EL FINAL DE LA MATEMÁTICA HELENÍSTICA: DIOFANTO

Mariano Martínez Pérez
Facultad de Matemáticas
Universidad Complutense. Madrid

Desde finales del siglo II, con la muerte del gran Ptolomeo (ca. 180), hasta el año 529, en el que podemos considerar, siguiendo a Boyer, que se cierra el maravilloso milenio de matemática y filosofía griegas (véase al final), hay un intervalo de tres siglos y medio.

A este período vamos a dedicar estas dos charlas. No vamos, sin embargo, a tratarlo todo él con el mismo detalle por falta de tiempo para ello, pese a que presenta un gran interés. Se trata, en líneas generales, de un período de prolongada decadencia desde el punto de vista de la creación matemática, excluyendo desde ya a las dos figuras centrales (pero sólo a estas dos) que son Diofanto y Pappus de Alejandría, y ya se sabe que tales períodos de decadencia presentan siempre un peculiar y melancólico atractivo.

Me he decidido a dedicar una atención especial, que siempre resultará insuficiente, a la figura de Diofanto, por ser a la vez una de las más originales (lo que no significa de las más importantes ni de las más geniales) y de las menos conocidas de toda la historia de la matemática griega. De la obra de Pappus haremos unos comentarios mucho más breves, lo cual evidentemente no le hace justicia, pero esperamos que sea estudiado de manera especial en otra ocasión en este mismo Seminario.

I. Diofanto de Alejandría

De Diofanto sólo sabemos que vivió en Alejandría hacia el año 250, y que murió a los 84 años, si hemos de creer en la fidelidad de un conocido epigrama de la «Antología Griega» en forma de problema que hace referencia a él.

I.1. La Aritmética

Se trata de la más importante de las dos obras de Diofanto que nos han llegado, aunque sólo fragmentariamente. La *Aritmética* constaba originalmente de trece libros, de los que nos han llegado únicamente los seis primeros (un presunto séptimo libro de algunas ediciones resulta de dividir en siete partes el material de los seis mencionados). Los siete libros perdidos de la *Aritmética* lo fueron sin duda ya en la antigüedad. Según Tannery, la causa principal de esta pérdida fue que Hypatia sólo escribió comentarios de los seis primeros libros, con lo que los siete restantes primero cayeron en el olvido y finalmente se perdieron. Y concretamente no tenemos evidencia alguna de que los árabes conocieran ya más que los seis libros que nos han llegado.

Antes de entrar en el contenido de la *Aritmética* se impone de manera natural el problema de estimar la importancia de la pérdida de esos siete libros. Según Nesselmann, después de minuciosos estudios de la obra, podemos consolarnos con el hecho de que muy probablemente la pérdida es mucho menor que lo que podría indicar la relación de siete libros perdidos frente a seis conservados, y la razón principal que exhibe es la de que los libros perdidos no son los últimos de la obra, sino que la mayor parte caería casi con seguridad entre los libros 1 y 2 supervivientes (véase Heath, 3, vol. II, p. 450). Nos congratula que el códice más antiguo y a la vez el mejor de todos es el «Matritensis 48» (llamado A por Tannery), de la Biblioteca Real de Madrid, que data del siglo XIII. Por desgracia parece estar sensiblemente estropeado por algún desaprensivo que se dedicó a hacer correcciones sobre él, principalmente en los libros 1 y 2.

La *Aritmética* fue traducida al árabe por Qustá ibn Lúgá a mediados de la segunda mitad del siglo IX. De las ediciones modernas, una de las más famosas fue la de Bachet (1621) que publicó por primera vez el texto griego con traducción latina y notas; ésta fue la famosa edición utilizada por Fermat para dejar en ella anunciada su misteriosa «demostración» de su teorema o conjetura, como veremos más adelante. La edición standard hoy día de las obras de Diofanto es la de Tannery en dos volúmenes (Teubner, 1893, 1895). De las ediciones modernas, hemos utilizado las 2, 6, 7 y 8.

La originalidad de Diofanto en esta obra tiene un doble aspecto. El primero consiste en que se trata del único matemático griego (excluyendo quizás a los primeros pitagóricos) que no es un «geómetra», sino un «aritmético» en estado puro. Los problemas son todos de «teoría de números», incluso los que están disfrazados por un lenguaje aparentemente geométrico («Hallar un triángulo, rectángulo tal que...»). Como es bien sabido, a partir del descubrimiento de los segmentos inconmensurables, con la consecuencia de que los números no podían dar cuenta del continuo, la geometría pura se independizó de la aritmética y se convirtió en la auténtica reina de la matemática griega, dominándola prácticamente toda. Otra de las novedades importantes que introduce Diofanto es la siguiente. Los objetos propios de la artmética griega eran los números naturales y sus razones, que *no eran* números sino relaciones entre números («en cuanto al tamaño», nos dirá Euclides). Diofanto considera por primera vez a los números fraccionarios (positivos solamente, por supuesto) como auténticos números. Hay que recordar que la «manipulación» por parte de los egipcios y mesopotamios de los «números fraccionarios» en un sentido puramente «partitivo» (que sin duda es el mejor método de introducirlos a los niños), no tiene nada que ver con la matemática pura griega. Por otra parte, el reconocimiento pleno de los números racionales con su independencia «ontológica», hubo de esperar hasta el siglo XVII.

El punto de vista en el que se sitúa Diofanto le permite en primer lugar librarse de las limitaciones dimensionales de la geometría, donde sólo se podían «multiplicar» tres magnitudes, puesto que tres es la dimensión del espacio. Diofanto admite sin ningún problema productos y potencias hasta seis factores y sus inversos.

El segundo aspecto innovador de Diofanto, tan importante al menos como el primero, fue su introducción del primer simbolismo propiamente matemático. La matemática griega había carecido de cualquier tipo de simbolismo especial: era una matemática «retórica». Diofanto introduce un simbolismo adaptado al cálculo algebraico y muy flexible. Esta notación diofántica recibió el nombre de notación «sincopada» y, pese a sus indudables ventajas «algebraicas», se perdió inmediatamente después de Diofanto, al parecer, y ya ni siquiera la recuperaría la matemática árabe. Sólo durante el Renacimiento, desde finales del siglo XV hasta bien entrado el XVII, se volverá a introducir, lenta y trabajosamente la nueva notación algebraica, que culminará en 1637 con la de Descartes, que es ya la nuestra. Es muy educativo repasar algunos de los muchísimos intentos fallidos de construir una notación flexible para el cálculo algebraico. Se trata de un hecho que tuvo una enorme importancia en la evolución de toda la matemática posterior al siglo XVII, en lo que suele llamarse el proceso de «algebrización» de la matemática.

Los seis libros de la Aritmética conservados contienen unos 130 problemas resueltos, que resultan de muy difícil clasificación, exceptuado el principio general de que la resolución de los problemas anteriones suele facilitar la de los posteriores. Utilizando un criterio estricto podemos clasificar todos estos problemas en unos ¡50 tipos distintos!

El libro I contiene únicamente ecuaciones algebraicas determinadas. Los libros II al V están constituidos en su mayor parte por problemas indeterminados, en los que expresiones de primero o de segundo grado en dos o más incógnitas han de ser cuadrados o cubos. Por último, el libro VI se ocupa de triángulos rectángulos tratados de manera puramente aritmética, en los que alguna función lineal o cuadrática de los lados ha de ser igual a un cuadrado o a un cubo.

Los métodos de resolución de problemas de Diofanto

Los distintos métodos de Diofanto los podemos clasificar, siguiendo a Heath, de acuerdo con el tipo de ecuación o ecuaciones a que conducen, en dos grandes apartados: (A) Ecuaciones determinadas, y (B) Ecuaciones indeterminadas, y en cada caso según los grados de dichas ecuaciones.

(A) Ecuaciones determinadas

Obviamente Diofanto no tenía ninguna dificultad en resolver ecuaciones individuales de primero y de segundo grado, siempre que tuvieran raíces racionales positivas y fueran determinadas. Sólo hay un caso de ecuación cúbica en toda la *Aritmética*.

Un tipo especialmente sencillo de ecuaciones determinadas es el que se reduce, después de hacer operaciones a la fórmula

$$AX^n = B$$

o sea, a una «ecuación pura». Esta ecuación sólo es resoluble, evidentemente, si $\frac{B}{A}$ es una potencia n-ésima positiva.

En general, en un problema se presentan varias incógnitas, pero Diofanto las reduce hábilmente a una sola.

En los casos de ecuaciones cuadráticas Diofanto nos da sumariamente la raíz, o sin demasiadas explicaciones.

Vale la pena detenerse un momento a estudiar el caso de la cúbica. El problema 17 del Libro VI conduce a la ecuación

$$X^2+2x+3= X^3+3x - 3x^2 - 1$$

de la que Diofanto nos dice lacónicamente: «La solución es x=4». ¿De dónde la obtiene? Es fácil ver que la ecuación anterior se reduce a la

$$X^3+X= 4x^2+4$$

es decir

$$x(x^2+1)=4(x^2+1)$$

luego $x = 4$, puesto que las otras dos raíces, $x=\pm\, i$ no son de recibo.

(B) Ecuaciones indeterminadas

Se trata de unos cuantos casos particulares del caso general, que respondería a la forma

$$P_n(x,y)=0$$

donde P_n es un polinomio de grado n en las indeterminadas x e y con coeficientes racionales (o lo que es lo mismo, enteros).

Diofanto no estudia ningún caso de ecuación indeterminada lineal ($n=1$). (Los problemas del libro I que podrían haber conducido a ecuaciones indeterminadas lineales se ven convertidos en ecuaciones determinadas al suponer un valor arbitrario, pero fijo, para una de las dos incógnitas. Como es natural, el sentido que tiene resolver una ecuación indeterminada lineal

$$Ax+By=C$$

es la búsqueda de sus posibles soluciones *enteras,* puesto que para cada valor racional de x habrá trivialmente otro de y tal que (x,y) sea solución de la ecuación. Desde el punto de vista de Diofanto este caso no tiene interés alguno.

Ecuaciones indeterminadas de segundo grado

Todos los problemas se reducen a hallar valores de x que hagan el trinomio cuadrático Ax^2+Bx+C (o un caso particular con A o B o C nulos) un cuadrado perfecto, es decir a resolver la ecuación $Ax^2+Bx+C=y^2$ o bien a un sistema de dos ecuaciones simultáneas (nunca más de dos) de este tipo.

I Una sola ecuación

Hay varios subcasos:

1. Ecuaciones que siempre admiten soluciones racionales, como:

a) $A=C=0$, es decir, $Bx=y^2$. Diofanto se limita a tomar como y un cuadrado concreto, $y^2=m^2$, y se tiene simplemente $x=\dfrac{m^2}{B}$

b) $A=0$, es decir, $Bx+C=y^2$. Análogo al anterior.

c) $C=0$, es decir, $Ax^2+Bx=y^2$. Tomando $y=\frac{m}{n}x$ se tiene

$$Ax^2+Bx=x=\frac{m^2}{n^2}x^2 \qquad \text{luego } Ax+B=\frac{m^2}{n^2}x$$

(prescindiendo sin más de la raíz $x=0$), de donde,

$$x=\frac{Bn^2}{m^2-An^2}$$

2. Ecuaciones solubles racionalmente sólo bajo ciertas condiciones sobre los coeficientes:

Caso en que $B=0$, es decir, $Ax^2+C=y^2$

a) A es un cuadrado positivo a^2. Tomando $y=ax\pm m$
(el signo a elegir lo determinará el que el resultado final en x sea positivo), claramente

$$x=\frac{C-m^2}{\pm 2am}$$

al eliminarse astutamente el término cuadrático.

b) C es un cuadrado positivo C^2. Tomando $y=mx\pm c$ se tiene

$$x=\frac{\pm 2cm}{A-m^2}$$

c) Diofanto hace notar expresamente (en dos de los escasos pasajes «semiteóricos» de la *Aritmética*) en el Lema II al problema VI-12 y en el Lema al problema VI-15, dos situaciones en las que hay infinitas soluciones en x.

En el Lema a VI-15 dice que en el caso $Ax^2+C=y^2$, si se tiene una solución x_0, entonces se puede obtener otra mayor. Sea $Ax_0^2-C=q^2$; entonces tenemos $x=x_0+\xi$ e $y=q-k\xi$, con k entero. de $A(x_0+\xi)^2-C = (q-k\xi)^2$ se obtiene que

$$\xi=\frac{2(Ax_0+kq)}{k^2-A}$$

donde se requiere obviamente que $k^2>A$.

En el Lema a VI-12 hace lo mismo para el caso $Ax^2+C=y^2$, con tal de que $x=1$ sea una raíz, es decir, que $A+C$ sea un cuadrado perfecto, $A+C=q^2$. El proceso que sigue se basa en hacer $x=1+\xi$, y todo lo demás como en el caso anterior.

Dos observaciones al respecto de estos dos lemas, que no dejan muy bien parado el prestigio de Diofanto. La primera es la de que, en los problemas III-10 y III-11, ante las ecuaciones respectivas $52x^2+12=y^2$ y $266x^2-10=y^2$ Diofanto las declara «imposibles», pese a que $x=1$ es clara solución de ambas, y caen de lleno bajo el Lema a VI-12 (que, bien es cierto, es bastante posterior, pero ¡hay que repasar las cosas!). La segunda, quizás más grave que el «lapsus» anterior, consiste en la observación de que el procedimiento que se aplica en los dos Lemas a VI-15 y a VI-12 vale también para el caso general

$$Ax^2+Bx+C=y^2$$

sin *ninguna* restricción sobre los coeficientes, como puede comprobar trivialmente el lector.

En este mismo contexto, resulta en cambio notable la observación de Diofanto al problema VI-14, en el sentido de que la ecuación $Ax^2-C^2=y^2$ es imposible, *salvo que* A *sea suma de dos cuadrados*, cosa de comprobación inmediata.

Consideremos de nuevo la ecuación general

$$Ax^2+Bx+C=y^2$$

sabemos que se puede eliminar siempre el término de primer grado mediante un simple cambio de variable $x=z+h$, pero Diofanto aplica directamente a la ecuación completa la estrategia de los casos anteriores para $B=0$

a) A= cuadrado positivo (problemas II-20, 21, etc.)
b) C= cuadrado positivo (problemas IV-8, 9, etc.), y un tercero nuevo
c) cuando B^2-4AC = cuadrado positivo (problema IV-31, sin mencionarlo).

II Sistemas de dos ecuaciones

Se trata de hallar valores de x que hagan simultáneamente cuadrados perfectos a dos expresiones en x lineales o cuadráticas.

Sistemas de dos ecuaciones de primer grado

Diofanto aplica un método más o menos general para resolver un sistema de la forma

$$\left.\begin{array}{l}\alpha x+a=u^2\\ \beta x+b=w^2\end{array}\right\}$$

según los coeficientes. Se basa en la identidad, muy útil para él,

$$u^2-v^2=(u+v)(u-v)$$

Si es posible factorizar la diferencia u^2-v^2
es decir, $u^2-v^2=(u+v)(u-v)=pq$, entonces podemos escribir

$$\left.\begin{array}{l}u+v=p\\ u-v=q\end{array}\right\}$$

luego

$$\left.\begin{aligned} u&=\frac{1}{2}\ (p+q) \\ v&=\frac{1}{2}\ (p-q) \end{aligned}\right\}$$

es decir,

$$u^2=\alpha x+a=\frac{1}{4}(p+q)^2$$

de donde resulta, haciendo cuentas

$$(\alpha-\beta)^2x^2+2[(\alpha-\beta)(a-b+p^2)-2p^2\alpha]x+[p^4-2p^2(a+b)+(a-b)^2]=0$$

Hay dos casos en los que esta ecuación se reduce de grado:

i) $\alpha=\beta$

ii) $p^4-2p^2(a+b)+(a-b)^2=0$

o bien $[p^2-(a+b)]^2=4ab$

luego *ab* debe ser un cuadrado; es decir, o bien *a* y *b* son cuadrados, o la razón de *a* a *b* es la de un cuadrado a otro,

$$\frac{a}{b}=\frac{\gamma^2}{s^2}$$

Es interesante que al caso i) se reduce el de que $\dfrac{\alpha}{\beta}=\dfrac{m^2}{n^2}$ puesto que, en vista de que $\alpha n^2=\beta m^2$ nos queda nuestro sistema en la forma

$$\left.\begin{aligned} \alpha n^2x+a'&=u'^2 \\ \beta m^2x+b'&=w'^2 \end{aligned}\right\} \qquad (1)$$

y la ecuación anterior es ahora lineal.

En el caso ii), si $a=c^2$ y $b=d^2$ nos queda

$$\left.\begin{aligned} \alpha x+c^2&=u^2 \\ \beta x+d^2&=w^2 \end{aligned}\right\}$$

o, equivalentemente

$$\left.\begin{aligned} \alpha d^2x+c^2d^2&=u'^2 \\ \beta c^2x+c^2d^2&=w'^2 \end{aligned}\right\} \qquad (2)$$

La manera de resolver el sistema (1) es ahora claro; restando

$$u'^2-w'^2=a'-b'=p.q$$

luego

$$\left.\begin{aligned} u'+w'&=p \\ u'-w'&=q \end{aligned}\right\}$$

de donde

$$u'^2=\frac{1}{4}(p+q)^2$$

es decir

$$\alpha n^2x+a'=\frac{1}{4}(p+q)^2$$

$$x=\frac{\frac{1}{4}(p^2+q^2)-\frac{1}{2}(a'+b')}{\alpha n}$$

pudiéndose elegir los factores p y q de cualquier manera, con tal que x sea positivo. Como ejemplo puede servir el problema IV-32, que conduce a las ecuaciones

$$\left.\begin{aligned} 65-6x&=u^2 \\ 65-24x&=w^2 \end{aligned}\right\}$$

En el caso ii) podemos pasar del sistema

$$\left.\begin{aligned} \alpha x+c^2&=u^2 \\ \beta x+d^2&=w^2 \end{aligned}\right\}$$

al

$$\left.\begin{aligned} \alpha d^2x+c^2d^2&=u'^2 \\ \beta c^2x+c^2d^2&=w'^2 \end{aligned}\right\}$$

Supongamos que u' es el mayor. La diferencia es $=(\alpha d^2-\beta c^2)x$

Sean los factores px y q Es decir

$$\left.\begin{aligned} u'^2&=\frac{1}{4}(px+q)^2 \\ w'^2&=\frac{1}{4}(px-q)^2 \end{aligned}\right\}$$

y x se calcula de la ecuación

$$\alpha d^2x+c^2d^2=\frac{1}{4}(px+q)^2$$

que da

$$p^2x^2+2x(pq-2\alpha d^2)+q^2-4c^2d^2=0$$

es decir, dado que $pq=(\alpha d^2-\beta c^2)$

$$p^2x^2-2x(\alpha d^2+\beta c^2)+q^2-4c^2d^2=0$$

y para que se reduzca a una ecuación sencilla, Diofanto exige que se anule el término independiente, o lo que es lo mismo, que $q^2=4c^2d^2$ o $q=2cd$

Así, nuestro método nos da sólo *una solución* del sistema, al restringirse *q* al valor 2cd, solución que es

$$x=\frac{2(\alpha d^2+\beta c^2)}{p^2} = \frac{8c^2d^2(\alpha d^2+\beta c^2)}{(\alpha d^2-\beta c^2)^2}$$

Este método lo usa Diofanto una sola vez en un caso particular (problema IV-39) con $c^2 = d^2$, y las ecuaciones son

$$\left.\begin{array}{l} 8x+4=u^2 \\ 6x+4=w^2 \end{array}\right\}$$

Otra posibilidad para la forma original de ii)

$$\left.\begin{array}{l} \alpha x+c^2=u^2 \\ \beta x+d^2=w^2 \end{array}\right\}$$

es la de tomar directamente

$$u^2-w^2=(\alpha-\beta)x+(c^2-d^2)=pq$$

con,

$$p=c\pm d$$

es decir,

$$q=\frac{\alpha-\beta}{c\pm d}x+c\mp d$$

y

$$u^2=\alpha x+c^2=\frac{1}{4}\left(\frac{\alpha-\beta}{c\pm d}\,x+2c\right)^2$$

luego

$$\left(\frac{\alpha-\beta}{c\pm d}\right)^2 x+4\left(\frac{c(\alpha-\beta)}{c\pm d}-\alpha\right)=0$$

lo que puede dar dos soluciones en *x* si $c>d$. Como ejemplo nos vale el problema III-15, con el sistema de ecuaciones

$$\left.\begin{array}{l} 10x+9=u^2 \\ 5x+4=w^2 \end{array}\right\}$$

Como hemos dicho ya, q Diofanto no parece preocuparle el obtener otras soluciones a partir de una dada $x=a$, excepto en algunos casos de ecuaciones simples, pero *no* en sistemas. Según Heath, Fermat fue el primero en darse cuenta de que siempre se podía hacerlo también en este caso, sustituyendo x por $a+\xi$ en las dos ecuaciones, pudiendo llegarse así a una raíz positiva incluso si a fuese negativa. Diofanto usa un proceso alternativo en un único caso, el problema IV-39, para evitar las dificultades que plantearía el método usual. El sistema es el

$$\left.\begin{aligned} hx+n^2&=u^2 \\ (h+f)x+n^2&=w^2 \end{aligned}\right\}$$

Se trata de un sistema de la forma

$$\left.\begin{aligned} 6x+4&=u^2 \\ 8x+4&=w^2 \end{aligned}\right\}$$

Llamemos

$$A=(h+f)x+n^2, \qquad B=hx+n^2, \qquad C=n^2$$

entonces, supongamos

$$\begin{gathered} B=hx+n^2=(y+n)^2 \\ hx=y^2+2ny \end{gathered}$$

y

$$A=\frac{f}{h}(y^2+2ny)+(y+n)^2$$

a la que hay que obligar a ser un cuadrado (B ya lo es por hipótesis).

Supongamos que sea

$$\left(1+\frac{f}{h}\right)y^2+2n\left(\frac{f}{h}+1\right)y+n^2=(py-n)^2$$

ecuación lineal en y. Variando p podemos obtener diferentes valores de y, y por lo tanto de x.

Sistemas de dos ecuaciones de segundo grado

De la forma general

$$\left.\begin{aligned} Ax^2+Bx+C&=u^2 \\ A'x^2+B'x+C'&=w^2 \end{aligned}\right\}$$

sólo estudia Diofanto tres tipos muy particulares, para los que se pueden generalizar fácilmente los procedimientos que también funcionaban en el caso de los sistemas lineales.

Primer tipo:

$$\left.\begin{array}{r}\varphi^2x^2+\alpha x+a+u^2\\ \varphi^2x^2+\beta x+b=w^2\end{array}\right\}$$

entonces

$$u^2-w^2=(\alpha+\beta)x+(a-b)=p.q$$

poniendo

$$\left.\begin{array}{l}p=a-b\\[2ex] q=\dfrac{\alpha-\beta}{a-b}\,x+1\end{array}\right\}$$

luego

$$u^2=\varphi^2x^2+\alpha x+a=\frac{1}{4}\left(\frac{\alpha-\beta}{a-b}\;x+1+a-b\right)^2$$

y para asegurar la racionalidad de x impone Diofanto que sea

$$\varphi=\frac{1}{2}\;\frac{\alpha-\beta}{a-b}$$

en el único problema de este tipo en que $a\neq b$, que es el problema III-13.

En todos los demás casos se tiene que $a=b$, con lo que la diferencia de los cuadrados se reduce a

$$u^2-w^2=(\alpha-\beta)x=p.q$$

con

$$\left.\begin{array}{l}p=\dfrac{\alpha-\beta}{2\varphi}\\[2ex] q=2\varphi x\end{array}\right\}$$

luego

$$u^2=\varphi^2x^2+\alpha x+a=\frac{1}{4}\left(\frac{\alpha-\beta}{2\varphi}+2\varphi x\right)^2$$

es decir

$$\frac{\alpha+\beta}{2}\;x-\left(\frac{\alpha-\beta}{4\varphi}\right)^2+a=0$$

Un buen ejemplo es el problema VI-8, que conduce al sistema

$$\left.\begin{aligned} x^2+14x+1=u^2 \\ x^2+1=w^2 \end{aligned}\right\}$$

Segundo tipo:

$$\left.\begin{aligned} x^2+\alpha x+a=u^2 \\ \beta x+a=w^2 \end{aligned}\right\}$$

Es decir, una de las ecuaciones es lineal y $a=b$. Entonces

$$u^2 - w^2=x^2+(\alpha - \beta)x=p.q$$

con

$$\left.\begin{aligned} &p=x \\ &q=x+(\alpha - \beta) \end{aligned}\right\}$$

y ahora

$$w^2=\beta x+a=\frac{1}{4}(\alpha - \beta)^2$$

que nos da x inmediatamente. Ejemplo puede ser el problema VI-22, con el sistema

$$\left.\begin{aligned} x^2 - 6144x+1048576=u^2 \\ x+64=w^2 \end{aligned}\right\}$$

Tercer tipo:

$$\left.\begin{aligned} \alpha x^2+ax=u^2 \\ \beta x^2+bx=w^2 \end{aligned}\right\}$$

que no puede resolverse como los casos anteriores, y para el cual Diofanto inventa un camino distinto que funciona bien en algunos casos particulares.

Consideremos que

$$u^2=m^2x^2$$

cosa que siempre será posible tomando

$$m=\frac{u^2}{x^2}$$

entonces, de la primera ecuación

$$x=\frac{a}{m^2 - \alpha}$$

y sustituyendo en la segunda

$$\beta\left(\frac{a}{m^2-\alpha}\right)^2+\frac{ba}{m^2-\alpha}=w^2$$

$$\frac{\alpha^2\beta+ba(m^2-\alpha)}{(m^2-\alpha)^2}=w^2$$

para lo cual basta que el numerador sea un cuadrado

$$abm^2+a(a\beta-\alpha b)=y^2$$

ecuación en *m* que podrá resolverse o no. Casos favorables son aquellos en que $\frac{\alpha\beta-ab}{a}$ o $\frac{a}{b}$ sean cuadrados. un ejemplo puede ser el problema VI-14

$$\left.\begin{array}{l}6x^2-5x=u^2\\6x^2-3x=w^2\end{array}\right\}$$

Ecuaciones indeterminadas de grado mayor que dos

a) Ecuaciones individuales

Hay en la *Aritmética* dos clases de problemas que conducen a ecuaciones individuales de grado mayor que dos.

Primera clase:

$$Ax^n+Bx^{n-1}+\ldots+Kx+L=y^2$$

con $2<n\leqslant 6$ De ella podemos encontrar seis tipos distintos.

Tipo 1: Ecuación

$$Ax^3+Bx^2+Cx+d^2=y^2$$

Podemos hacer $y=mx+d$ y hallar *m* de manera que el coeficiente de *x* en la ecuación resultante se anule, lo cual implica que

$$m=\frac{c}{2d}$$

con lo que Diofanto se sitúa ingeniosamente en la ecuación

$$Ax+B=\frac{c^2}{4d^2}$$

luego

$$x=\frac{c^2-4d^2B}{4d^2A}$$

Un buen ejemplo lo tenemos en el problema VI-18

$$X^3 - 3x^2+3x+1=y^2$$

Diofanto podría haber mejorado la jugada tomando

$$y=m^2x^2+nx+d$$

para eliminar los términos en x de grados 1 y 2, pero no lo hace.

Tipo 2: Ecuación

$$Ax^4+Bx^3+Cx^2+Dx+E=y^2$$

Los únicos casos que estudia Diofanto son los de la forma particular

$$a^2x^4+Bx^3+Cx^2+Dx+e^2=y^2$$

en la que, haciendo

$$y=ax^2+kx+e$$

se puede calcular k para que desaparezca el término de grado 1 o de grado 3 en x, lo que reduce de nuevo la ecuación. Un ejemplo puede ser el problema IV-28, con la ecuación

$$9x^4 - 4x^3+6x^2 - 12x+1=y^2$$

Tipo 3: Ecuación bicuadrada

$$Ax^4 - Cx^2+E=y^2$$

Se trata, con el tipo 4 siguiente, de dos casos particularmente difíciles, incluso si A o E o ambas son cuadrados perfectos.

Los casos concretos que aparecen obedecen, de hecho, a la forma

$$a^2x^4 - c^2x^2+e^2=y^2$$

que Diofanto transforma con ingenio en la

$$a^2x^2 - c^2+\frac{e^2}{x^2} = y'^2$$

haciendo entonces $y'=ax$ o bien $y'=\frac{e}{x}$ resultan raícez racionales. Un ejemplo lo tenemos en el problema V-28:

$$\frac{25}{4}x^2 - 25+\frac{25}{4x^2} =y^2$$

donde Diofanto supone

$$y^2=\frac{25}{4}x^2$$

Tipo 4: Ecuación

$$Ax^4+E=y^2$$

Pese al aparente aspecto sencillo, esta ecuación se le resiste a Diofanto hasta el punto de que en el problema V-29 se enfrenta con el caso $x^4+97=y^2$, haciendo $y=x^2-10$ lo que le lleva a

$$x^2=\frac{3}{20}$$

que naturalmente no es ninguna solución racional. En vez de intentar otra sustitución, abandona esa ecuación por otra, la $x^4+337=y^2$ en la que haciendo $y=x^2-25$ obtiene con éxito

$$x=\frac{12}{5}$$

A esta especie de «regula falsi» la llamó Nesselman «cálculo hacia atrás»

Tipo 5: Ecuación de la forma

$$x^6-Ax^3+Bx+C^2=y^2$$

Basta hacer $y=x^3+c$ con lo que queda

$$-Ax^2+B=2cx^2$$

es decir

$$x^2=\frac{B}{A+2c}$$

que da una solución racional sólo si $\frac{B}{A+2c}$ es un cuadrado perfecto, claro.

Tipo 6: Ecuación

$$x^6-Ax^3+Bx+C^2=y^2$$

con $\frac{B}{A+2C} \neq$ un cuadrado. Se da el caso en el problema IV-18 con la ecuación

$$x^6-16x^3+x+64=y^2$$

Ante las dificultades Diofanto, en un «cálculo hacia atrás», consigue sustituir esa ecuación por la

$$x^6-128x^3+x+4096=y^2$$

que ya es del tipo 5, y haciendo $y=x^3+64$ resulta $x=\frac{1}{16}$

Segunda clase

Se trata de ecuaciones de la forma

$$Ax^n+Bx^{n-1}+.......+Kx+L=y^3$$

Excepto casos tan sencillos como $Ax^2=y^3$, $Ax^4=y^3$ donde lo único que hay que hacer es suponer $y=mx$, los demás que aparecen en Diofanto son de una de las dos formas:

$$Ax^2+Bx+C=y^3$$
$$Ax^3+Bx^2+Cx+D=y^3$$

1. Ecuación

$$Ax^2+Bx+C=y^3$$

Sólo se encuentra en los problemas VI-1 y VI-17, y los datos parecen claramente preparados «ad-hoc» para la sencillez del resultado.

2. Ecuación

$$Ax^3+Bx^2+Cx+D=y^3$$

Si *A* o *D* son cubos, la solución es sencilla. En efecto, si $A=a^3$ basta con poner

$$y=ax+\frac{B}{3a^2}$$

para simplificar. Si $D=d^3$ ponemos

$$y=\frac{C}{3d^2}\ x+d$$

y ocurre lo mismo.

Si ocurren las dos cosas al mismo tiempo, podemos hacer cualquiera de los dos cambios anteiores o mejor hacer simplemente $y=ax+d$ para simplificar. Parece ser que Diofanto sólo conocía este último caso, porque en el problema IV-27 rechaza como imposible la ecuación

$$8x^3 - x^2+8x - 1=y^2$$

porque al hacer $y=2x - 1$ da el valor negativo

$$x= -\frac{2}{11}$$

mientras que cualquiera de los dos primeros métodos nos da una raíz racional positiva.

b) Sistemas de dos ecuaciones

Hay unos pocos ejemplos en los que, de dos funciones de *x*, una hay que hacerla un cuadrado y la otra un cubo, para el mismo valor racional de *x*. La mayoría de los casos son muy sencillos por ejemplo, en el problema VI-19 hay que resolver el sistema

$$\left.\begin{array}{r}4x+2=y^3\\2x+1=y^2\end{array}\right\}$$

y obviamente

$$y^3=2z^2 \quad y \quad z=2$$

Más complicado es el caso de VI-21, que nos conduce al sistema

$$2x^2+2x=y^2$$
$$x^3+2x^2+x=z^3$$

Diofanto supone que y=mx, luego $x=\frac{2}{m^2-2}$ y se tiene

$$\left(\frac{2}{m^2-2}\right)^3+2\left(\frac{2}{m^2-2}\right)^2+\frac{2}{m^2-2}=z^3$$

o

$$\frac{2m^4}{(m^2-2)^3}=z^3$$

y para hacer $2m^4$ un cubo, tenemos que hacerlo a 2m poniendo, por ejemplo, m=4, lo que da

$$x=\frac{1}{4}$$

Los casos más generales resultarían, evidentemente, demasiado difíciles.

II. Unas breves palabras sobre Pappus

Tal como hemos mencionado al comienzo, los cuatro o cinco últimos siglos de la matemática helenística significan un descenso notable en el nivel teórico, si los comparamos con la época gloriosa de Euclides, Arquímedes y Apolonio.

No obstante, dos figuras destacan míticamente del nivel general. De la primera, Diofanto, hemos hablado con detalle en las páginas anteriores. La segunda es Pappus de Alejandría, que debió vivir en torno al año 350 d.c.

La obra principal de Pappus es su *Synagoge* o *Colección Matemática*, una obra en 8 libros (de los que se han perdido el primero y buena parte del segundo).

Los seis libros restantes son un tratado de geometría de un tipo más enciclopédico que sistemático, en el que se tratan temas muy variados, sin pretender unidad alguna.

A parte de los resultados concretos incluidos por Pappus en su obra, ésta tiene una gran importancia como recopilación «histórica» de problemas como los tres clásicos, así como la recuperación de partes de obras que se han perdido (especialmente en el famoso libro 7).

Pappus es así el último de los grandes matemáticos griegos.

Después de él se producirá una verdadera avalancha de enciclopedistas, comentaristas, etc. de los clásicos (Proclo, Simplicio, Teón, Hypatia), que significará el auténtico final de más de un milenio de la maravillosa matemática y filosofía griega, lo cual ocurrirá a lo largo del siglo V de nuestra era.

BIBLIOGRAFÍA

BASMAKOVA, I.G. «Diophant und diophantische Gleichungen», col. UTB, n.º 360 (Birkhäuser, Basel, 1974).

HEATH, T.L «Diophantus of Alexandria: A Study in the History of Greek Algebra» (Dover, New York, 1964).

HEATH, T.L. «A History of Greek Mathematics: vol. II: From Aristarchus to Diophantus» (Dover, New York, 1981).

MIDONICK, H. «The Treasury of Mathematics» (Peter Owen, Londres, 1965).

MORDELL, L.J. «Diophantine Equations», col. Pure and Applied Mathematics, n.º 30 (Academic Press, New York, 1969).

RASHED, R. «Diophante: Les Arithmétiques», tome III, Livre IV; tome IV, Livres V, VI, VII, col. des Universités de France (Les Belles Lettres, Paris, 1984).

SESIANO, J. «Books IV to VII of Diophantus» Aritmetica in the arabic translation attributed to Qusta ibn Luga», col. Sources in the History of Mathematics and Physical Sciences, n.º 3 (Springer Verlag, New York, 1982).

VER EECKE, P. «Diophante d'Alexandrie: Les six Livres Arithmétiques et le Livre des Nombres Polygones» (Albert Blanchard, Paris, 1959).