UNIVERSITAT DE BARCELONA

FACULTAT DE MATEMÀTIQUES

ON INTEGRAL REPRESENTATIONS BY QUADRATIC FORMS

by

A. ARENAS

PRE– PRINT N.º 44

JUNY – 1986

ON INTEGRAL REPRESENTATIONS BY QUADRATIC FORMS

A. Arenas.

Facultat de Matemàtiques. Dpt. d'Àlgebra i Fonaments. Gran Via de les Corts Catalanes, 585. Univ. de Barcelona. 08007 Barcelona, SPAIN.

Introduction

In this paper we generalise the well-known Gauss algorithm for counting primitive representations of positive integers by positive definite ternary quadratic forms ([3], Arts 278-292) to the case of quadratic forms in k variables. Our main considerations are based on the systematic use of exterior algebra which, in our opinion, simplifies the whole treatment and helps to understand some apparently hidden ideas.

Some applications of our treatment are given.

1. Preliminaries

Let $f(x_1,\ldots,x_k) = \sum_{i,j=1}^{k} f_{ij}\, x_i\, x_j$ be a k-quadratic form with associated matrix $F = (f_{ij})$. We will assume throughout that all our quadratic forms are *integral* in the classical sense (i.e., with $f_{ij} \in \mathbb{Z}$), *symmetric* (i.e., $F = F^t$ where F^t denotes the transpose of F) and *non singular* (i.e., $\det F \neq 0$). We shall also assume that our forms are *positive* *definite* though most results still hold for the general case. We shall write indistinctly either f or F for a quadratic form. We will say that f is *primitive* if the entries of F generate the unit ideal.

The *adjoint* M^{adj} of a square k-matrix M can be introduced as follows: it is the matrix associated to the endomorphism $(\overset{k-1}{\Lambda}\varphi)^{*} : \overset{k-1}{\Lambda} E^{*} \longrightarrow \overset{k-1}{\Lambda} E^{*}$ in the basis $\{(-1)^{i-1} e_1^{*}\wedge\ldots\wedge\hat{e}_i^{*}\wedge\ldots\wedge e_k^{*}\}_{1\leq i\leq k}$, where is the endomorphism of $E = \mathbb{Z}^k$ with matrix M in the (canonical) basis $e_1,\ldots,e_k$ and where $e_1^{*},\ldots,e_k^{*}$ denotes its dual basis.

From the commutative diagram

$$
(1)\qquad
\begin{array}{ccc}
\overset{t}{\Lambda} E & \xrightarrow{\ \overset{t}{\Lambda}\varphi\ } & \overset{t}{\Lambda} E \\
{\scriptstyle \det\varphi\,.\,(\lrcorner e^{*})}\Big\downarrow & & \Big\downarrow{\scriptstyle \lrcorner e^{*}} \\
\overset{k-t}{\Lambda} E & \xleftarrow{\ (\overset{k-t}{\Lambda}\varphi)^{*}\ } & \overset{k-t}{\Lambda} E^{*}
\end{array}
$$

where $\lrcorner e^{*}$ stands for the *contraction* (on the left) with $e_1^{*}\wedge\ldots\wedge e_k^{*}$ (the commutativity of (1) is easily checked), we infer, taking t = 1, the well-known expression

$$M^{adj} . M = \det M . I_k$$

and, by duality, that $M.M^{adj} = \det M.I_k$, with I_k standing for the identity matrix of order k . If det M ≠ O, we obtain $\det (M^{adj}) = (\det M)^{k-1}$ and $(M^{adj})^{adj} = (\det M)^{k-2}.M$.

When we speak of the adjoint of a quadratic form f we will mean the quadratic form associated with the adjoint of the matrix F(symmetry and nonsingularity are obviously preserved).

We remark in passing that Laplace's expansion rule for determinants is a consequence of the commutativity of (1) -which holds for an arbitrary commutative ring R and a finitely generated free R-module E- provided that we take $\{e_I\}_I$ as basis in $\Lambda^t E$, where $I = \{i_1<\ldots<i_t\}$ runs over the ordered subsets of t elements of $\{1,\ldots,k\}$ and e_I stands for $e_{i_1}\wedge\ldots\wedge e_{i_t}$, and $\{\omega_{I'}\}_I$ as basis in $\Lambda^{k-t} E^*$, where I' is the ordered complement $\{j_1,\ldots,j_{k-t}\}$ of I in $\{1,\ldots,k\}$ and $\omega_{I'} = \mathrm{sgn}(I,I')\ e^*_{j_1}\wedge\ldots\wedge e^*_{j_{k-t}}$. Actually it is easy to see, with the above bases, that the matrix of $\Lambda^t\varphi$ is the t-th exterior power $\Lambda^t M$ of the matrix M, i.e.,(M_{IJ}), where M_{IJ} stands for the t-minor of M defined by the rows of I and the columns of J. The matrix $(A_{I'J'})$ associated with $\Lambda^{k-t}\varphi^*$ satisfies $A_{I'J'} = \mathrm{sgn}(I,I')\ \mathrm{sgn}(J,J')\ M_{JI}$.

(Observe that the t-th exterior power can be defined for a nonsquare matrix).

<u>Remark</u>. In the case t = 1, we observe that the adjoint M^{adj} of M is the matrix $\Delta.\Lambda^{k-1} M^t.\Delta$ where $\Delta = ((-1)^{i-1}\delta_{ij})$. If, for a square k-matrix N we put $\lambda^{k-1} N = \Delta(\Lambda^{k-1} N)\Delta$ we see that $M^{adj} = \lambda^{k-1}(M)^t = (\lambda^{k-1} M)^t$ and that $\lambda^{k-1}(NP) = \lambda^{k-1} N.\lambda^{k-1} P$, if P is also a square k-matrix.

Let f be as before, i.e., a k-quadratic form and g an h-quadratic form with $h\leq k$. The set $R^*(g,f)$ of *primitive representations of* g *by* f is defined as

$$R^*(g,f) = \{A\in M_{k\times h}(\mathbb{Z}) \mid A^tFA = G, \text{g.c.d. of the entries of } \Lambda^h A=1\}.$$

The condition that the entries of $\Lambda^h A$ have g.c.d. one means exactly that the columns of A may extended to a basis of $E = \mathbb{Z}^k$.

Similarly, if n is an integer, the *primitive representations of* n *by* f is the set

$$R^*(n,f) = \{(x_i) \in \mathbb{Z}^k \mid f(x_1,\dots,x_k) = n,\ \text{g.c.d.}(x_1,\dots,x_k) = 1\}.$$

This coincides with $R^*(g,f)$, for g the form nx^2.

The proper isotropy group of f is defined as

$$O^+(f) = \{A \in SL_k(\mathbb{Z}) \mid A^tFA = F\}.$$

We set $r^*(g,f) := \# R^*(g,f)$, $r\ (n,f) = \# R^*(n,f)$ and $o^+(f) = \# O^+(f)$.

Two k-forms f, f'are *properly* equivalent if and only if there exists a matrix $A \in SL_k(\mathbb{Z})$ such that $F' = A^tFA$.

2. Primitive representations of positive integers by quadratic forms

Proposition 1. Let f be a k-quadratic form. Then there exists a primitive representation X of a positive integer n by f if and only if there exists a (k-1) - quadratic form g of determinant $n.(\det(f))^{k-2}$ and a primitive representation A of g by f^{adj} such that $X = \Lambda \stackrel{k-1}{\Lambda} A$.

Proof. Let X be a primitive representation of n, so that, in particular, $X^tFX = n$. As $\overset{k-1}{\Lambda} E^* \simeq E$ (by contraction) and each element of $\overset{k-1}{\Lambda} E^*$ is decomposable (see [1] p.A III 171, Cor., which also holds for a free module), there exists an integral $k\times(k-1)$ matrix Y such that $\overset{k-1}{\Lambda} Y = \Delta X$ or, equivalently, $\Delta.\overset{k-1}{\Lambda} Y = X$. Let $G = Y^tF^{adj}Y$. By the symmetry of F^{adj} we have

$$\det G = \overset{k-1}{\Lambda} G = (\Lambda^{k-1}Y)^t(\overset{k-1}{\Lambda} F^{adj})(\overset{k-1}{\Lambda} Y) =$$

$$= (\overset{k-1}{\Lambda} Y)^t\ \Delta\Delta(\overset{k-1}{\Lambda} F^{adj}).\Delta\Delta\ (\overset{k-1}{\Lambda} Y) = X^t(F^{adj})^{adj}X =$$

$$= X^t.(\det F)^{k-2}.F.X = n.(\det F)^{k-2}\ .$$

Obviously Y is primitive because X is so. The converse is clear from the above. #

Remark. If k = 2, this proposition is vacous, so we will assume henceforth that $k > 2$.

From the preceding proposition we can assure that the map $A \longmapsto \Delta\ \overset{k-1}{\Lambda} A$ from the set $\mathcal{A}$ of primitive representations of (k-1) - quadratic forms of determinant $n.(\det(f))^{k-2}$ by f^{adj} to $R^*(n,f)$ is surjective. With this notation we have.

Proposition 2. If A and B are in $\mathcal{A}$, then $\overset{k-1}{\Lambda} A = \overset{k-1}{\Lambda} B$ if and only if there exists a matrix $C \in SL_{k-1}(\mathbb{Z})$ such that $A = BC$.

Proof. Let $v_1,\dots,v_{k-1}$ and $w_1,\dots,w_{k-1}$ be the respective columns of A and B. We can complete $v_1,\dots,v_{k-1}$ to a basis of $\mathbb{Z}^k$ with a suitable v, because A is primitive. Then

$w_1,\dots,w_{k-1}$, v is also a basis of $\mathbb{Z}^k$ with the same orientation as $v_1,\dots,v_{k-1},v$, because, by hypothesis, $v_1\wedge\dots\wedge v_{k-1} = w_1\wedge\dots\wedge w_{k-1}$.

If we now write each v_i, $1 \leq i \leq k$, as a linear combination of $w_1,\dots,w_{k-1},v$:

$$v_i = \lambda_1 w_1+\dots+\lambda_{k-1}w_{k-1}+\lambda v ,$$

we see, by making the wedge product with $v_1\wedge\dots\wedge v_{k-1}$, that $\lambda = 0$, from which follows the existence of C. The converse is obvious. #

<u>Proposition 3</u>. Let g and g' be two (k-1) - quadratic forms of determinant $n(\det(f))^{k-2}$. Then the images under $A \longmapsto \Delta \overset{k-1}{\Lambda} A$ of the subsets $R^*(g,f^{adj})$ and $R^*(g',f^{adj})$ of $\mathfrak{a}$ are either equal or disjoint according as g and g' are properly equivalent or not.

<u>Proof</u>. Let $G = A^tF^{adj}A$ and $G' = B^tF^{adj}B$. If $\overset{k-1}{\Lambda} A = \overset{k-1}{\Lambda} B$ then, by proposition 2, $A = BC$ for some $C \in SL_{k-1}(\mathbb{Z})$ and this implies that $G = C^tG'C$, i.e., that g and g' are properly equivalent, in which case $A \longmapsto AC$ establishes a bijection between $R^*(g,f^{adj})$ and $R^*(g',f^{adj})$, and these two sets have the same image in $R^*(n,f)$ because $\overset{k-1}{\Lambda} A = \overset{k-1}{\Lambda} (AC)$. #

<u>Remark</u>. In the above proof, observe that if $G = G'$, then C automatically belongs to $O^+(g)$.

From the preceding results the next theorem is obvious.

<u>Theorem 4</u>. $r^*(n,f) = \sum \frac{r^*(g,f^{adj})}{o^+(g)}$,

where the sum is extended to a complete set of representatives g of (k-1) - quadratic forms of determinant $n(\det f)^{k-2}$ modulo proper equivalence.

3. Evaluation of $r^*(g,f)$

For simplicity, instead of f^{adj}, we take f as a k - quadratic form and g a (k-1) - quadratic form primitively represented by f.

For each primitive representation B of g by f let us now construct a *square root* of - $\det(f)\, g^{adj}$ modulo det(g) :

Extend B to an oriented basis $\bar{B}$ of $\mathbb{Z}^k$ and put $\bar{G} = \bar{B}^t F \bar{B}$. Then $\bar{G}$ is an *extension* of G properly equivalent to F. In particular $\det \bar{G} = \det f$.

From $\bar{G}.\bar{G}^{adj} = \det(f).I_k$ we infer

$$\overset{2}{\Lambda}\bar{G} \;.\; \overset{2}{\Lambda}(\bar{G}^{adj}) = (\det(f))^2.I_{\binom{k}{2}} .$$

On the other hand, by the diagram (1),

$$\overset{2}{\Lambda}\bar{G} \;.\; (\overset{k-2}{\Lambda}\bar{G})^* = \det(f).I_{\binom{k}{2}} .$$

These two expressions yield

$$\overset{2}{\Lambda}(\bar{G}^{adj}) = \det(f).(\overset{k-2}{\Lambda}\bar{G})^* ,$$

from which, writing $G^{adj} = (G_{ij})$, $\bar{G}^{adj} = (\bar{G}_{ij})$, $\overset{2}{\Lambda}(\bar{G}^{adj}) = (\bar{G}^{(2)}_{IJ})$, and setting $I = \{i,k\}$, $J = \{j,k\}$, with $i,j < k$, we get, taking into account $\bar{G}_{kk} = \det(g)$ and $\operatorname{sgn}(I,I').\operatorname{sgn}(J,J') = (-1)^{i+j}$, that

$$(2) \qquad \bar{G}^{(2)}_{IJ} = \bar{G}_{ij}.\det(g) - \bar{G}_{ik}\,\bar{G}_{jk} = \det(f).(\overset{k-2}{\Lambda}\bar{G})^{*}_{I',J'} =$$

$$= \det(f).(\overset{k-1}{\Lambda}G)^{*}_{\{i\}',\{j\}'} = \det(f).G_{ij} ,$$

i.e.,

$$\bar{G}_{ik}\,\bar{G}_{jk} \equiv -\det(f).G_{ij} \pmod{\det(g)},$$ which means

that

$$\Big(\sum_{i=1}^{k-1} \bar{G}_{ik}\, x_i\Big)^2 \equiv -\det(f).G^{adj} \pmod{\det(g)}. \qquad \#$$

<u>Remark</u>. Obviously, if g and g' are properly equivalent then $r^*(g,f) = r^*(g',f)$.

<u>Proposition 5</u>. With our previous notation, the association $B \longmapsto \sum_{i=1}^{k-1} \bar{G}_{ik}\, x_i$ induces a well defined map from $R^*(g,f)$ to the set of homogeneus linear forms in $(\mathbb{Z}/_{\det(g)\mathbb{Z}})[x_1,\ldots,x_{k-1}]$ which are square-roots of $-\det(f).g^{adj}$ modulo $\det(g)$.

<u>Proof</u>. Let us extend B to another oriented basis $\tilde{B}$ of $\mathbb{Z}^k$. Then $\tilde{B} = \bar{B}T$ for some T of the form

$$(3) \qquad \left(\begin{array}{c|c} I_{k-1} & \begin{matrix}\alpha_1\\ \vdots \\ \alpha_{k-1}\end{matrix} \\ \hline 0\ldots 0 & 1 \end{array}\right)$$

If $\tilde{G} = \tilde{B}^t\ F\ \tilde{B}$, then $\tilde{G} = T^t\ \bar{G}\ T$, and by applying $\overset{k-1}{\lambda}(\ \ )^t$, i.e., passing to adjoints, we get

$$\tilde{G}^{adj} = T^{adj}\ \bar{G}^{adj}\ (T^t)^{adj} .$$

An explicit calculation for the last column of $\tilde{G}^{adj}$ gives

$$(4) \qquad \tilde{G}_{ik} = \bar{G}_{ik} - \alpha_i \det(g),$$

for $1 \le i < k$, so that

$$\tilde{G}_{ik} \equiv \bar{G}_{ik} \pmod{\det(g)}. \qquad \#$$

To the square roots of $-\det(f)\ g^{adj}$ modulo $\det(g)$, we next associate extensions of g. More precisely,

<u>Proposition 6.</u> Let f be a k-quadratic form, g a(k-1)-quadratic form and $b = b_1x_1+\ldots+b_{k-1}x_{k-1} \in \mathbb{Z}[x_1,\ldots,x_{k-1}]$ a square root of $-\det(f)\ g^{adj}$ modulo $\det(g)$. Then there exists a unique k-quadratic form $\bar{g}_b$ (with matrix $\bar{G}_b = (\bar{g}_{ij})$), extension of g with $\det \bar{G}_b = \det(f)$, such that $\bar{G}_{ik} = b_i$, for $1 \le i \le k$, where $(\bar{G}_{ij}) = (\bar{G}_b)^{adj}$. The entries of $\bar{G}_b$ are not necessarily integral.

Proof. From the expression (see formula (2))

(5) $\bar{G}_{ij}.\det g - b_i b_j = \det(f).G_{ij}$

we have that $\bar{g}_b^{adj}$ is unique and therefore $\bar{g}_b$ is unique too. #

Remark. The k-quadratic form $\bar{g}_b$ in the preceding proposition can have all its entries integral but this implies neither that $\bar{g}$ is equivalent to f nor that $\bar{g}_b$ belongs to the genus of f (cf. [2] Ch.9).

For each square root $b = b_1x_1+\ldots+b_{k-1}x_{k-1} \in \mathbb{Z}[x_1,\ldots,x_{k-1}]$ of $-\det(f).g^{adj}$ modulo $\det(g)$, such that $\bar{g}_b$ is properly equivalent to f, which implies that $\bar{g}_b$ has integral entries, let $\mathcal{T}^+(\bar{g}_b,f)$ denote the set of *proper* representations of $\bar{g}_b$ by f, i.e.,

$$\mathcal{T}^+(\bar{g}_b,f) = \{M \in SL_k(\mathbb{Z}) \mid M^tFM = \bar{G}_b\}.$$

Obviously, $\mathcal{T}^+(\bar{g}_b,f)$ is in bijection with $O^+(f)$.

We map $\mathcal{T}^+(\bar{g}_b,f)$ to $R^*(g,f)$ by sending each M to the submatrix obtained from M by deleting its last column.

Remark. Let φ the map induced from the union of the sets $\mathcal{T}^+(\bar{g}_b,f)$ to $R^*(g,f)$. Clearly φ is surjective : if $B \in R^*(g,f)$, extend B to a oriented basis $\bar{B}$ of $\mathbb{Z}^k$ and put $\bar{G} = \bar{B}^t F \bar{B}$. Then, if b is the square root associated to $\bar{G}^{adj}$ then by uniqueness (cf. prop. 6), $\bar{G} = \bar{g}_b$, so that $\bar{B} \in \mathcal{T}^+(\bar{g}_b,f)$ and $\varphi(\bar{B}) = B$.

<u>Proposition 7</u>. Let $b = b_1x_1+\dots+b_{k-1}x_{k-1}$ and $c = c_1x_1+\dots+c_{k-1}x_{k-1}$ be square roots of $-\det(f)\ g^{adj}$ modulo $\det(g)$ such that both $\bar{g}_b$ and $\bar{g}_c$ are properly equivalent to f. Then, the images under φ of $\mathfrak{T}^+(\bar{g}_b,f)$ and $\mathfrak{T}^+(\bar{g}_c,f)$ are either disjoint or coincide according to $b \not\equiv c$ or $b \equiv c \pmod{\det(g)}$ respectively. Moreover, the restriction of φ to each $\mathfrak{T}^+(\bar{g}_b,f)$ is injective.

<u>Proof</u>. Let $M \in \mathfrak{T}^+(\bar{g}_b,f)$ and $M' \in \mathfrak{T}^+(\bar{g}_c,f)$ be such that $\varphi(M) = \varphi(M')$. Then necessarily there exists $T \in SL_k(\mathbb{Z})$ of type (3) such that $M = M'T$. But then $\bar{G}_b = T^t\bar{G}_c\,T$ and proceeding as in the proof of proposition 5 we get (cf. formula (4))

$$b_i = c_i - \alpha_i \det(g) \ ,$$

which implies $b \equiv c$ (mod det g), and the injectivity statement if $b = c$. Moreover, from $\bar{G}_b = T^t\ \bar{G}_c\ T$ we see that $M \longmapsto MT$ establishes a bijection between $\mathfrak{T}^+(\bar{g}_c,f)$ and $\mathfrak{T}^+(\bar{g}_b,f)$ and as $\varphi(M) = \varphi(MT)$, because T is of type (3), these sets have the same image under φ.

Conversely, if $b \equiv c$ (mod det g), write $b_i = c_i - \alpha_i \det g$ for suitable integers α_i and consider

$$T = \left(\begin{array}{c|c} I_{k-1} & \begin{matrix}\alpha_1\\ \vdots \\ \alpha_{k-1}\end{matrix} \\ \hline 0\dots0 & 1 \end{array}\right) .$$

Then a simple calculation shows that the last column of $T^{adj}\ \bar{G}_c^{adj}\ (T^t)^{adj}$ is $(b_1,\ldots,b_{k-1},\det g)^t$ and so, by uniqueness (cf. propos. 6), $T^{adj}\ \bar{G}_c^{adj}\ (T^t)^{adj} = \bar{G}_b^{adj}$. In other words, $T^t\bar{G}_c T = \bar{G}_b$, and thus, as we have just seen, $\varphi(\mathcal{C}^+(\bar{g}_c,f) = \varphi(\mathcal{C}^+(\bar{g}_b,f)$. #

Corollary 8. If g is a (k-1)-quadratic form primitively represented by a k-quadratic form f, then

$$r^*(g,f) = o^+(f).s(g,f),$$

where s(g,f) denotes the total number of inequivalent (mod. det(g)) square roots $b = b_1x_1+\ldots+b_{k-1}x_{k-1}$ of $-\det(f).g^{adj}$ whose associated $\bar{g}_b$ are properly equivalent to f.

Remark. In fact s(g,f) is an invariant of the genus of g (for the definition of genus see [2] , Ch. 9). If g' is in the genus of g , then (cf. [2] , p. 140) there exists a form g" properly equivalent to g such that g" ≡ g' (mod M), for all M > 1. Then, obviously for each f_j in the genus of f, $s(g,f_j)$ is an invariant of the genus of g. We shall write $s(\text{gen } g,f_j)$.

3. Sums of squares

We now give some special properties that appear when $f = I_k$, i.e., $f(x_1\ldots,x_k) = x_1^2+\ldots+x_k^2$. We keep all the preceding notations.

Proposition 9. If g is primitively represented by I_k . Then, g is necessarily primitive.

Proof. Let p be a prime which divides all the entries of g. Then $p|\det(g)$ and $p|G_{ij}$ so that from (2), for $i = j$, we infer $p|\bar{G}_{ik}$, for all i, in which case, expanding the determinant of $\bar{G}^{adj}$ by its last column, we get $p|\det(\bar{G}^{adj}) = (\det I_k)^{k-1}$, which is impossible. #

Proposition 10. If $f = I_k$, the unique k-quadratic form $\bar{g}_b$ obtained in proposition 6 is in fact integral.

Proof. As in this case $(\bar{G}_b{}^{adj})^{adj} = \bar{G}_b$, it suffices to see that $\bar{G}_b{}^{adj}$ is integral. This assertion is immediate from the expression (5) .

$$\bar{G}_{ij}.\det(g) - b_i b_j = G_{ij}$$

together with the fact that $\sum_{i=1}^{k-1} b_i x_i$ is a square root of $-g^{adj}$, i.e., that

$$b_i b_j = -G_{ij} + \lambda_{ij} \det(g),$$

for suitable integers λ_{ij} . #

4. Applications

i) As a first application we give a formula for $r^*(n,I_3)$ known by Gauss, and which, in fact, motivated the developments of some techniques we have just already explained.

We assume that n is a positive integer non congruent to 0,4 or 7 modulo 8. Otherwise, as is well-known, n is not a primitive sum of three squares.

Under this condition, by theorem 4 and proposition 9,

$$r^*(n,I_3) = \sum \frac{r^*(g,I_3)}{o^+(g)}$$

where the sum is extended to a complete set of representatives g of primitive 2-quadratic forms of determinant n, i.e., of discriminant -4n, modulo proper equivalence. Moreover, in this sum we can reject the terms such that $r^*(g,I_3) = 0$. If $n > 3$, then we know $o^+(g) = 2$ (see [9] , p. 63). If $n = 3$, we observe that if $g = ax^2+2bxy+cy^2$ is a primitive, i.e., g.c.d.(a,b,c)=1, binary form represented by I_3, then g.c.d.(a,2b,c) = 2 so that $o^+(g) = 6$.

Thus, for $n > 3$, the above sum may be written as

$$r^*(n,I_3) = \frac{1}{2} \quad r^*(g,I_3) \quad ,$$

but by corollary 8, $r^*(g,I_3) = o^+(I_3).s = 24.s$.

Now, for a square - root of $-g^{adj}$(mod n), there exist a unique integral extension $\bar{g}_b$ of g, with det $\bar{g}_b = 1$ (cf. proposition 10). Such a $\bar{g}_b$ must be necessarily positive-definite and consequently properly equivalent to I_3, because I_3 has improper automorphs, that is, there exists $U \quad GL_3(\mathbb{Z})$, with det $U = -1$, such that $U^t I_3 U = I_3$ (cf. [6] , Section 9.2). This shows that s is equal to the total number of square-roots of $-g^{adj}$ (mod n). Let us now calculate these.

We have to solve for $b = b_1x_1+b_2x_2$ the congruences

(6) $b_1^2 \equiv -g_{22} \pmod{n}$

(7) $b_1b_2 \equiv g_{12} \pmod{n}$

(8) $b_2^2 \equiv -g_{11} \pmod{n}$

By the chinese remainder theorem, if

$n = 2^{\mu} p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ (μ = o or 1, $\alpha_i >$ o), this is reduced to solve the same system modulo 2^{μ} (if $\mu = 1$) and the different $p_i^{\alpha_i}$.

The case modulo 2 obviously has a unique solution.

Let us now consider the case modulo $p_i^{\alpha_i}$ (this occurs if and only if $n > 2$), and observe that g_{11} and g_{22} cannot both be divisible by p_i, since, otherwise, $p_i | g_{12}$ and g would not be primitive. So, assume for instance, that $p_i \nmid g_{22}$. Then (6) has exactly 2 solutions (cf. [5] p.44), because g is primitively represented by I_3 and this implies the existence of solutions for the above system as we have seen in §2. But, for each solution b_1 of (6), there exists a unique solution b_2 of (7) . this is because b_1 is invertible (mod $p_i^{\alpha_i}$), since $p_i \nmid g_{22}$. This solution for b_2 in (7) satisfies (8) automatically :

$$b_2^2 \equiv (b_1^{-1}g_{12})^2 \equiv -g_{22}^{-1}\, g_{12}^2 \equiv -g_{22}^{-1}\cdot(g_{11}\cdot g_{22})$$

$$\equiv -g_{11} \pmod{p_i^{\alpha_i}} .$$

Thus the above system has exactly 2 solutions modulo $p_i^{\alpha_i}$ and, consequently, 2^s solutions modulo n. So we have

<u>Theorem 11</u>. If $n \not\equiv 0,4,7 \pmod 8$ is an integer greater than 3, then

$$r^*(n,I_3) = 12.2^t.\ell \quad ,$$

where ℓ is the number of proper equivalence classes of primitive binary quadratic forms of determinant n which are primitively represented by I_3 and t is the number of distinct odd prime factors which divide n. #

ii) Recall (cf. [7]) that the weight of the number of primitive representations of n by all the forms in the genus of f is

$$\mu^*(n,\ \text{gen}\ f) := \sum_{i=1}^{k} \frac{r^*(n,f_j)}{o^+(f_j)}$$

with the f_j running over a complete set of representatives of the classes in the genus of f and k denotes the number of proper classes in the genus of f.

Now, let $\mu(\text{gen}\ f)$ be the weight of the genus of f, i.e.,

$$\mu(\text{gen}\ f) = \sum_{j=1}^{k} \frac{1}{o^+(f_j)}$$

So, if $s(\text{gen}\ g_i,\ \text{gen}\ f)$ is the number of square roots of $-\det(f^{adj}).g_i^{adj}$ whose associated $\bar{g}_b$ are in the same of f, we obtain

Proposition 12. $\mu^*(n, \text{gen } f) = \sum_{i=1}^{m} s(\text{gen } g_i, \text{gen } f).\mu(\text{gen } g_i)$

where m is the number of genera of (k-1)-quadratic forms of determinant $\det(f)^{k-2}.\ n$.

Proof. We first observe that $o^+(f^{adj}) = o^+(f)$, and so, by theorem 4 and corollary 8, we have

$$\frac{r^*(n,f_j)}{o^+(f_j)} = \sum \frac{s(g_i,f_j)}{o^+(g_i)} = \sum_{i=1}^{m} s(\text{gen } g_i, f_j).\mu(\text{gen } g_i) ,$$

which concludes the proof, because obviously
$s(\text{gen } g_i, \text{gen } f) = \sum_{j=1}^{k} s(\text{gen } g_i, f_j)$. #

iii) We now consider the congruent number problem (see [8]), and denote by h(-4n) the number of classes of primitive binary quadratic forms of discriminant -4n, i.e., of determinant n. We give another proof of the fact (cf. [8]) that no prime congruent to 3 modulo 8 is a congruent number.

Proposition 13. Let $p \equiv 3 \pmod 8$ be a prime integer. Then p is not congruent.

Proof. We let f stand for the quadratic form $2x^2+y^2+32z^2$ and g for $2x^2+y^2+8z^2$, and use the fact that if n is congruent then $r^*(n,g) = 2r^*(n,f)$, for n a square free positive integer (see [8]).

By applying Siegel's "Hauptsatz" [7] we know that $r^*(n, \text{gen } g) = 4h(-4n)$.

As the genus of g consist of a unique class (see [4]), we conclude that for a congruent square-free positive integer, we must have $r^*(n,f) = 2h(-4n)$.

On the other hand, we have seen that $r^*(n,f) = 4t$, for some positive t, so, if n is congruent then h(-4n) is even.

Now, take a prime $p \equiv 3 \pmod 8$. We have that h(-p) is odd (cf. [9] p. 112 Korollar), and that h(-4p) = 3 h(-p) (cf. Ex. 8)d), p. 74 cf. [9]). We thus conclude that p is not congruent. #

References.

[1] Bourbaki, N.: *Algèbre*, Chap. 3. Hermann, 1970.

[2] Cassels, J.W.S.: *Rational Quadratic Forms*, Academic Press, 1978.

[3] Gauss, C.F.: *Disquisitiones Arithmeticae*, Lipsiae, 1801. English traslation: Arthur A. Clarke, 1966, New Haven: Yale Univ. Press.

[4] Jones, B.W., Pall, G.: *Regular and semiregular positive ternary quadratic forms*. Acta Math. vol. 70 (1939), 165-191.

[5] Loo Keng, Hua: *Introduction to Number theory*. Springer 1982.

[6] Scharlau, W., Opolka, H.: *Von Fermat bis Minkowski.* Springer, 1980.

[7] Siegel, C.L.: *Uber die analytische theorie der quadratischen Formen.* Ann. of Math. 36 (1935), 527-606. Gesammelte Abhand., Band 1, Springer, 1966.

[8] Tunell, J.B.: *A classical diophantine problem and modular forms of weight* 3/2. Invent. Math. 72 (1983), 323-334.

[9] Zagier, D.B.: *Zeta funktionen und quadratische Körper.* Springer, 1981.

publicacions edicions universitat de barcelona

Dipòsit Legal, B.: 22.341-1986
BARCELONA-1986