J. Austral. Math. Soc. 22 (Series A) (1976), 431–441.

AN EXTENDED INHOMOGENEOUS MINIMUM

E. S. BARNES

(Received 5 September 1975)

Abstract

A new arithmetic invariant $E(f)$ is defined for integral binary quadratic forms f. It has the property that, denoting by f_m the norm-form of a quadratic number field $Q(\sqrt{m})$, $E(f_m) < 1$ if and only if $Q(\sqrt{m})$ has class number one.

1

The inhomogeneous minimum of a form has proved to be an important concept in the study of algebraic number fields with a Euclidean algorithm. I present here a generalization of this concept, for integral binary quadratic forms, which bears a similar relation to the question of unique factorization in quadratic fields.

Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form with real coefficients and discriminant $D = b^2 - 4ac$. The inhomogeneous minimum $M(f)$ of f may be defined thus: for real x_0, y_0, and writing $\boldsymbol{x}_0 = (x_0, y_0)$, set

$$M(f; \boldsymbol{x}_0) = \inf_{(x, y) \in \Gamma} |f(x + x_0, y + y_0)|, \tag{1.1}$$

where Γ denotes the integral lattice in the plane; then

$$M(f) = \sup_{\boldsymbol{x}_0} M(f; \boldsymbol{x}_0). \tag{1.2}$$

Suppose from now on that f is a primitive integral form, and let $\mathscr{S} = \mathscr{S}(f)$ be the set of linear transformations of the plane with matrix of the form

$$T = \begin{pmatrix} t & -cu \\ au & t + bu \end{pmatrix} \quad t, u \quad \text{integral}. \tag{1.3}$$

It is easily seen that, under composition of transformations, $\mathscr{S}$ is a semigroup with identity I. (This follows most easily from the fact that an integral T belongs to $\mathscr{S}$ if and only if T transforms f into $(\det T)f$.)

For $\boldsymbol{x}_0 \notin \Gamma$, define

$$E(f;\boldsymbol{x}_0) = \inf_{\substack{T\in\mathcal{S}\\ T\boldsymbol{x}_0\notin\Gamma}} M(f;T\boldsymbol{x}_0) \tag{1.4}$$

and

$$E(f) = \sup_{\boldsymbol{x}_0\notin\Gamma} E(f;\boldsymbol{x}_0). \tag{1.5}$$

We call $F(f)$ the 'extended inhomogeneous minimum' of f. Trivially, since $I \in \mathcal{S}$,

$$E(f) \leqq M(f) \tag{1.6}$$

for all f. Note also that since the transformations T of $\mathcal{S}$ are integral,

$$E(f;\boldsymbol{x}_1) = E(f;\boldsymbol{x}_0) \quad \text{if} \quad \boldsymbol{x}_1 \equiv \boldsymbol{x}_0 \pmod{\Gamma}.$$

We show first that, like $M(f)$, $E(f)$ is an arithmetical invariant.

LEMMA 1.1. *If g is equivalent to f (under integral unimodular tranformation) then $E(g) = E(f)$.*

PROOF. Suppose that $g(\boldsymbol{x}) = f(U\boldsymbol{x})$ where U is integral unimodular, and so $U\Gamma = \Gamma$. Then, for all $\boldsymbol{x}_0$, it is easily seen that

$$M(f;\boldsymbol{x}_0) = M(g;U^{-1}\boldsymbol{x}_0).$$

Hence

$$M(f;T\boldsymbol{x}_0) = M(g;U^{-1}TU(U^{-1}\boldsymbol{x}_0))$$

The required result will follow at once when we show that

$$\mathcal{S}(g) = U^{-1}\mathcal{S}(f)U;$$

and for this it suffices, by symmetry, to show that

$$U^{-1}\mathcal{S}(f)U \subseteq \mathcal{S}(g). \tag{1.7}$$

A straightforward calculation shows that, with

$$f(x,y) = ax^2 + bxy + cy^2, \quad g(x,y) = a'x^2 + b'xy + c'y^2,$$

if $\det U = 1$ and $T \in \mathcal{S}(f)$ is given by (1.3),

$$U^{-1}TU = \begin{pmatrix} t + \frac{1}{2}(b-b')u & -c'u \\ a'u & t + \frac{1}{2}(b+b')u \end{pmatrix} \in \mathcal{S}(g).$$

A similar calculation shows that $U^{-1}TU \in \mathcal{S}(g)$ also if $\det U = -1$, so (1.7) is proved.

https://doi.org/10.1017/S1446788700016281 Published online by Cambridge University Press

To establish the connection with unique factorization in quadratic fields, let $F = Q(\sqrt{m})$ where m is square-free and not 0 or 1. Set

$$f_m(x, y) = \begin{cases} x^2 - my^2 & \text{if} \quad m \equiv 2 \text{ or } 3 \pmod 4 \\ x^2 + xy + \frac{1}{4}(1-m)y^2 & \text{if} \quad m \equiv 1 \pmod 4. \end{cases}$$

THEOREM 1. *$Q(\sqrt{m})$ has class number 1 if and only if $E(f_m) < 1$.*

We first need

LEMMA 1.2. *If $\mathbf{x}_0$ is not a rational point, then $E(f; \mathbf{x}_0) = 0$.*

PROOF. Given any $\varepsilon, 0 < \varepsilon < 1$, we may, by Minkowski's theorem on linear forms, choose integers x, y, t, u not all zero so that

$$| x + tx_0 - cuy_0 | < \varepsilon$$

and

$$| y + aux_0 + (t + bu)y_0 | < \varepsilon.$$

Since $\varepsilon < 1$, $t, u \neq 0, 0$; hence if T is defined by (1.3), $T \in \mathcal{S}(f)$ and $T \neq 0$ and so, since $\mathbf{x}_0$ is not rational, $T\mathbf{x}_0 \notin \Gamma$. Hence

$$E(f; \mathbf{x}_0) \leqq | f(\mathbf{x} + T\mathbf{x}_0) | < \varepsilon^2(| a | + | b | + | c |).$$

Since ε is arbitrary, we have $E(f; \mathbf{x}_0) = 0$.

PROOF OF THEOREM 1. The Dedekind–Hasse criterion states (see for example Pollard 1950):
if F is an algebraic number field and J its ring of integers, then F has class number 1 if and only if, given any non-zero elements α, β of J with $\beta \nmid \alpha$, $\exists \gamma, \delta \in J$ satisfying

$$0 < | N(\alpha\gamma + \beta\delta) | < | N\beta |$$

(where N is the norm in F/Q). Setting $\rho = \alpha/\beta$, so that $\rho \notin J$, we can write this condition as: given any $\rho \in F - J$, $\exists \gamma, \delta \in J$ satisfying

$$0 < | N(\gamma\rho + \delta) | < 1.$$

Trivially, this inequality cannot be satisfied for any δ if $\gamma\rho \in J$; while if $\gamma\rho \notin J$, $N(\gamma\rho + \delta) \neq 0$ for all $\delta \in J$. Thus we can finally write the condition as: *given any $\rho \in F - J$, $\exists \gamma, \delta \in J$ with $\gamma\rho \notin J$ satisfying*

$$| N(\gamma\rho + \delta) | < 1. \tag{1.8}$$

Let now F be a quadratic field, so that $F = Q(\sqrt{m})$ where $m \neq 0$ or 1 and m is square-free. A basis of J/Z is $\{1, \omega\}$, where

$$\omega = \begin{cases} \sqrt{m} & \text{if} \quad m \equiv 2 \text{ or } 3 \pmod 4 \\ \frac{1}{2}(1+\sqrt{m}) & \text{if} \quad m \equiv 1 \pmod 4); \end{cases}$$

and then, for rational x, y,

$$N(x+\omega y) = f_m(x, y).$$

Writing $\rho = x_0 + \omega y_0$ $(x_0, y_0 \in Q)$, $\gamma = t + \omega u$ $(t, u \in Z)$, $\delta = x + \omega y$ $(x, y \in Z)$, we can translate the Dedekind–Hasse criterion into: $Q(\sqrt{m})$ has class number 1 if and only if, given any rational $\boldsymbol{x}_0 = (x_0, y_0) \notin \Gamma$, there exists a

$$(1.9) \quad T = \begin{pmatrix} t & mu \\ u & t \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} t & \frac{1}{4}(-1+m)u \\ u & t+u \end{pmatrix} \quad \text{respectively} \quad (t, u \in Z)$$

with $T\boldsymbol{x}_0 \notin \Gamma$ and an $\boldsymbol{x} = (x, y) \in \Gamma$ satisfying

$$(1.10) \qquad |f_m(T\boldsymbol{x}_0 + \boldsymbol{x})| < 1.$$

Since clearly T has the shape (1.9) if and only if $T \in \mathscr{S}(f_m)$, we see that (1.10) holds precisely when

$$E(f_m; \boldsymbol{x}_0) < 1.$$

For irrational $\boldsymbol{x}_0$, Lemma 1.2 shows that this inequality is always satisfied; so Theorem 1 follows immediately.

2

Although it is trivially true that $E(f) \leqq M(f)$ for all f, it appears that E does not satisfy any stronger general inequality than M. More precisely, we have

THEOREM 2.1. *If f is a primitive integral indefinite quadratic form of discriminant $D > 0$, then*

$$(2.1) \qquad E(f) < \tfrac{1}{4}\sqrt{D};$$

and the constant $\frac{1}{4}$ is best possible.

PROOF. (i) A well-known result of Minkowski states that, for indefinite f,

$$M(f) \leqq \tfrac{1}{4}\sqrt{D},$$

where equality holds only for forms equivalent to a multiple of

$$f_0(x, y) = xy.$$

Now $\mathscr{S}(f_0)$ contains the transformations $\left(\begin{smallmatrix}1 & 0 \\ 0 & 0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0 & 0 \\ 0 & 1\end{smallmatrix}\right)$, from which it is easy to see that $E(f_0) = 0$. Hence (2.1) now follows from the fact that $E(f) \leqq M(f)$.

https://doi.org/10.1017/S1446788700016281 Published online by Cambridge University Press

(ii) Consider, for positive integral k, the form

$$\varphi_k(x, y) = x^2 + 2kxy - y^2$$

with discriminant $D = 4(k^2 + 1)$. Davenport (1946) showed that

$$M(\varphi_k) = M(\varphi_k\,;\,(\tfrac{1}{2}, \tfrac{1}{2})) = \tfrac{1}{2}k.$$

If now $T \in \mathcal{S}(\varphi_k)$,

$$T = \begin{pmatrix} t & u \\ u & t + 2ku \end{pmatrix}, \quad t, u \in Z$$

and so

$$T(\tfrac{1}{2}, \tfrac{1}{2}) = (\tfrac{1}{2}(t + u), \tfrac{1}{2}(t + u) + ku) \equiv (\tfrac{1}{2}(t + u), \tfrac{1}{2}(t + u)) \,(\mathrm{mod}\, \Gamma).$$

Hence if $T(\frac{1}{2}, \frac{1}{2}) \not\in \Gamma$, necessarily $T(\frac{1}{2}, \frac{1}{2}) \equiv (\frac{1}{2}, \frac{1}{2})\,(\mathrm{mod}\,\Gamma)$. It follows that

$$E(\varphi_k\,;\,(\tfrac{1}{2}, \tfrac{1}{2})) = M(\varphi_k\,;\,(\tfrac{1}{2}, \tfrac{1}{2})) = \tfrac{1}{2}k.$$

The result of the theorem now follows on noting that $\frac{1}{2}k/\sqrt{D} \to \frac{1}{4}$ as $k \to \infty$.

For a simple result in the opposite direction, define

$$\mu(f) = \inf_{\substack{x \in \Gamma \\ x \neq 0}} |f(x, y)|$$

(the homogeneous minimum of f).

THEOREM 2.2. *If $f(x, y)$ does not represent zero (for integral $x, y \neq 0, 0$), then*

$$E(f) \geqq \tfrac{1}{4}\mu(f) \geqq \tfrac{1}{4}.$$

PROOF. An element T of $\mathcal{S}(f)$ maps each of the points $(\frac{1}{2}, 0)$, $(0, \frac{1}{2})$, $(\frac{1}{2}, \frac{1}{2})$ either into a point of Γ or into a point of this set modulo Γ. It follows that

$$\begin{aligned} E(f) &\geqq \min\{M(f; (\tfrac{1}{2}, 0)), M(f; (0, \tfrac{1}{2})), M(f; (\tfrac{1}{2}, \tfrac{1}{2}))\} \\ &\geqq \tfrac{1}{4}\mu(f). \end{aligned}$$

It is known that there exists a constant $\kappa > 0$ such that, if f is indefinite and does not represent zero, then $M(f) > \kappa\sqrt{D}$. It is an open question whether a similar result holds for $E(f)$; if it does, it could immediately be deduced from Theorem 1.1 that there exist only finitely many real quadratic fields with class number one (contrary to a well-known conjecture of Gauss!).

3. The evaluation of $E(f_m)$

We indicate here a procedure for calculating $E(f_m)$ for given m, and in particular for determining whether or not $E(f_m) < 1$. The methods apply with obvious modifications to any integral form f, and indicate the necessarily close relation between the value of $E(f)$ and the number of classes of forms of given discriminant $D = D(f)$. It is convenient here to restrict attention to forms which do not represent zero.

By Lemma 1.2, it suffices in evaluating $E(f)$ to consider $E(f; \mathbf{x}_0)$ for rational $\mathbf{x}_0 \notin \Gamma$, say $\mathbf{x}_0 = \left(\frac{r}{q}, \frac{s}{q}\right)$ where $\gcd(r, s, q) = 1$ and $q \geqq 2$. Since all integral multiples of the identity belong to $\mathscr{S}(f)$ for all f, it follows easily that

$$E\left(f; \left(\frac{r}{q'}, \frac{s}{q'}\right)\right) \leqq E\left(f; \left(\frac{r}{q}, \frac{s}{q}\right)\right) \quad \text{if} \quad q \mid q'.$$

We may therefore restrict our attention to prime q, and define for such q

$$E_q(f) = \max_{\substack{\mathbf{x}_0 \notin \Gamma \\ q\mathbf{x}_0 \in \Gamma}} E(f; \mathbf{x}_0), \tag{3.1}$$

whence

$$E(f) = \max_{q \text{ prime}} E_q(f). \tag{3.2}$$

LEMMA 3.1. *Suppose that f does not properly represent zero modulo q. Then*

$$E_q(f) \leqq \frac{1}{4} \mu(f). \tag{3.3}$$

PROOF. By applying a suitable equivalence transformation, we may assume that

$$f(x, y) = ax^2 + bxy + cy^2 \quad \text{with} \quad \mu(f) = |a|.$$

Let $\mathbf{x}_0 = \left(\frac{r}{q}, \frac{s}{q}\right)$, $\mathbf{x}_0 \notin \Gamma$. Choose

$$T = \begin{pmatrix} ar + bs & cs \\ -as & ar \end{pmatrix} \in \mathscr{S}(f).$$

Then

$$T\mathbf{x}_0 = \left(\frac{1}{q} f(r, s), 0\right)$$

where, by hypothesis, $f(r, s) \not\equiv 0 \pmod{q}$, so that $T\mathbf{x}_0 \notin \Gamma$. Choosing an integer x with $|x + (1/q) f(r, s)| \leqq \frac{1}{2}$, we obtain

$$E(f; \mathbf{x}_0) \leqq M(f; T\mathbf{x}_0) \leqq \left| f\left(x + \frac{1}{q} f(r, s), 0\right) \right| \leqq \frac{1}{4} |a| = \frac{1}{4} \mu(f).$$

Since this result holds for all x_0 with $qx_0 \in \Gamma$, (3.3) follows.

We now look particularly at the forms f_m.

LEMMA 3.2. *If q is prime and $\frac{1}{4} < \lambda \leqq 1$, then $E_q(f_m) < \lambda$ if*

(i) $m < 0$, $m \equiv 2$ *or* $3 \pmod 4$ *and* $q^2 > \dfrac{4|m|}{3\lambda^2}$;

or (ii) $m < 0$, $m \equiv 1 \pmod 4$ *and* $q^2 > \dfrac{|m|}{3\lambda^2}$;

or (iii) $m > 0$, $m \equiv 2$ *or* $3 \pmod 4$ *and* $q^2 > \dfrac{|m|}{2\lambda^2}$;

or (iv) $m > 5$, $m \equiv 1 \pmod 4$ *and* $q^2 > \dfrac{|m|}{8\lambda^2}$.

PROOF. Since $\mu(f_m) = 1$, Lemma 3.1 shows that it suffices to consider only primes q for which f_m properly represents zero modulo q.

Let $x_0 = \left(\dfrac{r}{q}, \dfrac{s}{q}\right)$, $x_0 \notin \Gamma$. If $f(r, s) \not\equiv 0 \pmod q$, the argument of Lemma 3.1 shows that $E_q(f_m; x_0) \leqq \frac{1}{4} < \lambda$. We may therefore suppose that

$$f_m(r, s) \equiv 0 \pmod q;$$

and since $r, s \not\equiv 0, 0 \pmod q$, we see that $s \not\equiv 0 \pmod q$. Hence there exists an integral z with $r \equiv sz \pmod q$ and so

$$x_0 \equiv \left(\frac{sz}{q}, \frac{s}{q}\right) \pmod q, \quad s \not\equiv 0 \pmod q \tag{3.4}$$

where

$$f_m(z, 1) \equiv 0 \pmod q. \tag{3.5}$$

It is easily verified that the set of points (3.4) is permuted by the transformations of $\mathcal{S}(f_m)$; and that, although z is not uniquely defined by (3.5), two different z yield the same value of $M(f_m; x_0)$ for the point (3.4). It thus follows that, if $E_q(f_m) > \frac{1}{4}$, then

$$E_q(f_m) = \min_{s \not\equiv 0 \pmod q} M\left(f_m; \left(\frac{sz}{q}, \frac{s}{q}\right)\right) \tag{3.6}$$

z is any integer satisfying (3.5).

Now

$$f_m\left(x' + \frac{sz}{q}, y' + \frac{sz}{q}\right) = \frac{1}{q^2} f_m(qx' + sz, qy' + s)$$

$$= \frac{1}{q^2} f_m(qx + zy, y),$$

https://doi.org/10.1017/S1446788700016281 Published online by Cambridge University Press

where

$$x = x' - zy', \quad y = qy' + s$$

so that $(x', y') \in \Gamma$ iff $(x, y) \in \Gamma$ and $y \equiv s \pmod{q}$. Now

$$(3.7) \qquad \frac{1}{q} f_m(qx + zy, y) = \begin{cases} qx^2 + 2zxy + \dfrac{1}{q}(z^2 - m)y^2 & m \not\equiv 1 \pmod 4 \\ qx^2 + (2z+1)xy + \dfrac{1}{q}\left(z^2 + z - \dfrac{m-1}{4}\right)y^2 & m \equiv 1 \pmod 4 \end{cases}$$

$$= f_m^{(q)}(x, y),$$

say, where $f_m^{(q)}$ is an integral quadratic form of discriminant $D = 4m$ or m. It now follows from (3.6) that, if $E_q(f_m) > \frac{1}{4}$,

$$(3.8) \qquad E_q(f_m) = \frac{1}{q} \min_{\substack{(x,y) \in \Gamma \\ y \not\equiv 0 \pmod q}} |f_m^{(q)}(x, y)|.$$

By classical results on the homogeneous minima of quadratic forms, there exist $(x, y) \in \Gamma$, $(x, y) \neq (0, 0)$ satisfying

$$(3.9) \qquad |f_m^{(q)}(x, y)| \leqq \sqrt{\frac{|D|}{3}} \quad \text{if } m < 0$$

and

$$(3.10) \qquad |f_m^{(q)}(x, y)| \leqq \sqrt{\frac{D}{8}} \quad \text{if } m > 0 \text{ and } m \neq 5.$$

Hence, firstly, if $m < 0$ and $\frac{1}{3}|D| < \lambda^2 q^2$, we have $(x, y) \in \Gamma - \{\mathbf{0}\}$ satisfying

$$|f_m^{(q)}(x, y)| < \lambda q;$$

since $f_m^{(q)}(x, y) \equiv 0 \pmod q$ if $y \equiv 0 \pmod{(q)}$, and since $f_m^{(q)}$ is not a zero form, it follows from (3.8) that

$$E_q(f_m) < \lambda.$$

The results (i) and (ii) of the Lemma follow with $|D| = 4|m|$ and $|m|$ respectively.

A similar analysis yields the results (iii) and (iv) in the case $m > 0$ $(m \neq 5)$.

When $m < 0$, it is possible to obtain somewhat stronger results by using the properties of reduced quadratic forms. Suppose that, in (3.5), we choose z to satisfy

$$(3.11)\quad \begin{cases} -\frac{1}{2}q < z \leqq \frac{1}{2}q & \text{when}\quad m \equiv 2 \text{ or } 3 \pmod 4 \\ z = 0 \quad \text{if}\quad q = 2 & \text{and}\quad m \equiv 1 \pmod 4 \\ -\frac{1}{2}(q+1) < z \leqq \frac{1}{2}(q-1) & \text{when}\quad m \equiv 1 \pmod 4 \text{ and } q \text{ is odd}. \end{cases}$$

Then $f_m^{(q)}$ is reduced in the sense of Gauss if also

$$(3.12)\qquad f_m^{(q)}(0,1) = \frac{1}{q} f_m(z,1) \geqq q;$$

and it then follows that, since $f_m^{(q)}(0,1)$ is the least value assumed by $f_m^{(q)}(x,y)$ with $y \neq 0$,

$$E_q(f_m) = \frac{1}{q} f_m^{(q)}(0,1) = \frac{1}{q^2} f_m(z,1):$$

If however (3.12) does not hold, we have in any case

$$E_q(f_m) \leqq \frac{1}{q} f_m^{(q)}(0,1) = \frac{1}{q^2} f_m(z,1).$$

Summarizing, we have:

LEMMA 3.3. *If $m < 0$, q is prime and z satisfies* (3.5) *and* (3.11), *then*
(i) $E_q(f_m) = \frac{1}{q^2} f_m(z,1)$ *if* $f_m(z,1) \geqq q^2$;
(ii) $E_q(f_m) \leqq \frac{1}{q^2} f_m(z,1)$ *if* $f_m(z,1) < q^2$.

We conclude with some examples of the evaluation of $E(f_m)$.
(1) $E(f_{-35}) = 1$. We have

$$f_{-35}(x,y) = x^2 + xy + 9y^2.$$

Since the congruence $f_{-35}(z,1) \equiv 0 \pmod 2$ is insoluble, $E_2(f_{-35}) = \frac{1}{4}$. Next

$$f_{-35}^{(3)}(x,y) = 3x^2 + xy + 3y^2,$$

so, by Lemma 3.3 (this form being reduced), $E_3(f_{-35}) = 1$. Finally, by Lemma 3.2 (ii), $E_q(f_{-35}) < 1$ if $q^2 > 35/3$ and so if $q \geqq 5$. Hence

$$E(f_{-35}) = E_3(f_{-35}) = 1$$

(2) $E(f_{38}) = \frac{1}{2}$. First

$$f_{38}^{(2)}(x,y) = 2x^2 - 19y^2 \quad \text{and} \quad f_{38}^{(2)}(3,1) = -1,$$

so that

$$E_2(f_{38}) = \tfrac{1}{2}.$$

Next, the congruence

$$f_{38}(z, 1) = z^2 - 38 \equiv 0 \pmod q$$

is insoluble for $q = 3, 5$ and 7, whence

$$E_q(f_{38}) \leqq \tfrac{1}{4} \quad \text{for } q = 3, 5 \text{ and } 7.$$

Finally, by Lemma 3.2 (iii),

$$E_q(f_{38}) < \tfrac{1}{2} \quad \text{if} \quad q^2 > 76$$

and so for all prime $q > 7$. Hence

$$E(f_{38}) = E_2(f_{38}) = \tfrac{1}{2}.$$

(3) $E(f_{42}) = \frac{3}{2}$. First, $f_{42}^{(2)}(x, y) = 2x^2 - 21y^2$; congruences mod 8 give

$$f_{42}^{(2)}(x, y) \equiv \pm 3 \pmod 8$$

for odd y; *also* $f_{42}^{(2)}(3, 1) = -3$. *Hence*

$$E_2(f_{42}) = \tfrac{3}{2}.$$

Next

$$f_{42}^{(3)}(x, y) = 3x^2 - 14y^2 \quad \text{and} \quad f_{42}^{(3)}(2, 1) = -2,$$

so that

$$E_3(f_{42}) \leqq \tfrac{2}{3}.$$

Finally, $E_q(f_{42}) < 1$ if $q^2 > 21$, by Lemma 3.2 (iii), and so for all primes $q > 3$. Hence

$$E(f_{42}) = E_2(f_{42}) = \tfrac{3}{2}.$$

(4) $E(f_{97}) = \frac{1}{2}$. Here

$$f_{97}(x, y) = x^2 + xy - 24y^2.$$

Hence

$$f_{97}^{(2)}(x, y) = 2x^2 + xy - 12y^2 \quad \text{and} \quad f_{97}^{(2)}(19, -7) = 1,$$

and so

$$E_2(f_{97}) = \tfrac{1}{2}.$$

Next

$$f_{97}^{(3)}(x, y) = 3x^2 + xy - 8y^2 \quad \text{and} \quad f_{97}^{(3)}(3, 2) = 1,$$

and so

$$E_3(f_{97}) = \tfrac{1}{3}.$$

The congruence

$$f_{97}(z, 1) \equiv 0 \pmod 5)$$

is insoluble, whence $E_5(f_{97}) \leqq \frac{1}{4}$. Finally, by Lemma 3.2 (iv), $E_q(f_{97}) < \frac{1}{2}$ if $q^2 > \frac{97}{2}$ and so for all prime $q \geqq 7$. Hence

$$E(f_{97}) = E_2(f_{97}) = \tfrac{1}{2}.$$

This example is of interest, since $Q(\sqrt{97})$, while simple, is not Euclidean.

References

H. Davenport, (1946) 'Non-homogeneous binary quadratic forms', *Proc. K. Ned. Akad. van Wet.* **49**, 815–821.

H. Pollard, (1950) *The theory of algebraic numbers* (Math. Association of America, New York, 1950).

University of Adelaide,
South Australia.