

Remark. As we noted, the assumption (*) is valid for $n = 2$ and 3 , and κ in Theorem is $5/2, 8/3$ for $n = 2, 3$, respectively [8]. Thus in the case of $n = 2$ the assumptions needed in Theorem are $dN > (\min N)^{32.2}$ and the sufficient size of $\min N$ as in the introduction.

References

- [1] J. S. Hsia, Y. Kitaoka, M. Kneser, *Representations of positive definite quadratic forms*, J. Reine Angew. Math. 301 (1978), 132–141.
 [2] Y. Kitaoka, *Lectures on Siegel modular forms and representation by quadratic forms*, Tata Institute of Fundamental Research, Bombay; Springer, Berlin–Heidelberg–New York, 1986.
 [3] — *Local densities of quadratic forms*, in: *Investigations in Number Theory*, Advanced Studies in Pure Math. 13, 1987, 433–460.
 [4] — *Modular forms of degree n and representation by quadratic forms II*, Nagoya Math. J. 87 (1982), 127–146.
 [5] — *Modular forms of degree n and representation by quadratic forms IV*, *ibid.* 107 (1987), 25–47.
 [6] — *Modular forms of degree n and representation by quadratic forms V*, to appear in Nagoya Math. J.
 [7] O. T. O'Meara, *Introduction to quadratic forms*, Springer, Berlin–Heidelberg–New York 1963.
 [8] G. L. Watson, *Quadratic diophantine equations*, Philos. Trans. Roy. Soc. London Ser. A 253 (1960/61), 227–254.

DEPARTMENT OF MATHEMATICS
 FACULTY OF SCIENCE
 NAGOYA UNIVERSITY
 Chikusa-ku, Nagoya, 464-01
 Japan

Received on 2.5.1988

and in revised form on 25.8.1988

(1822)

On Eisenstein's problem

by

NOBURO ISHII* (Osaka), PIERRE KAPLAN** (Nancy)
 and KENNETH S. WILLIAMS*** (Ottawa)

1. Introduction. Let D be a positive nonsquare integer such that $D \equiv 1 \pmod{4}$. In this paper we shall be concerned with the solvability or insolvability of the equation

$$(1.1) \quad T^2 - DU^2 = +4$$

in coprime integers T and U (equivalently in odd integers T and U). If there are odd integers T and U satisfying $T^2 - DU^2 = 4$ we say that (1.1) has odd solutions, and if there are no odd integers T and U satisfying $T^2 - DU^2 = 4$ we say that (1.1) has no odd solution. When $D \equiv 1 \pmod{8}$ simple congruence considerations modulo 8 show that (1.1) has no odd solution. When $D \equiv 5 \pmod{8}$ the equation (1.1) may ($D = 5$) or may not ($D = 37$) have odd solutions.

In 1844 Eisenstein [1] asked for a necessary and sufficient condition for (1.1) to have odd solutions. In fact Gauss in his *Disquisitiones Arithmeticae* (1801) (see [2], §256, VI) had already mentioned this problem, in a slightly different setting, and given the list of all $D \equiv 5 \pmod{8}$, $D < 1000$, for which (1.1) has no odd solution.

When the equation

$$(1.2) \quad V^2 - DW^2 = -1$$

is solvable a necessary and sufficient condition for the solvability of (1.1) in odd integers was given recently by Kaplan and Williams [5], in terms of the lengths l and l^* of the continued fraction expansions of \sqrt{D} and $(1 + \sqrt{D})/2$ respectively (see Theorem 0 below). It was known that $l \equiv l^* \pmod{2}$, and also that $l \equiv l^* \equiv 1 \pmod{2}$ if, and only if, (1.2) is solvable.

* Research supported by the Government of Japan.

** Research supported by the Government of Canada.

*** Research supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

THEOREM 0. *Let $D \equiv 1 \pmod{4}$ be a positive nonsquare integer such that (1.2) is solvable. Then the equation (1.1) has odd solutions if, and only if, $l \equiv l^* \pmod{4}$.*

The following corollary is an immediate consequence of Theorem 0.

COROLLARY. *If $D \equiv 1 \pmod{8}$ is a positive nonsquare integer such that (1.2) is solvable then $l \equiv l^* + 2 \pmod{4}$.*

In this paper we use the theory of integral indefinite binary quadratic forms to treat the solvability of (1.1) in odd integers. We state our results in terms of the lengths L_0 and L_0^* of the principal periods of reduced integral binary quadratic forms of discriminants $4D$ and D . These terms will be explained in Section 2. It suffices to remark here that,

$$(1.3) \quad \begin{cases} L_0 = l, & L_0^* = l^*, & \text{if (1.2) is insolvable,} \\ L_0 = 2l, & L_0^* = 2l^*, & \text{if (1.2) is solvable,} \end{cases}$$

and to note that L_0 and L_0^* are always even.

Our first result (Section 2) contains the following theorem as a special case.

THEOREM 1. $L_0 \equiv L_0^* \pmod{4}$.

We emphasize that Theorem 1 depends neither upon the solvability of (1.1) in odd integers, nor upon the solvability of (1.2). When (1.2) is solvable Theorem 1 reduces to $l \equiv l^* \pmod{2}$, and when (1.2) is insolvable it has been proved by Halter-Koch [3] when D is squarefree.

Our second main result (Section 4) concerns the case when (1.1) has odd solutions.

THEOREM 2. (a) *Let D be an integer > 5 such that $D \equiv 5 \pmod{8}$ and such that the equation (1.1) has odd solutions. Then $L_0^* + 4 \leq L_0 \leq 5L_0^*$.*

(b) *If, furthermore, the equation (1.2) is solvable then $L_0^* + 8 \leq L_0 \leq 5L_0^*$.*

Table 1 below gives a few values of D illustrating Theorem 2(a), and Table 2 a few values illustrating Theorem 2(b).

Table 1

$D \equiv 5 \pmod{8}$ (1.1) has odd solutions	L_0	L_0^*	$L_0^* + 4$	$5L_0^*$
501	28	8	12	40
509	38	14	18	70
517	22	10	14	50
525	6	2	6	10
533	10	2	6	10
541	78	22	26	110
549	18	6	10	30
565	26	10	14	50
581	24	8	12	40
589	40	16	20	80
597	22	10	14	50

Table 2

$D \equiv 5 \pmod{8}$ (1.1) has odd solutions (1.2) solvable	L_0	L_0^*	$L_0^* + 8$	$5L_0^*$
733	10	2	10	10
773	22	6	14	30
797	22	14	22	70
821	58	18	26	90
845	10	2	10	10
853	46	14	22	70
941	34	10	18	50
949	54	14	22	70

We note that (b) results from (a) and Theorem 0, but we shall prove Theorem 2(b) directly, without appealing to Theorem 0.

When the equation (1.1) has no odd solution we prove a result (Theorem 6 in Section 6) which includes the following result.

THEOREM 3. *Let $D \equiv 1 \pmod{4}$ be a positive nonsquare integer such that the equation (1.1) has no odd solution. Then*

$$L_0^*/3 \leq L_0 \leq 3L_0^* - 8.$$

A few values of $D \equiv 5 \pmod{8}$ illustrating Theorem 3 are given in Table 3 below.

Table 3

$D \equiv 5 \pmod{8}$ (1.1) has no odd solution	L_0	L_0^*	$L_0^*/3$	$3L_0^* - 8$
813	6	6	2	10
829	34	38	12.66	106
877	30	18	6	46
885	4	4	1.33	4
901	2	6	2	10
909	8	12	4	28
925	10	14	4.66	34
933	8	12	4	28
997	26	14	4.66	34

Since (1.1) is always insolvable in odd integers when $D \equiv 1 \pmod{8}$, we have the following corollary to Theorem 3.

COROLLARY 1. *If D is a positive nonsquare integer such that $D \equiv 1 \pmod{8}$ then $L_0^*/3 \leq L_0 \leq 3L_0^* - 8$, equivalently*

$$l^*/3 \leq l \leq 3l^* - 4, \quad \text{if } V^2 - DW^2 = -1 \text{ is solvable,}$$

$$l^*/3 \leq l \leq 3l^* - 8, \quad \text{if } V^2 - DW^2 = -1 \text{ is insolvable.}$$

Table 4

$D \equiv 1 \pmod{8}$				
$V^2 - DW^2 = -1$ solvable	l	l^*	$l^*/3$	$3l^* - 4$
185	5	3	1	5
401	1	3	1	5
409	21	27	9	77
425	7	5	1.66	11
$D \equiv 1 \pmod{8}$				
$V^2 - DW^2 = -1$ insolvable	l	l^*	$l^*/3$	$3l^* - 8$
105	2	6	2	10
369	12	16	5.33	40
377	4	4	1.33	4
385	16	12	4	28
393	20	16	5.33	40

The next two corollaries follow from Theorems 1, 2 and 3.

COROLLARY 2. *Let $D \equiv 1 \pmod{4}$ be a positive nonsquare integer (> 5) such that $L_0^* = 2$. Then the equation (1.1) has odd solutions and $L_0 = 6$ or $L_0 = 10$. If, moreover, (1.2) is solvable, then $L_0 = 10$.*

We remark that if $L_0^* = 2$, Proposition 5 of Section 7 gives a criterium for $L_0 = 6$ or 10.

COROLLARY 3. *Let $D \equiv 1 \pmod{4}$ be a positive nonsquare integer such that (1.2) is insolvable and $L_0^* \geq 4$. Then, if $L_0 \leq L_0^*$ the equation (1.1) has no odd solution whereas if $L_0 \geq 3L_0^* - 4$ the equation (1.1) has odd solutions.*

We note that if $D = 69$ then (1.1) has odd solutions ($T = 25, U = 3$) and $L_0 = 8, L_0^* = 4$ showing that the inequality $L_0 \leq L_0^*$ in Corollary 3 cannot be replaced by $L_0 \leq L_0^* + 4$. Also, if $D = 189$, then (1.1) has no odd solution and $L_0 = L_0^* = 4$ showing that the inequality $L_0 \geq 3L_0^* - 4$ in Corollary 3 cannot be replaced by $L_0 \geq 3L_0^* - 8$.

2. The congruence $L_0 \equiv L_0^* \pmod{4}$. We consider integral binary quadratic forms

$$(2.1) \quad f = f(x, y) = ax^2 + bxy + cy^2 = [a, b, c]$$

of discriminant $\Delta = b^2 - 4ac$, where Δ is equal to $4D$ or D . All forms $[a, b, c]$ are assumed to be primitive, that is $\text{GCD}(a, b, c) = 1$. If f denotes the form

$[a, b, c]$, we use \tilde{f} to denote the form $[c, b, a]$. The matrix of the form $f = [a, b, c]$ is $F = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$. An ambiguous form is a form $[a, b, c]$ with $a|b$. A form $[a, b, c]$ of discriminant $\Delta > 0$ is said to be reduced (see [2], § 183) if it satisfies the inequalities

$$(2.2) \quad 0 < \sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b,$$

or equivalently

$$(2.3) \quad 0 < \sqrt{\Delta} - b < 2|c| < \sqrt{\Delta} + b.$$

If the form $[a, b, c]$ is reduced then

$$(2.4) \quad \begin{cases} ac < 0, b > 0, \\ |a|, b, |c| < \sqrt{\Delta}, \end{cases}$$

and the form can be rewritten as

$$f = [\varepsilon a, b, -\varepsilon c]$$

with $a > 0, b > 0, c > 0, \varepsilon = \pm 1$.

Two forms $f = [a, b, c]$ and $f' = [a', b', c']$ are said to be *equivalent*, written $f \sim f'$, if there exists an integral 2×2 matrix M of determinant $+1$ such that $F' = M^T F M$. The class of forms equivalent to the principal form of discriminant Δ

$$[1, 0, -D], \quad \text{if } \Delta = 4D; \quad \left[1, 1, -\frac{(D-1)}{4} \right], \quad \text{if } \Delta = D,$$

is called the *principal class*.

The set of classes of a given discriminant Δ forms a finite abelian group G_Δ under gaussian composition, whose unit element is the principal class. There exists a surjective homomorphism $\theta: G_{4D} \rightarrow G_D$ which has the following property:

Each class of G_{4D} contains forms of the type $[a, 2b, 4c]$ and of the type $[4a', 2b', c']$. If we denote by $\{r, s, t\}$ the class of the form $[r, s, t]$, then

$$(2.5) \quad \begin{cases} \theta(\{a, 2b, 4c\}) = \{a, b, c\}, \\ \theta(\{4a', 2b', c'\}) = \{a', b', c'\}. \end{cases}$$

The kernel of θ is the subgroup of G_{4D} consisting of the classes representing properly 1 or 4, and

$$(2.6) \quad \text{card}(\ker \theta) = \begin{cases} 3, & \text{if } D \equiv 5 \pmod{8} \text{ and (1.1) has no odd solution,} \\ 1, & \text{if } D \equiv 1 \pmod{8} \text{ or if (1.1) has odd solutions,} \end{cases}$$

(see [2], § 256, [4], p. 127, [6], § 150-151).

Let $f = [\varepsilon a, b, -\varepsilon c]$ be a reduced form of discriminant Δ , and let the integer $t(f)$ and the matrix $T(f)$ be defined by

$$(2.7) \quad t(f) = -\varepsilon \left[\frac{b + \sqrt{\Delta}}{2c} \right], \quad T(f) = \begin{bmatrix} 0 & -1 \\ 1 & t(f) \end{bmatrix},$$

where, for a real number α , $[\alpha]$ denotes the unique integer such that

$$[\alpha] \leq \alpha < [\alpha] + 1.$$

Then the form $f' = [-\varepsilon c, b', \varepsilon a']$ obtained from f by means of the transformation of matrix $T(f)$ is reduced. Moreover, $t(f)$ is the only integer t such that the transformation of matrix $\begin{bmatrix} 0 & -1 \\ 1 & t \end{bmatrix}$ transforms f into a reduced form. The form f' is said to be the *right neighbouring form to f* , and we denote this relation by $f \approx f'$. In addition one has

$$(2.8) \quad t(f) = -\varepsilon \frac{(b+b')}{2c} = -\varepsilon \left[\frac{b'+\sqrt{\Delta}}{2c} \right].$$

If an initial reduced form f_0 is specified in a class C of discriminant Δ , the reduced forms make a periodic sequence $\{f_n\}$ such that $f_n \approx f_{n+1}$. The length of the period of this sequence is always even.

We shall compare the period of a class of discriminant $4D$ with the period of its image by θ ; our main results will be obtained by comparing the principal classes. The length of a period of discriminant $4D$ will be denoted by L and the length of its image by θ by L^* . The length of the period of the principal class of discriminant $4D$ (respectively D) will be denoted by L_0 (respectively L_0^*). The reduced forms of classes corresponding by θ will usually be denoted by

$$f_n = [\varepsilon a_{n-1}, 2b_n, -\varepsilon a_n], \quad n = 0, \dots, L-1, \quad (\Delta = 4D),$$

$$g_m = [\varepsilon' a'_{m-1}, b'_m, -\varepsilon' a'_m], \quad m = 0, \dots, L^*-1, \quad (\Delta = D),$$

so that a_n, b_n, a'_m, b'_m are positive integers such that

$$(2.9) \quad D = b_n^2 + a_{n-1}a_n = b'_m{}^2 + 4a'_{m-1}a'_m.$$

As the forms f_n and g_m are primitive and $D \equiv 1 \pmod{4}$ we see that

$$(2.10) \quad \begin{cases} b_n \equiv 0 \pmod{2} \Rightarrow a_{n-1} \equiv a_n \equiv 1 \pmod{2}, & a_{n-1} \equiv a_n \pmod{4}, \\ b_n \equiv 1 \pmod{2} \Rightarrow a_{n-1} \equiv 0 \pmod{4}, & a_n \equiv 1 \pmod{2} \text{ or} \\ & a_{n-1} \equiv 1 \pmod{2}, & a_n \equiv 0 \pmod{4}, \end{cases}$$

and

$$(2.11) \quad \begin{cases} b'_m \equiv 1 \pmod{2}, & a'_{m-1}a'_m \equiv 0 \pmod{2}, & \text{if } D \equiv 1 \pmod{8}, \\ b'_m \equiv a'_{m-1} \equiv a'_m \equiv 1 \pmod{2}, & & \text{if } D \equiv 5 \pmod{8}. \end{cases}$$

Next we consider ambiguous classes, that is classes of order 2 in the class group. The ambiguous classes are the classes which contain ambiguous forms, and each ambiguous class contains exactly two ambiguous reduced forms; furthermore the indices n and n' of these ambiguous forms in the sequence of reduced forms satisfy

$$(2.12) \quad n' \equiv n + (A/2) \pmod{A},$$

where A ($= L$ or L^*) is the length of the period (see [2], § 187). If f_0 (resp. g_0) is chosen to be ambiguous then the period is symmetric, that is we have $f_{L-1-n} = \tilde{f}_n$ ($0 \leq n \leq L-1$), $g_{L^*-1-m} = \tilde{g}_m$ ($0 \leq m \leq L^*-1$). We have

LEMMA 1. *Let $f = [\varepsilon a, 2b, -\varepsilon c]$ be an ambiguous reduced form in a class A of discriminant $4D$. Then a divides b , say $b = ka$, and the class $\theta(A)$ contains the ambiguous reduced form $[\varepsilon a, la, -\varepsilon c']$, where $l = k$, if k is odd, and $l = k-1$, if k is even.*

Proof. We first note that a is odd, otherwise, by (2.10), $a \equiv 0 \pmod{4}$ could not divide $2b \equiv 2 \pmod{4}$. Therefore a divides b , say $b = ka$, and $f = [\varepsilon a, 2ka, -\varepsilon c]$.

If k is odd then, by (2.10), $c \equiv 0 \pmod{4}$, so that $\theta(A)$ contains the form $g = [\varepsilon a, ka, -\varepsilon c/4]$.

If k is even, say $k = 2K$, then the class A contains the form $[\varepsilon a, 2(2K-1)a, -\varepsilon c']$, where $c' \equiv 0 \pmod{4}$, so that $\theta(A)$ contains the form $g = [\varepsilon a, (2K-1)a, -\varepsilon c'/4]$.

We prove that g is reduced in both cases. As f is reduced

$$(2.13) \quad 0 < \sqrt{D} - ka < a < \sqrt{D} + ka,$$

which implies $a < \sqrt{D}$, and so

$$0 < \sqrt{D} - ka < 2a < \sqrt{D} + ka,$$

showing that, if k is odd, g is reduced. If k is even (2.13) becomes

$$0 < \sqrt{D} - 2Ka < a < \sqrt{D} + 2Ka,$$

which implies (as $a < \sqrt{D}$)

$$0 < \sqrt{D} - (2K-1)a < 2a < \sqrt{D} + (2K-1)a,$$

showing that if k is even, g is reduced. This completes the proof of Lemma 1.

THEOREM 1'. *The lengths L and L^* of periods of ambiguous classes corresponding by θ satisfy*

$$L \equiv L^* \pmod{4}.$$

Proof. By Lemma 1 the first coefficients of the reduced ambiguous forms of A and $\theta(A)$ are respectively equal, so that, by (2.12), $L/2 \equiv (L^*/2) \pmod{2}$, which proves Theorem 1'.

Later we shall need the following reduced forms. Let $d = [\sqrt{D}]$, let d' denote the greatest odd integer $< \sqrt{D}$, and set $d'' = d' - 2$. The reduced forms

$$(2.14) \quad \begin{cases} h = [1, 2d, d^2 - D], & \text{of discriminant } 4D, \\ h^* = [1, d', (d'^2 - D)/4], & \text{of discriminant } D, \end{cases}$$

belong to the principal classes of their discriminant.

If $D \equiv 5 \pmod{8}$ the forms of discriminant $4D$

$$(2.15) \quad h' = [4, 2d', (d'^2 - D)/4], \quad h'' = [4, 2d'', (d''^2 - D)/4]$$

are reduced for $D > 5$ and belong to a class of $\ker \theta$.

If $\text{card}(\ker \theta) = 3$ then each of the nonprincipal classes C' and C'' of $\ker \theta$ contains respectively the form h' and h'' , and simple symmetry considerations show that the lengths L'_0 and L''_0 of their periods satisfy

$$(2.16) \quad L'_0 = L''_0.$$

We conclude this section by indicating the relation between the period of the principal class of discriminant $4D$ (resp. D) and the continued fraction expansion of \sqrt{D} (resp. $(1 + \sqrt{D})/2$). For discriminant $4D$ (respectively D) choose $f_0 = h$ (respectively $g_0 = h^*$), and set $t(f_n) = t_n$ (respectively $t(g_n) = t'_n$). Then we have

$$\sqrt{D} = [d; |t_0|, |t_1|, |t_2|, \dots]$$

and

$$\frac{1 + \sqrt{D}}{2} = \left[\frac{1 + d'}{2}; |t'_0|, |t'_1|, |t'_2|, \dots \right].$$

3. The mapping Ψ and its properties. In this section we introduce a mapping Ψ from the set of reduced forms of discriminant $4D$ to the set of reduced forms of discriminant D . This mapping will be central to everything we do in the rest of this paper.

From now on a, b, c denote positive integers. We classify the reduced forms of discriminant $4D$ into five types, where

$$(3.1) \quad \begin{cases} D = b^2 + ac, & \text{for type (I)} \\ D = b^2 + 4ac, & \text{for types (II), (III), (IV), (V),} \end{cases}$$

as follows:

- I : $[\varepsilon a, 2b, -\varepsilon c]$, $ac \equiv 1 \pmod{4}$, $b \equiv 0 \pmod{2}$,
- II : $[\varepsilon a, 2b, -4\varepsilon c]$, $a \equiv 1 \pmod{2}$, $[\varepsilon a, b, -\varepsilon c]$ reduced,

III : $[\varepsilon a, 2b, -4\varepsilon c]$, $a \equiv 1 \pmod{2}$, $[\varepsilon a, b, -\varepsilon c]$ not reduced,

IV : $[4\varepsilon a, 2b, -\varepsilon c]$, $c \equiv 1 \pmod{2}$, $[\varepsilon a, b, -\varepsilon c]$ reduced,

V : $[4\varepsilon a, 2b, -\varepsilon c]$, $c \equiv 1 \pmod{2}$, $[\varepsilon a, b, -\varepsilon c]$ not reduced,

where $\varepsilon = \pm 1$. We define the mapping Ψ from the set of reduced forms f of discriminant $4D$ to the set of forms of discriminant D as follows:

$$(3.2) \quad \Psi(f) = \begin{cases} \left[\frac{-\varepsilon(-a+2b+c)}{4}, \frac{a+c}{2}, \frac{\varepsilon(a+2b-c)}{4} \right], & f \text{ of type (I),} \\ [\varepsilon a, b, -\varepsilon c], & f \text{ of type (II),} \\ [\varepsilon(a-b-c), b+2c, -\varepsilon c], & f \text{ of type (III),} \\ [\varepsilon a, b, -\varepsilon c], & f \text{ of type (IV),} \\ [\varepsilon a, 2a+b, -\varepsilon(-a-b+c)], & f \text{ of type (V).} \end{cases}$$

We remark that the form $\Psi(f)$ is obtained from the form f by means of the rational linear transformation with matrix M (of determinant $1/2$) given by

$$(3.3) \quad M = \begin{bmatrix} \varepsilon/2 & 1/2 \\ -1/2 & \varepsilon/2 \end{bmatrix} \text{ (I), } \begin{bmatrix} 1 & 0 \\ 0 & 1/2 \end{bmatrix} \text{ (II), } \begin{bmatrix} 1 & 0 \\ -\varepsilon/2 & 1/2 \end{bmatrix} \text{ (III),} \\ \begin{bmatrix} 1/2 & 0 \\ 0 & 1 \end{bmatrix} \text{ (IV), } \begin{bmatrix} 1/2 & \varepsilon/2 \\ 0 & 1 \end{bmatrix} \text{ (V).}$$

For convenience we note the values of M^{-1} :

$$(3.4) \quad M^{-1} = \begin{bmatrix} \varepsilon & -1 \\ 1 & \varepsilon \end{bmatrix} \text{ (I), } \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \text{ (II), } \begin{bmatrix} 1 & 0 \\ \varepsilon & 2 \end{bmatrix} \text{ (III),} \\ \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \text{ (IV), } \begin{bmatrix} 2 & -\varepsilon \\ 0 & 1 \end{bmatrix} \text{ (V).}$$

PROPOSITION 1. *If f is a reduced form of discriminant $4D$ then $\Psi(f)$ is an integral primitive form of discriminant D , which is reduced.*

Proof. It is easily checked that $\Psi(f)$ is an integral primitive form of discriminant D . Moreover $\Psi(f)$ is reduced. This is clear if f is of types II or IV. If f is of type III we have $0 < \sqrt{D} - b < 4c < \sqrt{D} + b$ but not $0 < \sqrt{D} - b < 2c < \sqrt{D} + b$ so that $\sqrt{D} - b > 2c$; this implies $0 < \sqrt{D} - b - 2c < 2c < \sqrt{D} + b + 2c$, showing that $\Psi(f)$ is reduced. The proof for f of type V is similar.

Now we consider the case of a form f of type I. As f is reduced we have

$$0 < \sqrt{D} - b < a < \sqrt{D} + b, \quad 0 < \sqrt{D} - b < c < \sqrt{D} + b.$$

Thus we have

$$\sqrt{D} < b + c, \quad -\sqrt{D} < -a + b,$$

and

$$-\sqrt{D} < b-c, \quad \sqrt{D} < a+b.$$

Adding the inequalities, we obtain

$$-a+2b+c > 0, \quad a+2b-c > 0,$$

and so

$$4D-(a+c)^2 = (-a+2b+c)(a+2b-c) > 0,$$

giving

$$(3.5) \quad 0 < 2\sqrt{D}-a-c.$$

From $\sqrt{D}-b < a$ we obtain

$$(3.6) \quad 2\sqrt{D}-a-c < a+2b-c.$$

As $D-(b-c)^2 = (a+2b-c)c > 0$ we have

$$(3.7) \quad a+2b-c < 2\sqrt{D}+a+c.$$

The inequalities (3.5), (3.6), (3.7) show that $\Psi(f)$ is reduced.

Proposition 1 shows that Ψ maps the set of reduced forms of discriminant $4D$ into the set of reduced forms of discriminant D .

PROPOSITION 2. *The class of the image by Ψ of a reduced form f of discriminant $4D$ is the image by θ of the class of f .*

Proof. By (2.5) the result is clear if f is of type II or IV. To prove Proposition 2 for f of type III or V it is enough to note the equivalences

$$[\varepsilon(a-b-c), b+2c, -\varepsilon c] \sim [\varepsilon a, b, -\varepsilon c] \sim [\varepsilon a, 2a+b, -\varepsilon(-a-b+c)].$$

If f is of type I then

$$f = [\varepsilon a, 2b, -\varepsilon c] \sim [\varepsilon a, 2(a+b), \varepsilon(a+2b-c)],$$

whereas

$$\Psi(f) = \left[-\varepsilon \frac{(-a+2b+c)}{4}, \frac{a+c}{2}, \varepsilon \frac{(a+2b-c)}{4} \right] \sim \left[\varepsilon a, a+b, \varepsilon \frac{(a+2b-c)}{4} \right]$$

proving Proposition 2.

The following corollary follows immediately from Proposition 2.

COROLLARY. (1) *If $f_1 \sim f_2$ then $\Psi(f_1) \sim \Psi(f_2)$.*

(2) *If f belongs to the principal class of discriminant $4D$ then $\Psi(f)$ belongs to the principal class of discriminant D .*

PROPOSITION 3. *The restriction of Ψ to reduced forms of any given type is one to one.*

Proof. Each of the matrices M listed in (3.3) is invertible.

COROLLARY. *The lengths of the periods of classes corresponding by θ satisfy $L \leq 5L^*$.*

Proof. Each reduced form of the class $\theta(C)$ is the image by Ψ of at most 5 forms of C .

We shall need the following properties of the mapping Ψ .

LEMMA 2. *If $f \approx f'$ then the type of (f, f') is one of the following ten pairs: (I, I), (I, II), (I, III), (II, IV), (II, V), (III, IV), (III, V), (IV, I), (IV, II), (V, I).*

Proof. Suppose that $f = [4ea, 2b, -\varepsilon c] \approx f' = [-\varepsilon c, 2b', 4ea']$ so that, as $b \equiv b' \equiv c \equiv 1 \pmod{2}$, the positive integer $(b+b')/c$ is ≥ 2 , that is

$$(3.8) \quad b+b' \geq 2c.$$

From (3.8) and the fact that f and f' are reduced one deduces easily that the two forms $g = [\varepsilon a, b, -\varepsilon c]$ and $g' = [-\varepsilon c, b', \varepsilon a']$ are reduced, which shows that f is of type IV and f' of type II, so that the type pairs (IV, III), (V, II) and (V, III) are not possible. The other twelve impossibilities are obtained immediately by comparing the parity of the last coefficient of f and the first coefficient of f' .

If $f = [a, b, c]$, we set $\bar{f} = [-a, b, -c]$.

LEMMA 3. $\Psi(\bar{f}) = \overline{\Psi(f)}$, $\Psi(\bar{f}) = \overline{\Psi(f)}$.

Proof. Lemma 3 is an immediate consequence of the definition of Ψ .

4. Proof of Theorem 2. In this section we suppose that the equation $T^2 - DU^2 = 4$ has odd solutions, so that $D \equiv 5 \pmod{8}$ and the homomorphism θ is an isomorphism. We first prove a result showing that for any class C the length of the period of $\theta(C)$ is not greater than the length of the period of C .

PROPOSITION 4. *If the equation (1.1) has odd solutions then, for any class C , the mapping Ψ is a bijection of the reduced forms of type I of C on the reduced forms of $\theta(C)$.*

Proof. Let $g = [\varepsilon a, b, -\varepsilon c]$ be a reduced form of $\theta(C)$. As $D \equiv 5 \pmod{8}$, we have $a \equiv b \equiv c \equiv 1 \pmod{2}$. We consider the form $f = [-\varepsilon(-a+b+c), 2(a+c), \varepsilon(a+b-c)]$ of discriminant $4D$. As a, b, c are odd, the integers $-a+b+c$ and $a+b-c$ are odd, and as g is primitive so is f . Moreover, as the form g is reduced, we have

$$(4.1) \quad 0 < \sqrt{D}-b < 2a < \sqrt{D}+b, \quad 0 < \sqrt{D}-b < 2c < \sqrt{D}+b,$$

so that

$$(2a+b)^2 - D = 4a(a+b-c) > 0, \quad (b+2c)^2 - D = 4c(-a+b+c) > 0,$$

showing that $-a+b+c$ and $a+b-c$ are positive integers. Thus to show that f is reduced of type I it is enough to prove

$$0 < \sqrt{D}-(a+c) < -a+b+c < \sqrt{D}+a+c.$$

We have

$$D - (a + c)^2 = b^2 - (a - c)^2 = (b - a + c)(b + a - c) > 0,$$

which proves the first inequality. The second and third inequalities are respectively equivalent to $\sqrt{D} < b + 2c$ and to $b < \sqrt{D} + 2a$, which follow from (4.1). A straightforward calculation shows that $\Psi(f) = g$. As θ is an isomorphism we see that $f \in C$. The result now follows on appealing to Proposition 3.

We have thus shown that, if (1.1) has odd solutions, for any pair $(C, \theta(C))$, where C is a class of forms of discriminant $4D$,

$$(4.2) \quad L^* \leq L \leq 5L^*.$$

Now we consider the principal classes. The forms h' and h'' defined in (2.14), as well as the forms \tilde{h}' and \tilde{h}'' , are reduced for $D > 5$, and they are in the principal class as they represent 4 and $\text{card}(\ker \theta) = 1$. Clearly none of $h', h'', \tilde{h}', \tilde{h}''$ is of type I, so that we have

$$L_0^* + 4 \leq L_0 \leq 5L_0^*.$$

Moreover, if the equation (1.2) is solvable, the forms obtained by changing the signs of the first and last coefficients of $h', h'', \tilde{h}', \tilde{h}''$ are also in the principal class so that

$$L_0^* + 8 \leq L_0 \leq 5L_0^*.$$

This completes the proof of Theorem 2.

5. Order preserving property of Ψ . Let C be a class of forms of discriminant $4D$ and $\theta(C)$ its image by the mapping θ . We choose an initial form $f_0 \in C$ and denote by f_0, f_1, f_2, \dots , the sequence of reduced forms of C , defined by $f_n \approx f_{n+1}$. In the class $\theta(C)$ we choose as initial form $g_0 = \Psi(f_0)$, and define the sequence g_0, g_1, g_2, \dots by $g_m \approx g_{m+1}$. The integers $t(f_n), t(g_m)$ being defined as in (2.7), we set

$$(5.1) \quad T_n = \begin{bmatrix} 0 & -1 \\ 1 & t(f_n) \end{bmatrix}, \quad T'_m = \begin{bmatrix} 0 & -1 \\ 1 & t(g_m) \end{bmatrix},$$

so that T_n (respectively T'_m) is a matrix of the transformation of f_n (respectively g_m) into its right neighbouring form. We denote by I the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and define:

$$(5.2) \quad A_n = \begin{cases} I, & \text{if } n = 0, \\ T_0 \dots T_{n-1}, & \text{if } n \geq 1, \end{cases} \quad A'_m = \begin{cases} I, & \text{if } m = 0, \\ T'_0 \dots T'_{m-1}, & \text{if } m \geq 1, \end{cases}$$

so that the transformation of matrix A_n (respectively A'_m) sends f_0 (respectively g_0) into f_n (respectively g_m).

Then we consider the matrix

$$(5.3) \quad B_n = M_0^{-1} A_n M_n,$$

where M_0, M_n (depending upon the types of f_0, f_n) are defined by (3.3) and (3.4). Clearly B_n is the matrix of a rational linear transformation of $\Psi(f_0)$ into $\Psi(f_n)$. We prove

THEOREM 4. (a) *The matrix B_n is integral and there exists an integer $m(n) \geq 1$ such that $\Psi(f_n) = g_{m(n)}$ and*

$$(5.4) \quad B_n = \pm A'_{m(n)}.$$

(b) *The function $m(n)$ is a nondecreasing function of n which satisfies*

- (b₁) $m(n+1) = m(n)$, if (f_n, f_{n+1}) is of type (I, III) or (V, I),
- (b₂) $m(n+1) = m(n) + 2$, if (f_n, f_{n+1}) is of type (I, II) or (IV, I),
- (b₃) $m(n+1) = m(n) + 3$, if (f_n, f_{n+1}) is of type (I, I) such that $|t(f_n)| > 2$,
- (b₄) $m(n+1) = m(n) + 1$, otherwise.

(c) *The function $m(n)$ satisfies*

$$(5.5) \quad m(n+L) = \begin{cases} m(n) + 3L^*, & \text{if (1.1) has odd solutions,} \\ m(n) + L^*, & \text{if (1.1) has no odd solution.} \end{cases}$$

Proof. We first prove (a) and (b). As

$$B_n = M_0^{-1} T_0 \dots T_{n-1} M_n = (M_0^{-1} T_0 M_1)(M_1^{-1} T_1 M_2) \dots (M_{n-1}^{-1} T_{n-1} M_n),$$

it is enough to consider the last term $M_{n-1}^{-1} T_{n-1} M_n$. Then $f_n = [\varepsilon a, 2b, -\varepsilon c]$ and $f_{n+1} = [-\varepsilon c, 2b', \varepsilon a']$ are two reduced forms of discriminant $4D$ such that $f_n \approx f_{n+1}$, and $t = t(f_n) = -\varepsilon(b+b')/c$, so that $\varepsilon t < 0$. We shall calculate the matrix $U_n = M_n^{-1} T_n M_{n+1}$ according to the ten possible types of the pair (f_n, f_{n+1}) .

(1) (f_n, f_{n+1}) is of type (I, I). Here $b \equiv b' \equiv 0 \pmod{2}$, $c \equiv 1 \pmod{2}$ so that $t \equiv 0 \pmod{2}$, and one finds

$$U_n = \begin{bmatrix} \varepsilon + t/2 & \varepsilon t/2 \\ -\varepsilon t/2 & \varepsilon - t/2 \end{bmatrix}.$$

If $|t| = 2$, that is $t = -2\varepsilon$, then $U_n = \begin{bmatrix} 0 & -1 \\ 1 & 2\varepsilon \end{bmatrix}$ so that $\Psi(f_n) \approx \Psi(f_{n+1})$ with $t(\Psi(f_n)) = 2\varepsilon$, which shows that $m(n+1) = m(n) + 1$.

If $|t| \geq 4$, that is $[(b + \sqrt{D})/c] \geq 4$, we consider the forms

$$\Psi(f_n) = \left[-\varepsilon \frac{(-a + 2b + c)}{4}, \frac{a + c}{2}, \varepsilon \frac{(a + 2b - c)}{4} \right],$$

$$g' = \left[\varepsilon \frac{(a + 2b - c)}{4}, b - c, -\varepsilon c \right],$$

$$g'' = \left[-\varepsilon c, b' - c, \varepsilon \frac{-c + 2b' + a'}{4} \right],$$

$$\Psi(f_{n+1}) = \left[\varepsilon \frac{-c + 2b' + a'}{4}, \frac{c + a'}{2}, -\varepsilon \frac{(c + 2b' - a')}{4} \right].$$

The forms g' and g'' are reduced that is

$$0 < \sqrt{D} - b + c < 2c < \sqrt{D} + b - c \quad \text{and} \quad 0 < \sqrt{D} - b' + c < 2c < \sqrt{D} + b' - c.$$

The two first inequalities of each set are clear, as f_n and f_{n+1} are reduced. The third inequalities of each set can be rewritten as

$$\frac{\sqrt{D} + b}{c} > 3, \quad \frac{\sqrt{D} + b'}{c} > 3,$$

which are true, as

$$|t(f_n)| = \left[\frac{\sqrt{D} + b}{c} \right] = \left[\frac{\sqrt{D} + b'}{c} \right] \geq 4.$$

One sees then that $\Psi(f_n) \approx g' \approx g'' \approx \Psi(f_{n+1})$ with

$$t(\Psi(f_n)) = t(g'') = \varepsilon, \quad t(g_1) = t/2 + \varepsilon,$$

so that $\Psi(f_n)$ is changed into $\Psi(f_{n+1})$ by the transformation of matrix

$$\begin{bmatrix} 0 & -1 \\ 1 & \varepsilon \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & t/2 + \varepsilon \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & \varepsilon \end{bmatrix} = \begin{bmatrix} -\varepsilon - t/2 & -\varepsilon t/2 \\ \varepsilon t/2 & -\varepsilon + t/2 \end{bmatrix} = -U_n.$$

This proves that $m(n+1) = m(n) + 3$ when $|t| \geq 4$.

(2) (f_n, f_{n+1}) is of type (I, II) or (IV, I). We consider the type (I, II). Here

$$f_n = [\varepsilon a, 2b, -\varepsilon c], \quad f_{n+1} = [-\varepsilon c, 2b', 4\varepsilon a'],$$

with $b \equiv 0 \pmod{2}$, $b' \equiv c \equiv 1 \pmod{2}$ so that

$$t(f_n) = t = \frac{b + b'}{-\varepsilon c} \equiv 1 \pmod{2}.$$

One finds

$$U_n = \begin{bmatrix} -1 & (-t - \varepsilon)/2 \\ \varepsilon & (\varepsilon t - 1)/2 \end{bmatrix}.$$

As f_{n+1} is of type II, $\Psi(f_{n+1}) = [-\varepsilon c, b', \varepsilon a']$ is reduced. We prove first that $|t| \geq 3$. Otherwise $|t| = 1$, so that $b + b' = c$, giving

$$0 < \sqrt{D} - b < b + b' < \sqrt{D} + b \quad (f_n \text{ reduced}),$$

$$0 < \sqrt{D} - b' < 2(b + b') < \sqrt{D} + b' \quad (\Psi(f_{n+1}) \text{ reduced}),$$

which would imply that $2b + b' < \sqrt{D} < 2b + b'$.

From the fact that $|t| \geq 3$, that is $(\sqrt{D} + b)/c > 3$ we see, as in the case where (f_n, f_{n+1}) is of type (I, I), that the form

$$g' = \left[\varepsilon \frac{(a + 2b - c)}{4}, b - c, -\varepsilon c \right]$$

is reduced, so that

$$\Psi(f_n) \approx g' \approx \Psi(f_{n+1})$$

with

$$t(\Psi(f_n)) = \varepsilon, \quad t(g') = (t + \varepsilon)/2.$$

Therefore $\Psi(f_n)$ is transformed into $\Psi(f_{n+1})$ by the transformation of matrix

$$\begin{bmatrix} 0 & -1 \\ 1 & \varepsilon \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & (t + \varepsilon)/2 \end{bmatrix} = \begin{bmatrix} -1 & (-t - \varepsilon)/2 \\ \varepsilon & (\varepsilon t - 1)/2 \end{bmatrix} = U_n,$$

which proves that $m(n+1) = m(n) + 2$ for (f_n, f_{n+1}) of type (I, II), and also of type (IV, I) by considering \tilde{f}_n and \tilde{f}_{n+1} .

(3) (f_n, f_{n+1}) is of type (I, III) or (V, I). We consider the type (I, III), that is $f_n = [\varepsilon a, 2b, \varepsilon c]$, $f_{n+1} = [-\varepsilon c, 2b', 4\varepsilon a']$, with $b \equiv 0 \pmod{2}$, $b' \equiv c \equiv 1 \pmod{2}$ so that $t(f_n) \equiv 1 \pmod{2}$. As f_{n+1} is of type III, the form $[-\varepsilon c, b', \varepsilon a']$ is not reduced, so that one of the inequalities $0 < \sqrt{D} - b' < 2c < \sqrt{D} + b'$ is not satisfied; but, as f_{n+1} is reduced, $0 < \sqrt{D} - b' < c < \sqrt{D} + b'$, so that $\sqrt{D} + b' < 2c$.

Taking (2.8) into account this shows that $|t| = 1$.

Now one finds

$$U_n = \begin{bmatrix} (-3 - \varepsilon t)/2 & (-\varepsilon - t)/2 \\ (\varepsilon + t)/2 & (-1 + \varepsilon t)/2 \end{bmatrix}$$

so that $U_n = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, which proves that $m(n+1) = m(n)$ for (f_n, f_{n+1}) of type (I, III), and (by considering $(\tilde{f}_n, \tilde{f}_{n+1})$) for (f_n, f_{n+1}) of type (V, I).

(4) (f_n, f_{n+1}) not of above types. One finds that

$$U_n = \begin{bmatrix} 0 & -1 \\ 1 & t' \end{bmatrix}$$

with $t' = 2t$ (type (II, IV)), $t' = -\varepsilon + 2t$ (types (II, V) and (III, IV)), $t' = -2\varepsilon + 2t$ (type (III, V)), $t' = t/2$ (type (IV, II) in which case $t \equiv 0 \pmod{2}$).

This completes the proof of (a) and (b).

Next we prove (c). We define the integer α by

$$(5.6) \quad \alpha = \begin{cases} 1, & \text{if (1.1) has no odd solution,} \\ 3, & \text{if (1.1) has odd solutions.} \end{cases}$$

We denote by T_0, U_0 (respectively T'_0, U'_0) the smallest even positive solution (respectively, the smallest solution) of (1.1). The automorphs of $f_0 = [ea, 2b, -ec]$ are given by

$$A_{(T,U)} = \begin{bmatrix} (T-bU)/2 & ecU/2 \\ eaU/2 & (T+bU)/2 \end{bmatrix},$$

where (T, U) is any even solution of (1.1), and also by (recall (5.2))

$$\pm(A_L)^{\pm k} = \pm(A_{kL})^{\pm 1}, \quad k \geq 0.$$

Similarly the automorphs of $\Psi(f_0) = [e'a', b', -e'c']$ are given by

$$A'_{(T,U)} = \begin{bmatrix} (T-b'U)/2 & e'c'U \\ e'a'U & (T+b'U)/2 \end{bmatrix},$$

where here (T, U) is any solution of (1.1), and also by (recall (5.2))

$$(5.7) \quad \pm(A'_{L'})^{\pm k} = \pm(A_{kL'})^{\pm 1}, \quad k \geq 0.$$

It is known (see [7], p. 123) that

$$(5.8) \quad A_L = A_{(T_0, U_0)}, \quad A'_{L'} = A'_{(T'_0, U'_0)},$$

and also that (see [6], § 99)

$$(5.9) \quad A'_{(T'_0, U'_0)} = [A'_{(T'_0, U'_0)}]^\alpha.$$

Now, by a straightforward calculation, one checks, for each of the five types of f_0 , that

$$(5.10) \quad M^{-1} A_{(T,U)} M = A'_{(T,U)}$$

with the same value of (T, U) . Therefore by (5.4), (5.8), (5.9), (5.10) one finds successively

$$\pm A'_{m(L)} = M^{-1} A_L M = M^{-1} A_{(T_0, U_0)} M = A'_{(T_0, U_0)} = [A'_{(T'_0, U'_0)}]^\alpha = (A'_{L'})^\alpha = A'_{2L'},$$

which implies $m(L) = \alpha L'$ and completes the proof of Theorem 4.

COROLLARY. (a) $m(n) = m(n+1) = m(n+2) \Leftrightarrow (f_n, f_{n+1}, f_{n+2})$ is of type (V, I, III).

(b) If $m(n_1) = m(n_2) = m(n_3) = m(n_4)$ at least two of the integers n_1, n_2, n_3, n_4 are equal.

As a first application of Theorem 4 we give a new proof of a generalization of Theorem 0, the main result of [5]. We prove

THEOREM 5. Let D be a positive nonsquare integer $\equiv 1 \pmod{4}$ such that the equation (1.2) is solvable. Let A be an ambiguous class of discriminant $4D$, $\theta(A)$ its

ACTA ARITHMETICA

a S. LUBELSKI et A. WALFISZ fundata, a W. SIERPIŃSKI continuata

NUNC EDUNTUR A

J. W. S. CASSELS, P. ERDŐS, A. SCHINZEL (EDITOR), R. TIJDEMAN;

J. BROWKIN (SECRETARIUS)

ADIUVANTIBUS

A. N. ANDRIANOV, A. BAKER, L. CARLITZ, K. CHANDRASEKHARAN, M. EICHLER,
E. HLAWKA, H. IWANIEC, H. KOCH, J. KUBILIUS, D. H. LEHMER, D. J. LEWIS,
H. L. MONTGOMERY, W. NARKIEWICZ, K. G. RAMANATHAN, W. M. SCHMIDT,
H. P. F. SWINNERTON-DYER, I. R. SHAFAREVICH, M. WALDSCHMIDT

LIV

WARSZAWA 1989-1990

P A Ń S T W O W E W Y D A W N I C T W O N A U K O W E

A R I T H M E T I C A

V I I

V I I

© Copyright by Instytut Matematyczny PAN, Warszawa 1989-1990

Published by PWN - Polish Scientific Publishers

PRINTED IN POLAND

image by the homomorphism θ , and let L and L^* denote the lengths of the periods of A and $\theta(A)$ respectively. Then $L = L^* = 2 \pmod{4}$, and $L = L^* \pmod{8}$ if and only if the equation (1.1) has *no* solutions.

Proof. As the equation (1.2) is solvable, we can choose the notation so that, for the class A ,

Conspectus materiae tomi LIV

	Pagina
A.-M. Bergé et J. Martinet, Notions relatives de régulateurs et de hauteurs	155-170
A. J. F. Biagioli, The construction of modular forms as products of transforms of the Dedekind eta function	273-300
D. W. Boyd, On linear recurrence relations satisfied by Pisot sequences. Addenda and errata	255-256
S. D. Cohen, Galois groups of trinomials	43-49
J. Cougnard, Modèle de Legendre d'une courbe elliptique à multiplication complexe et monogénéité d'anneaux d'entiers	191-212
J. C. Douai, Sur les extensions totalement décomposées de certains corps de fonctions	185-190
J. Herzog, Weak asymptotic formulas for partitions free of small summands	257-271
K. Inkeri, On a diophantine equation of a modified Fermat type	1-7
N. Ishii, P. Kaplan and K. S. Williams, On Eisenstein's problem	323-345
P. Kaplan <i>vide</i> N. Ishii, P. Kaplan and K. S. Williams	
Y. Kitaoka, A note on representation of positive definite binary quadratic forms by positive definite quadratic forms in 6 variables	317-322
A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique	75-80
Г. А. Ломадзе, О представлении чисел суммами квадратичных форм $x_1^2 + x_1x_2 + x_2^2$	9-36
S. Louboutin, Groupes des classes d'idéaux triviaux	61-74
J. Martinet <i>vide</i> A.-M. Bergé et J. Martinet	
M. Mignotte, Sur un théorème de M. Langevin	81-86
M. B. Nathanson and A. Sárközy, Sumsets containing long arithmetic progressions and powers of 2	147-154
Ö. J. Rødseth, An upper bound for the h -range of the postage stamp problem	301-306
A. Sárközy <i>vide</i> M. B. Nathanson and A. Sárközy	
W. Scharlau, Generating functions of finitely generated Witt rings	51-59
P. G. Schmidt, Über die Anzahl quadratvoller Zahlen in kurzen Intervallen und ein verwandtes Gitterpunktproblem. Corrigendum zu Acta Arithmetica L(1988), 195-201	251-254
J. Stopple, Selberg zeta functions with virtual characters and the class number	37-42
S. J. Suchower, Subfield permutation polynomials and orthogonal subfield systems in finite fields	307-315
G. Terjanian, Sur la loi de réciprocité des puissances l -èmes	87-125
N. Q. Thang, A note on the Hasse principle	171-184
P. Thurnheer, On Dirichlet's theorem concerning diophantine approximation	241-250
L. H. Walling, Hecke operators on theta series attached to lattices of arbitrary rank	213-240
K. S. Williams <i>vide</i> N. Ishii, P. Kaplan and K. S. Williams	
J. Wolfskill, Bounding squares in second order recurrence sequences	127-145

Finally a straightforward calculation shows that $\sqrt{1 - 4x} = 1 - 2x + 2x^2 - 4x^3 + 8x^4 - 16x^5 + \dots$ so that, as the sign of the first coefficient of $\sqrt{1 - 4x}$ is 1 , we have

$$(5.6) \quad \alpha = \begin{cases} 1, & \text{if (1.1) has no odd solution,} \\ 3, & \text{if (1.1) has odd solutions.} \end{cases}$$

We denote by T_0, U_0 (respectively T'_0, U'_0) the smallest even positive solution (respectively, the smallest solution) of (1.1). The automorphs of $f_0 = [\varepsilon a, 2b, -\varepsilon c]$ are given by

$$A_{(T,U)} = \begin{bmatrix} (T-bU)/2 & \varepsilon cU/2 \\ \varepsilon aU/2 & (T+bU)/2 \end{bmatrix},$$

where (T, U) is any even solution of (1.1), and also by (recall (5.2))

$$\pm(A_L)^{\pm k} = \pm(A_{kL})^{\pm 1}, \quad k \geq 0.$$

Similarly the automorphs of $\Psi(f_0) = [\varepsilon' a', b', -\varepsilon' c']$ are given by

$$A'_{(T,U)} = \begin{bmatrix} (T-b'U)/2 & \varepsilon' c'U \\ \varepsilon' a'U & (T+b'U)/2 \end{bmatrix},$$

where here (T, U) is any solution of (1.1), and also by (recall (5.2))

$$(5.7) \quad \pm(A'_{L'})^{\pm k} = \pm(A_{kL'})^{\pm 1}, \quad k \geq 0.$$

It is known (see [7], p. 123) that

$$(5.8) \quad A_L = A_{(T_0,U_0)}, \quad A'_{L'} = A'_{(T'_0,U'_0)},$$

and also that (see [6], § 99)

$$(5.9) \quad A'_{(T_0,U_0)} = [A'_{(T'_0,U'_0)}]^\alpha.$$

Now, by a straightforward calculation, one checks, for each of the five types of f_0 , that

$$(5.10) \quad M^{-1} A_{(T,U)} M = A'_{(T,U)}$$

with the same value of (T, U) . Therefore by (5.4), (5.8), (5.9), (5.10) one finds successively

$$\pm A'_{m(L)} = M^{-1} A_L M = M^{-1} A_{(T_0,U_0)} M = A'_{(T_0,U_0)} = [A'_{(T'_0,U'_0)}]^\alpha = (A'_{L'})^\alpha = A_{\alpha L'},$$

which implies $m(L) = \alpha L^*$ and completes the proof of Theorem 4.

COROLLARY. (a) $m(n) = m(n+1) = m(n+2) \Leftrightarrow (f_n, f_{n+1}, f_{n+2})$ is of type (V, I, III).

(b) If $m(n_1) = m(n_2) = m(n_3) = m(n_4)$ at least two of the integers n_1, n_2, n_3, n_4 are equal.

As a first application of Theorem 4 we give a new proof of a generalization of Theorem 0, the main result of [5]. We prove

THEOREM 5. Let D be a positive nonsquare integer $\equiv 1 \pmod{4}$ such that the equation (1.2) is solvable. Let A be an ambiguous class of discriminant $4D$, $\theta(A)$ its

image by the homomorphism θ , and let L and L^* denote the lengths of the periods of A and $\theta(A)$ respectively. Then $L \equiv L^* \equiv 2 \pmod{4}$, and $L \equiv L^* \pmod{8}$ if, and only if, the equation (1.1) has odd solutions.

Proof. As the equation (1.2) is solvable we can choose the notation so that, for the class A ,

$$(5.11) \quad f_0 = [a, 2ka, -c], \quad f_{L/2} = [-a, 2ka, c],$$

with $a, c, k > 0$. For the class $\theta(A)$ we take $g_0 = \Psi(f_0)$.

By Theorem 4(c) we have $m(L) = \alpha L^*$ so that (5.11) shows that

$$(5.12) \quad m\left(\frac{L}{2}\right) = \alpha \frac{L^*}{2}.$$

The form f_0 is of type I or II according as k is even or odd. If f_0 is of type I, so are the forms $f_{L/2-1} = [c, 2ka, -a]$ and $f_{L/2}$. Moreover, $|t(f_{L/2-1})| = 2k \geq 4$ so that, by Theorem 4(b), one has

$$m\left(\frac{L}{2}\right) = m\left(\frac{L}{2}-1\right) + 3.$$

If f_0 is of type II, then $f_{L/2-1}, f_{L/2}$ are of types IV, II respectively so that

$$m\left(\frac{L}{2}\right) = m\left(\frac{L}{2}-1\right) + 1.$$

We set $\beta = 1$ if f_1 is of type I, $\beta = 0$ if f_1 is of type II, so that in both cases we have

$$(5.13) \quad m\left(\frac{L}{2}\right) = m\left(\frac{L}{2}-1\right) + 2\beta + 1.$$

Now define the integer λ by $L/2 = 2\lambda + 1$. As (1.2) is solvable it is known (see [2], § 265, [4], p. 171) that there exists an $\varepsilon = \pm 1$ and a decomposition

$$D = A^2 + B^2, \quad A \equiv 1 \pmod{2}, \quad A > 0, \quad B > 0,$$

such that $f_\lambda = [\varepsilon A, 2B, -\varepsilon A]$. Since $f_{\lambda+\mu} = [-t, 2s, -r]$ if $f_{\lambda-\mu} = [r, 2s, t]$ one sees, using Lemma 3, that

$$(5.14) \quad m\left(\frac{L}{2}-1\right) = 2m(\lambda).$$

Finally a straightforward calculation shows that $\Psi(f_\lambda) = [-\varepsilon B/2, A, \varepsilon B/2]$ so that, as the sign of the first coefficient of $\Psi(f_0) = g_0$ is $(-1)^\beta$, we have

$$(5.15) \quad m(\lambda) \equiv \lambda + 1 + \beta \pmod{2}.$$

Using (5.12), (5.13), (5.14), we obtain

$$\alpha \frac{L^*}{2} = m\left(\frac{L}{2}\right) = m\left(\frac{L}{2}-1\right) + 2\beta + 1 = 2m(\lambda) + 2\beta + 1,$$

which by (5.15) gives

$$\alpha \frac{L^*}{2} \equiv 2\lambda + 3 + 4\beta \equiv 2\lambda + 3 \equiv \frac{L}{2} + 2 \pmod{4}.$$

In view of the definition (5.6) of α , this completes the proof of Theorem 5.

6. Comparison between lengths of corresponding periods when the equation (1.1) has no odd solution. In this section we suppose that the equation (1.1) has no odd solution. Then, by Proposition 4, Ψ induces a nondecreasing mapping $n \rightarrow m(n)$ of the period of a class C into the period of the class $\theta(C)$. Furthermore Theorem 4(b) shows that the possibilities for $f_n, f_{n+1}, \dots, f_{n+k}$ to have the same image by Ψ are limited to the following cases:

$$(6.1) \quad \begin{cases} k = 1, & (f_n, f_{n+1}) & \text{of type (V, I) or (I, III),} \\ k = 2, & (f_n, f_{n+1}, f_{n+2}) & \text{of type (V, I, III).} \end{cases}$$

This clearly shows that $L \leq 3L^*$.

Theorem 4 also shows that the gaps between images by Ψ in the class $\theta(A)$ have length at most 2, so that $L^* \leq 3L$.

Now we consider the case of an ambiguous class A , and we shall prove that a reduced ambiguous form of the class $\theta(A)$ is the image by Ψ of at most one reduced form belonging to the class A .

Let $f = [\epsilon a, 2ka, -\epsilon c]$ be an ambiguous form of the class A , so that $\tilde{f} \approx f$, and $g = [\epsilon a, la, -\epsilon c]$ the ambiguous form of $\theta(A)$ given by Lemma 1, where $l = k$ or $k-1$ according as k is odd or even.

If k is odd, f is of type II, \tilde{f} of type IV, $\Psi(f) = g$ and, by Theorem 4(b), g is the image by Ψ of no other form than f .

If k is even, so that \tilde{f} and f are of type I, $|t(\tilde{f})| = 2k \geq 4$. Then, with the notation of the proof of Theorem 4 (1) we have

$$\Psi(\tilde{f}) \approx g' \approx g'' \approx \Psi(f),$$

where $g'' = [\epsilon a, al, -c']$ is the ambiguous form corresponding to f given by Lemma 1, and, as Ψ is monotonic on the period of $\tilde{f} \approx f$, g'' cannot be the image by Ψ of any form of A .

Thus we see that the two ambiguous forms g, h of $\theta(A)$, and also the forms \tilde{g}, \tilde{h} , have at most one antecedent.

Let N_r ($r \geq 0$) denote the number of reduced forms of the class $\theta(A)$ which are the image of Ψ of r reduced forms of A . By (5.1), $N_r = 0$ for $r \geq 4$ and we have proved that $N_0 + N_1 \geq 4$. On the other hand it is clear that

$$N_1 + 2N_2 + 3N_3 = L,$$

$$N_0 + N_1 + N_2 + N_3 = L^*,$$

so that

$$3L^* = L + 3N_0 + 2N_1 + N_2 \geq L + 2(N_0 + N_1) \geq L + 8.$$

This completes the proof of the following generalization of Theorem 3.

THEOREM 6. *If the equation (1.1) has no odd solution, the lengths L and L^* of the period of the ambiguous classes A and $\theta(A)$ respectively satisfy*

$$L^*/3 \leq L \leq 3L^* - 8.$$

7. Cases $L_0^* = 2$ and $L_0^* = 4$. We first consider the case where $L_0^* = 2$. We prove

PROPOSITION 5. *Let $D \equiv 1 \pmod{4}$ be a positive nonsquare integer. Then $L_0^* = 2$ if, and only if, there exist positive odd integers a and l such that*

$$(7.1) \quad D = a^2 l^2 + 4a.$$

If (7.1) holds then

$$L_0 = \begin{cases} 2, & \text{if } a = l = 1 (D = 5), \\ 6, & \text{if } a \geq 3, l = 1, \\ 10, & \text{if } l \geq 3. \end{cases}$$

Proof. Clearly $L_0^* = 2$ if, and only if, the principal period consists of the two forms (see (2.14))

$$h^* = \left[1, d', \frac{d'^2 - D}{4} \right] \approx \tilde{h}^* = \left[\frac{d'^2 - D}{4}, d', 1 \right],$$

where d' is the greatest odd integer $< \sqrt{D}$. Thus if $L_0^* = 2$ there exist positive odd integers a and l such that $a = (D - d'^2)/4$, $d' = al$, giving (7.1).

Conversely suppose that (7.1) holds, with a, l odd and positive. Then, as $a^2 l^2 < D < (al+2)^2$, the greatest odd integer $< \sqrt{D}$ is al so that the period of the principal class of discriminant D is

$$h^* = [1, al, -a] \approx \tilde{h}^* = [-a, al, 1].$$

If $a = l = 1$, $D = 5$ and $L_0 = 2$. Suppose now $al > 1$, so that $D > 5$. Then, by Corollary 2, the principal class of discriminant $4D$ contains the reduced forms

$$h' = [4, 2al, -a] \approx \tilde{h}' = [-a, 2al, 4].$$

The form \tilde{h}' is ambiguous, as well as the principal form

$$h = \begin{cases} [1, 2al, -4a], & \text{if } l > 1, \\ [1, 2(a+1), 1-2a], & \text{if } l = 1. \end{cases}$$

If $l = 1$ the form $\tilde{h}'' = [1-2a, 2(a-2), 4]$ satisfies

$$h \approx \tilde{h}'' \approx h'$$

proving that $L_0 = 6$.

If $l > 1$ the last coefficient of h and the first coefficient of h' are even, so no

primitive form f exists such that $h \approx f \approx h'$, which implies $L_0 > 6$, so that $L_0 = 10$. This completes the proof of Proposition 5.

For the case $L_0^* = 4$, Theorem 1, Corollary 3 and (4.2) give the following result.

PROPOSITION 6. For D such that $L_0^* = 4$, the equation (1.1) has no odd solution if $L_0 = 4$, whereas it has odd solutions if $L_0 = 8, 12, 16$ or 20 .

Moreover, we have

PROPOSITION 7. (a) $L_0^* = 4$ if, and only if, there exist integers a, l and t such that

$$(7.2) \quad a \geq 3, \quad l \geq 1, \quad t \geq 1, \quad a \equiv l \equiv 1 \pmod{2},$$

$$(7.3) \quad t \text{ divides } a-1 \text{ and } al + \left(\frac{a-1}{t}\right),$$

$$(7.4) \quad D = \frac{a}{t^2} [a(lt+2)^2 - 4].$$

In this case the nonprincipal reduced ambiguous form of the principal class of discriminant D (respectively $4D$) is

$$g_{L_0^*/2} = \left[a, al, \frac{al}{t} + \frac{a-1}{t^2} \right] \quad (\text{respectively } f_{L_0/2} = \left[a, 2ka, \frac{k^2 a^2 - D}{a} \right]),$$

where (d and d' are defined in § 2)

$$(7.5) \quad \begin{cases} d = d' + 1, & k = l + 1, & \text{if } t = 1, \\ d = d', & k = l, & \text{if } t \neq 1. \end{cases}$$

Furthermore, we have

$$(b) \quad L_0 = 4, \quad \text{if and only if } t \equiv 0 \pmod{2},$$

$$(c_1) \quad L_0 = 8, \quad \text{if } t = l = 1,$$

$$(c_2) \quad L_0 = 12, \quad \text{if } t = 1, \quad l \geq 3,$$

$$(c_3) \quad L_0 = 16, \quad \text{if } t \geq 3, \quad l = 1, \quad t \equiv 1 \pmod{2},$$

$$(c_4) \quad L_0 = 20, \quad \text{if } t \geq 3, \quad l \geq 3, \quad t \equiv 1 \pmod{2}.$$

Proof. Clearly $L_0^* = 4$ if, and only if, the principal period P' of discriminant D has the following shape

$$g_0 = \left[1, d', \frac{d'^2 - D}{4} \right] \approx g_1 = \left[\frac{l^2 a^2 - D}{4a}, la, a \right] \approx g_2 = \tilde{g}_1 \approx g_3 = \tilde{g}_0,$$

that is if, and only if, there exist integers a, l, t satisfying (7.2) and

$$(7.6) \quad 2(d' + la) = t(D - d'^2),$$

$$(7.7) \quad D - l^2 a^2 = a(D - d'^2),$$

$$(7.8) \quad la < \sqrt{D} < (l+2)a.$$

From (7.7) we obtain $(a-1)(D - d'^2) = d'^2 - al^2$, so that (7.6) gives

$$(7.9) \quad 2(a-1) = t(d' - al),$$

which shows that t divides $a-1$ and that

$$(7.10) \quad d' = al + 2\left(\frac{a-1}{t}\right),$$

which, by (7.6), shows that t divides $al + \left(\frac{a-1}{t}\right)$, proving (7.3). Also (7.7) follows from (7.6) and (7.9), and a straightforward calculation proves (7.4).

Conversely, suppose that (7.2) and (7.3) hold. Then one checks that D , defined by (7.4), is a positive integer $\equiv 1 \pmod{4}$ and that, if one sets, $d' = al + 2\left(\frac{a-1}{t}\right)$, then (7.9), (7.6) and (7.7) are satisfied, as well as the inequalities (7.8) and $d' < \sqrt{D} < d' + 2$, proving that $L_0^* = 4$.

Furthermore one checks easily that

$$t = 1 \Leftrightarrow d' + 1 < \sqrt{D}; \quad t = 1 \Leftrightarrow a(l+1) < \sqrt{D},$$

proving (7.5), and completing the proof of (a).

Next we prove (b). If $L_0 = 4$ then the principal period P of discriminant $4D$ is

$$f_0 \approx \tilde{f}_{L_0/2} \approx f_{L_0/2} \approx \tilde{f}_0.$$

If d were even these four forms would be of type I, contradicting Theorem 4(b₃) and (c), as $t(\tilde{f}_0) > 2$. Therefore we have $d = d', k = l$ and, as $f_0 \approx \tilde{f}_{L_0/2} = f_1$, there exists a positive integer u such that

$$la + d' = u(D - d'^2),$$

which, compared with (7.6), shows that $t = 2u$.

Conversely, if t is even, say $t = 2u$, then (7.6) and (7.9) imply

$$D = d'^2 + \left(\frac{d' + la}{u}\right) = d'^2 + \frac{2d'}{u} - \left(\frac{a-1}{u}\right) < (d' + 1)^2,$$

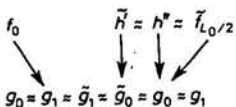
showing that $d = d'$. Then (7.6) and (7.7) with $d' = d$ and $t = 2u$ show that $f_0 \approx \tilde{f}_{L_0/2}$, that is $L_0 = 4$. This completes the proof of (b).

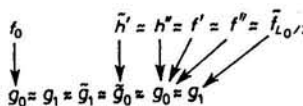
We suppose from now on that $L_0 > 4$. Then the equation (1.1) has odd solutions, so that, by Theorem 4, Ψ maps in an order-preserving fashion the first half H of P on the sequence of six forms

$$g_0 \approx g_1 \approx g_2 = \tilde{g}_1 \approx g_3 = \tilde{g}_0 \approx g_4 = g_0 \approx g_5 = g_1,$$

so that $\Psi(\tilde{f}_{L_0/2}) = g_4$ or g_5 according as k is even or odd. Moreover H contains a couple of contiguous forms $f_{k-1} \approx f_k$, equal to $\tilde{h}' \approx h''$ or to $\tilde{h}' \approx h'$, such that $\Psi(f_k) = g_4$. We show that $f_k = h''$. Otherwise h' (of type IV) would be followed by f_{k+1} of type I and $\Psi(f_{k+1}) = g_6$, or by f_{k+1} (of type II) with $\Psi(f_{k+1}) = g_5$,

and so $\Psi(\tilde{h})$ would be g_m with $m > 5$. Therefore $f_k = h''$, of type V, so that one has the following diagram

(7.11)  if d is even

(7.12)  if d is odd

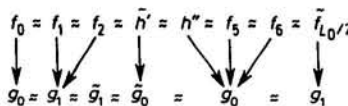
Suppose first that d is even. Then, appealing to Lemma 2 and Theorem 4, one sees easily that either

(7.13) $f_0 \approx \tilde{h}, \quad L_0 = 8,$

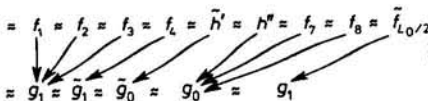
or

(7.14) $f_0 \approx f_1 \approx f_2 \approx \tilde{h}', \quad L_0 = 12,$
 $\Psi(f_1) = g_1, \quad \Psi(f_2) = g_2, \quad f_2$ of type IV.

Now we consider the case where d is odd, and complete the diagram (7.12). The form f_1 such that $f_0 \approx f_1$ is of type IV or V and $\Psi(f_1) = g_1$. If f_1 were of type IV, then either f_2 is of type II with $\Psi(f_2) = g_2$, and f_3 is of type IV or V with $\Psi(f_3) = g_3$, or f_2 is of type I, with $\Psi(f_2) = g_3$, which in both cases contradicts the fact that \tilde{h}' is of type II and that $\Psi(\tilde{h}') = g_3$. Therefore f_1 is of type V, and $\Psi(f_1) = g_1$, and thus f_2 is of type I with $\Psi(f_2) = g_1$. As the mapping Ψ , restricted to the forms of type I is a bijection, there cannot be another form of type I between f_2 and \tilde{h}' , so that either f_3 is of type II with $\Psi(f_3) = g_3$, that is $f_3 = \tilde{h}'$, or f_3 is of type III with $\Psi(f_3) = g_1$, and f_4 is of type IV with $\Psi(f_4) = g_2$ and $f_4 \approx \tilde{h}'$; f_4 cannot be of type V which would be followed by a form of type I. Thus when d is odd we have the two possibilities:

(7.15)  ($L_0 = 16$)

or

(7.16)  ($L_0 = 20$)

Thus we see that $L_0 = 12$ (if d is even) or $L_0 = 20$ (if d is odd) if, and only if, the form $g_2 = \tilde{g}_1 = [a, la, (l^2 a^2 - D)/4a]$ is the image by Ψ of a form of type IV, that is if, and only if, the form $[4a, 2la, (l^2 a^2 - D)/4a]$ is reduced, that is if, and only if,

(7.17) $0 < \sqrt{D} - la < 4a < \sqrt{D} + la.$

But, as \tilde{g}_1 is reduced, we have

(7.18) $0 < \sqrt{D} - la < 2a < \sqrt{D} + la,$

so that, as $la < \sqrt{D}$, (7.17) is true provided $l \geq 3$. When $l = 1$ the last inequality of (7.17) reduces to $3a < \sqrt{D}$, which contradicts the definition of l (and also the second inequality of (7.18)). This completes the proof of Proposition 7.

COROLLARY. (1) $L_0^* = 4$ and $L_0 = 8$ if, and only if, $D = 9a^2 - 4a$, with a odd and $a \geq 3$.

(2) $L_0^* = 4$ and $L_0 = 12$ if, and only if, $D = m^2 a^2 - 4a$ with $a \equiv m \equiv 1 \pmod{2}$ and $m \geq 5$.

8. Acknowledgement. The authors wish to thank Iain deMille for writing and running the computer programs needed for this work.

References

[1] Gotthold Eisenstein, *Aufgaben*, J. Reine Angew. Math. 27 (1844), 86-87. (Werke I. pp. 111-112, Chelsea Publishing Company, New York 1975.)
 [2] Carl Friedrich Gauss, *Arithmetische Untersuchungen (Disquisitiones Arithmeticae)*, Chelsea Publishing Company, New York 1965.
 [3] Franz Halter-Koch, *Über Pell'sche Gleichungen und Kettenbrüche*, Arch. Math. 49 (1987), 29-37.
 [4] Pierre Kaplan, *Cours d'Arithmétique*, Université de Nancy I, U.E.R. de Sciences Mathématiques, 1973.
 [5] Pierre Kaplan and Kenneth S. Williams, *Pell's equation $X^2 - mY^2 = -1, -4$ and continued fractions*, J. Number Theory 23 (1986), 169-182.
 [6] P. G. Lejeune Dirichlet and R. Dedekind, *Vorlesungen über Zahlentheorie*, Chelsea Publishing Company, New York 1968.
 [7] Arnold Scholz and Bruno Schoeneberg, *Einführung in die Zahlentheorie*, Walter de Gruyter & Co., Berlin 1973.

DEPARTMENT OF MATHEMATICS
 UNIVERSITY OF OSAKA PREFECTURE
 Sakai, Osaka, Japan
 10, Allée Jacques Offenbach
 54420 Saulxures lès Nancy, France

DEPARTMENT OF MATHEMATICS AND STATISTICS
 CARLETON UNIVERSITY
 Ottawa, Ontario, Canada K1S 5B6

Received on 1.7.1988

(1840)