Pub. Mat. UAB
Vol. 30 Nº 1 Maig 1986

THE CONCEPT OF k-LEVEL FOR POSITIVE INTEGERS

Àngela Arenas

Introduction.

It is said (cf. [4]) that a positive integer n satisfies property (N) if there exists a representation of n as a sum of 3 squares, $n = x_1^2+x_2^2+x_3^2$, with $(x_1,n) = 1$ and $x_1^2 \leq \frac{n+1}{3}$. It has been checked that every positive integer $n \leq 600000$, $n \equiv 3 \pmod 8$, verifies property (N).

Such property appears in connection with the resolution of a *Galois embedding problem* in the following sense [4] : every central extension of the alternating group A_n can be realised as a Galois group over $\mathbb{Q}$ if $n \equiv 3 \pmod 8$ and n satisfies property (N).

In this paper, we introduce, for a positive integer n, the concept of k-*level* related to the representations of n as a sum of k squares. By considering the case k = 3 we exhibit a class of positive integers satisfying property (N).

We recall Lemma 1 of [1] since it will be used twice in this paper: *If* $n = x_1^2+x_2^2+x_3^2$ *is a primitive representation of* n *as a sum of three positive squares and* p *is a prime factor of* n *which divides one of the summands, then* $p \equiv 1$ *or* $2 \pmod 4$.

Definition. For a positive integer n we define the k-level, $\ell(n,k)$, of n as the *maximun* value of ℓ such that there exists a representation of n as a sum of k squares, $n = \sum_{i=1}^{k} x_i^2$, $x_i \in \mathbb{Z}$, with ℓ summands prime to n.

It is well known that every positive integer is a sum of four squares. If n is not a sum of k squares ($k \leq 3$), then we agree that $\ell(n,k) = -1$.

Obviously, for every positive integer n is $-1 \leq \ell(n,k) \leq k$. If $k<k'$, then $\ell(n,k) \leq \ell(n,k')$. And for every $k \geq 1$ is $\ell(1,k) = k$.

The determination of $\ell(n,2)$ is fairly easy and it is given in

<u>Proposition 1</u>. *Let* $n>1$ *be a positive integer. Then* :

i) If $4 \nmid n$ *and every odd prime divisor of* n *is congruent to* 1 *modulo* 4, *then* $\ell(n,2) = 2$.

ii) *Either if* $4|n$ *and* n *is a sum of two squares or if each prime divisor of* n *congruent to* 3 *modulo* 4 *appears in the factorization of* n *into primes with a positive even exponent, then* $\ell(n,2) = 0$.

iii) *In all the other cases is* $\ell(n,2) = -1$.

The following proposition characterizes the positive integers n having strictly positive 4-level

<u>Proposition 2</u>. $\ell(n,4) \geq 1$ *if and only if* $n \not\equiv 0 \pmod 8$.

<u>Proof</u>. If $n \equiv 0 \pmod 8$, then every representation of n as a sum of 4 squares, $n = x^2+y^2+z^2+t^2$, verifies that $\text{g.c.d.}(x,y,z,t) \geq 2$, and so $\ell(n,4) = 0$.

Furthermore, if $n \equiv 2,3,4,6,7 \pmod 8$, then obviously $n-1 \equiv 1,2,3,5,6 \pmod 8$ and, thus, $n-1$ is a sum of 3 squares, so we have $\ell(n,4) \geq 1$. Finally, if $n \equiv 1,5 \pmod 8$, then $n-4 \equiv 5,1 \pmod 8$ and, consequently, n-4 is also a sum of three squares so that $\ell(n,4) \geq 1$, because $2 \nmid n$.

Remark. For $k>4$, we have $\ell(n,k) \geq 1$ for all n, just because n-1 is a sum of four squares.

Let us concentrate from now on in the case $k=3$. It is well known that a positive integer n is expressible as a sum of three integer squares if and only if n is not of the form $4^a(8m+7)$. Gauss ([2], Art. 291) proved, moreover, that a positive integer admits a primitive representation as a sum of three squares if and only if $n \not\equiv 0,4,7 \pmod 8$.

For $\ell(n,3)$ we have the following elementary

Proposition 3. *Let* $n \in \mathbb{Z}^+$, *then* :

i) $\ell(n,3) \leq 0$ *if* $n \equiv 0 \pmod 4$,

ii) $\ell(n,3) < 3$ *if* $n \equiv 0 \pmod 2$ *or* $\pmod 5$.

The proof is immediate by passing to $\mathbb{Z}/m\mathbb{Z}$ with $m = 4,2,5$.

We next prove that given an odd positive integer with $\ell(n,3) \geq 1$, if we increase, preserving their parity, the exponents of its prime factors congruent to 1 modulo 4, then one can obtain level greater than or equal to 2.

Lemma 4. (see [1]) *If* $a, n \in \mathbb{Z}^+$ *are such that* $a = a_1^2+a_2^2$ *and* $n = b_1^2+b_2^2+b_3^2$, *then*

$$a^2 n = c_1^2+c_2^2+c_3^2 ,$$

with

$$c_1 = ab_1 - 2(a_1b_1+a_2b_2)a_1 ,$$

$$c_2 = ab_2 - 2(a_1b_1+a_2b_2)a_2 ,$$

$$c_3 = ab_3 .$$

The interest of the above lemma lies on the special values of the c_i which allow us to obtain the

<u>Proposition 5</u>. *Let* $n = 2^{\alpha} p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$ *, with* $p_i \equiv 1 (mod\ 4)$*,* $1 \leq i \leq r$ *and* $q_j \equiv 3 (mod\ 4)$*,* $1 \leq j \leq s$ *,* $\alpha = 0$ *or* 1*,* $\alpha_i > 0$*. Then if* $\ell(n,3) \geq 1$*, and* $m = 2^{\alpha} p_1^{\gamma_1} \cdots p_r^{\gamma_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$ *, with* $\gamma_i > \alpha_i$ *and* $\gamma_i \equiv \alpha_i$ $(mod\ 2)$*, it turns out that :*

i) *If* $\alpha = 0$*, then* $\ell(m,3) \geq 2$ *,*

ii) *If* $\alpha = 1$*, then* $\ell(m,3) \geq 1$ *.*

<u>Proof.</u>

Write $m = a^2 n$, with

$a = p_1^{\delta_1} \cdots p_r^{\delta_r}$, so that $\gamma_i = 2\delta_i + \alpha_i$, $i=1,\ldots,r$; $\delta_i \geq 1$.

Then a is a sum of two squares : $a = a_1^2 + a_2^2$ with $(a_i, a) = 1$; $1 \leq i \leq 2$.

As $\ell(n,3) \geq 1$ we can write $n = b_1^2 + b_2^2 + b_3^2$ with $(b_3, n) = 1$ and $(b_1, b_2, b_3) = 1$.

Now apply lemma 4 to write $m = a^2 n = c_1^2 + c_2^2 + c_3^2$.

Let $p \equiv 1 (mod\ 4)$ be a prime dividing m such that $p \nmid b_1$ and $p | b_2$; then

$$c_1 \equiv -2a_1b_1a_1 \not\equiv 0 \pmod p,$$

and

$$c_2 \equiv -2a_1b_1a_2 \not\equiv 0 \pmod p \quad ,$$

because $p|a$.

Interchanging the roles of b_1 and b_2 the same result is obtained.

Let $p \equiv 1 \pmod 4$ be a prime dividing m with $p \nmid b_1$ and $p \nmid b_2$ now, if $c_i \equiv 0 \pmod p$ for some $i \in \{1,2\}$, then

$$a_1b_1+a_2b_2 \equiv 0 \pmod p \quad ,$$

As $p \nmid b_1$ we are allowed to write

$$a_1 \equiv -\frac{a_2b_2}{b_1} \pmod p$$

and as $p|a$ we get

$$0 \equiv \frac{a_2^2b_2^2}{b_1^2} + a_2^2 = \frac{a_2^2}{b_1^2}(b_2^2+b_1^2) \pmod p \quad ,$$

whence $b_1^2+b_2^2 \equiv 0 \pmod p$. Thus $n \equiv b_3^2 \pmod p$, which is a contradiction since p divides n but not b_3.

We have thus proved that both $c_1 \not\equiv 0 \pmod p$ and $c_2 \not\equiv 0 \pmod p$, for every prime factor $p \equiv 1 \pmod 4$ of m.

On the other hand, if $q \equiv 3 \pmod 4$ is a prime factor of m, we necessarily have that $q \nmid c_3$, and as both c_1 and c_2 are nonzero, by lemma 1 of [1] we have that $q \nmid c_1c_2$.

So, in the case (i) we have $\ell(n,3) \geq 2$ and in the case (ii), as $2 \nmid c_3$ and $4 \nmid m$, we get $(c_1,2) = 1$ or $(c_2,2) = 1$ from which we infer that $\ell(n,3) \geq 1$.

Next we state the following

<u>Theorem 6</u>. *Let* n *be a positive integer, and write its factorization into prime factors as*

$$n = 2^{\alpha} p_1^{\alpha_1} \ldots p_r^{\alpha_r} q_1^{\beta_1} \ldots q_s^{\beta_s} \quad ,$$

with $p_i \equiv 1 (mod\ 4)$, $q_j \equiv 3 (mod\ 4)$. *With this notation we have :*

i) *If* $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, *then* $\ell(n,3) \geq 2$.

ii) *If* $n = 2^{\alpha} 5^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, $\alpha + \alpha_1 > 0$, $0 \leq \alpha \leq 1$, $0 \leq \alpha_1$, *then* $\ell(n,3) = 2$.

iii) *If* $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ *and* n *is a numerus idoneus of Euler, then* $\ell(n,3) = 2$.

iv) *If* $n = q_1^{\beta_1} \ldots q_s^{\beta_s}$ *and* $n \not\equiv 7 (mod\ 8)$, *then* $\ell(n,3) = 3$.

v) *If* $n = 2^{\beta} 5^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$ *and* $n \not\equiv 7 (mod\ 8)$ $\beta + \beta_1 > 0$, $0 \leq \beta \leq 1$ *then* $\ell(n,3) = 2$ *if* β *or* $\beta_1 = 0$, *and* $\ell(n,3) \geq 1$ *otherwise.*

vi) *If* $n = p_1^{\alpha_1} q_1^{\beta_1} \ldots q_s^{\beta_s}$ *and* $n \not\equiv 7 (mod\ 8)$, *then* $\ell(n,3) \geq 2$.

vii) *If* $n = p_1^{\alpha_1} p_2^{\alpha_2} q_1^{\beta_1} \ldots q_s^{\beta_s}$ *and* $n \not\equiv 7 (mod\ 8)$, *then* $\ell(n,3) \geq 1$.

viii) *If* $n = 2 p_1^{\alpha_1} q_1^{\beta_1} \ldots q_s^{\beta_s}$, *then* $\ell(n,3) \geq 1$.

Proof.

i) In this case n admits a primitive representation as a sum of two squares and therefore $\ell(n,3) \geq 2$.

ii) It suffices to apply i) and proposition 3.

iii) These integers admit a primitive representation as a sum of two squares but do not have any representation as a sum of 3 positive squares (cf. [3]). Integers of this type are 13 and 37, and these are up to now the only known examples not greater than 5.10^{10} (see [5]).

iv), vi), vii) and viii) are immediate consequences of lemma 1 of [1].

v) Under these conditions n admits a primitive representation as a sum of three positive squares and it suffices to apply lemma 1 of [1] together with proposition 3.

Now we give an application of the above theorem to the Galois embedding problem (cf. [4], Th. 5.1).

Theorem 7. *Let* $n = q_1^{\beta_1} \ldots q_s^{\beta_s}$ *with* $q_i \equiv 3 \pmod 4$, $1 \leq i \leq s$, *and* $n \equiv 3 \pmod 8$ *then every central extension of the alternating group* A_n *can be realised as a Galois group over* $\mathbb{Q}(T)$ *and, so, over* $\mathbb{Q}$.

Bibliography

[1] Arenas Sola, A.: *On a certain type of primitive representations of rational integers as sum of squares*. Pub. Sec. Mat. Univ. Autò noma de Barcelona. Vol. 28; Núm. 2-3 (1984), 75-80.

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

[3] Schinzel, A.: *Sur les sommes de trois carrés*. Bull. Acad. Pol. des Sciences. Vol. II, 6 (1959), 22-25.

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

[5] Weinberger, P.J.: *Exponents of the class group of complex quadratic fields*. Acta Arith. 22 (1973), 118-124.

The author thanks to the referee for some useful suggestions.

Rebut el 15 d'octubre del 1985

Departamento de Algebra y Fundamentos
Facultad de Matemáticas
Universidad de Barcelona
C/ Gran Via, 585
08007 Barcelona

SPAIN