THE CONCEPT OF k-LEVEL FOR POSITIVE INTEGERS

Angela 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, 
\[
 n = x_1^2 + x_2^2 + x_3^2 , \quad \text{with} \quad (x_1,n) = 1 \quad \text{and} \quad x_1^2 \leq \frac{n+1}{3} .
\]
It has been checked that every positive integer \( n \leq 600000 \), \( n \equiv 3(\text{mod} \ 8) \), 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 \( n \equiv 3(\text{mod} \ 8) \) 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 3 positive squares and \( p \) is a prime factor of \( n \) which divides one of the summands, then \( p \equiv 1 \) or \( 2(\text{mod} \ 4) \).

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

**Proposition 1.** 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 \( 4 \mid n \) 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

**Proposition 2.** \( \ell(n,4) \geq 1 \) if and only if \( n \not\equiv 0 \pmod{8} \).

**Proof.** 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 \( \gcd(x,y,z,t) \geq 2 \), 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 $\lambda(n,4) \geq 1$, because $2\mid n$.

Remark. For $k>4$, we have $\lambda(n,k) \geq 1$ 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 $n \not\equiv 0,4,7(\text{mod } 8)$.

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

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

i) $\lambda(n,3) \leq 0$ if $n \equiv 0(\text{mod } 4)$,

ii) $\lambda(n,3) < 3$ if $n \equiv 0(\text{mod } 2)$ or $(\text{mod } 5)$.

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 $\lambda(n,3) \geq 1$, 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
\[ c_1 = a b_1 - 2(a_1 b_1 + a_2 b_2) a_1, \]
\[ c_2 = a b_2 - 2(a_1 b_1 + a_2 b_2) a_2, \]
\[ c_3 = a b_3. \]

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

**Proposition 5.** Let \( n = 2 p_1 \ldots p_r q_1 \ldots q_s \), with \( p_i \equiv 1 \pmod{4} \), \( 1 \leq i \leq r \) and \( q_j \equiv 3 \pmod{4} \), \( 1 \leq j \leq s \), \( \alpha = 0 \) or \( 1 \), \( \alpha_i > 0 \). Then it turns out that:

i) If \( \alpha = 0 \), then \( k(m,3) \geq 2 \).

ii) If \( \alpha = 1 \), then \( k(m,3) \geq 1 \).

**Proof.**

Write \( m = a^2 n \), with
\[ a = p_1 \ldots p_r \], 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 \( k(n,3) \geq 1 \) 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 \( p \equiv 1 \pmod{4} \) be a prime dividing \( m \) such that \( p \mid b_1 \) and \( p \mid b_2 \); then

44
\[ c_1 \equiv -2a_1 b_1 a_1 \not\equiv 0 \pmod{p}, \]

and

\[ c_2 \equiv -2a_1 b_1 a_2 \not\equiv 0 \pmod{p}, \]

because \( p \mid a \).

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 \( p \not\mid b_1 \) and \( p \not\mid b_2 \) now, if \( c_i \equiv 0 \pmod{p} \) for some \( i \in \{1, 2\} \), then

\[ a_1 b_1 + a_2 b_2 \equiv 0 \pmod{p}, \]

As \( p \not\mid b_1 \) we are allowed to write

\[ a_1 \equiv -\frac{a_2 b_2}{b_1} \pmod{p} \]

and as \( p \mid a \) we get

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

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 \( q \mid c_3 \), and as both \( c_1 \) and \( c_2 \) are nonzero, by lemma 1 of [1] we have that \( q \mid c_1 c_2 \).
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

**Theorem 6.** Let \( n \) be a positive integer, and write its factorization into prime factors as

\[
n = 2 p_1 \ldots p_r q_1 \ldots q_s,\]

with \( p_i \equiv 1 (\text{mod } 4) \), \( q_j \equiv 3 (\text{mod } 4) \). With this notation we have:

i) If \( n = p_1 \ldots p_r \), then \( \ell(n,3) \geq 2 \).

ii) If \( n = 2^a p_1^{\alpha_1} \ldots p_r^{\alpha_r} \), \( a = a_1 \geq 0, 0 \leq \alpha_1 \leq 1, \), then

\( \ell(n,3) = 2 \).

iii) If \( n = p_1 \ldots p_r \) and \( n \) is a numerus idoneus of Euler, then

\( \ell(n,3) = 2 \).

iv) If \( n = q_1 \ldots q_s \) and \( n \not\equiv 7 (\text{mod } 8) \), then \( \ell(n,3) = 3 \).

v) If \( n = 2^5 q_1 \ldots q_s \) and \( n \not\equiv 7 (\text{mod } 8) \), \( \beta_1 > 0, 0 \leq \beta \leq 1 \) then

\( \ell(n,3) = 2 \) if \( \beta \) or \( \beta_1 = 0 \), and \( \ell(n,3) \geq 1 \) otherwise.

vi) If \( n = p_1 q_1 \ldots q_s \) and \( n \not\equiv 7 (\text{mod } 8) \), then \( \ell(n,3) \geq 2 \).

vii) If \( n = p_1 p_2 q_1 \ldots q_s \) and \( n \not\equiv 7 (\text{mod } 8) \), then \( \ell(n,3) \geq 1 \).

viii) If \( n = 2p_1 q_1 \ldots q_s \), 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 \( n = q_1 \cdots q_s \) 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 \( \mathbb{Q}(\tau) \) and, so, over \( \mathbb{Q} \).

Bibliography


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