MAG-M
C824
c 1

UNA GENERALIZACION DEL TEOREMA DE HOLZER

Tesis

entregada a la

Universidad de Chile

en cumplimiento parcial de los requisitos

para optar al grado de

Magister en Ciencias Matemáticas

FACULTAD DE CIENCIAS

por

IVAN ALEJANDRO CORREA SIERRA

Diciembre, 1988

Patrocinante: Dr. Ricardo Baeza R.

FACULTAD DE CIENCIAS
BIBLIOTECA CENTRAL
U. DE CHILE

I N D I C E

	Pág.
INTRODUCCION.	i
CAPITULO I.	1
1. Formas Cuadráticas sobre $\mathbb{Q}_p$.	1
2. Principio Local Global.	8
3. Contraejemplo al Principio Local Global.	16
CAPITULO II.	18
1. La ecuación diofántica $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$. Teorema de Holzer.	18
2. La ecuación diofántica $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 0$.	22
3. Condiciones necesarias y suficientes para la solubilidad en $\mathbb{Z}$.	26
4. Generalización del Teorema de Holzer.	27
5. Solución efectiva en $\mathbb{Z}$.	30

Pág.

APENDICE. 36

Ejemplos. 36

Problema Final. 43

BIBLIOGRAFIA. 46

FACULTAD DE CIENCIAS
BIBLIOTECA CENTRAL
U. DE CHILE

I N T R O D U C C I O N

Un problema de interés en años recientes ha sido el de encontrar una estimación para la magnitud de la solución no trivial más pequeña de una ecuación diofántica, i.e. si $f \in \mathbb{Z}[x_1, \ldots, x_n]$, interesa encon - trar la solución entera más pequeña de la ecuación

$$f(x_1, \ldots, x_n) = 0 \ .$$

En general el problema de decidir la solubilidad en $\mathbb{Q}$ (equiva - lentemente en $\mathbb{Z}$) de ecuaciones como la anterior, donde f es una forma cuadrática, está resuelto por el Principio de Hasse o Principio Local Global, que proporciona una condición necesaria y suficiente para la solubilidad de estas ecuaciones.

En 1798, Legendre demostró que si la ecuación diofántica

$$a_1x^2 + a_2x_2^2 + a_3x_3^2 = 0 \qquad (1)$$

está en su forma normal, i.e. a_1, a_2, a_3 son enteros libres de cuadrados, primos entre sí de dos en dos y no todos del mismo signo, entonces la solubilidad de las tres congruencias

$$x^2 \equiv -a_2a_3 \pmod{a_1}$$
$$x^2 \equiv -a_1a_3 \pmod{a_2} \qquad (2)$$
$$x^2 \equiv -a_1a_2 \pmod{a_3}$$

es condición necesaria y suficiente para la solubilidad de la ecuación (1) en $\mathbb{Z}$.

En la demostración de suficiencia de la condición (2) se deduce que la ecuación (1), ó la ecuación

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = -a_1a_2a_3 \qquad (3)$$

tiene una solucïón en el dominio entero

$$|x_1| \leq \sqrt{|a_2a_3|} \; ; \quad |x_2| \leq \sqrt{|a_1a_3|} \; ; \quad |x_3| \leq \sqrt{|a_1a_2|} \; . \qquad (4)$$

En caso de ser x_1,x_2,x_3 una solución de la ecuación (3), los números z_1,z_2,z_3 definidos por $z_1 = -a_2x_2 + x_1x_3$, $z_2 = a_1x_1 + x_2x_3$ y $z_3 = x_3^2 + a_1a_2$ forman una solución para la ecuación (1).

En 1950 Holzer utilizando un profundo resultado sobre números pri - mos en una progresión aritmética en un cuerpo cuadrático, demostró que si la ecuación (1) es soluble (no trivialmente) en $\mathbb{Z}$, entonces tiene una solución en el dominio (4).

Skolem y Mordell intentaron dar demostraciones utilizando métodos más elementales, logrando solo versiones más toscas del Teorema. Finalmente, en 1968 Mordell logró el objetivo (demostración del Teorema 5).

Con un sencillo programa computacional es posible advertir que en

muchos casos la ecuación (1) tiene varias soluciones en su dominio (4) respectivo, por lo que se puede pensar que en esos es posible optimizar las cotas de (4). Kneser estudió este problema en 1958. Es fácil deducir que la tercera desigualdad de (4) implica las otras dos; Kneser demuestra que si (1) es soluble, entonces existe una solución x_1, x_2, x_3 con

$$|x_3| \leq k \sqrt{|a_1 a_2|}$$

donde en muchos casos $k < 1$ (ver [K]).

Es claro entonces que resulte interesante preguntarse qué sucede con la ecuación con cuatro variables

$$a_1 x_1^2 + a_2 x_2^2 + a_3 x_3^2 + a_4 x_4^2 = 0 \ . \qquad (5)$$

La demostración del Teorema de Hasse Minkowski depende esencialmente del número de variables de la ecuación, y es posible, basándose en este Teorema para los casos $n = 3$ y $n = 4$, establecer un conjunto de condiciones para la solubilidad de (5). Con este propósito, en el Capítulo I se enuncian algunos Teoremas y Lemas concernientes a formas cuadráticas sobre los cuerpos p-ádicos $\mathbb{Q}_p$.

Aplicando en forma adecuada una versión efectiva del Teorema de la Progresión Aritmética de Dirichlet, empleando una función que acote al primo más pequeño que aparece en dicha sucesión (ver [J-R]), es posible establecer una generalización del Teorema de Holzer para la ecuación (5) (Teorema 8).

La optimización de esta generalización depende en gran medida del

porte de la cota para el primer primo en la progresión, cabe agregar que este último problema ha sido muy estudiado y existe una versión mucho más general que se puede encontrar en [L-O].

En cuanto al Teorema de Holzer, es seguro que de una forma u otra, en un futuro próximo, se logrará una generalización con cotas mucho mejores, por ejemplo, como las que se proponen en el problema del Apéndice.

C A P I T U L O I

FORMAS CUADRATICAS SOBRE $\mathbb{Q}_p$

§ 1. PRELIMINARES.

DEFINICION 1. Clásicamente una forma cuadrática sobre un cuerpo K es un polinomio homogéneo de grado dos de la forma

$$f(X_1, \ldots, X_n) = \sum_{i,j} a_{ij} X_i X_j$$

en n indeterminadas $X_1, \ldots, X_n$, con coeficientes $a_{ij} \in K$.

La matriz simétrica $A = (a_{ij})$ se denomina la matriz de f.

Mediante el conocido proceso de diagonalización de A se puede transformar f en una forma diagonal

$$\sum_{i=1}^{n} a_i x_i^2 \quad , \quad a_i \in K \, , \quad (\text{Car } K \neq 2) \, .$$

Para nuestro propósito, consideraremos en adelante las formas cuadráticas diagonalizadas, y $K = \mathbb{Q}$ el cuerpo de los números racionales, ó

$K = \mathbb{Q}_p$ cuerpo de los números p-ádicos según sea el caso, además escribiremos el cuerpo de los números reales $\mathbb{R} = \mathbb{Q}_\infty$.

Las demostraciones del Teorema 1, su Corolario y del Teorema 2, pueden verse en [B-S].

TEOREMA 1 (Hensel). Sea $F(X_1, \ldots, X_n) \in \mathbb{Z}_p[X_1, \ldots, X_n]$ y $(\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}_p^n$ tal que para cierto i , $1 \leq i \leq n$

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{2\delta+1}}$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p^{\delta}}$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod{p^{\delta+1}}$$

cierto $\delta \in \mathbb{N}$, entonces existen enteros p-ádicos $\theta_1, \ldots, \theta_n$ tales que

$$F(\theta_1, \ldots, \theta_n) = 0$$

y $$\theta_i \equiv \gamma_i \pmod{p^{\delta+1}} , \quad 1 \leq i \leq n .$$

COROLARIO. Sea $F(X_1, \ldots, X_n) \in \mathbb{Z}_p[X_1, \ldots, X_n]$ y $(\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}_p^n$ tal que para cierto i , $1 \leq i \leq n$

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \pmod{p}$$

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_m) \not\equiv 0 \pmod{p}$$

entonces existen enteros p-ádicos $\theta_1, \ldots, \theta_n$ tales que

$$F(\theta_1, \ldots, \theta_n) = 0$$

y $\theta_i \equiv \gamma_i \pmod p$; $1 \leq i \leq n$.

Luego, toda solución $\gamma_1, \ldots, \gamma_n$ de la congruencia $F(X_1, \ldots, X_n) \equiv 0 \pmod p$ puede extenderse a una solución de la ecuación $F = 0$ en $\mathbb{Z}_p$ salvo que

$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) = 0 \quad \text{, para todo } i \text{ , } 1 \leq i \leq n .$$

TEOREMA 2 (Chevalley). Si $F(X_1, \ldots, X_n)$ es una forma homogénea de grado estrictamente menor que n , entonces la congruencia

$$F(X_1, \ldots, X_n) \equiv 0 \pmod p$$

tiene solución no nula $(X_1, \ldots, X_n) \pmod p$.

LEMA 1. Sea p primo impar y $0 < r < n$; $\varepsilon_1, \ldots, \varepsilon_n$ unidades p-ádicas, entonces la forma

$$F = F_o + pF_1 = \varepsilon_1 x_1^2 + \ldots + \varepsilon_r x_r^2 + p(\varepsilon_{r+1} x_{r+1}^2 + \ldots + \varepsilon_n x_n^2)$$

representa cero en $\mathbb{Q}_p$ sí y sólo si F_o ó F_1 representa cero en $\mathbb{Q}_p$.

Demostración: Sea F soluble en $\mathbb{Q}_p$ y $\xi_1, \ldots, \xi_n$ una solución, entonces podemos suponer que $\xi_i \not\equiv 0 \pmod p$ para al menos un i , $1 \leq i \leq n$.

Si $1 \leq i \leq r$, supongamos $i = 1$, entonces

$$F_o(\xi_1, \ldots, \xi_r) \equiv 0 \pmod p$$

$$\frac{\partial F_o}{\partial x_1}(\xi_1, \ldots, \xi_r) = 2\varepsilon_1 \xi_1 \not\equiv 0 \pmod p .$$

Por el Corolario del Teorema 1, F_o representa cero.

Si $\xi_1 \equiv \ldots \equiv \xi_r \equiv 0 \pmod{p}$, entonces $F_o(\xi_1, \ldots, \xi_r) \equiv 0 \pmod{p^2}$ de donde $F_1(\xi_{r+1}, \ldots, \xi_n) \equiv 0 \pmod{p}$ con al menos un ξ_j , $r + 1 \leq j \leq n$ no divisible por p , por Corolario del Teorema 1, F_1 representa cero en $\mathbb{Q}_p$.

COROLARIO 1. Si p es primo impar y $\varepsilon_1, \ldots, \varepsilon_r$ son unidades p-ádicas entonces la forma

$$f = \varepsilon_1 x_1^2 + \ldots + \varepsilon_r x_r^2$$

representa cero en $\mathbb{Q}_p$ sí y sólo si la congruencia $f(x_1, \ldots, x_r) \equiv 0 \pmod{p}$ tiene una solución no trivial en $\mathbb{Z}_p$.

Demostración: Consecuencia inmediata del Lema.

COROLARIO 2. Si p es primo impar y $\varepsilon_1, \ldots, \varepsilon_n$ son unidades p-ádicas con $n \geq 3$, entonces la forma

$$\varepsilon_1 x_1^2 + \ldots + \varepsilon_n x_n^2$$

representa cero en $\mathbb{Z}_p$.

Demostración: Consecuencia del Teorema 2 y el Corolario 1.

LEMA 2. Si $p = 2$, la forma F del Lema 1 representa cero en $\mathbb{Q}_2$ sí y sólo si la congruencia

$$F \equiv 0 \pmod{16}$$

admite una solución con al menos una de las incógnitas impar.

Demostración: Sea $F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod{16}$ con ξ_i impar algún $1 \leq i \leq n$. Si $i \leq r$, sin restricción sea ξ_1 impar, entonces

$$F(\xi_1, \ldots, \xi_n) \equiv 0 \pmod{8}$$

$$\frac{\partial F}{\partial x_1}(\xi_1, \ldots, \xi_n) \not\equiv 0 \pmod{4} .$$

Por Teorema 1, F representa cero en $\mathbb{Q}_2$.

Supongamos ahora que $\xi_i \equiv 0 \pmod{2}$ para $1 \leq i \leq r$, y $\xi_i = 2\lambda_i$, $\lambda_i \in \mathbb{Z}_p$, $1 \leq i \leq r$, entonces

$$4 \sum_{i=1}^{r} \varepsilon_i \lambda_i^2 + 2 \sum_{i=r+1}^{n} \varepsilon_i \xi_i^2 \equiv 0 \pmod{16} .$$

Luego

$$\sum_{i=r+1}^{n} \varepsilon_i \xi_i^2 + 2 \sum_{i=1}^{r} \varepsilon_i \lambda_i^2 \equiv 0 \pmod{8}$$

con al menos un ξ_i, $r + 1 \leq i \leq n$ impar, así la forma $F_1 + 2F_o$ y por lo tanto F representa cero en $\mathbb{Q}_2$.

El recíproco del Lema es claro.

De la demostración anterior se deduce el siguiente

COROLARIO. Si la forma F del Lema 1 admite una solución para la congruencia

$$F \equiv 0 \pmod{8}$$

con al menos una de las incógnitas $x_1, \ldots, x_r$ impar, entonces la forma representa cero en $\mathbb{Q}_2$.

LEMA 3. Si p es un primo impar, una unidad p-ádica

$$\varepsilon = c_o + c_1 p + c_2 p^2 + \ldots ; \qquad (0 \leq c_i < p \ , \ c_o \neq 0)$$

es un cuadrado en $\mathbb{Q}_p$ sí y sólo si c_o es resto cuadrático módulo p .

e.d. $\varepsilon \in \mathbb{Q}_p^2 \iff \left(\frac{c_o}{p}\right) = 1$; $\left(\frac{\cdot}{p}\right)$ símbolo de Legendre.

Demostración: Si $\varepsilon = \beta^2$ en $\mathbb{Q}_p$, y $\beta \equiv b \pmod p$ con $b \in \mathbb{Z}$, entonces $c_o \equiv b^2 \pmod p$.

Para el recíproco, consideremos el polinomio $F(x) = x^2 - \varepsilon$, entonces $F(b) \equiv 0 \pmod p$ y $F'(b) = 2b \not\equiv 0 \pmod p$. Por Corolario del Teorema 1 existe $\alpha \in \mathbb{Z}_p$ tal que $F(\alpha) = 0$ y $\alpha \equiv b \pmod p$, de donde $\varepsilon = \alpha^2$.

LEMA 4. Si ε es una unidad 2-ádica, entonces ε es un cuadrado en $\mathbb{Q}_2$ sí y sólo si $\varepsilon \equiv 1 \pmod 8$.

Demostración: Si $\varepsilon \in \mathbb{Q}_2^2$, el cuadrado de todo número impar es congruente a 1 módulo 8, luego $\varepsilon \equiv 1 \pmod 8$.

Si $\varepsilon \equiv 1 \pmod 8$ aplicar Corolario del Teorema 1 al polinomio $F(x) = x^2 - \varepsilon$ de donde resulta $\varepsilon \in \mathbb{Q}_2^2$.

LEMA 5. Si una forma cuadrática no singular representa cero en un cuerpo K , entonces representa todos los elementos de K .

Demostración: Consideremos la forma $F = a_1 x_1^2 + \ldots + a_n x_n^2$, y $a_1 \alpha_1^2 + \ldots + a_n \alpha_n^2 = 0$ una representación de cero no nula en K . Sin restricción supongamos $\alpha_1 \neq 0$. Sean las variables

$x_1 = \alpha_1(1 + t)$; $x_k = \alpha_k(1 - t)$, $k = 2, \ldots, n$ con t variable a determinar. Entonces

$$F(x_1, \ldots, x_n) = 2a_1\alpha_1^2 t - 2a_2\alpha_2^2 t - \ldots - 2a_n\alpha_n^2 t = 4a_1\alpha_1^2 t .$$

Basta considerar $t = \dfrac{\gamma}{4a_1\alpha_1^2}$.

LEMA 6. Sea K un cuerpo con más de 5 elementos, si la forma diagonal

$$F = a_1x_1^2 + \ldots + a_nx_n^2$$

representa cero en K , entonces existe una representación de cero por F con todas las variables no nulas.

<u>Demostración</u>: Basta ver que si $a_1\xi^2 \neq 0$ entonces existen $\alpha_1, \alpha_2 \neq 0 \in K$ con $a_1\alpha_1^2 + a_2\alpha_2^2 = a_1\xi^2$ $(a_2 \neq 0)$.

Considerar la identidad

$$a_1\left(\xi\frac{t - 1}{t + 1}\right)^2 + a_1t\left(\frac{2\xi}{t + 1}\right)^2 = a_1\xi^2 \quad , \text{ cierto } \quad t \neq \pm 1 .$$

Como $^{\#}K > 5$, y para cada ecuación

$$a_2x^2 - a_1 = 0 \quad y \quad a_2x^2 + a_1 = 0$$

hay a lo más 2 soluciones en K , podemos elegir λ de modo que $t = t_o = \dfrac{a_2\lambda^2}{a_1} \neq \pm 1$, luego

$$a_1\left(\xi\frac{t_o - 1}{t_o + 1}\right)^2 + a_2\left(\frac{2\xi\lambda}{t_o + 1}\right)^2 = a_1\xi^2 .$$

§ 2. PRINCIPIO LOCAL GLOBAL PARA FORMAS CUADRATICAS.

TEOREMA 3 (Hasse-Minkowski). El principio local global se cumple para formas cuadráticas, e.d. la ecuación $a_1x_1^2 + \ldots + a_nx_n^2 = 0$ tiene solución no trivial en $\mathbb{Q}$ sí y sólo si existe solución no trivial en todos los cuerpos $\mathbb{Q}_p$, $p = 2,3, \ldots, \infty$.

Demostración: Si la ecuación tiene solución en $\mathbb{Q}$, como $\mathbb{Q} \subset \mathbb{Q}_p \quad \forall\, p$, es soluble en todos los cuerpos p-ádicos.

Supongamos entonces que la ecuación tiene solución en $\mathbb{Q}_p$, $p = 2,3, \ldots, \infty$. La demostración de esta parte del Teorema depende esencialmente del número n de variables.

El caso $n = 1$ es trivial, veamos el

Caso $n = 2$. En cada cuerpo $\mathbb{Q}_p$, elijamos una solución α_1, α_2 no trivial, como la ecuación es soluble en particular en $\mathbb{Q}_\infty = \mathbb{R}$, no puede tener todos los coeficientes con el mismo signo, es decir debe ser no definida.

Sin restricción supongamos $a_1 > 0$ y $a_2 < 0$, así en cada cuerpo $\mathbb{Q}_p$ $a_1\alpha_1^2 + a_2\alpha_2^2 = 0$ y por lo tanto $-a_1 / a_2 = (\alpha_2 / \alpha_1)^2$, así $v_p(-a_1 / a_2) \in 2\mathbb{Z} \quad \forall\, p$ (v_p valuación p-ádica). Luego si escribimos $-a_1 / a_2 = \prod p^{r_i}$, $r_i = v_{p_i}(-a_1 / a_2) = 2s_i$ se tiene que $-a_1 / a_2 = [\prod p_i^{s_i}]^2$ es un cuadrado en $\mathbb{Q}$. Sea $-a_1 / a_2 = b^2$ cierto $b \in \mathbb{Q}$, entonces $a_1 + a_2b^2 = 0$. Luego la ecuación es soluble en $\mathbb{Q}$.

Caso $n = 3$. Podemos considerar en este caso la ecuación reducida a su forma normal, e.d.

(i) a_1, a_2, a_3 son enteros libres de cuadrados,

(ii) no todos los coeficientes tienen igual signo,

(iii) $(a_i, a_j) = 1$ para $i \neq j$;

sin restricción supongamos $a_1, a_2, a_3 > 0$ y escribamos la ecuación como

$$a_1x_1^2 + a_2x_2^2 - a_3x_3^2 = 0 .$$

Sea p primo impar tal que $p \mid a_3$. Por hipótesis esta ecuación tiene solución en $\mathbb{Q}_p$, luego por Corolario 1 del Lema 1, la congruencia

$$a_1x_1^2 + a_2x_2^2 \equiv 0 \pmod{p}$$

tiene una solución no trivial (x_o, y_o) , de donde

$$a_1x_1^2 + a_2x_2^2 \equiv a_1y_o^{-2}(x_1y_o + x_2x_o)(x_1y_o - x_2x_o) \pmod{p}$$

y por lo tanto, como $p \mid a_3$

$$a_1x_1^2 + a_2x_2^2 - a_3x_3^2 = L^{(p)}(x_1, y_1, z_1)M^{(p)}(x_1, y_1, z_1) \pmod{p} \qquad (1)$$

donde $L^{(p)}$ y $M^{(p)}$ son formas lineales en $\mathbb{Z}[x_1, x_2, x_3]$ que dependen de p .

Para $p = 2$

$$a_1x_1^2 + a_2x_2^2 - a_3x_3^2 \equiv (a_1x_1 + a_2x_2 - a_3x_3)^2 \pmod{2} .$$

Así para cada primo $p \mid 2a_1a_2a_3$ existen formas lineales $L^{(p)}$ y $M^{(p)}$ con la propiedad (1).

Por el Teorema Chino de los restos existen formas lineales L y M en $\mathbb{Z}[x_1,x_2,x_3]$ tales que

$$a_1x_1^2 + a_2x_2^2 - a_3x_3^2 \equiv L(x_1,x_2,x_3)M(x_1,x_2,x_3) \pmod{a_1a_2a_3} \ . \qquad (2)$$

Si $a_1a_2a_3 = 1$, la ecuación tiene una solución obvia. Supongamos $a_1a_2a_3 \neq 1$, entonces uno de los números $\sqrt{a_1a_2}$, $\sqrt{a_1a_3}$, $\sqrt{a_2a_3}$ no es entero. Sea $V = \{(x_1,x_2,x_3) \in \mathbb{Z}^3 \ / \ 0 \leq x_1 < \sqrt{a_2a_3}$; $0 \leq x_2 < \sqrt{a_1a_3}$; $0 \leq x_3 < \sqrt{a_1a_2}\}$, es fácil ver que $^{\#}V > a_1a_2a_3$, luego $^{\#}V > {}^{\#}(\mathbb{Z}/a_1a_2a_3\,\mathbb{Z})$, así existen (x_1,x_2,x_3) y (y_1,y_2,y_3) distintos en V tales que

$$L(x_1,x_2,x_3) \equiv L(y_1,y_2,y_3) \pmod{a_1a_2a_3} \ .$$

Luego si $x_o = x_1 - y_1$, $y_o = x_2 - y_2$, $z_o = x_3 - y_3$

$$L(x_o,y_o,z_o) \equiv 0 \pmod{a_1a_2a_3} \ . \qquad (3)$$

Además, como (x_1,x_2,x_3) y (y_1,y_2,y_3) están en V , $(x_o,y_o,z_o) \in V$, de donde resulta

$$-a_1a_2a_3 < a_1x_o^2 + a_2y_o^2 - a_3z_o^2 < 2a_1a_2a_3 \ . \qquad (4)$$

De (1) y (2) se obtiene

$$a_1x_o^2 + a_2y_o^2 - a_3z_o^2 = da_1a_2a_3 \ , \quad \text{cierto } d \in \mathbb{Z} \ , \qquad (5)$$

(4) y (5) son compatibles sólo si $d = 0$ ó 1 .

Si $d = 0$, (x_o,y_o,z_o) es solución de la ecuación. Si $d = 1$, entonces

$$a_1x_o^2 + a_2y_o^2 - a_3z_o^2 = a_1a_2a_3 \ ,$$

pero entonces

$$a_1(x_o z_o + a_2 y_o)^2 + a_2(y_o z_o - a_1 x_o)^2 - a_3(z_o^2 + a_1 a_2)^2 = 0$$

y luego, de esta relación, que es de fácil comprobación se obtiene una solución entera para la ecuación.

Como se menciona en la Introducción, este Teorema para el caso $n = 3$ fue originalmente resuelto por Legendre en 1798.

OBSERVACION 1. Es importante observar que en la demostración anterior no se utilizó la solubilidad de la ecuación en $\mathbb{Q}_2$, e.d. la solubilidad de la ecuación en tres variables en todos los cuerpos $\mathbb{Q}_p$, para p impar y en $\mathbb{Q}_\infty$ implica su solubilidad en $\mathbb{Q}_2$ y por lo tanto en $\mathbb{Q}$.

Existe este mismo resultado para cualquier primo q finito, y es consecuencia de lo visto hasta ahora y la Ley de Reciprocidad Cuadrática.

LEMA 7. Si la forma $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ representa cero en todos los cuerpos p-ádicos, $p = 2,3, \ldots, \infty$, salvo quizás en $\mathbb{Q}_q$, para algún primo q finito, entonces la forma también representa cero en $\mathbb{Q}_q$.

El siguiente Teorema es la base fundamental para la demostración del Teorema para $n = 4$, y para el propósito de generalizar el Teorema de Holzer a este caso.

TEOREMA 4 (Dirichlet). Sean a,b enteros, $b > 0$ y $(a,b) = 1$, entonces existen infinitos primos de la forma $a + kb$, $k \in \mathbb{N}$.

La demostración de este Teorema es bastante extensa y se puede encontrar por ejemplo en [A].

Demostración del Teorema 3.

Caso $n = 4$. Consideremos la ecuación

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 0 \qquad (6)$$

normalizada, e.d.

i) a_i libres de cuadrados,

ii) p primo y $p \mid a_1a_2a_3a_4$ entonces divide a lo más a dos coeficientes,

iii) $a_1 > 0$, $a_4 < 0$.

OBSERVACION 2. Si en la ecuación existen tres coeficientes divisibles por un primo p , multiplicando (6) por p y haciendo $x_ip = y_i$ se obtiene una ecuación con la condición (ii), este mismo tipo de observación puede hacerse para otro número de variables, obteniéndose así la ecuación normalizada.

Sean $p_1, p_2, \ldots, p_s$ los primos impares que dividen a $a_1a_2a_3a_4$, y para cada $p = 2$, $p_1, \ldots, p_s$ sea $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ una solución de la ecuación (6) en $\mathbb{Q}_p$.

Por Lema 6 podemos suponer todos los α_i distintos de cero, para cada p .

Consideremos las formas

$$h(x_1,x_2) = a_1x_1^2 + a_2x_2^2 \qquad y \qquad g(x_3,x_4) = -a_3x_3^2 - a_4x_4^2 \qquad (7)$$

y sea $b_p = h(\alpha_1,\alpha_2) = g(\alpha_3,\alpha_4)$.

OBSERVACION 3. Si $b_p = 0$ las formas (7) son isótropas y por lo tanto universales, así podemos suponer $b_p = 1$.

Si $b_p \neq 0$ podemos suponer que es un entero racional divisible a lo más por la potencia p^1 de p .

Esto último es fácil de ver, pues si $b_p = a_o + a_1 p + a_2 p^2 + \ldots \in \mathbb{Z}_p$

$b_p = a_o \left(1 + \frac{a_1}{a_o} p + \frac{a_2}{a_o} p^2 + \ldots \right)$ $(a_o \not\equiv 0 (\mathrm{mod}\ p))$ y por lemas 3 y 4,

$1 + \frac{a}{a_o} p + \frac{a_2}{a_o} p^2 + \ldots \in \mathbb{Q}_p^2$, dividiendo la ecuación por este término queda lo deseado, análogamente si $a_o = 0$.

Por el Teorema Chino de los restos existe $a > 0$ en $\mathbb{Z}$ que satisface

$$\begin{aligned} a &\equiv b_2 (\mathrm{mod}\ 2^4) \\ a &\equiv b_{p_i} (\mathrm{mod}\ p_i^2) \qquad 1 \leq i \leq s \ . \end{aligned} \tag{8}$$

Por la Observación 3, para cada $p = 2, p_1, \ldots, p_s$, $b_p^{-1} a$ es una unidad p-ádica y además

$$b_2^{-1} a \equiv 1 (\mathrm{mod}\ 8) \quad , \quad b_{p_i}^{-1} a \equiv 1 (\mathrm{mod}\ p_i)$$

y por lo tanto, por Lemas 3 y 4 , $b_2^{-1} a \in \mathbb{Q}_2^2$ y $b_{p_i}^{-1} a \in \mathbb{Q}_{p_i}^2$, $1 \leq i \leq s$. Luego

$$h\left(\alpha_1 \cdot \sqrt{b_p^{-1} a} \ , \ \alpha_2 \cdot \sqrt{b_p^{-1} a}\right) = g\left(\alpha_3 \cdot \sqrt{b_p^{-1} a} \ , \ \alpha_4 \cdot \sqrt{b_p^{-1} a}\right) = a$$

$$p = 2, p_1, \ldots, p_s \ ;$$

por lo tanto las formas

$$-ax_o^2 + h(x_1,x_2) \qquad y \qquad -ay_o^2 + g(x_3,x_4) \tag{9}$$

representan cero en $\mathbb{Q}_p$, $p = 2, p_1, \ldots, p_s$.

Si p es un primo tal que $p \nmid a$ y $p \neq p_1, \ldots, p_s$, entonces por Corolario 2 del Lema 1, las formas (9) representan cero en $\mathbb{Q}_p$.

Como supusimos $a_1 > 0$, $a_4 < 0$ y $a > 0$, las formas (9) son indefinidas por lo que también representan cero en $\mathbb{Q}_\infty$.

Si pudieramos elegir a , de tal forma que además en su descomposición en primos, hubiese un único primo q distinto de $p_1, \ldots, p_s$, entonces por Lema 7 las formas (9) representarían cero en $\mathbb{Q}_p$, $p = 2,3, \ldots, \infty$.

Tal elección de a es posible gracias al Teorema de Dirichlet.

Si a es el entero positivo solución del sistema (8), única módulo $m = 2^4 \prod_{i=1}^{s} p_i^2$, sea $d = (a,m)$.

Por Teorema 4 existe $k > 0 \in \mathbb{Z}$, tal que

$$q = \frac{a}{d} + k\,\frac{m}{d}$$

es primo, además $q \cdot d \equiv a \pmod{m}$.

Sea $a_o = qd$, entonces a_o cumple la condición deseada, así las formas (9) representan cero en $\mathbb{Q}$, ó equivalentemente las formas h y g representan a_o en $\mathbb{Q}$, y como

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = h(x_1,x_2) - g(x_3,x_4)$$

la ecuación (6) representa cero en $\mathbb{Q}$.

Caso $n = 5$. Consideremos la forma

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = 0$$

normalizada, y sin restricción supongamos $a_1 > 0$ y $a_5 < 0$. Sean

$$g(x_1,x_2) = a_1x_1^2 + a_2x_2^2 , \quad h(x_3,x_4,x_5) = -a_3x_3^2 - a_4x_4^2 - a_5x_5^2$$

Igual que en el caso $n = 4$ es posible encontrar un entero racional $a_o > 0$ representable por g y h en $\mathbb{Q}_\infty$ y $\mathbb{Q}_p$ $\forall_p$, salvo quizás en un cuerpo $\mathbb{Q}_p$, donde q es un primo impar que divide a $\prod_{i=1}^{5} a_i$.

Por Lema 7 la forma $-a_ox_o^2 + g$ representa cero en todos los cuerpos $\mathbb{Q}_p$, y en $\mathbb{Q}_\infty$, pues supusimos $a_1 > 0$ y $a_o > 0$. Por el Teorema para el caso $n = 3$, representa cero en $\mathbb{Q}$ ó equivalentemente g representa a_o en $\mathbb{Q}$.

Por Corolario 2 del Lema 1, la forma h representa cero en $\mathbb{Q}_q$, y por Lema 5 es universal en $\mathbb{Q}_q$, en particular representa a_o en $\mathbb{Q}_q$, así la forma $-a_ox_o^2 + h$ representa cero en todos los cuerpos p-ádicos, y por el Teorema para el caso $n = 4$, representa cero en $\mathbb{Q}$, o equivalentemente h representa a_o en $\mathbb{Q}$, de donde la forma

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2 = g - h$$

representa cero en $\mathbb{Q}$.

Caso $n > 5$. Para este caso basta ver que si F es una forma con más de 5 variables, $F = F_o + F_1$ donde F_o ó F_1 es una forma indefinida de 5 variables y así F_o ó F_1 y por lo tanto F representa cero en $\mathbb{Q}$.

COROLARIO. Toda forma $x_1^2 + \ldots + x_n^2 \in \mathbb{Q}[x_1, \ldots, x_n]$, no definida con $n \geq 5$ representa cero en $\mathbb{Q}$.

§ 3. CONTRAEJEMPLOS AL PRINCIPIO LOCAL GLOBAL.

Luego de ver el Teorema de Hasse-Minkowski, se podría pensar en una eventual generalización de éste a formas de grado mayor, pero esto no es posible.

Ejemplo 1. La forma

$$F(x,y,z) = 2x^3 + 4y^3 + 5z^3$$

representa cero en todos los cuerpos p-ádicos, pero no en $\mathbb{Q}$.

Este ejemplo fué dado por E.S. Selmer (Acta Math., 85(1951), 203-361). La demostración de que la forma es isótropa en $\mathbb{Q}_p$, $\forall$ p y en $\mathbb{Q}_\infty$ es relativamente sencilla, no así la demostración de que no representa cero en $\mathbb{Q}$ que es mucho más delicada.

Ejemplo 2. Es fácil dar ejemplos más sencillos como el siguiente: la forma $F = 41x_1^2 + 231x_2^2 + 123x_3^2 - 319x_4^2$ tiene ceros en $\mathbb{Q}_2$ pero no en $\mathbb{Q}_{41}$.

La forma $G = 6x_1^2 + 13x_2^2 + x_3^2 - 2x_4^2$ representa cero en todos los cuerpos

$\mathbb{Q}_p$ y en $\mathbb{Q}_\infty$, pero no en $\mathbb{Q}_2$.

Luego la forma

$$F(x_1,x_2,x_3,x_4)\cdot G(x_1,x_2,x_3,x_4)$$

tiene ceros en todos los cuerpos $\mathbb{Q}_p$ y en $\mathbb{Q}_\infty$, pero no en $\mathbb{Q}$ pues F ni G los tienen.

OBSERVACION. En el caso de formas binarias sobre $\mathbb{Q}$, se puede demostrar que el principio de Hasse se cumple para formas de grado ≤ 4 .

C A P I T U L O II

§ 1. LA ECUACION DIOFANTICA $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0$.

TEOREMA 6 (Horzel). Si la ecuación diofántica

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 = 0 \tag{10}$$

en su forma normal tiene solución entera, entonces tiene una solución x_1, x_2, x_3 tal que

$$|x_1| \leq \sqrt{|a_2a_3|} \; ; \quad |x_2| \leq \sqrt{|a_1a_3|} \; ; \quad |x_3| \leq \sqrt{|a_1a_2|} \, . \tag{11}$$

Demostración: (Mordell). Consideremos la ecuación (10) normalizada, y sea x_o, y_o, z_o una solución entera, se puede suponer $(x_o, y_o) = 1$, $a_1 > 0$, $a_2 > 0$ y $a_3 < 0$.

OBSERVACION 4. Si $|z_o| \leq \sqrt{|a_1a_2|}$ entonces de $a_1x_o^2 + a_2y_o^2 + a_3z_o^2 = 0$ se deduce que $a_1x_o^2 + a_2y_o^2 = -a_3z_o^2$, luego $a_1x_o^2 \leq -a_3z_o^2$ de donde $|x_o| \leq \sqrt{|a_2a_3|}$, análogamente se deduce $|y_o| \leq \sqrt{|a_1a_3|}$. Luego para demostrar el teorema basta ver que si x_o, y_o, z_o es una solución de (10)

y $|z_o| > \sqrt{|a_1 a_2|}$, entonces existe solución x,y,z con $|z| \leq \sqrt{|a_1 a_2|}$. Supongamos entonces $z_o > \sqrt{|a_1 a_2|}$.

Consideremos una solución de la forma

$$x = x_o + tX \ , \quad y = y_o + tY \ , \quad z = z_o + tZ$$

donde X,Y,Z son enteros a determinar.

Reemplazando x,y,z en la ecuación (10), como x_o,y_o,z_o es solución, se obtiene la condición

$$(a_1X^2 + a_2Y^2 + a_3Z^2)t + 2(a_1x_oX + a_2y_oY + a_3z_oZ) = 0 \ ,$$

despejando t y reemplazando en los términos x,y,z queda

$$x = \frac{x_o(a_1X^2 + a_2Y^2 + a_3Z^2) - 2X(a_1x_oX + a_2y_oY + a_3z_oZ)}{a_1X^2 + a_2Y^2 + a_3Z^2} \ ,$$

$$y = \frac{y_o(a_1X^2 + a_2Y^2 + a_3Z^2) - 2Y(a_1x_oX + a_2y_oY + a_3z_oZ)}{a_1X^2 + a_2Y^2 + a_3Z^2} \ ,$$

$$z = \frac{z_o(a_1X^2 + a_2Y^2 + a_3Z^2) - 2Z(a_1x_oX + a_2y_oY + a_3z_oZ)}{a_1X^2 + a_2Y^2 + a_3Z^2} \ .$$

Así, obviando un denominador obtenemos solución x,y,z dada por

$$\left.\begin{aligned} \delta x &= x_o(a_1X^2 + a_2Y^2 + a_3Z^2) - 2X(a_1x_oX + a_2y_oY + a_3z_oZ) \\ \delta y &= y_o(a_1X^2 + a_2Y^2 + a_3Z^2) - 2Y(a_1x_oX + a_2y_oY + a_3z_oZ) \\ \delta z &= z_o(a_1X^2 + a_2Y^2 + a_3Z^2) - 2Z(a_1x_oX + a_2y_oY + a_3z_oZ) \end{aligned}\right\} \qquad (12)$$

donde δ es un común denominador de las tres expresiones de la derecha. El siguiente paso, es demostrar que si δ es tal que

$$\delta \mid a_3 \qquad y \qquad \delta \mid Xy_o - Yx_o \qquad (13)$$

entonces x,y,z son tres números enteros; supongamos que (13) se cumple.

De $a_1x_o^2 + a_2y_o^2 + a_3z_o^2 = 0$ se deduce que $(\delta, a_1a_2x_oy_o) = 1$. De (12) vemos que basta demostrar que

$$\delta \mid a_1X^2 + a_2Y^2 \quad \text{y que} \quad \delta \mid a_1x_oX + a_2y_oY \ .$$

De (13) $X \equiv \dfrac{x_oY}{y_o} \pmod{\delta}$ y por lo tanto

$$a_1X^2 + a_2Y^2 \equiv a_1\left(\frac{x_oY}{y_o}\right)^2 + a_2Y^2 = \frac{Y^2}{y_o^2}(a_1x_o^2 + a_2y_o^2) \equiv 0 \pmod{\delta}$$

pues $\delta \mid a_3$.

Por otra parte

$$a_1x_oX + a_2y_oY \equiv a_1x_o\left(\frac{x_oY}{y_o}\right) + a_2y_oY = \frac{Y}{y_o}(a_1x_o^2 + a_2y_o^2) \equiv 0 \pmod{\delta} \ ,$$

que era lo deseado.

Ahora veremos que con δ, X, Y, Z apropiados y con las condiciones anteriores, z será tal que $|z| < |z_o|$.

Se puede obtener de (12) la siguiente igualdad

$$-\frac{\delta z}{a_3 z_o} = \left(z + \frac{a_1 x_o X + a_2 y_o Y}{a_3 z_o} \right)^2 + \frac{a_1 a_2}{a_3^2 z_o} (y_o X - x_o Y)^2 . \qquad (14)$$

Como $(x_o, y_o) = 1$, podemos encontrar X e Y tales que

$$y_o X - x_o Y = \delta .$$

Si a_3 es par, tomemos $\delta = \frac{a_3}{2}$ y Z tal que

$$\left| z + \frac{a_1 x_o X + a_2 y_o Y}{a_3 z_o} \right| \leq \frac{1}{2} .$$

Así, de (14)

$$\frac{1}{2} \left| \frac{z}{z_o} \right| < \frac{1}{4} + \frac{1}{4} \quad \text{y} \quad |z| < |z_o| .$$

Continuando este proceso se obtiene una solución con $|z| \leq \sqrt{|a_1 a_2|}$.

Si a_3 es impar, imponemos además la condición

$$a_1 X + a_2 Y + a_3 Z \equiv 0 \pmod 2 .$$

Esto define la paridad de Z . Como δ es impar, las tres expresiones de la derecha de (12) son divisibles por 2δ , y así obtenemos (14) con 2δ en vez de δ .

Tomamos ahora $\delta = a_3$ y Z tal que

$$\left| z + \frac{ax_o X + by_o Y}{a_3 z_o} \right| \leq 1$$

con la paridad asignada, así de (14) obtenemos finalmente

$$2\left|\frac{z}{z_o}\right| < 1 + 1 \qquad y \qquad |z| < |z_o| \ .$$

Esto completa la demostración.

Ejemplo: La ecuación $14x_1^2 + 3x_2^2 - 13x_3^2 = 0$ no es soluble en $\mathbb{Z}$, pues no posee solución no trivial tal que

$$|x_1| \leq \sqrt{39} \quad , \quad |x_2| \leq \sqrt{182} \quad , \quad |x_3| \leq \sqrt{42}$$

(fácilmente comprobable con un computador).

§ 2. LA ECUACION DIOFANTICA $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 0$. (15)

Soluciones de (15) en los cuerpos p-ádicos $p \mid 2a_1a_2a_3a_4$.

Sea p primo con $p \mid a_1a_2a_3a_4$ y consideremos la ecuación (15) normalizada, así p divide a lo más a dos de los coeficientes a_i .

Caso 1: p divide a un único coeficiente, sin restricción supongamos $p \mid a_4$.

Si $p \neq 2$, entonces la forma $a_2x_2^2 + a_3x_3^2$ es universal en $\mathbb{F}_p$, en efecto: Si $b = 0$ en $\mathbb{F}_p$ entonces

$$\#\{a_2x_2^2 / x_2 \in \mathbb{F}_p\} = \#\{b - a_2x_3^2 / x_3 \in \mathbb{F}_p\} = \frac{p-1}{2} \ ,$$

luego la intersección de estos dos conjuntos es no vacía y por lo tanto existen enteros α_2,α_3 tales que $0 \leq \alpha_2,\alpha_3 < p$ y

$$a_2\alpha_2^2 + a_3\alpha_3^2 = -a_1 - kp = -a_1\left(1 + \frac{k}{a_1}p\right) \quad \text{cierto } k \in \mathbb{Z} ,$$

por Lema 3 $1 + \frac{k}{a_1}p$ es un cuadrado en $\mathbb{Q}_p$ y así

$$a_1\left(\sqrt{1 + kp/a_1}\right)^2 + a_2\alpha_2^2 + a_3\alpha_3^2 = 0$$

es una representación de cero en $\mathbb{Q}_p$.

OBSERVACION 5. Eligiendo los α_i tales que $0 < \alpha_i < p$ y usando el Lema 6 se puede encontrar una representación de cero en $\mathbb{Q}_p$ con todas las variables no nulas.

Si $p = 2$, en este caso también hay solución, en efecto: sea

$$\alpha = \frac{a_1 + a_2}{2} ,$$

entonces

$$a_1 + a_3 + a_4\alpha^2 \equiv 2\alpha + 2\alpha^2 = 2\alpha(\alpha + 1) \equiv 0 \pmod 4$$

luego

$$a_1 + a_3 + a_4\alpha^2 = 4\beta \qquad \text{cierto } \beta \in \mathbb{Z} ,$$

y

$$a_1 + a_2(2\beta)^2 + a_3 + a_4\alpha^2 \equiv 4\beta + 4\beta^2 \equiv 0 \pmod 8 ,$$

luego

$$a_2(2\beta)^2 + a_3 + a_4\alpha^2 = -a_1 - 8t \qquad \text{cierto } t \in \mathbb{Z} .$$

Por Lema 4 $(1 + 8t/a_1)$ es un cuadrado en $\mathbb{Q}_2$ y así

$$a_1\left(\sqrt{1 + 8t/a_1}\right)^2 + a_2(2\beta)^2 + a_3 + a_4\alpha^2 = 0 ,$$

es una representación de cero en $\mathbb{Q}_2$.

Debemos observar aquí que en ambos casos es posible efectivizar en pocos pasos una solución para la ecuación (15) en $\mathbb{Q}_p$.

Caso 2: p divide a dos coeficientes.

Supongamos primero $p \neq 2$, y sin restricción $p \mid a_3$ y $p \mid a_4$.
La ecuación tiene la forma $a_1x_1^2 + a_2x_2^2 + a_3'px_3^2 + a_4'px_4^2 = 0$.

Por Lema 1 esta ecuación es soluble en $\mathbb{Q}_p$ sí y sólo si una de las ecuaciones $a_1x_1^2 + a_2x_2^2 = 0$ ó $a_3'x_3^2 + a_4'x_4^2 = 0$ tiene solución en $\mathbb{Q}_p$, y esto ocurre sí y sólo si $-a_1a_2$ ó $-a_3'a_4'$ es un cuadrado en $\mathbb{Q}_p$. Si por ejemplo $-a_1a_2 \in \mathbb{Q}_p^2$ entonces

$$a_1\left(\sqrt{-a_1a_2}\right)^2 + a_2a_1^2 = 0$$

es una solución de la ecuación (15) en $\mathbb{Q}_p$.

De esta forma, por Lema 3 y utilizando la fórmula de Euler, una condición necesaria para la solubilidad de la ecuación (15) en $\mathbb{Q}$ (equivalentemente en $\mathbb{Z}$) es que

$$(-a_1a_2)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \qquad \text{ó} \qquad (-a_3'a_4')^{\frac{p-1}{2}} \equiv 1 \pmod{p} .$$

Ejemplo 1. La ecuación $3x_1^2 - 6x_2^2 + 5x_3^2 - 7x_4^2 = 0$ no es soluble en $\mathbb{Z}$, pues para $p = 3$ ni $-(1\cdot-2)$ ni $-(5\cdot-7)$ son resto cuadrático módulo 3, e.d. $\left(\frac{2}{3}\right) = \left(\frac{35}{3}\right) = -1$.

Ejemplo 2.

$$41x_1^2 + 231x_2^2 + 123x_3^2 - 319x_4^2 = 0$$

no es soluble en $\mathbb{Z}$, pues $\left(\frac{38}{41}\right) = \left(\frac{12}{41}\right) = -1$.

Si $p = 2$, $p \mid a_3$ y $p \mid a_4$:

Por Lema 2 la forma representa cero en $\mathbb{Q}_2$ sí y sólo si existen y_1, y_2, y_3, y_4 donde al menos un y_i es impar, con

$$a_1y_1^2 + a_2y_2^2 + a_3y_3^2 + a_4y_4^2 \equiv 0 \pmod{16} .$$

Esto es fácil y rápidamente verificable con un pequeño programa computacional.

Los cuadrados módulo 16 son 0,1,4 y 9, si por ejemplo para una ecuación existen tales y_i, y $y_1 = 1$ ó 3 . Entonces

$$a_1y_1^2 + a_2y_2^2 + a_3y_3^2 + a_4y_4^2 \equiv 0 \pmod{16} .$$

Luego $a_2y_2^2 + a_3y_3^2 + a_4y_4^2 = -a_1y_1^2 - 8t$, cierto $t \in \mathbb{Z}$, por Lema 4 $\left(1 + 8t / a_1y_1^2\right)$ es un cuadrado en $\mathbb{Q}_2$, así

$$a_1\left(y_1 \cdot \sqrt{1 + 8t / a_1y_1^2}\right)^2 + a_2y_2^2 + a_3y_3^2 + a_4y_4^2 = 0$$

es una representación de cero en $\mathbb{Q}_2$.

Ejemplo 3. La ecuación

$$6x_1^2 + 13x_2^2 + x_3^2 - 2x_4^2 = 0$$

no es soluble en $\mathbb{Z}$, pues la congruencia

$$6x_1^2 + 13x_2^2 + x_3^2 - 2x_4^2 \equiv 0 \pmod{16}$$

no tiene ninguna solución con alguna de sus incógnitas impar.

OBSERVACIONES.

6. Del caso 1, se deduce que una ecuación indefinida de la forma (15) tal que $a_1a_2a_3a_4$ es par y $(a_i,a_j) = 1$ para $i \neq j$, siempre es soluble en $\mathbb{Q}$.

7. Si $2 \nmid a_1a_2a_3a_4$ la solubilidad de la congruencia $F \equiv 0 \pmod 8$ con al menos una incógnita impar, es condición suficiente para la solubilidad de la ecuación (15) en $\mathbb{Q}_2$ (Corolario del Lema 2).

§ 3. CONDICIONES NECESARIAS Y SUFICIENTES PARA LA SOLUBILIDAD DE LA ECUACION (15) EN $\mathbb{Z}$.

Resumamos los resultados anteriores como sigue. Escribamos las condiciones de § 2. para la ecuación (15) normalizada:

$$\left.\begin{array}{l} \text{Para todo primo } p \text{ que divide a dos de los coeficientes } a_{i_1} \text{ y } a_{i_2} \text{ , se debe tener} \\ \left(\dfrac{-a_{i_1}a_{i_2}}{p^2}\right)^{\frac{p-1}{2}} \equiv 1 \pmod p \quad \text{ó} \quad \left(-a_{i_3}a_{i_4}\right)^{\frac{p-1}{2}} \equiv 1 \pmod p \end{array}\right\} \qquad (16)$$

La congruencia $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \equiv 0 \pmod{16}$ debe tener una solución con al menos una de las incógnitas impar. (17)

LEMA 8.

i) Si la ecuación (15) tiene un único coeficiente par, es soluble en $\mathbb{Z}$ sí y sólo si cumple la condición (16).

ii) Si la ecuación (15) tiene dos o ningún coeficiente par, es soluble en $\mathbb{Z}$ sí y sólo si cumple ambas condiciones (16) y (17).

§ 4. GENERALIZACION DEL TEOREMA DE HOLZER A FORMAS CUADRATICAS CON CUATRO VARIABLES (ECUACION (15)).

Es posible obtener una generalización del Teorema 6 para una ecuación con cuatro incógnitas.

Si la ecuación (15) tiene solución en $\mathbb{Z}$, entonces vimos en la demostración del Teorema 3, para el caso $n = 4$, existe $a_o > 0 \in \mathbb{Z}$ tal que las ecuaciones

$$-a_ox_o + a_1x_1^2 + a_2x_2^2 = 0 \qquad y \qquad a_oy_o^2 + a_3x_3^2 + a_4x_4^2 = 0 ,$$

tienen solución.

Por Teorema de Holzer, estas ecuaciones tienen soluciones x_o, x_1, x_2 y y_o, x_3, x_4 en los dominios enteros

$$\left.\begin{array}{l} |x_o| \leq \sqrt{|a_1 a_2|} \; ; \quad |x_1| \leq \sqrt{|a_o a_2|} \; ; \quad |x_2| \leq \sqrt{|a_o a_1|} \\ \text{y} \\ |y_o| \leq \sqrt{|a_3 a_4|} \; ; \quad |x_3| \leq \sqrt{|a_o a_4|} \; ; \quad |x_4| \leq \sqrt{|a_o a_3|} \end{array}\right\} \qquad (18)$$

respectivamente.

Si x_o ó $y_o = 0$, entonces una de las formas (7) representa cero en $\mathbb{Q}$. Si $x_o, y_o \neq 0$, entonces

$$a_1(x_1 y_o)^2 + a_2(x_2 y_o)^2 + a_3(x_3 x_o)^2 + a_4(x_4 x_o)^2 = 0$$

es una solución para (15).

Así, de (18) se obtiene una solución $\omega_1, \omega_2, \omega_3, \omega_4$ para la ecuación (15) con

$$|\omega_1| \leq \sqrt{|a_o a_2 a_3 a_4|} \quad , \qquad |\omega_2| \leq \sqrt{|a_o a_1 a_3 a_4|}$$

$$|\omega_3| \leq \sqrt{|a_o a_1 a_2 a_4|} \quad , \qquad |\omega_4| \leq \sqrt{|a_o a_1 a_2 a_3|}$$

Para que estas cotas tengan sentido, es preciso acotar el número a_o , recordemos que $a_o = qd$, $d = (m,a)$ donde $m = 16\Pi p_i^{\alpha_i}$, $p_i \mid a_1 a_2 a_3 a_4$ (ver § 2, Cap. 1) . Así, conociendo la máxima magnitud que tiene el primo $q = \frac{a}{d} + k\frac{m}{d}$, se puede acotar a_o .

El problema de acotar mediante una función al primo más pequeño que aparece en la progresión aritmética de Dirichlet, ha sido estudiado por muchos matemáticos, entre ellos, Linnik, Graham, Chowla y Jing Run.

Si a y b son enteros, $(a,b) = 1$, $b > 0$ y $P(a,b)$ denota al primo más pequeño de la forma $a + kb$, Linnik demostró que existe constante c con

$$P(a,b) \ll b^{c} .$$

Graham demostró que $c \ll 20$, y Chowla conjetura que

$$P(a,b) \ll b^{1+\varepsilon} \qquad \text{para cada } \varepsilon > 0 .$$

En 1979, Chen Jing Run demuestra el siguiente resultado:

TEOREMA 7 (Jing-Run).

$$P(a,b) \ll b^{17} .$$

La demostración de este Teorema puede verse en [J-R].

De este Teorema tenemos entonces que

$$q \ll \left(\frac{m}{d}\right)^{17} \qquad \text{y} \qquad a_o \ll \left(\frac{m}{d}\right)^{16} \cdot m .$$

De esta forma se tiene el siguiente

TEOREMA 8. Si la ecuación (15) en su forma normal es soluble en $\mathbb{Z}$, entonces tiene una solución $\omega_1, \omega_2, \omega_3, \omega_4$ tal que

$$\left.\begin{aligned} |\omega_1| &\ll \left(\frac{m}{d}\right)^{8} \sqrt{|a_2 a_3 a_4| m} \quad ; \quad |\omega_2| \ll \left(\frac{m}{d}\right)^{8} \sqrt{|a_1 a_3 a_4| m} \\ |\omega_3| &\ll \left(\frac{m}{d}\right)^{8} \sqrt{|a_1 a_2 a_4| m} \quad ; \quad |\omega_4| \ll \left(\frac{m}{d}\right)^{8} \sqrt{|a_1 a_2 a_3| m} \end{aligned}\right\} \qquad (19)$$

§ 5. SOLUCION EFECTIVA DE LA ECUACION (15) EN $\mathbb{Z}$.

Para solucionar efectivamente una ecuación (15), debemos igual que en el caso de tres variables, calcular el dominio (19) respectivo y chequear computacionalmente si existe allí una solución no nula.

El inconveniente evidente que presenta este dominio es la magnitud que pueden llegar a tener estas cotas, lo que no es problema utilizando un pequeño programa en un computador.

El otro cálculo necesario es el del número d que aparece en la demostración del Teorema 3, caso $n = 4$.

Esto se puede hacer fácilmente dando el siguiente algoritmo. Recordemos que $d = (a_o, m)$, donde a_o es solución del sistema (8), luego lo primero es el cálculo de los números b_p , $p = 2, p_1, \ldots, p_s$ (ver demostración Teorema 4, caso $n = 3$) .

Sea p primo , $p \mid a_1 a_2 a_3 a_4$, y supongamos que la ecuación (15) es soluble en $\mathbb{Z}$.

Caso 1: p divide a un único coeficiente, $p \neq 2$. Si $p \mid a_4$, vimos en § 2, Cap. II que existe en $\mathbb{Q}_p$ una solución de la forma

$$a_1\left(\sqrt{1 + kp / a_1}\right)^2 + a_2\alpha_2^2 + a_3\alpha_3^2 = 0 ,$$

luego

$$h\left(\sqrt{1 + kp / a_1}\,/\,\alpha_3 \, , \, \alpha_2 / \alpha_3\right) = g(1,0) = -a_3 ,$$

donde h y g son las formas (7), luego se puede elegir $b_p = -a_3$.

Análogamente se puede elegir:

Si $\quad p \mid a_3 \ , \quad b_p = -a_4$

$\quad p \mid a_1 \ , \quad b_p = a_2$

$\quad p \mid a_2 \ , \quad b_p = a_1 \ .$

Si $p = 2$, sin restricción $p \mid a_4$:

Vimos que en este caso existe una solución de la forma

$$a_1\left(\sqrt{1 + 8t/a_1}\right)^2 + a_2(2\beta)^2 + a_3 + a_4\alpha^2 = 0$$

con $\alpha = \dfrac{a_1 + a_3}{2}$.

Dividiendo si es necesario por una potencia par de 2, se puede suponer que $a_3 + a_4\alpha^2$ es divisible a lo más por la potencia 2^1 de 2, y se puede elegir

$$b_2 = g(1,\alpha) = -a_3 - a_4\alpha^2 \ .$$

Caso 2: p divide a dos coeficientes, $p \neq 2$. Si p divide a los coeficientes de h , $a_1 = pa_1'$ y $a_2 = pa_2'$; según (16) hay dos posibilidades:

Si $\left(\dfrac{-a_1'a_2'}{p}\right) = 1$, entonces

$$a_1\left(\sqrt{-a_1a_2}\right)^2 + a_2a_1^2 = 0 \qquad \text{en } \mathbb{Q}_p \ .$$

Por Lema 6 encontramos $\alpha_1, \alpha_2, \alpha_3 \neq 0$ en $\mathbb{Q}_p$ tales que

$$a_1\alpha_1^2 + a_2\alpha_2^2 + a_3\alpha_3^2 = 0 \ ,$$

de donde $\qquad h(\alpha_1/\alpha_3,\ \alpha_2/\alpha_3) = -a_3 \ .$

Elegimos entonces $b_p = -a_3$ (o $b_p = -a_4$) . En forma análoga se deducen los demás casos (ver tabla resumen).

Si p divide a un coeficiente de h y uno de g , entonces se puede elegir siempre b_p como el coeficiente de h con el cual se cumple una de las condiciones (16), por ejemplo: Si $p \mid a_1$ y $p \mid a_3$, y $\left(\frac{-a_2a_4}{p}\right) = 1$, entonces $b_p = a_2$ ya que

$$a_2\left(\sqrt{-a_2a_4}\right)^2 + a_4a_2^2 = 0 \qquad \text{en } \mathbb{Q}_p$$

luego

$$h(0,1) = g\left(0,\ a_2 / \sqrt{-a_2a_4}\right) = a_2 .$$

<u>Si $p = 2$</u> : Casos $p \nmid a_1a_2a_3a_4$ y p divide a dos coeficientes, se puede suponer siempre $p \mid a_3$ y $p \mid a_4$.

Si y_1,y_2,y_3,y_4 es la solución de la congruencia en (17), podemos suponer $y_i \neq 0$, $1 \leq i \leq 4$.

Si y_1 ó y_2 es impar, entonces elegir $b_p = g(y_3,y_4)$.

Si y_1 y y_2 son pares, entonces y_3 ó y_4 es impar, elegir $b_p = \frac{1}{4}\, h(y_1,y_2)$. (20)

OBSERVACION. Si $2 \mid a_3$ y $2 \mid a_4$, y la congruencia $a_1x_1^2 + a_2x_2^2 \equiv 0 \pmod 8$ es satisfecha con y_1 ó y_2 impar por Corolario del Lema 2, y Lema 6 se puede tomar $b_p = -a_3$.

Si $2 \nmid a_1a_2a_3a_4$ y y_1, y_2, y_3, y_4 es solución de la congruencia $F \equiv 0 \pmod 8$ con algún y_i impar, se elige b_p igual que en (20) para este caso.

TABLA RESUMEN. $p \neq 2$

p		b_p
a_1, a_2	$\left(\frac{-a_1'a_2'}{p}\right) = 1$ / $\left(\frac{-a_3a_4}{p}\right) = 1$	$-a_3$ / a_1
a_1, a_3	$\left(\frac{-a_1'a_2'}{p}\right) = 1$ / $\left(\frac{-a_2a_4}{p}\right) = 1$	a_1 / a_2
a_1, a_4	$\left(\frac{-a_1'a_4'}{p}\right) = 1$ / $\left(\frac{-a_2a_3}{p}\right) = 1$	a_1 / a_2
a_2, a_3	$\left(\frac{-a_2'a_3'}{p}\right) = 1$ / $\left(\frac{-a_1a_4}{p}\right) = 1$	a_2 / a_1
a_2, a_4	$\left(\frac{-a_2'a_4'}{p}\right) = 1$ / $\left(\frac{-a_1a_3}{p}\right) = 1$	a_2 / a_1
a_3, a_4	$\left(\frac{-a_3'a_4'}{p}\right) = 1$ / $\left(\frac{-a_1a_2}{p}\right) = 1$	a_1 / $-a_3$
a_1		a_2
a_2		a_1
a_3		$-a_4$
a_4		$-a_3$

$p = 2$

$2 \mid a_4$	$b_2 = -a_3 - a_4\left(\frac{a_1 + a_3}{2}\right)^2$ *
$2 \mid a_3, a_4$	ver (20)
$2 \nmid a_1 a_2 a_3 a_4$	*

* En ambos casos, dividir si es necesario a b_2, de modo que $4 \nmid b_2$.

A P E N D I C E

§ 1. EJEMPLOS.

Aplicación del Lema 8:

1. La ecuación

$$21x_1^2 + 5x_2^2 + x_3^2 - 2x_4^2 = 0$$

es del tipo (i) del Lema, además $(21,5) = (21,2) = (5,2) = 1$, luego por Observación 6, es soluble en $\mathbb{Z}$.

2. La ecuación

$$3x_1^2 + 17x_2^2 - 13x_3^2 - 31x_4^2 = 0$$

es del tipo (ii), además $3 \cdot 2^2 + 17 - 13 = 16$, así cumple condición (17), por Observación 6 es soluble en $\mathbb{Z}$.

3. $$67x_1^2 + 53x_2^2 + 17x_3^2 - 101x_4^2 = 0$$

Es del tipo (ii), cumple (17) pues $17 - 101 = 48 \equiv 0 \pmod{16}$, tiene solución en $\mathbb{Z}$.

4. $$6x_1^2 + 10x_2^2 + 3x_3^2 - 7x_4^2 = 0$$

Es del tipo (ii), cumple (16) para $p = 3$ (es el único primo $\neq 2$ que divide a dos coeficientes), además claramente satisface (17) y por lo tanto es soluble en $\mathbb{Z}$.

5. $$37x_1^2 + 15x_2^2 + 47x_3^2 - 51x_4^2 = 0$$

Es del tipo (ii) y $37 + 15 + 47 - 51 = 48 \equiv 0 \pmod{16}$, luego es soluble en $\mathbb{Z}$.

6. $$71x_1^2 + 13x_2^2 - 11x_3^2 + 2x_4^2 = 0$$

Es del tipo (ii), por Observación 6 es soluble en $\mathbb{Z}$.

7. Encontremos ahora, un dominio entero donde la ecuación del ejemplo 1 es soluble:

Los primos impares a considerar son $3,7,5$ y 2 . Por la tabla resumen encontramos

$$b_3 = b_7 = 5 \ , \quad b_5 = 21 \ , \quad b_2 = -1 + 2\left(\frac{21 + 1}{2}\right)^2 = 241 \equiv 1 \pmod{16} \ .$$

Resolviendo el sistema

$$x \equiv 1 \pmod{16}$$

$$x \equiv 5 \pmod{49}$$

$$x \equiv 5 \pmod{9}$$

$$x \equiv 21 \pmod{5}$$

encontramos que $x \equiv 33521 \pmod{m}$ y $m = 176.400$, luego si $a = 33521$ y $d = (a,m) = 1$, el primer primo $q \equiv \frac{a}{d} \left(\mod \frac{m}{d}\right)$ es

$\ll a^{17}$, así la ecuación debe tener una solución x_1, x_2, x_3, x_4 tal que

$$|x_1| \ll m^8 \ 420 \sqrt{10} \ ; \quad |x_2| \ll m^8 \ 420 \sqrt{42}$$

$$|x_3| \ll m^8 \ 420 \sqrt{210} \ ; \quad |x_4| \ll m^8 \ 420 \sqrt{105} \ ,$$

con ayuda de un computador es fácil ver que hay muchas soluciones de la ecuación en este dominio, y que la magnitud de la más pequeña, $(1,2,3,5)$ está muy por debajo de las cotas (como lo dice el signo $\ll$) . Lo interesante sería poder optimizar de alguna forma estas cotas, a lo menos para alguna familia de ecuaciones (15).

8. Consideremos la ecuación más sencilla

$$x_1^2 + x_2^2 - 7x_3^2 + 2x_4^2 = 0 \ .$$

Los primos a considerar son 2 y 7, $b_2 \equiv -3$ y $b_7 = 1$. La solución de

$$x \equiv -3 \pmod{16}$$

$$x \equiv 1 \pmod{49} \quad \text{es} \quad 589 \pmod{784} \ , \quad (589,784) = 1$$

luego la ecuación es soluble en

$$|x_1| \ll 28 \ m^8 \sqrt{14} \quad ; \quad |x_2| \ll 28 m^8 \sqrt{14}$$

$$|x_3| \ll 28 \ m^8 \sqrt{2} \quad ; \quad |x_4| \ll 28 m^8 \sqrt{7} \ .$$

La ecuación tiene muchas soluciones en este dominio, algunas son las siguientes

x_1	x_2	x_3	x_4
1	2	1	1
1	2	7	13
1	3	2	3
1	3	6	11
1	11	10	17
1	18	7	3
1	19	10	13

Para cada una de las ecuaciones siguientes, es posible calcular en su dominio (19) respectivo, con la ayuda de un sencillo programa computacional mediante un sistema de "barrido" (ver pág. 45), un conjunto de soluciones enteras:

$$13x_1^2 - 27x_2^2 - 15x_3^2 + 11x_4^2 = 0$$

2	7	2	11
3	12	3	19
3	4	12	15
4	2	5	5
4	3	4	5
6	1	6	3
6	4	3	3
6	8	9	15
7	2	6	1
7	8	4	11

$x_1^2 + x_2^2 + 2x_3^2 - 7x_4^2 = 0$

1	2	1	1
1	2	13	7
1	3	3	2
1	3	11	6
1	11	17	0
1	18	3	7
1	19	13	10

$3x_1^2 + 3x_2^2 + 5x_3^2 - 11x_4^2 = 0$

1	1	1	1
2	3	1	2
2	3	10	7
2	6	14	10

$11x_1^2 + 5x_2^2 - x_3^2 - 3x_4^2 = 0$

1	1	2	2
1	2	2	3
1	10	2	13
1	1	4	0
1	8	16	5
1	7	16	0

$37x_1^2 + 15x_2^2 + 47x_3^2 - 51x_4^2 = 0$

1	5	1	3
2	5	4	5
2	10	2	6
3	2	3	4
3	8	9	10

$3x_1^2 + 5x_2^2 + 13x_3^2 - 11x_4^2 = 0$	1	14	3	10
	3	2	2	3
	17	4	7	12
	3	11	6	10
	13	5	6	10
$13x_1^2 + 11x_2^2 + 19x_3^2 - 33x_4^2 = 0$	11	2	0	7
	11	7	0	8
	11	10	0	9
	11	17	0	2
$x_1^2 + x_2^2 + 2x_3^2 - 31x_4^2 = 0$	2	3	3	1
	2	5	1	1
	2	7	19	5
$5x_1^2 - 7x_2^2 + 3x_3^2 + 10x_4^2 = 0$	1	3	4	1
	1	12	11	8
	2	3	1	2
$3x_1^2 + 6x_2^2 + 5x_3^2 - 7x_4^2 = 0$	1	8	6	9
	2	1	3	3
	2	5	9	9
$-11x_1^2 + 2x_2^2 + x_3^2 + 2x_4^2 = 0$	1	1	1	2
	5	11	5	2
	1	0	3	1

$11x_1^2 - 33x_2^2 + 7x_3^2 + x_4^2 = 0$	1	2	4	3
	1	6	12	3
	1	2	0	11
$13x_1^2 + 6x_2^2 + 2x_3^2 - 7x_4^2 = 0$	1	6	13	9
	1	8	15	11
	1	0	5	3
$2x_1^2 + 3x_2^2 + 7x_3^2 - x_4^2 = 0$	1	3	1	6
	1	0	1	3
	1	4	5	15
$11x_1^2 - 6x_2^2 - 13x_3^2 + 10x_4^2 = 0$	1	3	3	4
	1	8	3	7
$x_1^2 + x_2^2 + 3x_3^2 - 10x_4^2 = 0$	1	3	20	11
	1	6	1	2
$6x_1^2 + 3x_2^2 - 7x_3^2 + 10x_4^2 =$	1	2	18	15
	1	2	2	1
$5x_1^2 + 5x_2^2 + 33x_3^2 - 2x_4^2 = 0$	1	3	4	17
	1	3	0	5
$6x_1^2 - 5x_2^2 + 7x_3^2 + x_4^2 = 0$	2	4	1	7
	4	5	2	1
$x_1^2 + 3x_2^2 + 5x_3^2 - 14x_4^2 = 0$	1	1	10	6
	1	0	5	3

$13x_1^2 + 3x_2^2 + x_3^2 - 2x_4^2 = 0$	1	1	4	4
	1	2	5	5
$3x_1^2 + 17x_2^2 - 13x_3^2 - 31x_4^2 = 0$	3	1	1	1
$67x_1^2 + 53x_2^2 + 17x_3^2 - 101x_4^2 = 0$	9	4	15	10
$-x_1^2 - 2x_2^2 + 7x_3^2 + 103x_4^2 = 0$	2	9	3	1
$13x_1^2 - 117x_2^2 + 47x_3^2 - 111x_4^2 = 0$	2	3	4	1
$14x_1^2 - 87x_2^2 + 23x_3^2 + 41x_4^2 = 0$	4	4	7	1
$7x_1^2 + 6x_2^2 - 5x_3^2 + 11x_4^2 = 0$	2	1	3	1
$21x_1^2 + 5x_2^2 + x_3^2 - 2x_4^2 = 0$	1	2	3	5
$3x_1^2 + 5x_2^2 + x_3^2 - 2x_4^2 = 0$	2	1	1	3
$3x_1^2 + 15x_2^2 + 7x_3^2 - 2x_4^2 = 0$	2	5	3	15
$5x_1^2 + 5x_2^2 + 7x_3^2 - 11x_4^2 = 0$	2	4	5	5
$-6x_1^2 + 7x_2^2 + 11x_3^2 + 5x_4^2 = 0$	4	1	2	3

§ 2. PROBLEMA FINAL.

Motivado un poco por la natural generalización del Teorema de Holzer y la simetría que encerraría un resultado de esta forma, y por lo que se comprobó para una cantidad considerable de ejemplos (más de 300) con la valiosa ayuda de un computador, es que me atrevo a plantear el siguiente problema:

PROBLEMA.

Demostrar o dar un contraejemplo a la siguiente afirmación:

Si la ecuación diofántica (en su forma normal)

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = 0$$

es soluble no trivialmente, entonces tiene una solución en el dominio entero

$$|x_1| \leq \sqrt{|a_2a_3a_4|} \quad ; \quad |x_2| \leq \sqrt{|a_1a_3a_4|}$$

$$|x_3| \leq \sqrt{|a_1a_2a_4|} \quad ; \quad |x_4| \leq \sqrt{|a_1a_2a_3|} \ .$$

El siguiente es el programa en lenguaje Pascal utilizado para en - contrar soluciones de la ecuación (15) en el dominio entero del problema propuesto en la página anterior.

```
program cuatro;
 var
  x, y, z, w, a, b, c, d : real;
begin
 a := -1;
 b := -1;
 c := -1;
 d := -1;
 writeln('ingrese a1,a2,a3,a4');
 read(x, y, z, w);
 writeln;
 repeat
  a := a + 1;
  b := -1;
  c := -1;
  d := -1;
  repeat
   b := b + 1;
   c := -1;
   d := -1;
   repeat
    c := c + 1;
    d := -1;
    repeat
     d := d + 1;
     if ((a * a * x) + (b * b * y) + (c * c * z) + (d * d * w)) = 0 then
      writeln(a : 2 : 1,'  ', b : 2 : 1,'  ', c : 2 : 1,'  ', d : 2 : 1);
    until (d > sqrt(abs(a * b * c)));
   until (c > sqrt(abs(a * b * d)));
  until (b > sqrt(abs(a * c * d)));
 until (a > sqrt(abs(b * c * d)));
end.
```

B I B L I O G R A F I A

[A] Apostol, T.M., Introduction to analytic number theory, New York, Springer-Verlag, 1976.

[B] Baeza, R., Métodos local globales en Aritmética, Curso 12a. Semana de la Matemática, Universidad Católica de Valparaíso, 1985.

[B-S] Borevitch, Z.I., Chafarevitch, I.R., Théorie des nombres, Paris, Gauthier-Villars, 1967.

[H] Holzer, L., Minimal solutions of diophantine equations. Canadian Journal of Mathematics 2, (1950), 238-244.

[J-R] Jingrun, Ch., On the least prime in an arithmetical progression and theorems concerning the zeros of Dirichlet's L' functions (II), Scientia Sinica 22, (1979), 859-889.

[K] Kneser, M., Kleine Losungen der diophantischen Gleichung $ax^2 + by^2 = cz^2$, Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg 23, (1959), 163-173.

[L-O] Lagarias, J.C., Odlyzko, A.M., Effective versions of the Chebotarev density theorem, Algebraic Number Fields. Ed. A. Frohlich, Academic Press (1977), 409-464.

[M] Mordell, L.J., On the magnitude of the integer solutions of the equations $ax^2 + by^2 + cz^2 = 0$, Journal of Number Theory 1, (1969), 1-3.