Boletín de Matemáticas
Volumen VII Nº 4 , pp. 219-232

EL SEÑOR DE FERMAT [1] Y SUS PROBLEMAS, I

VICTOR SAMUEL ALBIS GONZALEZ *

1. Introducción.

El propósito de este trabajo es analizar en parte la obra de Fermat y mostrar cómo sus ideas han influido en el desarrollo ulterior de la teoría de los números. Transcribiremos en seguida apartes de una carta de Fermat a Carcavi [2], en la cual curiosamente aparecen juntos los problemas de los cuales arranca el desarrollo del cual queremos hablar :

"Y, como los métodos que están en los libros eran insuficientes para demostrar proposiciones tan difíciles, he encontrado al fin un camino verdaderamente singular, para hacerlas. He llamado esta manera de demostrar el *descenso infinito*, y al principio me he servido de él para demostrar proposiciones negativas, como, por ejemplo, ..., que no hay ningún triángulo rectángulo, expresado en números enteros cuya área sea un cuadrado. La demostración se hace por reducción al absurdo, de esta manera : si hubiese un triángulo en números enteros que tuviese un área igual a un cuadrado, habría un otro triángulo menor que éste, que tendría la misma propie-

*) El autor quiere agradecer la hospitalidad que le brindó el NEPEC (Río de Janeiro), permitiéndole concluir la redacción de este trabajo.

1) Pierre S. de Fermat nació el 17 de agosto de 1601 en Beaumont-de-Lomagne y murió en Castres el 12 de enero de 1665.

2) La carta está fechada el 14 de agosto de 1659; Carcavi la comunicó luego a Huygens.

dad. Si hubiese un segundo menor que el primero que tuviese esta misma propiedad, habría, por un razonamiento parecido, un tercero menor que el segundo, que tendría la misma propiedad y en fin, un cuarto, un quinto y así descendiendo hasta el infinito; pero, dado un número entero, no existe más que un número finito de números enteros menores que aquél. De donde se concluye que es pues imposible que haya un triángulo rectángulo cuya área sea un cuadrado. No añado la razón de la cual infiero que, si hubiese un triángulo rectángulo de esta naturaleza, habría otro de la misma naturaleza menor que el primero, pues el discurso se haría muy largo y es allí donde está todo el misterio de mi método. Me gustaría que los Pascales y los Robervales y tantos otros sabios lo busquen bajo mis indicaciones. Por mucho tiempo, no pude aplicar mi método a las proposiciones afirmativas porque el rodeo y el prejuicio para llegar allí eran mucho más difíciles. De suerte que cuando me fue necesario probar que todo primo que sobrepasa por la unidad a un múltiplo de cuatro, está compuesto de dos cuadrados, me encontraba en gran dificultad. Pero nuevos principios me permitieron lograrlo. Mi razonamiento sobre las cuestiones afirmativas es así : si un tal número tomado a discreción, no es el compuesto de dos cuadrados, habría un número de la misma naturaleza menor que el dado, y así sucesivamente, descendiendo hasta el infinito, hasta que llegaríais a 5, que es el menor, el cual,se seguiría, no es el compuesto de dos cuadrados, y sin embargo lo es, de donde se debe inferir, por la reducción al imposible, que todos aquellos de la misma naturaleza son, en consecuencia, compuestos de dos cuadrados. He considerado en seguida ciertas cuestiones que, si bien negativas, contienen grandes dificultades y el método para practicar el descenso es de hecho diferente a los precedentes, como será fácil comprobar. Tales son las siguientes : no hay ningún cubo dividido en dos cubos. Sólo hay un cuadrado (25) en enteros que aumentado del binario haga

un cubo. Sólo hay dos cuadrados (4 y 121), los cuales aumentados de cuatro, hagan un cubo" [3].

Analizando esta carta, observamos que, usando el *método del descenso infinito*, Fermat *demuestra* o *dice que es capaz de demostrar* las siguientes proposiciones:

A. *El área de un triángulo rectángulo de lados enteros no puede ser un cuadrado perfecto.*

B. $x^3 + y^3 = z^3$ *no tiene soluciones en números enteros* x, y, z, *con* $xyz \neq 0$.

C. $y^2 + 2 = x^3$ *tiene como únicas soluciones enteras a* $x = 3$, $y = \pm 5$.

C'. $y^2 + 4 = x^3$ *tiene como únicas soluciones enteras a* $x = 2$, $y = \pm 2$ *y* $x = 5$, $y = \pm 11$.

D. *Todo primo de la forma* $p = 4n + 1$ *es unívocamente la suma de dos cuadrados.*

Pues bien, el método del descenso infinito (que parece ya encontrarse en Euclides) se ha mostrado infalible cada vez que puede usarse, pero usualmente la dificultad estriba en hallar el esencial *paso de descenso*, tal como lo señala en la anterior carta el propio Fermat: "No añado la razón de la cual infiero que, si hubiese un triángulo rectángulo de esta naturaleza, habría otro de la misma naturaleza menor que el primero, pues el discurso se haría muy largo y es allí donde está todo el misterio de mi método". El uso posterior que han hecho de él Lejeune-Dirichlet, Mirimanoff, Mordell y A. Weil le han mantenido en posición privilegiada. Para sosiego de modernistas y puristas, transcribimos este método a un lenguaje más contemporáneo:

Se supone que existe un número natural n que posee una cierta propiedad P (ésta es *la hipótesis de descenso*). Esta suposición implica entonces la existencia

3) Tomado de R. Nougés [13]. Mencionada también en L. E. Dickson [3; v. 2, pág. 228].

de un número natural m menor que el dado el cual posee también la propiedad P (éste es *el paso de descenso*); pero esto nos lleva a una contradicción, pues siempre existe un menor número natural que posee la propiedad P. En consecuencia, la hipótesis de descenso es falsa para todo número natural.

Vale la pena anotar que, en algunos casos, para ciertos valores de n no se aplica el paso de descenso; en ellos, la hipótesis de descenso puede ser cierta para un número finito, o quizá infinito, de números naturales. Usando una modificación adecuada del anterior raciocinio, es posible a menudo determinar todos los números naturales que poseen la propiedad P. Algunos ejemplos de esta situación pueden verse en el libro de T. Nagell [12; págs. 232-235].

Las proposiciones A, B, C, C' y D han conducido a tres áreas de intensa investigación -en diferentes épocas- en la teoría de las ecuaciones diofánticas. De esto tratarán los siguientes apartes de este trabajo. En cada uno de ellos discutiremos la posible solución de dada por Fermat, la manera como estos problemas condujeron a extensos capítulos de la teoría de los números, así como también, y en lo posible, el estado actual de cada uno de estos capítulos.

La determinación de las soluciones enteras de ecuaciones algebraicas de coeficientes enteros -las llamadas *ecuaciones diofánticas*- es uno de los problemas más difíciles y antiguos de la matemática; un primer estudio sistemático de ellas fue hecho por Diofanto (siglo IV a. de J.C.)[4], estudio que fue continuado en el siglo dieciocho por Fermat, Euler (1707 - 1783), J. Lagrange (1736 - 1813) y otros. Veamos como plantean hoy en día los matemáticos este problema : Dados los polinomios $P_j(x_1, \ldots, x_n)$, $j = 1, 2, \ldots, m$, de coeficientes enteros, determinar :

4) Véase la traducción parcial del libro de Diofanto que se halla en F. Vera, Científicos griegos, vol. 2, Aguilar, Madrid, 1970. En este libro se encontrarán también traducciones de Euclides, Papo, Proclo y otros.

a) *si existen soluciones enteras del sistema*

$$(1)\qquad \begin{cases} P_1(x_1, \ldots, x_n) = 0 \\ P_2(x_1, \ldots, x_n) = 0 \\ \cdots\cdots\cdots \\ P_m(x_1, \ldots, x_n) = 0 \end{cases}$$

b) *en caso de que existan estas soluciones, cómo se obtienen y cuántas de ellas existen .*

La similitud con la geometría algebraica, no es una mera coincidencia, pues los métodos de ésta pueden utilizarse con éxito en los problemas diofánticos.

2. *La conjetura de Fermat .*

Hoy todos coincidemos en que Fermat dió un impulso decisivo a las ecuaciones diofánticas. Las proposiciones A, B, C y C' dan fe de que él entendía el problema en la misma forma que nosotros lo hacemos actualmente; nos limitaremos en este aparte a los problemas A y B, los cuales están íntimamente ligados entre sí. Cuando aquí hablemos de las soluciones de una ecuación, entenderemos siempre soluciones enteras, salvo indicación contraria. Demostremos en primer lugar la siguiente proposición debida a Diofanto [16; pág. 1056] :

Proposición 1. *La ecuación diofántica*

$$(2)\qquad x^2 + y^2 = z^2$$

admite un número infinito de soluciones $[x, y, z]$ *, todas ellas satisfaciendo las condiciones* $xyz \neq 0$ *y* x, y, z *primos entre sí de dos en dos. Estas soluciones están dadas por* $x = 2ab$, $y = a^2 - b^2$, $z = a^2 + b^2$ *o bien por* $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$ *, donde* a *y* b *son primos entre sí y sólo uno de ellos es impar.*

Demostración [5]. Es claro que (2) tiene una solución $[x, y, z]$, entonces 2 es un divisor de xyz. Por lo tanto, si $(x,y) = (x,z) = (y,z) = 1$ [6], sólo uno de los números x, y, z es par. Si suponemos que $x = 2m + 1$, $y = 2n+1$, $z = 2k$, encontramos que

$$x^2 + y^2 \equiv 2 \text{ (mód } 4) \quad \text{y} \quad z^2 \equiv 0 \text{ (mód } 4) \text{ [7]},$$

lo cual es imposible pues $2 \not\equiv 0$ (mód 4) (es decir, 4 no es un divisor de 2). Podemos, en consecuencia, suponer en primer lugar que $x = 2q$ y que z é y son impares. De modo que $z + y = 2m$ y $z - y = 2n$ son números pares, pudiéndose escribir (2) en la forma

$$x^2 = 4q^2 = z^2 - y^2 = (2m)\,(2n),$$

es decir, $q^2 = mn$. Pero $(m,n) = 1$ y, consecuentemente, $m = a^2$, $n = b^2$ con $(a,b) = 1$ [8]. De aquí resulta que

$$z = m + n = a^2 + b^2, \quad y = m - n = a^2 - b^2, \quad x = 2ab, \quad (a,b) = 1.$$

Finalmente, a y b no son simultáneamente impares, pues de otro modo 2 sería un divisor tanto de x como de y, lo cual no es posible ya que $(x,y) = 1$. Trastocando los papeles desempeñados por x é y en el anterior argumento, completamos la demostración de la proposición.

---

5) Esta demostración nos puede parecer hoy sencilla y tersa. Pero esto no fue siempre así: en el manuscrito más antiguo que copia la obra de Diofanto (éste se encuentra en El Escorial, España) aparece una nota marginal al lado de esta proposición: "Vete con Satanás, Diofanto, por la dificultad de tus problemas y en especial de éste".

6) La notación (a,b) designa el máximo común divisor de los números enteros a y b; por lo lo tanto, (a,b) = 1 indica que a y b son primos entre sí.

7) La notación $a \equiv b \text{ (mod } m)$ significa que $a-b$ es divisible por m. La negación se escribe $a \not\equiv b$ (mód m). Las siguientes relaciones se demuestran fácilmente: $a \equiv a$(mód m); $a \equiv b$(mód m) $\Rightarrow b \equiv a$(mód m); $a \equiv b$(mód m), $b \equiv c$(mód m) implican $a \equiv c$(mód m). Véanse, verbigracia, [5], [9], [12].

8) Estamos usando el siguiente hecho: si $x^2 = y_1 y_2 \cdots y_n$, donde los y_i son primos entre sí tomados de dos en dos, entonces $y_1 = n_1^2, \ldots, y_n = n_n^2$, donde los n_i son números enteros positivos, primos entre sí de dos en dos.

Proposición A. *Si los lados de un triángulo rectángulo son números enteros, entonces el área del triángulo no es un cuadrado perfecto.*

Demostración. Nos serviremos del método del descenso infinito ; de acuerdo con la carta de Fermat, bástanos demostrar que dado un triángulo rectángulo de lados enteros y cuya área sea un cuadrado, es posible construir un triángulo con la misma propiedad cuya área sea menor que la del primero. Por la proposición anterior y el teorema de Pitágoras, tenemos

$$(a^2 + b^2)^2 = (a^2 - b^2)^2 + (2ab)^2, \quad (a,b) = 1 ,$$

donde a y b son números enteros positivos, $a^2 + b^2$ representa la hipotenusa del triángulo, y $2ab$ y $a^2 - b^2$ sus catetos. Por hipótesis, el área $ab(a^2 - b^2)$ de este triángulo es un cuadrado perfecto, de donde resulta que $a = m^2$, $b = n^2$, $a^2 - b^2 = t^2$, donde m,n,t son enteros positivos , puesto que $(a,b) = (a,a^2 - b^2) = (b, a^2 - b^2) = 1$; es decir,

$$m^4 = t^2 + n^4 \tag{3}$$

tiene soluciones enteras que satisfacen $(m,n) = (m,t) = (n,t) = 1$. Ahora bien, si a es par, m es par y n y t son impares; si a es impar, b es par y, por lo tanto, m es impar y n es par; luego t es impar. Es decir, en cualquier caso, t es impar . Escribiendo

$$(m^2)^2 = t^2 + (n^2)^2$$

y usando de nuevo la proposición *1*, deducimos que $m^2 = \alpha^2 + \beta^2$; $n^2 = 2\alpha\beta$, $t = \alpha^2 - \beta^2$, donde $(\alpha, \beta) = 1$, y sólo uno de entre α y β es impar. Resulta entonces que $(1/2)\,\alpha\beta = (n/2)^2$ es el area del triángulo de lados m, α, β ; pero el área del triángulo original está dada por $ab(a^2 - b^2) = 2\alpha\beta(\alpha^2 - \beta^2)(\alpha^2 + \beta^2) > 0$ la cual es evidentemente mayor que $(1/2)\alpha\beta$.

Corolario 1. *La ecuación diofántica*

(3) $$m^4 = t^2 + n^4$$

no tiene soluciones enteras que satisfagan $(m,n) = (m,t) = (n,t) = 1$ y $mtn \neq 0$.

Demostración. En el curso de la demostración de la proposición anterior, hemos visto que si *(3)* admite soluciones con las condiciones dadas, existen entonces α y β tales que

$$m^2 = \alpha^2 + \beta^2,\ n^2 = 2\alpha\beta,\ t = \alpha^2 - \beta^2,\ \text{donde}\ (\alpha, \beta) = 1.$$

De $m^2 = \alpha^2 + \beta^2$ y observando que m, α, β son primos entre sí de dos en dos, deducimos nuevamente de la proposición 1 la existencia de enteros p y q, tales que, sin pérdida sustancial de generalidad, cumplen

$$m = p^2 + q^2,\ \beta = 2pq,\ \alpha = p^2 - q^2,\ (p,q) = 1.$$

De aquí resulta que

$$n^2 = 4pq\,(p^2 - q^2),$$

y, por lo tanto, existen r, s, u, enteros positivos, tales que

$$p = r^2,\ q = s^2,\ p^2 - q^2 = u^2 = r^4 - s^4,$$

con

$$(p,q) = (p,u) = (q,u) = 1.$$

Ahora bien,

$$m^2 = (p^2 + q^2)^2 = (r^4 + s^4)^2 > r^4,$$

es decir,

$$m > r^2 \geq r.$$

Por el descenso infinito, llegamos a una contradicción que demuestra el corolario.

Corolario 2. *La ecuación diofántica*

(4) $$x^4 + y^4 = z^4$$

no tiene soluciones enteras .

Demostración . Podemos suponer que $(x,y) = (y,z) = (x,z) = 1$. En tal caso, por el corolario 1,

$$z^4 = (x^2)^2 + y^4$$

no tiene soluciones de esta naturaleza, y, en consecuencia, tampoco *(4)* las tiene.

El anterior corolario, así como también la proposición *B*, son casos particulares de la siguiente proposición, conocida como *la conjetura de Fermat* ó *el último teorema de Fermat*.

La ecuación

(5) $$x^n + y^n = z^n$$

no tiene soluciones en números enteros x, y, z, *que satisfagan* $xyz \neq 0$, *si* $n > 2$.

Esto no es más que la versión contemporánea de la siguiente afirmación hecha por Fermat, en uno de los márgenes de su copia del libro de aritmética de Diofanto (edición de Bachet[9]): "*Cubum in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos et generaliter nullan in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere. Cujus rei demostrationem mirabilem sane detexi : hanc marginis exiguitas non caperet.*"

Veamos cómo es posible hacer algunas simplificaciones al enunciado de la conjetura. Si $n > 2$ no es un número primo, entonces n es una potencia de 2 o admite un divisor primo impar q. En el primer caso, $n = 4k$ y podemos escribir $(x^k)^4 + (y^k)^4 = (z^k)^4$, la cual no tiene soluciones enteras, en virtud del corolario 2 de la proposición *A*. En el segundo caso, $n = qr$ implica que $(x^r)^q + (y^r)^q = (z^r)^q$;

9) La edición de Bachet lleva el siguiente título : Diophanti Alexandrini Arithmeticorum libri sex: et de Numeris multangulis liber unus. Nunc primun graece et latini editi atque absolutissimis commentariis illustrati.

luego para demostrar que *(5)* no admite soluciones enteras, basta demostrar que no las tiene cuando $n = p$ es un primo impar. Pero en este caso, la conjetura es equivalente a la afirmación de que

(6) $$x^p + y^p + z^p = 0$$

no tiene soluciones enteras con $xyz \neq 0$, si p es un primo > 2 (si $p = 3$ recobramos la proposición *B)*. Podemos por último suponer que $(x,y) = (y,z) = (x,z) = 1$. Las triplas $[x, y, z]$ que satisfacen las anteriores condiciones y son soluciones de (6), se dicen *soluciones primitivas* .

Hasta hoy nadie ha demostrado la falsedad o la verdad del anterior aserto. Euler produjo una demostración incompleta para el caso $n = 3$ (Fermat en su carta sólo dice que posee una demostración por descenso infinito); intentando completar esta demostración, Kummer logra demostrar que para una cierta clase de exponentes, los llamados *números primos regulares* o *kummerianos* , la conjetura es correcta. Pero hoy sabemos ([7], [2: pág. 381]) que *el número de primos irregulares es infinito*; de modo que el resultado de Kummer es más bien "modesto" cuando aún no sabemos tan siquiera si el número de primos regulares es infinito [10]. Pero obteniendo este "modesto resultado", echó las bases de la teoría de los números algebraicos, la teoría de los ideales, y muchas otras que fundamentan la actual álgebra abstracta . La importancia de una demostración de la conjetura parece desvanecerse ante estos hechos.

En efecto, Kummer observó que es posible factorizar *(6)* en la siguiente forma :

(6') $$(x + y)(x + \zeta_p y) \ldots (x + \zeta_p^{p-1} y) = z^p ,$$

10) Kummer demostró la conjetura para algunas clases de primos irregulares.

donde ζ_p es una raiz primitiva p-ésima de *1*. Los elementos $x+\zeta_p^k\ (k=0,\ldots,n-1)$ pertenecen al *cuerpo* $\mathbb{Q}[\zeta_p]$ conformado por todos los números complejos de la forma

$$(7)\qquad a_o+a_1\zeta_p+\cdots+a_{n-2}\zeta_p^{p-2}\ ,\ a_k\in\mathbb{Q}\ ^{11)},$$

con respecto a la adición y multiplicación ordinarias de números complejos. $\mathbb{Q}[\zeta_p]$ se llama el *p-ésimo cuerpo ciclotómico* ; cuando todos los a_k en *(7)* son números enteros, decimos que *(7)* representa un *entero (algebraico)* de $\mathbb{Q}[\zeta_p]$; el conjunto $\mathbb{Z}[\zeta_p]=\{a_o+a_1\zeta_p+\cdots+a_{p-2}\zeta_p^{p-2}\ ;\ a_k\in\mathbb{Z}\}$ conforma un anillo, llamado el *anillo de los enteros (algebraicos)* de $\mathbb{Q}[\zeta_p]$. Kummer creyó que en $\mathbb{Z}[\zeta_p]$ existía una *factorización única de sus elementos en irreducibles (= primos)* y basándose en ella produjo una "demostración" de la conjetura de Fermat. Dedekind le señaló en donde residía la falla y para subsanarla Kummer introdujo sus *números ideales*, los cuales, más tarde, se convirtieron en nuestros *ideales*. Más preciso, un *ideal (fraccionario)* $\mathfrak{A}$ de $\mathbb{Q}[\zeta_p]$ que satisface las siguientes condiciones :

I1) Si $\alpha\ ,\ \beta\in\mathfrak{A}$, entonces $\lambda\alpha+\mu\beta\in\mathfrak{A}$ para cualesquiera λ y μ en $\mathbb{Q}[\zeta_p]$.

I2) Existe $\nu\in\mathbb{Z}[\zeta_p]$, $\nu\neq 0$, que cumple $\nu\alpha\in\mathbb{Z}[\zeta_p]$, para todo $\alpha\in\mathfrak{A}$.

El *producto de dos ideales* $\mathfrak{A}$ y $\mathfrak{B}$ se define como el conjunto

$$\mathfrak{A}\mathfrak{B}=\{\sum_{j=1}^{n}\alpha_j\beta_j\ ;\ \alpha_j\in\mathfrak{A},\ \beta_j\in\mathfrak{B}\ ,\ j\geq 1\}$$

Es fácil verificar que $\mathfrak{A}\mathfrak{B}$ es también un ideal de $\mathbb{Q}[\zeta_p]$ y que la multiplicación de ideales es asociativa y conmutativa. Dados dos ideales $\mathfrak{A}$ y $\mathfrak{B}$ es posible definir un único ideal $\mathfrak{C}$ tal que $\mathfrak{B}=\mathfrak{A}\mathfrak{C}$; este ideal lo notamos $\mathfrak{B}/\mathfrak{A}$; el ideal $(1)=\mathbb{Z}[\zeta_p]$ satisface $\mathfrak{A}\ (1)=\mathfrak{A}$ para todo ideal $\mathfrak{A}$, y al único ideal $\mathfrak{C}$ que satisface $(1)=\mathfrak{A}\mathfrak{C}$ le llamamos el inverso de $\mathfrak{A}$ y le denotamos por $\mathfrak{A}^{-1}$. Podemos

11) Usando $\zeta_n^{n-1}+\zeta_n^{n-2}+\cdots+\zeta_n+1=0$, se ve fácilmente que $\zeta_n^{n-1}\in\mathbb{Q}[\zeta_n]$.

concluir, pues, que *el conjunto* I *de todos los ideales de* $\mathbb{Q}[\zeta_p]$ *conforma un grupo abeliano con respecto a la multiplicación de ideales.*

Si el ideal $\mathfrak{A}$ está contenido en $\mathbb{Z}[\zeta_p]$, decimos que es un *ideal entero*; si $\mathfrak{A}\mathfrak{B}^{-1}$ es entero, decimos que $\mathfrak{B}$ *divide al ideal* $\mathfrak{A}$; una definición más : si los únicos divisores de un ideal entero $\mathfrak{P}$ son él mismo y *(1)*, decimos que $\mathfrak{P}$ es un *ideal primo de* $\mathbb{Q}[\zeta_p]$.

El teorema fundamental encontrado por Kummer y Dedekind y que sustituye la falta de factorización única en $\mathbb{Q}[\zeta_p]$, es el siguiente :

Todo ideal $\mathfrak{A}$ *de* $\mathbb{Q}[\zeta_p]$ *se escribe de manera única, salvo el orden de los factores, en la forma*

$$\mathfrak{A} = \mathfrak{P}_1^{\alpha_1} \ldots \mathfrak{P}_n^{\alpha_n}$$

donde los $\mathfrak{P}_j$ *son ideales primos y* $\alpha_j \in \mathbb{Z}$, *para* $j = 1, \ldots, n$.

Es decir, los ideales primos constituyen una base del grupo abeliano I. Los detalles de las anteriores afirmaciones pueden consultarse en [6: págs. 88-96 y 113-115]. Un ideal de la forma $\mathfrak{A} = \{\lambda\alpha ; \lambda \in \mathbb{Q}[\zeta_p]\}$ se denomina *principal* ; es fácil verificar que el conjunto P de todos los ideales principales es un subgrupo de I. El grupo cociente $I/P = C(\mathbb{Q}[\zeta_p])$ se llama *el grupo clasal* de $\mathbb{Q}[\zeta_p]$, y es un teorema fundamental de la teoría de los números algebraicos el hecho de que es un grupo finito, cuyo orden h se denomina el *número clasal* [6: págs. 119]. Si $p \mid h$, decimos que p es un *primo regular* o *kummeriano*. En particular, si $h = 1$, todo ideal de $\mathbb{Q}[\zeta_p]$ es principal y, por lo tanto, $\mathbb{Z}[\zeta_p]$ es un anillo factorial, es decir, sus elementos no nulos se pueden escribir unívocamente, salvo el orden y unidades, como un producto de elementos primos. El teorema demostrado por Kummer y mencionado anteriormente es el siguiente :

Teorema 1. *Si p es un primo regular, entonces (6) no tiene soluciones primitivas enteras con $xyz \neq 0$.*

Las demostraciones del anterior teorema utilizan en alguna forma el descenso infinito. (Véanse [5: chap. 11] y [2: chap. 5].) Kummer encontró también curiosas condiciones necesarias y suficientes para la regularidad de un primo. Así, por ejemplo, tenemos el siguiente

Teorema 2. *El primo $p \geq 3$ es regular si, y sólo si, el numerador de los números de Bernoulli $B_2, B_4, \ldots, B_{p-3}$ no es divisible por p.*

Los números de Bernoulli aparecen en varias partes de la matemática, como, por ejemplo, en

$$\frac{z}{e^z - 1} = 1 + \sum_{n=1}^{\infty} \frac{B_n}{n!} z^n .$$

Finalmente queremos indicar que los investigadores han encontrado conveniente distinguir dos casos para estudiar la conjetura :

I. $p \nmid xyz$

II. $p \mid xyx$

Con ayuda de las computadoras electrónicas se ha podido verificar que la conjetura es cierta hasta el primo $p = 253'747.889$, en el caso I, y hasta $p = 4.001$, en el caso II. (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 Bernouilliske 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 University Press, Cambridge, 1921.

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

13. R. Nougués, *Théoreme de Fermat, son histoire*, Vuibert, Paris, 1932.

14. O. T. O'meara, *Introduction to quadratic forms*, Springer-Verlag, Berlin, 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.