NÚMEROS PERFECTOS Y MATEMÁTICOS IMPERFECTOS

JOSÉ L. BUESO MONTERO

INTRODUCCIÓN

Excelentísimo Señor Presidente de la Academia de Ciencias Matemáticas, Físico-Químicas y Naturales de Granada, Excelentísimos e Ilustrísimos Académicos, queridos amigos y compañeros.

Quisiera empezar agradeciendo a esta Academia el haberme nombrado miembro de la misma. Espero que no se arrepientan después de leer el título del discurso.

1. ¿CUÁNTOS NÚMEROS PRIMOS EXISTEN?

Como es bien sabido, Dios creó los infinitos números naturales, siendo todos los demás creación del hombre.

En Matemáticas, un «número primo», es un número natural cuyos únicos divisores positivos son 1 y él mismo.

La sucesión de números primos empieza por 2, 3, 5, 7, 11, 13, 17, ... Disculpen que no enumere todos, pero son también infinitos.

La demostración más antigua que se conoce sobre la infinitud de los números primos fue dada sobre el año 300 AC por el matemático griego Euclides en la Proposición 20, del Libro IX de sus «Elementos» [15]:

Teorema 1 (Euclides)**.** *Hay más números primos que cualquier cantidad dada de números primos.*

Supongamos que existe solo un número finito de números primos. Sea m el producto de todos ellos. Consideremos el número $m + 1$. No puede ser primo, ya que es mayor que todos los primos.

Luego es compuesto. Entonces de acuerdo a VII.31, algún primo q lo divide. Pero q no puede ser ninguno de los primos, ya que estos dividen m y no dividen $m + 1$.

Así, la hipótesis de que existe un número finito de primos proporciona una contradicción. Por tanto, el número de primos no es finito.

Su demostración es pues la primera demostración conocida realizada por contradicción o reducción al absurdo.

Si bien el número de primos es infinito, podemos estudiar cuantos primos existen menores que un cierto número dado.

Sea n un número entero y denotemos por $\pi(n)$ el número de primos menores o iguales que n.

Así, por ejemplo, $\pi(3) = 2$, $\pi(10) = 4$ y $\pi(25) = 9$.

En 1798 Legendre publica la primera conjetura significativa acerca del tamaño de $\pi(n)$, cuando en su libro «Essai sur la Théorie des Nombres» [17] establece que

$$\pi(n) \sim \frac{n}{\ln(n) - 1{,}08366},$$

donde $f(n) \sim g(n)$ significa que $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$.

Parece ser que Gauss en 1792 y a la edad de 15 años proponía

$$\pi(n) \sim \frac{n}{\ln(n)}$$

Más tarde refinaba su estimación a

$$\pi(n) \sim \mathrm{Li}(n)$$

donde

$$\mathrm{Li}(n) = \int_2^n \frac{dx}{\ln(x)} = \frac{n}{\ln(n)} + \frac{1!n}{\ln^2(n)} + \frac{2!n}{\ln^3(n)} + \cdots$$

Gauss no publica esta hipótesis, si bien es mencio-

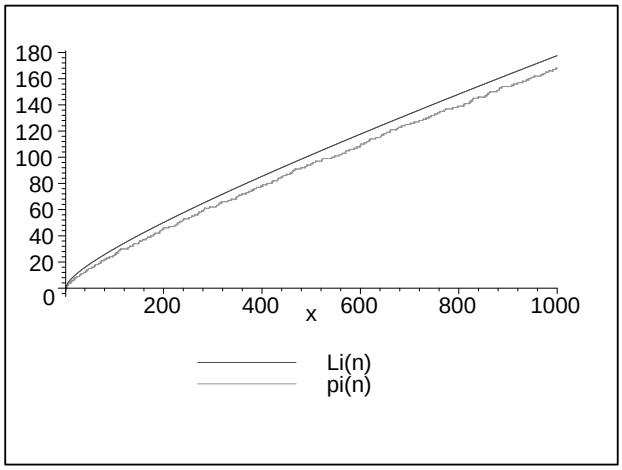

FIGURA 1. Las funciones π y Li

nada en 1849 en una carta a Encke. Finalmente es publicada en 1863 a la muerte de Gauss [13].

La hipótesis de Gauss fue demostrada en 1896, independientemente, por Hadamard [14] y De la Vallée Poussin [6] y es ahora es conocida como el teorema de los números primos.

1.1. La hipótesis de Riemann. Euler estudia la serie

$$\sum_{n=1}^{\infty} \frac{1}{n^t}$$

donde t es real. Sea $s = \sigma + it$ con $\sigma > 1$. Entonces la función zeta de Riemann es definida como

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

En 1737 Euler descubre que la serie $\zeta(s)$ puede representarse en términos de los números primos:

Para p primo y $s = \sigma + it$, $\sigma > 1$,

$$\zeta(s) = \prod_{p} (1 - \frac{1}{p^s})^{-1}.$$

También demuestra que $\zeta(s)$ no tiene ceros en el semiplano $\sigma > 1$. La función zeta se extiende a una función meromorfa en todo el plano. Esta función tiene un único polo en $s = 1$ y no se anula en $\Re(s) > 1$. Tiene ceros simples en los puntos $s = -2, -4, -6, \ldots$, y estos son sus únicos ceros en $\Re(s) < 0$. Estos son llamados los «ceros triviales». Los únicos ceros no triviales posibles se encuentran en la banda crítica $0 \leq \Re(s) \leq 1$.

Riemann [31] probó que existían infinitos ceros no triviales y conjeturó que todos los ceros no triviales se encuentran en la recta $\Re(s) = 1/2$. Esta conjetura es la que se conoce como hipótesis de Riemann.

En 1914, Hardy prueba que existen infinitos ceros no triviales en la recta $\Re(s) = 1/2$.

En 2004, Xavier Gourdon ha comprobado la veracidad de la conjetura para los primeros diez billones de raices.

La tradicional formulación de la hipótesis de Riemann oscurece la verdadera importancia de la conjetura. La función zeta de Riemann tiene una profunda conexión con la distribución de primos y Helge von Koch probó en 1902 [35] que la hipótesis de Riemann

es equivalente a

$$| \operatorname{Li}(n) - \pi(n) | \leq c\sqrt{n}\ln(n)$$

para algún c.

En 1900, Hilbert incluye la hipótesis de Riemann en su famosa lista de 23 problemas no resueltos (es parte del problema 8). Es uno de los más importantes problemas abiertos de las matemáticas contemporáneas y en la actualidad existe un premio de 1 000 000 de dólares para quien lo demuestre.

El número de demostraciones erróneas de la conjetura de Riemann crece exponencialmente con el paso del tiempo.

En junio de 2004, Louis De Branges, el mismo matemático que resolvió la conjetura de Bieberbach, afirma haber probado la conjetura de Riemann, en un trabajo titulado «Riemann Zeta Functions» [1]. Su demostración se halla en fase de revisión. Hay que decir que fracasó en anteriores intentos de dar una demostración de la conjetura.

Existe la siguiente anécdota sobre Hardy. Hardy pensaba que Dios le tenía manía. En cierta ocasión teniendo que atravesar el Mar del Norte en un barco que presentaba mal aspecto, antes de partir envía una postal a su amigo Harald Bohr con el siguiente texto:

> He probado la Conjetura de Riemann.
> G.H.Hardy

La razón de tal hecho es que, si moría en el viaje, todo el mundo pensaría que él había probado la conjetura, pero tenía el convencimiento, de que Dios no permitiría tal honor para él.

---

[1] http://www.math.purdue.edu/ftp-pub/branges/riemannzeta.pdf

La hipótesis de Riemann generalizada probablemente fue formulada por primera vez por Piltz en 1884. Como la hipótesis de Riemann original, tiene consecuencias de mucho alcance sobre la distribución de los números primos.

Un carácter de Dirichlet es una función aritmética multiplicativa, χ, tal que existe un natural, k, con $\chi(n+k) = \chi(n)$ para todo n y $\chi(n) = 0$ cuando m.c.d.$(n,k) > 1$. Si tal carácter está dado,definimos la correspondiente «L-función de Dirichlet» por

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

para todo número complejo s con $\Re(s) > 1$. Por prolongación analítica, esta función puede extenderse a una función meromorfa definida sobre todo el plano complejo.

La hipótesis de Riemann generalizada asegura que para todo carácter de Dirichlet, χ, y todo número complejo, s, con $L(\chi, s) = 0$: si $0 \leq \Re(s) \leq 1$, entonces $\Re(s) = 1/2$.

El caso $\chi(n) = 1$ para todo n, establece la hipótesis de Riemann ordinaria.

Un teorema de Dirichlet establece que para dos enteros positivos primos entre sí a y d existen infinitos primos de la forma $a + nd$, donde $n > 0$, esto es, en la progresión $a, a+d, a+2d, a+3d, \ldots$ existen infinitos primos (no que todos ellos sean primos).

Sea $\pi(x, a, d)$ el número de números primos en esta progresión que son menores o iguales que x. Si la hipótesis generalizada de Riemann fuese verdadera, entonces

$$\mid \pi(x, a, d) - \frac{Li(x)}{\varphi(d)} \mid \leq c\sqrt{x}\ln(x)$$

para algún c y donde $\varphi(d)$ denota la función phi de Euler.

¿Pero cómo puede haber algo sin duda menor, como son los números primos, que una cantidad infinita, como son los números naturales, y que sea a su vez infinito?

Hilbert elaboró un ejemplo de infinito, conocido como el «hotel de Hilbert», para explicarlo. Este hotel posee un número infinito de habitaciones. Al llegar un nuevo cliente, se lleva la desagradable sorpresa de que a pesar de que existen infinitas habitaciones, todas están ocupadas. Hilbert que es el recepcionista, pide a todos sus clientes que se muden a la habitación siguiente a la que están alojados. Todos los huéspedes siguen teniendo habitación y ha quedado vacía la habitación número uno, donde ahora se puede alojar el nuevo visitante.

La noche siguiente, aparece un autobús con un número infinito de pasajeros. Hilbert sin perder los nervios, pide a sus clientes que ahora se muden a la habitación cuyo número sea el doble del que hasta ahora tienen. Todos sus clientes siguen teniendo habitación y ahora tiene libres infinitas habitaciones, todas las impares, donde alojar a los pasajeros del autobús.

2. Números perfectos y números de Mersenne

En opinión de Martin Gadner,

> «Es complicado encontrar un conjunto de números naturales con una historia más fascinante y con propiedades rodeadas de profundos misterios pero a su vez más inútiles, que los números perfectos.»

Los números primos y sus propiedades fueron estudiados intensamente por los antiguos matemáticos griegos, especialmente por la escuela Pitagórica.

Pitágoras de Samos (569-475 AC) es uno de los personajes más misteriosos de las matemáticas. Estudió las propiedades de cada número, las relaciones entre ellos y las figuras que forman. Fundó la Hermandad Pitagórica, una comuna formada con discípulos que debían prestar juramento de no revelar al mundo exterior ninguno de sus descubrimientos. Esto explica que hoy dispongamos de tan pocos datos fidedignos sobre sus logros matemáticos. La hermandad era, de hecho, una secta religiosa y uno de sus ídolos era el «Número» . De entre la infinidad de números la hermandad se fijó en los que poseen propiedades especiales y entre ellos se encontraban los números primos y los números perfectos o divinos.

Según Pitágoras, la perfección numérica dependía de los divisores del número.

Un número perfecto es uno cuya suma de divisores propios es el propio número, por ejemplo, los cuatro primeros son

$$\begin{aligned} 6 &= 1+2+3 \\ 28 &= 1+2+4+7+14 \\ 496 &= 1+2+4+8+16+31+62+124+248 \\ 8128 &= 1+2+4+8+16+32+64+127+254 \\ &\quad +508+1016+2032+4064 \end{aligned}$$

Además del significado matemático que tenían para la hermandad, la perfección del seis y del veintiocho fué tomada de otras culturas, que observaron

que 28 es la duración del ciclo lunar/menstrual y que afirmaron que Dios creó el mundo en seis días.

Como aparece en el libro IX, proposición 36 de sus «Elementos», Euclides escribe:

> «Si tantos números como se quiera a partir de una unidad se disponen en proporción duplicada hasta que su suma total resulte un número primo, y el total multiplicado por el último produce algún número, el producto será un número perfecto.»

Notemos que la suma, $s = 1 + 2 + 2^2 + \cdots + 2^{n-1}$, es igual a 2^n–1, por IX.35. Así podemos establecer este enunciado de la siguiente manera:

Teorema 2 (Euclides)**.** *Si* 2^n–1 *es un número primo, entonces* $(2^n–1) \cdot 2^{n-1}$ *es un número perfecto.*

El siguiente estudio significativo de los números perfectos fue realizado por Nicómaco de Gerasa (60-120) alrededor del año 100 D.C. En su «Introducción a la Aritmética» [24] da una clasificación de los números basada en los números perfectos. Nicómaco divide a los números en tres clases: los números abundantes, que tienen la propiedad de que la suma de sus divisores propios es mayor que el número, números deficientes, que tienen la propiedad de que la suma de sus divisores propios es menor que el número y números perfectos, que tienen la propiedad de que la suma de sus divisores propios es igual al número.

$$1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14 \ldots$$

son números deficientes,

$$12, 18, 20, 24, 30, 36, \ldots$$

son números abundantes, y

$$6, 28, 496, 8128, \ldots$$

son números perfectos.

Describe también una serie de propiedades de los números perfectos, sin proporcionar una demostración y con algunos errores:

(1) El n-ésimo número perfecto tiene n cifras.
(2) Todos los números perfectos son pares.
(3) Todos los números perfectos acaban en 6 u 8 alternativamente
(4) Todo número perfecto es de la forma $2^{p-1}(2^p-1)$, donde $2^p - 1$ es primo.
(5) Existen infinitos números perfectos.

Nicómaco no ofrece ninguna justificación de dichas propiedades.

Las afirmaciones (1) y (3) son falsas y las restantes serán cuestiones abiertas.

Los números perfectos seguían teniendo consideraciones religiosas. San Agustín (354-430) escribía en su libro «La ciudad de Dios» ,

> «Seis es un número perfecto en sí mismo, y no porque Dios crease el mundo en 6 días; es justamente lo contrario: Dios creó el mundo en 6 días porque este número es perfecto. »

Alcuin de York (735-804), consejero y maestro de Carlomagno, observa que el género humano desciende de las 8 personas que se salvaron en el arca (Noé, sus tres hijos y sus cuatro mujeres). Ya que 8 es un número deficiente, concluye que esta segunda creación era imperfecta en comparación con la primera, que estaba basada sobre el número perfecto 6.

El quinto y sexto números perfectos han sido encontrados en varios manuscritos elaborados por Johan Müller (1436-1476), también conocido por «Regiomantanus», alrededor de 1460.

Durante años se pensó que los números de la forma $2^n - 1$ eran primos para todo primo n, pero en 1536, Hudalrichus Regius [29] publica «Utriusque arithmetices» donde comprueba que $2^{11} - 1 = 2\,047 = 23 \cdot 89$, encontrando el primer primo, $p = 11$, tal que $2^p - 1$ no es primo. También demuestra que $2^{13} - 1 = 8\,191$ es primo, encontrando indirectamente el quinto número perfecto $2^{12}(2^{11} - 1) = 33\,550\,336$. Esto además refuta la primera afirmación de Nicómaco, pues el quinto número perfecto tiene 8 cifras y no 5.

El siguiente paso lo da Pietro Cataldi quien en 1603 escribe «Tratatto de numeri perfetti» [4] donde tabula los factores de todos los números menores que 800 y todos los primos menores que 750. Con el uso de sus tablas demuestra que $2^{17} - 1 = 131\,071$ es primo y por tanto puede encontrar el sexto número perfecto $2^{16}(2^{17} - 1) = 8\,589\,869\,056$. También cae por tierra la tercera afirmación de Nicómaco, sobre la alternancia del 6 y del 8 en la cifra final de los números perfectos. Con el mismo método demuestra que $2^{19} - 1 = 524\,287$ es primo y por tanto puede hallar el séptimo número perfecto $2^{18}(2^{19} - 1) = 137\,438\,691\,328$. Escribe en el tratado que los exponentes 2, 3, 5, 7, 13, 17, 19, 23, 29, 31, 37 dan números perfectos, pero estaba equivocado con 23, 29, 31 y 37. La historia de los números perfectos está plagada de errores.

En el siglo XVII, la ciencia en Francia no estaba aún organizada. Habrá que esperar a 1665 para que nazca la primera revista científica en la que los científicos puedan publicar sus resultados, se trata del «Journal

des Savants» , y a 1666 para que se cree la Academia de Ciencias. Mientras tanto, para intercambiar sus ideas y comunicarse, los investigadores utilizaban la correspondencia. El monje Marin Mersenne (1588-1648) jugaba un papel central, hacía copiar a los monjes de su convento los trabajos conforme los recibía y los distribuía por toda Europa. Mersenne era el Internet del siglo XVII.

En 1640, Pierre Fermat, abogado y aficionado a las Matemáticas, escribe a Mersenne con su investigación sobre los números perfectos:

> «aquí están tres proposiciones que he descubierto, sobre las que espero erigir una gran estructura. A partir de las sucesiones
>
> | n | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
> |---|---|---|---|---|---|---|---|
> | 2^n-1 | 1 | 3 | 7 | 15 | 31 | 63 | 127 |
>
> puedo decir
>
> (I) Si n es compuesto, entonces $2^n - 1$ es compuesto.
> (II) Si n es primo, entonces $2^n - 2$ es un múltiplo de $2n$.
> (III) Si n es primo y p es un divisor primo de $2^n - 1$, entonces $p - 1$ es un múltiplo de n.»

Poco después Fermat escribe a Frenicle de Bessy. En su carta incluye una generalización de los resultados de la anterior carta estableciendo el resultado ahora conocido como el Teorema pequeño de Fermat:

Teorema 3 (pequeño de Fermat)**.** *Para todo primo, p, y todo natural, a, no divisible por p, $a^{p-1} - 1$ es divisible por p.*

Usando casos especiales de su pequeño teorema, Fermat, en una carta a Mersenne, es capaz de refutar los casos $p = 23$ y $p = 37$ de Cataldi. Prueba que $2^{23} - 1$ y $2^{37} - 1$ son compuestos dando sus factorizaciones y el procedimiento seguido para encontrarlas:

$$2^{23} - 1 = 47 \cdot 178\,481, \qquad 2^{37} - 1 = 223 \cdot 616\,318\,177.$$

Mersenne, en 1644, establece en el prefacio a su obra «Cogitata Physica Mathematica» [22] que los números $2^n - 1$ eran primos para

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

y eran compuestos para todos los demás naturales, $n < 257$. La conjetura (una vez más, incorrecta) de Mersenne difiere poco de la de Regius, sin embargo este tipo de números son conocidos como números de Mersenne, $M_n = 2^n - 1$.

Resulta evidente que Mersenne no había comprobado los números de su lista. Euler en 1738, [9] prueba que Cataldi también estaba equivocado con el 29. Algo después Euler, en 1750, prueba que la aseveración de Cataldi sobre el número 31 era correcta, verificando que $2^{31} - 1$ es primo. En dos manuscritos publicados después de su muerte, Euler, en 1747 [10] demuestra que todo número perfecto es de la forma $2^{p-1}(2^p - 1)$, lo que demuestra la propiedad 4) de Nicómaco.

Teorema 4 (Euler)**.** *Si n es un número perfecto par, entonces $n = 2^{p-1}(2^p - 1)$, donde $2^p - 1$ es primo. Sea n un número perfecto par. Ya que n es par, puede escribirse en la forma $n = 2^{p-1}m$, donde m es impar. Ya que n es perfecto, es igual a la suma de todos sus divisores propios. Si $\sigma(n)$ es la suma de todos los*

divisores de n, entonces $\sigma(n) = 2n$. Por tanto

$$\begin{aligned} 2^p m &= \sigma(n) = \sigma(2^{p-1})\sigma(m) \\ &= (2^p - 1)\sigma(m) \end{aligned}$$

de donde

$$\sigma(m) = \frac{2^p}{2^p - 1} m = m + \frac{m}{2^p - 1}$$

Así, $\frac{m}{2^p-1}$ tiene que ser un entero y es un divisor de m. Ahora bien $\sigma(m)$ es la suma de todos los divisores de m y existen solo dos sumandos, luego m debe ser primo y $1 = \frac{m}{2^p-1}$, esto es, $m = 2^p - 1$ es primo.

En relación con la propiedad 4) de Nicómaco proporciona una facil demostración de que todos los números perfectos acaban en 6 u 8 (pero no alternativamente).

En realidad, los números perfectos acaban todos en 6 o 28, los dos primeros números perfectos.

Teorema 5. *Sea n un número perfecto de la forma $(2^p - 1)2^{p-1}$, donde $2^p - 1$ es un número primo.*

1. *Si $p = 2$ o $p \equiv 1(\mod 4)$ entonces la última cifra de n es 6*
2. *Si $p \equiv 3(\mod 4)$ entonces las dos últimas cifras de n son 28*

El primer error en la lista de Mersenne fue descubierto en 1876 por Lucas, probando que $2^{67} - 1$ era compuesto, aunque no halla sus factores. Asimismo prueba que $2^{127} - 1$ es un número primo. El procedimiento empleado por Lucas fue posteriormente convertido en algoritmo por Lehmer en 1930 y en la actualidad es la base de toda búsqueda de primos de Mersenne.

En 1883, el monje ruso Pervushin prueba que $2^{61} - 1$ era primo, luego Mersenne había errado con este.

Mientras, otros errores de Mersenne siguen apareciendo. En 1911 Powers [27] muestra que Mersenne también había errado con los primos $2^{89}-1$ y $2^{107}-1$, en 1922 Kraitchik prueba que $2^{257}-1$ no es primo

Finalmente, en 1947 la lista de Mersenne, $n < 258$, había sido verificada completamente y se había determinado que la lista correcta era:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127.$$

En los últimos años los primos de Mersenne se han buscado utilizando el siguiente test de Lucas-Lehmer [19]:

Teorema 6. *Para p un primo impar, el número de Mersenne 2^p-1 es primo si y solo si 2^p-1 divide a S_{p-1} donde $S_1 = 4$ y $S_{n+1} = S_n^2 - 2$.*

Su código en Maple®, podría ser el siguiente:

```
Lucas_Lehmer_Test:=proc(p)
local S,i,M;
 M:=Power(2,p)-1;
 S:=4;
 for i from 1 to p-2 do
 S:=S*S-2 mod M;
 end do;
 if (S=0) then RETURN(‘primo‘);
 else RETURN(‘compuesto‘);
 end if;
 end proc:
```

La teoría para este test fue iniciada por Lucas en 1876, [21] y convertida en algoritmo en 1930 por Lehmer [18].

En 1952, Robinson [32] usando un primitivo ordenador encuentra M_{521}, M_{607}, M_{1279}, M_{2203} y M_{2281}.

El algoritmo de Lucas-Lehmer es excepcionalmente rápido. Es también tan fácil de implementar que, en

1978, dos estudiantes con apenas conocimientos matemáticos, además de implementarlo fueron capaces de encontrar M_{21701}, el primo de Mersenne que hace el número 25 y un año después, uno de ellos en solitario, encontrar el siguiente, M_{23209} [25].

El 15 de mayo de 2004, Josh Findley ha encontrado el último descubierto hasta ahora, $M_{24036583}$, que tiene 7 235 733 cifras. Es ahora el mayor número primo conocido. Para hacerse una idea del tamaño del número, baste decir que se necesitan 137 folios para imprimirlo o 226 días para leer el número leyendo 8 horas cada día.

Los números perfectos, como los matemáticos perfectos, escasean, hasta el momento solo se han encontrado 41.

Relacionadas con los números perfectos, algunas preguntas están hoy aún sin responder

Conjetura 1. *No existen números perfectos impares.*

Este es, probablemente, el problema más antiguo en todas las matemáticas que está sin resolver.

Conjetura 2. *Existen infinitos primos de Mersenne y por tanto infinitos números perfectos pares.*

Conjetura 3. *Existen infinitos compuestos de Mersenne.*

Mientras, la tediosa búsqueda de primos de Mersenne, y por consiguiente de números perfectos, continúa.

3. Primos de Fermat

Fermat, en su estudio de los números de la forma $2^n - 1$, comprueba el siguiente resultado:

	p	cifras M_p	cifras P_p	año	descubridor
1	2	1	1		
2	3	1	2		
3	5	2	3		
4	7	3	4		
5	13	4	8	1536	Johan Müller
6	17	6	10	1536	Johan Müller
7	19	6	12	1588	Cataldi
8	31	10	19	1772	Euler
9	61	19	37	1883	Pervushin
10	89	27	54	1911	Powers
11	107	33	65	1914	Powers
12	127	39	77	1876	Lucas
13	521	157	314	1952	Robinson
14	607	183	366	1952	Robinson
15	1279	386	770	1952	Robinson
16	2203	664	1327	1952	Robinson
17	2281	687	1373	1952	Robinson
18	3217	969	1937	1957	Riesel
19	4253	1281	2561	1961	Hurwitz
20	4423	1332	2663	1961	Hurwitz
21	9689	2917	5834	1963	Gillies
22	9941	2993	5985	1963	Gillies
23	11213	3376	6751	1963	Gillies
24	19937	6002	12003	1971	Tuckerman
25	21701	6533	13066	1978	Noll,Nickel
26	23209	6987	13973	1979	Noll
27	44497	13395	26790	1979	Nelson,Slowinski
28	86243	25962	51924	1982	Slowinski
29	110503	33265	66530	1988	Colquitt,Welsh
30	132049	39751	79502	1983	Slowinski
31	216091	65050	130100	1985	Slowinski
32	756839	227832	455663	1992	Slowinski,Gage
33	859433	258716	517430	1994	Slowinski,Gage
34	1257787	378632	757263	1996	Slowinski,Gage
35	1398269	420921	841842	1996	Armengaud, Woltman,...
36	2976221	895932	1791864	1997	Spence, Woltman,...
37	3021377	909526	1819050	1998	Clarkson, Woltman,...
38	6972593	2098960	4197919	1999	Hajratwala, Woltman,...
39	13466917	4053946	8107892	2001	Cameron, Woltman,...
40	20996011	6320430	12640858	2003	Shafer, Woltman,...
41	24036583	7235733	14471465	2004	Findley, Woltman,...

CUADRO 1. Números primos de Mersenne y números perfectos

Teorema 7. *Si* $2^n + 1$ *es un número primo, entonces* n *es una potencia de* 2.

Si $n = qr$*, donde* q *es un divisor impar de* n *y* r *es par, entonces*

$$2^n+1 = (2^r)^q+1 = (2^r+1)(2^{r(q-1)}-2^{r(q-2)}+\cdots+1)$$

Ya que $1 < 2^r+1 < 2^n+1$*, vemos que* 2^n+1 *no puede ser un primo.*

Los números $F_k = 2^{2^k}+1$ son, ahora, llamados números de Fermat. En una de sus cartas a Mersenne, conjetura que son primos y verifica que los cinco primeros

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537,$$

son primos.

En 1732, Euler [8] comprobó que el sexto número de Fermat, $F_5 = 4\ 294\ 967\ 297 = 641 \cdot 6\ 700\ 417$ no es primo. Hasta el momento no se ha encontrado ningún otro número de Fermat primo.

Para los números de Fermat existe un algoritmo específico muy rápido que es el test de Pepin [26], que en Maple® es

```
test_pepin:=proc(n)
local m,k;
‘mod‘:=mods;
m:=Power(2,Power(2,n))+1;
if Power(3,(m-1)/2) mod m=-1
 then return(‘es primo‘);
 else return(‘es compuesto‘);
end if;
end proc:
```

Ya que los números de Fermat que iban apareciendo eran compuestos, el objetivo marcado a continuación fue descomponerlos en primos.

A pesar del resultado de Lucas, quien en 1878 probó que todo factor de F_n es de la forma $k \cdot 2^{n+2} + 1$, hasta la fecha, solo unos pocos de ellos han podido ser factorizados.

Nuevamente tenemos algunas preguntas sin contestar en forma de conjeturas.

Conjetura 4. *Solo un número finito de números de Fermat son primos.*

Conjetura 5. *Los únicos primos de Fermat son* 3, 5, 17, 257, 65537.

3.1. Polígonos construibles y primos de Fermat. En matemáticas, un polígono constructible es un polígono regular que puede construirse con regla (sin marcas de numeración) y compás. Por ejemplo, un pentágono regular es constructible con regla y compás mientras que un heptágono no lo es.

La pregunta que nos queremos plantear es ¿qué polígonos regulares son constructibles?

La construcción de un triángulo equilátero es sencilla y era conocida desde la antigüedad. La construcción del pentágono regular viene descrita en los Elementos de Euclides.

Si bien Gauss en 1796 prueba que el polígono regular de 17 lados es constructible, sin embargo no dice como hacerlo. La primera construcción es debida a Erchinger, unos pocos años después del trabajo de Gauss.

La primera construcción explícita del polígono regular de 257 lados es debida a F.J. Richelot (1832) y la del polígono regular de 65537 lados a J. Hermes (1894).

En 1801, Gauss,en su obra «Disquisitiones Arithmeticae» [12], formula una condición suficiente para la constructibilidad de los polígonos regulares:

Teorema 8 (Gauss)**.** *Un polígono regular de n lados puede construirse con regla y compás si n es el producto de una potencia de 2 y cualquier producto de primos de Fermat distintos.*

Gauss conjetura que esta condición también es necesaria, lo que sería probado por Pierre Wantzel en (1836) [36]. Así un polígono regular de n lados es constructible si

$$n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, \ldots$$

y no lo será si

$$n = 7, 9, 11, 13, 14, 18, 19, 21, 22, 23, 25, \ldots$$

De la imposibilidad de construir un polígono regular de 9 lados se deduce inmediatamente la imposibilidad de trisecar un ángulo de 120 grados, aunque aún en la actualidad numerosos aficionados a las matemáticas se empeñan en querer publicar métodos de trisecar ángulos, cuadricular un círculo o duplicar un cubo. Un ejemplo cercano lo tenemos en un programa del Canal Sur de TV, el día 3 de enero de 2005.

4. Números primos y algoritmos eficientes

Un test de primalidad es un algoritmo que, dado un entero n, decide si n es primo o no. El algoritmo más sencillo está basado en la criba de Erastótenes, pero es muy ineficiente cuando n es un número grande.

En 200 AC el matemático griego Erastótenes idea un procedimiento para calcular primos llamado la criba de Erastótenes, que en Maple® es.

```
test_erastotenes:=proc(n::integer)
local i;
if n<=1 then
return(‘n debe ser > 1‘);
end if;
if n=2 then return(‘primo‘); end if;
for i from 3 by 2 to floor(sqrt(n)) do
 if (irem(n,i)=0) then
  return (‘compuesto‘);
 end if;
end do;
return (‘primo‘);
end proc:
```

Para números pequeños, el test es muy eficiente, pero para números grandes es muy ineficiente. Por ejemplo, para un número con 50 cifras, el tiempo de ejecución sobrepasaría la edad del universo.

Afortunadamente, existen algoritmos eficientes para determinar si n es primo. Los más usados son probabilísticos; proporcionan la respuesta correcta con muy alta probabilidad. Todos los algoritmos eficientes para comprobar la primalidad están basados, de alguna manera, en el teorema pequeño de Fermat.

Los siguientes desarrollos importantes fueron hechos por Fermat al comienzo del Siglo XVII. Ideó un nuevo método para factorizar números grandes y así por ejemplo consiguió factorizar el número

$$2\,027\,651\,281 = 44\,021 \cdot 46\,061.$$

Fue Euler quien realmente proporcionó la primera demostración, de lo que ahora es conocido como el teorema pequeño de Fermat (para distinguirlo de su llamado último teorema). Este prueba la mitad de lo

que se conoce como hipótesis china que data de 2000 años antes y que dice,

> un entero n es primo si y solo si el número $2^n - 2$ es divisible por n.

La otra mitad es falsa, ya que, por ejemplo, $2^{341} - 2$ es divisible por 341 pero sin embargo $341 = 31 \cdot 11$ no es primo.

El teorema pequeño de Fermat proporciona una poderosa herramienta para saber si un número es compuesto: dado $n > 1$, elegimos $b > 1$ y calculamos b^{n-1} módulo n. Si el resultado no es 1 módulo n, entonces n es compuesto. Si es 1 módulo n, entonces n podría ser primo, así n es llamado pseudoprimo relativo a la base b. Un número n es llamado un pseudoprimo de Fermat si es pseudoprimo relativo a toda base $0 < b < n$.

Por el teorema pequeño de Fermat, todo primo es pseudoprimo de Fermat.

También tenemos que, por ejemplo,

- $341 = 11 \cdot 31$ es pseudoprimo relativo a 2
- $91 = 7 \cdot 13$ es pseudoprimo relativo a 3
- $217 = 7 \cdot 31$ es peudoprimo relativo a 5
- $25 = 5 \cdot 5$ es pseudoprimo relativo a 7

Desafortunadamente, existen números compuestos que son pseudoprimos de Fermat. Tales números son llamados números de Carmichael [3]. El menor de tales números es

$$561 = 3 \cdot 11 \cdot 17.$$

Si bien los números de Carmichael son extremadamente raros, menores que 25 000 000 000 solo hay 2 163 y los menores que 100 000 son

$$561, 1105, 1729, 2465, 2821, 6601,$$

$$8911, 10585, 15841, 29341, 41041,$$

$$46657, 52633, 62745, 63973, 75361,$$

ha sido demostrado en 1994 por W. R. Alford, A. Granville y C. Pomerance [1], que existen infinitos.

Con objeto de evitar los problemas que dan los números de Carmichael y por tanto aumentar la probabiblidad de no errar al declarar primo a un número que no lo sea, conviene retocar los conceptos.

Descomponemos el exponente $n-1$ en la forma $2^k \cdot e$, con e impar, y se considera la sucesión:

$$p_0 = ae, p_1 = a^2e, p_2 = a^4e, p_3 = a^8e, \ldots, p_k = a^n - 1$$

(efectuando todos los cálculos módulo n). Cada p_i ($i > 0$) es el cuadrado del anterior, luego si n es primo:

- el último término, p_k, de la sucesión vale 1 (por el teorema pequeño de Fermat) ;
- la ecuación $x^2 = 1 (\mod n)$ tiene exactamente dos soluciones, 1 y -1.

Se deduce fácilmente que dos casos, y solo dos, son posibles para la sucesión de los p_i cuando n es primo:

- $p_0 = 1$, y por tanto para todo i, $p_i = 1$;
- existe $i < k$ tal que $p_i = -1$, y por tanto para todo $j > i$, $p_j = 1$.

Si la sucesión de los p_i no verifica ninguna de estas dos condiciones, n es con toda certeza compuesto; si por contra verifica una de estas dos condiciones, n puede ser primo y se dice que n es fuertemente pseudoprimo para la base a. En Maple® tenemos

```
test_fpp := proc(p,a)
 local j,m,b,i,s;
 `mod`:=mods;
 i := 0;
```

```
m := p-1;
while mod(m,2)=0 do
m := m / 2;
i := i+1;
end do;
b :=  Power(a,m) mod p;
if ( b=1 or b=-1 ) then
RETURN(1):
end if;
for j from 1 to (i-1) do;
b := Power(b,2) mod p;
if b = -1 then
RETURN(1):
end if;
if b = 1 then
RETURN(0):
end if;
end do:
RETURN(0):
end proc:
```

En particular, todo número fuertemente pseudoprimo es un pseudoprimo de Fermat y todo primo es fuertemente pseudoprimo.

Además hemos evitado los incómodos números de Carmichael, pues es facil probar que no existen números compuestos que sean fuertemente pseudoprimos.

Rabin en 1980 [28], prueba que si n es compuesto, entonces n es fuertemente pseudoprimo para la base b para a lo sumo un $25\,\%$ de los elementos $b \in \{1, \ldots, n-1\}$.

Aplicando la anterior proposición a k bases, tendremos que la probabilidad de equivocarnos es menor que $(1/4)^k$ y, por ejemplo, para $k = 50$, tendríamos que dicha probabilidad de error sería $0{,}78886 \cdot 10^{-30}$, que es menor que la probabilidad de error del procesador de nuestro ordenador.

Como resultado de estas observaciones, obtenemos un algoritmo eficiente de tipo probabilístico para comprobar la primalidad.

Este algoritmo es conocido como el algoritmo de Miller-Rabin, que en Maple® se puede escribir como

```
test_mr := proc(n)
 local j,tries, result;
 tries := 50;
 if(n<2) then
 RETURN(‘n\’umero no v\’alido‘)
 end if;
 if(n=2) then
 RETURN(‘es primo‘)
 end if;
 if mod(n,2)=0 then;
 RETURN(‘es compuesto‘);
 end if;
 for j from 1 to tries do;
 result := test_fpp(n,j);
 if (result = 0) then
 RETURN(‘es compuesto‘);
 end if;
 end do;
 RETURN(‘es probablemente primo‘);
 end proc:
```

El método es tan rápido que no existe ninguna razón para guardar una gran lista de números primos

en el ordenador, pues se tardaría más en leer el fichero que en comprobar la primalidad.

En 1993, Jaeschke [16] ha probado que para todo número n menor que 341 550 071 321, si es fuertemente pseudoprimo para las bases 2, 3, 5, 7, 11, 13, 17, entonces n es primo, convirtiéndose el test de Miller-Rabin en determinista para estos números.

Además en el supuesto de que la hipótesis de Riemann generalizada fuera verdadera [23], [2] tendriamos que si n es fuertemente pseudoprimo para toda base $a < 2(\ln(n))^2$, entonces n es primo. El test de Miller-Rabin, sería, en este supuesto, determinista.

Manindra Agrawal y dos de sus estudiantes, Nitin Saxena y Neeraj Kayal, han hallado en 2002 un algoritmo determinista en tiempo polinómico para probar si un número es primo o no.

Una de las características principales de este resultado es que la prueba no es demasiado compleja ni demasiado larga (su «preprint» tiene sólo 9 páginas de longitud), y depende de un uso muy innovador y perspicaz del teorema pequeño de Fermat.

Teorema 9. *Supongamos que a y p son enteros primos relativos, con $p > 1$. p es primo si y solo si $(x - a)^p \equiv (x^p - a)(\mod p)$*

Si p es primo, entonces p divide a $\binom{p}{r}$ para $r = 1, 2, \ldots p-1$. Esto demuestra que $(x-1)^p = (x^p - a^p)(\mod p)$, y la ecuación anterior se sigue del teorema pequeño de Fermat. Por otro lado, si $p > 1$ es compuesto, entonces tiene un divisor primo, q. Sea q^k la mayor potencia de q que divide a p. Entonces q^k no divide a $\binom{p}{q}$ y es primo relativo con a^{p-q}, luego el coeficiente del término x^q en el lado izquierdo de la ecuación en el teorema es no nulo, pero es nulo en el de la derecha.

Sin embargo por el momento sigue siendo más rápido usar el test probabilístico de Miller-Rabin.

4.1. El sistema RSA de encriptación. La idea de la criptografía de clave pública nace en 1976. La idea es trabajar con dos claves separadas, e y d. La clave e es usada para encriptar y la clave d es usada para desencriptar. Una persona que quiere recibir mensajes cifrados genera un par de claves (e, d), publica e (la «clave pública») y mantiene en secreto d (la «clave secreta»). Así, cualquiera puede usar e para encriptar un mensaje, pero solo la persona autorizada que posee la clave d es capaz de desencriptar el mensaje.

El esquema de encriptación más popular en la actualidad es el sistema RSA. Fue inventado en 1977 por Ron Rivest, Adi Shamir, y Leonard Adleman. Su seguridad radica en la dificultad actual de factorizar números grandes en primos.

Para generar las claves, hacemos lo siguiente: se eligen dos números primos grandes p y q, y se hace su producto $n = pq$ que es llamado el módulo. Recordemos que $\varphi(n) = (p-1)(q-1)$. Se elige aleatoriamente un número e, con $1 < e < n$. A continuación se elige otro número d tal que $ed \equiv 1 (\mod \varphi(n))$. Si desgraciadamente e no tiene inverso, elegimos aleatoriamente otro e. La clave pública es el par (n, e) y la clave privada es d. Los números p y q deben permanecer secretos o sería posible calcular $\varphi(n)$ y así d, a partir de (n, e).

Un mensaje es un elemento $m \in \{0, \ldots, n-1\}$, por ejemplo su representación en ASCII (donde cada carácter es un número comprendido entre 0 y 255) es interpretado como un entero escrito en la base 256.

Para encriptar m, calculamos

$$c \equiv m^e (\mod n).$$

El mensaje encriptado c también es llamado el «ciphertext» , y el mensaje original m es llamado el «plaintext» . Notemos que para efectuar la encriptación solo necesitamos conocer (n, e) y, lógicamente, el mensaje, m.

Para descifrar c, calculamos

$$m' \equiv c^d (\mod n).$$

Los siguientes dos resultados nos revelan las razones del funcionamiento del sistema

Teorema 10. *Sean $p \neq q$ dos primos diferentes y sea $x \in \mathbb{Z}$. Si $x \equiv 1 (\mod p)$ y $x \equiv 1 (\mod q)$, entonces $x \equiv 1 (\mod pq)$.*

Por el teorema chino del resto, existe un único $x \in \mathbb{Z}_{pq}$ tal que $x \equiv 1 (\mod p)$ y $x \equiv 1 (\mod q)$. Ya que 1 es tal número, se deduce que $x = 1$ en $\mathbb{Z}_{pq}$.

Teorema 11. *El mensaje descifrado, m', es el mismo que el mensaje original, $m \in \mathbb{Z}_n$.*

$$m' \equiv c^d \equiv m^{ed} (\mod n).$$

Así, necesitamos demostrar que $m^{ed} \equiv m (\mod n)$. En primer lugar veamos que $m^{ed} \equiv m (\mod p)$. Si $p \mid n$, esto es trivial. Supongamos por tanto que $p \nmid n$. Entonces por el teorema pequeño de Fermat, tenemos $m^{p-1} \equiv 1 (\mod p)$. Pero $(p-1) \mid n \mid (ed-1)$, luego $m^{ed-1} \equiv 1 (\mod p)$, luego $m^{ed} \equiv m (\mod p)$. Análogamente tenemos que $m^{ed} \equiv m (\mod q)$. Finalmente por 1., tenemos que $m^{ed} \equiv m (\mod pq)$.

La seguridad del sistema se basa en que en el momento actual no existe ningún procedimiento eficiente para factorizar números grandes. Baste recordar

que en 1999, en el ataque al sistema RSA-155, esto es, para factorizar un número de 155 cifras, se necesitaron 290 ordenadores conectados en red y un superordenador trabajando durante 4 meses. La potencia de computación necesaria fue estimada en 8000 Mips-año (un Mips es un millón de instrucciones de procesador por segundo).

En la actualidad se suele usar el sistema RSA-300, esto es, n con 300 cifras. Cualquier actividad en Internet que requiera seguridad usa dicho sistema, como pueden comprobar con un programa tan popular como Microsoft Messenger®.

5. El último teorema de Fermat

Antes de comenzar con esta sección, debo recomendar la lectura del libro «El último teorema de Fermat», de Simon Singh, [34] del que he extraido algunos pasajes.

El último teorema de Fermat (también llamado el gran teorema de Fermat) es uno de los teoremas más famosos en la Historia de las Matemáticas. El enunciado del teorema dice: la ecuación

$$x^n + y^n = z^n$$

no tiene soluciones no nulas en los enteros si $n > 2$.

Mientras que el propio teorema no tiene ningún uso directo conocido (por ejemplo, no ha sido utilizado para probar ningún otro teorema) sin embargo sus continuos y fallidos intentos de demostración han iniciado la investigación sobre muchos tópicos matemáticos importantes.

La ecuación $x^2 + y^2 = z^2$ tiene muchas soluciones donde x, y, y z son números enteros, por ejemplo,

$3^2 + 4^2 = 5^2$, o $5^2 + 12^2 = 13^2$. Realmente tiene infinitas soluciones:

$$x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2$$

para todo $a > b > 0$ con m.c.d.$(a, b) = 1$.

La demostración descansa en el siguiente resultado:

Lema 12. *Si a, b son números naturales primos entre sí, y si $ab = u^n$ para algún natural u, entonces $a = v^n$ y $b = w^n$ para algunos naturales v, w.*

Supongamos que $a = p_1^{e_1} \cdots p_r^{e_r}$ y $b = q_1^{f_1} \cdots q_s^{f_s}$ las factorizaciones en primos de a y b. Ya que a y b son primos entre sí, los primos p_i y q_j son diferentes. Ya que $ab = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$, si $ab = u^n$, por la unicidad de la factorización $e_1 = \cdots = e_r = f_1 = \cdots f_s$ y $u = p_1 \cdots p_r q_1 \cdots q_s$. Luego es suficiente tomar $v = p_1 \cdots p_r$ y $w = q_1 \cdots q_s$.

Tales soluciones son llamadas ternas pitagóricas, porque según el teorema de Pitágoras tal terna representa los lados de un triángulo rectángulo.

En una tabla de arcilla babilónica fechada hace 3,500 años (cerca de 1,000 años antes de Pitágoras) se encuentra una lista de quince ternas pitagóricas.

Es razonable suponer, por el tamaño de los números en la lista, que su creador tuvo un sistema para encontrar las ternas pitagóricas, pero no sabemos su método. Una técnica para crear la lista infinita de todas las ternas pitagóricas aparece en los Elementos de Euclides.

El problema de encontrar ternas pitagóricas es un ejemplo de un tipo de ecuaciones que interesó a Diofanto de Alejandría, matemático griego del siglo tercero. En estas ecuaciones, el número de incógnitas

FIGURA 2. Tabla de arcilla Plimpton 322

es mayor que el número de ecuaciones, y la solución buscada debe estar en los números enteros. Sólo diez de los trece volúmenes de su tratado Arithmetica han sobrevivido a las diversas destrucciones de la biblioteca de Alejandría. En 1621, Claude Bachet publicó una traducción latina de los seis que en aquel momento se habían encontrado. En 1982, la editorial Springer ha publicado los cuatro últimos volúmenes hallados [33].

Al leer el libro de Diofanto, Fermat pensó sobre una versión más general de la ecuación pitagórica, donde la potencia sea $3, 4, \ldots$ y escribió en 1637 en su copia de la traducción realizada por Bachet del tratado Arithmetica de Diofanto : .

> Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem

> nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.
>
> Es imposible escribir un cubo como la suma de dos cubos o escribir una cuarta potencia como la suma de dos cuartas potencias o escribir, en general, cualquier potencia mayor que dos como la suma de dos potencias iguales.
>
> Poseo una prueba en verdad maravillosa para esta afirmación a la que este margen viene demasiado estrecho.

Fermat no se molestaba en publicar su trabajo, y tan solo un ensayo matemático escrito por él fué publicado en vida. A su muerte, su hijo se dedicó a publicar todos sus escritos, incluso la traducción de Bachet del libro de Diofanto, con todas las observaciones escritas por Fermat en los márgenes del libro. La costumbre de Fermat de no proporcionar demostraciones a sus teoremas exigió mucho trabajo de sus contemporáneos y de matemáticos de las generaciones siguientes, especialmente Euler, que debieron probar esos teoremas.

Relativo al último teorema, Fermat sólo dejó la demostración del siguiente resultado: El área de un triángulo rectángulo no puede ser un cuadrado. Esto es, no existen números enteros x, y, z con $x^2 + y^2 = z^2$ y $xy/2$ un cuadrado, que podemos expresar en el siguiente teorema como

Teorema 13 (Fermat)**.** *Las únicas soluciones enteras de la ecuación*

$$X^4 + Y^4 = Z^2$$

son las triviales, esto es, x, y, z enteros con $xyz = 0$.

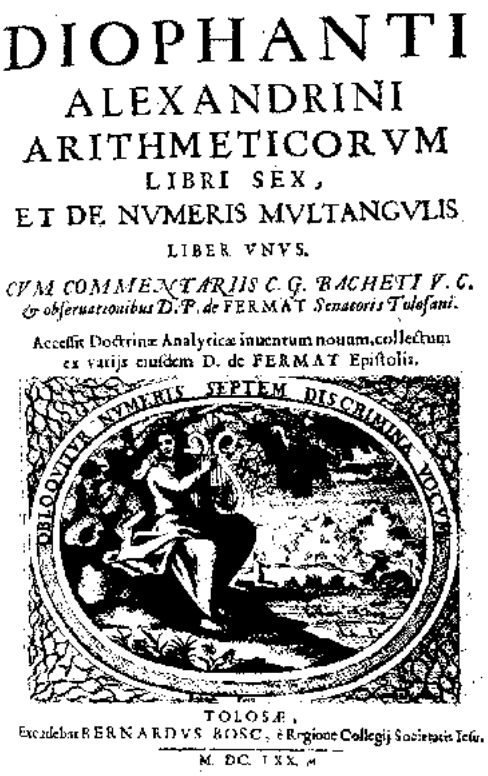
DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obſeruationibus D. P. de FERMAT Senatoris Tolosani.
Acceſſit Doctrinæ Analyticæ inuentum nouum, collectum
ex variis eiuſdem D. de FERMAT Epiſtolis.
DEMONSTRATIONEM NVMERIS SEPTEM DISCRIMINA VOLVVNT
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Ieſu.
M. DC. LXX.

FIGURA 3. Traducción de Bachet del libro de Diofanto con las anotaciones de Fermat

Supongamos que x, y, z *es una solución no trivial y supongamos que es minimal en el sentido de que* $|z|$ *es minimal y por tanto* $\text{m.c.d.}(x, y, z) = 1$. *Sin pérdida de generalidad podemos suponer que* x, y, z *son positivos y que* x *o* y *es impar. Supongamos que* x *es impar. Por el caso* $n = 2$, *existen enteros* $a > b > 0$ *con* $\text{m.c.d.}(a, b) = 1$ *y*

$$x^2 = a^2 - b^2,\ y^2 = 2ab,\ z = a^2 + b^2.$$

Consideremos la primera ecuación, $x^2 + b^2 = a^2$. *Ya que* $\text{m.c.d.}(x, a, b) = 1$, *de nuevo por el caso* $n = 2$ *obtenemos*

$$x = c^2 - d^2,\ b = 2cd,\ a = c^2 + d^2,$$

para ciertos enteros, $c > d > 0$ *con* $\text{m.c.d.}(c, d) = 1$. *Sustituyendo en la ecuación* $y^2 = 2ab$ *obtenemos*

$$y^2 = 2ab = 2(2cd)(c^2 + d^2),$$

esto es,

$$(y/2)^2 = cd(c^2 + d^2).$$

Ya que $\text{m.c.d.}(c, d, c^2 + d^2) = 1$ *y su producto es un cuadrado, existen enteros* u, v, w *tales que*

$$c = u^2,\ d = v^2,\ c^2 + d^2 = w^2,$$

de donde $\text{m.c.d.}(u, v, w) = 1$ *y*

$$u^4 + v^4 = w^2.$$

Hemos obtenido por tanto una nueva solución con $w \neq 0$, $y \mid w \mid < w^2 = c^2 + d^2 = a < a^2 < \mid z \mid$, *lo que contradice la minimalidad de* z.

De aquí es fácil deducir el caso $n = 4$.

Lo más interesante es su procedimiento de demostración, ahora llamado del descenso infinito, que será utilizado en los sucesivos intentos de encontrar la solución para los demás casos.

Además de este resultado se sigue que solo es necesario probar el teorema para n primo impar.

Teorema 14. *El último teorema de Fermat es verdadero si y solo si para todo primo* $p > 2$ *la ecuación*

$$X^p + Y^p = Z^p$$

solo tiene soluciones triviales, esto es, soluciones enteras x, y, z *con* $xyz = 0$. *Si el teorema de Fermat es*

verdadero, en particular es verdadero para todo primo $p > 2$. *Sea ahora* $n > 2$ *y sean* x, y, z *enteros solución a la ecuación*

$$X^n + Y^n = Z^n.$$

Si n *es divisible por un primo impar* p, $n = pm$, *entonces tenemos*

$$(x^m)^p + (y^m)^p = (z^m)^p.$$

Por tanto $(xyz)^m = 0$, *de donde* $xyz = 0$. *Si* n *no es divisible por un primo impar, entonces es una potencia de* 2 *y como* $n > 2$, *debe ser divisible por* 4, $n = 4m$. *Por tanto tenemos*

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

Por el caso $n = 4$, *tenemos que* $(xyz)^m = 0$, *de donde* $xyz = 0$.

Euler, el genio más grande de su siglo, apenas puede probar el caso $n = 3$ y trata con desesperación de encontrar en la casa de Fermat algún otro papel escrito por Fermat que hubiese podido pasar desapercibido a su hijo cuando publicó su obra completa.

A lo largo de la vida de Euler su investigación matemática vino a suponer una producción de unas 800 páginas anuales de promedio; pocos matemáticos superan la producción de este hombre (escribió más de 886 libros y artículos).

En 1753 Euler escribe a Goldbach comunicándole que tenía una demostración para el caso $n = 3$. Sin embargo la demostración que aparece en su libro «Anleitung zur Algebra» (1770) [10] contenía un error. El error de Euler es subsanable utilizando argumentos que aparecen en demostraciones de otros de sus resultados.

En los elementos de Euclides, en el libro VII, Proposición 32, encontramos:

Teorema 15. *Todo número o bien es número primo o es medido por algún número primo.*

que nos dice que todo número natural se puede factorizar en números primos y en la Proposición 30 del libro VII:

Teorema 16. *Si dos números, al multiplicarse entre sí, hacen algún número y algún número primo mide a su producto, también medirá a uno de los números iniciales.*

que nos dice que la factorización es única.

Euler necesita hallar cubos de la forma

$$p^2 + 3q^2.$$

Para ello demuestra que, para todo a, b si ponemos

$$p = a^3 - 9ab^2,\ q = 3(a^2b - b^3)$$

entonces

$$p^2 + 3q^2 = (a^2 + 3b^2)^3.$$

Realmente está calculando con números de la forma

$$a + b\sqrt{-3}.$$

Afortunadamente para él, pues sin probarlo y ese es el error anteriormente mencionado, este conjunto de números tiene también la propiedad de factorización única.

En 1825, Dirichlet [20] prueba y publica el caso $n = 5$.

El caso $n = 7$ es resuelto por Gabriel Lamé (1795-1870) en 1839.

Lamé a principios de 1847, presenta a los miembros de la Academia de Ciencias de Francia una demostración general del teorema. Lamé menciona que

llegó al resultado después de discutirlo con su colega Joseph Liouville (1809-1882).

Lamé imitando la demostración de Euler para $p = 3$, considera la factorización

$$X^p + Y^p = (X + Y)(X + \eta Y) \cdots (X + \eta^{p-1} Y) = Z^p.$$

donde $\eta^p = 1$, $\eta \neq 1$,

A continuación, trabaja en el conjunto

$$\mathbb{Z}[\eta] = \{a + b\eta\}$$

como si tuviese una unicidad de factorización, y de ahí el error, pues necesita usar el siguiente resultado

Lema 17. *Si $a, b \in \mathbb{Z}[\eta]$ son primos entre sí, y si $ab = u^p$ para algún $u \in \mathbb{Z}[\eta]$, entonces $a = v^p$ y $b = w^p$ para algunos $v, w \in \mathbb{Z}[\eta]$.*

cuya demostración se basa en la unicidad de la factorización.

Inmediatamente después de la presentación, Liouville sugiere que el problema de esta aproximación está en la unicidad de la factorización en primos que es necesaria y que duda que sea cierto.

En las semanas siguientes, Lamé y Cauchy, tratan en vano de arreglar la demostración, intentando dar una prueba de la unicidad de la factorización.

Poco después Ernest Edward Kummer prueba que el error de Lamé no tiene arreglo, por ejemplo para $p = 23$, la factorización no es única; realmente falla para todo primo $p \geq 23$. Es fácil ver que

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

En 1847, usando su teoría de números ideales prueba:

Teorema 18 (Kummer)**.** *Sea $p > 2$ un primo. Si p es un primo regular, esto es, no divide a los numeradores*

de los números de Bernoulli $B_2, B_4, \ldots, B_{p-3}$, entonces la ecuación

$$X^p + Y^p = Z^p$$

admite solo soluciones triviales, esto es, x, y, z enteros con $xyz = 0$.

Los números de Bernoulli pueden obtenerse mediante la fórmula recursiva

$$B_0 = 1, \ \sum_{j=0}^{n} \binom{n+1}{j} B_j = 0$$

Sus primeros valores son

$$B_2 = \frac{1}{6}, \ B_4 = -\frac{1}{30}, \ B_6 = \frac{1}{42}, \ B_8 = -\frac{1}{30},$$

$$B_{10} = \frac{5}{66}, \ B_{12} = -\frac{691}{2730}, \ B_{14} = \frac{7}{6}, \ B_{16} = -\frac{3617}{510}$$

De los valores de los primeros números de Bernoulli, Kummer deduce que el teorema es cierto para los números primos $p < 100$ salvo para $p = 37$, 59 y 67. Por ejemplo, para $p = 37$, tenemos que

$$B_{32} = -\frac{7709321041217}{510}$$

y

$$7\,709\,321\,041\,217 = 37 \cdot 683 \cdot 305\,065\,927.$$

En 1857, Kummer también consigue probar los casos pendientes, con lo que el teorema que da probado para todo primo menor que 100.

Desgraciadamente Jensen, en 1915, prueba que existen infinitos primos no regulares.

La importancia de los números ideales sobrepasa el alcance de la Teoría de Números, y sirve para que Richard Dedekind en 1876 en la tercera edición de su libro «Lecciones sobre teoría de números» [7] desarrolle una rama matemática separada, la Teoría de

Ideales. Más adelante el concepto fue extendido por David Hilbert y especialmente por Emmy Noether.

En la línea principal de la historia, hay a principios del siglo XX un paso inesperado de comedia que le da nueva vida al problema. Paul Wolfskehl, el hijo de una familia de industriales alemanes, con una gran fortuna propia, era también aficionado a la Matemática, y uno de los tantos que había intentado suerte con el teorema. En algún momento de su juventud se obsesionó con una mujer muy hermosa, que lo rechazó. El joven Wolfskehl, desesperado, planeó suicidarse con un tiro en la cabeza que se daría estrictamente a medianoche.

Mientras que le llegaba su hora, como no disponía ni de TV ni de ordenador personal, decidió ponerse a leer un libro de Kummer, ya que le pareció la lectura apropiada para una ocasión tan solemne.

Le pareció encontrar entonces una pequeña laguna en una implicación, se le ocurrió la idea de que Kummer tal vez se hubiera equivocado, lo que reabriría la esperanza de una demostración elemental, y hasta la madrugada estuvo haciendo cálculos febriles. Kummer, por supuesto, no se había equivocado, pero a Wolfskehl se le había pasado la hora del suicidio y descubrió que inesperadamente le habían vuelto las ganas de vivir. Rompió las cartas de despedida de la noche anterior y rehizo ese mismo día su testamento. A su muerte, su familia descubrió que había legado buena parte de su fortuna para quien publicara la primera demostración completa del teorema de Fermat. El premio de 100 000 marcos, fijaba cien años de plazo y tenía como fecha límite setiembre del año 2007.

A pesar de los numerosos premios ofrecidos a quien diese una demostración del teorema, este seguía sin

ser resuelto y con el dudoso honor de ser el teorema con mayor número de demostraciones erróneas. Entre 1908 y 1912 fueron publicadas más de 1 000 demostraciones falsas.

Un afamado matemático que era uno de los que recibía la avalancha de demostraciones erradas, decidió devolver los manuscritos con una anotación en el margen:

> He hallado una refutación verdaderamente admirable de su demostración, pero este margen es demasiado exiguo para contenerla.

En 1993, aplicando las técnicas de Kummer y usando ordenadores, se comprobó la veracidad del teorema para $n < 4\,000\,000$.

Taniyama y Shimura, en 1955, comienzan a conectar dos ramas de la matemática hasta entonces totalmente inconexas: las curvas elípticas y las formas modulares. El posterior trabajo de Shimura, le hace convencerse, aunque no fue capaz de probarlo, de que toda curva elíptica es modular. Nace así la conjetura de Taniyama-Shimura.

Las curvas elípticas son curvas definidas por ecuaciones de la forma

$$Y^2 = aX^3 + bX^2 + cX + d.$$

Una de las propiedades más destacadas de las curvas elípticas es que, dadas unas cuantas soluciones enteras de las ecuaciones, es posible combinarlas y deducir de ellas otras soluciones.

En 1983, Gerd Faltings demostró la conjetura de Mordell. La conjetura de Mordell podemos expresarla en la siguiente forma:

Teorema 19 (Mordell-Faltings)**.** *Toda curva algebraica no singular con coeficientes racionales tiene un número finito de puntos racionales si su género es* ≥ 2

Ya que la ecuación de Fermat, $X^n + Y^n = Z^n$, corresponde a una curva de género $(n-1)(n-2)/2$, la conjetura de Mordell implica que, en caso de que la ecuación tuviera alguna solución entera, habría de tener como mucho un número finito de ellas.

Aunque el progreso es grande, ya que ahora sabemos que como mucho el número de soluciones si las hubiere es finito, el problema general sigue abierto.

Gerhard Frey [11] en 1985, logra establecer una conexión crucial entre el último teorema de Fermat y las curvas elípticas.

Sea p un número primo impar. Frey considera $Y^2 = X(X-a^p)(X+b^p)$, donde a, b, c satisfacen $a^p + b^p = c^p$, y m.c.d.$(a,b,c) = 1$. Sin pérdida de generalidad, podemos suponer que a es par y $b \equiv 1 \pmod{p}$. Esta curva es una curva elíptica sobre $\mathbb{Q}$. Si reducimos la ecuación módulo un primo q, obtenemos una curva elíptica sobre el cuerpo finito $\mathbb{Z}_q$. Esta curva puede ser singular con un nodo o una cúspide, dependiendo de que la ecuación $X(X-a^p)(X+b^p)$ tenga 2 o 3 raíces iguales en $\mathbb{Z}_p$. En este caso las raíces son $0, a^p, -b^p$. Si $a^p \equiv b^p \equiv 0 \pmod{q}$, entonces $q \mid a$ y $q \mid b$, lo que es una contradicción con m.c.d.$(a,b,c) = 1$. Así la curva E de Frey es o no singular o tiene un nodo al reducirla módulo cualquier primo q. Tales curvas se dicen semiestables.

Frey conjetura que la curva no puede ser modular.

En 1986, Ribet [30] dió forma a la idea de Frey. Demostró que toda curva elíptica semiestable no es modular, de donde, ya que la curva de Frey es semiestable, no puede ser modular. Por tanto, el caso semiestable de la conjetura de Taniyama-Shimura probado por Wiles, implica que la curva es modular. Esta contradicción a su vez implica que la hipótesis de la existencia de una solución no trivial de la ecuación de Fermat debe ser errónea, y por tanto el último teorema de Fermat está probado.

En 1994, en la tercera y última de una serie de lecciones tituladas «Modular Forms, Elliptic Curves, and Galois Representations» en el «Isaac Newton Institute» en Cambridge, Andrew Wiles sorprende al auditorio comunicándoles que va a exponer la demostración del caso semiestable de la conjetura de Taniyama-Shimura.

Para no ser menos que sus antecesores, durante el proceso de revisión del trabajo, son descubiertos algunos fallos. Con la ayuda de su alumno Richard Taylor [37], y variando los métodos utilizados ve la luz finalmente una demostración rigurosa, de aproximadamente 200 páginas, en la revista «Annals of Mathematics».

A la vista de los métodos usados en la demostración, parece claro que en el caso de que Fermat hubiese dispuesto de una demostración, no se parecería en nada a la de Wiles.

En contra de lo que pudiera parecer, la historia del último teorema de Fermat no ha finalizado. Continúa la búsqueda de esa posible demostración elemental.

Finalmente, comentar que en 1999, C.Breuil, B.Conrad, F.Diamond y R.Taylor estudiantes de Andrew Wiles, han conseguido probar la «Conjetura de Taniyama-Shimura» en el caso general [5].

El sueño de Hilbert de preservar la unidad de las matemáticas y que éstas no se descompongan en ramas separadas, se plasma en la demostración del último teorema de Fermat realizada por Wiles. Para dicha demostración ha de hacer uso de varias ramas de las matemáticas, como son la variable compleja, la geometría diferencial, la teoría de representación, la geometría no euclídea, la geometría algebraica, la teoría de Galois y la teoría de números.

6. Otras conjeturas sobre primos

Finalizaremos con dos conjeturas pendientes de resolver acerca de números primos.

6.1. Conjetura de los primos gemelos. Dos primos gemelos son un par de primos de la forma $(n, n+2)$. Ejemplos son $(3,5)$, $(5,7)$, $(11,13)$.

Conjetura 6. *Existen infinitos pares de primos gemelos.*

Hardy y Littlewood han conjeturado que el número de primos gemelos $\leq n$ es

$$2\prod_{p\geq 3}\frac{p(p-2)}{(p-1)^2}\int_2^n\frac{dx}{(\ln(x))^2}$$

Los mayores primos compañeros encontrados hasta la fecha son

$$33,218,925\cdot 2,169,690-1$$

y

$$33,218,925\cdot 2,169,690+1$$

con 51,090 cifras.

6.2. Conjetura de Goldbach. Goldbach escribió una carta a Euler en 1742 sugiriendo que cualquier número mayor que 5 es la suma de tres primos. Euler replicó que esto es equivalente a que todo número par mayor que 3 es la suma de dos primos. Este problema ahora es conocido como la conjetura de Goldbach. Es fácil comprobar con los primeros números, la veracidad de la conjetura. Por ejemplo $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5$, $12 = 5 + 7$.

En 1998, Joerg Richstein ha verificado la hipótesis hasta $4 \cdot 10^{14}$, pero queda aún por probarse la conjetura.

Al tratarse de conjeturas que tienen el respaldo de un premio en metálico, se aconseja a aquellos que tengan problemas con el pago de la hipoteca de su casa, resolver dichas conjeturas.

Referencias

[1] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Ann. Math.*, 140:703–722, 1994.
[2] E. Bach. *Analityic Methods in the Analysis and Design of Number-Theoretic Algorithms*. MIT Press, 1985.
[3] R. D. Carmichael. Note on a new number theory function. *Bull. Amer. Math. Soc.*, 16:232–238, 1910.
[4] P. A. Cataldi. *Trattato de Numeri Perfetti*. Bologna, 1603.
[5] F.Diamond C.Breuil, B.Conrad and R.Taylor. On the modularity of elliptic curves over q. *J. Amer. Math. Soc.*, 14:843–939, 2001.
[6] C. J. de la Vallée Poussin. Recherches analytiques la théorie des nombres premiers. *Ann. Soc. Sci. Bruxelles*, 20:183–256, 1896.
[7] J. W. R. Dedekind. *Gesammelte Mathematishe Werke*. Vieweg, 1932.

[8] L. Euler. Methodus generalis summandi progressiones. *Comm. Acad. Sci. Petrop.*, 6:68–97, 1732.
[9] L. Euler. Observationes de theoremate quodam fermatiano aliisque ad numeros primos spectantibus. *Acad. Sci. Petropol.*, 6:103–107, 1738.
[10] L. Euler. *Opera Omnia*. Teubner, 1911-1957.
[11] G. Frey. Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Sarav. Math. Ser.*, 1:1–40, 1986.
[12] C. F. Gauss. *Disquisitiones Arithmeticae*. G. Fleischer, Leipzig, 1801. English translation by A. A. Clarke, Springer-Verlag, 1986.
[13] C. F. Gauss. *Werke*, volume Band 10, Teil I. 1863.
[14] J. Hadamard. Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Société Mathématique de France*, 24:199–220, 1896.
[15] T. L. Heath. *The Thirteen Books of Euclid's Elements*, volume II. Dover, 1956.
[16] G. Jaeschke. *On strong pseudoprimes to several bases*, volume 1993. Math. Comp., 61.
[17] A.-M. Legendre. *Essai sur la Théorie des Nombres*. Duprat, Paris, 1798.
[18] D. H. Lehmer. An extended theory of Lucas' functions. *Ann. Math.*, 31:419–448, 1930.
[19] D. H. Lehmer. On lucas's test for the primality of mersenne's numbers. *J. London Math. Soc.*, 10:162–165, 1935.
[20] P. G. Lejeune-Dirichlet. *Werke*. Reimer, 1889-1897.
[21] E. Lucas. Sur la recherche des grands nombres premiers. *Assoc. Française pour l'Avancement des Sciences; Comptes Rendus*, 5:61–68, 1876.
[22] M. Mersenne. *Cogitata Physico Mathematica*. Paris, 1644.
[23] G. Miller. Riemann's hypothesis and tests for primality. *J. Comput. System Sci.*, 13:300–317, 1976.
[24] Nicomachus. *Introduction to Arithmetic*. Ann Arbor: University of Michigan Press, m.l. d'ooge, translator edition, 1938.
[25] C.Ñoll and L.Ñickel. The 25th and 26th mersenne primes. *Math. Comp.*, 35:1387–1390, 1980.
[26] T. Pepin. Sur la formule $2^{2^n} + 1$. *C. R. Acad. Sci. Paris*, 85:329–331, 1877.

[27] R. E. Powers. The tenth perfect number. *Amer. Math. Monthly*, 18:195–197, 1911.
[28] M. O. Rabin. Probabilistic algorithm for testing primality. *J. Number Theory*, 12:128–138, 1980.
[29] H. Regius. *Utriusque arithmetices epitome*. Reiss and Sohn, 1536.
[30] K. Ribet. From the taniyama-shimura conjecture to fermat's last theorem. *Ann. Fac. Sci. Toulouse Math.*, 11:116 – 139, 1990.
[31] G. F. B. Riemann. Über die anzahl der primzahlen unter einer gegebenen grösse. *Monatsberichte der Königlichen Preussischen Akademie der Wissenschaften zu Berlin*, pages 671–680, 1859.
[32] R. M. Robinson. Mersenne and Fermat numbers. *Proc. Amer. Math. Soc.*, 5:842–846, 1954.
[33] J. Sesiano. *Books IV to VII of Diophantus' Arithmetica*. Springer, 1982. Arabic Translation Attributed to Qusta Ibn Luqa.
[34] S. Singh. *El enigma de Fermat*. Planeta, 1998.
[35] H. von Koch. Ueber die riemann'sche primzahlfunction. *Math. Ann.*, 55:441–464, 1902.
[36] M. L. Wantzel. Recherches sur les moyens de reconnaître si un problème de géométrie peut se résoudre avec la règle et le compas. *J. Math. Pures Appl.*, 1:366–372, 1836.
[37] A. Wiles and R.Taylor. Ring theoretic properties of certain hecke algebras. *Ann. Math.*, 141:553–572, 1995.

Discurso de contestación

Manuel Barros Díaz
Académico Numerario de la Sección de Matemáticas.

Excmos. e Ilmos. Sres. Académicos
Señoras y Señores

Quiero, en primer lugar, agradecer a la Academia de Ciencias Matemáticas, Fisico-Químicas y Naturales, el honor que me hace y el privilegio que me concede, de presentar al Prof. D. José Luis Bueso Montero en este solemne acto de su ingreso en la Academia.

Este privilegio resulta grato y placentero por diversas y variadas circunstancias, algunas de las cuales me gustaría comentar.

En primer lugar entre el Prof. Bueso y yo mismo, existe una relación de amistad pero también de afinidad y paralelismo. Yo lo conocí, el siglo pasado, al principio de los setenta. Fuímos casi compañeros de promoción en esta Facultad. Después, al acabar la licenciatura, coincidimos en nuestro interés por tratar de seguir estudiando, investigando. Esto, en aquellos tiempos, no se sabía muy bien lo que era, al menos en los Departamentos de Matemática pura o fundamental. Los dos coincidimos en el mismo Departamento, el de Álgebra, Geometría y Topología. En realidad eran dos Departamentos, el de Álgebra y el de Geometría y Topología, que por razones, digamos que administrativas estaban unidos formando una entidad con algo más de cincuenta profesores. Aquí, cuando digo profesores me refiero a licenciados que dábamos clases y solo eso. Había un único doctor que a su vez

era el único numerario y el resto éramos profesores no numerarios.

De la misma manera que a mí me atraía el estudio de la Geometría Diferencial, el hoy Prof. Bueso tenía una idea muy clara y una tremenda obstinación, estudiar Álgebra. Los primeros tiempos fueron duros, muy duros. No existía una mínima orientación, un simple consejo, una pequeña indicación. No había hemeroteca, cuatro revistas de Matemática se recibían y se usaban para decorar una estantería, que por otro lado era horrible.

Después y afortunadamente, dos personas de las escuelas de la Universidad de Santiago de Compostela consiguieron plazas de numerario en el Departamento. Primero, el Prof. Antonio Martínez Naveira (Geometría V, Diferencial), tuve la suerte de ser su primer discípulo oficial. Poco después, el Prof. Alfredo Rodríguez-Granjeán López-Valcarcel (hoy tristemente desaparecido) consiguió la cátedra de Álgebra y entonces se separaron los dos Departamentos. Jose Luis Bueso Montero, fue su primer discípulo en Granada. Este hecho, por similitud, también nos une. A partir de entonces, el entusiasmo, la gran capacidad y la férrea voluntad de Jose Luis Bueso por y para el Álgebra empezaron a actuar. Se puede decir, que es uno de los pioneros, una de las personas que ocupan un lugar muy destacado, uno de los responsables de la tremenda realidad que hoy es la Matemática en la Universidad de Granada.

Yo creo que José Luis Bueso Montero nació para ser matemático y con toda seguridad hubiera destacado en cualquier área de la Matemática. No obstante, donde realmente ha sido y es feliz es en el mundo del Álgebra. Posee unas condiciones excepcionales para

el estudio del Álgebra y su entusiasmo por esta materia se transmite, de manera natural, a todos los que le rodean. Con esto quiero apuntar una de sus principales características, su manera de hacer Matemática, de hacer Álgebra, es tremendamente solidaria. Con toda seguridad, hubiera desarrollado su obra de manera individualista, facultades para ello le sobran, sin embargo ha hecho partícipe de ella a una secuencia de personas, unas estudiantes otras colegas, que han colaborado con él para crear una potente escuela de Álgebra en la Universidad de Granada. Entre los primeros baste con citar a Blas Torrecillas, Pascual Jara, José Gómez Torrecillas, Francisco José Lobillo etc.

A estas alturas, debe de resultar obvio que no es mi intención la de leer el impresionante curriculum del Prof. Bueso. Estoy seguro de que este es de fácil acceso para cualquier persona interesada o curiosa. Mas bien intento corresponder, señalando de manera torpe o cuanto menos modesta, algunas de las cosas sobre el nuevo académico y sobre la obra de este que no se pueden leer directamente en aquel. Ya he hecho notar la enorme culpa que José Luis Bueso ha tenido en la creación del prestigioso grupo de Álgebra de esta Universidad.

Otro rasgo importante, al menos para mí, de su obra es el siguiente. Paralelamente a una importante lista de artículos, por él publicados, en las más prestigiosas revistas especializadas, llama la atención, por no ser ni mucho menos frecuente, el hecho de haber publicado cuatro importantes libros en otras tantas editoriales, seguramente las más importantes de ediciones matemáticas (Springer, Pitman, Marcel Dekker

y Kluwer). Este hecho, cuanto menos, refleja una cierta perdurabilidad en el trabajo del Prof. Bueso.

La labor docente e investigadora de nuestro nuevo y recién académico, se completa con la dirección de diversos proyectos de investigación financiados a nivel nacional y regional así como la organización de Congresos internacionales sobre distintos tópicos de su especialidad. No le falta ni la consecución de premios de investigación como por ejemplo el concedido por esta Academia.

El Doctor Bueso es el primer algebrista que ingresa en nuestra Academia. Pienso que es un doble acierto por parte de la misma el haberlo elegido como académico de número. En primer lugar por llenar un vacío en el amplio espectro de la Ciencia. No se podría concebir, de otra manera la universalidad de la Matemática. En segundo lugar y más importante, por haber recaído el nombramiento en la persona de José Luis Bueso Montero. El prestigio del mismo, yo creo que aumentará el de esta institución. El Álgebra estará, a partir de ahora, plenamente representada en esta Academia a través de la figura del nuevo académico.

Seguramente, este Discurso de Contestación puede parecer atípico. He tratado de no caer en la tentación de leer el amplio e importante listado de méritos que concurren en la persona del nuevo académico. Esto sería muy fácil como también lo hubiera sido para el Prof. Bueso el haber realizado una disertación sobre alguno de sus profundos trabajos de investigación. Sin embargo, su discurso de recepción como nuevo académico me ha invitado a actuar de esta manera.

En efecto, el discurso leído por el nuevo académico es una nueva prueba de su excelente formación matemática. Lejos de ser un discurso basado en una profunda disertación algebraica, el Prof. Bueso nos ha sorprendido con una deliciosa conferencia sobre números perfectos y matemáticos no tanto. Pienso que el esfuerzo que ha realizado en su preparación es de agradecer en toda su valía. Su trabajo ha servido para que aprendamos un montón de resultados seguramente muy fáciles de entender pero muy difíciles de probar. De él se pueden extraer bastantes ideas que nos permitirán entender mejor y aprender más sobre la esencia del método matemático. No es, ni mucho menos, fácil entusiasmar hablando de matemática pura. Varias razones y otros tantos tópicos se podrían proponer en este sentido. Sin embargo, quiero detenerme, sin ser ni mucho menos exhaustivo, en algunas de las cuestiones y otras tantas claves que, en mi opinión hacen a su discurso extremadamente bello.

En su discurso, el Prof. Bueso nos hace una invitación a la lectura del mismo a través de una forma de pasatiempo matemático. De una manera sencilla, nos ofrece una prueba rigurosa de la infinitud de los números primos. Sin embargo, la prueba es una coartada perfecta para que el lector aprenda el sentido de una demostración por contadicción o reducción al absurdo.

Después, usa la distribución de los números primos para introducirnos en el estudio de la función zeta y de la correspondiente conjetura de Riemann. Es posible que al lector profano le cueste entender el planteamiento del problema. Sin embargo, ya en las primeras páginas de este discurso, José Luis Bueso

nos muestra, a través de uno de los problemas más famosos de la Matemática, lo que es una conjetura y esto si es de general entendimiento. No solo eso, además nos pone al día en el estado actual del problema. Aprovecha la ocasión para desmitificar a la Matemática o mejor a los matemáticos. La primera es perfecta aunque los segundos no. Sin embargo benditos sean los errores que nos ayudan a descubrir la verdad.

A continuación y a través del discurso, nos paseamos por el paraíso de los números perfectos. Nos encontramos de bruces con unos cuantos pasatiempos (conjeturas) que nadie ha podido resolver.

Descubrimos después los números y los primos de Fermat. Un par de pasatiempos más y un hermoso resultado para la clase de dibujo. Aprendemos lo que son los algoritmos de primalidad y como se pueden usar estos en criptografía. Parece que RSA-300, esto es usando un módulo con 300 cifras, es bastante seguro.

La parte final del discurso es una bella exposición del popular último teorema de Fermat. Es seguramente el más popular problema de Matemáticas que se ha resuelto recientemente y que tiene su origen en 1637, cuando Pierre Fermat afirmó haberlo resuelto en un margen de un ejemplar de la Aritmética de Diofanto.

Como despedida, el nuevo académico nos obsequia con otro par de pasatiempos (conjeturas) muy populares pero que tampoco nadie ha podido resolver.

Yo quisiera acabar, señalando, a modo de resumen que la obra del Doctor Bueso merece ser calificada de creadora y solidaria. Su excelente espíritu universitario le ha hecho fácil el trabajar por y para la Universidad. Su excelente curriculum es la prueba palpable de lo que estoy afirmando. Esta academia, a partir

de hoy tendrá un algebrista, el primero de su historia, entre sus miembros de número. El Departamento de Algebra de esta Universidad goza de un excelente prestigio internacional y el nuevo académico ha tenido mucha culpa de este éxito.

Es por todo ello una gran alegría la incorporación a esta Academia, como Académico de número, del Prof. D. José Luis Bueso Montero.

En nombre de la misma le doy la bienvenida con mi más cordial felicitación.