JOURNAL OF NUMBER THEORY 27, 273–284 (1987)

Arithmetic Behaviour of the Sums of Three Squares

A. ARENAS AND P. BAYER

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

Communicated by D. Zagier

Received July 5, 1986; revised August 3, 1986

Let $n \neq 4^a(8b+7)$ be an integer. We deal with the problem of the solvability of the equation $n = x_1^2 + x_2^2 + x_3^2$ in integers x_1, x_2, x_3 prime to n. By a theorem of Vila (*Arch. Math.* **44** (1985), 424–437), the existence of such a solution implies that every central extension of the alternating group A_n, for $n \equiv 3 \pmod 8$, can be realized as a Galois group over $\mathbf{Q}$. © 1987 Academic Press, Inc.

INTRODUCTION

Let $n \neq 4^a(8b+7)$ be an integer and let $l(n)$ be the maximum value of l such that there exists a representation of n as a sum of 3 integral squares with l summands prime to n. Clearly $l(n) \leqslant 3$ for all n (by definition) and $l(n) \leqslant 2$ for all n not prime to 10 (because the sum of 3 squares prime to 2 is odd and the sum of 3 squares prime to 5 is $\not\equiv 0 \pmod 5$).

The purpose of this paper is the determination of $l(n)$. Our main result, Theorem 3, shows that for all but finitely many of the integers n all of whose prime factors belong to a fixed finite set of prime numbers, one has:

$$l(n) = \begin{cases} 3 & \text{if} \quad \text{g.c.d.}(n, 10) = 1, \\ 2 & \text{if} \quad \text{g.c.d.}(n, 10) \neq 1. \end{cases}$$

That is, the above inequalities are equalities when n increases keeping its radical fixed.

The proof of the theorem relies on an asymptotic evaluation of the number of solutions of the equation

$$n = x_1^2 + x_2^2 + x_3^2,$$

which are of a suitable type.

0022-314X/87 $3.00

The main term in the evaluation of $l(n)$ is obtained recursively, by applying Siegel's formula on the average number of representations of an integer by a quadratic form. It is relevant for our purposes to have an exact knowledge of all the p-adic densities involved. Those corresponding to prime numbers which divide the determinant of the form are calculated in Proposition 3, since they are not covered by Siegel.

Recent results of Schulze–Pillot [5] allow to relate the main term to Fourier coefficients of Eisenstein series of weight $\frac{3}{2}$, and the error term to Fourier coefficients of cusp forms of the same weight.

Since all integers with a given radical fall into finitely many quadratic families $\{n_0 s^2\}$, Shimura's theory on liftings of modular forms from half-integral to integral weight is applicable and the error term can be controlled. Clearly, the estimation of the error term becomes important only when n increases in such quadratic classes. For this reason the square-free case was handled separately in a previous paper [1].

Finally, we give an application to Galois theory which was the main motivation for the study of the problem: By Vila's results [8], it is now an immediate consequence of Theorem 3 that the universal central extension of the alternating group A_n can be realized as a Galois group over $\mathbf{Q}(T)$ for $n \equiv 3 \pmod 8$, and n large enough, in the above sense.

The authors want to express their gratitude to E. Nart and to the referees to their careful reading and improvements of an earlier version of this paper.

1. The Main Term in the Determination of $l(n)$

As in [1], given a positive integer $n \not\equiv 0, 4, 7 \pmod 8$, we define the level of n as the maximum value of l such that there exists a representation of n as a sum of three integer squares with l summands prime to n. It will denoted by $l(n)$.

We consider also the functions

$$g_1(n) = \frac{s_3(n)}{r(n, I_3)},$$

$$g_2(n) = \frac{s_2(n) - 2s_3(n)}{r(n, I_3)},$$

$$g_3(n) = \frac{s_1(n) - s_2(n) + s_3(n)}{r(n, I_3)},$$

where

$$s_i(n) = \rho_i \sum_{(1)} (-1)^i \mu(a_1)\, \mu(a_2)\, \mu(a_3)\, r(n, \langle a_1^2, a_2^2, a_3^2 \rangle),$$

for $i=1$, 2, 3. The sum (1) is taken over those square-free positive integers a_j, $j=1,2,3$, such that $1<a_j|n$ for $j\leqslant i$ and $a_j=1$ for $j>i$. We take $\rho_i=3-2[i/3]$.

We recall [1, Proposition 1] that $l(n)\geqslant i$ is equivalent to $g_i(n)<1$.

Let $f=\langle a_1^2, a_2^2, a_3^2\rangle$ be a quadratic form such that $r(n, f)\neq 0$, and where the a_j's are assumed to be square-free positive integers dividing n. Let

$$d_{ij}=\text{g.c.d.}(a_i, a_j), \qquad 1\leqslant i, j\leqslant 3, i\neq j,$$
$$d_{123}=\text{g.c.d.}(a_1, a_2, a_3),$$
$$d=d_{123}^{-2}d_{12}d_{13}d_{23}.$$

The possible common factors of the a_j's can be avoided by setting

$$r(n, \langle a_1^2, a_2^2, a_3^2\rangle)=r(nd^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle),$$

where $b_i=d_{ij}^{-1}d_{ik}^{-1}d_{123}a_i$, for $i=1$, 2, 3. In particular we have g.c.d.$(b_i, b_j)=1$, for $i\neq j$ and g.c.d.$(d, b_i)=1$, for $i=1$, 2, 3.

Throughout this paper, a_i, b_i, for $i=1$, 2, 3, and d will have the meaning just explained.

Next, we introduce the average alternating sums

$$S_i(n)=\rho_i \sum_{(1)} (-1)^i \mu(a_1)\,\mu(a_2)\,\mu(a_3)\, r(nd^{-2}, \text{gen}\langle b_1^2, b_2^2, b_3^2\rangle),$$

for $i=1$, 2, 3. The sum (1) and ρ_i are defined as for $s_i(n)$. Here gen f stands for the genus of the quadratic form f (see [7]).

Note that if n is square-free, the average alternating sums $S_i(n)$ are equal to the ones introduced in [1].

Now we define, as in [1],

$$S_i'(n)=r(n, I_3)^{-1}\, S_i(n), \qquad i=1, 2, 3.$$

We make the convention that $S_i'(1)=0$, for $i=1, 2, 3$.

PROPOSITION 1. *If* $n\not\equiv 0$, 4, 7 (mod 8), *then*

$$S_i'(n)=\rho_i \sum_{(1)} (-1)^i \mu(a_1)\,\mu(a_2)\,\mu(a_3) \prod_{q|a_1a_2a_3} \frac{\partial_q(nd^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle)}{q\,\partial_q(n, I_3)}$$

for $i=1$, 2, 3, *where* q *runs over all prime factors of* $a_1a_2a_3$, *and* ∂_q *stands for the q-adic density* (*see* [7]).

Proof. It suffices to apply Siegel's formula [7] and observe that

$$\partial_q(nd^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle)=\partial_q(n, I_3),$$

for all prime q not dividing $a_1 a_2 a_3$ and that

$$\partial_\infty(nd^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle)\cdot\partial_\infty(n, I_3)^{-1} = \prod_{q|a_1a_2a_3} q^{-1},$$

for q prime.

The preceding formulae allow to extend the definition of the $S_i'(n)$ to those integers $n \equiv 7 \pmod 8$. This extension will be needed later in an inductive step.

We define the main term $G_i(n)$ in the determination of the level of n as

$$G_1(n) = S_3'(n),$$
$$G_2(n) = S_2'(n) - 2S_3'(n),$$
$$G_3(n) = S_1'(n) - S_2'(n) + S_3'(n).$$

Since the evaluation of the main term leads to consider quotients of densities $\partial_q(nd^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle)\cdot\partial_q(n, I_3)^{-1}$, we begin by studying these densities first.

We denote by $v_p(n)$ the p-adic valuation of n.

Definition. Let $n \not\equiv 0, 4 \pmod 8$ be a positive integer and let p be a prime such that $v_p(n) = \alpha > 0$. Writing $n = mp^\alpha$, we introduce the following notation:

$$\frac{\partial_p(mp^\alpha d^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle)}{p\,\partial_p(mp^\alpha, I_3)} = \begin{cases}\partial_p'(m,\alpha) & \text{if } p|b_i \text{ for exactly one } i,\\ \partial_{p^2}'(m,\alpha) & \text{if } p|d.\end{cases}$$

That is, the above quotient is denoted by $\partial_p'(m, \alpha)$ if p divides exactly one a_i, and by $\partial_{p^2}'(m, \alpha)$ if p divides more than one a_i.

From the definition of p-adic density (cf. [7]) it follows immediately that

(i) $\partial_p'(m, \alpha) = \partial_p(n, \langle p^2, 1, 1\rangle)/p\,\partial_p(n, I_3)$,

(ii) $\partial_{p^2}'(m, \alpha) = \partial_p(np^{-2}, I_3)/p\,\partial_p(n, I_3)$.

Siegel in his paper [7] about representations of positive integers n by integral quadratic forms f gave formulae to calculate the p-adic densities $\partial_p(n, f)$ when $p \nmid 2 \det f$. In the case $f = I_3$, we get

Proposition 2. *Let n be a positive integer such that $4 \nmid n$. Let p be a prime such that $v_p(n) = \alpha > 0$ and write $n = mp^\alpha$. Then:*

(i) $$\partial_p(n, I_3) = \begin{cases}(1+p^{-1})(1-p^{-(\beta+1)}), & \textit{if } \alpha = 2\beta+1,\\ (1+p^{-1})(1-p^{-\beta}) + (p^2-1)p^{-(\beta+2)}\{1-(-m/p)p^{-1}\}^{-1} & \\ \qquad\qquad \textit{if } \alpha = 2\beta,\end{cases}$$

for $p \neq 2$.

$$\text{(ii)}\quad \partial_2(n, I_3) = \begin{cases} 3/2 & \textit{if} \;\; n \equiv 1, 2, 5, 6 \pmod 8, \\ 1 & \textit{if} \;\; n \equiv 3 \pmod 8, \\ 0 & \textit{if} \;\; n \equiv 7 \pmod 8). \end{cases}$$

Proof. (i) This is an immediate consequence of [7, (Hilfssatz 16)]. (ii) $\partial_2(n, I_3)$ is reduced to count $r_{2^3}(n, I_3)$, from which the result follows.

Next, we explicit the values of $\partial_p(n, \langle p^2, 1, 1\rangle)$ when $v_p(n) > 0$.

For a positive integer n let $\varepsilon_n = 1$ if $n \equiv 1 \pmod 4$, and $\varepsilon_n = i$ if $n \equiv 3 \pmod 4$.

The densities appearing in the next proposition are not covered by Siegel.

PROPOSITION 3. *Let n be a positive integer such that $4 \nmid n$. Let p be a prime such that $v_p(n) = \alpha > 0$ and write $n = mp^\alpha$. Then*:

$$\text{(i)}\quad \partial_p(n, \langle p^2, 1, 1\rangle)$$

$$= \begin{cases} 2 + \varepsilon_p^2(1 - p^{-1}) - p^{-\beta}(1 + p^{-1}) & \textit{if} \;\; \alpha = 2\beta + 1, \\ 2 + \varepsilon_p^2(1 - p^{-1}) - \{1 - (-m/p)\}\, p^{-\beta} & \textit{if} \;\; \alpha = 2\beta, \end{cases}$$

for $p \neq 2$.

$$\text{(ii)}\quad \partial_2(n, \langle 2^2, 1, 1\rangle) = \begin{cases} 3/2 & \textit{if} \;\; n \equiv 1, 5 \pmod 8, \\ 1 & \textit{if} \;\; n \equiv 2, 6 \pmod 8, \\ 0 & \textit{if} \;\; n \equiv 3, 7 \pmod 8). \end{cases}$$

Proof. (i) In order to calculate these densities we consider the following Gauss–Weber sums associated to a quadratic ternary form $f(x_1, x_2, x_3)$,

$$\theta_{p^s}(m, f) = \sum_{x \in (\mathbf{Z}/p^s\mathbf{Z})^3} \exp\left(\frac{2\pi\, \mathrm{imf}(x)}{p^s}\right);$$

for $m \in (\mathbf{Z}/p^s\mathbf{Z})^*$.

Each $\xi \in \mathbf{Q}_p/\mathbf{Z}_p$, $\xi \neq 0$ admits a unique representative in $\mathbf{Q}_p$ of the form mp^{-s} with $0 < m < p^s$, g.c.d.$(m, p) = 1$. This allows us to define

$$\theta(\xi, f) = p^{-3s}\theta_{p^s}(m, f).$$

Then, one can see (cf. [2]) that

$$\partial_p(n, f) = \sum_{\xi \in \mathbf{Q}_p/\mathbf{Z}_p} \theta(\xi, f)\langle \xi, -n\rangle,$$

where $\langle\ ,\ \rangle$ denotes the usual pairing between $\mathbf{Z}_p$ and $\mathbf{Q}_p/\mathbf{Z}_p$.

Let

$$B_s(n, f) = \sum_{\substack{\xi \in \mathbf{Q}_p/\mathbf{Z}_p \\ v_p(\xi) = -s}} \theta(\xi, f)\langle \xi, -n \rangle.$$

From now on, f will be the quadratic form $\langle p^2, 1, 1 \rangle$. Then, for any $m \in (\mathbf{Z}/p^s\mathbf{Z})^*$,

$$\theta_{p^s}(m, f) = p\theta_{p^s}(m, I_3) \qquad \text{if} \quad s \geqslant 3.$$

Therefore

$$B_s(n, f) = pB_s(n, I_3) \qquad \text{for} \quad s \geqslant 3.$$

So

$$\partial_p(n, f) = \sum_{s > 2} pB_s(n, I_3) + B_2(n, f) + B_1(n, f) + B_0(n, f).$$

Taking into account well-known results about the values taken for the ordinary Gauss sums (cf. [4, Chap. 7]), it is easy to evaluate the sums $B_s(n, f)$. They are given by:

$$\text{(i)} \quad B_s(n, f) = \begin{cases} -p^{-s/2}(p-1) & \text{if} \quad s \leqslant \alpha \\ -p^{-(\alpha+1)/2} & \text{if} \quad s = \alpha + 1 \\ 0 & \text{if} \quad s > \alpha + 1, \end{cases}$$

s even, $\geqslant 2$.

$$\text{(ii)} \quad B_s(n, f) = \begin{cases} 0 & \text{if} \quad s \leqslant \alpha \\ (-m/p)\, p^{-\alpha/2} & \text{if} \quad s = \alpha + 1 \\ 0 & \text{if} \quad s > \alpha + 1, \end{cases}$$

s odd, $\geqslant 3$.

To achieve the asserted results, it suffices now to substitute these values in the expression of $\partial_p(n, f)$. (ii) If $p = 2$, the calculation of $\partial_2(n, f)$ can be reduced to that of $r_{2^3}(n, f)$.

If $n \not\equiv 0, 4 \pmod 8$ is a positive integer, we consider a prime p dividing n such that $v_p(n) = \alpha > 0$ is even if not all the exponents in the factorization of n are odd. We can further assume that $p \neq 2$ (unless $n = 2$, in which case the values of $\partial_p(2, f)$, for $f = I_3$ or $\langle 2^2, 1, 1 \rangle$, were already calculated). We shall write $n = mp^\alpha$. Under this convention we have

LEMMA 1. *With our previous notations, if q is a prime dividing $a_1a_2a_3$, $q \neq p$, it holds*:

(i) $\partial_q(mp^\alpha, I_3) = \partial_q(m, I_3)$.

(ii) $\partial_q(mp^\alpha d^{-2}, \langle b_1^2, b_2^2, b_3^2 \rangle)$

$$= \begin{cases} \partial_q(md^{-2}, \langle b_1^2, b_2^2, b_3^2 \rangle & \text{if } p \nmid a_1a_2a_3, \\ \partial_q(md^{-2}, \langle b_1^2 p^{-2}, b_2^2, b_3^2 \rangle) & \text{if } p \mid a_1, p \nmid a_2a_3, \\ \partial_q(md^{-2}p^2, \langle b_1^2, b_2^2, b_3^2 \rangle) & \text{if } p^2 \mid a_1a_2. \end{cases}$$

Proof. (i) This follows, under our convention on p^α, immediately from Proposition 2.

(ii) Let us suppose that $p \nmid a_1a_2a_3$.

If q divides exactly one a_i, say a_1, then, as is easily seen

$$\partial_q(mp^\alpha d^{-2}, \langle b_1^2, b_2^2, b_3^2 \rangle) = \partial_q(mp^\alpha, \langle q^2, 1, 1 \rangle).$$

Similarly, $\partial_q(md^{-2}, \langle b_1^2, b_2^2, b_3^2 \rangle) = \partial_q(m, \langle q^2, 1, 1 \rangle)$. Applying now Proposition 3, under the convention made on p^α, we get

$$\partial_q(mp^\alpha, \langle q^2, 1, 1 \rangle) = \partial_q(m, \langle q^2, 1, 1 \rangle).$$

If q divides more than one a_i, then

$$\partial_q(mp^\alpha d^{-2}, \langle b_1^2, b_2^2, b_3^2 \rangle) = \partial_q(mp^\alpha d^{-2}, I_3)$$

and

$$\partial_q(md^{-2}, \langle b_1^2, b_2^2, b_3^2 \rangle) = \partial_q(md^{-2}, I_3).$$

By Proposition 2, account being taken of the convention made on p^α, we get

$$\partial_q(mp^\alpha d^{-2}, I_3) = \partial_q(md^{-2}, I_3).$$

This proves the first case of (ii).

The other two cases of (ii) can be proved in a similar manner.

If one substitutes all the values obtained in Propositions 2 and 3 in the corresponding expressions of the main term, there appear rather complicated alternating sums. However, the preceding lemma allows to simplify most of the densities by comparing $G_i(n)$ with $G_i(m)$, $m = np^{-\alpha}$. In this way, we obtain the following recursive formulae for the evaluation of the main term.

THEOREM 1. *Let n be a positive integer such that $4 \nmid n$ and write $n = mp^{\alpha}$, with $\alpha = v_p(n) > 0$. We assume that α is even if not all the exponents occurring in the factorization of n are odd. Then*:

$$\begin{aligned} \text{(i)} \quad G_1(n) &= G_1(m) + \partial'_p(m, \alpha)(G_2(m) - G_1(m)) \\ &\quad + \partial'_{p^2}(m, \alpha)(1 - G_2(m)), \\ \text{(ii)} \quad G_2(n) &= G_2(m) + 2\partial'_p(m, \alpha)(G_3(m) - G_2(m)) \\ &\quad + \partial'_{p^2}(m, \alpha)(1 + G_2(m) - 2G_3(m)), \\ \text{(iii)} \quad G_3(n) &= G_3(m) + (3\partial'_p(m, \alpha) - 2\partial'_{p^2}(m, \alpha))(1 - G_3(m)). \end{aligned}$$

Proof. Let us consider the sums $S'_i(n)$. We break them up into partial sums according to the number of a_j's such that $p | a_j$.

Applying the results of Lemma 1 and the definitions of $\partial'_p(m, \alpha)$ and $\partial'_{p^2}(m, \alpha)$ we obtain

$$\begin{aligned} S'_1(mp^{\alpha}) &= S'_1(m) + \partial'_p(m, \alpha)(3 - S'_1(m)), \\ S'_2(mp^{\alpha}) &= S'_2(m) + 2\partial'_p(m, \alpha)(S'_1(m) - S'_2(m)) \\ &\quad + \partial'_{p^2}(m, \alpha)(3 - 2S'_1(m) + S'_2(m)), \\ S'_3(mp^{\alpha}) &= S'_3(m) + \partial'_p(m, \alpha)(S'_2(m) - 3S'_3(m)) \\ &\quad + \partial'_{p^2}(m, \alpha)(1 - S'_2(m) + 2S'_3(m)). \end{aligned}$$

So, the assertion of the theorem follows from the definition of the main term.

2. BOUND OF THE MAIN TERM

In order to bound the main term we first bound the values of $\partial'_p(m, \alpha)$ and $\partial'_{p^2}(m, \alpha)$. From Propositions 2 and 3, we get

PROPOSITION 4. *Let $n \not\equiv 0,\ 4 \pmod 8$ be a positive integer. Write $n = mp^{\alpha}$, with $v_p(n) = \alpha > 0$ and $p \neq 2$. Then*

$$\text{(i)} \quad \partial'_p(m, \alpha) = \frac{(2 + \varepsilon_p^2)p^{\beta+1} - \varepsilon_p^2 p^{\beta} - (p+1)}{(p+1)(p^{\beta+1} - 1)} \qquad \text{if} \quad \alpha = 2\beta + 1.$$

$$\text{(ii)} \quad \partial'_p(m, \alpha) = \frac{(2 + \varepsilon_p^2)p^{\beta} - \varepsilon_p^2 p^{\beta-1} - \{1 - (-m/p)\}}{(p+1)[(p^{\beta} - 1) + (1 - p^{-1})\{1 - (-m/p)p^{-1}\}^{-1}]} \qquad \text{if} \quad \alpha = 2\beta.$$

$$\text{(iii)} \quad \partial'_{p^2}(m, \alpha) = \frac{p^{\beta} - 1}{p^{\beta+1} - 1} \qquad \text{if} \quad \alpha = 2\beta + 1.$$

$$\text{(iv)}\quad \partial'_{p^2}(m,\alpha)=\begin{cases} p^{-1} & \textit{if}\ \left(\dfrac{-m}{p}\right)=1,\quad \alpha=2\beta,\\ \dfrac{p^\beta+p^{\beta-1}-2}{p^{\beta+1}+p^\beta-2} & \textit{if}\ \left(\dfrac{-m}{p}\right)=-1,\ \alpha=2\beta.\end{cases}$$

(vii) *if* $p=2$, *then*

$$\partial'_2(m,1)=\tfrac{1}{3},\qquad \partial'_{2^2}(m,1)=0.$$

COROLLARY. *Let* $n \not\equiv 0, 4 \pmod 8$ *be a positive integer. Write* $n=mp^\alpha$ *with* $v_p(n)=\alpha>0$ *and* $p\neq 2$. *Then.*

(i) $0\leqslant \partial'_p(m,\alpha)<\frac{1}{2}$.

(ii) $0\leqslant \partial'_{p^2}(m,\alpha)\leqslant p^{-1}$

(iii) $0\leqslant 3\partial'_p(m,\alpha)-2\partial'_{p^2}(m,\alpha)<\frac{7}{13}$, *if* $p\neq 5$, *and* $3\partial'_5(m,\alpha)-2\partial'_{5^2}(m,\alpha)=1$.

(iv) $0\leqslant 2\partial'_p(m,\alpha)-\partial'_{p^2}(m,\alpha)<\frac{4}{5}$.

Proof. The proof of the above statements is elementary. One needs only to consider the different cases: $p\equiv 1$ or $3 \pmod 4$, α being odd or even, $(-m/p)=1$ or -1, and use the expressions of Proposition 4.

THEOREM 2. *Let* $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ *be a positive integer with* $4\nmid n$. *Then there exist constants* $c_i=c_i(p_1\cdots p_k)$ *such that*

$$G_i(n)<c_i(p_1\cdots p_k)<1,$$

for $i=1, 2, 3$ *if* g.c.d.$(n, 10)=1$; *and* $i=1, 2$ *if* g.c.d.$(n, 10)\neq 1$. *In the latter case we have* $G_3(n)=1$.

Proof. Let us suppose that g.c.d.$(n, 10)=1$. We prove the assertion of the theorem by induction on the number of distinct prime factors of n.

If $p\neq 2, 5$. Then, by the corollary of Proposition 4 we have

$$G_3(p^\alpha)=3\partial'_p(1,\alpha)-2\partial'_{p^2}(1,\alpha)<\tfrac{7}{13}<1;$$

and we can take $c_3(p)=\frac{7}{13}$. Now, let $n=p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}p_k^{\alpha_k}$, with $k>1$ and $p_k^{\alpha_k}$ chosen as in Theorem 1, and write $m=p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}$. Then, we have, by virtue of Theorem 1, the corollary of Proposition 4 and the induction hypothesis, that

$$G_3(n)<G_3(m)+\tfrac{7}{13}(1-G_3(m))=\tfrac{7}{13}+\tfrac{6}{13}G_3(m)<c_3(p_1\cdots p_k)<1;$$

with

$$c_3(p_1\cdots p_k):=\tfrac{7}{13}+\tfrac{6}{13}c_3(p_1\cdots p_{k-1}).$$

By induction and applying again Theorem 1 and the corollary of Proposition 4, we get that $0 \leqslant G_1(n) \leqslant G_2(n) \leqslant G_3(n) < 1$. Therefore, it suffices to take $c_1 = c_2 = c_3$.

Let us now consider the case g.c.d.$(n, 10) \neq 1$. If $2 \mid n$, proceeding by induction on the number of distinct prime factors of n, and taking into account Theorem 1 and the corollary of Proposition 4, we get $G_3(n) = 1$. On the other hand, in order to prove that there exist $c_2(p_1 \cdots p_k)$ such that $G_2(n) < c_2 < 1$, we write $n = mp_k^{\alpha_k}$ in accordance with Theorem 1, where p_k can be taken different from 2, unless $n = 2$ in which case $G_2(2) = \partial'_{2^2}(1, 1) = 0$. The fact that $G_3(m) = 1$, together again with Theorem 1 and the corollary of Proposition 4, allows us to estimate $G_2(n)$ also by induction as

$$\begin{aligned} G_2(n) &= G_2(m) + (2\partial'_{p_k}(m, \alpha_k) - \partial'_{p_k^2}(m, \alpha_k))(1 - G_2(m)) \\ &< G_2(m) + \tfrac{4}{5}(1 - G_2(m)) < c_2(p_1 \cdots p_k) < 1, \end{aligned}$$

with

$$c_2(p_1 \cdots p_k) := \tfrac{4}{5} + \tfrac{1}{5} c_2(p_1 \cdots p_{k-1}).$$

If $5 \mid n$, we proceed in an analogous way, distinguishing the case $p_k = 5$ from the one in which $p_k \neq 5$.

By induction and applying again Theorem 1 and the corollary of Proposition 4, we get $0 \leqslant G_1(n) \leqslant G_2(n) < G_3(n) = 1$. Therefore, it suffices to take $c_1 = c_2$.

3. The Error Term in the Determination of $l(n)$. Asymptotic Behaviour of $l(n)$

In this section we first estimate the growth of $r(n, f) - r(n, \text{gen } f)$.

Lemma 2. *Let $n = n_0 s^2$ be a positive integer, $n \not\equiv 0, 4, 7 \pmod 8$, where n_0 is its square-free part. Let $f = \langle b_1^2, b_2^2, b_3^2 \rangle$ be a quadratic form such that $b_i \mid n$, g.c.d.$(b_i, b_j) = 1$, for $i \neq j$, and b_i square-free for $i = 1, 2, 3$. Then*

$$r(n, f) - r(n, \text{gen } f) = O_{\varepsilon, n_0, f}(s^{1/2 + \varepsilon}),$$

for evey $\varepsilon > 0$.

Proof. Under these conditions, the theta series $\theta(f, z)$ associated to f belongs to the space $M_0(\frac{3}{2}, 4b_1^2 b_2^2 b_3^2)$ of modular forms of weight $\frac{3}{2}$ with respect to $\Gamma_0(4b_1^2 b_2^2 b_3^2)$. Then, Theorem 4.6 of [3] implies that gen f = spn f, where spn f stands for the spinorial genus of f.

By results of Schulze–Pillot [5], we have that $\theta(f, z) - \theta(\operatorname{spn} f, z)$ lies in $U^{\perp}$, where $U^{\perp}$ is the orthogonal complement, in the space of cusp forms $S_0(\frac{3}{2}, 4b_1^2 b_2^2 b_3^2)$ of the space $U = \oplus U(n_0)$, n_0 square-free, with

$$U(n_0) = S_0(\tfrac{3}{2}, 4b_1^2 b_2^2 b_3^2) \cap \left\{ f(z) = \sum_{n=1}^{\infty} \psi(n)\, n \exp(2\pi i n_0 n^2 z) \right\},$$

with $\psi(n)$ a character modulo an integer r such that $r^2 n_0 \mid b_1^2 b_2^2 b_3^2$.

If n runs into a quadratic class $n = n_0 s^2$, then by Shimura's n_0-lifting [6] and the theorem of Eichler–Igusa (i.e., Ramanujan–Petersson for weight 2), we know the growth of the Fourier coefficients $a(n)$ of a cusp form g lying in $U(n_0)^{\perp}$, in the sense that

$$a(n_0 s^2) = O_{\varepsilon, n_0 . g}(s^{1/2 + \varepsilon}),$$

for every $\varepsilon > 0$ (cf. [5, Hilfssatz 5]).

Therefore, it suffices to apply these results to the coefficients of $\theta(f, z) - \theta(\operatorname{spn} f, z)$.

THEOREM 3. *Let* $n = n_0 s^2$, $n \not\equiv 0, 4, 7 \pmod 8$, let $m_0 = \operatorname{rad} n$ *be the product of the distinct prime factors of n. For every* $\varepsilon > 0$, *we have*

$$g_i(n) - G_i(n) = O_{\varepsilon, m_0}(s^{-1/2 + \varepsilon}),$$

for $i = 1, 2, 3$.

Proof. Immediate from Lemma 2 if we bear in mind that all positive integers whose prime factors belong to a fixed finite set fall into finitely many quadratic families $\{n_0 s^2\}$ and that for every $\varepsilon > 0$, $r(n, I_3)^{-1} = O_\varepsilon(n^{-1/2 + \varepsilon})$.

Let m_0 be a square-free positive integer. We define the following family

$$F(m_0) := \{n \not\equiv 0, 4, 7 \pmod 8\colon \operatorname{rad} n = m_0\}.$$

THEOREM 4. *Let* $n \not\equiv 0, 4, 7 \pmod 8$ *be a positive integer, let* $F(m_0)$ *be the family to which n belongs. There exists a constant* $c(m_0)$ *such that if* $n > c(m_0)$, *then*

$$l(n) = \begin{cases} 2 & \textit{if} \ \text{g.c.d.}(n, 10) \neq 1, \\ 3 & \textit{if} \ \text{g.c.d.}(n, 10) = 1. \end{cases}$$

Proof. From Theorems 2 and 3 it is obvious that for s large enough one has $g_2(n) < 1$ and $g_3(n) < 1$ according to whether g.c.d.$(n, 10)$ is different from one or not.

The following table, computed by P. Llorente, shows that the constants $c(m_0)$ are, in general, non-trivial. All non-square-free positive integers $n \leqslant 10^5$ not contained in the table have the level expected from Theorem 2.

TABLE

$F(m_0)$	n	$l(n)$	$c(m_0) \geqslant$
$F(30)$	$90 = 2.5.3^2$	1	90
$F(390)$	$1170 = 2.5.13.3^2$	1	1170
$F(570)$	$1710 = 2.5.19.3^2$	1	1710
$F(1230)$	$3690 = 2.5.41.3^2$	1	3690
$F(6630)$	$19890 = 2.5.13.17.3^2$	1	19890

Finally, we give an application to solve an embedding problem of Galois theory.

COROLLARY. *Let* $n \equiv 3 \pmod 8$ *be a positive integer such that* $n > c(m_0)$. *Then, every central extension of the alternating group* A_n *can be realized as a Galois group over* $\mathbf{Q}$.

Proof. One needs only to observe that all these integers have level equal to 3 and apply Theorem 5.1 of [8], (cf. also [9]).

REFERENCES

1. A. ARENAS, An arithmetic problem on the sums of three squares. *Acta Arith.* **51**, No. 3, in press.
2. P. BAYER AND E. NART, Zeta functions and genus of quadratic forms, to appear.
3. A. J. EARNEST AND J. S. HSIA, Spinor norms of local integral rotations II, *Pacific J. Math.* **61** (1975), 71-86.
4. H. LOO KENG, "Introduction to Number Theory," Springer, Berlin, 1982.
5. R. SCHULZE-PILLOT, Theta-reihen positiv definiter quadratischer Formen. *Invent. Math.* **75** (1984), 283-299.
6. G. SHIMURA, On modular forms of half integral weight, *Ann. of Math.* **97** (1973). 440-481.
7. C. L. SIEGEL, Über die analytische Theorie der quadratischen Formen, *Ann. of Math.* **36** (1935), 527-606; "Gesammelte Abhand," Band 1, Springer, Berlin, 1966.
8. N. VILA, On central extensions of A_n as a Galois group over $\mathbf{Q}$, *Arch. Math.* **44** (1985), 424-437.
9. N. VILA, On stem extensions of S_n as Galois group over number fields. *J. Algebra*, in press.