# El diablo de los números

Sección a cargo de

**Javier Cilleruelo Mateo**

## Desde los números de Fermat hasta la geometría

por

**Michal Křížek, Florian Luca, Lawrence Somer**

En 1640 Pierre de Fermat conjeturó que todos los números de la forma

$$F_m = 2^{2^m} + 1, \qquad m = 0,\ 1,\ 2, \ldots,$$

eran primos. Esta conjetura, aunque después resultaría ser incorrecta, habría de causar una revolución en la teoría de los números y en la geometría. Los primeros cinco miembros de la sucesión son realmente primos:

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

pero en 1742 Leonhard Euler observó que $F_5 = 641 \times 6700417$ (ver Figura 1). Los números $F_m$ se llaman *números de Fermat* y aquellos que son primos se denominan *primos de Fermat*.

Hasta 1796 los números de Fermat eran contemplados como una curiosidad matemática. Pero el interés por ellos aumentó cuando el matemático alemán Carl Friedrich Gauss (1777–1855) encontró, de manera inesperada mientras estaba estudiando las raíces de la ecuación $z^n = 1$, un teorema que conectaba los primos de Fermat con la construcción con regla y compás de los polígonos regulares (ver Figura 1). Cuando apenas tenía diecinueve años escribió un pequeño artículo sobre la división del círculo en 17 partes iguales usando herramientas geométricas donde esencialmente usó el hecho de que 17 es un primo de Fermat. Este descubrimiento fundamental está representado en la base de su estatua en Braunschweig donde el nació (ver Figura 2). Como el polígono regular con 17 vértices se hubiera parecido demasiado a un círculo, su estatua está ilustrada con una estrella de 17 vértices. Mencionamos que varios autores sitúan incorrectamente al polígono regular de 17 vértices sobre su tumba en Göttingen, donde él había pedido que se pusiera.

Euclides (siglo IV–III a.c.): *Existe una construcción con regla y compás del polígono regular de $n$ vértices para*

$$n = 2^i 3^j 5^k,$$

*donde $n \geq 3$ e $i \geq 0$ son enteros y $j, k \in \{0, 1\}$.*

*Pierre de Fermat (1601–1665): Para $m = 0,\ 1,\ 2, \ldots$ la sucesión $F_m = 2^{2^m} + 1$ consiste solamente de primos.* (Un enunciado incorrecto.)

Leonhard Euler (1707–1783): *El número de Fermat $F_5$ es compuesto.*

*Carl Friedrich Gauss (1777–1855): Existe una construcción con regla y compás para el polígono regular de $n$ vértices si y sólo si*

$$n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j},$$

*donde $n \geq 3$, $i \geq 0$, $j \geq 0$, y $F_{m_1},\ F_{m_2}, \ldots,\ F_{m_j}$ son primos de Fermat distintos.*

*Figura 1: Logros importantes en la construcción con regla y compás de los polígonos regulares.*

Figura 2: Estatua de Carl Friedrich Gauss en su ciudad natal Braunschweig. En la parte izquierda de la base, la estrella dorada con 17 vértices brilla en honor de su descubrimiento.

Unos años después Gauss enunció una condición necesaria y suficiente (ver Figura 1) para la existencia de la construción con regla y compás de los polígonos regulares. Su demostración original, que ocupa más de 50 páginas (ver [3, Sect. VII]), es sin embargo incompleta. La condición necesaria fue demostrada correctamente en 1837 por Wantzel [15] (ver también [11]). Según el teorema de Gauss, el polígono regular de $n$ lados, $n$ impar, se puede construir con la regla y el compás sólo para

$$n = 3,\ 5,\ 15,\ 17,\ 51,\ 85,\ 255,\ 257, \dots , \tag{1}$$

donde $15 = 3 \cdot 5$, $51 = 3 \cdot 17$, $85 = 5 \cdot 17$, $255 = 3 \cdot 5 \cdot 17, \dots$ son productos de primos de Fermat distintos.

La investigación de la primalidad de los números de Fermat se ha convertido desde entonces en una tarea importante. En 1855, el astrónomo alemán Thomas Clausen escribió a Gauss anunciándole que $F_6$ era un producto de dos factores primos. El creía que el más grande de los dos factores era el primo más grande conocido en su tiempo, lo que resultó ser correcto. Una copia de

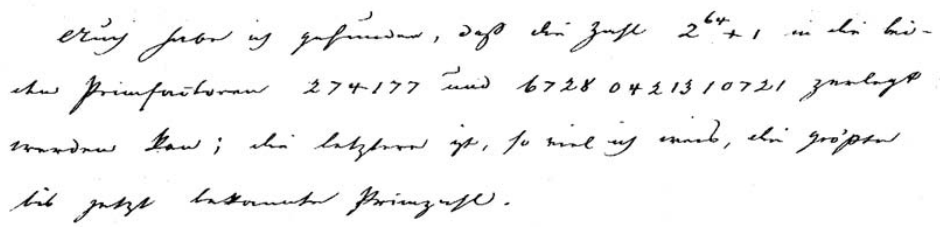


Figura 3: Una parte de la carta que Thomas Clausen escribió a Carl Friedrich Gauss anunciándole la factorización de $F_6$ en 1855 (antes de la factorización de Landry): «*Auch habe ich gefunden, daß die Zahl $2^{64}+1$ in die beiden Primfactoren 274177 und 67280421310721 zerlegt werden kann; die letztere ist, so viel ich weiß, die größte bis jetzt bekannte Primzahl*».

esta carta está guardada en la biblioteca de la Universidad de Göttingen (ver Figura 3)[1].

Hay que señalar que el mismo resultado fue publicado independientemente por Landry en 1880 [7].

En 1878, el matemático francés François Édouard Anatole Lucas demostró [9] el siguiente teorema, que se ha convertido en una herramienta muy poderosa para encontrar factores primos de otros números de Fermat más grandes.

Teorema (Lucas). *Si un primo $p$ divide a $F_m$ para algún $m > 1$, entonces existe un número natural $k$ tal que*

$$p = k2^{m+2} + 1.$$

La utilidad del Teorema de Lucas se puede ilustrar con un ejemplo que trató A. E. Western en 1903. El quería saber si $F_{18}$, que tiene cerca de 80 000 dígitos, era compuesto. Western buscó un número natural $k$ tal que $k2^{20} + 1$ dividiera a $F_{18}$. La divisibilidad se necesita comprobar sólo para aquellos $k$ para los que $k2^{20} + 1$ es un primo. Como los números $k2^{20} + 1$ son compuestos para todo $k \leq 13$ excepto para $k = 7$ y $k = 13$, Western descubrió fácilmente que la divisibilidad se cumple cuando $k = 13$.

La comprobación de que $p = 13 \cdot 2^{20} + 1 = 13631489$ realmente divide al gigantesco número de Fermat $F_{18}$ se puede realizar fácilmente a través de la

[1]Los autores agradecen a Niedersächsische Staats- und Universitätsbibliothek en Göttingen por permitirles publicar la parte de la carta mostrada en la Figura 3.

siguiente cadena de congruencias:

$$\begin{aligned}
2^{2^5} &= 65536^2 \equiv 1048261 \pmod{p},\\
2^{2^6} &\equiv 1048261^2 \equiv 3164342 \pmod{p},\\
2^{2^7} &\equiv 3164342^2 \equiv 9153547 \pmod{p},\\
&\vdots \qquad\qquad \vdots\\
2^{2^{17}} &\equiv 1598622^2 \equiv 1635631 \pmod{p},\\
2^{2^{18}} &\equiv 1635631^2 \equiv 13631488 \pmod{p}.
\end{aligned}$$

Por lo tanto, $2^{2^{18}} + 1 \equiv 0 \pmod{13631489}$.

Con los métodos matemáticos actuales y las potentes ordenadores, hoy en día sabemos que

$$F_m \text{ es compuesto para } 5 \leq m \leq 32,$$

aunque para $F_{14}$, $F_{20}$, $F_{22}$, y $F_{24}$ todavía no conocemos ningún factor primo no trivial. El número de Fermat $F_{24}$, que tiene más de 5 millones de dígitos decimales, se probó que es compuesto en 1999 [2]. Esta computación ha sido la más grande computación efectuada en la historia para obtener una simple respuesta «si o no». Se necesitaron $10^{17}$ operaciónes de computadora para verificar la siguiente congruencia (2):

Teorema (Test de Pepin). *Para $m \geq 1$ el número de Fermat $F_m$ es primo si y sólo si*

$$3^{(F_m-1)/2} \equiv -1 \pmod{F_m}. \tag{2}$$

Pepin, en su artículo original de 1877, usó la base 5 en vez de la base 3 [10].

Aunque se conocen muchas condiciones necesarias y suficientes para la primalidad de $F_m$, y se han encontrado más de 245 factores de los números de Fermat, nadie ha sido capaz de descubrir ningún principio general que respondiera a la pregunta de si $F_4$ es el primo de Fermat más grande que existe. Por lo tanto, hasta ahora todavía no sabemos si el listado que disponemos de polígonos regulares que se pueden construir con regla y compás es completo.

C. F. Gauss descubrió también cómo dividir a la lemniscata en cinco partes iguales con regla y compás (i.e., cómo construir puntos de división). Este resultado fue generalizado más tarde por Niels Henrik Abel.

Teorema (Abel). *La lemniscata se puede dividir en $n$ partes iguales si y sólo si $n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j}$, donde $i \geq 0$ y $j \geq 0$ son enteros y $F_{m_1}, F_{m_2}, \ldots, F_{m_j}$ son primos de Fermat distintos.*

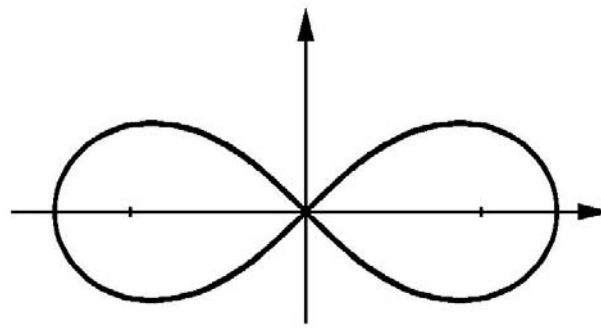


Figura 4: La Lemniscata $\left(x^2+y^2\right)^2 = \alpha^2\left(x^2-y^2\right)$.

Para una demostración, ver [12]. Recordamos que la lemniscata (de Bernoulli) es una curva cuyos puntos tienen un producto constante (e igual a $\alpha^2/2$) de sus distancias a dos puntos fijos $(\pm(\alpha/2)\sqrt{2}, 0)$, donde $\alpha > 0$ es un parámetro real ($\alpha = \sqrt{2}$ en la Figura 4).

Ahora mostraremos otra conexión notable entre la teoría de los números y la geometría. Escribimos el triángulo de Pascal módulo 2 (comparar con la Figura 5):

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 0 & & 1 & & & \\
 & & 1 & & 1 & & 1 & & 1 & & \\
 & 1 & & 0 & & 0 & & 0 & & 1 & \\
1 & & 1 & & 0 & & 0 & & 1 & & 1 \\
 & 1 & & 0 & & 1 & & 0 & & 1 & \\
1 & & 1 & & 1 & & 1 & & 1 & & 1 \\
 & 1 & & 0 & & 0 & & 0 & & 0 & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
$$

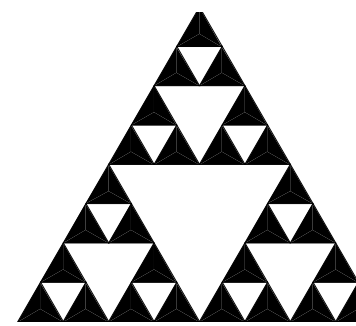


Figura 5: Triángulo de Pascal módulo 2 y el conjunto fractal de Sierpiński.

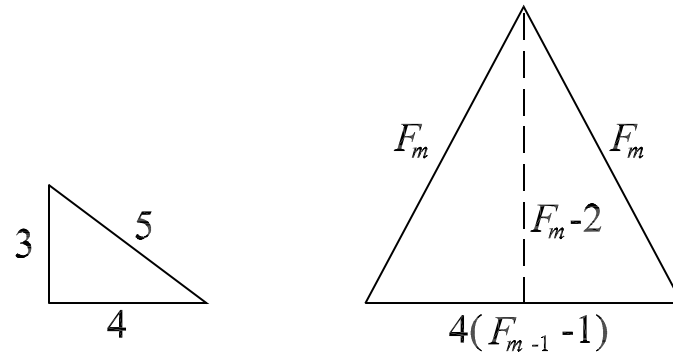



Figura 6: Los únicos triángulos de Heron posibles cuyos lados son potencias de primos.

Leyendo las primeras 32 filas como representaciones binarias de enteros, obtenemos la siguiente sucesión creciente

$$1,\ 3,\ 5,\ 15,\ 17,\ 51,\ 85,\ 255,\ 257, \ldots,$$

Observamos que la sucesión de arriba es precisamente la misma sucesión que aquella que aparece en (1) (excepto el primer término), que da todos los polígonos regulares de lados impares que se pueden construir con la regla y el compás en sus primeros 31 términos. ¿No es esto un pequeño milagro? Esta propiedad interesante de los números de Fermat ha sido probada por van der Waall [14] (ver también [1, p. 140] ó [6, Theorem 8.1]). Además, observan que el triángulo de Pascal módulo 2 tiene una estructura similar al del famoso conjunto fractal de Sierpiński (ver la Figura 5).

Los primos de Fermat aparecen no solamente en conexión con la construcción de los polígonos regulares, sino también en conexión con los triángulos de Heron. Recordemos que un *triángulo de Heron* es un triángulo tal que las longitudes de sus tres lado y también su área son enteros. En el siguiente teorema (ver [8]), mostramos una relación interesante entre los primos de Fermat y los triángulos de Heron cuyos lados son potencias de primos (ver Figura 6).

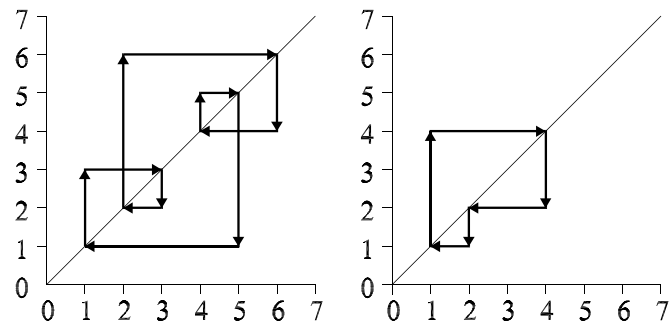
Teorema (Luca). *Si las tres longitudes de los lados de un triángulo de Heron son potencias de primos, entonces estas longitudes son* $3, 4, 5$, *ó* $F_m$, $F_m$, $4(F_{m-1} - 1)$ *para algún* $m \geq 1$ *tal que* $F_m$ *es primo.*

A continuación, introducimos otra condición necesaria y suficiente (ver [4]) para la primalidad de los números de Fermat que tiene una bonita interpretación geométrica. Con este propósito, primero presentamos un procedimiento gráfico que transforma fracciones algebraicas en imágenes.

Sea $b > 1$ y $n$ enteros positivos. Si $r_i$ es el resto producido en el paso $i$ del algoritmo de división que permite escribir $1/n$ en base $b$, entonces el resto producido en el paso $(i+1)$-ésimo obviamente cumple la congruencia

$$r_{i+1} \equiv br_i \pmod{n}.$$

Empezando por $r_0 = 1$, obtenemos la sucesión de restos $r_0, r_1, r_2, \ldots$ de $1/n$ obtenidos por el procedimiento de división en base $b$. Analizaremos dicha división gráficamente. El análisis empieza en el punto $(r_0, r_0)$, va verticalmente, después horizontalmente a $(r_1, r_1)$, después se mueve una vez más verticalmente, después horizontalmente hasta $(r_2, r_2)$, y continua de esta manera (ver Figura 7). Si el resto es cero en el paso $i$, paramos el proceso. De esta manera, la sucesión de los restos determina completamente la gráfica asociada a la fracción.




$b = 10$ $\qquad$ $b = 11$

Figura 7: Análisis gráfico de $\frac{1}{7}$ para dos bases distintas.

Consideramos, por ejemplo, la fracción $\frac{1}{7}$, que tiene la representación en base-10 (decimal) igual a $0.\overline{142857}$. La sucesión correspondiente de restos es periódica:

$$\begin{aligned} r_0 &= 1, \\ r_1 &= 3 \equiv 10 \pmod{7}, \\ r_2 &= 2 \equiv 30 \pmod{7}, \\ r_3 &= 6 \equiv 20 \pmod{7}, \\ r_4 &= 4 \equiv 60 \pmod{7}, \\ r_5 &= 5 \equiv 40 \pmod{7}, \\ r_0 = r_6 &= 1 \equiv 50 \pmod{7}, \end{aligned}$$

etc.

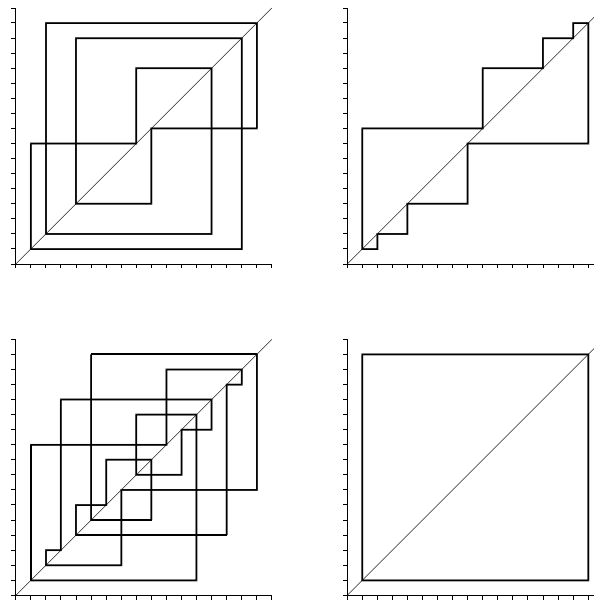


Figura 8: Análisis gráfico de $\frac{1}{17}$ para $b = 8,\ 9,\ 10$, y 16.

En la Figura 7, vemos que la gráfica asociada tiene simetría rotacional respecto al punto (3,5, 3,5) para la base $b = 10$, pero la gráfica es asimétrica para $b = 11$.

Un entero $n > 1$ se llama *perfectamente simétrico* si la gráfica asociada a su recíproco $1/n$ es rotacionalmente simétrica respecto al punto $(n/2, n/2)$ en todas las bases $b$, tales que $b \not\equiv 0 \pmod{n}$ y $b \not\equiv 1 \pmod{n}$.

Teorema (Jones, Pearce). *Un entero $n > 1$ es perfectamente simétrico si y sólo si $n = 2$ o $n$ es un primo de Fermat.*

Para la demostración, ver [4]. El análisis gráfico de la fracción $1/F_m$ para $m = 2$ se ilustra en la Figura 8.

A continuación vamos a introducir la *función de Euler* $\phi$. Para cada $n \in \mathbb{N}$ el valor de $\phi(n)$ es define como el número de enteros positivos y no mayores que $n$ que son coprimos con $n$, i.e.,

$$\phi(n) = \text{card}\{m \in \mathbb{N} \mid 1 \leq m \leq n,\ \text{mcd}(m, n) = 1\}.$$

Teorema (Euler, Fermat). *Sean $a, n \in \mathbb{N}$. Entonces*

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{3}$$

*si y sólo si* $\mathrm{mcd}(a, n) = 1$.

Si $\phi(n)$ es el entero positivo más pequeño tal que la congruencia (3) se cumple, entonces $a$ se llama *raíz primitiva módulo n* (ver Figura 9). Sean $n > 1$ y $a$ enteros tal que $\mathrm{mcd}(a, n) = 1$. Si la congruencia cuadrática

$$x^2 \equiv a \pmod{n}$$

no tiene ninguna solución entera $x$, entonces $a$ se llama *residuo no cuadrático módulo n*.

Para un entero $n > 1$ definimos

$$M(n) = \{a \in \{1, ..., n-1\} \mid a \text{ es una raíz primitiva} \pmod{n}\}$$

y

$$K(n) = \{a \in \{1, ..., n-1\} \mid \mathrm{mcd}(a, n) = 1 \text{ y } a \text{ es un residuo no cuadrático } (\mathrm{mod}\ n)\}.$$

La siguiente condición necesaria y suficiente ha sido demostrada en [6].

Teorema (Křížek, Somer). *El entero $n \geq 3$ es un primo de Fermat si y sólo si $n$ es impar y $M(n) = K(n)$.*

Asociamos ahora a cada $n \in \mathbb{N}$ una digrafo (grafo orientado) cuyo conjunto de vértices es $H = \{0, 1, \ldots, n-1\}$ y tal que hay una arista de $x \in H$ a $y \in H$ si

$$x^2 \equiv y \pmod{n}.$$

A las componentes conexa del grafo no orientado las denominamos *componentes* del digrafo. En la Figura 10 observamos las características estructurales particulares de los digrafos asociados a los primos de Fermat 5 y 17.

Teorema (Szalay). *El entero $n \geq 3$ es un primo de Fermat si y sólo si el digrafo asociado tiene precisamente dos componentes, uno de los cuales es el cero que es un punto fijo aislado.*

Para la demostración, ver [13]. El digrafo asociado a los primos de Fermat tiene una estructura binaria muy especial (ver Figura 10). Todas las raíces primitivas módulo un primo de Fermat «están en la cima» del digrafo. Según (3), el número 3 es una raíz primitiva módulo un primo de Fermat (ver también Figura 9). Por lo tanto, la Figura 10 nos da una interpretación gráfica del test de Pepin.

Los números de Fermat tienen muchas aplicaciones útiles en la teoría de los números, e.g., en probar que hay una infinidad de primos y pseudoprimos

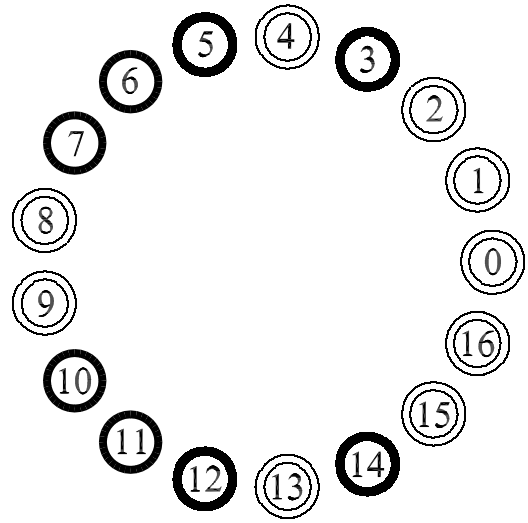
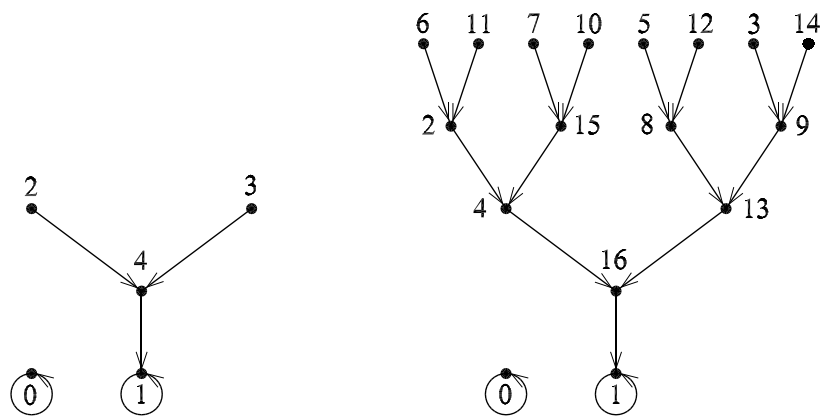



Figura 9: Las raíces primitivas módulo 17 están indicadas con un círculo negro.




$n = 5$ $n = 17$

Figura 10: Digrafos asociados a primos de Fermat.

y en establecer la existencia de números de Sierpiński [5]. Sin embargo, hay aplicaciones más prácticas de estos números. En particular, los números de Fermat se usan en varias transformaciones relacionadas con la aritmética binaria módulo $F_m$ que conducen a multiplicaciones rápidas de números grandes; en generadores de números aleatorios y pseudoaleatorios; en hashing schemes; en el modelo chiral de Potts; y en el análisis de las bifurcaciones de la ecuación logística que conduce al caos [5].

Agradecimientos: Los autores agradecen a Javier Cilleruelo y a Alena Šolcová sus valiosas sugerencias. El trabajo para este artículo ha sido apoyado por el proyecto ME 749 de la Republica Checa.

## Referencias

[1] J.H. Conway, R.K. Guy, *The book of numbers*. Springer-Verlag, New York, 1996.

[2] R.E. Crandall, E. Mayer, J. Papadopoulos, The twenty-fourth Fermat number is composite. *Math. Comp.* **72** (2003) 1555–1572.

[3] C.F. Gauss, *Disquisitiones arithmeticae*. Springer, Berlin, 1986.

[4] R. Jones, J. Pearce, A postmodern view of fractions and the reciprocals of Fermat primes. *Math. Mag.* **73** (2000) 83–97.

[5] M. Křížek, F. Luca, L. Somer, *17 lectures on Fermat numbers: From number theory to geometry*. CMS Books in Mathematics, vol. 9, Springer-Verlag, New York, 2001.

[6] M. Křížek, L. Somer, A necessary and sufficient condition for the primality of Fermat numbers. *Math. Bohem.* **126** (2001) 541–549.

[7] F. Landry, Sur la décomposition du nombre $2^{64} + 1$. *C. R. Acad. Sci. Paris* **91** (1880) 138.

[8] F. Luca, Fermat numbers and Heron triangles with prime power sides. *Amer. Math. Monthly* **110** (2003) 46–49.

[9] E. Lucas, Théorèmes d'arithmétique. *Atti della Reale Accademia delle Scienze di Torino* **13** (1878) 271–284.

[10] P. Pepin, Sur la formule $2^{2^n} + 1$. *C. R. Acad. Sci.* **85** (1877) 329–331.

[11] J. Pierpont, On an undemostrated theorem of the Disquisitiones Arithmeticæ. *Bull. Amer. Math. Soc.* **2** (1895/96) 77–83.

[12] M. Rosen, Abel's theorem on the lemniscate. *Amer. Math. Monthly* **88** (1981) 387–395.

[13] L. Szalay, A discrete iteration in number theory (Hungarian). *BDTF Tud. Közl. VIII. Természettudományok 3., Szombathely* (1992) 71–91.

[14] R.W. van der Waall, Oplossing. *Nieuw archief voor wiskunde* **XXIV** (1976) 262–263.

[15] P.L. Wantzel, Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas. *J. Math.* **2** (1837) 366–372.

Michal Křížek
Mathematical Institute, Academy of Sciences
Žitná 25, CZ – 115 67 Prague 1
Czech Republic
Correo electrónico: krizek@math.cas.cz

Florian Luca
Instituto de Matemáticas, UNAM
Campus Morelia
Apartado Postal 61-3 (Xangari)
CP. 58 089, Morelia, Mexico
Correo electrónico: fluca@churipo.matmor.unam.mx

Lawrence Somer
Department of Mathematics
Catholic University of America
Washington, D.C. 20064, U.S.A.
Correo electrónico: somer@cua.edu