Literaturverzeichnis

[1] P. Billingsley, *Ergodic Theory and Information*, New York-London-Sydney 1965.

[2] W. Doeblin, *Remarques sur la théorie metrique de fractions continues*, Compositio Math. 7 (1940), S. 353-371.

[3] I. S. Gal and J. F. Koksma, *Sur l'ordre de grandeur des fonctions sommables*, Proc. Akad. Amsterdam 53 (1950), S. 638-653.

[4] S. Hartman, E. Marczewski et C. Ryll-Nardzewski, *Théorèmes ergodiques et leurs applications*, Coll. Math. 2 (1951), S. 109-123.

[5] A. Ya. Khintchine, *Continued Fractions*, Groningen 1963.

[6] W. Philipp, *Some metrical theorems in number theory*, Pacific J. Math. 20 (1967), S. 109-127.

[7] A. Rényi, *Representations for real numbers and their ergodic properties*, Acta Math. Ac. Sci. Hung. 8 (1957), S. 477-493.

[8] V. A. Rohlin, *Exact endomorphismus of a Lebesgue space*, Izv. Akad. Nauk SSSR, Ser. Mat. 25 (1961), S. 499-530 (Russian), English Transl.: Amer. Math. Soc. Trans. (2) 39, S. 1-36.

[9] P. Roos, *Iterierte Resttransformationen von Zahlendarstellungen*, Z. Wahrscheinlichkeitstheorie 4 (1965), S. 45-63.

[10] C. Ryll-Nardzewski, *On the generalized ergodic theorems*, Studia Math. 12 (1951), S. 65-73.

[11] — *On the ergodic theory of continued fractions*, Studia Math. 12 (1951), S. 74-79.

[12] F. Schweiger, *Ein Kuzminscher Satz über den Jacobischen Algorithmus*, Erscheint im Journal für Reine und Angewandte Mathematik.

[13] P. Szüsz, *Über einen Kuzminschen Satz*, Hungar. Acta Math. 12 (1961), S. 447-453.

Reçu par la Rédaction le 23. 10. 1967

ACTA ARITHMETICA
XV (1968)

A note on factorizations in quadratic fields

by

W. Narkiewicz (Wrocław)

1. In [1] and [2] the following result was obtained:

If K is a quadratic number field with the class-number $h \neq 1, 2$ moreover k and l are natural numbers and $D = (k, l)$ has all its factorizations into integers irreducible in K of the same length, then for the number $G_{k,l}(x)$ of the rational positive integers not exceeding x, congruent to $l \pmod k$ and having all factorizations into integers irreducible in K with the same length one has the following asymptotic evaluation:

$$G_{k,l}(x) \sim C(k, l, K)x(\log\log x)^N(\log x)^{(1+S(D)-h)/2h},$$

where $C(k, l, K)$ is a positive constant, N is a nonnegative rational integer depending on the class-group H of K, and finally $S(D)$ is a rational integer satisfying the inequality $0 \leqslant S(D) \leqslant g$, with g equal to the number of even invariants of H.

In the case $D = 1$ it was shown that $S(1) = g$, and it was conjectured that the equality $S(D) = g$ holds for every D.

This conjecture was shown to be false by A. Schinzel, who produced the following counterexample: $K = Q(\sqrt{-14})$, $D = 9$ in which case $H \simeq C_4$, thus $g = 1$, but $S(9) = 0$.

The aim of the present note is to characterize all those quadratic fields K for which $S(D)$ does not depend on D, and so is equal to g. (We assume that D satisfies the condition stated above, as otherwise the number $S(D)$ is undefined.) We prove the following

THEOREM. *The equality $S(D) = g$ holds for every D (subject to the condition stated above) if and only if either the field K has an odd class-number, or its class-group H has the form $C_2 \times C_2 \times \ldots \times C_2$.*

At first we recall some definitions and notations introduced in [1]. Let $C_{h_1} \times \ldots \times C_{h_r}$ be a factorization of the class-group H into cyclic groups and let X_i be the generator of C_{h_i} for $i = 1, 2, \ldots, r$. For a given rational integer a and $i = 1, 2, \ldots, r$ define

$$[a]_i = \begin{cases} h_i - a & \text{if} \quad a \neq 0, \\ 0 & \text{if} \quad a = 0 \end{cases}$$

and consider the set T of all r-tuples $(a_1, \dots, a_r)$ of nonnegative rational integers (not all equal to zero), satisfying the following conditions:

(i) $0 \leqslant a_i \leqslant h_i - 1$ $(i = 1, 2, \dots, r)$,

(ii) $a_1 \leqslant [a_1]_1$ and if for $i = 1, 2, \dots, t-1$ (with some t) one has $a_i = [a_i]_i$, then $a_t \leqslant [a_t]_t$.

As observed in [1], the mapping

$$(a_1, \dots, a_r) \to (X_1^{a_1} \dots X_r^{a_r}, X_1^{-a_1} \dots X_r^{-a_r})$$

gives a one-to-one correspondence between T and the set of all orbits of H under the action of the Galois group C_2 of K, distinct from the orbit (E, E) (where E is the unit element of H). A rational prime p which does not generate a prime ideal in K is said to *belong to the orbit* (X, X^{-1}) if $p = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \in X$, $\mathfrak{p}_2 \in X^{-1}$.

Now let $a^{(i)} = (a_1^{(i)}, \dots, a_r^{(i)}) \in T$ for $i = 1, 2, \dots, n$, and assume that the distinct r-tuples $a^{(1)}, \dots, a^{(s)}$ $(s \geqslant 0)$ correspond to orbits of the form (X, X), i.e. $2a_j^{(i)} \equiv 0 \pmod{h_j}$ for $i = 1, 2, \dots, s$ and $j = 1, 2, \dots, r$, whereas the remaining r-tuples do not share this property. For any rational integer m let us denote by $\Omega_i(m)$ the number of prime divisors of m belonging to the orbit corresponding to $a^{(i)}$, each divisor counted according to its multiplicity. Let finally $A_{s+1}, \dots, A_n$ be given positive rational integers.

We shall say, the system $V = (a^{(1)}, \dots, a^{(n)}; A_{1+s}, \dots, A_n)$ is *admissible* if it satisfies the condition

(iii) For every two different sequences $(\varepsilon_1, \dots, \varepsilon_n)$, $(\eta_1, \dots, \eta_n)$ with $0 \leqslant \varepsilon_i, \eta_i \leqslant 1$ for $i = 1, 2, \dots, s$ and $0 \leqslant \varepsilon_i, \eta_i \leqslant A_i$ for $i = s+1, \dots, n$ there exists an index j such that

$$\sum_{k=1}^{n} \varepsilon_k a_j^{(k)} \not\equiv \sum_{k=1}^{n} \eta_k a_j^{(k)} \pmod{h_j}.$$

We shall say also that the admissible system V is *D-admissible* if for $i = 1+s, \dots, n$ one has $\Omega_i(D) \leqslant A_i$ and moreover every prime divisor of D either generates a prime ideal in K, or belongs to one of the orbits corresponding to $a^{(1)}, \dots, a^{(n)}$ or finally belongs to the orbit (E, E).

It was shown in [1] that $S(D) = \max_V s(V)$ where V ranges over all D-admissible systems.

2. Proof of the theorem. The case of odd h is trivial, as then $0 \leqslant S(D) \leqslant g = 0$, hence we may assume in the sequel that h is even.

We introduce now a partial order in the set of all admissible systems by defining

$$V_1 = (a^{(1)}, \dots, a^{(n)};\ A_{1+s}, \dots, A_n) \leqq V_2 = (b^{(1)}, \dots, b^{(m)}; B_{1+s_1}, \dots, B_m)$$

if $\{a^{(1)}, \dots, a^{(n)}\} \subset \{b^{(1)}, \dots, b^{(m)}\}$ and moreover the equality $a^{(j)} = b^{(k)}$ for some j, k implies $A_j \leqslant B_k$.

Observe that for every D there exists a minimal D-admissible system $V(D)$ such that for every D-admissible system V one has $V(D) \leqq V$. In fact let $a^{(1)}, \dots, a^{(n)}$ be the r-tuples from T such that $\Omega_i(D) \geqslant 1$ for $i = 1, 2, \dots, n$, ordered in such a way that $a^{(1)}, \dots, a^{(s)}$ are all of them which correspond to orbits of the form (X, X), and define

$$V(D) = \big(a^{(1)}, \dots, a^{(n)};\ \Omega_{1+s}(D), \dots, \Omega_n(D)\big).$$

As it was assumed that D has all its factorizations of the same length, Lemma 3 of [1] implies that $V(D)$ is admissible, and its D-admissibility and minimal property follows immediately.

Note also that every admissible system V is of the form $V = V(D)$ for some D. In fact, if $V = (a^{(1)}, \dots, a^{(n)}; A_{s+1}, \dots, A_n)$ then take $D = p_1 \dots p_s p_{s+1}^{A_{s+1}} \dots p_n^{A_n}$, where for $i = 1, \dots, n$ the number p_i is a rational prime belonging to the orbit corresponding to the r-tuple $a^{(i)}$.

Finally note, that if V is D-admissible, and $V \leqq V_1$, then V_1 is also D-admissible.

Now we prove

(i) *The equality $S(D) = g$ holds for all D if and only if to every admissible system V there exists an admissible system V_1 with $V \leqq V_1$ and $s(V_1) = g$.*

Proof. Assume the equality $S(D) = g$ for all D, and let V be admissible. For some D, $V = V(D)$. As $S(D) = g$ there is a D-admissible system V_1 with $s(V_1) = g$, and the remark made above shows that $V \leqq V_1$.

Conversely, let D have all its factorizations of the same length, and consider $V = V(D)$, which is admissible by Lemma 3 of [1], and let V_1 be admissible and such that $s(V_1) = g$, and $V \leqq V_1$. As V_1 is D-admissible, $S(D) = g$ follows.

Now we can establish one part of our theorem:

(ii) *If $H \simeq C_2 \times \dots \times C_2$, then $S(D) = g$ holds for all D.*

Proof. In this case every r-tuple from T is of the form $(\varepsilon_1, \dots, \varepsilon_g)$ with $\varepsilon_i = 0, 1$, and so, after adjoining the r-tuple $(0, 0, \dots, 0)$, we may treat T as g-dimensional vector space over the field GF(2). From the definition of admissibility follows that a system $(a^{(1)}, \dots, a^{(m)})$ is admissible if and only if it is linearly independent. Moreover in our case the relations $V_1 \leqq V_2$ and $V_1 \subset V_2$ coincide, whence the equality $S(D) = g$ follows from (i) and the fact that every independent system in T can be extended to a basis, necessarily of g elements.

To prove the remaining part of our theorem let $H = C_{h_1} \times \dots \times C_{h_r}$ (where $h_1, \dots, h_g$ are even and $h_{g+1}, \dots, h_r$ are odd), with $g \geqslant 1$ and $\max_j h_j \geqslant 3$. Note that the system $V = \big((1, 1, \dots, 1); N-1\big)$ with $N = \text{l.c.m.}(h_1, \dots, h_r)$ is admissible, as the congruences $x \equiv y \pmod{h_i}$

for $i = 1, 2, \ldots, r$ imply $x \equiv y \pmod N$. The theorem will be proved if we show that no system $V_1 = \left(a^{(1)}, \ldots, a^{(g)}, (1, 1, \ldots, 1); A\right)$ with $A \geqslant N-1$ and $a^{(i)}$ corresponding for $i = 1, 2, \ldots, g$ to orbits of the form (X, X) can be admissible. Assume the contrary, and let

$$a^{(i)} = (\varepsilon_1^{(i)} h_1/2, \ldots, \varepsilon_g^{(i)} h_g/2, 0, \ldots, 0) \quad \text{with} \quad \varepsilon_j^{(i)} = 0, 1.$$

The vectors $\bar{e}_i = (\varepsilon_1^{(i)}, \ldots, \varepsilon_g^{(i)})$ are linearly independent over GF(2) (due to admissibility of V_1), thus we can find $\eta_1, \ldots, \eta_g = 0, 1$ such that with $M = \text{l.c.m.}\,(h_1/2, \ldots, h_g/2, h_{g+1}, \ldots, h_r)$ and some integral $n_1, \ldots, n_g$

$$\eta_1 \bar{e}_1 + \ldots + \eta_g \bar{e}_g = (2n_1 + 2M/h_1, \ldots, 2n_g + 2M/h_g).$$

Now an easy checking shows us that the kth component of

$$\eta_1 a^{(1)} + \ldots + \eta_g a^{(g)} + M(1, 1, \ldots, 1)$$

is congruent to zero $(\bmod h_k)$ for $k = 1, 2, \ldots, r$, which in view of admissibility of V_1 implies $M > A$, but clearly $M \leqslant N/2$, and as $A \geqslant N-1$, we obtain a contradiction. The theorem is thus proved.

References

[1] W. Narkiewicz, *On natural numbers having unique factorization in a quadratic number field*, Acta Arith. 12 (1966), pp. 1-22.

[2] — — II, ibidem, 13 (1967), pp. 123-139.

MATHEMATICS INSTITUTE OF THE WROCŁAW UNIVERSITY

Reçu par la Rédaction le 7. 11. 1967

ACTA ARITHMETICA
XV (1968)

Modules and binary quadratic forms

by

HUBERT S. BUTTS and GORDON PALL* (Baton Rouge, La.)

1. Introduction. The basic result of this article is Theorem 6.1, which gives an algorithm whereby the transformations T of a primitive binary quadratic form f into a multiple $e \cdot g$ of a primitive binary quadratic form g are uniquely related to representations of e by one of two specific forms according as $e(\det T)$ is positive or negative. Allowing e to vary, one deduces certain remarkable additive properties of the transformations of a binary quadratic form into an arbitrary multiple of another. These, it may be mentioned, are useful in a new theory of reduction of the quaternary quadratic forms which arise as norm forms of modules in quaternion rings.

The article developed when we sought to interpret these phenomena in connection with modules in a quadratic field. This led us to re-examine the Dedekind relations between classes of modules (or ideals) in a quadratic field under multiplication and classes of binary quadratic forms under composition. It appeared that Dedekind had somewhat artificially forced the one-one association between module and form classes, by adopting a different convention for definite and indefinite forms, by restricting bases artificially, and by defining a narrow module equivalence. Technically what he did was correct. But he did obscure the essential simplicity of the relationship, which we will describe in § 3, and which seems to us to be more natural and still pleasing. Our approach generalizes better. Dickson's *History of the Theory of Numbers* lists on p.70 of Vol. III several items concerned with the Dedekind relation (H. Weber [15], R. König [11], J. Sommer [14], who mentions in § 35 a paper by E. E. Kummer [10], P. Bachmann [1], R. Fricke [6]). Subsequent items that we know of are due to E. Hecke [8], E. Landau [12], and Z. I. Borevich and I. R. Shafarevich [2].

---

* This work was supported in part by National Science Foundation grants GP 6467 and GP 3956.