Boletín de Matemáticas
Vol. XIV , Nos. 1,2,3, (1980) pags, 1 - 14

TABLA DE SOLUCIONES MINIMAS DE LA ECUACION DE FERMAT (O ECUACION DE PELL)

Eduardo CARO .

INTRODUCCION

Las soluciones de las ecuaciones diofánticas de segundo grado , o sea aquellas cuya forma más general es : $Au^2+2Buv+Cv^2+2Du+2Ev+F = 0$ (con A,B,C,..., números enteros , y donde se supone que los valores de las soluciones deben ser números naturales) pueden hacerse depender siempre de las de la ecuación , de tipo más simple ,

(1) $z^2 \pm Nw^2 = \pm a$ donde tanto N como a , lo mismo que z y w deben ser números naturales .

Es indudable que el caso de $z^2 + Nw^2 = - a$ no puede tener soluciones , mientras que el de $z^2+Nw^2=+a$ tiene , si acaso , un número limitado de ellas que generalmente se encuentran por tanteo . De manera que únicamente son de interés aquellas de la forma $z^2 - Nw^2= \pm a$ que , o carecen de solución , o tienen un número infinito de ellas ; y en este último caso si por cualquier razón se conoce una de ellas , las demás se pueden hacer depender de las de la ecuación aún más simple

$$x^2 - Ny^2 = 1 .$$

Esta última es mal conocida en la literatura matemática como la ecuación de Pell cuando en justicia debería llevar , como lo hago en el presente trabajo , el nombre de FERMAT .

Trataremos entonces , en primer lugar , de la ecuación de Fermat y sus soluciones y luego de las de la ecuación $z^2 - Nw^2 = \pm a$ basándonos en los resultados anteriores y en el supuesto de que conocemos una de sus soluciones .

LA ECUACION DE FERMAT .

La solución clásica y definitiva de la ecuación de Fermat se logra por medio del desarrollo de $\sqrt{N}$ en fracción continua que , como se sabe (1)(2) siempre será periódica y con un periodo que comienza en el segundo denominador parcial y termina en un denominador parcial igual al doble del primero (que es la parte en tera de $\sqrt{N}$) ; y en la que , además , los denominadores parciales equidistantes de los extremos , son iguales . O sea , $\sqrt{N}$ puede expresarse siempre como una fracción continua de la forma :

$$\sqrt{N} = a + \frac{1}{b_1+}\ \frac{1}{b_2+}\ \frac{1}{b_3+}\ \cdots\ \frac{1}{b_3+}\ \frac{1}{b_2+}\ \frac{1}{b_1+}\ \frac{1}{2a+}\ \cdots$$

cuyas reductas (1),(2),(7) sucesivas corresponden a soluciones para algunos valores de a en $z^2-Nw^2 = \pm a$. Las correspondientes al penúltimo cociente parcial de cada período nos dan soluciones consecutivas de la ecuación de Fermat , si el número de denominadores parciales del período es par ; y soluciones alternadas de $x^2 - Ny^2 = -1$ y de la ecuación de Fermat , si este número es impar.

Por ejemplo , de (5,6)

$$\sqrt{19} = 4 + \frac{1}{2+}\ \frac{1}{1+}\ \frac{1}{3+}\ \frac{1}{1+}\ \frac{1}{2+}\ \frac{1}{8+}\ \cdots$$

cuyo período tiene un número par de denominadores parciales y cuyas reductas son

$$\frac{4}{1}, \frac{9}{2}, \frac{13}{3}, \frac{48}{11}, \frac{61}{14}, \frac{170}{39} \text{ etc.}$$

deducimos :

$$4^2-19\times1^2 = -3 \qquad 48^2-19\times11^2 = 5$$

$$9^2-19\times2^2 = 5 \qquad 61^2-19\times14^2 = -3$$

$$13^2-19\times3^2 = -2 \quad \text{y} \quad 170^2-19\times39^2 = 1$$

De manera similar , de

$$\sqrt{13} = 3 + \frac{1}{\underset{\sim}{1} +}\ \frac{1}{1 +}\ \frac{1}{1 +}\ \frac{1}{1 +}\ \frac{1}{\underset{\sim}{6} +}\ \cdots$$

con un número impar de denominadores parciales en el período , deducimos $18^2-13\times5^2 = -1$ de la reducta final del primer período y $649^2-13\times180^2 = 1$ de la del segundo período .

Una vez encontrada una solución , pueden hallarse tantas como se quiera por diversos procedimientos . Entre ellos escojo el siguiente que ya he utilizado con éxito en otros contextos . [5,6]

Sean p y q los valores de una solución de $x^2 - Ny^2 = 1$, es decir que $p^2 - Nq^2 = 1$. Factorizando el primer miembro tendremos $(p+q\sqrt{N})(p-q\sqrt{N}) = 1$ expresión que , elevada a cualquier potencia , nos dará un producto de la misma forma

$$(p+q\sqrt{N})^t (p-q\sqrt{N})^t = (P+Q\sqrt{N})(P-Q\sqrt{N}) = 1$$

del cual , a su vez , obtenemos $P^2-NQ^2 = 1$, otra solución .

Si partiendo de la menor de las soluciones, la elevamos sucesivamente al cuadrado, al cubo, etc., obtendremos entonces, en forma ordenada, las diferentes soluciones de la ecuación de Fermat como se puede ver con las soluciones de $x^2 - 3y^2 = 1$ en el siguiente ejemplo.

Es obvio que $2^2 - 3x1^2 = 1$ de donde

$$(2+\sqrt{3})(2-\sqrt{3}) = 1$$

cuya potencia n es

$$(p_n+q_n\sqrt{3})(p_n-q_n\sqrt{3}) = 1,$$

y cuyo producto es

$$[(2p_n+3q_n) + (p_n+2q_n)\sqrt{3}]\,[(2p_n+3q_n) - (p_n+2q_n)\sqrt{3}] = 1.$$

De donde deducimos las relaciones

$$p_{n+1} = 2p_n + 3q_n \quad y \quad q_{n+1} = p_n + 2q_n.$$

que nos permiten calcular fácilmente tantas soluciones como queramos. Como se ve en la tabla siguiente, en la que a $p_1 = 2$, $q_1 = 1$ de la solución mínima, hemos agregado $p_o = 1$, $q_o = 0$ de la solución trivial

$$1^2 - 3.0^2 = 1.$$

n	p_n	q_n	$p_n^2 - q_n^2 N = 1$
0	1	0	$1^2 - 3x0^2 = 1$
1	2	1	$2^2 - 3x1^2 = 1$
2	$7=2x2+3x1$	$4=2+2x1$	$7^2 - 3x4^2 = 1$
3	26	15	$26^2 - 3x15^2 = 1$
4	97	56	$97^2 - 3x56^2 = 1$
etc.	etc.	etc.	etc.

Observando los valores de p y de q vemos que , independientemente uno del otro , forman dos sucesiones recurrentes , con la misma ley de formación .

De $p_{n+1} = 2p_n + 3q_n$ y $q_n = p_{n-1} + 2q_{n-1}$

obtenemos

$$p_{n+1} = 2p_n + 3(p_{n-1} + 2q_{n-1}) = 2p_n + 3p_{n-1} + 6q_{n-1}$$

$$= 2p_n + 3p_{n-1} + 6q_{n-1} + p_{n-1} - p_{n-1}$$

$$= 2p_n + 4p_{n-1} + 6q_{n-1} - p_{n-1}$$

$$= 2p_n + 2(2p_{n-1} + 3q_{n-1}) - p_{n-1}$$

$$= 2p_n + 2p_n - p_{n-1} = 4p_n - p_{n-1}$$

En forma parecida , de

$$q_{n+1} = p_n + 2q_n \quad \text{y} \quad p_n = 2p_{n-1} + 3q_{n-1}$$

obtenemos

$$q_{n+1} = 2p_{n-1} + 3q_{n-1} + q_{n-1} - q_{n-1} + 2q_n$$

$$= 2(p_{n-1} + 2q_{n-1}) + 2q_n - q_{n-1} = 4q_n - q_{n-1}$$

Estas fórmulas nos permiten calcular aún más fácil y rápidamente que las anteriores , las soluciones sucesivas de $x^2 - 3y^2 = 1$.

De la misma manera puede demostrarse que los valores sucesivos de p_n y q_n , soluciones de $x^2-Ny^2=1$ forman sendas sucesiones recurrentes de la forma :

$$p_{n+1} = (2p_1)\ p_n - p_{n-1}$$

$$q_{n+1} = (2p_1)\ q_n - q_{n-1}$$

que se inician con los valores $p_o = 1$, $q_o = 0$ de la solución trivial $(1^2 - Nx0^2 = 1)$ y con p_1 , q_1 los correspondientes a la solución mínima .

Cuando se está calculando una tabla como la presente , de soluciones mínimas de la ecuación de Fermat, para muchos valores de N y aún , a veces , para valores aislados , puede que no sea siempre conveniente emplear el método de las fracciones continuas , el cual aunque seguro , no es necesariamente el más fácil ni el más rápido .

De $p_1^2 - Nq_1^2 = 1$ ó $Nq_1^2 + 1 = p_1^2$

obtenemos $(p_1 + q_1\sqrt{N})(p_1 - q_1\sqrt{N}) = 1$

x $\underline{(p_n + q_n\sqrt{N})(p_n - q_n\sqrt{N}) = 1}$

$$[(p_n p_1 + Nq_n q_1) + (p_n q_1 + q_n p_1)\sqrt{N}][(A) - (B)\sqrt{N}] = 1$$

donde $A = p_n p_1 - Nq_n q_1$ y $B = p_n q_1 + q_n p_1$.

De esta manera se tiene :

$$p_{n+1} = p_1 p_n + Nq_1 q_n \quad y \quad q_{n+1} = q_1 p_n + p_1 q_n \; .$$

Ahora bien ,

$$\begin{aligned}
\underline{\underline{p_{n+1}}} &= p_1 p_n + Nq_1^2 p_{n-1} + Nq_1 p_1 q_{n-1} + p_{n-1} - p_{n-1} \\
&= p_1 p_n + (Nq_1^2 + 1)\, p_{n-1} + Nq_1 p_1 q_{n-1} - p_{n-1} \\
&= p_1 p_n + p_1^2\, p_{n-1} + Nq_1 p_1 q_{n-1} - p_{n-1} \\
&= p_1 p_n + p_1\,(p_1 p_{n-1} + Nq_1 q_{n-1}) - p_{n-1} = \underline{\underline{2p_1 p_n - p_{n-1}}}
\end{aligned}$$

$$\begin{aligned}
\underline{\underline{q_{n+1}}} &= q_1 p_1 p_{n-1} + Nq_1^2\, q_{n-1} + p_1 q_n + q_{n-1} - q_{n-1} \\
&= q_1 p_1 p_{n-1} + (Nq_1^2 + 1)\, q_{n-1} + p_1 q_n - q_{n-1} \\
&= q_1 p_1 p_{n-1} + p_1^2 q_{n-1} + p_1 q_n - q_{n-1} \\
&= p_1\,(q_1 p_{n-1} + p_1 q_{n-1}) + p_1 q_n - q_{n-1} = 2p_1 q_n - q_{n-1}
\end{aligned}$$

Por ejemplo , si N admite un factor cuadrado perfecto $(N = Ma^2)$, a veces se puede hacer que la solución de la ecuación en N dependa de la ecuación en M . Este es el caso de $N = 5x2^2$ en donde , a partir de $q^2 - 5x4^2 = 1$, hallamos $q^2-(5x2^2)(4/2)^2=q^2-20x2^2=1$, y el caso de $N = 12 = 3x2^2$ en donde , con algo más de trabajo , encontramos :

$$2^2 - 3x1^2 = 1$$

multiplicando por 2^2

$$2^2x2^2 - 3x2^2x1^2 = 2^2$$

$$4^2 - 12x1^2 = 4$$

factorizando

$$(4 - \sqrt{12})(4 + \sqrt{12}) = 4$$

elevando al cuadrado

$$(16+12+8\sqrt{12})(16+12-8\sqrt{12}) = 4^2$$

$$28^2 - 12x8^2 = 4^2$$

y , dividiendo por 4^2

$$7^2 - 12x2^2 = 1 .$$

Puede deducirse una fórmula más importante para el caso en que $N = n^2 + a$ $(a \in \mathbb{Z})$ donde a divide a $2n$. En este caso $ka = 2n$ y $n = \frac{ka}{2}$.

Partimos de la identidad :

$$n^2 - N \times 1^2 = n^2 - (n^2+a) = -a$$

Factorizando ,

$$(n+\sqrt{N})(n-\sqrt{N}) = -a$$

elevando al cuadrado ,

$$[(n^2+N) + 2n\sqrt{N}][(n^2+N) - 2n\sqrt{N}] = a^2 .$$

Pero cada uno de los factores del primer miembro resulta divisible por a , como puede comprobarse al reemplazar a N por $a^2 + n$ y a n por $\frac{ka}{2}$ como sigue :

$$[(2\frac{k^2a^2}{4} + a) + ka\sqrt{N}][(2\frac{k^2a^2}{4} + a) - ka\sqrt{N}] = a^2 ;$$

dividiendo por a^2 se obtiene

$$[(\frac{k^2a}{2} + 1) + k\sqrt{N}][(\frac{ka^2}{2} + 1) - k\sqrt{N}] = 1 \quad ó ,$$

$$(\frac{k^2a}{2} + 1)^2 - Nk^2 = 1 .$$

Teniendo en cuenta que $n = \frac{ka}{2}$, tendremos finalmente :

$$(kn + 1)^2 - Nk^2 = 1 ,$$

la cual es una fórmula directa para hallar la solución mínima deseada .

Por ejemplo , en el caso de $N = 20 = 4^2+4$, con

$n = 4$ $a = 4$ $k = 2$ y $(4\times2+1)^2 - 20(2^2) =$

$q^2 - 20 \times 2^2 = 1$ ó también con $N = 20 = 5^2 - 5$, con $n = 5$ $a = -5$ $k = -2$ y

$$(5 \times (-2) + 1)^2 - 20(-2)^2 = q^2 - 20 \times 2^2 = 1$$

(El caso particular en el que a vale -1 ó ± 2 ocurre para todos los valores de N. Esta fué una de las razones que me llevaron a incluir las soluciones de $x^2 - Ny^2 = -1$ y $x^2 - Ny^2 = \pm 2$ en la tabla de las páginas 15 a 66.

Por último, en los casos en que el número de denominadores parciales del desarrollo en fracción continua de $\sqrt{N}$ es par y la penúltima reducta de cada período nos da soluciones de $x^2 - Ny^2 = 1$, basta calcular hasta la reducta correspondiente al denominador parcial inmediatamente anterior al central del período. Esta corresponderá a valores de $p^2 - Nq^2 = a$ con la particularidad de que a divide a $2N$, o sea, que $N = \frac{ka}{2}$. Luego, a divide a $Nq^2 = \frac{ka}{2} q^2$ ya que este valor debe ser entero. En consecuencia, divide también a p^2 y tenemos:

$$p^2 - Nq^2 = (p + q\sqrt{N})(p - q\sqrt{N}) = a$$

$$(p + q\sqrt{N})^2 (p - q\sqrt{N})^2 =$$

$$[(p^2 + Nq^2) + 2pq\sqrt{N}][(p^2 + Nq^2) - 2pq\sqrt{N}] = a^2 \quad y,$$

siendo p y Nq^2 divisibles por a, obtenemos

$$\left(\frac{p^2+Nq^2}{a}\right)^2 - N\left(\frac{2pq}{a}\right)^2 = 1$$

fórmula que economiza la mitad del trabajo.

LA ECUACION $x^2 - Ny^2 = \pm a$.

Suponemos conocida una solución (p,q)[1]. (Esta se puede encontrar algunas veces, por medio de las fracciones continuas, otras por el contexto de un problema dado y otras por tanteo); factorizando $p^2 - Nq^2 = \pm a$ y multiplicando por la factorización de la correspondiente ecuación de Fermat,

$$(p + q\sqrt{N})(p - q\sqrt{N}) = a$$

$$\underline{(p_n + q_n\sqrt{N})(p_n - q_n\sqrt{N}) = 1}$$

$$[(pp_n + Nqq_n) + (pq_n + qp_n)\sqrt{N}][(A) - (B)\sqrt{N}] = a$$

donde $A = pp_n + Nqq_n$ y $B = pq_n + qp_n$,

de donde

$$(pp_n + Nqq_n)^2 - N(pq_n + qp_n)^2 = a$$

con p,q la solución de la ecuación propuesta y p_n, q_n una de las de la ecuación de Fermat.

BIBLIOGRAFIA

(1) Hall and Knight , <u>Higher Algebra</u> , MacMillan and Co. Ltd. , Londres (1957) .

(2) G. Chrystal , <u>Textbook of Algebra</u> , Chelsea Publishing Co. New York , (1952) .

(3) Beiler Albert H. , <u>Recreations in the Theory of Numbers</u> , Dover Publications Inc. Nueva York , (1964) .

(4) Degan C. F. , <u>Canon Pellianus</u> , Copenague, (1817).

Da las soluciones de $y^2-Cx^2 = 1$ para $1000 \geq C$, esencialmente las mismas del presente trabajo . Desgraciadamente no lo conozco sino por referencias .

(5) Caro E. A. , <u>Apuntes sobre la raiz cuadrada (2a. parte)</u>, Notas de Matemáticas No. 5 , (1976) .

(6) Caro E. A. , <u>Divagaciones Matemáticas</u> , Revista de la Academia de Ciencias .

(7) Caro E. A. , <u>Las Fracciones Contínuas</u> , Matemática , enseñanza universitaria No. 10 (1979) .

Eduardo Caro .

Departamento de Matemáticas

Universidad Nacional

Bogotá - Colombia .