UNIVERSITAT DE BARCELONA

FACULTAT DE MATEMÀTIQUES

ARITHMETIC BEHAVIOUR OF THE SUMS OF THREE SQUARES II

by

A. ARENAS – P. BAYER

PRE–PRINT N.º 38

ENERO 1986

ARITHMETIC BEHAVIOUR OF THE SUMS OF THREE SQUARES II

A. Arenas - P. Bayer

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

Introduction

The purpose of this paper is the determination of the level, $\ell(n)$, of an integer n with respect to the sum of three squares, when n is not necessarily square-free.

We keep the definitions and basic notations given in [1].

A recursive formula for the main term in the evaluation of $\ell(n)$ is given in theorem 5, using p-adic densities.

The error term in the determination of $\ell(n)$ can be now estimated, unconditionally, thanks to Shimura's lifting, which allows to know the growth of the Fourier coefficients of certain cusp forms of weight 3/2 from some of weight 2, when the index runs through a fixed quadratic class. This estimation of the error term becomes important when n increases in such a quadratic class. For this reason, the square-free case was handled separately in a previous paper [1].

We conclude that if $n \not\equiv 0,4,7 \pmod 8$ is a positive integer sufficiently large (see Section 3), then

i) $\ell(n) = 2$, if $\text{g.c.d.}(n,10) \neq 1$,

ii) $\ell(n) = 3$, if $\text{g.c.d.}(n,10) = 1$.

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

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

1. The main term in the determination of $\ell(n)$

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 be denoted by $\ell(n)$.

We consider also the functions

$$g_1(n) = \frac{s_3(n)}{r(n,I_3)} \quad , \qquad g_2(n) = \frac{s_2(n) - 2s_3(n)}{r(n,I_3)} \quad ,$$

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

where

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

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 $j \leq i$ and $a_j = 1$ for $j > i$. We take $\rho_i = 3 - 2[i/3]$.

We recall ([1], prop. 1) that $\ell(n) \geq i$ 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

$$d_{ij} = \text{g.c.d.}(a_i, a_j) \ , \quad 1 \leq i \ , \ j \leq 3 \ , \ i \neq j \ ,$$

$$d_{123} = \text{g.c.d.}(a_1, a_2, a_3) \ ,$$

$$d = d_{123}^{-2} \, d_{12} \, d_{13} \, d_{23} \, .$$

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 $\text{g.c.d.}(b_i, b_j) = 1$, for $i \neq j$ and $\text{g.c.d.}(d, b_i) = 1$, 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 following 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 [6]).

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] :

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

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

Proposition 1. *If* $n \not\equiv 0,4,7 (\mathrm{mod}\ 8)$, *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* [1]*).*

Proof. It suffices to apply Siegel's Hauptsatz 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 $a_1a_2a_3$ 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 $n \equiv 7 (\mathrm{mod}\ 8)$. 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 follows (cf. [1], Sect. 1) :

$$G_1(n) = S_3'(n) \ , \ G_2(n) = S_2'(n) - 2S_3'(n) \ ,$$

$$G_3(n) = S_1'(n) - S_2'(n) + S_3'(n) \ .$$

Since the evaluation of the main term leads tc 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* $n \not\equiv 0,4 (mod\ 8)$ *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. [1]) it follows immediately that

$$\text{i)}\quad \partial_p'(m,\alpha) = \frac{\partial_p(n,\langle p^2,1,1\rangle)}{p\ \partial_p(n,I_3)} \quad ,$$

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

Siegel in his paper [6] 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 the following

<u>Proposition 2.</u> *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:*

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

for $p \neq 2$.

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

Proof. i) This is an immediate consequence of [6] 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 $\partial_p(n,<p^2,1,1>)$ 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's formulae.

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:*

$$\text{i)} \quad \partial_p(n, \langle p^2,1,1\rangle) = \begin{cases} 2+\varepsilon_p^2(1-p^{-1}) - p^{-\beta}(1+p^{-1}), & \text{if } \alpha = 2\beta+1, \\ 2+\varepsilon_p^2(1-p^{-1}) - \{1-(\frac{-m}{p})\}p^{-\beta}, & \text{if } \alpha = 2\beta, \end{cases}$$

for $p \neq 2$.

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

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

$$\Theta_{p^s}(m,f) = \sum_{x \in (\mathbb{Z}/p^s\mathbb{Z})^3} \exp\left(\frac{2\pi i m f(x)}{p^s}\right) \quad ;$$

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

Each $\xi \in \mathbb{Q}_p/\mathbb{Z}_p, \xi \neq 0$ admits a unique representative in $\mathbb{Q}_p$ 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. [3], [8]) that

$$\partial_p(n,f) = \sum_{\xi \in \mathbb{Q}_p/\mathbb{Z}_p} \Theta(\xi,f) < \xi, -n > ,$$

where $<,>$ denotes the usual pairing between $\mathbb{Z}_p$ and $\mathbb{Q}_p/\mathbb{Z}_p$.

Let $B_s(n,f) = \sum_{\substack{\xi \in \mathbb{Q}_p/\mathbb{Z}_p \\ v_p(\xi) = -s}} \Theta(\xi,f) < \xi, -n >$.

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

$\Theta_{p^s}(m,f) = p\Theta_{p^s}(m,I_3)$, if $s \geq 3$. Therefore

$B_s(n,f) = p\, B_s(n,I_3)$ for $s \geq 3$. So :

$$\partial_p(n,f) = \sum_{\substack{\xi \in \mathbb{Q}_p/\mathbb{Z}_p \\ v(\xi) < -2}} p\, B_s(n,I_3) + B_2(n,f) + B_1(n,f) + B_o(n,f).$$

Taking into account well-known results about the values taken for the ordinary Gauss sums (cf. [2], Ch.7), it is easy to evaluate the sums $B_s(n,f)$. They are given by :

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

if s is odd.

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

if s is even.

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.

<u>Lemma 4.</u> *With our previous notations, if* q *is a prime dividing* $a_1a_2a_3$, $q \neq p$, *it holds* :

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

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

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

ii) Let us suppose that $p \nmid a_1 a_2 a_3$.

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 prop. 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

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

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

By prop. 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 props. 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.

<u>Theorem 5.</u> *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 ocurring in the factorization of* n *are odd. Then:*

i) $$G_1(n) = G_1(m) + \partial'_p(m,\alpha)(G_2(m) - G_1(m)) + \\ + \partial'_{p^2}(m,\alpha)(1-G_2(m)),$$

ii) $$G_2(n) = G_2(m) + \partial'_p(m,\alpha)(G_3(m) - G_2(m)) + \\ + \partial'_{p^2}(m,\alpha)(1 + G_2(m) - 2G_3(m)),$$

iii) $$G_3(n) = G_3(m) + (3\partial'_p(m,\alpha) - 2\partial'_{p^2}(m,\alpha))(1 - G_3(m)).$$

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 4 and the definitions of $\partial'_p(m,\alpha)$ and $\partial'_{p^2}(m,\alpha)$ we obtain :

$$S'_1(mp^{\alpha}) = S'_1(m) + \partial'_p(m,\alpha)(3 - S'_1(m)),$$

$$S_2'(mp^{\alpha}) = S_2'(m) + 2\partial_p'(m,\alpha)(S_1'(m) - S_2'(m)) +$$

$$+ \partial_{p^2}'(m,\alpha)(3 - 2S_1'(m) + S_2'(m)) ,$$

$$S_3'(mp^{\alpha}) = S_3'(m) + \partial_p'(m,\alpha)(S_2'(m) - 3S_3'(m)) +$$

$$+ \partial_{p^2}'(m,\alpha)(1 - S_2'(m) + 2\, S_3'(m)) .$$

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 props. 2 and 3, we get the following

Proposition 6. *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) $$\partial_p'(m,\alpha) = \frac{(2+\varepsilon_p^2)\; p^{\beta+1} - \varepsilon_p^2\; p^{\beta} - (p+1)}{(p+1)(p^{\beta+1} - 1)} , \text{ if } \alpha = 2\beta+1 .$$

ii) $$\partial_p'(m,\alpha) = \frac{(2+\varepsilon_p^2)p^{\beta} - \varepsilon_p^2\; p^{\beta-1} - \{1-(\frac{-m}{p})\}}{(p+1)\left[(p^{\beta}-1)+(1-p^{-1})\{1-(\frac{-m}{p})p^{-1}\}^{-1}\right]} , \text{ if } \alpha = 2\beta.$$

iii) $\partial'_{p^2}(m,\alpha) = \dfrac{p^{\beta} - 1}{p^{\beta+1} - 1}$, *if* $\alpha = 2\beta+1$.

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

vii) *If* $p = 2$, *then*

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

Corollary 7. *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) $0 \leq \partial'_p(m,\alpha) < \frac{1}{2}$.

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

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

and

$$3\partial'_5(m,\alpha) - 2\partial'_{5^2}(m,\alpha) = 1 \ .$$

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

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, $(\frac{-m}{p}) = 1$ or -1, and use the expressions of prop. 6.

Theorem 8. *Let* $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ *be a positive integer with* $4 \nmid n$. *Then there exist constants* $c_i = c_i(p_1 \dots p_k)$ *such that :*

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

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 cor. 7 we have

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

$c_3(p) = 7/13$.

Let now $n = p_1^{\alpha_1} \dots p_{k-1}^{\alpha_{k-1}} p_k^{\alpha_k}$, with $k > 1$ and $p_k^{\alpha_k}$ chosen as in th. 5, and write $m = p_1^{\alpha_1} \dots p_{k-1}^{\alpha_{k-1}}$. Then, we have, by virtue of th. 5, cor. 7 and the induction hypothesis, that

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

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

By induction and applying again th. 5 and cor. 7, we get that $0 \leq G_1(n) \leq G_2(n) \leq G_3(n) < 1$. 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 $2|n$, proceeding by induction on the number of distinct prime factors of n, and taking into account th. 5 and cor. 7, we get $G_3(n) = 1$. On the other hand, in order to prove that there exist $c_2(p_1 \dots p_k)$ such that $G_2(n) < c_2 < 1$, we write $n = mp_k^{\alpha_k}$ in accordance with th. 5, 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 th. 5 and lemma 7, allows us to estimate $G_2(n)$ also by induction as follows :

$$G_2(n) = G_2(m) + (2\partial'_{p_k}(m,\alpha_k) - \partial'_{p_k^2}(m,\alpha_k))(1-G_2(m)) <$$

$$< G_2(m) + \frac{4}{5}(1 - G_2(m)) < c_2(p_1 \dots p_k) < 1 ,$$

with $c_2(p_1 \dots p_k) := \frac{4}{5} + \frac{1}{5} c_2(p_1 \dots p_{k-1})$.

If $5|n$, 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 th. 5 and cor. 7, we get $0 \leq G_1(n) \leq G_2(n) < G_3(n) = 1$. Therefore, it suffices to take $c_1 = c_2$.

3. The error term in the determination of $\ell(n)$. Asymptotic behaviour of $\ell(n)$

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

Lemma 9. *Let* $n = n_o s^2$ *be a positive integer,* $n \not\equiv 0,4,7 \pmod 8$, *where* n_o *is its square-free part. Let* $f = \langle b_1^2, b_2^2, b_3^2 \rangle$ *be a quadratic form such that* $b_i | n$, g.c.d.$(b_i, b_j) = 1$, *for* $i \neq j$, *and* b_i *square-free for* $i = 1,2,3$. *Then*

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

for every $\varepsilon > 0$.

Proof. Under these conditions, the theta series $\Theta(f,z)$ associated to f belongs to the space $M_o(3/2,\ 4b_1^2 b_2^2 b_3^2)$ of modular forms of weight 3/2 with respect to $\Gamma_o(4b_1^2 b_2^2 b_3^2)$. Then, we can prove as in lemma 6 of [1] that $r(n,\text{gen } f) = r(n,\text{spn } f)$, where spn f stands for the spinorial genus of f.

By results of Schulze-Pillot [4], we have that $\Theta(f,z) - \Theta(\text{spn } f,z)$ lies in $U^{\perp}$, where $U^{\perp}$ is the orthogonal complement, in the space of cusp forms $S_o(3/2,\ 4b_1^2 b_2^2 b_3^2)$ of the space $U = \oplus\, U(n_o)$, n_o square-free, with

$$U(n_o) = S_o(3/2, 4b_1^2 b_2^2 b_3^2) \cap \{f(z) = \sum_{n=1}^{\infty} \psi(n)\, n \exp(2\pi i n_o n^2 z)\} ,$$

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

If n runs into a quadratic class $n = n_o s^2$, then by Shimura's n_o - lifting [5] 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 $U(n_o)^{\perp}$, in the sense that

$$a(n_o s^2) = O_{\varepsilon, n_o, g}(s^{\frac{1}{2}+\varepsilon}) ,$$

for every $\varepsilon > 0$, (cf. [4], Hilfssatz 5).

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

From lemma 9 we can give the growth of the error term: $g_i(n) - G_i(n)$.

<u>Theorem 10.</u> *Let* $n = n_o s^2$, $n \not\equiv 0,4,7 \pmod 8$, *let* m_o = *rad* n *be the product of the distinct prime factors of* n. *For every* $\varepsilon > 0$, *we have*

$$g_i(n) - G_i(n) = O_{\varepsilon, n_o, m_o}(s^{-\frac{1}{2}+\varepsilon}) ,$$

for $i = 1,2,3$.

Let n_o, m_o be two square-free positive integers. We define the following family

$$F(n_o, m_o) := \{ n \not\equiv 0,4,7 \pmod 8 \mid n = n_o s^2, \ \mathrm{rad}\, n = m_o \}.$$

Theorem 11. *Let* $n \not\equiv 0,4,7 \pmod 8$ *be a positive integer, let* $F(n_o,m_o)$ *the family to which* n *belongs. Then, there exists a constant* $c(n_o,m_o)$ *such that if* $n > c(n_o,m_o)$, *then* :

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

Proof. Write $n = n_o s^2 = p_1 \dots p_j (p_{j+1}^{\alpha_{j+1}} \dots p_k^{\alpha_k})^2$, where $p_1,\dots,p_j$ may appear among $p_{j+1},\dots,p_k$. Let

$\alpha(n) = \sum_{i=j+1}^{k} \alpha_i$, and $\varepsilon = 4/9$.

If g.c.d.$(n,10) = 1$, by th. 8 there exist a constant $c_3(m_o)$; and by th. 10 there exist a constant $c_4 = c_4(4/9,n_o,m_o)$ such that :

$g_3(n) < c_3 + c_4\, s^{-1/18}$. Therefore, to achieve that $g_3(n) < 1$ it suffices to take $\alpha(n) > 18 \log(\frac{c_4}{1-c_3})$, if $m_o = n_o$ and $\alpha(n) > 18 \log\left(\frac{c_4}{1-c_3}\right) \cdot \frac{1}{\log p_o}$, if $n_o \neq m_o$. Here p_o denotes the least prime factor of n.

Then, we can take :

$$c(n_o,m_o) = \begin{cases} n_o + 18 \log\left(\frac{c_4}{1-c_3}\right) & \text{if } n_o = m_o , \\ n_o \exp\left[36 \log\left(\frac{c_4}{1-c_3}\right) \frac{\log p_1}{\log p_o}\right] & \text{if } n_o \neq m_o . \end{cases}$$

Here p_1 denotes the greatest prime factor of n.

Obviously, if $n > c(n_o,m_o)$, $\alpha(n)$ verifies the above inequalities, and so $g_3(n) < 1$.

Similarly, if g.c.d.$(n,10) \neq 1$, to achieve that $g_2(n) < 1$, it suffices to take :

$$c(n_o,m_o) = \begin{cases} n_o + 18 \log \left(\frac{c_5}{1-c_2}\right) , & \text{if } n_o = m_o \ ; \\ n_o \exp \left[36 \log \left(\frac{c_5}{1-c_2}\right) \frac{\log p_1}{\log p_o}\right] , & \text{if } n_o \neq m_o \ ; \end{cases}$$

where $c_2(m_o)$ is the constant given in th. 8, and $c_5(4/9,n_o,m_o)$ the O-constant in th. 10 corresponding to the error term $g_2(n) - G_2(n)$.

The following table, computed by P. Llorente, shows that the constants $c(n_o,m_o)$ are, in general, non-trivial. All non-square-free positive integers $n \leq 10^5$ not contained in table II have the level expected from th. 8.

Table II

$F(n_o,m_o)$	$n = n_o s^2$	$\ell(n)$	$c(n_o,m_o) \geq$
F(10,30)	$90 = 2.5.3^2$	1	90
F(130,390)	$1170 = 2.5.13.3^2$	1	1170
F(190,570)	$1710 = 2.5.19.3^2$	1	1710
F(2210,6630)	$19890 = 2.5.13.17.3^2$	1	19890

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

Corollary 12. *Let* $n \equiv 3 \pmod 8$, *and* $n \not\equiv 0 \pmod 5$ *be a positive integer such that* $n > c(n_o, m_o)$. *Then, every central extension of the alternating group* A_n *can be realised as a Galois group over* $\mathbb{Q}(T)$ *and, moreover, over* $\mathbb{Q}$.

Proof. One needs only to observe that all these integers have level equal to 3, and apply th. 5.1 of [7].

References

1. Arenas, A.: Arithmetic behaviour of the sums of three squares I, to appear.
2. Hua Loo Keng: Introduction to Number Theory. Springer, 1982.
3. Lachaud, G.: Une présentation adélique de la série singulière et du problème de Waring. L'Enseig. Math., 28 (1982), 139-169.
4. Schulze-Pillot, R.: Thetareihen positiv definiter quadratischer Formen. Inv. Math. 75 (1984), 283-299.
5. Shimura, G.: On modular forms of half integral weight. Ann. of Math. 97 (1973), 440-481.
6. Siegel, C.L.: Über die analytische Theorie der quadratischen Formen. Ann. of Math. 36 (1935), 527-606. Gesammelte Abhand., Band 1. Springer, 1966.

7. Vila, N.: On central extensions of A_n as a Galois group over Q . Arch. Math., 44 (1985), 424-437.

8. Weil, A.: Sur la formule de Siegel dans la théorie des groupes classiques. Acta Math., 113 (1965), 1-87.

Dipòsit Legal B.: 2.104-1986
BARCELONA – 1986