Un problema aritmético sobre las sumas de tres cuadrados

Ángela Arenas Sola

UN PROBLEMA ARITMETICO

SOBRE LAS SUMAS DE TRES CUADRADOS

Angela Arenas Sola

Memoria presentada para aspirar al grado de doctor en Ciencias Matemáticas.

Facultad de Matemáticas.
Universidad de Barcelona.

HAGO CONSTAR que la presente memoria ha sido realizada por Angela Arenas Sola bajo mi dirección, en la Facultad de Matemáticas de la Universidad de Barcelona.

P. Bayer

Barcelona, mayo de 1985

Dra. Pilar Bayer Isant.

INDICE

INTRODUCCION

Fermat, motivado por la lectura de Diofanto, conjeturó que todo entero primo congruente con 1 módulo 4 es representable, de manera única salvo el signo y el orden, como suma de dos cuadrados; así como que todo entero positivo es suma de cuatro cuadrados. Estos resultados fueron probados por Euler y Lagrange.

La caracterización de los enteros representables como suma de tres cuadrados fue dada por Legendre. Gauss dió el número total de representaciones primitivas de un entero n como suma de tres cuadrados, en función del número de clases de formas cuadráticas binarias de discriminante -n.

El cálculo del número de representaciones de un entero como suma de 2,4,6 y 8 cuadrados fue llevado a cabo por Jacobi, mediante la teoría de funciones elípticas. Las fórmulas correspondientes se obtienen igualando coeficientes en ciertas identidades satisfechas por su función theta. Las investigaciones de Jacobi fueron proseguidas por Liouville y Ramanujan, entre otros, y en ellas se encuentra uno de los orígenes del estudio de las llamadas formas modulares de peso entero.

En general, el cálculo del número de representaciones

de un entero por una forma cuadrática, entera, concreta es muy complicado y resulta imposible obtener fórmulas exactas que expresen dicho número. Para paliar este inconveniente, Gauss, en el caso de formas cuadráticas binarias, introdujo el concepto de género; éste fué convenientemente extendido por Eisenstein, Smith y Minkowski a formas de un número mayor de variables. Siegel en 1935 dió fórmulas para una media, convenientemente ponderada, del número de representaciones de un entero por todas las formas que integran un género.

El estudio por vía analítica, análogo al de Jacobi, del número de representaciones de un entero como suma de un número impar de cuadrados fue comenzado por Hardy y Mordell, y conduce al estudio de las formas modulares de peso semientero. Este último concepto puede decirse que no ha sido completamente clarificado hasta los trabajos de Shimura de 1973. El caso de tres variables es el más delicado; así no ha sido hasta 1984, en el trabajo de Schulze-Pillot, que se ha probado que la serie theta del género de una forma cuadrática ternaria es una serie de Eisenstein.

En esta memoria nos ocupamos del siguiente problema relativo a las sumas de tres cuadrados:

Dado un entero n, *hallar el valor de* ℓ *máximo del cual se puede afirmar que existe una representación de* n *como suma de tres cuadrados*

$$n = x_1^2+x_2^2+x_3^2 ,$$

con ℓ *sumandos primos con* n.

Este problema, aparte de su interés intrínseco, ha sido motivado por su conexión con la búsqueda de enteros n para los cuales toda extensión central del grupo alternado A_n es grupo de Galois sobre $\mathbb{Q}$.

La única referencia existente en la literatura de un problema análogo al que nos ocupa es el resultado elemental de Catalan, de 1880, de que toda potencia de 3 es suma de tres cuadrados primos con 3.

La memoria está dividida en seis capítulos.

En el primer capítulo se hace la presentación del problema, diciéndose de él todo lo que se puede mediante métodos elementales. Se detalla asimismo su relación con el problema inverso de la teoría de Galois, antes mencionado.

En el segundo capítulo se dan fórmulas que, de todas las representaciones de un entero como suma de tres cuadra

dos, *descuentan* aquellas que tienen k términos no primos con n, para k = 1,2,3. Como estas fórmulas son de evaluación imposible, se definen a su vez, en este capítulo, unas fórmulas en "media" que aproximan a las primeras y son evaluables.

El estudio de estas últimas se lleva a cabo en los capítulos III y IV.

En el capítulo V se estudia el error cometido en la utilización de las fórmulas en "media" en vez de las fórmulas exactas.

Todo ello permite en el capítulo VI dar una respuesta al problema. Se obtiene que, si un entero n es suma de tres cuadrados, entonces :

i) Si $4 \mid n$, es $\ell = 0$.

ii) Si $4 \nmid n$ y m.c.d.$(n,10) \neq 1$, es $\ell = 2$, si n es suficientemente grande.

iii) Si m.c.d.$(n,10) = 1$, es $\ell = 3$, si n es suficientemente grande.

Se pone de manifiesto mediante ejemplos, que la condición de que n sea suficientemente grande en ii) y iii) es irrefinable. Es decir, la solución del problema es de natu

raleza asintótica.

Todas las proposiciones no originales van acompañadas de la correspondiente cita bibliográfica.

Agradezco a Nuria García la facilitación de tablas con las representaciones de enteros n como suma de tres cuadrados, para $n \leq 10^4$ y al Dr. Pascual Llorente la programación de los cálculos necesarios para la confección de las tablas del capítulo VI. Asimismo, quiero agradecer al Dr.R.Schulze-Pillot por las aclaraciones que ha tenido a bien comunicarme.

Finalmente, deseo expresar mi agradecimiento a la Dra. Pilar Bayer por su inestimable confianza, orientación y ayuda que me ha dedicado en todo momento.

CAPITULO I

EL CONCEPTO DE NIVEL

En este capítulo se presenta el concepto de nivel de un entero, relativo a las representaciones de éste como suma de un número fijo de cuadrados.

§1. Niveles

Definición. Dada una representación de un entero n como suma de k cuadrados,

$$n = \sum_{i=1}^{k} x_i^2 \quad , \quad x_i \in \mathbb{Z} \quad ,$$

diremos que ésta tiene *nivel* ℓ , si ℓ es el número de sumandos que son primos con n , es decir si

$$\ell = \#\{ i \mid \text{m.c.d.}(x_i, n) = 1 \} \ .$$

Dado un entero k , denominaremos k-nivel de n , designándolo por $\ell(n,k)$, al nivel máximo de las representaciones de n como suma de k cuadrados; o sea

$$\ell(n,k) = \text{máx}\{ \ell \mid \ell = \text{nivel de } (n = \sum_{i=1}^{k} x_i^2) \} \ .$$

Es bien sabido que todo entero positivo es suma de 4 cuadrados. Si n no es suma de k cuadrados, ($k \leq 3$), convendremos en escribir $\ell(n,k) = -1$.

Evidentemente, para todo entero n es $-1 \leq \ell(n,k) \leq k$. Si $k<k'$, entonces $\ell(n,k) \leq \ell(n,k')$. Y para todo entero k es $\ell(1,k) = k$.

La determinación de $\ell(n,2)$ no ofrece dificultad, como muestra la siguiente

Proposición 1.1. Para un entero cualquiera $n>1$ se tiene que

i) Si $4 \nmid n$ y todo divisor primo impar de n es congruente con 1 módulo 4, entonces $\ell(n,2) = 2$.

ii) Si $4 \mid n$ ó si todo divisor primo de n congruente con 3 módulo 4 aparece en la descomposición de n en factores primos con exponente par, entonces $\ell(n,2) = 0$.

iii) En los casos restantes, ésto es si algún primo congruente con 3 módulo 4 divide a n con exponente impar, entonces $\ell(n,2) = -1$.

Demostración.

i) Bajo estas condiciones n admite al menos una representación *primitiva* como suma de dos cuadrados, es decir, $n = x^2+y^2$ con $(x,n) = (y,n) = 1$, indicando por (x,n) el m.c.d.(x,n). Por tanto es $\ell(n,2) = 2$.

ii) En estas condiciones n es suma de dos cuadrados, pero no admite ninguna representación primitiva, así que $\ell(n,2) = 0$.

iii) En este caso n no es suma de dos cuadrados y por tanto, es $\ell(n,2) = -1$. #

Si $k \geq 4$ es fácil determinar los enteros n para los cuales $\ell(n,k) \geq 1$, como vemos a continuación.

Proposición 1.2. $\ell(n,4) \geq 1$ si y sólo si $n \not\equiv 0 (\text{mód } 8)$.

Demostración. Si $n \equiv 0 (\text{mód } 8)$, se tiene que toda representación de n como suma de 4 cuadrados, $n = x^2+y^2+z^2+t^2$ verifica que $\text{m.c.d.}(x,y,z,t) \geq 2$, de donde $\ell(n,4) = 0$.

Ahora bien, si $n \equiv 2,3,4,6,7 (\text{mód } 8)$, entonces $n-1 \equiv 1,2,3,5,6 (\text{mód } 8)$ y, por tanto, en estos casos n-1 es suma de tres cuadrados; es pues $\ell(n,4) \geq 1$.

Si $n \equiv 1,5 (\text{mód } 8)$, entonces $n-4 \equiv 5,1 (\text{mód } 8)$. Así pues, como n-4 es suma de tres cuadrados y como en ambos casos $2 \nmid n$ se tiene que $\ell(n,4) \geq 1$. #

Obsérvese que para todo entero positivo n, n-1 es suma de cuatro cuadrados, con lo cual $\ell(n,k) \geq 1$, para $k > 4$.

§2. El 3-nivel de un entero

Es bien conocido que todo entero positivo $n \neq 4^a(8m+7)$ puede expresarse como suma de 3 cuadrados. Está claro que si $\ell(n,3) \geq 1$, entonces n posee, a fortiori, una representación primitiva como suma de 3 cuadrados :

$$n = x^2+y^2+z^2 \qquad , \qquad m.c.d.(x,y,z) = 1 \ .$$

Dirichlet (cf.[12]) probó que todo entero positivo $n \neq 0,4,7$(mód 8) admite una representación *primitiva* como suma de 3 cuadrados. Así pues, es precisamente para estos enteros para los que cabe preguntarse cuándo es $\ell(n,3) \geq 1$. La observación de todas las representaciones de enteros positivos, $n \neq 0,4,7$(mód 8), como suma de tres cuadrados para $n \leq 10^5$ ha puesto de manifiesto que $\ell(n,3) \geq 1$ para todos ellos.

Nótese que una determinada representación primitiva no tiene por qué tener nivel 1 , por ejemplo $870 = 2\cdot3\cdot5\cdot29$ tiene la representación de nivel cero $870 = 2^2+5^2+29^2$. No obstante, $\ell(870,3) = 1$ ya que las representaciones, salvo orden y signos, de 870 como suma de 3 cuadrados son las siguientes :

$$\begin{aligned} 870 &= 5^2 + 13^2 + 26^2 \\ &= 5^2 + 19^2 + 22^2 \\ &= 7^2 + 14^2 + 25^2 \\ &= 2^2 + \ 5^2 + 29^2 \ . \end{aligned}$$

Consideramos ahora diferentes casos en los que $\ell(n,3)$ se puede estimar mediante métodos elementales.

Proposición 1.3.

i) Si $n \equiv 0 (\text{mód } 4)$ entonces $\ell(n,3) \leq 0$.

ii) Si $n \equiv 0 (\text{mód } 2)$ ó $(\text{mód } 5)$, entonces $\ell(n,3) < 3$.

Demostración.

i) Si $n \equiv 0 (\text{mód } 4)$ y si n es suma de tres cuadrados, basta tomar congruencias módulo 4 para ver que no admite ninguna representación primitiva. Por tanto, $\ell(n,3) \leq 0$.

ii) Si n admite una representación primitiva como suma de tres cuadrados no nulos, entonces basta pasar a clases de restos módulo 2, ó módulo 5, respectivamente, para obtener que $\ell(n,3) < 3$.

Observemos que no hace falta hacer ninguna restricción sobre n ya que :

Si n no es suma de tres cuadrados, es $-1 = \ell(n,3) < 3$.

Si n es suma de tres cuadrados y toda representación como tal es

$$n = x^2+y^2+z^2 \quad , \quad \text{con} \quad y = z = 0 \quad ,$$

entonces $\ell(n,3) = 0$.

Si n es suma de tres cuadrados y todas sus representaciones son del tipo

$$n = x^2+y^2+z^2 \quad , \quad z = 0 \text{ , está claro que}$$

$$\ell(n,3) = \begin{cases} 0 \text{ si } (x,y) > 1 \text{ para todo } x,y \text{ .} \\ 2 \text{ si } (x,y) = 1 \text{ para algún } x,y \text{ .} \end{cases} \quad \#$$

Lema 1.4. Si $n = x^2+y^2+z^2$ es una representación primitiva como suma de tres cuadrados *no nulos* y p un factor primo de n que divide a uno de los sumandos, entonces $p \equiv 1$ ó $2 (\text{mód } 4)$.

Demostración. Bajo estas condiciones -1 es un cuadrado módulo p . #

Teorema 1.5. Sea n un entero positivo y escribamos su descomposición en factores primos en la forma

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

con $p_i \equiv 1 (\text{mód } 4)$, $q_j \equiv 3 (\text{mód } 4)$. Tenemos que :

i) Si $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, entonces $\ell(n,3) \geq 2$.

ii) Si $n = 2^{\alpha} 5^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $\alpha + \alpha_1 > 0$, $0 \leq \alpha \leq 1$, $0 \leq \alpha_1$, entonces $\ell(n,3) = 2$.

iii) Si $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ con $p_i \equiv 1 (\text{mód } 4)$ y n es un número idóneo de Euler, entonces $\ell(n,3) = 2$.

iv) Si $n = q_1^{\beta_1} \ldots q_s^{\beta_s}$ y $n \not\equiv 7 (\text{mód } 8)$, entonces $\ell(n,3) = 3$.

v) Si $n = 2^{\beta} 5^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$, y $n \not\equiv 7 (\text{mód } 8)$ $\beta + \beta_1 > 0$, $0 \leq \beta \leq 1$, entonces $\ell(n,3) = 2$ si β ó $\beta_1 = 0$ y $\ell(n,3) \geq 1$ en otro caso.

vi) Si $n = p_1^{\alpha_1} q_1^{\beta_1} \ldots q_s^{\beta_s}$ y $n \not\equiv 7 (\text{mód } 8)$, entonces $\ell(n,3) \geq 2$.

vii) Si $n = p_1^{\alpha_1} p_2^{\alpha_2} q_1^{\beta_1} \ldots q_s^{\beta_s}$ y $n \not\equiv 7 (\text{mód } 8)$, entonces $\ell(n,3) \geq 1$.

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

Demostración.

i) En este caso n admite representaciones primitivas como suma de 2 cuadrados, por tanto, $\ell(n,3) \geq 2$.

ii) Basta tener en cuenta i) y la proposición 1.3.

iii) En efecto, estos enteros admiten una representación primitiva como suma de dos cuadrados y no admiten ninguna representación como suma de tres cuadrados no nulas [33]. Enteros de estas características tenemos 13 y 37 , y no se conoce ningún otro ejemplo por debajo de 10^7 [9].

iv) y v) En estos casos, n admite una representación primitiva como suma de tres cuadrados no nulos y basta aplicar el lema 1.4 ; y la proposición 1.3.

Un caso particular de iv) , es el resultado de Catalan (1880, cf. [10]) de que $\ell(3^\alpha,3) = 3$, para todo $\alpha \geq 1$.

vi) , vii) y viii) Son consecuencia inmediata del lema 1.4. #

Es fácil construir familias particulares de enteros $n > 0$ para los que $\ell(n,3) \geq 2$, aparte de las ya mencionadas. Por ejemplo, así sucede con todos los números de la forma $n = 4a^2+4a+33$ ó bien $n = 4a^2+4a+3$, $a \in \mathbb{Z}^+$. En efecto, las familias anteriores son casos particulares de enteros de la forma

$$n = 4a^2+4a+((2^b)^2 + (2^c)^2 + 1^2) .$$

que, obviamente, admiten la representación $n = (2^b)^2+(2^c)^2+(2a+1)^2$, siendo los dos primeros sumandos primos con n .

Probamos a continuación que dado un entero positivo impar n tal que $\ell(n,3) \geq 1$, si se aumentan, conservando la paridad, los exponentes de sus factores primos congruentes con 1(mód 4), entonces se consigue nivel mayor ó igual a 2 .

Lema 1.6. (v.[2]) Si $a,b \in \mathbb{Z}^+$ verifican que $a = a_1^2+a_2^2$ y $b = b_1^2+b_2^2+b_3^2$, entonces

$$a^2b = c_1^2+c_2^2+c_3^2 \quad ,$$

siendo

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

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

$$c_3 = ab_3 \quad .$$

Proposición 1.7. Sea $n = 2^{\alpha}p_1^{\alpha_1}\cdots p_r^{\alpha_r}q_1^{\beta_1}\cdots q_s^{\beta_s}$, con $p_i \equiv 1(\text{mód } 4)$, $1 \leq i \leq r$ y $q_j \equiv 3(\text{mód } 4)$, $1 \leq j \leq s, \alpha = 0$ ó 1 . Entonces si $\ell(n,3) \geq 1$, y $m = 2^{\alpha}p_1^{\gamma_1}\cdots p_r^{\gamma_r}q_1^{\beta_1}\cdots q_s^{\beta_s}$, con $\gamma_i > \alpha_i$ y $\gamma_i \equiv \alpha_i(\text{mód } 2)$, resulta que :

i) Si $\alpha = 0$, entonces $\ell(m,3) \geq 2$,

ii) Si $\alpha = 1$, entonces $\ell(m,3) \geq 1$.

Demostración.

i) Escribamos $m = a^2 b$, siendo
$a = p_1^{\delta_1} \cdots p_r^{\delta_r}$, con $\gamma_i = 2\delta_i + \alpha_i$, $i = 1,\ldots,r$; $\delta_i \geq 1$,
y $b = n$. Entonces $a = a_1^2 + a_2^2$, con $(a_i, a) = 1$; $1 \leq i \leq 2$,
y $b = b_1^2 + b_2^2 + b_3^2$, con $(b_3, b) = 1$; $(b_1, b) > 1$; $(b_2, b) > 1$
y $(b_1, b_2, b_3) = 1$.

Veamos ahora que $(c_1, m) = (c_2, m) = 1$, con lo que quedará probado que $\ell(m,3) \geq 2$.

1er caso. Sea $p \equiv 1 (\text{mód } 4)$ tal que $p \mid m$, con $p \nmid b_1$ y $p \mid b_2$; entonces

$$c_1 \equiv -2a_1 b_1 a_1 \not\equiv 0 \ (\text{mód } p) \ ,$$

y

$$c_2 \equiv -2a_1 b_1 c_2 \not\equiv 0 \ (\text{mód } p) \ ,$$

ya que $p \mid a$.

2º caso. Sea $p \equiv 1 (\text{mód } 4)$ tal que $p \mid m$, con $p \mid b_1$ y $p \nmid b_2$; entonces

$$c_1 \equiv -2a_2 b_2 a_1 \not\equiv 0 \ (\text{mód } p) \ ,$$

$$c_2 \equiv -2a_2 b_2 a_2 \not\equiv 0 \ (\text{mód } p) \ ,$$

ya que $p \mid a$.

3er caso. Sea $p \equiv 1 (\text{mód } 4)$ tal que $p \mid m$, con $p \nmid b_1$ y $p \nmid b_2$; entonces tanto la condición $c_1 \equiv 0 (\text{mód } p)$, como $c_2 \equiv 0 (\text{mód } p)$

implicarían que

$$a_1 b_1 + a_2 b_2 \equiv 0 \pmod{p} \quad ,$$

pero como $p \nmid b_1$, resultaría que

$$a_1 \equiv - \frac{a_2 b_2}{b_1} \pmod{p} \quad ,$$

y como $p \mid a_1$ que

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

de donde, $b_1^2 + b_2^2 \equiv 0 \pmod{p}$ y, por tanto, $b \equiv b_3^2 \pmod{p}$, lo cual es absurdo ya que $b \equiv 0 \pmod{p}$ y $p \nmid b_3$.

Así que en este caso también se verifica que $c_1 \not\equiv 0 \pmod{p}$ y $c_2 \not\equiv 0 \pmod{p}$, para todo $p \equiv 1 \pmod{4}$ tal que $p \mid m$.

Además como para todo factor primo de m , $q \equiv 3 \pmod{4}$ se tiene que $q \nmid c_3$, resulta, al ser $c_1 \neq 0$ y $c_2 \neq 0$ por el lema 1.4, que $q \nmid c_1$ y $q \nmid c_2$ y, por tanto, es $\ell(n,3) \geq 2$. Esto concluye la demostración de i).

ii) En este caso tomamos
$a = p_1^{\delta_1} \ldots p_r^{\delta_r}$, con $\gamma_i = 2\delta_i + \alpha_i$, $1 \leq i \leq r$, $\delta_i \geq 1$; y
$b = 2q_1^{\beta_1} \ldots q_s^{\beta_s}$. Igual que en el caso anterior es $m = a^2 b$.

Para todo divisor primo $p \neq 2$ de m se tiene que $c_1 \not\equiv 0 \pmod{p}$ y $c_2 \equiv 0 \pmod{p}$. Como $c_3 = ab_3$ resulta que $2 \nmid c_3$ y al ser $2^2 \nmid m$, obtenemos que $2 \nmid c_1$ ó $2 \nmid c_2$ y, por tanto, $\ell(m,3) \geq 1$. #

§3. Relación del 3-nivel con la propiedad (N)

En este apartado relacionamos el concepto de nivel con la propiedad (N) de los números enteros, indicando el papel que juega esta propiedad en el contexto del problema inverso de la teoría de Galois.

Según Vila, ([44]), recordemos que un entero $n \not\equiv 0,4,7 (\text{mód } 8)$ se dice que tiene la propiedad (N) si existen enteros x_1, x_2, x_3 tales que $n = x_1^2+x_2^2+x_3^2$ y, para algún i, $1 \leq i \leq 3$, $(x_i, n) = 1$ y $x_i^2 \leq (n+1)/3$.

Evidentemente, resulta la siguiente

Proposición 1.8. Si $\ell(n,3) = 3$, entonces n verifica la propiedad (N). #

Como es sabido, el problema inverso de la teoría de Galois pregunta si, dado un grupo finito G, existe una extensión de Galois K del cuerpo de las racionales $\mathbb{Q}$ que tenga a G como grupo de Galois.

La conexión de la propiedad (N) con el problema inverso de la teoría de Galois se establece en el siguiente

Teorema 1.9. ([44],5.18) Si $n \equiv 3 (\text{mód } 8)$ es un entero que verifica la propiedad (N), entonces toda extensión central, del grupo alternado A_n se realiza como grupo de Galois sobre $\mathbb{Q}$. #

El objetivo de los siguientes capítulos es la determinación exacta del 3-nivel de cada entero.

Siempre que no haya posibilidad de confusión hablaremos de nivel de un entero para designar el 3-nivel.

$$r(n,f) = \#\{ (x_i) \in \mathbb{Z}^k \mid f(x_1,\ldots,x_k) = n \} \quad ,$$

$$r^*(n,f) = \#\{(x_i) \in \mathbb{Z}^k \mid f(x_1,\ldots,x_k) = n \text{ y } \text{m.c.d.}(x_i) = 1 \} ,$$

$$r_m(n,f) = \#\{(x_i) \in (\mathbb{Z}/m\,\mathbb{Z})^k \mid f(x_1,\ldots,x_k) \equiv n (\text{mód } m)\} \quad ;$$

denominando a $r(n,f)$ *el número de representaciones enteras de* n *por* f ; $r^*(n,f)$ *el número de representaciones primitivas de* n *por* f y, por último, $r_m(n,f)$ *el número de representaciones de* n *por* f, *módulo* m.

Como que f es una forma definida positiva, $r(n,f)$ es finito.

Si f es una forma cuadrática diagonal, abreviadamente escribiremos $f = \langle a_1,\ldots,a_k \rangle$, e indicaremos por I_k la forma $\langle \overbrace{1,\ldots,1}^{k} \rangle$.

Evidentemente, se tiene que

$$r(n,f) = \sum_{d^2 \mid n} r^*\left(\frac{n}{d^2},f\right) .$$

Ello a su vez permite expresar $r^*(n,f)$ en función de $r(\frac{n}{d^2},f)$, mediante la fórmula de inversión de Möbius. Se obtiene así

$$r^*(n,f) = \sum_{d^2 \mid n} \mu(d)\ r\left(\frac{n}{d^2},f\right) ,$$

CAPITULO II

CRITERIOS CUANTITATIVOS PARA LA OBTENCION DEL NIVEL DE UN ENTERO

En este capítulo se introducen fórmulas para la determinación del 3-nivel de un entero. Si éstas fuesen evaluables, el estudio de $\ell(n,3)$ sería directamente abordable. Sin embargo no lo son y es sólo posible un cálculo en promedio de dichas expresiones. Ello conduce a la definición de *término principal* en la evaluación del 3-nivel de un entero.

§1. Número de representaciones de un entero por una forma

Sea f una forma cuadrática entera, definida positiva de k variables :

$$f(X) = \sum_{i=1}^{k} a_{ii}X_i^2 + 2 \sum_{i<j} a_{ij}X_iX_j \quad ,$$

con $a_{ij} \in \mathbb{Z}$.

Sea n un entero positivo, un vector (x_i) de $\mathbb{Z}^k$ es una representación de n por f si es solución de la ecuación $f(X) = n$. Se definen las cantidades

en donde

$$\mu(n) = \begin{cases} 1 & \text{Si } n = 1 . \\ 0 & \text{Si } a^2 \mid n \text{ para algún } a > 1. \\ (-1)^r & \text{Si } n = p_1 \ldots p_r \text{ , } p_i \text{ primos distintos,} \end{cases}$$

es la conocida función de Möbius.

§2. Planteo de los cálculos para la determinación del 3-nivel de un entero

Sea n un entero positivo, $n \neq 4^a(8m+7)$. Designamos por $D_i(n)$ al conjunto de soluciones enteras de la ecuación

$$X_1^2 + X_2^2 + X_3^2 = n$$

con, exactamente, i componentes no primas con n. Designamos por $d_i(n)$ al cardinal de $D_i(n)$:

$$d_i(n) = \# D_i(n) \text{ , para } i = 1,2,3.$$

Definimos las siguientes cantidades

$$g_1(n) = \frac{d_3(n)}{r(n,I_3)} \quad ,$$

$$g_2(n) = \frac{d_2(n) + d_3(n)}{r(n,I_3)} \quad ,$$

$$g_3(n) = \frac{d_1(n) + d_2(n) + d_3(n)}{r(n,I_3)} \quad .$$

Se tiene el siguiente

Lema 2.1.

i) Sea n un entero positivo impar, $n \not\equiv 7 (\text{mód } 8)$.

Entonces

$$\ell(n,3) \geq i \quad \text{si y sólo si } g_i(n) < 1 ,$$

para $i = 1,2,3$.

ii) Sea n un entero par $n \not\equiv 0,4 (\text{mód } 8)$.

Entonces

$$\ell(n,3) \geq i \quad \text{si y sólo si } g_i(n) < 1 ,$$

para $i = 1,2$.

Observación. En el caso en que $n \equiv 0,4 (\text{mód } 8)$ y $n \neq 4^a(8m+7)$ se tiene que $d_1(n)=d_2(n)=0$ y $d_3(n)=r(n,I_3)$. En consecuencia es $g_i(n) = 1$, $i = 1,2,3$.

Ahora bien, si n es par, $n \not\equiv 0,4 (\text{mód } 8)$, se tiene (cf. proposición 1.3) que $g_3(n) = 1$.

Definimos a continuación unas sumas auxiliares para la evaluación de $d_i(n)$, en donde los enteros a_1, a_2, a_3, se supondrán siempre libres de cuadrados.

$$s_3(n) := \sum_{\substack{a_i \mid n \\ a_i \neq 1}} - \mu(a_1 a_2 a_3)\, r(n, \langle a_1^2, a_2^2, a_3^2 \rangle) ,$$

$$s_2(n) := \sum_{\substack{a_i \mid n \\ a_i \neq 1}} \mu(a_1 a_2)\, r(n, \langle a_1^2, a_2^2, 1\rangle)$$

$$+ \sum_{\substack{a_i \mid n \\ a_i \neq 1}} \mu(a_1 a_2)\, r(n, \langle a_1^2, 1, a_2^2\rangle)$$

$$+ \sum_{\substack{a_i \mid n \\ a_i \neq 1}} \mu(a_1 a_2)\, r(n, \langle 1, a_1^2, a_2^2\rangle)$$

$$s_1(n) := \sum_{\substack{a \mid n \\ a \neq 1}} -\mu(a)\, r(n, \langle a^2, 1, 1\rangle)$$

$$+ \sum_{\substack{a \mid n \\ a \neq 1}} -\mu(a)\, r(n, \langle 1, a^2, 1\rangle)$$

$$+ \sum_{\substack{a \mid n \\ a \neq 1}} -\mu(a)\, r(n, \langle 1, 1, a^2\rangle),$$

siendo μ la función de Möbius.

Puesto que,

$$r(n, \langle a^2, 1, 1\rangle) = r(n, \langle 1, a^2, 1\rangle) = r(n, \langle 1, 1, a^2\rangle);$$

$$r(n, \langle a_1^2, a_2^2, \rangle) = r(n, \langle a_1^2, 1, a_2^2\rangle) = r(n, \langle 1, a_1^2, a_2^2\rangle),$$

resulta que podemos escribir

$$s_1(n) = 3 \sum_{\substack{a \mid n \\ a \neq 1}} -\mu(a)\, r(n, \langle a^2, 1, 1\rangle),$$

$$s_2(n) = 3 \sum_{\substack{a_i \mid n \\ a_1 \neq 1}} \mu(a_1 a_2)\, r(n, \langle a_1^2, a_2^2, 1 \rangle).$$

Las sumas $s_i(n)$, $i=1,2,3$, dan cuenta del número de representaciones de n de nivel menor o igual a $(3-i)$. En el siguiente teorema se da la relación existente entre el valor de estas sumas y las cantidades $d_i(n)$.

Teorema 2.2. Sea $n \not\equiv 0,4,7 (\text{mód } 8)$. Se verifica:

i) $s_3(n) = d_3(n)$;

ii) $s_2(n) = d_2(n) + 3\, d_3(n)$,

iii) $s_1(n) = d_1(n) + 2\, d_2(n) + 3\, d_3(n)$.

Demostración. i) Sea (x_1, x_2, x_3) una representación de n como suma de tres cuadrados, perteneciente a $D_3(n)$, es decir $(x_i, n) > 1$, para $i=1,2,3$. Designemos por A_i el producto de los diferentes primos, todos con exponente 1, que son comunes a x_i y a n, para $i=1,2,3$.

Entonces (x_1, x_2, x_3) se cuenta exactamente una vez en $r(n, \langle a_1^2, a_2^2, a_3^2 \rangle)$ si y sólo si $a_i \mid A_i$.

Escribamos $\omega(a_i) = k_i$, y $\omega(A_i) = t_i$, $(i=1,2,3)$, en donde, como es usual, $\omega(n)$ designa el número de divisores primos distintos de n. Como A_i posee exactamente $\binom{t_i}{k}$ divisores distintos que se expresen como producto de k factores primos y ya que $-\mu(abc) = (-1)^{k+1}$, siendo $k = \omega(a) + \omega(b) + \omega(c)$, resulta

que un elemento cualquiera (x_1,x_2,x_3) de $D_3(n)$ se cuenta en $s_3(n)$ un número de veces igual a :

$$\sum_{\substack{k_i=1 \\ i=1,2,3}}^{t_i} (-1)^{k_1+k_2+k_3} \binom{t_1}{k_1} \binom{t_2}{k_2} \binom{t_3}{k_3}$$

$$= - \sum_{k_1=1}^{t_1} (-1)^{k_1} \binom{t_1}{k_1} \cdot \sum_{k_2=1}^{t_2} (-1)^{k_2} \binom{t_2}{k_2} \cdot \sum_{k_3=1}^{t_3} (-1)^{k_3} \binom{t_3}{k_3}$$

$$= - (-1)\ (-1)\ (-1) = 1.$$

Además, como en $s_3(n)$ sólo se cuentan representaciones de n con las 3 componentes no primas con n, queda probado que $s_3(n) = d_3(n)$.

ii) En este caso, en $s_2(n)$ se cuentan soluciones de $X_1^2+X_2^2+X_3^2 = n$ con un sumando como máximo primo con n, ésto es, soluciones de $D_2(n) \cup D_3(n)$. Ahora bien, conviene distinguir las soluciones de $D_2(n)$ de las de $D_3(n)$.

Si (x_1,x_2,x_3) es de $D_2(n)$, supongamos que son $(x_i,n)>1$ para i=1,2 y escribamos A_i la parte común a x_i y a n. Entonces, procediendo análogamente al caso anterior, resulta que ese elemento se cuenta en $s_2(n)$ sólo en el primer sumando y concretamente un número de veces igual a

$$\sum_{\substack{k_i=1 \\ i=1,2}}^{t_i} (-1)^{k_1+k_2} \binom{t_1}{k_1} \binom{t_2}{k_2}$$

$$= \sum_{k_1=1}^{t_1} (-1)^{k_1} \binom{t_1}{k_1} \cdot \sum_{k_2=1}^{t_2} (-1)^{k_2} \binom{t_2}{k_2} = (-1)(-1) = 1 .$$

Si tomamos ahora (x_1,x_2,x_3) de $D_3(n)$ y volvemos a escribir A_i para la parte común de x_i y n , $(i = 1,2,3)$, resulta que esta solución de $D_3(n)$, se ha contado una vez en el primer sumando de $s_2(n)$ al considerar exclusivamente divisores de A_1 y A_2, otra en el segundo sumando considerando los de A_1 y A_3 y una tercera y última vez en el tercer sumando al considerar los de A_2 y A_3 .

En consecuencia, en $s_2(n)$ hemos contado los elementos de $D_3(n)$ tres veces y como $D_2(n)$ y $D_3(n)$ son evidentemente disjuntos, queda probado que $s_2(n) = d_2(n) + 3d_3(n)$.

iii) En $s_1(n)$ se cuentan soluciones de $X_1^2 + X_2^2 + X_3^2 = n$ con dos sumandos como máximo primos con n, esto es soluciones de $D_1(n) \cup D_2(n) \cup D_3(n)$.

Si (x_1,x_2,x_3) es de $D_1(n)$, con $(x_1,n) > 1$ y A_1 la parte común entre x_1 y n , resulta,como en los casos anteriores, que en $s_1(n)$ se cuenta un número de veces igual a

$$\sum_{k_1=1}^{t_1} (-1)^{k_1+1} \binom{t_1}{k_1} = 1 .$$

Si (x_1,x_2,x_3) es de $D_2(n)$, siendo por ejemplo $(x_i,n) > 1$, para $i = 1,2$ entonces se cuenta una vez en el primer sumando

al considerar los divisores de A_1 y una vez en el segundo al considerar los de A_2 .

Por último, si (x_1,x_2,x_3) es de $D_3(n)$, procediendo como en el caso anterior, se tiene que se cuenta tres veces en $s_1(n)$.

Por consiguiente, al ser $D_1(n)$, $D_2(n)$ y $D_3(n)$ disjuntos dos a dos tenemos probado el teorema. #

Basta despejar $d_i(n)$, i = 1,2,3, en las expresiones dadas por el teorema 2.2 para obtener el siguiente

Corolario 2.3. Sea $n \not\equiv 0,4,7 (\text{mód } 8)$. Entonces

$$\text{i)}\quad g_1(n) = \frac{s_3(n)}{r(n,I_3)} \quad ,$$

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

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

§3. Planteo de los cálculos mediante representaciones primitivas

Sea $n \not\equiv 0,4,7 (\text{mód } 8)$ un entero libre de cuadrados ó, más en general, un entero libre de cuadrados respecto de sus divisores primos congruentes con 1 módulo 4. Escribamos

$$n = 2^{\alpha} mt \quad ,$$

siendo :

$\alpha = 0$ ó 1 ;

$m = p_1 \cdots p_r$, $p_i \equiv 1 (\text{mód } 4)$, $r \geq 1$

$t = q_1^{\beta_1} \cdots q_s^{\beta_s}$, $q_j \equiv 3 (\text{mód } 4)$, $s \geq 0$

En este caso si un primo $q \equiv 3(\text{mód } 4)$ divide a n, por el lema 1.4 está claro que no puede dividir a ningún sumando de cualquier representación *primitiva* de n como suma de tres cuadrados.

Así que si un sumando de una representación primitiva como suma de tres cuadrados tiene factores primos en común con n, éstos tienen que ser congruentes con 1 módulo 4, si n es impar. Si n es par aparece también el 2 . Obviamente, si un factor primo de éstos aparece en un sumando, no puede aparecer en los otros ya que n es libre de cuadrados respecto a tales factores primos.

Entonces en este caso se tiene que podemos definir, además de las anteriores, otras expresiones para calcular el nivel de n, teniendo en cuenta el número de sus representaciones primitivas.

Designamos por $D_i^*(n)$ al conjunto de soluciones primitivas de la ecuación

$$X_1^2 + X_2^2 + X_3^2 = n$$

con exactamente i componentes no primas con n. Designamos por $d_i^*(n)$ al cardinal de $D_i^*(n)$.

Definimos las siguientes cantidades :

$$g_1^*(n) = \frac{d_3^*(n)}{r^*(n,I_3)} \quad ,$$

$$g_2^*(n) = \frac{d_2^*(n) + d_3^*(n)}{r^*(n,I_3)} \quad ,$$

$$g_3^*(n) = \frac{d_1^*(n) + d_2^*(n) + d_3^*(n)}{r^*(n,I_3)} \quad .$$

Tenemos el siguiente

Lema 2.4.

i) Sea n un entero positivo impar, $n \not\equiv 7 (\text{mód } 8)$. Entonces

$$\ell(n,3) \geq i \text{ si y sólo si } g_i^*(n) < 1 \ ,$$

para $i = 1,2,3$.

ii) Sea n un entero positivo par, $n \not\equiv 0,4 (\text{mód } 8)$. Entonces

$$\ell(n,3) \geq i \text{ si y sólo si } g_i^*(n) < 1 \ ,$$

para $i = 1,2$.

Observación. Si n es par $n \not\equiv 0,4 (\text{mód } 8)$, entonces (cf. proposición 1.3), se tiene $g_3^*(n) = 1$.

Definimos a continuación unas sumas auxiliares para la evaluación de $d_i^*(n)$, en el caso en que $n \not\equiv 0,4,7 (\text{mód } 8)$ y n sea libre de cuadrados respecto de sus divisores primos congruentes con 1 módulo 4.

Caso n impar, $n \not\equiv 7 (\text{mód } 8)$.

$$s_3^*(n) := \sum_{\substack{1<a_i \mid m \\ (a_i,a_j)=1}} - \mu(a_1a_2a_3)\, r^*(n,<a_1^2,a_2^2,a_3^2>) ,$$

$$s_2^*(n) := \sum_{\substack{1<a_i \mid m \\ (a_1,a_2)=1}} \mu(a_1a_2)\, r^*(n,<a_1^2,a_2^2,1>)$$

$$+ \sum_{\substack{1<a_i \mid m \\ (a_1,a_2)=1}} \mu(a_1a_2)\, r^*(n,<a_1^2,1,a_2^2>)$$

$$+ \sum_{\substack{1<a_i \mid m \\ (a_1,a_2)=1}} \mu(a_1a_2)\, r^*(n,<1,a_1^2,a_2^2>) ,$$

$$s_1^*(n) := \sum_{\substack{a \mid m \\ a \neq 1}} - \mu(a)\, r^*(n,<a^2,1,1>)$$

$$+ \sum_{\substack{a \mid m \\ a \neq 1}} - \mu(a)\, r^*(n,<1,a^2,1>)$$

$$+ \sum_{\substack{a \mid m \\ a \neq 1}} - \mu(a)\, r^*(n,<1,1,a^2>) ,$$

siendo μ la función de Möbius, e indicando por (a_i,a_j) el m.c.d.(a_i,a_j).

Puesto que,

$$r^*(n,<a^2,1,1>) = r^*(n,<1,a^2,1>) = r^*(n,<1,1,a^2>) ,$$

$$r^*(n,<a_1^2,a_2^2,1>) = r^*(n,<a_1^2,1,a_2^2>) = r^*(n,<1,a_1^2,a_2^2>) \ ,$$

resulta que podemos escribir

$$s_1^*(n) = 3 \sum_{\substack{a \mid m \\ a \neq 1}} - \mu(a)\ r^*(n,<a^2,1,1>) \quad ,$$

$$s_2^*(n) = 3 \sum_{\substack{a_i \mid m \\ a_i \neq 1}} \mu(a_1 a_2)\ r^*(n,<a_1^2,a_2^2,1>) \quad .$$

Observación. Si n posee un único factor primo congruente con 1 módulo 4, entonces, evidentemente, es $s_2^*(n) = s_3^*(n) = 0$.

Si n posee exactamente dos factores primos congruentes con 1 módulo 4, entonces $s_3^*(n) = 0$.

Tenemos el siguiente

Teorema 2.5. Si n es un entero impar, $n \not\equiv 7 (\text{mód } 8)$, libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4, entonces :

i) $s_1^*(n) = d_1^*(n) + 2d_2^*(n) + 3d_3^*(n)$,

ii) $s_2^*(n) = d_2^*(n) + 3d_3^*(n)$,

iii) $s_3^*(n) = d_3^*(n)$.

Demostración. Consiste en proceder análogamente a la demostración del teorema 2.2, pero restringiéndose a considerar

sólo primos congruentes con 1 módulo 4. Es decir, en este caso A_i designará el producto de los diferentes primos congruentes con 1 módulo 4, todos con exponente 1, que son comunes a x_i y a n , para i = 1,2,3 .

Este razonamiento es correcto ya que al ser n libre de cuadrados en los factores primos congruentes con 1 módulo 4, se tiene que, si (y_1,y_2,y_3) es una solución primitiva de $\sum_{i=1}^{3} A_i^2X_i^2 = n$, entonces $(\frac{A_1}{a_1}y_1, \frac{A_2}{a_2}y_2, \frac{A_3}{a_3}y_3)$, para $a_i|A_i$, es también una solución primitiva de $\sum_{i=1}^{3} a_i^2X_i^2 = n$. En efecto, si un primo q congruente con 3 módulo 4 fuera común a $\frac{A_1}{a_1}y_1$, $\frac{A_2}{a_2}y_2$, $\frac{A_3}{a_3}y_3$, como las A_i constan sólo de factores primos congruentes con 1 módulo 4 , resultaría que q dividiría a y_1, y_2 e y_3, lo cual es absurdo. Por otra parte, si un primo congruente con 1 módulo 4 fuese común a $\frac{A_1}{a_1}y_1$, $\frac{A_2}{a_2}y_2$, $\frac{A_3}{a_3}y_3$, no podría dividir simultáneamente a todas las y_i, digamos $p\nmid y_1$. Entonces $p|A_1$ y, por consiguiente, $p\nmid A_2$, $p\nmid A_3$, pues por construcción $(A_i,A_j) = 1$ si $i\neq j$, así que $p|y_2$, $p|y_3$. Como $p|n$ resultaría $p^2|n$, lo cual es absurdo ya que n es libre de cuadrados en los primos congruentes con 1 módulo 4. #

Corolario 2.6. Si n es un entero impar, $n \not\equiv 7 (\text{mód } 8)$, libre de cuadrados respecto de sus divisores primos congruentes con 1 módulo 4, se verifica :

$$\text{i)}\quad g_1^*(n) = \frac{s_3^*(n)}{r^*(n,I_3)} \quad ,$$

$$\text{ii)}\quad g_2^*(n) = \frac{s_2^*(n) - 2s_3^*(n)}{r^*(n,I_3)} \quad ,$$

$$\text{iii)}\quad g_3^*(n) = \frac{s_1^*(n) - s_2^*(n) + s_3^*(n)}{r^*(n,I_3)} \quad .$$

Caso n par, $n \not\equiv 0,4 \pmod 8$.

Observando que toda representación de n como suma de tres cuadrados posee un único sumando múltiplo de 2, definimos :

$$s_3^*(n) := \sum_{\substack{1<a_i|m \\ (a_1,a_2)=1}} \mu(a_1a_2)\, r^*(n,<a_1^2,a_2^2,2^2>)$$

$$+ \sum_{\substack{1<a_i|m \\ (a_1,a_2)=1}} \mu(a_1a_2)\, r^*(n,<a_1^2,2^2,a_2^2>)$$

$$+ \sum_{\substack{1<a_i|m \\ (a_1,a_2)=1}} \mu(a_1a_2)\, r^*(n,<2^2,a_1^2,a_2^2>) \quad ,$$

$$s_2^*(n) := \sum_{1<a|m} -\mu(a)\, r^*(n,<a^2,2^2,1^2>)$$

$$+ \sum_{1<a|m} -\mu(a)\, r^*(n,<a^2,1^2,2^2>)$$

$$+ \sum_{1<a|m} -\mu(a)\, r^*(n,<2^2,a^2,1^2>)$$

$$+ \sum_{1<a|m} -\mu(a)\, r^*(n,<2^2,1^2,a^2>)$$

$$+ \sum_{1<a|m} -\mu(a)\, r^*(n,<1^2,a^2,2^2>)$$

$$+ \sum_{1<a|m} -\mu(a)\, r^*(n,<1^2,2^2,a^2>) \quad .$$

Como en casos anteriores se tiene que podemos escribir :

$$s_2^*(n) = 6 \sum_{\substack{a|m \\ a\neq 1}} -\mu(a)\, r^*(n,<a^2,2^2,1^2>) \quad ,$$

$$s_3^*(n) = 3 \sum_{\substack{1<a_i|m \\ (a_1,a_2)=1}} \mu(a_1a_2)\, r^*(n,<a_1^2,a_2^2,2^2>) \quad .$$

Procediendo igual que en el caso impar se obtiene el siguiente

Teorema 2.7. Si n es un entero positivo par, $n \not\equiv 0,4 \pmod 8$, libre de cuadrados respecto de sus divisores primos congruentes con 1 módulo 4, entonces

i) $s_2^*(n) = d_2^*(n) + 2d_3^*(n)$,

ii) $s_3^*(n) = d_3^*(n)$.

Por tanto, se verifica el siguiente

Corolario.2.8. Si n es un entero positivo par, $n \not\equiv 0,4 (\text{mód } 8)$, libre de cuadrados respecto de sus divisores primos congruentes con 1 módulo 4, entonces

i) $g_1^*(n) = \dfrac{s_3^*(n)}{r^*(n,I_3)}$,

ii) $g_2^*(n) = \dfrac{s_2^*(n) - s_3^*(n)}{r^*(n,I_3)}$. #

Si r(n,f) fuese calculable para las formas que aparecen en $s_i(n)$ y en $s_i^*(n)$, ya sería abordable el estudio de $\ell(n,3)$. Sin embargo, sólo se conoce este valor de manera exacta cuando $f = I_3$.

El cálculo de $r^*(n,I_3)$ fue iniciado por Legendre y Gauss. Este último dió la siguiente fórmula (cf. [10]) :

$r^*(n,I_3) = 3.2^{\omega+2}h$, si $n \equiv 1,2,5,6 (\text{mód } 8)$,

$r^*(n,I_3) = 2^{\omega+2}h$, si $n \equiv 3 (\text{mód } 8)$,

siendo ω el número de factores primos distintos de n y h el número de clases de formas cuadráticas binarias de discriminante -4n.

Dirichlet (cf.[13]) aplicando su fórmula analítica, para el número de clases de formas binarias, a la fórmula precedente de Gauss obtuvo

$$r^*(n,I_3) = 2\pi n^{1/2}\, L(1,\chi_{-4n}) \ ,$$

siendo $L(s,\chi_{-4n})$ la L-serie de Dirichlet asociada al carácter χ_{-4n} .

En general, para r(n,f) sólo es posible un cálculo en *promedio*. Para establecer este promedio es fundamental el concepto clásico de género, que a continuación se recuerda.

§4. Género de una forma cuadrática. "Hauptsatz" de Siegel

Dado un anillo R se dice que dos formas cuadráticas f_1, f_2 de k variables con coeficientes en R son R-*equivalentes*, o que pertenecen a la misma clase,si existe una transformación $u\in GL(k,R)$ tal que $f_1(uX) = f_2(X)$; en términos de matrices

$$F_2 = U^T F_1 U \quad .$$

Evidentemente, si f_1 y f_2 son dos formas enteras definidas positivas y $\mathbb{Z}$-equivalentes, se tiene que

$$r(n,f_1) = r(n,f_2) \text{ y } \det(f_1) = \det(f_2) \ ,$$

indicando por det(f) el determinante de la matriz de f.

Si f_1 y f_2 son dos formas cuadráticas con coeficientes en $\mathbb{Z}_p$ y $\mathbb{Z}_p$-equivalentes, entonces

$$r_{p^t}(n,f_1) = r_{p^t}(n,f_2) \quad ,$$

para todo $t \geq 1$, siendo $\mathbb{Z}_p$ el anillo de enteros p-ádicos.

Si f es una forma cuadrática entera definida positiva se definen el *grupo de isotropía* de f, O(f), y el *grupo de isotropía* de f *módulo* m, $O_m(f)$, del siguiente modo :

$$O(f) = \{u \in GL(k,\mathbb{Z}) \mid U^T F U = F\} \quad .$$

$$O_m(f) = \{u \in GL(k,\mathbb{Z}/m\mathbb{Z}) \mid U^T F U \equiv F (\text{mód } m)\} \quad .$$

Se escribe $o(f) = \# O(f)$ y $o_m(f) = \# O_m(f)$.

Definición. (cf. [41]) Se dice que dos formas cuadráticas enteras $f_1(x)$ y $f_2(x)$ pertenecen a un mismo *género* si son equivalentes en cada anillo de enteros p-ádicos, y sobre los reales; es decir, si son equivalentes en $\mathbb{Z}_p$, para cada p, incluyendo $p = \infty$.

Evidentemente, todo género está formado por una unión de $\mathbb{Z}$-clases. En el caso de formas definidas positivas, la teoría de Hermite garantiza que el número de clases en un género es finito.

Trabajos de Gauss, Eisenstein, Smith, Minkowski y Siegel condujeron al concepto de *número promedio de representacio-*

nes de un entero por un género, r(n,gen f), que es un valor medio del número de representaciones de n por todas las formas que integran un género. Pasamos a considerarlo a continuación.

Sea $f = f_1,\ldots,f_h$ un sistema completo de representantes de $\mathbb{Z}$-clases de formas en el género de f, f definida positiva, entonces se define

$$r(n,\text{gen } f) = \left(\sum_{i=1}^{h} \frac{1}{o(f_i)} \right)^{-1} \cdot \left(\sum_{i=1}^{h} \frac{r(n,f_i)}{o(f_i)} \right) \quad .$$

Al número

$$M(\text{gen } f) := \sum_{i=1}^{h} \frac{1}{o(f_i)} \quad ,$$

se le llama la *masa del género* de f .

Análogamente, se define el número promedio de representaciones primitivas de n por el género de f mediante la fórmula

$$r^*(n,\text{gen } f) = \left(\sum_{i=1}^{h} \frac{1}{o(f_i)} \right)^{-1} \cdot \left(\sum_{i=1}^{h} \frac{r^*(n,f_i)}{o(f_i)} \right) \quad ,$$

verificándose la igualdad

$$r^*(n,\text{gen } f) = \sum_{d^2|n} \mu(d)\, r(nd^{-2}, \text{gen } f) \quad ,$$

siendo μ, como siempre, la función de Möbius.

Siegel [41] en sus investigaciones sobre la teoría analítica de formas cuadráticas enteras definidas positivas obtu

vo una fórmula que expresa el valor r(n,gen f) mediante densidades p-ádicas :

Lema 2.9. ([41],Cap. 1) Sea p^b la máxima potencia de p que aparece en 2n y $a > 2b$, $q = p^a$.
Entonces el valor

$$\partial_p(n,f) := q^{1-k} r_q(n,f) \quad ,$$

es independiente de a, y se denomina *densidad p-ádica* de las representaciones de n por f.

Del mismo modo, Siegel (cf.[41])definió una densidad para $p = \infty$, $\partial_\infty(n,f)$. Considerando n como un punto de $\mathbb{R}$, se define

$$\partial_\infty(n,f) := \lim_{t \to o} \frac{\mathrm{vol}(f^{-1}[n-t/2,\ n+t/2])}{t} \quad ,$$

siendo $\mathrm{vol}(f^{-1}([n-t/2,\ n+t/2])$ el volumen en $\mathbb{R}^k$. La existencia del límite precedente fue probada por Siegel ([41] Cap. 2).

La fórmula antes mencionada viene dada por el siguiente

"Hauptsatz" de Siegel ([41]). Sea $n > 0$ un entero y f una forma cuadrática entera definida positiva. Entonces

$$r(n,\mathrm{gen}\ f) = \partial_\infty(n,f) \cdot \prod_p \partial_p(n,f) \quad .$$

Observaciones.

i) El producto $\prod_p \partial_p(n,f)$ es siempre convergente por ser f definida positiva (cf.[41],Hilfssatz 25).

ii) Todas las definiciones anteriores se pueden extender al caso de representaciones de formas por formas. Por ejemplo, si f es una k-forma cuadrática entera definida positiva y g una m-forma ($m \leq k$) con las mismas condiciones, se dice que f representa a g si existe una matriz entera S , k x m, tal que

$$S^T F S = G \quad .$$

Entonces, r(g,f) designa el número de representaciones de g por f . Análogamente se definen $r^*(g,f)$, $\partial_p(g,f)$ $\partial_\infty(g,f)$ etc.; obteniéndose un *Hauptsatz* de Siegel generalizado[41], a saber :

$$r(g,\text{gen } f) = \varepsilon \partial_\infty(g,f) \prod_p \partial_p(g,f) \quad ,$$

con $\varepsilon = 1$, si $k > m+1$ ó $k = m = 1$,

y $\varepsilon = 1/2$, si $k = m+1$ ó $k = m > 1$.

iii) Al calcular r(f,gen f) se obtiene para la masa del género la expresión

$$M(\text{gen } f)^{-1} = 1/2 \; \partial_\infty(f,f) \prod_p \partial_p(f,f) \quad .$$

iv) Si el género de f consta de una sóla clase, se tiene que $r(n,f) = r(n,\text{gen } f)$, con lo que en este caso el teorema de Siegel proporciona el valor exacto de $r(n,f)$. Esto ocurre si $f = I_3$.

Siegel no dió fórmulas para hallar las densidades p-ádicas en todos los casos. Los casos resueltos por Siegel vienen dados en los siguientes lemas

Lema 2.10. ([41] Cap. II) Sea f una forma cuadrática entera definida positiva de k variables, para todo entero $n > o$ se tiene que

$$\partial_\infty(n,f) = \frac{\pi^{\frac{k}{2}} \, n^{\frac{k-2}{2}}}{\Gamma(\frac{k}{2})(\det f)^{\frac{1}{2}}} \quad .$$

Lema 2.11. ([41] Hilfssatz 16) Sea $(p, 2\det f) = 1$, y $n = p^b n_1$ con $(n_1,p) = 1$; escribamos

$$\varepsilon = \frac{(-1)^{\frac{k}{2}} \det f}{p} \quad , \quad \ell = p^{1-\frac{1}{2}} \quad \text{si k es par ,}$$

$$\varepsilon = \frac{(-1)^{k-1} \det f \cdot n_1}{p} \quad , \quad \ell = p^{2-k} \quad \text{si k es impar .}$$

Entonces, para $q = p^a$, $a > b$, se tiene la fórmula

$$q^{1-k} r_q(n,f) = (1-\varepsilon p^{-\frac{k}{2}})(1+\varepsilon\ell+\varepsilon^2\ell^2+\ldots+\varepsilon^b\ell^b) \quad (k \text{ par}) ,$$

$$= (1-p^{1-k})(1+\ell+\ell^2+\ldots+\ell^{\frac{b-1}{2}}) \quad (k \text{ impar, } b \text{ impar}) ,$$

$$= (1-p^{1-k})(1+\ell+\ell^2+\ldots+\frac{\ell^{b/2}}{1-\varepsilon p^{\frac{1-k}{2}}}) \quad (k \text{ impar, } b \text{ par}) . \#$$

Ya vimos en el Capítulo I, proposición 1.3., que si un entero n posee como máximo 2 divisores primos congruentes con 1 módulo 4, entonces se puede asegurar que $\ell(n,3) > 0$. En el caso en que $n = p_1p_2p_3 \prod_{j=1}^{s} q_j$, $n \not\equiv 7 (\text{mód } 8)$, con $p_i \equiv 1 (\text{mód } 4)$, $q_j \equiv 3 (\text{mód } 4)$, si $q \mid n$, entonces $q=q_j$, y $n = x^2+y^2+z^2$, resulta que $q \nmid xyz$ (cf. Lema 1.4). Por tanto, en este caso, siendo n libre de cuadrados, está claro que

$$\ell(n,3) > 0 \iff \frac{r(n,\langle p_1^2,p_2^2,p_3^2\rangle)}{r(n,I_3)} < 1 .$$

Si gen $\langle p_1^2,p_2^2,p_3^2\rangle$ tuviera una *única* clase, el "Hauptsatz" de Siegel permitiría conocer el valor $r(n,\langle p_1^2,p_2^2,p_3^2\rangle)$, previo cálculo de las densidades p-ádicas correspondientes. Pero vamos a ver a continuación que incluso en este caso "sencillo", gen$\langle p_1^2,p_2^2,p_3^2\rangle$ no coincide con la clase de $\langle p_1^2,p_2^2,p_3^2\rangle$.

Lema 2.12. Sea $f = \langle p_1^2,p_2^2,p_3^2\rangle$, con $p_i \equiv 1 (\text{mód } 4)$, $i = 1,2,3$, y sea $p = p_i$ para algún i . Entonces

$$o_{p^5}(f) \leq 4p^{17} .$$

Demostración. Sea S una matriz de $O_{p^5}(f)$, que representaremos

$$S = \left(\begin{array}{c|c} A & C \\ \hline D & B \end{array}\right) \quad ;$$

de modo que $A \in \mathbb{Z}/p^5\mathbb{Z}$, $C \in M_{1x2}(\mathbb{Z}/p^5\mathbb{Z})$, $D \in M_{2x1}(\mathbb{Z}/p^5\mathbb{Z})$ y $B \in M_{2x2}(\mathbb{Z}/p^5\mathbb{Z})$.

Si llamamos E a la matriz

$$\begin{pmatrix} p_2^2 & 0 \\ 0 & p_3^2 \end{pmatrix} ,$$

por ser S de $O_{p5}(f)$ se verifica :

$$A^T p^2 A + D^T E D \equiv p^2 \pmod{p^5} \qquad (1)$$

$$A^T p^2 C + D^T E B \equiv (0,0) \pmod{p^5} \qquad (2)$$

$$C^T p^2 C + B^T E B \equiv E \pmod{p^5} \qquad (3) \quad .$$

De (3) tenemos $B^T E B \equiv E \pmod{p}$, con lo que $(\det E)(\det B)^2 \equiv \equiv \det E \pmod{p}$ y como el det E es inversible en $\mathbb{Z}/p\mathbb{Z}$ resulta que det B es inversible, módulo p^5 .

Al ser E y B inversibles módulo p^5, resulta de (2)

$$D^T \equiv -A^T p^2 C B^{-1} E^{-1} \pmod{p^5} .$$

Por tanto dadas A,B,C queda D unívocamente determinada.

Dividiendo por p^2 en (1) se tiene

$$A^2 + \frac{D^T E D}{p^2} \equiv 1 \pmod{p^3} \quad ;$$

ahora bien, reduciendo módulo p^2 resulta que $D \equiv (0,0)$ módulo p^2 , así que $p^{-2}(D^T E D)$ es múltiplo de p^2, con lo que $A^2 \equiv 1 (\text{mód } p)$. Por tanto, el número de posibilidades para A módulo p^3, y, en consecuencia, en (1), es menor o igual que $2p^2$.

Pasamos otra vez a (3) :

$$B^T E B \equiv E - C^T p^2 C \quad (\text{mód } p^5) \ ,$$

está claro que para cada valor fijo de C, que tiene $(p^5)^2$ posibilidades, el número máximo de posibilidades para B es $o_{p^5}(E)$.

Como $p \nmid p_2 p_3$, se tiene ([41] Hilfssatz 18) :

$$o_{p^5}(E) = 2p^5 \left(1-\left(\frac{-1}{p}\right) p^{-1}\right) = 2p^5(1-p^{-1}) < 2p^5 \ ;$$

así que $o_{p^5}(f) \leq 2p^2 p^{10} 2p^5 = 4p^{17}$. #

Lema 2.13. $o_{2^3}(f) \leq 3.2^{14}$.

Demostración. La matriz F de $f = \langle p_1^2, p_2^2, p_3^2 \rangle$ verifica $F \equiv I_3 \ (\text{mód } 2^3)$ y, por tanto,

$$A \in O_{2^3}(f) \iff A^T A \equiv I_3 \ (\text{mód } 2^3) \ ,$$

de lo que se deduce, también, $AA^T \equiv I_3 \ (\text{mód } 2^3)$.

Si escribimos,

$$A = \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{pmatrix} \ ,$$

de $a^2+b^2+c^2 \equiv 1 \pmod{2^3}$ resulta que las soluciones posibles (en cuadrados) son las ternas : (1,0,0), (1,4,4), con todas las permutaciones posibles. Por tanto, la primera columna tiene 3.2^5 posibilidades.

De $AA^T \equiv I_3 \pmod{2^3}$ resulta $a^2+a'^2+a''^2 \equiv 1 \pmod{2^3}$. Si tenemos la primera columna fijada entonces la primera fila tiene 2^4 posibilidades. Ahora la segunda fila tiene 2^2 posibilidades y la tercera queda ya determinada con 2^3 posibilidades.

Por consiguiente

$$o_{2^3}(f) \leq 3\cdot 2^5\cdot 2^4\cdot 2^2\cdot 2^3 = 3\cdot 2^{14} \quad . \qquad \#$$

Lema 2.14. M(gen f) > 322 .

Demostración. Sabemos que :

$$M(\text{gen } f)^{-1} = 1|2\ \partial_\infty(f,f) \prod_p \partial_p(f,f) \quad ,$$

en donde, sustituyendo $\partial_\infty(f,f)$ por su valor ([41] , Cap. II).

$$\partial_\infty(f,f) = \frac{\pi^{3/2}}{\Gamma(\frac{3}{2})}(\det f)^{-2} = 2\pi^2 \frac{1}{p_1^4 p_2^4 p_3^4} \quad ,$$

se obtiene

$$M(\text{gen } f) = \frac{p_1^4 p_2^4 p_3^4}{\pi^2 \prod_p \partial_p(f,f)}$$

Pasemos pues a evaluar $\partial_p(f,f)$, para todo primo p .

Si $p \neq p_i$, $i = 1,2,3$, $p > 2$, claramente ([41] Hilfssatz 18), es $\partial_p(f,f) = (1-p^{-2}) < 1$.

Si $p = p_i$ para algún i , por el Hilfssatz 18 de [41] tenemos

$$\partial_p(f,f) = 1 \mid 2\ p^{-15} o_{p^5}(f) ,$$

y por el lema 2.12 resulta que

$$\partial_p(f,f) \leq 2p^2 .$$

Si p = 2, entonces por el lema 2.13 tenemos $\partial_2(f,f) \leq 3 \cdot 2^4$. De todo ello resulta

$$M(\text{gen } f) \geq \frac{p_1^2 p_2^2 p_3^2}{\pi^2 \cdot 3 \cdot 2^7}$$

Esta expresión toma su valor mínimo para $p_1 = 5$, $p_2 = 13$, y $p_3 = 17$, o sea $M(\text{gen } f) > 322$. #

Proposición 2.15. En $\text{gen}\langle p_1^2, p_2^2, p_3^2\rangle$ hay por lo menos 645 clases.

Demostración. Como $f = \langle p_1^2, p_2^2, p_3^2\rangle$ es una forma ternaria diagonal con los tres elementos distintos se tiene que $o(f) = 8$. En general, toda forma ternaria definida positiva g, verifica $o(g) \geq 2$, ya que $\pm I_3 \in O(g)$.

Por tanto, para $f = \langle p_1^2, p_2^2, p_3^2\rangle$ se tiene

$$M(\text{gen } f) \leq \frac{1}{8} + \frac{1}{2} + \overbrace{\ldots +}^{h-1} \frac{1}{2} \quad ,$$

siendo h el número de clases pertenecientes al género de f. En consecuencia

$$\frac{1}{8} + \frac{h-1}{2} > 322 \quad \text{y} \quad h \geq 645 \quad . \qquad \#$$

§5. Género espinorial de una forma cuadrática

Eichler (en[14]) introdujo el concepto de género espinorial, que da una clasificación más fina de las clases de formas cuadráticas que la dada por el género anterior.

Sea R un dominio de ideales principales y K su cuerpo de cocientes. Sea (V,ψ) un K-espacio cuadrático regular de dimensión k . Dos R-redes L y M de V, se dice que son equivalentes si

$$L = uM \ ,$$

para algún u de O(V), siendo

$$O(V) = \{u \in GL(V) \mid f(u(x)) = u(x), \text{ para todo } x \text{ de } V\} \ .$$

Si $L = Re_1 \oplus \ldots \oplus Re_k$ es una R-red de V, entonces la fórmula

$$f(x_1,\ldots,x_k) = \psi(x_1e_1+\ldots+x_ke_k),$$

define una forma cuadrática f sobre R^k que toma valores en K. Diferentes elecciones de R-bases de L dan todas las formas que son R-equivalentes a f(cf.§4.Cap II). Fácilmente se demuestra el siguiente

Lema 2.16. (cf.[8] Ch. 11). La correspondencia anteriormente citada da lugar a una biyección entre el conjunto de clases de R-redes de(V,ψ) y el conjunto de R-clases de formas cuadráticas que son K-equivalentes a ψ.

Si dos formas cuadráticas enteras f y g pertenecen a un mismo género, entonces por el teorema de Hasse-Minkowski son $\mathbb{Q}$-equivalentes, y por tanto, les podemos hacer corresponder redes en el mismo $\mathbb{Q}$-espacio cuadrático : $(V,f) \sim (V,g)$.

Se dice que dos $\mathbb{Z}$-redes L y M de V son del mismo *género* si para cada primo p, incluyendo ∞, existe una isometría u_p de $O(V_p)$ tal que

$$L_p = u_p M_p \quad ,$$

siendo $V_p = V \otimes_{\mathbb{Q}} \mathbb{Q}_p$, y

$$O(V_p) = \{u_p \in GL(V_p) \mid f(u_p(x)) = u_p(x), \text{ para todo } x \text{ de } V_p\} .$$

De hecho, dadas dos $\mathbb{Z}$-redes L y M en un mismo espacio cuadrático (V,ψ), entonces

$$L_p = M_p \quad , \text{ para casi todo } p \quad .$$

Obviamente, por el lema 2.16, un género de $\mathbb{Z}$-redes define un género de formas y viceversa.

Un elemento s de $O(V)$ se dice que es una *simetría* si existe un vector x de V tal que $\psi(x) \neq 0$ y

$$s(x) = x ,$$

$$s(z) = -z \text{ , si } z \in \langle x \rangle^{\perp} .$$

En este caso se escribe $s = s_x$. Todo elemento u de $O(V)$ es producto de simetrías

$$u = s_{y_1} \ldots s_{y_t} \text{ , } (t \leq k) .$$

Si, además, $u = s_{z_1} \ldots s_{z_r}$, entonces

$s_{y_1} \ldots s_{y_t} s_{z_r} \ldots s_{z_1} = Id$ y, por tanto (cf. [3] Lema 5.3),

$$\psi(y_1) \ldots \psi(y_t)\psi(z_1) \ldots \psi(z_r) \in (K^*)^2 ,$$

de manera que la aplicación

$$S : O(V) \longrightarrow K^*/(K^*)^2$$

$$u \longmapsto \psi(y_1) \ldots \psi(y_t)(K^*)^2$$

está bien definida. Es fácil ver que se trata de un morfismo de grupos. Su restricción a $O^+(V) = \{u \in O(V) \mid \det u = +1\}$ se llama *norma espinorial*. Se tiene la sucesión exacta

$$1 \longrightarrow O'(V) \longrightarrow O^+(V) \xrightarrow{S} K^*/(K^*)^2 ,$$

siendo $O'(V)$ el núcleo de S .

Para $O'(V)$ se tiene la sucesión exacta

$$1 \longrightarrow \{\pm 1\} \longrightarrow Spin(V) \longrightarrow O'(V) \longrightarrow 1 ,$$

en donde Spin(V) designa el grupo de los espinores (cf. [8] Ch. 10 §3).

Se dice que dos $\mathbb{Z}$-redes L, M de (V,f) pertenecen al mismo *género espinorial* si existe un elemento u de O(V) y un elemento v_p de $O'(V_p)$ para cada p, tal que

$$L_p = u\, v_p\, M_p \quad ,$$

para todo p.

Es consecuencia inmediata de la definición que dos $\mathbb{Z}$-redes equivalentes pertenecen al mismo género espinorial, y que dos redes que pertenezcan al mismo género espinorial pertenecen al mismo género. El número de clases de un espacio cuadrático, en el caso definido positivo, en un género espinorial es, por tanto, finito.

Observación. Dados un entero n y una $\mathbb{Z}$-red L de (V,f), con f una forma cuadrática entera, definida positiva, se designa por r(n,L) :

$$r(n,L) = \#\{x \in L \mid f(x) = n\} \quad ,$$

y por $r^*(n,L)$ el número de representaciones primitivas. Análogamente se definen

$$r(n,\text{gen } L) = \left(\sum_{M \in \text{gen } L} \frac{1}{o(M)}\right)^{-1} \cdot \left(\sum_{M \in \text{gen } L} \frac{r(n,M)}{o(M)}\right) \quad ,$$

$$r^*(n,\text{gen } L) = \left(\sum_{M \in \text{gen } L} \frac{1}{o(M)}\right)^{-1} \cdot \left(\sum_{M \in \text{gen } L} \frac{r^*(n,M)}{o(M)}\right) \quad ,$$

en donde

$$o(M) = \#\, O(M) = \#\left\{u \in O(V) \mid u(M) = M\right\} \quad .$$

Análogamente para el género espinorial se define

$$r(n,\text{spn } L) = \left(\sum_{M \in \text{spn } L} \frac{1}{o(M)}\right)^{-1} \cdot \left(\sum_{M \in \text{spn } L} \frac{r(n,M)}{o(M)}\right) \quad ,$$

$$r^*(n,\text{spn } L) = \left(\sum_{M \in \text{spn } L} \frac{1}{o(M)}\right)^{-1} \cdot \left(\sum_{M \in \text{spn } L} \frac{r^*(n,M)}{o(M)}\right) \quad .$$

Claramente, se tiene que si gen L es el género de $\mathbb{Z}$- redes asociado al género de una forma f, entonces

$$r(n,L) = r(n,f) \quad , \quad r^*(n,L) = r^*(n,f) \quad .$$

$$r(n,\text{gen } L) = r(n,\text{gen } f) \quad , \quad r^*(n,\text{ gen } L) = r^*(n,\text{gen } f) \quad .$$

Los valores promedio obtenidos a partir del género espinorial tienen la ventaja de que aproximan mejor, como veremos, los valores de r(n,f). Sin embargo, su principal inconveniente es que para ellos no se dispone de fórmulas evaluables como las que proporciona el "Hauptsatz" de Siegel. Es por ello que, en nuestro problema, debemos trabajar simultáneamente con los dos conceptos de género.

§6. Término principal en la determinación del 3-nivel de un entero

Para calcular el nivel vamos ahora a aproximarnos a los

valores $g_i(n)$ para $i = 1,2,3$, mediante ciertos valores correspondientes en promedio.

Dado un entero positivo $n \not\equiv 0,4,7 \pmod 8$, representaremos por $\langle a_1^2, a_2^2, a_3^2 \rangle$ una forma cuadrática tal que $a_i \mid n$, $1 \neq a_i$ y a_i sea libre de cuadrados $(i = 1,2,3)$.

Lema 2.17. Sea $\langle a_1^2, a_2^2, a_3^2 \rangle$ una forma cuadrática ; sea $d_{ij} = \text{m.c.d.}(a_i, a_j)$, $1 \leq i < j \leq 3$ y $d_{123} = \text{m.c.d.}(a_1, a_2, a_3)$. Sean también,

$$b_i = d_{ij}^{-1} \, d_{ik}^{-1} \, d_{123} \, a_i \ ,$$

y

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

con $1 \leq i \leq 3$, $1 \leq j, k \leq 3$, $i \neq j \neq k$, $i \neq k$. Se obtiene, evidentemente, que

i) $r(n, \langle a_1^2, a_2^2, a_3^2 \rangle) = r(nd^{-2}, \langle b_1^2, b_2^2, b_3^2 \rangle)$.

ii) $\text{m.c.d.}(b_i, b_j) = \text{m.c.d.}(b_1, b_2, b_3) = 1$ y $1 \leq b_i$, para $i = 1,2,3$. #

El apartado i) nos hace ver que nos podemos aproximar a $r(n, \langle a_1^2, a_2^2, a_3^2 \rangle)$ por $r(n, \text{gen} \langle a_1^2, a_2^2, a_3^2 \rangle)$ ó bien por $r(nd^{-2}, \text{gen } \langle b_1^2, b_2^2, b_3^2 \rangle)$. Por exigencias posteriores (cf. las observaciones que siguen al teorema 5.10) nos aproximaremos a $r(n, \langle a_1^2, a_2^2, a_3^2 \rangle)$ mediante el valor promedio $r(nd^{-2}, \text{gen } \langle b_1^2, b_2^2, b_3^2 \rangle)$.

Obsérvese que si $m.c.d.(a_i,a_j) = m.c.d.(a_1,a_2,a_3) = 1$, entonces $d = 1$ y $b_i = a_i$, para $i = 1,2,3$.

Definimos a continuación las correspondientes sumas auxiliares en promedio.

Sea n un entero positivo $n \not\equiv 0,4,7 (\text{mód } 8)$. Sean

$$S_1(n) := 3 \sum_{1<a|n} - \mu(a)\, r(n, \text{gen } \langle a^2,1,1\rangle) \quad ,$$

$$S_2(n) := 3 \sum_{\substack{a_i|n \\ a_i \neq 1}} \mu(b_1 b_2)\, r(nd^{-2}, \text{ gen } \langle b_1^2, b_2^2, 1\rangle) \quad ,$$

$$S_3(n) := \sum_{\substack{a_i|n \\ a_i \neq 1}} - \mu(b_1 b_2 b_3)\, r(nd^{-2}, \text{ gen } \langle b_1^2, b_2^2, b_3^2\rangle) \quad ,$$

en donde el sumatorio se entenderá extendido a las ternas (b_1,b_2,b_3) que resulten de todas las correspondientes ternas (a_1,a_2,a_3), manteniendo siempre a_1,a_2,a_3 libres de cuadrados.

Nótese que $S_i(1) = 0$, para $i = 1,2,3$.

Definimos a continuación el *término principal* $G_i(n)$, para todo entero $n \not\equiv 0,4,7 (\text{mód } 8)$. El nombre de término principal se justificará en el capítulo V.

$$G_1(n) := \frac{S_3(n)}{r(n,I_3)} \quad ,$$

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

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

En el caso en que n sea libre de cuadrados respecto de sus divisores primos congruentes con 1 módulo 4, teníamos también definidos los valores $g_i^*(n)$. Vamos a aproximarnos mediante los valores correspondientes en promedio.

Definimos a continuación las correspondientes sumas auxiliares en promedio

Caso n impar, $n \not\equiv 7 (\text{mód } 8)$.

$$S_1^*(n) := 3 \sum_{1<a|m} -\mu(a)\ r^*(n, \text{gen } \langle a^2,1,1\rangle) \ ,$$

$$S_2^*(n) := 3 \sum_{\substack{1<a_i|m \\ (a_1,a_2)=1}} \mu(a_1a_2)\ r^*(n, \text{gen } \langle a_1^2,a_2^2,1\rangle) \ ,$$

$$S_3^*(n) := \sum_{\substack{1<a_i|m \\ (a_i,a_j)=1}} -\mu(a_1a_2a_3)\ r^*(n, \text{gen } \langle a_1^2,a_2^2,a_3^2\rangle) \ .$$

Caso n par, $n \not\equiv 0,4 \pmod 8$.

$$S_2^*(n) := 6 \sum_{1<a|m} -\mu(a)\, r^*(n, \text{gen } \langle a^2, 2^2, 1^2 \rangle) \quad ,$$

$$S_3^*(n) := 3 \sum_{\substack{1<a_i|m \\ (a_1,a_2)=1}} \mu(a_1 a_2)\, r^*(n, \text{gen } \langle a_1^2, a_2^2, 2^2 \rangle) \quad .$$

Definimos a continuación el término principal $G_i^*(n)$, en este caso:

Caso n impar, $n \not\equiv 7 \pmod 8$.

$$G_1^*(n) := \frac{S_3^*(n)}{r^*(n, I_3)} \quad ,$$

$$G_2^*(n) := \frac{S_2^*(n) - 2S_3^*(n)}{r^*(n, I_3)} \quad ,$$

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

Caso n par, $n \not\equiv 0,4 \pmod 8$.

$$G_1^*(n) := \frac{S_3^*(n)}{r^*(n, I_3)} \quad ,$$

$$G_2^*(n) := \frac{S_2^*(n) - S_3^*(n)}{r^*(n, I_3)} \quad .$$

Nótese que las funciones $S_i^*(n)$ tienen expresiones diferentes según sea n impar ó par.

CAPITULO III

EXPRESION DEL TERMINO PRINCIPAL MEDIANTE DENSIDADES P-ADICAS

En este capítulo se calculan, en primer lugar, todas las densidades p-ádicas que forman parte del término principal y que no se pueden obtener directamente a partir de los resultados de Siegel. Al sustituir los valores correspondientes en las expresiones $G_i(n)$, $G_i^*(n)$, se obtienen al principio expresiones muy complicadas. No obstante, el conocimiento exacto de estas densidades es lo que nos va a permitir dar una fórmula recurrente para $G_i(n)$ y una fórmula exacta para $G_i^*(n)$, aptas para el control del término principal.

§1. Cálculo de $r(n,I_3)$ mediante densidades p-ádicas

Aplicamos en primer lugar el teorema de Siegel, para la reobtención del valor clásico del número de representaciones de un entero n como suma de tres cuadrados.

Teorema 3.1. Si n es un entero positivo, tal que $4^a \mid n$ y $4^{a+1} \nmid n$, con $a \geq 0$ y si $p > 2$ es un entero primo tal que

$p^{2b} \mid n$ y $p^{2b+2} \nmid n$, con $b \geq 1$, resulta

$$r(n,I_3) = \frac{A(n)}{\pi}\, n^{1/2}\, L(1,\chi_{-4n}) \prod_{\substack{p^2 \mid n \\ p \neq 2}} \left(1+\frac{1}{p}+\ldots+\frac{1}{p^b}\,\kappa_p(n,b)\right),$$

con

$$A(n) = \begin{cases} 0 & \text{si } 4^{-a}n \equiv 7 (\text{mód } 8) \\ 2^{-a}.16 & \text{si } 4^{-a}n \equiv 3 (\text{mód } 8) \\ 2^{-a}.24 & \text{si } 4^{-a}n \equiv 1,2,5,6 (\text{mód } 8) \end{cases},$$

siendo $\kappa_p(n,b) := \left(1 - \left(\frac{-p^{-2b}n}{p}\right)\frac{1}{p}\right)^{-1}$.

<u>Demostración.</u> Sea n un entero positivo impar. Por el teorema de Siegel se tiene

$$r(n,I_3) = \partial_\infty\, \partial_2 \prod_{p \neq 2} \partial_p \quad ,$$

en donde ∂_p designa $\partial_p(n,I_3)$.

Procedemos, pues, al cálculo de las densidades :

$\partial_\infty = 2\pi n^{1/2}$.

$\partial_2 = 2^{-6}\, r_{2^3}(n,I_3)$. Por tanto, si $n \equiv 1,5 (\text{mód } 8)$, es $\partial_2 = 3/2$; si $n \equiv 3 (\text{mód } 8)$, entonces $\partial_2 = 1$ y si $n \equiv 7 (\text{mód } 8)$, se tiene $\partial_2 = 0$.

Si $p \neq 2$ y $p \nmid n$ resulta por el lema 2.11 que

$\partial_p(n,I_3) = (1-p^{-2})\left(1-\left(\frac{-n}{p}\right)p^{-1}\right)^{-1}$.

Si $p \neq 2$ y $p \mid n$, supongamos b como en el enunciado; entonces, por el lema 2.11 se tiene que

$$\partial_p(n,I_3) = (1-p^{-2})\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^b}\kappa_p(n,b)\right) \quad .$$

Si escribimos $\kappa_p = \kappa_p(n,0)$, se tiene :

$$r(n,I_3) = 2\pi n^{1/2}\,\partial_2 \prod_{\substack{p\nmid n\\ p\neq 2}}(1-p^{-2}) \prod_{\substack{p\nmid n\\ p\neq 2}}\kappa_p \quad .$$

$$\cdot \prod_{p\mid n}\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^b}\kappa_p(n,b)\right) \quad .$$

La prueba en el caso n impar concluye al tener presente que $\zeta(2)^{-1} = \prod_p(1-p^{-2})$, y observando que

$$\prod_{\substack{p\nmid n\\ p\neq 2}}\kappa_p = \prod_{\substack{p\nmid n\\ p\neq 2}}\frac{1}{(1-(\frac{-n}{p})p^{-1})} = \sum_{k\ \text{impar}}\frac{(\frac{-n}{k})}{k} =$$

$$= \sum_k \frac{(\frac{-4n}{k})}{k} = L(1,\chi_{-4n}) \quad ,$$

en donde $L(1,\chi_{-4n})$ designa la L-serie de carácter χ_{-4n} .

Si n es par consideraremos dos casos :

<u>1er caso.</u> Sea n un entero positivo par no divisible por 4 . Entonces en el cálculo de $r(n,I_3)$ la única diferencia con el caso impar es el cálculo de $\partial_2(n,I_3)$, que según el lema 2.11 es

$$\partial_2(n,I_3) = 2^{-10}\, r_{2^5}(n,I_3) \quad .$$

Esto obliga a contar número de soluciones módulo 32,pero

se puede reducir este cálculo mediante la siguiente

Proposición 3.2. Sea n un entero positivo par no divisible por 4. Entonces si $k \geq 3$, resulta que

$$r_{2^{k+1}}(n,I_3) = 2^2\, r_{2^k}(n,I_3) \ .$$

Demostración. El núcleo de la proyección $\mathbb{Z}/(2^{k+1}) \longrightarrow \mathbb{Z}/(2^k)$, consta de dos elementos, por tanto cada elemento, $x + \mathbb{Z}\,2^k$, de $\mathbb{Z}/(2^k)$ posee exactamente dos antiimágenes : $x + \mathbb{Z}\,2^{k+1}$ y $x + 2^k + \mathbb{Z}\,2^{k+1}$.

Recordemos que como $2|n$ y $4\nmid n$ toda representación de n como suma de tres cuadrados posee una única componente par.

Sea (x_o,y_o,z_o) una representación de n como suma de tres cuadrados módulo 2^k , es decir $x_o^2 + y_o^2 + z_o^2 \equiv n(\text{mód } 2^k)$. Entonces, tanto x_o,y_o,z_o, como n tienen dos antiimágenes en $\mathbb{Z}/(2^{k+1})$. Por tanto si vemos que $r_{2^{k+1}}(n,I_3) = r_{2^{k+1}}(n+2^k,I_3)$, tendremos que $r_{2^{k+1}}(n,I_3) = \frac{2^3}{2}\, r_{2^k}(n,I_3) = 2^2 r_{2^k}(n,I_3)$, que es lo que queremos probar.

Sea (x_1,y_1,z_1) tal que $x_1^2 + y_1^2 + z_1^2 \equiv n(\text{mód } 2^{k+1})$. Entonces le asociamos una solución de $X^2+Y^2+Z^2 \equiv n+2^k(\text{mód } 2^{k+1})$ del siguiente modo : como dos componentes de (x_1,y_1,z_1) son impares, supongamos que son x_1,y_1 , entonces a (x_1,y_1,z_1) le hacemos corresponder (x_1+2^{k-1},y_1,z_1) que evidentemente verifica

$$(x_1+2^{k-1})^2+y_1^2+z_1^2 = x_1^2+y_1^2+z_1^2+2^k x_1+2^{k-2} \equiv n+2^k (\text{mód } 2^{k+1}) \quad ,$$

ya que $k \geq 3$ y x_1 es un entero impar. Esta correspondencia es inyectiva y su inversa es aquella que a (x_1,y_1,z_1), solución de $X^2+Y^2+Z^2 \equiv n+2^k (\text{mód } 2^{k+1})$, le asocia, si x_1 es la primera componente impar, (x_1-2^{k-1},y_1,z_1) que es solución de $X^2+Y^2+Z^2 \equiv n (\text{mód } 2^{k+1})$. #

Basta aplicar el resultado del lema precedente para obtener el siguiente

Corolario 3.3. Si $n \equiv 2,6 (\text{mód } 8)$, entonces $\partial_2(n,I_3) = 3/2$.

2º caso. Sea ahora n divisible por 4 y llamemos a al máximo exponente tal que $4^a | n$. Entonces, se tiene

$$r(n,I_3) = r(4^{-b}n,I_3) \ ,$$

para todo $b \leq a$.

Por tanto si consideramos $4^{-a}n$, este entero ya ó es impar ó, si es par, no es divisible por 4 y resulta que

$$r(n,I_3) = r(4^{-a}n,I_3) = r(n(2^a)^{-2},n)$$

$$= \frac{2\pi n^{1/2}}{2^a} \partial_2(4^{-a}n,I_3) L(1,\chi_{-4n}) \prod_{p^2|n} (1+\frac{1}{p}+\ldots+\frac{1}{p^b}\kappa_p(n,b)),$$

ya que $L(1,\chi_{-4.4^{-a}n}) = L(1,\chi_{-4n})$ y al ser p un primo impar que divide a n con exponente ≥ 2, lo mismo ocurre al considerarlo como divisor de $4^{-a}n$.

Por tanto, queda probado el teorema. #

Pasamos a continuación a dar el número de representaciones primitivas de un entero cualquiera como suma de tres cuadrados.

§2. Cálculo de $r^*(n,I_3)$

Teorema 3.4. $r^*(n,I_3) = \frac{A(n)}{\pi}\, n^{1/2}\, L(1,\chi_{-4n})$,

con $$A(n) = \begin{cases} 0 & \text{si } n \equiv 0,4,7 \pmod 8, \\ 16 & \text{si } n \equiv 3 \pmod 8, \\ 24 & \text{si } n \equiv 1,2,5,6 \pmod 8. \end{cases}$$

Demostración. Sea n un entero positivo tal que $n \not\equiv 0,4 \pmod 8$. Expresamos n en la forma:

$n = 2^{\alpha}\, p_1^{\alpha_1} \cdots p_s^{\alpha_s}\, p_{s+1} \cdots p_t$, con $0 \le \alpha \le 1$, $\alpha_i \ge 2$ y representando por $p_j (j = 1,\ldots,t)$ todos los factores primos impares de n.

Recordemos (cf. §4. Cáp. II) que

$$r^*(n,I_3) = \sum_{d^2 \mid n} \mu(d)\, r(nd^{-2},I_3)$$

$$= r(n,I_3) - \sum_{i=1}^{s} r(np_i^{-2},I_3) + \sum_{1 \le i < j \le s} r(np_i^{-2}p_j^{-2},I_3)$$

$$+ \ldots + (-1)^s\, r(np_1^{-2} \cdots p_s^{-2},I_3).$$

En donde, si $d = p_1 \ldots p_\ell$ con $0 \leq \ell \leq s$, se tiene que

$$r(nd^{-2}, I_3) = 2\pi n^{1/2}\, d^{-1}\, \partial_2(nd^{-2}, I_3)\, L(1, \chi_{-4nd^{-2}})$$
$$\prod_{p^2 \mid nd^{-2}} \left(1 + \frac{1}{p} + \ldots + \frac{1}{p^b}\, \kappa_p(n,b)\right).$$

Obviamente, tanto si $\alpha = 0$ como si $\alpha = 1$, resulta que

$$\partial_2(nd^{-2}, I_3) = \partial_2(n, I_3),$$

para todo $d^2 \mid n$.

Puesto que (cf. [24] 12.11)

$$L(1, \chi_{-4np^{-2}}) = L(1, \chi_{-4n}) \left(1 - \left(\frac{-p^{-2}n}{p}\right) \frac{1}{p}\right)^{-1}$$

$$L(1, \chi_{-4n(p_1 \ldots p_\ell)^{-2}}) = L(1, \chi_{-4n}) \prod_{i=1}^{\ell} \left(1 - \left(\frac{-p_i^{-2}n}{p}\right)\frac{1}{p_i}\right)^{-1},$$

resulta,

$$r^*(n, I_3) = 2\pi n^{1/2}\, \partial_2(n, I_3)\, L(1, \chi_{-4n})\, A,$$

en donde,

$$A = \prod_{i=1}^{s} \left(1 + \frac{1}{p_i} + \ldots + \frac{1}{p_i^{b_i}}\, \kappa_{p_i}(n, b_i)\right)$$

$$-\sum_{i=1}^{s} \frac{1}{p_i}\, \kappa_{p_i}(n,1)\left(1 + \frac{1}{p_i} + \ldots + \frac{1}{p_i^{b_i - 1}}\, \kappa_{p_i}(n, b_i) \prod_{j \neq 1} \left(1 + \frac{1}{p_j} + \ldots + \frac{1}{p_j^{b_j}}\, \kappa_{p_j}(n, b_j)\right)\right.$$

$$+ \ldots + (-1)^s \prod_{i=1}^{s} \frac{1}{p_i}\, \kappa_{p_i}(n,1)\left(1 + \frac{1}{p_i} + \ldots + \frac{1}{p_i^{b_i - 1}}\, \kappa_{p_i}(n, b_i)\right).$$

Lema 3.5. $A = 1$.

Demostración. Pongamos

$$X_i = 1 + \frac{1}{p_i} + \ldots + \frac{1}{p_i^{b_i}} \kappa_{p_i}(n,b_i); \quad B_i = \frac{1}{p_i}\left(1 + \frac{1}{p_i} + \ldots + \frac{1}{p_i^{b_i}} \kappa_{p_i}(n,b_i)\right).$$

$$Y_i = \kappa_{p_i}(n,1)\, B_i, \text{ para } i = 1,\ldots,s.$$

Entonces la expresión A se puede escribir en la forma

$$\prod_{i=1}^{s} X_i - \sum_{i=1}^{s} Y_i \prod_{j\neq i} X_i + \sum_{1\leq i<j\leq s} Y_i Y_j \prod_{k\neq i,j} X_k + \ldots + (-1)^s \prod_{i=1}^{s} Y_i$$

$$= \prod_{i=1}^{s} (X_i - Y_i).$$

Ahora bien, resulta que

$$B_i = \begin{cases} 1/p_i & \text{si } b_i = 1, \\ X_i - 1 & \text{si } b_i > 1, \end{cases}$$

y como $Y_i = \kappa_{p_i}(n,1)B_i$, para $i = 1,\ldots,s$, se tiene que $Y_i = X_i - 1$, para cualquier valor de b_i. Por tanto $X_i - Y_i = 1$, para $i = 1,\ldots,s$ con lo que queda probado que $A = 1$. Y por consiguiente el teorema está probado si $n \not\equiv 0,4 (\text{mód } 8)$.

Sea ahora $n \equiv 0,4 (\text{mód } 8)$. Recordemos que $r(n,I_3) = r(4^{-1}n,I_3)$. Por tanto, si escribimos

$$n = 4^{\alpha} p_1^{\alpha_1} \cdots p_s^{\alpha_s} p_{s+1} \cdots p_t$$

con $\alpha \geq 1$, $\alpha_i \geq 2$, $i = 1,\ldots,s$, y representando por p_j, para $j = 1,\ldots, t$, todos los factores primos impares de n, resulta que

$$r^*(n,I_3) = r(n,I_3) - r(4^{-1}n,I_3) - \sum_{i=1}^{s} r(np_i^{-2},I_3)$$
$$+ \sum_{i=1}^{s} r(4^{-1}n\, p_i^{-2},I_3) + \sum_{1\leq i<j\leq s} r(np_i^{-2}p_j^{-2},I_3)$$
$$+ \ldots + (-1)^s\, r(4^{-1}n\, p_1^{-2}\ldots p_s^{-2},I_3) = 0.$$

Por tanto, queda ya probado el teorema. #

§3. Cálculo de $r(n\ ,\ \text{gen} < b_1^2,\ b_2^2,\ b_3^2 >)$ en el caso n impar

Sea $n \not\equiv 7 (\text{mód } 8)$ un entero impar, en este párrafo vamos a proceder al cálculo de $r(n,\ \text{gen} < b_1^2,\ b_2^2,\ b_3^2 >)$ con las condiciones $b_i \mid n$, $i=1,2,3$; $(b_i,b_j) = 1$, $i \neq j$.
Este cálculo, junto con el de los párrafos anteriores, es necesario para el estudio de las expresiones $G_i(n)$.

Por el Hauptsatz de Siegel tenemos,

$$r(n,\text{gen } f) = \partial_\infty \cdot \partial_2 \cdot \prod_{\substack{p\nmid b_1b_2b_3 \\ p\nmid n \\ p\neq 2}} \partial_p \cdot \prod_{\substack{p\nmid b_1b_2b_3 \\ p\mid n \\ p\neq 2}} \partial_p \cdot \prod_{p\mid b_1b_2b_3} \partial_p,$$

siendo $f = \langle b_1^2, b_2^2, b_3^2\rangle$ y $\partial_p = \partial_p(n,f)$.

Basta aplicar los lemas 2.10 y 2.11 para obtener la siguiente

Proposición 3.6. Se tiene que

i) $\partial_\infty(n,f) = \dfrac{n^{1/2}\,\pi^{3/2}}{b_1 b_2 b_3\,\Gamma(3/2)}$.

ii) Si $p \nmid b_1 b_2 b_3$, $p \nmid n$ y $p \neq 2$

$$\partial_p(n,f) = (1-p^{-2})\,\kappa_p .$$

iii) Si $p \nmid b_1 b_2 b_3$, $p \mid n$ y $p \neq 2$ entonces $\partial_p(n,f) = (1 - p^{-2}) \cdot (1 + \frac{1}{p} + \ldots + \frac{1}{p^b}\,\kappa_p(n,b))$, en donde $p^{2b} \mid n$ y $p^{2b+2} \nmid n$.

Si $p \mid b_1$, como m.c.d. (det f,p) = p, resulta que no se pueden aplicar las fórmulas de Siegel. Pasamos a continuación a calcular las densidades correspondientes en este caso.

Se indica por $v_p(n)$ la valoración de n en p.

Lema 3.7. Para todo $t \geq 1$ se verifica

$$\#\{x \ (\text{mód } p^t) \mid v_p(x) = i\} = \varphi(p^{t-i}),$$

en donde φ designa el indicador de Euler.

Demostración. Basta observar que el conjunto

$$\{x(\text{mód } p^t) \mid v_p(x) = i\},$$

es la imágen de los unitarios de $\mathbb{Z}/_{p^{t-i}\mathbb{Z}}$ mediante el monomorfismo de grupos:

$$\mathbb{Z}/_{p^{t-i}\mathbb{Z}} \xrightarrow{\cdot p^i} \mathbb{Z}/_{p^t\mathbb{Z}} \quad . \qquad \#$$

Proposición 3.8.

i) Si $p \equiv 1(\text{mód } 4)$, y $p \mid b_1$ con $v_p(n) = 2\alpha + 1$, $\alpha \geq 0$, resulta que

$$\partial_p(n, \langle b_1^2, b_2^2, b_3^2 \rangle) = p^{-(\alpha+1)} \, (3p^{\alpha+1} - p^{\alpha} - p - 1).$$

ii) Si $p \equiv 3(\text{mód } 4)$, $p \mid b_1$ y $v_p(n) = 2\alpha + 1$, $\alpha \geq 0$, entonces

$$\partial_p(n, \langle b_1^2, b_2^2, b_3^2 \rangle) = p^{-(\alpha+1)} (p+1)(p^{\alpha} - 1).$$

Demostración.

i) Recordemos (cf. lema 2.9) que en este caso es:

$$\partial_p(n, \langle b_1^2, b_2^2, b_3^2 \rangle) = p^{-2(4\alpha+3)} \, r_{p^{4\alpha+3}}(n, \langle b_1^2, b_2^2, b_3^2 \rangle).$$

Luego se ha de calcular:

$$r_{p^{4\alpha+3}}(n, \langle b_1^2, b_2^2, b_3^2 \rangle) = \sum_{x_1 (\text{mód } p^{4\alpha+3})} r_{p^{4\alpha+3}}(n - b_1^2 x_1^2, \langle b_2^2, b_3^2 \rangle).$$

Basta, pues, distinguir qué ocurre para cada valor de $x_1(\text{mód } p^{4\alpha+3})$, según sea $v_p(x_1)$.

Si $v_p(x_1) = i$, con $0 \leq i \leq \alpha - 1$, entonces $v_p(n-b_1^2x_1^2) = 2(i+1)$, y por el lema 2.11 resulta que al ser $p \equiv 1 (\text{mód } 4)$ se tiene

$$r_{p^{4\alpha+3}}(n-b_1^2x_1^2, <b_2^2,b_3^2>) = (2(i+1)+1)\ (1-p^{-1})\ p^{4\alpha+3}.$$

Si $v_p(x_1) = i$, con $i \geq \alpha$ entonces $v_p(n-b_1^2x_1^2) = 2\alpha+1$, y es pues,

$$r_{p^{4\alpha+3}}(n-b_1^2x_1^2, <b_2^2,b_3^2>) = (2\alpha+2)(1-p^{-1})\ p^{4\alpha+3}.$$

Por tanto, teniendo en cuenta el lema 3.7 , el valor de $\partial_p(n, <b_1^2,b_2^2,b_3^2>)$ es:

$$p^{-4\alpha+3}(1-p^{-1})\ (3\varphi(p^{4\alpha+3}) + 5\ \varphi(p^{4\alpha+2}) + \ldots$$

$$\ldots + (2\alpha+1)\ \varphi(p^{3\alpha+4}) + (2\alpha+2)\ p^{3\alpha+3})$$

$$= p^{-(4\alpha+4)}(p-1)(3p^{4\alpha+3} + 2p^{4\alpha+2} + 2p^{4\alpha+1} + \ldots + 2p^{3\alpha+4} + 2p^{3\alpha+3})$$

$$= p^{-(\alpha+1)}(p-1)\ (3p^{\alpha} + 2p^{\alpha-1} + \ldots + 2p + 1).$$

Teniendo en cuenta que

$$2p^{\alpha-1} + \ldots + 2p = \frac{2(p^{\alpha} - p)}{p - 1},$$

resulta que, si $p \equiv 1 (\text{mód } 4)$, entonces

$$\partial_p(n, <b_1^2,b_2^2,b_3^2>) = p^{-(\alpha+1)}(3p^{\alpha+1} - p^{\alpha} - p - 1).$$

ii) Si $p \equiv 3 (\text{mód } 4)$ y $v_p(n) = 2\alpha + 1$, con $\alpha \geq 0$, procediendo igual que en apartado i), resulta que si $v_p(x_1) = i$, con $0 \leq i \leq \alpha - 1$, entonces $v_p(n-b_1^2x_1^2) = 2(i + 1)$ y por el lema 2.11 se obtiene que

$$r_{p^{4\alpha+3}}(n-b_1^2.x_1^2,<b_2^2,b_3^2>) = (1 + p^{-1})\ p^{4\alpha+3}.$$

Si $v_p(x_1) = i$, con $i \geq \alpha$, entonces $v_p(n-b_1^2x_1^2) = 2\alpha+1$, y es pues:

$$r_{p^{4\alpha+3}}(n-b_1^2.x_1^2,<b_2^2,b_3^2>) = 0.$$

Por tanto, si $p \equiv 3(\text{mód } 4)$, teniendo en cuenta el lema 3.7 , resulta que

$$\partial_p(n,<b_1^2,b_2^2,b_3^2>) = p^{-(4\alpha+3)}(1+p^{-1})(\varphi(p^{4\alpha+3}) + \varphi(p^{4\alpha+2}) + \ldots$$

$$\ldots + \varphi(p^{3\alpha+4}))$$

$$= p^{-(\alpha+1)}(p+1)(p^{\alpha}-1). \qquad \#$$

Los resultados anteriores permiten enunciar el siguiente

<u>Teorema 3.9.</u> Sea n un entero positivo *libre de cuadrados* respecto de sus divisores primos congruentes con 1 módulo 4. Entonces

$$r^*(n,\text{gen } <b_1^2,b_2^2,b_3^2>) = \frac{A(n)}{\pi}\ n^{1/2}\ L(1,\chi_{-4n}) \prod_{p \mid b_1b_2b_3} 2(1+p)^{-1},$$

siendo $(b_i,b_j)=1$, para $i \neq j$; y tomando A(n) los mismos valores que en el teorema 3.1.

Demostración. Recordemos que

$$r^*(n,\text{gen } \langle b_1^2,b_2^2,b_3^2\rangle) = \sum_{d^2|n} \mu(d)\, r(nd^{-2},\text{gen } \langle b_1^2,b_2^2,b_3^2\rangle).$$

Si escribimos $n = p_1 \dots p_r \prod_{j=1}^{s} q_j^{\beta_j}$, entonces

$$r^*(n,\text{gen } \langle b_1^2,b_2^2,b_3^2\rangle) = r(n,\text{gen } f) - \sum_{i=1}^{s} r(nq_i^{-2},\text{gen } f) +$$

$$+ \sum_{1\le i<j\le s} r(nq_i^{-2}q_j^{-2},\text{gen } f) - \sum_{1\le i<j<k\le s} r(nq_i^{-2}q_j^{-2}q_k^{-2},\text{gen } f) +$$

$$+ \dots + (-1)^s\, r(nq_1^{-2}\dots q_s^{-2},\text{gen } f).$$

En donde, si $Q = \prod_{j=i}^{t} q_j$, $t \le s$, resulta, sustituyendo por los valores de las densidades p-ádicas anteriormente obtenidos, que

$$r(nQ^{-2},\text{gen } f) = \frac{2\pi n^{1/2}}{b_1b_2b_3}\, \partial_2 \prod_{p|b_1b_2b_3} 2(1-p^{-1}) \prod_{\substack{p\nmid b_1b_2b_3\\ p|nQ^{-2}\\ p\equiv 1(4)}} (1-p^{-2})$$

$$\cdot \prod_{p\nmid nQ^{-2}} (1-p^{-2})\, \kappa_p(nQ^{-2},0).\{Q^{-1} \prod_{\substack{p\nmid b_1b_2b_3\\ p|nQ^{-2}\\ p\equiv 3(4)}} (1-p^{-2})(1+\frac{1}{p}+\dots+\frac{1}{p^b}\kappa_p(nQ^{-2},b))\},$$

en donde,

$$p^{2b}|nQ^{-2},\ p^{2b+2}\nmid nQ^{-2} \text{ y } \kappa_p(nQ^{-2},b) = \{1-(\frac{-p^{-2b}nQ^{-2}}{p})\frac{1}{p}\}^{-1}.$$

Observemos que,

$$\prod_{p \nmid nQ^{-2}} (1-p^{-2})\, \kappa_p(nQ^{-2},0) = \prod_{p \nmid n} (1-p^{-2}) \left\{1-\left(\frac{-nQ^{-2}}{p}\right)\frac{1}{p}\right\}^{-1}$$

Además, como el símbolo de Legendre es una función completamente multiplicativa:

$$\left(\frac{-n}{p}\right) = \left(\frac{-nQ^{-2}}{p}\right).$$

Teniendo en cuenta estos hechos, el lema 3.5, y procediendo igual que en el teorema 3.1, se obtiene el resultado enunciado. #

El caso en que $v_p(n) = 2\alpha$, $p \neq 2$, es más complicado. Por ello distinguiremos según sea $\left(\frac{p^{-2\alpha}n}{p}\right) = -1$ ó $\left(\frac{p^{-2\alpha}n}{p}\right) = 1$.

<u>Proposición 3.10.</u> Si $v_p(n) = 2\alpha$, $\alpha \geq 1$, $\left(\frac{p^{-2\alpha}n}{p}\right) = -1$ y $p \mid b_1$, resulta que

i) $\partial_p(n, \langle b_1^2, b_2^2, b_3^2\rangle) = p^{-\alpha}(3p^{\alpha} - p^{\alpha-1} - 2)$, si $p \equiv 1 \pmod 4$,

ii) $\partial_p(n, \langle b_1^2, b_2^2, b_3^2\rangle) = (1+p^{-1})$, si $p \equiv 3 \pmod 4$.

<u>Demostración</u>.

i) Recordemos (cf. lema 2.9) que

$$\partial_p(n, \langle b_1^2, b_2^2, b_3^2\rangle) = p^{-2(4\alpha+1)} r_{p^{4\alpha+1}}(n, \langle b_1^2, b_2^2, b_3^2\rangle).$$

Como en los casos anteriores vamos a contar el número de soluciones de

$$b_2^2 X_2^2 + b_3^2 X_3^2 \equiv n - b_1^2 X_1^2 \pmod{p^{4\alpha+1}},$$

para cada uno de los diferentes valores x_1 de X_1, distinguiendo según sea su valoración en p.

Si $v_p(x_1) = i$, con $0 \leq i \leq \alpha - 2$, entonces como $(\frac{-p^{-2\alpha}n}{p}) = -1$, se tiene que $v_p(n-b_1^2x_1^2) = 2(i+1)$, y es pues, al ser $p \equiv 1 \pmod 4$, (cf. lema 2.11)

$$r_{p^{4\alpha+1}}(n-b_1^2x_1^2, <b_2^2, b_3^2>) = (2(i+1)+1)(1-p^{-1})\ p^{4\alpha+1}.$$

Si $v_p(x_1) = i$, con $i \geq \alpha-1$, como $(\frac{p^{-2\alpha}n}{p}) = -1$, es

$v_p(n-b_1^2x_1^2) = 2\alpha$, y

$$r_{p^{4\alpha+1}}(n-b_1^2x_1^2, <b_2^2, b_3^2>) = (2\alpha+1)(1-p^{-1})\ p^{4\alpha+1}.$$

Por tanto, teniendo en cuenta el lema 3.7 , resulta que el valor de $\partial_p(n, <b_1^2, b_2^2, b_3^2>)$, en este caso es,

$$p^{-(4\alpha+1)}(1-p^{-1})(3\varphi(p^{4\alpha+1}) + 5\varphi(p^{4\alpha}) + \ldots$$

$$\ldots + (2\alpha-1)\,\varphi(p^{3\alpha+3}) + (2\alpha+1)\ p^{3\alpha+2})$$

$$= p^{-(4\alpha+2)}(p-1)\ (3p^{4\alpha+1} + 2p^{4\alpha} + 2p^{4\alpha-1} + \ldots + 2p^{3\alpha+3} + 2p^{3\alpha+2})$$

$$= p^{-\alpha}(3p^{\alpha} - p^{\alpha-1} - 2).$$

ii) Si $p \equiv 3 \pmod 4$, basta observar que para cualquier valor de $v_p(x_1)$, el valor correspondiente de $v_p(n-b_1^2x_1^2)$ es un ente-

ro par y,por tanto, para cualquier valor de $x_1 (\text{mód } p^{4\alpha+1})$ se tiene, al ser $p \equiv 3 (\text{mód } 4)$, (cf. lema 2.11)

$$r_{p^{4\alpha+1}}(n-b_1^2x_1^2, <b_2^2,b_3^2>) = (1+p^{-1})\, p^{4\alpha+1}.$$

Por consiguiente, en este caso

$$\partial_p(n,<b_1^2,b_2^2,b_3^2>) = (1+p^{-1}). \qquad \#$$

Observación. Si $p|b_1$ y $p\nmid b_2$, $p\nmid b_3$, entonces está claro que b_2 y b_3 son invertibles módulo p^t, para todo $t \geq 1$. Si escribimos $b_1 = b_1' p$, también b_1' es invertible módulo p^t. Por tanto,

$$r_{p^t}(n, <b_1^2,b_2^2,b_3^2>) = r_{p^t}(n, <p^2,1,1>);$$

de ahora en adelante lo escribiremos con esta última notación.

En el caso en que $(\frac{p^{-2\alpha}n}{p}) = 1$ y $v_p(n) = 2\alpha$, $\alpha \geq 1$, la valoración p-ádica de $p^{-2\alpha}(n-b_1^2x_1^2)$ puede no coincidir siempre con cero, si $v_p(x_1) = \alpha-1$. Determinamos a continuación el valor de $\partial_p(n, <p^2,1,1>)$, $p \neq 2$, en este caso.

Lema 3.11. Sea $\alpha \geq 1$. Entonces el valor de $r_{p^{4\alpha+1}}(0, <1,1>)$ es:

i) $p^{4\alpha}$, si $p \equiv 3 (\text{mód } 4)$,

ii) $\dfrac{2(p^{4\alpha+2}-1) + p^{4\alpha}(p+1)}{p+1}$, si $p \equiv 1 (\text{mód } 4)$.

Demostración.

i) Si $p \equiv 3 (\text{mód } 4)$ e (y,z) una solución de

$$Y^2 + Z^2 \equiv 0 (\text{mód } p^{4\alpha+1}),$$

como $(\frac{-1}{p}) = -1$, resulta que $v_p(y) \geq 2\alpha+1$, $v_p(z) \geq 2\alpha+1$. Por tanto, hay $p^{2\alpha}$ posibilidades para Y y otras tantas para Z, así que el número total de soluciones es $p^{4\alpha}$.

ii) Si $p \equiv 1 (\text{mód } 4)$, además de las $p^{4\alpha}$ soluciones citadas en el apartado i), existen otras:

Si z es tal que $v_p(z) = i < \frac{4\alpha+1}{2}$, entonces cualquier solución y de

$$Y^2 + z^2 \equiv 0 (\text{mód } p^{4\alpha+1}),$$

verifica $v_p(y) = v_p(z)$. En efecto, de $y^2+z^2 \equiv 0 (\text{mód } p^{4\alpha+1})$ se obtiene $y^2 \equiv 0 (\text{mód } p^{2i})$ por ser $i < \frac{4\alpha+1}{2}$, o sea $v_p(y) \geq i$, y por simetría $v_p(y) = v_p(z)$.

De ésto último se deduce, dividiendo por p^{2i}, que el número de soluciones (y,z) de

$$Y^2 + Z^2 \equiv 0 (\text{mód } p^{4\alpha+1}),$$

con $v_p(z) = i < \frac{4\alpha+1}{2}$, coincide con el de soluciones (y,z), con $v_p(z) = 0$, de

$$Y^2 + Z^2 \equiv 0 (\text{mód } p^{4\alpha+1-2i}).$$

Esta última ecuación equivale a

$$(\frac{1}{z} Y)^2 \equiv -1 (\text{mód } p^{4\alpha+1-2i}),$$

que tiene dos soluciones por ser $p \equiv 1 (\text{mód } 4)$, (cf. [24] §3.5.). Por tanto, hay

$$2\,\varphi(p^{4\alpha+1-2i})$$

soluciones (y,z) de $Y^2+Z^2 \equiv 0 (\text{mód } p^{4\alpha+1})$ con la condición $v_p(z) = i < \frac{4\alpha+1}{2}$.

Resumiendo, si $p \equiv 1 (\text{mód } 4)$, el valor de $r_{p^{4\alpha+1}}(0,<1,1>)$ es:

$$p^{4\alpha} + 2(\varphi(p^{4\alpha+1}) + \varphi(p^{4\alpha-1}) + \varphi(p^{4\alpha-3}) + \ldots + \varphi(p))$$

$$= \frac{2(p^{4\alpha+2}-1) + p^{4\alpha}(p+1)}{p+1} . \quad \#$$

Si $(\frac{p^{-2\alpha}n}{p}) = 1$, entonces (cf. [24] §3.5), resulta que $p^{-2\alpha}n$ es un cuadrado módulo p^t, para $t \geq 1$:

$$p^{-2\alpha}n \equiv a^2 (\text{mód } p^t).$$

Pasemos ahora al cálculo de $v_p(a^2-x^2)$ módulo p^t, $t \geq 1$, $p \neq 2$.

Lema 3.12. Si $p \nmid a$ se verifica:

i) El número de elementos x, módulo p^t, $p \neq 2$, con $v_p(a^2-x^2)=i$, $1 \leq i \leq t$, es $2\varphi(p^{t-i})$.

ii) El número de elementos x, módulo p^t, $p \neq 2$, con $v_p(a^2-x^2)=0$ es $p^t - 2p^{t-1}$.

Demostración.

i) Observemos en primer lugar que si $v_p(a-x)>0$ entonces $v_p(a+x)=0$ y viceversa. En efecto, si $v_p(a-x)= k>0$, y

$v_p(a+x) = h>0$, tenemos para ciertos λ, μ.

$$\mu p^k = a-x = -(a+x) + 2a = -\lambda p^h + 2a,$$

de donde $2a \equiv 0 (\text{mód } p)$, lo cual es absurdo.

Por tanto,

$$\{x(\text{mód } p^t) \mid v_p(a^2-x^2)=i\} = \{x(\text{mód } p^t) \mid v_p(a-x)=i\} \cup \{x(\text{mód } p^t) \mid v_p(a+x)=i\}.$$

Así que, por el lema 3.7 , el número de elementos distintos $x(\text{mód } p^t)$ con $v_p(a^2-x^2)=i$, $1 \leq i \leq t$, es $2\varphi(p^{t-i})$.

ii) Por paso al complementario tenemos que el número de elementos $x(\text{mód } p^t)$ tales que $v_p(a^2-x^2)=0$ es:

$$p^t - 2\sum_{i=1}^{t} \varphi(p^{t-i}) = p^t - 2p^{t-1}. \quad \#$$

<u>Teorema 3.13.</u> Sea $v_p(n) = 2\alpha$, $\alpha \geq 1$ y $\left(\frac{p^{-2\alpha}n}{p}\right) = 1$. Se verifica:

i) Si $p \equiv 3 (\text{mód } 4)$, entonces

$$r_{p^{4\alpha+1}}(n, \langle p^2,1,1\rangle) = p^{7\alpha+2}(p^\alpha + p^{\alpha-1} - 2).$$

ii) Si $p \equiv 1 (\text{mód } 4)$, entonces el valor de $r_{p^{4\alpha+1}}(n, \langle p^2,1,1\rangle)$ es:

$$(p+1)^{-1} p^{\alpha+1}(3p^{7\alpha+2} + 2p^{7\alpha+1} - p^{7\alpha} - (8\alpha)p^{4\alpha+2} + (8\alpha+4)p^{4\alpha} - 4).$$

<u>Demostración</u>.

i) Es claro que

$$r_{p^{4\alpha+1}}(n, \langle p^2,1,1\rangle) = \sum_{x\,(\text{mód } p^{4\alpha+1})} r_{p^{4\alpha+1}}(n-p^2x^2, \langle 1,1\rangle).$$

Es decir, estudiaremos la congruencia

$$Y^2+ Z^2 \equiv n-p^2X^2 \ (\text{mód } p^{4\alpha+1}).$$

Si $v_p(x)=i$, con $0\leq i\leq \alpha-2$, se tiene que $v_p(n-p^2x^2) = 2(i+1)$. Luego, vía el lema 2.11, se puede calcular su contribución fácilmente.

Indiquemos ahora por $v_p(\ ,t)$ la aplicación inducida por v_p en $\mathbb{Z}/p^t\mathbb{Z}$, mediante

$$v_p(\bar{x},t) = \begin{cases} \infty & \text{si } \bar{x} = \bar{0}, \\ v_p(x) & \text{si } \bar{x} \neq \bar{0}, \ x \text{ un representante cualquiera de } \bar{x}. \end{cases}$$

Ahora bien, $v_p(x,4\alpha+1)\geq \alpha-1$ es equivalente a $v_p(n-p^2x^2, 4\alpha+1) \geq 2\alpha$, y a su vez es equivalente a que x sea de la imágen del monomorfismo "multiplicar" por $p^{\alpha-1}$ de $\mathbb{Z}/p^{3\alpha+2}\mathbb{Z}$ en $\mathbb{Z}/p^{4\alpha+1}\mathbb{Z}$.

Por tanto, podemos escribir $x = p^{\alpha-1}y$ con y único módulo $p^{3\alpha+2}$.

Puesto que $\left(\frac{p^{-2\alpha}n}{p}\right) = 1$ resulta que $p^{-2\alpha}n \equiv a^2 (\text{mód } p^{4\alpha+1})$, y $n-p^2x^2 \equiv p^{2\alpha}(a^2-y^2) (\text{mód } p^{4\alpha+1})$, y $v_p(n-p^2x^2, 4\alpha+1)$ puede calcularse a partir de $v_p(a^2-y^2, 3\alpha+2)$, en el sentido de que

$$v_p(n-p^2x^2,4\alpha+1) = \begin{cases} 2\alpha + v_p(a^2-y^2,3\alpha+2), & \text{si } v_p(a^2-y^2,3\alpha+2) \leq 2\alpha, \\ \infty, & \text{si } v_p(a^2-y^2,3\alpha+2) > 2\alpha. \end{cases}$$

Nos remitimos al lema 3.12 para el cálculo de

$v_p(a^2-y^2,\ 3\alpha+2)$.

Además, se verifica :

$$\#\ \{x(\text{mód } p^{4\alpha+1}) \mid v_p(n-p^2x^2,4\alpha+1) = i + 2\alpha;\ i \geq 0\}$$

$$= \#\ \{y(\text{mód } p^{3\alpha+2}) \mid v_p(a^2-y^2,3\alpha+2) = i\}$$

Con todos estos datos podemos construir la siguiente tabla:

nº de y's = nº de x's	$v_p(a^2-y^2,3\alpha+2)$	$v_p(n-p^2x^2,4\alpha+1)$
$p^{3\alpha+2} - 2p^{3\alpha+1}$	0	2α
$2\ (p^{3\alpha+1})$	1	$2\alpha+1$
$2\ (p^{3\alpha})$	2	$2\alpha+2$
.	.	.
.	.	.
.	.	.
$2\ (p^{\alpha+2})$	2α	4α
	$2\alpha+1$	∞
	.	.
$2p^{\alpha+1}$	.	.
	.	.
	$(4\alpha+1=)\infty$	∞

Entonces el valor de $r_{p^{4\alpha+1}}(n,<p^2,1,1>)$, si $p\equiv 3(\text{mód } 4)$, es:

$$p^{4\alpha+1}(1+p^{-1})\ (\varphi(p^{4\alpha+1}) + \varphi(p^{4\alpha}) + \ldots + \varphi(p^{3\alpha+3}) +$$

$$+(p^{3\alpha+2} - 2p^{3\alpha+1}) + 2\varphi(p^{3\alpha}) + 2\varphi(p^{3\alpha-2}) + \ldots$$

$$\ldots + 2\varphi(p^{\alpha+2})) + 2p^{\alpha+1}p^{4\alpha}$$

$$= p^{7\alpha+2}(p^{\alpha} + p^{\alpha-1} - 2).$$

ii) Sea ahora $p\equiv 1 (\text{mód } 4)$. Si $v_p(x)=i$, con $0\leq i\leq \alpha-2$, basta aplicar el lema 2.11 para obtener su contribución en el cálculo de $r_{p^{4\alpha+1}}(n, <p^2,1,1>)$.

Si $v_p(x) \geq \alpha-1$, obtenemos la misma tabla de valores que en el apartado i). Pero cada uno de ellos se ha de multiplicar por su valor correspondiente, dado en los lemas 2.11 y 3.12. Así que si $p\equiv 1 (\text{mód } 4)$, se tiene que el valor de $r_{p^{4\alpha+1}}(n, <p^2,1,1>)$ es:

$$(1-p^{-1})\ p^{4\alpha+1}(3\varphi(p^{4\alpha+1}) + 5\varphi(p^{4\alpha}) + \ldots + (2\alpha-1)\varphi(p^{3\alpha+3}) +$$

$$+ (2\alpha+1)(p^{3\alpha+2} - 2p^{3\alpha+1}) + 2(2\alpha+2)\varphi(p^{3\alpha+1}) +$$

$$+ 2(2\alpha+3)\varphi(p^{3\alpha}) + \ldots + 2(4\alpha+1)\varphi(p^{\alpha+2})) +$$

$$+ 2p^{\alpha+1}\left(\frac{2(p^{4\alpha+2}-1) + p^{4\alpha}(p+1)}{p+1}\right)$$

$$= (p+1)^{-1}\ p^{\alpha+1}(3p^{7\alpha+2} + 2p^{7\alpha+1} - p^{7\alpha} - 8\alpha p^{4\alpha+2} + (8\alpha+4)\ p^{4\alpha} - 4). \quad \#$$

Recordando que si $v_p(n) = 2\alpha$, entonces

$$\partial_p(n, <p^2,1,1>) = p^{-2(4\alpha+1)} r_{p^{4\alpha+1}}(n, <p^2,1,1>),$$

obtenemos el siguiente

Corolario 3.14. Sea $v_p(n) = 2\alpha$, $\alpha \geq 1$, y $(\frac{p^{-2\alpha}n}{p}) = 1$. Entonces:

i) Si $p \equiv 3 \pmod 4$,

$$\partial_p(n, \langle p^2,1,1\rangle) = p^{-\alpha}(p^{\alpha}+p^{\alpha-1}-2) .$$

ii) Si $p \equiv 1 \pmod 4$, entonces $\partial_p(n, \langle p^2,1,1\rangle)$ vale:

$$(p+1)^{-1}\ p^{-(7\alpha+1)}(3p^{7\alpha+2}+ 2p^{7\alpha+1}- p^{7\alpha}- (8\alpha)\ p^{4\alpha+2}+ (8\alpha+4)p^{4\alpha}- 4).$$

Está claro ahora que para obtener el valor de $r(n,\text{gen } \langle b_1^2,b_2^2,b_3^2\rangle)$ basta sustituir en la fórmula del "Hauptsatz" de Siegel los valores de las densidades p-ádicas que hemos obtenido.

§4. Cálculo de $r(n,\text{gen } \langle b_1^2,b_2^2,2^2\rangle)$ en el caso n par

En todo este párrafo n designará un entero positivo par tal que $4 \nmid n$.

La única diferencia con el caso impar viene dada por el cálculo de ∂_∞ y ∂_2.

Por el lema 2.10 se tiene

$$\partial_\infty(n, \langle b_1^2,b_2^2,2^2\rangle) = \frac{n^{1/2}\ \pi^{3/2}}{2b_1b_2\Gamma(3/2)}$$

El cálculo de

$\partial_2(n, <b_1^2,b_2^2,2^2>) = 2^{-10}\, r_{2^5}(n, <b_1^2,b_2^2,2^2>)$ se simplifica gracias a la siguiente

Proposición 3.15. Si n es par y $4 \nmid n$, entonces si $k \geq 3$, resulta que

$$r_{2^{k+1}}(n, <b_1^2,b_2^2,2^2>) = 2^2\, r_{2^k}(n, <b_1^2,b_2^2,2^2>).$$

Demostración. Paralela a la proposición 3.2, teniendo en cuenta que b_1, b_2 son unitarios en $\mathbb{Z}/2^k\mathbb{Z}$, para todo k. #

Corolario 3.16. Si $n \equiv 2,6 \pmod 8$, entonces $\partial_2(n, <b_1^2,b_2^2,2^2>) = 1$.

Demostración. Por la proposición precedente se tiene que

$$\partial_2(n, <b_1^2,b_2^2,2^2>) = \frac{r_{2^3}(n, <b_1^2,b_2^2,2^2>)}{2^6} = 1. \quad \#$$

Sustituyendo por los valores hallados de ∂_2 y ∂_∞, y procediendo como en el teorema 3.9 , se obtiene el siguiente

Teorema 3.17. Si $n \equiv 2,6 \pmod 8$ y n es libre de cuadrados respecto de sus divisores primos congruentes con 1 módulo 4, se verifica:

$$r^*(n, \text{gen } <b_1^2,b_2^2,2^2>) = \frac{8}{\pi}\, n^{1/2}\, L(1,\chi_{-4n}) \prod_{p \mid b_1 b_2} 2(1+p)^{-1}.$$

§5. Expresión de $G_i(n)$ mediante densidades p-ádicas

Sea $n \not\equiv 0,4,7 (\text{mód } 8)$; por comodidad escribiremos:

$$S_i'(n) = \frac{S_i(n)}{r(n,I_3)} ,$$

para $i = 1,2,3$. Tenemos la siguiente

Proposición 3.18. Sea $n \not\equiv 0,4,7(\text{mód } 8)$. Entonces

$$\text{i) } S_1'(n) = 3 \sum_{\substack{a_i \mid n \\ a \neq 1}} - \mu(a) \prod_{p \mid a} \frac{\partial_p(n, <a^2,1,1>)}{p\, \partial_p(n,I_3)} ,$$

$$\text{ii) } S_2'(n) = 2 \sum_{\substack{a_i \mid n \\ a_i \neq 1}} - \mu(b_1 b_2) \prod_{p \mid a_1 a_2} \frac{\partial_p(nd^{-2}, <b_1^2,b_2^2,1>)}{p\, \partial_p(n,I_3)} ,$$

$$\text{iii) } S_3'(n) = \sum_{\substack{a_i \mid n \\ a_i \neq 1}} - \mu(b_1 b_2 b_3) \prod_{p \mid a_1 a_2 a_3} \frac{\partial_p(nd^{-2}, <b_1^2,b_2^2,b_3^2>)}{p\, \partial_p(n,I_3)} ,$$

en donde a_1, a_2 y a_3 son libres de cuadrados.

Demostración. Basta tener en cuenta la definición de $S_i(n)$, $i = 1,2,3$ y que, según los cálculos precedentes, si $p \nmid a_1 a_2 a_3$ es:

$$\partial_p(nd^{-2}, <b_1^2,b_2^2,b_3^2>) = \partial_p(n,I_3).$$

Así como que

$$\frac{\partial_\infty(nd^{-2},\ <b_1^2,b_2^2,b_3^2>)}{\partial_\infty(n,I_3)} = \prod_{p|a_1a_2a_3} \frac{1}{p}\ . \qquad \#$$

La proposición precedente nos permite *extender* las expresiones $S_i'(n)$ a enteros $n \equiv 7(\text{mód } 8)$, no representables, por tanto, como suma de tres cuadrados.

Definición. Si $n \equiv 7(\text{mód } 8)$, entonces

$$S_1'(n) := 3 \sum_{\substack{a|n \\ a\neq 1}} - \mu(a) \prod_{p|a} \frac{\partial_p(n,\ <a^2,1,1>)}{p\ \partial_p(n,I_3)}\ ,$$

$$S_2'(n) := 3 \sum_{\substack{a_i|n \\ a_i\neq 1}} \mu(b_1b_2) \prod_{p|a_1a_2} \frac{\partial_p(nd^{-2},\ <b_1^2,b_2^2,1>)}{p\ \partial_p(n,I_3)}\ ,$$

$$S_3'(n) := \sum_{\substack{a_i|n \\ a_i\neq 1}} - \mu(b_1b_2b_3) \prod_{p|a_1a_2a_3} \frac{\partial_p(nd^{-2},\ <b_1^2,b_2^2,b_3^2>)}{p\ \partial_p(n,I_3)}\ .$$

Estas definiciones son posibles debido que al ser n impar y $p \neq 2$ siempre se verifica que $\partial_p(n,I_3) \neq 0$, aunque $r(n,I_3) = 0$.

Ahora podemos definir $G_i(n)$ para estos enteros $n \equiv 7(\text{mód } 8)$ del siguiente modo:

$$G_1(n) := S_3'(n),$$

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

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

§6. Fórmulas recurrentes para $G_i(n)$

En este párrafo se van a hallar fórmulas recurrentes para $G_i(n)$, $i = 1,2,3$, $n \not\equiv 0,4 (8)$, en función de cocientes de densidades p-ádicas.

Sea n un entero no divisible por un primo p. A fin de relacionar $G_i(np^\alpha)$ con $G_i(n)$ introducimos los siguientes conceptos:

Definición. Sea $np^\alpha \not\equiv 0,4,7 (\text{mód } 8)$ y $n \not\equiv 0,4,7 (\text{mód } 8)$.

i) Si $a_i | np^\alpha$, $p | a_i$ para exactamente un i y $d = d(a_1,a_2,a_3)$ (cf.§6 Cap.II), entonces el cociente

$$\left(\frac{r(np^\alpha d^{-2},\ \text{gen } \langle b_1^2,b_2^2,b_3^2\rangle)}{r(np^\alpha,I_3)}\right)\cdot\left(\frac{r(nd^{-2},\ \text{gen } \langle b_1^2p^{-2},b_2^2,b_3^2\rangle)}{r(n,I_3)}\right)^{-1}$$

lo designamos por $\partial_p'(n,\alpha)$, en donde $p \nmid d$ y $p | b_i$ para exactamente un i, que hemos supuesto i = 1.

Si n = 1, escribiremos

$$\partial_p'(\alpha) := \partial_p'(1,\alpha) .$$

ii) Si $a_i | np^\alpha$ y $p | a_i$ para exactamente 2 ó 3 índices, entonces $p | d(a_1,a_2,a_3)$ y si llamamos

$$d := d(p^{-1}a_1,p^{-1}a_2,a_3)$$

ó

$$d := d(p^{-1}a_1,p^{-1}a_2,p^{-1}a_3)$$

según el caso, entonces el cociente

$$\left(\frac{r(np^{\alpha-2}d^{-2},\ \text{gen}\ \langle b_1^2,b_2^2,b_3^2\rangle)}{r(np^{\alpha},I_3)}\right)\cdot\left(\frac{r(nd^{-2},\ \text{gen}\ \langle b_1^2,b_2^2,b_3^2\rangle)}{r(n,I_3)}\right)^{-1}$$

lo designamos por $\partial'_{p^2}(n,\alpha)$, en donde $p\nmid d$ y $p\nmid b_i$, para $i=1,2,3$.

Si $n = 1$, escribiremos

$$\partial'_{p^2}(\alpha) := \partial'_{p^2}(1,\alpha)\ .$$

Lema 3.19. Sea p un primo y n, $np^{\alpha} \not\equiv 0,4,7 (\text{mód } 8)$. Se tiene:

i) Si $p\nmid d$ y $p\nmid b_i$, para $i = 1,2,3$, entonces

$$\frac{r(np^{\alpha}d^{-2},\ \text{gen}\ \langle b_1^2,b_2^2,b_3^2\rangle)}{r(np^{\alpha},I_3)} = \frac{r(nd^{-2},\ \text{gen}\ \langle b_1^2,b_2^2,b_3^2\rangle)}{r(n,I_3)}\ ,$$

ii) Si $p\nmid d$ y $p\nmid b_i$ para exactamente un i, entonces

$$\partial'_p(n,\alpha) = \frac{\partial_p(np^{\alpha}d^{-2},\ \langle b_1^2,b_2^2,b_3^2\rangle)}{p\ \partial_p(np^{\alpha},I_3)}\ .$$

iii) Si $p\nmid d$ y $p\nmid b_i$ para $i = 1,2,3$, entonces

$$\partial'_{p^2}(n,\alpha) = \frac{\partial_p(np^{\alpha-2}d^{-2},\langle b_1^2,b_2^2,b_3^2\rangle)}{p\ \partial_p(np^{\alpha},I_3)}\ .$$

Demostración.

i) Basta comprobar, aplicando los resultados de los párrafos precedentes, que los cocientes de densidades coinciden en ambos términos.

ii) y iii) Basta aplicar las definiciones de $\partial'_p(n,\alpha)$ y $\partial'_{p^2}(n,\alpha)$. El factor $1/p$ proviene del cociente de las densidades del infinito.

Proposición 3.20. Sean $n, np^{\alpha} \not\equiv 0,4,7 \pmod 8$ y $p \nmid n$, entonces:

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

$$\text{ii)} \quad \partial'_{p^2}(n,\alpha) = \frac{\partial_p(p^{\alpha-2}, I_3)}{p\ \partial_p(p^{\alpha}, I_3)} \ .$$

Demostración.

i) Si $p \nmid d$ y $p \mid b_i$ para exactamente un i, por ejemplo $i = 1$, entonces está claro que b_2 y b_3 son invertibles módulo $p^{2\alpha+1}$ y si escribimos $b_1 = p\, b_1'$, también b_1' es invertible módulo $p^{2\alpha+1}$. Por tanto,

$$\partial'_p(n,\alpha) = \frac{\partial_p(np^{\alpha}d^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle)}{p\ \partial_p(np^{\alpha}, I_3)} = \frac{\partial_p(np^{\alpha}, \langle p^2,1,1\rangle)}{p\ \partial_p(np^{\alpha}, I_3)} \ ,$$

y como $\partial_p(np^{\alpha}, I_3) = \partial_p(p^{\alpha}, I_3)$, para todo $n \geq 1$, resulta que

$$\partial'_p(n,\alpha) = \frac{\partial_p(np^{\alpha}, \langle p^2,1,1\rangle)}{p\ \partial_p(p^{\alpha}, I_3)} \ .$$

ii) Si $p \nmid d$ y $p \nmid b_i$, para $i = 1,2,3$, entonces todos los b_i son invertibles módulo $p^{2\alpha+1}$ y resulta que

$$\partial'_{p^2}(n,\alpha) = \frac{\partial_p(np^{\alpha-2}d^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle)}{p\ \partial_p(np^{\alpha}, I_3)} = \frac{\partial_p(np^{\alpha-2}, I_3)}{p\ \partial_p(np^{\alpha}, I_3)} \ ,$$

y claramente, por tratarse de I_3, este último cociente coincide con

$$\frac{\partial_p(p^{\alpha-2}, I_3)}{p\ \partial_p(p^{\alpha}, I_3)} \quad . \qquad \#$$

Esta proposición justifica la notación $\partial'_p(n,\alpha)$, $\partial'_{p^2}(n,\alpha)$, ya que su valor no depende de b_1, b_2, b_3, sino sólo de sus valoraciones en p.

Observaciones.

i) Como $\partial'_{p^2}(n,\alpha)$ no depende de n, podemos escribir, para todo $n \geq 1$.

$$\partial'_{p^2}(n,\alpha) = \partial'_{p^2}(\alpha).$$

ii) En el caso en que el exponente de p sea impar, por la proposición 3.8, resulta que también podemos escribir

$$\partial'_p(n,2\alpha+1) = \partial'_p(2\alpha+1)$$

para todo $n \geq 1$.

Así sólo escribiremos $\partial'_p(n,2\alpha)$ en el caso en que el exponente de p sea par y distinguiendo según sea $\left(\frac{n}{p}\right) = -1$ ó $\left(\frac{n}{p}\right) = 1$.

Convendrá extender también los valores $\partial'_p(n,\alpha)$, $\partial'_{p^2}(\alpha)$, al caso en que $np^{\alpha} \equiv 7 \pmod 8$. Se definen

$$\partial'_p(n,\alpha) = \frac{\partial_p(np^{\alpha}, \langle p^2,1,1\rangle)}{p\ \partial_p(p^{\alpha}, I_3)},$$

$$\partial'_{p^2}(\alpha) = \frac{\partial_p(p^{\alpha-2}, I_3)}{p\,\partial_p(p^{\alpha}, I_3)} ,$$

en donde $\partial_p(p^{\alpha}, I_3) \neq 0$ ya que $p \neq 2$.

La obtención de las fórmulas recurrentes para $G_i(n)$, $i = 1,2,3$, resultará de las fórmulas recurrentes para las correspondientes sumas auxiliares, que se dan en el siguiente

Teorema 3.21. Sea n un entero positivo impar. Y sea p un primo tal que $p \nmid n$. Entonces para todo entero $\alpha \geq 1$ se verifica.

i) $S'_1(np^{\alpha}) = S'_1(n) + \partial'_p(n,\alpha)(3 - S'_1(n))$,

ii) $S'_2(np^{\alpha}) = S'_2(n) + \partial'_p(n,\alpha)(S'_1(n) - S'_2(n)) + \partial'_{p^2}(n,\alpha)(3 - S'_1(n) + S'_2(n))$,

iii) $S'_3(np^{\alpha}) = S'_3(n) + \partial'_p(n,\alpha)(S'_2(n) - 3S'_3(n)) + \partial'_{p^2}(n,\alpha)(1 - S'_2(n) + 2S'_3(n))$.

Demostración.

i) Recordemos que

$$S'_1(np^{\alpha}) = 3 \sum_{\substack{a \mid np^{\alpha} \\ 1 \neq a}} \mu(a) \prod_{q \mid a} \frac{\partial_q(np^{\alpha}, \langle a^2, 1, 1\rangle)}{q\,\partial_q(np^{\alpha}, I_3)} ,$$

en este caso designamos por q los divisores primos de a.

Entonces podemos escribir

$$S_1'(np^\alpha) = 3 \sum_{(1)} - \mu(a) \prod_{q|a} \frac{\partial_q(np^\alpha, <a^2,1,1>)}{q\ \partial_q(n,I_3)},$$

$$+ 3 \sum_{(2)} - \mu(a) \prod_{q|a} \frac{\partial_q(np^\alpha, <a^2,1,1>)}{q\ \partial_q(n,I_3)},$$

estando sujeto el sumatorio (1) a las condiciones:

$a|np^\alpha$, $a \neq 1$, con $(a,p) = 1$.

Y el sumatorio (2) a las condiciones:

$a|np^\alpha$, $a \neq 1$ y $p|a$.

Por el lema 3.19 se obtiene

$$3 \sum_{(1)} - \mu(a) \prod_{q|a} \frac{\partial_q(np^\alpha, <a^2,1,1>)}{q\ \partial_q(n,I_3)} = S_1'(n),$$

$$3 \sum_{(2)} - \mu(a) \prod_{q|a} \frac{\partial_q(np^\alpha, <a^2,1,1>)}{q\ \partial_q(n,I_3)} = \partial_p'(n,\alpha)(3-S_1'(n)).$$

Por tanto,

$$S_1'(np^\alpha) = S_1'(n) + \partial_p'(n,\alpha)(3-S_1'(n)).$$

ii) Podemos descomponer

$$S_2'(np^\alpha) = 3 \sum_{\substack{a_i|np^\alpha \\ a_i\neq 1}} \mu(b_1b_2) \prod_{q|a_1a_2} \frac{\partial_q(np^\alpha d^{-2}, <b_1^2,b_2^2,1>)}{q\ \partial_q(n,I_3)}$$

en tres sumatorios,

$$\sum_{\substack{a_i|np^\alpha \\ a_i\neq 1}} = \sum_{(1)} + \sum_{(2)} + \sum_{(3)},$$

en donde el sumatorio (1) está sujeto a las condiciones $a_i | np^\alpha$, $a_i \neq 1$ y $(a_i, p) = 1$, para $i = 1,2$. De donde $p \nmid d$ y $p \nmid b_i$, $i = 1,2,3$.

El sumatorio (2) está sujeto a las condiciones: $a_i | np^\alpha$, $a_i \neq 1$ y $p | a_i$ para exactamente un i. Por tanto, $p \nmid d$ y $p | b_i$ para exactamente un i.

El sumatorio (3) está sujeto a: $a_i | np^\alpha$, $a_i \neq 1$, $p | a_1$ y $p | a_2$. Por tanto $p | d$ y $p \nmid b_i$, $i = 1,2$.

Entonces por el lema 3.19 se tiene que

$$3 \sum_{(1)} \mu(b_1 b_2) \prod_{q | a_1 a_2} \frac{\partial_q(np^\alpha d^{-2}, \langle b_1^2, b_2^2, 1\rangle)}{q\, \partial_q(n, I_3)} = S_2'(n).$$

En el segundo sumatorio si p divide a a_i puede ocurrir que $a_i = p$ ó bien $a_i = pa_i'$, con $(a_i', p) = 1$, para exactamente un i, $i = 1,2$. En el primer caso la contribución en $3 \sum_{(2)}$ es, otra vez por el lema 3.19, $2\, \partial_p'(n,\alpha)\, S_1'(n)$ y en el segundo es: $-2\, \partial_p'(n,\alpha)\, S_2'(n)$; en donde el coeficiente 2 proviene de que p puede dividir a a_1 ó a_2 (ó lo que es lo mismo a b_1 ó b_2). Así que

$$3 \sum_{(2)} \mu(b_1 b_2) \prod_{q | a_1 a_2} \frac{\partial_q(np^\alpha d^{-2}, \langle b_1^2, b_2^2, 1\rangle)}{q\, \partial_q(n, I_3)} =$$

$$= 2\, \partial_p'(n,\alpha)(S_1'(n) - S_2'(n)).$$

Por último, en el tercer sumatorio hay que distinguir según sea

$a_1 = a_2 = p$;

$a_1 = p$, $a_2 = pa_2'$ con $(a_2', p) = 1$, $a_2' \neq 1$ ó viceversa;

$a_i = pa_i'$ con $(a_i', p) = 1$, $a_1' \neq 1$, para $i = 1,2$.

Por tanto, teniendo en cuenta el lema 3.19 se obtiene

$$3 \sum_{(3)} \mu(b_1 b_2) \prod_{q \mid a_1 a_2} \frac{\partial_q(np^\alpha d^{-2}, \langle b_1^2, b_2^2, 1\rangle)}{q\, \partial_q(np^\alpha, I_3)} =$$

$$= \partial'_{p^2}(n,\alpha)(3 - 2\, S_1'(n) + S_2'(n)).$$

Sumando estos resultados queda probado ii).

iii) Descompongamos

$$S_3'(np^\alpha) = \sum_{\substack{a_i \mid np^\alpha \\ a_i \neq 1}} - \mu(b_1 b_2 b_3) \prod_{q \mid a_1 a_2 a_3} \frac{\partial_q(np^\alpha d^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle)}{q\, \partial_q(np^\alpha, I_3)}$$

en tres sumatorios,

$$\sum_{\substack{a_i \mid np^\alpha \\ a_i \neq 1}} = \sum_{(1)} + \sum_{(2)} + \sum_{(3)}$$

con el sumatorio (1) sujeto a las condiciones: $a_i \mid np^\alpha$, $a_i \neq 1$ y $(a_i, p) = 1$ para $i = 1,2,3$. De donde $p \nmid d$ y $(b_i, p) = 1$, para $i = 1,2,3$.

El sumatorio (2) está sujeto a las condiciones: $a_i \mid np^\alpha$, $a_i \neq 1$ y $p \mid a_i$ para exactamente un i, $i = 1,2$. De donde $p \nmid d$ y $p \mid b_i$ para exactamente un i.

El sumatorio (3) está sujeto a las condiciones: $a_i \mid np^\alpha$, $a_i \neq 1$ y p divide a 2 ó 3 a_i. De lo que se deduce que $p \mid d$ y $p \nmid b_i$ $i = 1,2,3$.

Aplicando el lema 3.19 y procediendo exactamente igual

como en los apartados anteriores resulta

$$\sum_{(1)} - \mu(b_1b_2b_3) \prod_{q \mid a_1a_2a_3} \frac{\partial_q(np^\alpha d^{-2}, <b_1^2,b_2^2,b_3^2>)}{q\ \partial_q(np^\alpha, I_3)} = S_3'(n).$$

$$\sum_{(2)} - \mu(b_1b_2b_3) \prod_{q \mid a_1a_2a_3} \frac{\partial_q(np^\alpha d^{-2}, <b_1^2,b_2^2,b_3^2>)}{q\ \partial_q(np^\alpha, I_3)} =$$

$$= \partial_p'(n,\alpha)\ (S_2'(n) - 3S_3'(n)).$$

$$\sum_{(3)} - \mu(b_1b_2b_3) \prod_{q \mid a_1a_2a_3} \frac{\partial_q(np^\alpha d^{-2}, <b_1^2,b_2^2,b_3^2>)}{q\ \partial_q(np^\alpha, I_3)} =$$

$$= \partial'_{p^2}(n,\alpha)\ (1-S_2'(n) + 2S_3'(n)).$$

Al sumar estas expresiones se obtiene iii). #

Las relaciones (cf. Cap. III §5)

$$G_1(np^\alpha) = S_3'(np^\alpha),$$

$$G_2(np^\alpha) = S_2'(np^\alpha) - 2S_3'(np^\alpha),$$

$$G_3(np^\alpha) = S_1'(np^\alpha) - S_2'(np^\alpha) + S_3'(np^\alpha),$$

junto con el teorema 3.21 nos permiten obtener la fórmula recurrente para el término principal, dada en el siguiente

Teorema 3.22. Sea n un entero positivo impar y p un primo tal que $p \nmid n$. Entonces para todo entero $\alpha \geq 1$ se verifica que

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

Corolario 3.23. En el caso particular en que n = 1 se obtiene:

$$G_1(p^\alpha) = \partial'_{p^2}(\alpha),$$
$$G_2(p^\alpha) = \partial'_{p^2}(\alpha),$$
$$G_3(p^\alpha) = 3\partial'_p(\alpha) - 2\partial'_{p^2}(\alpha).$$

Pasamos a continuación a la obtención de las fórmulas recurrentes en el caso par. Como sólo nos interesan enteros pares no divisibles por 4, sólo calcularemos $G_i(n2)$, i=1,2. Se tiene el siguiente

Teorema 3.24. Sea n un entero impar. Entonces

i) $S'_2(2n) = S'_2(n) + \partial'_2(1)(S'_1(n) - S'_2(n))$.

ii) $S'_3(2n) = S'_3(n) + \partial'_2(1)(S'_2(n) - 3S'_3(n))$.

Demostración. Basta tener en cuenta las definiciones de S'_i, i=1,2; que $\partial'_{2^2}(1)=0$ y proceder como en el teorema 3.21. #

Aplicando el teorema precedente obtenemos el siguiente

Corolario 3.25. Sea n un entero impar. Entonces

i) $G_1(2n) = G_1(n) + \partial_2'(1)(G_2(n) - G_1(n))$,

ii) $G_2(2n) = G_2(n) + 2\partial_2'(1)(G_3(n) - G_2(n))$.

§7. Expresión de $G_i^*(n)$ mediante densidades p-ádicas

Recordemos (cf. Cap. II §6) que si $n \not\equiv 0,4,7 (\text{mód } 8)$ es un entero libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4, entonces $\ell(n,3)$ se puede estudiar, si es impar, mediante las funciones

$$G_1^*(n) = S_3^{*'}(n),$$

$$G_2^*(n) = S_2^{*'}(n) - 2S_3^{*'}(n),$$

$$G_3^*(n) = S_1^{*'}(n) - S_2^{*'}(n) + S_3^{*'}(n).$$

Y si es par mediante

$$G_1^*(n) = S_3^{*'}(n),$$

$$G_2^*(n) = S_2^{*'}(n) - S_3^{*'}(n),$$

en donde

$$S_i^{*'}(n) := \frac{S_i^*(n)}{r(n,I_3)} .$$

Caso n impar, $n \not\equiv 7 (\text{mód } 8)$.

Por el teorema 3.9 sabemos que en este caso

$$r^*(n,\text{gen } \langle a_1^2,a_2^2,a_3^2\rangle) = \frac{A(n)}{\pi}\, n^{1/2}\, L(1,\chi_{-4n}) \prod_{p\mid a_1a_2a_3} 2(1+p)^{-1}.$$

Por tanto, se obtiene

$$S_1^{*'}(n) = 3 \sum_{1<a\mid m} - \mu(a) \prod_{p\mid a} 2(1+p)^{-1},$$

$$S_2^{*'}(n) = 3 \sum_{\substack{1<a_i\mid m \\ (a_i,a_j)=1}} \mu(a_1a_2) \prod_{p\mid a_1a_2} 2(1+p)^{-1},$$

$$S_3^{*'}(n) = \sum_{\substack{1<a_i\mid m \\ (a_i,a_j)=1}} - \mu(a_1a_2a_3) \prod_{p\mid a_1a_2a_3} 2(1+p)^{-1},$$

siendo $n = mt$, con $m = p_1 \ldots p_r$, $t = q_1^{\beta_1} \ldots q_s^{\beta_s}$, $p_i \equiv 1 (\text{mód } 4)$ y $q_j \equiv 3 (\text{mód } 4)$.

Caso n par, $n \not\equiv 0,4 (\text{mód } 8)$

Por el teorema 3.17 sabemos que

$$r^*(n,\text{gen } \langle a_1^2,a_2^2,2^2\rangle) = \frac{8}{\pi}\, n^{1/2}\, L(1,\chi_{-4n}) \prod_{p\mid a_1a_2} 2(1+p)^{-1}.$$

Por tanto, se verifica

$$S_2^{*'}(n) = 2 \sum_{1<a\mid m} - \mu(a) \prod_{p\mid a} 2(1+p)^{-1},$$

$$S_3^{*'}(n) = \sum_{\substack{1<a_i\mid m \\ (a_1,a_2)=1}} \mu(a_1a_2) \prod_{p\mid a_1a_2} 2(1+p)^{-1},$$

siendo $n = 2mt$; m y t como antes.

§8. Fórmulas exactas para $G_i^*(n)$ en el caso n impar

En este párrafo n designará un entero impar $n \not\equiv 7 (\text{mód } 8)$, libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Escribiremos $n = mt$, con

$m = p_1 \cdots p_r$, $p_i \equiv 1 (\text{mód } 4)$;

$t = q_1^{\beta_1} \cdots q_s^{\beta_s}$, $q_j \equiv 3 (\text{mód } 4)$.

Definición. Sea $x_i = 2(1+p_i)^{-1}$, $1 \leq i \leq r$. Designaremos por $P_j = P_j(m)$, $j = 1,2,3$, a

$$P_j = \prod_{i=1}^{r} (1 - jx_i),$$

para $j = 1,2,3$.

Teorema 3.26. Sea $n \not\equiv 7 (\text{mód } 8)$ un entero impar libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Se satisface:

$$G_1^*(n) = S_3^{*'}(n) = 1 - 3P_1 + 3P_2 - P_3 .$$

Demostración. Por el teorema 3.9 se tiene que

$$G_1^*(n) = \sum_{\substack{1<a_i \mid m \\ (a_i,a_j)=1}} - \mu(a_1a_2a_3) \prod_{p \mid a_1a_2a_3} 2(1+p)^{-1}.$$

Para evaluar esta suma agrupamos previamente todos aquéllos sumandos que difieren entre sí por una permutación de

a_1, a_2, a_3 y que, por tanto, son iguales.

Tenemos:

$$\sum_{\substack{1<a_i|m \\ (a_i,a_j)=1}} = 3! \sum_{(1)} ,$$

en donde el sumatorio (1), que indica un modo de seleccionar un representante de cada familia de las ternas anteriores, está sujeto a las condiciones:

$a_i | m$, $i = 1,2,3$;

$\omega(a_1) \geq \omega(a_2) \geq \omega(a_3) \geq 1$;

si $\omega(a_1) = \omega(a_2)$, entonces $a_1 > a_2$;

si $\omega(a_2) = \omega(a_3)$, entonces $a_2 > a_3$;

$m.c.d.(a_i,a_j) = 1$, $i \neq j$.

Aquí como es usual $\omega(n)$ designa el número de factores primos de un entero positivo n.

Si escribimos $\omega(a_i) = k_i$, $i = 1,2,3$, con $k = k_1+k_2+k_3$ y $3 \leq k \leq r$, podemos escribir

$$G_1^*(n) = 3! \sum_{k=3}^{r} (-1)^{k+1} 2^k \sum_{(2)} \sum_{(3)} (1+p_{ij})^{-1},$$

estando el sumatorio (2) sujeto a las condiciones:

$k_1 + k_2 + k_3 = k$;

$k_1 \geq k_2 \geq k_3 \geq 1$;

si $k_1 = k_2$ entonces $a_1 > a_2$;

si $k_2 = k_3$ entonces $a_2 > a_3$;

y en donde el sumatorio (3) está extendido a todas las posibi

lidades de escoger 3 subconjuntos disjuntos de $\{p_1,\ldots p_r\}$ de cardinales respectivos k_1, k_2 y k_3 pero ésto equivale a:

1) extraer de todas las formas posibles k primos de $\{p_1,\ldots p_r\}$, y luego

2) repartir estos k primos escogidos de todas las maneras distintas posibles en subconjuntos de k_1, k_2 y k_3 primos. Por tanto podemos escribir el sumatorio (3) de la siguiente forma

$$\sum_{(3)} \prod_{j=1}^{k} (1+p_{ij})^{-1} = \sum_{C_k^r} \sum_{(4)} \prod_{j=1}^{k} (1+p_{ij})^{-1},$$

con $\sum_{C_k^r}$ indicando que se tiene que sumar respecto a todas las combinaciones ó subconjuntos de k elementos de $\{p_1,\ldots,p_r\}$, y el sumatorio (4) que se tiene que sumar tantas veces como modos distintos haya de repartir k primos en 3 subconjuntos de k_1, k_2 y k_3 elementos respectivamente.

Como $\prod_{j=1}^{k} (1+p_{ij})^{-1}$ no depende del reparto de los k primos, tenemos

$$\sum_{C_k^r} \sum_{(4)} \prod_{j=1}^{k} (1+p_{ij})^{-1} = \left(\sum_{C_k^r} \prod_{j=1}^{k} (1+p_{ij})^{-1}\right) \left(\sum_{(4)} 1\right),$$

y $\sum_{(4)} 1$ es fácil de evaluar: los k primos escogidos se pueden permutar de k! formas; ahora bien, cada elección de k_1 primos es la misma que la de éstos k_1 elementos permutados y lo mismo sucede con los k_2 y k_3 restantes.

Por tanto,

$$\sum_{(4)} 1 = \frac{k!}{k_o!\ k_1!\ k_2!\ k_3!}\ ,$$

en donde k_o indica el número de igualdades que hay en $k_1 \geq k_2 \geq k_3$ más una unidad.

Como por otra parte es obvio que $\sum_{(2)}$ y $\sum_{C_k^r}$ permutan, lo que tenemos que calcular, es, pues,

$$\sum_{k=3}^{r} (-1)^{k+1}\ 2^k \sum_{C_k^r} \prod_{j=1}^{k} (1+p_{ij})^{-1} \sum_{(2)} \frac{k!}{k_o!\ k_1!\ k_2!\ k_3!}\ .$$

Abreviaremos el último sumatorio poniendo

$$\sum_{(2)} \frac{k!}{k_o!\ k_1!\ k_2!\ k_3!} = j_3(k),$$

cuyo valor calcularemos después.

Como, por otra parte,

$$\sum_{C_k^r} \prod_{j=1}^{k} (1+p_{ij})^{-1} = \sigma_k((1+p_1)^{-1},\ldots,(1+p_r)^{-1}),$$

en donde $\sigma_k(X_1,\ldots,X_r)$ es el k-ésimo polinomio simétrico elemental, esto es,

$$\sigma_k(X_1,\ldots,X_r) = \sum_{1\leq i_1\leq\ldots\leq i_k\leq r} X_{i_1}\ldots X_{i_k},$$

la suma anterior queda pues en la forma

$$G_1^*(n) = 3!\ \sum_{k=3}^{r} (-1)^{k+1}\ 2^k\ j_3(k)\ \sigma_k\ ((1+p_1)^{-1},\ldots,(1+p_r)^{-1}).$$

Antes de proseguir con la demostración del teorema procedemos al cálculo que $j_3(k)$, cuyo valor viene dado en el si

guiente

Lema 3.27. $j_3(k) = \frac{1}{2}(3^{k-1} - 2^k + 1)$.

Demostración. En la fórmula de Leibniz

$$(X+Y+Z)^k = \sum_{\substack{k_1+k_2+k_3=k \\ k_1,k_2,k_3\geq 0}} \frac{k!}{k_1!\ k_2!\ k_3!}\ X^{k_1}\ Y^{k_2}\ Z^{k_3},$$

tomemos $X = Y = Z = 1$. Separemos en esta suma los sumandos en los que aparece el valor cero para alguno ó algunos de los índices k_1, k_2, k_3:
Si sólo un índice es cero, por ejemplo $k_1 = 0$, los sumandos correspondientes suman

$$\sum_{\substack{k_2+k_3=k \\ k_2,k_3>0}} \frac{k!}{k_2!\ k_3!} = \sum_{i=1}^{k-1} \binom{k}{i} = 2^k - 2.$$

Además, como dos ceros exactamente aparecen sólo en tres sumandos, cada uno de los cuales vale 1, tenemos que

$$3^k = \sum_{\substack{k_1+k_2+k_3=k \\ k_1,k_2,k_3>0}} \frac{k!}{k_1!\ k_2!\ k_3!} + 3(2^k-2) + 3$$

$$= \sum_{\substack{k_1+k_2+k_3=k \\ k_1,k_2,k_3>0}} \frac{k!}{k_1!\ k_2!\ k_3!} + 3(2^k-1).$$

Ahora bien, todas las ternas (k_1,k_2,k_3) con $k_1+k_2+k_3=k$, pueden obtenerse por permutaciones de las sujetas a cualquie

ra de las condiciones siguientes:

i) $k_1 > k_2 > k_3$,

ii) $k_1 = k_2 \neq k_3$ (ó lo que es equivalente, $k_1 = k_2 > k_3$ ó $k_1 > k_2 = k_3$),

iii) $k_1 = k_2 = k_3$, si las hay.

Como cada terna del primer tipo por permutaciones da lugar a 3! ternas, cada una del segundo a 3!/2! y cada una del tercero a 3!/3!= 1, resulta que podemos escribir

$$3^k = 3! \sum_{\substack{k_1+k_2+k_3=k \\ k_1>k_2>k_3>0}} \frac{k!}{k_1!\ k_2!\ k_3!} + 3! \sum_{\substack{k_1+k_2+k_3=k \\ 0\ k_1=k_2\neq k_3>0}} \frac{k!}{2!\ k_1!\ k_2!\ k_3!} +$$

$$+ 3! \sum_{\substack{k_1+k_2+k_3=k \\ k_1=k_2=k_3>0}} \frac{k!}{3!\ k_1!\ k_2!\ k_3!} + 3(2^k-1)$$

$$= 3! \sum_{\substack{k_1+k_2+k_3=k \\ k_1\geq k_2\geq k_3>0}} \frac{k!}{k_o!\ k_1!\ k_2!\ k_3!} + 3(2^k-1)$$

$$= 3!\ j_3(k) + 3(2^k-1).$$

Por tanto,

$$j_3(k) = \frac{1}{2}\,(3^{k-1} - 2^k + 1). \qquad \#$$

Prosigamos con la demostración del teorema. Sustituyendo $j_3(k)$ por su valor resulta que

$$G_1^*(n) = 3! \sum_{k=3}^{r} (-1)^{k+1} j_3(k)\ \sigma_k(2(1+p_1)^{-1},\ldots,\ 2(1+p_r)^{-1})$$

$$= 3!\ \{\ \frac{1}{6} \sum_{k=3}^{r}(-1)^{k-1}\ \sigma_k(6(1+p_1)^{-1},\ldots,\ 6(1+P_r)^{-1})$$

$$- \frac{1}{2} \sum_{k=3}^{r}(-1)^{k+1}\ \sigma_k(4(1+p_1)^{-1},\ldots,\ 4(1+p_r)^{-1})$$

$$+ \frac{1}{2} \sum_{k=3}^{r}(-1)^{k+1}\ \sigma_k(2(1+p_1)^{-1},\ldots,\ 2(1+p_r)^{-1})\}\ (*)$$

Los últimos términos se pueden transformar mediante

$$P_j = \prod_{i=1}^{r} (1 - \frac{2j}{1+P_i})$$

$$= 1-2_j\ \sigma_1((1+p_1)^{-1},\ldots,(1+p_r)^{-1}) + (2_j)^2\ \sigma_2((1+p_1)^{-1},\ldots,(1+p_r)^{-1}) +$$

$$+ \ldots + (-1)^r\ (2_j)^r\ \sigma_k((1+p_1)^{-1},\ldots,(1+p_r)^{-1});$$

es decir para j=1,2,3 se obtiene

$$\sum_{k=3}^{r}(-1)^{k+1}\ \sigma_k(\frac{2j}{1+p_1},\ldots,\frac{2j}{1+p_r})$$

$$= 1-2j \sum_{i=1}^{r}(1+p_i)^{-1} + (2j)^2 \sum_{1\le i<\ell\le r} (1+p_i)^{-1}\ (1+p_\ell)^{-1} - P_j.$$

Sustituyendo este valor en (*) se obtiene el resultado deseado:

$$G_1^*(n) = 3!\ \{\frac{1}{6} - \frac{1}{2}\ P_1 + \frac{1}{2}\ P_2 - \frac{1}{6}\ P_3\}$$

$$= 1 - 3P_1 + 3P_2 - P_3\ .\qquad \#$$

Procedemos a continuación a evaluar $G_2^*(n)$.

Teorema 3.28. Sea $n \not\equiv 7 (\text{mód } 8)$ un entero impar libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Entonces:

i) $S_2^{*'}(n) = 3 - 6P_1 + 3P_2$,

ii) $G_2^*(n) = 1 - 3P_2 + 2P_3$.

Demostración.

i) El teorema 3.9 permite escribir:

$$S_2^{*'}(n) = 3 \sum_{\substack{1<a_i|m \\ (a_1,a_2)=1}} \mu(a_1a_2) \prod_{p|a_1a_2} 2(1+p)^{-1}.$$

Para evaluar esta suma agrupamos previamente todos aquéllos sumandos que difieren entre sí por una permutación de a_1 y a_2 y que, por tanto, son iguales.

Tenemos:

$$\sum_{\substack{1<a_i|m \\ (a_1,a_2)=1}} = 2 \sum_{(1)}$$

en donde el sumatorio (1), que indica un modo de seleccionar un representante de cada família de las parejas anteriores, está sujeto a las condiciones:

$a_i | m$, $i = 1,2$;

$\omega(a_1) \geq \omega(a_2) \geq 1$;

si $\omega(a_1) = \omega(a_2)$ entonces $a_1 > a_2$;

$(a_1, a_2) = 1$.

Si escribimos $\omega(a_i) = k_i$, $i = 1,2$, con $k = k_1 + k_2$ y $2 \leq k \leq r$; se tiene que

$$S_2^{*'}(n) = 3! \sum_{k=2}^{r} (-1)^k \sum_{(2)} \sum_{(3)} \prod_{j=1}^{k} 2(1+p_{ij})^{-1},$$

estando sujeto el sumatorio (2) a las condiciones:

$k_1 + k_2 = k$;

$k_1 \geq k_2 \geq 1$;

si $k_1 = k_2$ entonces $a_1 > a_2$;

$(a_1, a_2) = 1$.

El sumatorio (3) está extendido a todas las posibilidades de escoger 2 subconjuntos disjuntos de $\{p_1, \ldots, p_r\}$ de cardinales respectivos k_1 y k_2. Procediendo igual que en el teorema 3.26 se obtiene que este tercer sumatorio se puede escribir de la siguiente forma

$$\sum_{C_k^r} \sum_{(4)} \prod_{j=1}^{k} (1+p_{ij})^{-1},$$

con el sumatorio (4) indicando que se tiene que sumar tantas veces como modos distintos haya de repartir k primos en dos subconjuntos disjuntos de k_1 y k_2 elementos.

Como $\prod_{j=1}^{k} (1+p_{ij})^{-1}$ no depende del reparto de los k pri-

mos, se tiene

$$\sum_{C_k^r} \sum_{(4)} \prod_{j=1}^{k} (1+p_{ij})^{-1} = \left(\sum_{C_k^r} \prod_{j=1}^{k} (1+p_{ij})^{-1} \right) \left(\sum_{(4)} 1 \right),$$

y escribimos

$$j_2(k) := \sum_{(4)} 1 = \frac{k!}{k_o!\, k_1!\, k_2!} ,$$

en donde k_o indica el número de igualdades que hay en $k_1 \geq k_2$, más una unidad.

Como por otra parte, es obvio que $\sum_{(2)}$ y $\sum_{C_k^r}$ se pueden permutar, se tiene que procediendo como en el teorema 3.26

$$S_2^{*'}(n) = 3! \sum_{k=2}^{r} (-1)^k \sigma_k \left(2(1+p_1)^{-1}, \ldots, 2(1+p_r)^{-1}\right) j_2(k).$$

Procediendo análogamente al lema 3.27 se obtiene

$$j_2(k) = 2^{k-1} - 1.$$

Por tanto,

$$S_2^{*'}(n) = 3!/2 \sum_{k=2}^{r} (-1)^k \sigma_k \left(4(1+p_1)^{-1}, \ldots, 4(1+p_r)^{-1}\right)$$

$$- 3! \sum_{k=2}^{r} (-1)^k \sigma_k \left(2(1+p_1)^{-1}, \ldots, 2(1+p_r)^{-1}\right)$$

$$= 3 - 6P_1 + 3P_2.$$

ii) $G_2^*(n) = S_2^{*'}(n) - 2S_3^{*'}(n) = 3 - 6P_1 + 3P_2 -$

$$- 2 + 6P_1 - 6P_2 + 2P_3$$

$$= 1 - 3P_2 + 2P_3 . \quad \#$$

Procedemos a continuación a efectuar los cálculos para $G_3^*(n)$.

Teorema 3.29. Sea $n \not\equiv 7 (\text{mód } 8)$ un entero impar libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Entonces:

i) $S_1^{*'}(n) = 3 - 3P_1$,

ii) $G_3^*(n) = 1 - P_3$.

Demostración.

i) Recordemos (cf. teorema 3.9) que:

$$S_1^{*'}(n) = 3 \sum_{1<a|m} - \mu(a) \prod_{p|a} 2(1+p)^{-1}.$$

Si escribimos $\omega(a) = k \geq 1$, se tiene que

$$S_1^{*'}(n) = 3 \sum_{k=1}^{r} (-1)^{k+1} \prod_{j=1}^{k} 2(1+p_{ij})^{-1}$$

$$= 3 \sum_{k=1}^{r} (-1)^{k+1} \sigma_k(2(1+p_1)^{-1}, \ldots, 2(1+p_r)^{-1})$$

$$= 3 - 3P_1.$$

ii) $G_3^*(n) = S_1^{*'}(n) - S_2^{*'}(n) + S_3^{*'}(n)$

$$= 1 - P_3. \quad \#$$

Observemos que en todos estos casos es $G_i^*(n) = G_i^*(m)$,

pues en realidad las expresiones $S_i^*(n)$ sólo dependen de $m = p_1 \cdots p_r$, con $p_i \equiv 1 (\text{mód } 4)$.

§9. Fórmulas exactas para $G_i^*(n)$, en el caso n par

Sea $n \not\equiv 0,4 (\text{mód } 8)$ un entero par libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Escribiremos $n = 2mt$, con

$m = p_1 \cdots p_r, \quad p_i \equiv 1 (\text{mód } 4);$

$t = q_1^{\beta_1} \cdots q_s^{\beta_s}, \quad q_j \equiv 3 (\text{mód } 4).$

Teorema 3.30. Sea $n \not\equiv 0,4 (\text{mód } 8)$ un entero par libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Entonces

$$G_1^*(n) = S_3^{*'}(n) = 1 - 2P_1 + P_2.$$

Demostración. Por el §7. Cap. III tenemos que

$$G_1^*(n) = \sum_{\substack{1<a_i \mid m \\ (a_1,a_2)=1}} \mu(a_1 a_2) \prod_{p \mid a_1 a_2} 2(1+p)^{-1}.$$

Procediendo como en el teorema 3.28 se obtiene que

$G_1^* = 1 - 2P_1 + P_2.$ #

Teorema 3.31. Sea $n \not\equiv 0,4 (\text{mód } 8)$ un entero par libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Entonces

i) $S_2^{*'}(n) = 2 - 2P_1$.

ii) $G_2^*(n) = 1 - P_2$.

Demostración.

i) Por el §7, Cap. III, tenemos que

$$S_2^{*'}(n) = 2 \sum_{1<a|m} - \mu(a) \prod_{p|a} 2(1+p)^{-1}.$$

Procediendo exactamente igual como en el teorema 3.29, se obtiene

$S_2^{*'}(n) = 2 - 2P_1$.

ii) $G_2^*(n) = S_2^{*'}(n) - S_3^{*'}(n) = 1 - P_2$. #

Igual que en el caso impar se tiene que $G_i^*(n) = G_i^*(m)$, pues las sumas $S_i^*(n)$ sólo dependen de m.

CAPITULO IV

ACOTACION DEL TERMINO PRINCIPAL

En este capítulo se determinan, en primer lugar, los enteros n para los que $G_i(n) < 1$, para i = 1,2,3. Ahora bien, esta acotación del término principal no es suficiente para la posterior evaluación del "término de error" $g_i(n) - G_i(n)$; hace falta además, dado un entero $n = p_1^{\alpha_1}...p_k^{\alpha_k}$, disponer de acotaciones de $G_i(n)$ uniformes respecto de la suma $\alpha = \alpha_1+...+\alpha_k$. Ello se lleva a cabo en los teoremas 4.6 , 4.9 , 4.11 y 4.14.

Asimismo se determinan los enteros $n = 2^{\alpha}mt$ para los que $G_i^*(n) < 1$, para i = 1,2,3. Puesto que $G_i^*(n) = G_i^*(m)$, la acotación es automáticamente uniforme en t.

La acotación de $G_i(n)$ se consigue mediante las fórmulas recurrentes del capítulo III y la de $G_i^*(n)$ mediante las fórmulas exactas del mismo capítulo.

§1. Acotación uniforme de $G_i(p^{\alpha})$.

Vamos a ver que para todo primo $p \neq 2$ y para todo $\alpha \geq 1$ se puede dar una cota, menor que 1 , de $G_i(p^{\alpha})$, independiente de α .

Para ello empezamos por explicitar los valores de $\partial'_p(\alpha)$, $\partial'_{p^2}(\alpha)$.

Recordemos que (corolario 3.23)

$$G_1(p^\alpha) = \partial'_{p^2}(\alpha) \quad ,$$

$$G_2(p^\alpha) = \partial'_{p^2}(\alpha) \quad ,$$

$$G_3(p^\alpha) = 3\partial'_p(\alpha) - 2\partial'_{p^2}(\alpha) \quad .$$

Proposición 4.1.

i) Para todo entero primo $p \neq 2$ y para todo $\alpha \geq 0$ es

$$\partial'_p(2\alpha+1) = \begin{cases} \dfrac{3p^{\alpha+1} - p^\alpha - p - 1}{(p+1)(p^{\alpha+1}-1)} & , \text{ si } p \equiv 1 \pmod 4; \\ \dfrac{p^\alpha - 1}{p^{\alpha+1} - 1} & , \text{ si } p \equiv 3 \pmod 4. \end{cases}$$

ii) Si n es un entero $n \not\equiv 0,4 \pmod 8$, $p \nmid n$ y $(\frac{n}{p}) = -1$, entonces para todo $\alpha \geq 1$ resulta :

$$\partial'_p(n,2\alpha) = \begin{cases} \dfrac{3p^\alpha - p^{\alpha-1} - 2}{p^{\alpha+1} + p^\alpha - 2} & , \text{ si } p \equiv 1 \pmod 4; \\ \dfrac{1}{p} & , \text{ si } p \equiv 3 \pmod 4 \quad . \end{cases}$$

iii) Si $n \geq 1$ es un entero $n \not\equiv 0,4 \pmod 8$ $p \nmid n$ y $(\frac{n}{p}) = 1$, entonces para todo $\alpha \geq 1$ resulta :

$$\partial'_p(n,2\alpha) = \begin{cases} \dfrac{p^{7\alpha}(3p^2+2p-1) + p^{4\alpha}(-8\alpha p^2+8\alpha+4) - 4}{(p+1)^2\, p^{7\alpha+1}} \\ \text{si } p \equiv 1 \pmod 4 \ ; \\ \dfrac{p^{\alpha} + p^{\alpha-1} - 2}{p^{\alpha+1} + p^{\alpha} - 2} \quad , \text{ si } p \equiv 3 \pmod 4. \end{cases}$$

Demostración.

i) Si $p \equiv 1 \pmod 4$, por la proposición 3.8 se tiene que $\partial_p(p^{2\alpha+1}, \langle p^2,1,1\rangle) = p^{-(\alpha+1)}(3\, p^{\alpha+1} - p^{\alpha} - p - 1)$, y como

$$\partial'_p(2\alpha+1) = \frac{\partial_p(p^{2\alpha+1}, \langle p^2,1,1\rangle)}{p\ \partial_p(p^{2\alpha+1}, I_3)} \quad ,$$

resulta

$$\partial'_p(2\alpha+1) = \frac{p^{-(\alpha+1)}(3p^{\alpha+1} - p^{\alpha} - p - 1)}{p(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha}}\ \kappa_p(p^{2\alpha+1},\alpha))}$$

$$= \frac{p^{-(\alpha+1)}(3p^{\alpha+1} - p^{\alpha} - p - 1)}{p(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha}})}$$

$$= \frac{p^{-(\alpha+1)}(3p^{\alpha+1}-p^{\alpha}-p-1)}{p(1-p^{-2})\ \frac{(p^{\alpha+1}-1)}{p^{\alpha}(p-1)}}$$

$$= \frac{3p^{\alpha+1}-p^{\alpha}-p-1}{(p+1)(p^{\alpha+1}-1)} \ ,$$

puesto que, en este caso

$$\kappa_p(p^{2\alpha+1},\alpha) = \left(1 - (\tfrac{-p}{p})p^{-1}\right)^{-1} = 1 \ .$$

Si $p \equiv 3$ (mód 4), por la proposición 3.8 se tiene

$$\partial'_p(2\alpha+1) = \frac{p^{(p^{2\alpha+1},<p^2,1,1>)}}{p\ \partial_p(p^{2\alpha+1},I_3)}$$

$$= \frac{(p+1)\ (p^{\alpha}-1)}{p^{\alpha+1}p(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha}}\ \kappa_p(p^{\alpha},\alpha))}$$

$$= \frac{p^{\alpha}-1}{p^{\alpha+1}-1} \ ,$$

ya que en este caso $\kappa_p(p^{\alpha},\alpha) = 1$.

ii) Sabemos que

$$\partial'_p(n,2\alpha) = \frac{\partial_p(np^{2\alpha},<p^2,1,1>)}{p\ \partial_p(np^{2\alpha},I_3)} \quad ,$$

y ésto, según la proposición 3.10, es

$$\frac{3p^{\alpha}-p^{\alpha-1}-2}{p^{\alpha}p(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha}}\ \kappa_p(np^{2\alpha},\alpha))}$$

si $p \equiv 1(\text{mód } 4)$,

siendo $\kappa_p(np^{2\alpha},\alpha)=(1-(\frac{-n}{p})\frac{1}{p})^{-1} = \frac{p}{p+1}$, por ser $p \equiv 1(\text{mód } 4)$ y $(\frac{n}{p}) = -1$.

Por tanto, basta sustituir el valor de $\kappa_p(np^{2\alpha},\alpha)$ en la expresión anterior de $\partial'_p(n,2\alpha)$ para obtener el resultado enunciado.

Si $p \equiv 3(\text{mód } 4)$, según la proposición 3.10, es

$$\partial'_p(n,2\alpha) = \frac{(1+p^{-1})}{p(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha}}\ \kappa_p(np^{2\alpha},\alpha))} \quad ,$$

siendo, ahora, $\kappa_p(np^{2\alpha},\alpha) = \frac{p}{p-1}$. Para obtener el resultado enunciado basta sustituir $\kappa_p(np^{2\alpha},\alpha)$ por su valor.

iii) De $\partial'_p(n,2\alpha) = \frac{\partial_p(np^{2\alpha},<p^2,1,1>)}{p\ \partial_p(np^{2\alpha},I_3)}$,

teniendo en cuenta el Cor.3.14 se tiene que ,

si $p \equiv 3\ (4)$ entonces

$$\partial'_p(n,2\alpha) = \frac{(p^{\alpha}+p^{\alpha-1}-2)}{p^{\alpha}p(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha}}\ \kappa_p(np^{2\alpha},\alpha))}\ ,$$

con $\kappa_p(np^{2\alpha},\alpha) = (1-(\frac{-n}{p})\ \frac{1}{p})^{-1}$.

En este caso es $(\frac{n}{p}) = 1$, de donde $(\frac{-n}{p}) = -1$ al ser $p \equiv 3(\text{mód } 4)$. Por tanto

$$\kappa_p(np^{2\alpha},\alpha) = \frac{p}{p+1}\ .$$

Entonces

$$\partial'_p(n,2\alpha) = \frac{p^{\alpha}+p^{\alpha-1}-2}{p^{\alpha-1}(p^2-1)(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha-1}}+\frac{1}{p^{\alpha-1}(p+1)})}$$

$$= \frac{p^{\alpha}+p^{\alpha-1}-2}{p^{\alpha+1}+p^{\alpha}-2}\ .$$

Ahora bien si $p \equiv 1(\text{mód } 4)$ por el Cor.3.14 se tiene

$$\partial'_p(n,2\alpha) = \frac{3p^{7\alpha+2}+2p^{7\alpha+1}-p^{7\alpha}-8\alpha p^{4\alpha+2}+(8\alpha+4)p^{4\alpha}-4}{(p+1)p^{7\alpha+1}p(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha}}\ \kappa_p(np^{2\alpha},\alpha))}\ ,$$

siendo $\kappa_p(np^{2\alpha},\alpha) = \frac{p}{p-1}$, al ser $p \equiv 1(\text{mód } 4)$.

Basta sustituir $\kappa_p(np^{2\alpha},\alpha)$ para obtener el resultado enunciado. #

Proposición 4.2.

i) Para todo entero primo $p \neq 2$ y para todo $\alpha \geq 0$ es

$$\partial'_{p^2}(2\alpha+1) = \frac{p^{\alpha} - 1}{p^{\alpha+1}-1} .$$

ii) Para todo entero primo $p \neq 2$ y para todo $\alpha \geq 1$ es

$$\partial'_{p^2}(2\alpha) = \begin{cases} \frac{1}{p} , \text{ si } p \equiv 1(\text{mód } 4) , \\ \\ \frac{p^{\alpha}+p^{\alpha-1}-2}{p^{\alpha+1}+p^{\alpha}-2} , \text{ si } p \equiv 3(\text{mód } 4). \end{cases}$$

Demostración.

i) Recordemos (proposición 3.20) que

$$\partial'_{p^2}(2\alpha+1) = \frac{\partial_p(p^{2\alpha-1}, I_3)}{p\ \partial_p(p^{2\alpha+1}, I_3)} ,$$

por tanto

$$\partial'_{p^2}(2\alpha+1) = \frac{(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha-1}})}{p(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha}})} = \frac{p^{\alpha} - 1}{p^{\alpha+1} - 1} .$$

ii) Se verifica que (proposición 3.20)

$$\partial'_{p^2}(2\alpha) = \frac{\partial_p(p^{2\alpha-2}, I_3)}{p\ \partial_p(p^{2\alpha}, I_3)} ,$$

por tanto,

$$\partial'_{p^2}(2\alpha) = \frac{(1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha-1}}\kappa_p(p^{2\alpha-2},\alpha-1)}{p\ (1-p^{-2})(1+\frac{1}{p}+\ldots+\frac{1}{p^{\alpha}}\kappa_p(p^{2\alpha},\alpha)} .$$

Si $p \equiv 1 (\text{mód } 4)$, entonces

$\kappa_p(p^{2\alpha-2},\alpha-1) = \kappa_p(p^{2\alpha},\alpha) = \frac{p}{p-1}$ y por tanto $\partial'_{p^2}(2\alpha) = \frac{1}{p}$.

Si $p \equiv 3 (\text{mód } 4)$, entonces

$\kappa_p(p^{2\alpha-2},\alpha-1) = \kappa_p(p^{2\alpha},\alpha) = \frac{p}{p+1}$ y basta sustituir para obtener el resultado enunciado. #

Proposición 4.3. Si $p = 2$, se verifica

i) $\partial'_2(1) = 1/3$.

ii) $\partial'_{2^2}(1) = 0$.

Demostración. Se verifica

$$\partial'_2(1) = \frac{\partial_2(2,\langle 2^2,1,1\rangle)}{2\ \partial_2(2,I_3)} ,$$

siendo $\partial_2(2,<2^2,1,1>) = 1$, (cf. corolario 3.16)

y

$$\partial_2(2,I_3) = 3/2 \quad , \text{ (cf. corolario 3.3).}$$

Basta considerar los cálculos precedentes para obtener el siguiente

Lema 4.4. Para todo $p \neq 2$ y para todo $\alpha \geq 1$, se verifica:

i) $0 \leq \partial'_p(n,\alpha) < 1$.

ii) $0 \leq \partial'_{p^2}(n,\alpha) \leq \frac{1}{p} < 1$.

iii) $\partial'_{p^2}(n,\alpha) \leq \partial'_p(n,\alpha)$.

iv) $0 \leq 3\,\partial'_p(n,\alpha) - 2\,\partial'_{p^2}(n,\alpha) \leq 1$.

v) $2\partial'_p(n,\alpha) < 1 + \partial'_{p^2}(n,\alpha)$.

Demostración.

i) , ii) Inmediatas.

iii) Si $v_p(n) = 2\alpha+1$, y $p \equiv 1(\text{mód } 4)$, entonces:

$$\partial'_{p^2}(2\alpha+1) = \frac{p^\alpha - 1}{p^{\alpha+1} - 1} \quad , \qquad \partial'_p(2\alpha+1) = \frac{3p^{\alpha+1}-p^\alpha-p-1}{(p+1)(p^{\alpha+1}-1)}$$

y $\partial'_{p^2}(2\alpha+1) < \partial'_{p}(2\alpha+1)$, ya que $p > 1$.

Si $v_p(n) = 2\alpha+1$, y $p \equiv 3(\text{mód } 4)$, entonces (proposición 4.1 y 4.2)

$$\partial'_{p^2}(2\alpha+1) = \partial'_{p}(2\alpha+1) \quad .$$

Si $v_p(n) = 2\alpha$, $(\frac{n}{p}) = -1$ y $p \equiv 1(\text{mód } 4)$, entonces

$$\partial'_{p^2}(n,2\alpha) = \frac{1}{p} \quad ; \quad \partial'_{p}(n,2\alpha) = \frac{3p^{\alpha} - p^{\alpha-1} - 2}{p^{\alpha+1} + p^{\alpha} - 2} \quad ,$$

y evidentemente $\partial'_{p^2}(n,2\alpha) < \partial'_{p}(n,2\alpha)$.

Si $v_p(n) = 2\alpha$, $(\frac{n}{p}) = -1$ y $p \equiv 3(\text{mód } 4)$, entonces

$$\partial'_{p^2}(n,2\alpha) = \frac{p^{\alpha} + p^{\alpha-1} - 2}{p^{\alpha+1} + p^{\alpha} - 2} \quad , \quad \partial'_{p}(n,2\alpha) = \frac{1}{p} \quad ,$$

y $\partial'_{p^2}(n,2\alpha) < \partial'_{p}(n,2\alpha)$, ya que $p > 1$.

Si $v_p(n) = 2\alpha$, $(\frac{n}{p}) = 1$, y $p \equiv 1$ (mód 4) , entonces (proposiciones 4.1 y 4.2) evidentemente es

$$\partial'_{p^2}(n,2\alpha) < \partial'_{p}(n,2\alpha) \quad ;$$

y en el caso $p \equiv 3(\text{mód } 4)$, es

$$\partial'_{p^2}(n,2\alpha) = \partial'_{p}(n,2\alpha) \quad .$$

iv) Vamos a distinguir como en el apartado iii) los diferentes casos que se presentan:

Si $v_p(n) = 2\alpha+1$, y $p \equiv 1 (\text{mód } 4)$,

$$3\,\partial'_p(2\alpha+1) - 2\,\partial'_{p^2}(2\alpha+1) = \frac{7\,p^{\alpha+1} - 5p^{\alpha} - p - 1}{(p+1)(p^{\alpha+1} - 1)} ,$$

Si $p = 5$,

$$3\,\partial'_5(2\alpha+1) - 2\,\partial'_{5^2}(2\alpha+1) = \frac{7\cdot 5^{\alpha+1} - 5^{\alpha+1} - 6}{6\,(5^{\alpha+1} - 1)} = 1 .$$

Si $p > 5$, se tiene,

$$\frac{7\,p^{\alpha+1} - 5p^{\alpha} - p - 1}{(p+1)(p^{\alpha+1} - 1)} < \frac{7(p^{\alpha+1} - 1)}{(p+1)(p^{\alpha+1} - 1)} \leq \frac{7}{14} = \frac{1}{2} ,$$

pues,

$$7p^{\alpha+1} - 5p^{\alpha} - p - 1 < 7p^{\alpha+1} - p - 1 < 7p^{\alpha+1} - 7 = 7(p^{\alpha+1} - 1).$$

Si $v_p(n) = 2\alpha+1$, y $p \equiv 3 (\text{mód } 4)$, entonces,

$$3\,\partial'_p(2\alpha+1) - 2\,\partial'_{p^2}(2\alpha+1) = \frac{p^{\alpha} - 1}{p^{\alpha+1} - 1} < \frac{1}{p} ,$$

luego se verifica el resultado enunciado.

Si $v_p(n) = 2\alpha$, $\left(\frac{n}{p}\right) = -1$, y $p \equiv 1 (\text{mód } 4)$,

$$3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha) = \frac{7p^{\alpha+1} - 3p^{\alpha} - 8p + 4}{p(p^{\alpha+1} + p^{\alpha} - 2)} ,$$

que evidentemente verifica $0 \leq 3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha) < 1$,

además si $p \geq 13$, se puede conseguir la siguiente cota:

$$\frac{7\,p^{\alpha+1} - 3\,p^{\alpha} - 8\,p+4}{p\,(p^{\alpha+1} + p^{\alpha} - 2)} \leq \frac{7}{13} ,$$

ya que al ser $7\,p^{\alpha+1} - 3\,p^{\alpha} - 8\,p+4 < 7\,p^{\alpha+1}$ y $p^{\alpha} - 2 > 0$

se obtiene

$$\frac{7\,p^{\alpha+1} - 3\,p^{\alpha} - 8\,p+4}{p(p^{\alpha+1} + p^{\alpha} - 2)} < \frac{7\,p^{\alpha+1}}{p\,p^{\alpha+1}} \leq \frac{7}{13} , \text{ si } p \geq 13.$$

Si $v_p(n) = 2\alpha$, $(\frac{n}{p}) = -1$, $p \equiv 3 (\text{mód } 4)$, entonces:

$$3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha) = \frac{p^{\alpha+1} + p^{\alpha} + 4p-6}{p(p^{\alpha+1} + p^{\alpha} - 2)} ,$$

por un lado es

$$\frac{p^{\alpha+1} + p^{\alpha} - 6}{p(p^{\alpha+1} + p^{\alpha}-2)} < \frac{1}{p} \leq \frac{1}{3} ;$$

además

$$\frac{4p}{p(p^{\alpha+1} + p^{\alpha}-2)} = \frac{4}{p^{\alpha+1} + p^{\alpha} -2} \leq \frac{4}{10} , \text{ pues } p \geq 3 .$$

Así que

$$0 \leq 3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha) \leq \frac{11}{15} \ .$$

Si $v_p(n) = 2\alpha$, $(\frac{n}{p}) = 1$ y $p \equiv 1 (\text{mód } 4)$, se verifica:

$$3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha) =$$

$$= 3 \cdot \left(\frac{3p^{7\alpha+2} + 2p^{7\alpha+1} - p^{7\alpha} - 8\alpha p^{4\alpha+2} + (8\alpha+4)p^{4\alpha} - 4}{(p+1)^2\, p^{7\alpha+1}} \right) - \frac{2}{p} \ .$$

Por tanto,

$$3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha) = \frac{9p^{7\alpha+2} + 6p^{7\alpha+1} - 3p^{7\alpha}}{(p+1)^2\, p^{7\alpha+1}} - \frac{24\alpha}{(p+1)^2\, p^{3\alpha-1}}$$

$$+ \frac{24\alpha + 12}{(p+1)^2\, p^{3\alpha+1}} - \frac{12}{(p+1)^2\, p^{7\alpha+1}} - \frac{2}{p} \ .$$

Agrupando el primer sumando y el último resulta que el valor de $3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha)$ es

$$\frac{7p^2 + 2p - 5}{p(p+1)^2} - \frac{24\alpha}{(p+1)^2\, p^{3\alpha-1}} + \frac{24\alpha + 12}{(p+1)^2\, p^{3\alpha+1}} - \frac{12}{(p+1)^2\, p^{7\alpha+1}} \ .$$

Ahora bien, si $p = 5$, se obtiene

$$\frac{7p^2 + 2p - 5}{p(p+1)^2} = \frac{7\cdot 5^2 + 5}{5\cdot 36} = 1 \quad ,$$

y como la contribución de los sumandos restantes es negativa resulta que

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

Si $p \equiv 1 (\text{mód } 4)$ y $p \geq 13$, entonces :

$\frac{7p^2 + 2p - 5}{p(p+1)^2} < \frac{1}{2}$, pues esta desigualdad se verifica para $p = 13$ y se trata de una función decreciente en p . En resumen, si $p \equiv 1 (\text{mód } 4)$, $p \geq 13$, resulta

$$3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha) \leq \frac{1}{2} + \frac{24\alpha + 12}{p^{3\alpha+1}(p+1)^2} < \frac{1}{2} + \frac{2\alpha + 1}{p^{3\alpha+1}(p+1)},$$

y como $2\alpha+1$ es menor que $p^{3\alpha+1}$, para todo $\alpha \geq 1$ y $p \geq 13$, resulta que

$$3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha) < \frac{1}{2} + \frac{1}{14} = \frac{4}{7} < 1 \ .$$

Si $\beta = 2\alpha$, $(\frac{n}{p}) = 1$, y $p \equiv 3 (\text{mód } 4)$, se tiene

$$3\,\partial'_p(n,2\alpha) - 2\,\partial'_{p^2}(n,2\alpha) = \frac{p^\alpha + p^{\alpha-1} - 2}{p^{\alpha+1} + p^\alpha - 2} < \frac{1}{p} \quad ,$$

que verifica claramente las condiciones del enunciado.

v) Si $v_p(n) = 2\alpha+1$, y $p \equiv 1 (\text{mód } 4)$,

$$2\,\partial'_p(2\alpha+1) = \frac{6\,p^{\alpha+1} - 2\,p^{\alpha} - 2p - 2}{(p+1)\,(p^{\alpha+1} - 1)} \quad ,$$

$$1 + \partial'_{p^2}(2\alpha+1) = \frac{p^{\alpha+1} + p^{\alpha} - 2}{p^{\alpha+1} - 1} \quad ,$$

y claramente

$$2\,\partial'_p(2\alpha+1) < 1 + \partial'_{p^2}(2\alpha+1) \quad ,$$

ya que $4p < p^2 + 3$, para todo $p \equiv 1 (\text{mód } 4)$.

Si $v_p(n) = 2\alpha+1$, y $p \equiv 3 (\text{mód } 4)$,

$$2\,\partial'_p(2\alpha+1) = \frac{2\,p^{\alpha} - 2}{p^{\alpha+1} - 1} \quad ,$$

$$1 + \partial'_{p^2}(2\alpha+1) = \frac{p^{\alpha+1} + p^{\alpha} - 2}{p^{\alpha+1} - 1} \quad ,$$

y como $p > 1$, se verifica la desigualdad deseada.

Si $v_p(n) = 2\alpha$, $(\frac{n}{p}) = -1$ y $p \equiv 1 (\text{mód } 4)$,

$$2\,\partial'_p(n,2\alpha) = \frac{6\,p^{\alpha} - 2\,p^{\alpha-1} - 4}{p^{\alpha+1} + p^{\alpha} - 2} \quad ,$$

$$1 + \partial'_{p^2}(n,2\alpha) = \frac{p+1}{p} ,$$

y al ser $p \equiv 1 (\text{mód } 4)$, se verifica $p^{\alpha+2} > 4\, p^{\alpha+1}$ y por tanto se tiene la desigualdad enunciada.

Si $v_p(n) = 2\alpha$, $(\frac{n}{p}) = -1$ y $p \equiv 3 (\text{mód } 4)$

$$2\,\partial'_{p}(n,2\alpha) = \frac{2}{p} ,$$

$$1 + \partial'_{p^2}(n,2\alpha) = \frac{p^{\alpha+1} + 2p^{\alpha} + p^{\alpha-1} - 4}{p^{\alpha+1} + p^{\alpha} - 2} ,$$

y se verifica la desigualdad deseada ya que $p^{\alpha+2} > p^{\alpha} + 4p$.

Si $v_p(n) = 2\alpha$, $(\frac{n}{p}) = 1$ y $p \equiv 1 (\text{mód } 4)$,

$$2\,\partial'_{p}(n,2\alpha) = 2 \cdot \left(\frac{p^{7\alpha}(3p^2 + 2p - 1) + p^{4\alpha}(-8\alpha p^2 + 8\alpha + 4) - 4}{(p+1)^2\, p^{7\alpha+1}} \right)$$

$$1 + \partial'_{p^2}(n,2\alpha) = \frac{p+1}{p} ,$$

al comparar estas cantidades se llega a que

$2\,\partial'_{p}(n,2\alpha) < 1 + \partial'_{p^2}(n,2\alpha)$ si y sólo si

$$3\, p^{7\alpha+2} + p^{7\alpha+1} + (16\alpha+8)\, p^{4\alpha} < p^{7\alpha+3} + 3p^{7\alpha} + 16\alpha\, p^{4\alpha+2} + 4 ,$$

lo cual es cierto, ya que al ser $p^2 > 3p+1$ se verifica que

$$p^{7\alpha+3} + 3p^{7\alpha} > 3p^{7\alpha+2} + p^{7\alpha+1}$$

Si $v_p(n) = 2\alpha$, $(\frac{n}{p}) = 1$ y $p \equiv 3 (\text{mód } 4)$,

$$2\ \partial'_p(n,2\alpha) = \frac{2\ p^{\alpha} + 2\ p^{\alpha-1} - 4}{p^{\alpha+1} + p^{\alpha} - 2} ,$$

$$1 + \partial'_{p^2}(n,2\alpha) = \frac{p^{\alpha+1} + 2\ p^{\alpha} + p^{\alpha-1} - 4}{p^{\alpha+1} + p^{\alpha} - 2} ,$$

y evidentemente es $2\ \partial'_p(n,2\alpha) < 1 + \partial'_{p^2}(n,2\alpha)$. #

Proposición 4.5. Para todo entero primo $p \neq 2,5$ y para todo $\alpha \geq 1$ es :

i) $0 \leq G_i(p^{\alpha}) < 1$, para $i = 1,2,3$.

ii) $G_1(p^{\alpha}) = G_2(p^{\alpha}) \leq G_3(p^{\alpha})$.

iii) Si $p = 5$, entonces

$G_3(5^{2\alpha+1}) = 1$, $G_3(5^{2\alpha}) < 1$.

Demostración.

i), iii) Basta tener presentes los resultados y la demostración del lema 4.4.

ii) Recordemos que $G_1(p^{\alpha}) = \partial'_{p^2}(\alpha)$, y que $G_2(p^{\alpha}) = \partial'_{p^2}(\alpha)$, por tanto es

$$G_1(p^{\alpha}) = G_2(p^{\alpha}) .$$

Además, al ser $G_3(p^\alpha) = 3\,\partial'_p(\alpha) - 2\,\partial'_{p^2}(\alpha)$, resulta que

$G_2(p^\alpha) \leq G_3(p^\alpha)$ si y sólo si $\partial'_{p^2}(\alpha) \leq \partial'_p(\alpha)$, lo cual es cierto (corolario 4.4). #

Hemos probado que para todo primo $p \neq 2,5$ es $G_i(p^\alpha) < 1$, para $i = 1,2,3$; y si $p = 5$ que $G_i(5^\alpha) < 1$, para $i = 1,2,3$ si α par y $G_i(5^\alpha) < 1$, para $i = 1,2$, si α es impar.

Ahora bien, para la estimación de la diferencia $g_i(p^\alpha) - G_i(p^\alpha)$ ésto no es suficiente. Por ello pasamos a probar que se puede conseguir una acotación uniforme:

Teorema 4.6.

i) Para todo entero primo impar, $p \neq 5$, existe una constante $c_i = c_i(p)$ tal que

$$G_i(p^\alpha) \leq c_i < 1 \ , \ i = 1,2,3 \ ,$$

para todo $\alpha \geq 1$.

ii) Si $p = 5$, existe una constante $c_i = c_i(5)$ tal que

$$G_i(5^\alpha) \leq c_i < 1 \ , \quad i = 1,2 \ ,$$

para todo $\alpha \geq 1$.

iii) Si $p = 2$, se tiene

$$G_i(2) = 0 \ , \ G_2(2) = 0 \ , \ G_3(2) = 1 \ .$$

Demostración.

i) y ii) Según el lema 4.4, ii), sabemos que

$$G_i(p^\alpha) \leq \frac{1}{p} < 1 \text{ , para } i = 1,2 \text{ ,}$$

por tanto podemos escoger

$$c_1(p) = c_2(p) = \frac{1}{p} \text{ .}$$

Si $p \neq 5$ también por la demostración del lema 4.4 , iv) se tiene

$$c_3 = c_3(p) = \frac{4}{7} \text{ ;}$$

y $$G_3(5^{2\alpha+1}) = \frac{7\cdot 5^{\alpha+1} - 5\cdot 5^{\alpha} - 5 - 1}{6\ (5^{\alpha+1} - 1)} = 1 \text{ .}$$

Ya que,

$$G_3(5^{2\alpha}) = 1 - \frac{24\alpha}{6^2 \cdot 5^{3\alpha-1}} + \frac{24\alpha + 12}{6^2 \cdot 5^{3\alpha+1}} - \frac{12}{6^2 \cdot 5^{7\alpha+1}} \text{ ,}$$

tenemos

$G_3(5^{2\alpha}) < 1$, pero $\lim_{\alpha\to\infty} G_3(5^{2\alpha}) = 1$,

por lo cual, en este caso, no se puede alcanzar una cota menor que 1 , independiente del exponente. Sin embargo

$$G_i(5^\alpha) \leq \frac{1}{5} < 1 \quad \text{si} \quad i = 1,2 \text{ .} \qquad \#$$

§2. Acotación uniforme de $G_i(n)$ en el caso m.c.d.(n,10) = 1

La expresión del término principal $G_i(n)$, como combinación lineal de las sumas auxiliares $S_i^!(n)$, muestra que éste es una suma alternada de $\sum_{j=4-i}^{3} (2^{\omega(n)}-1)^j$ sumandos. El lema 4.4 pone de manifiesto que todos esos sumandos son menores que 1. Vamos a ver a continuación que la *suma total* es menor que 1, generalizando así la proposición 4.5 al caso en que n tenga un número arbitrario de factores primos.

Proposición 4.7. Sea n un entero positivo impar, tal que si $5 \mid n$ entonces $v_5(n)$ es par. Se verifica:

i) $0 \leq G_3(n) < 1$,

ii) $0 \leq G_1(n) \leq G_2(n) \leq G_3(n)$.

Demostración.

i) Veamos en primer lugar que $0 \leq G_3(n) < 1$, por inducción sobre el número de factores primos distintos de n .

Si $n = p^\alpha$, $p \neq 2$, ya sabemos (proposición 4.5) que $0 \leq G_3(p^\alpha) < 1$.

Supongamos ahora cierto el resultado para enteros impa

res con a lo sumo k-1 factores primos distintos y escribamos : $n = p_1^{\alpha_1} \ldots p_{k-1}^{\alpha_{k-1}} p_k^{\alpha_k}$. Entonces por las fórmulas de recurrencia (teorema 3.22), si llamamos $m = p_1^{\alpha_1} \ldots p_{k-1}^{\alpha_{k-1}}$, se tiene que

$$G_3(n) = G_3(m) + (3\, \partial'_{p_k}(n,\alpha_k) - 2\, \partial'_{p_k^2}(n,\alpha_k))\ (1 - G_3(m)).$$

Como por hipótesis de inducción es $0 \leq G_3(m) < 1$ y por el lema 4.4, en nuestra situación, es siempre

$$0 \leq 3\, \partial'_{p_k}(n,\alpha_k) - 2\, \partial'_{p_k^2}(n,\alpha_k) < 1 ,$$

resulta pues que $0 \leq G_3(n) < 1$.

ii) Procedamos ahora a probar que $G_2(n) \leq G_3(n)$, también por inducción sobre el número de factores primos distintos de n.

Si $n = p^\alpha$, $p \neq 2$, ya sabemos (proposición 4.5) que $G_2(p^\alpha) \leq G_3(p^\alpha)$.

Sea ahora $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ y supongamos cierto el resultado para enteros impares de a lo sumo k-1 factores primos distintos. Igual que antes escribamos $m = p_1^{\alpha_1} \ldots p_{k-1}^{\alpha_{k-1}}$.

Por el teorema 3.22 tenemos que

$$G_2(n) = G_2(m) + 2\, \partial'_{p_k}(n,\alpha_k)(G_3(m) - G_2(m)) +$$

$$+ \partial'_{p_k^2}(n,\alpha_k)(1 + G_2(m) - 2\, G_3(m)) .$$

Por tanto,

$$G_3(n) - G_2(n) = G_3(m) - G_2(m) +$$

$$+ \partial'_{p_k}(n,\alpha_k)(3(1-G_3(m)) - 2(G_3(m) - G_2(m)) +$$

$$+ \partial'_{2\,p_k}(n,\alpha_k)(-3(1-G_3(m)) + (G_3(m) - G_2(m))$$

$$= (1 - 2\,\partial'_{p_k}(n,\alpha_k) + \partial'_{2\,p_k}(n,\alpha_k))(G_3(m) - G_2(m)) +$$

$$+ 3(\partial'_{p_k}(n,\alpha_k) - \partial'_{2\,p_k}(n,\alpha_k))(1 - G_3(m)) \quad .$$

En consecuencia, aplicando la hipótesis de inducción, el lema 4.4 , junto con que $G_3(m) < 1$, se obtiene que

$$G_3(n) - G_2(n) \geq 0 \ .$$

Procedamos igual para comparar $G_1(n)$ y $G_2(n)$.

Por el teorema 3.22 se tiene que:

$$G_1(n) = G_1(m) + \partial'_{p_k}(n,\alpha_k)(G_2(m) - G_1(m)) +$$

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

Por tanto, por hipótesis de inducción es $G_1(n) \geq 0$ y

$$G_2(n) - G_1(n) = G_2(m) - G_1(m) +$$

$$+ \partial'_{p_k}(n,\alpha_k)(2(G_3(m) - G_2(m)) - (G_2(m) - G_1(m)))$$

$$+ \partial'_{p_k^2}(n,\alpha_k)(-2(G_3(m) - G_2(m))$$

$$= (1 - \partial'_{p_k}(n,\alpha_k))(G_2(m) - G_1(m)) +$$

$$+ 2(\partial'_{p_k}(n,\alpha_k) - \partial'_{p_k^2}(n,\alpha_k))(G_3(m) - G_2(m)) .$$

Aplicando la hipótesis de inducción, el lema 4.4 junto con el hecho de que $G_2(m) \leq G_3(m)$, resulta que todos esos sumandos son mayores ó iguales que cero y, en consecuencia,

$$G_1(n) \leq G_2(n) .$$

En particular, se obtiene también que $G_i(n) < 1$, para $i = 1,2$. #

Procediendo análogamente se obtiene la siguiente

<u>Proposición 4.8.</u> Sea n un entero positivo impar, con $v_5(n)$ impar. Se verifica :

i) $0 \leq G_2(n) < 1$,

ii) $0 \leq G_1(n) \leq G_2(n) < G_3(n) = 1$.

Demostración. El único punto distinto a probar ahora es que $G_3(n) = 1$. Lo probaremos por inducción sobre el número de factores primos distintos de n .

Si $n = 5^{2\alpha+1}$ entonces por la proposición 4.5 se verifica que $G_3(5^{2\alpha+1}) = 1$.

Si $n = 5^{2\alpha+1}\, p^{\beta}$, por la fórmula recurrente (teorema 3.22) tenemos

$$G_3(5^{2\alpha+1}p^{\beta}) = G_3(5^{2\alpha+1}) + (3\,\partial'_p(n,\beta) - 2\,\partial'_{p^2}(n,\beta))(1-G_3(5^{2\alpha+1}))$$

$$= 1 .$$

Supongamos que la hipótesis sea cierta para enteros impares divisibles por 5 , con $v_5(n)$ impar, con a lo sumo k-1 factores primos impares distintos de 5 ; y sea

$$n = 5^{2\alpha+1}p_1^{\alpha_1}\ldots p_k^{\alpha_k}$$

Entonces :

$$G_3(n) = G_3(5^{2\alpha+1}p_1^{\alpha_1}\ldots p_{k-1}^{\alpha_{k-1}}) +$$

$$+ (3\,\partial'_{p_k}(n,\alpha_k) - 2\,\partial'_{p_k^2}(n,\alpha_k))(1 - G_3(5^{2\alpha+1}p_1^{\alpha_1}\ldots p_{k-1}^{\alpha_{k-1}})) .$$

Basta aplicar la hipótesis de inducción para obtener que $G_3(n) = 1$. #

Para poder estimar la diferencia $g_i(n) - G_i(n)$ no nos bastará con que $G_i(n) < 1$, sino que hace falta que esa cota sea independiente de los exponentes de los factores pri-

mos de n . Empezamos por dar una cota uniforme de $G_3(n)$ en el caso m.c.d.(n,10) = 1 .

Teorema 4.9. Para todo entero positivo impar $n = p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ tal que $5 \nmid n$, existe una constante $c_3 = c_3(p_1\ldots p_k)$ tal que

$$G_3(n) \leq c_3 < 1 ,$$

para todo $\alpha = \alpha_1+\ldots+\alpha_k$.

Demostración. Por inducción sobre el número de factores primos de n.

Si $n = p^{\alpha}$, $p \neq 2,5$, ya sabemos, por el teorema 4.6 , que $G_3(p^{\alpha}) \leq c_3(p) < 1$.

Supongamos ahora cierto el teorema para enteros con a lo sumo k-1 factores primos distintos, $p_i \neq 2,5$, y distingamos dos casos

1er caso. Si escribimos $n = p_1^{\alpha_1}\ldots p_k^{\alpha_k}$, consideremos ahora el caso en que α_k sea impar ó , si es par, el caso en que

$$\left(\frac{p^{-\alpha_k} n}{p_k}\right) = 1 \quad ;$$

de este modo $\partial'_p(n,\alpha_k) = \partial'_p(\alpha_k)$.

Observemos en primer lugar que, en este caso, es

$$3\,\partial'_{p_k}(\alpha_k) - 2\,\partial'_{2,p_k}(\alpha_k) = G_3(p_k^{\alpha_k}) \ ,$$

(corolario 3.23).

Por tanto, aplicando la hipótesis de inducción, la fórmula recurrente (teorema 3.22) y la acotación uniforme de $G_3(p^{\alpha})$ (teorema 4.6) se obtiene :

$$G_3(n) = G_3(p_1^{\alpha_1}\ldots p_{k-1}^{\alpha_{k-1}}\, p_k^{\alpha_k})$$

$$= G_3(p_k^{\alpha_k}) + G_3(p_1^{\alpha_1}\ldots p_{k-1}^{\alpha_{k-1}})\ (1 - G_3(p_k^{\alpha_k}))$$

$$\leq G_3(p_k^{\alpha_k}) + c_3(p_1\ldots p_{k-1})\ (1 - G_3(p_k^{\alpha_k}))$$

$$= c_3(p_1\ldots p_{k-1}) + G_3(p_k^{\alpha_k})\ (1 - c_3(p_1\ldots p_{k-1}))$$

$$\leq c_3(p_1\ldots p_{k-1}) + c_3(p_k)\ (1 - c_3(p_1\ldots p_{k-1})) \ .$$

Siendo esta última expresión menor que 1 ya que $0 \leq c_3(p_k) < 1$ y $0 \leq c_3(p_1\ldots p_{k-1}) < 1$.
Escribiremos

$$c_3(p_1\ldots p_k) := c_3(p_1\ldots p_{k-1}) + c_3(p_k)\ (1-c_3(p_1\ldots p_{k-1})) \ .$$

2º caso. Sea ahora α_k par y $\left(\frac{p_k^{-\alpha_k} n}{p_k}\right) = -1$.

Escojamos [26] el primer primo impar $q > 5$ tal que $\left(\frac{q}{p_k}\right) = -1$. Por hipótesis de inducción es

$$G_3(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}) \leq c_3(p_1\cdots p_{k-1}) < 1 .$$

Si "añadimos" el primo q con la condición anterior se obtiene, procediendo igual que en el 1er caso, que

$$G_3(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}\ q) \leq c_3(p_1\cdots p_{k-1}\ q) < 1 .$$

Ahora bien, aplicando la fórmula recurrente (teorema 3.22) y teniendo en cuenta que

$$\left(\frac{p_k^{-\alpha_k}\ n\ q}{p_k}\right) = 1 \quad ,$$

se obtiene

$$G_3(nq) = G_3(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}\ q\ p_k^{\alpha_k})$$

$$= G_3(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}\ q) +$$

$$+ (3\ \partial'_{p_k}(n,\alpha_k) - 2\ \partial'_{2,p_k}(n,\alpha_k))\,(1-G_3(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}\ q)),$$

y al ser (cf. demostración iv) corolario 4.4) :

$$0 \leq 3\ \partial'_{p_k}(n,\alpha_k) - 2\ \partial'_{2,p_k}(n,\alpha_k) \leq \frac{11}{15} \quad , \text{ se obtiene}$$

$$G_3(nq) \leq G_3(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}\ q) + \frac{11}{15}\,(1-G_3(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}\ q)) =$$

$$= \frac{11}{15} + \frac{4}{15}\, G_3(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}\, q) \leq \frac{11}{15} + \frac{4}{15}\, c_3(p_1\cdots p_{k-1}\, q) \ .$$

Así que

$$G_3(nq) = G_3(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}\, q\, p_k) \leq \tilde{c}_3(p_1\cdots p_{k-1}\, q\, p_k) < 1 \ ,$$

siendo

$$\tilde{c}_3(p_1\cdots p_{k-1}\, q\, p_k) := \frac{11}{15} + \frac{4}{15}\, c_3(p_1\cdots p_{k-1}\, q) \ .$$

Por otra parte es

$$G_3(nq) = G_3(n) + (3\partial'_q(1) - 2\partial'_{q^2}(1))\,(1 - G_3(n)) \ ,$$

y como todos estos términos son cantidades positivas o nulas se deduce que

$$G_3(n) \leq G_3(nq) \leq \tilde{c}_3(p_1\cdots p_{k-1}\, q\, p_k) < 1 \ .$$

Entonces $G_3(n) \leq c_3(p_1\cdots p_k) < 1$, siendo

$$c_3(p_1\cdots p_k) := \tilde{c}_3(p_1\cdots p_{k-1}\, q\, p_k) \ . \quad \#$$

Teniendo en cuenta que por la proposición 4.7 es

$$G_1(n) \leq G_2(n) \leq G_3(n) \ ,$$

y tomando $c_1 = c_2 = c_3$ podemos enunciar el siguiente

<u>Corolario 4.10.</u> Para todo entero positivo impar $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ tal que $5 \nmid n$, existen constantes $c_i = c_i(p_1\cdots p_k)$, tales que

$$G_i(n) \leq c_i < 1 \ , \ i = 1,2,3,$$

para todo $\alpha = \alpha_1+\ldots+\alpha_k$.

§3. Acotación uniforme de $G_i(n)$ en el caso m.c.d.$(n,10) \neq 1$

Empezaremos por acotar uniformemente $G_2(n)$ en el caso en que $2|n$ pero $4\nmid n$ y $5\nmid n$.

Teorema 4.11. Para todo entero positivo par $n = 2\, p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ tal que $n \not\equiv 0,4 (\text{mód } 8)$ y $5\nmid n$ existe una constante $c_2 = c_2(2.p_1 \ldots p_k)$ tal que

$$G_2(n) \leq c_2 < 1,$$

para todo $\alpha = \alpha_1 + \ldots + \alpha_k$.

Demostración. Recordemos (teorema 3.22) que

$$G_2(n) = G_2(m) + 2\, \partial_2'(1)\, (G_3(m) - G_2(m)),$$

en donde $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$.

Ahora bien como $\partial_2'(1) = 1/3$ y $G_3(m) < 1$, se obtiene

$$G_2(n) < G_2(m) + 2/3\, (1 - G_2(m)) = \frac{2}{3} + \frac{1}{3}\, G_2(m).$$

Aplicando el corolario 4.10 resulta que

$$G_2(n) < \frac{2}{3} + \frac{1}{3}\, c_2(p_1 \ldots p_k) =$$

$$= c_2(p_1 \ldots p_k) + \frac{2}{3}\, (1 - c_2(p_1 \ldots p_k)),$$

y como $c_2(p_1 \ldots p_k) < 1$, se obtiene que $G_2(n) < c_2(2.p_1 \ldots p_k) < 1$, siendo $c_2(2\, p_1 \ldots p_k) := \frac{2}{3} + \frac{1}{3}\, c_2(p_1 \ldots p_k)$. #

En el caso en que n sea un entero divisible por 5, par ó no, necesitamos los siguientes lemas.

Lema 4.12. Todo entero positivo par n no divisible por 4 verifica que

$$G_3(n) = 1.$$

Demostración. Por inducción sobre el número de factores primos distintos de n.

Si n = 2 entonces recordemos (teorema 4.6.) que $G_3(2) = 1$.

Si $n = 2p^{\alpha}$, por la fórmula recurrente (teorema 3.22) tenemos

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

Supongamos que la hipótesis sea cierta para enteros pares no múltiplos de 4 con a lo sumo k-1 factores primos impares distintos; y sea $n = 2\,p_1^{\alpha_1}\ldots p_k^{\alpha_k}$. Entonces:

$$G_3(n) = G_3(2\,p_1^{\alpha_1}\ldots p_{k-1}^{\alpha_{k-1}}) +$$

$$+ (3\,\partial'_{p_k}(n,\alpha_k) - 2\,\partial'_{p_k^2}(n,\alpha_k))\,(1 - G_3(2\,p_1^{\alpha_1}\ldots p_{k-1}^{\alpha_{k-1}})).$$

Basta aplicar la hipótesis de inducción para obtener que $G_3(n) = 1$. #

Lema 4.13. Para todo entero $n \not\equiv 0,4 \pmod 8$, tal que $5 \nmid n$ y para todo $\alpha \geq 1$ se tiene que

$$0 \leq 2\,\partial'_5(n,\alpha) - \partial'_{5^2}(n,\alpha) < \frac{4}{5}\,.$$

Demostración. Como siempre basta aplicar los resultados de las proposiciones 4.1 , 4.2 y distinguir los casos :

. Si $v_p(n) = 2\alpha+1$, entonces :

$$2\partial'_5(2\alpha+1) - \partial'_{5^2}(2\alpha+1) =$$

$$= \frac{6.5^{\alpha+1} - 2\cdot 5^{\alpha} - 12}{6(5^{\alpha+1} - 1)} - \frac{5^{\alpha} - 1}{5^{\alpha+1} - 1} = \frac{6\cdot 5^{\alpha+1} - 8\cdot 5^{\alpha} - 6}{6(5^{\alpha+1} - 1)} =$$

$$= 1 - \frac{4}{3}\cdot\frac{5^{\alpha}}{5^{\alpha+1} - 1} = 1 - \frac{4}{3}\cdot\frac{1}{5 - \frac{1}{5^{\alpha}}} < 1 - \frac{4}{3}\cdot\frac{1}{5} = \frac{11}{15}\,.$$

. Si $v_p(n) = 2\alpha$, y $(\frac{n}{5}) = -1$, entonces :

$$2\partial'_5(n,2\alpha) - \partial'_{5^2}(n,2\alpha) =$$

$$= \frac{6.5^{\alpha+1} - 2\cdot 5^{\alpha} - 2\cdot 5 - 2}{6(5^{\alpha+1} - 1)} - \frac{1}{5}\,.$$

Observemos que,

$$\frac{6.5^{\alpha+1} - 2\cdot 5^{\alpha} - 12}{6(5^{\alpha+1} - 1)} = \frac{6(5^{\alpha+1} - 1) - 2\cdot 5^{\alpha} - 6}{6(5^{\alpha+1} - 1)} =$$

$$= 1 - \frac{2\cdot 5^{\alpha} + 6}{6(5^{\alpha+1} - 1)} < 1\,.$$

Así que $2\,\partial'_5(n,2\alpha) - \partial'_{5^2}(n,2\alpha) < \frac{4}{5}$.

. Por último si $v_p(n) = 2\alpha$, y $\left(\frac{n}{5}\right) = 1$, entonces:

$$2\,\partial'_5(n,2\alpha) - \partial'_{5^2}(n,2\alpha) =$$

$$= \frac{6.5^{7\alpha+2} + 4.5^{7\alpha+1} - 2.5^{7\alpha} - 16\alpha.5^{4\alpha+2} + (16\alpha+8).\,5^{4\alpha} - 8}{6^2.\,5^{7\alpha+1}} - \frac{1}{5}$$

Resulta que:

$$\frac{6.5^{7\alpha+2} + 4.5^{7\alpha+1}}{6^2.\,5^{7\alpha+1}} = \frac{(6.5+4)\,.\,5^{7\alpha+1}}{6^2.\,5^{7\alpha+1}} = \frac{17}{18}\,;$$

Además,

$$\frac{(16\alpha+8)\,.\,5^{4\alpha}}{36\,.\,5^{7\alpha+1}} = \frac{16\alpha+8}{36\,.\,5^{3\alpha+1}}\,,$$

y esta última expresión si $\alpha = 1$, vale: $\frac{24}{36\,.\,5^4} < \frac{1}{18}$,

y como $\frac{16\alpha+8}{36.5^{3\alpha+1}}$ es una función decreciente en α, para cualquier $\alpha \geq 1$ vale que $\frac{16\alpha+8}{36.5^{3\alpha+1}} < \frac{1}{18}$.

Así que podemos, aquí, también asegurar que

$$2\,\partial'_5(n,2\alpha) - \partial'_{5^2}(n,2\alpha) < \frac{4}{5}\,.$$

En los tres casos está claro que siempre es

$$2\,\partial'_5(n,\alpha) - \partial'_{5^2}(n,\alpha) \geq 0. \quad \#$$

Podemos pues pasar a enunciar el siguiente:

Teorema 4.14. Para todo entero positivo $n \not\equiv 0,4 (\text{mód } 8)$, $n = 2^{\alpha_1} 5^{\alpha_2} p_3^{\alpha_3} \ldots p_k^{\alpha_k}$, con $0 \leq \alpha_1 \leq 1$ y $0 < \alpha_2$, existe una constante $c_2 = c_2(p_1 \ldots p_k)$ tal que

$$G_2(n) \leq c_2 < 1 ,$$

para todo $\alpha = \alpha_1 + \ldots + \alpha_k$.

Demostración. Vamos a distinguir dos casos:

i) Sea n tal que $\alpha_1 = 1$. Escribamos $m = p_3^{\alpha_3} \ldots p_k^{\alpha_k}$, por la fórmula recurrente (teorema 3.22.) se tiene

$$G_2(2.5^{\alpha}m) = G_2(2m) + 2\, \partial'_5(2m,\alpha)\, (G_3(2m) - G_2(2m)) +$$

$$+ \partial'_{5^2}(2m,\alpha)\, (1 + G_2(2m) - 2G_3(2m)).$$

Por el lema 4.12 sabemos que $G_3(2m) = 1$, por tanto

$$G_2(2.5^{\alpha}m) = G_2(2m) + (2\, \partial'_5(2m,\alpha) - \partial'_{5^2}(2m,\alpha))(1-G_2(2m)).$$

Por el lema 4.13 se tiene que

$$G_2(2.5^{\alpha}m) < G_2(2m) + \frac{4}{5}\, (1 - G_2(2m)),$$

ahora aplicando el teorema 4.11 :

$$G_2(2.5^{\alpha}m) < c_2(2.5.p_3 \ldots p_k) := \frac{4}{5} + \frac{1}{5}\, c_2(2\, p_3 \ldots p_k) < 1.$$

ii) Sea n un entero con $\alpha_1 = 0$. Escribamos $n = 5^{\alpha} m$, es decir $\alpha = \alpha_2$, entonces:

$$G_2(2.5^{\alpha}m) = G_2(5^{\alpha}m) + 2\,\partial_2'(1)\,(G_3(5^{\alpha}m) - G_2(5^{\alpha}m))$$

$$= G_2(5^{\alpha}m) + 2/3\,(G_3(5^{\alpha}m) - G_2(5^{\alpha}m)).$$

Como se tiene que (proposiciones 4.7 y 4.8):

$$G_3(5^{\alpha}m) - G_2(5^{\alpha}m) \geq 0$$

y

$$G_2(5^{\alpha}m) \geq 0\ ,$$

resulta que al ser todos los sumandos positivos entonces

$$G_2(5^{\alpha}m) \leq G_2(2.5^{\alpha}m) \leq c_2(2.5.p_3\ldots p_k) < 1;$$

Así que,

$$G_2(5^{\alpha}m) \leq c_2(5\ p_3\ldots p_k) < 1,$$

siendo,

$$c_2(5\ p_3\ldots p_k) := c_2(2.5\ p_3\ldots p_k). \qquad \#$$

Con todos estos resultados se tiene el siguiente

<u>Corolario 4.15.</u> Para todo entero positivo, $n \neq 0,4(\text{mód } 8)$, $n = p_1^{\alpha_1}\ldots p_k^{\alpha_k}$, existen constantes $c_i = c_i(p_1\ldots p_k)$ tales que

$$G_i(n) \leq c_i < 1\ ,\quad i = 1,2\ ,$$

para todo $\alpha = \alpha_1 + \ldots + \alpha_k$.

§4. Acotación uniforme de $G_i^*(n)$ en el caso n impar

Sea $n \not\equiv 7 (\text{mód } 8)$ un entero impar libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Escribamos $n = mt$, con

$m = p_1 \ldots p_r$, $p_i \equiv 1 (\text{mód } 4)$; $r \geq 1$;

$t = q_1^{\beta_1} \ldots q_s^{\beta_s}$, $q_j \equiv 3 (\text{mód } 4)$.

Probaremos a continuación que $G_i^*(n) < 1$. Al ser $G_i^*(n) = G_i^*(m)$, la acotación será automáticamente uniforme en t.

Lema 4.16. Sea $x_i = \dfrac{2}{1 + p_i}$ y $P_j(m) = \prod_{i=1}^{r} (1-x_i) = 1 - y_j$, $j = 1,2,3$. Se verifica:

i) $y_3 \leq 2y_2 - y_1$,

ii) $y_3 \geq 3(y_2 - y_1)$.

Demostración.

i) Por inducción sobre r. Para $r = 1$ es evidente. Supongamos cierto el aserto hasta $r - 1$ y escribamos

$$1 - y_j' = P_j' = \prod_{i=1}^{r} (1 - jx_i) = P_j(1 - jx_r) = (1 - y_j)(1 - jx_r),$$

para $j = 1,2,3$; en donde $P_j' = P_j'(m)$ y $P_j = P_j(m)$.

Para abreviar escribiremos $x = x_r$; igualando coeficien-

tes tenemos

$y_1' = y_1 + x - xy_1$, $y_2' = y_2 + 2x - 2xy_2$, $y_3' = y_3 + 3x - 3xy_3$,

con lo que

$y_3' = y_3(1 - 3x) + 3x \leq 2(y_2 - y_1)(1 - 3x) + 3x$,

ya que $x_i = \frac{2}{1+p_i} \leq \frac{1}{3}$, pues $p_i \equiv 1(\text{mód } 4)$, $i = 1,\ldots,r$; y como la condición $y_1 \leq y_2$ implica que $-6y_2 + 3y_1 \leq -4y_2 + y_1$, resulta que: $y_3' \leq 2y_2' - y_1'$.

ii) Por inducción sobre r. Si $r = 1$, entonces

$P_1 = 1-x$, $P_2 = 1-2x$, $P_3 = 1-3x$,

es por tanto $y_3 = 3x \geq 3(2x-x) = 3(y_2-y_1)$.

Apliquemos la hipótesis de inducción y el apartado i):

$y_3' = y_3 + 3x - 3xy_3 \geq 3(y_2 - y_1) + 3x - 3x(2y_2 - y_1) = 3(y_2'-y_1')$. #

<u>Teorema 4.17.</u> Sea n un entero impar, $n \not\equiv 7(\text{mód } 8)$, libre de cuadrados respecto de sus divisores primos congruentes con 1 módulo 4. Entonces si $5 \nmid n$ se tiene que:

$$0 \leq G_i^*(n) < 1,$$

para $i = 1,2,3$.

Si $5 \mid n$, resulta que

$$0 \leq G_i^*(n) < 1,$$

para $i = 1,2$.

Demostración.

i) Recordemos (teorema 3.26) que :

$$G_1^*(n) = 1 - 3P_1 + 3P_2 - P_3 ,$$

como $P_2 < P_1$ y $P_j \geq 0$, $j = 1,2,3$, es evidente que $G_1^*(n) < 1$.

La condición $G_1^*(n) \geq 0$ equivale a que $y_3 \geq 3(y_2 - y_1)$, resultado que ya se probó en el lema 4.16.

ii) Recordemos (teorema 3.28) que :

$$G_2^*(n) = 1 - 3P_2 + 2P_3 ,$$

como $P_3 < P_2$, resulta evidentemente que $G_2^*(n) < 1$.

Además, podemos escribir

$$G_2^*(n) = G_1^*(n) + 3(P_1 - 2P_2 + P_3) ,$$

es decir

$$G_2^*(n) \geq 0 \quad \text{si y sólo si } P_1 - 2P_2 + P_3 \geq 0 ,$$

lo cual se verifica si y sólo si $2y_2 - y_1 \geq y_3$, hecho ya probado en el lema 4.16.

iii) Recordemos (teorema 3.29)

$$G_3^*(n) = 1 - P_3 ,$$

y por tanto,

$$G_3^*(n) < 1 \quad \text{si y sólo si } 5 \nmid n ,$$

ya que

$$P_3 = \prod_{i=1}^{r} (1 - 6(1+p_i)^{-1}) .$$

Por otra parte, como

$$G_3^*(n) = G_1^*(n) + 3\ (P_1 - P_2),$$

y $P_2 \leq P_1$, resulta que $G_3^*(n) \geq 0$. #

§5. Acotación uniforme de $G_i^*(n)$ en el caso n par

Sea $n \not\equiv 0,4 (\text{mód } 8)$ un entero par libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Escribamos $n = 2mt$, con

$$m = p_1 \ldots p_r, \quad p_i \equiv 1 (\text{mód } 4);\ r \geq 1,$$

$$t = q_1^{\beta_1} \ldots q_s^{\beta_s}, \quad q_j \equiv 3 (\text{mód } 4).$$

Probaremos a continuación que $G_i^*(n) < 1$; $i = 1,2$. Al ser $G_i^*(n) = G_i^*(m)$, la acotación será automáticamente uniforme en t.

Lema 4.18. Sea $x_i = \dfrac{2}{1 + p_i}$ y $P_j(m) = \prod_{i=1}^{r} (1 - x_i) = 1 - y_j$, $j = 1,2$. Se verifica:

i) $y_2 \geq y_1$,

ii) $2y_1 \geq y_2$.

Demostración.

i) De $P_1 > P_2$ se desprende automáticamente que $y_2 \geq y_1$.

ii) Por inducción sobre r. Si r = 1 entonces

$$2y_1 = 2x_1 = y_2.$$

Apliquemos la hipótesis de inducción y el apartado i):

$$2y_1' = 2y_1 + 2x_r - 2x_r\, y_1 \geq y_2 + 2x_r - 2x_r\, y_2 = y_2'. \qquad \#$$

Teorema 4.19. Sea n un entero par, $n \not\equiv 0,4 (\text{mód } 8)$, libre de cuadrados respecto de sus factores primos congruentes con 1 módulo 4. Entonces

$$0 \leq G_i^*(n) < 1,$$

para i = 1,2.

Demostración.

i) Por el teorema 3.30 tenemos que

$$G_1^*(n) = 1 - 2P_1 + P_2,$$

como $P_2 < P_1$ y $P_j \geq 0$, j = 1,2,3, es evidente que $G_1^*(n) < 1$.

Además,

$G_1^*(n) \geq 0$ si y sólo si $2y_1 \geq y_2$,

resultado que se probó en el lema 4.18.

ii) Por el teorema 3.31 tenemos que

$$G_2^*(n) = 1 - P_2,$$

evidentemente es $G_2^*(n) < 1$, pues $P_2 \geq 0$.

Como,

$$G_2^*(n) = G_1^*(n) + 2(P_1 - P_2) ,$$

es claro que $G_2^*(n) \geq 0$. #

§6. Aproximación en promedio al 3-nivel de un entero

Las expresiones $G_i(n)$, $G_i^*(n)$ son valores aproximados de $g_i(n)$ y $g_i^*(n)$, respectivamente. A la vista de los teoremas 4.9 y 4.14 definimos

$$\ell_a(n,3) = \begin{cases} -1 & \text{si } n = 4^a(8m + 7), \\ 0 & \text{si } 4 \mid n \text{ y } n \neq 4^a(8m + 7) , \\ 2 & \text{si m.c.d.}(n,10) \neq 1 , \\ 3 & \text{si m.c.d.}(n,10) = 1 ; \end{cases}$$

pensando esta cantidad como una primera aproximación al valor exacto de $\ell(n,3)$.

Claramente, para todo entero positivo n es $\ell(n,3) \leq \ell_a(n,3)$, y $\ell(n,3) = \ell_a(n,3)$ en los dos primeros casos (cf. §2 Cap. I).

Para los enteros positivos $n \leq 10^5$, P.Llorente ha calculado, mediante el ordenador, el valor de $\ell(n,3)$. Se obtiene así la siguiente

Proposición 4.20. Para todo entero $n \leq 10^5$ se verifica

$$\ell(n,3) = \ell_a(n,3) ,$$

salvo para los 24 valores siguientes:

n = 30, 70, 90, 210, 310, 330, 430, 670, 790, 870, 1170, 1330, 1710, 2170, 2190, 2230, 2530, 3070, 3690, 3910, 6790, 15990, 19890, 27190,

para los que $\ell(n,3) = 1$ y $\ell_a(n,3) = 2$; y para los 4 valores:

n = 13, 37, 403, 793, para los cuales $\ell(n,3) = 2$ y $\ell_a(n,3) = 3$.

Por tanto, se impone el estudio de las diferencias $g_i(n) - G_i(n)$, $g_i^*(n) - G_i^*(n)$, para explicar las discrepancias entre $\ell_a(n,3)$ y $\ell(n,3)$.

Definición. Sea $n \in \mathbb{Z}^+$, $n \not\equiv 0,4,7 \pmod 8$, denominaremos a las diferencias

$g_3(n) - G_3(n)$, $g_3^*(n) - G_3^*(n)$ si m.c.d.(n,10) = 1

$g_2(n) - G_2(n)$, $g_2^*(n) - G_2^*(n)$ si m.c.d.(n,10) $\neq$ 1 ,

el *término de error* en la determinación del 3-nivel de n .

CAPITULO V

INTERPRETACION DEL TERMINO DE ERROR MEDIANTE FORMAS MODULARES

En este capítulo se interpretan las diferencias

$$g_i(n) - G_i(n) \ , \quad g_i^*(n) - G_i^*(n) \ ,$$

como coeficientes de Fourier de formas modulares parabólicas de peso 3/2. La conjetura de Ramanujan - Petersson permite entonces estudiar el comportamiento del término de error en la determinación del 3-nivel de n, en función de n.

§1. Serie theta asociada a una red

Sea V un $\mathbb{Q}$-espacio vectorial de dimensión $k \geq 3$, f una forma cuadrática en V, definida positiva, y

$$B(x,y) = f(x+y) - f(x) - f(y) \ ,$$

su forma bilineal asociada.

Dada una $\mathbb{Z}$-red L de V de rango k, se designa por

$$L^{\#} = \{ \ y \in V \mid B(y,L) \subseteq \mathbb{Z} \ \}$$

su red dual.

Se llama *determinante* de L al de la matriz $(B(e_i,e_j))$, siendo $\{e_i\}_{1\leq i\leq k}$ una $\mathbb{Z}$-base de L.

La *función theta asociada a* L se define por

$$\theta(L,z) = \sum_{x\in L} e(f(x)z) = \sum_{n=o}^{\infty} r(n,L)\, e(nz) ,$$

en donde $e(z) = \exp(2\pi iz)$, $z\in\mathbb{C}$.

Sea

$$\mathbb{H} = \{z\in\mathbb{C} \mid \mathrm{Im}z > 0\}$$

el semiplano superior complejo. La serie $\theta(L,z)$ es absolutamente convergente (cf. por ejemplo [17], 0.2) y además uniformemente convergente en toda región de la forma $\mathrm{Im}z \geq \delta > 0$; representa por tanto una función holomorfa en $\mathbb{H}$.

En particular, si $L = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_k$, con $\{e_i\}_{1\leq i\leq k}$ la base canónica, entonces la serie

$$\theta(f,z) := \sum_{n=o}^{\infty} r(n,f)\, e(nz),$$

coincide con $\theta(L,z)$, y se denomina *función theta asociada a la forma cuadrática* f.

Se definen las funciones theta asociadas al género de L, y al género espinorial de L, mediante las fórmulas :

$$\theta(\text{genL},z) = \sum_{n=o}^{\infty} r(n,\text{genL})e(nz)$$

$$= \left(\sum_{M\in\text{genL}} \frac{1}{o(M)}\right)^{-1} \left(\sum_{M\in\text{genL}} \frac{\theta(M,z)}{o(M)}\right) ;$$

$$\theta(\text{spnL},z) = \sum_{n=o}^{\infty} r(n,\text{spnL})e(nz)$$

$$= \left(\sum_{M\in\text{spnL}} \frac{1}{o(M)}\right)^{-1} \left(\sum_{M\in\text{spnL}} \frac{\theta(M,z)}{o(M)}\right) .$$

La primera de estas series que se consideró históricamente fué la *serie theta de Jacobi*, dada por

$$\theta(z) = \theta(I_1,z) = \sum_{n=o}^{\infty} r(n,I_1)e(nz) = 1+2\sum_{n=1}^{\infty} e(n^2z),$$

con $z\in H$.

A partir de la serie theta de Jacobi se obtienen las funciones $\theta^k(z)$, $k \geq 1$, que dan una función generadora del número de representaciones de un entero como suma de k cuadrados, es decir :

$$\theta^k(z) = \theta(I_k,z) = \left(\sum_{x\in\mathbb{Z}} e(x^2z)\right)^k$$

$$= \sum_{(x_i)\in\mathbb{Z}^k} e((x_1^2+\ldots+x_k^2)z)$$

$$= \sum_{n=o}^{\infty} r(n,I_k)e(nz) .$$

La serie theta de Jacobi verifica la siguiente fórmula de transformación:

$$\theta(\gamma(z)) = j(\gamma,z)\ \theta(z)\ ,$$

para todo elemento $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(4)$.

Siendo para todo entero N,

$$\Gamma_o(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ \middle|\ c \equiv 0 \ (\text{mód } N) \right\}\ ,$$

el subgrupo discreto de $SL_2(\mathbb{Z})$, denominado el 0-ésimo grupo modular de nivel N. Y siendo

$$\gamma(z) = \frac{az + b}{cz + d}\ , \text{ para todo } z \in \mathbb{H}\ .$$

La función $j(\gamma,z)$, llamada *factor de automorfía*, es holomorfa en $\mathbb{H}$ y puede probarse [40] que

$$j(\gamma,z) = \varepsilon_d^{-1}\ \left(\frac{c}{d}\right)\ (cz+d)^{1/2}\ ,$$

con

$$\varepsilon_d = \begin{cases} 1 & \text{si } d \equiv 1 (\text{mód } 4), \\ i=\sqrt{-1} & \text{si } d \equiv 3 (\text{mód } 4), \end{cases}$$

siendo $\left(\frac{c}{d}\right)$ la extensión del símbolo de Jacobi dada por :

$$\left(\frac{c}{d}\right) = \begin{cases} -\left(\dfrac{c}{|d|}\right) & \text{si } c < 0,\ d < 0\ , \\ \left(\dfrac{c}{d}\right) & \text{en otro caso si } c \neq 0\ , \\ \left(\dfrac{c}{-1}\right) = 1 \text{ ó } -1 \text{ según } c > 0 \text{ ó } c < 0\ , \\ \left(\dfrac{0}{\pm 1}\right) = 1\ . \end{cases}$$

La raíz cuadrada $w^{1/2}$ de cualquier número complejo w se escoge de forma que

$$-\frac{\pi}{2} < \arg w^{1/2} \leq \frac{\pi}{2} \ .$$

Observemos que

i) $j(-I_2, z) = 1$,

ii) $\left(j\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right)^2 = \left(\frac{-1}{d}\right)(cz+d)$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(4)$.

Claramente, para todo elemento $\gamma \in \Gamma_o(4)$ se verifica la fórmula de transformación

$$\theta^k(\gamma(z)) = j^k(\gamma, z) \ . \ \theta^k(z), \quad k \geq 1 \ .$$

Las principales propiedades de las series theta asociadas a una red se obtienen al caracterizarlas como *formas modulares*. Como en nuestro problema utilizamos formas cuadráticas ternarias, nos interesará conocer las propiedades de las formas modulares de peso semientero y, más concretamente, de peso 3/2.

§2. Formas modulares de peso semientero

Pasamos a exponer, de manera sucinta, las principales propiedades de las formas modulares de peso semientero, si

guiendo las ideas expuestas por Shimura (cf. [38], [40]).

Sea G el grupo formado por todas las parejas $(\alpha,\phi(z))$ tales que

$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL^{+}(2, \mathbb{R})$ y $\phi : \mathbb{H} \longrightarrow \mathbb{C}$ es una función holomorfa del tipo :

$$\phi(z)^2 = t \det(\alpha)^{-1/2}(cz+d) \ , \ z \in \mathbb{H};$$

en donde $t \in \mathbb{C}$, $|t| = 1$, es fijo. La ley de composición del grupo G se define por

$$(\alpha_1,\phi_1(z))\ (\alpha_2,\phi_2(z)) = (\alpha_1\alpha_2, \phi_1(\alpha_2(z))\ \phi_2(z)) \ .$$

Claramente, $GL^{+}(2,\mathbb{R})$ opera en $\mathbb{H}\cup\mathbb{R}\cup\{\infty\}$. Se define la acción de (α,ϕ) en $\mathbb{H}\cup\mathbb{R}\cup\{\infty\}$ igual a la de α . Para una función $f : \mathbb{H}\longrightarrow\mathbb{C}$, y para un entero k, se define una acción de G, por la derecha, sobre f mediante la fórmula

$$(f|\ [\xi]_k)(z) = f(\alpha(z)).\ \phi(z)^{-k} \ ,$$

con $\xi = (\alpha,\phi) \in G$, por lo que

$$f|\ [\xi\eta]_k = (f|\ [\xi]_k)\ |\ [\eta]_k \ .$$

Nótese que si f es holomorfa, también lo es $f|\ [\xi]_k$.

Sea G_1 el subgrupo de G definido por

$$G_1 = \{(\alpha,\phi) \in G \mid \det \alpha = 1\} \ .$$

Entonces, dado un entero N divisible por 4, se representa por $\Delta_o(N)$ el siguiente subgrupo discreto de G_1 :

$$\Delta_o(N) = \{ (\gamma, j(\gamma,z)) \mid \gamma \in \Gamma_o(N) \} \ ;$$

siendo $j(\gamma,z)$ la misma función que aparece en la fórmula de transformación de la serie theta de Jacobi.

Un punto s de $\mathbb{R} \cup \{\infty\}$ se dice que es un *punto parabólico* de $\Gamma_o(N)$, ó de $\Delta_o(N)$ indistintamente, si existe un elemento de $\Gamma_o(N)$ que tiene a s como único punto fijo. El transformado de un punto parabólico por cualquier elemento de $\Gamma_o(N)$ vuelve a ser un punto parabólico. Se dice que dos puntos parabólicos s,t son $\Gamma_o(N)$ - equivalentes si existe un elemento γ de $\Gamma_o(N)$ tal que $\gamma(s) = t$. El conjunto de puntos parabólicos de $\Gamma_o(N)$ es $\mathbb{Q} \cup \{\infty\}$ ([38], 1.4).

Sea s un punto parabólico de $\Delta_o(N)$ y sea

$$(\Delta_o(N))_s = \{\xi \in \Delta_o(N) \mid \xi(s) = s\}$$

su grupo de isotropía. Como que $-I_2 \in \Gamma_o(N)$, resulta que $(\Delta_o(N))_s$ es el producto directo de un grupo cíclico libre y de un grupo cíclico de orden 2 , generado por $(-I_2,1)$,([38] Prop 1.17). Sea η un generador de la parte cíclica libre de $(\Delta_o(N))_s$ y ρ un elemento de G_1 tal

que $\rho(\infty) = s$, (tal elemento existe siempre ya que G_1 actúa transitivamente sobre $\mathbb{Q} \cup \{\infty\}$) . Entonces $\rho^{-1}\eta\rho$ es un elemento de G_1 que deja fijo ∞ ; ello implica (v. [40])

$$\rho^{-1}\eta\rho = \left(\pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} , t \right) ,$$

en donde h es un número real positivo y $t \in \mathbb{C}$ con $|t| = 1$, que sólo dependen de la $\Gamma_0(N)$-clase de equivalencia de s (ver por ejemplo [27] Cap. IV, prop. 2).

Proposición 5.1. Sea k un entero, f una función holomorfa definida en $\mathbb{H}$ y ρ un elemento de G_1. Supongamos que $f|[\rho]_k$ es invariante por $\left(\pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} , t \right)$, con $t \in \mathbb{C}$, $|t| = 1$ y $h \in \mathbb{R}^+$. Entonces si ponemos $t^k = e^{2\pi i r}$, $0 \leq r < 1$, se tiene :

$$(f|[\rho]_k)(z) = \sum_{n=-\infty}^{\infty} a(n)\, e^{2\pi i (n+r) z/h} \quad , \text{ con } a(n) \in \mathbb{C} .$$

Demostración. Al ser $f|[\rho]_k$ invariante bajo $\left(\pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} , t \right)$ se tiene

$$(f|[\rho]_k)(z+h) = t^k (f|[\rho]_k)(z) = e^{2\pi i r} (f|[\rho]_k)(z) .$$

Como la función

$$\frac{(f|[\rho]_k)(z)}{e^{2\pi i r z/h}}$$

es holomorfa y de período h, resulta que admite un desarrollo en serie de Fourier :

$$\sum_{n=-\infty}^{\infty} a(n)\, e^{2\pi i n z/h} \quad , \quad a(n)\in\mathbb{C} \quad ,$$

de lo cual resulta

$$(f|[\rho]_k)(z) = \sum_{n=o}^{\infty} a(n)\, e^{2\pi i (n+r) z/h} \quad . \qquad \#$$

Definición. [40] Dados un entero k, un entero N divisible por 4 y un carácter χ de $(\mathbb{Z}/N\mathbb{Z})^*$, se dice que una función holomorfa f definida en $\mathbb{H}$ es una *forma modular entera de peso* k/2 y *carácter* χ respecto de $\Gamma_o(N)$ *si*

i) $f|[\delta]_k = \chi(d) f$, para todo $\delta = (\gamma, j(\gamma,z))$ de $\Delta_o(N)$;

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(N) \quad .$$

Es decir si

$$f(\gamma(z)) = \chi(d)\, j(\gamma,z)^k\, f(z) \quad , \text{ para todo } z\in\mathbb{H} \quad .$$

ii) f es holomorfa en todo punto parabólico de $\Gamma_o(N)$.

El significado de la segunda condición es el siguiente:

Si s es un punto parabólico, sea $\rho\in G_1$ tal que $\rho(\infty) = s$, y $\rho(\pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}, t)\, \rho^{-1}$ genere la parte cíclica libre de $(\Delta_o(N))_s$, con $h\in\mathbb{R}^+$, y $t\in\mathbb{C}$, $|t| = 1$. Pongamos $t^k = e^{2\pi i r}$, $0 \leq r < 1$. Entonces por i), $f|[\rho]_k$ es invariante

bajo $[\sigma]_k$ para todo $\sigma \in \rho^{-1}(\Delta_o(N))_s\rho$, en particular bajo $(\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}, t)$, y estamos pues en las condiciones de la proposición 5.1.

Se dice que f es holomorfa en s si

$$(f|[\rho]_k)(z) = \sum_{n=o}^{\infty} a(n)\, e^{2\pi i(n+r)z/h} .$$

Un punto parabólico s se llama k-*regular* respecto de $\Gamma_o(N)$ si $t^k=1$, es decir si r=0, y k-*irregular* en caso contrario.

Se dice que f es una *forma parabólica* si a(0)=0 en todo punto parabólico k-regular.

El espacio de las formas modulares enteras de peso k/2 y carácter χ respecto de $\Gamma_o(N)$ se representa por $M_o(k/2,N,\chi)$ y el subespacio de las formas parabólicas por $S_o(k/2,N,\chi)$. Está claro que $M_o(k/2,N,\chi)$ consiste sólo en la función nula, a menos que χ sea par, es decir que satisfaga $\chi(-1)=1$. En el caso en que χ sea trivial se escribirá simplemente $M_o(k/2,N)$ y $S_o(k/2,N)$.

Respecto de $\Gamma_o(4)$, ∞, 0 y 1/2 son representantes no equivalentes de todos los puntos parabólicos [39].

Las afirmaciones de las proposiciones 5.2 y 5.4 son bien conocidas. Detallamos, sin embargo, su demostración por no haberla encontrado en la literatura.

Proposición 5.2. Si k es impar, entonces ∞ y 0 son puntos parabólicos regulares y 1/2 es irregular con $t^k = e^{k\pi i/2}$.

Demostración.

i) Evidentemente ∞ es un punto parabólico regular de $\Gamma_o(4)$ ya que

$$(\Delta_o(4))_\infty = \{ (\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}, 1),\ h\in\mathbb{Z} \} .$$

ii) Es fácil ver que el grupo de isotropía de cero en $\Delta_o(4)$ viene dado por

$$(\Delta_o(4))_o = \{ (\gamma_{m,\varepsilon}, j(\gamma_{m,\varepsilon},z)) \,|\, \gamma_{m,\varepsilon} = \begin{pmatrix} \varepsilon & 0 \\ 4m & \varepsilon \end{pmatrix},\ m\in\mathbb{Z},\ \varepsilon = \pm 1 \} .$$

Y como la aplicación $(m,\varepsilon) \longmapsto \gamma_{m\varepsilon,\varepsilon} = \begin{pmatrix} \varepsilon & 0 \\ 4m\varepsilon & \varepsilon \end{pmatrix}$

de $\mathbb{Z} \times \{\pm 1\}$ en $(\Delta_o(4))_o$ es un isomorfismo de grupos y $\mathbb{Z} \times \{\pm 1\}$ tiene dos partes cíclicas libres, a saber las generadas por (±1,1) y (±1,-1), resulta que las partes cíclicas libres de $(\Delta_o(4))_o$ son los subgrupos generados por

$$\eta = (\gamma_{1,1}, j(\gamma_{1,1},z)) = \left(\begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, (1+4z)^{1/2}\right)$$

y por

$$\bar{\eta} = (\gamma_{-1,-1}, j(\gamma_{-1,-1},z)) = \left(\begin{pmatrix} -1 & 0 \\ 4 & -1 \end{pmatrix}, (1-4z)^{1/2}\right)$$

respectivamente, o bien por

$$\eta^{-1} = (\gamma_{-1,1}, j(\gamma_{-1,1},z)) = \left(\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}, (1-4z)^{1/2}\right)$$

y por

$$\bar{\eta}^{-1} = (\gamma_{1,-1},\ j(\gamma_{1,-1}, z)) = \left(\begin{pmatrix} -1 & 0 \\ -4 & -1 \end{pmatrix},\ (1+4z)^{1/2}\right)$$

respectivamente.

Sean, ahora, $\rho = \left(\begin{pmatrix} a & d \\ c & b \end{pmatrix},\ t_o\ (cz+d)^{1/2}\right) \in G_1$, tales que $\rho(\infty)=0$ y $\rho\left(\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix},\ t\right)\rho^{-1}$, genere una parte cíclica libre cualquiera de $(\Delta_o(4))_o$, con $t,\ t_o \in \mathbb{C}$, $|t|=|t_o| = 1$ y $h \in \mathbb{R}^+$.

En general, se tiene

$$\rho\left(\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix},\ t\right)\rho^{-1} = \left(\pm\begin{pmatrix} 1-ahc & a^2h \\ -c^2h & 1+ahc \end{pmatrix},\ t(1+ach-c^2hz)^{1/2}\right);$$

En nuestro caso como $\rho(\infty)=0$, es $a=0$ y por tanto,

$$\rho\left(\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix},\ t\right)\rho^{-1} = \left(\pm\begin{pmatrix} 1 & 0 \\ -c^2h & 1 \end{pmatrix},\ t(1-c^2hz)^{1/2}\right),$$

imponiendo que esta expresión genere al menos una de las partes cíclicas libres de $(\Delta_o(4))_o$ se obtiene

$$\rho\left(\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix},\ t\right)\rho^{-1} = \left(\begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix},\ t(1-4z)^{1/2}\right) = \eta^{-1},$$

ó

$$\rho\left(\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix},\ t\right)\rho^{-1} = \left(\begin{pmatrix} -1 & 0 \\ 4 & -1 \end{pmatrix},\ t(1-4z)^{1/2}\right) = \bar{\eta},$$

siendo en ambos casos $h = 4c^{-2} \in \mathbb{R}^+$.

Igualando segundas componentes de las dos expresiones, tanto de η^{-1} como de $\bar{\eta}$, se obtiene $t = 1$ y, por tanto, $t^k = 1$.

iii) Mediante un cálculo sencillo, pero más laborioso que en el caso ii), se obtiene que

$$(\Delta_o(4))_{1/2} = \{ (\gamma_{m,\varepsilon}, j(\gamma_{m,\varepsilon},z)) \,|\, \gamma_{m,\varepsilon} = \begin{pmatrix} \varepsilon+2m & -m \\ 4m & \varepsilon-2m \end{pmatrix},\ m\in\mathbb{Z}, \varepsilon=\pm 1\}$$

y las partes cíclicas libres de $(\Delta_o(4))_{1/2}$ son los subgrupos generados por

$$\eta = (\gamma_{1,1},\ j(\gamma_{1,1},z)) = ((\begin{smallmatrix} 3 & -1 \\ 4 & -1 \end{smallmatrix}),\ -i(4z-1)^{1/2}),$$

y por

$$\bar{\eta} = (\gamma_{-1,-1},\ j(\gamma_{-1,-1},z)) = ((\begin{smallmatrix} -3 & 1 \\ -4 & 1 \end{smallmatrix}),\ i(4z-1)^{1/2}),$$

respectivamente, o bien por

$$\eta^{-1} = (\gamma_{-1,1},\ j(\gamma_{-1,1},z)) = ((\begin{smallmatrix} -1 & 1 \\ -4 & 3 \end{smallmatrix}),\ i(3-4z)^{1/2}),$$

y por

$$\bar{\eta}^{-1} = (\gamma_{1,-1},\ j(\gamma_{1,-1},z)) = ((\begin{smallmatrix} 1 & -1 \\ 4 & -3 \end{smallmatrix}),\ i(3-4z)^{1/2}),$$

respectivamente.

Sean, ahora, $\rho = ((\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}),\ t_o(cz+d)^{1/2}) \in G_1$, $t_o\in\mathbb{C}$, $|t_o|=1$ y $h\in\mathbb{R}^+$ tales que $\rho(\infty)=1/2$ y $\rho(\pm(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}),\ t)\rho^{-1}$ genere al menos una de las partes cíclicas libres de $(\Delta_o(4))_{1/2}$, con $t\in\mathbb{C}$ y $|t|=1$. Entonces, resulta que $c=2a$ y

$$\rho(\pm(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}),t)\rho^{-1} = \left(\pm\begin{pmatrix} 1-2a^2h & a^2h \\ -4a^2h & 1+2a^2h \end{pmatrix},\ t(1+2a^2h-4a^2hz)^{1/2}\right)$$

$$= ((\begin{smallmatrix} -1 & 1 \\ -4 & 3 \end{smallmatrix}),\ t(3-4z)^{1/2}) = \eta^{-1},$$

de lo que, igualando segundas componentes, se obtiene que $t=i$ y, por tanto, $t^k = e^{k\pi i/2}$. #

Corolario 5.3. El ∞ es un punto parabólico regular de $\Gamma_o(N)$.

Demostración. Basta observar que para todo $N \equiv 0(\text{mód } 4)$ es

$$(\Delta_o(N))_\infty = (\Delta_o(4))_\infty . \qquad \#$$

Proposición 5.4. Si k es par, entonces $t^k = \pm 1$; es decir $r=0$ ó $1/2$ para cualquier punto parabólico s de $\Delta_o(N)$.

Demostración. Sean $\rho=\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, t_o(cz+d)^{1/2}\right) \in G_1$ y $h\in\mathbb{R}^+$ tales que

$$\rho\left(\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}, t\right)\rho^{-1}$$

genere una parte cíclica libre de $(\Delta_o(N))_s$, con s un punto parabólico de $\Gamma_o(N)$ y $\rho(\infty)=s$. Entonces, se verifica

$$\rho\left(\delta\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}, t\right)\rho^{-1} = \left(\delta\begin{pmatrix} 1-ahc & a^2h \\ -c^2h & 1+ahc \end{pmatrix}, t(1+ach-c^2hz)^{1/2}\right),$$

en donde $\delta=\pm 1$. Para que esta expresión sea un generador de una de las partes cíclicas libres de $(\Delta_o(N))_s$ se ha de cumplir:

$-c^2h = N\lambda$, $\lambda\in\mathbb{Z}$, $1+ahc\in\mathbb{Z}$ impar, y la segunda componente ha de ser $j(\gamma,z)$, con

$$\gamma = \delta\begin{pmatrix} 1-ahc & a^2h \\ -c^2h & 1+ahc \end{pmatrix} \in \Gamma_o(N).$$

Pero

$$j(\gamma,z) = \varepsilon^{-1}_{\delta(1+ahc)} \left(\frac{-\delta N\lambda}{\delta(1+ahc)}\right) \delta^{1/2}(-c^2hz+1+ach)^{1/2} \ ;$$

distingamos, pues, varios casos:

i) Si $(1+ahc) \equiv 1 (\text{mód } 4)$ y $\delta = \pm 1$, entonces en ambos casos, es

$$j(\gamma,z) = \pm 1(1+ach-c^2hz)^{1/2} \ ,$$

y por tanto, $t = \pm 1$, de donde $t^k = t^{2k_1} = 1$.

ii) Si $(1+ahc) \equiv 3 (\text{mód } 4)$ y $\delta = \pm 1$, entonces en ambos casos, es

$$j(\gamma,z) = \pm i(1+ach-c^2hz)^{1/2} \ ,$$

y por tanto, $t = \pm i$, de donde $t^k = t^{2k_1} = \pm 1$. #

Corolario 5.5. Si k es par, $k = 2k_1$, entonces la condición i) de forma modular entera significa que

$$f(\gamma(z)) = \chi_1(d)\ (cz+d)^{k_1}\ f(z), \text{ para todo } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_o(N) \ ,$$

siendo, $\chi_1(d) = \chi(d)\ \left(\frac{-1}{d}\right)^{k_1}$.

Además, por la proposición 5.4 para todo punto parabólico es $t^k = \pm 1$. Se recupera de esta manera la definición estandar de forma modular entera de peso entero ([38] 2.1).

Pasamos a continuación a interpretar la serie theta de una red como forma modular.

Sea (V,f) un $\mathbb{Q}$-espacio cuadrático de rango $k \geq 3$ y f una forma cuadrática definida positiva. Sea L una $\mathbb{Z}$-red de V verificando que el ideal generado por $f(L)$ coincide con $\mathbb{Z}$ ($f(L)\mathbb{Z} = \mathbb{Z}$) y que $f(L^{\#})\mathbb{Z} = N^{-1}\mathbb{Z}$. Estas $\mathbb{Z}$-redes las denominaremos de *nivel* N. Las principales propiedades de la serie theta asociada a una red de este tipo se resumen en el siguiente

Teorema 5.6. ([34],[40],[41]) Sea L una $\mathbb{Z}$-red de nivel N. Se verifica

i) $\theta(L,z)$ es un elemento de $M_o(k/2, N, \chi)$, siendo

$$\chi(d) = \begin{cases} \left(\frac{2\ \det L}{d}\right) & \text{si } k \text{ es impar,} \\ \left(\frac{(-1)^{k/2}\det L}{d}\right) & \text{si } k \text{ es par,} \end{cases}$$

para todo d.

ii) $\theta(L,z) - \theta(\mathrm{gen}L,z)$ es un elemento de $S_o(k/2,N,\chi)$.

Corolario 5.7. Para cada $k \geq 1$ se tiene que $\theta^k(z)$ es un elemento de $M_o(k/2,4)$.

§3. Formas modulares de peso 3/2. Conjetura de Ramanujan-Petersson

Sean f una forma parabólica entera y g una forma modular entera, ambas de peso 3/2 respecto de $\Gamma_o(N)$. Sea D un dominio fundamental para $\Gamma_o(N)$ en $\mathbb{H}$ y sea μ la siguiente medida, finita, $\mu = \iint_D y^{-2}dxdy$.

Se define, en este caso, el *producto escalar de Petersson*, $\langle f,g\rangle$, como la integral

$$\langle f,g\rangle = \iint_D \overline{f(z)}\, g(z)\, y^{3/2}\, \frac{dxdy}{y^2} \quad , \quad z = x+iy \in \mathbb{H} \ ;$$

esta integral es absolutamente convergente ([40], lema 3.3).

Al ser $\overline{f(z)}g(z)y^{3/2}$, $y^{-2}dxdy$, invariantes [40] bajo la acción de $\Gamma_o(N)$, resulta que el producto escalar de Petersson no depende de la elección de D. Sobre $S_o(3/2,N,\chi)$ el producto escalar de Petersson es hermítico y definido positivo. Además, $\langle g,g\rangle > 0$ si $\langle g,g\rangle$ está definido y $g \neq 0$.

Se verifica [34] que

$$M_o(3/2,N,\chi) = E_o(3/2,N,\chi) \perp S_o(3/2,N,\chi) \ ,$$

en donde $E_o(3/2,N,\chi)$ es el espacio ortogonal, respecto del producto escalar de Petersson, al espacio de formas parabólicas.

Como ha probado Ting Yi Pei [43], el espacio $E_o(3/2,N,\chi)$ viene generado por las *series de Eisenstein*:

$$E(\chi,N),\ f_1(I,4N_o) \text{ y } f_1(I,8N_o) \ ,$$

y por todas sus transformadas mediante los elementos del grupo G. Las series anteriores [43] vienen definidas por:

$$E(\chi,N)(z) = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_o(N)} \bar{\chi}(d)\ j(\gamma,z)^{-3}$$

$$= \sum_{\gamma\in\Gamma_\infty\backslash\Gamma_o(N)} \frac{1}{(cz+d)^{3/2}} \cdot \frac{\overline{\chi(d)}\ \varepsilon_d^3}{(\frac{c}{d})^3} \quad ,$$

siendo $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_\infty\backslash\Gamma_o(N)$ y $\Gamma_\infty = (\Gamma_o(N))_\infty$;

$$f_1(I,4N_o) = E(\bar{I},4N_o) - (1-i)(4N_o)^{-1}\ E(\bar{\chi}_{N_o},4N_o)(\frac{-1}{4N_o z})\ z^{-3/2};$$

$$f_1(I,8N_o) = E(\bar{I},8N_o) - (1-i)(8N_o)^{-1}\ E(\bar{\chi}_{2N_o},8N_o)(\frac{-1}{8N_o z})\ z^{-3/2};$$

en donde $\bar{\chi}_{N_o}$ es el conjugado del carácter de Kronecker χ_{N_o}.

Sean a un entero libre de cuadrados y s un entero positivo tales que $4s^2a|N$. Se designa por U(a) el subespacio de $S_o(3/2,N,\chi)$ generado por las funciones

$$h_\psi(az) = \sum_{n=1}^{\infty} \psi(n)\ n\ e(an^2z),$$

en donde ψ es un carácter primitivo módulo s y tal que $\psi(-1) = -1$, y $\chi(d) = \psi(d)(\frac{-a}{d})$, para todo d.

Los espacios U(a), para los diferentes valores de a, son ortogonales dos a dos [40] respecto del producto escalar de Petersson. Sea $U = \perp U(a)$. En general se tiene que

$$S_o(3/2,N,\chi) = U \perp U^{\perp},$$

en donde $U^{\perp}$ es el complemento ortogonal de U en $S_o(3/2,N,\chi)$.

Teorema 5.8. (cf. [34]) Si L es una $\mathbb{Z}$-red de rango 3, de nivel N, se verifica

i) $\theta(\text{gen } L, z)$ es un elemento de $E_o(3/2,N,\chi)$.

ii) Sea $\pi: M_o(3/2,N,\chi) \longrightarrow E_o(3/2,N,\chi)$ la proyección canónica, entonces

$$\pi(\theta(L,z)) = \theta(\text{gen}L, z).$$

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

En el espacio de las formas parabólicas $S_o(3/2,N,\chi)$, el crecimiento de los coeficientes de Fourier de las formas de $U^{\perp}$ está controlado mediante la

Conjetura de Ramanujan-Petersson para peso 3/2 .(cf.[19],[28],[35])

$$\text{Sea } g(z) = \sum_{n=1}^{\infty} a(n)\, e^{2\pi i n z}$$

una forma parabólica de peso 3/2 de $U^{\perp}$ y sea n un entero *libre de cuadrados*. Para todo $\varepsilon > 0$ es

$$a(n) = O(n^{\frac{1}{4}+\varepsilon}) \quad ,$$

en donde la O-constante depende de ε y de g.

Por diferentes métodos se ha probado que siempre es válido ([19],[45]),

$$a(n) = O(n^{\frac{1}{2}+\varepsilon}) \quad ,$$

para n libre de cuadrados.

El crecimiento de a(n), cuando n se restringe a una clase cuadrática $n=n_o s^2$, es del mismo orden que el que figura en la conjetura de Ramanujan-Petersson. Ello se pone de manifiesto en el siguiente

Teorema 5.9. ([34], Hilfssatz 5) Sea n_o un entero positivo libre de cuadrados, y sea

$$g(z) = \sum_{n=1}^{\infty} a(n)\, e^{2\pi i n z}$$

una forma parabólica de peso 3/2 de $U(n_o)^{\perp}$. Entonces se verifica

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

en donde la O-constante depende de ε, n_o y g.

Demostración. (esbozo) Es sabido que la n_o-correspondencia de Shimura (v.[34],[40]) aplica el espacio $U(n_o)^{\perp}$ en $S_o(2,N/2,\chi^2)$. Las fórmulas de transformación de los coeficientes en esta correspondencia [39], junto con la conjetura de Ramanujan-Petersson para peso 2, probada, en este caso, por

Eichler [15], permiten deducir que existe una constante c_4 tal que

$$|a(n_o s^2)| \leq c_4 s^{1/2}\, d(s)^2,$$

en donde $c_4 = c_4(n_o, g)$ y $d(s) = \sum_{s'|s} 1$ es el número de divisores de s.

Como para todo $\delta > 0$ es $d(s) = O(s^{\delta})$, ([23], teorema 315), se verifica que existe una constante $c_5 = c_5(\delta)$; tal que

$$d(s) \leq c_5 s^{\delta},$$

por tanto, basta tomar $\delta = \varepsilon/2$ para obtener que

$$|a(n_o s^2)| \leq c_4 s^{1/2} c_5 s^{\varepsilon} = c_6 s^{\frac{1}{2}+\varepsilon},$$

siendo $c_6 := c_4 c_5$ y, en consecuencia, $c_6 = c_6(\varepsilon, n_o, g)$. #

§4. Comportamiento del término de error

Para estudiar el comportamiento del término de error, empezaremos por precisar los espacios a los que pertenecen las series theta de las formas cuadráticas que intervienen en nuestro problema.

Proposición 5.10. Sea $f = \langle b_1^2, b_2^2, b_3^2 \rangle$ una forma cuadrática entera con $(b_i, b_j)=1$, $i \neq j$, y cada b_i libre de cuadrados. Se verifica

i) $\theta(f,z)$ es un elemento de $M_o(3/2, 4b_1^2 b_2^2 b_3^2)$.

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

iii) Si los b_i son impares, $i = 1,2,3$, entonces

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

Demostración.

i) Si consideramos la $\mathbb{Z}$-red $L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$, con e_1, e_2, e_3 la base canónica, entonces $\theta(L,z) = \theta(f,z)$. Como b_1^2, b_2^2 son representados por f y son coprimos resulta que $f(L)\mathbb{Z} = \mathbb{Z}$. Calculemos ahora la red dual

$$L^{\#} = \{ y \in V \mid B(y,L) \subseteq \mathbb{Z} \},$$

siendo

$$B(x,y) = 2 \sum_{i=1}^{3} b_i^2 x_i y_i .$$

Si un elemento $y = y_1 e_1 + y_2 e_2 + y_3 e_3$ de V es de $L^{\#}$, entonces ha de verificar que

$$2(b_1^2 \lambda_1 y_1 + b_2^2 \lambda_2 y_2 + b_3^2 \lambda_3 y_3) \in \mathbb{Z},$$

para todo $\lambda_1, \lambda_2, \lambda_3$ de $\mathbb{Z}$. De aquí que

$$y_i \in \frac{1}{2b_i^2}\, \mathbb{Z}, \quad i = 1,2,3.$$

Es decir

$$L^{\#} = \mathbb{Z}\,\frac{e_1}{2b_1^2} \oplus \mathbb{Z}\,\frac{e_2}{2b_2^2} \oplus \mathbb{Z}\,\frac{e_3}{2b_3^2} \quad ,$$

y tenemos que $f(L^{\#})\mathbb{Z} = (4b_1^2b_2^2b_3^2)^{-1}\,\mathbb{Z}$, de donde la red canónica es una red de (V,f) con nivel $N = 4b_1^2b_2^2b_3^2$.

Como, por el teorema 5.6 , el carácter asociado es

$$\chi(d) = \left(\frac{2\,\det L}{d}\right) = \left(\frac{2.8b_1^2b_2^2b_3^2}{d}\right) = 1,$$

por todo d, resulta que $\theta(f,z)$ es un elemento de $M_o(3/2,\ 4b_1^2b_2^2b_3^2)$.

ii) Basta aplicar el teorema 5.8.

iii) Si los b_i son impares, entonces al ser $(b_i,b_j)=1$, $i\neq j$, se tiene que el género de f contiene un único género espinorial ([8], Ch.11, th. 1.3), por tanto, spnf = genf, y la afirmación resulta de ii). #

Observaciones.

i) Si $f = \langle a_1^2, a_2^2, a_3^2\rangle$ es una forma cuadrática tal que a_i es libre de cuadrados ($i = 1,2,3$), pero con m.c.d.$(a_1,a_2,a_3)\neq 1$, se tiene

$$f(L)\ \mathbb{Z} \subsetneq \mathbb{Z}\ ,$$

siendo $L = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$ la red canónica. Por tanto, L no es una red de nivel N y no tenemos información del comportamiento de $\theta(f,z)$ como forma modular.

ii) Si m.c.d.$(a_1,a_2,a_3)= 1$ pero $(a_i,a_j)\neq 1$, $i\neq j$, aunque en este caso tengamos información sobre $\theta(f,z)$ no se puede asegurar que spn f = gen f.

Para evitar estos problemas es por lo que se ha hecho en el Capítulo II, §6, la transformación

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

En el caso en que $2|b_1$ y $2\nmid b_i$, $i=2,3$, para poder llegar a los mismos resultados que en el caso anterior, necesitamos hacer una serie de consideraciones previas ya que no podemos asegurar que spn f = gen f.

Proposición 5.11. Sea $m=2^{\alpha}p_1\ldots p_r$ un entero libre de cuadrados, con $p_i\equiv 1 (\text{mód } 4)$, $0 \leq i \leq r$. Sea $f = <a_1^2,a_2^2,a_3^2>$ una forma cuadrática tal que $a_i|m$, $(a_i,a_j)= 1$, $i\neq j$. Sea $n\not\equiv 7 \pmod 8$, $n=mt$ en donde $t = q_1^{\beta_1}\ldots q_s^{\beta_s}$, $s \geq 0$ con $q_j\equiv 3(\text{mód } 4)$. Se verifica

$$r(n,\text{spn } f) = r(n,\text{spn } g),$$

para toda forma cuadrática g tal que gen g = gen f.

Demostración. Si $2\nmid a_i$, i= 1,2,3, como que en este caso spn f = gen f, es inmediato que spn f = spn g y, por tanto, r(n,spn f) = r(n,spn g).

Si $2|a_1$ y $2\nmid a_i$, $i=2,3$, escribamos $n = n_o s^2$, con n_o libre de cuadrados. Sean $N = 4a_1^2a_2^2a_3^2$ el nivel de la red canónica de (V,f), y $\psi(s)$ la función definida por

$$\psi(s).s = r(n_o s^2, spn f) - r(n_o s^2, spn g).$$

Si $4n_o \nmid N$ entonces ψ es idénticamente nula ([34], Kor.2) y por tanto $r(n, spn f) = r(n, snp g)$.

Si $4n_o | N$, entonces escribamos:

$$N = 4a_1^2a_2^2a_3^2 = 4n_o n_o h^2 .$$

Sea $p\neq 2$ un primo tal que $p|h$, entonces $p|a_i$ para exactamente un i, ya que $(a_i,a_j)= 1$ si $i\neq j$; por esta misma razón se tiene que $p\nmid n_o$. Por tanto $p|s$.

Si $p=2$ y $2|h$ con $v_2(h)= \nu$ se tiene que $v_2(4n_o n_o h^2) = 4+2\nu$ ya que $n\not\equiv 0,4 (\text{mód } 8)$. Por otra parte, es $v_2(4a_1^2a_2^2a_3^2) = 4$, de donde $\nu = 0$ y $2\nmid h$; con lo cual este caso no se presenta.

De todo lo expuesto se deduce que $h|s$ y, por tanto, $\psi(s)= 0$ (cf.[34], Kor.2). #

Corolario 5.12. Sea $m=2^{\alpha}p_1\ldots p_r$ un entero libre de cuadrados, con $p_i\equiv 1 (\text{mód } 4)$, $0 \leq i \leq r$. Sea $f = \langle a_1^2, a_2^2, a_3^2\rangle$ una forma cuadrática tal que $a_i|m$, $(a_i,a_j)=1$, $i\neq j$. Sea $n\not\equiv 7 (\text{mód } 8)$; escribamos $n=mt$, en donde t es también un entero libre de cuadrados y si $q|t$, q primo, entonces $q\equiv 3 (\text{mód } 4)$. La validez de la conjetura de Ramanujan-Petersson implica que, para todo $\varepsilon>0$ es

i) $r(n,f) - r(n,\text{gen}\, f) = O(t^{\frac{1}{4}+\varepsilon})$,

ii) $r^*(n,f) - r^*(n,\text{gen}\, f) = O(t^{\frac{1}{4}+\varepsilon})$,

en donde la O-constante depende de ε, m y f.

Demostración.

i) Si n es impar, por la proposición 5.10 tenemos que $\theta(f,z) - \theta(\text{gen}\, f,z) \in U^{\perp}$, por tanto i) es una consecuencia inmediata de la afirmación de la conjetura de Ramanujan-Petersson.

Si n es par, la forma $f = \langle a_1^2, a_2^2, a_3^2 \rangle$ formada a partir de n puede contener más de un género espinorial. Si f contiene un único semigénero espinorial respecto de $n=n_o$ entonces $r(n_o s^2, \text{spn}\, f) = r(n_o s^2, \text{gen}\, f)$ para $s \geq 1$. Si el género de f contiene dos semigéneros, sea g una forma cuadrática del género de f, perteneciente a distinto semigénero espinorial que f, se tiene ([34]):

$$r(n_o s^2, \text{spn}\, f) + r(n_o s^2, \text{spn}\, g) = 2r(n_o s^2, \text{gen}\, f),$$

para $s \geq 1$.

Por la proposición 5.11 sabemos que $r(n_o, \text{spn}\, f) = r(n_o, \text{spn}\, g)$ y por tanto es $r(n_o, \text{spn}\, f) = r(n_o, \text{gen}\, f)$. Basta, pues, tomar $c_7^*(\varepsilon,m,f) := c_6^*(\varepsilon,m,\theta(f,z) - \theta(\text{spn}\, f,z))$, en donde c_6^* es la O-constante dada por la conjetura de Ramanujan-Petersson.

ii) Inmediata pues, en este caso, es $r^*(n,f) = r(n,f)$ y $r^*(n,\text{gen}\, f) = r(n,\text{gen}\, f)$. #

Pasamos a continuación a dar el comportamiento del término de error, $g_i^*(n) - G_i^*(n)$, para n libre de cuadrados.

Teorema 5.13. Sea $m=2^{\alpha}p_1\dots p_r$ un entero libre de cuadrados, con $p_i\equiv 1 \pmod 4$, $0 \leq i \leq r$. Sea $f=<a_1^2,a_2^2,a_3^2>$ una forma cuadrática tal que $a_i \mid m$, $(a_i,a_j)=1$, $i\neq j$. Sea $n=mt$, $n\not\equiv 7 \pmod 8$, en donde t es también un entero libre de cuadrados y si $q \mid t$, q primo, entonces $q\equiv 3 \pmod 4$. La conjetura de Ramanujan-Petersson implica que, para todo $\varepsilon > 0$ es

$$g_i^*(n) - G_i^*(n) = O(t^{-\frac{1}{4}+\varepsilon}),$$

en donde la O-constante depende de ε y m.

Demostración. Observemos en primer lugar que al ser n libre de cuadrados se verifica $r^*(n,I_3) = r(n,I_3)$; $g_i^*(n) = g_i(n)$, pero $G_i^*(n) \neq G_i(n)$, por lo que mantenemos la notación.

Empezamos por probar que para todo $\varepsilon > 0$ es

$$g_i^*(n) - G_i^*(n) = O\left(\frac{t^{\frac{1}{4}+\frac{\varepsilon}{2}}}{r^*(n,I_3)}\right),$$

en donde la O-constante depende ε y m.

Por el corolario 5.12, para todo $\varepsilon > 0$ existe una constante $c_7^* = c_7^*(\varepsilon/2,m,<a_1^2,a_2^2,a_3^2>)$ tal que

$$|g_i^*(n) - G_i^*(n)|$$

$$= \Big| \sum_{a_i | m} \Big(\frac{r^*(n,<a_1^2,a_2^2,a_3^2>) - r^*(n, \text{gen} <a_1^2,a_2^2,a_3^2>)}{r^*(n,I_3)} \Big) \Big|$$

$$\leq \sum_{a_i | m} \frac{|r^*(n,<a_1^2,a_2^2,a_3^2>) - r^*(n, \text{gen} <a_1^2,a_2^2,a_3^2>)|}{r^*(n,I_3)}$$

$$\leq \sum_{a_i | m} c_7^* \frac{t^{\frac{1}{4}+\frac{\varepsilon}{2}}}{r^*(n,I_3)} .$$

Aquí las a_i son las correspondientes a las definiciones de $G_i^*(n)$, con $(a_i,a_j)=1$, para $i \neq j$. Si llamamos

$$c_8^* = c_8^*(\varepsilon,m) := \sum_{a_i | m} c_7^*(\varepsilon/2,m,<a_1^2,a_2^2,a_3^2>),$$

resulta que

$$|g_i^*(n) - G_i^*(n)| \leq c_8^* \frac{t^{\frac{1}{4}+\frac{\varepsilon}{2}}}{r^*(n,I_3)} .$$

Lema 5.14. Sea $n \not\equiv 0,4,7 \pmod 8$. Para todo $\varepsilon > 0$ es

$$\frac{1}{r^*(n,I_3)} = O(n^{-\frac{1}{2}+\frac{\varepsilon}{2}}) ,$$

en donde la O-constante depende de ε .

Demostración. Recordemos (teorema 3.4) que

$$r^*(n,I_3) = \frac{A(n)}{\pi}\ n^{1/2}\ L(1,\chi_{-4n}) .$$

El teorema de Siegel, relativo al comportamiento del número de clases de formas cuadráticas binarias para discriminante negativo, garantiza que para todo $\varepsilon > 0$ existe una constante $c_9^* = c_9^*(\varepsilon/2) > 0$ tal que

$$L(1,\chi_{-4n}) \geq c_9^* \cdot (4n)^{-\varepsilon/2} ,$$

([24],Ch. 12, th. 15.4).

Por tanto,

$$r^*(n,I_3) \geq \frac{8}{\pi}\ c_9^*\ 4^{-\varepsilon/2}\ n^{\frac{1}{2}-\frac{\varepsilon}{2}} ,$$

y si $n \not\equiv 0,4,7 \pmod 8$ se tiene que

$$\frac{1}{r^*(n,I_3)} \leq c_{10}^*\ n^{-\frac{1}{2}+\frac{\varepsilon}{2}} ,$$

en donde

$$c_{10}^* = c_{10}^*(\varepsilon) := \frac{\pi}{2^{3-\varepsilon}\ c_9^*} . \qquad \#$$

Aplicando ahora este lema se obtiene

$$|g_i^*(n) - G_i^*(n)| \leq c_8^* \cdot c_{10}^* \frac{t^{\frac{1}{4}+\frac{\varepsilon}{2}}}{n^{\frac{1}{2}-\frac{\varepsilon}{2}}} = c_{11}^* t^{-\frac{1}{4}+\varepsilon} ,$$

siendo $c_{11}^* = c_{11}^*(\varepsilon,m) := c_8^* \cdot c_{10}^*\ m^{-\frac{1}{2}+\frac{\varepsilon}{2}}$; y con ello conclu-

ye la demostración del teorema. #

Proposición 5.15. Sean n_o y m_o dos enteros positivos libres de cuadrados. Sea $\langle a_1^2, a_2^2, a_3^2\rangle$ una forma cuadrática, con a_i libres de cuadrados y $a_i | n_o m_o$. Sean $f = \langle b_1^2, b_2^2, b_3^2\rangle$ y $d \in \mathbb{N}$ los obtenidos a partir de $\langle a_1^2, a_2^2, a_3^2\rangle$ según el procedimiento del §6, Capítulo II. Sea $n = n_o s^2$, $n \not\equiv 0,4 \pmod 8$, con s un entero tal que rad $s = m_o$. Se verifica

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

para toda forma cuadrática g tal que gen g = gen f.

Demostración.

i) Si $2 \nmid b_i$, i= 1,2,3, como que en este caso spn f = gen f, es inmediato que r(,spn f) = r(,spn g).

ii) Si $2 | b_1$ y $2 \nmid b_i$, i=2,3, sean $N = 4b_1^2 b_2^2 b_3^2$ el nivel de la red canónica de (V,f) y $\psi(s)$ la función definida por

$$\psi(s).s = r(n_o s^2 d^{-2}, \text{spn} f) - r(n_o s^2 d^{-2}, \text{spn} g).$$

Si $4n_o \nmid N$, entonces ψ es idénticamente nula.

Si $4n_o | N$, entonces escribamos

$$N = 4n_o n_o h^2 = 4b_1^2 b_2^2 b_3^2 .$$

Sea $p \neq 2$ un primo tal que $p | h$, entonces $p | b_i$ para exactamente un i, ya que $(b_i, b_j)=1$ si $i \neq j$; por esta misma razón se tiene que $p \nmid n_o$ y como, por construcción, $(d, b_i)=1$, resulta

que $p|s$.

Si $p=2$ y $2|h$ con $v_2(h)=\nu$ se tiene que $v_2(4n_on_oh^2)= 4+2\nu$ ya que $n\not\equiv 0,4 (\text{mód } 8)$. Por otra parte, es $v_2(4b_1^2b_2^2b_3^2)= 4$, de donde $\nu = 0$ y $2\nmid h$; con lo cual este caso no se presenta.

De todo lo expuesto se deduce que $h|s$ y, por tanto, $\psi(s) = 0$ ([34], Kor. 2). #

Corolario 5.16. Sean n_o, m_o dos enteros positivos libres de cuadrados. Sea $\langle a_1^2,a_2^2,a_3^2\rangle$ una forma cuadrática, con a_i libre de cuadrados y $a_i|n_om_o$. Sean $f= \langle b_1^2,b_2^2,b_3^2\rangle$, $d\in \mathbb{N}$ los obtenidos a partir de $\langle a_1^2,a_2^2,a_3^2\rangle$ según §6, Capítulo II. Sea $n=n_os^2$, $n\not\equiv 0,4 (\text{mód } 8)$, con s un entero tal que $\text{rad}\, s=m_o$. Se verifica, para todo $\varepsilon > 0$

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

en donde la O-constante depende de ε, n_o y f.

Demostración. Basta proceder como en la demostración del corolario 5.12 pero teniendo aquí en cuenta el teorema 5.9 y la proposición 5.15, la cual asegura que

$$r(n_os^2d^{-2},\text{spn}f) = r(n_os^2d^{-2},\text{spn}g),$$

para toda forma g, tal que $\text{gen}g = \text{gen}f$, si $s= \text{rad}\, m_o$, o sea si $n_os^2= n$. Tomemos, pues, en este caso

$c_7(\varepsilon,n_o,f) := c_6(\varepsilon,n_o,\theta(f,z) - \theta(\text{spn}\, f,z))$, en donde c_6 es la O-constante del teorema 5.9. #

Teorema 5.17. Sean n_o y m_o dos enteros positivos libres de cuadrados. Sea $\langle a_1^2, a_2^2, a_3^2\rangle$ una forma cuadrática, con a_i libres de cuadrados, $a_i | n_o m_o$. Sean $f = \langle b_1^2, b_2^2, b_3^2\rangle$ y $d \in \mathbb{N}$ los obtenidos a partir de $\langle a_1^2, a_2^2, a_3^2\rangle$ según §6, Capítulo II. Sea $n = n_o s^2$, $n \not\equiv 0,4,7 \pmod 8$, con s un entero tal que $\operatorname{rad} s = m_o$. Se verifica que para todo $\varepsilon > 0$

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

en donde la O-constante depende de ε, n_o y m_o.

Demostración. Empezamos por probar que para todo $\varepsilon > 0$ es

$$g_i(n) - G_i(n) = O\left(\frac{s^{\frac{1}{2}+\frac{\varepsilon}{2}}}{r(n, I_3)}\right) ,$$

en donde la O-constante depende de ε, n_o y m_o.

Por el corolario 5.16, para todo $\varepsilon > 0$ existe una constante $c_7 = c_7(\varepsilon/2, n_o, \langle b_1^2, b_2^2, b_3^2\rangle)$ tal que

$$\begin{aligned}
&|g_i(n) - G_i(n)| \\
&= \left| \sum_{a_i | n_o m_o} \left(\frac{r(nd^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle) - r(nd^{-2}, \operatorname{gen}\langle b_1^2, b_2^2, b_3^2\rangle)}{r(n, I_3)} \right) \right| \\
&\leq \sum_{a_i | n_o m_o} \frac{\left| r(nd^{-2}, \langle b_1^2, b_2^2, b_3^2\rangle) - r(nd^{-2}, \operatorname{gen}\langle b_1^2, b_2^2, b_3^2\rangle) \right|}{r(n, I_3)} \\
&\leq \sum_{a_i | n_o m_o} c_7 \frac{s^{\frac{1}{2}+\frac{\varepsilon}{2}}}{r(n, I_3)} .
\end{aligned}$$

Aquí las a_i son las correspondientes a las definiciones

de $G_i(n)$, para i= 1,2,3. Si llamamos

$$c_8 = c_8(\varepsilon, n_o, m_o) := \sum_{a_i | n_o m_o} c_7(\varepsilon/2, n_o, <b_1^2, b_2^2, b_3^2>),$$

resulta que

$$|g_i(n) - G_i(n)| \leq c_8 \frac{s^{\frac{1}{2}+\frac{\varepsilon}{2}}}{r(n, I_3)} .$$

Lema 5.18. Sea $n \neq 4^a(8m+7)$. Para todo $\varepsilon > 0$ es

$$\frac{1}{r(n, I_3)} = O(n^{-\frac{1}{2}+\frac{\varepsilon}{4}}),$$

en donde la O-constante depende de ε.

Demostración. Recordemos (teorema 3.1) que

$$r(n, I_3) = \frac{A(n)}{\pi} n^{1/2} L(1, \chi_{-4n}) \prod_{p^2 | n} (1 + \frac{1}{p} + \ldots + \frac{1}{p^b} \kappa_p(n,b)),$$

aplicando el teorema de Siegel que garantiza que para todo $\varepsilon > 0$ existe una constante $c_9 = c_9(\varepsilon/4) > 0$ tal que

$$L(1, \chi_{-4n}) \geq c_9 (4n)^{-\varepsilon/4} ,$$

por tanto,

$$r(n, I_3) \geq \frac{8}{\pi} c_9 \, 4^{-\varepsilon/4} \, n^{\frac{1}{2}-\frac{\varepsilon}{4}} ,$$

y si $n \neq 4^a(8m + 7)$ se tiene que

$$\frac{1}{r(n, I_3)} \leq c_{10} \, n^{-\frac{1}{2}+\frac{\varepsilon}{4}} ,$$

en donde

$$c_{10} = c_{10}(\varepsilon) := \frac{\pi}{2^{3-\frac{\varepsilon}{2}} c_9} \quad . \qquad \#$$

Aplicando ahora este lema se obtiene

$$|g_i(n) - G_i(n)| \leq c_8\, c_{10}\, s^{\frac{1}{2}+\frac{\varepsilon}{2}}\, n^{-\frac{1}{2}+\frac{\varepsilon}{4}} = c_{11}\, s^{-\frac{1}{2}+\varepsilon} \quad ,$$

siendo $c_{11} = c_{11}(\varepsilon, n_o, m_o) := c_8\, c_{10}\, n_o^{-\frac{1}{2}+\frac{\varepsilon}{4}}$; y con ello concluye la demostración del teorema. #

CAPITULO VI

DETERMINACION DEL 3-NIVEL DE UN ENTERO

Por medio de los resultados obtenidos en los capítulos precedentes se procede a la clasificación de los enteros que son sumas de tres cuadrados en familias. Se prueba que en cada una de ellas el nivel se hace estacionario y se determina su valor.

§1. Acotación de $g_i^*(n)$. Constantes indicadoras del nivel

La acotación del término principal $G_i^*(n)$, junto con la información obtenida del término de error, permiten pasar a la acotación de $g_i^*(n)$.

Teorema 6.1. Sea n un entero positivo libre de cuadrados, $n \not\equiv 7 \pmod 8$. Escribamos

$$n = mt = 2^{\alpha} p_1 \cdots p_r \, q_1 \cdots q_s \ ,$$

con $0 \leq \alpha \leq 1$; $m = 2^{\alpha} p_1 \cdots p_r$, $r \geq 0$ y $t = q_1 \cdots q_s$, $s \geq 0$, $q_j \equiv 3 \pmod 4$. Sea

$t(n) := q_1 \ldots q_s$.

Entonces, existe una constante $c_{12}^* = c_{12}^*(m)$ tal que si $t(n) > c_{12}^*$ es

i) $g_3^*(n) < 1$, si m.c.d.$(n,10) = 1$.

ii) $g_2^*(n) < 1$, si m.c.d.$(n,10) \neq 1$.

Demostración.

i) Sea $\varepsilon = 2/9$; por el teorema 4.17, existe una constante $c_3^*(m) := G_3^*(m)$, $0 \leq c_3^*(m) < 1$ y por el teorema 5.13 una constante $0 < c_{11}^* = c_{11}^*(2/9,m)$ de forma que

$g_3^*(n) \leq c_3^* + c_{11}^* \, t^{-1/36}$; por tanto,

$g_3^*(n) < 1$ si $c_3^* + c_{11}^* \, t^{-1/36} < 1$,

lo cual se verifica si y sólo si

$$t > \left(\frac{c_{11}^*}{1-c_3^*} \right)^{36} .$$

Basta ahora tomar $c_{12}^*(m) := \left(\frac{c_{11}^*}{1-c_3^*} \right)^{36}$, para obtener el resultado enunciado.

ii) En este caso tomamos $c_2^*(m) := G_2^*(m)$. Por los teoremas 4.17 y 4.18 podemos asegurar que $0 \leq c_2^*(m) < 1$; definimos por tanto en este caso

$$c_{12}^{*}(m) := \left(\frac{c_{11}^{*}}{1-c_{2}^{*}}\right)^{36} . \qquad \#$$

Este teorema nos conduce a la siguiente

Definición. Sea $m = 2^{\alpha}p_1 \ldots p_r$ libre de cuadrados, con $0 \leq \alpha \leq 1$, y $p_i \equiv 1 (\text{mód } 4)$, $0 \leq i \leq r$. Definimos la familia de enteros positivos

$$F^{*}(m) := \{n \not\equiv 7 (\text{mód } 8) \mid n = mt \text{ con } t \text{ libre de cuadrados y tal que si } q \mid t, \text{ } q \text{ primo, es } q \equiv 3 (\text{mód } 4)\} .$$

Definimos la constante

$$c^{*}(m) := mc_{12}^{*}(m) .$$

Denominamos a $c^{*}(m)$ la *constante indicadora del nivel* de la familia $F^{*}(m)$.

Consecuencia inmediata de esta definición y del teorema precedente es el siguiente

Teorema 6.2. Sea n un entero positivo libre de cuadrados, $n \not\equiv 7 (\text{mód } 8)$. Escribamos

$$n = mt = 2^{\alpha}p_1 \ldots p_r \, q_1 \ldots p_s ,$$

con $0 \leq \alpha \leq 1$; $m = 2^{\alpha}p_1 \ldots p_r$, $r \geq 0$ y $t = q_1 \ldots q_s$, $s \geq 0$, $q_j \equiv 3 (\text{mód } 4)$. Si $n > c^{*}(m)$ entonces

$\ell(n,3) = \ell_a(n,3)$.

Este resultado motiva la siguiente

Definición. Llamaremos a $\ell_a(n,3)$ el nivel *asintótico* de n.

Los ejemplos, mencionados en el §6 del capítulo IV, de enteros tales que $\ell(n,3) \neq \ell_a(n,3)$ refuerzan la naturaleza asintótica del resultado del problema.

En la tabla siguiente se clasifican dichos enteros, en el caso libre de cuadrados, según a la familia a que pertenecen.

Enteros $n \leq 10^5$, *libres de cuadrados con nivel inferior al asintótico*

$F^*(p_1 \cdots p_r)$	$n = p_1 \cdots p_r\ q_1 \cdots p_s$	$\ell(n,3)$	$\ell_a(n,3)$	$c^*(m) \geq$
(13)	13	2	3	403
	403 = 13.31	2	3	
(2.5)	30 = 2.5.3	1	2	27190
	70 = 2.5.7	1	2	
	210 = 2.5.3.7	1	2	
	310 = 2.5.31	1	2	
	330 = 2.5.3.11	1	2	
	430 = 2.5.43	1	2	
	670 = 2.5.67	1	2	
	790 = 2.5.79	1	2	
	1330 = 2.5.7.19	1	2	
	2170 = 2.5.7.31	1	2	
	2230 = 2.5.223	1	2	
	2530 = 2.5.11.23	1	2	
	3070 = 2.5.307	1	2	
	27190 = 2.5.2719	1	2	
(37)	37	2	3	37
(13.61)	793 = 13.61	2	3	793
(2.5.29)	870 = 2.5.29.3	1	2	870
(2.5.73)	2190 = 2.5.73.3	1	2	2190
(2.5.17)	3910 = 2.5.17.23	1	2	3910
(2.5.97)	6790 = 2.5.97.7	1	2	6790
(2.5.13.41)	15990 = 2.5.13.41.3	1	2	15990

Recordemos que 13 y 37 son números idóneos de Euler, de los que ya se sabía, por el capítulo I, que el nivel es 2.

Existen exactamente 12 enteros $n \equiv 3 (\text{mód } 8)$ y tales que $r(n, I_3) = 1$, el mayor de los cuales es 427(v.[6]), todos ellos libres de cuadrados. Por la tabla vemos que sólo el 403 no alcanza el nivel asintótico :

$$403 = 3^2+13^2+35^2 .$$

793 posee una única representación como suma de tres cuadrados no nulos, de nivel 2 ,

$$793 = 6^2+9^2+26^2 ,$$

aunque, al ser todos sus factores primos congruentes con 1 módulo 4, es $r(n, I_3) > 1$.
870 es el primer entero, con nivel distinto del asintótico, que admite una representación de nivel cero.

Observando la tabla vemos que, en general, las constantes indicadoras del nivel no son triviales.

En el caso de la familia (2.5) se han proseguido los cálculos para todos los enteros $n \leq 10^6$ *no hallándose* más enteros con nivel distinto del asintótico, aparte de los ya mencionados en la tabla, lo que permite suponer que el comportamiento del nivel en la familia (2.5) estabiliza a partir del 27190.

En la siguiente proposición se ponen de manifiesto las constantes básicas que intervienen en la definición de $c^*(m)$.

Proposición 6.3.

Sea $m = 2^{\alpha}p_1 \ldots p_r$, con $0 \leq \alpha \leq 1$ y $p_i \equiv 1 (\text{mód } 4)$.

Se verifica

$$c^*(m) = \frac{\pi^{36}}{2^{100}m} \left(\frac{c_8^*}{c_9^*(1-c_i^*)} \right)^{36} ,$$

en donde $i = 2$ si $m.c.d.(m,10) \neq 1$ e $i = 2$ si $m.c.d.(m,10)=1$. #

Comentario sobre las constantes

i) $c_3^*(m)$ y $c_2^*(m)$ son exactamente calculables por los teoremas 4.17 y 4.19.

ii) Pasemos a $c_9^* = c_9^*(1/9)$, que es la constante que interviene en el teorema de Siegel. Para tener una idea del valor de esta constante, podemos considerar el valor de $L(1,\chi_{-4n})$.

Para todo entero n es (cf. lema 5.14)

$$\frac{2\pi h(-4n)}{(4n)^{7/18}} \geq c_9^*(1/9) .$$

Si $n = 163$, entonces $h(-4n) = 3$, y, por tanto, en este caso

$$\frac{2\pi h(-652)}{652^{7/18}} = 1,5166013 \ldots$$

con lo cual podemos asegurar que

$$c_q^*(1/9) \leq 1{,}52 \ .$$

Así que,

$$c^*(m) = \frac{\pi^{36}}{2^{100} m^{13}} \left(\frac{c_8^*}{c_9^*(1-c_i^*)} \right)^{36}$$

$$\geq \frac{\pi^{36}}{2^{100} m^{13}} \left(\frac{c_8^*}{1{,}52(1-c_i^*)} \right)^{36}$$

$$= \frac{\pi^{36}}{2^{100} 1{,}52^{36} m^{13}} \left(\frac{c_8^*}{1-c_i^*} \right)^{36} \quad ;$$

en donde i = 2 si m.c.d.(m,10) $\neq$ 1 e i = 3 si m.c.d.(m,10) = 1.

Observemos, además, que la constante c_9^* podría evitarse si se conociera una cotá inferior de $L(1,\chi_{-4n})$, para todo n. El valor mínimo de $L(1,\chi_{-N})$ que se conoce se alcanza para N = 84148631888752647283 , y es $L(1,\chi_{-N})$ = 0,17009 [29].

Entrando el valor 0,17 en el teorema se obtendría, en tal caso, una constante $c^*(m)$, mejor que la anterior, dada por

$$c^*(m) = \frac{\pi^{36}}{2^{108} \cdot 0{,}17^{36} m^{17}} \cdot \left(\frac{c_8^*}{1-c_i^*} \right)^{36} \ .$$

iii) Para c_8^* se tiene

$$c_8^*(2/9,m) = \sum_{a_i | m} c_7^*(2/9,m,<a_1^2,a_2^2,a_3^2>)$$

en donde, si llamamos $f = \langle a_1^2, a_2^2, a_3^2 \rangle$) , es

$$c_7^*(2/9,m,f) = c_6^*(2/9,m,\theta(f,z) - \theta(\text{spn } f,z))$$

y

$$c_6^* = c_4^*(2/9,m,\theta(f,z) - \theta(\text{spn } f,z)) \cdot c_5^*(2/9) .$$

La constante $c_5^*(2/9)$ es calculable [30] y vale

$$c_5^*(2/9) = \prod_p \max_{x \geq 0} \left\{ \frac{x+1}{p^{2x/9}} \right\} ,$$

que es un producto finito ya que casi todos los factores son iguales a 1.

Ahora bien, $c_4^*(2/9)$ proviene de la conjetura, aún no probada, de Ramanujan-Petersson para peso 3/2, y, por tanto, se desconoce. #

§2. Acotación de $g_i(n)$. Constantes indicadoras del nivel

La acotación del término principal $G_i(n)$, junto con la información del término de error, permiten pasar a la acotación de $g_i(n)$.

Teorema 6.4. Sea $n = n_o s^2$ un entero positivo, $n \not\equiv 0,4,7 \pmod 8$, con n_o su parte libre de cuadrados y sea $m_o = \text{rad } s$. Escribamos

$$n = n_o s^2 = p_1 \cdots p_j (p_{j+1}^{\alpha_{j+1}} \cdots p_k^{\alpha_k})^2 ,$$

(con m.c.d.(n_o,m_o) no necesariamente igual a 1) y sea

$$\alpha(n) := \sum_{i=j+1}^{k} \alpha_i \quad .$$

Entonces, existe una constante $c_{12} = c_{12}(n_o,m_o)$ tal que si $\alpha(n) > c_{12}$ es

i) $g_3(n) < 1$, si m.c.d.$(n,10) = 1$.

ii) $g_2(n) < 1$, si m.c.d.$(n,10) \neq 1$.

Demostración.

i) Sea $\varepsilon = 4/9$. Por el teorema 4.9, existe una constante $0 \leq c_3(p_1 \ldots p_k) < 1$, que, evidentemente, puede considerarse como función de n_o,m_o ; y por el teorema 5.17 existe $c_{11} = c_{11}(4/9,n_o,m_o)$ de forma que

$$g_3(n) \leq c_3 + c_{11}\, s^{-1/18} \quad ; \quad \text{por tanto,}$$

$$g_3(n) < 1 \quad \text{si} \quad c_3 + c_{11}\, s^{-1/18} < 1 \ ,$$

lo cual se verifica si y sólo si

$$\log s > 18 \log \left(\frac{c_{11}}{1-c_3} \right) \quad .$$

Si $m_o = 1$, escribamos $c_{12} := 18 \log \left(\frac{c_{11}}{1-c_3} \right)$.

Si $m_o \neq 1$, se tiene

$$\log s = \sum_{i=j+1}^{k} \alpha_i \log p_i > \alpha(n) \log p_o ,$$

siendo p_o el menor factor primo de m_o. En consecuencia, para asegurar que $g_3(n) < 1$, basta que

$\alpha(n) > c_{12}(n_o, m_o)$, siendo

$$c_{12}(n_o, m_o) := 18 \log \left(\frac{c_{11}}{1-c_3} \right) \cdot \frac{1}{\log p_o} .$$

ii) En el caso en que m.c.d.$(n,10) \neq 1$, basta tomar

$$c_{12}(n_o, m_o) := \begin{cases} 18 \log \left(\frac{c_{11}}{1-c_2} \right) , & \text{si } m_o = 1 ; \\ 18 \log \left(\frac{c_{11}}{1-c_2} \right) \frac{1}{\log p_o} , & \text{si } m_o \neq 1 ; \end{cases}$$

en donce $0 \leq c_2(n_o, m_o) < 1$ es la constante dada en el teorema 4.14. #

Este teorema nos conduce a la siguiente

<u>Definición.</u> Sean n_o y m_o enteros positivos libres de cuadrados. Definimos la familia de enteros positivos

$$F(n_o, m_o) := \{ n \neq 4^a(8b+7) \mid n = n_o s^2, \text{ rad } s = m_o \} .$$

Nótese, que si $m_o = 1$ entonces $F(n_o, 1) = \{n_o\}$, mien-

tras que en los demás casos las familias $F(n_o,m_o)$ son infinitas. Por esta razón se ha tratado el caso n libre de cuadrados mediante las familias $F^*(n)$ para poder asegurar que estos enteros tienen nivel igual al asintótico si $n > c^*(m)$.

Si $m_o = 1$, sea

$$c(n_o,1) := n_o + c_{12}(n_o,1) .$$

Si $m_o \equiv 0 (\text{mód } 2)$, sea

$$c(n_o,m_o) := 1 .$$

Si $m_o \neq 1$ y $m_o \not\equiv 0 (\text{mód } 2)$, sea p_1 el mayor factor primo de m_o y sea

$$c(n_o,m_o) := n_o \exp(2c_{12} \log p_1) .$$

La constante $c(n_o,m_o)$ la denominaremos *constante indicadora del nivel* de la familia $F(n_o,m_o)$. #

<u>Teorema 6.5.</u> Sea $n = n_o s^2$ un entero positivo, $n \neq 4^a(8b+7)$, con n_o su parte libre de cuadrados y sea $m_o = \text{rad } s$. Escribamos

$$n = n_o s^2 = p_1 \ldots p_j (p_{j+1}^{\alpha_{j+1}} \ldots p_k^{\alpha_k})^2 ,$$

(con el m.c.d.(n_o,m_o) no necesariamente igual a 1). Si $n > c(n_o,m_o)$, entonces

$$\ell(n,3) = \ell_a(n,3) . \qquad \#$$

Demostración. Basta observar que si $n > c(n_o,m_o)$, entonces $\alpha(n) > c_{12}(n_o,m_o)$ y aplicar el teorema 6.4. #

Al igual que en el caso anterior, podemos construir con los ejemplos del §6, capítulo IV la siguiente tabla

Enteros $n \leq 10^5$ *, no libres de cuadrados, con nivel inferior al asintótico*

$F(n_o,m_o)$	$n = n_o s^2$	$\ell(n,3)$	$\ell_a(n,3)$	$c(n_o,m_o) \geq$
(10,3)	$90 = 2.5.3^2$	1	2	90
(130,3)	$1170 = 2.5.13.3^2$	1	2	1170
(190,3)	$1710 = 2.5.19.3^2$	1	2	1710
(410,3)	$3690 = 2.5.41.3^2$	1	2	3690
(2210,3)	$19890 = 2.5.13.17.3^2$	1	2	19890

Nótese que, en general, las constantes indicadoras del nivel $c(n_o,m_o)$ no son triviales. Para los enteros, libres de cuadrados, reseñados en la tabla de la página 181 es $c(n_o,1) \geq n_o$.

El teorema 1.5 del capítulo I permite afinar algunas de las constantes, como muestra la siguiente

Proposición 6.6. Sea $n \in F(n_o,m_o)$. Supongamos que se presenta uno de los casos siguientes

i) $n_o = 2^{\alpha}5^{\beta}p_1 \cdots p_j$, $m_o = 5^{\gamma}p_{j+1} \cdots p_k$, con $\alpha + \beta + \gamma > 0$, y $p_i \equiv 1 (\text{mód } 4)$, $0 \leq i \leq j$;

ii) $n_o = 2q_1 \cdots q_j$, $m_o = q_{j+1} \cdots q_k$, con $q_j \equiv 3 (\text{mód } 4)$;

iii) $n_o = 5^{\alpha}q_1 \cdots q_j$, $m_o = 5^{\beta}q_{j+1} \cdots q_k$, $1 \leq j \leq k$, $n_o \not\equiv 7 (\text{mód } 8)$, con $\alpha + \beta > 0$;

para todos ellos es $\ell(n,3) = 2$, para todo n. Podemos, pues, tomar $c(n_o,m_o) = 1$.

iv) Si $n_o = q_1 \cdots q_j$, $m_o = q_{j+1} \cdots q_k$, entonces $\ell(n,3) = 3$, para todo n. Podemos tomar, por tanto, $c(n_o,m_o) = 0$.

v) Si $n \in F^*(1)$, entonces $\ell(n,3) = 3$ y podemos, pues, tomar $c^*(1) = 0$. #

En la siguiente proposición se ponen de manifiesto las constantes básicas que intervienen en la definición de $c(n_o,m_o)$.

Proposición 6.7. Sean n_o y m_o ($m_o \not\equiv 0 (\text{mód } 2)$) dos enteros libres de cuadrados. Se tiene

i) $c(n_o,1) = n_o + \log\left(\frac{\pi^{18}}{2^{50}.n_o^7}\right) + 18\log\left(\frac{c_8}{c_9(1-c_i)}\right)$.

ii) $c(n_o,m_o) = n_o \exp\left\{\left[\log\left(\frac{\pi^{36}}{2^{100}n_o^{14}}\right) + 36\log\left(\frac{c_8}{c_9(1-c_i)}\right)\right] \cdot \frac{\log p_1}{\log p_o}\right\}$

en donde $i = 2$ si $m.c.d.(n_o m_o, 10) \neq 1$ e $i = 3$ si $m.c.d.(n_o m_o, 10) = 1$. #

Comentario sobre las constantes.

i) c_3 y c_2 son calculables de forma recurrente (v. teoremas 4.9 y 4.14).

ii) Pasemos a $c_9 = c_9(1/9)$. Por ser la constante de Siegel en el punto 1/9 valen los mismos comentarios de la página 183.

iii) Para c_8 se tiene

$$c_8(4/9,n_o,m_o) = \sum_{a_i \mid n_o m_o} c_7(4/9,n_o,<b_1^2,b_2^2,b_3^2>) ,$$

en donde, si llamamos $f = <b_1^2,b_2^2,b_3^2>$,

$$c_7(4/9,n_o,f) = c_6(4/9,n_o,\theta(f,z) - \theta(\text{spn } f, z))$$

y

$$c_6(4/9,n_o,\theta(f,z) - \theta(\text{spn } f, z)) = c_4(n_o,\theta(f,z) - \theta(\text{spn } f, z)) \cdot c_5(4/9).$$

La constante $c_5(4/9)$ es calculable y vale

$$c_5(4/9) = \prod_p \max_{x \geq 0} \left\{ \frac{x+1}{p^{4x/9}} \right\} .$$

La constante c_4 proviene de la conjetura de Ramanujan-Petersson para peso 2 (cf. [15], [25], [4]) y de la aplicación de Shimura. Para la determinación de esta constante sería preciso disponer de una base de vectores propios, respecto de los operadores de Hecke, del espacio de formas parabólicas $S_o(2,N')$, con $N' = 2b_1^2 b_2^2 b_3^2$. Si bien estas bases teóricamente se conocen [4], se está lejos de tener de ellas un conocimiento efectivo.

Como

$$S_o(2,N') \xrightarrow{\sim} H^o(\overline{S}, \Omega^1) \quad ,$$

$$f \longmapsto f\,dz$$

en donde $\overline{S}$ representa la superficie de Riemann compacta $\Gamma_o(N') \backslash \mathbb{H}^*$. La dimensión de este espacio es pues igual al género de dicha superficie. Este es calculable en función de los primos que dividen a b_1, b_2, b_3 (v. [38]). #

§3. Expresión de la solución del problema

Teorema 6.8. Sea $n \not\equiv 7 (\text{mód } 8)$ un entero libre de cuadrados.

Sea $F^*(m)$ la familia a la cual n pertenece. Si $n > c^*(m)$, entonces la conjetura de Ramanujan-Petersson para peso 3/2 implica que

i) $\ell(n,3) = 2$ si m.c.d.$(n,10) \neq 1$,

ii) $\ell(n,3) = 3$ si m.c.d.$(n,10) = 1$. #

La conexión del 3-nivel con la propiedad (N) (§3, capítulo I) permite enunciar el siguiente

Corolario 6.9. Sea n un entero libre de cuadrados, $n \equiv 3 (\text{mód } 8)$ y $n \not\equiv 0 (\text{mód } 5)$. La validez de la conjetura de Ramanujan-Petersson para peso 3/2 implica que si $n \in F^*(m)$ y $n > c^*(m)$, entonces toda extensión central del grupo alternado A_n se realiza como grupo de Galois sobre $\mathbb{Q}$. #

Los resultados que ahora pasamos a enunciar son válidos, *independientemente* de la conjetura de Ramanujan-Petersson para peso 3/2.

Teorema 6.10. Sea $n \neq 4^a(8b+7)$ un entero positivo arbitrario. Sea $F(n_o,m_o)$ la familia a la cual pertenece n. Si $n > c(n_o,m_o)$, se verifica

i) $\ell(n,3) = 0$ si $4 \mid n$,

ii) $\ell(n,3) = 2$ si m.c.d.$(n,10) \neq 1$ y $4 \nmid n$,

iii) $\ell(n,3) = 3$ si m.c.d.$(n,10) = 1$. #

Corolario 6.11. Sea n un entero positivo $n \equiv 3 (\text{mód } 8)$ y $n \not\equiv 0 (\text{mód } 5)$. Si $n \in F(n_o, m_o)$ y $n > c(n_o, m_o)$, entonces toda extensión central del grupo alternado A_n se realiza como grupo de Galois sobre $\mathbb{Q}$. #

SIMBOLOS

A la derecha de cada símbolo indicamos la página en la que se define por vez primera.

BIBLIOGRAFIA

1. Apostol, T.M.: Introducción a la teoría analítica de números. Reverté, 1980.

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

3. Artin, E.: Geometric Algebra. Interscience, 1957.

4. Atkin, A., Lehner, J.: Hecke operators on $\Gamma_0(m)$. Math. Ann. 185 (1970), 134-160.

5. Bateman, P.: On the representations of a number as the sum of three squares. Trans. Amer. Soc. 71 (1951), 70-101.

6. Bateman, P., Grosswald, E.: Positive integers expressible as a sum of three squares essentially only one way. J. of Number Theory 19, (1984), 301-308.

7. Borevitch, Z.I., Chafarevitch, I.R.: Théorie des nombres. Gauthier-Villars, 1966.

8. Cassels, J.W.S.: Rational Quadratic Forms. Academic Press, 1978.

9. Chowla, S., Briggs, W.: On discriminants of binary quadratic forms with a single class in each genus. Can J. of Match. 6 (1954), 463-470.

10. Dickson, L.E.: History of the theory of numbers, vol. II. Chelsea Pub. Comp., 1971.

11. Dieudonné, J.: Abrége d'historie des Mathématiques 1700-1900, Vols. I y II. Hermann, 1978.

12. Dirichlet, P.G., Lejeune: La possibilité de la décomposition des nombres en trois carrés. J. de Math pures et appl. (2), 4 (1859), 233-240.

13. Dirichlet, P.G., Lejeune: Recherches sur diverses applications de l'Analyse infinitésimale a la Théorie des Nombres. Werke, 1 : 441-496.

14. Eichler, M.: Quadratische Formen und orthogonale Gruppen. Springer, 1952.

15. Eichler, M.: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktionen. Arch. math. 5 (1954), 355-366.

16. Eisenstein, G.: Neue Theoreme der höheren Arithmetik. Math. Abhand. Georg Olms, 1967.

17. Freitag, E.: Siegelsche Modulfunktionen. Springer, 1983.

18. Gauss, C.F.: Disquisitiones Atirmeticae. Yale Univ. Press, 1966.

19. Goldfeld, D., Hoffstein, J., Patersson, S.J.: On automorphic functions of half-integral weight with applications to elliptic curves. Number Theory related to Fermat's last theorem. Progress in Maths. Vol. 26. Birkhäuser, 1982.

20. Gunning, R.C.: Lectures on modular forms. Princeton Univ. Press, 1961.

21. Hardy, G.H.: On the representation of a number as a sum of any number of squares, and in particular of five. Trans. Amer. Math. Soc. 21 (1920), 255-288.

22. Hardy, G.H.: Ramanujan, twelve lectures on subjects suggested by his life and work. Chelsea Pub., 1940.

23. Hardy, G.H., Wright, E.M.: An introduction to the Theory of Numbers. Oxford at the Clar. Press, 1960.

24. Hua Loo Keng: Introduction to Number Theory. Springer, 1982.

25. Igusa, J.-I.: Kroneckerian model of fields of elliptic modular fuctions. Amer. J. Math. 81 (1959), 561-577.

26. Ireland, K., Rosen, M.: A classical introduction to Modern Number Theory. Springer, 1980.

27. Koblitz, N.: Introduction to elliptic curves and modular forms. Springer, 1984.

28. Kohnen, W.: Fourier coefficients of modular forms of half integral weight. Math. Ann. 271 (1985), 237-268.

29. Lehmer, D.H., Lehmer, E., Shanks, D.: Integer sequences having prescribed quadratic character. Math. Comp. 24 (1970), 433-451.

30. LeVeque, W.J.: Topics in number theory. Vol. I. Addison Wesley Pub. Comp., 1958.

31. O'Meara, O.T.: Introduction to quadratic forms. Springer, 1963.

32. Ramanujan, S.: On certain arithmetical functions. Trans. of the Cambridge Phil. Soc., XXII, 9 (1916),159-184. Collected Papers. Chelsea Pub. Comp. 1927, 1962.

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

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

35. Schulze-Pillot, R.: Carta personal. Noviembre 1984.

36. Schulze-Pillot, R.: Darstellungsmasse von Spinorgeschlechtern ternärer quadratischer Formen. J. für die reine und ang. Math. 352 (1984), 114-132.

37. Serre, J-P.: Cours d'arithmétique. Press Univ. de France, 1970.

38. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Iwanami Shoten Publ.and Princeton Univ. Press, 1971.

39. Shimura, G.: Modular forms of half integral weight. Springer Lect. N. 320, 1972.

40. Shimura, G.: On modular forms of half integral weight. Ann. of Math. 97 (1973), 440-481.

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

42. Siegel, C.L.: Über die Classenzahl quadratischer Zahlkörper. Acta Arit. 1 (1935) 83-86. Gesammelte Abhand.,Band 1. Springer, 1966.

43. Ting-Yi Pei: Eisenstein series of weight 3/2. I y II. Trans. Amer. Math. Soc. Vol. 274, 2 (1982), 573-606. Idem Vol. 283, 2 (1984), 589-603.

44. Vila, N.: Sobre la realització de les extensions centrals del grup alternat com a grup de Galois sobre el cos dels racionals. Tesi doctoral. Pub. Sec. Mat. Univ. Autònoma de Barcelona. Vol. 27, Num. 3 (1983), 43-143.

45. Waldspurger, J.-L.: Sur les coefficients de Fourier des formes modulaires de poids demi-entier. J. Math. Pures et Appl. 60 (1981), 375-484.

46. Weil, A.: Number Theory. An approach through history. From Hammurapi to Legendre. Birkhäuser, 1984.

47. Zagier, D.B.: Zetafunktionen und Quadratische Körper. Springer, 1981.