rijksuniversiteit groningen
faculteit Wiskunde en Natuurwetenschappen

Polynomial Pell's equation and continued fractions over finite fields

Bacheloronderzoek Wiskunde

2013

Student: J.H. Stegink

Eerste Begeleider: prof. dr. J. Top

Tweede Begeleider: prof. dr. H.W. Broer

Abstract

To obtain solutions of Pell's equation for polynomials in $K[X]$, one can try to use the same method as in the integer case. That is, to express the square root as a continued fraction. And examine wether some of the partial continued fractions (convergents) provide solutions to Pell's equation.

The continued fraction expression is found with an algorithm similar to the one used in classical number theory to find the continued fraction of an irrational number. We investigate this method.

Contents

Chapter 1

Introduction

Pell's equation is a diophantine equation mistakingly named after John Pell by Euler. The original equation is as follows:

$$x^2 - d \cdot y^2 = 1 \tag{1.1}$$

where x, y and $d > 0$ are integers and d is not a perfect square. In the classical case, one can find non trivial solutions by finding the continued fraction expansion of $\sqrt{d}$.
For the polynomial case, we will look at a slightly different version of the equation:

$$x^2 - f \cdot y^2 = 1 \tag{1.2}$$

where f is a nonsquare polynomial. To find solutions in the polynomial case, we attempt to express $\sqrt{f}$ as a continued fraction.

Continued fractions of integers and polynomials have many properties in common, but some things cannot be translated from one to the other.

Chapter 2

Integer Continued Fractions

2.1 Basics

In this chapter, we explain the basics of continued fractions and show some properties based on chapter 12 from [2].

An integer continued fraction is an expression of the following form:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{... + \cfrac{1}{a_n}}}}$$

in which all $a_i \in \mathbb{Z}$ and $a_i > 0$ for $i > 0$. We can also denote this expression as $x = [a_0; a_1, ..., a_n]$, which saves space.
Given that $x \in \mathbb{Q}$, it can be expressed as a finite continued fraction. The coefficients a_i of which can be found using the Euclidian algorithm. As an example, look at $\frac{105}{143}$:

$$\begin{array}{c|c} 105 = 0 * 143 + 105 & {}^{105}/_{143} = 0 + {}^{105}/_{143} \\ 143 = 1 * 105 + 38 & {}^{143}/_{105} = 1 + {}^{38}/_{105} \\ 105 = 2 * 38 + 29 & {}^{105}/_{38} = 2 + {}^{29}/_{38} \\ 38 = 1 * 29 + 9 & {}^{38}/_{29} = 1 + {}^{9}/_{29} \\ 29 = 3 * 9 + 2 & {}^{29}/_{9} = 3 + {}^{2}/_{9} \\ 9 = 4 * 2 + 1 & {}^{9}/_{2} = 4 + {}^{1}/_{2} \end{array}$$

The coefficients for the continued fraction are the integers on the right hand side of the table and the final fraction is also included. So the continued fraction expansion for $\frac{105}{143}$ is:

$$\frac{105}{143} = 0 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \frac{1}{2}}}}}}$$

or $\frac{105}{143} = [0; 1, 2, 1, 3, 4, 2]$.
Given $(a_i)_{i\geq 0}$, with $a_i \in \mathbb{Z}$ and $a_1 > 0$ for $i > 0$, the sequence $([a_0; a_1, ..., a_n])_{n\geq 1}$ is known to converge. The limit is called an infinite continued fraction and is denoted $[a_0; a_1, ...]$. Any $x \in \mathbb{R}$ can be expressed as a (possibly infinite) continued fraction. An algorithm for finding the coefficients for an irrational numer α is to take:

$$\begin{aligned} \alpha &= \alpha_0 \\ a_k &= [\alpha_k] \\ \alpha_{k+1} &= \frac{1}{\alpha_k - a_k} \end{aligned}$$

where $[\alpha_k]$ is the integer part of α_k. As an example, we will look at the continued fraction expansion of $\sqrt{6}$.

$$\begin{array}{l|l} \alpha_0 = \sqrt{6} & a_0 = 2 \\ \alpha_1 = \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2} & a_1 = 2 \\ \alpha_2 = \frac{2}{\sqrt{6}-2} = \sqrt{6}+2 & a_2 = 4 \\ \alpha_3 = \frac{1}{\sqrt{6}-2} = \alpha_1 & a_3 = a_1 = 2 \end{array}$$

So the continued fraction expansion of $\sqrt{6}$ is $[2; 2, 4, 2, 4, 2, 4, ...]$ or $[2; \overline{2, 4}]$. This expansion is periodic, because $\alpha_3 = \alpha_1$. Not every irrational number has a periodic expansion, for example $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, ...]$.

2.2 Theorems

Now we will show some properties of continued fractions, finishing with a proof of why certain expansions must be periodic.

Definition 1. *The kth convergent C_k of the infinite continued fraction of $x \in \mathbb{R} \setminus \mathbb{Q}$; $x = [a_0; a_1, ...]$ is the partial continued fraction $[a_0; a_1, ..., a_k]$.*

As mentioned before, it is known that the C_k converge, in this case to x, as k goes to infinity.

Theorem 1. *Let a_0,a_1,... be integers and let p_0,p_1,... and q_0,q_1,... be defined recursively by:*

$$\begin{array}{ll} p_0 = a_0 & q_0 = 1 \\ p_1 = a_0 a_1 + 1 & q_1 = a_1 \\ p_k = a_k p_{k-1} + p_{k-2} & q_k = a_k q_{k-1} + q_{k-2} \end{array}$$

for $k = 2, 3, ...$
Then the kth convergent $C_k = [a_0; a_1, ..., a_k]$ is given by $C_k = \frac{p_k}{q_k}$.

Proof. This theorem can be proved with mathematical induction; we will first find the three initial convergents.

$$C_0 = [a_0] = \frac{a_0}{1} = \frac{p_0}{q_0}$$

$$C_1 = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$$

$$C_2 = [a_0; a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_2(a_0a_1 + 1) + a_0}{a_2a_1 + 1} = \frac{p_2}{q_2}$$

So the theorem holds for $k = 0, 1, 2$. Assume it holds for a certain $k \geq 2$, so that

$$C_k = [a_0; a_1, a_2, ..., a_k] = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}} \tag{2.1}$$

Because the theorem holds for this k, all the p_js and q_js depend on $a_0, ..., a_{k-1}$. So we can replace a_k by $a_k + \frac{1}{a_{k+1}}$ in (2.1) to obtain the following:

$$\begin{aligned} C_{k+1} &= [a_0; a_1, ..., a_{k-1}, a_k, a_{k+1}] \\ &= [a_0; a_1, ..., a_{k-1}, a_k + \frac{1}{a_{k+1}}] \\ &= \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + p_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}} \end{aligned}$$

So by the principle of mathematical induction, this finishes the proof. □

Now we can state and prove the next important property:

Theorem 2. *Let $C_k = \frac{p_k}{q_k}$ be the kth convergent of the continued fraction $[a_0; a_1, ...]$, with $k > 0$. If the p_k and q_k are defined as in theorem (1), then*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Proof. This theorem can also be proved using mathematical induction. For $k = 1$, we get

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1) * 1 - a_0 a_1 = 1.$$

Assume the theorem holds for a certain $k \geq 1$, so that

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Then we have

$$\begin{aligned} p_{k+1}q_k - p_k q_{k+1} &= (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k+1}) \\ &= p_{k-1}q_k - p_k q_{k-1} \\ &= -(-1)^{k-1} = (-1)^k \end{aligned}$$

So by the principle of mathematical induction, this finishes the proof. □

Note that the property in Theorem 2 implies that $gcd(p_k, q_k) = 1$.
It also leads to the following useful corollary:

Corollary 1. *Let $C_k = \frac{p_k}{q_k}$ be the kth convergent of the continued fraction $[a_0; a_1, ...]$. Then*

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

for all integers $k \geq 1$ and

$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}$$

for all integers $k \geq 2$.

Proof. Subtracting the fractions and applying theorem 2 shows that the first identity holds;

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{p_k q_{k-1} - p_{k-1} q_k}{q_k q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}.$$

The second identity is not as straightforward:

$$C_k - C_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}}.$$

Now substitute $p_k = a_k p_{k-1} + p_{k-2}$ and $q_k = a_k q_{k-1} + q_{k-2}$ and we get the second identity:

$$\begin{aligned} C_k - C_{k-2} &= \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}} \\ &= \frac{(a_k p_{k-1} + p_{k-2}) q_{k-2} - p_{k-2}(a_k q_{k-1} + q_{k-2})}{q_k q_{k-2}} \\ &= \frac{a_k(p_{k-1} q_{k-2} - p_{k-2} q_{k-1})}{q_k q_{k-2}} \\ &= \frac{a_k(-1)^{k-2}}{q_k q_{k-2}} = \frac{a_k(-1)^k}{q_k q_{k-2}} \end{aligned}$$

□

For the following theorems we first need to define what a "quadratic irrationality" is, as the properties of such a number are necessary for the proofs.

Definition 2. *The real number α is said to be a quadratic irrationality if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.*

Because of this, α can always be written as

$$\alpha = \frac{a + \sqrt{b}}{c}.$$

Lemma 1. *If α is a quadratic irrationality, then α can be written as*

$$\alpha = \frac{P + \sqrt{d}}{Q},$$

where P, Q and d are integers, $Q \neq 0$, $d > 0$, d is not a perfect square and $Q|(d - P^2)$.

Proof. Because α is a quadratic irrationality,

$$\alpha = \frac{a + \sqrt{b}}{c},$$

where a, b and c are integers, $b > 0$ and $c \neq 0$. Multiplying both the numerator and denominator by $|c|$ we obtain:

$$\alpha = \frac{a|c| + \sqrt{bc^2}}{c|c|}$$

Now, let $P = a|c|$, $Q = c|c|$ and $d = bc^2$. Then P, Q and d are integers, $Q \neq 0$ because $c \neq 0$, $d > 0$ because $b > 0$, d is not a perfect square because $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\alpha)$ is quadratic over $\mathbb{Q}$ and $Q|(d-P^2)$ because $d-P^2 = bc^2-a^2c^2 = c^2(b-a^2) = \pm Q(b-a^2)$. $\square$

One final theorem is needed before the periodicity of the continued fraction expression of quadratic irrationalities can be proved, which contains an adapted algorithm for creating the continued fraction expansion of a quadratic irrationality.

Theorem 3. *Let α be a quadratic irrationality, so by lemma 1 there are integers P_0, Q_0 and d such that*

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0},$$

where $Q_0 \neq 0$, $d > 0$, d is not a perfect square and $Q_0|(d - P_0^2)$. Recursively define

$$\begin{aligned} \alpha_k &= \frac{P_k + \sqrt{d}}{Q_k}, \\ a_k &= [\alpha_k], \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k}, \end{aligned}$$

for $k \geq 0$. Then $\alpha = [a_0; a_1, a_2, ...]$

Proof. First we need to show that P_k and Q_k are integers with $Q_k \neq 0$ and $Q_k|(d - P_k^2)$ for all $k \geq 0$. It is obviously so for $k = 0$. Assume it holds for a certain $k \geq 0$.
Then $P_{k+1} = a_k Q_k - P_k$ is also an integer, as for Q_{k+1};

$$\begin{aligned} Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k} \\ &= \frac{d - (a_k Q_k - P_k)^2}{Q_k} \\ &= \frac{d - P_k^2}{Q_k} + 2a_k P_k - a_k^2 Q_k \end{aligned}$$

because $Q_k|(d - P_k^2)$ it follows that Q_{k+1} is an integer, and because d is not a perfect square $d \neq P_{k+1}^2$, so $Q_{k+1} \neq 0$. Also, because

$$Q_k = \frac{d - P_{k+1}^2}{Q_{k+1}}$$

it is clear that $Q_{k+1}|(d - P_{k+1}^2)$.
To show that the a_i are the coefficients of the continued fraction of α we show that for $k \geq 0$

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$$

and $\alpha_j > 1$ for all $j \geq 1$.
Note that because $a_k < \alpha_k < a_k + 1$ we have $0 < \alpha_k - a_k < 1$, so the inverse is always larger than one, so $\alpha_j > 1$ for any $j \geq 1$. And indeed

$$\begin{aligned}
\alpha_k - a_k &= \tfrac{P_k+\sqrt{d}}{Q_k} - a_k \\
&= \tfrac{\sqrt{d}-(a_kQ_k-P_k)}{Q_k} \\
&= \tfrac{\sqrt{d}-P_{k+1}}{Q_k} \\
&= \tfrac{(\sqrt{d}-P_{k+1})(\sqrt{d}+P_{k+1})}{Q_k(\sqrt{d}+P_{k+1})} \\
&= \tfrac{d-P_{k+1}^2}{Q_k(\sqrt{d}+P_{k+1})} \\
&= \tfrac{Q_kQ_{k+1}}{Q_k(\sqrt{d}+P_{k+1})} \\
&= \tfrac{Q_{k+1}}{\sqrt{d}+P_{k+1}} = \tfrac{1}{\alpha_{k+1}}
\end{aligned}$$

Now $\alpha = [a_0; a_1, a_2, ...]$, as we wanted to show. □

Now we can move on to Lagrange's theorem.

Theorem 4. *The infinite continued fraction of an irrational number is periodic if and only if this number is a quadratic irrationality.*

Proof. ($\Rightarrow$) Let the continued fraction of α be periodic, so that

$$\alpha = [a_0; a_1, ..., a_{N-1}, \overline{a_N, a_{N+1}, ..., a_{N+k}}]$$

Now, let

$$\beta = [\overline{a_N, a_{N+1}, ..., a_{N+k}}],$$

then

$$\beta = [a_N; a_{N+1}, ..., a_{N+k}, \beta].$$

So by theorem 1, we see that

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}},$$

where p_k/q_k and p_{k-1}/q_{k-1} are convergents of $[a_N; a_{N+1}, ..., a_{N+k}]$. Hence,

$$q_k\beta^2 + (q_{k-1} - p_k)\beta - p_{k-1} = 0,$$

and because the continued fraction of β is infinite, β is irrational and so β is a quadratic irrationality. Now since

$$\alpha = [a_0; a_1, ..., a_{N-1}, \beta],$$

it follows that

$$\alpha = \frac{\beta p_{N-1} + p_{N-2}}{\beta q_{N-1} + q_{N-2}},$$

where p_{N-1}/q_{N-1} and p_{N-2}/q_{N-2} are convergents of $[a_0; a_1, ..., a_{N-1}]$. Because β is a quadratic irrationality, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Now, since α is irrational and $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\beta)$, it follows that α is a quadratic irrationality. □

Proof. ($\Leftarrow$) Let α be a quadratic irrationality, then by lemma 1 and theorem 3; $\alpha = [a_0; a_1, a_2, ...]$ with a_i as in theorem 3. Because this is the same as $[a_0; a_1, ..., a_{k-1}, \alpha_k]$, theorem 1 gives us the following equality:

$$\alpha = \frac{p_{k-1}\alpha_k + p_{k-2}}{q_{k-1}\alpha_k + q_{k-2}}.$$

Taking conjugates of both sides of this equation, it becomes:

$$\alpha' = \frac{p_{k-1}\alpha'_k + p_{k-2}}{q_{k-1}\alpha'_k + q_{k-2}}.$$

Solving this for α'_k leads to

$$\alpha'_k = \frac{-q_{k-2}}{q_{k-1}}\left(\frac{\alpha' - \frac{p_{k-2}}{q_{k-2}}}{\alpha' - \frac{p_{k-1}}{q_{k-1}}}\right).$$

Since p_{k-2}/q_{k-2} and p_{k-1}/q_{k-1} are convergents of α, they tend to α as k tends to infinity, so the fraction between brackets tends to 1. So there is an integer N such that $\alpha'_k < 0$ for $k \geq N$. Because $\alpha_k > 0$ for $k > 1$ we have

$$0 < \alpha_k - \alpha'_k = \frac{P_k + \sqrt{d}}{Q_k} - \frac{P_k - \sqrt{d}}{Q_k} = \frac{2\sqrt{d}}{Q_k},$$

so $Q_k > 0$ for $k \geq N$. Also, because $Q_k Q_{k+1} = d - P_{k+1}^2$, for $k \geq N$

$$Q_k \leq Q_k Q_{k+1} = d - P_{k+1}^2 \leq d.$$

And

$$P_{k+1}^2 < d = P_{k+1}^2 + Q_k Q_{k+1}$$

so that

$$-\sqrt{d} < P_{k+1} < \sqrt{d}.$$

These inequalities, which hold for $k \geq N$, show that there is only a finite number of possible values for the pair of integers P_k, Q_k for $k > N$. Because there are infinitely many integers k with $k \geq N$, there are two integers i and j such that $P_i = P_j$ and $Q_i = Q_j$ with $i < j$. Hence, from the definition of α_k, it is clear that $\alpha_i = \alpha_j$. Consequently, $a_i = a_j$, $a_{i+1} = a_{j+1}$, etc. Hence,

$$\alpha = [a_0; a_1, a_2, ..., a_{i-1}, \overline{a_i, a_{i+1}, ..., a_{j-1}}].$$

This shows that α has a periodic continued fraction expansion. □

2.3 Reducedness

In this paragraph we will show that the periodic part of a quadratic irrationality always starts at $k = 1$ and that it is palindromic, i.e. $\alpha = [a_0; \overline{a_1, ..., a_n}]$ with $a_n = 2 \cdot a_0$, $a_1 = a_{n-1}$, $a_2 = a_{n-2}$, etc.

Definition 3. *A quadratic irrationality α is called reduced if $\alpha > 1$ and $-1 < \alpha' < 0$, where α' is the conjugate of α*

Since α is a quadratic irrationality, it can be written as $\alpha = (P+\sqrt{D})/Q$, its conjugate is $\alpha' = (P - \sqrt{D})/Q$.

Theorem 5. *The continued fraction of the quadratic irrationality α is purely periodic if and only if α is reduced.*

Proof. ($\Leftarrow$) Assume α is a quadratic irrationality. Recall that the partial fractions of the continued fraction are given by

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k},$$

where $a_k = [\alpha_k]$ for $k = 0, 1, ...$ and $\alpha_0 = \alpha$. It follows that

$$\frac{1}{\alpha_{k+1}} = \alpha_k - a_k,$$

and by taking conjugates, we see that

$$\frac{1}{\alpha'_{k+1}} = \alpha'_k - a_k.$$

Using mathematical induction, we can prove that $-1 < \alpha'_k < 0$ for $k = 0, 1, ...$ First, note that because $\alpha_0 = \alpha$ is reduced, $-1 < \alpha'_0 < 0$. Assume that $-1 < \alpha'_k < 0$, then because $a_k \geq 1 \, \forall k$ (where $a_0 \geq 1$ because $\alpha > 1$), we see that

$$1/\alpha'_{k+1} < -1,$$

so that $-1 < \alpha'_{k+1} < 0$. Hence, $-1 < \alpha'_k < 0$ for $k = 0, 1, ...$ Next note that

$$\alpha'_k = a_k + \frac{1}{\alpha'_{k+1}},$$

and because $-1 < \alpha'_k < 0$ it follows that

$$-1 < a_k + \frac{1}{\alpha'_{k+1}} < 0.$$

Consequently

$$-1 - \frac{1}{\alpha'_{k+1}} < a_k < -\frac{1}{\alpha'_{k+1}},$$

so that

$$a_k = [-\frac{1}{\alpha'_{k+1}}].$$

Because α is a quadratic irrationality, the proof of theorem 4 shows that there are $i, j \in \mathbb{Z}_{>0}$, $i < j$ such that $\alpha_i = \alpha_j$, and hence with $-1/\alpha_i = -1/\alpha_j$. Because $a_{i-1} = [-1/\alpha_i]$ and $a_{j-1} = [-1/\alpha_j]$, it is clear that $a_{i-1} = a_{j-1}$. Furthermore, because $\alpha_{i-1} = a_{i-1} + 1/\alpha_i$ and $\alpha_{j-1} = a_{j-1} + 1/\alpha_j$, it's also clear that $\alpha_{i-1} = \alpha_{j-1}$. Continuing this argument, we see that $\alpha_{i-2} = \alpha_{j-2}$, $\alpha_{i-3} = \alpha_{j-3}$, ..., and, finally, that $\alpha_0 = \alpha_{j-i}$. Since

$$\begin{aligned}\alpha_0 = \alpha &= [a_0; a_1, ..., a_{j-i-1}, \alpha_{j-i}] \\ &= [a_0; a_1, ..., a_{j-i-1}, \alpha_0] \\ &= [\overline{a_0; a_1, ..., a_{j-i}}],\end{aligned}$$

we see that the continued fraction of α is purely periodic. □

Proof. ($\Rightarrow$) Assume that α is a quadratic irrationality with a purely periodic continued fraction, i.e. $\alpha = [\overline{a_0; a_1, ..., a_k}]$. Then, because $\alpha = [a_0; a_1, ..., a_k, \alpha]$, theorem 1 gives us

$$\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}},$$

where p_{k-1}/q_{k-1} and p_k/q_k are the $(k-1)$th and kth convergents of the continued fraction expansion of α. We can rewrite this to obtain

$$q_k\alpha^2 + (q_{k-1} - p_k)\alpha - p_{k-1} = 0.$$

Now let β be a quadratic irrationality such that $\beta = [\overline{a_k; a_{k-1}, ..., a_1, a_0}]$, that is, with the period of the continued fraction of α reversed. Then $\beta = [a_k; a_{k-1}, ..., a_0, \beta]$, so that

$$\beta = \frac{\beta p'_k + p'_{k-1}}{\beta q'_k + q'_{k-1}},$$

where p'_{k-1}/q'_{k-1} and p'_k/q'_k are the $(k-1)$th and kth convergents of the continued fraction expansion of β. Note that

$$p_k/p_{k-1} = [a_k; a_{k-1}, ..., a_1, a_0] = p'_k/q'_k$$

and

$$q_k/q_{k-1} = [a_k; a_{k-1}, ..., a_1] = p'_{k-1}/q'_{k-1}.$$

Because p'_{k-1}/q'_{k-1} and p'_k/q'_k are convergents, they are in lowest terms. Also, p_k/p_{k-1} and q_k/q_{k-1} are in lowest terms, because theorem 2 tells us that $p_kq_{k-1} - p_{k-1}q_k = (-1)^k$. Hence,

$$p'_k = p_k, \quad q'_k = p_{k-1}, \quad p'_{k-1} = q_k, \quad q'_{k-1} = q_{k-1}.$$

Inserting these values into our equation for β, we see that

$$\beta = \frac{\beta p_k + q_k}{\beta p_{k-1} + q_{k-1}}.$$

Rewriting this, we obtain

$$p_{k-1}\beta^2 + (q_{k-1} - p_k)\beta - q_k = 0$$

Which in turn gives,

$$q_k(-1/\beta)^2 + (q_{k-1} - p_k)(-1/\beta) - p_{k-1} = 0.$$

So the two roots of the quadratic equation

$$q_k x^2 + (q_{k-1} - p_k)x - p_{k-1}$$

are α and $-1/\beta$, so that, by the quadratic equation, we have $\alpha' = -1/\beta$. Because $\beta = [\overline{a_k; a_{k-1}, ..., a_1, a_0}]$, we see that $\beta > 1$, so that $-1 < \alpha' = -1/\beta < 0$. Hence α is a reduced quadratic irrationality. Furthermore, note that because $\beta = -1/\alpha'$, it follows that

$$-1/\alpha' = [\overline{a_k; a_{k-1}, ..., a_0}].$$

□

Theorem 6. *Let $d \in \mathbb{Z}_{>0}$ nonsquare. define $\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$, $a_k = [\alpha_k]$, $P_{k+1} = a_k Q_k - P_k$, and $Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}$, for $k = 0, 1, 2...$, where $\alpha_0 = \sqrt{d}$. Furthermore, let p_k/q_k denote the kth convergent of the continued fraction expansion of $\sqrt{d}$. Then*

$$p_k^2 - d \cdot q_k^2 = (-1)^{k-1} Q_{k+1}.$$

Proof. Because $\sqrt{d} = \alpha_0 = [a_0; a_1, ..., a_k, \alpha_{k+1}]$, theorem 1 tells us that

$$\sqrt{d} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}.$$

And since $\alpha_{k+1} = (P_{k+1} + \sqrt{d})/Q_{k+1}$, we have

$$\sqrt{d} = \frac{(P_{k+1} + \sqrt{d})p_k + Q_{k+1} p_{k-1}}{(P_{k+1} + \sqrt{d})q_k + Q_{k+1} q_{k-1}}.$$

Rewriting this, we obtain

$$dq_k + (P_{k+1} q_k + Q_{k+1} q_{k-1})\sqrt{d} = (P_{k+1} p_k + Q_{k+1} p_{k-1}) + p_k \sqrt{d}.$$

This gives us $dq_k = P_{k+1} p_k + Q_{k+1} p_{k-1}$ and $P_{k+1} q_k + Q_k q_{k-1} = p_k$.
Multiply the first of these two equations by q_k and the second by p_k, then subtract the first from the second to get

$$p_k^2 - d \cdot q_k^2 = (p_k q_{k-1} - p_{k-1} q_k) Q_{k+1} = (-1)^{k-1} Q_{k+1},$$

where theorem 2 gives the last equality. □

Chapter 3

Solving Pell's equation; the integer case

Pell's equation, as mentioned earlier, is

$$a^2 - d \cdot b^2 = 1.$$

where $a, b, d \in \mathbb{Z}$, $a, b \neq 0$ and $d > 0$ nonsquare. Solutions are found using the continued fraction expansion of $\sqrt{d}$.

On $\mathbb{Z}[\sqrt{d}]$ we have the norm;

$$N(a + b\sqrt{d}) = a^2 - d \cdot b^2.$$

Any $\alpha = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ is a unit of $\mathbb{Z}[\sqrt{d}]$ if and only if it has $N(\alpha) = \pm 1$, which means if and only if $a^2 - d \cdot b^2 = \pm 1$. So every solution of Pell's equation or the negative variant of Pell's equation is a unit of $\mathbb{Z}[\sqrt{d}]$.

Because $\mathbb{Z}[\sqrt{d}] \subset \mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$, $\sqrt{d}$ can be expressed as a continued fraction. And because $\sqrt{d}$ is a quadratic irrationality, with $P = 0$ and $Q = 1$, its continued fraction expansion is periodic.

All that's left is to find which convergents of the continued fraction of $\sqrt{d}$ actually solve Pell's equation. To do so, we first show that the periodic part of every quadratic irrationality of the form $\alpha = \sqrt{d}$ starts at $k = 1$.

Lemma 2. *The periodic part of every quadratic irrationality of the form $\alpha = \sqrt{d}$ starts at $k = 1$, i.e. $\alpha = [a_0; \overline{a_1, ..., a_n}]$. Furthermore, the periodic part itself is palindromic.*

Proof. It is clear that α is not reduced, as it's conjugate $\alpha' = -\sqrt{d}$, is not between -1 and 0. However, the quadratic irrationality $[\alpha] + \alpha$ is reduced, because it's conjugate, $[\alpha] - \alpha$, does lie between -1 and 0. Therefore, from theorem 5, we know that the continued fraction of $[\alpha] + \alpha$ is purely periodic. Because the initial part of the continued fraction of $[\alpha] + \alpha$ is $[[\alpha] + \alpha] = 2[\alpha] = 2a_0$, we can write

$$\begin{aligned} [\alpha] + \alpha &= \overline{[2a_0; a_1, ..., a_n]} \\ &= [2a_0; a_1, ..., a_n, 2a_0, a_1, ..., a_n, ...] \end{aligned}$$

Subtracting $[\alpha] = a_0$ from both sides, we find that

$$\begin{aligned}\alpha &= [a_0; a_1, ...a_n, 2a_0, a_1, ...] \\ &= [a_0; \overline{a_1, ..., a_n, 2a_0}]\end{aligned}$$

To see that the periodic part is palindromic, note that from theorem 5, the simple continued fraction expansion of $-1/([\alpha] - \alpha)$ can be obtained from that for $[\alpha] + \alpha$ by reversing the period, so that

$$1/(\alpha - [\alpha]) = [\overline{a_n; a_{n-1}, ..., a_1, 2a_0}].$$

But also note that

$$\alpha - [\alpha] = [0; \overline{a_1, a_2, ..., a_n, 2a_0}],$$

so that by taking reciprocals, we find that

$$1/(\alpha - [\alpha]) = [\overline{a_1; a_2, ..., a_n, 2a_0}].$$

Therefore,

$$a_1 = a_n, \quad a_2 = a_{n-1}, \quad ..., \quad a_n = a_1,$$

so that the periodic part of α is palindromic, i.e.

$$\alpha = [a_0; \overline{a_1, a_2, ..., a_2, a_1, 2a_0}].$$

□

Theorem 7. *Let $d \in \mathbb{Z}_{>0}$ nonsquare, let p_k/q_k denote the kth convergent of the continued fraction of $\sqrt{d}$, $k = 1, 2, ...$, and let n be the period length of the continued fraction.*

Then, when n is even, p_k/q_k provides a solution for $p_k^2 - dq_k^2 = 1$ when $k = jn - 1$, with $j = 1, 2, ...$, and provides no solutions for $p_k^2 - dq_k^2 = -1$.

When n is odd, p_k/q_k provides a solution for $p_k^2 - dq_k^2 = 1$ when $k = 2jn - 1$, and provides a solution for $p_k^2 - dq_k^2 = -1$ when $k = (2j-1)n - 1$, with $j = 1, 2, ...$

Proof. From theorem 6, we know that

$$p_k^2 - d \cdot q_k^2 = (-1)^{k-1} Q_{k+1},$$

where Q_{k+1} is defined as before.
Because the period of the continued fraction expansion of $\sqrt{d}$ is n and the period starts at $k = 1$, we know that $Q_{jn} = Q_0 = 1$ for $j = 1, 2, ...$, because $\alpha_0 = \sqrt{d} = \frac{P_0 + \sqrt{d}}{Q_0}$. Hence,

$$p_{jn-1}^2 - d \cdot q_{jn-1}^2 = (-1)^{jn-2} Q_{jn} = (-1)^{jn}.$$

This equality shows that when n is even, (p_{jn-1}, q_{jn-1}) is a solution of $p_k^2 - dq_k^2 = 1$, and when n is odd, (p_{2jn-1}, q_{2jn-1}) is a solution of $p_k^2 - dq_k^2 = 1$, and $(p_{(2j-1)n-1}, q_{(2j-1)n-1})$ is a solution of $p_k^2 - dq_k^2 = -1$. □

As an example, look at $d = \sqrt{6}$. We know the continued fraction of $\sqrt{6}$ is $[2; \overline{2, 4}]$, it's convergents are:

$$\begin{aligned} C_0 &= \frac{2}{1} & C_1 &= \frac{5}{2} \\ C_2 &= \frac{22}{9} & C_3 &= \frac{49}{20} \\ C_4 &= \frac{218}{89} & C_5 &= \frac{485}{198} \end{aligned}$$

Because the period length is 2, only the odd k will solve Pell's equation;

$$\begin{aligned} k = 0 \quad & 4 - 6 * 1 = -2 \\ k = 1 \quad & 25 - 6 * 4 = 1 \\ k = 2 \quad & 484 - 6 * 81 = -2 \\ k = 3 \quad & 2401 - 6 * 400 = 1 \\ k = 4 \quad & 47524 - 6 * 7921 = -2 \\ k = 5 \quad & 235225 - 6 * 39204 = 1 \\ \vdots \quad & \vdots \end{aligned}$$

The continued fraction expansion of $\sqrt{41}$ has an odd period; $\sqrt{41} = [6; \overline{2, 2, 12}]$. With it's first few convergents $C_0 = \frac{6}{1}$, $C_1 = \frac{13}{2}$, and $C_2 = \frac{32}{5}$. Because the period is odd, (p_2, q_2) solves $p^2 - 41 * q^2 = -1$:

$$\begin{aligned} k = 0 \quad & 36 - 41 * 1 = -5 \\ k = 1 \quad & 169 - 41 * 4 = 5 \\ k = 2 \quad & 1024 - 41 * 25 = -1 \end{aligned}$$

It can be shown that the first pair (p_k, q_k) to solve Pell's equation for a certain d, is the smallest solution. That is, the solution (x, y) with $x + y\sqrt{d} > 1$ where $x + y\sqrt{d}$ is as small as possible. Which makes it the smallest, non trivial, unit in $\mathbb{Z}[\sqrt{d}]$.

Chapter 4

Polynomial Continued Fractions

4.1 Basics

A polynomial continued fraction is of the form $[a_0; a_1, ..., a_n]$, in which the a_i are polynomials over a field K, in a variable X and $deg(a_i) > 0$ for $i > 0$. As in the integer case, given $(a_i)_{i\geq 0}$ the sequence $([a_0; a_1, ..., a_n])_{n\geq 1}$ of rational functions in $K(X)$, we would like to have convergence to an infinite continued fraction; $[a_0; a_1, ...]$.
Let $K((\frac{1}{X}))$ be the field of formal power series in the variable $\frac{1}{X}$ over K, with elements

$$\sum_{n=-N}^{\infty} b_n X^{-n},$$

where $b_n \in K$ for all n, and $b_{-N} \neq 0$. In it, we define the norm:

$$\left| \sum_{n=-N}^{\infty} b_n X^{-n} \right| := e^N$$

With respect to this norm, the field $K((\frac{1}{X}))$ is known to be complete, so any Cauchy-sequence in $K((\frac{1}{X}))$ converges. Now, it can be shown that $([a_0; a_1, ..., a_n])_{n\geq 1}$ is a Cauchy-sequence, it converges in $K((\frac{1}{X}))$ with an infinite continued fraction as the limit and that every $\alpha \in K((\frac{1}{X}))$ has such a continued fraction expansion.

In the integer case, for $d \in \mathbb{Z}$ nonsquare, we look at the units of $\mathbb{Z}[\sqrt{d}]$ to find solutions for Pell's equation. To find these units, the continued fraction expansion of $\sqrt{d}$ needs to be constructed. Note that this fraction and all it's convergents are in $\mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$. So starting from the rings $\mathbb{Z} \subset \mathbb{Z}[\sqrt{d}]$ move to the fields $\mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$ that they are subrings of.

Proposition 1. *If $f \in K[X]$ has odd degree, the only $x, y \in K[X]$ that satisfy*

$$x^2 - fy^2 = 1$$

are $(x, y) = (\pm 1, 0)$.

Proof. Say $y \in K[X]$, $y \neq 0$, then $deg(y^2)$ is even, and $deg(fy^2)$ is odd, as well as $deg(fy^2 + 1)$, but since $x^2 - fy^2 = 1$, $deg(fy^2 + 1) = deg(x^2)$ is even. So $y = 0$ and $x^2 = 1$. □

Proposition 2. *If $f \in K[X]$ has leading coefficient a_n which is not a square in K, then the only $x, y \in K[X]$ that satisfy*

$$x^2 - fy^2 = 1$$

are $(x, y) = (\pm 1, 0)$.

Proof. Say $f \in K[X]$ has leading coefficient a_n, nonsquare in K, $y = y_0 + ... + y_k X^k \in K[X]$ and $x = x_0 + ... + x_m X^m \in K[X]$. Then the leading coefficient of fy^2; $a_n y_k^2$ is not a square. Whereas the leading coefficient of x^2; x_m^2 is a square. In that case, $x^2 - fy^2$ doesn't have degree zero, unless $y = 0$ and $m = 0$, and it will only solve the equation when $x = \pm 1$. □

If the leading coefficient of f is a square, say λ^2 for some $\lambda \in K^*$, then dividing f by λ^2 and multiplying b by λ changes the equation $a^2 - fb^2 = \alpha$ into $a^2 - \tilde{f}\tilde{b}^2 = \alpha$ in which $\tilde{f}$ is monic. So without loss of generality, we may assume from now on that f is a monic polynomial.

Now we know that f is monic and has even degree, but we also need f to be nonsquare and have $deg(f) > 0$, because otherwise, the solutions will once again be trivial;

(a) In case $\deg(f) = 0$, then we have $f = 1$ hence the equation is $a^2 - b^2 = \alpha$. This means that $a + b$ and $a - b$ are units in $K[X]$, so they are constant. Write $a + b = \lambda$, then $a - b = \alpha\lambda^{-1}$. This implies $a = \frac{\lambda + \alpha\lambda^{-1}}{2}$ and $b = \frac{\lambda - \alpha\lambda^{-1}}{2}$. In particular, both a and b are constants, and any nonzero $\lambda \in K$ yields a solution a, b.

(b) In case $\deg(f) > 0$ and moreover f is a square, write $f = g^2$ for a polynomial g of positive degree. The equation now looks like $(a + gb)(a - gb) = \alpha$. Arguing as above, one obtains $\lambda \in K^*$ such that $a + gb = \lambda$ and $a - gb = \alpha\lambda^{-1}$. It follows that $gb = \frac{\lambda - \alpha\lambda^{-1}}{2}$. Since g has positive degree, this implies that $b = 0$. Now $a^2 = \alpha$, so a has to be constant, and to have a solution one needs that α is a square in $K^\times$. In particular for $\alpha = 1$, this special case only has the trivial solutions $(a, b) = (\pm 1, 0)$.

To find solutions for Pell's equation, we look at units of $K[X][\sqrt{f}]$. Now, $K[X]$ and $K[X][\sqrt{f}]$ are subrings of the field $K(X)[\sqrt{f}]$. (Compare $\mathbb{Q}[\sqrt{d}]$ in the integer case.)
For the convergence to a continued fraction, we want to move to $K((\frac{1}{X}))$. It is clear that $K(X) \subset K((\frac{1}{X}))$ because $K((\frac{1}{X}))$ is a field that contains both K and X. All that's left is to show that $\sqrt{f} \in K((\frac{1}{X}))$. For that, we expand the definition of the degree of an element of $K[X]$ to $K((\frac{1}{X}))$.

Definition 4. *For $\beta \in K((\frac{1}{X}))$ of the form*

$$\beta = \sum_{n=-d}^{\infty} b_n X^{-n}$$

$deg(\beta) = d$.

Note that this

Lemma 3. *Let K be a field with $char(K) > 2$, then for any $f \in K[X]$ nonsquare, monic and of even degree, $\sqrt{f} \in K((\frac{1}{X}))$.*

Proof. To see that $\sqrt{f} \in K((\frac{1}{X}))$, an element of $K((\frac{1}{X}))$ whose square is f needs to be constructed. First, rewrite f as

$$f = X^{2d}(1 + ... + a_0 X^{-2d}).$$

Now, to find $\sqrt{f}$ we only need to find a $\sum_{n=0}^{\infty} b_n x^{-n} \in K((\frac{1}{X}))$ so that

$$\left(b_0 + \frac{b_1}{X} + ...\right)^2 = 1 + ... + a_0 X^{-2d},$$

or

$$b_0^2 + \frac{2b_0 b_1}{X} + ... = 1 + ... + a_0 X^{-2d}.$$

(For the next step, we use that $char(K) > 2$.) Choose $b_0 = 1$, so that

$$\frac{2b_1}{X} = \frac{a_{2d-1}}{X},$$

which gives us b_1;

$$b_1 = \frac{a_{2d-1}}{2}.$$

Say $b_1, ..., b_m$ have been chosen, then for b_{m+1}, look at X^{-m-1} with coefficient

$$\sum_{i+j=m+1} b_i b_j = a_{2d-m-1}.$$

Rewrite this as

$$2b_{m+1} + \sum_{\substack{i+j=m+1 \\ (i,j)\neq(0,m+1)\neq(j,i)}} b_i b_j = a_{2d-m-1},$$

then all terms are known except for $2b_{m+1}$, so we can also choose the correct b_{m+1}. Since all b_n can be chosen, $\sqrt{f} \in K((\frac{1}{X}))$;

$$\sqrt{f} = \sum_{n=-d}^{\infty} b_n X^{-n}$$

. □

Every $\beta \in K((\frac{1}{X}))$ can be written uniquely as $\beta = [\beta] + \{\beta\}$, where $[\beta] \in K[X]$ and $\{\beta\} \in \frac{1}{X}K[[\frac{1}{X}]]$. For instance

$$\begin{aligned}\sqrt{f} = \sum_{n=-d}^{\infty} b_n X^{-n} &= \sum_{i=0}^{d} b_{-i} X^i + \sum_{n=1}^{\infty} b_n X^{-n} \\ &= [\sqrt{f}] + \{\sqrt{f}\}\end{aligned}$$

To construct continued fractions of polynomials, such as $\alpha = \sqrt{f}$, the following algorithm can be used:

$$\begin{aligned}\alpha_0 &= \alpha \\ a_k &= [\alpha_k] \\ \alpha_{k+1} &= \frac{1}{\alpha_k - a_k}.\end{aligned}$$

As an example, look at $f = X^6 + X + 1$, a nonsquare polynomial in $\mathbb{F}_3[X]$.

$$\begin{array}{ll}
\alpha_0 = \sqrt{f} = \sqrt{X^6 + X + 1} & a_0 = X^3 \\
\alpha_1 = \frac{X^3+\sqrt{f}}{X+1} & a_1 = 2X^2 + X + 2 \\
\alpha_2 = \frac{2X^3+1+2\sqrt{f}}{X^2+2X} & a_2 = X + 1 \\
\alpha_3 = \frac{X^3+X+1+\sqrt{f}}{2X^2+X+2} & a_3 = X + 1 \\
\alpha_4 = \frac{X^3+2X+1+\sqrt{f}}{X^2} & a_4 = 2X \\
\alpha_5 = \frac{2X^3+2X+1+\sqrt{f}}{2X^2+X+1} & a_5 = 2X + 2 \\
\alpha_6 = \frac{X^3+X+2+\sqrt{f}}{X^2} & a_6 = 2X \\
\alpha_7 = \frac{2X^3+X+2+\sqrt{f}}{X^2+X+1} & a_7 = X + 1 \\
\alpha_8 = \frac{X^3+X+1+\sqrt{f}}{2X^2+X} & a_8 = X + 1 \\
\alpha_9 = \frac{X^3+2+\sqrt{f}}{X+1} & a_9 = 2X^2 + X + 2 \\
\alpha_{10} = X^3 + \sqrt{f} & a_{10} = 2X^3 \\
\alpha_{11} = \frac{X^3+\sqrt{f}}{X+1} = \alpha_1 & a_{11} = 2X^2 + X + 2 = a_1
\end{array}$$

This expansion is periodic, because $\alpha_{11} = \alpha_1$.

4.2 Theorems

Some of the theorems for integers can be directly applied to polynomials as well:

Theorem 8. *Let a_0, a_1,... be nonzero polynomials over a field K in a variable X. Let p_0, p_1,... and q_0, q_1,... be defined recursively by:*

$$\begin{array}{ll}
p_0 = a_0 & q_0 = 1 \\
p_1 = a_0 a_1 + 1 & q_1 = a_1 \\
p_k = a_k p_{k-1} + p_{k-2} & q_k = a_k q_{k-1} + q_{k-2}
\end{array}$$

for $k \geq 2$. Then the kth convergent $C_k = [a_0; a_1, ..., a_k]$ is given by $C_k = \frac{p_k}{q_k}$.

The proof is exactly the same as that of theorem 1.

Theorem 9. *Let $C_k = \frac{p_k}{q_k}$ be the kth convergent of the continued fraction $[a_0; a_1, ...]$, where $k \in \mathbb{Z}_{>0}$ and p_k and q_k as defined in theorem 8, then*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$$

The proof is the same as that of theorem 2.

Corollary 2. *Let C_k be the kth convergent of $[a_0; a_1, ...]$, then*

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

for all $k \leq 1$, and

$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}$$

for all $k \leq 2$.

The proof is the same as that of corollary 1.

The other theorems are a bit trickier, as we first need to define what a quadratic irrationality is in the polynomial case.

Definition 5. *An $\alpha \in K((\frac{1}{X}))$ is said to be a quadratic irrationality if*

$$[K(X)(\alpha) : K(X)] = 2.$$

Because of this, α can again be written as

$$\alpha = \frac{a + \sqrt{b}}{c}$$

by solving the quadratic equation for α and renaming the coefficients as a, b and c.

Lemma 4. *If α is a quadratic irrationality, it can be written as*

$$\frac{P + \sqrt{f}}{Q},$$

where $f \in K[X]$, nonsquare, $P \in K[X]$, $Q \neq 0 \in K[X]$ and $Q|(f - P^2)$.

Proof. Because α is a quadratic irrationality, it can be written as

$$\alpha = \frac{a + \sqrt{b}}{c},$$

where $a, b, c \in K[X]$, $deg(b) > 0$ and $c \neq 0$. Multipliying both the numerator and denominator by $|c|$, we obtain:

$$\alpha = \frac{a|c| + \sqrt{bc^2}}{c|c|}.$$

Now, let $P = a|c|$, $Q = c|c|$ and $f = bc^2$. Then $P, Q, f \in K[X]$, $Q \neq 0$, f is nonsquare because $K[X](\sqrt{f}) = K[X](\sqrt{b}) = K[X](\alpha)$ is quadratic over $K[X]$ and $Q|(f - P^2)$ because $d - P^2 = bc^2 - a^2c^2 = c^2(b - a^2) = \pm Q(b - a^2)$. □

With a slight change in the proof, we can now construct a theorem similar to theorem 3:

Theorem 10. *Let α be a quadratic irrationality, so there are P_0, Q_0 and f such that*

$$\alpha = \frac{P_0 + \sqrt{f}}{Q_0},$$

where Q_0 is not identically zero, $deg(f) > 0$, f is a nonsquare polynomial and $Q_0|(f - P_0^2)$. Define:

$$\begin{aligned} \alpha_k &= \frac{P_k + \sqrt{f}}{Q_k} \\ a_k &= [\alpha_k] \\ P_{k+1} &= a_k Q_k - P_k \\ Q_{k+1} &= \frac{f - P_{k+1}^2}{Q_k} \end{aligned}$$

for all $k > 0$ then $\alpha = [a_0; a_1, a_2, ...]$.

Proof. For $k = 0$, we have P_k and Q_k polynomials, Q_k not identically zero and $Q_k|(f - P_k^2)$. Assume it holds for some $k \leq 0$, then

$$P_{k+1} = a_k Q_k - P_k$$

is also a polynomial. Furthermore,

$$\begin{aligned} Q_{k+1} &= \frac{f - P_{k+1}^2}{Q_k} \\ &= \frac{f - (a_k Q_k - P_k)^2}{Q_k} \\ &= \frac{f - P_k^2}{Q_k} + 2a_k P_k - a_k^2 Q_k \end{aligned}$$

So because $Q_k|(f - P_k^2)$ we see that Q_{k+1} is also a polynomial. And because f is nonsquare, $f \neq P_{k+1}^2$, so that Q_{k+1} is not identically zero. Finally, because

$$Q_k = \frac{f - P_{k+1}^2}{Q_{k+1}}$$

we can conclude that $Q_{k+1}|(f - P_{k+1}^2)$. To show that the a_i are the coefficients of the continued fraction of α we show that for $k \geq 0$

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$$

and $deg(\alpha_j) > 0$ for all $j \geq 1$.
Note that because a_k is the polynomial part of α_k, $\alpha_k - a_k$ has $deg < 0$. So that $deg(\alpha_{k+1})$

must be larger than 0. And indeed

$$\begin{aligned}\alpha_k - a_k &= \frac{P_k+\sqrt{d}}{Q_k} - a_k \\ &= \frac{\sqrt{f}-(a_kQ_k-P_k)}{Q_k} \\ &= \frac{\sqrt{f}-P_{k+1}}{Q_k} \\ &= \frac{(\sqrt{f}-P_{k+1})(\sqrt{f}+P_{k+1})}{Q_k(\sqrt{f}+P_{k+1})} \\ &= \frac{f-P_{k+1}^2}{Q_k(\sqrt{f}+P_{k+1})} \\ &= \frac{Q_kQ_{k+1}}{Q_k(\sqrt{f}+P_{k+1})} \\ &= \frac{Q_{k+1}}{\sqrt{f}+P_{k+1}} = \frac{1}{\alpha_{k+1}}\end{aligned}$$

So $\alpha = [a_0; a_1, a_2, ...]$, as required. □

Up to here, the theorems held for polynomials over any field, but for Lagrange's theorem, we need the field to be finite. The theorem is quite different in $\mathbb{F}_q((\frac{1}{X}))$, but we again prove the periodicity by showing that there are limited options for P_k and Q_k.

Theorem 11. *The infinite continued fraction expansion of $\sqrt{f}$ is periodic for $f = X^{2d}+...$ nonsquare in $\mathbb{F}_q[X]$, where $Char(\mathbb{F}_q) > 2$.*

Proof. Let $\alpha_0 = \sqrt{f}$, a quadratic irrationality, then

$$\alpha_0 = \frac{P_0 + \sqrt{f}}{Q_0},$$

with $P_0 = 0$ and $Q_0 = 1$ and $a_0 = [\alpha_0]$ has degree d.
Using the algortihm from theorem 10 we can construct α_1;
$P_1 = a_0$ with $deg(P_1) = d$ and $Q_1 = f - a_0^2$ with $0 \leq deg(Q_1) < 2d$. Now

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{a_0 + \sqrt{f}}{f - a_0^2},$$

so

$$\begin{aligned}deg(\alpha_1) &= deg(a_0 + \sqrt{f}) - deg(f - a_0^2) \\ &\leq max(d, d) - deg(Q_1) \\ &\leq d - deg(Q_1)\end{aligned}$$

and because we want $deg(\alpha_1) > 0$, this implies that $deg(Q_1) < d$ must hold as well. This implies that $0 < deg(\alpha_1) \leq d$ and $0 \leq deg(Q_1) \leq d - deg(\alpha_1)$.

Now assume that for a certain $k \geq 1$ we have

$$\begin{aligned}0 \leq deg(Q_k) \leq d - deg(\alpha_k); \\ 0 \leq deg(P_k) \leq d; \\ 0 < deg(\alpha_k) \leq d.\end{aligned}$$

Then $a_k = [\alpha_k]$ has the same degree as α_k, so

$$deg(P_{k+1}) = deg(a_kQ_k - P_k) \leq max(deg(\alpha_k) + d - deg(\alpha_k), d) = d$$

Also, the proof of theorem 10 shows us that $Q_{k+1} = (P_{k+1} + \sqrt{f})/\alpha_{k+1}$, hence

$$\begin{aligned} deg(Q_{k+1}) &= deg(P_{k+1} + \sqrt{f}) - deg(\alpha_{k+1}) \\ &\leq max(d, d) - deg(\alpha_{k+1}) \\ &= d - deg(\alpha_{k+1}) \end{aligned}$$

Because Q_{k+1} is a polynomial, it has degree ≥ 0, so $deg(\alpha_{k+1})$ must be less than or equal to d. So

$$\begin{aligned} 0 \leq deg(Q_{k+1}) &\leq d - deg(\alpha_k); \\ 0 \leq deg(P_{k+1}) &\leq d; \\ 0 < deg(\alpha_{k+1}) &\leq d, \end{aligned}$$

and by the principle of mathematical induction, these inequalities are true for all $k \geq 1$.

Since the degrees of P_k and Q_k are bounded, there is only a finite number of choices for P_k and Q_k in $\mathbb{F}_q[X]$, so there is a pair of integers (i, j) with $i \neq j$ for which $P_i = P_j$, $Q_i = Q_j$ and by the construction of α_k, this implies that $\alpha_i = \alpha_j$.
So $\sqrt{f} = \alpha = [a_0; a_1, ..., a_{i-1}, \overline{a_i, ..., a_{j-1}}]$ has a periodic continued fraction expansion. □

4.3 Purely periodic continued fractions

To prove the next theorem, we need a non-recursive definition of the p_ks and q_ks for an $\alpha = [a_0, a_1, ..., a_n]$. We know this is possible because they are all a certain sum of products of the a_i with $0 \leq i \leq k$. The definition was found by Euler [1, p. 82-83].

Definition 6. *We define the bracket product $\langle a_0, a_1, ..., a_n \rangle$ to be the product of all consecutive terms, plus the products obtained from omitting a pair of consecutive terms, plus the products obtained from omitting two disjoint pairs of consecutive terms, and so on.*

An example:

$$\langle a_0, a_1, a_2 \rangle = a_0 a_1 a_2 + a_0 + a_2.$$

Lemma 5. *Given $a_0, \ldots, a_n$, and p_n and q_n as defined in Theorems 1 and 8. Then*

$$p_n = \langle a_0, ..., a_n \rangle \quad \textit{and} \quad q_n = \langle a_1, ..., a_n \rangle.$$

Proof. For $n = 0$ and $n = 1$ this is immediate from the definitions; here we use the conventions that the product over an empty set has value 1 and a sum over zero terms has value 0. For $n \geq 2$, note that the sequences $(p_j), (q_j), (\langle a_0, ..., a_j \rangle)$ and $(\langle a_1, ..., a_j \rangle)$ all satisfy the same second order linear recursion. From this, the lemma follows. □

A fortunate consequence of Euler's definition is that the value of $\langle a_0, a_1, ..., a_n \rangle$ is unchanged if the terms are written in the opposite order.

$$\langle a_0, a_1, ..., a_n \rangle = \langle a_n, a_{n-1}, ..., a_0 \rangle.$$

Theorem 12. *If α is a quadratic irrationality with a purely periodic continued fraction expansion, then the quadratic irrationality with the period of α reversed is equal to $-1/\alpha'$, where α' is the conjugate of α.*

Proof. Since α is a purely periodic quadratic irrationality, we can write it as $\alpha = [\overline{a_0; a_1, ..., a_k}] = [a_0; a_1, ..., a_k, \alpha]$. By theorem 8, this gives the equality

$$\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}},$$

where p_k/q_k and p_{k-1}/q_{k-1} are the kth and $(k-1)$th convergents of α. We rewrite this to obtain the quadratic equality

$$q_k\alpha^2 + (q_{k-1} - p_k)\alpha - p_{k-1} = 0.$$

Now, look at $\beta = [\overline{a_k; a_{k-1}, ..., a_1, a_0}] = [a_k; a_{k-1}, ..., a_0, \beta]$. Again, from theorem 8, this gives us

$$\beta = \frac{\beta p'_k + p'_{k-1}}{\beta q'_k + q'_{k-1}},$$

where p'_k/q'_k and p'_{k-1}/q'_{k-1} are the kth and $(k-1)$th convergents of β. We rewrite this to find

$$q'_k\beta^2 + (q'_{k-1} - p'_k)\beta - p'_{k-1} = 0.$$

From the new definition of the p_i and q_i, we know that, for α,

$$\begin{aligned} p_k &= \langle a_0, ..., a_k\rangle, \qquad & p_{k-1} &= \langle a_0, ..., a_{k-1}, \rangle \\ q_k &= \langle a_1, ..., a_k\rangle, \qquad & q_{k-1} &= \langle a_1, ..., a_{k-1}\rangle \end{aligned}$$

and for β,

$$\begin{aligned} p'_k &= \langle a_k, a_{k-1}, ..., a_0\rangle, \qquad & p'_{k-1} &= \langle a_k, a_{k-1}..., a_1\rangle, \\ q'_k &= \langle a_{k-1}, a_{k-2}, ..., a_0\rangle, \qquad & q'_{k-1} &= \langle a_{k-1}, a_{k-2}, ..., a_1\rangle. \end{aligned}$$

Because reversing the order still gives the same bracket product, we see that

$$\begin{aligned} p'_k &= p_k, \qquad & p'_{k-1} &= q_k, \\ q'_k &= p_{k-1}, \qquad & q'_{k-1} &= q_{k-1}. \end{aligned}$$

So the equation for β becomes

$$p_{k-1}\beta^2 + (q_{k-1} - p_k)\beta - q_k = 0,$$

dividing by $(-1/\beta)^2$ we get

$$q_k(-1/\beta)^2 + (q_{k-1} - p_k)(-1/\beta) - p_{k-1} = 0.$$

So the two roots of

$$q_kx^2 + (q_{k-1} - p_k)x - p_{k-1} = 0$$

are α and $\alpha' = -1/\beta$. □

The following equivalent of theorem 6 also holds for polynomial continued fractions.

Theorem 13. *Let $f \in \mathbb{F}_q[X]$ nonsquare, monic and of even degree. Define α_k, a_k, P_{k+1} and Q_{k+1} as in theorem 10, with $\alpha_0 = \sqrt{f}$. Furthermore, let p_k/q_k denote the kth convergent of the continued fraction expansion of $\sqrt{f}$. Then*

$$p_k^2 - f \cdot q_k^2 = (-1)^{k-1} Q_{k+1}$$

.

Proof. Because $\sqrt{f} = \alpha_0 = [a_0; a_1, ..., a_k, \alpha_{k+1}]$, theorem 8 tells us that

$$\sqrt{f} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}.$$

And since $\alpha_{k+1} = (P_{k+1} + \sqrt{f})/Q_{k+1}$, we have

$$\sqrt{f} = \frac{(P_{k+1} + \sqrt{f}) p_k + Q_{k+1} p_{k-1}}{(P_{k+1} + \sqrt{f}) q_k + Q_{k+1} q_{k-1}}.$$

Rewriting this, we obtain

$$f q_k + (P_{k+1} q_k + Q_{k+1} q_{k-1}) \sqrt{f} = (P_{k+1} p_k + Q_{k+1} p_{k-1}) + p_k \sqrt{f}.$$

This gives us $f q_k = P_{k+1} p_k + Q_{k+1} p_{k-1}$ and $P_{k+1} q_k + Q_k q_{k-1} = p_k$.
Multiply the first of these two equations by q_k and the second by p_k, then subtract the first from the second to get

$$p_k^2 - f \cdot q_k^2 = (p_k q_{k-1} - p_{k-1} q_k) Q_{k+1} = (-1)^{k-1} Q_{k+1},$$

where theorem 9 gives the last equality. □

To prove that every purely periodic infinite continued fraction of an integer is a reduced quadratic irrationality, we used a property that stems from the definition of the convergents of a continued fraction. Namely, that $\alpha = [\overline{a_0; ..., a_k}] = [a_0; ..., a_k, \alpha]$ can be written as

$$\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}},$$

which can be rewritten to obtain the quadratic equation

$$q_k \alpha^2 - (q_{k-1} - p_k)\alpha - p_{k-1} = 0.$$

However, when looking at purely periodic examples, of the form $\alpha = \sqrt{f} + a_0$, this equality does not seem to hold for α. Even though it should hold, since the equation comes from the definition of the very convergents used to compute the result, as used in the proof of theorem 8.

Chapter 5

Solving Pell's equation; the polynomial case

For the polynomial case, we look at

$$a^2 - f \cdot b^2 = 1,$$

for given $f \in K[X]$, nonsquare, monic and of even degree. Because of theorem 12, we see that lemma 2 also holds for polynomials. And thus, the following theorem has a proof equivalent to that of theorem 7.

Theorem 14. *Let $f \in \mathbb{F}_q[X]$ nonsquare, monic and of even degree. Let p_k/q_k denote the kth convergent of the continued fraction of $\sqrt{f}$, $k = 1, 2, ...$, and let n be the period length of the continued fraction.*

Then, when n is even, p_k/q_k provides a solution for $p_k^2 - fq_k^2 = 1$ when $k = jn - 1$, with $j = 1, 2, ...$, and provides no solutions for $p_k^2 - fq_k^2 = -1$.

When n is odd, p_k/q_k provides a solution for $p_k^2 - fq_k^2 = 1$ when $k = 2jn - 1$, and provides a solution for $p_k^2 - fq_k^2 = -1$ when $k = (2j - 1)n - 1$, with $j = 1, 2, ...$

In the integer case, we can also prove that the solutions found through the continued fraction expansion are the only solutions[2, p. 556], for polynomials, this is not necessarily so. Furthermore, there are also pairs of polynomials (x, y) to be found that solve

$$x^2 - f \cdot y^2 = e \in \mathbb{F}_q^* \neq \pm 1.$$

For example[1] , look at $f = X^2 + 2$ over $\mathbb{F}_5$ with the "solution"

$$X^2 - f \cdot 1^2 = 3.$$

In the integer case we have the concept of a smallest solution for a given d, for the polynomial case, this can be compared to the solution of the lowest degree.

For $f = X^6 + X + 1 \in \mathbb{F}_3[X]$ the "smallest" solution is, quite obviously, the first. Note that the period is 10, so the pair (p_9, q_9) solves Pell's equation;

$$p_9 = 2 + X^2 + X^3 + 2X^4 + 2X^5 + 2X^6 + X^7 + X^8 + X^9 + X^{10} + X^{12} + 2X^{14}$$
$$q_9 = X + 2X^4 + X^7 + X^9 + 2X^{11}$$
$$p_9^2 - (X^6 + X + 1)q_9^2 = 1$$

[1] The third example in the appendix also solves for e

For $f = X^6 + X + 1 \in \mathbb{F}_5[X]$, the period of the continued fraction is 25. Here the "smallest" solution for Pell's equation is the pair (p_{49}, q_{49}), while the pair (p_{24}, q_{24}) solves $p_k^2 - fq_k^2 = -1$.

Chapter 6

Conclusion

Given a field K of characteristic $\neq 2$ and a polynomial $f \in K[X]$, the Pell equation

$$a^2 - fb^2 = 1$$

has no solution $(a, b) \neq (\pm 1, 0)$ in polynomials a, b, in the following two cases:

- The degree of f is odd;
- The leading coefficient of f is not a square.

In the remaining case one can reduce the problem to the case that f is monic. Under that condition, so for f monic of even degree, we obtained the following results.

- For $f = 1$, all solutions are constants and they are explicitly described in terms of the units of K.
- For f the square of a nonconstant polynomial, only the trivial solution $(a, b) = (\pm 1, 0)$ occurs.
- If the monic polynomial f is not a square and moreover the field K is a finite field $\mathbb{F}_q$, then a variant of the classical continued fraction algorithm can be used to prove that nontrivial solutions exist, and moreover the algorithm explicitly constructs such solutions. In this variant, the integers $\mathbb{Z}$ and the fractions $\mathbb{Q}$ appearing in the classical algorithm are replaced by the polynomials $\mathbb{F}_q[X]$ and the rational functions $\mathbb{F}_q(X)$, respectively. Moreover, the real numbers $\mathbb{R}$ are replaced by the field of formal Laurent series $\mathbb{F}_q((\frac{1}{X}))$.

We found examples in which the adapted continued fraction algorithm also found solutions to an equation $a^2 - fb^2 = \alpha$ for a constant $\alpha \in \mathbb{F}_q$ different from 1 (and even from -1). The existence of such solutions is clear because one can multiply a, b in a solution to the Pell equation, by a nonzero constant. However, it is not clear which of these extra solutions will be found by the adapted algorithm (if it finds any).

Finally, although we proved that the continued fraction algorithm finds a nontrivial solution to the Pell equation for polynomials over a finite fields, we did not prove that it finds all solutions (upto multiplying a, b by ± 1), as is true for the classical case.

Chapter 7

Appendix

7.1 Examples

7.1.1 $X^6 + X + 1$ mod 3

$f = X^6 + X + 1 \in \mathbb{F}_3[X]$	$\alpha = \sqrt{f}$	k	$p_k^2 - f q_k^2$
$\alpha_0 = \alpha$	$a_0 = [\alpha] = X^3$	0	$2X + 2$
$\alpha_1 = \frac{X^3+\sqrt{f}}{X+1}$	$a_1 = 2X^2 + X + 2$	1	$2X^2 + X$
$\alpha_2 = \frac{2X^3+1+2\sqrt{f}}{X^2+2X}$	$a_2 = X + 1$	2	$X^2 + 2X + 1$
$\alpha_3 = \frac{X^3+X+1+\sqrt{f}}{2X^2+X+2}$	$a_3 = X + 1$	3	X^2
$\alpha_4 = \frac{X^3+2X+1+\sqrt{f}}{X^2}$	$a_4 = 2X$	4	$2X^2 + X + 1$
$\alpha_5 = \frac{2X^3+2X+1+\sqrt{f}}{2X^2+X+1}$	$a_5 = 2X + 2$	5	X^2
$\alpha_6 = \frac{X^3+X+2+\sqrt{f}}{X^2}$	$a_6 = 2X$	6	$X^2 + 2X + 1$
$\alpha_7 = \frac{2X^3+X+2+\sqrt{f}}{X^2+X+1}$	$a_7 = X + 1$	7	$2X^2 + X$
$\alpha_8 = \frac{X^3+X+1+\sqrt{f}}{2X^2+X}$	$a_8 = X + 1$	8	$2X + 2$
$\alpha_9 = \frac{X^3+2+\sqrt{f}}{X+1}$	$a_9 = 2X^2 + X + 2$	9	1
$\alpha_{10} = X^3 + \sqrt{f}$	$a_{10} = 2X^3$	10	$2X + 2$
$\alpha_{11} = \frac{X^3+\sqrt{f}}{X+1} = \alpha_1$	$a_{11} = 2X^2 + X + 2 = a_1$	11	$2X^2 + X$

7.1.2 $X^6 + X + 1$ mod 5

$f = X^6 + X + 1 \in \mathbb{F}_5[X]$	$\alpha = \sqrt{f}$	k	$p_k^2 - f q_k^2$
$\alpha_0 = \alpha$	$a_0 = [\alpha] = X^3$	0	$4X + 4$
$\alpha_1 = \frac{X^3+\sqrt{f}}{X+1}$	$a_1 = 2X^2 + 3X + 2$	1	$X^2 + 4X + 2$
$\alpha_2 = \frac{4X^3+3+4\sqrt{f}}{4X^2+X+3}$	$a_2 = 2X + 2$	2	$4X^2 + 3X + 4$
$\alpha_3 = \frac{X^3+2X+2+\sqrt{f}}{X^2+2X+1}$	$a_3 = 2X + 1$	3	X^2
$\alpha_4 = \frac{X^3+2X+4+\sqrt{f}}{X^2}$	$a_4 = 2X$	4	$X^2 + 2X + 4$
$\alpha_5 = \frac{4X^3+2X+4+4\sqrt{f}}{X^2+2X+4}$	$a_5 = 3X + 4$	5	$4X^2 + 3X + 2$
$\alpha_6 = \frac{X^3+2X+3+\sqrt{f}}{4X^2+3X+2}$	$a_6 = 3X + 4$	6	$3X^2 + 4X + 2$
$\alpha_7 = \frac{X^3+X+\sqrt{f}}{2X^2+X+3}$	$a_7 = X + 2$	7	$X^2 + X$
$\alpha_8 = \frac{X^3+4X+1+\sqrt{f}}{X^2+X}$	$a_8 = 2X + 3$	8	$3X^2 + 1$
$\alpha_9 = \frac{4X^3+X+1+4\sqrt{f}}{3X^2+1}$	$a_9 = X$	9	$4X$
$\alpha_{10} = \frac{4X^3+4+4\sqrt{f}}{X}$	$a_{10} = 3X^2$	10	$2X^2 + 1$
$\alpha_{11} = \frac{X^3+4+\sqrt{f}}{3X^2+4}$	$a_{11} = 4X$	11	$X^2 + X$
$\alpha_{12} = \frac{X^3+X+1+\sqrt{f}}{X^2+X}$	$a_{12} = 2X + 3$	12	$4X^2 + 4X$
$\alpha_{13} = \frac{X^3+2X+4+\sqrt{f}}{X^2+X}$	$a_{13} = 2X + 3$	13	$3X^2 + 4$
$\alpha_{14} = \frac{4X^3+4X+4+4\sqrt{f}}{2X^2+1}$	$a_{14} = 4X$	14	X
$\alpha_{15} = \frac{4X^3+1+4\sqrt{f}}{X}$	$a_{15} = 3X^2$	15	$2X^2 + 4$
$\alpha_{16} = \frac{3X^3+3+3\sqrt{f}}{X^2+2}$	$a_{16} = X$	16	$4X^2 + 4X$
$\alpha_{17} = \frac{X^3+4X+4+\sqrt{f}}{X^2+X}$	$a_{17} = 2X + 3$	17	$2X^2 + X + 3$
$\alpha_{18} = \frac{4X^3+X+4+4\sqrt{f}}{3X^2+4X+2}$	$a_{18} = X + 2$	18	$X^2 + 2X + 3$
$\alpha_{19} = \frac{X^3+X+\sqrt{f}}{4X^2+3X+2}$	$a_{19} = 3X + 4$	19	$4X^2 + 3X + 1$
$\alpha_{20} = \frac{X^3+2X+3+\sqrt{f}}{4X^2+3X+1}$	$a_{20} = 3X + 4$	20	$4X^2$

$f = X^6 + X + 1 \in \mathbb{F}_5[X]$	$\alpha = \sqrt{f}$	k	$p_k^2 - f q_k^2$
$\alpha_{21} = \frac{X^3+3X+1+\sqrt{f}}{X^2}$	$a_{21} = 2X$	21	$X^2 + 2X + 1$
$\alpha_{22} = \frac{4X^3+3X+1+4\sqrt{f}}{4X^2+3X+4}$	$a_{22} = 2X + 1$	22	$4X^2 + X + 3$
$\alpha_{23} = \frac{X^3+2X+2+\sqrt{f}}{X^2+4X+2}$	$a_{23} = 2X + 2$	23	$X + 1$
$\alpha_{24} = \frac{4X^3+3+4\sqrt{f}}{4X+4}$	$a_{24} = 2X^2 + 3X + 2$	24	$4 = -1$
$\alpha_{25} = X^3 + \sqrt{f}$	$a_{25} = 2X^3$	25	$X + 1$
$\alpha_{26} = \frac{X^3+\sqrt{f}}{X+1} = \alpha_1$	$a_{26} = 2X^2 + 3X + 2$	26	$4X^2 + X + 3$

7.1.3 $X^4 + X + 1$ mod 7

$f = X^4 + X + 1 \in \mathbb{F}_7[X]$	$\alpha = \sqrt{f}$	k	$p_k^2 - f q_k^2$
$\alpha_0 = \sqrt{f}$	$a_0 = X^2$	0	$6X + 6$
$\alpha_1 = \frac{X^2+\sqrt{f}}{X+1}$	$a_1 = 2X + 5$	1	$4X + 4$
$\alpha_2 = \frac{2X^2+3+2\sqrt{f}}{X+1}$	$a_2 = 4X + 3$	2	5
$\alpha_3 = 4X^2 + 4\sqrt{f} = 4(\alpha_0 + a_0)$	$a_3 = X^2 = a_0$	3	$4X + 4$
$\alpha_4 = \frac{2X^2+2\sqrt{f}}{X+1} = 2\alpha_1$	$a_4 = 4X + 3 = 2a_1$	4	$6X + 6$
$\alpha_5 = \frac{X^2+5+\sqrt{f}}{X+1} = 4\alpha_2$	$a_5 = 2X + 5 = 4a_2$	5	1
$\alpha_6 = X^2 + \sqrt{f}$	$a_6 = 2X^2$	6	$6X + 6$
$\alpha_7 = \frac{X^2+\sqrt{f}}{X+1} = \alpha_1$	$a_7 = 2X + 5 = a_1$	7	$4X + 4$

Bibliography

[1] H. Davenport, The Higher Arithmetic, Cambridge University Press, 6th edition, 1993.

[2] K.H. Rosen, Elementary Number Theory, Pearson International, 6th edition, 2011.