STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

ZW 1961- 15a

Unpublished results on number theory II

Composition theory of binary quadratic forms

S. Lubelski

Reprinted from
Acta Arithmetica, 7(1961), p 9-17

1961

ACTA ARITHMETICA
VII (1961)

Unpublished results on number theory II
Composition theory of binary quadratic forms

by

S. LUBELSKI †
Edited by C. SCHOGT (Amsterdam)

1. This second note gives an elementary exposition of the composition of binary quadratic forms. It is shown that the classical theory (¹) carries over to the case that the coefficients are taken from a (commutative) Euclidean ring (²).

Firstly, following Dirichlet and Dedekind, the forms to be compounded will be replaced by suitable equivalent ones, and it will be proved that this leads to a unique composition of the corresponding (proper) equivalence classes. In doing this, the use of quadratic congruences and, of course, of irrational numbers will be avoided. Next, a theorem on the decomposition of a given class will be deduced, and a characterization of ambiguous classes will be given. The connection in the classical case with ideal theory shall not be discussed (³).

Helpful advices were given by Dr. C. G. Lekkerkerker who also simplified the proof of theorem 5.

2. Let I be a Euclidean ring with characteristic $\neq 2$. Then in I factorization in prime elements is possible and unique, in the usual sense. The one-element will be written 1. We consider quadratic forms

$$f(x, y) = ax^2 + bxy + cy^2 \qquad (a, b, c, x, y \in I),$$

(¹) For the history of the subject the reader is referred to L. E. Dickson, *History of the theory of numbers*, Vol. III, New York 1934, ch. III, p. 60-79.

(²) Actually, the considerations of this note apply more generally to all principal ideal rings with characteristic $\neq 2$, which moreover are integral domains and in which the factorization property holds.

(³) It may be recalled that in that case there is a one-to-one correspondence between classes of forms and classes of ideals. See e.g. E. Landau, *Vorlesungen über Zahlentheorie*, Bd. III, Leipzig 1927, p. 187-196; B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Math. Monographs, No 10 (1950), p. 153-168. See also S. Lubelski, *Über Klassenzahlrelationen quadratischer Formen in quadratischen Körpern*, Journal reine ang. Math. 174 (1936), p. 160-184.

shortly denoted by $f = [a, b, c]$. Such a form is called *primitive* if the coefficients a, b, c are relatively prime. Further, $b^2 - 4ac$ is called the discriminant of the form. In the following we always suppose, without saying it explicitly, that our forms are *primitive forms whose discriminant has a fixed value* D.

We say that $m \in I$ is *represented properly* by a form f if there are $x, y \in I$ with

$$m = f(x, y), \quad (x, y) = 1.$$

Two forms f, g are called *properly* or *improperly equivalent* if f is transformed into g by a linear transformation $\binom{x}{y} = \begin{pmatrix}\alpha\beta\\ \gamma\delta\end{pmatrix}\binom{x'}{y'}$ whose determinant $\alpha\delta - \beta\gamma$ is 1 or a unit $\varepsilon \neq 1$ respectively. A form f is called *ambiguous* if it is improperly equivalent to itself; then, necessarily, $\varepsilon = -1$. Below we shall consider *classes of properly equivalent forms*, and denote them by C, C_1, C_2, etc.

It is well known that equivalent forms represent the same elements and that, if m is represented properly by f, there is a form g in the same class, which has first coefficient m ([4]).

3. We first prove the following

LEMMA 1. *If $m \neq 0$ is arbitrary, then any form $f = [a, b, c]$ represents properly a value $n \neq 0$, such that $(m, n) = 1$.*

Proof. Clearly, $a, c, a+b+c$ are represented properly by f. If m is a unit, then one of these elements may be taken as n. So we may suppose that m is not a unit.

Let $p_1, \ldots, p_r$ be the different prime factors of m. Each p_i is not a divisor of one at least of $a, c, a+b+c$, as these elements are relatively prime. So, for each p_i, there exist $x_i, y_i \in I$, such that

$$f(x_i, y_i) \not\equiv 0 \pmod{p_i}.$$

Now, since the Euclidean algorithm holds in I, the Chinese remainder theorem is valid in I. Then we can find x, y such that

$$x \equiv x_i \pmod{p_i}, \quad y \equiv y_i \pmod{p_i} \quad (i = 1, 2, \ldots, r).$$

Let δ be a g.c.d. of x, y. Then $x' = x/\delta$, $y' = y/\delta$ are relatively prime. Further $f(x, y) \not\equiv 0 \pmod{p_i}$, hence

$$f(x', y') \not\equiv 0 \pmod{p_i} \quad (i = 1, 2, \ldots, r).$$

Thus $n = f(x', y')$ fulfills the requirements.

([4]) Cf. lemma 1 in the first note on p. 218 (Acta Arith. 6 (1961), pp. 217-224).

We now deduce

THEOREM 1. *For each pair of classes C_1, C_2 (not necessarily different) there are forms $f_i \in C_i$ $(i = 1, 2)$ of the following type*

$$f_1 = [a_1, b, a_2 c], \quad f_2 = [a_2, b, a_1 c], \quad (a_1, a_2) = 1. \tag{1}$$

Proof. Take any form $f_1 = [a_1, b_1, c_1] \in C_1$ with $a_1 \neq 0$. Then, by lemma 1, any form $f_2 = [a_2, b_2, c_2] \in C_2$ represents properly a value $n \neq 0$ with $(a_1, n) = 1$. We may suppose that $f_2 \in C_2$ has already been chosen in such a way that $a_2 = n$.

We now observe that

$$b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2 = D,$$

so that

$$(b_1 + b_2)(b_1 - b_2) = b_1^2 - b_2^2 \equiv 0 \pmod 4. \tag{2}$$

Further, $b_1 + b_2 \equiv b_1 - b_2 \pmod 2$.

Now take any prime factor p of 2, and let p^s be the highest power of it, which divides 2. Then we must have

$$b_1 - b_2 \equiv 0 \pmod{p^s}.$$

For, if $b_1 - b_2 \not\equiv 0 \pmod{p^s}$, we should also have $b_1 + b_2 \not\equiv 0 \pmod{p^s}$, hence $b_1^2 - b_2^2 \not\equiv 0 \pmod{p^{2s}}$, in contradiction with (2). Since this is true for each prime factor of 2, it follows that

$$b_1 - b_2 \equiv 0 \pmod 2. \tag{3}$$

By (3), since $(a_1, a_2) = 1$, there are ξ_1, ξ_2 such that

$$a_1\xi_1 - a_2\xi_2 = -\frac{b_1 - b_2}{2}.$$

Transforming f_1 by $\begin{pmatrix} 1 & \xi_1 \\ 0 & 1 \end{pmatrix}$ and f_2 by $\begin{pmatrix} 1 & \xi_2 \\ 0 & 1 \end{pmatrix}$ we get two forms

$$[a_1, b', \gamma_1] \quad \text{and} \quad [a_2, b', \gamma_2],$$

where $b' = 2a_1\xi_1 + b_1 = 2a_2\xi_2 + b_2$ and γ_1, γ_2 satisfy

$$b'^2 - 4a_1\gamma_1 = b'^2 - 4a_2\gamma_2 = D,$$

so that $a_1\gamma_1 = a_2\gamma_2$. Since $(a_1, a_2) = 1$, γ_1 and γ_2 have the form

$$\gamma_1 = a_2c', \quad \gamma_2 = a_1c'.$$

Hence the transformed forms are of the required type.

The two forms f_i in (1) are closely related to the form

$$f = [a_1a_2, b, c]. \tag{4}$$

This is shown by the following identity of Lagrange

(5) $$(a_1x^2+bxy+a_2cy^2)(a_2x'^2+bx'y'+a_1cy'^2) = a_1a_2X^2+bXY+cY^2\,,$$

where

(6) $$X = xx'-cyy'\,,\qquad Y = a_1xy'+a_2x'y+byy'\,.$$

It is clear that f is again a primitive form with discriminant D. We agree to call f the *compound* of f_1 and f_2, and write

$$[a_1, b, a_2c]\cdot[a_2, b, a_1c] = [a_1a_2, b, c]\,.$$

Clearly, if m_1, m_2 are values of f_1, f_2 respectively, then m_1m_2 is a value of f.

LEMMA 2. *If $(m_1, m_2) = 1$ and m_1, m_2 are represented properly by f_1, f_2 respectively, then m_1m_2 is represented properly by f.*

Proof. Let the proper representations of m_1, m_2 be given by

$$a_1x^2+bxy+a_2cy^2 = m_1\,,\qquad a_2x'^2+bx'y'+a_1cy'^2 = m_2\,.$$

Eliminating x', y' from (6) we get

$$(a_1x^2+bxy+a_2cy^2)x' = (a_1x+by)X+cyY\,,$$
$$(a_1x^2+bxy+a_2cy^2)y' = -a_2yX+xY\,.$$

So a common factor of X, Y would be contained in m_1, because $(x', y') = 1$. Similarly, such a factor would be contained in m_2. Hence X, Y are relatively prime, whereas $f(X, Y) = m_1m_2$.

The compound is only defined for forms of the special type (1). But the main objective of composition theory is to compose classes, not forms. We now proceed to prove

THEOREM 2. *Let C_1, C_2 be given classes of forms. Then for each pair of forms $f_i \in C_i$ $(i = 1, 2)$ of the type (1) their compound f belongs to one fixed class C.*

We call C the *compound* of C_1 and C_2 and write $C = C_1C_2$.

Proof of theorem 2. We consider any two pairs of forms

$$f_1 = [g_1, h, g_2d]\,,\qquad f_2 = [g_2, h, g_1d]\,,$$
$$F_1 = [a_1, b, a_2c]\,,\qquad F_2 = [a_2, b, a_1c]\,,$$

such that

$$f_1, F_1 \in C_1;\qquad f_2, F_2 \in C_2;\qquad (g_1, g_2) = (a_1, a_2) = 1\,.$$

We shall prove that then $[g_1g_2, h, d]$ and $[a_1a_2, b, c]$ belong to the same class.

Let

$$f_1(x, y) = F_1(\alpha_1x+\beta_1y, \gamma_1x+\delta_1y)\,,\qquad f_2(x, y) = F_2(\alpha_2x+\beta_2y, \gamma_2x+\delta_2y)\,,$$

so that $\alpha_1\delta_1-\beta_1\gamma_1 = \alpha_2\delta_2-\beta_2\gamma_2 = 1$. A simple calculation gives

$$h\alpha_1 = 2g_1\beta_1+b\alpha_1+2a_2c\gamma_1\,,\qquad h\gamma_1 = 2g_1\delta_1-2a_1\alpha_1-b\gamma_1\,.$$

From $h^2-4g_1g_2d = b^2-4a_1a_2c = D$ it follows as in the proof of theorem 1 that

$$h-b \equiv h+b \equiv 0 \pmod 2 .$$

Then $\frac{h\pm b}{2}$ are elements of I, and we can write

$$g_1\beta_1 = \frac{h-b}{2}\alpha_1 - a_2c\gamma_1 , \qquad g_1\delta_1 = \frac{h+b}{2}\gamma_1 + a_1\alpha_1 .$$

Let ξ, η be the values of the expressions (6), where for x, y, x', y' we substitute $\alpha_1, \gamma_1, \alpha_2, \gamma_2$. Then we have

$$\begin{aligned}\frac{h-b}{2}\xi - c\eta &= \frac{h-b}{2}(\alpha_1\alpha_2 - c\gamma_1\gamma_2) - c(a_1\alpha_1\gamma_2 + a_2\alpha_2\gamma_1 + b\gamma_1\gamma_2)\\ &= \left(\frac{h-b}{2}\alpha_1 - a_2c\gamma_1\right)\alpha_2 - \left(\frac{h+b}{2}\gamma_1 + a_1\alpha_1\right)c\gamma_2\\ &= g_1(\beta_1\alpha_2 - c\delta_1\gamma_2) .\end{aligned}$$

For reasons of symmetry we also have

$$\frac{h-b}{2}\xi - c\eta = g_2(\alpha_1\beta_2 - c\gamma_1\delta_2) .$$

Then, since $(g_1, g_2) = 1$,

$$\frac{h-b}{2}\xi - c\eta \equiv 0 \pmod{g_1g_2} .$$

Similarly, one proves that

$$\frac{h+b}{2}\eta + a_1a_2\xi \equiv 0 \pmod{g_1g_2} .$$

So in I there are elements

$$\mu = \frac{(h-b)\xi - 2c\eta}{2g_1g_2} , \qquad \nu = \frac{(h+b)\eta + 2a_1a_2\xi}{2g_1g_2} .$$

Now $\begin{pmatrix}\xi & \mu\\ \eta & \nu\end{pmatrix}$ is a transformation with determinant 1 which transforms $[a_1a_2, b, c]$ into $[g_1g_2, h, d]$. This is easily verified if only one observes that, by (5),

$$a_1a_2\xi^2 + b\xi\eta + c\eta^2 = g_1g_2 .$$

The theorem is now proved.

4. We discuss some properties of the composition of classes. First we prove

THEOREM 3. *The classes form a commutative group, with the composition as group operation.*

Proof. It follows immediately from the definition that the composition of classes is commutative.

We now prove the associativity. Let C_1, C_2, C_3 be three classes. By theorem 1 and lemma 1 we can choose forms $f_i \in C_i$ $(i = 1, 2, 3)$ of the following type

$$f_1 = [a_1, b, a_2 c], \quad f_2 = [a_2, b, a_1 c], \quad f_3 = [a_3, b_3, c_3],$$

where a_1, a_2, a_3 are all $\neq 0$ and any two of them are relatively prime. Further $b - b_3$ is divisible by 2. Then there exist $\xi, \eta \in I$ such that

$$a_1 a_2 \xi - a_3 \eta = -\frac{b - b_3}{2}.$$

Transforming f_1 by $\begin{pmatrix} 1 & a_2\xi \\ 0 & 1 \end{pmatrix}$, f_2 by $\begin{pmatrix} 1 & a_1\xi \\ 0 & 1 \end{pmatrix}$, f_3 by $\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$ we get three forms of the following type:

$$(7) \qquad [a_1, b', c_1'], \quad [a_2, b', c_2'], \quad [a_3, b', c_3'].$$

Since $a_1 c_1' = a_2 c_2' = a_3 c_3'$ and any two of the a_i are relatively prime, we can write

$$c_1' = a_2 a_3 c', \quad c_2' = a_3 a_1 c', \quad c_3' = a_1 a_2 c'.$$

It is then clear that composing the three forms (7) we get the law

$$(C_1 C_2) C_3 = C_1 (C_2 C_3).$$

Next, we note that the forms representing 1 constitute a single class E. For $[1, b, c]$ is transformed into $[1, b', c']$ by the transformation $\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}$ with $\xi = -(b - b')/2$. If C is an arbitrary class, then in E, C we can choose forms f_1, f_2 of the type $f_1 = [1, b, ac]$, $f_2 = [a, b, c]$ (note that in theorem 1 we may require that a_1 is any element $\neq 0$ represented properly by f_1). Their compound is f_2. Hence,

$$CE = C.$$

Finally, two forms $[a, b, c]$ and $[c, b, a]$ have the compound $[ac, b, 1]$. Hence each class C has an inverse C^{-1}.

Another theorem on composition is given by

THEOREM 4. *Let $m \neq 0$ be represented properly by some form f, such that m and D are relatively prime. Let $m = p_1^{s_1} \dots p_r^{s_r}$ be a canonical decomposition of m. Then there are forms representing properly any p_i $(i = 1, 2, \dots, r)$. Further, if $C_1, \dots, C_r$ are the corresponding classes, then each form representing m properly belongs to a class of the type*

$$C = C_1^{\pm s_1} \dots C_r^{\pm s_r}.$$

Proof. The first assertion follows from the observation that if $[m_1m_2, b, c]$ is a primitive form with discriminant D, then so is $[m_1, b, m_2c]$. In order to prove the second assertion we distinguish first some special cases.

Case I. *m is a prime element p.* Let us consider two forms with first coefficient p, say

$$[p, q, r], \quad [p, q', r'].$$

Since both forms have discriminant D, we have

$$(q+q')(q-q') \equiv 0 \pmod{4p}.$$

Hence

$$q+q' \equiv 0 \pmod{2p} \quad \text{or} \quad q-q' \equiv 0 \pmod{2p}.$$

In the second case $[p, q, r]$ is properly equivalent to $[p, q', r']$, in the first case to $[p, -q', r']$ and so to $[r', q', p]$. We thus find that $[p, q', r']$ belongs to the same class as $[p, q, r]$ or to its inverse.

Case II. *m is a power of a prime element, say $m = p^s$.* Then p does not divide D. Let C_0 be a class containing some form $[p, q, r]$. We have

$$q^2 \equiv D \pmod{p}, \quad \text{hence} \quad q \not\equiv 0 \pmod{p}.$$

We first show that then the congruence

$$pt^2+qt+r \equiv 0 \pmod{p^k} \tag{8}$$

has a solution t for all positive integers k.

For $k=1$ the congruence reduces to $qt+r \equiv 0 \pmod{p}$ and so is solvable because of $q \not\equiv 0 \pmod{p}$. Suppose now that for some k there is a solution t_0. Taking $t = t_0+p^ky$ we have

$$pt^2+qt+r \equiv pt_0^2+qt_0+r+p^kqy \pmod{p^{k+1}}.$$

Clearly, we can choose y so that the expression on the right is $\equiv 0 \pmod{p^{k+1}}$. Hence (8) is solvable for all k.

Now take a solution t of (8), with $k = s-1$. The transformation $\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}$ transforms the form $[p, q, r]$ into the form

$$p(x+ty)^2+q(x+ty)y+ry^2 = px^2+(2pt+q)xy+(pt^2+qt+r)y^2.$$

It follows that C_0 contains a form of the type $[p, Q, p^{s-1}R]$. Then the class C_0^s contains the form

$$[p, Q, p^{s-1}R]^s = [p^s, Q, R], \tag{9}$$

as follows from the formula

$$[p, Q, p^{s-1}R]\cdot[p^i, Q, p^{s-i}R] = [p^{i+1}, Q, p^{s-i-1}R] \quad (i = 1, 2, \ldots, s-1).$$

Conversely, let us consider an arbitrary form $[p^s, Q', R']$. According to (9) it can be obtained from the form $[p, Q', p^{s-1}R']$; by what we have proved above, this last form belongs to C_0 or C_0^{-1}. It follows that any form $[p^s, Q', R']$ belongs to one of the classes $C_0^{\pm s}$.

General case. *m arbitrary.* Let $m = p_1^{s_1} \dots p_r^{s_r}$ and let $f_i \in C_i$ be a form representing p_i $(i = 1, 2, \dots, r)$. Then, by case II, there are forms $F_i \in C_i^{s_i}$ representing properly $p_i^{s_i}$ $(i = 1, 2, \dots, r)$. Then it follows from lemma 2 that there is a form in $C_1^{s_1} \dots C_r^{s_r}$ representing m properly. The same is true, of course, for each other class of the type $C_1^{\pm s_1} \dots C_r^{\pm s_r}$.

Conversely, consider any form $[m, Q, R]$. We have

$$[m, Q, R] = \left[p_1^{s_1}, Q, \frac{m}{p_1^{s_1}} R\right] \cdot \left[\frac{m}{p_1^{s_1}}, Q, p_1^{s_1} R\right]$$
$$= \dots = \prod_{i=1}^{r} \left[p_i^{s_i}, Q, \frac{m}{p_i^{s_i}} R\right] = \prod_{i=1}^{r} \left[p_i, Q, \frac{m}{p_i} R\right]^{s_i}.$$

It follows that $[m, Q, R]$ belongs to one of the classes $C_1^{\pm s_1} \dots C_r^{\pm s_r}$. This completes the proof of the theorem.

5. Finally, we deal with ambiguous classes. A class C is called *ambiguous*, if it contains an ambiguous form. Then each form in C is ambiguous. Further, if $f = [a, b, c]$ is a form in C, then also each form which is improperly equivalent to f, e.g. the form $[c, b, a]$. It follows that the ambiguous classes C are characterized by the relation

$$C = C^{-1}.$$

Another characterization is given by

THEOREM 5. *Suppose that $D \neq 0$. Then the ambiguous classes are those containing a form of the type $[a, a\varrho, c]$. Here ϱ can be taken in a given residue system* mod 2.

Proof. Let C be an ambiguous class. Let $f = [a, b, c]$ be any form in C and let A denote the matrix $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$, so that $\det A \neq 0$. Further, let T be a transformation with determinant -1 leaving f invariant. Then we have (the symbol * denoting the passage to the transposed matrix)

$$T^* A T = A, \quad \det T = -1. \tag{10}$$

We first deduce from (10) that $\operatorname{sp} T = 0$. In fact, if B is the adjoint matrix of A, then [5] $(\det A) \cdot T = BAT = BT^{*-1}A$, hence

$$\det A \cdot \operatorname{sp} T = \operatorname{sp}(BT^{*-1}A) = \operatorname{sp}(ABT^{*-1}) = \det A \cdot \operatorname{sp} T^{*-1},$$

and so

$$\operatorname{sp} T = \operatorname{sp} T^{*-1},$$

---

[5] We can take the inverse of T^*, as $\det T$ is a unit.

since $\det A \neq 0$. One easily deduces from $\det T = -1$, that $\operatorname{sp} T^{*-1} = -\operatorname{sp} T$. So one finds $\operatorname{sp} T = 0$.

Next, we prove the existence of a matrix S such that

$$\det S = 1\,, \quad S^{-1}TS = \begin{pmatrix} 1 & \varrho \\ 0 & -1 \end{pmatrix} \quad (\varrho \in I)\,. \tag{11}$$

Since $\det T = -1$ and $\operatorname{sp} T = 0$, the characteristic equation of T reads $\xi^2 - 1 = 0$, and so T has two eigenvalues ± 1. Then there is an eigenvector $X = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ with $TX = X$ and $(\alpha, \beta) = 1$. Further, there are elements γ, δ with $\alpha\delta - \beta\gamma = 1$. Then, since $\det T = -1$, the matrix $S = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ satisfies (11).

Now S transforms f into a form g which is invariant under the transformation $S^{-1}TS = \begin{pmatrix} 1 & \varrho \\ 0 & -1 \end{pmatrix}$. One easily finds that then g is of the type $[a, a\varrho, c]$. Conversely, a form of this type is invariant under the transformation $\begin{pmatrix} 1 & \varrho \\ 0 & -1 \end{pmatrix}$. This proves the first assertion. The second assertion now follows from the fact that two forms $[a, a\varrho, c]$, $[a, a\varrho', c']$ are equivalent if $\varrho \equiv \varrho' \pmod 2$.

MATHEMATISCH CENTRUM, AMSTERDAM

Reçu par la Rédaction le 31. 10. 1960