Premios del Departamento de Matemáticas de la Universidad Autónoma de Madrid para Estudiantes de Secundaria

Cuarta Edición, 2009/2010

TRABAJO: Lo racional no interesa

GANADOR EN LA CATEGORÍA DE BACHILLERATO

AUTORES:

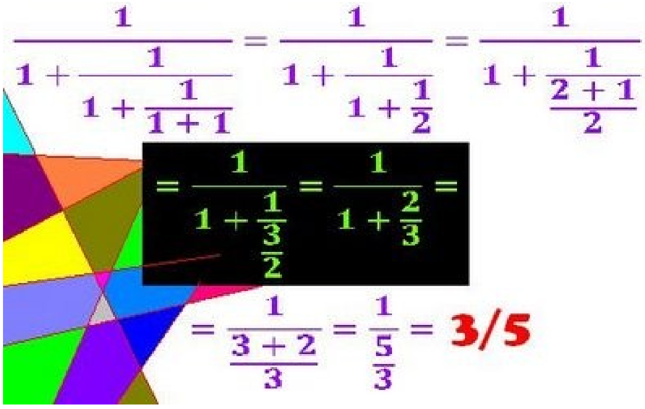
- Javier Alcaide Pérez
- Helia Santiago Colomer

TUTORA:

- Ángela Vallego Martín Albo

CENTRO: I.E.S. El Escorial (El Escorial, Madrid)

LO RACIONAL NO INTERESA



Javier Alcaide Pérez
Helia Santiago Colomer

IES EL ESCORIAL

ÍNDICE

1. INTRODUCCIÓN

> *"Si,…, el conocimiento útil es aquel que probablemente va a contribuir al bienestar material de la humanidad, ahora o en el futuro próximo, de tal forma que la mera satisfacción intelectual resulte irrelevante, entonces la mayor parte de las matemáticas superiores son inútiles"*
>
> G.H. Hardy

En su libro "Apología de un matemático" Hardy *[Referencia de G. H. Hardy]* dice que hay dos tipos de matemáticas, las "auténticas, hechas por auténticos matemáticos", y las "triviales". En cierta manera, identifica la matemática trivial con la matemática útil y defiende con vehemencia las "matemáticas auténticas" aún reconociendo la inutilidad de la mayor parte de ellas. Dice Hardy que las auténticas matemáticas perdurarán a lo largo del tiempo pues "como ocurre con la mejor literatura, puede causar una satisfacción intensa a miles de personas miles de años después de ser creadas".

Desde este punto de vista, el tema de nuestra investigación pertenece a esa parte de la matemática que, según Hardy, se podría llamar inútil. Pretendemos exponer una pequeñísima parte de auténtica matemática, la que se refiere a un tipo singular de ecuaciones, las llamadas ecuaciones diofánticas. El trabajo nos ha salido salpicado de referencias a algunos matemáticos importantes que han tenido que ver con este tema, ya sea por sus aportaciones matemáticas a él o simplemente porque se han interesado en el asunto, y nos ha parecido adecuado introducir en el texto una referencia cruzada que conduzca a una pequeña reseña de la vida de ese matemático. Por ejemplo, Hilbert fue un gran matemático que tuvo algo que ver con las ecuaciones diofánticas. Veamos:

En agosto de 1900 David Hilbert *[Referencia de David Hilbert]* propuso a la comunidad matemática, reunida en el Congreso Internacional de Matemáticas de París una serie de problemas, concretamente 23, cuya resolución podría encuadrarse perfectamente en lo que Hardy llama las auténticas matemáticas. Se trataba de problemas que apenas conectaban con la realidad, que no resolvían problemas prácticos, pero que preocupaban mucho a los matemáticos teóricos.

El décimo problema de Hilbert planteaba:

Dada una ecuación diofántica cualquiera, ¿existe algún algoritmo que permita decidir si esa ecuación tiene o no tiene soluciones enteras?

Pero ¿qué es una ecuación diofántica?

El nombre a estas ecuaciones fue dado en honor de Diofanto [Referencia de Diofanto] de Alejandría, matemático de la "Edad de Plata" de la matemática griega (época que va desde el 250 al 350 d. C. aprox.), conocido como el padre del Álgebra. Actualmente, se llama ecuación diofántica a una ecuación con una o varias incógnitas, cuyos coeficientes son todos números enteros, y de la que se buscan todas las soluciones que sean números enteros. Por ejemplo:

$5x+10 = 0$ es una ecuación diofántica con una incógnita. Su solución es x = –2 porque 5·(-2) + 10 = 0, y esta solución es única.

$15x + 10y – 20 = 0$ es una ecuación diofántica con dos incógnitas. Una de sus soluciones es x = 2 y = –1, porque 15·2 + 10·(–1) – 20 = 0; pero esta ecuación tiene muchas mas soluciones. De hecho, tiene infinitas soluciones.

$3x^2 – 6y^2 + 4x – 47 = 0$ es una ecuación diofántica con dos incógnitas. Una de sus soluciónes es x = 1 y = 9.

El reto que Hilbert planteó cuando formuló su décimo problema, era el de encontrar un procedimiento automático que permita decidir en un número finito de pasos (algoritmo) si una ecuación diofántica tiene o no tiene soluciones enteras.

Obsérvese que Hilbert no se interesaba tanto por las soluciones como por si se podía decidir con antelación la existencia de ellas.

Después de un largo proceso en el que intervinieron varios matemáticos, Matiyasevich [Referencia de Yuri Matiyasevich] demostró en 1970 que no existe tal algoritmo.

Eso no quiere decir que, a lo largo de la historia de las Matemáticas, no se haya demostrado que determinados grupos de ecuaciones diofánticas tienen solución. Es más, se ha demostrado, para ciertos tipos, cómo determinar si existen o no soluciones enteras (es decir lo que quería Hilbert para cualquier ecuación diofántica) y cómo encontrar esas soluciones.

2. OBJETIVOS DEL TRABAJO.

- Presentar algunos casos de ecuaciones diofánticas de las que se puede decidir si tienen o no solución, y cuántas y cómo son, en caso de que las haya, dichas soluciones.
- Entender y exponer las demostraciones de los resultados que se mencionen de forma completa y clara.
- Conocer los detalles generales de la vida de algunos matemáticos que han tenido que ver de una u otra forma con las ecuaciones diofánticas.

Hemos resaltado en color azul los resultados importantes y hemos sombreado en gris las demostraciones, todo ello con el objetivo de facilitar una lectura más rápida, pudiendo saltarse las partes grises si así se desea o buscar fácilmente uno de los resultados anteriores en el texto.

3. ECUACIONES EN UNA VARIABLE

3.1. ECUACIONES DE PRIMER GRADO.

Las ecuaciones con una incógnita de la forma $ax + b = 0$, con $a, b \in Z$, siempre tienen una solución: $x = -\frac{b}{a}$, que, en el contexto de las ecuaciones diofánticas, sólo nos interesará si $a|b$ (b es divisible entre a) lo que implicaría $\frac{b}{a} \in Z$. Es decir:

3.1.1.

La ecuación $ax+b = 0$ con $a,b \in$ Z, tiene solución entera si $a \mid b$ y esa solución es $x = -\frac{b}{a}$

Por ejemplo la ecuación 5x – 25 = 0 tiene solución entera x = 5 (observamos que $5|25$), mientras que la ecuación 4x + 21 = 0 carece de estas soluciones (observamos que 21 no es divisible entre 4).

3.2. ECUACIONES DE GRADO SUPERIOR A UNO

Una ecuación de la forma $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$ *, con* $a_n \neq 0$ *y* $a_i \in Z$ *,* $0 \le i \le n$ puede tener soluciones enteras, pero estarán caracterizadas por el siguiente teorema:

3.2.1.

x es solución entera de $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0 \Rightarrow$ x divide a a_0

El resultado anterior es lo que se llama una condición necesaria pero no suficiente, es decir, el teorema no asegura que los divisores del término independiente sean soluciones de la ecuación. Como dicen algunos profesores, sólo son candidatos. Por ejemplo, la ecuación $x^2 + 1 = 0$ sólo tiene como soluciones a $x = \pm i$, que no son números enteros (son números complejos).

Los divisores del término independiente en la ecuación $x^5 + 4x^2 - 3 = 0$ son ± 1 y ± 3, pero de ellos sólo es solución $x = -1$.

Demostración

Si x es solución entera de la ecuación $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$ entonces, $a_0 = -a_n x^n - a_{n-1} x^{n-1} - \dots - a_1 x = -x(a_n x^{n-1} + a_{n-1} x^{n-2} + \dots\dots + a_1)$

Como $a_i \in Z$, $a_n x^{n-1} + a_{n-1} x^{n-2} + \dots + a_1$ es un número entero y por tanto, a_0 es divisible entre x, ya que se puede expresar como producto de x por un número entero.

4. ECUACIONES LINEALES EN DOS VARIABLES

La forma general de las ecuaciones que vamos a estudiar en este apartado es

$ax + by = c$, con $a,b,c \in Z,\ \ a \neq 0\ \ y\ \ b \neq 0$

4.1.

Sean $a,b,c \in Z,\ \ a \neq 0\ \ y\ \ b \neq 0$. $ax + by = c$ tiene solución entera $\Leftrightarrow$ $mcd(a,b) | c$

Demostración

Llamemos $m.c.d.(a,b) = d \Rightarrow d | a$ y $d | b \Rightarrow a = a_1 d$ y $b = b_1 d$, con a_1 y b_1 primos entre sí (de lo contrario d no sería el mcd de a y b).

$\Rightarrow$ Supongamos que $x = x_0$ e $y = y_0$ es una solución de la ecuación $ax + by = c \Rightarrow ax_0 + by_0 = a_1 d x_0 + b_1 d y_0 = d(a_1 x_0 + b_1 y_0) = c$, lo cual implica que $d | c$ (pues $\exists\ a_1 x_0 + b_1 y_0 \in \mathbb{Z}$ tal que $d(a_1 x_0 + b_1 y_0) = c$) .

$\Leftarrow$ Supongamos que $m.c.d.(a,b) = d$ y $d | c$

$a = a_1 d$ y $b = b_1 d$, con a_1 y b_1 primos entre sí (de lo contrario d no sería el mcd de a y b) y además $c = c_1 d$. Entonces

$ax + by = c \Rightarrow a_1 dx + b_1 dy = c_1 d \Rightarrow d(a_1 x + b_1 y) = c_1 d \Rightarrow a_1 x + b_1 y = c_1$ siendo $m.c.d.(a_1,b_1) = 1$

Vamos a suponer de ahora en adelante que $m.c.d.(a,b) = 1$ pues, en caso de no lo sea, y suponiendo la existencia de la solución, es decir suponiendo que $m.c.d.(a,b) = d \mid c$, la ecuación se puede transformar en otra equivalente en la que a y b sí serían primos entre sí.

Demostración

Por ser $m.c.d.(a,b) = d$ se tiene $a = a_1 d$ y $b = b_1 d$, con a_1 y b_1 primos entre sí .

Como $d \mid c$, se tiene $c = c_1 d$. Entonces:

$$ax + by = c \Leftrightarrow a_1 dx + b_1 dy = c_1 d \Leftrightarrow d(a_1 x + b_1 y) = c_1 d \Leftrightarrow a_1 x + b_1 y = c_1$$

siendo $m.c.d.(a_1,b_1) = 1$

A continuación nos ocuparemos de encontrar un método para hallar todas las soluciones de la ecuación ax+by=c, con $a,b,c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ y mcd(a,b) = 1.

En primer lugar demostraremos cómo se pueden obtener todas las soluciones de una ecuación de este tipo a partir de una solución concreta conocida.

4.2.

Si $x=\alpha$ $y=\beta$ es una solución de la ecuación $ax + by = c$, $a,b,c \in Z$, $a \neq 0$, $b \neq 0$ y $mcd(a,b) = 1$ *entonces:*

1) Los números de la forma $\begin{cases} x = \alpha + bt \\ y = \beta - at \end{cases}$ con $t \in \mathbb{Z}$, son también solución de la ecuación.

2) Cualquier otra solución de la ecuación se puede escribir de esa forma.

Observemos que el primer apartado de este resultado implica que una vez demostrada la existencia de una solución, habremos demostrado que hay infinitas soluciones.

Demostración

1) Supongamos que (α,β) es solución de la ecuación $ax + by = c$. Tomemos $t \in \mathbb{Z}$ y consideremos los números $\alpha + bt$ y $\beta - at$; veamos que esos números son solución de $ax+by=c$

$ax+by = a(\alpha+bt) + b(\beta-at) = a\alpha + abt + b\beta - bat = a\alpha + b\beta = c$ (puesto que (α,β) es solución de la ecuación) .

2) Supongamos que (α_1,β_1) es otra solución distinta de (α,β); veamos que $\exists\, t \in Z$ tal que $\begin{cases} \alpha_1 = \alpha + bt \\ \beta_1 = \beta - at \end{cases}$

Por ser (α,β) *solución* $\Rightarrow a\alpha + b\beta = c$ (1)

Por ser (α_1,β_1) *solución* $\Rightarrow a\alpha_1 + b\beta_1 = c$ (2)

Restando (2) – (1): $a(\alpha_1 - \alpha) + b(\beta_1 - \beta) = 0$ (3) $\Rightarrow a(\alpha_1 - \alpha) = b(\beta - \beta_1) \Rightarrow$
$\Rightarrow a$ divide a $b(\beta - \beta_1) \Rightarrow a$ divide a $\beta - \beta_1$, pues $mcd(a,b)=1 \Rightarrow \exists\, t \in Z / at = \beta - \beta_1 \Rightarrow$
$\Rightarrow \beta_1 = \beta - at$.

Sustituyendo en (3): $a(\alpha_1 - \alpha) + b(\beta_1 - \beta) = 0 \Rightarrow a(\alpha_1 - \alpha) + b(\beta - at - \beta) = 0 \Rightarrow$
$\Rightarrow a(\alpha_1 - \alpha) - abt = 0 \Rightarrow a\alpha_1 - a\alpha - abt = 0 \Rightarrow \alpha_1 = \alpha + bt$

Para cerrar el problema de la existencia de soluciones nos queda encontrar una primera solución, la que hemos llamado $x=\alpha$ $y=\beta$.

Consideramos la ecuación diofántica $ax+by=c$, $a,b,c\in Z$, $a\neq 0$, $b\neq 0$ y $mcd(a,b)=1$; se pretende hallar una solución inicial de ella.

4.3.

Algoritmo de Euclides [Referencia de Euclides Si dividimos a entre b, obtenemos un cociente q_1 y un resto r_2. Si $r_2\neq 0$, dividimos b entre r_2, obteniendo un cociente q_2 y un resto r_3. Si $r_3\neq 0$, dividimos r_2 entre r_3, obteniendo un cociente q_3 y un resto r_4, y así sucesivamente. Este proceso tendrá fin y llegaremos a una división de resto $r_{n+1}=0$.

Supongamos que $a,b\in Z$, $a\neq 0$, $b\neq 0$. Mediante sucesivas divisiones enteras, obtenemos:

$a=b\cdot q_1+r_2$ con $r_2<|b|$ (dividiendo a entre b, cociente $\equiv q_1$, resto $\equiv r_2$)

$b=r_2\cdot q_2+r_3$ con $r_3<r_2$ (dividiendo b entre r_2, cociente $\equiv q_2$, resto $\equiv r_3$)

$r_2=r_3\cdot q_3+r_4$ con $r_4<r_3$ (dividiendo r_2 entre r_3, cociente $\equiv q_3$, resto $\equiv r_4$)

$r_3=r_4\cdot q_4+r_5$ con $r_5<r_4$ (dividiendo r_3 entre r_4, cociente $\equiv q_3$, resto $\equiv r_5$)

....

Como $|b|>r_2>r_3>r_4>\ldots>0$ y la cantidad de números enteros positivos menores que un número dado b es finita, debe existir $n\in N$, con $r_{n+1}=0$. Así:

....

$r_{n-2}=r_{n-1}\cdot q_{n-1}+r_n$ con $r_n<r_{n-1}$ (dividiendo r_{n-2} entre r_{n-1}, cociente $\equiv q_{n-1}$, resto $\equiv r_n$)

$r_{n-1}=r_n\cdot q_n+0$ (dividiendo r_{n-1} entre r_n, cociente $\equiv q_n$, resto $\equiv r_{n+1}=0$)

Teniendo en cuenta todas las igualdades anteriores, se puede escribir:

$$\frac{a}{b}=q_1+\frac{r_2}{b}=q_1+\frac{1}{\frac{b}{r_2}}=q_1+\frac{1}{q_2+\frac{r_3}{r_2}}=q_1+\frac{1}{q_2+\frac{1}{\frac{r_2}{r_3}}}=q_1+\frac{1}{q_2+\frac{1}{q_3+\frac{r_4}{r_3}}}=$$

$$=q_1+\frac{1}{q_2+\frac{1}{q_3+\frac{1}{\frac{r_3}{r_4}}}}=q_1+\frac{1}{q_2+\frac{1}{q_3+\frac{1}{q_4}}}=\ldots\ldots$$

Es decir

4.4.

Si a,b∈Z, a≠0, b≠0 y mcd(a,b) = 1

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ddots \cfrac{}{\ddots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}}$$

Por otra parte, consideramos las siguientes cantidades:

$$\delta_1 = q_1,\ \delta_2 = q_1 + \frac{1}{q_2},\ \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}},\ \ldots\ \delta_k = q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_k}}$$ con $1 \le k \le n$

4.5.

Sean *a,b∈Z, a≠0, b≠0 y mcd(a,b) = 1*

Si efectuamos las divisiones enteras a:b, b:r_2, r_2: r_3,… siendo r_2, r_3, r_4,… los sucesivos restos y q_1, q_2, q_3,… los sucesivos cocientes de estas divisiones y consideramos los números $\delta_k = q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_k}}$, $k \in N$, $k \le n$ cada uno de los números δ_k se puede escribir como una fracción de la forma que se describe a continuación:

$$\delta_k = \frac{P_k}{Q_k} \quad \text{donde } P_1 = q_1,\ P_2 = q_1 \cdot q_2 + 1,\ Q_1 = 1,\ Q_2 = q_2 \text{ y}$$

$$P_k = q_k \cdot P_{k-1} + P_{k-2},\quad Q_k = q_k \cdot Q_{k-1} + Q_{k-2}$$

Veamos cómo. Es fácil comprobar los primeros casos. La demostración se completará por inducción.

$$\delta_1 = \frac{P_1}{Q_1} = q_1 \Rightarrow \begin{cases} P_1 = q_1 \\ Q_1 = 1 \end{cases}$$

$$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_1 \cdot q_2 + 1}{q_2} = \frac{q_2 \cdot P_1 + 1}{q_2 \cdot Q_1 + 0} = \frac{P_2}{Q_2} \Rightarrow \begin{cases} P_2 = q_2 \cdot P_1 + 1 \\ Q_2 = q_2 \cdot Q_1 \end{cases}$$

$$\delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}} = q_1 + \frac{q_3}{q_2 \cdot q_3 + 1} = \frac{q_1 \cdot q_2 \cdot q_3 + q_1 + q_3}{q_2 \cdot q_3 + 1} = \frac{q_3 \cdot P_2 + P_1}{q_3 \cdot Q_2 + Q_1} \Rightarrow \begin{cases} P_3 = q_3 \cdot P_2 + P_1 \\ Q_3 = q_3 \cdot Q_2 + Q_1 \end{cases}$$

Numerador: $q_1 \cdot q_2 \cdot q_3 + q_1 + q_3 = P_1 \cdot q_2 \cdot q_3 + q_1 + q_3 = (P_2 - 1) \cdot q_3 + q_1 + q_3 = P_2 \cdot q_3 + q_1 = P_2 \cdot q_3 + P_1$.

Denominador: $q \cdot q + 1 = q \cdot q + Q = Q \cdot q + Q$)

$$\delta_4 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4}}} = q_1 + \cfrac{1}{q_2 + \cfrac{q_4}{q_3 \cdot q_4 + 1}} = q_1 + \frac{q_3 \cdot q_4 + 1}{q_2 \cdot q_3 \cdot q_4 + q_2 + q_4} =$$

$$\frac{q_1 \cdot q_2 \cdot q_3 \cdot q_4 + q_1 \cdot q_2 + q_1 \cdot q_4}{q_2 \cdot q_3 \cdot q_4 + q_2 + q_4} = \frac{q_4 \cdot P_3 + P_2}{q_4 \cdot Q_3 + Q_2} \Rightarrow \begin{cases} P_4 = q_4 \cdot P_3 + P_2 \\ Q_4 = q_4 \cdot Q_3 + Q_2 \end{cases}$$

Demostración

Por inducción sobre k.

Como ya lo hemos comprobado para los primeros valores de k (hasta k=4), sólo faltará demostrar que si suponemos ciertas las formulas para k, entonces también lo son para k+1.

Supongamos que se cumple $P_k = q_k \cdot P_{k-1} + P_{k-2}$ y $Q_k = q_k \cdot Q_{k-1} + Q_{k-2}$

Si observamos la formación de los δ_k vemos que para calcular δ_{k+1} se puede sustituir en el valor de δ_k, q_k por $q_k + \frac{1}{q_{k+1}}$. Por tanto, y dado que en las expresiones de $P_{k-1},\ P_{k-2},\ Q_{k-1}\ y\ Q_{k-2}$ no interviene nunca el valor de q_k, podemos escribir:

$$\delta_{k+1} = \frac{\left(q_k + \frac{1}{q_{k+1}}\right) \cdot P_{k-1} + P_{k-2}}{\left(q_k + \frac{1}{q_{k+1}}\right) \cdot Q_{k-1} + Q_{k-2}} = \frac{q_k \cdot P_{k-1} + \frac{P_{k-1}}{q_{k+1}} + P_{k-2}}{q_k \cdot P_{k-1} + \frac{P_{k-1}}{q_{k+1}} + P_{k-2}} = \frac{P_k + \frac{P_{k-1}}{q_{k+1}}}{Q_k + \frac{Q_{k-1}}{q_{k+1}}} = \frac{\frac{q_{k+1} \cdot P_k + P_{k-1}}{q_{k+1}}}{\frac{q_{k+1} \cdot Q_k + Q_{k-1}}{q_{k+1}}} =$$

$$= \frac{q_{k+1} \cdot P_k + P_{k-1}}{q_{k+1} \cdot Q_k + Q_{k-1}} = \frac{P_{k+1}}{Q_{k+1}} \Rightarrow \begin{cases} P_{k+1} = q_{k+1} \cdot P_k + P_{k-1} \\ Q_{k+1} = q_{k+1} \cdot Q_k + Q_{k-1} \end{cases}$$

Recordemos que nuestro propósito es obtener una solución inicial a la ecuación diofántica ax+by=c, presentamos a continuación el proceso:

_4.6._

Siendo δ_k los números del resultado ***4.5.*** se tiene:

$$\delta_{k+1} - \delta_k = \frac{(-1)^{k-1}}{Q_{k+1} Q_k}$$

Demostración

$$\delta_{k+1}-\delta_k=\frac{P_{k+1}}{Q_{k+1}}-\frac{P_k}{Q_k}=\frac{P_{k+1}\cdot Q_k-P_k\cdot Q_{k+1}}{Q_{k+1}\cdot Q_k}=\frac{\left(q_k\cdot P_k+P_{k-1}\right)\cdot Q_k-P_k\cdot\left(q_k\cdot Q_k+Q_{k-1}\right)}{Q_{k+1}\cdot Q_k}=$$

$$=\frac{P_{k-1}\cdot Q_k-P_k\cdot Q_{k-1}}{Q_{k+1}\cdot Q_k}=\frac{-\left(P_k\cdot Q_{k-1}-P_{k-1}\cdot Q_k\right)}{Q_{k+1}\cdot Q_k}$$

Observando que $P_{k+1}\cdot Q_k-P_k\cdot Q_{k+1}=-\left(P_k\cdot Q_{k-1}-P_{k-1}\cdot Q_k\right)$, se puede escribir :

$$\delta_{k+1}-\delta_k=\frac{P_{k+1}\cdot Q_k-P_k\cdot Q_{k+1}}{Q_{k+1}\cdot Q_k}=\frac{-\left(P_k\cdot Q_{k-1}-P_{k-1}\cdot Q_k\right)}{Q_{k+1}\cdot Q_k}=\frac{(-1)^2\left(P_{k-1}\cdot Q_{k-2}-P_{k-2}\cdot Q_{k-1}\right)}{Q_{k+1}\cdot Q_k}=$$

$$=\frac{(-1)^3\left(P_{k-2}\cdot Q_{k-3}-P_{k-3}\cdot Q_{k-2}\right)}{Q_{k+1}\cdot Q_k}=\ldots=\frac{(-1)^{k-1}\left(P_2\cdot Q_1-P_1\cdot Q_2\right)}{Q_{k+1}\cdot Q_k}=\frac{(-1)^{k-1}\left(\left(q_2\cdot q_1+1\right)\cdot 1-q_1\cdot q_2\right)}{Q_{k+1}\cdot Q_k}=$$

$$=\frac{(-1)^{k-1}}{Q_{k+1}\cdot Q_k}$$

4.7.

Consideremos la ecuación $ax+by=c$, $a,b,c\in Z$, $a\neq 0$, $b\neq 0$ y $mcd(a,b)=1$ entonces

$$\begin{cases} x_0=(-1)^n\cdot Q_{n-1}\cdot c \\ y_0=(-1)^n\cdot P_{n-1}\cdot c\end{cases}\quad \text{con}\quad \frac{P_{n-1}}{Q_{n-1}}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots+\cfrac{1}{q_{n-1}}}}$$

es una solución de esa ecuación.

<u>Demostración</u>

Si en el resultado **3.1.6.** se considera $\delta_{k+1}=\delta_n=\frac{a}{b}$, se obtiene:

$$\frac{a}{b}-\delta_{n-1}=\frac{(-1)^{n-2}}{Q_n\cdot Q_{n-1}}=\frac{(-1)^n}{b\cdot Q_{n-1}}\Rightarrow\frac{a}{b}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^n}{b\cdot Q_{n-1}}\Rightarrow a\cdot Q_{n-1}-b\cdot P_{n-1}=(-1)^n$$

Multiplicando la última expresión por c:

$$a\cdot Q_{n-1}\cdot c-b\cdot P_{n-1}\cdot c=(-1)^n\cdot c\Rightarrow\left((-1)^nQ_{n-1}\cdot c\right)\cdot a+\left((-1)^{n-1}P_{n-1}\cdot c\right)\cdot b=(-1)^{2n}\cdot c=c$$

Lo cual demuestra que una solución inicial para la ecuación $ax+by=c$ es:

$$\begin{cases} x=(-1)^n\cdot Q_{n-1}\cdot c \\ y=(-1)^{n-1}\cdot P_{n-1}\cdot c\end{cases}\quad \text{siendo}\quad \frac{P_{n-1}}{Q_{n-1}}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots+\cfrac{1}{q_{n-1}}}}$$

(De la anterior demostración, se observa que para hallar la solución inicial de la ecuación diofántica $ax + by = c$, únicamente tenemos que calcular la diferencia $\frac{a}{b} - \delta_{n-1}$ y multiplicar por c)

A continuación veamos dos situaciones en las que se requiere el planteamiento y la resolución de una ecuación de este tipo.

Ejemplo 1: El promotor de un concierto decide establecer el precio de la entrada para la zona en la que el público está de pie en 20 € y el precio de las entradas numeradas de asiento en 50 €. ¿Cómo se puede distribuir la venta de entradas si quiere recaudar 38700 €?

Planteamos la ecuación: *20x+50y=38700* $\Leftrightarrow$ *2x+5y=3870*

- ¿Tiene soluciones la ecuación? Si, ya que el m.*c.d(2, 5) =1*
- Hallemos una primera solución:

$\frac{5}{2} = 2 + \frac{1}{2}$; de manera que $\delta_{n-1} = 2$

$\frac{5}{2} - 2 = \frac{1}{2}$ $\Leftrightarrow$ *5·(1)+2·(–2) =1* $\Leftrightarrow$ (multiplicando por *3870)* *2·(–7740)+5·3870 = 3870*

Por tanto, una de las soluciones de la ecuación es $\begin{cases} x_0 = -7740 \\ y_0 = 3870 \end{cases}$

- Todas las soluciones de la ecuación son de la forma $\begin{cases} x = -7740 + 5t \\ y = 3879 - 2t \end{cases} \quad con \;\; t \in \mathbb{Z}$
- Solo nos interesan las soluciones positivas, asi que:

$-7740 + 5t \geq 0 \Rightarrow t \geq \frac{7740}{5} \approx 1550 \qquad y \qquad 3870 - 2t \geq 0 \Rightarrow t \leq \frac{3870}{2} \approx 1930$

Por tanto sólo valen las soluciones que se obtienen para t entre 1550 y 1930.
Hay 380 soluciones distintas. En el contexto de nuestro problema, tres de ellas serían:

Si t = 1550 → Nº de entradas de 20 € = 10 y Nº de entradas de 50 € = 770

Si t = 1740 → Nº de entradas de 20 € = 960 y Nº de entradas de 50 € = 390

Si t = 1930 → Nº de entradas de 20 € = 1910 y Nº de entradas de 50 € = 10

Ejemplo 2: *Una persona compra 40 sellos por un valor total de 10 euros. Los sellos son de 10 cts, 40 cts, y 1,4 €. ¿Cuántos sellos ha comprado de cada clase?*

Planteamos la ecuación: *10x+40y+140(40 – x – y) = 1000*

en la que *x* son los sellos de 10 cts, y los sellos de 40cts y $40 - x - y$ los sellos de 1,40€.

$$10x + 40y + 140(40 - x - y) = 1000 \Leftrightarrow 10x + 40y + 140\cdot 40 - 140x - 140y = 1000 \Leftrightarrow$$
$$\Leftrightarrow 130x + 100y = 4600 \Leftrightarrow 13x + 10y = 460$$

- ¿Tiene soluciones la ecuación? Si, ya que el m.*c.d(13,10) =1*
- Hallemos una primera solución:

$$\frac{13}{10} = 1 + \frac{3}{10} = 1 + \cfrac{1}{3 + \cfrac{1}{3}} \qquad \text{Por lo que } \delta_{n-1} = 1 + \frac{1}{3} = \frac{4}{3}$$

$$\frac{13}{10} - \frac{4}{3} = -\frac{1}{30} \;\; ; \;\; 13\cdot(3) + 10\cdot(-4) = -1 \;\; ; \;\; 13\cdot(-1380) + 10\cdot(1840) = 460$$

Una de las soluciones es $\begin{cases} x = -1380 \\ y = 1840 \\ z = 40 - x - y = -420 \end{cases}$

(Obtenemos z = 40 – (–1380+10t) – (1840 – 13t) = –420 + 3t)

– Todas las soluciones son de la forma $\begin{cases} x = -1380 + 10t \\ y = 1840 - 13t \qquad t \in \mathbb{Z} \\ z = -420 + 3t \end{cases}$

– Solo nos interesan las soluciones positivas, asi que: $\begin{array}{l} -1380 + 10t \geq 0 \Leftrightarrow t \geq 138 \\ 1840 - 13t \geq 0 \Leftrightarrow t \leq 141 \\ -420 + 3t \geq 0 \Leftrightarrow t \geq 140 \end{array}$

y por tanto las soluciones válidas son las que obtenemos para t = 140 y t = 141, que son:

$$\begin{cases} x = 20 \\ y = 20 \\ z = 0 \end{cases} \; y \; \begin{cases} x = 30 \\ y = 7 \\ z = 3 \end{cases}$$

5. TERNAS PITAGÓRICAS

Consideremos la ecuación: $x^2 + y^2 = z^2$.

Es obvio que esta ecuación tiene solución. Por ejemplo, una de ellas es la formada por los números 3, 4 y 5. En realidad, una solución de esta ecuación está formada por las medidas de los lados de un triángulo rectángulo, por ello las soluciones de esta ecuación reciben el nombre de *ternas pitagóricas.* En el contexto de las ecuaciones diofánticas, consideraremos solamente las soluciones formadas solamente por números enteros.

En este apartado, vamos a intentar describir la forma de obtener todas las soluciones de esta ecuación. El proceso requiere algunos resultados previos:

5.1.

Si (x_0, y_0, z_0) es una solución de la ecuación $x^2 + y^2 = z^2$ y si λ es cualquier número entero, entonces $(\lambda x_0, \lambda y_0, \lambda z_0)$ también es otra solución de la misma ecuación.

<u>Demostración</u>

Es evidente ya que: $(\lambda x_0)^2 + (\lambda y_0)^2 = \lambda^2 \cdot (x_0^2 + y_0^2) = \lambda^2 \cdot z_0^2 = (\lambda z_0)^2$

5.2.

Si (x_0, y_0, z_0) es una solución de la ecuación $x^2 + y^2 = z^2$ y m.c.d.$(x_0,y_0) = d$ entonces

d también divide a z_0 y además los números enteros $\left(\frac{x_0}{d},\frac{y_0}{d},\frac{z_0}{d}\right)$ forman también una

solución de esa ecuación.

Demostración

Podemos escribir:

$$\begin{cases} x_0 = d\cdot x_1 \\ y_0 = d\cdot y_1 \end{cases} \Rightarrow z_0^{\ 2} = x_0^{\ 2} + y_0^{\ 2} = (dx_1)^2 + (dy_1)^2 = d^2\cdot\left(x_1^{\ 2} + y_1^{\ 2}\right) \Rightarrow$$

$\Rightarrow d^2$ divide a $z_0^{\ 2} \Rightarrow$ d divide a z_0

Por tanto los números $\frac{x_0}{d}, \frac{y_0}{d}$ y $\frac{z_0}{d}$ son enteros y forman una nueva solución ya que:

$$\left(\frac{x_0}{d}\right)^2 + \left(\frac{y_0}{d}\right)^2 = \frac{x_0^{\ 2} + y_0^{\ 2}}{d^2} = \frac{z_0^{\ 2}}{d^2} = \left(\frac{z_0}{d}\right)^2$$

Gracias a las proposiciones anteriores, es suficiente con hallar las soluciones de la ecuación $x^2 + y^2 = z^2$ en las que los números x e y sean primos entre sí; a estas soluciones las denominaremos soluciones primitivas El resto de soluciones se obtendrán sin más que multiplicar los tres números iniciales por un mismo número entero.

¿Cómo hallar una solución primitiva de la ecuación $x^2 + y^2 = z^2$?

5.3.

Si $x,y,z \in \mathbb{Z}$ y se cumple $x^2 + y^2 = z^2$ con x e y primos entre sí, es decir m.c.d.(x,y) = 1 entonces los números $z + y$ y $z - y$ también son primos entre sí.

Demostración

Como x e y son primos entre sí uno de ellos tiene que ser impar (si los dos fueran pares no serían primos entre sí). Supongamos sin perder generalidad que x es impar. Sea λ = mcd($z + y$, $z - y$). Entonces:

$$\exists\, u,v \in \mathbb{Z}, mcd(u,v) = 1 \ \ tales\ que \left.\begin{matrix} z + y = \lambda u \\ z - y = \lambda v \end{matrix}\right\} \Rightarrow$$

$$\Rightarrow\ x^2 = z^2 - y^2 = (z + y)(z - y) = \lambda u\cdot\lambda v = \lambda^2\cdot uv \Rightarrow$$

$$\Rightarrow\ \lambda^2\ divide\ a\ x^2 \Rightarrow\ \lambda\ divide\ a\ x$$

Por otra parte λ debe ser impar ya que de lo contrario $x^2 = \lambda^2\cdot uv$ sería múltiplo de 4 y, por tanto, x sería par en contra de la hipótesis inicial.

Ahora restamos $z + y$ y $z - y$

$$z + y - (z - y) = \lambda u - \lambda v \Rightarrow 2y = \lambda(u - v) \Rightarrow y = \lambda \cdot \frac{u - v}{2} \Rightarrow \lambda \text{ divide a } y$$

Como λ divide a *x* y λ divide a *y* y m.c.d.(x,y) = 1 , tendremos λ = 1

Como $x^2 = \lambda^2 \cdot uv = uv,\ mcd(u,v) = 1 \Rightarrow$ *u* y *v* deben ser cuadrados perfectos.

Sean $u = a^2$ y $v = b^2$ donde a y b serán también primos entre sí.

Tenemos, pues, la ecuación $x^2 = a^2 \cdot b^2 \Rightarrow x = a \cdot b$ donde a y b son primos entre sí e impares. Volviendo al sistema:

$$\left.\begin{matrix} z + y = u \\ z - y = v \end{matrix}\right\} \Rightarrow \begin{cases} z + y + z - y = u + v \\ z + y - z + y = u - v \end{cases} \Rightarrow \begin{cases} 2z = a^2 + b^2 \\ 2y = a^2 - b^2 \end{cases} \Rightarrow \begin{cases} z = \dfrac{a^2 + b^2}{2} \\ y = \dfrac{a^2 - b^2}{2} \end{cases}$$

Es decir:

5.4.

Si *x,y,z* $\in Z$ con *x* e *y* primos entre sí, las soluciones primitivas de la ecuación

$x^2 + y^2 = z^2$ vienen dadas por

$$x = a \cdot b \quad y = \frac{a^2 - b^2}{2} \quad z = \frac{a^2 + b^2}{2}$$

con a, b impares, primos entre sí y b<a.

Así hemos encontrado un método para obtener infinitas ternas pitagóricas. Estas infinitas ternas ya aparecen descritas en Los Elementos de Euclides. Veamos unos ejemplos:

Ejemplos:

x = a·b	a	b	$y = \frac{a^2 - b^2}{2}$	$z = \frac{a^2 + b^2}{2}$	**Terna**
3	3	1	4	5	**(3,4,5)**
5	5	1	12	13	**(5,12,13)**
7	7	1	24	25	**(7,24,25)**
9	9	1	40	41	**(9,40,41)**
11	11	1	60	61	**(11,60,61)**
15	5	3	8	17	**(15,8,17)**
15	15	1	112	113	**(15,112,113)**
21	7	3	20	28	**(21,20,28)**

6. EL ÚLTIMO TEOREMA DE FERMAT.

Por fin se había demostrado el último teorema de Fermat *[Referencia de Fermat* . La noticia salió en aquellos días de en algún telediario y en algún periódico, cosa muy excepcional porque no suele haber noticias relacionadas con las Matemáticas. Esta historia es bastante conocida entre los matemáticos y los profesores de matemáticas: Fermat estudiaba el libro Aritmética de Diofanto y en el margen escribía numerosas anotaciones que ampliaban lo que en su Aritmética exponía Diofanto.

Una parte de ese libro se dedicaba a las ternas pitagóricas. En lenguaje actual, ¿para qué valores enteros de x, y, y z, se cumple que $x^2 + y^2 = z^2$? Sobre ellas ya hemos hablado en el punto anterior de este trabajo y ya sabemos que hay infinitas soluciones y cómo hallarlas.

Pero ¿qué ocurre si se cambia el dos del exponente por un tres, por un cuatro, por un cinco,…? Fermat escribe en una de sus anotaciones que ha encontrado una demostración maravillosa de que no existen números enteros que cumplan $x^n + y^n = z^n$ para $n = 3, 4, 5, \ldots$. pero que esa demostración no le cabe en ese margen (se excluye el caso $xyz = 0$; al decir enteros, se entiende enteros positivos). Desde entonces hasta ningún matemático había podido demostrar ese resultado.

> *"Cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet"*

¿Fermat se había tirado un farol?

Parece que Fermat si pudo demostrar este resultado para $n = 4$ porque, en una de las pocas demostraciones completas que se conservan dejadas por él, se demuestra - utilizando un método famoso: el método de Fermat de descenso infinito - que el área de un triángulo rectángulo cuyos lados son números enteros, no puede ser el cuadrado de un número entero y a partir de este resultado se deduce la demostración del último teorema de Fermat para $n = 4$.

De todos los teoremas que Fermat dejó enunciados sin demostración los matemáticos, - especialmente de los siglos XVIII y XIX, fueron demostrando uno a uno todos menos éste y de ahí el sobrenombre de "el último".

Pronto se descubrió que si el teorema de Fermat fuese cierto para n primo y $n = 4$, entonces sería cierto para todos los números.

En 1753 Euler [Referencia de Euler afirmó haber encontrado una demostración para el caso $n = 3$. Aunque esta demostración contenía un error, relacionado con una suposición que Euler hacía con respecto a la descomposición en factores primos, la comunidad matemática admite a Euler como el autor de la demostración para este caso.

En 1895 Dirichlet y Legendre demostraron el teorema para $n = 5$. Y en 1839 fue Lamé el que demostró el teorema para $n = 7$.

Pero fue Kummer en el 1847 el matemático que fue capaz de pasar de los casos particulares a un caso mas general y, gracias a la teoría de los números ideales que desarrolló, hoy ideales sin mas, consiguió demostrar que el último teorema de Fermat se cumplía para todos los exponentes primos regulares (NOTA: hemos leído que la mayoría de los números primos son primos regulares pero que la definición de "primo regular" es muy difícil y por eso no la ponemos aquí).

Posteriormente los intentos de encontrar la demostración provocaron que surgiera, gracias a Kummer y Dedekind sobre todo, una nueva rama de la matemática, la geometría algebraica (estudio de curvas y superficie a través de objetos algebraicos. Así el punto (2,3) es el punto en el que se hacen cero los polinomios $x – 2$, $y – 3$). Después, en 1983, Faltings demuestra la conjetura de Mordell ("Toda curva racional de género mayor que 1 tiene, como mucho un número finito de puntos con coordenadas enteras") cuya comprensión se nos escapa pero que al parecer supuso otro gran avance. El resto es más difícil todavía. Citemos solamente algunos hechos y fechas.

En 1955 Taniyama conecta las curvas elípticas y las funciones modulares. Y este hecho es el que propicia la aparición del autor de la demostración definitiva, Wiles, que era especialista en curvas elípticas.

Ribet demuestra en 1985 la conjetura de Frey, que relaciona las curvas elípticas con el último teorema de Fermat.

Andrew Wiles [Referencia de A. Wiles anuncia en junio de 1993 que había logrado demostrar la conjetura de Shimura Taniyama, lo cual implicaría la demostración completa del último teorema de Fermat. Pero en diciembre tuvo que admitir un error encontrado en su demostración. Corregir ese error, con ayuda de otro matemático, Taylor, que era alumno suyo, le llevó otro año y pico de trabajo.

Finalmente, en septiembre de 1994, el último teorema de Fermat quedó demostrado.

Y terminamos casi volviendo al punto de partida del trabajo:

> *"La pregunta surge inevitable. El teorema está demostrado, ¿y qué?, ¿para qué tanto esfuerzo inútil? La respuesta es también inevitable. ¿Inútil?, ¿seguro que inútil?"*

Capi Corrales

7. CONCLUSIONES.

Como ya dijimos en el apartado de objetivos, una de las cosas que se pretendían en este trabajo era mostrar algunos casos de ecuaciones con soluciones enteras, y demostrar si tienen solución y como hallarla. No podemos alargarnos más, tanto por falta de tiempo y espacio, como por falta de conocimientos. Sin embargo, creemos haber conseguido dar una visión general de lo que son estas ecuaciones, su forma y sus soluciones.

Queda demostrado, pues, la existencia (o no existencia) de soluciones en algunos de los casos mas importantes de las ecuaciones diofánticas como son $ax+by=c$ ó $x^2+y^2=z^2$. También, inevitablemente, hemos hecho un repaso del proceso histórico que llevo a la demostración del Último Teorema de Fermat.
Sin embargo dejamos atrás el estudio de otro tipo de ecuaciones que también tienen solución, como por ejemplo las de la forma $x^2 – Ay^2 = 1$, donde A es un entero positivo no cuadrado perfecto, y de otras que no la tienen, por ejemplo $x^4 + 2y^4 = z^2$.

Después de 4 meses de trabajo, creemos haber conseguido los objetivos que nos propusimos al comienzo y estamos contentos porque cada uno de nosotros ha podido aportar algo para lo que tiene más facilidad. No es lo mismo entender una demostración, que redactar la parte de objetivos, o que hacer la presentación electrónica en formato A1. Quizás la organización de este concurso considere mejor un trabajo en el que todos hagan todo, pero hemos de reconocer que nosotros no hemos podido. Sin embargo, consideramos más real y mas útil para nuestra vida conocer nuestros puntos fuertes y nuestras limitaciones y sacar partido de ello.

8. DATOS BIOGRÁFICOS DE LOS MATEMÁTICOS CITADOS, POR ORDEN DE APARICIÓN.

Referencia de G. H. Hardy (1877-1947). Matemático británico, discípulo de B Russell, con una producción muy extensa dedicada sobre todo al Análisis y a la Teoría de Números. Colaboró fundamentalmente con Littlewood y con Ramanujan (al que junto descubrió). Con el primero demostró que "existen infinitos ceros sobre la recta, lo que no demuestra la hipótesis de Riemann", pero la reafirma. *[Volver página **3**]*

Referencia de David Hilbert (1862-1943). Matemático alemán que lideró la llamada escuela formalista frente a los matemáticos que se agruparon en torno a Poincaré, más intuicionistas. Fueron llamados formalistas e intuicionistas dependiendo de sus puntos de vista con respecto a los fundamentos de la matemática; también existía la escuela logicista, cercana a los formalistas, encabezada por B. Russell. Hilbert, famoso por su discurso en el Congreso Internacional de París, dejó para la posteridad numerosos avances en teoría de números, lógica matemática, ecuaciones diferenciales y física matemática sobre todo *[Volver a página **3**]*

Referencia de Diofanto de Alejandría (vivió alrededor del año 250 d.C.). Fue el mas importante de los algebristas griego y vivió durante la llamada "Edad de Plata" de la matemática griega, también conocida como "Edad Alejandrina Tardía" . Poco mas se sabe de su vida pero de su obra mas importante, su *Arithmetica* , un tratado dedicado a la resolución exacta de ecuaciones determinadas e indeterminadas, nos han llegado los seis primeros libros. La Arithmetica de Diofanto constaba de trece libros y a lo largo de los seis que no se han perdido, se ve cómo Diofanto anticipa anticipa por ejemplo el uso de abreviaturas para potencias y el uso de una letra, la letra *s,* para representar un número desconocido. *[Volver a la página **3**]*

Referencia de Yuri Matiyasevich. Matemático ruso conocido especialmente por resolver el décimo problema de Hilbert. Actualmente es Director del Laboratorio de Lógica Matemática del Instituto Steklov de Matemáticas en San Petersburgo, Director del Instituto Euler para las Matemáticas, y Profesor (en excedencia) del Computer Software en la Universidad de San Petersburgo en Rusia. En 1964 obtuvo una medalla de oro en la IMO celebrada en Moscú. *[Volver a la página **4**]*

Referencia de Euclides (vivió aproximadamente entre el 335 a.C. y el 265 a.C.) Ptolomeo I le llamó para formar parte de los sabios que enseñaron en la Biblioteca de Alejandría. Su obra más famosa es un conjunto de libros, Los Elementos, en el que se exponen en orden lógico los fundamentos de la matemática elemental conocida hasta entonces, es decir de aritmética (en el sentido de teoría de números), de geometría (de puntos, rectas, planos, círculos y esferas) y de álgebra (no en el sentido moderno sino en el sentido griego de álgebra geométrica*)* *[Volver a la página **7**]*

Referencia de Fermat (1601 – 1665). Francés, abogado de carrera y magistrado de profesión, por lo que fue apodado como "el príncipe de los aficionados", reconociendo la gran pasión y los importantes resultados matemáticos que obtuvo a lo largo de su vida sin ser un matemático de profesión. Transmitió sus ideas por carta sin publicar sus importantes descubrimientos realizados sobre todo en el campo de la teoría de números, de la probabilidad y en el cálculo diferencial *[Volver a la página **15**]*

Referencia de Euler (1707 – 1783). Muchos autores le describen como uno de los mayores genios de la historia que además plasmaba por escrito y muy rápidamente sus descubrimientos. Se le calcula una media de 800 páginas anuales de resultados brillantes e importantes. Sus logros en partes de la matemática ya conocidas, como teoría de números, cálculo, álgebra y geometría, no le impidieron que alumbrara casi en solitario nuevas ramas de la matemática como la topología, sobresaliendo también en Matemáticas aplicadas. *[Volver a la página **15**]*

Referencia de A. Wiles (1953 – …) Matemático británico que alcanzó fama mundial cuando en 1993 en unas conferencias que pronunciaba en el Instituto Isaac Newton, de la Universidad de Cambridge, anunció la demostración del último teorema de Fermat. Posteriormente se encontró un error que fue subsanado en septiembre del 94. En este año Wiles fue designado *Eugene Higgins Professor of Mathematics en Princeton.* El artículo en el que prueba el Último Teorema de Fermat es "*Modular elliptic curves and Fermat's Last Theorem*" y fue publicado en el *Annals of Mathematics* en 1995. A partir de 1995 Wiles comenzó a recibir premios y distinciones por su trabajo pero no pudo llegar a tiempo de que se le otorgara una de las más famosas distinciones matemáticas, La medalla Field, que no se concede a matemáticos mayores de 40 años. *[Volver a la página **16**]*

BIBLIOGRAFÍA

Boyer, C. B. *Historia de la matemática*. Ed. Alianza Universidad Textos.

Corrales, C. "El último teorema de Fermat" *S.M.P.M.Emma Castelnuovo*, nº 9.

Devlin, K. El lenguaje de las Matemáticas. Ed MA Non Troppo, 2002.

Guelfond, A.O. *Resolución de ecuaciones en números enteros.* Ed. Mir, 1984

Hardy, G.H. *Apología de un matemático*. Madrid: Ed. Nivola, 1999

Fariña, J. C. "Los 23 problemas de Hilbert". *Las matemáticas del siglo XX. Una mirada en 101 artículos*. Madrid: Ed. Nivola, 2000.

Población Sáez, Jesús. "Julia Robinson y el H 10" DivulgaMat. Revista virtual. Enero 2010.

ANEXO:

PROGRAMA EN PASCAL QUE PROPORCIONA TERNAS PITAGÓRICAS PRIMITIVAS

Adjuntamos además un programa informático escrito en lenguaje PASCAL que proporciona ternas pitagóricas primitivas. El programa solicita introducir un número impar u y devuelve todas las ternas pitagóricas primitivas de la forma:

$$\left(uv, \frac{u^2 - v^2}{2}, \frac{u^2 + v^2}{2} \right)$$

siendo v otro número impar menor que u y u y v primos entre sí

PROGRAMA

```
program ternas_pitagoricas;
uses crt;
var
  i, u:integer;
  cont: char;

      (* se programa una función que decida si dos números enteros
         son o no primos entre sí *)

function primos_entre_si (n,m:integer):boolean;
```

```
var control: boolean;
    a:integer;
  begin
    control:=true;
    if n=m then control:=false;
    if n<m then
      begin
        for a:=2 to n do
            if (n mod a=0) and (m mod a=0) then control:=false;
      end;
    if n>m then
      begin
        for a:=2 to m do
            if (n mod a=0) and (m mod a=0) then control:=false;
      end;
    primos_entre_si:=control;
  end;

begin

  clrscr;
  (*Se solicita un número impar*)

  write ('Introduce un número entero impar mayor que 1: ');
  readln (u);
  while ((u mod 2=0) or (u=1)) do
     begin
       write ('El número introducido no es correcto. Por favor introduce otro: ');
       readln (u);
     end;
  clrscr;

  (*Se escribe todas las ternas pitagóricas que contienen
  al n£mero solicitado*)
  writeln ('       TERNAS PITAGÓRICAS PRIMITIVAS (con base u=',u,')');
  writeln;
  for i:=1 to u-2 do
    begin
      if i=1 then
        writeln (u,'  ',(u*u-1)/2:0:0, '  ',(u*u+1)/2:0:0);

      if ( (i>1) and (i mod 2=1) and (primos_entre_si(u,i)=true) ) then
        begin
         writeln (u*i,'  ',(u*u-i*i)/2:0:0, '  ', (u*u+i*i)/2:0:0);
        end;
    end;

      writeln;
      writeln ('Nota: tomando como base estas ternas primitivas,');
      writeln('se pueden obtener otras sin más que multiplicar los');
      writeln('tres números que las forman por un mismo número.');
```

```
  (*Se pregunta si se quieren más ternas*)
writeln;
writeln;
writeln ('                ¨Quieres más ternas?');
writeln;
writeln( '                     MENU:');
writeln ('                      SÍ     (S)');
writeln ('                      SALIR  (Z)');
readln(cont);
while (cont='s') or (cont='S') do
    begin
     clrscr;
      (*Se solicita un número impar*)

     write ('Introduce un número entero impar mayor que 1: ');
     readln (u);
     while ((u mod 2=0) or (u=1)) do
       begin
         write ('El número introducido no es correcto. Por favor introduce otro: ');
         readln (u);
       end;

       (*Se escribe todas las ternas pitagóricas que contienen
        al n£mero solicitado*)
     writeln ('       TERNAS PITAGÓRICAS PRIMITIVAS (con base u=',u,')');
     writeln;
     writeln (u,'  ',(u*u-1)/2:0:0, '  ', (u*u+1)/2:0:0);
     for i:=3 to u-2 do
      begin
        if (((i mod 2=1) and (primos_entre_si(u,i)=true))) then
          begin
           writeln (u*i,'  ',(u*u-i*i)/2:0:0, '  ', (u*u+i*i)/2:0:0);
          end;
      end;
     writeln;
     writeln ('Nota: tomando como base estas ternas primitivas,');
     writeln('se pueden obtener otras sin más que multiplicar los');
     writeln('tres números que las forman por un mismo número.');
         (*Se pregunta si se quieren más ternas*)
     writeln;
     writeln;
     writeln ('           ¨Quieres obtener más ternas?');
     writeln;
     writeln( '                MENU:');
     writeln ('                  SÖ     (S)');
     writeln ('                  SALIR  (Z)');
     readln(cont);
    end;
end.
```