Boletín de Matemáticas
Volumen X (1976). págs. 86 - 95

EL SEÑOR DE FERMAT Y SUS PROBLEMAS, III

VICTOR SAMUEL ALBIS GONZALEZ

Finalizamos con esta entrega el estudio, iniciado en [19], de la influencia de Fermat en el desarrollo de la teoría de los números.

4. La génesis de la teoría aritmética de las formas cuadráticas.

Nos proponemos mostrar en este aparte que en la Proposición *D* [19] : *Todo número primo de la forma* $p=4n+1$ *es* [*unívocamente*] *la suma de dos cuadrados*, es posible encontrar el germen fecundo de la *teoría aritmética de las formas cuadráticas*, una de las ramas más hermosas y venerables de la Matemática.

Es posible aún encontrar rastros de esta teoría en la Aritmética [17] de Diofanto de Alejandría, pero no de manera sistemática; por ejemplo, ya hemos visto que éste propone encontrar las soluciones de

$$(18) \qquad Q(x,y,z) = x^2 + y^2 - z^2 = 0 ,$$

Ahora bien, la expresión $Q(x,y,z) = x^2 + y^2 - z^2$ es un ejemplo de una forma cuadrática, y la situación descrita en la proposición 1, es un ejemplo del problema general de la teoría aritmética de las formas cuadráticas, problema que expli -

citaremos a continuación :

Dada la forma cuadrática, de coeficientes enteros,

$$Q(x_1, \ldots, x_n) = \sum_{i,j} a_{ij} x_i x_j$$

determinar los números enteros m *para los cuales la ecuación*

(19) $$Q(x_1, \ldots, x_n) = m$$

tiene soluciones enteras. En caso de que (19) tenga soluciones, encontrar alguna manera de determinarlas.

Cuando existe una solución de (19) decimos que $Q(x_1, \ldots, x_n)$ *representa al número* m ; luego el problema puede expresarse de esta otra manera : *determinar los* m *que son representables por la forma cuadrática* $Q(x_1, \ldots, x_n)$, y determinar esas representaciones. Así, la proposición de Diofanto diría que 0 es representable por $Q(x,y,z) = x^2 + y^2 - z^2$ (y de manera no trivial, es decir, con $[x,y,z] \neq [0,0,0]$) y provee un método para hallarlas, mientras que la proposición D diría que los primos impares de la forma $4n+1$ son representables por $Q(x,y) = x^2 + y^2$. En seguida veremos cómo encontrar las soluciones de $x^2 + y^2 = m$.

Para ilustrar la teoría aritmética de las formas cuadráticas, haremos aquí un estudio completo, aunque elemental, de la

(20) $$Q(x,y) = x^2 + y^2 .$$

El hecho siguiente :

(21) $$(x^2 + y^2)(x_1^2 + y_1^2) = (xx_1 - yy_1)^2 + (xy_1 + x_1 y)^2 ,$$

o bien,

(22) $$Q(x,y)\,Q(x_1,y_1) = Q(xx_1 - yy_1, xy_1 + x_1 y),$$

era conocido por Fermat [3, vol. II ; pág. 227] ; a partir de él es fácil convencerse de que para saber si $p_1^{\alpha_1} \ldots p_r^{\alpha_r} > 0$ [12] es representable por $Q(x,y)$, basta saber si cada p_i lo es. Parece, pues, posible que partiendo de la proposición D y la relación (21), podamos obtener todos los m representables por la forma (20). Como veremos, esto es bastante exacto. Un teorema como el contenido en la Proposición D , que nos indica qué primos son representables por una forma cuadrática, se llama un *teorema de género,* mientras que una relación como la (21), que nos indica cómo componer $Q(x,y)$ consigo misma para obtener, a partir de un teorema de género, nuevos números representables por la forma cuadrática, se llama un *teorema de composición.* Es claro ahora porqué decíamos antes que estos resultados de Fermat eran germinales.

Para ilustrar lo anterior, tomemos

(23) $$3^2 + 2^2 = 13 \quad , \quad [x,y] = [3,2] \ ,$$

$$2^2 + 1^2 = 5 \quad , \quad [x_1, y_1] = [2,1] \ .$$

Usando (21), obtenemos

$$4^2 + 7^2 = 65 \ , \ [xx_1 - yy_1 \ , \ xy_1 + x_1 y] = [4,7] \ .$$

Mientras que haciendo

$$(-3)^2 + 2^2 = 13 \ , \quad [x,y] = [-3,2] \ ,$$

$$2^2 + 1^2 = 5 \ , \quad [x_1, y_1] = [2,1] \ ,$$

---

(12) Dado que $Q(x,y) = x^2 + y^2 > 0$, sólo son de interés los enteros positivos.

obtenemos

$$(-8)^2 + 1^2 = 65 , \quad [xx_1 - yy_1 , xy_1 + x_1 y] = [-8 , 1] .$$

Es fácil verificar, además, que $7^2 + 4^2 = 8^2 + 1^2$ son las únicas representaciones de 65 en la forma $x^2 + y^2$, salvo el orden o los cambios de signos.

Pasemos ahora sí a demostrar los resultados anunciados e ilustrados anteriormente.

Teorema 6. *Un primo p es representable por $x^2 + y^2$ $(xy \neq 0)$ si, y sólo si, $p=2$ ó $p \equiv 1$* (mód. 4).[13]

La demostración de este teorema, debida esencialmente a Euler en la forma que vamos a presentarla, la dividiremos en varios lemas :

Lema 1. *Ningún entero de la forma $4n + 3$ es la suma de dos cuadrados.*

En efecto, si $x^2 + y^2 = 4m + 3$, entonces sería $x^2 + y^2 \equiv 3$ *(mód. 4)* ; pero esto es imposible, pues siempre tendremos $x^2 + y^2 \equiv 0, 1, 2$ *(mód. 4).*

Lema 2 (Euler) [3, vol. II ; pág. 231] · *Si $p=4n+1$ es un primo, entonces existe una solución en enteros $[x,y,m]$ de la ecuación*

$$x^2 + y^2 = pm$$

que satisface $0 < m < p$.

En efecto, como $p \equiv 1$ *(mód. 4)*, existe $s \in Z$ tal que $s^2 + 1 \equiv 0$ *(mód. p)* [12 ; pág. 135] . Por otra parte, siempre es posible encontrar $S \equiv \pm s$ *(mód. p)* que cumpla $|S| < p/2$. Luego $0 < mp = 1 + S^2 < 1 + p^2/4 < p^2$, para algún entero m ; y como $0 < mp < p^2$ implica que $0 < m < p$, resulta que $[1, S , m]$ satisface la ecuación dada y la condición adicional requerida.

(13) A. Girard [3, vol. II, pág. 227] ya había hecho, en 1625, una determinación de los números expresables como suma de cuadrados; pero parece que Fermat fue quien indicó la importancia de este resultado, llamándole de paso el teorema fundamental de los triángulos rectángulos.

Lema 3. *(Paso de descenso). Si* $p = 4n + 1$ *es un primo y* $x^2 + y^2 = mp$, *con* $0 < m < p$, *entonces existen enteros* x_1, y_1 *y* m_1 *tales que* $x_1^2 + y_1^2 = pm_1$ *con* $1 \leq m_1 < m$.

En efecto, si m es par, x é y tienen entonces la misma paridad (i.e., $x \equiv y$ *(mód. 2)*); por consiguiente, podemos escribir

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = \left(\frac{m}{2}\right) p ,$$

y el lema resulta entonces con $x_1 = (x+y)/2$, $y_1 = (x-y)/2$ y $m_1 = m/2$. Si m es impar, escribimos

$$x = am + a_1 , \quad \text{con} \quad |a_1| < m/2 ,$$
$$y = bm + b_1 , \quad \text{con} \quad |b_1| < m/2 ;$$

luego

$$(24) \qquad a_1^2 + b_1^2 + 2Am + (a^2 + b^2) m^2 = mp ,$$

donde $a = aa_1 + bb_1$; por lo tanto,

$$a_1^2 + b_1^2 = m_1 m , \quad \text{con} \quad m_1 + 2a + (a^2 + b^2) m = p .$$

De aquí resulta que :

$$m_1^2 + 2Am_1 + (a^2 + b^2)(a_1^2 + b_1^2) = (m_1 + A)^2 + B^2 = m_1 p ,$$

donde $B = ab_1 - ba_1$.

Si $m_1 = 0$, tendríamos $a_1 = b_1 = 0$, lo cual implicaría, usando (24), que $m^2 \mid x^2 + y^2 = mp$, y , por consiguiente, que $m \mid p$. Como $0 < m < p$, esto es

imposible. Por lo tanto, $m_1 \geq 1$. Pero entonces

$$m_1 m = a_1^2 + b_1^2 < m^2/2 < m^2 \Rightarrow m_1 < m \ ;$$

luego $x_1 = m_1 + A$, $y_1 = B$ y m_1 satisfacen las condiciones requeridas en el lema.

Demostración del teorema 6. Por el lema 2, existen x, y tales que $x^2 + y^2 = mp$, con $1 \leq m < p$. Si $m > 1$, aplicamos el lema 3 varias veces para descender hasta $x_k^2 + y_k^2 = p$. Luego si $p \equiv 1 \ (mód\ 4)$, $Q(x,y)$ representa a p. Como $2 = 1^2 + 1^2$, el primo 2 es también representable por $Q(x,y)$. Lo recíproco resulta finalmente del lema 1.

Señalemos ahora que es posible demostrar con cierta facilidad que las soluciones de $Q(x,y) = p$ son *esencialmente únicas*, con excepción hecha de los signos y el orden en que aparecen x é y ([9; pág. 63], [28; pág. 106]). Sin embargo, es importante distinguir entre soluciones que difieren por los signos ya que esta distinción nos permitirá en general encontrar nuevos números representables por $Q(x,y)$, tal como lo hemos observado anteriormente en un ejemplo.

El teorema de composición (21) nos permitirá ahora demostrar el siguiente resultado:

Teorema 7. *Si $m = x^2 + y^2$ tiene una solución $[x,y]$ que cumple $(x,y) = 1$, entonces*

$$m = 2^{\alpha} p_1^{\alpha_1} \ldots p_r^{\alpha_r} \ , \tag{25}$$

en donde $p_i \equiv 1$(mód. 4), $i = 1, \ldots, r$. Recíprocamente, todo m de la forma (25) es representable por $Q(x,y) = x^2 + y^2$.

En efecto, en virtud de (21) y el teorema 6, todo entero de la forma (25) es representable por $Q(x,y)$. Recíprocamente, si $m = x^2 + y^2 \equiv 0 \ (mód.\ p)$, en donde $(x,y) = 1$ y p es un divisor primo impar de m, vemos que necesariamente $(y,p) = 1$. Pero entonces existe $z \in Z$ tal que $zy \equiv 1 \ (mód.\ p)$, con lo cual

$$x^2 z^2 = 1 \equiv 0 \ (mód.\ p) \ ;$$

pero esta congruencia tiene solución si, y sólo si, $p \equiv 1 (mód.4)$. ([12; pág. 135])

Es importante ahora anotar que los números de la forma (25) no agotan el conjunto de los números representables por $Q(x,y)$, puesto que $245 = 5(7)^2$ no la tiene y sin embargo

$$7^2 x 5 = 7^2 (1^2 + 2^2) = (7 \times 1)^2 + (7 \times 2)^2 \ .$$

A título de ejercicio proponemos el siguiente corolario del teorema 7 [28; pág. 108], el cual aclara la situación que se presenta en el anterior ejemplo :

Corolario. *Sea*

$$m = 2^{\alpha} p_1^{\alpha_1} \ldots p_r^{\alpha_r} q_1^{2\beta_1} \ldots q_s^{2\beta_s} \ ,$$

en donde $p_i \equiv 1 (mód.4)$ *y* $q_j \equiv 3 (mód.4)$, *la descomposición canónica de* m. *Entonces* m *es representable por* $Q(x,y) = x^2 + y^2$. *Recíprocamente, si* m *es representable por* $Q(x,y)$, *los factores primos de* m *que son congruentes con* 3 $(mód.4)$ *aparecen con exponente par en la descomposición canónica de* m.

Por otra parte, dado que $k^2 m = (kx)^2 + (ky)^2$, es fácil convencerse, teniendo en cuenta el anterior resultado, que siempre podremos limitarnos al caso $(x,y) = 1$.

Pasamos ahora a ilustrar una extensión de lo que hemos hecho hasta aquí, con la intención de esclarecer aún más la noción de *composición de formas cuadráticas*. Sea, pues, el par de formas cuadráticas :

$$Q_1(x,y) = x^2 + 5y^2 \ ,$$

$$Q_2(x,y) = 2x^2 + 2xy + 3y^2 \ .$$

Preguntamos entonces por los números enteros m representados sea por $Q_1(x,y)$ sea por $Q_2(x,y)$. Para empezar, observemos que

$$(26)\qquad \begin{cases} Q_1(x,y)\,Q_1(x_1,y_1) = Q_1(xx_1 - 5yy_1\,,\; x_1y + xy_1) \\ Q_1(x,y)\,Q_2(x_1,y_1) = Q_2(xx_1 - x_1y - 3yy_1,\; xy_1 + 2x_1y + yy_1)\,, \\ Q_2(x,y)\,Q_2(x_1,y_1) = Q_1(2xx_1 + xy_1 + x_1y - 2yy_1,\; xy_1 + x_1y + yy_1)\,, \end{cases}$$

relaciones que podemos obtener por verificación directa. Ellas nos dicen que si, por ejemplo, m es representable por Q_1 y n es representable por Q_2, su producto mn será representable por Q_2; luego para obtener los números representables sea por Q_1 sea por Q_2, basta obtener aquellos números primos que lo son por una de ellas. Estos a su vez están determinados por el siguiente teorema de género :

Teorema 8. a) *$Q_1(x,y)$ representa al primo p si, y sólo si, $p \equiv 1,9$ (mód. 20) ó $p = 5 = Q_1(0,1)$.*

b) *$Q_2(x,y)$ representa al primo p si, y sólo si, $p \equiv 3,7$ (mód. 20) ó $p = 2 = Q_2(1,0)$.*

Este resultado no lo demostraremos aquí. Sin embargo, veamos cómo usarlo en combinación con las relaciones (26) (Teorema de composición) : tenemos

$$Q_2(1,1) = 7 \quad \text{y} \quad Q_2(0,1) = 3 \qquad \text{(Teorema 8)} ;$$

luego

$$21 = 7x3 = Q_2(1,1)\,Q_2(0,1) = Q_1(-1,2)\,,$$

usando la última de las relaciones (26). Éstas, entre otras cosas, insinúan *una estructura de grupo* ; más precisamente, *$\{Q_1, Q_2\}$ es un grupo que satisface* $Q_1Q_1 = Q_1$, $Q_1Q_2 = Q_2$, $Q_2Q_2 = Q_1$. En la situación descrita para $Q(x,y) = x^2 + y^2$, *$\{Q\}$ es un grupo que satisface* $QQ = Q$. Empezamos, pues a sospechar la intromisión del álgebra en nuestro problema original. Este en toda su generalidad fue discutido brillantemente por Gauss en sus *Disquisitiones Arithmeticae* [30 ; págs. 118 y sigs.]. Hoy en día en vez de trabajar directamente con las for-

mas, como Gauss, preferimos hacerlo con ideales de un cuerpo cuadrático $Q(\sqrt{d})$, asociando a cierta clase de formas cuadráticas un ideal de $Q(\sqrt{d})$. Una exposición, por demás interesante desde el punto de vista histórico, que sigue estas pautas se encuentra en [29].

Bibliografía

1. E. T. Bell, Mathematics : *Queen and servant of science*. McGraw-Hill Co.,Nueva York, 1951.
2. Z.I. Borevich é 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. Gelfand, *The solution of equations in integers*, W.H. Freeman, San Francisco, 1961.
5. E. Grosswald, *Topics from the theory numbers*, Macmillan Co., Nueva York , 1966.
6. E. Hecke, *Vorlesunger. über die Theorie der algebraischen Zahlen*, 2a. ed., Chelsea Pub. Co., Nueva York, 1970.
7. D. Hilbert, *Théorie des corps de nombres algébriques*, Hermann, Paris, 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 Pub. 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 vols., 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. (Bogotá), 7(1973), 219-232.

20. A. Markushévich, *Teoría de las funciones analíticas*, 2 vols., 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. Le Veque, "A brief survey of diophantine equations", en "Studies in Number Theory", Math. Asoc. America, Prentice-Hall Inc., Englewood Cliffs, 1969.

28. Víctor S. Albis González, *Temas de Aritmética y Algebra*, Soc. Col. Mat., Bogotá, 1976.

29. H. Cohn, *A second course in number theory*, Wiley, Nueva York, 1964.

30. C. F. Gauss, *Recherches Arithmétiques*, Courciers, Paris, 1807.

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