Miscelánea Matemática **34** (2001) 113–123 SMM

La peor conjetura de Fermat sigue abierta

Javier Alfaro Pastor y Carlos Bosch Giral
Departamento de Matemáticas
Instituto Tecnológico Autónomo de México
Río Hondo No. 1
Tizapán, San Angel
01000 México, D.F.
México
cbosch@gauss.itam.mx

1. Introducción.

Los comentarios y las conjeturas de Fermat transformaron la teoría de los números. Fermat probó sólo algunos teoremas e hizo muchas afirmaciones y conjeturas que otros matemáticos se preocuparon por demostrar fue asi como un siglo después Euler al probar varias de las conjeturas de Fermat dio otro gran empujón a la teoría de números. Pero ¿qué fue exactamente lo que pasó en ese siglo entre Fermat y Euler? ¿Por qué esa falta de interés en la teoría de números durante tanto tiempo? Esa falta de progreso puede haberse debido a la euforia que creó el descubrimiento del cálculo el cual monopolizó a casi todos los matemáticos de final del siglo XVII, a la falta de aplicaciones de la teoría de números a problemas reales y a que las afirmaciones de Fermat eran muy difíciles.

Euler mantenía correspondencia con Christian Goldbach, un gran entusiasta de la teoría de números. Inicialmente fue Golbach el que hizo del conocimiento de Euler muchas de las afirmaciones de Fermat y lo animó a trabajar en esta área de las matemáticas.

2. El pequeño Teorema de Fermat.

Una de las afirmaciones más importantes de Fermat aparece en una carta que escribió en 1640. Ahí asegura que si a es un entero positivo y p es un primo que no divide a a, entonces p debe ser un factor de $a^{p-1} - 1$. Como de costumbre Fermat anunció que había encontrado una prueba de esta curiosa propiedad, pero no la incluyó en la carta, en cambio puso que "...enviaría la demostración si no fuese tan larga". Ese resultado es conocido como el pequeño teorema de Fermat.

Por ejemplo si $p = 5$ y $a = 8$ el teorema afirma que $8^4 - 1$ es divisible entre 5.

¿Cómo hizo Fermat para encontrar esa conjetura? Esto es algo que no discutiremos aquí ya que las opiniones varian. Una prueba completa de esta propiedad tuvo que esperar hasta 1736, cuando Euler en una serie de teoremas llegó a la prueba del pequeño teorema de Fermat.

El primero de diciembre de 1729 Christian Goldbach le volvió a escribir una carta a Euler en la que de manera inocente le preguntó "...¿Conoce usted la observación de Fermat de que todos los números de la forma $2^{2^n} + 1$ son primos? Él dijo que no lo puede probar, yo tampoco y no se de alguien que lo haya hecho..."

Lo que Fermat aseguró fue haber encontrado una fórmula que siempre genera primos.

Claramente si

$$\begin{aligned}
n = 1: &\quad 2^{2^1} + 1 = 2^2 + 1 = 5 && \text{es primo} \\
n = 2: &\quad 2^{2^2} + 1 = 2^4 + 1 = 17 && \text{es primo} \\
n = 3: &\quad 2^{2^3} + 1 = 2^8 + 1 = 257 && \text{es primo} \\
n = 4: &\quad 2^{2^4} + 1 = 2^{16} + 1 = 65537 && \text{es primo.}
\end{aligned}$$

Este último es un poco más latoso pero se llega a demostrar que es un número primo. Ahora si $n = 5$ se obtiene un número enorme que Fermat indicó que era un primo.

$$2^{2^5} + 1 = 2^{32} + 1 = 4294967297$$

No había por qué dudar de la afirmación de Fermat debido a la cantidad de conjeturas que hizo y que fueron todas correctas. Por otro lado probar que $2^{2^5} + 1$ no es primo requería, en esa época, de la factorización de ese número de 10 dígitos en dos más pequeños, (en la

actualidad hay varias pruebas para detectar si un número es compuesto sin necesidad de factorizarlo) y quién podría saber si efectivamente Fermat tenía razón y el número no se podía factorizar. En resumen todo indicaba que deberíamos aceptar una vez más la palabra de Fermat y preocuparnos por otros asuntos.

3. Euler ataca la conjetura de Fermat sobre primos.

Pero esa no fue la actitud de Euler. Centró su atención en ese número y al poco tiempo Euler lo había factorizado y la factorización no fue producto de la casualidad como veremos a continuación.

Euler tomó un número a y un primo p que no fuera factor de a. Luego trató de encontrar cómo debería de ser p para que éste fuera un factor de $a+1$ o a^2+1 o a^4+1 o en general $a^{2^n}+1$. Dada la aseveración de Fermat, Euler estaba interesado en el caso $a = 2$ y $n = 5$, es decir quería saber más sobre los factores de $2^{2^5} + 1 = 2^{32} + 1$.

Lo curioso del trabajo de Euler es que usó el pequeño teorema de Fermat para ver que la conjetura de Fermat sobre $2^{2^n} + 1$ era falsa. Dicho de otra forma, Fermat sembró la semilla que prueba que estaba equivocado en esa conjetura. Analicemos el trabajo de Euler.

Sea a un número par y p un primo que no divide a a pero que divide a $a + 1$. Como a es par, $a + 1$ es impar y como p divide a $a + 1$, p no puede ser 2 así que existe k tal que $p = 2k + 1$.

El siguiente paso es más importante por lo que lo enunciamos como un teorema:

Teorema 1. *Sea a un número par y p un primo que no divide a a y tal que p divide a $a^2 + 1$. Entonces para alguna k, $p = 4k + 1$.*

Demostración: a es par, a^2 es par y a^2+1 es impar por lo tanto cualquier divisor de $a^2 + 1$ es impar. Así que p será de la forma $4k + 1$ o bien $4k + 3$. Euler eliminó la forma $4k + 3$ suponiendo que $p = 4k + 3$ y llegando a una contradicción. En efecto por hipótesis p no divide a a y por el pequeño teorema de Fermat p divide a

$$a^{p-1} - 1 = a^{(4k+3)-1} - 1 = a^{4k+2} - 1$$

Por otro lado sabemos que p divide a $a^2 + 1$ y por lo tanto divide a

$$\left(a^2 + 1\right)\left(a^{4k} - a^{4k-2} + a^{4k-4} - \ldots + a^4 - a^2 + 1\right) = a^{4k+2} + 1$$

Así que p debe dividir a:

$$\left(a^{4k+2}+1\right)-\left(a^{4k+2}+1\right)=2$$

La cual es una contradicción por lo que p debe ser de la forma $4k+1$ □

Teorema 2. *Sea a un número par y p un primo que no divide a a y tal que p divide a a^4+1 entonces para alguna k, $p=8k+1$.*

Demostración: Primero observemos que $a^4+1=\left(a^2\right)^2+1$ por lo tanto podemos aplicar el teorema anterior y deducir que p es de la forma $4k+1$. Ahora si dividimos a p entre 8 tenemos 8 posibilidades:
$p=8k$, $p=8k+1$, $p=8k+2$, $p=8k+3$, $p=8k+4$,$p=8k+5$, $p=8k+6$, $p=8k+7$.

Afortunadamente, y esto estaba en el centro del análisis de Euler, se pueden eliminar varios casos. p debe ser impar. ya que divide a un número impar: a^4+1, así que eliminamos. $8k$, $8k+2$, $8k+4$, $8k+6$.

Además como $8k+3=4\left(2k\right)+3$ también se puede eliminar ya que por la observación inicial p es de la forma $4k+1$. Del mismo modo podemos eliminar $8k+7=8k+4+3=4\left(2k+1\right)+3$.

Así que las únicas formas posibles para p son $8k+1$ y $8k+5$. Para eliminar la segunda posibilidad supongamos que $p=8k+5$ y lleguemos a una contradicción.

Como p no divide a a, por el pequeño teorema de Fermat p divide a

$$a^{p-1}-1=a^{8k+5-1}-1=a^{8k+4}-1$$

Por otro lado p divide a a^4+1, así que divide a

$$\left(a^4+1\right)\left(a^{8k}-a^{8k-4}+a^{8k-8}-a^{8k-12}+\ldots+a^8-a^4+1\right)=a^{8k+4}+1$$

De modo que p divide a

$$\left(a^{8k+4}+1\right)-\left(a^{8k+4}-1\right)=2$$

lo cual es una contradicción así que p debe ser de la forma: $8k+1$.

Euler estableció otros casos usando la misma técnica que en los teoremas anteriores y así obtuvo que para un número par a y un primo p:

si p divide a $a+1$	entonces p es de la forma	$2k+1$
si p divide a a^2+1	entonces p es de la forma	$4k+1$
si p divide a a^4+1	entonces p es de la forma	$8k+1$
si p divide a a^8+1	entonces p es de la forma	$16k+1$
si p divide a $a^{16}+1$	entonces p es de la forma	$32k+1$
si p divide a $a^{32}+1$	entonces p es de la forma	$64k+1$

En general si p divide a $a^{2^n}+1$ entonces p es de la forma $(2^{n+1})\,k+1$ para algún número k.

Alrededor de 1870, Edouard Lucas hizo una extensión de este problema y demostró que si p es un divisor de $2^{2^n}+1$, entonces $p = (2^{n+2})\,k+1$ usando nuevamente el pequeño teorema de Fermat.

Regresemos ahora a la conjetura de Fermat.

Euler aseguró entonces que $2^{32}+1$ no es primo. Como $a=2$ podemos usar el trabajo anterior y si $2^{32}+1$ tiene un factor primo p, éste debe ser de la forma $p=64k+1$ donde k es un entero. Ahora sólo debemos ver si esos números dividen o no a $2^{32}+1$.

Primero debemos ver si para distintos valores de k tenemos un primo y segundo debemos ver si ese primo divide a 4294967297

si $k=1$	$64k+1=64+1=65$	no es primo
si $k=2$	$64k+1=128+1=129=3\times 43$	no es primo
si $k=3$	$64k+1=192+1=193$	es primo pero no divide al número
si $k=4$	$64k+1=256+1=257$	es primo pero no divide al número
si $k=5$	$64k+1=320+1=321=3+107$	no es primo
si $k=6$	$64k+1=384+1=385$	no es primo
si $k=7$	$64k+1=448+1=449$	es primo pero no divide al número
si $k=8$	$64k+1=512+1=513=3^3+19$	no es primo

si $k = 9$ $\quad 64k + 1 = 576 + 1 = 577$ es primo pero no divide al número

si $k = 10$ $\quad 64k + 1 = 640 + 1 = 641$ es primo y

$$¡¡ \quad 4294967297 \div 641 = 6700417 \quad !!$$

de modo que $2^{32} + 1$ no es primo.

Si observamos la lista Euler sólo tuvo que hacer cinco divisiones. Este es sin lugar a dudas un ejemplo espectacular de una labor de detective matemático para encontrar un divisor de $2^{32} + 1$.

La afirmación de Fermat que $2^{2^n} + 1$ es un número primo para toda n es falsa para $n = 5$ pero ¿qué pasa para $n > 5$?

Si $n = 6$ tenemos $\quad 2^{2^6} + 1 = 2^{64} + 1 = 18\ 446\ 744\ 073\ 709\ 551\ 617$ que por cierto es divisible por $p = 274177$ que es un número de la forma $128k + 1$ lo cual no es de sorprender dados los descubrimientos de Euler $\quad 274\ 177 = 128 \times 2142 + 1$.

La situación empeoró para $n > 6$ ya que en 1905 se demostró que $2^{2^7} + 1 = 2^{128} + 1$ también es compuesto aunque la prueba no da explícitamente un divisor de este enorme número. Fue hasta 1971 cuando se dio explícitamente un factor de ese número, ese factor tiene 17 cifras.

A partir de 1988 se sabe que $2^{2^8} + 1, \ldots, 2^{2^{21}} + 1$ son todos números compuestos. Actualmente se cree que para $n > 4$ todos los números de la forma $2^{2^n} + 1$ son compuestos de modo que la conjetura de Fermat a ese respecto no estaba sólo mal sino que muy mal, en el sentido de que estaba lejos de ser cierta.

Un último comentario respecto a esos números es que Gauss probó en 1796 que el polígono regular de 17 lados se podía construir con regla y compás, $17 = 2^{2^2} + 1$, más aún probó que un polígono regular de N lados es constructible con regla y compás si y sólo si N es producto de una potencia de 2 y de números primos diferentes del tipo $2^{2^n} + 1$. □

4. Calculistas prodigio.

Los calculistas prodigio a veces verifican si ciertos números son primos o no, aunque esta labor es más difícil que la de multiplicar o dividir números enormes. El caso de Zerah Colburn $(1804 - 1840)$ es de llamar la atención a ese respecto. A la edad de 10 años era famoso en

América y en Europa. Faraday le hizo una serie de preguntas, Morse le hizo un retrato, Laplace lo midió con ciertos cálculos, Napoleón expresó su deseo de conocerlo... Se conoce bien su vida ya que este prodigio escribió sus memorias con cuidado. Zerah nació en Vermont y como peculiaridad diremos que tenía seis dedos en cada mano y cada pie, lo cual sucedió también a dos de sus hermanos, todos seguramente lo adquirieron de su padre quien tenía también seis dedos. Puede ser que la diferencia entre el sistema de numeración que le era natural, base 12 y, el que aprendió en la escuela, base 10, haya sido el desarrollo de sus habilidades de calculista, pero eso es un misterio. Su padre descubrió sus aptitudes cuando su hijo tenía 5 años y le preguntaba las tablas de multiplicar, después de preguntarle los clásicos... 8×7, 8×8, 8×9,... por juego le preguntó cuánto era 13×97 y su hijo dió la respuesta casi instantánea: 1 261 lo dejó perplejo. Después de asegurarse que eso no era una casualidad y hacerle más preguntas, el padre se convenció de las aptitudes de su hijo e hizo que le dieran un entrenamiento especial para que perfeccionara sus capacidades. El padre, deseoso de aprovechar esta oportunidad y de no depender económicamente de su única entrada que era el campo, promovió un espectáculo en el que su hijo era la estrella.

La vida del pequeño Colburn se convirtió en un largo viaje. Toda clase de público asistía a sus espectáculos y así visitó Boston, Nueva York, Filadelfia, Washington y más tarde Londres, Dublín, Liverpool, Glasgow, Edimburgo, y hasta a París fue a dar. El anuncio de su espectáculo en Londres decía lo siguiente:

El matemático francés Fermat afirmó que el número $4294967297 = 2^{2^5}+1 = 2^{32}+1$ *es un número primo. Pero el célebre Euler encontró el error y descubrió que ese número era igual a* 641×6700417. *El mismo número se le propuso a este niño y de memoria encontró los mismos factores.*

Sin lugar a dudas es extraño que un niño de nueve años resuelva un problema que estuvo sin solución cien años. Colburn encontraba fácilmente los factores primos hasta un millón y de ahí en adelante se le complicaba el asunto. Aunque hay que decir que más que otros calculistas prodigio, Colburn tenía la capacidad de "ver" instantáneamente los factores de un número entero. Se le preguntó cómo lo hacía pero era incapaz de contestar y en general se ponía a llorar. Sin embargo un día le reveló a su padre cómo hacía sus cuentas. Su padre tomó nota y creó unas tablas que eran las que tenía en la memoria Colburn para

factorizar. A pesar de esas indicaciones sigue siendo un misterio cómo tenía tal facilidad.

Es interesante observar que el hecho de tener facilidad para los cálculos no es sinónimo de entender o de poder hacer matemáticas. Colburn no probó teoremas matemáticos. El calcular y el razonar en matemáticas parecen ser habilidades ajenas. Aunque también es interesante observar que para los matemáticos de las épocas anteriores a la computadora, era de gran ayuda ser un buen calculista. Euler es un ejemplo de alguien con esas dos habilidades sumamente desarrolladas.

5. Los números de Fermat en la actualidad.

Como suele suceder con las conjeturas de Fermat estas generan bastantes matemáticas a su alrededor. Es en cierto modo increíble que a pesar de que Euler trabajó en la conjetura de los primos de Fermat, actualmente con ayuda de las computadoras se sigue trabajando en esta dirección. Denotemos por $F_n = 2^{2^n} + 1$ al número de Fermat correspondiente a n. En 1877 Pepin probó un teorema para decidir si F_n es primo o no:

Sea $F_n = 2^{2^n} + 1, F_n$ es primo si y sólo si $3^{\frac{F_n-1}{2}} \equiv -1 \mod(F_n)$; es decir que $3^{\frac{F_n-1}{2}} + 1$ es un múltiplo de F_n. Es interesante observar que este criterio en caso de cumplirse prueba que F_n es primo pero en caso de no cumplirse, a pesar de que el número es compuesto no indica ni cuáles son ni cómo encontrar los factores del número. Por ejemplo Selfridge y Hurwitz probaron en 1963 que F_{14} era compuesto pero todavía no se conocen los factores.

Con esta notación se tiene que los números F_0, F_1, F_2, F_3, F_4 son primos. Los números $F_n = 2^{2^n} + 1$ crecen tan rápido que pueden pasar años para saber si un número F_n es compuesto a menos que por suerte se encuentre un divisor lo cual fue el caso para F_{31}. En efecto el 12 de abril del 2001 Alexander Kruppa encontró que 46931635677864055013377 divide a F_{31} de manera que F_{33} es ahora el menor número de ese tipo del cual no se sabe nada.

El resumen de la situación de los números del tipo F_n al 30 de Julio del 2001 es la siguiente:

	n
Primos	$0, 1, 2, 3, 4$
Completamente factorizados	$5, 6, 7, 8$ (dos factores), 9 (tres factores), 10 (cuatro factores), 11 (cinco factores)
Cinco factores primos conocidos	12
Cuatro factores primos conocidos	13
Tres factores primos conocidos	$15, 25$
Dos factores primos conocidos	$16, 18, 19, 27, 30, 36, 38$
	$52, 77, 147, 150, 284, 416$
Un factor primo conocido	$17, 21, 23, 28, 29, 31, 32, 37, 39,$ $42, 43$ y 152 valores de m para $43 < m \leq 382447$.
Compuestos pero no se conoce un factor	$14, 20, 22, 24$
No se sabe	$33, 34, 35, 40, 41, 44, 45, 46, 47,$
	$49, 50, ...$

Hay 225 primos distintos que son factores de los F_n y ciento noventa y dos números F_n de los que se sabe que son compuestos.

Por supuesto que para calcular estos factores y decidir si algunos números son compuestos el uso de la computadora es indispensable. El profesor Richard E Crandall está llevando a cabo un proyecto para encontrar factores de los números de Fermat "pequeños" F_{25} a F_{1000} y el profesor Leonid Duman para los números "grandes" F_{1000} a $F_{5000000}$. En este proyecto los directores afirman que la mayoría de los usuarios de computadoras usan la máquina una fracción de su potencial. Muchos tienen imágenes en la pantalla cuando no usan la computadora, "screen savers", lo que la convierte en un aparato inútil. Con el proyecto de estos dos matemáticos se puede poner a trabajar la máquina para buscar divisores de los números de Fermat mientras no se utiliza. Hay más información al respecto en la página http://www.fermat.search.org.

Para terminar reproducimos aquí una página que otorga premios por encontrar factores de los números de Fermat.

http://www.perfsci.com/prizes.html

Sin lugar a dudas la conjetura de Fermat sobre los números primos todavía está dando algo quehacer.

Referencias

[1] J.P. Delahaye, Merveilleux nombres premiers. Berlin. Pour la science, 2000.

[2] W. Dunham, Journey through genious. Penguin books, 1990.

[3] G. Godefroy, Láventure des nombres. Ed. Odile Jacob,1997.

[4] I. Nivens, H. Zuckerman, Introducción a la teoría de los números. Limusa Wiley 1969

[5] I. Stewart, From here to infinity. Oxford University Press. 1996.

hppt://www.perfsci.com/prizes.html
hppt://www.prothsearch.net/fermat.html
hppt://www.utm.edu/research/primes/glossary/
GeneralizedFermatNumber.html
hppt://www.utm.edu/research/primes/prove/prove3_1.html

hppt://www.utm.edu/research/primes/glossary/FermatDivisor.html
hppt://www.utm.edu/research/primes/list/top20/FermatDivisor.html
hppt://www.utm.edu/research/primes/prove/prove3.html
hppt://www.fermatsearch.org/program.htm
hppt://www.utm.edu/research/primes/glossary/Fermats.html
hppt://www.fermatsearch.org/status.htm