SOLUBILIDAD EN ENTEROS NO NULOS, MEDIANTE FORMAS CUADRATICAS BINARIAS, DE ECUACIONES PITAGORICAS DE GRADO SUPERIOR

por

FEDERICO PEREZ CASTRO

A) EXPOSICION GENERAL

En este apartado se desarrolla un método para resolver ecuaciones del tipo $aX^2 + cXY + bY^2 = Z^n$, donde a, b, c son enteros conocidos y n es un entero también conocido y positivo.

B) SOLUCION DE ALGUNAS ECUACIONES

Aplicando el método anterior se resuelven las siguientes ecuaciones:

1.º $aX^2 + bY^2 = Z^{2n+1}$

2.º $X^2 + abY^2 = Z^{2n}$

3.º $aX^2 + bY^2 = (ac^2 + bd^2)\, Z^{2n}$

4.º $X^2 + abY^2 = (ac^2 + bd^2)\, z^{2n+1}$

donde a, b, c, d son enteros conocidos y n un entero también conocido y positivo.

C) CRITERIOS DE SOLUBILIDAD DE LA ECUACION $aX^2 + cXY + bY^2 = Z^n$

En este apartado se estudian las condiciones que deben cumplir los coeficientes de la forma para que la ecuación $aX^2 + cXY + bY^2 = Z^n$ sea soluble en el campo Z^*.

A) EXPOSICION GENERAL

Dada una forma cuadrática binaria: $G(\alpha, \beta) = a\alpha^2 + c\alpha\beta + b\beta^2$, supongamos que:

$$G(\alpha, \beta) \cdot G(\alpha, \beta) = G(X_2, Y_2) \quad (I)^*$$

luego $[G(\alpha, \beta)]^2 = G(X_2, Y_2) = Z^2$, siendo $Z = G(\alpha, \beta)$.

Análogamente, y en el supuesto (I):

$$G(\alpha, \beta) \cdot G(\alpha, \beta) \cdot G(\alpha, \beta) = G(X_2, Y_2) \cdot G(\alpha, \beta) = G(X_3, Y_3) = Z^3$$

y en general:

$$\overbrace{G(\alpha, \beta) \cdot \ldots\ldots G(\alpha, \beta)}^{n} = G(X_{n-1}, Y_{n-1}) \cdot G(\alpha, \beta) = G(X_n, Y_n) = Z^n \quad [3]$$

Pero:

$$X_2 = e_2(a, b, c, \alpha, \beta) \qquad X_3 = e_3(a, b, c, \alpha, \beta, X_2, Y_2)$$

$$Y_2 = f_2(a, b, c, \alpha, \beta) \qquad Y_3 = f_3(a, b, c, \alpha, \beta, X_2, Y_2)$$

y en general:

$$\begin{aligned} X_n &= e_n(a, b, c, \alpha, \beta, X_{n-1}, Y_{n-1}) \\ Y_n &= f_n(a, b, c, \alpha, \beta, X_{n-1}, Y_{n-1}) \end{aligned} \qquad [2]$$

El grupo de ecuaciones [2] definen unas funciones de recurrencia entre las X_i e Y_i, mediante convenientes eliminaciones, podemos hallar la escala o ley de recurrencia y, por tanto, la ecuación característica $\varepsilon(r) = 0$, y, finalmente, el término general.

Luego:

$$X_n = E(a, b, c, \alpha, \beta, n) \qquad Y_n = F(a, b, c, \alpha, \beta, n)$$

y como $Z = G(\alpha, \beta) = G(a, b, c, \alpha, \beta)$, se tiene por [3] que la ecuación $G(X_n, Y_n) = Z^n$, o lo que es igual:

$$aX^2_n + cX_nY_n + bY^2_n = Z^n$$

tiene como soluciones:

$$X_n = E(a, b, c, \alpha, \beta, n); \quad Y_n = F(a, b, c, \alpha, \beta, n); \quad Z = G(a, b, c, \alpha, \beta)$$

---

* La condición (I), hipótesis esencial del problema, será desarrollada en el apartado C.

Usando el método de coeficientes indeterminados se obtendrán las condiciones que deben cumplir los coeficientes de la forma cuadrática para que le sea aplicable el método.

B) SOLUCION DE ALGUNAS ECUACIONES

Aplicando la teoría expuesta en el apartado A, vamos a resolver las ecuaciones pitagóricas siguientes:

$$\begin{aligned}
&1.^{a}\quad X^2 + abY^2 = Z^{2n}\\
&2.^{a}\quad aX^2 + bY^2 = Z^{2n+1}\\
&3.^{a}\quad aX^2 + bY^2 = (ac^2 + bd^2)\, Z^{2n}\\
&4.^{a}\quad X^2 + abY^2 = (ac^2 + bd^2)\, Z^{2n+1}
\end{aligned} \qquad [4]$$

siendo a, b, c, d números enteros conocidos y n un entero positivo también dado.

Para ello procedamos de la forma siguiente:

Tomemos la forma cuadrática binaria $G(\alpha, \beta) = a\alpha^2 + b\beta^2$ y se tendrá:

$$(a\alpha^2 + b\beta^2)\cdot(a\alpha^2 + b\beta^2) = (a\alpha^2 - b\beta^2)^2 + ab(2\alpha\cdot\beta)^2 = X^2{}_2 + abY^2{}_2 = Z^2$$

$$\begin{aligned}(a\alpha^2 + b\beta^2)\cdot(a\alpha^2 + b\beta^2)\cdot(a\alpha^2 + b\beta^2) &= (X_2{}^2 + abY_2{}^2)\cdot(a\alpha^2 + b\beta^2) =\\ &= a(\alpha X_2 - b\beta Y_2)^2 + b(\beta X_2 + a\alpha Y_2)^2 = aX^2{}_3 + bY^2{}_3 = Z^3\end{aligned}$$

$$\begin{aligned}&(a\alpha^2 + b\beta^3)\cdot(a\alpha^2 + b\beta^3)\cdot(a\alpha^2 + b\beta^2)\cdot(a\alpha^2 + b\beta^2) = (aX^2{}_3 + bY^2{}_3)\cdot\\ &\cdot(a\alpha^2 + b\beta^2) = (a\alpha X_3 - b\beta Y_3)^2 + a\cdot b(\alpha Y_3 + \beta X_4)^2 = X^2{}_4 + abY^2{}_4 = Z^4\end{aligned}$$

en general:

$$\begin{aligned}&\overbrace{(a\alpha^2 + b\beta^2)\ldots\ldots(a\alpha^2 + b\beta^2)}^{2n} = (aX^2{}_{2n-1} + bY^2{}_{2n-1})\cdot(a\alpha^2 + b\beta^2) =\\ &= (a\alpha X_{2n-1} - b\beta Y_{2n-1})^2 + ab(\alpha Y_{2n-1} + \beta X_{2n-1})^2 = X^2{}_{2n} + abY^2{}_{2n} = Z^{2n}\end{aligned}$$

$$\begin{aligned}&\overbrace{(a\alpha^2 + b\beta^2)\ldots\ldots(a\alpha^2 + b\beta^2)}^{2n+1} = (X^2{}_{2n} + abY^2{}_{2n})\cdot(a\alpha^2 + b\beta^2) = a(\alpha X_{2n} -\\ &- b\beta Y_{2n})^2 + b(a\alpha Y_{2n} + \beta X_{2n})^2 = aX^2{}_{2n+1} + bY^2{}_{2n+1} = Z^{2n+1}\end{aligned}$$

Luego:

$$\begin{aligned}X_{2n} &= a\alpha X_{2n-1} - b\beta Y_{2n-1}\ (p) \qquad & X_{2n+1} &= \alpha X_{2n} - b\beta Y_{2n}\ (i)\\ Y_{2n} &= \alpha\cdot Y_{2n-1} + \beta X_{2n-1}\ (pp) \qquad & Y_{2n+1} &= a\alpha Y_{2n} + \beta X_{2n}\ (ii)\end{aligned}$$

De (i), (ii), (p), (pp) se tiene:

$$X_{2n+2} - 2(a\alpha^2 - b\beta^2)\cdot X_{2n} + (a\alpha^2 + b\beta^2)^2\cdot X_{2n-2} = 0$$

que es la ley o escala de recurrencia, la ecuación característica será:

$$\varepsilon(r) = r^2 - 2(a\alpha^2 - b\beta^2)\, r + (a\alpha^2 + b\beta^2) = 0$$

luego:

$$r = (\alpha\sqrt{a} \pm i\,\beta\sqrt{b})^2 = \rho^2(\cos\omega \pm i\,\mathrm{sen}\,\omega)^2 = \rho^2(\cos 2\omega \pm i\,\mathrm{sen}\,2\omega)$$

siendo:

$$\rho^2 = a\alpha^2 + b\beta^2$$

y

$$tg\ \omega = \frac{\beta\sqrt{b}}{\alpha\sqrt{a}}$$

conociendo las raíces de $\varepsilon(r) = 0$ y los dos primeros términos de la serie se halla el término general, que será:

$$X_{2n} = (a\alpha^2 + b\beta^2)^n \cos 2n\ \omega$$

como

$$Z_{2n} = G(\alpha, \beta) = a\alpha^2 + b\beta^2$$

se tendrá:

$$Y_{2n} = \frac{(a\alpha^2 + b\beta^2)^n}{\sqrt{a \cdot b}} \operatorname{sen} 2n\ \omega$$

Desarrollando sen $2n\ \omega$ y cos $2n\ \omega$ en función de sen ω y cos ω se tiene:

$$X_{2n} = \sum_{k=0}^{k=n} (-1)^k \binom{2n}{2k} a^{n-k} \cdot b^k \cdot \alpha^{2(n-k)} \cdot \beta^{2k}$$

$$Y_{2n} = \sum_{k=0}^{k=n-1} (-1)^k \binom{2n}{2k+1} a^{n-k-1} \cdot b^k \cdot \alpha^{2(n-k)-1} \cdot \beta^{2k+1}$$

$$Z = a\alpha^2 + b\beta^2$$

Ejemplo: para $n = 3$

$$X^2 + abY^2 = Z^6$$

$$X = a^3\alpha^6 - 15\ a^2 b\alpha^4 \cdot \beta^2 + 15\ ab^2\alpha^2 \cdot \beta^4 - b^3 \cdot \beta^6$$

$$Y = 6a^2\alpha^5 \cdot \beta - 20\ ab\ \alpha^3 \cdot \beta^3 + 6b^2 \cdot \alpha \cdot \beta^5$$

$$Z = a\alpha^2 + b\beta^2$$

Si $a = 3$, $b = 2$, $\alpha = \beta = 1$

$$X^2 + 6 \cdot Y^2 = Z^6 \qquad X = 71;\ Y = 42;\ Z = 5$$

$$71^2 + 6 \cdot 42^2 = 5^6, \text{ etc.}$$

Procediendo de análoga forma con la ecuación 2.ª de [4] se tiene:

$$a \cdot X^2 + b \cdot Y^2 = Z^{2n+1} \quad \begin{cases} X = \dfrac{1}{\sqrt{a}} (a\alpha^2 + b\beta^2)^{n+\frac{1}{2}} \cdot \cos(2n+1)\,\omega \\ Y = \dfrac{1}{\sqrt{b}} (a\alpha^2 + b\beta^2)^{n+\frac{1}{2}} \cdot \operatorname{sen}(2n+1)\,\omega \\ Z = a\alpha^2 + b\beta^2 \end{cases}$$

Desarrollando las funciones trigonométricas:

$$\begin{cases} X = \displaystyle\sum_{0}^{k=n} (-1)^k \binom{2n+1}{2k} a^{n-k} \cdot b^k \cdot \alpha^{2(n-k)+1} \cdot \beta^{2k} \\ Y = \displaystyle\sum_{0}^{k=n} (-1)^k \binom{2n+1}{2k+1} a^{n-k} \cdot b^k \cdot \alpha^{2(n-k)} \cdot \beta^{2k+1} \\ Z = a\alpha^2 + b\beta^2 \end{cases}$$

Si $n = 3$, $a = 5$, $b = 6$, $\qquad 5\,X^2 + 6\,Y^2 = Z^7$

$$X = a^3 \cdot \alpha^7 - 21\,a^2 \cdot b \cdot \alpha^5 \cdot \beta^2 + 35 \cdot a \cdot b^2 \cdot \alpha^3 \cdot \beta^4 - 7 \cdot b^3 \cdot \alpha \cdot \beta^6$$
$$Y = 7 \cdot a^3\,\alpha^6 \cdot \beta - 35 \cdot a^2 \cdot b \cdot \alpha^4 \cdot \beta^3 + 21 \cdot a \cdot b^2 \cdot \alpha^2 \cdot \beta^5 - b^3 \cdot \beta^7$$
$$Z = a \cdot \alpha^2 + b \cdot \beta^2$$

Si $\alpha = 1$, $\beta = 1$ $\qquad 5 \cdot 1763^2 + 6 \cdot 811^2 = 11^7$

Para resolver las ecuaciones 3.ª y 4.ª de [4] procederemos de la forma siguiente:

$$aX^2 + bY^2 = Z^{2n+1};\ (aX^2 + bY^2) \cdot (ac^2 + bd^2) = (ac^2 + bd^2)\,Z^{2n+1}$$
$$(aX^2 + bY^2) \cdot (ac^2 + bd^2) = (acX - bdY)^2 + ab(dX + cY)^2 = X^2\varphi + abY^2\varphi$$

luego:

$$\begin{cases} X\varphi = acX - bdY \\ Y\varphi = dX + cY \\ Z = a\alpha^2 + b\beta^2 \end{cases} \qquad [5]$$

Siendo X e Y las soluciones correspondientes a la ecuación 2.ª de [4].

Luego, $X^2 + abY^2 = (ac^2 + bd^2)Z^{2n+1}$, tiene como soluciones:

$$\left|\begin{array}{l} X = (a\alpha^2 + b\beta^2)^{n+\frac{1}{2}} \cdot (ac^2 + bd^2)^{\frac{1}{2}} \cdot \cos[(2n+1)\,\omega + \varphi] \\ \\ Y = \dfrac{1}{\sqrt{a \cdot b}} (a\alpha^2 + b\beta^2)^{n+\frac{1}{2}} \cdot (ac^2 + bd^2)^{\frac{1}{2}} \cdot \operatorname{sen}[(2n+1)\,\omega + \varphi) \\ \\ Z = a\alpha^2 + b\beta^2 \end{array}\right.$$

siendo:

$$tg\ \omega = \frac{\beta\sqrt{b}}{\alpha\sqrt{a}} \text{ y } tg\ \varphi = \frac{d\sqrt{b}}{c\sqrt{a}}$$

Desarrollando las funciones sen y cos se tiene:

$$\left|\begin{array}{l} X = c \displaystyle\sum_{0}^{k=n} (-1)^k \binom{2n+1}{2k} a^{n-k+1} \cdot b^k \cdot \alpha^{2(n-k)+1} \cdot \\ \qquad \cdot \beta^{2k} - d \displaystyle\sum_{0}^{k=n} (-1)^k \binom{2n+1}{2k+1} a^{n-k} \cdot b^{k+1} \cdot \alpha^{2(n-k)} \cdot \beta^{2k+1} \\ \\ Y = c \displaystyle\sum_{0}^{n} (-1)^k \binom{2n+1}{2k+1} a^{n-k} \cdot b^k \cdot \alpha^{2(n-k)} \cdot \beta^{2k+1} + \\ \qquad + d \displaystyle\sum_{0}^{n} (-1)^k \binom{2n+1}{2k} a^{n-k} \cdot b^k \cdot \alpha^{2(n-k)+1} \cdot \beta^{2k} \\ \\ Z = a\alpha^2 + b\beta^2 \end{array}\right.$$

Si $n = 2$, $a = 3$, $b = 2$, $c = 2$, $d = 5$, $\alpha = 1$, $\beta = 2$, $X^2 + 6 \cdot Y^2 = 62 \cdot Z^5$

$3154^2 + 6 \cdot 79^2 = 62 \cdot 11^5$, etc.

Procediendo de análoga manera, la ecuación $aX^2 + bY^2 = (ac^2 + bd^2)\, Z^{2n}$ tiene como soluciones:

$$\left|\begin{array}{l} X = \dfrac{1}{\sqrt{a}} (a\alpha^2 + b\beta^2)^n \cdot (ac^2 + bd^2)^{\frac{1}{2}} \cdot \cos\,[2n\,\omega + \varphi] \\ \\ Y = \dfrac{1}{\sqrt{b}} (a\alpha^2 + b\beta^2)^n \cdot (ac^2 + bd^2)^{\frac{1}{2}} \cdot \operatorname{sen}\,[2n\,\omega + \varphi] \\ \\ Z = a\alpha^2 + b\beta^2 \end{array}\right.$$

siendo:

$$tg\ \omega = \frac{\beta\sqrt{b}}{\alpha\sqrt{a}} \text{ y } tg\ \varphi = \frac{d\sqrt{b}}{c\sqrt{a}}$$

Desarrollando sen y cos:

$$\left|\begin{array}{l} X = c \displaystyle\sum_{0}^{k=n} (-1)^k \binom{2n}{2k} a^{n-k} \cdot b^k \cdot \alpha^{2(n-k)} \cdot \beta^{2k} - \\ \qquad - d \displaystyle\sum_{0}^{k=n-1} (-1)^k \binom{2n}{2k+1} a^{n-k-1} \cdot b^{k+1} \cdot \alpha^{2(n-k)-1} \cdot \beta^{2k+1} \\ \\ Y = c \displaystyle\sum_{0}^{k=n-1} (-1)^k \binom{2n}{2k+1} a^{n-k} \cdot b^k \cdot \alpha^{2(n-k)-1} \cdot \beta^{2k+1} + \\ \qquad + d \displaystyle\sum_{0}^{n} (-1)^k \binom{2n}{2k} a^{n-k} \cdot b^k \cdot \alpha^{2(n-k)} \cdot \beta^{2k} \\ \\ Z = a\alpha^2 + b\beta^2 \end{array}\right.$$

Si $n = 3$, $a = 2$, $b = 3$, $c = 2$, $d = 5$, $\alpha = 2$, $\beta = 1$,

$2\,X^2 + 3\,Y^2 = 83 \cdot Z^6$ $\qquad$ $2 \cdot 1370^2 + 3 \cdot 6911^2 = 83 \cdot 11^6$, etc.

El método anteriormente expuesto está basado en las siguientes igualdades:

$$(a\alpha^2 + b\beta^2) \cdot (a\gamma^2 + b\delta^2) = \left\{\begin{array}{ll} (a \cdot \alpha \cdot y - b \cdot \beta \cdot \delta)^2 + ab(\alpha \cdot \delta + \beta \cdot y)^2 & [6] \\ (a \cdot \alpha \cdot y + b \cdot \beta \cdot \delta)^2 + ab(\alpha \cdot \delta - \beta \cdot y)^2 & [7] \end{array}\right.$$

No se ha aplicado más que la igualdad [6]; aplicando la [7] nos encontraríamos con otro grupo de valores para resolver las ecuaciones pitagóricas [4], aunque dichas soluciones tienen un factor común, es decir, no son primitivas.

En la relación [5], por lo anteriormente expuesto, podría hacerse:

$$\begin{cases} V\varphi = acX + bdY \\ W\varphi = cY - dX \\ Z = a\alpha^2 + b\beta^2 \end{cases}$$

con lo que tendríamos otro grupo de soluciones para la ecuación cuarta de [4].

Como entonces el valor de Z permanece invariante, se tendrá:

$$X^2 + abY^2 = V^2 + abW^2 = (ac^2 + bd^2) \cdot Z^{2n+1}$$

Análogamente, para la ecuación 3.ª de [4], resultaría:

$$aX^2 + bY^2 = aV^2 + bW^2 = (ac^2 + bd^2) \cdot Z^{2n}$$

Haciendo aplicación a los ejemplos numéricos antes expuestos se tendrá:

$$3154^2 + 6 \cdot 79^2 = 2086^2 + 6 \cdot 969^2 = 62 \cdot 11^5$$

$$2 \cdot 1370^2 + 3 \cdot 6911^2 = 2 \cdot 3890^2 + 3 \cdot 6239^2 = 83 \cdot 11^6$$

Un caso particular, que puede revestir algún interés, es el siguiente:

Si en las ecuaciones 3.ª ó 4.ª de [4] hacemos $a = b = 1$, se tendrá:

$$X^2 + Y^2 = (c^2 + d^2)\, Z^n$$

cuyas soluciones son:

$$\begin{cases} X = (\alpha^2 + \beta^2)^{\frac{n}{2}} \cdot (c \cdot \cos n\ \omega - d \cdot \operatorname{sen} n\ \omega) \\ Y = (\alpha^2 + \beta^2)^{\frac{n}{2}} \cdot (d \cdot \cos n\ \omega + c \cdot \operatorname{sen} n\ \omega) \\ Z = \alpha^2 + \beta^2 \end{cases}$$

siendo

$$tg\ \omega = \frac{\beta}{\alpha}$$

Desarrollando:

$$\left|\begin{array}{l} X = -d\left(\binom{n}{1}\alpha^{n-1}\cdot\beta - \binom{n}{3}\alpha^{n-3}\cdot\beta^3 + \ldots\right) + c\left(\binom{n}{0}\alpha^n - \binom{n}{2}\alpha^{n-2}\cdot\beta^2 + \ldots\right) \\ Y = d\left(\binom{n}{0}\alpha^n - \binom{n}{2}\alpha^{n-2}\cdot\beta^2 + \ldots\right) + c\left(\binom{n}{1}\alpha^{n-1}\cdot\beta - \binom{n}{3}\alpha^{n-3}\cdot\beta^3 + \ldots\right) \\ Z = \alpha^2 + \beta^2 \end{array}\right.$$

También puede hacerse $d = 0$, $c = 1$, con lo que se tendrá:

$$X^2 + Y^2 = Z^n$$

En general, combinando adecuadamente las ecuaciones [4], sumándolas, restándolas, etc., pueden resolverse gran número de ecuaciones cuadráticas.

C) CRITERIOS DE SOLUBILIDAD DE LA ECUACION $aX^2 + cXY + bY^2 = Z^n$

Examinaremos la condición (I) del apartado A, con más detalle.

Llamaremos forma ipsofactorizable aquella G(X, Y), tal que se verifique:

$$G(X, Y) = G(\alpha, \beta) \times G(\gamma, \delta)$$

siendo:

$$\alpha, \beta, \gamma, \delta \in \mathbf{Z}^*$$

Veamos qué condición tiene que cumplir una forma cuadrática binaria f: para que sea ipsofactorizable.

Supongamos el caso general:

$$f = a\varphi^2 + c\varphi\omega + b\omega^2 = (a\alpha^2 + c\alpha\beta + b\beta^2) \times (a\gamma^2 + c\gamma\delta + b\delta^2)$$

siendo

$$a, b, c, \varphi, \omega \in \mathbf{Z}^*$$

Haciendo:

$$\left|\begin{array}{l} \varphi = x(\alpha + \beta)(\gamma + \delta) - \gamma\alpha y \\ \omega = z\beta\delta - v(\alpha + \beta)(\gamma + \delta) \end{array}\right.$$

y aplicando el método de coeficientes indeterminados, se hallan x, y, z, v, resultando:

$$\left|\begin{array}{l} \varphi = \dfrac{b}{\sqrt{a + b - c}}(\alpha + \beta)(\gamma + \delta) - \sqrt{a + b - c}\,\alpha\gamma \\ \omega = \sqrt{a + b - c}\,\beta\delta - \dfrac{a}{\sqrt{a + b - c}}(\alpha + \beta)(\gamma + \delta) \end{array}\right. \qquad [8]$$

luego la condición para que una forma f sea ipsofactorizable es:

$$\boxed{a + b - c = K^2}$$

($K \neq 0$), el caso de $K = 0$ se estudia más adelante.

Como φ, $\omega \in \mathbf{Z}^*$, bastará elegir α, β, γ, δ tales que:

$$(\alpha + \beta) \cdot (\gamma + \delta) \equiv 0 \text{ (mód. } \sqrt{a + b - c} = K)$$

Ahora bien: en general, una forma cuadrática binaria $f = ax^2 + cxy + by^2$, donde $a, b, c, \in \mathbf{Z}^*$, no cumplirá con la condición $a + b - c = K^2$; si esto sucede encontremos otra forma

$$f^1 = a^1 X^2 + c^1 XY + b^1 Y^2$$

que sea ipsofactorizable.

Si a la forma f se le aplica la transformación

$$\left| \begin{array}{l} x = \mu X + \nu Y \\ y = \varepsilon X + \eta Y \end{array} \right.$$

donde $\mu, \nu, \varepsilon, \eta \in \mathbf{Z}$, se tendrá:

$$f \equiv f^1 = a(\mu X + \nu Y)^2 + c(\mu X + \nu Y)(\varepsilon X + \eta Y) + b(\varepsilon X + \eta Y)^2$$

$$f^1 \equiv f = (a\mu^2 + c\mu\varepsilon + b\varepsilon^2) X^2 + (2a\mu\nu + c\mu\eta + c\varepsilon\nu + 2b\varepsilon\eta) XY + (a\nu^2 + c\nu\eta + b\eta^2) Y^2$$

es decir:

$$f^1 \equiv f = a^1 X^2 + c^1 XY + b^1 Y^2$$

Exigiendo que $a^1 + b^1 - c^1 = \lambda^2$, se tendrá:

$$\boxed{a(\mu - \nu)^2 + c(\mu - \nu)(\varepsilon - \eta) + b(\varepsilon - \eta)^2 = \lambda^2} \qquad [9]$$

Llamando:

$\Omega^2 \cdot \Delta$ al discriminante de la forma f(Δ exento de cuadrados).
$\Delta\lambda$ al discriminante de la ecuación [9].

Se tendrá:

$$(\mu - \nu) = \frac{-c(\varepsilon - \eta) \pm \sqrt{\Delta\lambda}}{2a}$$

luego $\Delta\lambda = \theta^2$, $\theta^2 = c^2(\varepsilon - \eta)^2 - 4a[b(\varepsilon - \eta)^2 - \lambda^2]$, como $c^2 - 4ab = \Omega^2 \cdot \Delta$

$$\boxed{-\theta^2 + [(\varepsilon - \eta)\Omega]^2 \Delta + a(2\lambda)^2 = 0} \qquad [10]$$

La ecuación [10] es del tipo $A x^2 + B y^2 + C z^2 = 0$; sabemos (*) que las condiciones necesarias y suficientes, para que dicha ecuación tenga solución en el campo $\mathbf{Z}^*$, son:

1.º El producto A, B, C sea exento de cuadrados.

2.º Los coeficientes A, B, C $\in \mathbf{Z}^*$ no sean todos del mismo signo.

3.º $-B \cdot C$, $-A \cdot C$, $-A \cdot B$, sean restos cuadráticos módulos. A, B, C, respectivamente.

BIBLIOGRAFIA

L. J. MORDELL, «On the equation $a x^2 + b y^2 - c z^2 = 0$» (1951).

TH. SKOLEM, «A simple proof of the solvability of the Diophantine equation $a x^2 + b y^2 - c z^2 = 0$» (1952).

I. NIVEN y H. S. ZUCKERMAN, «An introduction to the Theory of Numbers» (1960).

Aplicando las condiciones anteriores a la ecuación [10], se tendrá:

1.º $a \cdot \Delta \cdot (-1)$ tiene que ser exento de cuadrados, como Δ ya lo está, es suficiente que $a \neq n^2$ (más adelante, se estudiará el caso contrario).

2.º a, Δ, -1 tienen que ser todos no del mismo signo.

3.º
$$\Delta = \text{resto cuadrático módulo } a \ (1.^a)$$
$$a = \text{resto cuadrático módulo } \Delta \ (2.^a)$$
$$-a \cdot \Delta = \text{resto cuadrático módulo 1} \ (3.^a)$$

Las condiciones 1.ª y 3.ª del apartado 3.º se cumplen siempre, ya que la 1.ª se verifica por Gauss y la 3.ª es evidente.

Luego la única condición a imponer es la 2.ª, que a sea resto cuadrático módulo Δ.

Procediendo de análoga forma en la ecuación [9] y tomando $(\varepsilon - \eta)$ como incógnita se tendrá: b tiene que ser resto cuadrático módulo Δ.

Luego:

TEOREMA I.

La condición necesaria y suficiente para que una forma cuadrática binaria $f = a x^2 + c x y + b y^2$, $a, b, c \in \mathbf{Z}^*$ *represente un cuadrado perfecto, es que* a *ó* b *sean restos cuadráticos módulo el discriminante de la forma exento de cuadrados.*

Por tanto, la condición de que

$$a(\mu - \nu)^2 + c(\mu - \nu)(\varepsilon - \eta) + b(\varepsilon - \eta)^2 = \lambda^2$$

es la que se desprende del teorema I.

(*) Aunque dichas condiciones se conocían desde Legendre, la demostración de las mismas es relativamente reciente.

Supongamos cumplida en la forma de la ecuación dada:

$$\underline{a\,x^2 + c\,x\,y + b\,y^2 = z^{n+1}}$$

la condición exigida por el teorema I.

Mediante la fórmula [10] calculamos $\underline{\theta}$, $\underline{\lambda}$ y $\underline{(\varepsilon - \eta)}$ y entrando en la fórmula [9] calculamos $\underline{(\mu - \nu)}$, por lo tanto, se han hallado:

$$\underline{\mu}\,,\ \underline{\nu}\,,\ \underline{\varepsilon}\,,\ \underline{\eta}$$

La nueva forma $f^1 \equiv f = a^1\,X^2 + c^1\,XY + b^1\,Y^2$ ya es ipsofactorizable, puesto que $a^1 + b^1 - c^1 = \lambda^2$, y por tanto, mediante las fórmulas [8] se tendrá:

$$\left|\begin{array}{l} X = \dfrac{b^1}{\lambda}(\alpha^1 + \beta^1)(\gamma^1 + \delta^1) - \lambda\,\alpha^1\,\gamma^1 \\ \\ Y = \lambda\,\beta^1\,\delta^1 - \dfrac{a^1}{\lambda}(\alpha^1 + \beta^1)(\gamma^1 + \delta^1) \end{array}\right.$$

Para que: $X, Y \in \mathbf{Z}^*$ basta elegir α^1, β^1, γ^1, δ^1 tales que

$$(\alpha^1 + \beta^1)(\gamma^1 + \delta^1) \equiv 0 \ (\text{mód. } \lambda)$$

Por lo tanto:

$$a^1\,X^2 + c^1\,XY + b^1\,Y^2 = [a^1(\alpha^1)^2 + c^1\alpha^1\beta^1 + b^1(\beta^1)^2]\,[a^1(\gamma^1)^2 + c^1\gamma^1\delta^1 + b^1(\delta^1)^2]$$

y procediendo como se indicó en el apartado A, se tienen las soluciones

$$\left|\begin{array}{l} X = f_x(\alpha^1\ \beta^1) \\ Y = f_y(\alpha^1,\ \beta^1) \\ Z = a\,(\alpha^1)^2 + c^1\,\alpha^1\,\beta^1 + b^1\,(\beta^1)^2 \end{array}\right.$$

para la ecuación:

$$\underline{a^1\,X^2 + c^1\,XY + b^1\,Y^2 = Z^{n+1}}$$

pero como

$$\left|\begin{array}{l} x = \mu\,X + \nu\,Y \\ y = \varepsilon\,X + \eta\,Y \end{array}\right.$$

se tendrá, finalmente, las soluciones de la ecuación

$$\underline{a\,x^2 + c\,x\,y + b\,y^2 = z^{n+1}}$$

De lo anteriormente expuesto se deduce el siguiente

TEOREMA II

La ecuación $a\,x^2 + c\,x\,y + b\,y^2 = z^{n+1}$, *donde* $a, b, c, n \in \mathbf{Z}^*$, *tiene solución en el campo* $\mathbf{Z}^*$, *si y sólo si* a ó b *son restos cuadráticos módulo el discriminante de la forma exento de cuadrados.*

De la ecuación [9], $a(\mu - \nu)^2 + c(\mu - \nu)(\varepsilon - \eta) + b(\varepsilon - \eta)^2 = \lambda^2$, se deduce:

Si los coeficientes a y b están ligados por una relación del tipo

$$a \cdot A^2 + c \cdot A \cdot B + b \cdot B^2 = D^2$$

donde A, B, D $\in \mathbf{Z}$. se tendrá que la ecuación [9] admite como soluciones:

$$\left| \begin{array}{l} \mu - \nu = A \\ \varepsilon - \eta = B \\ \lambda = D \end{array} \right.$$

luego una vez conocidos μ, ν, ε, η, se tiene resuelto el problema sin necesidad de recurrir a la ecuación [10].

Luego:

COROLARIO

La ecuación $a\,x^2 + c\,x\,y + b\,y^2 = Z^{n+1}$, *admite siempre solución en el campo* $\mathbf{Z}^*$, *si* $a\,A^2 + c\,AB + b\,B^2 = D^2$, *donde* A, B, D $\in \mathbf{Z}$.

De este corolario se deduce que la ecuación $a\,x^2 + c\,x\,y + b\,y^2 = \mathbf{Z}^{n+1}$ tiene siempre solución en el campo $\mathbf{Z}^*$ en los casos siguientes:

1.º Cuando a o b sean cuadrados perfectos (B = 0, D = $a \cdot$ A).

2.º Cuando $a + b + c$ sea cuadrado perfecto (A = B = 1).

3.º Cuando $a + b - c$ sea cuadrado perfecto (A = 1, B = — 1).

4.º Cuando a o b y Δ (discriminante de la forma exento de cuadrados), sean primos impares no todos del tipo $\dot{4} + 3$.

Esta última condición se desprende de la ley de reciprocidad cuadrática.

Veamos algún ejemplo.

1.º $f = 6\,x^2 + 22\,xy + 19\,y^2$, el discriminante de la forma es igual a 28, luego $\Omega = 2$; $\Delta = 7$, como

$$\left| \begin{array}{l} \Delta \equiv 3 \text{ (mód. 4)} \\ 19 \equiv 3 \text{ (mód. 4)} \end{array} \right.$$

la forma f no representa nunca un cuadrado perfecto y, por tanto, la ecuación [9] no tiene solución en el campo $\mathbf{Z}^*$.

2.º $f = 3\,x^2 + 11\,xy + 7\,y^2$, $\Delta = 37$, luego

$$\left| \begin{array}{l} \Delta \equiv\!|\!\equiv 3 \text{ (mód. 4)} \\ 7 \equiv 3 \text{ (mód. 4)} \end{array} \right.$$

luego la forma f representa un cuadrado perfecto y, por tanto, la ecuación [9] tiene solución en el campo $\mathbf{Z}^*$.

Veamos el caso en que el discriminante de la forma sea un cuadrado perfecto.

Entonces se tendrá: $c^2 - 4\,a \cdot b = \rho^2$; la ecuación [9] puede ponerse:

$$\frac{1}{4\,a}\,[2\,a(\mu - \nu) + c(\varepsilon - \eta) - \rho(\varepsilon - \eta)]\,[2\,a(\mu - \nu) + \\ + c(\varepsilon - \eta) + \rho(\varepsilon - \eta)] = \lambda^2$$

y sin recurrir a la ecuación [10] se resuelve la ecuación [9] sin más que poner:

$$\left|\begin{array}{l} \mu - \nu = \rho(p^2 + 4\,a\,m^2) - c(p^2 - 4\,a\,m^2) \\ \varepsilon - \eta = 2a\,(p^2 - 4a\,m^2) \end{array}\right.$$

donde

$$m,\ p \in \mathbf{Z},$$

una vez conocidos, μ, ν, ε, η tenemos resuelto el problema.

Luego la ecuación

$$\underline{a\,x^2 + c\,x\,y + b\,y^2 = Z^{n+1}}$$

tiene siempre solución en el campo $\mathbf{Z}^*$ si el discriminante de la forma es un cuadrado perfecto (*).

Veamos el caso en que a + b — c = 0.

En este supuesto, el discriminante de la forma es: $c^2 - 4\,a \cdot b = (a - b)^2$; luego: $\Omega = \pm\,(a - b)$, $\Delta = 1$; por tanto, la ecuación tiene siempre solución (bien por ser el discriminante de la forma un cuadrado perfecto o bien por ser siempre $\underline{a}$ o $\underline{b}$ restos cuadráticos módulo 1).

La ecuación [9] puede en este caso reducirse a la siguiente:

$$a(\mu - \nu)^2 + (a + b)\,(\mu - \nu)\,(\varepsilon - \eta) + b(\varepsilon - \eta)^2 = \lambda^2$$

y también:

$$[a(\mu - \nu) + b(\varepsilon - \eta)] \cdot [(\mu - \nu) + (\varepsilon - \eta]) = \lambda^2.$$

Ecuación que se resuelve con:

$$\left|\begin{array}{l} \mu - \nu = p^2 - b\,q^2 \\ \varepsilon - \eta = a\,q^2 - p^2 \\ \lambda = (a - b)q \end{array}\right. \qquad [11]$$

donde $p,\ q \in \mathbf{Z}$.

(*) Fácilmente se comprueba que en este caso: $\Omega = \rho$, $\Delta = 1$, con lo que $\underline{a}$ o $\underline{b}$ siempre son restos cuadráticos mód. 1. Si se ha operado de la forma anterior, es para obtener las soluciones de la ecuación [9].

Se llega, por tanto, a la conclusión de que si

$$a + b - c = 0$$

la ecuación

$$a\,x^2 + c\,x\,y + b\,y^2 = Z^{n+1}$$

tiene siempre solución en el campo $\mathbf{Z}^*$.

EJEMPLOS NUMERICOS

Resolver, en el campo $\mathbf{Z}^*$, las siguientes ecuaciones:

1.º $2\,x^2 + 7\,xy + 11\,y^2 = Z^{n+1}$: el discriminante de la forma es: —39; luego: $\Omega = 1$, $\Delta = -39$, como 2 u 11 *no son* restos cuadráticos módulo 39, la ecuación no tiene solución.

2.º $2\,x^2 + 3\,xy + 5\,y^2 = Z^{n+1}$, el discriminante de la forma es: —31; luego, $\Omega = 1$, $\Delta = -1$, como 2 ó 5 *son* restos cuadráticos módulo 31, la ecuación tiene solución.

Como: $a + b - c = 2 + 5 - 3 = 4 = 2^2$, se aplican directamente las fórmulas 8; y haciendo $\alpha = \gamma$, $\beta = \delta$, se tiene:

$$\left| \begin{array}{l} x = \dfrac{5}{2}(\alpha + \beta)^2 - 2\,\alpha^2 \\ \\ y = 2\,\beta^2 - (\alpha + \beta)^2 \end{array} \right.$$

procediendo por recurrencia, como se indicó en el apartado A:

$$\left| \begin{array}{l} x = (2\,\alpha^2 + 3\,\alpha\,\beta + 5\,\beta^2)^{\frac{n}{2}} \cdot \left(\alpha \cos n\,\omega + \dfrac{3\,\alpha + 10\,\beta}{\sqrt{31}} \operatorname{sen} n\,\omega\right) \\ \\ y = (2\,\alpha^2 + 3\,\alpha\,\beta + 5\,\beta^2)^{\frac{n}{2}} \cdot \left(\beta \cos n\,\omega - \dfrac{4\,\alpha + 3\,\beta}{\sqrt{31}} \operatorname{sen} n\,\omega\right) \\ \\ Z = 2\,\alpha^2 + 3\,\alpha\,\beta + 5\,\beta^2 \end{array} \right.$$

siendo

$$\operatorname{tg} \omega = \frac{(\alpha + \beta)\sqrt{31}}{7\,\beta - \alpha}$$

Haciendo

$$p \cdot e : n = 2,\ \begin{matrix}\alpha = 5\\ \beta = 3\end{matrix} \left| \begin{matrix} x = \quad 180 \\ y = -780 \\ Z = \quad 140 \end{matrix} \right. \quad \underline{2.180^2 - 3.180 \cdot 788 + 5.788^2 = 140^2}$$

3.º $\underline{7x^2 - xy + 10y^2 = Z^{n+1}}$, el discriminante de la forma es $= -279$; luego, $\Omega = 3$, $\Delta = -31$, como 7 ó 10 *son* restos cuadráticos módulo 31, la ecuación tiene solución.

Como $a + b - c = 7 + 10 + 1 = 18 \neq k^2$, la ecuación [10] será

$$-\theta^2 + [3(\varepsilon - \eta)]^2 (-31) + 7(2\lambda)^2 = 0$$

$$\underline{\theta^2 + 31\ [3(\varepsilon - \eta)]^2 = 7(2\lambda)^2}$$

dicha ecuación tiene la solución

$$\left| \begin{matrix} \theta = 117\,p^2 - 403\,q^2 + 588\,pq \\ \varepsilon - \eta = -9\,p^2 + 31\,q^2 + 26\,pq \\ \lambda = 4(9\,p^2 + 31\,q^2) \end{matrix} \right.$$

donde $p, q \in \mathbf{Z}$.

Si hacemos

$$\left| \begin{matrix} 9\,p^2 = 1 \\ \\ q = 0 \end{matrix} \right. \Rightarrow \left| \begin{matrix} \theta = 13 \\ \varepsilon - \eta = -1 \\ \lambda = 4 \end{matrix} \right.$$

y entrando en la ecuación [9]

$$\mu - \nu = \frac{\varepsilon - \eta \pm \theta}{14} = \begin{cases} -1 \\ -\dfrac{6}{7} \end{cases}$$

luego

$$\left| \begin{matrix} \mu - \nu = -1 \\ \varepsilon - \eta = -1 \end{matrix} \right.$$

Si hacemos

$$\mu = 0,\ \nu = 1,\ \varepsilon = 1,\ \eta = 2$$

se tiene

$$\left| \begin{matrix} x = Y \\ y = X + 2Y \end{matrix} \right. \qquad [12]$$

luego

$7x^2 - xy + 10y^2 = \underline{10X^2 + 39XY + 45Y^2 = Z^{n+1}}$, esta última ecuación verifica que $a + b - c = 10 + 45 - 39 = 16 = 4^2$, y ya se ha visto en el caso anterior su resolución.
Una vez halladas X e Y, entrando en [12], se calculan x, y, con lo que se resuelve el problema.

4.º $\underline{3x^2 + 5xy + 2y^2 = Z^{n+1}}$, al discriminante de la forma es $=1$, luego $\Omega = 1$, $\Delta = 1$; luego la ecuación tiene solución al ser 3 ó 2 restos cuadráticos módulo 1.
Siendo $= a + b - c = 3 + 2 - 5 = 0$, la ecuación tiene solución (página 00).
Aplicando las fórmulas [11]

$$\left|\begin{array}{l} \mu - \nu = p^2 - 2q^2 \\ \varepsilon - \eta = 3q^2 - p^2 \end{array}\right.$$

Si hacemos $p \cdot e : p = q = 1$

$$\left|\begin{array}{l} \mu - \nu = -1 \\ \varepsilon - \eta = 2 \end{array}\right.$$

luego $p \cdot e = \mu = 1$, $\nu = 2$, $\varepsilon = 2$, $\eta = 0$, luego

$$\left|\begin{array}{l} x = X + 2Y \\ y = 2X \end{array}\right.$$

luego $3x^2 + 5xy + 2y^2 = \underline{21X^2 + 32XY + 12Y^2 = Z^{n+1}}$, forma que verifica $a + b - c = 21 + 12 - 32 = 1$, luego se procede análogamente al problema 3.º

Otro tipo de ecuación que puede resolverse, aplicando los métodos anteriormente indicados, es el siguiente:

$$\underline{ax^2 + cxy + by^2 = (aA^2 + cAB + bB^2)\, Z^n}$$

donde a, b, c, A, B, $n \in \mathbf{Z}^*$ son conocidos.

La forma $f = ax^2 + cxy + by^2$ es ipsofactorizable (si no lo fuera se harían los cambios

$$\left|\begin{array}{l} x = \mu X + \nu Y \\ y = \varepsilon X + \eta Y \end{array}\right.$$

necesarios para que lo fuera, análogamente a lo expuesto en páginas anteriores).

Por tanto:

$$ax^2 + cxy + by^2 = (a\alpha^2{}_1 + c\alpha_1\beta_1 + b\beta^2{}_1) \cdot (a\alpha^2{}_2 + c\alpha_2\beta_2 + b\beta^2{}_2) \ldots (a\alpha^2{}_{n+1} + c\alpha_{n+1}\beta_{n+1} + b\beta^2{}_{n+1})$$

y haciendo

$$Z^n = (a\ \alpha^2{}_2 + c\ \alpha_2\ \beta_2 + b\ \beta^2{}_2) \ldots (a\ \alpha^2{}_{n+1} + c\alpha_{n+1}\ \beta_{n+1} + b\ \beta^2{}_{n+1})$$

procediendo de forma análoga a la efectuada en los apartados A y B se resuelven este tipo de ecuaciones.

En lugar de considerar formas cuadráticas binarias, podríamos hacer uso de la identidad de EULER:

$$(\alpha_1{}^2 + \beta_1{}^2 + \gamma_1{}^2 + \delta_1{}^2) \cdot (\alpha_2{}^2 + \beta_2{}^2 + \gamma_2{}^2 + \delta_2{}^2) =$$

$$\begin{aligned} &= (-\alpha_1\alpha_2 + \beta_1\beta_2 + \gamma_1\gamma_2 + \delta_1\delta_2{}^2) + \\ &+ (\alpha_1\delta_2 - \beta_1\gamma_2 + \gamma_1\beta_2 + \delta_1\alpha_2)^2 + \\ &+ (\alpha_1\beta_2 + \beta_1\alpha_2 - \gamma_1\delta_2 + \delta_1\gamma_2)^2 + \\ &(\alpha_1\gamma_2 + \beta_1\delta_2 + \gamma_1\alpha_2 - \delta_1\beta_2)^2 \end{aligned}$$

Siguiendo el mismo método expuesto en los apartados anteriores, se tiene:

$$G(\alpha, \beta, \gamma, \delta) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

luego:

$$G(\alpha, \beta, \gamma, \delta) \cdot G(\alpha, \beta, \gamma, \delta) = G(X, Y, Z, V) = W^2$$

siendo:

$$\begin{aligned} X &= -\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \\ Y &= 2\,\alpha\,\delta \\ Z &= 2\,\alpha\,\beta \\ V &= 2\,\alpha\,\gamma \end{aligned}$$

De esta manera, y análogamente a lo dicho para las formas cuadráticas binarias del tipo $ax^2 + by^2$, se podría llegar a la solución de ecuaciones del tipo

$$\underline{X^2 + Y^2 + Z^2 + V^2 = W^n}$$

y

$$\underline{X^2 + Y^2 + Z^2 + V^2 = (a^2 + b^2 + c^2 + d^2)\ W^n}$$