Formalising Continued Fractions (With Applications to Pell's Equation)

Manuel Eberl[1][0000−0002−4263−6571]

University of Innsbruck, Technikerstr. 21a, 6020 Innsbruck, Austria
manuel.eberl@uibk.ac.at

Abstract. This article presents an Isabelle/HOL formalisation of simple continued fractions with a focus on executable algorithms. In particular, the two-way correspondence between real numbers and continued fractions is established and various important results are proven, e.g. the connection to best rational approximations.
Additional contributions are: the study of periodic continued fractions, efficient computation of the continued fraction for $\sqrt{D}$ where D is a positive non-square integer, the continued fraction expansion of Euler's number e, and the connection to Pell's equation.
This machinery is then applied to solve Archimedes' cattle problem, which involves solving an instance of Pell's equation where the solution has over 10^5 decimals.

Keywords: continued fractions· Pell's equation· rational approximation· Isabelle/HOL

1 Introduction

Continued fractions are a fairly old and important piece of mathematics that has received surprisingly little treatment in proof assistants so far. Like decimal expansions, they provide a representation of arbitrary real numbers as a (possibly infinite) sequence of integers. While decimal expansions represent a real number as a potentially infinite sum

$$\sum_{i \geq n_0} a_i 10^{-i}$$

for a sequence $(a_i)_{i \geq n_0}$ with $a_i \in \{0, \ldots, 9\}$, a continued fraction has the form

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \ldots}}} \tag{1}$$

for sequences of integers $(a_i)_{i \geq 0}$ and $(b_i)_{i \geq 1}$. We will focus entirely on *simple* continued fractions, where $b_i = 1$ for all i. This case is of particular interest

since it allows a (mostly) unique representation of real numbers (similar to decimal expansions). We will use the notation $[a_0; a_1, a_2, \ldots]$ for a simple continued fraction such as the one in Eq. (1) (with all $b_i = 1$). Whenever I say *continued fraction* in this article, I will mean a *simple* continued fraction.

One important application of continued fractions is their behaviour under truncation: While truncating a decimal expansion at any point gives us a rational approximation of the real number being represented, truncating a continued fraction expansion gives the *best* rational approximation (among fractions with limited denominator). Moreover, any sufficiently good rational approximation of a real number x can also be shown to be a truncation of its continued fraction.

Several other interesting results were also formalised:

- Euler's number e has the very regular (but non-periodic) continued fraction expansion $[2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots]$.
- By connecting the formalisation to Isabelle's `approximation` framework, continued fraction expansion can be computed for any real constant supported by this framework (e.g. π, e, $\ln 2$, $\sqrt{129}$).
- Periodic continued fractions correspond to *quadratic irrationals*, i.e. irrational numbers x with $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{Z}$.
- In particular, the expansion for $\sqrt{D}$ for a non-square integer $D > 0$ begins with $\lfloor \sqrt{D} \rfloor$ followed by a period of a very restricted form that can be computed efficiently.
- The connection between Pell's equation with parameter D and the continued fraction expansion of $\sqrt{D}$ is made, in particular giving us an efficient executable solver for Pell's equation based on computing this expansion.

All of this material is available in the Archive of Formal Proofs [3].[1]

A remark on notation: when talking about a particular continued fraction, I will always implicitly assume it to be of the form $[a_0; a_1, a_2, a_3, \ldots]$. The a_i are called its *coefficients* and the real number it represents will be denoted x. The sequences $(h_n)_{n\geq 0}$ and $(k_n)_{n\geq 0}$ will denote the *continuants* of the continued fraction (a notion that will be defined later).

For a more in-detail presentation of most of the material I recommend Khinchin's brief introduction [8], which guided much of my formalisation as well (although many other sources were also used, since the material is essentially folklore).

2 Definition

For now, let us consider continued fractions merely as a (possibly infinite) sequence of numbers $[a_0; a_1, a_2, \ldots]$ with the interpretation as a (possibly infinitely)

[1] Some minor details in the formalisation were tweaked when preparing this article for submission and these changes are currently only visible in the development version for the AFP, but for the most part everything is already available in AFP-2025-2. The material on Archimedes' Cattle Problem has been submitted to the AFP but is not yet accepted. It will probably be in the AFP for the camera-ready version; meanwhile it is available on GitHub [4].

nested fraction from Eq. (1) in mind but without making it formally explicit just yet. For reasons that will become clear once we make the connection to real numbers, we allow a_0 to be an arbitrary integer, but we require $a_1, a_2, a_3, \ldots$ to be *positive* integers.

In Isabelle, this is modelled as a type *cfrac* which is internally a pair consisting of the integer a_0 and a *lazy list* of natural numbers containing the $a_i - 1$. Wrappers around this internal structure are defined so that we need not deal with this anymore after the initial setup. Lazy lists in Isabelle are a *codatatype*, so we can use corecursive definitions and prove facts about them using coinduction. A coinduction rule for continued fractions can also be derived.

Basic operations are then defined:

- The n-th coefficient of a continued fraction is the integer a_n, written `cfrac_nth` in Isabelle.
- The *length* of a continued fraction (written `cfrac_length` in Isabelle) is its (possibly infinite) length as a sequence of coefficients, minus 1; e.g. the continued fractions of length 0 are the ones of the form $[k;]$ for an integer k.
- Given a continued fraction $[a_0; a_1, a_2, \ldots]$, we define its *tail* (written `cfrac_tl` in Isabelle) as $[a_1; a_2, a_3, \ldots]$. Clearly, if the tail of a continued fraction corresponds to some real number y, then the full fraction corresponds to $a_0 + 1/y$.
- Similarly, *dropping* the first k coefficients (written `cfrac_drop`) results in the continued fraction $[a_k; a_{k+1}, a_{k+2}, \ldots]$.
- Operations to convert any lazy list or stream of integer coefficients (within the appropriate bounds) to a continued fraction are also provided.

Note that operations like `cfrac_nth` and others we will introduce later are only well-defined for indices up to the length of the continued fraction. Since HOL is a total logic, `cfrac_nth` will still return a result for such inputs, but the result holds no meaning. Theorems talking about these operations will therefore typically require assumptions about the indices being in bounds.

To work towards the connection between a continued fraction and the real number it represents, let us move on to studying the truncations of a continued fraction, the so-called *convergents*. Since these are finitely nested, their interpretation as a real number is more immediately obvious.

3 Convergents

The n-th convergent of a continued fraction $[a_0; a_1, a_2, \ldots]$ is the rational number obtained by truncating it after the n-th coefficient and interpreting it as a fraction in the way shown in Eq. (1). Formally, we have

```
fun conv :: cfrac ⇒ nat ⇒ real where
  conv c 0 = of_int (cfrac_nth c 0)
  conv c (Suc n) =
      of_int (cfrac_nth c 0) + 1 / conv (cfrac_tl c) n
```

The numerator and denominator of the convergent (also called its *continuants*) can also be specified recursively:[2]

```
fun conv_num :: cfrac ⇒ nat ⇒ int where
  conv_num c 0 = cfrac_nth c 0
  conv_num c 1 = cfrac_nth c 1 * cfrac_nth c 0 + 1
  conv_num c (n+2) =
      cfrac_nth c (n+2) * conv_num c (n+1) + conv_num c n

fun conv_denom :: cfrac ⇒ nat ⇒ int where
  conv_denom c 0 = 1
  conv_denom c 1 = cfrac_nth c 1
  conv_denom c (n+2) =
      cfrac_nth c (n+2) * conv_denom c (n+1) + conv_denom c n
```

From now on, we will write c_n for the n-th convergent of our continued fraction and h_n and k_n for the continuants.

In some cases it is convenient to extend the domain of h_n and k_n to $n \in \{-2, -1\}$ by setting $h_{-2} = k_{-1} = 0$ and $h_{-1} = k_{-2} = 1$. Corresponding variants of `conv_num` and `conv_denom` are provided.

Note that, again, for continued fractions of finite length l, the continuants and convergents are "morally" only defined up to index l. Since `cfrac_nth` c n is meaningless if $n > l$, so are h_n and k_n.

In addition to these operations, it is also useful to introduce a generalised notion of the convergent where rather than truncating the continued fraction after the n-th coefficient, we truncate after the $(n-1)$-th coefficient and replace the remainder with a real number z. This can be defined tail-recursively as follows:

```
fun conv' :: cfrac ⇒ nat ⇒ real ⇒ real where
  conv' c 0 z = z
  conv' c (Suc n) = conv' c n (of_int (cfrac_nth c n) + 1 / z)
```

It is straightforward to prove that `conv c n = conv' c n (cfrac_nth c n)`.

A key lemma that can be proven by a straightforward induction expresses the generalised convergent `conv'` in terms of the continuants:

```
theorem conv'_num_denom:
  assumes z > 0
  shows   conv' c (n+1) z =
            (z * h (n+1) + h n) / (z * k (n+1) + k n)
```

[2] The reader may wonder why `conv` was defined to return a `real` rather than a `rat`. There is no good reason for this, but the `rat` type is not used much in Isabelle/HOL, and if one wants access to the numerator and denominator one can simply use the continuants. Still, this is a candidate for possible refactoring in the future.

Here, we write `h n` and `k n` for `conv_num c n` and `conv_denom c n`. A direct consequence of this is that `conv c n = h n / k n`, i.e. the convergent really is the quotient of the continuants.

By simple induction arguments, the monotonicity and growth properties of the continuants h_n and k_n can be established:

- k_n is nondecreasing and $k_n \geq F_{n+1}$ (where F_n is the n-th Fibonacci number).
- If $a_0 \geq 0$ then h_n is also nondecreasing and $h_n \geq F_n$.
- Under mild conditions these can be strengthened to *strictly increasing*.

Since the Fibonacci numbers grow at an exponential rate of $\left(\frac{1}{2}(1+\sqrt{5})\right)^n$, so do h_n and k_n.

Another remarkable result obtained by a fully automatic induction is the following Bézout-like identity for the continuants:

```
lemma conv_num_denom_prod_diff:
  "k n * h (Suc n) - k (Suc n) * h n = (-1) ^ n"
```

This simple result has far-reaching consequences: for one, it shows us that h_n and k_n are coprime, so not only is $c_n = h_n/k_n$, but h_n and k_n are in fact the numerator and denominator of c_n. Next, it also implies that

$$c_{n+1} - c_n = \frac{(-1)^n}{k_n k_{n+1}} \ ,$$

and by summing over this we obtain:

$$c_n = c_m + \sum_{i=m}^{n-1} \frac{(-1)^i}{k_i k_{i+1}}$$

The summand on the right-hand side is decreasing and alternates signs, so we can let $n \to \infty$ and find that c_n converges to a limit. By using the standard bounds for alternating decreasing sums, we can also estimate the remainder:

$$\frac{1}{k_m(k_m + k_{m+1})} \leq \left|c_m - \lim_{n\to\infty} c_n\right| \leq \frac{1}{k_m k_{m+1}}$$

Of course, this only makes sense if the continued fraction has infinite length. In that case, we define the number x that c_n converges to as its *limit* (`cfrac_lim` in Isabelle). Otherwise, for finite length l, we define the limit x to be the last convergent x_l. It is also easy to establish that all the even-index convergents are $\leq x$ and all the odd-index ones are $\geq x$. Thus, the convergents alternatingly give successively better lower and upper bounds for x.

`cfrac_lim` satisfies a number of obvious laws, e.g.

```
lemma cfrac_lim_reduce:
  assumes cfrac_length c > 0
  shows cfrac_lim c = cfrac_nth c 0 + 1 / cfrac_lim (cfrac_tl c)
```

More generally, letting `cfrac_remainder` c n = `cfrac_lim` (`cfrac_drop` n c), we obtain:

```
lemma conv'_cfrac_remainder:
  assumes n ≤ cfrac_length c
  shows   conv' c n (cfrac_remainder c n) = cfrac_lim c
```

We now know how to attach a real number to a continued fraction. To go in the other direction, we observe the following:

- If x is an integer, then the continued fraction $[x;]$ of length 0 is its obvious representation.
- Otherwise, we can set $a_0 := \lfloor x \rfloor$ and $y := 1/\operatorname{frac}(x)$ (where $\operatorname{frac}(x) = x - \lfloor x \rfloor$ is the fractional part of x) and continue corecursively with the expansion of y.

Corresponding operations `cfrac_of_int` and `cfrac_of_real` are defined in Isabelle. The latter is defined via corecursion.

For rational x, this process terminates after finitely many steps, giving us a finite continued fraction whose last convergent is x. For irrational x, the process clearly does not terminate and we get an infinite continued fraction whose convergents converge to some limit. With a straightforward induction, one can show that the convergents are alternatingly above and below x, so that the limit must be x.

3.1 Uniqueness of the Representation

Clearly, every continued fraction corresponds to exactly one real number, namely its limit. The next question is now whether this is a one-to-one relationship, i.e. whether the representation of a real number as a continued fraction is unique. For decimal expansions, this is not the case, since e.g. $0.\overline{9} = 1.\overline{0}$. It turns out that it is also not the case for continued fractions: while $[n;]$ is a valid continued fraction expansion of an integer n (we call this the *canonical* representation), so is $[n-1;1]$. For the same reason, every number $x \in \mathbb{Q} \setminus \mathbb{Z}$ also has a canonical representation ending in $\ldots, a_l]$ with $a_l \geq 2$ and a non-canonical one ending in $\ldots, a_l - 1, 1]$.

However, this turns out to be the only way in which the representation fails to be unique, i.e. every rational number has two representations and every irrational number has exactly one: Consider any continued fraction $c = [a_0; a_1, a_2, a_3, \ldots]$ whose convergents converge to x. Then:

- First, we note that $a_0 \leq x \leq x_1 = a_0 + \frac{1}{a_1} \leq a_0 + 1$. Therefore we must either have $a_0 = \lfloor x \rfloor$ or $a_0 = \lfloor x \rfloor - 1$, and if $x \notin \mathbb{Z}$ then only the first option is possible.
- Moreover, in the "non-canonical" case $a_0 = \lfloor x \rfloor - 1$, the tail of the continued fraction is 1, which then has the unique representation $[1;]$ so that x must be an integer and the entire continued fraction is of the form $[x-1;1]$

– By induction, it follows that if x is irrational then c agrees with the canonical continued fraction for x, and if x is rational then it agrees with either the canonical or the non-canonical one.

Having dealt with this uniqueness issue, we now go on to look at the question of how good an approximation continued fractions provide.

3.2 Best Approximations

We have seen that the convergents give increasingly better upper and lower bounds. One very useful aspect of continued fractions is that these are not only good approximations, but the *best possible approximations*. To be precise, given a continued fraction of length l for any $n \leq l$, the convergent $x_n = h_n/k_n$ is the best rational approximation with denominator strictly less than k_{n+1}:

```
lemma conv_best_approximation_ex_weak:
  fixes a b :: int
  assumes n ≤ cfrac_length c
  assumes 0 < b and b < k (Suc n) and coprime a b
  shows   |k n * cfrac_lim c - h n| ≤ |b * cfrac_lim c - a|
```

Note that `a` and `b` are variables of type `int`. Isabelle automatically inserts a coercion `of_int :: int ⇒ real` as needed.

Unlike all the previous proofs, this one is a rather messy 120-line case distinction.[3] A slightly weaker version that shows the "best approximation" property more clearly is the following:

```
theorem conv_best_approximation:
  assumes n ≤ cfrac_length c
  assumes 0 < b and b < k n and coprime a b
  shows   |cfrac_lim c - conv c n| ≤ |cfrac_lim c - a / b|
```

Perhaps somewhat surprisingly, the converse also holds in a sense: if a/b is a sufficiently good rational approximation of x, then a/b is a convergent of any continued fraction for x:

```
lemma frac_is_convergentI:
  assumes b > 0 and coprime a b
  assumes |cfrac_lim c - a / b| < 1 / (2 * b^2)
  shows   ∃n. enat n ≤ cfrac_length c ∧ (a, b) = (h n, k n)
```

The proof is again a rather messy 200-line case distinction; the rough idea is to find an r such that $k_r \leq b < k_{r+1}$, use the fact that h_n/k_n is a best approximation for x, and then derive a contradiction.

[3] A stronger version of this was also formalised, which shows that with some small additional assumptions, h_n/k_n is in fact *strictly* better than all other rational approximations of the same order. However, the proof is even messier than this one, so I will omit it.

4 Continued Fractions for Specific Numbers

In this section, we will look at some special cases for which the continued fraction expansion has a simple closed form or can be determined easily. We begin by showing how existing tools in Isabelle can be used to compute continued fractions up to some point for a wide range of numbers.

4.1 Computation via Interval Arithmetic

Isabelle's approximation package [6] allows computing bounding intervals for real-valued functions and constants constructed from a number of operations, including basic arithmetic, square roots, logarithms, exponentials, π, and trigonometric functions. One can read off the initial fragment of the continued fraction expansion of a real number x from such an interval bound in the following fashion: if we know that $x \in [l, u]$ and $\lfloor l \rfloor = \lfloor u \rfloor =: a$, it follows that also $\lfloor x \rfloor = a$, and this gives us the first coefficient. Moreover, $[l - a, u - a]$ is then also a bounding interval for $\text{frac}(x)$, and if $l \neq a$ we then also have $\frac{1}{\text{frac}(x)} \in [\frac{1}{u-a}, \frac{1}{l-a}]$ and can continue the process.

This is easy to prove and results in a function `cfrac_from_approx` l u, which given rational upper and lower bounds l and u (represented as pairs of numerator and denominator) returns a list $(a_0, \ldots, a_{n-1})$ such that the canonical continued fraction expansion of every real number $x \in [l, u]$ has i-th coefficient a_i for any $i < n$. Combining this with the approximation framework, we get a fully verified executable function for computing the first few coefficients of the continued fraction expansion of a real number, as long as it is definable in the expression language provided by the approximation package. The precision used by the approximation package has to be chosen upfront and there is no a-priori guarantee of how many coefficients will be able to be found given a particular precision.

As a demonstration, I used this to compute expansions for π, $\ln 2$, e, $\sqrt{129}$, $\frac{123}{97}$ and a few more numbers. The output for Euler's number e is as follows:

$$[2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, 1, 16, 1, 1, 18, 1, 1, 20, 1, 1]$$

This suggests a pattern, which we will confirm in the next section.

4.2 Euler's Number

The result from the previous section suggests that the continued fraction for e has coefficients a_n with $a_{3n+1} = a_{3n+3} = 1$ and $a_{3n+2} = 2(n+1)$. To prove this, I follow the very elegant proof from ProofWiki [14]. It is based on establishing recurrences for the continuants of the continued fraction defined by the aforementioned a_n, solving these recurrences in terms of three families of integrals A_n, B_n, C_n, and then determining the limit as $n \to \infty$. Since the proof is very elegant and easy to understand (only about 350 lines in Isabelle), I will sketch it here.

Let h_n and k_n denote the continuants resulting from our above choice of a_n. Then define $p_0 = p_1 = 1$ and $p_{n+2} = h_n$ and $q_0 = 1$, $q_1 = 0$, $q_{n+2} = k_n$ and:

$$a_n = \begin{cases} \frac{2}{3}(n+1) & \text{if } n = 2 \pmod 3 \\ 1 & \text{otherwise} \end{cases}$$

Observe that p and q are solutions of the recurrence $f_n = a_{n-2}f_{n-1} + f_{n-2}$.

Moreover, define the following families of integrals:

$$A_n = \int_0^1 \frac{e^x x^n (x-1)^n}{n!}\,\mathrm{d}x \qquad B_n = \int_0^1 \frac{e^x x^{n+1} (x-1)^n}{n!}\,\mathrm{d}x$$

$$C_n = \int_0^1 \frac{e^x x^n (x-1)^{n+1}}{n!}\,\mathrm{d}x$$

It is easy to see that $A_0 = e-1$, $B_0 = 1$, and $C_0 = 2-e$ (using the Fundamental Theorem of Calculus). Next, we establish the recurrences $A_{n+1} = -(B_n + C_n)$ and $B_{n+1} = C_n - 2(n+1)A_{n+1}$ and $C_n = B_n - A_n$ by simply combining the integrals and (in the first two cases) applying the Fundamental Theorem of Calculus again. A simple induction then shows that:

$$A_n = -(p_{3n} - q_{3n}e) \qquad B_n = p_{3n+1} - q_{3n+1}e \qquad C_n = p_{3n+2} - q_{3n+2}e$$

Using standard "maximum times length" bounds, one sees that $|A_n| \leq e/n!$ and analogously for B_n and C_n. This implies that $|q_n e - p_n| \leq e/(\lfloor n/3 \rfloor !)^3$ and therefore $|p_n/q_n - e| \longrightarrow 0$ and thus $|h_n/k_n - e| \longrightarrow 0$, i.e. $h_n/k_n \longrightarrow e$.

An interesting consequence of this (as we will see in the next section) is that e is neither rational nor a quadratic irrational. Much stronger results are of course known, namely that e is transcendental, and the basic techniques for deriving these are at least superficially similar.

4.3 Periodic Continued Fractions

One interesting fact about decimal expansions is that the numbers that have a periodic decimal expansion are precisely the rational numbers. In contrast, the numbers that have a periodic continued fraction expansion are precisely the *quadratic irrationals*, i.e. numbers that are irrational and the solution of a quadratic equation with integer coefficients (not all zero). Algebraically, these are the algebraic numbers with a minimal polynomial of degree 2. They can be written as a *surd* of the form $\frac{\sqrt{a}+b}{c}$ for integers a, b, c. The set of quadratic irrationals is clearly closed under negation, reciprocal, and addition of integers. A first important consequence of this is that the limit of a continued fraction c is a quadratic irrational iff the one obtained by dropping the first n coefficients of c is a quadratic irrational (for any n).

We now define a continued fraction to be periodic if it is infinite and there exists a period $l > 0$ and an N such that its coefficients satisfy $a_{i+l} = a_i$ for all $i \geq N$. We say that it is *purely periodic* if one can choose $N = 0$.

Let us now first prove that any periodic continued fraction c converges to a quadratic irrational x. The *irrational* part is clear, since infinite continued fractions always converge to irrational numbers. Next, we note that we can w.l.o.g. assume that c is purely periodic, since we can otherwise simply drop the first N coefficients. We then note that `cfrac_remainder` l $c = c$, and combining this with `conv'_cfrac_remainder` and `conv'_num_denom` we obtain the following identity:

$$x = \texttt{conv'}\ l\ x = \frac{h_{l-1}x - h_{l-2}}{k_{l-1}x + k_{l-2}}$$

After cross-multiplying and gathering terms, we can clearly see that x satisfies a quadratic equation. The proof is fairly short in Isabelle, at about 50 lines.

The proof for the other direction is a bit more dense and takes about 250 lines, so I will only sketch the basic idea here. Suppose we have an infinite continued fraction c converging to a limit x with $Ax^2+Bx+C = 0$ for integers A, B, C not all zero. Let X_i denote the limit of the continued fraction obtained by dropping the first i coefficients of c. Define

$$\begin{aligned}
A_n &= Ah_{n-1}^2 + Bh_{n-1}k_{n-1} + Ck_{n-1}^2 \\
B_n &= 2Ah_{n-1}h_{n-2} + B(h_{n-1}k_{n-2} + h_{n-2}k_{n-1}) + 2Ck_{n-1}k_{n-2} \\
C_n &= Ah_{n-2}^2 + Bh_{n-2}k_{n-2} + Ck_{n-2}^2
\end{aligned}$$

Then X_n is a solution of $A_nX^2 + B_nX + C_n = 0$ for any n. One can also show that A_n, B_n, and C_n are bounded, so that by the pigeonhole principle, there has to be a particular triple (A', B', C') that occurs for infinitely many n. For each of these n, we know that X_n is a root of $A'X^2 + B'X + C' = 0$. Since this is a quadratic equation that has at most 2 roots, there have to be m, l with $l > 0$ and $X_m = X_{m+l}$. Since the coefficients a_j with $j \geq m$ are completely determined by X_m, this shows that $a_j = a_{j+l}$ for any $j \geq m$.

An obvious corollary from this is that for any quadratic irrational, the range of coefficients $\{a_i \mid i \geq 0\}$ is finite. Since we showed that the continued fraction for e contains all positive even integers, this immediately tells us that e is not a quadratic irrational.

4.4 Square Roots of Natural Numbers

We already know that any number of the form $\frac{\sqrt{a}+b}{c}$ for integers a, b, c with $a \geq 0$ has a periodic continued fraction expansion. In this section, we want to make this a bit more explicit for the case of $\sqrt{D}$ where D is a positive integer that is not a perfect square. We will prove a bound for the length of the period and analyse the structure of the period. This then also allows us to give an executable algorithm to compute the period and thereby a closed form for the continued fraction. The proofs for all of this are fairly technical, so I will only sketch the basic ideas.

In this case, the continued fraction expansion of $\sqrt{D}$ clearly starts with $D' = \lfloor\sqrt{D}\rfloor$ and the tail of this continued fraction is purely periodic, i.e. it is formed by infinitely many repetitions of some list $[a_1, \ldots, a_l]$ with $l \geq 1$.

We will now analyse this in some more detail and show the following things:

- $l \leq D'(D'+1)$
- $a_l = 2D'$ and $a_i \leq D'$ for all $i < l$.
- The list $[a_1, \ldots, a_{l-1}]$ is a palindrome, i.e. $a_i = a_{l-i}$ for all $1 \leq i < l$.

It remains to show how to compute l and the list $[a_1, \ldots, a_l]$. To this end, we will first introduce a suitable data structure: Let us call a number of the form $\frac{\sqrt{D}+p}{q}$ for $p, q \in \mathbb{Z}$ a *reduced quadratic surd associated to* D if the following conditions hold:

$$q > 0 \qquad q \mid (D - p^2) \qquad \frac{\sqrt{D}+p}{q} > 1 \qquad \frac{-\sqrt{D}+p}{q} \in (-1, 0)$$

The initial value we are interested in, after having dealt with the first coefficient $a_0 = D'$, is $1/(\sqrt{D} - D')$. To convert this into a reduced surd associated to D, we note that $1/(\sqrt{D} - D') = (\sqrt{D} + D')/(D - D'^2)$.

Next, given such a surd $x = (\sqrt{D} + p)/q$, we would like to find $\lfloor x \rfloor$ and $1/\operatorname{frac}(x)$. With some arithmetic, one can find that $X = \lfloor (p + D')/q \rfloor$ gives us $\lfloor x \rfloor$, and $1/\operatorname{frac}(x) = (\sqrt{D} + p')/q'$ with $p' = Xq - p$ and $q' = (D - p'^2)/q$.

Thus we have a way to iterate through the coefficients a_i of $\sqrt{D}$ using only integer arithmetic, and to find the period we only have to iterate this until we find the number $2D'$, which we know to be the last number in the period. We also know that we will find the end after at most $D'(D'+1)$ steps.

With this, we can now efficiently compute the closed form of the continued fraction expansion of $\sqrt{D}$, and thereby also arbitrarily high coefficients and convergents. For example, for $\sqrt{129}$, we compute the triple

$$(10, 11, [2, 1, 3, 1, 6, 1, 3, 1, 2, 22]) \ ,$$

meaning that $\sqrt{129} = [11; \overline{2, 1, 3, 1, 6, 1, 3, 1, 2, 22}]$ with period length 10.

5 Application

We will now look at one important application of continued fractions, namely solving Pell's equation. We will then apply this in turn to a particularly massive instance of Pell's equation, namely Archimedes' Cattle Problem.

5.1 Solving Pell's Equation

For a positive integer D that is not a perfect square, Pell's equation is the diophantine equation given by:

$$x^2 = 1 + D\,y^2$$

The work described here builds on the Isabelle/HOL library for Pell's Equation by Eberl in the Archive of Formal Proofs [2].

The pairs $(x, y) = (\pm 1, 0)$ are trivial solutions to the equation. Furthermore, there is a symmetry w.r.t. $\pm x$ and $\pm y$, so it is mostly the positive solutions that are of interest.

By simple arithmetic, one can show that if (x_1, y_1) and (x_2, y_2) are solutions, then $(x_1, y_1) \otimes (x_2, y_2) = (x_1 x_2 + y_1 y_2 D, x_1 y_2 + y_1 x_2)$ is also a solution. Noting also that $(x, y) \otimes (x, -y) = (1, 0)$, this means that the solutions form a group G_D w.r.t. $\otimes$ and the neutral element $(1, 0)$. The structure of this group can be demystified somewhat by noting that $(x, y) \mapsto x + \sqrt{D}y$ is an injective homomorphism from G_D to the multiplicative group of the ring $\mathbb{Z}[\sqrt{D}]$. More precisely, G_D is isomorphic to the subgroup of those $z \in \mathbb{Z}[\sqrt{D}]$ with $N(z) = 1$, where N is the norm operator $N(x + y\sqrt{D}) = (x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2$.

A standard result in the theory of Pell's equation is that it has an infinite number of solutions. Let (x_0, y_0) be the smallest non-trivial positive solution and call this the *fundamental solution*. It can be shown that the fundamental solution generates the set of positive solutions, i.e. every solution with positive x, y can be obtained as an n-th power of the fundamental solution (in the sense of the group operation $\otimes$).

The relevance to continued fractions is now that there is a very close relationship between the solutions of Pell's equation with parameter D and the convergents of $\sqrt{D}$: for any solution (x, y) of Pell's equation, we have $\frac{x}{y} \approx \sqrt{D}$. In fact, the approximation is so good that $\frac{x}{y}$ must be a convergent of $\sqrt{D}$.

This can be made more precise: if l is the length of the period of the continued fraction of $\sqrt{D}$, then the non-trivial positive solutions of the Pell equation are precisely the n-th continuants of $\sqrt{D}$ where n is odd and $n + 1$ a multiple of l. In particular, the fundamental solution is equal to c_{l-1} if l is even and to c_{2l-1} if l is odd. This means that we can solve Pell's equation fairly efficiently by simply computing the period of the continued fraction expansion of $\sqrt{D}$. This is considerably better than the best previously formalised approach, namely brute-forcing through increasing values of y and checking whether $1 + Dy^2$ is a perfect square.

An additional optimisation was also formalised: Let us focus on the case where D is not squarefree, i.e. where there is an $a > 1$ such that a^2 divides D. In this case, the map $(x, y) \mapsto (x, ay)$ gives a one-to-one correspondence between the solutions of $x^2 = 1 + Dy^2$ and the solutions of $x^2 = 1 + (D/a^2)y^2$ where $a \mid y$. Thus we can find the fundamental solution for $x^2 = 1 + Dy^2$ by going through the non-trivial solutions of $x^2 = 1 + (D/a^2)y^2$, picking the first one that satisfies $a \mid y$, and dividing its second component by a. This optimisation, which is implemented in the file `Pell_Lifting`, significantly decreases the computational effort when applicable.

A consequence of this connection between Pell's equation and the convergents of $\sqrt{D}$ is that while convergents of $\sqrt{D}$ can be used to find the fundamental solution for Pell's equation, once one has found it, the relationship can also be

used in reverse: by squaring the fundamental solution, one can quickly compute very large convergents of $\sqrt{D}$ and thereby best rational approximations to $\sqrt{D}$ (this is essentially equivalent to Newton's method applied to the rational number corresponding to the fundamental solution as a starting point).

5.2 Archimedes' Cattle Problem

In the 3rd century BC, Archimedes challenged the mathematicians of the time with a puzzle: The sun god Helios has four herds of cattle in four different colours: white, black, dappled, and yellow. The white herd consists of W bulls and w cows, the black one of B bulls and b cows, and so on. The solution where all the herds have size 0 is technically a solution, but since Archimedes talks about how large the herds are in his prose, we additionally exclude this trivial solution.

He then gives three linear identities on the number of bulls, which in modern notation are:

$$W = \tfrac{5}{6}B + Y \qquad B = \tfrac{9}{20}D + Y \qquad D = \tfrac{13}{42}W + Y$$

He then gives four additional linear identities that give the number of cows of each colour in terms of the total size of another herd:

$$w = \tfrac{7}{12}(B + b) \qquad b = \tfrac{9}{20}(D + d) \qquad d = \tfrac{11}{30}(Y + y) \qquad y = \tfrac{13}{42}(W + w)$$

Solving this system of equations, we obtain

$$\begin{aligned} 297\,W &= 742\,Y & 1{,}383{,}129\,w &= 2{,}402{,}120\,Y \\ 99\,B &= 178\,Y & 461{,}043\,b &= 543{,}694\,Y \\ 891\,D &= 1{,}580\,Y & 125{,}739\,d &= 106{,}540\,Y \\ & & 461{,}043\,y &= 604{,}357\,Y \end{aligned}$$

We conclude that $\operatorname{lcm}(297; 99; 891; 1{,}383{,}129; 125{,}739; 461{,}043) = 4{,}149{,}387$ divides Y, so we write $Y = 4{,}149{,}387\,x$.

Archimedes then additionally says that $W + B$ is a square. Plugging in the solutions we found above, we find that $W + B = 2^2 \cdot 3 \cdot 11 \cdot 29 \cdot 4657 \cdot x$. Since this is required to be a square, we can write $x = 3 \cdot 11 \cdot 29 \cdot 4{,}657 \cdot y^2$ for some y.

Lastly, Archimedes adds the condition that $D + Y$ is a triangle number (i.e. $D + Y = \frac{1}{2}z(z + 1)$ for some z). We define $v = 2z + 1$ and note that:

$$v^2 = 1 + 8(D + Y) = 1 + 410{,}286{,}423{,}278{,}424\,u^2 \tag{2}$$

This means that (v, u) is a solution to Pell's equation with the rather large parameter 410,286,423,278,424, i.e. in particular there must be some $k > 0$ such that (v, u) is the k-th power of the fundamental solution. To summarise, we have:

$$\begin{aligned} W &= 46{,}200{,}808{,}287{,}018\,u^2 & w &= 32{,}116{,}937{,}723{,}640\,u^2 \\ B &= 33{,}249{,}638{,}308{,}986\,u^2 & b &= 21{,}807{,}969{,}217{,}254\,u^2 \\ D &= 32{,}793{,}026{,}546{,}940\,u^2 & d &= 15{,}669{,}127{,}269{,}180\,u^2 \\ Y &= 18{,}492{,}776{,}362{,}863\,u^2 & y &= 24{,}241{,}207{,}098{,}537\,u^2 \end{aligned} \tag{3}$$

It also follows from this that the total combined size of all the herds (which is what Archimedes asked for) is

$$224{,}571{,}490{,}814{,}418\,u^2 \tag{4}$$

In the other direction, we can also see that any nontrivial solution to the Pell equation gives rise to a solution to the cattle problem by taking the identities in (2) as definitions of W, B, etc. in terms of u:

- The seven linear identities are automatically satisfied for any u.
- $W + B = (8{,}913{,}498\,u)^2$, so $W + B$ is automatically a square.
- Since (v, u) is a solution of (2), clearly v must be odd and we can write $v = 2z + 1$. We have $v^2 = 1 + 8(D + Y)$ from (2). Plugging in $v = 2z + 1$ and dividing by 8, we obtain $D + Y = \frac{1}{2}z(z + 1)$, so $D + Y$ is a triangular number as well.

In summary, we know that the nontrivial solutions to the cattle problem are in one-to-one correspondence with the nontrivial solutions to the Pell equation. This also means that the smallest nontrivial solution to the cattle problem corresponds to the fundamental solution of the Pell equation.

The Isabelle formalisation of all of this is fairly straightforward, using Isabelle's automation for linear arithmetic and the `HOL-Computational_Algebra` and `HOL-Number_Theory` libraries from the Isabelle distribution. Additional automation to e.g. prove that a specific numeric constant is a square or squarefree or to quickly prove coprimality, evaluate GCDs/LCMs would have been helpful. A prototype of such automation in the form of specialised *simplification procedures* was recently developed by Pescoller and Eberl [13] but has not yet been added to the distribution or the Archive of Formal Proofs. In any case, the Isabelle formalisation is less than 300 lines long, including definitions and a few auxiliary lemmas on algebra.

We can now use our method for solving Pell's equation to find the smallest nontrivial solution to the puzzle. We note that the parameter 410,286,423,278,424 is not squarefree since it contains the factor $9{,}314^2$, so we can apply the optimisation mentioned in Section 5.1 and reduce the problem to a Pell equation with the significantly smaller parameter 4,729,494. The period of the continued fraction expansion of $\sqrt{4{,}729{,}494}$ turns out to be 92, so the 91^{th} continuants give us the fundamental solution (v', u') of the reduced Pell equation $v'^2 = 1 + 4{,}729{,}494\,u'^2$. After lifting this to a solution (v, u) of the original equation as described in Section 5.1, we can compute the total size of the herd via Eq. (4).

The final result is an integer $77602714064 \ldots 9455081800$ with 206,545 decimals. The computation, using the Standard ML code exported using Isabelle's code generator and running in the Isabelle Poly/ML runtime, took about 70 ms on a 2025 desktop PC with an AMD Ryzen 9950X CPU (single-threaded).

Historically, the approximate solution $7.76 \cdot 10^{206{,}544}$ was first computed in 1880 by Amthor [9]. The exact solution was only computed in 1965 by Williams et al. [16] in 8 hours using two IBM computers, and again by Nelson on a Cray 1 in 1981, taking a few minutes. Nelson also published the number in the *Journal of Recreational Mathematics* [11], filling 47 pages.

6 Related Work

It seems that surprisingly little has been formalised about continued fractions.

The earliest formalisations of continued fractions seem to be in Mizar. Li et al. [10] provide a definition of simple continued fractions and convergents and prove some basic properties. Watase [15] extends this and proves further properties, such as the Bézout-like identity $k_n h_{n+1} - k_{n+1} h_n = (-1)^n$ and Dirichlet's approximation theorem (which seems to be their main goal). Nothing seems to be published about this other than the Mizar code itself.

I was also able to find two formalisations in Rocq related to continued fractions: Niqui [12] studies binary representations of rational numbers using the Stern–Brocot tree, which has connections to the continued fraction representation of a rational number. Blot et al. [1] study the correctness of certain floating-point algorithms and, in the process of this, formalised a number of basic facts about continued fractions, including the Bézout-like identity for the continuants and the best rational approximation properties.

There is also some more recent work on continued fractions by Kappelmann [7] in Lean's Mathlib. He provides a definition of *general* continued fractions (not merely simple ones) but seems to focus mostly on defining things in a way that allows efficient computation of the convergents rather than proving theorems. The most noteworthy result proved is the Bézout-like identity for the continuants (only for simple continued fractions).

The work presented here goes into considerably more depth: it looks at continued fractions as an abstract "data structure" first and then links to concrete real numbers, with a detailed analysis of when this link is unique and in what way it fails to be unique for rational numbers. To my knowledge, none of the other contributions (periodic continued fractions and quadratic irrationals, the continued fraction for $\sqrt{n}$, the connection to Pell's equation, Archimedes' Cattle Problem) have been formalised before.

7 Conclusion

Continued fractions are a fascinating piece of mathematics that has received surprisingly little attention in proof assistants so far. The present work fills that gap by providing all the standard results for simple continued fractions, including computational aspects such as computing continued fractions via interval arithmetic and computing closed forms for the important special case of $\sqrt{n}$.

The connection to Pell's equation, an important class of diophantine equations, is also made. The practicality of this is demonstrated by solving Archimedes' famous cattle problem, which involves solving a very large instance of Pell's equation.

Acknowledgments. I would like to thank Daniel Fischer, a prolific answerer of questions on the Mathematics StackExchange, whose answers have often helped me. In this project in particular, his input on the continued fraction for $\sqrt{D}$ was very helpful [5].

References

1. Blot, A., Muller, J.M., Théry, L.: Formal correctness of comparison algorithms between binary64 and decimal64 floating-point numbers. In: Abate, A., Boldo, S. (eds.) Numerical Software Verification. pp. 25–37. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-63501-9_3
2. Eberl, M.: Pell's equation. Archive of Formal Proofs (June 2018), https://isa-afp.org/entries/Pell.html, Formal proof development
3. Eberl, M.: Continued fractions. Archive of Formal Proofs (March 2024), https://isa-afp.org/entries/Continued_Fractions.html, Formal proof development
4. Eberl, M.: An Isabelle/HOL formalisation of Archimedes' cattle problem. GitHub repository (2026), https://github.com/pruvisto/archimedes_cattle
5. Fischer, D.: Size of partial quotients in continued fraction expansion of $\sqrt{n}$. Mathematics Stack Exchange, https://math.stackexchange.com/q/2842816
6. Hölzl, J.: Proving inequalities over reals with computation in Isabelle/HOL. In: Proceedings of the ACM SIGSAM 2009 International Workshop on Programming Languages for Mechanized Mathematics Systems (PLMMS '09). pp. 38–45. ACM, Munich, Germany (2009)
7. Kappelmann, K.: Lean mathlib 4, `Algebra/ContinuedFractions` (2019)
8. Khinchin, A.Y.: Continued fractions. Dover Publications (1964)
9. Krumbiegel, B., Amthor, A.: Das Problema bovinum des Archimedes. Zeitschrift für Mathematik und Physik (Historisch-literarische Abtheilung) **25**, 121–136,153–171 (1880)
10. Li, B., Zhang, Y., Korniłowicz, A.: Simple continued fractions and their convergents. Formalized Mathematics **14**(3), 71–78 (2006). https://doi.org/10.2478/v10037-006-0009-9
11. Nelson, H.L.: A solution to Archimedes' Cattle Problem. Journal of Recreational Mathematics **13**(3), 162–176 (1980–1981), the first full computation of the 206,545-digit solution using a Cray-1 computer.
12. Niqui, M.: Exact arithmetic on the Stern–Brocot tree. Journal of Discrete Algorithms **5**(2), 356–379 (2007). https://doi.org/10.1016/j.jda.2005.03.007, 2004 Symposium on String Processing and Information Retrieval
13. Pescoller, A.: Arbitrary Base Numbers and Simprocs in Isabelle/HOL. Bachelor's thesis, Universität Innsbruck, Innsbruck, Austria (February 2026)
14. ProofWiki Contributors: Continued fraction expansion of Euler's number (2026), https://proofwiki.org/wiki/Continued_Fraction_Expansion_of_Euler%27s_Number
15. Watase, Y.: Introduction to diophantine approximation. Formalized Mathematics **23**(2), 101–106 (2015). https://doi.org/10.1515/forma-2015-0010
16. Williams, H.C., German, R.A., Zarnke, C.R.: Solution of the cattle problem of Archimedes. Mathematics of Computation **19**(92), 671–674 (1965). https://doi.org/10.2307/2003964