El algoritmo de Agrawal, Kayal y Saxena para decidir primalidad

José de Jesús Angel Angel
jjangel@computacion.cs.cinvestav.mx
Guillermo Morales-Luna
gmorales@cs.cinvestav.mx
CINVESTAV-IPN, Mexico

Resumen
Describimos el *algoritmo de Agrawal, Kayal y Saxena* (AKS) de una manera que estimamos simple, aunque detallada. Comentamos algunos de sus últimos perfeccionamientos, es decir, algunas modificaciones propuestas para mejorar su eficiencia.

1. Historia

Uno de los problemas más estudiados en la historia de las matemáticas ha sido el determinar si un número es primo o compuesto: Han existido diversos criterios, desde la criba de Eratóstenes, hasta los debidos a Cataldi (1548-1626), Fermat (1601-1665), Legendre (1752-1833), Gauss (1777-1855) y Lucas (1842-1895), y ya en nuestros tiempos, Solovay-Strassen y Miller-Rabin.

En 1983, Adleman, Pomerance y Rumely [1] presentan el primer algoritmo determinista, que posee una complejidad en tiempo $O\left(\log n^{c \log\log\log n}\right)$ donde n es el número de bits en la representación binaria del número a decidir si es primo. Este algoritmo es conocido como el *método ciclotómico* por usar precisamente los polinomios ciclotómicos, sin embargo, no es fácil de implementar.

En 1986, Goldwasser y Killian [15] proponen un algoritmo basado en curvas elípticas, el cual corre en un tiempo polinomial. Sin embargo es poco eficiente en la práctica. Atkin [6,7] propone otro algoritmo conocido como *Elliptic Curve Primality Proving* (ECPP) que es más eficiente en la práctica. Finalmente en 1992, Adleman y Huang [2] modifican el algoritmo de Goldwasser y Killian para obtener un algoritmo probabilístico polinomial que siempre produce un número primo.

Hasta agosto del 2002, el mejor algoritmo determinista era el de Adleman, Pomerance y Rumely con una complejidad superpolinomial y algunas modificaciones debidas a Mihăilescu.

El 6 de agosto del 2002 varios medios alrededor del mundo dieron a conocer que tres investigadores del Tecnológico de Madras, en la India, M. Agrawal, N. Kayal y N. Sexena encontraron un algoritmo polinomial determinista para certificar que un número es primo, cuando en efecto lo es.

Esto quita del camino a la suposición de mostrar primero la conjetura de Riemann y después encontrar un algoritmo determinista de primalidad. El nuevo método, conocido como AKS, es simple y no requiere de grandes teorías y se ha considerado como uno de los grandes descubrimientos en esta área.

2. Algoritmo AKS-2002

El algoritmo AKS, en su primera versión de agosto del 2002, es determinista y posee una complejidad en tiempo $O((\log n)^{12})$. Mas al igual que casi todo método, está sometido a un período de continuo perfeccionamiento.

El método AKS-2002 se puede ver en la Tabla 1.

Input: $n \geq 1$
Output: A decision whether n is PRIME or COMPOSITE

1.- If $(n = a^b)$, with $a \in \mathbb{N}$, $b > 1$, then
output COMPOSITE
2.- else $r = 2$
3.- While $(r < n)$ do {
4.- If (mcd $(n, r) \neq 1$) then
output COMPOSITE
5.- else If (r is prime) then
6.- let q be the largest prime factor of $r - 1$
7.- If $(q \geq 4\sqrt{r}\log n)$ and $n^{\frac{r-1}{q}} \not\equiv 1 \bmod r$
8.- then break:
9.- $r := r + 1$
10.- }
11.- For $a = 1$ to $2\sqrt{r}\log n$ do
12.- If $(x - a)^n \not\equiv (x^n - a) \bmod (x^r - 1, n)$ then
output COMPOSITE
13.- else output PRIME

Tabla 1: Algoritmo AKS-2002

2.1. Idea del algoritmo

El siguiente teorema es una generalización del Teorema Pequeño de Fermat (TPF) y es en sí un criterio determinista.

Teorema 1. *Sea $n \geq 2$ y $a < n$ un entero tal que* $\text{mcd}(n, a) = 1$. *Entonces*

$$n \text{ es primo} \iff (x + a)^n = (x^n + a) \bmod n.$$

Sin embargo, para números de considerable tamaño, el criterio dado por este teorema no es eficiente, ya que requiere evaluar $O(n)$ coeficientes.

Así, la idea básica de AKS fue reducir el número necesario de pasos para la verificación de la primalidad.

La aportación de AKS es verificar sólo $(x+a)^n = (x^n + a) \bmod (x^r - 1, n)$, para potencias r "pequeñas", donde mod $(x^r - 1, n)$ significa evaluar los polinomios en el anillo cociente $\mathbb{Z}_n[x]/(x^r - 1)$.

Resulta que todos los números primos cumplen este criterio.

Sin embargo también algunos números compuestos lo cumplen para pocas parejas (a, r), por lo que hay que descartar esos casos.

El algoritmo elige primero (pasos 3-10) una potencia r adecuada, es decir, tal que sea un número primo y $r-1$ tenga un factor q de valor alrededor de $r^{1/2}$. Se puede probar que tales potencias r existen. Finalmente el algoritmo verifica (pasos 11-13) que se cumpla la igualdad $(x+a)^n = x^n + a \bmod (x^r - 1, n)$ en el anillo $\mathbb{Z}_n[x]/(x^r - 1)$, para $a = 1, \ldots, 2\sqrt{r}\log n$. En caso que así suceda, esto es suficiente para declarar que n es primo.

Veamos primero paso a paso algunos detalles de implementación del algoritmo. Es importante mencionar que en aplicaciones criptográficas, donde es necesario generar un número primo de cierta longitud en bits, se procede primero a generar un número aleatorio impar n, y éste se somete a alguna prueba de primalidad. Si se da como salida COMPOSITE, entonces se intenta con $n+2$, y seguidamente con $n+4, n+6, \ldots$ hasta obtener el primo deseado. Se garantiza que esto ha de tener un costo mínimo por el TNP.

Paso 1 Aquí se descarta que el número n sea una potencia b-ésima de un número entero a, es decir, se decide si acaso "n es una potencia perfecta". Para encontrar un posible exponente $b \geq 2$, se procede a calcular un entero $c = \left\lfloor n^{1/b} \right\rfloor$. Entonces resultará que n es una potencia perfecta si y sólo si $c^b = n$. Así pues, el paso 1 se puede verificar con la siguiente rutina:

For $b = 2$ to $\lfloor \log n \rfloor$ do
  If $c = n^{1/b}$ is an integer, then COMPOSITE

Paso 2 En esta etapa del algoritmo se busca un número primo r tal que $r-1$ tenga un factor $q \geq 4\sqrt{r}\log n$ tal que $q | o_r(n)$, donde $o_r(n)$ denota al orden de n módulo r. Este número r se busca de manera exhaustiva, es decir, se comienza desde $r = 2$ y se detiene hasta que se encuentra el deseado. La existencia del número r está garantizada por un resultado debido a E. Fouvry en 1985. El segundo propósito de esta etapa es detectar si acaso n tiene factores pequeños.

Paso 3 Aquí simplemente se inicializa $r = 2$. Realmente debe de inicializarse con $r = 3$ para verificar sólo los números impares. Se ha de proseguir en la búsqueda de r en tanto $r < n$.

Paso 4 Si mcd $(n, r) \neq 1$, entonces hay un divisor de n. Por lo tanto, el resultado del algoritmo ha de ser COMPOSITE.

Paso 5 Sólo se pasa al siguiente paso si r es primo, lo que se puede verificar mediante el ensayo de divisiones. Realmente sólo aquellos r impares son verificados; esto es, el incremento del paso 9 debe ser $+2$.

Paso 6 Aquí se localiza el factor primo q más grande de $r-1$. Mediante búsqueda exhaustiva, se encuentra el factor impar más grande de $r-1$. Se puede realizar esta búsqueda mediante el siguiente seudocódigo:

For $i = 2$ to $r-1$ do
  While $(r \bmod i) = 0$ do $r := r/i$;
    output as a factor i

Paso 7 Se verifica si acaso $q \geq 4\sqrt{r}\log n$ y si q divide al orden de n módulo r, mediante la prueba $n^{\frac{r-1}{q}} \not\equiv 1 \bmod r$. Como q es primo y un factor de $r-1$, entonces si q no fuese un factor de $o_r(n)$ tendríamos que $(r-1)/q = o_r(n)k$. Por lo tanto $n^{\frac{r-1}{q}} \equiv 1 \bmod r$. Es decir $o_r(n) | r-1$, pero $o_r(n) | (r-1)/q$, por lo cual $q | o_r(n)$.

Input: $n \geq 1$
Output: A decision whether n is PRIME or COMPOSITE
1.- If $n = a^b$ then output COMPOSITE
2.- Find the smallest r such that $o_r(n) > 4\log^2 n$
3.- If $1 < \gcd(a, n) < n$, for some $a \leq r$, then output COMPOSITE
4.- If $n \leq r$ then ouput PRIME
5.- For $a = 1$ to $\left\lfloor 2\sqrt{\varphi(r)}\log n \right\rfloor$ do If $((x+a)^n \not\equiv (x^n + a) \bmod (x^r - 1, n))$ then output COMPOSITE
6.- Output PRIME

Tabla 2: Algoritmo AKS-revisado

Paso 8 Es importante notar que es necesario que n posea un tamaño al menos de 15 bits para poder encontrar el número r buscado.

Paso 9 Si r no es primo, se continúa buscando. La actualización debería ser $r := r + 2$ que es el siguiente número impar.

Paso 10 Se termina la búsqueda de r. Esto queda garantizado por el resultado de Fouvry.

En la última etapa del algoritmo, se revisa si acaso $(x-a)^n \equiv (x^n - a) \bmod (n, x^r - 1)$ para $a = 1, \ldots, 2\sqrt{r}\log n$. Si no se cumpliera para algún a, entonces n ha de ser compuesto. De lo contrario n, será un número primo.

Paso 11 Se recorren los números a que verifican si acaso n satisface todas las congruencias. En tal caso, n es primo.

Paso 12 Si se encuentra a tal que $(x-a)^n \not\equiv (x^n - a) \bmod (x^r - 1, n)$ entonces n es compuesto.

Paso 13 Si, finalmente, n cumple todas las equivalencias del paso 12, con el r encontrado, entonces n es primo.

2.2. Una versión nueva del algoritmo AKS

Con observaciones de H. Lenstra, se publica por los mismos autores una nueva versión del algoritmo AKS, mostrada en la Tabla 2.

Esta nueva versión del algoritmo tiene también tres etapas, la primera revisa si n es una potencia perfecta. Los métodos aquí conocidos pueden perfeccionarse hasta lograr un tiempo lineal [9, 10]. La segunda etapa consiste de nuevo en buscar un r adecuado y también eliminar la posibilidad de que n tenga factores pequeños. Finalmente la última etapa consiste en probar para $a = 1$ hasta $\left\lfloor 2\sqrt{\varphi(r)}\log n \right\rfloor$ que se cumpla $(x+a)^n \equiv (x^n + a) \bmod (x^r - 1, n)$. En tal caso, se declara que n es primo. Una vez más el esfuerzo mayor se hace en evaluar $(x+a)^n \bmod (x^r - 1)$ y particularmente, como se observa en el paso 5 del último algoritmo, si n fuese primo es necesario evaluar todos los a's posibles.

2.3. Demostración de AKS

De manera más formal, el resultado de AKS fue escrito por D. Bernstein, y se resume en el siguiente teorema.

Teorema 2 (Agrawal, Kayal, Saxena)**.** *Sea n un entero positivo, sean q, r dos números primos y sea S un conjunto finito de enteros. Suponiendo que:*

1. *q divide a $r-1$,*
2. *$n^{(r-1)/q} \bmod r \notin \{0,1\}$,*
3. *$\gcd(n, b-b') = 1$ para todos elementos diferentes $b, b' \in S$,*
4. *$\binom{\#S+q-1}{\#S} \geq n^{2\lfloor\sqrt{r}\rfloor}$,*
5. *$(x+b)^n = x^n + b$ en el anillo $\mathbb{Z}_n[x]/(x^r-1)$, para todo $b \in S$,*

entonces n es una potencia de un primo.

Porteriormente Lenstra propone refinar el resultado reformulándolo de la siguiente manera:

Teorema 3 (Agrawal, Kayal, Saxena, Lenstra)**.** *Sean n, r dos enteros positivos y sea S un conjunto finito de enteros. Suponiendo que:*

1. *n es una raíz primitiva módulo r,*
2. *$\gcd(n, b-b') = 1$ para todos elementos diferentes $b, b' \in S$,*
3. *$\binom{\#S+q-1}{\#S} \geq n^{2\lfloor\sqrt{r}\rfloor}$,*
4. *$(x+b)^n = x^n + b$ en el anillo $\mathbb{Z}_n[x]/(x^r-1)$, para todo $b \in S$,*

entonces n es una potencia de un primo.

Para mostrar que el algoritmo es correcto hay que verificar dos cosas: primero, si n es primo entonces el algoritmo debe dar como salida PRIME, pero esto es claro, ya que n no es una potencia perfecta ni posee factores pequeños ni satisface el teorema de AKS.

La parte difícil es demostrar que si el algoritmo produce como salida PRIME, entonces en efecto n es primo. Para esto último, se construye de manera conveniente un grupo cíclico G a partir de los elementos r, q dados por el algoritmo. G es un subgrupo del grupo multiplicativo $(\mathbb{F}_p[x]/h(x))^*$, siendo $h(x)$ un polinomio irreducible. Entonces se ha de mostrar que necesariamente n es una potencia del primo p o bien n tiene factores pequeños. Mas como esta segunda posibilidad ha sido descartada previamente, se ha de tener que n es primo. Para ver un bosquejo de la demostración del teorema AKS se puede consultar [17]. Para la demostración completa, detallada y presentada de varias maneras diferentes se puede consultar [3, 4, 5, 8, 16, 18, 21].

3. Estado actual y futuro de AKS

Finalmente revisemos el estado actual de AKS y algunas predicciones hechas. El problema de primalidad había sido tratado con teorías complicadas, tales como curvas elípticas, campos ciclotómicos, etc. Ha sido una gran sorpresa para muchos, que con métodos de álgebra básica se tenga una solución satisfactoria a este famoso problema. El algoritmo AKS, sin embargo, en su forma original [3] no es práctico, requiere un tiempo de ejecución $O(\log n^{10.5})$, mientras que el algoritmo más usado en la práctica (el de Miller-Rabin) tiene una complejidad en tiempo $O(\log n^3)$. Sin embargo, repetimos, como en casi todo nuevo invento hay una etapa de perfeccionamiento que casi siempre tiene buenos resultados.

En el caso de AKS el primer ajuste lo hizo Lenstra, como ya se mencionó, y fue publicado por los mismos autores, mejorando el tiempo asintótico a $O(\log n^{6.5})$ [4]. Posteriormente se dan otros perfeccionamientos, algunos de ellos presentados por D. Berstein en [8], particularmente con el cálculo mejorado de $(x+a)^n$ en el anillo $(\mathbb{Z}_n[x]/(x-1)^r)$. También se puede usar el método de Berstein para detectar potencias perfectas, lo cual se describe en [10], en un tiempo de ejecución lineal.

Otra propuesta fue hecha por P. Berrizbeitia y consiste en substituir la comprobación de la igualdad $(x+a)^n = (x^n+a) \bmod (x^r-1)$ por la de $(mx+1)^n = (1+mx^n) \bmod (x^{2^s}-a)$, para valores s, m adecuados. Esto reduce el número de evaluaciones polinomiales, lo cual, naturalmente es lo más deseado. La modificación da como resultado primos $n \equiv \pm 1 \bmod 4$.

Por otra parte, se han comparado los métodos AKS con el que utiliza curvas elípticas [20], y se ha propuesto combinar los dos métodos para hacer más eficiente la búsqueda [13]. Otras propuestas para mejorar el algoritmo se pueden consultar en [19, 22], así como análisis de su implementación en [11, 14]. Si se quiere ver la descripción de AKS como una lectura general, se puede ver [12], y para una consulta más completa y detallada [16, 21].

Finalmente los autores del algoritmo AKS prevén que si se resuelven algunas pequeñas conjeturas, (si $n \neq 1 \bmod r$ para algún $r > \log\log n$ y $(x-1)^n = (x^n-1) \bmod (x^r-1, n)$, entonces n necesariamente es primo), AKS puede alcanzar un perfeccionamiento $O(\log n^3)$, lo que sería una muy buena noticia. Los tiempos prácticamente aceptables son $O(\log n^4)$, mas por el momento uno se conforma con un algoritmo de tiempo promedio $O(\log n^6)$.

4. Problemas abiertos sobre números primos

Como tema final mencionamos algunos de los problemas abiertos que quedan aún en el tema de números primos, así como también algunos hechos importantes acerca de los números primos.

Conjetura de primos gemelos ¿Hay una cantidad infinita de números p tales que p y $p+2$ sean primos?

Conjetura de Goldbach Cada entero par, mayor a 2, puede escribirse como una suma de dos primos

¿Hay una cantidad infinita de primos de la forma n^2+1?

¿Existe siempre un primo entre n^2 y $(n+1)^2$?

Primos de Fermat ¿Hay una cantidad infinita de números de Fermat, $F_n = 2^{2^n}+1$ que sean primos? Más concretamente, ¿hay un entero $n > 4$, tal que

F_n sea primo?

¿Hay una cantidad infinita de números primos de la forma $n! \pm 1$?

¿Hay una cantidad infinita de números primos de la forma $n\# \pm 1$?

(donde por $n\#$ se denota al producto de todos los números primos menores o iguales a n.)

El número primo más grande conocido hasta hoy (anunciado en febrero del año 2005), es el 42° *primo de Mersenne*, $2^{25964951}-1$ de

7816230 dígitos decimales.

La última pareja de primos gemelos conocida hasta hoy (reportada en noviembre de 1995) es $(242206083 \cdot 2^{38880}-1, 242206083 \cdot 2^{38880}+1)$. Cada uno de los números que la componen posee 11713 dígitos decimales.

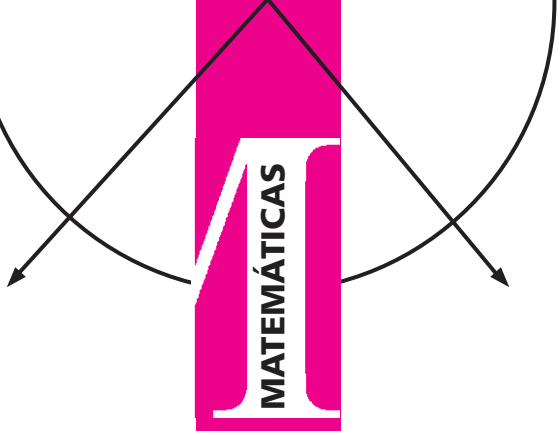
El primo más grande conocido hasta hoy de la forma $n! \pm 1$, es $3610!-1$, con 11277 dígitos, y fue anunciado en 1993.

Dado un primo p, se denota por $p\#$ al producto de todos los primos menores o iguales que p. El primo más grande conocido hasta hoy de la forma $p\# \pm 1$, es $24029\# + 1$, el cual se escribe con 10387 dígitos y fue reportado en 1993.

Bibliografía

1. L. M. Adleman, C. Pomerance, R. S. Rumely, "On Distinguishing Prime Numbers from Composite Number," *Ann. Math.* 117, 173-206, 1983.
2. L. M. Adleman, M. D. Huang, Primality testing and Abelian varieties over finite fields., Lecture Notes in Mathematics. 1512, Springer-Verlag. vii, 142 p. 1992
3. M. Agrawal, N. Kayal, N. Saxena, "Primes is in P," IITK Kanpur, August 6 2002. http://www.cse.iitk.ac.in/news/primality.pdf
4. M. Agrawal, N. Kayal, N. Saxena, "Primes is in P", revised version. IITK Kanpur. http://www.cse.iitk.ac.in/news/primality_v3.pdf
5. T. Alexander, C.S. Tou, "AKS Algorithm", Draft. University of Ottawa. http://padic.mathstat.uottawa.ca/~reports/AKS.pdf
6. A. O. L. Atkin, "Lecture notes of a conference," Boulder Colorado, Manuscript. 1986
7. A. O. L. Atkin and F. Morain, "Elliptic curves and primality proving," *Math. Comp.*, 61:203, pp. 29–68. July 1993
8. D. J. Bernstein, "Proving Primality After Agrawal-Kayal-Saxena", Draft. University of Illinois at Chicago. http://cr.yp.to/papers/aks.pdf
9. D. J. Bernstein, "Detecting Perfect Powers In Essentially Linear Time," *Mathemtics of Computation*, to appear. http://cr.yp.to/papers/powers.pdf
10. D. J. Bernstein, H.W. Lenstra, J. Pila, "Detecting Perfect Powers by Factoring into Coprimes," University of Illinois at Chicago. http://cr.yp.to/lineartime/powers2-20050509.pdf
11. V. Bhatt, G.K.Patra, "Analysis on Implementation and its further improvements of AKS class algorithms,", Research Report CM 0307, Bangalore 560 037, India. http://www.cmmacs.ernet.in/cmmacs/Publications/resch_rep/rrcm0307.pdf
12. F. Bornemann, "Primes Is in P: A Breakthrough for "Everyman"," *Notices of the AMS*, May 2003, translation of the German version 2002. http://www.ams.org/notices/200305/fea-bornemann.pdf
13. Q. Cheng, "Primality proving via one round in ECPP and one iteration in AKS', The University of Oklahoma, Norman OK 73019. http://cr.yp.to/bib/2003/cheng.pdf
14. R. Crandall, J. Papadopoulos, "On the implementation of AKS-class primality test", University of Maryland, Apple Computer, 18 Mar 2003. http://images.apple.com/acg/pdf/aks3.pdf
15. S. Goldwasser, J. Killian, "A provably correct and probably fast primality test", *Proceedings of the 18th Annual ACM Symposium on the Theory of Computing*, 1986.
16. A. Granville, "It is easy to determine whether a given integer is prime," *Bulletin of the American Mathematical Society,* Volumen 42, Number 1, Pages 3-38. http://www.mathematik.uni-wuerzburg.de/~mueller/Teach/granville.pdf
17. M. J. Jacobson Jr., *"An Exposition of the AKS Polynomial-Time Primality Test"*, University of Calgary, November 29, 2002.
18. A. Klappenecker, "An Introduction to the AKS Primality Test", Texas A&M University. http://faculty.cs.tamu.edu/klappi/629/aks.pdf
19. M. Mačaj, "Some remarks and questions about the AKS algorithm and related conjecture", Comenius University, Slovakia. http://thales.doa.fmph.uniba.sk/macaj/aksremarks.pdf
20. C. Rotella, "An efficient implementation of the AKS polynimial time proving algorithm," April 29, 2005. http://www-2.cs.cmu.edu/afs/cs.cmu.edu/user/mjs/ftp/thesis-05/rotella-thesis.pdf
21. M. Smid, "Primality testing in polynomial time", Carleton University Ottawa, Ontario. http://www.scs.carleton.ca/~michiel/primes.ps.gz
22. J.F. Voloch, "Improvements to AKS", University of Texas, Austin USA. http://www.ma.utexas.edu/users/voloch/Preprints/aks.pdf

Campos de funciones algebraicas



Felipe Zaldívar
fzc@oso.izt.uam.mx
UAM-Iztapalapa

Introducción. En la teoría de números es usual considerar el paralelismo entre el estudio de las extensiones finitas del campo de los números racionales, a las que se conoce como *campos de números*, y el estudio de las extensiones finitas del campo de funciones algebraicas en una variable sobre un campo finito, a las que se conoce como *campos de funciones algebraicas*, y para las cuales se tiene además la ventaja de poder estudiarlas desde el punto de vista de la geometría algebraica. La publicación reciente del libro *Topics in the Theory of Algebraic Function Fields*, de Gabriel Villa [15], motiva el ensayo siguiente, como introducción a una reseña del libro mencionado.

Aritmética de curvas algebraicas. Aunque, desde un punto de vista clásico, las curvas algebraicas están definidas sobre campos algebraicamente cerrados (usualmente, $\mathbb{C}$), en teoría de números es natural considerar curvas (o variedades algebraicas de dimensión superior) definidas, por ejemplo, sobre $\mathbb{Q}$, es decir definidas por los ceros de polinomios con coeficientes en $\mathbb{Q}$, y aunque todos los puntos de la curva C tienen coordenadas en $\overline{\mathbb{Q}}$, una cerradura algebraica de $\mathbb{Q}$, en teoría de números interesa detectar cuáles puntos de C están en $C(\mathbb{Q})$, i.e., tienen coordenadas en $\mathbb{Q}$, y una forma de detectar estos puntos con coordenadas racionales es considerar el grupo de Galois $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, el cual actúa naturalmente en los puntos de C (ya que C está definido por polinomios con coeficientes en $\mathbb{Q}$) y así se tiene que

$$C(\mathbb{Q}) = \{P \in C \ : \ \sigma P = P \quad \text{para todo } \sigma \in G_{\mathbb{Q}}\}.$$

Ahora, aún cuando uno sólo esté interesado en el problema diofantino de estudiar los puntos racionales en C, como la curva está definida por polinomios con coeficientes racionales, multiplicando por los denominadores de los coeficientes de estos polinomios, puede uno suponer que C está definida por polinomios con coeficientes enteros y las coordenadas proyectivas de los puntos en $C(\mathbb{Q})$ se pueden elegir enteras, es decir, para una curva proyectiva lisa C definida sobre $\mathbb{Q}$, y por lo tanto sobre $\mathbb{Z}$, se tiene que $C(\mathbb{Q}) = C(\mathbb{Z})$, por lo que si C tiene puntos con coordenadas racionales (i.e., enteras) podemos reducir módulo p, para p un primo arbitrario, las coordenadas de estos puntos para obtener puntos con coordenadas en el campo finito $\mathbb{F}_p$ en la curva $\overline{C}$ definida por la reducción módulo p de los polinomios que definen C. Así, si existiera un primo p tal que $\overline{C}(\mathbb{F}_p) = \emptyset$ entonces C no puede tener puntos racionales, i.e., $C(\mathbb{Q}) = \emptyset$. Lo anterior nos puede servir como motivación para el estudio de curvas, o variedades algebraicas de dimensión superior, definidas sobre campos finitos. En un principio este estudio fue modelado por lo que se conocía en el caso clásico de variedades algebraicas definidas sobre un campo algebraicamente cerrado, usualmente $\mathbb{C}$, y a la luz de lo anterior pueden interpretarse en este lenguaje resultados que se remotan a Gauss y Jacobi que, en su estudio de leyes de reciprocidad superiores, tuvieron que considerar congruencias de la forma

$$y^2 \equiv ax^4 - b \ (\mod p)$$

para las cuales necesitaban dar estimaciones asintóticas, en términos del primo p, al número de soluciones en $\mathbb{F}_p$ de estas ecuaciones cuando p varía en un conjunto infinito de primos (véase, por ejemplo, la introducción en [18]). Ya en el siglo XX, Mordell y Davenport generalizan lo anterior al considerar curvas de la forma

$$y^k \equiv f_n(x) \ (\mod p)$$

para $f_n(x)$ un polinomio de grado n, y con k y n pequeños, obteniendo estimaciones asintóticas del número de soluciones de tales ecuaciones, al variar el primo p.

La función zeta de una curva. Al inicio del siglo XX, Emil Artin en su tesis doctoral [1] estudia campos de funciones cuadráticos sobre un campo finito, en analogía con la teoría clásica de la aritmética de formas cuadráticas, desarrollando los fundamentos de la descomposición en ideales primos, ramificación, unidades del anillo de enteros, número de clases, análogos de la ley de reciprocidad cuadrática de Gauss e introduce una herramienta fundamental en el estudio de curvas sobre campos finitos: comenzando con un campo finito $\mathbb{F}_q$ y el campo de funciones racionales en una variable $k := \mathbb{F}_q(T)$ y una extensión cuadrática $K = k(\sqrt{D})$, donde $D = f(T)$ es un polinomio en T sin raíces múltiples, Artin observa que la cerradura entera $\mathcal{O}_K \subseteq K$ del anillo $\mathbb{F}_q[T] \subseteq k$ satisface que: (i) es un anillo de Dedekind, (ii) para todos los ideales primos $\mathfrak{p}$ de $\mathcal{O}_K$ el campo $\mathcal{O}_K/\mathfrak{p}$ es finito (de hecho, es una extensión finita de $\mathbb{F}_q$) y por lo tanto, siguiendo la construcción de Dedekind de las funciones zeta asociadas a campos de números (extensiones finitas de $\mathbb{Q}$) que generalizan a la clásica función zeta de Riemann, Artin puede asociar al campo K una función zeta que de hecho es más sencilla que la considerada por Dedekind porque la puede escribir de la forma $Z(q^{-s})$ donde $Z(t)$ es una *función racional* con coeficientes en $\mathbb{Q}$. Más aún, esta función zeta también satisface una ecuación funcional que expresa el cociente $Z(1/qt)/Z(t)$ como una función racional cuyos ceros y polos eran fácilmente discernibles y Artin demuestra que, para polinomios $f(T)$ de grado pequeño, los ceros de $Z(t)$ están en el círculo $|t| = q^{1/2}$, un hecho que puede ser interpretado como el análogo de la hipótesis de Riemann para estas nuevas funciones zeta. Basado en los ejemplos que había considerado, Artin conjetura que lo anterior debe ser cierto en general. Los resultados anteriores

de Artin pueden considerarse en el lenguaje de curvas sobre campos finitos, recordando que en el caso clásico, si C es una curva proyectiva lisa sobre un campo k algebraicamente cerrado, el campo $k(C)$, de funciones regulares en C, es una extensión finita del campo de funciones racionales $k(T)$ y, recíprocamente, si K es una extensión finita de $k(T)$, existe una (única, salvo isomorfismo) curva proyectiva lisa C sobre k, tal que $k(C)$ es k-isomorfo a K. Más aún, los puntos de C están en correspondencia biunívoca con los lugares de K. Así, al estudiar extensiones cuadráticas K de $\mathbb{F}_q(T)$, Artin estaba considerando curvas sobre el campo finito $\mathbb{F}_q$, y después de la tesis de Artin comenzó un estudio sistemático, por Sengenhorst, Rauter y F. K. Schmidt, de campos de funciones algebraicos con campo base finito, explorando la analogía con el caso de campos de números, obteniendo los resultados de estructura fundamentales, primero para la teoría aritmética y luego para la parte analítica, y se sistematiza el estudio de las funciones zeta asociada a estos campos, especialmente por Schmidt [13], que demuestra el teorema de Riemann-Roch para campos de funciones, y como consecuencia casi inmediata la racionalidad de la función zeta de un campo de funciones algebraicas en una variable sobre un campo finito (con respecto a la variable q^{-s}) y la existencia de una ecuación funcional para estas funciones zeta, generalizando los ejemplos cuadráticos de Artin. La hipótesis de Riemann para estas funciones zeta fue demostrada poco después por H. Hasse [8] en el caso de género 1, al probar que el número de puntos $\mathbb{F}_q$-racionales de una tal curva elíptica E definida sobre $\mathbb{F}_q$ satisface la desigualdad $||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}$, generalizando los resultados parciales de Artin, Mordell y Davenport en el caso de género 1, de donde la hipótesis de Riemann se sigue por argumentos formales. La hipótesis de Riemann fue demostrada para curvas en general por A. Weil [16] que tuvo que desarrollar la geometría algebraica necesaria para poder construir [17] la Jacobiana de una curva definida sobre un campo arbitrario (en particular, sobre un campo finito).

La conjetura de Weil. Es importante mencionar que lo anterior puede ser desarrollado para variedades algebraicas de dimensión arbitraria sobre campos finitos, incluyendo la definición de funciones zeta asociadas a estas variedades y en el mismo trabajo donde Weil demuestra la hipótesis de Riemann para curvas arbitrarias sobre campos finitos, puede demostrarla también para algunas variedades de dimensión superior y en el artículo [18] ya puede conjeturar que si X es una variedad algebraica sobre un campo finito, entonces la función zeta correspondiente, definida como

$$Z(X,t) := \exp\Big(\sum_{n=1}^{\infty} |X(\mathbb{F}_{q^n})| t^n/n\Big)$$

donde $|X(\mathbb{F}_{q^n})|$ es el número de puntos de X en el campo finito $\mathbb{F}_{q^n}$, debe satisfacer las propiedades siguientes:

- Tiene una descomposición en producto de Euler.
- Satisface una ecuación funcional que relaciona $Z(1/q^n t)$ con $Z(t)$
- Es una función racional, i.e., es el cociente de dos polinomios en t. De hecho, se puede escribir de la forma

$$Z(X,t) = \frac{f_1(t) f_3(t) \cdots f_{2d-1}(t)}{f_0(t) f_2(t) \cdots f_{2d}(t)}$$

  donde $d = \dim X$, cada $f_j(t)$ es un polinomio con coeficientes enteros y término independiente 1, y los grados de los polinomios $f_j(t)$ deben ser los j-ésimos números de Betti de X (más bien, si X aparece como la reducción de una variedad compleja $\hat{X}$, los números de Betti anterior deben ser los de $\hat{X}$).
- Los recíprocos λ de los ceros de f_j tienen el mismo valor absoluto $|\lambda| = q^{j/2}$ (lo cual es la hipótesis de Riemann para estas funciones zeta).

Y, siguiendo una analogía con la geometría algebraica clásica (i.e., sobre $\mathbb{C}$), la demostración de estas conjeturas debiera ser por medio de una *teoría de cohomología* adecuada, donde los invariantes involucrados sean los invariantes cohomológicos asociados. Para tener una idea de lo que se buscaba, observemos que si $\overline{\mathbb{F}}_q$ es una cerradura algebraica de $\mathbb{F}_q$, el grupo de Galois $G_{\mathbb{F}_q} := \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ actúa en forma natural sobre los puntos de X y así el conjunto $X(\mathbb{F}_q)$ de puntos de X con coordenadas $\mathbb{F}_q$-racionales está dado por

$$X(\mathbb{F}_q) = \{P \in X \ : \ \sigma(P) = P \quad \text{para todo } \sigma \in G_{\mathbb{F}_q}\}$$

y como el grupo $G_{\mathbb{F}_q}$ está (topológicamente) generado por el automorfismo de Frobenius $\mathrm{Fr} : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$, entonces $X(\mathbb{F}_q)$ está dado por los puntos fijos de este automorfismo, y si se tiene un análogo de la fórmula de punto fijo o de traza de Lefschetz, entonces al aplicarla a la potencia n-ésima del automorfismo de Frobenius $\mathrm{Fr} : X \to X$ se obtiene [7] la fórmula

$$Z(X,t) = \sum_{i=0}^{2d} \det\big(\mathrm{id} - tH^i(\mathrm{Fr})\big)^{(-1)^{i+1}}$$

donde $H^i(\mathrm{Fr})$ es el morfismo inducido en cohomología por el automorfismo de Frobenius en X, lo cual muestra que $Z(X,t)$ es racional y para probar las otras conjeturas de Weil es necesario probar que $\det\big(\mathrm{id} - tH^i(\mathrm{Fr})\big)$ es un polinomio con coeficientes enteros y que los valores propios λ de $H^i(\mathrm{Fr})$ tienen valor absoluto $q^{i/2}$. El desarrollo de este programa, para crear la teoría de cohomología adecuada, se debe a A. Grothendieck y su escuela, que al mismo tiempo reescribieron los fundamentos de la geometría algebraica para hacerlos adecuados a las exigencias de la formulación, interpretación y demostración de las conjeturas anteriores, un desarrollo cuyas consecuencias se han dejado sentir en casi toda la matemática.

Módulos de Drinfeld. Hacia 1935, otra forma de estudiar curvas sobre campos finitos fue iniciada por L. Carlitz [2] al asociar a una tal curva C no una función zeta compleja como había hecho Artin, sino una función exponencial $e_C(z)$ que compartía propiedades análogas a la función exponencial e^z usual pero, que un cierto sentido tomaba valores y es analítica en característica finita p y satisface una ecuación funcional de la forma

$$e_C(az) = C_a(e_C(z)) \qquad \text{para } a \in \mathbb{F}_q[T]$$

donde C_a es un polinomio aditivo, i.e., $C_a(x+y) = C_a(x) + C_a(y)$ (y notamos que estos polinomios aditivos sólo existen no trivialmente en característica finita), y también satisface que

$$C_{ab}(z) = C_a(C_b(z)) = C_b(C_a(z)) = C_{ba}(z).$$

Usando esta función exponencial, Carlitz pudo obtener análogos de objetos de interés aritmético tales como factoriales y números de Bernoulli, por ejemplo probando análogos del teorema de von Staudt-Claussen y la existencia de análogos de polinomios de Bernoulli, hasta que en 1974, D. Hayes [9] demuestra que los valores de torsión de $e_C(z)$ generan buenas extensiones ciclotómicas de $\mathbb{F}_q[T]$ en forma análoga a como los valores de torsión de la exponencial usual $e^{2\pi i z}$ generan las extensiones ciclotómicas $\mathbb{Q}(\omega)$ usuales.

En el mismo año 1974, V. Drinfeld [4] inicia el estudio de la teoría de funciones exponenciales de rango arbitrario que generalizan la función de Carlitz (siendo esta de rango 1) asociadas ahora a

un campo de funciones arbitrario. Drinfeld demuestra que estas funciones exponenciales dan lugar a ciertos objetos algebraicos, *módulos elípticos*, llamados ahora *módulos de Drinfeld*, donde la función $a \mapsto C_a(z)$, el *módulo de Carlitz* es ahora el más simple de los módulos de Drinfeld, y más importantemente, Drinfeld construye el espacio de parámetros de estos objetos y demuestra un teorema de uniformización para estos espacios de parámetros usando la teoría de Tate de espacios analíticos rígidos. El objetivo principal de Drinfeld [5], la demostración de las leyes de reciprocidad no abelianas para campos de funciones, es decir, de las conjeturas de Langlands para campos de funciones, fue completado con éxito por Lafforgue en [10].

Reseña. El libro de Gabriel Villa da un panorama introductorio, bastante completo, al estudio de las curvas sobre campos finitos, usando los dos puntos de vista descritos anteriormente, con énfasis en la teoría clásica, comenzando con un estudio de curvas algebraicas sobre un campo arbitrario, en el lenguaje equivalente de campos de funciones algebraicas en una variable, cubriendo los temas esperados: divisores, grupos de clases, diferenciales, género y el teorema de Riemann-Roch, con ejemplos para campos de funciones racionales y campos de funciones de género 0, curvas elípticas o campos de funciones elípticos y campos de funciones de género 1 y extensiones cuadráticas de campos de funciones, para después estudiar extensiones arbitrarias de campos de funciones, en particular extensiones de Galois y ramificación. En el capítulo 6 especializa la discusión a campos de funciones algebraicas con campo de constantes finito, i.e., curvas algebraicas sobre campos finitos, introduciendo las funciones zeta asociadas y probando algunas de sus propiedades, en particular la existencia de la ecuación funcional para estas funciones zeta, culminando en el capítulo 7 con la demostración de la hipótesis de Riemann para curvas sobre campos finitos siguiendo la demostración de Stepanov-Bombieri, y en los capítulos 8, 9 y 14 completa el estudio de la aritmética de curvas sobre campos finitos incluyendo una demostración de la fórmula de Riemann-Hurwitz que relaciona los géneros de los campos en una extensión finita separable de campos de funciones e incluye algunos ejemplos, notablemente el de curvas hiperelípticas. El capítulo 14, comienza con una demostración de la desigualdad de Castelnuovo-Severi (que Weil había usado en una de sus demostraciones de la hipótesis de Riemann para curvas) y hace un estudio cuidadoso de los puntos de Weierstrass en una curva para luego aplicarlo al grupo de automorfismos de un campo de funciones. En los capítulos 12 y 13 el libro toma el punto de vista de Carlitz-Drinfeld, comenzando con la teoría de Carlitz y Hayes sobre campos de funciones ciclotómicas, y donde ya usa la herramienta más avanzada de la teoría de campos de clases que convenientemente recordó en el capítulo 11, para demostrar, por ejemplo, la existencia de un número infinito de polinomios irreducibles en una progresión $N + Mu$, con N, m polinomios mónicos no constantes y coprimos, usando el teorema de densidad de Chebotarev, recordado en el capítulo 11, y culminando con la demostración [11] de un análogo del teorema de Brauer-Siegel para la clase de campos de funciones ciclotómicos sobre un campo de constantes finito, cuya versión *clásica* fue previamente presentada en §7.6 para curvas algebraicas sobre un campo finito. El capítulo 13 es una introducción a la teoría de módulos de Drinfeld, desde su definición como una generalización de los módulos de Carlitz hasta la demostración de su existencia usando retículas del rango correspondiente y culminando con una construcción explícita de la máxima extensión abeliana de un campo de funciones con campo de constantes finito. De alguna forma, y tal vez debido a la longitud y nivel elegido para el libro, faltó una introducción al estudio de las *shtukas* de Drinfeld que podría haber concluido con una discusión del trabajo más reciente de Lafforgue que culmina el proyecto de Drinfeld de probar las conjeturas de Langlands para campos de funciones en el caso global.

En la versión en español, el libro de Gabriel Villa, publicado por el Fondo de Cultura Económica, es el único en nuestro idioma y como tal ha venido a llenar un vacío en nuestra literatura. La versión en inglés, publicada por Birkhäuser, tiene más competencia: por ejemplo, los libros de Goss [6], Rosen [12] y Thakur [14] de publicación más o menos reciente intersectan con el libro de Villa en varios lugares; el libro de Goss está orientado totalmente al punto de vista de Carlitz-Hayes y Drinfeld, lo mismo que el libro de Thakur. Con respecto al libro de Rosen, se tienen más coincidencias: ambos tratan la teoría clásica de campos de funciones de Artin, Hasse, Schmidt y Weil, desde los fundamentos hasta la hipótesis de Riemann (ambos demostrándola siguiendo las ideas de Bombieri), el libro de Rosen incluye un capítulo dedicado a la conjetura de Brumer-Stark (conjetura para campos de números, teorema para campos de funciones, gracias al trabajo de Tate-Deligne y Hayes) y otro capítulo donde estudia una conjetura de Artin sobre raíces primitivas (de nuevo, conjetura para $\mathbb{Q}$ y teorema para campos de funciones; una versión de la conjetura de Artin, para $\mathbb{Q}$, sería que 2 es raíz primitiva de un conjunto infinito de primos). El libro de Rosen también incluye una introducción a la teoría de Carlitz-Drinfeld. En fin, los libros de G. Villa y M. Rosen ofrecen un panorama amplio de la teoría de campos de funciones algebraicas desde el punto de vista aritmético, enfatizando los paralelos existentes con la teoría de campos de números, al mismo tiempo que incluyen una introducción a la teoría de Carlitz, Hayes y Drinfeld, que puede ser estudiada más a profundidad en los textos de Goss y Thakur. Tanto el profesional como el estudiante que se inicia en estas áreas encontrará en estos libros el material que necesita, incluyendo una amplia gama de ejercicios que iluminan y complementan lo discutido en los textos.

Referencias

1. Artin, E., Quadratische Körper im Gebiet der höheren Kongruenzen I, II, *Math. Z.* **19**, 1924, 153-246. Collected Papers 1-94, Addison-Wesley, Reading, 1965.
2. Carlitz, L., On certain functions connected with polynomials in a Galois Field. *Duke Math. J.* **1**, 1935, 137-168.
3. Deligne, P., La Conjecture de Weil I. *Pub. Math. IHES*, **43**, 1974, 273-307.
4. Drinfeld, V., Elliptic modules. *Math. Sbornik*, **94**, 1974, 594-627. English translation: *Math. U.S.S.R. Sbornik*, **23**, 1976, 561-592.
5. Drinfeld, V., Proof of the Global Langlands Conjecture for GL(2) over a Function Field. *Funct. Anal. and its Appl.*, **11**, 1977, 223-225.
6. Goss, D., *Basic Structures of Function Field Arithmetic*. Springer Verlag, Berlín, 1996.
7. Grothendieck, A., Formule de Lefschetz et rationalité des fonctions L, *Séminaire Bourbaki*, Exp. No. 279, W. A. Benjamin, New York, 1966. Reeditado en *Astérisque*, **9**, 1995, 41-55.
8. Hasse, H., Zur Theorie der abstrakten elliptischen Funktionen körper. III. Die Struktur des Meromorphismenrings; die Riemannsche Vermutung. *J. Reine Angew. Math.*, **175**, 1936, 193-208.
9. Hayes, D., Explicit class-field theory for rational function fields. *Trans. Amer. Math. Soc.*, **189**, 1974, 177-91.

10. Lafforgue, L., Chtoucas de Drinfeld et correspondance de Langlands. *Inv. Math.*, **147**, 2002, 1-241.

11. Lam-Estrada, P. and Villa-Salvador, G. D., Some remarks on the theory of cyclotomic function fields. *Rocky Mountain J. Math.*, **31**, 2001, 483-502.

12. Rosen, M., *Number Theory in Funcion Fields*. Springer Verlag, Berlín, 2002.

13. Schmidt, F. K., Zur arithmetischen Theorie der algebraischen Funktionen. I. Beweis des Riemann-Rosches Satzes für algebraische Funktionen mit beliebigen Konstantenkörper. *Math. Z.* **41**, 1936, 415-438.

14. Thakur, D., *Function Field Arithmetic*. World Scientific, Singapore, 2004.

15. Villa Salvador, G. D., *Topics in the Theory of Algebraic Function Fields*. Birkhäuser Verlag, Boston, 2006.

16. Weil, A., On the Riemann Hypothesis in function fields. *Proc. Nat. Acad. Sci. U.S.A.*, **27**, 1941, 345-347.

17. Weil, A., *Varietés abéliennes et courbes algébriques*. Herman, París, 1948.

18. Weil, A., Numbers of Solutions of Equations in Finite Fields. *Bull. Amer. Math. Soc.* **55**, 1949, 497-508.

Álgebra Lineal
por
Fernando Barrera Mora
Grupo Editorial Patria, 2007

Uno de los temas de matemáticas más populares acerca de los cuales se han escrito innumerables textos es el álgebra lineal. Esto no es ninguna casualidad. El álgebra lineal aparece de manera natural en prácticamente todas las disciplinas, tanto de matemáticas como de otras ciencias, inclusive en las áreas de ciencias sociales y humanidades, teniendo presencia significativa en las áreas de ingeniería y no digamos de física.

Desde nuestros primeros estudios, digamos a nivel de secundaria, el álgebra lineal se estudia, aunque no se use el nombre, para la resolución de sistemas de ecuaciones lineales. Debido a lo anterior, cuando un nuevo texto relacionado con el álgebra lineal aparece en el mercado, uno se pregunta qué puede aportar este nuevo texto que no haya sido presentado y estudiado hasta la saciedad en algunos de los innumerables textos que ya existen.

El libro de Fernando Barrera está dedicado al álgebra lineal de un primer curso de licenciatura en matemáticas. El primer punto que me gustaría hacer notar es que el libro privilegia el empezar con problemas concretos que se nos presentan tanto en nuestra vida cotidiana, como en economía, en empresas productivas, etc. A partir de estos problemas concretos se empieza a elaborar sobre los ingredientes presentes que facilitan la visualización del estudiante de estas componentes cuando son planteados de manera general.

Asimismo, estos problemas concretos que se estudian sirven para establecer tanto los métodos como la teoría necesaria ya sea para resolverlos, para estudiarlos o para ubicarlos en un contexto más general. Un punto de vista valioso a resaltar en este trabajo es el tratamiento que se hace de lo que podríamos llamar la "teoría propia", esto es, la teoría que trata sobre los valores y los vectores propios. Lo más común para abordar la solución y estudio de los valores y vectores propios es el estudio de la matriz característica, es decir, encontrar los valores para los cuales esta matriz es no singular lo cual nos lleva inmediatamente al cálculo del determinante y por tanto al polinomio característico. Aunque el análisis de determinantes es indispensable en el estudio del álgebra lineal, el presentar un estudio exhaustivo de sus propiedades básicas es un problema ya sea laborioso o poco claro, dependiendo del enfoque que seleccionemos.

En este trabajo se selecciona un camino diferente. Se hace énfasis en propiedades inherentes a la matriz que dan origen al problema en estudio. Más precisamente, se estudia el operador asociado a la matriz con respecto a otra base seleccionada adecuadamente. Además de la ventaja natural que se tiene al estudiar de manera intrínseca al operador, se tiene que se hace una presentación sin ninguna necesidad de hacer referencia a los determinantes. Hay varias otras novedades que diferencían este texto de otros. Por ejemplo, en este trabajo se hace interactuar el álgebra lineal con la geometría analítica; se introducen y se trabajan subespacios sin haber siquiera definido formalmente lo que es un espacio vectorial; hay varias demostraciones novedosas o poco conocidas como por ejemplo la de la existencia del operador adjunto o que cualquier sistema linealmente independiente tiene cardinalidad menor o igual a la cardinalidad de un conjunto de generadores; se construye la base teórica necesaria a partir del espacio dos dimensional, se pasa al tres dimensional y finalmente a cualquier espacio finito dimensional; se presenta un algoritmo para el cálculo del polinomio mínimo de una matriz.

Otros aspectos dignos de mencionar son la forma en que se motiva el producto de matrices el cual se deriva a partir de un ejemplo concreto sobre producción y que se encuentran varios ejercicios ya sea originales o poco comunes en otros textos. Un punto final que es necesario enfatizar es, como se mencionó al principio, el álgebra lineal es de mucha importancia en todo curriculum de ciencias y de ingeniería e inclusive de otras áreas. Esta importancia se encuentra en la mente del autor a lo largo de este libro, lo cual se puede percibir por la concepción del álgebra lineal que se presenta durante todo el tratado.

Gabriel D. Villa Salvador
Departamento de Control Automático
CINVESTAV - IPN
México, D. F.

Cálculo y sus fundamentos para ingeniería y ciencias
Antonio Rivera Figueroa
arivera@cinvestav.mx
Grupo Editorial Patria, 2007
ISBN: 978-970-817-069-7

El libro está dirigido a estudiantes y profesores de las carreras de las áreas de ciencias físico-matemáticas o ingeniería. Los requisitos previos para su lectura son haber estudiado un curso de geometría analítica y un curso elemental de cálculo diferencial e integral de nivel bachillerato; aunque quienes carezcan de esos conocimientos podrán estudiarlo parcialmente, por ejemplo, podrán leer sólo algunos capítulos o fragmentos cuidadosamente seleccionados y de algunos de los teoremas podrán omitir la lectura de sus pruebas.

Como se expresa en el título mismo, se trata de un libro de cálculo diferencial e integral, pero también de sus fundamentos, lo que significa que en éste se establecen las propiedades de las funciones continuas que dan sustento al cálculo y se prueban con detalle los resultados acerca de la derivada y de la integral, desde los más simples hasta los más complicados. Con una selección adecuada de capítulos o secciones de capítulos, el libro puede usarse en los cursos de cálculo de ingeniería o estudiarse con plenitud en una carrera de ciencias físico-matemáticas. De igual modo, puede ser de utilidad para los lectores con conocimientos de cálculo que aspiren a una sólida formación matemática y sin duda resultará de interés para los profesores que enseñan cálculo en el nivel universitario, pues en la obra encontrarán las demostraciones de los principales resultados del cálculo, en particular las que suelen omitirse en obras similares. En suma, el libro se ofrece a un amplio público y es una opción para quienes deseen iniciarse en el arte de la demostración matemática.

Al planear y escribir este libro, el autor puso especial cuidado en la organización de los temas, conceptos y resultados, siempre teniendo en mente el orden lógico de los mismos, pero considerando a la vez que resultasen didácticos y útiles en el desarrollo de la teoría y sus aplicaciones. Por ejemplo, es común que en un tratamiento riguroso del cálculo en donde primero se estudia la derivada y después la integral, las funciones exponencial y logaritmo hagan su aparición después de haberse presentado el concepto de integral definida. La construcción de estas importantes funciones basada en la integral definida, resulta un poco tardía y desventajosa pues su ausencia durante el estudio de la derivada y la integral, limita y empobrece la ilustración, ejemplificación o aplicación de estos conceptos y de sus principales resultados; sin estas funciones y las trigonométricas directas e inversas, sólo dispondremos de las funciones polinomiales, racionales y algebraicas. En este libro, las potencias con exponentes irracionales se obtiene como resultado de aproximaciones de potencias con exponentes racionales, son límites de este tipo de expresiones, por lo que con esta construcción, la exponencial definida en los reales resulta una extensión natural de la exponencial con dominio los racionales. Para este acercamiento, en el libro se desarrollan propiedades de la exponencial definida sólo para racionales y se recurre a propiedades de las sucesiones y sus límites, ésta es una de las razones por lo que las sucesiones y las series se presentan casi al inicio del libro.

Cabe destacar que a lo largo de la obra se hacen algunas reflexiones sobre situaciones especiales en las que aun el lector experimentado quizá no haya reparado y que con seguridad le resultarán de gran interés.

Antonio Rivera Figueroa
arivera@cinvestav.mx
Centro de Investigación y de Estudios Avanzados del IPN
Departamento de Matemática Educativa

El legado matemático de Leonhard Euler a trescientos años de su nacimiento
Editado por: A. Anzaldo, J. Delgado, F. Monroy
Editorial UAM, México, 2007, v+335 pp. ISBN 978-970-773-375-6.

En 2007 se cumplieron 300 años del nacimiento de uno de los más grandes matemáticos que ha dado la humanidad: Leonhard Euler (1707-1783) lo cual ha sido una oportunidad magnífica para hacer un recuento, aunque sea parcial, de sus múltiples aportaciones en la ciencia, especialmente en la matemática y la física. El libro en cuestión se une a esta celebración, reuniendo una colección de artículos donde se comenta, resume y expone con diversos matices, énfasis y detalle, desde un breve esbozo de una biografía intelectual de Euler por J. L. Huerta y F. Monroy, pasando por algunas de las aportaciones de Euler a la mecánica celeste (M. Álvarez y J. Delgado), la hidrodinámica (J. Esquivel y M. Guzmán), la cuerda vibrante (G. Corona y S. Arellano) que podríamos pensar que dan un panorama de las aportaciones de Euler a la física, pasando luego a dar un repaso de algunas aportaciones de Euler a la teoría de números (J. Mejía y A. Cueto), desde su iniciación en el tema al reconstruir algunas aportaciones de Fermat, pasando por el problema de la suma de la serie de los inversos de los cuadrados de los enteros positivos (la función que ahora llamamos de Riemann) para después poner en contexto propio la importancia de la función zeta y la distribución de primos incluyendo algunas cuestiones sobre irracionalidad y trascendencia (J. Cruz Sampedro, S. Hernández, M. Tetzalmatzi), después se incluye un estudio de las aportaciones de Euler al estudio de curvas elásticas (A. Anzaldo y C. Romero) incluyendo algo de la contribución de Euler al estudio de integrales elípticas en su relación con el péndulo y así pasar al repaso de ciertas contribuciones de Euler al análisis (J. Navarro y D. Elizarraz), desde el método de máximos y mínimos y los inicios del cálculo de variaciones con una extrapolación a la actualidad, en particular considerando integrales de Feynman (H. Núñez y A. Salas), temas de estabilidad mediante funcionales (L. Aguirre y P. Seibert), análisis complejo, en particular incluyendo a la función gama de Euler y la función exponencial (L. Reséndiz y L. Tovar) y concluyendo con temas de teoría de gráficas, recordando su creación por Euler cuando resuelve el problema de los puentes de Königsberg y del inicio de la topología algebraica al calcular la característica de Euler-Poincaré de poliedros (G. Rodríguez y F. Zaragoza).

La oportunidad temporal del aniversario euleriano ha sido un pretexto invaluable para poner en contexto y difundir la importancia de la obra matemática de Euler, y de la matemática en general, a un público amplio, que en el caso del libro en cuestión se supone que tiene gusto y educación matemática media. La elección de los temas por los editores y el esfuerzo genuino puesto por los autores de los diversos artículos por hacer accesible, con un lenguaje matemático preciso y entendible aun por los no especialistas del tema, hacen de esta colección un magnífico instrumento para alcanzar sus objetivos, incluyendo el de poner al alcance de los jóvenes interesados en nuestra ciencia una obra que al mismo tiempo que celebra las aportaciones de uno de sus más grandes exponentes, pone a su alcance un panorama bastante amplio de la matemática que se cultiva en la actualidad realzando la *atemporalidad* característica de la matemática. Nuestra cultura, nuestro idioma, han estado durante mucho tiempo dependientes de traducciones de obras como la que ahora estamos comentando y es saludable encontrar que se pueden tener aportaciones originales que adornan el noble arte de difundir la ciencia a un público que bien puede suponerse amplio e importante. En nuestro medio, sólo la Sociedad Matemática Mexicana emprendió una empresa semejante al dedicar dos números monográficos de la revista *Miscelánea Matemática* a las aportaciones de Euler y felizmente la intersección de los contenidos con la obra que estamos discutiendo es mínima, lo cual sólo atestigua, si hiciera falta, la magnitud de la obra de Euler.

La publicación de esta colección de artículos, sirve no sólo a los objetivos comentados anteriormente, sino también coopera a poner en la atención de un público joven interesado en la ciencia, algunos nombres de profesores-investigadores de nuestro medio, sembrando, quizá, una semilla cuyos frutos vendrán en el futuro.

Felipe Zaldívar
fzc@oso.izt.uam.mx
Departamento de Matemáticas
UAM-Iztapalapa

1° Semana Internacional de la Estadística y la Probabilidad

Atenta Invitación.

La Facultad de Ciencias Físico Matemáticas de la Benemérita Universidad Autónoma de Puebla, a través del Cuerpo Académico de Probabilidad y Estadística, tiene el gusto de hacer una atenta invitación a toda la comunidad universitaria, investigadores, profesionistas y público en general, interesados en estas áreas, a asistir y participar en la

1ª Semana Internacional de la Estadística y la Probabilidad

en donde se llevarán a cabo actividades tales como exposiciones orales, exposiciones en forma de cartel, talleres, minicursos, mesas redondas, así como exposiciones magistrales por investigadores de gran prestigio internacional en el estudio y aplicación de las materias ya mencionadas. Este evento se llevará a cabo del 14 al 18 de julio , en las instalaciones de nuestra Facultad, teniendo como temáticas principales:

"Probabilidad y Estadística Orientada a la Aplicación y la Educación"

Este es un encuentro a nivel internacional cuyo objetivo principal es propiciar la reflexión, el intercambio de ideas, de experiencias y resultados en torno a la Probabilidad y la Estadística, su investigación, divulgación y su enseñanza. Va dirigido a todas aquellas personas que profesional o institucionalmente realicen labores relacionadas con tales disciplinas y que deseen exponer sus investigaciones y/o experiencias; así como a aquéllas que por los temas a tratar, se interesen por enriquecer sus conocimientos como asistentes. Los interesados en participar como ponentes, pueden hacerlo en exposición oral, o en forma cartel. De manera anticipada sean bienvenidos a nuestra **1ª Semana Internacional de la Probabilidad y la Estadística.**

COMITÉ ORGANIZADOR

M. C. JOSÉ DIONICIO ZACARIAS FLORES (RESPONSABLE), jzacarias@fcfm.buap.mx

DR. HUGO CRUZ SUÁREZ, hcs@fcfm.buap.mx

DR. BULMARO JUÁREZ HERNÁNDEZ, bjuarez@fcfm.buap.mx

DR. FRANCISCO SOLANO TAJONAR SANABRIA, ftajonar@fcfm.buap.mx

DRA. LIDIA HERNÁNDEZ REBOLLAR, lhernan@fcfm.buap.mx

DR. ALBERTO TAPIA AGUILAR, alberto@fcfm.buap.mx

INFORMES:

sne@fcfm.buap.mx
01-222-229-55-00 ext. 2138/7577/2164

Avisos

ICME 11

La décima primera edición del Congreso Internacional de Educación Matemática se realizara por primera vez en América Latina

Fechas: del 6 al 13 de Julio del 2008

La bella ciudad de Monterrey ha sigo elegida como la sede para tan importante reunión

La Sociedad Matemática Mexicana anuncia la

PRIMERA REUNIÓN CONJUNTA RSME - SMM

(Real Sociedad Matemática Española - Sociedad Matemática Mexicana)
a celebrarse en México del 6 al 9 de agosto de 2008 (Sede por anunciarse)
Comité Ejecutivo:

Olga Gil
Alejandro Díaz-Barriga
Isidoro Gitler
Lourdes Palacios
Carlos Signoret

Comité de Programa:

Por la SMM:
Hugo Arizmendi (IMATE-UNAM)
Lucero de Teresa (IMATE-UNAM)
Bertha Gamboa de Buen (CIMAT)
Clara Garza (IIMAS-UNAM)
Ernesto Pérez-Chavela (UAM-I)

Por la RSME:
Oscar Blasco (U. Valencia)
Antonio Campillo (U. Valladolid)
Marco Antonio López Cerdá (U. Alicante)
Enrique Zuazua (U. Autónoma de Madrid e IMDEA)

En fecha próxima se publicarán la Sede y la Convocatoria para Sesiones

CARTA INFORMATIVA

SOCIEDAD MATEMÁTICA MEXICANA

Número 55,
Enero de 2008

Publicación de la
Sociedad Matemática Mexicana, A.C.
Apartado Postal 70-450,
04510 México, D.F.
Tel. 5622-4481 / 82
Fax 5622-4479
smm@smm.org.mx

DISEÑO Y PRODUCCIÓN

S y G editores, SA de CV
Tels. 5619-5293 / 5617-5610
sygeditores@cablevision.net.mx

PORTADA

Fractal