Solvability of Pell-Like Equations

by
Clement Wan

Supervisor: Henry Kim
April 2021

Abstract

Given a non-square integer $d > 0$, and a nonzero integer $|l| < d$, there may exist integer solutions x, y to the Pell-Like Equation $x^2 - dy^2 = l$. This paper presents some known results relating to finding solutions to Pell-Like Equations:

1. Given d, we study which values of l have solutions by employing the theory of continued fractions.
   (a) We show any positive number a can be expressed as a continued fraction.
   (b) We show that when $\alpha = \alpha_0 = \sqrt{d} = [a_0, a_1, a_2, ...]$, and for any $k > 0$, $\alpha = [a_0, a_1, ..., a_k, \alpha_{k+1}]$, we can express each α_k as $\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$ for integers P_k, Q_k and the resulting sequences $\{a_n\}_{n \geqslant 0}, \{P_n\}_{n \geqslant 0}, \{Q_n\}_{n \geqslant 0}$ are periodic.
2. For any given period length p, we show a construction of a family of values of d so the corresponding sequence $\{Q_n\}_{n \geqslant 0}$ has period length p.
3. We identify and analyze some primes d with $d \equiv 3 \mod 4$ such that $x^2 - dy^2 = \pm l$ has a solution for all primes 2 and l with $l < 12(\log d)^2$ and $\left(\frac{d}{l}\right) = 1$ for l odd.

Acknowledgement

I would like to thank my family for the love and encouragement they have given me over the course of my undergraduate career.
I would also like to thank my research supervisor, Prof. Henry Kim, for all the support and guidance he has given me over the past year.

Contents

1 Introduction

Definition 1. *Let p be an odd prime number. An integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic nonresidue modulo p otherwise. The Legendre symbol is a function of a and p defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \mod p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } a \equiv 0 \mod p \end{cases}$$

Original Problem:

Are there infinitely many primes d with $d \equiv 3 \mod 4$
such that $x^2 - dy^2 = \pm l$ has a solution
for all primes 2 and l with $l < 12(\log d)^2$ and $\left(\frac{d}{l}\right) = 1$ for l odd?

Solving the above problem was the original goal of this thesis. An article by Eric Bach [1] connects the above unsolved problem to algebraic number theory, namely, providing a class number one criterion for the ring $\mathbb{Z}[\sqrt{d}]$, as $x^2 - dy^2$ is the norm function for the ring $\mathbb{Z}[\sqrt{d}]$.
While this problem remains unsolved, this paper presents some related known results outlined in the abstract, and ultimately we identify and analyze some primes d that satisfy the condition in question.

A class number one criterion is of great interest to algebraic number theorists, but a shallow introduction to unique factorization domains is sufficient to raise interesting questions that motivate interest in a class number one criterion.

Definition 2. *For $d > 0$, $\mathbb{Z}[\sqrt{d}]$ is a ring extension of the integers, and can be thought of as the set*

$$\mathbb{Z} \bigsqcup \{\sqrt{d}\}$$

closed under, and equipped with addition, subtraction, and multiplication.

Definition 3. *For $d > 0$, $\mathbb{Q}(\sqrt{d})$ is a field extension of the integers, and can be thought of as the set*

$$\mathbb{Q} \bigsqcup \{\sqrt{d}\}$$

closed under, and equipped with addition, subtraction, and multiplication, and division.

A ring is a **UFD** if there is "unique factorization" in the same way as we have unique prime factorization of integers.
For a counterexample, $\mathbb{Z}[\sqrt{5}]$ is not UFD:

$$4 = 2 \times 2 = (\sqrt{5}+1)(\sqrt{5}-1)$$

So, 4 does not have unique factorization.

Are there infinitely many $d > 0$ such that $\mathbb{Z}[\sqrt{d}]$ is a UFD?

For $d \equiv 1 \mod 4$, (mod 4), $\mathbb{Z}[\sqrt{d}]$ is not a UFD.
When $d \not\equiv 1 \mod 4$, the ring of integers of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Z}[\sqrt{d}]$. $\mathbb{Z}[\sqrt{d}]$ is a UFD if and only if it has trivial class group (i.e., the class number of $\mathbb{Q}(\sqrt{d})$ is 1).

However, it's an open question as to whether or not there are infinitely many $d > 0$ with $\mathbb{Q}(\sqrt{d})$ having class number 1, so the answer is not known.

2 Continued Fractions

Before exploring how the theory of continued fractions helps with solving Pell-like Equations, this section first establishes how continued fractions and some related terms are defined, and proves that any positive real number can be expressed as a continued fraction.

Definition 4. *For any finite sequence of positive real numbers $a_0, a_1, ..., a_N$, let the continued fraction*

$$a = [a_0, a_1, ..., a_N] = a_0 + \frac{1|}{|a_1} + \cdots + + \frac{1|}{|a_N}$$

be recursively defined as

$$a = \begin{cases} a_N & \text{if } N = 0 \\ a_0 + \frac{1}{[a_1,...,a_N]} & \text{if } N > 0 \end{cases}$$

Definition 5. *Let $\{a_i\}_{i \in \mathbb{Z}_{\geqslant 0}}$ be a sequence of positive integers for any $k \in \mathbb{Z}_{\geqslant 0}$. Then*

$$C_k = [a_0, ..., a_k].$$

What follows is sequence of proofs *(taken from the exercises of 8.2 from* [4]*)*

leading up to a proof that $\lim_{k\to\infty} C_k$ converges, giving us the natural definition:

$$[a_0, a_1, ...] = \lim_{k\to\infty} C_k.$$

Definition 6. *We call C_k the k^{th} convergent of $[a_0, a_1, ...]$.*

Definition 7. *Let $\{a_i\}_{i\in\mathbb{Z}_{\geqslant 0}}$ be a sequence of positive integers for any $k \in \mathbb{Z}_{\geqslant 0}$. Then*

$$\begin{aligned} p_0 &= a_0, & q_0 &= 1, \\ p_1 &= a_0a_1 + 1, & q_1 &= a_1, \\ p_k &= a_kp_{k-1} + p_{k-2}, & q_k &= a_kq_{k-1} + q_{k-2} \qquad \textit{for } k \geqslant 2. \end{aligned}$$

Theorem 1. *The k^{th} convergent $C_k = p_k/q_k$.*

Proof. $C_0 = a_0 = \frac{a_0}{1} = p_0/q_0$,
and $C_1 = a_0 + 1/a_1 = \frac{a_0a_1+1}{a_1} = p_0/q_0$,
and $C_2 = a_0 + \frac{1}{a_1+\frac{1}{a_2}} = a_0 + \frac{a_2}{a_1a_2+1} = \frac{a_0a_1a_2+a_0+a_2}{a_1a_2+1} = \frac{a_2p_1+p_0}{a_2q_1+q_0}$.
For $k \geqslant 2$, we may assume for induction that

$$p_k = a_kp_{k-1} + p_{k-2}, \qquad \textit{and } q_k = a_kq_{k-1} + q_{k-2}$$

And now it remains to show that

$$p_{k+1} = a_{k+1}p_k + p_{k-1}, \qquad \textit{and } q_{k+1} = a_{k+1}q_k + q_{k-1}$$

Notice that if we substitute a_k for $a_k + 1/a_{k+1}$ in the formula for C_k, we have the formula for C_{k+1}:

$$\begin{aligned} C_{k+1} &= \frac{(a_k + 1/a_{k+1})p_{k-1} + p_{k-2}}{(a_k + 1/a_{k+1})q_{k-1} + q_{k-2}} \\ &= \frac{(a_ka_{k+1} + 1)p_{k-1} + a_{k+1}p_{k-2}}{(a_ka_{k+1} + 1)q_{k-1} + a_{k+1}q_{k-2}} \\ &= \frac{a_{k+1}(a_kp_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_kq_{k-1} + q_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1}p_k + p_{k+1}}{a_{k+1}q_k + q_{k-1}} \end{aligned}$$

□

Theorem 2. *$p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}$, for $k \geqslant 1$.*

Proof. If $k = 1$, $p_k q_{k-1} - p_{k-1} q_k = (a_0 a_1 + 1)1 - a_0(a_1) = 1 = (-1)^{1-1}$
If $k = 2$,
$p_k q_{k-1} - p_{k-1} q_k = (a_0 a_1 a_2 + a_0 + a_2)a_1 - (a_0 a_1 + 1)(a_2 a_1 + 1)$
$= -1 = (-1)^{2-1}$
If $k \geqslant 2$, we may assume for induction $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$ for all $n \leqslant k$, and it remains to show $p_{k+1} q_k - p_k q_{k+1} = (-1)^k$.

$$\begin{aligned} p_{k+1} q_k - p_k q_{k+1} &= (a_{k+1} p_k + p_{k-1}) q_k - p_k (a_{k+1} q_k + q_{k-1}) \\ &= -(p_k q_{k-1} p_{k-1} q_1) \\ &= (-1)^k \end{aligned}$$

□

Theorem 3. *We have the identities*

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

for $1 \leqslant k \leqslant n$, *and*

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

for $2 \leqslant k \leqslant n$.

Proof. If $1 \leqslant k \leqslant n$,

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

If $2 \leqslant k \leqslant n$, we may use the above identity twice, applied to k and to $k-1$:

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

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

□

Theorem 4. *We have that*

$$C_1 > C_3 > C_5 > \cdots,$$

$$C_0 < C_2 < C_4 < \cdots,$$

and that every odd-numbered convergent $C_{2j+1}, j \geqslant 0$, is greater than every even-numbered convergent $C_{2k}, k \geqslant 0$.

Proof. Suppose k is odd. Then in Theorem 3 we showed $C_k - C_{k-2} < 0$, so $C_1 > C_3 > C_5 > \cdots$.
Suppose k is even. Then in Theorem 3 we showed $C_k - C_{k-2} > 0$, so $C_0 < C_2 < C_4 < \cdots$.

Suppose k is odd. Then $C_k - C_{k-1} > 0$, so $C_k > C_{k-1}$. □

Theorem 5. *Let $\{a_i\}_{i \geqslant 0}$ be an infinite sequence of integers with $a_i \geqslant 0$ for $i \geqslant 1$ and let $C_k = [a_0, ..., a_k]$. Then the sequence $\{C_k\}$ converges.*

Proof. By Theorem 5, q_n is a sequence of increasing integers, and must approach infinity as $n \to \infty$.
So $\forall \epsilon > 0$, $\exists N$ so that $1/q_N < \epsilon$. If N is not even, add 1 so that it is.
$|C_{N+1} - C_N| = \frac{1}{q_N q_{N+1}} < \epsilon$.
As a consequence of the fact $C_1 > C_3 > C > 5 > \cdots$ and $C_0 < C_2 < C_4 < \cdots$ and $C_{2j+1} > C_{2j}$,
For all even $n > N, C_N < C_n < C_{n+1} < C_{N+1}$
and likewise for all odd $n > N, C_N \leqslant C_{n-1} < C_n \leqslant C_{N+1}$.
So, $\forall n \geqslant N, |C_N - C_n| < \epsilon$, so we have a Cauchy sequence. □

Definition 8. *Now for any sequence of integers $\{a_i\}$ finite or infinite, we have a well-defined notion of the* ***simple continued fraction***

$$[a_0, a_1, ...].$$

I obmit the proof for this simple fact:

Theorem 6. *Let α be a positive rational number. Then $\alpha = [a_0, a_1, ..., a_N]$ has a representation as a simple finite continued fraction, and any simple finite continued fraction is a representation of some rational number.*

Theorem 7. *Let $\alpha = \alpha_0$ be an irrational real number greater than 0. Define the sequence $\{a_i\}_{i \geqslant 0}$ recursively as follows:*

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

so that for any $j \in \mathbb{Z}_{\geqslant 0}$,

$$\alpha = [a_0, a_1, ..., a_j, \alpha_{j+1}].$$

Then $\alpha = [a_0, a_1, ...]$ is a representation of α as a simple continued fraction.

Proof. By Theorem 5, it suffices to show that for each even k, $[a_0, ..., a_k] < \alpha$ and for every odd k, $[a_0, ..., a_k] > \alpha$
So that $\alpha = \lim_{k \to \infty} [a_0, a_1, ..., a_k]$.

Evidently $[a_0] = a_0 \leqslant \alpha_0 = \alpha$.
and $[a_0, a_1] = [\alpha] + \frac{1}{\left[\frac{1}{\alpha - [\alpha]}\right]} > [\alpha] + (\alpha - [\alpha]) = \alpha$
For $n \geqslant 1$, assume for induction that if n is odd, $p_k/q_k \geqslant \alpha$ and $p_{k-1}/q_{k-1} \leqslant \alpha$ and if n is even, $p_k/q_k \leqslant \alpha$ and $p_{k-1}/q_{k-1} \geqslant \alpha$
Both proofs are similar so assume WLOG n is odd.

$$\begin{aligned}
[a_0, ..., a_{n+1}] &= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}} \\
&= \frac{\left[\frac{1}{\alpha_n - [\alpha_n]}\right] p_n + p_{n-1}}{\left[\frac{1}{\alpha_n - [\alpha_n]}\right] q_n + q_{n-1}}
\end{aligned}$$

It remains to show that if $a/b < c/d$, i.e. $ad < bc$, and $\alpha \geqslant 1$, then

$$\begin{aligned}
\frac{a}{b} &< \frac{\alpha \times a + c}{\alpha \times b + d} \\
&\leqslant \frac{a + c}{b + d} \\
&< \frac{c}{d}
\end{aligned}$$

To show that $\frac{a}{b} < \frac{a+c}{b+d}$, we multiply through and see we are comparing

$$a(b+d) \overset{?}{<} b(a+c)$$

Subtracting ab from both sides, we have that $ad < bc$.
its a similar argument to show $\frac{a+c}{b+d} < \frac{c}{d}$.
Evidently, we also have $\frac{a}{b} = \frac{\alpha \times a}{\alpha \times b} < \frac{\alpha \times a+c}{\alpha \times b+d} < \frac{c}{d}$
and $\frac{a}{b} = \frac{(\alpha-1)a}{(\alpha-1)b} < \frac{\alpha \times a+c}{\alpha \times b+d} < \frac{a+c}{b+d}$

So, applying this fact to the convergents, we have that

$$\begin{aligned} p_{k-1}/q_{k-1} &\leqslant \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = p_{k+1}/q_{k+1} \\ &\leqslant \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} \\ &= \alpha \end{aligned}$$

□

3 Solving Pell-Like Equations with Continued Fractions

Consider the solutions to $x^2 - 2y^2 = 1$:

$$(3,2), (17,12), (99,70), (577,408), ...$$

Notice that the solutions x/y approximate $\sqrt{2} = 1.41421...$:

$$3/2 = 1.5, 17/12 = 1.41666..., 99/70 = 1.41428..., 577/408 = 1.41421...$$

This makes a lot of sense if we rearrange Pell's equation like so.

$$x^2 - Ny^2 = 1, y \neq 0 \iff N = \frac{x^2-1}{y^2} \simeq \frac{x^2}{y^2}$$

Finding good rational approximations of square roots is one of many motivators for studying Pell's equation, and so is the study of continued fractions:

Theorem 8. [3, Theoreom 10.3.1] *Suppose for $n \geqslant 1$ we write the n^{th} conver-*

gent $C_n = \frac{p_n}{q_n}$ *of* α *as an improper irreducible fraction. For* $0 < q \leqslant q_n$ *and* $p/q \neq p_n/q_n$,

$$|p_n/q_n - \alpha| < |p/q - \alpha|.$$

So, the convergents of a continued fraction give the best possible rational approximation of numbers, giving some intuition to their connection with Pell's Equation. To see a more concrete connection, consider the following theorem:

Theorem 9. [3, Theorem 10.8.2] *The equation* $x^2 - dy^2 = (-l)^n Q_n$ *is always soluble. If* $l \neq (-1)^n Q_n$ *and* $|l| < \sqrt{d}$, *then the equation* $x^2 - dy^2 = l$ *has no solution.*

4 Continued Fractions of Square Roots

In the previous section we saw how solving Pell-like equations is related to the continued fractions of square roots. In this section, we aim to prove some useful properties of continued fractions of square roots, namely that the sequences $\{a_n\}_{n\geqslant 0}, \{P_n\}_{n\geqslant 0}, \{Q_n\}_{n\geqslant 0}$ are periodic.

Theorem 10 (Theorem 8.1 from chapter 10 of [3])**.** *Consider the continued fraction of* $\sqrt{d}$ *for squarefree* d. *For each* $\alpha_j, j \in \mathbb{Z}_{\geqslant 0}$ *such that* $\alpha_0 = \alpha = \sqrt{d}$ *and*

$$\sqrt{d} = [a_0, a_1, ..., a_j, \alpha_{j+1}],$$

there exist integers P_j, Q_j *such that*

$$\alpha_j = \frac{\sqrt{d} + P_j}{Q_j}, P_j^2 \equiv d \mod Q_n.$$

Proof. We use induction on n. Applying Theorem 7,

$$a_n = [\alpha_{n+1}], \alpha_{n+1} = \frac{1}{\alpha_n - a_n}$$

so let's find integers P_{n+1}, Q_{n+1} such that

$$\frac{\sqrt{d} + P_n}{Q_n} = a_n + \frac{Q_{n+1}}{\sqrt{d} + P_{n+1}}$$

and

$$d - P_{n+1}^2 \equiv 0 \mod Q_{n+1}.$$

Clearing the denominator in the first equality,

$$\begin{aligned} d + P_nP_{n+1} + (P_n + P_{n+1})\sqrt{d} &= a_nQ_nP_{n+1} + Q_nQ_{n+1} + a_nQ_n\sqrt{d} \\ \therefore d + P_nP_{n+1} &= a_nQ_nP_{n+1} + Q_nQ_{n+1} \\ \textit{and } P_n + P_{n+1} &= a_nQ_n \qquad * \\ \therefore d + P_nP_{n+1} - P_{n+1}(P_n + P_{n+1}) &= a_nQ_nP_{n+1} + Q_nQ_{n+1} - a_nQ_nP_{n+1} \\ \therefore d - P_{n+1}^2 &= Q_nQ_{n+1} \qquad * \end{aligned}$$

Notice that in satisfying the equalities marked *, the remaining equalities follow. So, let

$$P_{n+1} = a_nQ_n - P_n.$$

As $P_{n+1}^2 \equiv P_n^2 \mod Q_n$, we have

$$d - P_{n+1}^2 \equiv 0 \mod Q_n$$

as desired, from which it follows there exists integer Q_{n+1} such that

$$d - P_{n+1}^2 = Q_nQ_{n+1}.$$

□

In summary, we guarantee the following definition is well-defined, where P_n, Q_n are integers:

Definition 9. *Let $\alpha_0 = \alpha = \sqrt{d}$, where d is squarefree, and recursively define*

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

Theorem 11. *For any $n \in \mathbb{Z}_{\geqslant 0}$,*

$$\begin{aligned} 0 < Q_n < \sqrt{d} + P_n \qquad & \textit{and} \qquad 0 < P_n < \sqrt{d} \\ \therefore 0 < Q_n < \sqrt{d} + P_n < 2\sqrt{d} & \end{aligned}$$

Proof. For $n = 0$, $Q_n = 1 < \sqrt{d} = \sqrt{d} + P_n$ and $P_n = 0 < \sqrt{d}$.
I claim that for $n \in \mathbb{Z}_{\geqslant 1}$,

$$0 < \frac{\sqrt{d} - P_n}{Q_n} < 1 < \frac{\sqrt{d} + P_n}{Q_n}$$

Notice that for any natural number k, as $\alpha_{k-1} - a_{k-1} < 1$,

$$\frac{1}{\alpha_{k-1} - a_{k-1}} = \alpha_k = \frac{P_k + \sqrt{d}}{Q_k} > 1.$$

As d is squarefree, there exists natural numbers N, j so that
$d = N^2 + j$, and $1 \leqslant j \leqslant 2N$.
$P_1 = 1 \times a_0 - 0 = a_0 = N = \lfloor \sqrt{d} \rfloor \in \mathbb{N}$ and $Q_1 = \frac{N^2 + j - N^2}{1} = j \in \mathbb{N}$. So,

$$0 < \frac{\sqrt{d} - \lfloor \sqrt{d} \rfloor}{Q_1} = \frac{\sqrt{d} - P_1}{Q_1} < 1$$

Now assume for induction

$$0 < \frac{\sqrt{d} - P_n}{Q_n} < 1 < \frac{\sqrt{d} + P_n}{Q_n}.$$

$P_{n+1} = a_n Q_n - P_n \in \mathbb{Z}$, so $\sqrt{d} + P_{n+1} \neq 0$.

$$\begin{aligned}
\frac{\sqrt{d} - P_{n+1}}{Q_{n+1}} &= \frac{\sqrt{d} - P_{n+1}}{Q_{n+1}} \times \frac{\sqrt{d} + P_{n+1}}{\sqrt{d} + P_{n+1}} \\
&= \frac{d - P_{n+1}^2}{Q_{n+1}(\sqrt{d} + P_{n+1})} \\
&= \frac{d - P_{n+1}^2}{Q_{n+1}(\sqrt{d} + a_n Q_n - P_n)} \\
&= \frac{\frac{d - P_{n+1}^2}{Q_n}}{a_n Q_{n+1} + \frac{\sqrt{d} - P_n}{Q_n}} \\
&= \frac{Q_{n+1}}{a_n Q_{n+1} + \frac{\sqrt{d} - P_n}{Q_n}}
\end{aligned}$$

So, $\alpha_{n-1} = \frac{P_{n-1} + \sqrt{d}}{Q_{n-1}}$ is not an integer, and so $\alpha_{n-1} - 1 < a_{n-1} < \alpha_{n-1}$.

$$\begin{aligned}
P_n &= a_{n-1} Q_{n-1} - P_{n-1} && \therefore P_n \in \mathbb{Z} \\
&< \alpha_{n-1} Q_{n-1} - P_{n-1}
\end{aligned}$$

$$
\begin{aligned}
&= Q_{n-1}\left(\frac{P_{n-1}+\sqrt{d}}{Q_{n-1}}\right) - P_{n-1} \\
&= \sqrt{d} && \therefore P_n < \sqrt{d} \\
P_n &= a_{n-1}Q_{n-1} - P_{n-1} \\
&> (\alpha_{n-1}-1)Q_{n-1} - P_{n-1} \\
&= Q_{n-1}\left(\frac{P_{n-1}+\sqrt{d}}{Q_{n-1}} - 1\right) - P_{n-1} \\
&= \sqrt{d} - Q_{n-1}
\end{aligned}
$$

□

Theorem 12. *Q_n (and P_n) are periodic.*

Proof. By the above theorem, there are finitely many possible values of both P_k, Q_k.
Suppose there are T unique tuples (P_k, Q_k) that appear in the sequence $\{(P_k, Q_k)\}_{k\geqslant 0}$. Then consider the first $T+1$ tuples in the sequence, and by the pigeonhole principle, there exists $1 \leqslant k_1 < k_2 \leqslant T+1$ such that

$$(P_{k_1}, Q_{k_1}) = (P_{k_2}, Q_{k_2}).$$

For any k,

$$a_k = \left\lfloor \frac{P_k + \sqrt{d}}{Q_k} \right\rfloor,$$

so each tuple (P_k, Q_k) is a function of the previous tuple (P_{k-1}, Q_{k-1}).
Let $k, k+l$ be the first occurence for which $(P_k, Q_k) = (P_{k+l}, Q_{k+l})$, and so for all $n > k$, let $n' \equiv n \mod l$ such that $k \leqslant n' \leqslant k+l$,

$$(P_n, Q_n) = (P_{n'}, Q_{n'}).$$

□

Notice that as a_k is a function of P_k and Q_k, the continued fraction $[a_0, a_1, ...]$ is also periodic.
Henceforth, if $\{A_n\}_{n\geqslant 0}$ is a periodic sequence with period p which begins to repeat at $n = k$, I denote:

$$\{A_n\}_{n\geqslant 0} = \{A_0, ..., A_{k-1}, \overline{A_k, ..., A_{k+p-1}}\}$$

and the periodic continued fraction $[a_0, a_1, ...]$ such that

$$\{a_n\}_{n\geqslant 0} = \{a_0, ..., a_{k-1}, \overline{a_k, ..., a_{k+p-1}}\}$$

I denote:

$$[a_0, a_1, ...] = [a_0, ..., a_{k-1}, \overline{a_k, ..., a_{k+p-1}}]$$

5 Patterns in Q_n

Given a nonsquare positive integer d, Theorem 9 specifies which nonzero values of $|l| < \sqrt{d}$ are such that $x^2 - dy^2 = \pm l$ have a solution, we can find these values if we calculate the continued fraction for $\sqrt{d}$. In the previous section, we showed that when considering the continued fraction for $\sqrt{d}$, the sequence $\{Q_n\}_{n\geqslant 0}$ is periodic. So, given any d, we can perform an algorithm which, in finitely many steps, tells us which nonzero values of $|l| < \sqrt{d}$ are such that $x^2 - dy^2 = \pm l$ have a solution.
While this does not characterize which values of l have solutions for all possible values of d, we might consider families of values of d.
A paper by Balkova and Hruskova [2] presents a collection of known families of continued fractions. This section presents some of these continued fractions, along with the sequences $\{Q_n\}_{n\geqslant 0}$, so that the application of Theorem 9 would describe which nonzero values of $|l| < \sqrt{d}$ have solutions to $x^2 - dy^2 = \pm l$ for some families of values of d.

Theorem 13. [2] *The continued fraction of $\sqrt{N}$ has period 1 iff $N = n^2 + 1$. It holds then that $\sqrt{N} = [n, \overline{2n}]$.*

For $k > 0$, we have $\alpha_k = \overline{[2n]} = n + \sqrt{N}$.
And therefore $P_k = n, Q_k = 1$.

Henceforth $N = n^2 + j$ where $1 \leqslant j \leqslant 2n$.
the continued fraction for $\sqrt{N}$ begins with $a_0 = n$, so
$P_0, Q_0 = 0, 1$ and

$$\begin{aligned} P_1 &= a_0 Q_0 - P_0 \\ &= n \times 1 - 0 = n \\ Q_1 &= \frac{N - P_1^2}{Q_0} \end{aligned}$$

$$= \frac{n^2 + j - n^2}{1} = j$$

Theorem 14. [2, Observation 2] *$\sqrt{N}$ has period 2 iff $\frac{2n}{j}$ is an integer. It holds then that $\sqrt{N} = [n, \overline{\frac{2n}{j}, 2n}]$*

$P_0, Q_0, P_1, Q_1 = 0, 1, n, j$

$$\begin{aligned}
P_2 &= a_1 Q_1 - P_1 \\
&= \frac{2n}{j} \times j - n = n \\
Q_2 &= \frac{N - P_2^2}{Q_1} \\
&= \frac{n^2 + j - n^2}{j} = 1
\end{aligned}$$

$$\begin{aligned}
P_3 &= a_2 Q_2 - P_2 \\
&= 2n \times 1 - n = n = P_1 \\
Q_3 &= \frac{N - P_2^3}{Q_2} \\
&= \frac{n^2 + j - n^2}{1} = j = Q_1 \\
\therefore \{P_k\}_{k \geqslant 0} &= \{0, \overline{n}\} \\
\text{and } (Q_k)_{k \geqslant 0} &= \{\overline{1, j}\}
\end{aligned}$$

Theorem 15. [2, Observation 3] *If the continued fraction of $\sqrt{N}$ has period of length 3, then j is an odd number and $\sqrt{N} = [n, \overline{x, x, 2n}]$, where x is an even number and*

$$j = \frac{2xn + 1}{x^2 + 1}$$

$P_0, Q_0, P_1, Q_1 = 0, 1, n, j$

$$\begin{aligned}
P_2 &= a_1 Q_1 - P_1 \\
&= x \times j - n \\
Q_2 &= \frac{N - P_2^2}{Q_1} \\
&= \frac{n^2 + j - (xj - n)^2}{j} \\
&= -jx^2 + 2nx + 1 \\
&= -\left(\frac{2xn + 1}{x^2 + 1}\right) x^2 + 2nx + 1 \\
&= \frac{2nx + 1}{x^2 + 1} \\
&= j
\end{aligned}$$

$$\begin{aligned}
P_3 &= a_2 Q_2 - P_2 \\
&= x \times j - (xj - n) = n \\
Q_3 &= \frac{N - P_3^2}{Q_2} \\
&= \frac{n^2 + j - n^2}{j} = 1 \\
P_4 &= a_3 Q_3 - P_3 \\
&= 2n \times 1 - n = n = P_1 \\
Q_4 &= \frac{N - P_4^2}{Q_3} \\
&= \frac{n^2 + j - n^2}{1} = j = Q_1 \\
\therefore \{P_k\}_{k \geqslant 0} &= \{0, \overline{n, xj - n, n}\} \\
\text{and } \{Q_k\}_{k \geqslant 0} &= \{\overline{1, j, j}\}
\end{aligned}$$

Theorem 16. [2, Observation 4]*Let $j = 4$. If n is even, then the length of the period is 2 and $\sqrt{N} = [n; \overline{\frac{2n}{j}, 2n}]$. If n is odd, then the length of the period is 5 and $\sqrt{N} = [n; \overline{\frac{n-1}{2}; 1; 1; \frac{n-1}{2}; 2n}]$.*

If n is even, we have $\sqrt{N} = [n, \overline{\frac{2n}{j}, 2n}]$, which after theorem 14 I showed implies

$$\{P_k\}_{k\geqslant 0} = \{0, \overline{n}\}$$
$$\textit{and } \{Q_k\}_{k\geqslant 0} = \{\overline{1, j}\}$$

where $j = 4$.
If n is odd, $P_0, Q_0, P_1, Q_1 = 0, 1, n, j$ (where $j = 4$).

$$\begin{aligned}
P_2 &= a_1Q_1 - P_1 \\
&= \frac{n-1}{2} \times j - n \\
&= n - 2 \\
Q_2 &= \frac{N - P_2^2}{Q_1} \\
&= \frac{n^2 + j - (n-2)^2}{j} \\
&= \frac{4n}{j} - \frac{4}{j} + 1 \\
&= n \\
P_3 &= a_2Q_2 - P_2 \\
&= 1 \times n - (n-2) \\
&= 2 \\
Q_3 &= \frac{N - P_3^2}{Q_2} \\
&= \frac{n^2 + j - 2^2}{n} \\
&= n \\
P_4 &= a_3Q_3 - P_3 \\
&= 1 \times n - 2
\end{aligned}$$

$$\begin{aligned}
Q_4 &= \frac{N - P_4^2}{Q_3} \\
&= \frac{n^2 + j - (n-2)^2}{n} \\
&= \frac{j + 4n - 4}{n} \\
&= 4 \\
P_5 &= a_4Q_4 - P_4 \\
&= \frac{n-1}{2} \times 4 - (n-2) \\
&= n \\
Q_5 &= \frac{N - P_5^2}{Q_4} \\
&= \frac{n^2 + j - n^2}{4} \\
&= 1 \\
P_6 &= a_5Q_5 - P_5 \\
&= 2n \times 1 - n \\
&= n = P_1 \\
Q_6 &= \frac{N - P_6^2}{Q_5} \\
&= \frac{n^2 + j - n^2}{1} \\
&= j = 4 = Q_1
\end{aligned}$$

$\therefore \{P_k\}_{k\geqslant 0} = \{0, \overline{n, n-2, 2, n-2, n}\}$ *and* $\{Q_k\}_{k\geqslant 0} = \{\overline{1, 4, n, n, 4}\}$

Observation 5. For $n > 1$ and $j = 2n-1$ the length of the period is 4 and the continued fraction is then $\sqrt{N} = [n, \overline{1, n-1, 1, 2n}]$.

$P_0, Q_0, P_1, Q_1 = 0, 1, n, j$ (where $j = 2n-1$).

$$
\begin{aligned}
P_2 &= a_1Q_1 - P_1 \\
&= 1 \times j - n \\
&= n - 1 \\
Q_2 &= \frac{N - P_2^2}{Q_1} \\
&= \frac{n^2 + j - (n-1)^2}{j} \\
&= \frac{n^2 + 2n - 1 - (n^2 - 2n + 1)}{2n-1} \\
&= 2 \\
P_3 &= a_2Q_2 - P_2 \\
&= (n-1) \times 2 - (n-1) \\
&= n - 1 \\
Q_3 &= \frac{N - P_3^2}{Q_2} \\
&= \frac{n^2 + j - (n-1)^2}{2} \\
&= \frac{n^2 + 2n - 1 - (n^2 - 2n + 1)}{2} \\
&= 2n - 1 \\
P_4 &= a_3Q_3 - P_3 \\
&= 1 \times (2n-1) - (n-1) \\
&= n \\
Q_4 &= \frac{N - P_4^2}{Q_3} \\
&= \frac{n^2 + j - n^2}{2n-1} \\
&= 1 \\
P_5 &= a_4Q_4 - P_4 \\
&= 2n \times 1 - n \\
&= n = P_1 \\
Q_5 &= \frac{N - P_5^2}{Q_4} \\
&= \frac{n^2 + j - n^2}{1} \\
&= j = Q_1 \\
\therefore \{P_k\}_{k\geqslant 0} &= \{0, \overline{n, n-1, n-1, n}\} \\
\text{and } \{Q_k\}_{k\geqslant 0} &= \{\overline{1, 2n-1, 2, 2n-1}\}
\end{aligned}
$$

Theorem 17. [2, Observation 6] *For $n > 3$ and $j = 2n-3$, either the length of the period is 4 if n is odd and the continued fraction is then $\sqrt{N} = [n, \overline{1, \frac{n-3}{2}, 1, 2n}]$, or the length of the period is 6 if n is even and the continued fraction is then $\sqrt{N} = [n, \overline{1, \frac{n}{2} - 1, 2, \frac{n}{2} - 1, 1, 2n}]$.*

Suppose n is odd. $P_0, Q_0, P_1, Q_1 = 0, 1, n, j$ (where $j = 2n-3$)

$$
\begin{aligned}
P_2 &= a_1Q_1 - P_1 \\
&= 1 \times j - n \\
&= n - 3 \\
Q_2 &= \frac{N - P_2^2}{Q_1} \\
&= \frac{n^2 + j - (n-3)^2}{j} \\
&= \frac{n^2 + 2n - 3 - (n^2 - 6n + 9)}{2n-3} \\
&= 4 \\
P_3 &= a_2Q_2 - P_2 \\
&= \frac{n-3}{2} \times 4 - (n-3) \\
&= n - 3 \\
Q_3 &= \frac{N - P_3^2}{Q_2} \\
&= \frac{n^2 + j - (n-3)^2}{4} \\
&= \frac{n^2 + 2n - 3 - (n^2 - 6n + 9)}{4} \\
&= 2n - 3 \\
P_4 &= a_3Q_3 - P_3 \\
&= 1 \times (2n-3) - (n-3) \\
&= n \\
Q_4 &= \frac{N - P_4^2}{Q_3} \\
&= \frac{n^2 + j - n^2}{2n-3} \\
&= 1 \\
P_5 &= a_4Q_4 - P_4 \\
&= 2n \times 1 - n \\
&= n = P_1 \\
Q_5 &= \frac{N - P_5^2}{Q_4} \\
&= \frac{n^2 + j - n^2}{1} \\
&= 2n - 3 = Q_1 \\
\therefore \{P_k\}_{k \geqslant 0} &= \{0, \overline{n, n-3, n-3, n}\} \\
\textit{and } \{Q_k\}_{k \geqslant 0} &= \{\overline{1, 2n-3, 4, 2n-3}\}
\end{aligned}
$$

Suppose n is even.

Once again, $\sqrt{N} = [n, \overline{1, \frac{n}{2} - 1, 2, \frac{n}{2} - 1, 1, 2n}]$. $P_0, Q_0, P_1, Q_1 = 0, 1, n, j$ (where $j = 2n - 3$)

$$
\begin{aligned}
P_2 &= a_1Q_1 - P_1 \\
&= 1 \times j - n \\
&= n - 3 \\
Q_2 &= \frac{N - P_2^2}{Q_1} \\
&= \frac{n^2 + j - (n-3)^2}{j} \\
&= \frac{n^2 + 2n - 3 - (n^2 - 6n + 9)}{2n-3} \\
&= 4 \\
P_3 &= a_2Q_2 - P_2 \\
&= \frac{n-2}{2} \times 4 - (n-3) \\
&= n - 1 \\
Q_3 &= \frac{N - P_3^2}{Q_2} \\
&= \frac{n^2 + j - (n-1)^2}{4} \\
&= \frac{n^2 + 2n - 3 - (n^2 - 2n + 1)}{4}
\end{aligned}
$$

$$
\begin{aligned}
&= n-1 \\
P_4 &= a_3Q_3 - P_3 \\
&= 2\times(n-1)-(n-1) \\
&= n-1 \\
Q_4 &= \frac{N-P_4^2}{Q_3} \\
&= \frac{n^2+j-(n-1)^2}{n-1} \\
&= \frac{n^2+2n-3-(n^2-2n+1)}{n-1} \\
&= 4 \\
P_5 &= a_4Q_4 - P_4 \\
&= \frac{n-2}{2}\times 4-(n-1) \\
&= n-3 \\
Q_5 &= \frac{N-P_5^2}{Q_4} \\
&= \frac{n^2+j-(n-3)^2}{4} \\
&= \frac{n^2+2n-3-(n^2-6n+9)}{4}
\end{aligned}
\qquad
\begin{aligned}
&= 2n-3 \\
P_6 &= a_5Q_5 - P_5 \\
&= 1\times(2n-3)-(n-3) \\
&= n \\
Q_6 &= \frac{N-P_6^2}{Q_5} \\
&= \frac{n^2+j-n^2}{2n-3} \\
&= 1 \\
P_7 &= a_6Q_6 - P_6 \\
&= 2n\times 1-n \\
&= n = P_1 \\
Q_7 &= \frac{N-P_7^2}{Q_6} \\
&= \frac{n^2+j-n^2}{1} \\
&= j = Q_1 \\
\therefore \{P_k\}_{k\geqslant 0} &= \{0,\overline{n,n-3,n-1,n-1,n-3,n}\} \\
\textit{and } \{Q_k\}_{k\geqslant 0} &= \left\{\overline{1,2n-3,4,n-1,4,2n-3}\right\}
\end{aligned}
$$

6 Arbitrary period length continued fractions

Given an arbitrary period length, this section proves a construction of families of values of d such that the continued fraction of $\sqrt{d}$ as presented by Sierpinski [5].
First, there is another useful notation for continued fractions:

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_n}}} = [a_1, a_2, ..., a_n] = \frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots + \frac{1|}{|a_n}$$

We will need the result of theorem 1, which says that if the k^{th} convergent $C_k = [a_0, ..., a_k] = p_k/q_k$,
the sequences $p_0, ..., p_n$, and $q_0, ..., q_n$ satisfy the recursive relation (*):

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

for $k \geqslant 2$.
Fact (**): For any natural number k,

$$\sqrt{k^2 + 1} = [k, \overline{2k}]$$

Proof.

$$\begin{aligned} \sqrt{n^2 + 1} &= n + \frac{\sqrt{n^2 + 1} - n}{1} \\ &= n + \frac{1}{\sqrt{n^2 + 1} + n} \\ &= n + \cfrac{1}{2n + \frac{\sqrt{n^2+1}-n}{1}} \end{aligned}$$

□

One last thing, we need the following lemma:
If n is a natural number $n > 1$ and $a_1, a_2, ..., a_n$ a symmetric sequence of natural numbers, and if, moreover, p_k/q_k denotes the k^{th} convergent of the continued

fraction

$$\frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots + \frac{1|}{|a_n},$$

then

$$p_n = q_{n-1}$$

To match the definition of the sequence p_k, q_k above, we can define $a_0 = 0$.

Proof. First, I claim that

$$\frac{q_n}{q_{n-1}} = a_n + \frac{1|}{|a_{n-1}} + \frac{1|}{|a_{n-2}} + \cdots + \frac{1|}{|a_2} + \frac{1|}{|a_1}$$

For $n = 2$,

$$\frac{q_2}{q_1} = \frac{a_2 q_1 + q_0}{q_1} = a_2 + \frac{q_0}{q_1} = a_2 + \frac{1}{a_1}$$

For $n > 2$, we may assume for induction that
$\frac{q_{n-1}}{q_{n-2}} = a_{n-1} + \frac{1|}{|a_{n-2}} + \cdots + \frac{1|}{|a_2} + \frac{1|}{|a_1}$ and so

$$\begin{aligned}
\frac{q_n}{q_{n-1}} &= \frac{a_n q_{n-1} + q_{n-2}}{q_{n-1}} \\
&= a_n + \frac{q_{n-2}}{q_{n-1}} \\
&= a_n + \frac{1}{q_{n-1}/q_{n-2}} \\
&= a_n + \frac{1|}{|a_{n-1}} + \frac{1|}{|a_{n-2}} + \cdots + \frac{1|}{|a_2} + \frac{1|}{|a_1}
\end{aligned}$$

Which proves the claim.
Returning to the lemma, notice the statement is true for $n = 1$:

$$\begin{aligned}
p_n &= p_1 \\
&= a_0 a_1 + 1 \\
&= 1 \\
&= q_0 \\
&= q_{n-1}
\end{aligned}$$

For $n > 1$, we use the claim:

$$\frac{q_{n-1}}{q_n} = \frac{1}{q_n/q_{n-1}}$$

$$= \frac{1|}{|a_n} + \frac{1|}{|a_{n-1}} + \frac{1|}{|a_{n-2}} + \cdots + \frac{1|}{|a_2} + \frac{1|}{|a_1}$$
$$= \frac{p_n}{q_n}$$

□

Theorem 18. [5, Theorem 8.6] *For any natural number s there exist infinitely many natural numbers D such that the representation of the number $\sqrt{D}$ as a simple continued fraction has a period of s terms.*

Proof. Let k, n be two given natural numbers and let $a_1, a_2, ..., a_n$ be a sequence whose terms are all equal to $2k$. By the above lemma, $p_n = q_{n-1}$.

Define p'_j, q'_j as the sequences so that $\frac{p'_j}{q'_j}$ is the j^{th} convergent of $[a'_0, a'_1, ..., a'_j]$ where $a'_0 = 0, a'_{j'} = 2k$ for $1 \leqslant j' \leqslant j$.

For any integer $t \geqslant 0$, define

$$y_t = [q'_n t + k, \overline{2k, 2k, ..., 2k, 2q'_n t + 2k}]$$

where the sequence $2k, ..., 2k$ has n terms. Then

$$\begin{aligned} y_t &= q'_n t + k + \frac{1|}{|2k} + \frac{1|}{|2k} + \cdots + \frac{1|}{|2k} + \frac{1|}{|2k} + \frac{1|}{|\overline{[2q'_n t + 2k, 2k, 2k, ..., 2k]}} \\ &= q'_n t + k + \frac{1|}{|a'_1} + \frac{1|}{|a'_2} + \cdots + \frac{1|}{|a'_{n-1}} + \frac{1|}{|a'_n} + \frac{1|}{|q'_n t + k + y_t} \\ &= q'_n t + k + [0, a_1, a_2, ..., a_n, q'_n t + k + y_t] \end{aligned}$$

Since

$$\frac{p'_n}{q'_n} = [0, a'_1, a'_2, ..., a'_n],$$

we can use the recurrence relation (*) to say

$$\begin{aligned} y_t - q'_n t - k &= \frac{p'_n(q'_n t + k + y_t) + p'_{n-1}}{q'_n(q'_n t + k + y_t) + q'_{n-1}} \\ &= \frac{p'_n(q'_n t + k + y_t) + p'_{n-1}}{q'_n(q'_n t + k + y_t) + p'_n} \qquad \textit{since } q'_{n-1} = p'_n \end{aligned}$$

$$\therefore (y_t - q'_n t - k)(q'_n(q'_n t + k + y_t) + p'_n) = p'_n(q'_n t + k + y_t) + p'_{n-1}$$

$$\therefore q'_n(y_t^2 - (q'_n t + k)^2) + (y_t - q'_n t - k)p'_n = p'_n(q'_n t + k + y_t) + p'_{n-1}$$
$$\therefore q'_n(y_t^2 - (q'_n t + k)^2) = 2p'_n(q'_n t + k) + p'_{n-1}$$

Fixing $t = 0$, we have

$$q'_n(y_0^2 - k^2) = 2p'_n k + p'_{n-1}$$

and by the definition of y_t, we also have

$$y_0 = [k, \overline{2k}] = \sqrt{k^2 + 1} \text{ by (**)}$$

$$\therefore q'_n = 2p'_n k + p'_{n-1}$$

Substituting this fact into

$$\begin{aligned} q'_n(y_t^2 - (q'_n t + k)^2) &= 2p'_n(q'_n t + k) + p'_{n-1}, \\ q'_n(y_t^2 - (q'_n t + k)^2) &= 2p'_n(q'_n t + k) + (q'_n - 2p'_n k) \\ &= 2p'_n q'_n t + q'_n \\ \therefore y_t^2 &= (q'_n t + k)^2 + 2p'_n t + 1 \\ \therefore y_t &= \sqrt{(q'_n t + k)^2 + 2p'_n t + 1} \end{aligned}$$

where by the recursive relation (*),

$$p'_m = \begin{cases} 0 & \text{if } m = 0 \\ 1 & \text{if } m = 1 \\ 2kp'_{m-1} + p'_{m-2} & \text{otherwise} \end{cases}$$
$$q'_m = p'_{m+1}$$

So, for any natural numbers n, k, t

$$D = (p'_{n+1} t + k)^2 + 2p'_n t + 1$$

has a period of $n + 1$ terms, each of the first n terms being equal to $2k$. Taking into account the fact the period

$$[k, \overline{2k}] = \sqrt{k^2 + 1}$$

has one term only, the proof is complete. □

With this theorem, we may construct continued families of periodic continued fractions with arbitrary period length, but to see how it relates to Pell's equation, we take note of the resulting values in the periodic sequence $\{Q_n\}_{n\geqslant 0}$ that results from this construction.

Given $l', k \in \mathbb{N}, t \geqslant 0$, let $l = l' + 1$, and

$$D = (q'_{l'}t + k)^2 + 2p'_{l'}t + 1.$$

If $t = 0$, $\sqrt{D} = \sqrt{k^2+1}$ has a period of 1.
If $t > 0$, D is such that the continued fraction of $\sqrt{D}$ has period $l' + 1 = l$.

$$p'_m = \begin{cases} 0 & \textit{if } m = 0 \\ 1 & \textit{if } m = 1 \\ 2kp'_{m-1} + p'_{m-2} & \textit{otherwise} \end{cases}$$
$$q'_m = p'_{m+1}$$

so $1 \leqslant 2p'_{l'}t + 1 \leqslant 2(q'_{l'}t + k)$, so $D = n^2 + j$ where $n = q'_{l'}t + k, j = 2p'_{l'}t + 1$.

$$\sqrt{D} = [q'_{l'}t + k, \overline{2k, 2k, ..., 2k, 2q'_{l'}t + 2k}]$$

$P_0, Q_0, P_1, Q_1 = 0, 1, n, j = 0, 1, q'_{l'}t + k, 2p'_{l'}t + 1$

6.1 Case 1: $k = 1, l' = 1$

$(P_0, Q_0, P_1, Q_1) = (0, 1, n, j) = (0, 1, 2t + 1, 2t + 1)$

$$\begin{aligned} D &= (2t+1)^2 + 2t + 1 \\ \therefore \sqrt{D} &= [2t + 1, \overline{2, 4t + 2}] \\ P_2 &= a_1Q_1 - P_1 \\ &= 2 \times (2t + 1) - (2t + 1) \\ &= 2t + 1 \\ Q_2 &= \frac{D - P_2^2}{Q_1} \\ &= \frac{(2t+1)^2 + 2t + 1 - (2t+1)^2}{2t+1} \end{aligned}$$

$$
\begin{aligned}
&= 1 \\
P_3 &= a_2Q_2 - P_2 \\
&= (4t+2) \times 1 - (2t+1) \\
&= 2t+1 = n = P_1 \\
Q_3 &= \frac{D - P_3^2}{Q_2} \\
&= \frac{(2t+1)^2 + 2t + 1 - (2t+1)^2}{1} \\
&= 2t+1 = j = Q_1 \\
\therefore \{P_k\}_{k\geqslant 0} &= \{0, \overline{2t+1}\} \\
and\ \{Q_k\}_{k\geqslant 0} &= \{\overline{1, 2t+1}\}
\end{aligned}
$$

6.2 Case 2: $k = 1, l' = 2$

$(P_0, Q_0, P_1, Q_1) = (0, 1, n, j) = (0, 1, 5t+1, 4t+1)$

$$
\begin{aligned}
D &= (5t+1)^2 + 4t + 1 \\
\therefore \sqrt{D} &= [5t+1, \overline{2, 2, 10t+2}] \\
P_2 &= a_1Q_1 - P_1 \\
&= 2 \times (4t+1) - (5t+1) \\
&= 3t+1 \\
Q_2 &= \frac{D - P_2^2}{Q_1} \\
&= \frac{(5t+1)^2 + 4t + 1 - (3t+1)^2}{4t+1} \\
&= 4t+1 \\
P_3 &= a_2Q_2 - P_2 \\
&= 2 \times (4t+1) - (3t+1) \\
&= 5t+1 \\
Q_3 &= \frac{D - P_3^2}{Q_2} \\
&= \frac{(5t+1)^2 + 4t + 1 - (5t+1)^2}{4t+1} \\
&= 1 \\
P_4 &= a_3Q_3 - P_3
\end{aligned}
$$

$$
\begin{aligned}
&= (10t+2) \times 1 - (5t+1) \\
&= 5t+1 = P_1 \\
Q_4 &= \frac{D - P_4^2}{Q_3} \\
&= \frac{(5t+1)^2 + 4t + 1 - (5t+1)^2}{1} \\
&= 4t+1 = Q_1
\end{aligned}
$$

$$
\begin{aligned}
\therefore \{P_k\}_{k \geqslant 0} &= \{0, \overline{5t+1, 3t+1, 5t+1}\} \\
and\ \{Q_k\}_{k \geqslant 0} &= \{\overline{1, 4t+1, 4t+1}\}
\end{aligned}
$$

6.3 Case 3: $k = 1, l' = 3$

$(P_0, Q_0, P_1, Q_1) = (0, 1, n, j) = (0, 1, 12t+1, 10t+1)$

$$
\begin{aligned}
D &= (12t+1)^2 + 10t + 1 \\
\therefore \sqrt{D} &= [5t+1, \overline{2, 2, 2, 24t+2}] \\
P_2 &= a_1 Q_1 - P_1 \\
&= 2 \times (10t+1) - (12t+1) \\
&= 8t+1 \\
Q_2 &= \frac{D - P_2^2}{Q_1} \\
&= \frac{(12t+1)^2 + 10t + 1 - (8t+1)^2}{10t+1} \\
&= 8t+1 \\
P_3 &= a_2 Q_2 - P_2 \\
&= 2 \times (8t+1) - (8t+1) \\
&= 8t+1 \\
Q_3 &= \frac{D - P_3^2}{Q_2} \\
&= \frac{(12t+1)^2 + 10t + 1 - (8t+1)^2}{8t+1} \\
&= 10t+1
\end{aligned}
$$

$$
\begin{aligned}
P_4 &= a_3 Q_3 - P_3 \\
&= 2 \times (10t+1) - (8t+1) \\
&= 12t + 1 \\
Q_4 &= \frac{D - P_4^2}{Q_3} \\
&= \frac{(12t+1)^2 + 10t + 1 - (12t+1)^2}{10t+1} \\
&= 1 \\
P_5 &= a_4 Q_4 - P_4 \\
&= (24t+2) \times 1 - (12t+1) \\
&= 12t + 1 = P_1 \\
Q_5 &= \frac{D - P_5^2}{Q_4} \\
&= \frac{(12t+1)^2 + 10t + 1 - (12t+1)^2}{1} \\
&= 10t + 1 = Q_1 \\
\therefore \{P_k\}_{k \geqslant 0} &= \{0, \overline{12t+1, 8t+1, 8t+1, 12t+1}\} \\
\textit{and } \{Q_k\}_{k \geqslant 0} &= \{\overline{1, 10t+1, 8t+1, 10t+1}\}
\end{aligned}
$$

7 Primes satisfying Original Problem Condition

In this section several values of d are considered that satisfy the condition described in the original problem:
d prime, $d \equiv 3 \mod 4$ such that$x^2 - dy^2 = \pm l$ has a solution for all primes 2 and l with $l < 12(\log d)^2$ and $\left(\frac{d}{l}\right) = 1$ for l odd.
Theorem 7 describes a process in which we can calculate the continued fraction for a number like $\sqrt{d}$, one number a_k at a time, and Theorem 12 provides a halting condition for this process, guaranteed to come in finitely many steps. For example, the first few steps for $d = 919$ are:

$$
\begin{aligned}
\alpha = \alpha_0 = \frac{0 + \sqrt{919}}{1} &= \left[30, \frac{30 + \sqrt{919}}{19}\right] \\
&= \left[30, 3, \frac{27 + \sqrt{919}}{10}\right] \\
&= \left[30, 3, 5, \frac{23 + \sqrt{919}}{39}\right]
\end{aligned}
$$

$$= \ldots$$

Eventually, we arrive at the periodic sequences:

$$\sqrt{919} = [30, \quad \overline{3,5,1,2,1,2,1,1,1,2,3,1,19,2,3,1,1,4,9,1,} \\ \overline{7,1,3,6,2,11,1,1,1,29,1,1,1,11,2,6,3,1,7,1,} \\ \overline{9,4,1,1,3,2,19,1,3,2,1,1,1,2,1,2,1,5,3,60}]$$

and

$$\{P_k\}_{k\geqslant 0} = \quad \{0, \overline{30,27,23,16,18,17,19,12,13,17,25,17,28,} \\ \overline{29,23,22,7,23,29,25,24,25,17,28,26,28,27,11,10,} \\ \overline{29,29,10,11,27,28,26,28,17,25,24,25,29,23,7,} \\ \overline{22,23,29,28,17,25,17,13,12,19,17,18,16,23,27,30}\}$$

$$\textit{and } \{Q_k\}_{k\geqslant 0} = \quad \{\overline{1,19,10,39,17,35,18,31,25,30,21,14,45,3,} \\ \overline{26,15,29,30,13,6,49,7,42,15,9,27,5,38,21,39,2,} \\ \overline{39,21,38,5,27,9,15,42,7,49,6,13,30,} \\ \overline{29,15,26,3,45,14,21,30,25,31,18,35,17,39,10,19}\}$$

Definition 10. *Let p be an odd prime number. An integer a is a quadratic residue modulo p if it is congruent to a perfect square modulo p and is a quadratic nonresidue modulo p otherwise. The Legendre symbol is a function of a and p defined as*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \mod p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } a \equiv 0 \mod p \end{cases}$$

For sufficiently large d, the bound $12(\log d)^2$ is less than $\sqrt{d}$, but for $d = 919$, $12(\log 919)^2 \simeq 558.6868$, and $\sqrt{919} \simeq 30.3150$.
The primes $\leqslant \sqrt{919}$ are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.
$1^2 \equiv 1 \mod 3 \equiv 919 \mod 3$, so $\left(\frac{919}{3}\right) = 1$.
$2^2 \equiv 4 \mod 5 \equiv 919 \mod 5$, so $\left(\frac{919}{5}\right) = 1$.
$3^2 \equiv 2 \mod 7 \equiv 919 \mod 7$, so $\left(\frac{919}{7}\right) = 1$.
$x^2 \equiv 919 \mod 11$ has no solutions, so $\left(\frac{919}{11}\right) = -1$.
$3^2 \equiv 9 \mod 13 \equiv 919 \mod 13$, so $\left(\frac{919}{13}\right) = 1$.

$1^2 \equiv 1 \mod 17 \equiv 919 \mod 17$, so $\left(\frac{919}{17}\right) = 1$.
$8^2 \equiv 7 \mod 19 \equiv 919 \mod 19$, so $\left(\frac{919}{19}\right) = 1$.
$x^2 \equiv 919 \mod 23$ has no solutions, so $\left(\frac{30}{23}\right) = -1$.
$7^2 \equiv 20 \mod 29 \equiv 919 \mod 29$, so $\left(\frac{919}{29}\right) = 1$.
Notice that $Q_{30} = 2, Q_{13} = 3, Q_{26} = 5, Q_{21} = 7, Q_{18} = 13, Q_4 = 17, Q_1 = 19$, and $Q_{16} = 29$, so without needing to find explicit solutions, 919 is a prime $\equiv 3 \mod 4$ such that $x^2 - 919y^2 = \pm l$ has a solution for all primes 2 and $l < \sqrt{d}$ such that $\left(\frac{919}{l}\right) = 1$.

Let $d = 67$. d is prime and $d \equiv 3 \mod 4$.

$$\sqrt{67} = [8, \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}$$

and

$$\{P_k\}_{k \geqslant 0} = \{0, \overline{8, 7, 5, 2, 7, 7, 2, 5, 7, 8}\}$$
$$\textit{and } \{Q_k\}_{k \geqslant 0} = \{\overline{1, 3, 6, 7, 9, 2, 9, 7, 6, 3}\}$$

Like with $d = 919$, we consider the bound $l < \sqrt{d} \simeq 8$, and the primes $\leqslant \sqrt{67}$ are $2, 3, 5, 7$.
$1^2 \equiv 1 \mod 3 \equiv 67 \mod 3$, so $\left(\frac{67}{3}\right) = 1$.
$x^2 \equiv 67 \mod 5$ has no solutions, so $\left(\frac{67}{5}\right) = -1$.
$2^2 \equiv 4 \mod 7 \equiv 67 \mod 7$, so $\left(\frac{67}{7}\right) = 1$.
$Q_5 = 2, Q_1 = 3, Q_3 = 7$, so 67 is also a prime $\equiv 3 \mod 4$ such that $x^2 - dy^2 = \pm l$ has a solution for all primes 2 and $l < \sqrt{d}$ such that $\left(\frac{d}{l}\right) = 1$.

Let $d = 11$. d is prime and $d \equiv 3 \mod 4$.

$$\sqrt{11} = [3, \overline{3, 6}$$

$$\{P_k\}_{k \geqslant 0} = \{0, \overline{3}\}$$
$$\textit{and } \{Q_k\}_{k \geqslant 0} = \{\overline{1, 2}\}$$

Like with $d = 919$, we consider the bound $l < \sqrt{d} \simeq 3$, and the primes $\leqslant \sqrt{11}$ are $2, 3$.
$x^2 \equiv 11 \mod 3$ has no solutions, so $\left(\frac{11}{3}\right) = -1$.

So, as $Q_1 = 2$, 11 is also a prime $\equiv 3 \mod 4$ such that $x^2 - dy^2 = \pm l$ has a solution for all primes 2 and $l < \sqrt{d}$ such that $\left(\frac{d}{l}\right) = 1$.
For this value of d we can verify Theorem 9 as indeed $x^2 - 11y^2 = -2$ has solution $x = 3, y = 1$.

8 Conclusion

In this paper, we present proofs to several known facts important to solving Pell-like equations, and found several primes $d \equiv 3 \mod 4$ such that $x^2 - dy^2 = \pm l$ is soluble for all primes 2 and l with $l < 12(\log d)^2$ and $\left(\frac{d}{l}\right) = 1$ for l odd.
However, it remains to be proved whether there are infinitely many such primes.

References

[1] Eric Bach, *Explicit bounds for primality testing and related problems*, Mathematics of Computation **55** (1990), no. 191, 355–380.

[2] Lubomíra Balková and Aranka Hrušková, *Continued fractions of quadratic numbers*, arXiv preprint arXiv:1302.0521 (2013).

[3] L-K Hua, *Introduction to number theory*, Springer Science & Business Media, 2012.

[4] M Ram Murty and Jody Esmonde, *Problems in algebraic number theory*, Vol. 190, Springer Science & Business Media, 2005.

[5] Waclaw Sierpinski, *Elementary theory of numbers*, 1964 (eng).