UNIVERSITAT DE BARCELONA

FACULTAT DE MATEMÀTIQUES

ON POSITIVE INTEGERS REPRESENTABLE AS A SUM OF THREE SQUARES

by

Angela Arenas Sola

PRE–PRINT N.º 30

novembre 1985

ON POSITIVE INTEGERS REPRESENTABLE AS A SUM OF THREE SQUARES

by
Angela Arenas Sola

We consider the following

Problem: For a given positive integer n, find out the maximum value of ℓ such that there exists a representation of n as a sum of three squares, $n = x_1^2+x_2^2+x_3^2$, $x_i \in \mathbb{Z}$, with ℓ summands prime to n.

We call ℓ the level of n and we put $\ell := \ell(n)$.

We agree that $\ell(n) = -1$ if $n = 4^a(8b+7)$. Since if $\ell(n) > 0$, then n has a primitive representation as a sum of three squares, we need only to consider integers n such that $n \not\equiv 0,4,7 \pmod 8$.

If 2 or 5 divides n, it is easy to see that $l(n) < 3$.

If $f = f(X_1,X_2,X_3)$ is a positive definite ternary quadratic form we put, as usual,

$$r(n,f) = \#\{(x_i) \in \mathbb{Z}^3 \mid f(x_1,x_2,x_3) = n\},$$
$$r_m(n,f) = \#\{(x_i) \in (\mathbb{Z}/n\mathbb{Z})^3 \mid f(x_1,x_2,x_3) \equiv n \pmod m\}.$$

We put $\langle a_1^2,a_2^2,a_3^2\rangle$ for a diagonal quadratic form and $1_3 = \langle 1,1,1\rangle$ for the identity.

To calculate $\ell(n)$ we define the following alternating sums, for i=1,2,3:

$$s_i(n) = \rho_i \sum_{a_j \mid n} (-1)^i \mu(a_1)\mu(a_2)\mu(a_3)\, r(n,\langle a_1^2,a_2^2,a_3^2\rangle)$$
$$a_j \neq 1, \text{ if } j \leq 1;$$
$$a_j = 1, \text{ if } j > 1$$

where

$$\rho_i = \begin{cases} 3 & \text{if } i=1,2 \\ 1 & \text{if } i=3 \end{cases}$$

and μ being the Möbius function.

Then, if we define

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

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

we have the following criterion for the evaluation of $\ell(n)$.

Theorem 1. $\ell(n) \geq i$ if and only if $g_i(n) < 1$.

As a_1,a_2,a_3 can have common factors we take them out and put

$$r(n,<a_1^2,a_2^2,a_3^2>) = r(nd^{-2}, <b_1^2,b_2^2,b_3^2>),$$

with d chosen such that $(b_i,b_j) = 1, \quad i \neq j$.

As in general the value of $r(n,f)$ can not be determined, we define the following average sums, for $i=1,2,3$:

$$S_i(n) = \rho_i \sum_{\substack{a_j \mid n \\ a_j \neq 1, \text{ if } j \leq i; \\ a_j = 1, \text{ if } j > i}} (-1)^i \mu(a_1)\mu(a_2)\mu(a_3)\, r(nd^{-2}, \text{gen}<b_1^2,b_2^2,b_3^2>),$$

with $r(nd^{-2}, \text{gen}<b_1^2,b_2^2,b_3^2>)$ meaning the average value of the number of representations of n by all the forms in the genus of $<b_1^2,b_2^2,b_3^2>$ (cf. [2]).

Now, we can consider the "main term" in the determination of the level defined by:

$$G_1(n) = \frac{S_3(n)}{r(n,I_3)} \quad , \qquad G_2(n) = \frac{S_2(n)-2S_3(n)}{r(n,I_3)} \quad ,$$

$$G_3(n) = \frac{S_1(n)-S_2(n)+S_3(n)}{r(n,I_3)} \quad .$$

Siegel's "Hauptsatz" [3] tells us that

$$r(nd^{-2},\ \text{gen} < b_1^2,b_2^2,b_3^2>) = \prod_p \partial_p(nd^{-2},\ <b_1^2,b_2^2,b_3^2>)\ ,$$

with the p-adic density ∂_p defined by

$$\partial_p\ (nd^{-2},f) = \lim_{\alpha\to\infty} \frac{r_{p^\alpha}(nd^{-2},f)}{p^{2\alpha}}\ ,$$

$f = <b_1^2,b_2^2,b_3^2>$.

Carrying out the exact evaluation of all the corresponding p-adic densities, including those with $p|2 \det f$, we prove the following recursive formulae

Theorem 2. Let n be a positive integer with $v_2(n)=0$ or 1 and p a prime not dividing n. Then we have:

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

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

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

for all even $\alpha>0$. If α is odd, these formulae are also valid in case that all the exponents occurring in the factorization of n are odd.

Here $\partial'_p(n,\alpha)$ and $\partial'_{p^2}(n,\alpha)$ are quotients of p-adic densities, depending on both n and α.

Corollary 3. Let $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, then there exists a constant $c_i = c_i(p_1\cdots p_k)$ such that

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

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

Next we give an interpretation of the "error term": $g_i(n)-G_i(n)$ in terms of Fourier coefficients of modular forms.

Let $\theta(f,z)$ and $\theta(\text{gen } f,z)$ be the theta series associated to f and gen f, with $f = \langle b_1^2, b_2^2, b_3^2 \rangle$ a quadratic form of our type. We know that $\theta(f,z) \in M_o(3/2,\ 4b_1^2b_2^2b_3^2)$, being $M_o(3/2,\ 4b_1^2b_2^2b_3^2)$ the space of modular forms of weight $3/2$ with respect to $\Gamma_o(4b_1^2b_2^2b_3^2)$. By recent results of Schulze-Pillot about theta series of positive definite quadratic forms [2], we know that

i) $\theta(\text{gen } f,\ z) \in E_o(3/2,\ 4b_1^2b_2^2b_3^2)$,

ii) $\theta(f,z) - \theta(\text{spn } f,\ z) \in U^{\perp}$.

Here E_o is the space spanned by Eisenstein series, $U^{\perp}$ the orthogonal complement, in the space of cusp forms, of the space U spanned by Shimura's theta functions and spn f denotes the spinorial genus.

In our case, the forms $f = \langle b_1^2, b_2^2, b_3^2 \rangle$ have the nice property

$$r(nd^{-2},\ \text{spn } f) = r(nd^{-2},\ \text{gen } f)\ .$$

We get, looking at the growth of the coefficients of the forms lying in $U^{\perp}$, the following

Theorem 4. Let $n = n_o s^2$, with n_o square-free. Then for every $\epsilon > 0$ we have

$$g_i(n) - G_i(n) = O(s^{-\frac{1}{2}+\epsilon})$$

with the O-constant depending on ϵ, n_o and $m_o = \text{rad } n$.

Summing up the preceding results we obtain the following answer to the problem: Let $n \in \mathbb{Z}^+$ then

$$\ell(n) = \begin{cases} -1 & \text{if } n \neq 3\square\ , \\ 0 & \text{if } n = 3\square \text{ and } 4 \mid n, \\ 2 & \text{if } n = 3\square, 4 \nmid n,\ (n,10) \neq 1 \text{ and } n > c(n_o,m_o) \\ 3 & \text{if } n = 3\square, (n,10) = 1 \text{ and } n > c(n_o,m_o). \end{cases}$$

The constants $c(n_o,m_o)$ are in general non trivial, for example, $c(2210,3) \geq 19890$.

The proofs of the above statements can be found in [1]. I want to express my thanks to my thesis adviser Professor P. Bayer for her valuable help.

Next, we give an application which, in fact, motivated the study of the preceding problem. After Vila [3], we obtain the following

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

Bibliography

[1] A. Arenas Solá: Un problema aritmético sobre las sumas de tres cuadrados. Tesis doctoral. Universidad de Barcelona (1985).

[2] R. Schulze-Pillot: Thetareihen positiv definiter quadratischer Formen. Inv. Math. 75 (1984), 283-299.

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

[4] N. Vila: On central extensions of A_n as a Galois group over $\mathbb{Q}$. Arch. Math., vol. 44, (1985), 424-437.

Angela ARENAS SOLA
Facultad de Matemáticas
Dpto. Algebra y Fundamentos
Universidad de Barcelona
Gran Via 585
08007 Barcelona
SPAIN

Dipòsit Legal B.: 35.909-1985
BARCELONA—1985