ACTA ARITHMETICA
VI (1961)

Unpublished results on number theory I

Quadratic forms in a Euclidean ring

by

S. LUBELSKI †

Edited by C. SCHOGT (Amsterdam)

1. The regretted Polish mathematician S. Lubelski, who met his death in world war II, left to his colleague J. G. van der Corput a manuscript titled: *Zahlentheorie*. In the years after the war this manuscript, which contained a preliminary version of a book on theory of numbers, was studied in the Mathematical Centre at Amsterdam. Although in the meantime a large number of books and memoirs on the subject had appeared it turned out that the manuscript contained several new results. After having been placed in the scope of the classical and modern literature, these results are worth to be published separately.

In the present note the first of these results are given.

As is well known Hermite has proved the following theorem:

If $f(x_1, \ldots, x_n)$ is a positive quadratic form with determinant D and $M(f)$ is the smallest positive value of f for integral values of the variables, we have $M(f) \leqslant (\frac{4}{3})^{(n-1)/2}\sqrt[n]{D}$.

A simple proof is found in Cassels [1]. Later considerably sharper results were derived, a. o. by Minkowski and Blichfeldt (see Koksma [2]). In the special case of integral positive quadratic forms this theorem can be used to prove, that the number of classes of equivalent forms with a given determinant is finite.

The analogous problem was also treated for other types of quadratic forms. Mordell [3] and Oppenheim [4] derived analogous results for indefinite quadratic forms. Here also must be mentioned the critical note by Landherr [7] and the treatment by Siegel [8], who uses Hermite's definition of a reduced indefinite form. Further, Oppenheim [5, 6] and Siegel [9] treated the analogous problem for integral Hermitian forms.

Here quadratic forms will be considered, whose coefficients are elements of a Euclidean ring, which is also the domain of values for the variables. In particular those Euclidean rings will be treated which consist of the integers of an imaginary quadratic number field.

The main results are given by theorems 1 and 2. In the rational case, theorem 1, 3° just gives Hermite's estimate. It may be remarked that theorem 1 is somewhat different from the original result in Lubelski's manuscript, in so far as he restricted himself to the statements 1° and 3°.

Several indications were given by C. G. Lekkerkerker.

2. In a Euclidean ring I we consider quadratic forms in n variables:

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \quad \text{with} \quad a_{ij} = a_{ji}.$$

(I is the set of possible values for the variables and also the coefficients a_{ij} are elements of I.)

The discriminant of f is defined as the determinant of the coefficients: $\det(a_{ij})$.

By a linear transformation

$$x_i = \sum_{j=1}^{n} c_{ij} y_j$$

the form $f(x_1, \ldots, x_n)$ is transformed into a form

$$F(y_1, \ldots, y_n) = \sum_{i,j=1}^{n} b_{ij} y_i y_j.$$

The inverse transformation exists (in I), if and only if $\det(c_{ij})$ is a unit of I. Then f and F represent the same elements of I. The forms are called (properly) *equivalent* in the case, that the transformation has determinant 1 (the element "one" of I). Equivalence is reflexive, symmetric and transitive. We have

$$(b_{mt}) = (c'_{mi})(a_{ij})(c_{jt}) \quad \text{with} \quad c'_{mi} = c_{im};$$

so

$$\det(b_{mt}) = \det(a_{ij})(\det(c_{jt}))^2.$$

It follows, that equivalent forms have the same discriminant. We say, that *f represents an element of I properly*, when this element occurs as a value of f with relatively prime $x_1, \ldots, x_n$. Equivalent forms also represent the same elements properly.

LEMMA 1. *If in a Euclidean ring the quadratic form f represents the element a properly, there exists a form, which is equivalent to f and whose first coefficient is a.*

Proof. a is represented properly by f, so we have $a = f(u_1, \ldots, u_n)$ with relatively prime $u_1, \ldots, u_n$. According to the theorem of the elementary divisors (1), in a Euclidean ring for a given matrix $\begin{pmatrix} a_{11} \cdots \\ \cdots \cdots \\ \cdots a_{nm} \end{pmatrix}$ we have

$$\begin{pmatrix} p_{11} \cdots \\ \cdots \cdots \\ \cdots p_{nn} \end{pmatrix} \begin{pmatrix} a_{11} \cdots \\ \cdots \cdots \\ \cdots a_{nm} \end{pmatrix} \begin{pmatrix} q_{11} \cdots \\ \cdots \cdots \\ \cdots q_{mm} \end{pmatrix} = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \ddots \end{pmatrix},$$

where $\det(p_{ij})$ and $\det(q_{ij})$ are units and ε_1 is a g.c.d. of the elements a_{ij}.

Applying this to the matrix $\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$ we have $m = 1$ and we find

$$\begin{pmatrix} p_{11} \cdots \\ \cdots \cdots \\ \cdots p_{nn} \end{pmatrix} \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} q = \begin{pmatrix} \varepsilon_0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Here $\det(p_{ij})$ and q are units; ε is also a unit, as ε is a g.c.d. of $u_1, \ldots, u_n$ and $u_1, \ldots, u_n$ are relatively prime. It is easy to prove that we can make $\det(p_{ij}) = q = \varepsilon = 1$.

Now let $y_i = \sum_{j=1}^{n} p_{ij} x_j$ transform $f(x_1, \ldots, x_n)$ into $F(y_1, \ldots, y_n)$. Then f and F are equivalent and $f(u_1, \ldots, u_n) = F(1, 0, \ldots, 0)$, so $F(1, 0, \ldots, 0) = a$.

LEMMA 2. *The integers of an imaginary quadratic number field $R(\sqrt{-d})$ form a Euclidean ring for $-d = -1, -2, -3, -7, -11$ (and in no other case).*

In these Euclidean rings for given α and β with $\beta \neq 0$ there always exists a number ξ, so that $|\alpha - \beta\xi|^2 \leqslant v|\beta|^2$, where

$$v = \tfrac{1}{2} \quad \text{for} \quad -d = -1, \qquad v = \tfrac{4}{7} \quad \text{for} \quad -d = -7,$$
$$v = \tfrac{3}{4} \quad \text{for} \quad -d = -2, \qquad v = \tfrac{9}{11} \quad \text{for} \quad -d = -11.$$
$$v = \tfrac{1}{3} \quad \text{for} \quad -d = -3,$$

These values of v cannot be replaced by smaller ones.

Remarks. 1. For $d \not\equiv 3 \pmod 4$ we have $v = \frac{1}{4}(1+d)$, for $d = 4k-1$ we have $v = k^2/(4k-1)$.

2. For the Euclidean ring of the rational integers the same holds with $v = \frac{1}{4}$.

(1) See van der Waerden, *Moderne algebra*, § 108.

3. The five imaginary quadratic number fields, whose integers form a Euclidean ring, were first mentioned by Dickson. The smallest possible values of v are due to Heinhold [10].

3. In the following we restrict the Euclidean rings to those of lemma 2 and the ring of the rational integers; as a further restriction we only consider forms with discriminant $\neq 0$. Now we introduce the notion of a reduced form (standard form). For $n = 1$ every form is a reduced one; further we define (by induction): a reduced form $f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ is a form, which has the following properties:

1. $|a_{1i}| \leqslant |a_{11}|\sqrt{v}$ *for all* $i > 1$, *where* v *is the number* v *of lemma 2 and* $v = \frac{1}{4}$ *for the ring of the rational integers.*

2. *There is no equivalent form, for which* $|a_{11}|$ *is smaller and positive.*

3. $\bar{f}(x_2, \ldots, x_n) = a_{11}f(x_1, \ldots, x_n) - \left(\sum_{i=1}^{n} a_{1i}x_i\right)^2$ *is a reduced form.*

THEOREM 1. 1° *Every class of equivalent forms contains a reduced form.*
2° *For a reduced form in* n *variables we have*

$$|a_{11}| \leqslant w^{(n-1)/2}\sqrt[n]{|D|},$$

where D *is the discriminant and* $w = \max\left((1-v)^{-1}, 4\right)$.

3° *If a form in* n *variables is reduced and is not a zero form, we have*

$$|a_{11}| \leqslant (1-v)^{-(n-1)/2}\sqrt[n]{|D|}.$$

(A *zero form* is a form, which has the value 0 for a set of values of the variables, which are not all 0.)

Proof. 1° We give a proof by induction. For $n = 1$ there is nothing to be proved. Now we suppose that the statement holds for $n-1$ variables, and prove it for n variables.

Let a be a number with smallest possible positive absolute value, represented properly by a given class of equivalent forms in n variables. According to lemma 1 this class contains a form

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j, \quad \text{with} \quad a_{11} = a.$$

This form satisfies the second condition for reduced forms. Now let

$$\bar{f}(x_2, \ldots, x_n) = a_{11}f(x_1, \ldots, x_n) - \left(\sum_{i=1}^{n} a_{1i}x_i\right)^2$$

and let Δ be the discriminant of $\bar{f}$. By the transformation (a_{ij}), with $a_{ij} = \delta_{ij}$ for $i > 1$, the form $x_1^2 + \bar{f}(x_2, \ldots, x_n)$ with discriminant Δ is transformed into the form $a_{11}f$ with discriminant $a_{11}^n D$. As the transformation has determinant a_{11}, we have $a_{11}^2\Delta = a_{11}^n D$. So $\Delta \neq 0$. Then we may apply the induction hypothesis to $\bar{f}$; this says, that $\bar{f}(x_2, \ldots, x_n)$ is equivalent to a reduced form $\bar{F}(y_2, \ldots, y_n)$. Let $(d_{ij})_{i,j=2,\ldots,n}$ be the corresponding transformation; it has determinant 1. Let $d_{12}, \ldots, d_{1n}$ be numbers of the Euclidean ring with

$$\left|a_{11}d_{1j} + \sum_{i=2}^{n} a_{1i}d_{ij}\right| \leqslant |a_{11}|\sqrt{v} \quad \text{for} \quad j = 2, \ldots, n;$$

such numbers exist according to lemma 2. Now we put $d_{11} = 1$, $d_{i1} = 0$ for $i = 2, \ldots, n$ and apply the transformation (d_{ij}) to $f(x_1, \ldots, x_n)$; this transformation also has determinant 1. We get a form $F(y_1, \ldots, y_n) = \sum_{i,j=1}^{n} b_{ij}y_iy_j$. Now we have

$$b_{ij} = \sum_{k,l=1}^{n} a_{kl}d_{ki}d_{lj}, \quad \text{where} \quad d_{11} = 1,\ d_{21} = \ldots = d_{n1} = 0.$$

For $i = 1$ this gives $b_{1j} = \sum_{l=1}^{n} a_{1l}d_{lj}$; from this it follows again, that $b_{11} = a_{11}$. Now for $j = 2, \ldots, n$ we have $|\sum_{l=1}^{n} a_{1l}d_{lj}| \leqslant |a_{11}|\sqrt{v}$, so $|b_{1j}| \leqslant |b_{11}|\sqrt{v}$. This means, that F satisfies the first condition for reduced forms.

By the transformation, the linear form $\sum_{i=1}^{n} a_{1i}x_i$ is transformed into $\sum_{i,j=1}^{n} a_{1i}d_{ij}y_j = \sum_{j=1}^{n} b_{1j}y_j$. As the transformation also transforms $\bar{f}$ into $\bar{F}$, we get

$$\bar{F}(y_2, \ldots, y_n) = b_{11}F(y_1, \ldots, y_n) - \left(\sum_{j=1}^{n} b_{1j}y_j\right)^2.$$

Here $\bar{F}$ is reduced, so F satisfies the third condition for reduced forms.

Now F satisfies the three conditions for reduced forms, hence F is a reduced form.

2° For $n = 1$ the statement is trivial.

Now at first we shall prove it for $n = 2$. So we consider a reduced form $f(x_1, x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$. We distinguish two cases: $a_{22} \neq 0$ and $a_{22} = 0$.

In the first case $|a_{11}| \leqslant |a_{22}|$, so

$$|a_{11}|^2 \leqslant |a_{11}a_{22}| \leqslant |a_{11}a_{22}-a_{12}^2|+|a_{12}|^2 \leqslant |a_{11}a_{22}-a_{12}^2|+v\,|a_{11}|^2$$
$$= |D|+v\,|a_{11}|^2,$$

hence $(1-v)\,|a_{11}|^2 \leqslant |D|$, and so

$$|a_{11}| \leqslant (1-v)^{-1/2}\sqrt{|D|} \leqslant w^{1/2}\sqrt{|D|}.$$

In the second case $f(x_1, x_2) = x_1(a_{11}x_1+2a_{12}x_2)$. In the Euclidean ring there is a number u, such that

$$0 < |a_{11}+2a_{12}u| \leqslant 2\,|a_{12}|, \quad \text{so} \quad 0 < |f(1,u)| \leqslant 2\,|a_{12}|.$$

Then

$$|a_{11}| \leqslant 2\,|a_{12}| = 4^{1/2}\sqrt{|D|} \leqslant w^{1/2}\sqrt{|D|}.$$

Now the proof for $n > 2$; we suppose that the statement is true for a smaller number of variables than n. We consider the reduced form $f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$. Then

$$\bar{f}(x_2, \ldots, x_n) = a_{11}f(x_1, \ldots, x_n) - \Big(\sum_{i=1}^{n} a_{1i}x_i\Big)^2$$

is also a reduced form; its first coefficient is $a_{11}a_{22}-a_{12}^2$ and its discriminant is $a_{11}^{n-2}D$ (see proof 1°). So according to the induction hypothesis

$$|a_{11}a_{22}-a_{12}^2| \leqslant w^{(n-2)/2}\sqrt[n-1]{|a_{11}|^{n-2}|D|}.$$

It is easy to see, that the form $a_{11}x_1^2+2a_{12}x_1x_2+a_{22}x_2^2$, whose discriminant is $a_{11}a_{22}-a_{12}^2$, is also a reduced form. So

$$|a_{11}| \leqslant w^{1/2}\sqrt{|a_{11}a_{22}-a_{12}^2|}.$$

Then

$$|a_{11}|^2 \leqslant w\,|a_{11}a_{22}-a_{12}^2| \leqslant w^{n/2}\sqrt[n-1]{|a_{11}|^{n-2}|D|},$$

which gives

$$|a_{11}|^n \leqslant w^{n(n-1)/2}|D|,$$

so that

$$|a_{11}| \leqslant w^{(n-1)/2}\sqrt[n]{|D|}.$$

3° For a reduced form in n variables, which is not a zero form, we find in the same way:

$$|a_{11}| \leqslant (1-v)^{-(n-1)/2}\sqrt[n]{|D|}.$$

Remark. A class of equivalent quadratic forms in n variables with discriminant D always contains a form with $|a_{11}| \leqslant (1-v)^{-(n-1)/2}\sqrt[n]{|D|}$.

If the forms of the class are zero forms, there is a form with $a_{11} = 0$ and for this it is true (but this form is not a reduced form in the sense of our definition).

As an important consequence of theorem 1 we have

THEOREM 2. *The number of classes of equivalent quadratic forms in n variables with a given discriminant is finite.*

Proof. According to theorem 1 every class contains a reduced form; so it is sufficient to prove, that the number of reduced forms in n variables with a given discriminant is finite. We prove this by induction. For $n = 1$ it is true. (For $n = 1$ and a given D there is one form: Dx_1^2.) Now let $f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ be a reduced form with discriminant D. It follows from

$$|a_{11}| \leqslant w^{(n-1)/2}\sqrt[n]{|D|}, \quad |a_{1i}| \leqslant |a_{11}|\sqrt{v} \quad (i = 2, \ldots, n),$$

that for a given D there is only a finite number of possible sets $a_{11}, \ldots, a_{1n}$. Next,

$$a_{11}f(x_1, \ldots, x_n) = \Big(\sum_{i=1}^{n} a_{1i}x_i\Big)^2 + \bar{f}(x_2, \ldots, x_n),$$

where $\bar{f}$ is again a reduced form. For given D and a_{11} the discriminant of $\bar{f}$ is determined ($a_{11}^{n-2}D$), so there is only a finite number of possibilities for $\bar{f}$ (induction hypothesis).

Then for a given D there is only a finite number of possibilities for f.

References

[1] J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer 1959, p. 31.

[2] J. F. Koksma, *Diophantische Approximationen*, Springer 1936.

[3] L. J. Mordell, *The arithmetically reduced indefinite quadratic forms in n variables*, Proc. Royal Soc. A 131 (1931), pp. 99-108.

[4] A. Oppenheim, *The arithmetical reduction of quadratic forms*, J. London Math. Soc. 6 (1931), pp. 222-226.

[5] — *The lower bounds of Hermitian quadratic forms in any quadratic field*, Proc. London Math. Soc. (2) 40 (1936), pp. 541-555.

[6] — *Über die Endlichkeit der Klassenzahl von ganzzahligen hermitischen Formen*, Monatshefte Math. Phys. 46 (1937), pp. 197-198.

[7] W. Landherr, *Über die arithmetische Reduktion quadratischer Formen*, J. London Math. Soc. 12 (1937), pp. 245-247.

[8] C. L. Siegel, *Einheiten quadratischer Formen*, Abh. Math. Sem. Hansischen Univ. 13 (1940), pp. 209-239.

[9] — *Discontinuous groups*, Annals of Math. 44 (1943), pp. 674-689.

[10] J. Heinhold, *Verallgemeinerung und Verschärfung eines Minkowskischen Satzes*, Math. Zeitschrift 44 (1939), pp. 659-688.

MATHEMATISCH CENTRUM AMSTERDAM

Reçu par la Rédaction le 20. 4. 1960

ACTA ARITHMETICA
VI (1961)

Über die Darstellung der Zahlen durch einige ternäre quadratische Formen

von

G. Lomadse (Tbilissi)

§ 1. In der vorliegenden Arbeit bezeichnen die Buchstaben M, N, a, d, k, q, r, λ, ω natürliche Zahlen (in § 4 bezeichnet jedoch q beliebige ganze Zahlen); b, u, v ungerade natürliche Zahlen; p Primzahlen; $\varkappa$, l nichtnegative ganze Zahlen; H, c, g, h, j, m, n, s, x, y, α, β, γ, δ ganze Zahlen; A, μ, ν, ϱ, σ, ξ, η, t, w reelle Zahlen; z, ζ, τ, A, B, C, D, G komplexe Zahlen, wobei $\operatorname{Im}\tau > 0$. Mit K werden positive Zahlen bezeichnet, die an den betreffenden Stellen definiert sind.

Diese Buchstaben werden nötigenfalls mit Indizes oder Strichen versehen.

(h, m) ist der größte gemeinsame Teiler von h und m.

$d \mid m$ bedeutet, daß d in m als Teiler aufgeht; $d \nmid m$, daß d nicht in m aufgeht; $p^l \| m$, daß $p^l \mid m$, aber $p^{l+1} \nmid m$.

$\left(\frac{h}{u}\right)$ ist das Jacobische Symbol für $(h, u) = 1$, $u > 1$; ist Null für $(h, u) > 1$; ist Eins für $u = 1$.

Weiter sei

$$e(z) = \exp 2\pi i z; \qquad I(u) = i^{(u-1)^2/4};$$

$$\operatorname{sgn}\xi = \begin{cases} \dfrac{\xi}{|\xi|} & \text{für} \quad \xi \neq 0, \\ 0 & \text{für} \quad \xi = 0, \end{cases}$$

In der Summe $\sum_{h \bmod q}$ durchläuft h ein vollständiges Restsystem $\bmod q$, in der Summe $\sum'_{h \bmod q}$ ein reduziertes System. Leere Summen sind gleich Null zu setzen, leere Produkte gleich Eins.

Für $z \neq 0$ sei

$$-\frac{\pi}{2} < \arg z^{1/2} \leqslant \frac{\pi}{2}, \qquad z^{k/2} = (z^{1/2})^k.$$