as a rational function on $\mathcal{C}$ via the $2:1$ covering $\mathcal{C} \to \mathbb{P}^1$. Therefore as p_n/q_n and p_m/q_m are convergents of the continued fraction of $\sqrt{D}$, the equality $q_n p_m = p_n q_m$ implies $m = n$ and $k - h = \deg(p_m) = \deg(p_n) = k$, contradicting the assumption that h is positive. $\square$

Lemma 3.70. *For every $l \geq 1$, the intersection of $B(l)$ and $A(l+1)$ is at most finite; more precisely, if $k \in B(l) \cap A(l+1)$ then $k \leq \frac{d-l-1}{2}$.*

Proof. We argue by contradiction. Let $k \geq 1$ be an element of $A(l+1)$ and also of $B(l)$. Since $k\delta \in W_{d-(l+1)}$, there exists an effective divisor σ of degree $d-(l+1)$ such that

$$k\delta = [\sigma - (d-l-1)(\infty_+)].$$

This implies that there exists a rational function φ over $\mathcal{C}$ such that

$$\operatorname{div}(\varphi) = -k((\infty_-) - (\infty_+)) + \sigma - (d-l-1)(\infty_+). \tag{3.11}$$

Since the divisor of poles of φ is supported only on $\{\infty_+, \infty_-\}$, then there exists two polynomials p and q in $K[t]$ such that $\varphi = p - qu$. Moreover, since $k \in B(l)$, there exists an integer $n \geq 1$ such that $\deg p_n = k$ and $\deg a_n = l$. Now, the function $\varphi_n = p_n - q_n u$ vanishes at ∞_+ with order $\deg q_n + l = k - d + l$. If we consider the rational function $pq_n - qp_n = q_n\varphi - q\varphi_n$, it has an order at ∞_+ at least

$$\min\{-\deg q_n + \operatorname{ord}(\varphi), -\deg q + \operatorname{ord}\varphi_n\} \geq \min\{l+1, -\deg q + k - d + l\}. \tag{3.12}$$

We want now to estimate the degree of q. If we consider the function $\varphi' = p + qu$, it will have order $\geq -k$ at ∞_+ and order $\geq k - d + l + 1$ at ∞_-, since it is the composition of the standard involution $(t, u) \mapsto (t, -u)$ of $K(\mathcal{C})$ with φ. Writing $uq = \frac{1}{2}(\varphi + \varphi')$, we have that

$$\operatorname{ord}_{\infty_+}(uq) \geq \min\{k - d + l + 1, -k\}.$$

If $k > \frac{d-l-1}{2}$, then the previous minimum is exactly $-k$, and we obtain that $-\deg q \geq -k + d$. Using (3.12), we have that

$$\operatorname{ord}_{\infty_+}(\varphi) \geq \min\{l + 1, l\} \geq 1.$$

This means that $qp_n - pq_n$ vanishes at infinity, so as before it has to be identically zero. Since we have $\deg q \leq k - d$ and p_n and q_n are coprime, this implies that, after replacing p and q by suitable scalar multiples, $p = p_n$ and $q = q_n$. But then the divisorial relation (3.11) shows that $\deg a_n \geq l + 1$, which contradicts our assumption. Hence we proved that if $k \in B(l) \cap A(l + 1)$, then $k \leq \frac{d-l-1}{2}$ as wanted. □

To ease the notation, for every $l \geq 1$ we will denote by $D(l) := B(l) \cap A(l + 1)$ and by $C_{>l} := \bigcup_{i>l} C(i)$.

Lemma 3.71. *For every $l \geq 1$, we have that $B(l) = D(l) \cup \big(A(l) \setminus \big(A(l + 1) \cup C_{>l}\big)\big)$.*

Proof. The inclusion $\subseteq$ was shown in Lemmas 3.68, 3.69 and 3.70, so it enough to prove that the inclusion $\supseteq$ holds as well. By definition, $D(l) \subseteq B(l)$, so we have only to care about the second set. Take $k \in A(l) \setminus \big(A(l+1) \cup C_{>l}\big)$; then, we have $k\delta \in W_{d-l}$; moreover, we can assume that $k \notin D(l)$. As in the proof of Lemma 3.70, there exist two polynomials p and q in $K[t]$ such that the divisorial relation

$$\operatorname{div}(p - qu) = -k((\infty_-) - (\infty_+)) + \sigma - (d - l)(\infty_+) \tag{3.13}$$

holds, where σ is an effective divisor of degree $d - l$. Moreover, as in the previous Lemma, we have that if $k \notin D(l)$, then $\deg q \leq k - d$.

A priori p and q need not be coprime, but we can prove the quotient p/q is a convergent in the continued fraction expansion of $\sqrt{D}$. Indeed, if r is the greatest common divisor between p and q, we can set $p = rp'$ and $q = rq'$. It is now easy to see that the rational function $p' - uq'$ has a zero at ∞_+ of order at least $k - d + l \geq \deg(q') + 1$, hence $p'/q' = p/q$ is a convergent by Proposition 3.20. Eventually replacing r by a suitable scalar multiple, this implies that there exists $n \geq 1$ such that $p = rp_n$ and $q = rq_n$.

Before showing that p and q are actually coprime, let us prove that the support of σ does not contain (∞_+). Indeed if this is not the case, then we can write $\sigma = \sigma' + (\infty_+)$. Then we find

$$\operatorname{div}(p - qu) = -k(\infty_-) - (\infty_+) + \sigma' - (d - l - 1)(\infty_+),$$

which in turn implies that $k \in A(l + 1)$ contrary to our assumption.

Let us finally show that p and q are coprime. As σ is not supported at ∞_+, we have that the order of $p - uq$ at ∞_+ is exactly $k - d + l$. On the other hand, the order of $p - uq$ at ∞_+ is also equal to $\operatorname{ord}_{\infty_+}(r(p_n - q_n u)) = -\deg r + \deg q_n + \deg a_n$. Using that $\deg q_n = \deg p_n - d$, we have that $\deg a_n + \deg p_n = k + l + \deg r$. Furthermore, $\deg p_n \leq k - \deg r$, hence $k \in C(l + \deg r)$ contradicting the hypothesis that $k \notin C_{>l}$ if $\deg r \geq 1$.

This implies that, eventually taking suitable scalar multiples, $p = p_n$ and $q = q_n$, hence $k = \deg p_n$ and $l = \deg a_n$, proving that $k \in B(l)$ as wanted. □

We will finally prove Theorem 3.30 for squarefree D using an inductive argument on l.

Proof of Theorem 3.30 for squarefree D. As we have noticed in 3.67, to prove that the sequence of $(\deg a_n)_n$ is eventually periodic it suffices to prove that for every $l \geq 1$ the set $B(l)$ is eventually periodic. This is certainly true for $l \geq d+1$, because in this case $B(l)$ is empty.

We proceed by downward induction on l. Fix $l \geq 1$, and suppose that $B(l')$ is eventually periodic for all $l' > l$. For every $i > l$, we can write $C(i)$ as

$$C(i) = \bigcup_{h \geq 1} \{B(i+h) + h\};$$

hence, using the inductive hypothesis, any of these $C(i)$ for $i > l$ is eventually periodic. This implies that $C_{>l} = \bigcup_{i>l} C(i)$ is also eventually periodic. Finally, applying Theorem 3.63, we have that the sets $A(l)$ and $A(l+1)$ are eventually periodic. From the equality in Lemma 3.71 and the fact that $D(l)$ is at most finite, we deduce that $B(l)$ is eventually periodic as well, proving the Theorem. □

3.10 Solutions to the exercises

Proposition 3.72. *Let $D(t) \in \mathbb{Z}[t]$ be a monic polynomial with the property that D is irreducible over any quadratic extension of $\mathbb{Q}$. Then $D(t)$ is not Pellian.*

Proof. Assume that D is Pellian, *i.e.* that there exist polynomials $A, B \in \mathbb{Q}[t]$ with $B \neq 0$ and

$$A^2 - B^2 D = 1.$$

Suppose moreover that this solution is minimal in terms of the degree of the polynomial A. Rearranging this equality and factorising we obtain

$$(A+1)(A-1) = B^2 D.$$

The two polynomials on the left-hand side are coprime in $\mathbb{Q}[t]$, and D is irreducible, therefore we can write (up to changing the sign of A)

$$\begin{cases} A+1 &= E^2/\alpha \\ A-1 &= \alpha C^2 D \end{cases}$$

where $\alpha \in \mathbb{Q}^*$ and $C, E \in \mathbb{Q}[t]$ are two polynomials such that $B = CE$. By taking the difference of these two equations and multiplying by α we obtain

$$2\alpha = E^2 - \alpha^2 C^2 D$$

which leads to

$$D = \frac{E^2 - 2\alpha}{\alpha^2 C^2}.$$

Let now $\beta = \sqrt{2\alpha}$. Then we have the factorisation over $\mathbb{Q}(\beta)$.

$$D = \frac{(E+\beta)(E-\beta)}{\alpha^2 C^2}.$$

Notice that $\beta \notin \mathbb{Q}$, otherwise $(E/\beta, \alpha C/\beta)$ would be a solution to the original Pell equation with $\deg E < \deg A$. Hence we see that on the right-hand side, after cancelling the denominator, there must be an even number of irreducible factors in $\mathbb{Q}(\beta)[t]$, against the hypothesis on D. □

Proposition 3.73. *Let $D \in \mathbb{Z}[t]$ be a monic polynomial irreducible over $\mathbb{Q}$, and assume that, for every prime p, D is not a square modulo p. Then, $D(t)$ is not Pellian.*

Proof. Assume that D is Pellian, i.e. there exist polynomials $A, B \in \mathbb{Q}[t]$, with $B \neq 0$, such that

$$A^2 - B^2 D = 1. \tag{3.14}$$

Suppose moreover that this solution is minimal in terms of the degree of the polynomial A. If we get rid of denominators, we obtain

$$a^2 A^2 - b^2 B^2 D = u^2,$$

with $A, B \in \mathbb{Z}[t]$ primitive polynomials and $a, b, u \in \mathbb{Z}$ with a, b, u pairwise coprime.

Suppose that $u^2 \neq 1$; then, if p is a prime dividing u and we reduce mod p, we have $b^2 B^2 D \equiv a^2 A^2 \mod p$, hence D is a square modulo p, contradicting the hypothesis. Moreover, if $a^2 \neq 1$ and we reduce modulo a prime p dividing a, then we have $B^2 D \equiv (b^2)^{-1} \mod p$ that is impossible as D is monic by hypothesis.
So we reduced to an equation of the form

$$A^2 - b^2 B^2 D = 1,$$

with $A, B \in \mathbb{Z}[t]$ primitive polynomials and $b \in \mathbb{Z}$.

Notice that b must be even, otherwise we would have that D is a square modulo 2 contradicting the hypothesis. Let us then write $b = 2^k b'$ with $k \geq 1$ and $(b', 2) = 1$.
Let us rewrite our equation as $A^2 - 1 = b^2 B^2 D$, *i.e.*

$$(A+1)(A-1) = b^2 B^2 D.$$

Since D is irreducible, D will divide one of the two factors.

As $(A+1, A-1) = 2$, then we can write (up to changing the sign of A)

$$\begin{cases} A+\epsilon = 2^{\alpha} e^2 E^2 \\ A-\epsilon = 2^{2k-\alpha} c^2 C^2 D \end{cases}$$

where $B = CE$ with $C, E \in \mathbb{Z}[t]$ and $(C, E) = 1$, $b^2 = 2^{2k} c^2 e^2$ with $(c, e) = 1$, $\epsilon = \pm 1$ and $\alpha = 1$ or $\alpha = 2k-1$.

Taking the difference between these two equations we have

$$\pm 2 = 2^{\alpha} e^2 E^2 - 2^{2k-\alpha} c^2 C^2 D$$

hence, dividing by 2, we have

$$\pm 1 = 2^{\alpha-1} e^2 E^2 - 2^{2k-\alpha-1} c^2 C^2 D.$$

Notice that we can exclude that $\alpha = 2k-1$, because otherwise D would be a square modulo 2, contradicting the hypothesis. So $\alpha = 1$ and the equation reduces to

$$e^2 E^2 - 2^{2k-2} c^2 C^2 D = \pm 1.$$

As done before, we have that $e^2 = 1$, otherwise if p is a prime dividing e ($p \neq 2$) and we reduce modulo p, we have $2^{2k-2} c^2 C^2 D \equiv \pm 1 \mod p$ which is impossible as D is monic.
So, we reduced to an equation of the form

$$E^2 - 2^{2k-2} c^2 C^2 D = \pm 1.$$

If the sign on the right-hand side is a plus, then $(E, 2^{k-1} cC)$ is again a solution of the Pell equation (3.14) for D, with $\deg E < \deg A$. But A was chosen to have minimal degree, which gives a contradiction.

Therefore we can assume that

$$E^2 - 2^{2k-2} c^2 C^2 D = -1. \tag{3.15}$$

If $2k-2 = 0$ then D is a square modulo 2, which contradicts our hypothesis.

On the other hand, if $2k-2 \geq 2$, we have that $E^2 \equiv 1 \mod 2$, hence $E = 2F+1$ with $F \in \mathbb{Z}[t]$. If we substitute in (3.15), we have

$$2^{2k-2} c^2 C^2 D - (1+2F)^2 = 1,$$

hence

$$2^{2k-2} c^2 C^2 D - 4F^2 - 4F = 2,$$

which gives a contradiction reducing modulo 4, thus concluding the proof. □

Remark 3.74. Notice that, in the previous proposition, the hypothesis *"for every prime p, D is not a square modulo p"* cannot be improved. Take for example

$$D(t) = t^2 + t + 1.$$

Then, D is Pellian, in fact:

$$\left(\frac{8}{3}t^2 + \frac{8}{3}t + \frac{5}{3}\right)^2 - \left(\frac{8}{3}t + \frac{4}{3}\right)^2 (t^2 + t + 1) = 1.$$

Moreover, D is monic and irreducible over $\mathbb{Q}$ and D is not a square modulo p for every prime $p \neq 3$ (we have instead that $t^2 + t + 1 \equiv (t+2)^2 \mod 3$). Furthermore, notice that 3 is exactly the prime which appears in the denominators of the solution of the Pell's equation, as also shown in the proof of the proposition.

Proposition 3.75. *Let $D \in \mathbb{Z}[t]$ be a monic polynomial. Assume D is irreducible over $\mathbb{Q}_2(\sqrt{5})$ and not a square modulo 2; then D is not Pellian.*

Proof. Assume that D is Pellian, i.e. there exist polynomials $A, B \in \mathbb{Q}[t]$, with $B \neq 0$, such that

$$A^2 - B^2 D = 1. \tag{3.16}$$

Suppose moreover that this solution is minimal in terms of the degree of the polynomial A. If we get rid of denominators, we obtain

$$a^2 A^2 - b^2 B^2 D = u^2,$$

with $A, B \in \mathbb{Z}[t]$ primitive polynomials and $a, b, u \in \mathbb{Z}$ with a, b, u pairwise coprime.

Suppose $a^2 \neq 1$; if we reduce modulo a prime p dividing a, then we have $B^2 D \equiv (b^2)^{-1} \mod p$ that is impossible as D is monic by hypothesis.
So we reduced to an equation of the form

$$A^2 - b^2 B^2 D = u^2,$$

with $A, B \in \mathbb{Z}[t]$ primitive polynomials and $b, u \in \mathbb{Z}$.

Notice that b must be even, otherwise we would have that D is a square modulo 2 contradicting the hypothesis. Let us then write $b = 2^k b'$ with $k \geq 1$ and $(b', 2) = 1$.
Let us rewrite our equation as $A^2 - u^2 = b^2 B^2 D$, *i.e.*

$$(A + u)(A - u) = b^2 B^2 D.$$

Since D is irreducible, D will divide one of the two factors. As $(A + u, A - u) = 2$, we can write (up to changing the sign of A and u)

$$\begin{cases} A + u = 2^{\alpha} e^2 E^2 \\ A - u = 2^{2k-\alpha} c^2 C^2 D \end{cases}$$

where $B = CE$ with $C, E \in \mathbb{Z}[t]$ and $(C, E) = 1$, $b^2 = 2^{2k}c^2e^2$ with $(c, e) = 1$, and $\alpha = 1$ or $\alpha = 2k - 1$.

Taking the difference between these two equations we have

$$2u = 2^{\alpha}e^2E^2 - 2^{2k-\alpha}c^2C^2D,$$

hence, dividing by 2, we have

$$2^{\alpha-1}e^2E^2 - 2^{2k-\alpha-1}c^2C^2D = u.$$

Notice that we can exclude that $\alpha = 2k - 1$, because otherwise D would be a square modulo 2, contradicting the hypothesis. So $\alpha = 1$ and the equation reduces to

$$e^2E^2 - 2^{2k-2}c^2C^2D = u. \tag{3.17}$$

Notice that, if u is a square in $\mathbb{Q}$, then $(eE/\sqrt{u}, 2^{k-1}cC/\sqrt{u})$ is again a solution of the Pell equation (3.16) for D, with $\deg E < \deg A$. But A was chosen to have minimal degree, which gives a contradiction.

Therefore we can assume that u is not a square in $\mathbb{Q}$. We can also assume that $2k - 2 \geq 2$, otherwise D would be a square modulo 2, contradicting the hypothesis.

We can then rewrite D as

$$D = \frac{e^2E^2 - u}{2^{2k-2}c^2C^2}. \tag{3.18}$$

As u is odd and $D \in \mathbb{Z}[t]$, we have that $4 \mid (e^2E^2 + u)$; In particular, this means that all coefficients of monomials of positive degree in E are even and, as u is odd, the constant term of e^2E^2 is congruent to 1 modulo 4. This means that $u \equiv 1 \mod 4$. If we factorize D, we obtain

$$D = \frac{(eE + \sqrt{u})(eE - \sqrt{u})}{2^{2k-2}c^2C^2},$$

which gives a non trivial factorization in $\mathbb{Q}(\sqrt{u})$ as u is not a square in $\mathbb{Q}$. Notice that this also gives a non trivial factorization in $\mathbb{Q}_2(\sqrt{5})$ because, if u is congruent to 1 modulo 8, then u is a square in $\mathbb{Q}_2$ while, if u is congruent to 5 modulo 8, then it is a square in $\mathbb{Q}_2(\sqrt{5})$, contradicting the hypothesis that D is irreducible over $\mathbb{Q}_2(\sqrt{5})$. This proves the proposition. □

[45] M. Rapoport, Th. Zink: *Period Spaces for p-divisible Groups*, Annals of Mathematics Studies **141**, Princeton University Press (1996).

[46] J.D. Rogawski: *Representations of $GL(n)$ and division algebras over a p-adic field*, Duke Mathematical Journal **50**:1 (1983), 161-196.

[47] S. Shatz: *Group Schemes, Formal Groups and p-Divisible Groups*, Cornell, Silverman (eds.), Arithmetic Geometry, Springer (1986).

[48] P. Scholze: *Perfectoid spaces*, Publ. Math. Inst. Hautes Études Sci. **116** (2012), 245-313.

[49] *Peter Scholze's lectures on p-adic geometry*, taken by Jared Weinstein (2014); available at `math.bu.edu/people/jsweinst/Math274/ScholzeLectures.pdf`.

[50] P. Scholze, J. Weinstein: *Moduli of p-divisible groups*, Camb. J. Math. **1**:2 (2013), 145-237.

[51] J. Tate: *p-divisible groups*, Springer (ed.), Proceedings of a Conference on Local Fields (Driebergen 1966), Springer, (1967).

[52] T. Wedhorn: *Adic spaces*, preprint (2012); available at `math.stanford.edu/~conrad/Perfseminar/refs/wedhornadic.pdf`.

[53] *Expository lecture notes from the Arbeitsgemeinschaft on "Geometric Langlands"*, taken by Tony Feng (2016); available at `web.stanford.edu/~tonyfeng/Arbeitsgemeinschaft2016.html`.

Minicourse Zannier:

[ACZ18] Y. André, P. Corvaja and U. Zannier: *The Betti map associated to a section of an abelian scheme (with an appendix by Z. Gao)*, arXiv:1802.03204 (2018).

[Ber13] D. Bertrand: *Unlikely intersections in Poincaré biextensions over elliptic schemes*, Notre Dame J. Form. Log. **54** (2013), no. 3-4, 365-375;

[Ber15] D. Bertrand: *Generalized jacobians and Pellian polynomials*, J. Thor. Nombres Bordeaux 27 (2015), no. 2, 439-461.

[BC97] E. Bombieri, P. B. Cohen: *Siegel's lemma, Padé approximations and Jacobians*, Ann. Sc. Norm. Super. Pisa, Cl. Sci., IV. Ser. **25**, No. 1-2 (1997), 155-178.

[BMPZ11] D. Bertrand, D. Masser, A. Pillay, and U. Zannier: *Relative Manin-Mumford for semi-abelian surfaces*, Proc. Edinb. Math. Soc., No.4 (2016), 837-875.

[CMZ13] P. Corvaja, D. Masser and U. Zannier: *Sharpening Manin-Mumford for Certain Algebraic Groups of dimension 2*, Enseign. Math., (with a letter of Serre to Masser as an appendix), **59**, no. 3-4 (2013), 225-269.

[CVZ18] L. Capuano, F. Veneziano and U. Zannier: *An effective criterion for periodicity of ℓ-adic continued fractions*, Math. Comp., published electronically 2018.

[Coh77] J. H. E. Cohn: *The length of the period of the simple continued fraction of $\sqrt{d}$*, Pacific J. Math. **71** (1977), 21-32.

[CMZ16] P. Corvaja, D. Masser and U. Zannier: *Torsion hypersurfaces on abelian schemes and Betti coordinates*, preprint (2016), 40 p.

[Eu1767] L. Euler: *De usu novi algorithmi in problemate pelliano solvendo*, Novi Commentarii acad. sci. Petropol. **11** (1767), 29-66.

[Hoo42] R. Hooke: *Linear p–adic groups and their Lie algebras*, Annals of Math. **43(4)** (1942), 641-655.

[Khi97] A. Ya. Khinchin: *Continued fractions*, Dover Pub. (1997).

[Lan65] S. Lang: *Division points on curves*, Ann. Mt. Pura Appl. **70** (1965), no. 4, 229-234.

[Lau94] M. Laurent: *Équations diophantiennes exponentielles*, Invent. Math. **78** no. 2 (1994), 299-327.

[Mal16] F. Malagoli: *Continued fractions in function fields: polynomial analogues of McMullen's and Zaremba's conjectures*, PhD Thesis (2016).

[Len02] H. W. Lenstra, Jr. : *Solving the Pell Equation*, Notices of the AMS **94** (2002), no. 2, 182-192.

[MZ15] D. Masser and U. Zannier, *Torsion points on families of simple abelian surfaces and Pells equation over polynomial rings*, J. Eur. Math. Soc. (JEMS) 17, no. 9 (2015), 2379-2416, With an appendix by E. V. Flynn.

[Mah34] K. Mahler: *Zur Approximation P-adischer Irrationalzahlen*, Nieuw Arch. Wisk. **18** (1934), 22-34.

[McL03] J. McLaughlin: *Polynomial solutions of Pell's equation and fundamental units in real quadratic fields*, J. London Math. Soc. **67**, no. 1 (2003), 16-28.

[McM09] C. McMullen: *Uniformly Diophantine numbers in a fixed real quadratic field.*, Compos. Math. **145**, no. 4 (2009), 827-844.

[Mer16] O. Merkert: *Reduction and specialiation of hyperelliptic continued fractions*, PhD Thesis (2016).

[Nat76] M. B. Nathanson: *Polynomial Pell's Equations.*, Proceedings of the AMS **56** (1976), 89-92.

[Pla12] V. P. Platonov: *Number-theoretic properties of hyperelliptic fields and the torsion problem in Jacobians of hyperelliptic curves over the rational number field*, Uspekhi Mat. Nauk 69 **415**, no. 1 (2014), 3-38.

[PT00] A. J. van der Poorten and X. C. Tran: *Quasi-elliptic integrals and periodic continued fractions*, Monatsch. Math. **131** (2000), 155-169.

[Ros54] M. Rosenlicht: *Generalised Jacobian Varieties*, Annals of Math. **59** (1954), 505-530.

[Ru00] M. Ru: *A weak effective Roths theorem over function fields*, Rocky mountain J. of Math. **30** (2000), 723-734.

[Rub70] A. Ruban: *Certain metric properties of the p-adic numbers*, Sibirsk. Mat. Z. **11** (1970), 222-227.

[SA94] P. Sarnak and S. Adams: *Betti numbers of congruence groups (with an appendix by Zeev Rudnick*, Israel J. Math. **88** nos. 1-3 (1994), 31-72.

[Sch15] H. Schmidt: *Multiplication polynomials and relative Manin-Mumford*, PhD Thesis (2015).

[Ser88] J. P. Serre: *Algebraic Groups and Class Fields*, Springer-Verlag GTM **117** (1988).

[Ser75] J. P. Serre: *Groupes algébriques et corps de classes*, Actualites sci. et ind., Hermann, Paris (1975).

[Son04] J. Sondow: *Irrationality Measures, Irrationality Bases, and a Theorem of Jarnik*, preprint, arXiv:0406300 (2004).

[S$^+$09] *SageMath, the Sage Mathematics Software System (Version 6.5)*, The Sage Developers, 2016, `http://www.sagemath.org`.

[Uch61a] S. Uchiyama: *Rational approximation to algebraic functions*, J.Fac.Sci. Hokkaido Univ. 15 (1961), 173-192.

[vdP98] A. J. van der Poorten: *Formal power series and their continued fraction expansion*, Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin (1998), 358-371.

[vdP99] A. J. van der Poorten: *Reduction of continued fractions of formal power series*, Continued fractions: from analytic number theory to constructive approximation (Columbia, MO, 1998), Contemp. Math., vol. 236, Amer. Math. Soc., Providence, RI (1999), 343-355.

[vdP99] A. J. van der Poorten, *Non-periodic continued fractions in hyperelliptic function fields*, Bull. Austral. Math. Soc. 64 (2001), no. 2, 331-343.

[Wan96] J. Wang: *An effective Roth's theorem for function fields*, Rocky Mountain J. of Math. **26** (1996), 1225-1234.

[Zan09] U. Zannier: *Lecture Notes on Diophantine Analysis*, Edizioni della Normale, (2009). With an appendix by Francesco Amoroso.

[Zan12] U. Zannier: *Some Problems of Unlikely Intersections in Arithmetic and Geometry*, Princeton University Press, (2012). With appendixes by David Masser.

[Zan14] *Unlikely Intersections and Pell's equations in polynomials*, Trends in Contemporary Mathematics, Springer INdAM Series, **8** (2014), 151-169.

[Zan16] U. Zannier: *Hyperelliptic Continued Fractions and Generalized Jacobians*, Amer. J. Math., to appear.

Minicourse Zhang:

[54] G. Anderson: *Logarithmic derivatives of Dirichlet L-functions and the periods of abelian varieties*, Compos. Math. **45** (1982), 315-332.

[55] Y. André: *Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire*, J. Reine Angew. Math. **505** (1998), 203–208.

[56] F. Andreatta, E. Goren, B. Howard, and K. Madapusi-Pera: *Faltings heights of abelian varieties with complex multiplication*, Annals of Math. **187** (2018), 391–531.

[57] S. J. Arakelov: *Families of algebraic curves with fixed degeneracies*, Izv. Akad. Nauk SSSR Ser. Mat. **35** (1971), no. 6, 1269-1293.

[58] Y. Bilu, F. Luca, and D. Masser: *Collinear CM-points*, Algebra Number Theory, Volume 11, number 5 (2017), 1047–1087.

[59] Y. Bilu, D. Masser, and U. Zannier: *An effective Theorem of André for CM-points on a plane curve*, Math. Proc. Cambridge Philos. Soc. **154** (2013), 145–152.

[60] H. Carayol: *Sur la mauvais réduction des courbes de Shimura*, Compos. Math. **59** (1986), 151-230.

[61] C-L. Chai, B. Conrad, and F. Oort: *Complex Multiplication and Lifting Problems*, American Mathematical Society (2014).

[62] S. Chowla: *On a conjecture of Marshall Hall*, Proc. Nat. Acad. Sci. **56** (1966), 417-418.

[63] S. Chowla: *Remarks on class-invariants and related topics, chapter VI of Seminar on Complex Multiplication (eds A. Borel et al.)* Lect. Notes Math. **21** (1966)

[64] S. Chowla and A. Selberg: *On Epstein's zeta function. I*, Proceedings of the National Academy of Sciences of the United States of America **35** (1949), 371-374.

[65] S. Chowla and A. Selberg: *On Epstein's Zeta-function*, Journal für die reine und angewandte Mathematik **227** (1967), 86-110.