Quadratics, continued fractions and divided cells

R. T. Bumby & M. E. Flahive
with contributions by J. L. Lagrange, K. F. Gauss, . . .

January 7, 2007

Quadratics

A subring of a number field K, finitely generated as a $\mathbb{Z}$ module, is called an **order** of K. If K has degree 2 over $\mathbb{Q}$, an order $\mathcal{O}$ has basis consisting of 1 and an element

$$\beta = \frac{a + \sqrt{D}}{2}$$

with $a \equiv D \pmod 2$ (we may take $a = 0$ or 1). The integer D is called the **discriminant** of $\mathcal{O}$. The **conjugate** of β is $a - \beta$. It is known that D is congruent to 0 or 1 mod 4 and **not a square**.

Ideals

An ideal for this order can be generated as a $\mathbb{Z}$ module by an ordinary integer N and an element of the form

$$c(b+\beta)$$

where $c \mid N$. The ideal determines b modulo N/c.

This requires proof.

Proof

Any nonzero ideal I contains some element $\xi \in \mathcal{O}$, $\xi \neq 0$. Multiplying by the conjugate of ξ gives a nonzero element of $\mathbb{Z} \cap \mathcal{O}$, and all such integers form an ideal in $\mathbb{Z}$. We take N to be a generator of this ideal. Now, consider the set of all q such that there is $p \in \mathbb{Z}$ with $p + q\beta \in I$. This is an ideal in $\mathbb{Z}$, and we let c be its generator. However, I is closed under multiplication by $\beta - a$ and the coefficient of β in $(\beta - a)\xi$ is the coefficient of 1 in ξ. Thus, c divides both coefficients. A similar argument shows that N divides c times the norm of $b + \beta$.

Ideal classes

Multiplying an ideal by an element of $\mathcal{O}$, or removing such a factor, leads to an equivalence relation on ideals with a finite number of equivalence classes according to a **fundamental theorem** of algebraic number theory (this is usually proved only for the full ring of integers, but it is valid for any order). For **quadratic** orders, **reduction** leads to a nice choice of representatives of the ideal classes.

Reduction of ideals, preliminaries

An $\mathcal{O}$ ideal I has a $\mathbb{Z}$ basis $\big(N, c(b+\beta)\big)$, but $c|N$, so there is an equivalent ideal of the same form with $c = 1$. Only ideals in this **standard form** will appear from here on. Since this is an ideal, the norm of $b + \beta$ divisible by N, and N will be the norm of the ideal. The other reduction steps will start by multiplying by something that introduces a rational factor. To return to standard form, we remove that factor.

Reduction of ideals, large norm

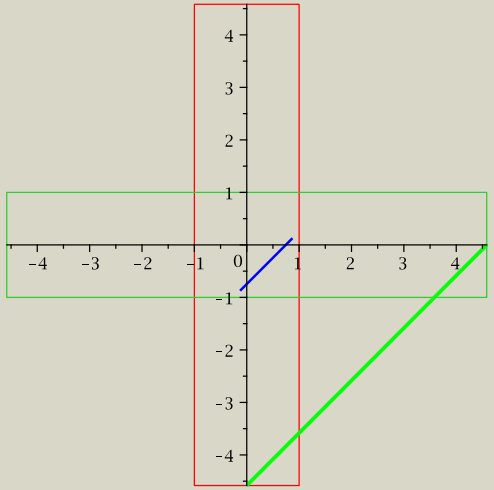
If $-N/2 < b \le N/2$, then

$$\beta(a-\beta) \le (b+\beta)(b+a-\beta) \le N^2/4 + aN/2$$

Thus, if $N > \sqrt{\beta(\beta-a)}$, $(b+\beta)(b+a-\beta) \in \mathbb{Z}$ is the product of N with a smaller integer, so multiplying by $(b+a-\beta)/N$ replaces I by an ideal of smaller norm. A similar reduction works for orders in imaginary quadratic fields, efficiently finding an essentially unique reduced ideal in a given ideal class. For the connection to continued fractions, we limit consideration to ideals with $N \le \sqrt{\beta(\beta-a)}$.

A picture

The dots show the points corresponding to 0, N, and $-N$ on axes that give the real completions of $\mathcal{O}$. The blue line contains the other generator in the large norm case; the green line contains the other generator in the small norm case.



Reduction of ideals, small norm

When $N \leq \sqrt{\beta(\beta - a)}$, b may be chosen to satisfy **either** $0 < b + \beta < N$ **or** $-N < b + a - \beta < 0$. It is possible to have a single choice of b satisfy both of these choices, and this will give a reduction of the ideal.

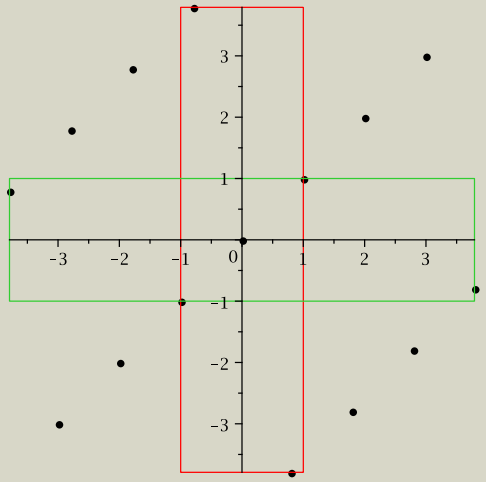
In the remaining cases, each of these choices will be considered **reduced**.

Connection with continued fractions

The bases that we call reduced have the property that the closed rectangle containing the basis has no point of I except the origin in its interior. This is exactly the defining property of consecutive minimal points in the continued fraction of the quadratic form given by applying the norm to elements of I. Furthermore, the partial quotient arising in the relation between three consecutive minimal points in just the distance between the elements $b + \beta$ in the two reduced bases of I. It is the fact that a reduced basis always has the form $(N, b + \beta)$ that forces the simple relation between reduced bases.

Seeing the connection

This figure shows the ideal generated by 1 and $\beta = (1 + \sqrt{21})/2$. Reduced bases for this lattice are $(1, 1 + \beta)$ and $(1, -2 + \beta)$.



Arithmetic continued fractions

One could also consider the **number**

$$\frac{b+\beta}{N}$$

The partial quotient is just the **integer part** of this number, as in the usual **arithmetic** continued fraction. However, this emphasizes only a forward sequence of partial quotients, but the **backward** extension of a purely period chain of partial quotients should not be treated differently from the forward extension.

A difference from continued fractions

In developing the continued fraction of a form, one related different bases of **the same** lattice. In the study of quadratics, it is the **discriminant**, or the element β that is fixed. The ideal I, which corresponds to the lattice, is allowed to change within an ideal class. A uniform way to organize the calculation is to use the generators N and $(c + \sqrt{D})/2$ and perform the step by multiplying by $(\sqrt{D} - c)/(2N)$ to get generators N' and $(\sqrt{D} - c)/2$ and adding a multiple of N' to the second generator to obtain the standard form. That multiple is recorded as the **partial quotient**.

The matrix viewpoint

When continued fractions are used to describe the reductions of a quadratic form on a lattice, they give a chain of bases for the lattice in which adjacent **ordered pairs** of generators are related by a matrix of the form

$$\begin{bmatrix} 0 & 1 \\ 1 & c \end{bmatrix}$$

where c is the partial quotient.

The approximation problem of finding the minimum of an indefinite quadratic form on a lattice may be represented by a 2 by 2 matrix whose rows are labeled by the factors of the form

The matrix viewpoint

and whose columns are labeled by the generators of the lattice. Usually the lattice is fixed, so the continued fraction uses only right multiplication by these **partial quotient** matrices to relate **reduced** bases of the lattice. When working with ideals of a quadratic order, our construction preserves the discriminant, so the matrix representing the ideal is also multiplied on the left by a diagonal matrix. This left action multiplies both the value of the norm form and the discriminant by the same factor, so the ratio of these quantities is preserved, and it is the value of this ratio that is recovered as the **Markoff value** of the chain of partial quotients.

The matrix viewpoint

For the example of $\beta = (1+\sqrt{21})/2$, one step is

$$\begin{bmatrix} \beta-2 & 0 \\ 0 & -1-\beta \end{bmatrix} \begin{bmatrix} 1 & 1+\beta \\ 1 & 2-\beta \end{bmatrix}$$

$$= \begin{bmatrix} \beta-2 & 3 \\ -1-\beta & 3 \end{bmatrix} =$$

$$\begin{bmatrix} 3 & 1+\beta \\ 3 & 2-\beta \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix}$$

The matrix viewpoint

and the next step is

$$\frac{1}{3}\begin{bmatrix} \beta-2 & 0 \\ 0 & -1-\beta \end{bmatrix}\begin{bmatrix} 3 & 1+\beta \\ 3 & 2-\beta \end{bmatrix}$$

$$= \begin{bmatrix} \beta-2 & 1 \\ -1-\beta & 1 \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 1+\beta \\ 1 & 2-\beta \end{bmatrix}\begin{bmatrix} -3 & 1 \\ 1 & 0 \end{bmatrix}$$

The order of an ideal

In this calculation, the order $\mathcal{O}$ is fixed. We only require that $\mathcal{O}I \subseteq I$. If $\mathcal{O}$ is not maximal, it may be that I is also an ideal for a larger order. Since this property is preserved by the operations we have used, the result will be identical to the calculation for the larger order. We may exclude such I from consideration for the order $\mathcal{O}$ since they can be studied using an order of smaller discriminant. Henceforth we assume that $\mathcal{O}$ contains all ξ in the field of fractions of $\mathcal{O}$ with $\xi I \subseteq I$

Periodicity

For a given order $\mathcal{O}$, there are only finitely many **reduced** $\mathcal{O}$-ideals, so the continued fraction must be periodic. In fact, since there is a **single chain** of reduced ideals the period must be given by a **fundamental** unit of $\mathcal{O}$. That is, when one returns to the **same** ideal, the reduction steps give a change of basis of the ideal that is the same as multiplying by the fundamental unit. Thus, the eigenvalues of the product of matrices in a period are a pair of conjugate **fundamental** units of $\mathcal{O}$. Since the matrix has nonnegative entries, this pair is always the smallest unit greater than 1 and its conjugate.

Submodules

If one takes a $\mathbb{Z}$-submodule of an $\mathcal{O}$-ideal of index p (a prime), the result is an ideal **either** for $\mathcal{O}$ **or** for an order that is either a suborder or superorder of $\mathcal{O}$ of index p. There are $p+1$ submodules of index p, but at most one can belong to a larger order and at most two can belong to $\mathcal{O}$, but not both of these are possible.

Index 2

An order $\mathcal{O}$ of discriminant $D \equiv 5 \pmod 8$ has no ideal of norm 2 but may contain a unit not in the order $\mathcal{O}'$ of index 2. The cube of such a unit belongs to $\mathcal{O}'$, and the three submodules of an $\mathcal{O}$ ideal are $\mathcal{O}'$ ideals in the same ideal class (e.g., $D = 5$). It is also possible that the fundamental unit for $\mathcal{O}$ belongs to $\mathcal{O}'$ (e.g., $D = 37$).

If $D \equiv 1 \pmod 8$, there is a split ideal of norm 2, so two of the submodules of index 2 are products with an ideal of norm 2, so are ideals for $\mathcal{O}$ (of odd order in the class group). Congruence modulo 8 show that the fundamental unit of $\mathcal{O}$ belongs to $\mathcal{O}'$.

Index 2

In other cases, either 2 is ramified or $\mathcal{O}$ is of index 2 in another order. Then one submodule belongs to $\mathcal{O}$ or a larger order and two belong to an order of index 2. The fundamental unit of $\mathcal{O}$ either belongs to the suborder or its square is the fundamental unit of the suborder.

The fundamental unit of the order of index 2 in $\mathcal{O}$ is either the first, second, or third power of the fundamental unit of $\mathcal{O}$. The matrix giving the period of the continued fraction of an $\mathcal{O}$ ideal contains this information because its reduction modulo 2 describes the permutation of the three submodules of index 2.

Doubling

There is also a simple algorithm for applying a transformation of determinant 2 to the matrices giving the steps of the continued fraction. With $D(x) = 2x$, $H(x) = x/2$ (for $x \geq 2$) and $K(x) = (x+1)/(x-1)$,

$$D[a, x] = [2a, Hx] \text{ or } D[a, 1, x] = [2a + 1, Kx]$$

$$H[2a, x] = [a, Dx] \text{ or } H[2a + 1, x] = [a, 1, Kx]$$

$$K[1, x] = 1 + Dx, \; K[2a + 1, x] = [1, a, Dx],$$

$$K[2, x] = [2, Kx], \text{ or } K[2a + 2, x] = [1, a, 1, Kx]$$

Problem 10556

Joseph Lewittes proposed a problem in the November 1996 issue of the American Mathematical Monthly. No solution has appeared in the *Monthly*, but the proposer's solution is contained in his article, "Continued Fractions and Quadratic Irrationals", pages 221–252 of "Number Theory: New York Seminar 2003" (ISBN 0-367-40655-7)

Problem Statement

After introducing notation for continued fractions of quadratics, the problem is stated as:

"Let $e(\alpha)$ be the number of a_i in the period of the continued fraction of α that are even. If α and α' have the same discriminant, show that $e(\alpha) \equiv e(\alpha') \pmod 2$."

What is odd about even partial quotients?

The 2-dimensional general linear group over $\mathbb{Z}/2\mathbb{Z}$ is isomorphic to S_3 with the rotations corresponding to the even permutations. For the matrices giving the continued fraction steps:

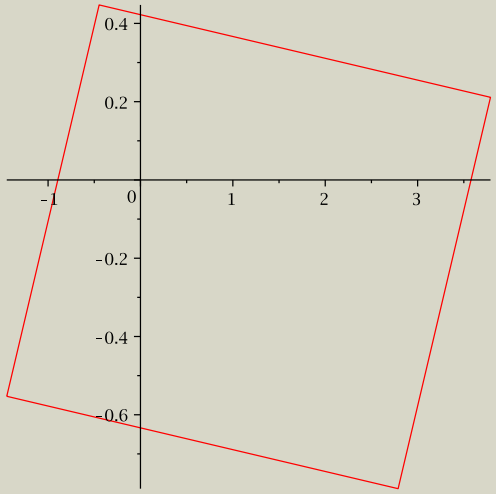
$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \text{ is even, } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ is odd}$$

An **odd** number of **even** partial quotients says that the fundamental unit of $\mathcal{O}$ induces an **odd** permutation of the submodules of index 2, which happens if its square is the fundamental unit of the order of index 2

Divided cells

Inhomogeneous problems are described by a 2 by 3 matrix. The first two columns give the directions of the generators of the lattice, as in the homogeneous case, and the third column gives the location of lattice point in the coordinates given by the factors of the expression to be approximated. Such a matrix is **reduced** if the lattice parallelogram based on the third column with sides in the directions of the first two columns has one vertex in each coordinate quadrant. Such figures have been called **divided cells**.

A picture of a divided cell



A divided cell for $x\,y$ on a lattice.

Some facts

For any product of linear expressions on a lattice:

(•) Each reduced lattice basis determines three cells, one of which is a divided cell for a given expression. Hence:

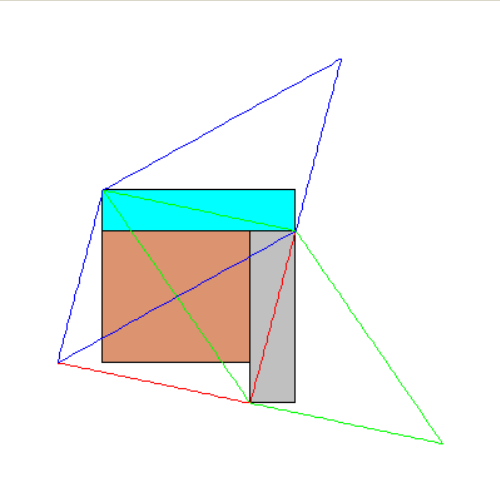
(•) Divided cells exist.

(•) All divided cells form a single chain.

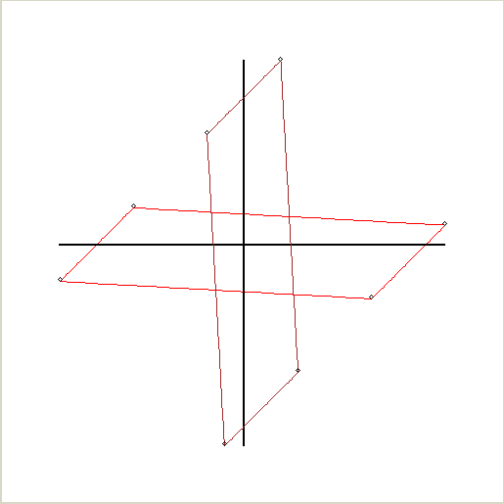
(•) There are other divided cells, but they do not contribute to finding the minimum of the expression on the lattice.

Illustrations of these facts follow.

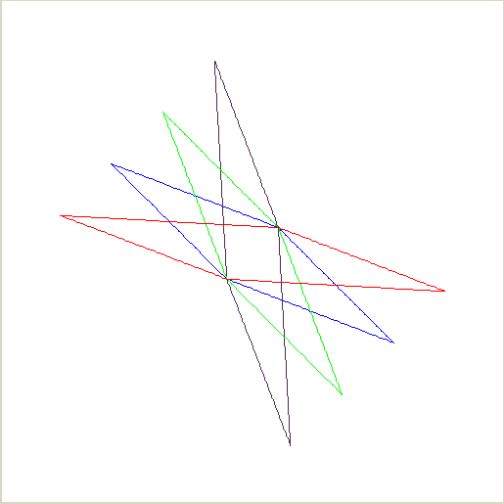
The three boxes



The divided cell step



Superfluous cells



Stepping through cells

If H and V are a **reduced** set of generators of a lattice with $0 < x_V < x_H$, the three cells associated with this are: G, with generators H and V; N+, with generators H and $H - V$ (and diagonal V); and N−, with generators $H + V$ and V (and diagonal H).

The NIM of a lattice

Given a lattice $\mathcal{L}$, and a point Q, one can consider the **N**ormalized **I**nverted **M**inimum

$$\mathrm{NIM}(\mathcal{L}, Q) = \sup_P \left\{ \frac{D(\mathcal{L})}{x_{P+Q}\, y_{P+Q}} : P \in \mathcal{L} \right\}$$

where we take $\mathrm{NIM}(\mathcal{L}, Q) = \infty$ if $Q \in \mathcal{L}$. Minkowski showed that this is always at least 4 and Davenport showed that there is an absolute constant K such that, for any $\mathcal{L}$, there is Q with $\mathrm{NIM}(\mathcal{L}, Q) < K$.

The central value of a cell

As a start on the computation of NIM($\mathcal{L}$, Q), one can consider a **divided cell** with vertices in $\mathcal{L}$ for axes translated to $-Q$, and find the supremum in the definition of NIM($\mathcal{L}$, Q) only for the vertices of the cell. The largest value of this is taken at the **center** of the cell and it is 4 times the discriminant divided by the smaller value of xy for a diagonal.

For an N cell, this central value is 4 times the **Markoff value** of the continued fraction.

The chain of central values

The center of each cell is also the center of **one** of the cells at the next step. The rule for identifying the appropriate cell is that N+ is always followed by N− because these cells share a diagonal; G is followed by N+ if the partial quotient is odd and by G if the partial quotient is even; and N− is followed by whichever type has not been claimed by one of the other cells. Again, the even partial quotients give an odd permutation.

The role of quadratics

If $\mathcal{L}$ is an ideal for a quadratic order, there are only a finite number of reduced bases, each with three cells, and we can consider the central values of each. There will be one, two, or three chains of central values. The largest value in a chain is a NIM for the lattice. Unfortunately, these can be arbitrarily large, since there is only one chain when the period consists of a single odd integer.

However, other finite sets of lattice point can be easily considered and examples have been tabulated that allow us to find several values of $\inf_Q \mathrm{NIM}(\mathcal{L}, Q)$.