Boletín de Matemáticas
Vol. VIII , pp. 198 - 210

EL SEÑOR DE FERMAT Y SUS PROBLEMAS, II (*)

VICTOR SAMUEL ALBIS GONZALEZ

Continuamos aquí el estudio, iniciado en [19], de la influencia de Fermat en el desarrollo de la teoría de los números.

3. *La ecuación* $y^2 + k = x^3$. *El teorema de Mordell - Weil .*

Los problemas C y C' [19] conducen naturalmente a la ecuación $y^2+k=x^3$, la cual, según el decir de L. J. Mordell [10 ; pág. 238] , ha representado un papel fundamental en el desarrollo de la teoría de los números. Comencemos por anotar que la ecuación

$$y^2 + 2 = x^3 \tag{8}$$

fue estudiada por Bachet quien, en 1621, indicó un método para obtener otras soluciones racionales cuando una de ellas $[x, y]$ era conocida; este método es el de las tangentes y secantes al gráfico de la ecuación *(1)* , el cual discutiremos más adelante. En la carta que da origen a esta serie de artículos divulgativos [19] , Fermat indica que las únicas soluciones enteras de *(8)* son $[3, \pm 5]$, y que las puede obtener por descenso infinito. Euler, en 1788, usando el descenso

(*) Este artículo corresponde a la conferencia sobre curvas Elípticas dictada por el autor en el IV Coloquio Colombiano de Matemáticas. N. del E.

infinito, mostró que $y^2 - 1 = x^3$ no tiene raíces racionales para $x \geq 0$, salvo si $x = 2$. Encontró también las soluciones enteras de *(8)*, asumiendo tácitamente que el anillo $Z[\sqrt{-2}] = \{ a + b\sqrt{-2} \; ; \; a,b \in Z \}$ es factorial, aunque del método empleado no resulta obvio que se encuentran todas las soluciones buscadas [3 ; vol. II , pág. 534].

De acuerdo con la anterior discusión en el estudio de la ecuación

(9) $$y^2 + k = x^3$$

aparecen naturalmente dos problemas que investigar :

(a) La determinación del número de soluciones enteras de *(9)* .

(b) Y cómo obtener soluciones racionales de *(9)* a partir de otras.

Para discutir mejor estos asuntos necesitaremos de algunas nociones geométrico-algebraicas. Así, una ecuación polinómica $f(x, y) = 0$ estará representada geométricamente por una cierta *curva (en el plano) real* $\{ [x, y] \; ; \; f(x,y) = 0 \}$ si x e y toman sólo valores reales o por una *superficie de Riemann* si x e y toman valores complejos. Por extensión, decimos que la superficie de Riemann en cuestión es una *curva (compleja)* .

Para el estudio de las curvas los geómetras han encontrado que ciertas transformaciones de una curva en otra "más sencilla" facilitan su estudio. Entre estas transformaciones encontramos las llamadas *transformaciones birracionales* ; ellas efectúan cambios de variables del tipo siguiente

(10) $$x = \varphi(z,u) \; , \; y = \psi(z,u) \; ;$$

(11) $$z = \Phi(x, y) \; , \; u = \Psi(x, y) \quad \text{si} \quad f(x, y) = 0 \; ,$$

donde φ, ψ, Φ y Ψ son funciones racionales de sus argumentos y mediante

(10) y *(11)* se establece una correspondencia biunívoca entre los puntos de las curvas $f(x,y)=0$ y $f(z,u)=f(\varphi(z,u),\psi(z,u))=0$, salvo un número finito de puntos. En esta situación solemos decir que las dos curvas $f(x,y)=0$ y $F(z,u)=0$ son *birracionalmente equivalentes*.

Mediante una transformación birracional de una curva en otra pueden cambiar el grado de la ecuación, la forma y muchas cosas más; pero hay algo que no varía, un número entero positivo llamado el *género* g *de la curva*. Este hecho es un conocido teorema de Riemann [22; págs. 185-180] cuya demostración no intentaremos aquí. Sin embargo, estando interesados en las curvas cúbicas (de tercer grado) es posible en este caso caracterizar las de géneros 0 y 1 (entre otras cosas, no hay más): si la curva $f(x,y)=0$ tiene un *punto singular*, es decir, si el sistema de ecuaciones

$$\frac{\partial f(x,y)}{\partial x}=0\,,\qquad \frac{\partial f(x,y)}{\partial y}=0\,,\qquad f(x,y)=0$$

tiene una solución $[x,y]$, la curva es de género 0; si este sistema no tiene solución, la curva es de género 1. Así, por ejemplo, la curva $f(x,y)=y^2-x^3-x^2=0$ es de género 0, pues el sistema

$$\frac{\partial f(x,y)}{\partial x}=-x(3x-2)=0\,,\qquad \frac{\partial f(x,y)}{\partial y}=2y=0\,,\qquad f(x,y)=0$$

admite al punto $[x,y]=[0,0]$ como solución; en cambio, la curva $f(x,y)=y^2-x^3+x=0$ es de género 1; pues el sistema

$$\frac{\partial f(x,y)}{\partial x}=3x^2+1=0\,,\qquad \frac{\partial f(x,y)}{\partial y}=2y=0\,,\qquad f(x,y)=0$$

no admite soluciones; de igual forma, puede mostrarse que si $k\neq 0$, la curva

$f(x,y) = y^2 + k - x^3 = 0$ es de género 1. De manera que para el estudio de la ecuación (9) sólo necesitaremos considerar cúbicas de género 1.

En esta situación, podemos suponer, sin pérdida sustancial de la generalidad, que el punto $[0,0]$ es un punto de la curva, efectuando si es necesario una traslación del origen de coordenadas; de igual forma podemos escoger los ejes coordenados como más nos convenga valiéndonos de una rotación, sin que por ello la curva pierda su forma. También dada una recta $ax + by + c = 0$, al sustituir sea x, sea y, en la ecuación cúbica $f(x,y) = 0$, obtenemos una ecuación sea en x, sea en y, de grado inferior a tres; de lo cual concluimos que una recta corta a una cúbica a lo más en tres puntos. En particular, como la cúbica es de género 1, es decir, sin puntos singulares, la tangente a la curva en cualquier punto $P_o = [x_o, y_o]$ está determinada unívocamente por

$$(12) \qquad \frac{\partial f(x_o, y_o)}{\partial x}(x - x_o) + \frac{\partial f(x_o, y_o)}{\partial y}(y - y_o) = 0 \quad ;$$

por lo dicho anteriormente, podemos suponer que $[x_o, y_o] = [0,0]$, de modo que despejando sea x, sea y, obtenemos sea $F(x) = 0$, sea $G(y) = 0$. En este caso es fácil ver que $x = 0$ (resp. $y = 0$) es una raíz doble de $F(x) = 0$ (resp. $G(y) = 0$) y que la recta tangente corta a la curva en otro punto, que bien puede ser el mismo punto de tangencia o el punto de coordenadas $[\infty, \infty]$.

Finalmente, recordemos [23; pág. 323] que podemos escribir un polinomio de grado total 3 en la forma $f(x,y) = f_o(x,y) + f_1(x,y) + f_2(x,y) + f_3(x,y)$, donde cada $f_i(x,y)$ es un polinomio homogéneo de grado i $(i = 0, 1, 2, 3)$. En particular, como $[0,0]$ pertenece a la curva, podemos escribir

$$f(x,y) = f_1(x,y) + f_2(x,y) + f_3(x,y) .$$

Bajo estas circunstancias nos proponemos demostrar el siguiente resultado :

Teorema 3. *Si una cúbica de género 1 y coeficientes racionales tiene un punto racional, entonces existe una transformación birracional que la transforma en una cúbica de ecuación*

$$Y^2 = X^3 - AX - B$$

donde $A, B \in \mathbb{Q}$ *y* $4A^3 - 27B^2 \neq 0$.

Demostración : Sea $P_o = [x_o , y_o]$ el punto de coordenadas racionales, y tomemos como origen el punto $P_1 = [x_1 , y_1]$, de coordenadas racionales, en que la tangente a la curva en P_o la corta nuevamente. La cúbica puede escribirse ahora en la forma

$$f_1(x, y) + f_2(x, y) + f_3(x, y) = 0 \quad , \tag{13}$$

donde las $f_i(x, y)$ son polinomios homogéneos de grado $i = 1, 2, 3,$ ya que la cúbica pasa por el origen. Hagamos ahora una rotación de ejes en tal forma que la tangente $P_o P_1$ no sea el eje de las y , escribiendo todavía la ecuación de la cúbica como en *(13)* . Haciendo $y = xt$, esta recta paramétrica cortará a la cúbica, además de hacerlo en el punto $[0, 0]$, en los puntos determinados por la ecuación de segundo grado en x

$$x^2 f_3(1, t) + x f_2(1, t) + f_1(1, t) = 0 \quad ;$$

es decir, en los puntos determinados por

$$Lx^2 + 2Mx + N = 0$$

donde L, M, N son polinomios en t , de coeficientes racionales y de grados respectivos $3, 2, 1$. De aquí resulta que

$$(Lx + M)^2 = M^2 - LN \ ;$$

como P_o y P_1 son puntos racionales y la tangente $P_o P_1$ está representada por una ecuación del tipo $y = xt_o$, encontramos que la cuártica en t, $M^2 - LN = 0$ tiene una raíz racional t_o, pues es claro que las raíces de $M^2 - LN = 0$ corresponden a las rectas que pasan por P_1 y son tangentes a la cúbica. Hagamos $t = t_o + 1/T$. Entonces

$$(Lx + M)^2 = F(T) / T^4 \ ,$$

donde $F(T)$ es una cúbica en T, de coeficientes racionales. Haciendo $T = CX + D$, C y $D \in \mathbb{Q}$, $Lx + M = NY \neq (CX + D)^2$, obtenemos una ecuación de la forma

$$Y^2 = 4X^3 - aX - b \ , \qquad (14)$$

donde $a, b \in \mathbb{Q}$. Obtiénense así las fórmulas

$$t = (EX + G) / (CX + D) \quad \text{e} \quad y = tx \ .$$

De aquí es fácil obtener expresiones $X = \varphi(x, y)$, $Y = \psi(x, y)$, $x = \Phi(X, Y)$, $y = \Psi(X, Y)$ que nos dan la transformación birracional buscada entre *(13)* y *(14)*. Claramente si $[X, Y]$ es racional obtendremos $[x, y]$ raciomal, y viceversa. La ecuación *(14)* se transforma en la siguiente

$$F(X, Y) = Y^2 - X^3 + AX + B = 0 \qquad (15)$$

al sustituir X, Y por X/R, $Y/4$, respectivamente. Finalmente, dado que *(15)* sigue siendo de género 1, pues el género no cambia por una transformación birracional, el sistema

$$\frac{\partial F}{\partial Y} = 2Y = 0 \quad ; \quad \frac{\partial F}{\partial X} = -3X^2 + A = 0 \quad ; \quad F(X, Y) = 0 \ ,$$

no tiene solución , es decir :

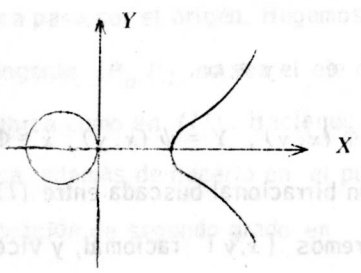
$$X^3 - AX - B = 0 \qquad \text{y} \qquad X^2 = A/3$$

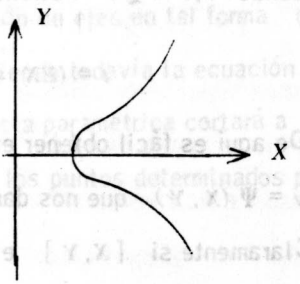
no tiene solución , o lo que es lo mismo, $d = 4A^3 - 27B^2 \neq 0$.

Si en *(15)* hacemos $Y = 0$. obtenemos

(16) $$X^3 - AX + B = 0 \ ,$$

y como $d = 4A^3 - 27B^2 \neq 0$, las tres raíces de *(16)* son todas distintas [23 ; págs. 240 - 242] ; de aquí resulta que la parte real de la curva *(15)* tendrá una y sólo una de las dos formas presentadas en la figura 1 ; en particular, la curva $Y^2 = X^3 - k$ se presentará siempre como en la figura 1, b) .





$Y^2 - X^3 + X = 0$ $\qquad$ $d = 4 > 0$ $\qquad$ a)

$Y^2 = X^3 - 2$ $\qquad$ $d = -108 < 0$ $\qquad$ b)

Figura 1

Supongamos ahora que P un punto de coordenadas racionales de la cúbica

(15). La tangente a la curva en el punto P corta a la cúbica en un tercer punto, tal como hemos indicado antes, y este punto tiene coordenadas racionales como es fácil verificar. Así mismo, si P_1 y P_2 son dos puntos racionales de *(15)* la recta que los une corta a la cúbica en otro punto (en general distinto) también de coordenadas racionales. Este procedimiento, debido a Bachet, sugiere la posibilidad de que todos los puntos racionales de la cúbica *(15)* se obtienen de esta forma. Intentando demostrar este hecho, L. J. Mordell demostró el siguiente resultado.

Teorema 4 [10; págs. 138 y siguientes] [21]. *En la cúbica (15) existen puntos* $P_1, \ldots, P_r$ *a partir de los cuales se obtienen todos los puntos racionales de la cúbica mediante el trazado de tangentes y secantes.*

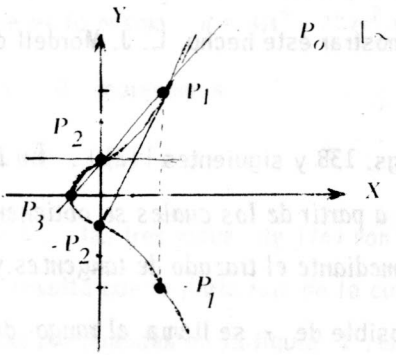
El menor valor posible de r se llama *el rango* de la curva. Si r tiene este valor, decimos que $P_1, \ldots, P_r$ forman una *base* de la curva.

Por este procedimiento parece posible obtener, en general, un número infinito de puntos sobre la cúbica *(15)*. Este no es el caso como lo demostró en primera instancia Euler para la cúbica $Y^2 = X^3 + 1$, la cual tiene exactamente los siguientes puntos racionales: $[2,3]$, $[0, 1]$, $[-1, 0]$, $[0, -1]$, $[2, -3]$, $[\infty, \infty]$.

El Teorema 4 fue generalizado luego por André Weil [25] al caso en que los puntos racionales de nuestra discusión se reemplazan por puntos de coordenadas en un cuerpo arbitrario de números algebraicos.

Podemos dar a los puntos racionales de *(15)* una estructura de grupo definiendo la suma $P_1 + P_2$ de dos puntos racionales como el punto P_{12} simétrico con respecto al eje OX del tercer punto de corte de la cúbica con la recta $P_1 P_2$. En particular, si $P_1 = P_2$, entonces $P_1 + P_1 = P_{11}$ representa el

simétrico con respecto a OX del tercer punto de corte de la tangente en P_1 con la cúbica. Si definimos $-P_1$ como el simétrico de P_1 con respecto a OX y $P_o = |\sim.\sim|$ como el elemento neutro, es fácil verificar que en esta forma se ha definido una ley de grupo en el conjunto de los puntos racionales de *(15)*. Así por ejemplo, para $Y^2 = X^3 + 1$ tenemos el gráfico y la tabla siguientes :



	P_o	P_1	P_2	P_3	$-P_1$	$-P_2$
P_o	P_o	P_1	P_2	P_3	$-P_1$	$-P_2$
P_1	P_1	P_2	P_3	$-P_2$	P_o	$-P_1$
P_2	P_2	P_3	$-P_2$	$-P_1$	P_1	P_o
P_3	P_3	$-P_2$	$-P_1$	P_o	P_2	P_1
$-P_1$	$-P_1$	P_o	P_1	P_2	$-P_2$	P_3
$-P_2$	$-P_2$	$-P_1$	P_o	P_1	P_3	P_2

Observación : $P_2 + P_2 = -P_2$, pues P_2 es un punto de inflexión de la cúbica $Y^2 = X^3 + 1$.

Podemos entonces re-enunciar el teorema 4, diciendo que los puntos racionales de la cúbica *(15)* forman un grupo neteriano.

La demostración del teorema 4 no la haremos aquí, remitiendo para ella a [10 ; págs. 138 - 144] . Es frecuente en la literatura que se diga que la ecuación cúbica *(15)* representa una *curva elíptica* ; la razón de ello proviene del hecho de que las coordenadas de sus puntos $P = [X, Y]$ pueden expresarse en términos de un parámetro elíptico u mediante

(16) $$X = \wp(u) \ , \qquad 2Y = \wp'(u) \ ,$$

donde $\wp(u)$ es la función de Weierstrass de invariantes $4A$, $4B$ y períodos w_1, w_2 , y $\wp'(u)$ es derivada ; existe entonces una correspondencia biunívoca entre el parámetro elíptico u , módulo $\Omega = \mathbb{Z} w_1 + \mathbb{Z} w_2$, y los puntos $P = (P(u) = (\wp(u) , \frac{1}{2} \wp'(u))$, la cual nos permite identificar la curva elíptica con un *toro* (Figura 2) . [Para todo lo referente a las funciones elípticas pue -

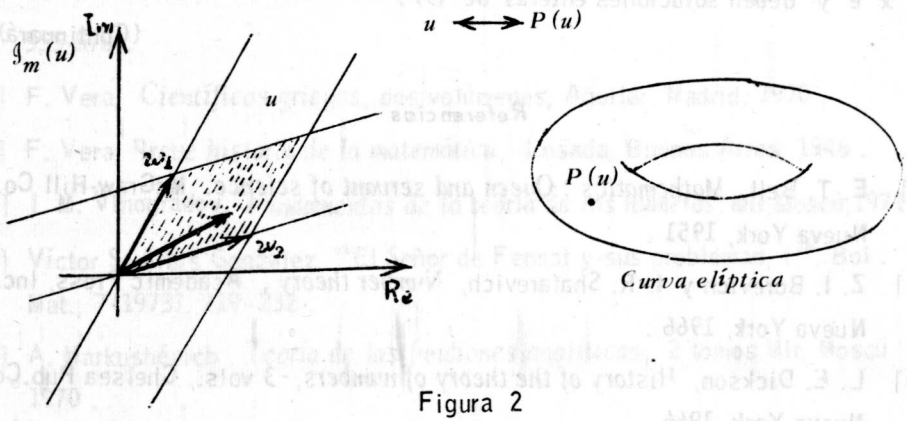


Figura 2

den consultarse los libros de Markusévich [20] y Knopp [24].

La otra pregunta que nos hicimos al principio se refería a la determinación de los puntos de coordenadas enteras de la ecuación *(9)*. Este problema es un poco más delicado, pudiéndose demostrar que *(9)* sólo tiene un número finito de soluciones enteras. La demostración [10; pág. 246] se basa en el siguiente teorema de Thue [10; págs. 186 y siguientes].

Teorema 5. *La ecuación*

$$(17) \qquad f(X,Y) = a_0 X^n + a_1 X^{n-1} Y + \cdots + a_n Y^n = m \quad (\neq 0),$$

cuando $n \geq 3$ *y* $f(X, Y) \in \mathbb{Z}[X, Y]$ *es irreducible sobre los racionales, tiene solamente un número finito de soluciones enteras.*

El problema siguiente, al saber que el número de soluciones es finito, consiste en obtener cotas para su número. En este sentido los resultados de A. Baker son notables [26]; así, por ejemplo, ha demostrado que

$$máx\{|x|, |y|\} \leq exp\,(10^{10} \cdot |k|^{10^4})$$

si x e y deben soluciones enteras de *(9)*.

(Continuará)

Referencias

[1] E. T. Bell, *Mathematics : Queen and servant of science.* McGraw-Hill Co., Nueva York, 1951.

[2] Z. I. Borevich y I. R. Shafarevich, *Number theory*, Academic Press, Inc., Nueva York, 1966.

[3] L. E. Dickson, *History of the theory of numbers*, 3 vols., Chelsea Pub.Co., Nueva York, 1966.

[4] A. O. Gelfond, *The solution of equations in integers*, W. H. Freeman, San Francisco, 1961 .

[5] E. Grosswald, *Topics from the theory of numbers*, Macmillan, Co., Nueva York, 1966 .

[6] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, 2a. ed., Chelsea Publ. Co., Nueva York, 1970.

[7] D. Hilbert, *Théorie des corps de nombres algébriques*, Hermann, París, 1913.

[8] K. L. Jensen, "Om talteoristike Egenskaber ved de Bernoulliske Tal", Nyt Tiusskrift for Math., 26 B (1915) , 73-83 .

[9] B. W. Jones, *Introducción a la teoría de números* , Rev. Mat. Elem., Monografías Matemáticas, No. 4 , Bogotá, 1968 .

[10] L. J. Mordell, *Diophantine equations*, Academic Press, Nueva York, 1969 .

[11] L. J. Mordell, *Three lectures on Fermat's last theorem*, Cambridge, 1921 .

[12] T. Nagell, *Introduction to number theory* , Chelsea, Publ. Co., Nueva York, 1964 .

[13] R. Nougués, *Théorème de Fermat, son histoire*, Vuibert, París, 1932 .

[14] O. T. O'Meara, *Introduction to quadratic forms*, Springer Verlag, Berlín, 1963.

[15] H. S. Vandiver, "Fermat's last theorem" , Amer. Math. Monthly, 53(1946) , 555-578 .

[16] F. Vera, *Científicos griegos*, dos volúmenes, Aguilar, Madrid, 1970 .

[17] F. Vera, *Breve historia de la matemática*, Losada, Buenos Aires, 1946 .

[18] I. M. Vinográdov, *Fundamentos de la teoría de los números*, Mir, Moscú, 1971.

[19] Víctor S. Albis González, "El Señor de Fermat y sus problemas, I", Bol . Mat., 7(1973), 219-232 .

[20] A. Markushévich , *Teoría de las funciones analíticas*, 2 tomos Mir, Moscú 1970 .

[21] L. J. Mordell, *A Chapter in the theory of numbers*, Cambridge University Press, Cambridge, 1947 .

[22] R. Walker, *Algebraic curves*, Dover, New York, 1962

[23] A. K. Kurosh , *Curso de álgebra superior*, Mir, Moscú, 1968 .

[24] K. Knopp , *Teoría de funciones*, Labor, Barcelona, 1950 .

[25] A. Weil , " L'Arithmétique sur les courbes algébriques", Acta Math., 52 (1928), 281-315.

[26] A. Baker, "On the representation of integers by binary forms", Phil. Trans. R. Soc., 263 (1968), 173-191 .

[27] W. J. LeVeque, *A brief survey of diophantine equations*, en "Studies in Number Theory", Math. Asoc. America, Prentice-Hall, Inc., Englewood Cliffs , 1969.

Departamento de Matemáticas y Estadística
Universidad Nacional de Colombia
Bogotá, Colombia.