# *14. FORMAS CUADRÁTICAS BINARIAS Y GRUPOS DE CLASES*

## 14.1 Ecuación Pell

### 1.1 Introducción y origen

En su obra A Dictionary of Mathematics Originally, el profesor de la Universidad de Oxford Christopher Clapham, define a la Ecuación Pell como una ecuación diofántica de la forma $x^2 = ny^2 + 1,$ donde $n$ es un entero *que no es cuadrado perfecto*.

Arquímedes (287-212 a.C.), la recoge en su obra Libro de los Lemas en el problema de los bueyes, donde plantea la ecuación $x^2 = 4729494y^2 + 1,$ de la que no da solución.

En su Aritmética, Diofanto de Alejandría (sobre 250 d.C.), plantea las ecuaciones $x^2 = 26y^2 + 1$ y $x^2 = 30y^2 + 1$ que, aunque no da solución, bien podrían considerarse como de Pell.

En el año 628, el astrónomo y matemático hindú Brahmagupta (598-665), plantea el primer método razonado para la solución de esta ecuación. Este método fue mejorado por otro astrónomo y matemático hindú, Bhaskara (1114-1185), que queda recogido en su obra Lilavati.

Fue Joseph-Louis Lagrange (1736-1813) el que, aprovechando las aportaciones de Pierre de Fermat (1601-1665) y de Leonhard Euler (1707-1783), y con la ayuda de fracciones continuas, aportó uno de los métodos que se aplica en la actualidad. Fue precisamente Euler el que, por equivocación dio a la ecuación el nombre de Pell, atribuyendo su descubrimiento a John Pell (1610-1685), matemático ingles que ha pasado a la historia de las matemáticas, precisamente por esta equivocación.

En 1799, la ecuación $x^2 = ny^2 + 1$ pasó a ser representada como $x^2 - Dy^2 = \pm 1,$ cuando Carl Friedrich Gauss (1777-1855) publicó su obra Disquisitiones Arithmeticae, donde expone la factorización única en cuerpos reales y, a partir del conjugado, establece la norma

$$N(\alpha) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 = \pm 1$$

que permite otra solución a la ecuación Pell

$$x = \frac{(x + y\sqrt{D})^n + (x - y\sqrt{D})^n}{2} \quad y = \frac{(x + y\sqrt{D})^n - (x - y\sqrt{D})^n}{2\sqrt{D}}$$

donde $D = b^2 - 4ac$ es el discriminante o dominio de integridad de los sistemas cuadráticos.

### 1.2 Algunos métodos de solución

La solución a esta ecuación no es fácil, pero tampoco imposible. Requiere, eso sí, la utilización de ciertas herramientas, como las fracciones continuas o métodos de solución de una ecuación modular. A continuación vamos a exponer alguno de estos métodos.

#### 1.2.1 Triángulos y cuadrados: la solución de Euler

Un número es cuadrado si responde a la forma $N = m^2$ y es triangular cuando es de la forma $N = n(n+1)/2.$ A partir de este razonamiento, Euler establece las siguientes igualdades:

$$n^2+n=2m^2 \;\rightarrow\; 4n^2+4n=8m^2$$
$$4n^2+4n+1=8m^2+1 \;\rightarrow\; (2n+1)^2=2(4m)^2+1$$

de donde, si $y=(2n+1)$ *e* $x=2m,$ resulta $y^2=2x^2+1,$ que es un caso particular de ecuación Pell $x^2-Dy^2=1,$ con infinitas soluciones cuando $D$ es libre de cuadrados. En este caso admite como solución $3^2-2\cdot 2^2=1.$

### 1.2.2 Método de Carmichael

En su obra Diophantine Analysis publicada en 1915, el profesor Robert Daniel Carmichael (1879-1967) partiendo de las ternas pitagóricas, propone para la solución de $x^2-Dy^2=z^2$ el siguiente generador:

$$x=m^2+Dn^2,\; y=2mn,\; z=m^2-Dn^2$$

Por ejemplo, para

$$m=5,\; n=3,\; D=7 \;\rightarrow\; x=5^2+7\cdot 3^2=88,\; y=2\cdot 5\cdot 3=30,\; z=5^2-7\cdot 3^2=-38$$
$$88^2-7\cdot 30^2=38^2$$

Por ejemplo, para

$$m=6,\; n=3,\; D=11 \;\rightarrow\; x=6^2+11\cdot 3^2=135,\; y=2\cdot 6\cdot 3=36,\; z=6^2-11\cdot 3^2=-63$$
$$135^2-11\cdot 36^2=63^2$$

En el primer caso la solución, mediante números algebraicos, podemos plantearla como

$$\left(5+3\sqrt{7}\right)^2\left(5-3\sqrt{7}\right)^2=\left(88+30\sqrt{7}\right)\left(88-30\sqrt{7}\right)=88^2-7\cdot 30^2=38^2$$

Esto es una forma cuadrática dentro de los campos reales. Si tenemos en cuenta que la suma de $\left(5+3\sqrt{7}\right)+\left(5-3\sqrt{7}\right)=10,$ el polinomio mínimo resulta $x^2-10x+38=0$ que tiene como solución $x=5\pm\sqrt{13}i,$ y teniendo en cuenta que esto es una cuadrática

$$\left(5+\sqrt{-13}\right)^2\left(5-\sqrt{-13}\right)^2=\left(5^2+13\cdot 1^1\right)^2=38^2$$

### 1.2.3 Mediante ecuaciones modulares

Al tratarse de una ecuación con dos variables, el método consiste en despejar una en función de la otra. Supongamos que debemos resolver la ecuación $x^2-7y^2=1.$

*Despejamos x en función de y*:

Escribimos la ecuación como $x^2\equiv 1(mód.7)$

El coeficiente independiente de esta ecuación es 1, y 1 siempre es resto cuadrático de cualquier ecuación, ya que $1^2-1=0,$ por tanto la primera raíz es $x_1=1+7t.$ Es una solución

paramétrica. Gauss nos enseña, que si una ecuación cuadrática mónica admite una raíz, también admitirá como segunda raíz, su inversa. La inversa de un número, respecto al módulo, es su complemento. En nuestro caso, la inversa de 1 respecto a 7 es 6, ya que $6+1=7$ entonces, la segunda raíz es $x_2 = 6+7t$. Observar que la suma de los coeficientes independientes de las raíces, en las ecuaciones mónicas, dan el módulo, $6+1=7$.

Al tratarse de una ecuación multivariable, si la primera tiene dos raíces, la segunda también.

*Por sustitución, despejamos y*

$$(1+7t)^2 - 7y^2 = 1 \ \rightarrow y_1^2 = \frac{-1+(1+7t)^2}{7} = 0+2t+7t^2$$

$$(6+7t)^2 - 7y^2 = 1 \ \rightarrow y_2^2 = \frac{-1+(6+7t)^2}{7} = 5+12t+7t^2$$

La solución a la ecuación es:

$$x^2 \equiv 1(mód.7) \ \rightarrow \begin{cases} x_1 = 1+7t \ \ y_1^2 = 0+2t+7t^2 \\ x_2 = 6+7t \ \ y_1^2 = 5+12t+7t^2 \end{cases}$$

Ahora se trata de que, dando valores a $t$, busquemos un cuadrado en $x$ tal que, restando la unidad y dividiendo por 7 obtengamos un cuadrado. O bien, busquemos un cuadrado que, multiplicado por 7 y sumándole la unidad obtengamos un cuadrado perfecto.

Observar que si en $x_1 = 1+7t$ damos valor 1 a $t$, resulta $8^2 = 64$ y $64-1 = 63 = 7\cdot 9 = 7\cdot 3^2$, por tanto la solución a la ecuación es $8^2 - 7\cdot 3^2 = 1$.

Ahora, observar otra cosa, $(8+3\sqrt{7})(8-3\sqrt{7}) = 1$ es la norma. Aplicando la solución de Gauss

$$x = \frac{(8+3\sqrt{7})^1 + (8-3\sqrt{7})^1}{2} = 8, \quad y = \frac{(8+3\sqrt{7})^1 - (8-3\sqrt{7})^1}{2\sqrt{7}} = 3$$

Hemos dado a la ecuación exponente 1. Para $2,3,4,\ldots$ las soluciones habrían sido

$x = 127,\ 2.024,\ 32.257,\ldots$ e $y = 48,\ 765,\ 12192,\ldots$

que producen los siguientes resultados.

$$127^2 - 7\cdot 48^2 = 1; \quad 2024^2 - 7\cdot 765^2 = 1; \quad 32257^2 - 7\cdot 12192^2 = 1$$

Como verán, es un tipo de ecuación que genera infinitas soluciones.

### 1.2.4 Método de los cuadrados

Si se tiene cuenta que la ecuación Pell tiene como solución la diferencia de un cuadrado y el producto de otro cuadrado con un entero, *que no sea un cuadrado*, esta solución puede encontrarse directamente utilizando cuadrados perfectos.

Supongamos que buscamos un cuadrado de la forma $4k+1=s^2$, a partir del cual podemos hallar las siguientes soluciones:

| | |
|---|---|
| $4\cdot 2+1=9 \rightarrow 3^2\text{-}2\cdot 2^2=1$ | $4\cdot 42+1=169 \rightarrow 13^2-42\cdot 2^2=1$ |
| $4\cdot 6+1=25 \rightarrow 5^2-6\cdot 2^2=1$ | $4\cdot 56+1=225 \rightarrow 15^2-56\cdot 2^2=1$ |
| $4\cdot 12+1=49 \rightarrow 7^2-12\cdot 2^2=1$ | $4\cdot 72+1=289 \rightarrow 17^2-72\cdot 2^2=1$ |
| $4\cdot 20+1=81 \rightarrow 9^2-20\cdot 2^2=1$ | $4\cdot 90+1=361 \rightarrow 19^2-90\cdot 2^2=1$ |
| $4\cdot 30+1=121 \rightarrow 11^2-30\cdot 2^2=1$ | $4\cdot 110+1=441 \rightarrow 21^2-110\cdot 2^2=1$ |

Para números de la forma $4k+3=ns^2$ hallamos, entre otros

| | |
|---|---|
| $4\cdot 15+3=63 \rightarrow 8^2\text{-}7\cdot 3^2=1$ | $4\cdot 24+3=99 \rightarrow 10^2-11\cdot 3^2=1$ |

Es importante observar la progresión que se produce para los valores de $k$, que pone de manifiesto la estructura de los números entre los de la forma $4k+1$ y $4k+3$.

Si tenemos en cuenta que $n^2-1=ds^2$ es una solución de la ecuación Pell, donde $d,n,s\in Z$, a partir de un cuadrado podemos encontrar algunas de las muchas soluciones en el cuadro siguiente:

| |
|---|
| $2^2-1=3=3\cdot 1^2 \rightarrow 2^2-3\cdot 1^2=1$ |
| $3^2-1=8=2\cdot 2^2 \rightarrow 3^2-2\cdot 2^2=1$ |
| $4^2-1=15=15\cdot 1^2 \rightarrow 4^2-15\cdot 1^2=1$ |
| $5^2-1=24=6\cdot 2^2 \rightarrow 5^2-6\cdot 2^2=1$ |
| $6^2-1=35=35\cdot 1^2 \rightarrow 6^2-35\cdot 1^2=1$ |
| $7^2-1=48=12\cdot 2^2 \rightarrow 7^2-12\cdot 2^2=1$ |
| $8^2-1=63=7\cdot 3^2 \rightarrow 8^2-7\cdot 3^2=1$ |
| $9^2-1=80=20\cdot 2^2 \rightarrow 9^2-20\cdot 2^2=1$ |
| $10^2-1=99=11\cdot 3^2 \rightarrow 10^2-11\cdot 3^2=1$ |

Así, sucesivamente, se puede generar una solución a partir de infinidad de cuadrados. En la reseña sobre el origen de la Ecuación Pell, hemos anotado las ecuaciones $x^2=26y^2+1$ y $x^2=30y^2+1$, atribuidas ambas a Diofanto de Alejandría, pero que no da solución. Bien, nosotros lo vamos a intentar, pero ignorando las fracciones continuas y los cuerpos cuadráticos, desconocidos en la época en la que vivió Diofanto, siglo III de nuestra Era.

Para la ecuación $x^2=26y^2+1$:

Por tanteo con $n$, buscamos $26n^2+1=s^2$. Para $n=1,2,3,4,5,6,7,8,9,10,\ldots$ encontramos que el 10 satisface la ecuación. Efectivamente, $26\cdot 10^2+1=2601=3^2\cdot 17^2=51^2$, por tanto

$$x^2=26y^2+1=51^2-26\cdot 10^2=1$$

donde la norma es $(51+10\sqrt{26})(51-10\sqrt{26})=1$.

Para la ecuación $x^2=30y^2+1$:

Por tanteo con $n$, buscamos $n^2-1=30s^2$. Para $n=1,2,3,4,5,6,7,8,9,10,11,\ldots$ encontramos que el 11 satisface la ecuación. Efectivamente, $11^2-1=120=2^3\cdot 3\cdot 5=2^2\cdot 30$, por tanto

$$x^2 = 30y^2 + 1 = 11^2 - 30 \cdot 2^2 = 1$$

donde la norma es $(11+2\sqrt{30})(11-2\sqrt{30}) = 1.$

### 1.2.5 Método de las fracciones continuas

El astrónomo y matemático hindú Aryabhata (476-550), se cree fue el primero en utilizar las fracciones continuas para resolver sistemas de ecuaciones indeterminados. Así se desprende de su obra Aryabhatiya, escrita en verso allá por el año 510. Fue John Wallis (1616-1703), el más importante matemático inglés anterior a Isaac Newton (1642-1727), el que, en 1655, introdujo y desarrolló el concepto de fracción continua en su obra Arithmética Infinitorum.

1. La relación de las fracciones continuas con los cuerpos cuadráticos se basa en que los desarrollos de los irracionales cuadráticos son periódicos.
2. Un número irracional $\alpha$ es cuadrático si, y sólo si, los coeficientes de su fracción continua se repiten periódicamente a partir de un cierto término.
3. Para desarrollar el irracional cuadrático $\alpha$ vamos a calcular los coeficientes $a_n$ al mismo tiempo que los restos $\alpha_n$. Concretamente $a_n$ es la parte entera de $\alpha_n$ y $\alpha_{n+1} = 1/(\alpha_n - a_n)$.

Para $\sqrt{7},$ como la raíz cuadrada está comprendida entre 2 y 3, entonces $a_0 = 2.$

Para $\alpha_1 = \dfrac{1}{\sqrt{7}-2} = \dfrac{2+\sqrt{7}}{3}$ y $a_1 = 2.$ Para $\alpha_2 = \dfrac{1}{\dfrac{2+\sqrt{7}}{3}-1} = \dfrac{1+\sqrt{7}}{2}$ y $a_2 = 1.$

Para $\alpha_3 = \dfrac{1}{\dfrac{1+\sqrt{7}}{2}-1} = \dfrac{1+\sqrt{7}}{3}$ y $a_3 = 1.$ Para $\alpha_4 = \dfrac{1}{\dfrac{1+\sqrt{7}}{3}-1} = 2+\sqrt{7}$ y $a_4 = 1.$

Para $\alpha_5 = \dfrac{1}{2+\sqrt{7}-4} = \dfrac{2+\sqrt{7}}{3} = \alpha_1$ y $a_5 = 4.$

Por tanto, obtenemos $\sqrt{7} = [2,\overline{1,1,4}],$ donde la barra indica el periodo que se repite.
Observar que en el paso $\alpha_5$ se repite la fracción de $\alpha_{1,}$ con lo que se termina un período y empieza otro.

$$\sqrt{7} = 2 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\ddots}}}}} = [2,\overline{1,1,1,4}]$$

Ahora, calcularemos los convergentes o reducidas de la siguiente forma:

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
|---|---|---|---|---|---|---|---|---|---|
| $a_n$ | *2* | *1* | *1* | *1* | *4* | *1* | *1* | *1* | *4* |
| $x$ | 2 | 3 | 5 | 8 | 37 | 45 | 82 | 127 | 590 |
| $y$ | 1 | 1 | 2 | 3 | 14 | 17 | 31 | 48 | 223 |
| $x^2-Dy^2$ | -3 | 2 | -3 | 1 | -3 | 2 | -3 | 1 | -3 |

Observar que los valores de $x^2-Dy^2$ forman una sucesión que se repite al igual que el período de restos. También, que los únicos valores que satisfacen a la ecuación son los de las columnas 4 y 8. El primero corresponde a la norma del cuerpo cuadrático, esto es $(8+3\sqrt{7})(8-3\sqrt{7})=1$, el segundo corresponde al exponente 2

$$x=\frac{(8+3\sqrt{7})^2+(8-3\sqrt{7})^2}{2}=127,\quad y=\frac{(8+3\sqrt{7})^2-(8-3\sqrt{7})^2}{2\sqrt{7}}=48$$

donde $8^2-7\cdot 3^2=(8^2-7\cdot 3^2)^2=127^2-7\cdot 48^2=1.$

Vamos a resolver la ecuación $x^2-23y^2=1.$

Como $\sqrt{23}$ está comprendido entre 4 y 5, entonces $a_0=4.$

$$\alpha_1=\frac{1}{\sqrt{23}-4}=\frac{4+\sqrt{23}}{7},\ a_1=4\quad \alpha_2=\frac{1}{\dfrac{1}{\dfrac{4+\sqrt{23}}{7}-1}}=\frac{3+\sqrt{23}}{2},\ a_2=1$$

$$\alpha_3=\frac{1}{\dfrac{1}{\dfrac{3+\sqrt{23}}{2}-3}}=\frac{3+\sqrt{23}}{7},\ a_3=3\quad \alpha_4=\frac{1}{\dfrac{1}{\dfrac{3+\sqrt{23}}{7}-1}}=4+\sqrt{23},\ a_4=1$$

$$\alpha_5=\frac{1}{\dfrac{1}{4+\sqrt{23}-8}}=\frac{4+\sqrt{23}}{7}=\alpha_1,\ a_5=8$$

Por tanto, obtenemos $\sqrt{23}=\left[4,\overline{1,3,1,8}\right],$ donde la barra indica el periodo que se repite.

$$\sqrt{23}=4+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{8+\cfrac{1}{\ddots}}}}}=\left[4,\overline{1,3,8}\right]$$

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
|---|---|---|---|---|---|---|---|---|---|
| $a_n$ | *4* | *1* | *3* | *1* | *8* | *1* | *3* | *1* | *8* |
| $x$ | 4 | 5 | 19 | 24 | 211 | 235 | 916 | 1151 | 10124 |
| $y$ | 1 | 1 | 4 | 5 | 44 | 49 | 191 | 240 | 2111 |
| $x^2-Dy^2$ | -7 | 2 | -7 | 1 | -7 | 2 | -7 | 1 | -7 |

A partir de estos datos, la norma es $(24+5\sqrt{23})(24-5\sqrt{23})=1$ y la solución a la ecuación propuesta

$$x=\frac{(24+5\sqrt{23})^1+(24-5\sqrt{23})^1}{2}=24,\quad y=\frac{(24+5\sqrt{23})^1-(24-5\sqrt{23})^1}{2\sqrt{7}}=5$$

Si hubiéramos resuelto mediante ecuaciones modulares, en $x^2-23y^2=1$ despejamos $x$

$$x^2\equiv 1(mód.23)$$

Sabemos que la unidad es raíz de una ecuación cuadrática, por tanto

$$x_1=1+23t$$

La segunda raíz será la inversa respecto al módulo 23, esto es

$$x_2=22+23t$$

Por sustitución despejamos $y,$ luego

$$(1+23t)^2-23y^2=1\ \rightarrow\ y_1^2=\frac{-1+(1+23t)^2}{23}=0+2t+23t^2$$

$$(22+23t)^2-23y^2=1\ \rightarrow\ y_1^2=\frac{-1+(22+23t)^2}{23}=21+44t+23t^2$$

Observar, que para $t=1,\ x=1+23=24$ es el valor de la norma, $(24+5\sqrt{7})(24-5\sqrt{7})=1.$ Para $y,\ y=2+23=25=5^2$, o también $24^2-1=575=23\cdot 25=23\cdot 5^2.$

### 1.2.6 Método de los cuerpos cuadráticos

Si $\alpha=a+b\sqrt{D}$ es un entero perteneciente al cuerpo cuadrático $\mathbb{Q}\sqrt{D}$ y $N(\alpha)=(a+b\sqrt{D})(a-b\sqrt{D})=a^2-Db^2=\pm 1,$ siendo $N(a,b)$ la norma del conjugado $a-b\sqrt{D},$ una solución para la ecuación Pell sería $x+y\sqrt{D})(x-y\sqrt{D})=x^2-Dy^2=1,$ donde el valor de $D$ puede ser calculado mediante fracciones continuas.

Si $\alpha,\beta$ es una solución de la ecuación $x^2-Dy^2=1,$ también $\alpha^2-D\beta^2=1$ y $(\alpha^2-D\beta^2)^n=1$ serán soluciones para cualquier valor de $n$ con $n\geqq 1,$ entonces

$$x^2-Dy^2=(\alpha^2-D\beta^2)^n$$

$$(x+y\sqrt{D})(x-y\sqrt{D})=(\alpha+\beta\sqrt{D})^n(\alpha-\beta\sqrt{D})^n$$

de donde

$$x+y\sqrt{D}=(\alpha+\beta\sqrt{D})^n\ \text{ y }\ x-y\sqrt{D}=(\alpha-\beta\sqrt{D})^n$$

Resolviendo el sistema

$$x=\left[(\alpha+\beta\sqrt{D})^n+(\alpha-\beta\sqrt{D})^n\right]\Big/2,\quad y=\left[(\alpha+\beta\sqrt{D})^n-(\alpha-\beta\sqrt{D})^n\right]\Big/(2\sqrt{D})$$

que es la solución planteada por Gauss.

Por ejemplo, vamos a resolver la ecuación $x^2-31y^2=1$.

Sabemos que $\alpha_0=\sqrt{D}=\sqrt{31},$ raíz que está comprendida entre $5$ y $6$.

A continuación calculamos los cocientes incompletos que se generan:

$$\alpha_1=\frac{1}{\alpha_0-a_0}=\frac{1}{\sqrt{31}-5}=\frac{5+\sqrt{31}}{6},\quad \alpha_2=\frac{1}{\alpha_1-a_1}=\frac{1}{\frac{5+\sqrt{31}}{6}-1}=\frac{1+\sqrt{31}}{5}$$

$$\alpha_3=\frac{1}{\alpha_2-a_2}=\frac{1}{\frac{1+\sqrt{31}}{5}-1}=\frac{4+\sqrt{31}}{3},\quad \alpha_4=\frac{1}{\alpha_3-a_3}=\frac{1}{\frac{4+\sqrt{31}}{3}-3}=\frac{5+\sqrt{31}}{2}$$

$$\alpha_5=\frac{1}{\alpha_4-a_4}=\frac{1}{\frac{5+\sqrt{31}}{2}-5}=\frac{5+\sqrt{31}}{3},\quad \alpha_6=\frac{1}{\alpha_5-a_5}=\frac{1}{\frac{5+\sqrt{31}}{3}-3}=\frac{4+\sqrt{31}}{5}$$

$$\alpha_7=\frac{1}{\alpha_6-a_6}=\frac{1}{\frac{4+\sqrt{31}}{5}-1}=\frac{1+\sqrt{31}}{6},\quad \alpha_8=\frac{1}{\alpha_7-a_7}=\frac{1}{\frac{1+\sqrt{31}}{6}-1}=\frac{5+\sqrt{31}}{1}$$

$$\alpha_9=\frac{1}{\alpha_8-a_8}=\frac{1}{5+\sqrt{31}-10}=\frac{5+\sqrt{31}}{6}=\alpha_1.$$

Planteamos su desarrollo

$$\sqrt{31}=5+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{5+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{10+\ddots}}}}}}}}=\left[5,\overline{1,1,3,5,3,1,1,10}\right]$$

Finalmente calculamos las reducidas o convergentes

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_n$ | *5* | *1* | *1* | *3* | *5* | *3* | *1* | *1* | *10* | *1* | *1* | *3* |
| $x$ | 5 | 6 | 11 | 39 | 206 | 657 | 863 | 1520 | 16063 | 17583 | 33646 | 118521 |
| $y$ | 1 | 1 | 2 | 7 | 37 | 118 | 155 | 273 | 2885 | 3158 | 6043 | 21287 |
| $x^2-Dy^2$ | -6 | 5 | -3 | 2 | -3 | 5 | -6 | 1 | -6 | 5 | -3 | 2 |

Como podemos comprobar, $(1520-273\sqrt{31})(1520-273\sqrt{31})=1$ es la unidad fundamental de norma $1$, y la solución a la ecuación $1520^2-31\cdot 273^2=1$.

Teniendo en cuenta que los valores de las variables vienen determinados por

$$x=\frac{(x+y\sqrt{D})^n+(x-y\sqrt{D})^n}{2},\quad y=\frac{(x+y\sqrt{D})^n-(x-y\sqrt{D})^n}{2\sqrt{D}}$$

Para $n=1,2\ y\ 3$, tenemos

$$x=\frac{(1520+273\sqrt{31})^n+(1520-273\sqrt{31})^n}{2}=1.520,\ 4.620.799,\ 14.047.227.440,\ldots$$

$$y=\frac{(1520+273\sqrt{31})^n-(1520-273\sqrt{31})^n}{2\sqrt{31}}=273,\ 829.920,\ 2.522.956.527,\ldots$$

En el cuadro siguiente se recogen, para números primos menores a 101, las unidades fundamentales para la norma $1$, así como los cocientes incompletos de los cuerpos cuadráticos $K=Q\sqrt{D}$.

| $D$ | $x$ | $y$ | $\left[a_o,\{a_1,a_2,a_3\}\right]$ |
|---|---|---|---|
| 2 | 3 | 2 | 1,{2} |
| 3 | 2 | 1 | 1,{1,2} |
| 5 | 9 | 4 | 2,{4} |
| 7 | 8 | 3 | 2,{1,1,1,4} |
| 11 | 10 | 3 | 3,{3,6} |
| 13 | 649 | 180 | 3,{1,1,1,1,6} |
| 17 | 33 | 8 | 4,{8} |
| 19 | 170 | 39 | 4,{2,1,3,1,2,8} |
| 23 | 24 | 5 | 4,{1,3,1,8} |
| 29 | 9801 | 1820 | 5,{2,1,1,2,10} |
| 31 | 1520 | 273 | 5,{1,1,3,5,3,1,1,10} |
| 37 | 73 | 12 | 6,{12} |
| 41 | 2049 | 320 | 6,{2,2,12} |

| $D$ | $x$ | $y$ | $\left[a_o,\{a_1,a_2,a_3\}\right]$ |
|---|---|---|---|
| 43 | 3482 | 531 | 6,{1,1,3,1,5,1,3,1,1,12} |
| 47 | 48 | 7 | 6,{1,5,1,12} |
| 53 | 66249 | 9100 | 7,{3,1,1,3,14} |
| 59 | 530 | 69 | 7,{1,2,7,2,1,14} |
| 61 | 1766319049 | 226153980 | 7,{1,4,3,1,2,2,1,3,4,1,14} |
| 67 | 48842 | 5967 | 8,{5,2,1,1,7,1,1,2,5,16} |
| 71 | 3480 | 413 | 8,{2,2,1,7,1,2,2,16} |
| 73 | 2281249 | 267000 | 8,{1,1.5,5,1,1,16} |
| 79 | 80 | 9 | 8,{1,7,1,16} |
| 83 | 82 | 9 | 9,{9,18} |
| 89 | 500001 | 53000 | 9,{2,3,3,2,18} |
| 97 | 62809633 | 6377352 | 9,{1,5,1,1,1,1,1,5,1,18} |
| 101 | 201 | 20 | 10,{20} |

## 14.2 Unidad Fundamental de la Norma

### 2.1 Unidad Fundamental de Norma 1

Sea $m$ un entero positivo libre de cuadrados. Entonces

$$S_D=\{(x,y)\mid x\in\mathbb{N},y\in\mathbb{N}\},\ si\ D\equiv 2,3(mód.4)$$

$$S_D=\left\{(\frac{x}{2},\frac{y}{2})\mid x\in\mathbb{N},y\in\mathbb{N},x\equiv y(mód.2)\right\},\ si\ \mathrm{D}\equiv 1(mód.4)$$

Sea $(a,b)\in S_D$ la solución de $a^2-Db^2=1$. Si $\epsilon=a+b\sqrt{D}$ donde $\epsilon$ es una unidad de $o_{\mathbb{Q}\sqrt{D}}$ de una norma, la unidad $\epsilon$ se llama unidad fundamente de norma 1. Si tenemos en cuenta de que

$$\epsilon \geq 1+\sqrt{D} \geq 1+\sqrt{2}, \quad si\ \mathrm{D} \equiv 2,3(mód.4)$$
$$\epsilon \geq \frac{1+\sqrt{D}}{2} \geq \frac{1+\sqrt{5}}{2}, \quad si\ \mathrm{D} \equiv 1(mód.4)$$

entonces $\epsilon > 1$.
Sea $D$ un entero positivo libre de cuadrados. Sea $\epsilon$ la unidad fundamental de norma 1, entonces:

1. $\epsilon$ es la unidad más pequeña en $O_{\mathbb{Q}\sqrt{D}}$ de una norma que es mayor que 1.
2. Cada unidad de $O_{\mathbb{Q}\sqrt{D}}$ de una norma 1 es de la forma $\pm \epsilon^n$ para cualquier entero $n$.
3. Si $\tau$ es una unidad de la norma 1 en $O_{\mathbb{Q}\sqrt{D}}$ tal que $\tau > 1$ y cada unidad de $O_{\mathbb{Q}\sqrt{D}}$ de norma 1 es de la forma $\pm \tau^k$ para cualquier entero $k$, entonces $\tau = \epsilon$.
4. Sea $D$ un entero positivo libre de cuadrados. La unidad fundamental $\eta$ de $O_{\mathbb{Q}\sqrt{D}}$ se define como $\sigma$ si $O_{\mathbb{Q}\sqrt{D}}$ contiene la unidad de la norma -1, y $\epsilon$ en caso contrario.
5. Sea $D$ un entero positivo libre de cuadrados. Entonces, cada unidad de $\eta$ de $O_{\mathbb{Q}\sqrt{D}}$ es de la forma $\pm \eta^n$, $n \in \mathbb{Z}$, donde $\eta$ es la unidad fundamental de $O_{\mathbb{Q}\sqrt{D}}$. Si contiene las unidades de la norma -1, estas se dan para $by \pm \eta^n$ con $n$ impar, y los de norma 1 para $by \pm \eta^n$ con $n$ par.

## 2.2 Unidad Fundamental de Norma -1

Sea $D$ un entero positivo libre de cuadrados tal que $O_{\mathbb{Q}\sqrt{D}}$ contiene la unidad de la norma -1. La única unidad $\sigma > 1$ de norma -1 de tal manera que cada unidad $O_{\mathbb{Q}\sqrt{m}}$ es de la forma $\pm \sigma^n$, $n \in \mathbb{Z}$, y se llama unidad fundamental de $O_{\mathbb{Q}\sqrt{m}}$ de norma -1.

## 2.3 Cálculo de la Unidad Fundamental

Sea $D$ un entero positivo libre de cuadrados, sean $h_n/k_n$, $n = 0,1,2,\ldots$ los convergentes de la fracción continua $\sqrt{D}$ y sea $l$ el período de expansión.

Si $l$ es par, tal que $x^2 - Dy^2 = -1$ no tiene solución en los enteros $x$ e $y$, la solución de $x^2 - Dy^2 = 1$, con los enteros positivos $x$ e $y$ es, al menos $(x, y) = (h_{l-1}, k_{l-1})$.

Si $l$ es impar, entonces $x^2 - Dy^2 = -1$ tiene solución en los enteros $x$ e $y$, y la solución de $x^2 - Dy^2 = 1$, con los enteros positivos $x$ e $y$, viene determinada con , al menos una $x$ dada, por $(x, y) = (h_{l-1}, k_{l-1})$.

Si $D \equiv 2,3(mód.4)$ ó $\mathrm{D} \equiv 1(mód.8)$, todas las unidades de $O_{\mathbb{Q}\sqrt{D}}$ son de la forma $x + y\sqrt{D}$, con $x$ e $y$ enteros, donde la unidad fundamental $\eta$ de $O_{\mathbb{Q}\sqrt{D}}$, viene determinada por $\eta = h_{l-1} + k_{l-1}\sqrt{D}$, $N(\eta) = (-1)^l$.

Si $D \equiv 5(mód.8)$, puede no ser unidades de $O_{\mathbb{Q}\sqrt{D}}$ de la forma $1/2(x + y\sqrt{m})$, con $x$ e $y$ enteros impares. Si no hay unidades de este tipo, $\eta \in \mathbb{Z} + \mathbb{Z}\sqrt{D}$ y, como en el caso anterior, $\eta = h_{l-1} + k_{l-1}\sqrt{D}$, $N(\eta) = (-1)^l$. Si hay unidades de este tipo, entonces $\eta \notin \mathbb{Z} + \mathbb{Z}\sqrt{D}$, y se puede demostrar que $\eta^3 \in \mathbb{Z} + \mathbb{Z}\sqrt{D}$. En este caso, $\eta^3 = x + y\sqrt{D}$, donde $x$ e $y$ son enteros

positivos que satisfacen, al menos para $x$, a $x^2 - Dy^2 = \pm 1$. La unidad fundamental viene determinada por $\eta^3 = h_{l-1} + k_{l-1}\sqrt{D}$, $N(\eta) = (-1)^l$.
Si $\eta = (A + B\sqrt{D})/2$, donde $A$ y $B$ son enteros impares positivos, entonces

$$((A + B\sqrt{D})/2)^3 = h_{l-1} + k_{l-1}\sqrt{D}$$

y así

$$A^3 + 3AB^2D = 8h_{l-1}, \quad 3A^2B + B^3D = 8k_{l-1}$$

por lo tanto

$$A \mid h_{l-1}, \ 1 \le A < 2h_{l-1}^{1/3} \text{ y } B \mid h_{l-1}, \ 1 \le B < 2\left(\frac{h_{l-1}}{2}\right)^{1/3}$$

A partir de este esquema desarrollamos el siguiente algoritmo que nos va a permitir determinar la unidad fundamental $\eta$ de $O_{\mathbb{Q}\sqrt{D}}$, para cualquier $D$ entero y libre de cuadrados.

$$h_{-1} = 1, \ k_{-1} = 0 \text{ y } P_o = 0, \ Q_o = 1, \ a_o = \left[\sqrt{D}\right], \ h_o = \left[\sqrt{D}\right], \ k_o = 1$$

Determinar $P_n$, $Q_n$, $a_n$, $h_n, k_n$, $con\ n = 1, 2, \ldots$ de forma recursiva a través de

$$P_n = a_{n-1}Q_{n-1} - P_{n-1}, \ con\ n = 1, 2, \ldots$$

$$Q_n = \frac{D - P_n^2}{Q_{n-1}}, \ con\ n = 1, 2, \ldots$$

$$a_n = \frac{P_n + \sqrt{D}}{Q_n}, \ con\ n = 1, 2, \ldots$$

$$h_n = a_n h_{n-1} + h_{n-2}, \ con\ n = 1, 2, \ldots$$

$$k_n = a_n k_{n-1} + k_{n-2}, \ con\ n = 1, 2, \ldots$$

Igualdad fundamental si $N > 1$

$$P_N = P_1, \ Q_N = Q_1$$

Para $N - 1 = l$, si $D \equiv 2, 3 (mód.4)$ ó $D \equiv 1 (mód.8)$, entonces

$$\eta = h_{l-1} + k_{l-1}\sqrt{D}, \ N(\eta) = (-1)^l$$

Si $D \equiv 5 (mód.8)$, determinar todos los divisores impares positivos $A$ de $h_{l-1}$ menores que $2h_{l-1}^{1/3}$ y todos los divisores impares positivos $B$ de $k_{l-1}$ menores que $2(k_{l-1}/D)^{1/3}$. Si para algún par $(A, B)$ tenemos $A^3 + 3AB^2D = 8h_{l-1}, \ 3A^2B + B^3D = 8k_{l-1}$ , entonces

$$\eta = \frac{A + B\sqrt{D}}{2}, \;\; N(\eta) = (-1)^l$$

de otra forma

$$\eta = h_{l-1} + k_{l-1}\sqrt{D}, \; N(\eta) = (-1)^l$$

## 2.4 Determinar la unidad fundamental de $D = 31 \equiv 3(mód.4)$.

Empecemos por calcular los términos de la fracción continua y sus convergentes:

$$\sqrt{31} = \left[5, \overline{5,1,1,3,5,3,1,1,10,1,...}\right] \text{ y } \frac{5}{1}, \frac{6}{1}, \frac{11}{2}, \frac{39}{7}, \frac{206}{37}, \frac{657}{118}, \frac{863}{155}, \frac{1520}{273}, \frac{16063}{2885}, \frac{17583}{3158}$$

Partimos con los valores de $h_{-1} = 1, \; k_{-1} = 0, \; P_o = 0, \; Q_o = 1, \; a_o = 5, \; h_o = 5, \; k_o = 1$ y calculamos, sucesivamente, los de $P_n, \; Q_n, \; a_n, \; h_n, k_n, \; con \; n = 1, 2, ...$ mediante la siguiente tabla:

| $n$ | **-1** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_n$ | | 5 | 1 | 1 | 3 | 5 | 3 | 1 | 1 | 10 | 1 |
| $P_n$ | | 0 | 5 | 1 | 4 | 5 | 5 | 4 | 1 | 5 | 5 |
| $Q_n$ | | 1 | 6 | 5 | 3 | 2 | 3 | 5 | 6 | 1 | 6 |
| $h_n$ | 1 | 5 | 6 | 11 | 39 | 206 | 657 | 863 | 1520 | 16063 | 17583 |
| $k_n$ | 0 | 1 | 1 | 2 | 7 | 37 | 118 | 155 | 273 | 2885 | 3158 |

Como $P_9 = P_1 = 5, \; Q_9 = Q_1 = 6,$ encontramos que

$$N = 9, \; l = N - 1 = 8, \; h_{l-1} = h_7 = 1520, \; k_{l-1} = k_7 = 273$$

$$\eta = h_{l-1} + k_{l-1}\sqrt{D} = 1520 + 273\sqrt{31}, \; N(\eta) = (-1)^l = (-1)^8 = 1$$

$$D = 31 \equiv 3(mód.4) \rightarrow 31 - 3 = 28 = 7 \cdot 4$$

La unidad fundamental de $O_{\mathbb{Q}\sqrt{31}}$ es $1520 + 273\sqrt{31}$ de norma 1.

Dado que $K = \mathbb{Q}\sqrt{31}$ es un cuerpo cuadrático real donde $N(a + b\sqrt{31}) = x^2 - 31y^2 = 1$ de donde $1520^2 - 31 \cdot 273^2 = 1,$ el polinomio mínimo que lo genera es $x^2 - 3040x + 1 = 0,$ ya que $(1520 + 273\sqrt{31}) + (1520 - 273\sqrt{31}) = 3040,$ por tanto la unidad fundamental de $O_{\mathbb{Q}\sqrt{31}}$ es $\epsilon = 1520 + 273\sqrt{31}$ de norma 1. No admite la norma -1.

## 2.5 Determinar la unidad fundamental de $D = 41 \equiv 1(mód.8)$.

Los términos de fracción y los convergentes son:

$$\sqrt{41} = \left[6, \overline{2,2,12,2,2,...}\right] \text{ y } \frac{6}{1}, \frac{13}{2}, \frac{32}{5}, \frac{397}{62}, \frac{826}{129}, \frac{2049}{320}$$

El siguiente cuadro recoge los valores necesarios:

| $n$ | **-1** | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|---|
| $a_n$ | | 6 | 2 | 2 | 12 | 2 | 2 |
| $P_n$ | | 0 | 6 | 4 | 6 | 6 | 4 |
| $Q_n$ | | 1 | 5 | 5 | 1 | 5 | 5 |
| $h_n$ | 1 | 6 | 13 | 32 | 397 | 826 | 2049 |
| $k_n$ | 0 | 1 | 2 | 5 | 62 | 129 | 320 |

El cálculo de $P_n$ y $Q_n$ lo hemos determinado de la forma siguiente:

$$P_n = a_{n-1}Q_{n-1} - P_{n-1}:\ P_1 = 6\cdot 1 - 0 = 6,\ P_2 = 2\cdot 5 - 6 = 4,\ P_3 = 2\cdot 5 - 4 = 6,$$
$$P_4 = 12\cdot 1 - 6 = 6,\ P_5 = 2\cdot 5 - 6 = 4$$

$$Q_n = (D - P_n^2)/Q_{n-1}:\ Q_1 = (41 - 6^2)/1 = 5,\ Q_2 = (41 - 4^2)/5 = 5,\ Q_3 = (41 - 6^2)/5 = 1,$$
$$Q_4 = (41 - 6^2)/1 = 5,\ Q_5 = (41 - 4^2)/5 = 5$$

Como $P_4 = P_1 = 6,\ Q_4 = Q_1 = 5,$ encontramos que

$$N = 4,\ l = N\text{-}1 = 3,\ h_{l\text{-}1} = h_2 = 32,\ k_{l\text{-}1} = k_2 = 5$$

$$\eta = h_{l-1} + k_{l-1}\sqrt{D} = 32 + 5\sqrt{41},\ N(\eta) = (-1)^l = (-1)^3 = -1$$

$$D = 41 \equiv 1(mód.8) \rightarrow 41 - 1 = 40 = 5\cdot 8$$

La unidad fundamental de $O_{\mathbb{Q}\sqrt{41}}$ es $32 + 5\sqrt{41}$ de norma -1.

Como $K = \mathbb{Q}\sqrt{41}$ es un cuerpo cuadrático real donde $N(a + b\sqrt{41}) = x^2 - 41y^2 = -1$ de donde $32^2 - 41\cdot 5^2 = -1,$ el polinomio mínimo que lo genera es $x^2 - 64x - 1 = 0,$ ya que $(32 + 5\sqrt{41}) + (32 - 5\sqrt{41}) = 64,$ por tanto la unidad fundamental de $O_{\mathbb{Q}\sqrt{41}}$ es $\sigma = 32 + 5\sqrt{41}$ de norma -1.

Vamos a utilizar el programa sobre teoría de números de Keith Matthews, profesor de matemáticas y físicas de la Universidad de Queensland, Australia, para demostrar que el supuesto anterior también admite la norma 1.

Para $P^2 \equiv 41(mód.1)$ la posible solución de $P$ la encontraremos en el rango $0 \le P \le 1/2:\ [0] = (0 + \sqrt{41})/1:$

$$(P_0 + \sqrt{41})/Q_0 = (0 + \sqrt{41})/1,\ h_o/k_o = 6/1$$
$$(P_1 + \sqrt{41})/Q_1 = (6 + \sqrt{41})/5,\ h_1/k_1 = 13/2$$
$$(P_2 + \sqrt{41})/Q_2 = (4 + \sqrt{41})/5,\ h_2/k_2 = 32/5$$
$$(P_3 + \sqrt{41})/Q_3 = (6 + \sqrt{41})/1,\ h_3/k_3 = 397/62$$
$$(P_4 + \sqrt{41})/Q_4 = (6 + \sqrt{41})/5,\ h_4/k_4 = 826/129$$
$$(P_5 + \sqrt{41})/Q_5 = (4 + \sqrt{41})/5,\ h_5/k_5 = 2049/320$$

de donde la unidad fundamental de $O_{\mathbb{Q}\sqrt{41}}$ es $2049+320\sqrt{41}$ de norma 1.

Como $K=\mathbb{Q}\sqrt{41}$ es un cuerpo cuadrático real donde $N(a+b\sqrt{41})=x^2-41y^2=1$ de donde $2049^2-41\cdot 320^2=1,$ el polinomio mínimo que lo genera es $x^2-4098x+1=0,$ ya que $(2049+320\sqrt{41})+(2049-320\sqrt{41})=4098,$ por tanto la unidad fundamental de $O_{\mathbb{Q}\sqrt{41}}$ es $\epsilon=2049+320\sqrt{41}$ de norma 1.

## 2.6 Determinar la unidad fundamental de $D=13\equiv 5(mód.8).$

Los términos de fracción y los convergentes son:

$$\sqrt{13}=\left[3,\overline{1,1,1,1,6,1,...}\right] \text{ y } \frac{3}{1},\frac{4}{1},\frac{7}{2},\frac{11}{3},\frac{18}{5},\frac{119}{33},\frac{137}{38}$$

El siguiente cuadro recoge los valores necesarios:

| $n$ | **-1** | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
|---|---|---|---|---|---|---|---|---|
| $a_n$ | | 3 | 1 | 1 | 1 | 1 | 6 | 1 |
| $P_n$ | | 0 | 3 | 1 | 2 | 1 | 3 | 3 |
| $Q_n$ | | 1 | 4 | 3 | 3 | 4 | 1 | 4 |
| $h_n$ | 1 | 3 | 4 | 7 | 11 | 18 | 119 | 137 |
| $k_n$ | 0 | 1 | 1 | 2 | 3 | 5 | 33 | 38 |

Si $P_6=P_1=3,\ Q_6=Q_1=4,$ tenemos $N=6,\ l=N\text{-}1=5,\ h_{l\text{-}1}=h_4=18,\ k_{l\text{-}1}=k_4=5.$

Para un $A$ impar, $A\mid h_{l-1},\ 1\le A<2h_{l-1}^{1/3}\ \Rightarrow\ A\mid 9,\ 1\le A<5.3\ \Rightarrow A=1$ ó $3.$

Para un $B$ impar, $B\mid k_{l-1},\ 1\le B<2\left(\frac{k_{l-1}}{D}\right)^{1/3}\ \Rightarrow\ B\mid 5,\ 1\le B<1{,}5\ \Rightarrow B=1.$

Del par $(A,B)=(1,1),\ (3,1)$ solamente el segundo satisface al par de ecuaciones

$$A^3+39AB^2=144,\ 3\mathrm{A}^2\mathrm{B}+13\mathrm{B}^3=40$$

por lo tanto la unidad fundamental $\eta(>1)$ de $O_{\mathbb{Q}\sqrt{13}}$ es

$$\eta=\left(\frac{3+\sqrt{13}}{2}\right)\left(\frac{3-\sqrt{13}}{2}\right)=-1,\ N(\eta)=-1$$

Esta solución es equivalente a $18^2-13\cdot 5^2=-1.$ ¿Por qué?

En el primer caso genera un polinomio mínimo $x^2-3x-1=0$ que tiene como solución $x=\pm\frac{3\pm\sqrt{13}}{2}.$

En el segundo caso, $x^2-36x-1=0$ es el polinomio mínimo generado que tiene como solución $x=18\pm 5\sqrt{13}.$

Las conclusiones de por qué de estas variaciones las dejamos en manos del lector.

En cuanto a $D=13\equiv 5(mód.8)\ \rightarrow\ 13-5=8=8\cdot 1.$

## 2.7 Determinar la unidad fundamental de $\sqrt{26}$.

Los términos de fracción y los convergentes son:

$$\sqrt{26}=\left[5,\overline{10,10,10,10,...}\right] \text{ y } \frac{5}{1},\frac{51}{10},\frac{515}{101},\frac{5201}{1020},\frac{52525}{10301}$$

Utilizando el programa del profesor Keith Matthews, calculamos

$$(P_0+\sqrt{26})/Q_0=(0+\sqrt{26})/1,\ h_o/k_o=5/1$$
$$(P_1+\sqrt{26})/Q_1=(5+\sqrt{26})/1,\ h_o/k_o=51/10$$
$$(P_2+\sqrt{26})/Q_2=(5+\sqrt{26})/1,\ h_o/k_o=5/1$$

de donde $(x,y)=(5,1)$ satisface a la unidad -1 y $(x,y)=(51,10)$ a la unidad 1. Por tanto la unidad fundamental de $O_{\mathbb{Q}\sqrt{26}}$ es $5+\sqrt{26}$ de norma -1 y $51+10\sqrt{26}$ de norma 1. Podemos representar estas normas como

$$\left(5+\sqrt{26}\right)^2\left(5-\sqrt{26}\right)^2=1 \text{ y } \left(5+\sqrt{26}\right)\left(5-\sqrt{26}\right)=-1$$

En la siguiente tabla recogemos valores de $D$ que generan norma doble de 1 y -1:

| $D$ | $(x,y),(+1)$ | $(x,y),(-1)$ |
|---|---|---|
| 2 | 3,2 | 1,1 |
| 5 | 9,4 | 2,1 |
| 10 | 19,6 | 3,1 |
| 13 | 649,180 | 18,5 |
| 17 | 33,8 | 4,1 |
| 26 | 51,10 | 5,1 |
| 29 | 9801,1820 | 70,13 |
| 37 | 73,12 | 6,1 |
| 41 | 2949,320 | 32,5 |
| 50 | 99,14 | 7,1 |
| 53 | 66249,9100 | 182,25 |

| $D$ | $(x,y),(+1)$ | $(x,y),(-1)$ |
|---|---|---|
| 58 | 19603,2574 | 99,13 |
| 61 | 1766319049,226153980 | 29718,3805 |
| 65 | 129,16 | 8,1 |
| 73 | 2281249,26700 | 1068,125 |
| 74 | 3699,430 | 43,5 |
| 82 | 163,18 | 9,1 |
| 85 | 285769,30996 | 378,41 |
| 89 | 500001,53000 | 500,53 |
| 97 | 62809633,6377352 | 5604,569 |
| 101 | 201,20 | 10,1 |
| 106 | 32080051,3115890 | 4005,389 |

## 2.8 Algoritmo de Lagrange

En el año 1768, Joseph-Louis Lagrange(1736-1813), demostró que si $x^2-Dy^2=N$, $\{x,y\}>0$, $mcd(x,y)=1$ y $|N|<\sqrt{D}$, entonces $x/y$ es un convergente $A_n/B_n$ de la fracción continua simple. Ya que si hacemos

$$(x+y\sqrt{D})(x-y\sqrt{D})=N,\ \left|x-y\sqrt{D}\right|=\frac{|N|}{x+y\sqrt{D}}<\frac{D}{x+y\sqrt{D}}$$

tenemos

$$\frac{x}{y}>\sqrt{D}\ \Rightarrow\ \left|\frac{x}{y}-\sqrt{D}\right|<\frac{1}{2y^2} \text{ y } \frac{x}{y}>\sqrt{D}\ \Rightarrow\ \left|\frac{y}{x}-\frac{1}{\sqrt{D}}\right|<\frac{1}{2x^2}$$

Si $\sqrt{D}=\left[a_o,\overline{a_1,...,a_l}\right]$, debido a la periodicidad de $(-1)^{n+1}(A_n^2-DB_n^2)$, para la solución, solamente tenemos que comprobar los valores del rango $0\le n\le\lfloor l/2\rfloor-1$. Para encontrar todas las soluciones, comprobamos el rango $0\le n\le l-1$.

Por ejemplo, para $\sqrt{13}=\left[3,\overline{1,1,1,,1,6}\right]$. Convergentes $\frac{3}{1},\frac{4}{1},\frac{7}{2},\frac{11}{3},\frac{18}{5}$.

| $n$ | $A_n/B_n$ | $A_n^2-13B_n^2$ |
|---|---|---|
| 0 | 3/1 | -4 |
| 1 | 4/1 | 3 |
| 2 | 7/2 | -3 |
| 3 | 11/3 | 4 |
| 4 | 18/5 | -1 |

La solución positiva $(x,y)$ viene determinada por

$$x+y\sqrt{13}=\begin{cases}\eta^{2n}(4+\sqrt{13}), & \text{n}\ge 0\\ \eta^{2n+1}(4+\sqrt{13}), & \text{n}\ge 0\end{cases}$$

donde $\eta=18+5\sqrt{13}$ y $7+2\sqrt{13}=\eta-(-4+\sqrt{13})$.
La solución cuadrática de la ecuación es $x^2-Dy^2=18^2-13\cdot 5^2=-1$.

## 2.9 Método de Gauss

El método propuesto por Carl Friedrich Gauss (1777-1855) se basa en el siguiente esquema: Supuesto $\alpha^2-D\gamma^2=N$, donde $N\ne 0$, $D>0$ libre de cuadrados y $mcd(\alpha,\gamma)=1$. Supuesto también $\alpha\delta-\beta\gamma=1$, entonces si $P=\alpha\beta-D\gamma\delta$, tenemos que

$$a)\ \alpha\equiv -P\gamma(mód.|N|)$$
$$b)\ P^2-D=N(\beta^2-D\delta^2)$$

y en particular

$$P^2\equiv D(mód.|N|)$$

Por ejemplo, para $P^2\equiv 3(mód.31)$ donde $\sqrt{31}=\left[5,\overline{1,1,3,5,3,1,...}\right]$ y los convergentes son $\left\{\frac{5}{1},\frac{6}{1},\frac{11}{2},\frac{39}{7},\frac{206}{37},\frac{657}{118}\right\}$, como ya hemos visto en un supuesto anterior.

Si tenemos en cuenta que $a_n=\frac{P_n+\sqrt{D}}{Q_n}$, $P_n=-P_{n-1}+a_{n-1}Q_{n-1}$ y $Q_n=\frac{D-P_n^2}{Q_{n-1}}$, de donde $P_o=0,\ Q_o=1,\ a_o=\left[\sqrt{D}\right]$ y $h_n=a_nh_{n-1}+h_{n-2},\ k_n=a_nk_{n-1}+k_{n-2}$, entonces para $m=31\equiv 3(mód.4)$ obtenemos:

$$h_{n-1}=1,\ k_{n-1}=0,\ P_o=0,\ Q_o=1,\ a_o=5,\ h_o=5,\ k_o=1$$

y el resto de valores de $P_n,\ Q_n,\ a_n,\ h_n,\ k_n$ los obtenemos el siguiente cuadro:

| $n$ | $P_n$ | $Q_n$ | $a_n$ | $h_n$ | $k_n$ |
|---|---|---|---|---|---|
| -1 | | | | 1 | 0 |
| 0 | 0 | 1 | 5 | 5 | 1 |
| 1 | 5 | 6 | 1 | 6 | 1 |
| 2 | 1 | 5 | 1 | 11 | 2 |
| 3 | 4 | 3 | 3 | 39 | 7 |
| 4 | 5 | 2 | 5 | 206 | 37 |
| 5 | 5 | 3 | 3 | 657 | 118 |
| 6 | 4 | 5 | 1 | 863 | 155 |
| 7 | 1 | 6 | 1 | 1520 | 273 |
| 8 | 5 | 1 | 10 | 16063 | 2885 |
| 9 | 5 | 6 | 1 | 17583 | 3158 |

Como $P_9 = P_1 = 5,\ \ Q_9 = Q_1 = 6,$ obtenemos

$$N = 9,\ l = N - 1 = 8,\ h_{l-1} = h_7 = 1520,\ k_{l-1} = k_7 = 273,$$

$$\eta = h_{l-1} + k_{l-1}\sqrt{D} = 1520 + 273\sqrt{31},\ \ N_{(\eta)} = (-1)^l = 1$$

de donde la unidad fundamental de $0_{Q(\sqrt{31})} = 1520 + 273\sqrt{31}$ de norma 1.

Hemos llegado a las mismas conclusiones que en la solución anterior aplicando otro método distinto.

## 14.3 Formas Cuadráticas Binarias

### 3.1 Definición

Una forma cuadrática binaria es un polinomio $f(x,y) \in \mathbb{Z}[x,y],$ el cual es homogéneo de grado 2. La forma cuadrática $f(x,y)$ tiene la forma general $f(x,y) = ax^2 + bxy + cy^2$ donde $< a,b,c > \in \mathbb{Z}$ son los coeficientes y $D = b^2 - 4ac$ el discriminante. Las propiedades de las formas cuadráticas binarias dependen de manera esencial de la naturaleza de los coeficientes.

En la ecuación $ax^2 + bxy + cy^2 = m,$ si $a = 0$ o $c = 0$ la solución es trivial, ya que una de las incógnitas ha de ser un divisor de $m$ y generar un número finito de soluciones. Supongamos el caso en que $a \neq 0$ o $c \neq 0.$

Si factorizamos el polinomio $ax^2 + bxy + cy^2 = a(x - \alpha)(x - \beta),$ la ecuación se convierte en

$$a(x - \alpha y)(x - \beta y) = m$$

donde los números $\alpha$ y $\beta$ son $\dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$

Si $D = 0$ entonces $\alpha = \beta = -b/2a,$ que multiplicada por $4a$ obtenemos la ecuación

$$(2ax + by)^2 = 4am,$$

con soluciones fáciles de determinar.

Si $D = k^2 \neq 0,$ entonces multiplicando por $4a$ obtenemos

$$(2ax + ky)(2ax - ky) = 4am$$

que a su vez se reduce a un número finito de sistemas de ecuaciones de la forma

$$2ax+ky=u \text{ y } 2ax-ky=v$$

donde $u$ y $v$ recorren las factorizaciones de $4am$. Si $n=0$ la ecuación se reduce a $2ax\pm ky=0,$ con solución fácil de obtener. Si $n\neq 0,$ el número de soluciones es finito.
Si $D$ no es un cuadrado perfecto, entonces $\alpha$ y $\beta$ son elementos del cuerpo $K=\mathbb{Q}\sqrt{D}$. Si llamamos $N$ a la norma en $\mathbb{Q}\sqrt{D},$ la ecuación puede ser expresada en la forma

$$N(x-\alpha y)=m/a$$

A partir de las funciones hiperbólicas, las formas cuadráticas binarias, que podemos escribir como $ax^2+bxy+cy^2=m,$ tienen como solución

$$x=\frac{-by\pm\sqrt{y^2(b^2-4ac)+4am}}{2a},\ y=\frac{-bx\pm\sqrt{x^2(b^2-4ac)+4cm}}{2c}$$

o bien

$$f(x,y)=\frac{(2ax+by)^2-Dy^2}{4a}=m$$

Matemáticamente hablando, es importante conocer el manejo de algunas herramientas utilizadas para la resolución de este tipo de ecuaciones:

$$\left(a+b\sqrt{D}\right)\left(a-b\sqrt{D}\right)=a^2-Db^2,\ \left(a+b\sqrt{D}\right)+\left(a-b\sqrt{D}\right)=2a,\ \frac{\left(a+b\sqrt{D}\right)-\left(a-b\sqrt{D}\right)}{\sqrt{D}}=2b$$

$$a=\frac{m-y(bx+cy^2)}{x^2},\ b=\frac{m-ax^2-cy^2}{xy},\ c=\frac{m-x(ax+by)}{y^2}$$

Ejemplo: Resolver $x^2+5xy+2y^2=1.$

Una solución sencilla de una forma cuadrática $ax^2+bxy+cy^2=m,$ requiere los siguientes pasos:

Calcular el discriminante:

$$b^2-4ac=5^2-4\cdot 1\cdot 2=17$$

Calcular la estructura del número algebraico:

$$\mathbb{Q}\sqrt{D}=\sqrt{17}$$

Calcular la norma:

$$N(\alpha,\beta)=(\alpha+\beta\sqrt{D})(\alpha-\beta\sqrt{D})=(33+8\sqrt{17})(33-8\sqrt{17})=1$$

Calcular una variable:

$$[(\alpha+\beta\sqrt{D})-(\alpha-\beta\sqrt{D})]/\left(\sqrt{D}\right)=\frac{(33+8\sqrt{17})-(33-8\sqrt{17})}{\sqrt{17}}=\pm 16$$

Calcular la otra variable:

$$x^2+bx+c=0=x^2+5x16+2\cdot 16^2-1=0=x^2+80x+511=\begin{cases}x_1=-7\\ x_2=-73\end{cases}$$

Por lo que, una de las muchas soluciones, es $(-7)^2+5\cdot 16(-7)+2\cdot 16^2=1,$ que podemos ratificar mediante

$$x=\frac{-5\cdot 16+\sqrt{16^2(5^2-4\cdot 1\cdot 2)+4\cdot 1\cdot 1}}{2\cdot 1}=-7,\ y=\frac{-5(-7)+\sqrt{7^2(5^2-4\cdot 1\cdot 2)+4\cdot 2\cdot 1}}{2\cdot 2}=16$$

$$f(x,y)=\frac{(2ax+by)^2-Dy^2}{4a}=m=\frac{(2\cdot 1\cdot(-7)+5\cdot 16)^2-17\cdot 16^2}{4\cdot 1}=1$$

Los valores de $<a,b,c>$ pueden ser determinados mediante las fórmulas

$$a=\frac{m-y(bx+cy^2)}{x^2}=\frac{1-16(5(-7)+2\cdot 16)}{(-7)^2}=1$$

$$b=\frac{m-ax^2-cy^2}{xy}=\frac{1-1(-7)^2-2\cdot 16^2}{(-7)16}=5$$

$$c=\frac{m-x(ax+by)}{y^2}=\frac{1-(-7)((1(-7)+5\cdot 16))}{16^2}=2$$

La solución a esta ecuación, mediante el programa Mathematicas 7, es:

Sea $x=-\frac{1}{2}\sqrt{\frac{4am+\left(b^2-4ac\right)y^2}{a^2}}-\frac{by}{2a}=-\frac{1}{2}\sqrt{\frac{4am+Dy^2}{a^2}}-\frac{by}{2a}$

$$y=\pm\frac{\left(33-8\sqrt{17}\right)^n-\left(33+8\sqrt{17}\right)^n}{\sqrt{17}},\ con\ n\in\mathbb{Z},n\geq 0$$

$$x=\frac{1}{34}\left(\pm 5\sqrt{17}\left(\left(33-8\sqrt{17}\right)^n-\left(33+8\sqrt{17}\right)^n\right)+17\left(\left(33-8\sqrt{17}\right)^n+\left(33+8\sqrt{17}\right)^n\right)\right),\ con\ n\in\mathbb{Z},n\geq 0$$

$$x=\frac{1}{34}\left(17\left(\pm\left(33-8\sqrt{17}\right)^n\pm\left(33+8\sqrt{17}\right)^n\right)\pm 5\sqrt{17}\left(\left(33-8\sqrt{17}\right)^n-\left(33+8\sqrt{17}\right)^n\right)\right),\ con\ n\in\mathbb{Z},n\geq 0$$

donde encontramos tantas soluciones como cambios de signos y/o valores a $n$ apliquemos. Vean el cuadro siguiente:

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $x$ | -1 | 7 | 463 | 30551 | 2015903 | 133019047 |
| $y$ | 0 | -16 | -1056 | -69680 | -4597824 | -303386704 |
| | | | | | | |
| $x$ | 1 | 73 | 4817 | 317849 | 20973217 | 1383914473 |
| $y$ | 0 | -16 | -1056 | -69680 | -4597824 | 303386704 |
| | | | | | | |
| $x$ | -1 | -73 | -4817 | -317849 | -20973217 | -1383914473 |
| $y$ | 0 | 16 | 1056 | 69680 | 4597824 | 303386704 |
| | | | | | | |
| $x$ | 1 | -7 | -463 | -30551 | -2015903 | -133019047 |
| $y$ | 0 | 16 | 1056 | 69680 | 4597824 | 303386704 |

Entre las muchas soluciones encontramos para $x=-73,\ y=16.$ Vamos a demostrar que son soluciones ciertas.

$$x^2+5xy+2y^2=1=(-73)^2+5(-73)\cdot 16+2\cdot 16^2$$

$$x=-\frac{1}{2}\sqrt{\frac{4am+Dy^2}{a^2}}-\frac{by}{2a}=-\frac{1}{2}\sqrt{\frac{4\cdot 1\cdot 1+17\cdot 16^2}{1^2}}-\frac{5\cdot 16}{2\cdot 1}=-73$$

$$y=-\frac{\left(33-8\sqrt{17}\right)^1-\left(33+8\sqrt{17}\right)^1}{\sqrt{17}}=16,\ con\ n\in\mathbb{Z}, n\geq 0$$

$$f(x,y)=\frac{(2ax+by)^2-Dy^2}{4a}=m=\frac{(2\cdot 1\cdot(-73)+5\cdot 16)^2-17\cdot 16^2}{4\cdot 1}=1$$

Ejemplo: Resolver la ecuación $x^2+6xy+2y^2=1.$

$$y=-\frac{\left(8-3\sqrt{7}\right)^n-\left(8+3\sqrt{7}\right)^n}{2\sqrt{7}},$$

$$x=\frac{1}{2}\left(-\left(8-3\sqrt{7}\right)^n-\left(8+3\sqrt{7}\right)^n\right)+\frac{3\left(\left(8-3\sqrt{7}\right)^n-\left(8+3\sqrt{7}\right)^n\right)}{2\sqrt{7}},\ con\ n\in\mathbb{Z}, n\geq 0$$

$$y=\frac{\left(8-3\sqrt{7}\right)^s-\left(8+3\sqrt{7}\right)^s}{2\sqrt{7}},$$

$$x=\frac{1}{2}\left(-\left(8-3\sqrt{7}\right)^s-\left(8+3\sqrt{7}\right)^s\right)-\frac{3\left(\left(8-3\sqrt{7}\right)^s-\left(8+3\sqrt{7}\right)^s\right)}{2\sqrt{7}},\ con\ n\in\mathbb{Z}, n\geq 0$$

$$y=-\frac{\left(8-3\sqrt{7}\right)^s-\left(8+3\sqrt{7}\right)^s}{2\sqrt{7}},$$

$$x=\frac{3\left(\left(8-3\sqrt{7}\right)^s-\left(8+3\sqrt{7}\right)^s\right)}{2\sqrt{7}}+\frac{1}{2}\left(\left(8-3\sqrt{7}\right)^s+\left(8+3\sqrt{7}\right)^s\right),\ con\ n\in\mathbb{Z}, n\geq 0$$

$$y=\frac{\left(8-3\sqrt{7}\right)^s-\left(8+3\sqrt{7}\right)^s}{2\sqrt{7}},$$

$$x=\frac{1}{2}\left(\left(8-3\sqrt{7}\right)^s+\left(8+3\sqrt{7}\right)^s\right)-\frac{3\left(\left(8-3\sqrt{7}\right)^s-\left(8+3\sqrt{7}\right)^s\right)}{2\sqrt{7}},\ con\ n\in\mathbb{Z}, n\geq 0$$

Dejamos en manos del lector la comprobación de estas soluciones.

## 3.2 Método de Harvey Cohn

En su obra Advanced Number Theory, el profesor Harvey Cohn de la Universidad de New York, propone el siguiente generador para dar soluciones a la ecuación binaria

$$f(x,y)=ax^2+bxy+cy^2=(x+y/2)^2+(3^{1/2}y/2)^2=m$$

Por ejemplo, para $x=5,\ y=6$

$$(x+y/2)^2+(3^{1/2}y/2)^2=(5+6/2)^2+(5^{1/2}\cdot 6/2)^2=64+45=109$$

## 3.3 Resolver la ecuación $x^2+6xy+4y^2=1.$

El discriminante de es esta ecuación es $D=6^2-4\cdot 1\cdot 4=20=5\cdot 2^2\rightarrow\Delta=5,$ que inicialmente no es libre de cuadrados.

A partir de las tablas, para $N(a+b\sqrt{5})=x^2-5y^2=1=9^2-5\cdot 4^2.$ Esto nos lleva a una forma cuadrática del campo real donde $(9+4\sqrt{5})(9-4\sqrt{5})=1$ y $(9+4\sqrt{5})+(9-4\sqrt{5})=18,$ generan un polinomio mínimo de $x^2-18x+1=0.$
Aplicado a la ecuación planteada, como una de las variables debe tener como solución

$$x=y=\pm\frac{(9+4\sqrt{5})-(9-4\sqrt{5})}{2\sqrt{5}}=\pm 4$$

basta sustituir en una de las variables para despejar la otra. Por ejemplo, para $\pm y,$ tenemos $x^2+24x\pm 64=0,$ que tiene como soluciones $x=\pm 3,\pm 21.$
Por este mismo procedimiento podemos encontrar algunas otras soluciones como:

| $x$ | $\pm 3,\pm 21$ | $\pm 55,\pm 377$ | $\pm 987,\pm 6765$ |
|---|---|---|---|
| $y$ | $\pm 4$ | $\pm 72$ | $\pm 1272$ |

Por el *Programa Mathematicas*, una solución puede ser:

$$y=\pm\frac{\left(9+4\sqrt{5}\right)^n-\left(9-4\sqrt{5}\right)^n}{2\sqrt{5}}$$

$$x=\pm\frac{3\left(\left(9+4\sqrt{5}\right)^n-\left(9-4\sqrt{5}\right)^n\right)}{2\sqrt{5}}+\frac{\left(9-4\sqrt{5}\right)^n+\left(9+4\sqrt{5}\right)^n}{2}, n\in Z$$

que tiene infinitas soluciones, tantas como valores le asignemos a $n.$

## 14.4 Grupos de clases.

### 4.1 Propiedades de las formas reducidas

Se dice que la forma definida positiva $< a,b,c >$ es reducida si $|b| \le a \le c$ y en caso de que $|b| = a$ ó $a = c$, entonces $b \ge 0$. Si el discriminante $D < 0$, $|b| \le \sqrt{\frac{|D|}{3}}$ o bien $|a| \le \sqrt{\frac{|D|}{3}}$, ya que $|D| = 4ac - b^2 \ge 4a^2 - a^2$. El número de formas reducidas del discriminante $-D$ es finito.

El entero $m$ se dice que está representado por la forma cuadrática binaria $< a,b,c >$, si existen números enteros $x$ e $y$ tales que $m = ax^2 + bxy + cy^2$. Así, por ejemplo 31 se representa por la forma $x^2 + xy + 3y^2$ cómo $31 = 1^2 + 1 \cdot 3 + 3 \cdot 3^2$, pero 2 no está representado por la forma $x^2 + 5y^2$. En el primer caso $D = 1^2 - 4 \cdot 1 \cdot 3 = -11$, y $D = 0^2 - 4 \cdot 1 \cdot 5 = -20$ para el segundo, dos discriminantes distintos.

Como $a + b\sqrt{m},\ a,b \in \mathbb{Z},\ (m = -1,-2)$ y $\frac{a + b\sqrt{m}}{2},\ a,b \in \mathbb{Z},\ (m = -3,-7,-11)$ son dominios euclídeos, podemos determinar cuándo un primo $p$ está representado por cada una de las formas $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + xy + y^2$, $x^2 + xy + 2y^2$ y $x^2 + xy + 3y^2$. Para ello aplicaremos las propiedades de la Ley de Reciprocidad Cuadrática de Legendre, valorando $p$ como número primo impar.

1. Si $p$ es un número primo tal que $p \equiv 1(mód.4)$, entonces existen dos enteros $x$ e $y$ tales que $p = x^2 + y^2$. Ejemplo: $29 = 5^2 + 2^2$.
2. Si $p$ es un número primo tal que $p \equiv 1,3(mód.8)$, entonces existen dos enteros $x$ e $y$ tales que $p = x^2 + 2y^2$. Ejemplo: $83 = 9^2 + 2 \cdot 1^2$.
3. Si $p$ es un número primo tal que $p \equiv 1(mód.3)$, entonces existen dos enteros $x$ e $y$ tales que $p = x^2 + xy + y^2$. Ejemplo: $43 = 7^2 + 7(-6) + (-6)^2$.
4. Si $p$ es un número primo tal que $p \equiv 1,2,4(mód.7)$, entonces existen dos enteros $x$ e $y$ tales que $p = x^2 + xy + 2y^2$. Ejemplo: $23 = 3^2 + 3 \cdot 2 + 2 \cdot 2^2$.
5. Si $p$ es un número primo tal que $p \equiv 1,3,4,5,9(mód.11)$, entonces existen dos enteros $x$ e $y$ tales que $p = x^2 + xy + 3y^2$. Ejemplo: $71 = 1^2 + 1 \cdot (-5) + 3 \cdot (-5)^2$.

Otras representaciones podrían ser:
Si $p$ es un número primo tal que $p \equiv 1,7(mód.8)$, entonces existen dos enteros $x$ e $y$ tales que $p = x^2 - 2y^2$. Por ejemplo: $41 = (-29)^2 - 2 \cdot 20^2$.
Si tenemos en cuenta que $\left(3 + 2\sqrt{2}\right)\left(3 - 2\sqrt{2}\right) = 1$

$$x = \frac{1}{2}\left(-7\left(3 - 2\sqrt{2}\right)^1 + 2\sqrt{2}\left(3 - 2\sqrt{2}\right)^1 - 7\left(3 + 2\sqrt{2}\right)^1 - 2\sqrt{2}\left(3 + 2\sqrt{2}\right)^1\right) = -29$$

$$y = \frac{1}{4}\left(4\left(3 - 2\sqrt{2}\right)^1 - 7\sqrt{2}\left(3 - 2\sqrt{2}\right)^1 + 4\left(3 + 2\sqrt{2}\right)^1 + 7\sqrt{2}\left(3 + 2\sqrt{2}\right)^1\right) = 20$$

Si $p$ es un número primo tal que $p \equiv 1,11(mód.12)$, entonces existen dos enteros $x$ e $y$ tales que, o $p = x^2 - 3y^2$ ó $p = 3y^2 - x^2$. Por ejemplo: $61 = 19^2 - 3 \cdot 10^2$.

Si tenemos en cuenta que $\left(2+\sqrt{3}\right)\left(2-\sqrt{3}\right)=1$

$$x=\frac{1}{2}\left(8\left(2-\sqrt{3}\right)^{1}-\sqrt{3}\left(2-\sqrt{3}\right)^{1}+8\left(2+\sqrt{3}\right)^{1}+\sqrt{3}\left(2+\sqrt{3}\right)^{1}\right)=19$$

$$y=\frac{1}{6}\left(3\left(2-\sqrt{3}\right)^{1}-8\sqrt{3}\left(2-\sqrt{3}\right)^{1}+3\left(2+\sqrt{3}\right)^{1}+8\sqrt{3}\left(2+\sqrt{3}\right)^{1}\right)=10$$

Por ejemplo: $p=3y^2-x^2=3\cdot 17^2-28^2=83.$ Como podemos comprobar.
Si $p$ es un número primo tal que $p\equiv 1,5,19,23(mód.24),$ entonces existen dos enteros $x$ e $y$ tales que, ó $p=x^2-6y^2$ ó $p=6y^2-x^2$. Ejemplo: $101=6\cdot 39^2-95^2$.
Si tenemos en cuenta que $\left(5+2\sqrt{6}\right)\left(5-2\sqrt{6}\right)=1$

$$y=\frac{1}{12}\left(30\left(5-2\sqrt{6}\right)^{1}-7\sqrt{6}\left(5-2\sqrt{6}\right)^{1}+30\left(5+2\sqrt{6}\right)^{1}+7\sqrt{6}\left(5+2\sqrt{6}\right)^{1}\right)=39$$

$$x=\frac{1}{2}\left(7\left(5-2\sqrt{6}\right)^{1}-5\sqrt{6}\left(5-2\sqrt{6}\right)^{1}+7\left(5+2\sqrt{6}\right)^{1}+5\sqrt{6}\left(5+2\sqrt{6}\right)^{1}\right)=95$$

Por ejemplo: $p=x^2-6y^2=91^2-6\cdot 37^2=67.$ Como podemos comprobar.
Podemos observar que, en las soluciones de estas últimas representaciones, los valores de $x$ e $y$ van expresados con exponente 1, lo que denota un sistema indeterminado con múltiples soluciones.

### 4.2 Calcular las representaciones de $p=x^2+21y^2$ donde $D=-84.$

Empecemos por calcular las soluciones de $x^2+21y^2\equiv r(mód.84)$. Con un poco de paciencia, obtenemos para $r$ :

$$r=0,1,4,9,16,18,21,22,25,28,30,36,37,42,46,49,57,58,60,64,70,72,78,81$$

Si ahora tomamos valores para $p=84k+r,$ algunas representaciones de $p=x^2+21y^2$ pueden ser:

$$p=x^2+21y^2=\begin{cases}277=16^2+21\cdot 1^2\\ 337=1^2+21\cdot 4^2\\ 541=4^2+21\cdot 5^2\end{cases}$$

Podemos encontrar muchas más.
Para el discriminante $D=-84,$ encontramos otras representaciones, tales como

$$3x^2+7y^2,\ \ 2x^2+2xy+11y^2,\ \ 5x^2+4xy+5y^2$$

con las que les invitamos a que, mediante

$$3x^2+7y^2\equiv r(mód.84),\ \ 2x^2+2xy+11y^2\equiv r(mód.84),\ \ 5x^2+4xy+5y^2\equiv r(mód.84)$$

busquen números primos $p$ que satisfagan algunas de estas representaciones.

## 4.3 Método de Jeffrey Stopple

Jeffrey Stopple, profesor de matemáticas de la Universidad de Santa Bárbara, en California, en su obra A Primer of Analytic Number Theory, nos propone el siguiente método sobre las reducidas que transcribimos a continuación. (*) La cuestión de si un número primo $p$ se puede escribir, por ejemplo, como $2x^2+3y^2$, obviamente, es la misma que si se puede escribir como $3x^2+2y^2$. Todo lo que hemos hecho es cambiar el papel de $x\ e\ y$. Un poco menos obvio, es $2x^2+4xy+5y^2$. La razón es que esto es sólo $2(x+y)^2+3y^2$. Hemos cambiado las variables $(x,y)$ por $(x+y,y)$, y pueden fácilmente cambiarse de nuevo: $2(x-y)^2+4(x-y)y+5y^2=2x^2+3y^2$. Una solución $(x,y)$ de $2x^2+3y^2=p$ es equivalente a la solución de $(x'=x-y,y'=y)$ de $2x'^2+4x'y'+5y'^2=p$. Para evitar este tipo de redundancia, Gauss propuso una relación de equivalencias de formas tales que $f=(a,b,c)\ y\ f'=(a',b',c')$ son equivalentes. Si hay un cambio de variables, $f$ se convierte en $f'$. Concretamente, Gauss define a $f$ como equivalente a $f'$ si es un entero de la matriz $M$, donde $(x,y)M$ denota la multiplicación de matrices:

$$(x,y)\begin{vmatrix} r & s \\ t & u \end{vmatrix} \text{ se define como } (rx+ty, sx+uy)$$

donde la inversa resulta

$$M=\begin{vmatrix} r & s \\ t & u \end{vmatrix} \quad \text{es} \quad \frac{1}{ru-st}\begin{vmatrix} r & s \\ t & u \end{vmatrix}$$

La inversa es un número entero de la matriz cuando $1/(ru-st)$ es un número entero, de modo que, el factor determinante $(ru-st)$ debe ser $\pm 1$. Se simplifican las cosas si, en nuestra relación de equivalencia el determinante de $M$ es $+1$. El conjunto de todas estas matrices constituyen otro ejemplo de grupo. En este ejemplo, la operación de grupo, de multiplicación de matrices, en general, no es conmutativa. El cambio de variables en $2x^2+3y^2 \sim 3x^2+2y^2$ corresponde a la matriz $M=\begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix}$, que cambia $(x,y)\to(-y,x)$.

El cambio de variables en $2x^2+3y^2 \sim 2x^2+4xy+5y^2$ corresponde a la matriz $M=\begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}$, que cambia $(x,y)\to(x+y,y)$.

El punto de la relación de equivalencia es que las formas equivalentes que toman los mismos valores, tienen el mismo rango de funciones. Diremos que $f$ representa un número entero $n$ si $n$ es siempre positivo en el rango de $f$, es decir, si existen números enteros $x\ e\ y$ tales que $n=f(x,y)$. La multiplicación muestra que

$$4x(ax^2+bxy+cy^2)=(2ax+by)^2+(4ac-b^2)y^2$$

Si $D=b^2-4ac<0$, la expresión de la derecha que es siempre positiva, significa que la ecuación $ax^2+bxy+cy^2$ siempre tiene el mismo signo que la constante $a$. En otras palabras,

una forma con discriminante negativo representa sólo números positivos o sólo los números negativos. Hay, obviamente, una estrecha relación entre los casos, la gama de valores de $(a,b,c)$ que es siempre positiva, y la gama de valores de $(-a,-b,-c)$ que es siempre negativa. Por esta razón, se consideran las únicas formas que representan números enteros positivos.

Estas formas se denominan definidas positivas, y tienen $a>0$. Debido a que $(a,b,c)$ es siempre positivo y equivalente a $(c,-b,a)$ de acuerdo con $(x,y)\to(-y,x)$, esta última forma también representa sólo números enteros positivos, por lo que su primer coeficiente $c$ es siempre positivo.

Todo lo expuesto puede ser reflejado en forma de matriz como:

$$f(x,y)=[x,y]\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}$$

y su equivalencia $f\sim f'$ con la matriz $M$, es

$$\begin{aligned} f'(x,y) &= [x,y]M\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}^{tr} M\begin{bmatrix} x \\ y \end{bmatrix} \\ &= [x,y]M\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}^{tr} \left([x \quad y]M\right) \end{aligned}$$

donde ${}^{tr}M$ denota la transpuesta de la matriz.

Demostrar que las formas equivalentes tienen el mismo discriminante $D$.

Por un lado, destacamos que Gauss también demostró que las clases de equivalencia de las formas cuadráticas binarias de un discriminante fija también la formar de un grupo. La ley de la composición es un poco complicado de explicar aquí.

Demostrar que la formas $f(x,y)=2x^2+3y^2$ y $x^2+6y^2$ ambas tienen discriminante $(-24)$. Demostrar que $G(x,y)$ representa a 1, y que $f(x,y)$ no lo hace, por lo tanto $f$ no puede ser equivalente a $G$.

Qué números enteros $D$ pueden producirse como el discriminante de una forma cuadrática binaria? Al reducir $D\equiv b^2-4ac(mód.4)$, vemos y que $D\equiv 0,1(mód.4)$. Esta condición es necesaria y suficiente. Si $D\equiv 0(mód.4)$, entonces $x^2-D/4y^2$ es el discriminante $D$. Por otra parte, si $D\equiv 1(mód.4)$, entonces $x^2+xy+(1-D)/4y^2$ es el discriminante $D$.

Para cada $D<0$, el número $h$ de clase es finito. De hecho, cada forma es equivalente a una forma $(a,b,c)$ con $|b|\le a\le c$. La prueba del teorema consiste en demostrar que si la desigualdad no se cumple, podemos encontrar una forma equivalente que reduce la suma de los coeficientes. Este proceso se puede repetir un número finito de veces, porque sólo hay un número finito de números enteros positivos menores que $a+c$. Así que, $\operatorname{sgn}(b)=\pm 1$ será el signo de $b$; entonces, $\operatorname{sgn}(b)b=|b|$. Si $a<|b|$, la matriz $\begin{vmatrix} 1 & 0 \\ -\operatorname{sgn}(b) & 1 \end{vmatrix}$ cambia $(x,y)$ por $(x-\operatorname{sgn}(b)y,y)$.

La forma correspondiente es

$$\begin{aligned} a(x-\operatorname{sgn}(b)y)^2+b(x-\operatorname{sgn}(b)y)y+cy^2 = \\ ax^2+(b-2\operatorname{sgn}(b)a)xy+(a+c-|b|)y^2 \end{aligned}$$

donde tenemos que $a+(a+c-|b|)<a+c,$ ya que $a<|b|$.

Demostrar que en el caso de $c<|b|,$ la matriz $\begin{vmatrix}1 & -\text{sgn}(b)\\ 0 & 1\end{vmatrix}$. Del mismo modo se reduce la suma de los otros coeficientes.

Si al final $a$ y $c$ son $\geq|b|$, en la matriz $\begin{vmatrix}0 & 1\\ -1 & 0\end{vmatrix}$ es necesario el intercambio de $a$ y $c$. Esto demuestra la desigualdad indicada anteriormente.

A continuación, demostramos que sólo hay un número finito de estos triples con discriminante $D$. Las desigualdades de $a,$ $|b|$ y $c$ implica que

$$3a^2=4a^2-a^2\leq 4ac-b^2=-D=|b|$$

Esto significa que $a\leq\sqrt{|D|/3}$ y $b\leq a\leq\sqrt{|D|/3}.$ Además, como se observó anteriormente, $b^2-4ac=D$ implica que $b^2\equiv D(mód.4),$ por tanto $b\equiv D(mód.2)$. En otras palabras, $b$ es impar si y sólo si $D$ lo es. Hay un número finito de opciones de $(a,b,c),$ lo que se demuestra por la ecuación del discriminante: $c=(b^2-D)/(4a)$.

(*) *Ver artículo en PDF titulado EXERCISES ON BINARY QUADRATIC FORMS, que pueden consultar en http://www.math.ucsb.edu/~stopple/BQF.exercises.pdf*

### 4.4 Calcular el número de clases de $D=-35.$

El teorema no sólo demuestra que el número de clases es finito, sino que también da un límite superior. Aquí hay un ejemplo con $D=-35.$ Tenemos $\sqrt{|D|/3}=3,41565..,$ por lo que $|b|\leq 3$ y $1\leq a\leq 3.$ Además, $b$ debe ser impar como $D,$ de modo que, $b$ se limita a $-3,\pm 1$ *ó* $3.$ Con $b=\pm 1,$ $b^2-D=36.$ Sólo tenemos una forma cuando $c=(b^2-D)/(4a)$ es un número entero. La elección $a=1$ da lugar a las formas $(1,\pm 1,9).$ La elección $a=2$ da $c=36/8,$ que no es un número entero. La elección $a=3$ da lugar a las formas $(3,\pm 1,3).$ Mientras tanto, si $b=\pm 3,$ entonces $a\geq|b|$ debe ser 3, y como $c=44/12$ no es un número entero, el número de clase es menor o igual a 4. Observar que $D=b^2-4ac=1^2-4\cdot 1\cdot 9=1^2-4\cdot 3\cdot 3=-35.$

Llevar a cabo este mismo análisis discriminante para obtener una cota en el número de clases. De hecho, la prueba anterior es algo más. En realidad, da un algoritmo para encontrar un representante de una clase que satisface las desigualdades. Por ejemplo, la forma $(33,-47,17)$ tiene discriminante $D=-35.$ Pero $47>33,$ por lo que el teorema dice que se debe sustituir $(x,y)$ por $(x+y,y),$ lo que nos da $(33,19,3).$ Elegimos el signo "+" debido a que $b$ es negativo. Ahora, $19>3,$ por lo debemos hacer el cambio $(x,y)$ por $(x,y-x),$ lo que da $(17,13,3).$ Una vez más $13>3,$ así que el cambio produce $(7,7,3)$ y $(3,1,3),$ que se puede reducir sin más, porque la desigualdad $1\leq 3\leq 3$ se cumple. Tenga en cuenta que la suma de la primera entrada y la última disminuye en cada paso. $33+17>33+3>17+3>7+3>3+3.$

### 4.5 Calcular el número de clases de $D=-23.$

Si $D=-23$: $b^2-4ac=-23$ con $b$ impar, $|b|\leq|a|\leq\sqrt{23/3}$ con $b=\pm 1.$ Así que si $ac=6,$ $a<c,$ obtenemos:

1. $(1,1,6)$
2. $(1,-1,6)$ no se reduce ya que $b=a,\ b<0,$ es equivalente a $(1,1,6)$ a través de $(x,y)$ con $(x+y,y)$
3. $(2,1,3)$
4. $(2,-1,3)$ reducida desde $|b|\neq a,\ a\neq c.$

Por lo que el grupo de clases de $D=-23$ es $h(-23)=3:\ (1,1,6),(2,\pm 1,3).$

## 14.5 Solución de los Sistemas Cuadráticos Binarios.

### 5.1 Calcular reducidas y soluciones de $3x^2+5xy+4y^2=13.$

En primer lugar calculamos el discriminante: $D=b^2-4ac=5^2-4\cdot 3\cdot 4=-23.$
Para aislar $5xy,$ resolvemos la ecuación con módulo 5, esto es

$$3x^2+5xy+4y^2\equiv 13(mód.5)$$

que es equivalente $3x^2+4y^2\equiv 3(mód.5)$ y que tiene como soluciones

$$(x,y)=(1,0),(2,2),(2,3),(3,2),(3,3) \text{ y } (4,0).$$

Las soluciones compatibles con la ecuación planteada son $(x,y)=(\pm 3,\pm 2).$
Ahora calculamos las formas reducidas del discriminante donde $D=b^2-4ac<0, a>0, c>0.$

1. Recordemos que $ax^2+bxy+cy^2=m,\ mcd(x,y)=1.$
2. Resolvemos la ecuación $n^2\equiv D(mód.2m), 0\leq n\leq 2m.$
3. Para cada solución de $n,$ debemos calcular $s,$ donde $n^2-4ms=D.$
4. Reducimos $(m,n,s)$ a $(a,b,c).$

En cuanto al discriminante:

Si $D$ es negativo, $f(a,b,c)$ es una reducida si $|b|\leq a\leq c$ y $b\geq 0,$ o bien $a=|b|$ ó $a=c.$

Si $D$ es positivo, $f(a,b,c)$ es una reducida si $\left|\sqrt{D}-2|c|\right|<b<\sqrt{D}.$

Si $n^2\equiv D(mód.2m), 0\leq n\leq 2m\Rightarrow n^2\equiv -23(mód.2\cdot 13),\ 0\leq n\leq 2\cdot 13\rightarrow n=9,17.$

Para $n^2-4ms=D=9^2-4\cdot 13s=-23\rightarrow s=2.$ Donde $(m,n,s)=(13,9,2).$
Para $n^2-4ms=D=17^2-4\cdot 13s=-23\rightarrow s=6.$ Donde $(m,n,s)=(13,17,6).$

Cálculo de reducidas:

Para $(13,9,2)$ se reduce a $(2,-1,3).$
Para $(13,17,6)$ se reduce a $(6,-5,2)$ y a $(2,1,3).$
En cuanto a la propuesta: $(3,5,4)$ se reduce a $(4,3,2)$ y finalmente a $(2,1,3).$

Por tanto, los grupos de representación para el discriminante $D=-23,$ son $(1,1,6),(2,\pm1,3),$ que podemos comprobar, ya que $D=b^2-4ac=1^2-4\cdot1\cdot6=(-1)^2-4\cdot2\cdot3=-23.$
Comprobemos si estas representaciones tienen solución en la ecuación propuesta:

Para $2x^2\pm xy+3y^2=13$ tiene como soluciones $(x,y)=(\pm2,\pm1).$
Para $x^2\pm xy+6y^2=13$ no tiene soluciones.

## 5.2 Calcular reducidas y soluciones de $3x^2+5xy+6y^2=18.$

El Máximo Común Divisor de esta ecuación es $D=b^2-4ac=5^2-4\cdot3\cdot6=-47.$
Resolvemos mediante el módulo 5 y obtenemos:

$$3x^2+5xy+6y^2=3x^2+y^2\equiv3(mód.5)$$

que tiene como soluciones $(x,y)=(1,0),(2,1),(2,4),(3,1),(3,4)\ y\ (4,0).$
De todas estas soluciones, son compatibles con la ecuación presentada $(x,y)=(\pm3,\pm1).$
Probamos que es cierto:

$$f(x,y)=\frac{(2ax+by)^2-Dy^2}{4a}=m=\frac{(2\cdot3\cdot3+5(-1))^2+47(-1)^2}{4\cdot3}=18$$

Si $n^2\equiv-47(mód.2\cdot18),\ 0\le n\le2\cdot18\rightarrow n=5,13,23,31.$

Para $n^2-4ms=D=5^2-4\cdot18s=-47\rightarrow s=1.$ Donde $(m,n,s)=(18,5,1).$
Para $n^2-4ms=D=13^2-4\cdot18s=-47\rightarrow s=3.$ Donde $(m,n,s)=(18,13,3).$
Para $n^2-4ms=D=23^2-4\cdot18s=-47\rightarrow s=8.$ Donde $(m,n,s)=(18,23,8).$
Para $n^2-4ms=D=31^2-4\cdot18s=-47\rightarrow s=14.$ Donde $(m,n,s)=(18,31,14).$

El proceso de reducción sigue las siguientes secuencias:

$(18,5,1)\rightarrow(1,1,12),\ \ (18,13,3)\rightarrow(3,-1,4),\ \ (18,23,8)\rightarrow(8,-7,3)\rightarrow(3,1,4),$
$(18,31,14)\rightarrow(14,-3,1)\rightarrow(1,1,12),\ \ (3,5,6)\rightarrow(6,-5,3)\rightarrow(3,-1,4)$

Para el discriminante $-47$ las representaciones son $(1,1,12),(2,\pm1,6),(3,\pm1,4)$ como podemos comprobar por las tablas.
Comprobamos también la representación de los coeficientes:

$$a=\frac{m-(bx+cy)y}{x^2}=\frac{18-(5\cdot3+6(-1))(-1)}{3^2}=3$$

$$b=\frac{m-ax^2-cy^2}{xy}=\frac{18-3(3)^2-6(-1)^2}{3(-1)}=5$$

$$c=\frac{m-x(ax+by)}{y^2}=\frac{18-3(3\cdot3+5(-1))}{(-1)^2}=6$$

### 5.3 Calcular reducidas y soluciones de $x^2+3xy+4y^2=14$.

El discriminante de esta ecuación es $D=3^2-4\cdot1\cdot4=-7$, y según las tablas la representación $(1,3,4)$ no es primitiva, ya que es equivalente a $(1,1,2)$, que como podemos comprobar, también tiene como discriminante $D=1^2-4\cdot1\cdot2=-7$.
Resolvemos mediante el módulo 3 y obtenemos:

$$x^2+3xy+4y^2=x^2+y^2\equiv 2(mód.3)$$

que tiene como soluciones $(x,y)=(1,1),(1,2),(2,1),(2,2)$.
Hay dos soluciones que se repiten en forma simétrica, $(1,2)$ y $(2,1)$, y que pueden ser soluciones de la ecuación planteada en $(\pm1,\pm2),(\pm2,\pm1)$. Comprobamos:

$$f(x,y)=\frac{(2ax+by)^2-Dy^2}{4a}=m=\frac{(2\cdot1\cdot2+3\cdot1)^2+7(-1)^2}{4\cdot1}=14$$

$$x=\frac{-by\pm\sqrt{y^2(b^2-4ac)+4am}}{2a}=\frac{3(-1)+\sqrt{(-1)^2(-7)+4\cdot1\cdot14}}{4\cdot1}=1$$

$$y=\frac{-bx\pm\sqrt{x^2(b^2-4ac)+4cm}}{2c}=\frac{3\cdot2-\sqrt{2^2(-7)+4\cdot4\cdot14}}{4\cdot1}=-1$$

que admite las soluciones. De hecho, esta ecuación admite como soluciones enteras

$$(x,y)=(\pm2,\pm1),(\pm5,\pm1)$$

y como soluciones reales

$$x=-4\sqrt{2},\ y=\frac{3}{\sqrt{2}}$$

Dejamos en manos del lector la solución de las reducidas.

### 5.4 Calcular reducidas y soluciones de $9x^2+7xy+11y^2=199$.

Aplicando módulo 7, la ecuación $9x^2+7xy+11y^2\equiv199(mód.7)$ es equivalente con

$$2x^2+4y^2\equiv3(mód.7)$$

que tienen como soluciones $(x,y)=(1,3),(1,4),(2,2),(2,5),(5,2),(5,5),(6,3),(6,4)$.
Las soluciones de la ecuación planteada son $(x,y)=(\pm5,\pm2)$, como podrán comprobar.
Comprobamos con el siguiente método: (*)
La ecuación tiene solución, ya que $mcd(9,7,11)=1$ y $1|199$.
Resolvemos aplicando módulos de 9,16 y 25:

$$9x^2+7xy+11y^2\equiv199(mód.9,16,25)$$

y en todos los casos hay soluciones, por lo tanto proseguimos.
Debemos convertir la ecuación en una de la forma $x'^2 + By^2 + Cy + D = 0,$ por lo que la multiplicamos por 36:

$$36(9x^2 + 7xy + 11y^2 - 199) = 324x^2 + 252xy + 396y^2 - 7164$$

que escribimos como $324x^2 + (252y)x + (396y^2 - 7164) = 0.$
Sumamos y restamos $(7y)^2$ para complementar el cuadrado y obtenemos:

$$(18x + 7y)^2 + (396y^2 - 7164) - (49y^2) = (18x + 7y)^2 + (347y^2 - 7164)$$

Ahora realizamos la sustitución para $x' = 18x + 7y$ y obtenemos $x'^2 + 347y^2 - 7164 = 0.$
Como $x'^2$ es siempre $\geq 0,$ $347y^2 - 7164$ debe ser menor o igual a cero.
Para $347y^2 - 7164 = 0$ tiene como solución $y = \pm 6\sqrt{\frac{199}{347}} = \begin{cases} -4,543736... \\ +4,543736... \end{cases}$ que deberemos reemplazar en $347y^2 - 7164,$ con valores desde $-4$ hasta $+4$. El resultado debe ser el negativo de un cuadrado perfecto. Para $y = \pm 2,$ tenemos:

$$x' = 18x + 7y = \pm\sqrt{5776} = \pm 76$$

que obtenemos como soluciones $(x, y) = (\pm 5, \pm 2).$

La ecuación planteada tiene como discriminante $-347$ y la representación $(a, b, c) = (9, 7, 11)$ es primitiva. De hecho para este discriminante, las representaciones son:

$$(a, b, c) = (1, 1, 87), (3, \pm 1, \pm 29) \; y \; (9, \pm 7, \pm 11)$$

Estas representaciones han sido calculadas a partir de los valores de

$$(m, n, s) = (199, 161, 33) \; y \; (199, 237, 71)$$

Dejamos en sus manos la comprobación de estos cálculos.

(*) Hemos aplicado el Programa de Alpertron, desarrollado por el profesor argentino Diario Alejandro Alpern, que pueden consultar en http://www.alpertron.com.ar/NUMBERT.HTM

## 5.5 Calcular reducidas y soluciones de $5x^2 - 6xy + 8y^2 = 41.$

La ecuación $5x^2 - 6xy + 8y^2 \equiv 41 (mód. 6)$ genera como soluciones

$$(x, y) = (1, 0), (1, 3), (3, 1), (3, 2), (3, 4), (3, 5)(5, 0), (5, 3)$$

de las que $(x, y) = (\pm 3, \pm 2),$ corresponden a la ecuación planteada.

El discriminante resulta ser $D = 6^2 - 4 \cdot 5 \cdot 8 = -124,$ que tiene como representaciones $(a, b, c) = (1, 0, 31), (5, \pm 4, 7),$ lo que demuestra que $(5, -6, 8)$ no es una representación primitiva. Estas representaciones se han conseguido a partir de $(m, n, s) = (41, 32, 7), (41, 50, 16),$ cómo podrán comprobar si aplican alguno de los métodos descritos anteriormente.

**5.6 Calcular reducidas y soluciones de** $x^2+13xy+7y^2=61.$

Este supuesto, con discriminante $141$ y una representación de la forma cuadrática binaria de $(a,b,c)=(1,11-5),$ que hemos conseguido aplicando la secuencia

$$(1,13,7)\to(7,1,-5)\to(-5,9,3)\to(1,11,-5)$$

admite una primera solución de $(x,y)=(\pm4,\pm1),$ pero se trata de un sistema indeterminado, con múltiples soluciones, entre otras:

$$(x,y)=(\pm11,\pm20),(\pm249,\pm20),(\pm439,\pm780),(\pm9701,\pm780),...$$

Utilicen el programa en línea http://www.wolframalpha.com/examples/ para comprobar estos resultados y buscar otros.

**5.7 Calcular reducidas y soluciones de** $x^2-3xy+6y^2+2x=17.$

Esta ecuación, que podemos escribirla como $x^2+x(2-3y)+6y^2-17=0,$ tiene como solución

$$(x,y)=(-1,-2),(-7,-2)$$

Los discriminantes, respecto a esta forma cuadrática, son:

Respecto a $x:-15y^2-12y+72,$ respecto a $y:-3(5x^2+16x-136)$

## 14.6 Formas Cuadráticas Binarias Especiales.

**6.1 Resolver la forma cuadrática** $x^2+xy+2x=43.$

Como $x^2+xy+2y^2-43=\left(x+\frac{y}{2}\right)^2+\frac{7y^2-172}{4}=0,$ encontramos como soluciones reales $x=\pm2\sqrt{\frac{86}{7}},\ y=\pm\sqrt{\frac{43}{14}}$

y como soluciones enteras $(x,y)=(\pm5,\pm2),(\pm7,\pm2).$

**6.2 Resolver la forma cuadrática** $x^2+xy+3y^2=37.$

Esta ecuación tiene como soluciones reales $x=\pm2\sqrt{\frac{111}{11}},\ y=\pm\sqrt{\frac{37}{33}}$ y como soluciones enteras $(x,y)=(\pm2,\pm3),(\pm5,\pm3).$

**6.3 Resolver la forma cuadrática** $x^2+xy+4y^2=19.$

Como $x^2+xy+4y^2-19=\left(x+\frac{y}{2}\right)^2+\frac{15y^2-76}{4}=0,$ encontramos como soluciones reales

$$x = \pm 4\sqrt{\frac{19}{15}},\ y = \pm\frac{\sqrt{\frac{19}{15}}}{2}$$

y como soluciones enteras $(x, y) = (\pm 3, \pm 2), (\pm 1, \pm 2).$

**6.4 Resolver la forma cuadrática** $x^2 + xy + 5y^2 = 47.$

Esta ecuación tiene como soluciones reales $x = \pm 2\sqrt{\frac{235}{19}},\ y = \pm\sqrt{\frac{47}{95}}$ y como soluciones enteras $(x, y) = (\pm 6, \pm 1), (\pm 7, \pm 1).$

**6.5 Resolver la forma cuadrática** $x^2 + xy + 6y^2 = 59.$

Como $x^2 + xy + 6y^2 - 59 = \left(x + \frac{y}{2}\right)^2 + \frac{23y^2 - 236}{4} = 0,$ encontramos como soluciones reales

$$x = \pm 2\sqrt{\frac{354}{23}},\ y = \pm\sqrt{\frac{59}{138}}$$

y como soluciones enteras $(x, y) = (\pm 5, \pm 2), (\pm 7, \pm 2).$

**6.6 Resolver la forma cuadrática** $x^2 + xy + 7y^2 = 97.$

Como $x^2 + xy + 7y^2 - 97 = \left(x + \frac{y}{2}\right)^2 + \frac{27y^2 - 388}{4} = 0,$ encontramos como soluciones reales

$$x = \pm\frac{2\sqrt{\frac{679}{3}}}{3},\ y = \pm\frac{\sqrt{\frac{97}{21}}}{3}$$

y como soluciones enteras $(x, y) = (\pm 9, \pm 1), (\pm 10, \pm 1).$

**6.7 Resolver la forma cuadrática** $2x^2 - 15xy + 27y^2 = 0.$

La factorización de esta ecuación es la siguiente:

$$\begin{aligned} 2x^2 - 15xy + 27y^2 &= 2x^2 + y(27y - 15x) \\ &= x(2x - 15y) + 2y^2 = (2x - 9y)(x - 3y) \end{aligned}$$

que también podemos expresar como

$$2x^2-15xy+27y^2=2\left(x-\frac{15x}{4}\right)^2-\frac{9y^2}{8}$$
$$=\frac{(4x-15y)-9y^2}{8}$$

donde $D=9y^2$.
Esta ecuación tiene como solución $x=9t,\ y=2t,\ con\ t\in\mathbb{Z}$.

Los supuestos planteados en este apartado son formas cuadráticas binarias especiales, la prueba son las soluciones, ya que con estructuras distintas, dan resultados parecidos. Lo que les propongo es que estudien todos y cada uno de los números primos que aparecen como coeficiente independiente e intenten encontrar la forma que les une. El supuesto resuelto en 4.2 les podrá servir de ayuda.

*Número de clases para* $D \equiv 0,1(mód.4)$

| $-D$ | $h$ | $< a,b,c >$ | $-D$ | $h$ | $< a,b,c >$ |
|---|---|---|---|---|---|
| 3 | 1 | $(1,1,1)$ | 63 | 4 | $(1,1,16),(2,\pm1,8),(4,1,4)$ |
| 4 | 1 | $(1,0,1)$ | 64 | 2 | $(1,0,16),(4,4,5)$ |
| 7 | 1 | $(1,1,2)$ | 67 | 1 | $(1,1,17)$ |
| 8 | 1 | $(1,0,2)$ | 68 | 4 | $(1,0,17),(2,2,9),(3,\pm2,6)$ |
| 11 | 1 | $(1,1,3)$ | 71 | 7 | $(1,1,18),(2,\pm1,9),(3,\pm1,6),$ $(4,\pm3,5)$ |
| 12 | 1 | $(1,0,3)$ | 72 | 2 | $(1,0,18),(2,0,9)$ |
| 15 | 2 | $(1,1,4),(2,1,2)$ | 75 | 2 | $(1,1,19),(3,3,7)$ |
| 16 | 1 | $(1,0,4)$ | 76 | 3 | $(1,0,19),(4,\pm2,5)$ |
| 19 | 1 | $(1,1,5)$ | 79 | 5 | $(1,1,20),(2,\pm1,10),(4,\pm1,5)$ |
| 20 | 2 | $(1,0,5),(2,2,3)$ | 80 | 4 | $(1,0,20),(4,0,5),(3,\pm2,7)$ |
| 23 | 3 | $(1,1,6),(2,\pm1,3)$ | 83 | 3 | $(1,1,21),(3,\pm1,7)$ |
| 24 | 2 | $(1,0,6),(2,0,3)$ | 84 | 4 | $(1,0,21),(3,0,7),(2,2,11),$ $(5,4,5)$ |
| 27 | 1 | $(1,1,7)$ | 87 | 6 | $(1,1,22),(2,\pm1,11),(3,3,8),$ $(4,\pm3,6)$ |
| 28 | 1 | $(1,0,7)$ | 88 | 2 | $(1,0,22),(2,0,11)$ |
| 31 | 3 | $(1,1,8),(2,\pm1,4)$ | 91 | 2 | $(1,1,23),(5,3,5)$ |
| 32 | 2 | $(1,0,8),(3,2,3)$ | 92 | 3 | $(1,0,23),(3,\pm2,8)$ |
| 35 | 2 | $(1,1,9),(3,1,3)$ | 95 | 8 | $(1,1,24),(2,\pm1,12),(3,\pm1,8),$ $(4,\pm1,6),(5,5,6)$ |
| 36 | 2 | $(1,0,9),(2,2,5)$ | 96 | 4 | $(1,0,24),(3,0,8),(5,2,5),$ $(4,4,7)$ |
| 39 | 4 | $(1,1,10),(2,\pm1,5),(3,3,4)$ | 99 | 2 | $(1,1,25),(5,1,5)$ |
| 40 | 2 | $(1,0,10),(2,0,5)$ | 100 | 2 | $(1,0,25),(2,2,13)$ |
| 43 | 1 | $(1,1,11)$ | 103 | 5 | $(1,1,26),(2,\pm1,13),(4,\pm3,7)$ |
| 44 | 3 | $(1,0,11),(3,\pm2,4)$ | 104 | 6 | $(1,0,26),(2,0,13),(3,\pm2,9),$ $(5,\pm4,6)$ |
| 47 | 5 | $(1,1,12),(2,\pm1,6),(3,\pm1,4)$ | 107 | 3 | $(1,1,27),(3,\pm1,9)$ |
| 48 | 2 | $(1,0,12),(3,0,4)$ | 108 | 3 | $(1,0,27),(4,\pm2,7)$ |
| 51 | 2 | $(1,1,13),(3,3,5)$ | 111 | 8 | $(1,1,28),(2,\pm1,14),(4,\pm1,7),$ $(3,3,10),(5,\pm3,6)$ |
| 52 | 2 | $(1,0,13),(2,2,7)$ | 112 | 2 | $(1,0,28),(4,0,7)$ |
| 55 | 4 | $(1,1,14),(2,\pm1,7),(4,3,4)$ | 115 | 2 | $(1,1,29),(5,5,7)$ |
| 56 | 4 | $(1,0,14),(2,0,7),(3,\pm2,5)$ | 116 | 6 | $(1,0,29),(2,2,15),(3,\pm2,10),$ $(5,\pm2,6)$ |
| 59 | 3 | $(1,1,15),(3,\pm1,5)$ | 119 | 10 | $(1,0,30),(2,\pm1,15),(3,\pm1,10),$ $(5,\pm1,6),(4,\pm3,8),(6,5,6)$ |
| 60 | 2 | $(1,0,15),(3,0,5)$ | 120 | 4 | $(1,0,30),(2,0,15),(3,0,10),$ $(5,0,6)$ |

*Número de clases para D libre de cuadrados*

| $D$ | $h$ | $< a,b,c >$ | $D$ | $h$ | $< a,b,c >$ |
|---|---|---|---|---|---|
| 2 | 1 | (1,2,-1) | 66 | 2 | (1,16,-2),(3,12,-10) |
| 3 | 1 | (1,2,-2) | 67 | 1 | (1,16,-3) |
| 5 | 1 | 1,1,-1) | 69 | 1 | (1,7,-5) |
| 6 | 1 | (1,4,-2) | 70 | 2 | (1,16,-6),(2,16,-3) |
| 7 | 1 | (1,4,-3) | 71 | 1 | (1,16,-7) |
| 10 | 2 | (1,6,-1),(2,4,-3) | 73 | 1 | (1,7,-6) |
| 11 | 1 | (1,6,-2) | 74 | 2 | (1,16,-10),(2,16,-5) |
| 13 | 1 | (1,3,-1) | 77 | 1 | (1,7,-7) |
| 14 | 1 | (1,6,-5) | 78 | 2 | (1,16,-14),(2,16,-7) |
| 15 | 2 | (1,6,-6),(2,6,-3) | 79 | 3 | (1,16,-15),(3,14,-10),(3,16,-5) |
| 17 | 1 | (1,3,-2) | 82 | 4 | (1,18,-1),(2,16,-9),(3,14,-11), (3,16,-6) |
| 19 | 1 | (1,8,-3) | 83 | 1 | (1,18,-2) |
| 21 | 1 | (1,3,-3) | 85 | 2 | (1,9,-1),(3,5,-5) |
| 22 | 1 | (1,8,-6) | 86 | 1 | (1,18,-5) |
| 23 | 1 | (1,8,-7) | 87 | 2 | (1,18,-6),(2,18,-3) |
| 26 | 2 | (1,10,-1),(2,8,-5) | 89 | 1 | (1,9,-2) |
| 29 | 1 | (1,5,-1) | 91 | 2 | (1,18,-10),(2,18,-5) |
| 30 | 2 | (1,10,-5),(2,8-7) | 93 | 1 | (1,9,-3) |
| 31 | 1 | (1,10,-6) | 94 | 1 | (1,18,-13) |
| 33 | 1 | (1,5,-2) | 95 | 2 | (1,18,-14),(2,18,-7) |
| 34 | 2 | (1,10,-9),(3,8,-6) | 97 | 1 | (1,9,-4) |
| 35 | 2 | (1,10,-10),(2,10,-5) | 101 | 1 | (1,9,-5) |
| 37 | 1 | (1,5,-3) | 102 | 2 | (1,20,-2),(3,18,-7) |
| 38 | 1 | (1,12,-2) | 103 | 1 | (1,20,-3) |
| 39 | 2 | (1,12,-3),(2,10-7) | 105 | 2 | (1,9,-6),(2,7,-7) |
| 41 | 1 | (1,5,-4) | 106 | 2 | (1,20,-6),(2,20,-3) |
| 42 | 2 | (1,12,-6),(2,12,-3) | 107 | 1 | (1,20,-7) |
| 43 | 1 | (1,12,-7) | 109 | 1 | (1,9,-7) |
| 46 | 1 | (1,12,-10) | 110 | 2 | (1,20,-10),(2,20,-5) |
| 47 | 1 | (1,12,-11) | 111 | 2 | (1,20,-11),(2,18,-15) |
| 51 | 2 | (1,14,-2),(3,12,-5) | 113 | 1 | (1,9,-8) |
| 53 | 1 | (1,7,-1) | 114 | 2 | (1,20,-14),(3,18,-11) |
| 55 | 2 | (1,14,-6),(2,14,-3) | 115 | 2 | (1,20,-15),(2,18,-17) |
| 57 | 1 | (1,7,-2) | 118 | 1 | (1,20,-18) |
| 58 | 2 | (1,14,-9),(2,12,-11) | 119 | 2 | (1,20,-19),(5,14,-14) |
| 59 | 1 | (1,14,-10) | 122 | 2 | (1,22,-1),(2,20,-11) |
| 61 | 1 | (1,7,-3) | 123 | 2 | (1,22,-2),(3,18,-14) |
| 62 | 1 | (1,14,-13) | 127 | 1 | (1,22,-6) |
| 65 | 2 | (1,7-4),(2,5,-5) | 129 | 1 | (1,11,-2) |

BIBLIOGRAFÍA

ALACA and KENNETH, Introductory Algebraic Number Theory, ISBN: 0-521-54011-9
BUCHMANN and VOLLMER, Binary Quadratic Forms an Algorithmic Approach, ISBN: 978-3-540-46367-2
CLAPHAM, Christopher, Dictionary of Mathematics Originally, ISBN: 84-89784-56-6
COHN, Harvey, Advanced Number Theory, ISBN: 0-486-64023-X
DICKSON, Leonard, Algebraic Theories, ISBN: 0-486-49573-6
DICKSON, Leonard, Algebraic Theories, ISBN: 0-489-49573-6
IVORRA CASTILLO, Carlos, Matemáticas, Apuntes en PDF, libres de descarga en Internet
IVORRA CASTILLO, Carlos, Teoría de Números, Apuntes en PDF, libres de descarga en Internet
SHIDLOVSKI,A.B., Aproximaciones Diofánticas y Números Transcendentes, ISBN: 84-7585-156-8
STOPPLE, Jeffrey, A Primer of Analytic Number Theory, ISBN: 0-521-01253-8

AYUDA INTERNET

http://es.wikipedia.org/wiki/Ra%C3%ADz_de_la_unidad
http://math.fau.edu/richman/pell-m.htm (Programa que calcula la ecuación Pell)
http://mathworld.wolfram.com/ (Todo el saber sobre Matemáticas (en inglés))
http://mathworld.wolfram.com/BinaryQuadraticForm.html
http://mathworld.wolfram.com/BinaryQuadraticFormDeterminant.html
http://mathworld.wolfram.com/ClassNumber.html
http://mathworld.wolfram.com/FundamentalUnit.html
http://mathworld.wolfram.com/PellEquation.html
http://mathworld.wolfram.com/QuadraticField.html
http://mathworld.wolfram.com/ReducedBinaryQuadraticForm.html
http://maxima.programas-gratis.net/ (Programa de Matemáticas gratis, que puedes descargar e instalar)
http://www.alpertron.com.ar/NUMBERT.HTM (Calculadoras en línea)
http://www.math.ucsb.edu/~stopple/BQF.exercises.pdf
http://www.maths.surrey.ac.uk/hosted-sites/R.Knott/Fibonacci/cfCALC.html# (Fracciones continuas)
http://www.numbertheory.org/php/php.html#quadratic_residues (Programa teoría de números)
http://www.wolframalpha.com/examples/ (Programa de matemáticas en línea. Realiza todo tipo de operaciones)