Pub. Mat. UAB
Vol. 28 Nº 2-3 Set. 1984

ON A CERTAIN TYPE OF PRIMITIVE REPRESENTATIONS OF RATIONAL INTEGERS AS SUM OF SQUARES

Angela Arenas

Introduction.

It is well known that a positive integer not of the form $4^a(8m+7)$ can be expressed as a sum of three integer squares. Dirichlet (cf. [1]) proved that a positive integer admits a *primitive* representation as a sum of three squares if and only if it is not of the form 8m+7 or 4m.

An interesting problem is to consider integers n which admit a representation as a sum of three squares with one summand prime to n. Of course, such a representation is *primitive*. This type of representations appears in the resolution of some Galois embedding problems (cf. [3]).

Obviously if n admits a *primitive* representation as a sum of two squares, (i.e. if $4 \nmid n$ and no $p \equiv 3 \pmod 4$ divides n), then each summand is prime to n. Hence, the problem makes only sense for the integers which admit a *primitive* representation as a sum of three *positive* squares. These integers were characterized by A. Schinzel ([2]).

We have checked with a computer that for every Schinzel integer ≤ 10000, there exists at least one representation as a sum of three positive squares with a summand prime to n.

In the present paper, we show that for some Schinzel integers, each *primitive* representation as a sum of three *positive* squares has at least one summand prime to n (Th. 1).

Moreover, we show (Th. 2) that given a prime number $p > 2$, its powers always have a representation as a sum of p squares prime to p. This statement for $p=3$ was first made by E. Catalan (cf. [1]).

We recall that a representation of a positive integer n as a sum of three squares $n = x^2+y^2+z^2$; $x,y,z \in \mathbb{Z}$, is said to be *primitive* if $(x,y,z) = 1$.

Definition. We say that an integer n is a Schinzel integer if it admits a *primitive* representation $n = x^2+y^2+z^2$ with $xyz \neq 0$.

As it is proved in [2], an integer n is a Schinzel integer if and only if it satisfies the following two conditions:

1) $n \not\equiv 0,4,7 \pmod{8}$

2) n has a prime factor $p \equiv 3 \pmod{4}$ or n is not a "numerous idoneus" in the sense of Euler.

Theorem 1. *If* n *is a Schinzel integer, and* n *has, at most, two distinct prime factors congruent to 1 or 2 (mod. 4), then every primitive representation of* n *as a sum of three positive squares has, at least, one summand prime to* n.

The proof of the above theorem follows immediately from the

Lemma 1. *If* $n = x^2+y^2+z^2$ *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 *(mod. 4).*

Proof. Under these conditions -1 is a square (mod. p).

Another consequence of this lemma is the following:

Corollary 1. *If* $n = x^2+y^2+z^2$ *is a primitive representation of* n *as a sum of three positive squares and every prime* p *which divides* n *is congruent to 3 (mod. 4), then* $(x,n) = (y,n) = (z,n) = 1$.

Remark.

Theorem 1 is not true for an arbitrary n, for example, $870 = 2.3.5.29$ is a Schinzel integer which admits the primitive representation: $870 = 2^2+5^2+29^2$.

Let us now consider the problem of representations of the powers of an odd prime p as a sum of p squares.

Theorem 2. *Every power of a prime* $p \neq 2$ *can be represented as a sum of* p *squares prime to* p.

Proof. Let p be an odd prime and $A=p-1$. Since the norm N in $Q(\sqrt{-A})$ is multiplicative, we obtain in $\mathbb{Z}[\sqrt{-A}]$ the identity:

$$(x_1^2+Ay_1^2)(x_2^2+Ay_2^2) = (x_1x_2 \pm Ay_1y_2)^2 + A(x_1y_2 \mp x_2y_1)^2.$$

So we have, $(x_1^2+Ay_1^2)^n = X_n^2+AY_n^2$. From this we get the following recursive formulae:

$$X_n = X_{n-1}x_1 \pm AY_{n-1}y_1 ,$$

$$Y_n = X_{n-1}y_1 \mp Y_{n-1}x_1$$

Clearly, $p = N(x_1 + \sqrt{-A}\, y_1)$ for $x_1=y_1=1$, hence $p^n = X_n^2+AY_n^2$, where X_n and Y_n are given by the above formulae.

Thus, every power of $p > 2$ can be written as a sum of p squares, being p-1 of them equal. One can easily see by induction that if X_{n-1} and Y_{n-1} are prime to p, then X_n and Y_n can be chosen to be so.

The values of X_n and Y_n can be explicitly given, in fact:

$$X_n = \frac{(x_1+y_1\sqrt{-A})^n + (x_1-y_1\sqrt{-A})^n}{2}, \qquad Y_n = \frac{(x_1+y_1\sqrt{-A})^n-(x_1-y_1\sqrt{-A})^n}{2\sqrt{-A}}$$

with $X_n, Y_n \in \mathbb{Z}$, $n \in \mathbb{Z}^+$.

We give now another proof of theorem 2. This new proof yields various representations of p^s as sum of squares prime to p. In particular, we can get different representations from the one obtained in the first proof. Let us consider the bilinear form:

$$\mathbb{Z}^k \times \mathbb{Z}^k \longrightarrow \mathbb{Z}$$
$$(a,b) \longmapsto a \cdot b = \sum_{i=1}^{k} a_i b_i ,$$

with $a=(a_1,\dots,a_k)$, $b=(b_1,\dots,b_k)$. Let $q(a)=a\cdot a=\sum_{i=1}^{n} a_i^2$, be the associated quadratic form; then the equation $q(Xa+Yb)=$ $=q(a)^2\cdot q(b)$ has at least two integer solutions given by $(x_1,y_1)=$ $=(0,q(a))$ and $(x_2,y_2)=(-2ab,q(a))$.

Proposition 1. *If an integer is a sum of* k *squares, then so are its powers.*

Proof. Let

$$n=\sum_{i=1}^{k} a_i^2, \qquad a_i\in\mathbb{Z}, \quad i=1,\dots,k.$$

We show by induction, that n^t is a sum of k squares, for every $t\in\mathbb{Z}^+$. We now distinguish two cases:

i) Let t be even, $t=2s$, $s\in\mathbb{Z}^+$. From the identity:

$$\left(\sum_{i=1}^{k} a_i^2\right)^2=(-a_1^2+a_2^2+\dots+a_k^2)^2+(2a_1a_2)^2+\dots+(2a_1a_k)^2, \qquad (1)$$

we deduce that n^t is a sum of k squares, because $n^t=(n^s)^2$ and, by induction, n^s is of this type.

ii) Let t be odd, $t=2s+1$, $s\in\mathbb{Z}^+$. It follows that

$$\left(\sum_{i=1}^{k} a_i^2\right)^2\left(\sum_{i=1}^{k} b_i^2\right)=\sum_{i=1}^{k} c_i^2,$$

with $c_i=q(a)b_i-(2ab)a_i$, $i=1,2,\dots,k$. From this identity we get that n^t is sum of k squares, because $n^t=(n^s)^2n$.

Second proof of theorem 2. If p is an odd prime, then p admits the obvious representation as a sum of p squares $p = b_1^2+\ldots+b_p^2$ given by $b_1=\ldots=b_p=1$. Then from proposition 1 we obtain that every power of p is a sum of p squares. Let us see that they can be chosen to be prime to p. As before, we distinguish two cases:

i) Let $t=2s$, $s\in\mathbb{Z}^+$. If by induction $a_1,\ldots,a_p$ are nonzero in $\mathbb{F}_p$, so are $2a_1a_j$ for $j=2,\ldots,p$. Since $p>2$, the rest follows immediately from (1).

ii) Let $t=2s+1$, $s\in\mathbb{Z}^+$. We have $p^t=(p^s)^2p$, where $p^s=a_1^2+\ldots+a_p^2$, $(a_i,p) = 1$, $i=1,2,\ldots,p$ (by induction), and $p = b_1^2+\ldots+b_p^2$, $b_1=\ldots$ $\ldots=b_p=1$. By proposition 1 we have

$$p^t = \sum_{i=1}^{p} c_i^2, \quad c_i = q(a)b_i-(2ab)a_i, \quad i=1,\ldots,p.$$

As $-2ab = -2(a_1+\ldots+a_p)$, we can always suppose that $-2ab \not\equiv 0 \pmod p$. Since $p^s \equiv 0 \pmod p$, we get $c_i \equiv (-2ab)a_i \pmod p$, hence, the integers c_i, $(i=1,\ldots,p)$, are also prime to p.

REFERENCES

[1] L.E. Dickson, *History of the Theory of Numbers*. Vol. II, p. 267 (1919).

[2] A. Schinzel, *Sur les sommes de trois carrés*. Acad. Polon. Sci. Sér. Sci. Math. Astr. Phys. 7, pp. 307-310 (1959).

[3] N. Vila, *Sobre la realització de les extensions centrals del grup alternat com a grup de Galois sobre el cos dels racionals*. Pub. Mat. UAB 27, núm. 3 (1983), 43-143.

Rebut el 19 de març del 1984

Departamento de Algebra y Fundamentos
Facultad de Matemáticas
Universidad de Barcelona.
C/ Gran Via, 585
Barcelona 7.
SPAIN