Essays on the arithmetic of quadratic fields

Bill Casselman
University of British Columbia
cass@math.ubc.ca

Continued fractions of quadratic irrationals

In this note I'll explain how to calculate the continued fraction of a quadratic irrational number. This will be used to find the units in the ring of integers in a real quadratic field and, as we shall see elsewhere, is related to the problem of computing the class numbers of orders in the field. My approach to the construction of units in a real quadratic field seems to be somewhat novel.

This is the third essay in a series on quadratic field extensions of $\mathbb{Q}$. The previous two are the essays 'Integer square roots' and 'Approximating irrational numbers . . . ' mentioned in the reference list, which I'll refer to as [ISQRT] and [CF].

Contents

1. Review of continued fractions

I begin by recalling the basic continued fraction algorithm, applied to an arbitrary irrational λ. Set $\lambda_0 = \lambda$, $\ell_0 = \lfloor \lambda \rfloor$. Thus

$$\lambda_0 = \ell_0 + \varepsilon$$

with $0 \le \varepsilon < 1$. Explicitly

$$\varepsilon = \lambda_0 - \ell_0 = \frac{1}{1/(\lambda_0 - \ell_0)} \,,$$

so we can write

$$\lambda_0 = \ell_0 + \frac{1}{\lambda_1}$$

if $\lambda_1 = 1/(\lambda - \ell_0)$. This gives us ℓ_1. Continue, step by step:

(1.1)
$$\lambda_n = \ell_n + \frac{1}{\lambda_{n+1}} \quad \text{with} \quad \ell_n = \lfloor \lambda_n \rfloor$$

so that

$$\lambda_{n+1} = \frac{1}{\lambda_n - \ell_n} > 1 \,.$$

The first step is a little different from the rest since ℓ_0 can be any integer, while $\ell_n \ge 1$ for $n \ge 1$. Since λ is irrational, the process will go on forever. At the n-th stage we get an expression for it as a finite fraction

(1.2)
$$\begin{aligned}\lambda &= \lambda_0 \\ &= \ell_0 + \cfrac{1}{\lambda_1} \\ &= \ell_0 + \cfrac{1}{\ell_1 + \cfrac{1}{\lambda_2}} \\ &= \ell_0 + \cfrac{1}{\ell_1 + \cfrac{1}{\ell_2 + \cfrac{1}{\lambda_3}}} \\ &\ldots\end{aligned}$$

Such fractions are conventionally written in more succinct fashion. For example, the last is written usually as

$$\lambda = \ell_0 + \frac{1}{\ell_1 +}\,\frac{1}{\ell_2 +}\,\frac{1}{\lambda_3}\,.$$

However, I'll write it as

$$\langle\!\langle\, \ell_0, \ell_1, \ell_2, \lambda_3 \rangle\!\rangle\,.$$

In the limit we have the converging 'continued fraction':

$$\lambda = \langle\!\langle\, \ell_0, \ell_1, \ell_2, \ldots \,\rangle\!\rangle\,.$$

As a consequence of (1.1)

(1.3)
$$\lambda = \frac{p_{n-1}\lambda_n + p_{n-2}}{q_{n-1}\lambda_n + q_{n-2}}$$

with coefficients computed inductively:

$$\begin{aligned}p_{-2} &= 0 \\ p_{-1} &= 1 \\ p_n &= p_{n-1}\ell_n + p_{n-2} \\ q_{-2} &= 1 \\ q_{-1} &= 0 \\ q_n &= q_{n-1}\ell_n + q_{n-2}\,.\end{aligned}$$

The ratios p_n/q_n approximate λ more and more closely as n grows. They are called the **convergents** in the expansion.

There is a simple formula for the error in the n-th approximation to λ:

$$\lambda - p_n/q_n = \frac{(-1)^n(\lambda_n - \ell_n)}{(q_{n-1}\lambda_n + q_{n-2})(q_{n-1}\ell_n + q_{n-2})}\,.$$

Since the determinant alternates sign with n, the approximation is alternately from above and from below.

2. A preliminary reduction

Starting with a quadratic irrational

$$\lambda = \frac{a\sqrt{D}+u}{v} .$$

we want to find a recipe for computing successive λ_n and ℓ_n in the continued fraction expansion of λ. We want to do this only in exact arithmetic, because computers handle floating point numbers with only limited precision that would inevitably cause serious problems.

From here on, I follow closely Chapter IV of [Davenport:1992].

The process will involve repeatedly finding $\lfloor \lambda \rfloor$ for λ in this form. To do this, the first step is to put the expression in the simpler form

$$\frac{\sqrt{D}+u}{v} ,$$

because this allows us to use a formula for $\lfloor \lambda \rfloor$ that depend in a simple way on explicit computation of $\lfloor \sqrt{D} \rfloor$ (see [ISQRT]). In the process to be described, λ_n will always be of this form.

So we start out by putting a inside the radical, replacing D by $a^2 D$.

GOOD FORM. The next step is to arrange the data so that v divides $D - u^2$. There is a simple way to do this, but I'll do it by introducing a useful relation with quadratic equations. The number λ is the root of some quadratic equation

$$ax^2 + bx + c = 0 .$$

Given λ, we see that

$$\begin{aligned} v\lambda &= \sqrt{D} + u \\ v\lambda - u &= \sqrt{D} \\ v^2\,\lambda^2 - 2uv\,\lambda + u^2 &= D \end{aligned}$$

so we may choose

$$\begin{aligned} a &= \quad v^2 \\ b &= -2uv \\ c &= \quad u^2 - D . \end{aligned}$$

But now, given a, b, and c we can construct an equivalent set of variables D, u, v. First we divide a, b, c by their common divisor. We now have

$$\lambda = \frac{-b + \sqrt{b^2 - 4ac}}{2a} .$$

leading to

$$\begin{aligned} D &= \quad b^2 - 4ac \\ u &= -b \\ v &= \quad 2a . \end{aligned}$$

If b is even, we can make these numbers a bit smaller:

$$\begin{aligned} D &= \quad (b/2)^2 - ac \\ u &= -b/2 \\ v &= \quad a . \end{aligned}$$

replacing b by $b/2$, D by $b^2 - ac$, $2a$ by a.

The point is that in either case we have arranged things so that v divides $D - u^2$. In the course of the algorithm to come, every λ_n will be expressed as $(\sqrt{D} + u)/v$ that always satisfies this condition.

MCELIECE'S LEMMA. The basic continued fraction computation will require a repeated application of:

2.1. Lemma. *If*

$$\lambda = \frac{\sqrt{D} + u}{v}$$

then

$$\lfloor \lambda \rfloor = \begin{cases} \left\lfloor \dfrac{\lfloor \sqrt{D} \rfloor + u}{v} \right\rfloor & \text{if } v > 0 \\[2ex] \left\lfloor \dfrac{\lfloor \sqrt{D} \rfloor + 1 + u}{v} \right\rfloor & \text{if } v < 0 \end{cases}$$

The second follows from the first and the basic equation

$$\lfloor -\lambda \rfloor = -\lfloor \lambda \rfloor - 1 \quad (\lambda \notin \mathbb{Z}, \lambda > 0)\,.$$

The first is not hard to prove, and it is also Exercise 35 in §1.2.4 of [Knuth:1968]. In the solution, Knuth points out that this is a special case of a useful result he attributes to Robert McEliece:

2.2. Lemma. *Suppose f to be a continuous and strictly monotonic function on the interval $I \subseteq \mathbb{R}$. The following are equivalent:*

(a) $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$ for all x in I;
(b) $\lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil$ for all x in I;
(c) $f(x)$ is an integer implies that x is an integer.

Proof. (a) implies (c): If $f(x)$ is an integer then $\lfloor f(x) \rfloor = f(x)$, which by assumption is $f(\lfloor x \rfloor)$. But since f is monotonic, $\lfloor x \rfloor = x$. Similarly (b) implies (c).

Suppose (c) to hold. If $\lfloor f(\lfloor x \rfloor) \rfloor < \lfloor f(x) \rfloor$, the by continuity there exists $\lfloor x \rfloor < y \leq x$ such that $f(y)$ is an integer. Then y must be an integer, a contradiction. ∎

3. The basic step

Suppose we are given $\lambda = (\sqrt{D} + u)/v$ such that v divides $D - u^2$. Set

$$\begin{aligned} u_0 &= u \\ v_0 &= v \\ \lambda_0 &= \lambda \end{aligned}$$

Write

$$\begin{aligned} \ell_0 &= \lfloor \lambda_0 \rfloor\,. \\ \lambda_0 &= \ell_0 + \frac{1}{\lambda_1} \\ \lambda_1 &= \frac{1}{\lambda_0 - \ell_0}\,. \end{aligned}$$

Since $0 < \lambda_0 - \ell_0 < 1$, $\lambda_1 > 1$. Continue inductively:

$$\begin{aligned} \ell_n &= \lfloor \lambda_n \rfloor \\ \lambda_n &= \ell_n + \frac{1}{\lambda_{n+1}} \\ \lambda_{n+1} &= \frac{1}{\lambda_n - \ell_n}\,. \end{aligned}$$

I shall prove by induction that

$$\lambda_n = \frac{\sqrt{D} + u_n}{v_n}$$

with v_n dividing $D - u_n^2$. With this assumption

$$\begin{aligned} \lambda_n - \ell_n &= \frac{\sqrt{D} + u_n}{v_n} - \ell_0 \\ &= \frac{\sqrt{D} + u_n - \ell_n v_n}{v_n} \\ &= \frac{\sqrt{D} - u_{n+1}}{v_n} \\ &\qquad \text{with } \ u_{n+1} = \ell_n v_n - u_n \\ &= \frac{D - u_{n+1}^2}{v_n(\sqrt{D} + u_{n+1})}\,. \end{aligned}$$

By assumption $D - u_n^2$ is divisible by v_n. So

$$D - u_{n+1}^2 = D - (u_n^2 - 2\ell_n v_n + \ell_n^2 v_n^2)$$

is divisible by v_n, and $v_{n+1} = (D - u_{n+1}^2)/v_n$ is an integer. Finally

$$\lambda_{n+1} = \frac{\sqrt{D} + u_{n+1}}{v_{n+1}}\,.$$

Since $v_n v_{n+1} = D - u_{n+1}^2$, the induction assumption remains valid.

One great virtue of this process is that we work with just the approximation $\lfloor \sqrt{D} \rfloor$ to the initial square root, and hence do not have to find integral square roots more than once. Another pleasant feature is that we don't have to carry out repeated long divisions in order to define the v_{n+1}:

3.1. Lemma. *For $n \ge 1$*

$$v_{n+1} = \ell_{n-1}(u_n - u_{n-1}) + v_{n-1}\,.$$

Proof. Because

$$\begin{aligned} v_{n-1} v_n &= D - u_{n-1}^2 \\ v_{n+1} v_n &= D - u_n^2 \\ (v_{n+1} - v_{n-1}) v_n &= u_n^2 - u_{n-1}^2 \\ &= (u_n + u_{n-1})(u_n - u_{n-1}) \\ &= \ell_n v_n (u_n - u_{n-1})\,. \end{aligned}$$

SUMMARY. I summarize the step from λ_n to λ_{n+1}.

$$\begin{aligned}
\ell_n &= \lfloor \lambda_n \rfloor \\
&= \left\lfloor \frac{\lfloor \sqrt{D} \rfloor + u_n}{v_n} \right\rfloor \\
u_{n+1} &= \ell_n v_n - u_n \\
v_{n+1} &= \frac{D - u_{n+1}^2}{v_n} \\
&= \ell_{n-1}(u_n - u_{n-1}) + v_{n-1} \quad (n \geq 1) \\
\lambda_{n+1} &= \frac{\sqrt{D} + u_{n+1}}{v_{n+1}} \, .
\end{aligned}$$

Remark. We shall see in a moment, in the example of $\sqrt{3}$, that even if λ is an algebraic integer, the continued fraction algorithm may produce values of λ_n that are not. This is harmless. Whether or not λ is an integer or not is unimportant.

4. Periodicity

When we run this algorithm on a few examples, something extraordinary appears. For example, if we apply it to $\lambda = \sqrt{3}$, we get:

$$\begin{aligned}
\ell_0 &= 1 \\
\lambda_1 &= \frac{1}{\sqrt{3} - 1} = \frac{-1 - \sqrt{3}}{-2} = \frac{1 + \sqrt{3}}{2} \\
\\
\ell_1 &= 1 \\
\lambda_2 &= \frac{1}{(1 + \sqrt{3})/2 - 1} = \frac{2}{-1 + \sqrt{3}} = 1 + \sqrt{3} \\
\\
\ell_2 &= 2 \\
\lambda_3 &= \frac{1}{(1 + \sqrt{3}) - 2} = \frac{1}{\sqrt{3} - 1} \\
&= \lambda_1 \, .
\end{aligned}$$

The calculation repeats from now on, so the values we get for ℓ_n are

$$1,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1,\ 2,\ 1 \ldots$$

In fact, as will be proved, this sort of thing happens for every quadratic irrational, and only those. This will take some time to explain. The first step is to characterize those real numbers with periodic continued fractions. It is apparent from the case looked at above, for example, that this is so for $\lambda = 1 + \sqrt{3} \sim 2.732$. Since $1 - \sqrt{3} \sim -0.732$ this illustrates:

4.1. Proposition. *The real number λ has a periodic continued fraction if and only if*

(a) it is a quadratic irrational
(b) $\lambda > 1$
(c) $-1 < \overline{\lambda} < 0$.

Here $\overline{\lambda}$ is the algebraic conjugate—the conjugate of $x + y\sqrt{N}$ is $x - y\sqrt{N}$. In these circumstances λ is said to be **reduced**.

It seems to have been Galois who first proved this, in his first paper, although predecessors must have known it.

Proof. **(a)** Suppose the continued fraction of λ to be periodic. According to Lemma 4.3, this implies that

$$\lambda = \frac{a\lambda + b}{c\lambda + d}$$

with suitable coefficients. But then λ is a root of the quadratic equation

$$cx^2 + x(d - a) - b = 0\,.$$

(b) In any continued fraction, $\ell_n > 1$ for $n \ge 1$. If the fraction has period n, then $\ell_0 = \ell_n > 1$ as well. So $\lambda > 1$.

(c) To show that $-1 < \overline{\lambda} < 0$, it suffices to show that $-1/\overline{\lambda} > 1$. Because of (b), there is a satisfying reason for this:

4.2. Lemma. *If the continued fraction of λ is periodic with period $[\ell_0, \ldots, \ell_{n-1}]$, the continued fraction of $-1/\overline{\lambda}$ is that with period $[\ell_{n-1}, \ldots, \ell_0]$.*

Proof. The equation (1.3) may be expressed as

$$\begin{bmatrix} \lambda \\ 1 \end{bmatrix} = C_n \begin{bmatrix} \lambda \\ 1 \end{bmatrix}$$

where

$$C_n = \begin{bmatrix} \ell_0 & 1 \\ 1 & 0 \end{bmatrix} \ldots \begin{bmatrix} \ell_{n-1} & 1 \\ 1 & 0 \end{bmatrix}.$$

But then the transpose of C_n is

$$\begin{bmatrix} \ell_{n-1} & 1 \\ 1 & 0 \end{bmatrix} \ldots \begin{bmatrix} \ell_0 & 1 \\ 1 & 0 \end{bmatrix}$$

with corresponding matrix

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}.$$

The number whose fraction has period $[\ell_{n-1}, \ldots, \ell_0]$ is therefore a root of

$$bx^2 + (d - a)x - c = 0\,.$$

But the roots of this are $-1/\lambda$ and $-1/\overline{\lambda}$. It cannot be $-1/\lambda$ which has the periodic expansion, since it is negative. So it must be $-1/\overline{\lambda}$.

This concludes the proof that (a)–(c) are necessary conditions.

It remains to prove the converse. Suppose λ to be a reduced quadratic irrational. *Why is the continued fraction of λ periodic?*

4.3. Lemma. *Suppose*

$$\lambda = \frac{\sqrt{D} + u}{v}\,.$$

Then λ is reduced if and only if

$$0 < u < \sqrt{D}, \quad \sqrt{D} - u < v < \sqrt{D} + u\,.$$

Proof. It is immediate that λ is reduced if the inequalities hold.

For the implication in the other direction, suppose λ to be reduced. We have

$$\overline{\lambda} = \frac{u - \sqrt{D}}{v} \,.$$

Since $\lambda > \overline{\lambda}$, we must have $v > 0$. Since $\lambda + \overline{\lambda} > 0$, we have also $u > 0$. Since $\lambda\overline{\lambda} < 0$, $u^2 - D < 0$. The rest is immediate. ∎

I claim that if $\lambda > 1$ and $-1 < \overline{\lambda} < 0$ then the same pair of inequalities hold for all λ_n in the course of the continued fraction computation. This will follow from two observations: (1) $\lambda > 1$ and only if $-1 < -1/\lambda < 0$; (2) if

$$\lambda = \ell + \frac{1}{\mu}$$

with $\lambda > 1$, $\mu > 1$ then $-1 < \overline{\lambda} < 0$ if and only if $-1 < \overline{\mu} < 0$, and in that case

$$\ell = \lfloor -1/\overline{\mu} \rfloor \,.$$

This is because $\lambda = \ell + 1/\mu$ if and only if

$$\frac{-1}{\overline{\mu}} = \ell + \frac{1}{-1/\overline{\lambda}} \,.$$

Now assume that $\lambda > 1$ and and $-1 < \overline{\lambda} < 0$. It follows from these observations that the same inequalities hold for all λ_n. But the inequalities in Lemma 4.3 imply that only a finite number of acceptable u_n, v_n arise in the computation. This implies that there must be eventual periodicity.

It reamins now to show full periodicity. Suppose $\lambda_m = \lambda_n$ for $m \ge 1$. I claim that then $\lambda_{m-1} = \lambda_{n-1}$ as well. We have

$$\lambda_{m-1} = \ell_{m-1} + \frac{1}{\lambda_m}, \quad \lambda_{n-1} = \ell_{n-1} + \frac{1}{\lambda_m} \,,$$

so that it suffices to show that $\ell_{m-1} = \ell_{n-1}$. This follows from observation (2) above. ∎

Remark. We have seen that the period of the expansion of $\mu = -1/\overline{\lambda}$ is the reverse of that of λ. Correspondingly, if

$$\lambda = \frac{a\lambda + b}{c\lambda + d}$$

then

$$\mu = \frac{a\mu + c}{b\mu + d} \,.$$

Finally:

4.4. Proposition. *Every quadratic irrational number has an eventually periodic continued fraction.*

Proof. Since $\lambda_n > 1$ for $n \ge 1$, Proposition 4.1 assures us that it suffices to show that $-1 < \overline{\lambda}_n < 0$ for $n \gg 0$.

we know that

$$\lambda = \frac{p_{n-1}\lambda_n + p_{n-2}}{q_{n-1}\lambda_n + q_{n-2}} \,.$$

Solving this for λ_n gives us However,

$$\overline{\lambda}_n = -\frac{q_{n-2}\overline{\lambda} - p_{n-2}}{q_{n-1}\overline{\lambda} - p_{n-1}} = -\frac{q_{n-2}}{q_{n-1}} \cdot \frac{\overline{\lambda} - (p_{n-2}/q_{n-2})}{\overline{\lambda} - (p_{n-1}/q_{n-1})}$$

for all n. What happens as $n \to \infty$? The coefficients here are all positive and grow indefinitely. The ratios p_{n-2}/q_{n-2} and p_{n-1}/q_{n-1} have limit λ as $n \to \infty$. Therefore λ_n is eventually negative. Furthermore, the ratios lie alternately on either side of λ, and $q_{n-1} > q_{n-2}$, so that eventually we come across some $\overline{\lambda}_n > -1$. From that point on, the expansion is periodic. ∎

5. Units

Suppose N square free, $F = \mathbb{Q}(\sqrt{N})$.

ORDERS. An element of F is an (algebraic) integer if it is a root of a monic polynomial

$$x^2 - bx + c = 0$$

with integral coefficients b, c. The integers in F form a ring $\mathfrak{o}_F$. Explicitly, this ring has $\mathbb{Z}$-basis 1 and

$$\omega_N = \begin{cases} \dfrac{1+\sqrt{N}}{2} & \text{if } N \equiv_4 1 \\ \sqrt{N} & \text{if } N \equiv_4 2 \text{ or } 3. \end{cases} .$$

The **discriminant** D_F of this ring is, respectively, N and $4N$.

An **order** $\mathfrak{o}$ in F is a subring of $\mathfrak{o}_F$ of finite index. According to the principal divisor theorem, the quotient $\mathfrak{o}_F/\mathfrak{o}$ will be cyclic, say of order f. Then $(1, f\omega_N)$ is a basis of $\mathfrak{o}$. Its discriminant is $f^2 D_F$. Every D congruent to either 0 or 1 modulo 4 is the discriminant of a unique order $\mathfrak{o}_D$ in $\mathbb{Q}(\sqrt{D})$.

It is convenient to deal with orders more uniformly. Each order is characterized by its discriminant D, and given a number D that is congruent either to 0 or 1 modulo 4, the element

$$\frac{D+\sqrt{D}}{2}$$

is part of a basis of $\mathfrak{o}_D$.

The ring $\mathfrak{o}_D$ contains a reduced element λ_D that serves as a basis element of $\mathfrak{o}_D$. Explicitly

$$\lambda_D = \frac{\delta + \sqrt{D}}{2}$$

in which δ is distinguished by the conditions

$$\delta \equiv_2 D, \quad \sqrt{D} - 2 < \delta < \sqrt{D}\,.$$

If $\delta = D + 2k$ then, if $d = \lfloor \sqrt{D} \rfloor$, the second condition becomes

$$\begin{aligned} \sqrt{D} - D < 2k &< \sqrt{D} - D \\ (d+1) - D - 2 \le 2k &\le d - D \\ d - D - 1 \le 2k &\le d - D \\ d - D - 2 < 2k &\le d - D \\ (d-D)/2 - 1 < k &\le (d-D)/2 \\ k &\le (d-D)/2 < k+1 \\ k &= \lfloor (d-D)/2 \rfloor\,. \end{aligned}$$

I define the **positive cone** in $\mathbb{R} \otimes F$ to be the closed real cone spanned by 1 and $\sqrt{D}$. Let $\mathfrak{o}_D^+$ be the set of integers in it. This region is a fundamental domain for the action of the group generated by sign change and conjugation.

Every element of $\mathfrak{o}_D$ has a unique expression

$$\lambda = m + n \cdot \frac{D + \sqrt{D}}{2}\,.$$

It can also be expressed uniquely as

$$\lambda = \begin{cases} m + n\sqrt{D} + \varepsilon \cdot \dfrac{\sqrt{D}}{2} & \text{if } D \equiv_4 0 \\[2ex] m + n\sqrt{D} + \varepsilon \cdot \dfrac{1+\sqrt{D}}{2} & \text{if } D \equiv_4 1. \end{cases} \tag{5.1}$$

In both of these, m and n are integers, and ε is 0 or 1. For elements of $\mathfrak{o}_D^+$, m and n are non-negative.

UNITS. A **unit** of $\mathfrak{o}_D$ is an element in $\mathfrak{o}_D$ whose inverse is also in $\mathfrak{o}_D$. These are also the elements of $\mathfrak{o}_D$ with norm 1. They form a group under multiplication. They are a discrete subset of $\mathfrak{o}_D \subset \mathbb{R} \otimes F$, contained in the hyperbolas $x^2 - y^2 D = \pm 1$. On general principles, then, they are either to the finite group $\{\pm 1\}$ or to the direct product of $\{\pm 1\}$ and an infinite cyclic group. We shall shortly construct explicit non-trivial unist, so it is the second possibility that occurs.

There is a good way to specify one particular generator. I'll put a linear order on $\mathfrak{o}_D^+$:

$$x_1 + y_1\sqrt{D} < x_2 + y_2\sqrt{D}$$

if and only if

$$y_1 < y_2 \quad \text{or } y_1 = y_2 \text{ and } x_1 < x_2 \,.$$

What I'll call the **positive basic unit** ε_D *is distinguished by requiring that it lie in* $\mathfrak{o}_D^+$ *and be least among all units in this region.* How to find it?

If $\lambda = x + y\sqrt{D}$ and $\mu = u + v\sqrt{D}$ then

$$\lambda\mu = (x + y\sqrt{D})(u + v\sqrt{D}) = (xu + vyD) + (yu + xv)\sqrt{D}\,,$$

so that if ε is a positive unit then $\varepsilon^n > \varepsilon$ for $n > 1$. The positive basic unit is the $x + y\sqrt{D}$ with the least value of y.

There is one special case worth noting. Sometimes the basic positive unit is easy to find.

5.2. Proposition. *The following are equivalent:*

(a) λ_D *is a unit;*
(b) $\lambda_D = \varepsilon_D$*;*
(c) $\delta^2 - D = -4$*;*
(d) the length of the period of the continued fraction of λ_D *is equal to* 1.

In this case the norm of ε_D is -1.

Proof. Left as exercise. ∎

REDUCED ELEMENTS AND UNITS. The main point of what is to come is a simple relationship between reduced elements of F and units. Suppose λ to be any reduced element of F. Its continued fraction expansion will be periodic. Suppose n to be the length of a period (which may be a sequence of shorter periods). Then

$$\lambda = \langle\!\langle \ell_0, \ldots, \ell_{n-1}, \ell_0, \ldots \rangle\!\rangle$$

and

$$\lambda = \frac{p_{n-1}\lambda + p_{n-2}}{q_{n-1}\lambda + q_{n-2}} = \text{ say } \frac{a\lambda + b}{c\lambda + d}\,.$$

Here the coefficients are those appearing in the continued fraction of λ.

Here a, b, c, d are positive integers satisfying $a > b > 0$, $c > d \geq 0$, and $ad - bc = \pm 1$. This gives us first of all

$$c\lambda^2 + (a - d)\lambda - b = 0$$

and then

$$(c\lambda)^2 - (a-d)(c\lambda) + cd = 0$$

which tells us that $c\lambda$ is an algebraic integer.

The basic fact is this:

5.3. Proposition. *In these circumstances $c\lambda + d$ is a unit of $\mathfrak{o}_D$.*

Proof. This can be seen by direct computation, but a slightly more enlightening way is to interpret multiplication by $c\lambda + d$ as a linear operator on F, given the basis $(\lambda, 1)$. Since

$$\begin{aligned}(c\lambda + d)\cdot\lambda &= a\lambda + b \\ (c\lambda + d)\cdot 1 &= c\lambda + d\,,\end{aligned}$$

its matrix is

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}.$$

But the norm of $c\lambda + d$ is the determinant of this matrix, which is $(-1)^n$.

In this way, every reduced λ produces a sequence of units in the endomorphism ring of the lattice spanned by 1 and λ, which is an order in F.

Actually, a given λ gives rise to an infinite sequence of units. For any matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

and real λ define

$$A(\lambda) = \frac{a\lambda + b}{c\lambda + d}\,.$$

Multiplication of matrices corresponds to composition of maps. If λ is a reduced element, $A(\lambda) = \lambda$ as above, and u is the associated unit, then $A^n(\lambda) = \lambda$ as well, and corresponds to u^n. These are all powers of one minimal unit, corresponding to the shortest period of λ.

5.4. Theorem. *The basic unit of $\mathfrak{o}_D$ is the unit constructed in this way if n is the length of the minimal period of λ_D.*

Proof. This will take several steps.

Step 1. I have taken the following, with minor modifications, from §83 of [Dirichlet:1863].

5.5. Lemma. *Suppose λ to be reduced and*

$$\lambda = \frac{a\lambda + b}{c\lambda + d}$$

with a, b, c, $d > 0$ and $|ad - bc| = 1$. Then $a > b > 0$ and $c > d > 0$.

Proof. The argument will depend on a simple fact. Multiplying the equation by $c\lambda + d$, we see that

$$P(\lambda) = c\lambda^2 - (a-d)\lambda - b = 0\,.$$

Since λ is reduced, $P(-1) > 0$ and $P(1) < 0$. This means that

$$(a) \qquad\qquad \begin{aligned} c + (a-d) - b &> 0 \\ c - (a-d) - b &< 0 \end{aligned}$$

hence

$$(b) \qquad\qquad -\,c + (a-d) + b > 0\,.$$

Adding (a) and (b) gives us **(i)** $a > d$.

Suppose $b \geq a$, say $b = a + x$ with $x \geq 0$. From the first inequality

$$c - d > b - a = x$$

so $c = d + y$ with $y > 0$. Then

$$\pm 1 = ad - bc = ad - (a + x)(d + y) = -ay - dx - xy\,.$$

If $x > 0$ the expression on the right is ≤ 3, a contradiction. If $x = 0$ then $-ay = \pm 1$. Since a, $y \geq 0$, $a = 1 = y$. Therefore $c = d + 1$. But then (b) says

$$c - (a - d) - b = (d + 1) - (1 - d) - 1 = 2d - 1 < 0\,,$$

which is again a contradiction. Hence **(ii)** $a > b$.

Since $\mu = -1/\overline{\lambda}$ is also reduced and

$$\mu = \frac{a\mu + c}{b\mu + d}\,,$$

we also deduce **(iii)** $a > c$. But the Euclidean algorithm tells us that if we find the continued fraction of a/c, then

$$aq_{n-1} - bp_{n-1} = \pm 1$$

with $0 < p_{n-1} < a$, $0 < q_{n-1} < b$, and that every other solution is of the form

$$(p_{n-1} + ka, q_{n-1} + kb)\,.$$

Our solution can be one of those only if $k = 0$, which means that **(iv)** $c > d$. ∎

Step 2.

5.6. Proposition. *If λ is reduced and*

$$\lambda = \frac{a\lambda + b}{c\lambda + d}$$

with $ad - bc = \pm 1$ and $a, b, c, d > 0$, then b/d and a/c are successive convergents in the continued fraction of λ.

Proof. The consequence of the Lemma together with Theorem 184 of [Hardy-Wright:1960] (also Proposition 7.1 of [CF]). ∎

Step 3.

I now return to the original question about units. I shall show that if u is any positive unit, then either (a) the matrix determined by u with respect to the basis $(1, \lambda_D)$ has positive entries or (b) it is the unit with a period of length 1 referred to in Proposition 5.2. Because of the previous result, this will conclude the proof of the Theorem.

Multiplication by any element of F is a linear tramnsformation of F. Let $\Delta = D - \delta^2 > 0$. With respect to the basis 1, λ_D it corresponds to a matrix. Since

$$\sqrt{D} = 2\lambda_D - \delta$$
$$\sqrt{D}\lambda_D = \delta\lambda_D + \Delta/2$$

the matrix corresponding to $x + y\sqrt{D}$ is

$$\begin{bmatrix} x + y\delta & 2y \\ y\Delta/2 & x - y\delta \end{bmatrix}$$

All the matrix entries are positive, except possibly that at lower right. I claim that that that one is at least non-negative. For this, it suffices to show that $x^2 - \delta^2 y^2 \ge 0$, since

$$x^2 - y^2\delta^2 = (x + y\delta)(x - y\delta)\,.$$

But if $x + y\sqrt{D}$ is unit, then

$$(x^2 - y^2\delta^2 = (x^2 - y^2 D) + y^2(D - \delta^2) = \pm 1 + y^2(D - \delta^2)\,.$$

But y lies in $\mathbb{Z}/2$ and $D \equiv_4 \delta^2$, so $y^2(D - \delta^2) = (2y)^2(D - \delta^2)/4 \ge 1$, and $x^2 - y^2\delta^2 \ge 0$. From here the claim is straightforward to verify

6. References

1. Bill Casselman, ‘Integer square roots’, preprint 2020. Available at
`http://www.math.ubc.ca/~cass/research/pdf/intsqrt.pdf`

2. ——, ‘Approximating irrational numbers by rational ones’, preprint 2020. Available at
`http://www.math.ubc.ca/~cass/research/pdf/cf.pdf`

3. Harold Davenport, **The higher arithmetic** Cambridge University Press, sixth edition, 1992.

4. Peter G. Lejeune-Dirichlet, **Vorlesungen über Zahlentheorie**, Braunschweig, 1863.

5. Évariste Galois, ‘Démonstration d’un théorème sur les fractions continues périodiques’, §II.1 in [Neumann:2011].

6. Donald E. Knuth, **Fundamental algorithms** (Volume 1 in the series *The art of computer programming*), Addison-Wesley, 1968/1973.

7. ——, **Seminumerical algorithms** (Volume 2 in the series *The art of computer programming*), Addison-Wesley, 1969/1981/1998.

8. Peter M. Neumann, **The mathematical writings of Évariste Galois**, European Mathematical Society, 2011.