Lecturas Matemáticas
Volumen **24** *(2003), páginas 169–175*

Noticias

PRIMOS $\in \mathcal{P}$

Método de Agrawal para verificar la primalidad de números naturales (agosto de 2002). El Profesor Manindra Agrawal y sus estudiantes, Neeraj Kayal y Nitin Saxena, han descubierto un algoritmo determinístico de tiempo polinomio (algoritmo que es,pues, eficiente en términos del tiempo que le toma para hacer los cálculos correspondientes) para verificar si un número natural dado es o no un número primo. Sabemos, desde Euclides, que existe un número infinito de números primos, pero sus distribución en la recta real es bastante caótica. El interés actual de saber si un número natural dado es no un número primo radica en sus aplicaciones cruciales no solo a la matemática sino también en ciencias de la computación. Por ejemplo, muchas aplicaciones a la moderna criptografía requiere rutinariamente la identificación de primos con cientos de dígitos.

Manindra Agrawal

Neeraj Kayal

NITIN SAXENA

Hasta ahora los algoritmos más utilizados para determinar la primalidad de un número eran aletaorios, pero aunque eficientes todavía subsistía la posibilidad de error, aunque fuese pequeña. De ahí el interés de un algoritmo completamente exacto. La solución de ARGRAWAL y su equipo es *corta, elegante y accesible aún para estudiantes de pregrado.*

El algoritmo fue dado a conocer el 4 de agosto de 2002, y colocado en forma de artículo en la red WWW el día 7 del mismo mes. En menos de 24 horas, 30.000 personas de todo el mundo lo habían bajado de la red. En declaraciones al New York Times, CARL POMMERANCE, una de las mayores autoridades mundiales en teoría de la computación, dijo que el algoritmo es un resultado *maravillosamente elegante.*

Los interesados en este algoritmo puede bajarlo desde el sitio:

www.cse.iitk.ac.in/news/primality.pdf [1]

[1]La información usada para elaborar la anterior nota se toma de diversas fuentes, principalmente de las páginas de *The New York Times* y la *American Mathematical Society.*

Recomendamos leer el artículo *PRIMES Is in P: A Breakthrough for "Everyman"*, de FOLKMAR BORNEMANN, publicado en el número de mayo de 2003 de las *Notices of the AMS*, 545–552, para saber más.

Integers, Electronical Journal of Combinatorial Number Theory

Editors-in Chief: MELVYN NATHANSON, JAROSLAV NESETRIL & CARL POMERANCE. Editor gerente: BRUCE LANDMAN

Integers is a refereed electronic journal devoted to research in the area of combinatorial number theory. It is published with the help of the State University of West Georgia, Charles University, and DIMATIA. Subscriptions to **Integers** are free. We welcome original research articles in combinatorics and number theory, with a preference for those that have a connection to both fields. Topics covered by the journal include additive number theory, multiplicative number theory, sequences and sets, extremal combinatorics, Ramsey theory, elementary number theory, classical combinatorial problems, hypergraphs, and probabilistic number theory. The principal subject areas, according to the American Mathematical Society subject classification scheme are 05A, 05C55, 05C65, 05D, 11A, 11B, 11K, 11N, 11P, 11Y, and 91A46. The site is

http://www.integers-ejcnt.org/

Premio A. M. Turing de la ACM

La *Association for Computing Machinery* (ACM) entregó este año el premio *A. M. Turing* a los matemáticos RONALD L. RIVEST, ADI SHAMIR & LEONARD M. ADLEMAN, correspondiente a la versión de 2002, por sus contribuciones a la *criptografía de clave pública*. El algoritmo *RSA* (por las iniciales de sus apellidos), desarrollado por los recipendiarios en 1977 mientras trabajaban en el MIT, se ha convertido en la fundamentación de toda una generación productos tecnológicos

relacionados con la seguridad en la trasmisión de mensajes: servidores y buscadores de Internet, transacciones electrónicas con tarjetas de crédito, telefonía móvil, etc.

Según el jurado del premio, el algoritmo *RSA es un avance significativo para permitir la comunicación segura entre computadores que usan la criptografía de clave pública.*

El algoritmo *RSA* fue publicado en un artículo en las *Communications of the ACM* en febrero de 1978.

El premio honra la memoria del matemático británico Alan M. Turing, quien articuló las bases y los límites matemáticos de la computación (la teoría de las llamadas *máquinas de Turing*), y cuya labor en la sección de decodificación en los servicos secretos británicos logró romper el código *Enigma* de los alemanes durante la II Guerra mundial.

Olimpiadas Matemáticas

La versión 44 de la *Olimpiada Matemática Internacional* (IMO) se celebró en Tokyo, del 7 al 20 de julio de 2003. Participaron 457 estudiantes de 82 países, más dos países invitados como observadores. Colombia envió 6 participantes, que obtuvieron tres medallas de bronce.

Olimpiadas Matemáticas Universitarias

Entre el 25 y 31 de julio, en Cluj-Napoca (Rumania), se celebraron las *Olimpiadas Matemáticas Universitarias.* Los participantes en este evento deben tener a lo sumo 22 años. Colombia envió 3 participantes. Todos ellos ganaran medallas, así:

- **Medalla de oro**: José González Zapata, Universidad Nacional de Colombia, sede de Medellín.
- **Medalla de plata**: Oscar Bernal, Universidad de los Andes, Bogotá.
- **Medalla de bronce**: Emerson León, Universidad Nacional de Colombia, sede de Bogotá.

Premio Abel, 2003

El primer *Premio Abel* ha sido otorgado a Jean-Pierre Serre, uno de los grandes matemáticos de nuestros días. Serre es Profesor Honorario del Colegio de Francia de París. Durante más de medio siglo, ha contribuido notablemente al progreso de las matemáticas, y lo sigue haciendo. Los trabajos de Serre son de una amplitud, profundidad e influencia extraordinarias. Serre ha desempeñado un papel central en la elaboración de la forma moderna de numerosas partes de las Matemáticas, en particular:

- La Topología, que trata de la cuestión siguiente: ¿Qué es lo que se mantiene constante en geometría aún cuando se deforme la longitud?
- La Geometría Algebraica, que trata de la cuestión siguiente: ¿Cómo resolver geométricamente los sistemas de ecuaciones polinómicas?
- La Teoría de los Números, el estudio de las propiedades básicas de los números. Por ejemplo los números primos y la resolución de las ecuaciones polinómicas en el Último Teorema de Fermat.

Serre desarrolló métodos algebraicos revolucionarios para el estudio de la Topología, ocupándose en particular de las transformaciones entre hiperesferas. A él se debe una espectacular aclaración de los trabajos de los geómetras algebristas italianos mediante la introducción y el desarrollo de los sistemas algebraicos adecuados para determinar cuándo funcionaban sus construcciones geométricas. Esta potente técnica de Serre, con su nuevo lenguaje y su punto de vista inédito, inauguró una nueva edad de oro de la Geometría Algebraica. Durante las últimas cuatro décadas, los magníficos trabajos de Serre y su visión de la Teoría de los Números han sido decisivos para dar a esta disciplina su éxito actual. Estos trabajos conectan y amplían en muchos aspectos las concepciones matemáticas introducidas por Abel, en particular su prueba de la imposibilidad de resolver las ecuaciones de quinto grado por radicales y sus técnicas de análisis para el estudio de las ecuaciones polinómicas con dos variables. Las investigaciones de Serre han sido centrales para abrir la vía a los descubrimientos recientes más destacados, inclusive la prueba por Wiles del Último Teorema de Fermat.

Si bien es cierto que SERRE ha centrado sus esfuerzos en las matemáticas más abstractas, sus aportaciones han encontrado importantes aplicaciones. Determinados problemas prácticos que plantean el desarrollo de eficaces códigos de corrección de errores y la criptografía de llave pública se resuelven mediante ecuaciones polinómicas (en particular en los campos finitos), y los trabajos de SERRE han profundizado realmente nuestra comprensión de este tema.

JEAN–PIERRE SERRE nació en 1926 en Bages, Francia. Cursó estudios en la Escuela Normal Superior y obtuvo el título de Doctor en Ciencias por la Universidad de la Sorbona de París en 1951. Después de haber ocupado varios puestos en el Centro Nacional de Investigaciones Científicas, fue Profesor Asociado en la Facultad de Ciencias de la Universidad de Nancy. En 1956, se le nombró Profesor del Colegio de Francia. SERRE es miembro de la Academia de las Ciencias de Francia. Es Gran Oficial de la Orden Nacional del Mérito y Comendador de la Legión de Honor. Ha sido nombrado miembro de varias Academias Nacionales, en particular las de Francia, Suecia, los Estados Unidos y los Países Bajos.

Entre las distinciones con que ha sido galardonado están la Medalla Fields en 1954 (sigue siendo el receptor más joven), el Premio Gaston Julia en 1970, el Premio Balzan en 1985, el Premio Steele en 1995 y el Premio Wolf en 2000. Ha sido nombrado Doctor Honoris Causa por numerosas universidades, en último lugar la Universidad de Oslo, en 2002, en ocasión de la conmemoración del bicentenario del nacimiento de NIELS HENRIK ABEL.

TOMADO DE LA PÁGINA DE LA ACADEMIA NORUEGA DE CIENCIAS Y LETRAS.

Medalla Fields

El francés LAURENT LAFFORGUE y el estadounidense VLADIMIR VOEVODSKY ganaron la *Medalla Fields* por su trabajo en algunas de las grandes ideas de las matemáticas. Las medallas les fueron entregadas por el presidente chino, JIANG ZEMIN, durante el *Congreso Internacional de matemáticos* que se realizó en Beijing, China.

Recordemos que la *Medalla Fields* recibe su nombre en memoria de John Fields, un matemático canadiense que estableció el premio en la década de los 30. Acuñada en oro, la medalla lleva la inscripción *Congregati ex toto orbe mathematici ob scriptia insignia tribuere*, que traducido al castellano nos diría: *Los matemáticos de todo el mundo aquí reunidos rinden tributo por un trabajo extraordinario.*

Laurent Lafforge, de 35 años, trabaja en lo que se ha dado en llamar el *Programa Langlands*, que busca una unidad subyacente entre varias disciplinas matemáticas. Lafforge es profesor del Instituto de Altos Estudios Científicos, ubicado en las cercanías de París.

Vladimir Voevodsky, de 36 años, se especializa en geometría algebraica abstracta. Voevodsky nació en Rusia y estudió en la Universidad Estatal de Moscú antes de trasladarse a Estados Unidos. En la actualidad es profesor del Instituto para Estudios Avanzados, en Princeton, Nueva Jersey.

Premio Nobel de economía

Nuevamente el Premio Nobel de Economía se otorga por trabajos realizados en áreas de la economía matemática. Esta vez, según anuncio de la Real Academia Sueca de Ciencias, el premio lo compartirán Robert F. Engle por el desarrollo de métodos para analizar series temporales económicas con volatibilitad variable con el tiempo (ARCH), y Clive W. J. Granger por el dearrollo de métodos para analizar series temporales económicas con tendencias comunes (co-integración)