Palabras del Dr. Alejandro Díaz-Barriga, Presidente de la SMM Ceremonia de Inauguración VII Reunión Conjunta AMS-SMM

Sociedad Matemática Méxicana
smm@smm.org.mx

Sra. Amalia García Medina, Gobernadora Constitucional del Estado de Zacatecas
Sr. Alfredo Femat Bañuelos, Rector de la Universidad Autónoma de Zacatecas
Sr. Flavio Campos Miramontes, Secretario de Educación del Estado de Zacatecas
Proffessor Robert Bryant, Vicepresident of the American Mathematical Society
Distinguidas personalidades del Presidium
Queridos colegas
Estimados amigos y amigas, dear friends

Es para la Sociedad Matemática Mexicana un orgullo, y a la vez un motivo de satisfacción, el estar hoy en esta hermosa y hospitalaria ciudad de Zacatecas, en este magnífico recinto del Teatro Calderón, reunidos para la inauguración de la VII Reunión Conjunta American Mathematical Society - Sociedad Matemática Mexicana.

Las Reuniones AMS-SMM se han ido consolidando como uno de los más importantes congresos de investigación para la comunidad matemática mexicana y estoy seguro que esta VII edición continuará con la tradición de alto nivel académico y excelencia matemática que han establecido las anteriores.

Se estrechan así los lazos, no sólo de amistad y compañerismo entre colegas con un interés común, si no de cooperación científica del más alto nivel y en el más noble espíritu internacional de solidaridad y colaboración entre nuestras Sociedades y comunidades.

La VII Reunión Conjunta es hoy una realidad, pero hemos llegado hasta esa realidad gracias al esfuerzo desinteresado, y en ocasiones sacrificado, de un gran número de colegas de ambos países que se han dado a la tarea de realizar las labores de organización de una reunión tan importante como ésta, tareas a veces grandes y pesadas, a veces pequeñas y minuciosas, pero igualmente necesarias.

Vaya un sincero agradecimiento al Comité Ejecutivo, al Comité de Programa, al Comité Organizador Local, a los Coordinadotes de Sesión, al Staff de la Sociedad y a todas las autoridades universitarias, municipales y estatales que han hecho posible llegar hasta este punto.

Agradezco muy especialmente a la Sra. Amalia García, Gobernadora de este maravilloso Estado, el interés que pone y ha puesto por todas las actividades científicas con una preclara visión para el futuro de México. Al Secretario de Educación y Cultura del Estado de Zacatecas Maestro Flavio Campos su constante apoyo; al Sr. Rector de la Universidad Autónoma de Zacatecas, Alfredo Femat. Esta reunión se lleva a cabo gracias a su decidido apoyo; a la Dra. Gema Mercado, Directora del Consejo Zacatecano de Ciencia y Tecnología, promotora incansable de esta reunión y precursora de la matemática en este Estado; a la maestra Lorena Jiménez, Directora de la Unidad Académica de Matemáticas, todo el interés y arduo trabajo en los mil detalles de la organización de esta reunión y al Maestro José Augusto Beltrán, Director de la Unidad Académica de Física por su hospitalidad en prestarnos las instalaciones para la realización de esta reunión.

Dear colleagues from Mexico, the United States and all around the World:

It is for the Sociedad Matemática Mexicana an honour and also a pleasure to have you here in this beautiful city of Zacatecas for the VII-th (seventh) Joint Meeting of the American Mathematical Society - Sociedad Matemática Mexicana.

Our Joint Meetings have become of the outmost importance for the Mexican mathematical community and I am sure that this VII-th edition will continue the tradition of high academic level and mathematical excellence established by the previous meetings.

This way we strengthen the links, not only of colleagues having a common interest, but also of scientific cooperation of the highest level between our Societies and communities. This VII-th Joint Meeting is becoming a reality; but we must remember that we are here thanks to a lot of colleagues from both countries that have provided their effort and sacrifice to make this meeting possible.

My acknowledgment to the Executive Committee, to the Program Committee, to the Local Organizing Committee, to the Session Organizers, to the administrative Staff and to all the authorities from the University, from the City and from the State, all of whom made this Meeting come true.

Quiero desear a todos los colegas de ambas naciones
I want to wish all the participants from both countries
Que disfruten esta Reunión Conjunta
To enjoy this Joint Meeting.

Y que tengan la más feliz estancia entre nuestra comunidad matemática y en nuestro país.
And to have a good time within our mathematical community and in our country.

Gracias.
Thank you.

Mensaje de la Secretaria de Educación Publica, Josefina Vázquez Mota

Sociedad Matemática Mexicana
smm@smm.org.mx

Muy buenos días y muy bienvenidos a la Secretaría de Educación Pública. Doctor Alejandro Javier Díaz Barriga Casales, Presidente de la Sociedad Matemática Mexicana, quiero públicamente reconocer y agradecer a usted y a la Sociedad el esfuerzo y el espíritu de colaboración con la Secretaría de Educación Pública, pero particularmente las iniciativas que hemos venido dialogando y que sin duda resultan indispensables hacia el futuro en la agenda educativa del país.

Muy queridos jóvenes medallistas, Pablo Soberón Bravo que nos ha dado la satisfacción de la primera medalla de oro en esta Olimpiada y que como hemos podido observar tiene un larga trayectoria, lo cual demuestra al igual que todos los medallistas, que esto no surge de manera espontánea, sino requieren de un esfuerzo, de una disciplina y de un trabajo cotidiano.

A Iván Joshua Hernández Maines, Manuel Ángel Guevara López, Saúl Iván Gallegos Bernal, Andrés Leonardo Gómez Emilsson, José Daniel Ríos Ferrusca, Alejandro Jiménez Martínez, Luis Ángel Isaías Castellanos, Manuel Guillermo López Buenfil.

Queridos jóvenes medallistas y miembros de la delegación mexicana que participarán en esta cuadragésima octava Reunión Internacional de Matemáticas en Vietnam: Fernando Campos García, Isaac Buenrostro Morales, Aldo Pacchiano Camacho, Cristian Manuel Oliva, Marco Antonio Ávila Ponce de León y Jesús Novelo Puc.

Distinguidos miembros de la directiva de la Sociedad Matemática Mexicana; estimadas maestras y maestros que nos acompañan, padres de familia, amigas y amigos.

Y de manera especial también, quisiera saludar esta mañana a don Guillermo Soberón, que fue Rector de la UNAM, Secretario de Salud, pero hoy su presencia obedece a un orgullo familiar y a esta medalla de oro que se ha logrado para nuestro país, enhorabuena también por estar aquí hoy en su calidad de abuelo, muy orgulloso seguramente de su nieto doctor Soberón, es un honor que nos acompañe, y a Lorenzo Samuel Gitler, miembro también del Colegio Nacional.

Una educación de calidad y con equidad son sin duda los grandes retos que ha planteado en Presidente Felipe Calderón para la agenda educativa del país. Por eso es de gran satisfacción esta reunión, con un destacado grupo de jóvenes que tantos logros le ha dado a nuestro país en las matemáticas y con estos integrantes incansables, luchadores incansables de la Sociedad Matemática Mexicana.

Quiero reconocer la labor de sus maestras, de sus maestros, pero también de sus padres de familia, sin los cuales me parece sería prácticamente imposible explicar estas medallas y estos reconocimientos.

Me parece que lo más alentador que tenemos esta mañana, como lo ha establecido quien hoy preside la Sociedad de Matemáticas, es observar como México ha venido avanzando y hoy ocupa un lugar destacado en el primer tercio de los países que asisten a la Olimpiada.

No fue así el inicio, lo cual nos demuestra que hay una esperanza real y posible de que no solamente los jóvenes que van a la Olimpiada avancen en el conocimiento de las matemáticas, sino que lo hagan miles de estudiantes en todo el país.

Si los jóvenes aquí presentes, no solamente son medallistas, sino son competidores de clase mundial, el reto que hoy tenemos es abrir este espacio de posibilidad a miles de jóvenes, que como señalaba el Presidente de la Sociedad, les gusta las matemáticas los primeros años de vida escolar para después de alejarse de ellas, probablemente para siempre.

Sé que la Olimpiada de Matemáticas ha sido un esfuerzo sin precedentes, sé que reconoce no solamente el reto de una nueva forma de pensar. Queremos las matemáticas no solamente para resolver los problemas de álgebra o de trigonometría, o de geometría que ya son muy importantes.

En México queremos las matemáticas también para fortalecer el ejercicio de la razón, para ser capaces de pensar en soluciones mejores y más justas no solamente en el mundo de las matemáticas, de la ingeniería o de la ciencia que resultan indispensables, necesitamos respuestas mucho más amplias y audaces en las agendas sociales, en las agendas de justicia, en la propia agenda educativa y de libertad para el país.

Nos urgen las matemáticas porque sin la mejora en la aplicación de la calidad de las matemáticas, tampoco podremos elevar los estándares de la agenda educativa nacional y no podremos la plataforma de talentos para desarrollar las carreras del presente, pero sobre todo las carreras del futuro.

Necesitamos las matemáticas también, para ir encontrando estos talentos. Hoy tenemos a este grupo de jóvenes, del cual nos sentimos muy orgullosos, pero tal vez la pregunta es cuántos pudiendo estar aquí no han podido ser reconocidos a edad temprana y tampoco han podido ser acompañados a lo largo de su vida.

Creo que entonces el reto y lo hemos venido conversando desde esta mañana, es no solamente fortalecer la Olimpiada, que convoca a jóvenes desde secundaria y bachillerato, es fortalecer el aprendizaje de las matemáticas en todo el ámbito de la agenda educativa.

Yo quiero esta mañana públicamente, pedirle a la Sociedad de Matemáticas que nos acompañe a por vez primera empezar a establecer las bases para que la Olimpiada de Matemáticas en México, no inicie en la secundaria, nos urge que la Olimpiada de Matemáticas inicie desde el primer año de primaria.

Tenemos que llevar la Olimpiada a la educación básica, tenemos que llevar la enseñanza de las matemáticas a nivel preescolar, que es cuando los niños y las niñas de México tienen más preguntas que respuestas. Muchas veces conforme avanzamos en la agenda educativa las preguntas se acaban por completo y solamente quisiéramos estar en el terreno de las respuestas, con una gran pobreza en el uso de la inteligencia y en la sociedad del conocimiento.

Así que le pido públicamente a la Sociedad que demos este paso, que sé que ha sido una inquietud de ustedes por años y que muy pronto podamos darle esta noticia a México y este desafío, de que la Olimpiada de Matemáticas va desde primero de primaria.

Y creo que tenemos que empeñarnos también, porque seguramente lo hay, en encontrar más talentos. Extraño en este grupo que me parece tan valioso y tan rico, una presencia femenina que seguramente no hemos fortalecido lo suficiente o no las hemos acompañado lo suficiente.

El próximo seis de julio ustedes partirán hacia Vietnam para participar en esta edición 2007 y no tengo la menor duda de que sabrán representar a México con una gran dignidad. Les deseo mucha suerte en esta Olimpiada y que regresen triunfadores y que regresen con medallas y que regresen mucho más orgullosos de lo que ya están en este momento.

Esta cooperación, también se ha dado desde el inicio de la gestión del Presidente Calderón con la Sociedad Matemática Mexicana. Quisiera informar que nos ayudaron de manera invaluable para la realización de la Prueba ENLACE, que se aplicó en meses pasados en nuestro país a más de once millones de estudiantes y algo muy importante, el día de hoy la Sociedad Matemática Mexicana hará entrega a la Secretaría de Educación Pública de esas llamadas "ligas" o enlaces vía Internet, que le permitirán a cada joven cuando reciba los resultados de su Prueba ENLACE, esos once millones y medio de estudiantes en México, ir directamente a reconocer cuáles fueron las respuestas que acertaron o cuales fueron aquellas donde no acertaron y se equivocaron, y a través de estos enlaces, estas "ligas", podrán ir directamente a encontrar como resolver favorablemente este problema, en el que probablemente fallaron en la aplicación de la Prueba ENLACE.

Quiere decir entonces que ENLACE es una evaluación que empieza a tener respuestas para el mejor aprovechamiento y conocimiento de las matemáticas. Es un trabajo que nunca antes se había tenido y que yo aprecio y valoro enormemente a la Sociedad Matemática Mexicana.

Se que han concluido con primaria, que están por concluir con secundaria, yo creo que nos tendremos que dar prisa Doctor, porque vamos aplicar ENALCE al bachillerato por vez primera y entonces tendremos que tener los materiales listos también para bachillerato.

La Olimpiada Mexicana de Matemáticas está unida a otros esfuerzos, la Olimpiada del Conocimiento, la Olimpiada Nacional de Ciencia, Química y Biología, la Olimpiada de Física, Informática, de Historia y también de Geografía.

Aquí les permite identificar talentos, pero tal como lo ha compartido la Sociedad Matemática Mexicana no basta encontrar los talentos, el gran reto es como los acompañamos, como les damos seguimiento, como les podemos becar, como los podemos fortalecer, como les podemos permitir acceso a estándares superiores a nivel internacional.

En este sentido, quisiera decir que actualmente participa un millón de niños y jóvenes en este tipo de olimpiadas. Pero esto es todavía insuficiente, hemos venido conversando sobre la urgencia de ampliar los diplomados y la formación para las maestras y los maestros de México, de al manera, que como decía hace unos minutos en mi oficina el Presidente de la Sociedad Matemática Mexicana, lo mejor debe suceder en el aula y es en el aula donde la enseñanza de las matemáticas debe llevar a esta sociedad del conocimiento, pero también a esta ampliación de posibilidades para millones de estudiantes en México.

Sé que en algunas entidades del país, como es el caso de Sonora, Querétaro y recientemente el Estado de México, se han fortalecido estos diplomados para las maestras y los maestros, y yo quisiera hacer un compromiso para que no sea solamente en estas tres entidades, sino estos diplomados sucedan a lo largo y ancho de todo el país.

La Sociedad Matemática me ha planteado la urgencia de ampliar este esfuerzo a la educación media superior, por lo cual estamos trabajando desde el día de hoy, para que se revise la curricula del bachillerato en la enseñanza de matemáticas y también la mejor formación de maestras y maestros.

Le instruido a mis colaboradores a que las normales se incluyan también en este proceso de fortalecer las currículas y la enseñanza de las matemáticas, desde la propia formación del magisterio en el país. Es muy importante el aprendizaje permanente, pero no podemos desestimar los aprendizajes primeros para llegar al salón de clases.

A partir del año que entra vamos a constituir un Fondo especial de común acuerdo con la Academia Mexicana de las Ciencias, es la primea vez que la SEP hará un esfuerzo financiero y quisiera informar cuál es el propósito de este Fondo especial con la Académica Mexicana de las Ciencias: primero la detección de talentos, con convocatorias más amplias de las olimpiadas que ya tenemos y estableciendo nuevas competencias en otras áreas de conocimiento.

En segundo lugar, la asesoría a los padres de familia, a los maestros y a las escuelas para la canalización y atención apropiada para potenciar esas capacidades. Tercero, la elaboración de materiales didácticos que estimulen el desarrollo de estas actitudes.

En cuarto lugar, la identificación de áreas en donde se debe reforzar esa enseñanza. Quinto, el acompañamiento tutorial de los jóvenes, desde el Programa Pauta, este programa lo ha venido incentivando la Academia Mexicana de Ciencias, que es este acompañamiento para jóvenes destacados y que queremos fortalecer desde la Secretaría de Educación Pública.

El día de hoy por la tarde recibiré también las recomendaciones del Consejo de Especialistas para la Educación, que tendrán que verse reflejadas en el Programa Sectorial y en nuestro Plan Nacional de Educación.

Hemos venido escuchando a todos los miembros de la comunidad educativa, esta tarde el Consejo de Especialistas, las sociedades de Ciencias, las academias de Ciencias, los maestros, los padres de familia, la sociedad civil, el Sindicato y todos aquellos que tienen algo que aportar o proponer a la agenda educativa del país.

Aquellas iniciativas que fortalezcan la calidad y la equidad de esta agenda, no solamente serán retomadas sino serán fortalecidas desde la autoridad en materia educativa.

Tenemos muy claro el camino de la agenda educativa y estas iniciativas serán reconocidas desde el ámbito en que se propongan.

Seguiremos en el empeño de la evaluación, creo que no podríamos explicar estas medallas y esta mejora en calidad, si no hubiera habido una evaluación de por medio, que es la Olimpiada propiamente de las matemáticas.

Por eso creemos en la evaluación que nos compara entre nosotros, pero creemos profundamente en la evaluación que no se limita a compararnos entre nosotros, sino que nos permite compararnos con los otros. Y esta es la apuesta de evaluación que tenemos en el país, sobre la cual no tenemos duda alguna y nos empeñaremos a todo lo largo y ancho de esta agenda educativa.

Nuevamente muchas felicidades jóvenes, mucha suerte, estamos muy orgullosos de que entregan su inteligencia, su concomiendo y que sean unos apasionados del mundo de las matemáticas y ojalá también con su testimonio nos ayuden a decirles a miles y millones de jóvenes en México que sí son divertidas las matemáticas, que son muy entretenidas, que son parte de su vida y que vale la pena no solamente encontrase casualmente con ellas en el camino, sino hacerlas cómplices permanentes a lo largo de toda su vida.

Sociedad Matemática Mexicana, Presidente, muchas gracias doctor por este empeño y colaboración; papás, felicidades, deben estar muy orgullosos, abuelitos también, por supuesto que aquí nos acompañan, maestras y maestros, y seguiremos adelante en este empeño. Mucha suerte, enhorabuena y muchas gracias a todos.

Palabras del Dr. Alejandro Díaz-Barriga, en la ceremonia de entrega de reconocimientos a medallistas olímpicos

Sociedad Matemática Mexicana
smm@smm.org.mx

Lic. Josefina Vázquez Mota, Secretaria de Educación Pública
Distinguidos Jóvenes Olímpicos, Señores Subsecretarios y Directores, Amigos todos

La Sociedad Matemática Mexicana ha cumplido la tarea de organizar año con año el trabajo asignado por la Secretaría de Educación Pública, consistente en organizar las Olimpiadas de Matemáticas. Iniciamos nuestra participación en 1988 en la Olimpiada Internacional de Matemáticas en Australia. Para darnos una idea del camino recorrido basta decir que en 1994, en Hong kong, obtuvimos el lugar sexagésimo quinto de 69 países. Los avances logrados en los últimos cuatro años son importantes. Para observar esto mencionamos lo siguiente:

México fue sede el año antepasado de este certamen internacional realizándose esta Olimpiada en Mérida; Yucatán. En esta ocasión de 91 países obtuvimos el lugar trigésimo primero. El año pasado asistimos a la cuadragésima séptima olimpiada internacional que se llevó a cabo en Eslovenia, obtuvimos el lugar vigésimo cuarto de noventa países. Para dimensionar lo que hemos logrado hay que decir que en toda su historia México tenía 3 medallas de plata. Sólo el año pasado ha ganado por primera vez una medalla de oro además de traer otras dos medallas de plata. Resaltamos también que por primera vez obtuvimos el primer lugar en la olimpiada iberoamericana y por sexta vez consecutiva el primer lugar en la centroamericana.

Señora secretaria, por todos estos datos podemos decir que la Sociedad Matemática Mexicana esta cumpliendo adecuadamente con esta tarea. La matemática es una y la ciencia matemática mantiene una gran vigencia, pues influye en casi todas las áreas del conocimiento, ya que ayuda a entender, aproximar y analizar cualquier fenómeno complejo, por ejemplo la modelación del clima, el estudio del ADN y los análisis moleculares de aplicación médica.

La matemática esta presente en la formación de todo individuo, no sólo por su aplicabilidad a otras áreas del conocimiento, sino también porque nos enseña formas de pensamiento. El papel que la matemática juega en la formación del ser humano, del mexicano, no debe solamente circunscribirse al manejo de números y medidas, sino debe impactar fuertemente las formas de pensamiento de éste. La matemática debe abonar a la capacidad de diseñar estrategias para resolver problemas, no sólo de esta ciencia, sino de la vida cotidiana y de otras ciencias. Además, debe colaborar en la capacidad de conjeturar soluciones y argumentar a favor de ellas. Es por esto que la matemática forma parte del currículo desde la primaria.

Esta tarea de enseñar matemática a todos los mexicanos, a nuestros niños y jóvenes, no la estamos haciendo correctamente. En pequeñas encuestas que se han realizado en la Sociedad Matemática Mexicana nos damos cuenta que a casi todos los niños de 1^o y 2^o de primaria les encanta la matemática, mientras que ya a la mayoría de niños de 5^o y 6^o de primaria y 1^o de Secundaria no les gusta la matemática, más bien la detestan. Tal parece que en la escuela los vamos vacunando contra esta hermosa y útil ciencia.

Son dos las tareas que debemos realizar en los niveles básico y medio superior, la de dar una sólida formación a todo mexicano que le permita tener una mejor y más humana calidad de vida y la de detectar talentos que posteriormente estudien una carrera de ingeniería o una carrera científica. Ingenieros y científicos de alto rendimiento son necesarios en este país para que realicen la investigación que nos dará un adecuado registro de patente. Ésta es la única vía que tiene un país para acceder a un mejor nivel de vida de sus habitantes y países emergentes como China, Singapur, etc. han tomado este camino.

Por esta última razón debemos también buscar que la enseñanza superior sea de calidad. Los estudiantes deben poder acceder a toda la información necesaria para que su formación sea completa y debemos tener profesores altamente capacitados en su especialidad.

La Sociedad Matemática Mexicana en los últimos años ha realizado acciones en estas direcciones, proyectos como Mi ayudante con la Universidad Pedagógica Nacional, como PUEMAC con el Instituto de Matemáticas de la UNAM, Diplomados dirigidos a profesores de primaria con el apoyo de CIMAT, de la Universidad de Sonora, de la Universidad Autónoma de Querétaro y recientemente con Instituciones Educativas del Estado de México. En estos diplomados buscamos aprovechar la experiencia de los docentes en Primaria para lograr en ellos una nueva visión de la matemática y de su enseñanza.

Las autoridades de la Secretaría de Educación Pública han manifestado una gran sensibilidad para buscar resolver el problema de la enseñanza de la matemática en todos los niveles educativos del país, es por esto que realizaremos conjuntamente la Secretaría de Educación Pública y la Sociedad Matemática Mexicana acciones encaminadas a mejorar esta enseñanza. Una acción relevante dentro de éstas, es la realización el próximo año en nuestro país del Congreso Internacional de Educación Matemática número 11. Tendremos la oportunidad los educadores mexicanos y los latinoamericanos de enterarnos de los últimos resultados que de investigación en educación matemática que se han realizado en el mundo.

Estamos seguros que este conjunto de acciones redundará en una mejor enseñanza de la matemática en niños y jóvenes de este país, más lúdica, más interesante y más profunda y como consecuencia de ello tengamos en un futuro un México mejor.
Muchas gracias.


IX Jornadas "Juan José Rivaud Morayta"
de Historia y Filosofía de las Matemáticas
13, 14 y 15 de Septiembre de 2007
CIMAT.A.C. Guanajuato, Gto.
El Centro de Investigación en Matemáticas, A.C., y la Sección de Metodología y Teoría de la Ciencia del CINVESTAV convocan a las IX Jornadas "Juan José Rivaud Morayta" de Historia y Filosofía de las Matemáticas, que tendrán lugar en las instalaciones del CIMAT en la Ciudad de Guanajuato los días 13, 14 y 15 de septiembre del presente año. En esta ocasión, la temática principal de las IX Jornadas tomarán como eje el concepto de: Dimensión.
"Espacio y tiempo no son objetos, sino formas de entender lo que ocurre". Con esta expresión, Leibniz convierte un problema ontológico en uno de orden epistemológico. Pero lo que es más importante aún, aclara el sentido de la multiplicación de espacios en matemáticas. Prácticamente toda área de las matemáticas ha ampliado sus perspectivas, aclarado conceptos, multiplicado sus opciones, gracias a la noción muy amplia de espacio. Los entes matemáticos "viven" en espacios que les dan sentido: espacios de funciones (continuas, diferenciables, medibles, etc.), espacios de operadores (hermitianos, unitarios, acotados, etc.) , espacios de probabilidad, de medida, de formas, de variedades, etc. A pesar de que cada uno puede tener características propias dependiendo de los objetos que alberga, la idea común de espacio permite reinterpretar mapeos entre espacios de distinto carácter, como sucede en topología algebraica y, más generalmente, en los functores de la teoría de categorías. La idea común de espacio va más allá de el empleo de una misma palabra. Al menos existe un invariante, algo que comparten entre sí las muy distintas estructuras asociadas a los diferentes espacios: la dimensión.
Esta es solamente una razón para que el tema de nuestras jornadas sea el concepto de dimensión. Ese número (aunque sea fractal) que significa más que un número y que define, limita y posibilita lo que puede hacerse o no en un cierto espacio, o que permite o no hacer entre espacios; ese término que ha evocado tantas fantasías entre los amantes de esa ficción que no es ciencia que se llama ciencia-ficción; esa magnitud que no es el tamaño de una cosa, pero que lo evoca. ¿De qué forma, de cuántas formas podemos entender lo que significa dimensión?
Como siempre, en respeto a nuestra tradición y al espíritu con que fueron creadas las Jornadas por Juan José Rivaud Morayta (Juanjo), otros temas de interés son bienvenidos. Se insiste, sin embargo, en que las presentación tenga como objeto plantear temas de interés conceptual sobre la matemática, y que sean expuestos tomando en cuenta a un público con formación matemática general, dada la diversidad formativa de los asistentes y nuestro deseo en ser comprendidos por nuestros estudiantes. La fecha límite para recibir resúmenes de los trabajos y ponencias es el 20 de agosto. El 31 de agosto el Comité Organizador comunicará al interesado si su propuesta fue aceptada.
INFORMACIÓN GENERAL
Recepción de ponencias y/o resúmenes:
Dr. Gerardo Hernández
ghernand@cinvestav.mx
CINVESTAV Sección de Metodología y Teoría de la Ciencia,
Av. Instituto Politécnico Nacional # 2508,
Col. San Pedro Zacatenco, 07360 México, D. F.
Teléfono: (55) 5061-3800 Exts.: 6781 y 6774
Fax: Extensión 6782
Profr. Francisco Mirabal García
mirabal@cimat.mx
Centro de Investigación en Matemáticas, A.C.
CIMAT-Guanajuato
Jalisco s/n, Mineral de Valenciana
Guanajuato, Gto., México, C.P.36240
Tel.: (473) 732-7155 Ext. 49576
Fax: (473) 732-5749
Se cuenta con un número limitado de becas para estudiantes. También tenemos a disposición un número reducido de habitaciones en el CIMATEL.
Becas: Dirigir solicitud a Profr. Francisco Mirabal García
mirabal@cimat.mx
Mayores informes sobre reservación de hospedaje: CIMAT José Castro López
Departamento de Eventos Tel. (473) 732-7155, Ext. 49517
eventos@cimat.mx
http://www.cimat.mx/Eventos/IX_jorna_hist_filos_07/
http://smtc.cinvestav.mx/
CINVESTAV
CIMAT


BENEMERITA
La Universidad Autónoma de Puebla
A través de la Academia de Matemáticas de la
Facultad de Ciencias Físico Matemáticas
CONVOCAN
3a
Gran Semana
Nacional de la
Matemática
3GSNM
Del 17 al 21 de septiembre de 2007
Teniendo como temáticas principales:
Enseñanza y Divulgación de las Matemáticas
Se ofrecerán:
– Conferencias Plenarias
– Conferencias de Investigación y Divulgación
– Minicursos
– Actividades Culturales
– Sesiones Especiales
– Reportes de Investigación y de Tesis
– Difusión de programas de
– Matemáticas en los diferentes niveles
– Difusión de libros
Inscripciones
* Público en general: $ 300.00
* Estudiantes presentando
credencial: $ 50.00
* Miembros de la FCFM-BUAP
(profesores y alumnos): Gratuito
En las instalaciones de la Facultad de Ciencias Físico Matemáticas, BUAP
Informes en:
Facultad de Ciencias Físico Matemáticas, BUAP
Universidad Autónoma de Puebla
Ciudad Universitaria, edificio 190 de la FCFM
Avenida San Claudio y Río Verde, CU, CP 72570
Puebla, Pue., México
Tel.(01 222) 2 29 55 00 ext. 7565
www.fcfm.buap.mx/semana-matematicas

La Hipótesis de Riemann y Primalidad

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

Resumen

En este reporte describimos los principios básicos de algunos algoritmos de primalidad, partiendo de una breve explicación de la hipótesis de Riemann, uno de los siete problemas del milenio [4], para cada uno de los cuales el *Clay Mathematical Institute* ha ofrecido un premio de un millón de dólares de los EUA. Puntualizamos la relación de la hipótesis de Riemman con algunas pruebas de primalidad.

1. La hipótesis de Riemann

El concepto de número primo ha existido acaso desde tiempos remotos, en los mismos albores de la humanidad. En un hueso encontrado en el Africa Central que data alrededor de 20 milenios antes de Cristo, se encontraron señas que pudieran ser los números 11, 13, 17, y 19 y hay, en consecuencia, quienes interpretan esto como indicios de que en el Paleolítico se tenía ya la idea de números primos. Lo que es una certeza, es que en la antigua Grecia, en la escuela de Pitágoras (S. V AC), se tenía bien entendido qué era un número primo y un número compuesto. Tiempo después, en las obras de Euclides se incluye la demostración de la existencia de una cantidad infinita de números primos. Enseguida Eratóstenes describe su criba, con la que se podía encontrar los números primos iniciales.

Desde entonces, las teorías alrededor de los números primos han sido cimientos fundamentales en la actual teoría de números.

Un buen inicio de la relación de los números primos con la hipótesis de Riemann es la "uniformidad de los primos". A la larga aparentemente los números primos "grandes" pueden irse separando cada vez más (dado un entero $n \geq 3$, entre $(n+1)!+2$ y $(n+1)!+(n+1)$ hay n números enteros contiguos que no son primos) pero también puede darse el caso de que haya algunos primos grandes cercanos entre sí (como lo pueden ser dos primos gemelos), sin embargo siempre se encuentran con cierto comportamiento "uniforme": Fijo un entero n al cabo de un cierto número, fijo que depende de n, de elecciones de enteros menores que n se obtendrá un primo con una alta probabilidad. Esto es algo así como pintar los primeros primos en una liga, estirar la liga, pintar en ella a los primos en un intervalo más grande y observar que la traza en la liga casi no cambia. Veamos de manera un poco más formal la formulación de esta idea.

x	$\pi(x)/\frac{x}{\ln x}$
10^5	1.104
10^7	1.071
10^9	1.054
10^{11}	1.043
10^{13}	1.036
10^{16}	1.028
10^{21}	1.021
10^{24}	1.019

Cuadro 1: Aproximaciones de $\pi(x)$ mediante $\frac{x}{\ln x}$

Definición 1 (Función de Euler)**.** *Se define la función* $\pi : \mathbb{R} \to \mathbb{N}$, $x \mapsto \pi(x) = \sum_{p \leq x} 1$, *donde el índice* p *varía sólo en los números primos.*

Es decir, la función π cuenta los números primos menores o iguales a x, por ejemplo, $\pi(20) = 8$, $\pi(100) = 25$. En 1792 Gauss estableció mediante evidencias numéricas la relación

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$$

conocida como el *Teorema de los Números Primos* (TNP). Algunos cálculos que ejemplifican el comportamiento de la razón $\frac{\pi(x)}{x/\ln x}$ los podemos ver en la Tabla 1

Independientemente, Legendre presentó en su libro *"Théorie des nombres"* (*"Teoría de los números"*) (1798) que la función π puede aproximarse mediante una de la forma $x \mapsto x/(A \log x + B)$, y dió como valores $A = 1$, $B = -1{,}08366$. Alrededor de 1852 Chebyshev demostró que $0{,}92129\frac{x}{\ln x} < \pi(x) < 1{,}1056\frac{x}{\ln x}$, y más rigurosamente, puesto en notación moderna, que $\pi(x) = \Omega(x/\ln x)$ y $\pi(x) = O(x/\ln x)$, es decir, que el cociente $(\pi(x)\ln x)/x$, se mantiene acotado a la larga tanto inferior como superiormente. En 1892 Sylvester realizó un refinamiento a esta aproximación: $0{,}95695\frac{x}{\ln x} < \pi(x) < 1{,}04423\frac{x}{\ln x}$. Alrededor de 1896 J.

Hadamard y C.-J. De la Vallée-Poussin proporcionaron independientemente sendas demostraciones del TNP.

Por otro lado, se ha considerado a Euler como quien introdujo la famosa función

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

que es convergente para cualquier real $s > 1$, y él mismo demostró la relación

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

llamada *producto de Euler*, la cual apareció en su libro "*Introductio in Analysin Infinitorum*" en 1748. De hecho ya eran conocidos casos particulares de esta función en términos de series. Por ejemplo, para $s = 1$ resulta la serie armónica $\sum_{n=1}^{\infty} \frac{1}{n}$, que ya desde 1350 N. dÓresme había demostrado ser divergente. En 1735, Euler muestra que para el caso $s = 2$, $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$, con $s = 4$ $\zeta(4) = \frac{\pi^4}{90}$, y, de hecho, se ocupó de casos con valores pares llegando a calcular hasta $\zeta(26)$. Actualmente se sabe que para valores enteros pares vale la relación,

$$\zeta(2k) = \frac{2^{2k-1}\pi^{2k}}{(2k)!}(-1)^{k+1}B_{2k},$$

donde cada B_{2k} es un *número de Bernoulli*. Desafortunadamente Euler no obtuvo resultados relevantes acerca de los casos impares, y más de dos siglos más tarde, apenas en 1978, R. Apréry demostró que $\zeta(3)$ es un número irracional.

Una consecuencia importante que proporciona la función ζ es una demostración alternativa de la existencia de una infinidad de números primos. En efecto, esto es una consecuencia de que $\zeta(s) \to \infty$, cuando $s \to 1$.

Por otro lado, en 1859 Georg Friedrich Bernhard Riemann edita un manuscrito titulado "*Über die Anzahl der Primzahlen unter einer gegerbenen Grösse*", ("*Sobre el número de primos menores que una magnitud dada*"), que es visto hoy como uno de los más célebres escritos de las matemáticas clásicas. En él, Riemann estudia la relación de los números primos con funciones de variable compleja. Riemann tiene la idea de extender la función ζ a todo el plano complejo (privado del punto $z = 1$) e intentó probar el TNP mediante esa extensión, y aunque no lo demostró, el esfuerzo sí le rindió muy buenas ideas. Riemann formuló varias conjeturas sobre la extensión de ζ (llamada desde entonces *la función zeta de Riemann*). Sin embargo el punto más alto de la discusión está en la distribución de los ceros de la función de Riemann, lo cual está íntimamente relacionado con la distribución de los números primos. Se tiene los siguientes hechos acerca de la función de Riemann:

1. ζ no tiene ceros en el semiplano $\text{Re}(z) > 1$.
2. ζ no tiene ceros en la línea $\text{Re}(z) = 1$. Este hecho implica el TNP.

Más aún, puede verse que los ceros de ζ pueden ser clasificados como sigue:

1. Los ceros que están fuera de la franja $0 < \text{Re}(z) < 1$ son números reales y son de hecho los enteros negativos pares, $-2, -4, -6, -8, \ldots$ Estos son llamados *ceros triviales* de ζ, o *ceros reales*, ya que ningún otro cero es real. Que éstos sean ceros resulta, por un lado, al expresar la función de Riemann en términos de los números de Bernoulli $\left[\zeta(-n) = -\frac{B_{n+1}}{n+1}\right]$, y también de la forma equivalente demostrada por Euler,

$$\zeta(z) = \frac{1}{1 - 2^{1-z}} \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (k+1)^{-z}.$$

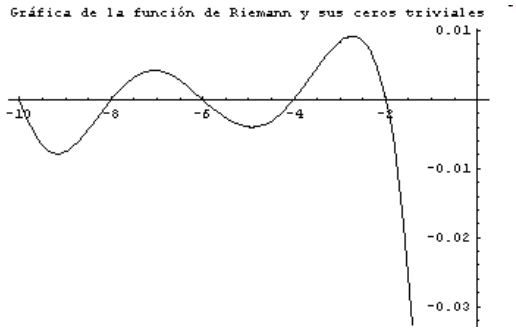


Figura 1: Raíces, o ceros, reales.

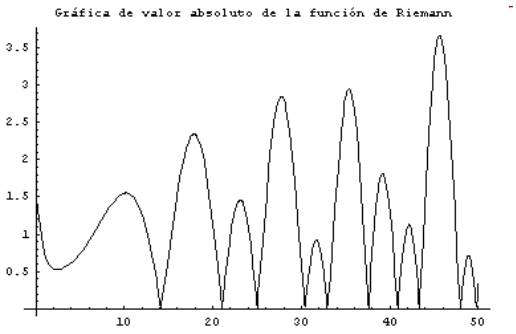


Figura 2: Ceros de la función real $y \mapsto 1/2 + yi$.

En la gráfica 1 se aprecia que, en efecto, los ceros triviales de ζ aparecen en el eje real negativo.

2. Los ceros que están en la franja $0 < \text{Re}(z) < 1$ son llamados *ceros no-triviales* de ζ y hay una cantidad infinita de ellos. Los ceros no-triviales no son reales, por lo que son llamados también *ceros complejos*.

   Los ceros de este tipo que han podido ser calculados están sobre la *línea crítica* $\text{Re}(z) = 1/2$, por lo que tienen la forma $1/2 + yi$ con $y \neq 0$. En la Tabla 2 las ordenadas de los primeros ceros complejos conocidos quedan enlistadas, y en la gráfica 2 se les puede observar, al graficar la función real $y \mapsto |\zeta(1/2 + iy)|$.

Riemann formuló entonces su conjetura acerca de los ceros no triviales:

Conjetura 1 (Hipótesis de Riemann (HR))**.** *Todos los ceros no triviales de ζ que están dentro de la franja $0 < Re(z) < 1$ están en la línea crítica $Re(z) = 1/2$.*

$y:\ \zeta(1/2 + yi) = 0$	
14.134725142	40.918719012
21.022039639	43.327073281
25.010857580	48.005150881
30.424876126	49.773832478
32.935061588	52.970321478
37.586178159	56.446247697

Cuadro 2: Las ordenadas de los primeros ceros no-triviales de ζ

año	n
1903	15
1914	79
1925	138
1935	1,041
1958	35,337
1966	250,000
1968	3,500,000
1977	40,000,000
1979	81,000,001
1983	300,000,001
1986	1,500,000,001
2001	10,000,000,000
2004	900,000,000,000
2004	10,000,000,000,000

Cuadro 3: Número de ceros no-triviales de ζ conocidos en las fechas indicadas.

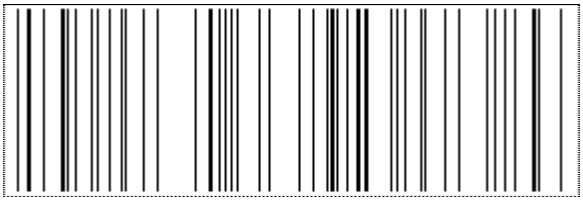


Figura 3: Distribución de Primos.

En [12] se puede ver también diversas características de la función ζ.

Hasta la fecha nadie ha podido demostrar que la conjetura de Riemann sea verdadera, o por el contrario, ha podido dar un contraejemplo. Este es uno de los problemas no resueltos más importantes de las matemáticas modernas. En [11] se presenta una colección actual de intentos por demostrarla. Lo que se tiene es sólo evidencia numérica de que la conjetura es cierta, en los aproximadamente 10^{13} primeros ceros. La cantidad de ceros calculados ha tenido el crecimiento bosquejado en la Tabla 3.

De manera visual, es posible captar una íntima relación entre los números primos y la función ζ. Tomemos muestras de m primos contiguos y de m ceros complejos de ζ contiguos a lo largo de la recta $x = \frac{1}{2}$ y marquémoslos con líneas verticales. En las gráficas 3 y 4 mostramos dos de tales patrones de números primos y de ceros de $zeta$ con $m = 50$, estos últimos elegidos de tablas de ceros [7]. Se observa que las distribuciones son "parecidas". Esto puede apreciarse mejor al tomar más muestras de tamaños mayores.

Tal relación se puede establecer de manera formal en la siguiente versión de la HR.

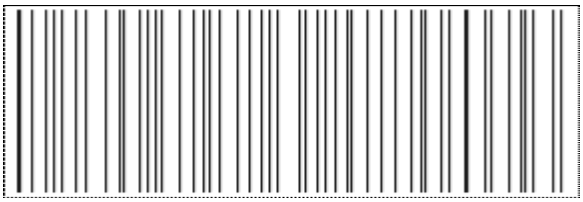


Figura 4: Distribución de ceros de ζ

Definición 2. *La* integral logarítmica $Li(x)$ *está definida por*

$$Li(x) = \int_2^x \frac{dt}{\log t}$$

Entonces se puede plantear de manera equivalente la hipótesis de Riemann como

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2+\epsilon}).$$

También se puede considerar a las funciones siguientes:

Definición 3. *Sean ψ y ϑ definidas como:*

$$\begin{aligned} x &\mapsto \psi(x) = \sum \{\log p | k \in \mathbb{N}\,,\, p \textit{ primo }\,,\, p^k \leq x\} \\ &\quad = \log\ \mathrm{mcm}\{i | 1 \leq i \leq \lfloor x \rfloor\} \\ x &\mapsto \vartheta(x) = \sum_{p \leq x} \log p \end{aligned}$$

Entonces la hipótesis de Riemann se expresa equivalentemente de dos formas:

$$\begin{aligned} \psi(x) &= x + O(x^{1/2+\epsilon}) \\ \vartheta(x) &= x + O(x^{1/2+\epsilon}) \end{aligned}$$

1.1. Aplicación del TNP en Criptografía

En la práctica criptográfica, involucrada de manera relevante en la seguridad de las comunicaciones, son muy comunes los *certificados digitales*. Un tal certificado consiste esencialmente de una clave pública, de los datos del propietario del certificado y de una firma digital de quien emite el certificado. La clave pública en un certificado RSA es un número entero producto de dos números primos, casi del mismo tamaño. Una de las preocupaciones más frecuentes es saber con certeza si acaso los números primos que componen la clave pública no podrán repetirse. Más aún, se trata de saber si hay suficientes números primos para una cantidad considerable de certificados digitales, o alternativamente si acaso es posible siempre encontrar números primos. La respuesta positiva a esto se implica si es posible contar los números primos y saber de qué manera están distribuidos.

Es entonces que el TNP puede resolver claramente estas dudas.

Por un lado, si se quiere tener primos de 512 bits, entonces éstos pueden buscarse en el intervalo $[2^{508}, 2^{509}]$. El TNP garantiza que en ese intervalo se puede encontrar aproximadamente $\pi(2^{509}) - \pi(2^{508})$ primos, es decir alrededor de

$$\begin{aligned} \frac{2^{509}}{\ln(2^{509})} - \frac{2^{508}}{\ln(2^{508})} &= (4{,}75034 - 2{,}37984) \cdot 10^{150} \\ &= 2{,}37049 \cdot 10^{150}. \end{aligned}$$

Si hubiese alrededor de 10^{80} moléculas en todo el universo, y mucho menos de 10^{10} individuos en el mundo, no es difícil darse cuenta que "nunca" se teminarán los primos a ser usados como certificados digitales.

Por otro lado, el TNP implica que dado un número x, hay aproximadamente $x/(\ln x)$ números primos menores a x. Haciendo estimaciones muy toscas, el siguiente primo puede esperarse en un valor y tal que $y/(\ln y) = x/(\ln x) + 1$. Presuponiendo además que $\ln(x) \sim \ln(y)$, se ha de tener $y \sim x + \ln x$. Esto quiere decir que si se tiene algún primo p, el siguiente ha de "aparecer" a una distancia aproximada de $\ln(p)$.

Así pues, sólo hay que recorrer alrededor de $\ln(2^{509}) \sim 352$ enteros, a partir de algún número aleatorio para encontrar un número primo como el requerido para un certificado digital. Las dudas referentes a los números primos en las aplicaciones mencionadas quedan resueltas en la práctica.

2. La Hipótesis Extendida de Riemann

Tal como sucede con la hipótesis de Riemann, la versión extendida se puede plantear de varias maneras. Veamos algunas de ellas:

Definición 4. *Sea p un número primo mayor que 2. La función $L_p : \mathbb{C} \to \mathbb{C}$ se define como:*

$$L_p(z) = \sum_{n=1}^{\infty} \left(\frac{n}{p}\right) \frac{1}{n^z}$$

donde $\left(\frac{n}{p}\right)$ es el llamado símbolo de Legendre.

Entonces la *Hipótesis Extendida de Riemann* (HER) se plantea como: *todos los ceros no-triviales de $z \mapsto L_p(z)$ tienen parte real* $1/2$.

Por otra parte, experimentalmente se puede observar que los números primos están "igualmente" distribuidos en diferentes clases de congruencia módulo un número n. Por ejemplo, entre los 1229 primos menores a 10000, 611 son congruentes con 1 y 617 lo son con 2, módulo 3. Es bien conocido el siguiente resultado acerca de los residuos de primos módulo un número n.

Teorema 1 (Dirichlet)**.** *Si* $\text{mcd}(a, n) = 1$ *entonces hay una cantidad infinita de números primos congruentes con a módulo n.*

Pero aún más, como una consecuencia del célebre *Teorema de Densidad de Cebatorov* se tiene que a la larga los números primos han de estar equidistribuidos en las clases de congruencia módulo n que contengan primos, por lo que puede esperarse un "mismo" número de primos en cada una de ellas. Como hay $\varphi(n)$ de tales clases (φ denota a la función clásica de Euler que cuenta para cada entero cuántos enteros existen menores que él y primos relativos con él), por el TNP "debería" haber alrededor de $x/(\varphi(n) \ln x)$ primos en cada una de tales clases de congruencia. Con lo cual queda motivada la siguiente

Definición 5. *Para tres enteros positivos x, a, n, con $a < n$, sea $\Pi(x, n, a)$ el conjunto de primos congruentes con a módulo n que son menores a x. Sea, ahora, $\pi : (x, n, a) \mapsto \pi(x, n, a) =$* $\text{card}(\Pi(x, n, a))$

A manera de ejemplos simples, $\pi(10000, 3, 1) = 611$, $\pi(10000, 3, 2) = 617$.

La HER también puede ser planteada de manera equivalente si tomamos dos enteros n y a primos relativos y $\epsilon > 0$. Entonces se ha de tener,

$$\pi(x, n, a) = \frac{\text{Li}(x)}{\phi(n)} + O(x^{1/2+\epsilon}).$$

Finalmente, escribiremos una última versión de HER después de la siguiente definición.

Definición 6. *Un* carácter *sobre un grupo abeliano G es un homomorfismo de G al círculo unitario $S^1 = \{z \in \mathbb{C} | z\overline{z} = 1\}$ (este último dotado de la multiplicación de números complejos).*

Definición 7. *Sea μ un carácter sobre el grupo multiplicativo $\mathbb{Z}_n^*$ de los enteros módulo n, entonces se define el* carácter de Dirichlet *$\chi : \mathbb{Z}^* \to S^1 \cup \{0\}$ como:*

$$\chi(m) = \begin{cases} \mu(m \bmod n) & \text{si } \text{mcd}(m, n) = 1 \\ 0 & \text{en otro caso} \end{cases}$$

Si χ asume sólo valores 0 o 1, se dice ser principal.

Input: $n \geq 3$ **Output:** A decision whether n is PRIME or COMPOSITE
1.- For $r = 2$ to $\lfloor \sqrt{n} \rfloor$ do 2- If $r \mid n$ then Output COMPOSITE 3.- Output PRIME

Cuadro 4: Método *Ensayar Divisiones*

La *función de Dirichlet* L es entonces

$$z \mapsto L(z, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^z}.$$

La HER afirma que *todos los ceros de L tienen parte real* $1/2$.

Para intentar explicar el uso de la HER, veamos el siguiente ejemplo: Supóngase que se quiere encontrar un residuo no-cuadrático b módulo un número primo p. Se sabe por observaciones que los residuos cuadráticos y los no cuadráticos están distribuidos de manera irregular. El primer impulso para encontrar una tal b es intentar con $2, 3, 4, \ldots$ hasta encontrarlo. Se puede observar que al variar el primo p, este número buscado no es muy grande, salvo para pocos primos p. Entonces es posible calcular el tiempo que nos costará encontrar tal b. Si la HER fuese cierta, vía la formulación anterior, entonces podemos tener una certidumbre de que existe una cota b_0 para la búsqueda. Por lo tanto basta buscar en $2, 3, 4, .., b_0$. Esto fue probado de manera formal por N. Ankeny [1], y fue generalizado para encontrar elementos fuera de un conjunto por E. Bach [2].

3. Antecedentes de Primalidad

El problema de *primalidad* consiste en decidir si un número n dado es primo o compuesto. Este problema ha sido sin duda uno de los más importantes a lo largo de la historia.

La *criba de Eratóstenes* es el método más antiguo (200 A.C.) para decidir si un número n dado es primo o compuesto. Este método comienza por construir una tabla de todos los números enteros positivos del 2 hasta n. Comenzando con el 2, declarado primo, se tacha a todos los múltiplos de él menores que n. Se regresa la inicio de la lista y se prosigue con el siguiente número no tachado, que obviamente es el 3, se le declara primo y se cancela ahora a todos los múltiplos de 3, que no hubiesen sido cancelados. Se regresa y se repite esto hasta que no queden primos o números por cancelar. Entonces se tendrá por conocidos a todos los factores primos de n o bien se podrá reconocer que n es primo.

Como consecuencia de la criba de Eratóstenes, tenemos el método de "ensayar divisiones". Este método se basa en el hecho de que es suficiente verificar, para n dado, si acaso todos los números primos menores a $\sqrt{n}$ no lo dividen, y entonces n debe ser un número primo. Ya que cuando n es compuesto, digamos $n = ab$, entonces uno de los factores es menor o igual a $\sqrt{n}$. Este procedimiento se puede ver en la Tabla 4 y aún es útil, en el caso que se quiera encontrar números primos pequeños.

Es bien conocido desde el siglo XVII, el *Teorema Pequeño de Fermat* (TPF): *Si $a > 0$ es un número entero positivo y p es un número primo, con* $\text{mcd}(a, p) = 1$*, entonces* $a^{p-1} \equiv 1 \bmod p$.

La proposición recíproca, sin embargo, no es cierta: si $a^{p-1} \equiv 1 \bmod p$, para todo a, con $\text{mcd}(a, p) = 1$, entonces p no necesariamente es un número primo.

Esto significa que hay números compuestos n tales que, para todo a con $\text{mcd}(a,n) = 1$, se cumple la relación $a^{n-1} \equiv 1 \bmod n$. R. Carmichael encontró por el año 1910 uno de tales números compuestos, a saber, $n = 561 = 3 \cdot 11 \cdot 17$. A partir de entonces a estos números se les llama *de Carmichael*.

Una forma equivalente al TPF es que si existe un número a con $\text{mcd}(a,n) = 1$ y $a^{n-1} \not\equiv 1 \bmod n$, entonces n es un número compuesto.

Lo anterior da un método para decidir si un número es compuesto, sin embargo es posible también usar el TPF para encontrar números "que parecen primos". El procedimiento consiste en fijar un número a, que llamaremos *testigo*, y evaluar $a^{n-1} \bmod n$. Si el resultado es diferente de 1, entonces el número es claramente compuesto y a es un *testigo de Fermat* de este hecho, pero si el resultado es 1, entonces el número n es un candidato a ser primo y a se dice ser un *seudoprimo respecto al testigo* a. El detalle en este último caso es ver qué tan "fuerte" es la candidatura de n a que sea primo. Muchos algoritmos probabilistas de primalidad se basan en el hecho de que, cuando esxisten testigos de Fermat, éstos se encuentran en un número pequeño de pruebas. Por tanto la probabilidad de que un seudoprimo respecto a un número relativamente pequeño de testigos sea efectivamente primo es muy alta. Los números de Carmichael, por supuesto, hacen que este criterio de decisión falle, pero éstos son muy raros, por ejemplo, R. Rivest [8] verificó que de 718 millones de números aleatorios de 128 bits de longitud, de los cuales 4 millones fueron seudoprimos respecto al testigo 2, ninguno dejó de cumplir la prueba de primalidad más fuerte a principios de la década de los 90 del siglo pasado. Hoy en día se sabe que aunque son raros los números de Carmichael hay una cantidad infinita de ellos, lo cual fue mostrado en 1992 por W. Alford, G. Granville y C. Pomerance. El último de tales números fue encontrado en 1998 y tiene 10200 dígitos decimales.

La discusión anterior nos lleva a pensar que es posible calcular y controlar la probabiliad de error en el caso de generar un número seudoprimo. De hecho, esto es la base de los algoritmos probabilísticos, los cuales son algoritmos que determinan si acaso un número es compuesto y si se falla en esto, entonces se declara como primo probable, con una probabilidad pequeña y controlada de error. En la siguiente sección hablaremos de cómo la HER influye en esos algoritmos para suprimir su carácter aleatorio.

4. Prueba de primalidad de Solovay-Strassen

Nuestro propósito en esta sección es ver que la aleatoriedad del *método de Solovay-Strassen* puede ser omitida bajo la suposición de que la HER es verdadera.

El métdo de Solovay-Strassen se presenta en la Tabla 5.

Lema 1. *Si n es un primo impar, entonces el algoritmo aleatorio de Solovay-Strassen produce el resultado* PRIME*, y si n es un compuesto impar produce* COMPOSITE *al menos para la mitad de posibles $a \in \{1,2,\ldots,n-1\}$. El algoritmo corre en tiempo polinomial, respecto al "tamaño de n". Su complejidad en tiempo es, precisamente, $O\left((\log n)^3\right)$.*

Como ya se sabe, este método es para certificar realmente composición, en lugar de primalidad. En lo que sigue se darán las herramientas para demostrar el lema 1.

Definición 8 (Símbolos de Jacobi y Legendre)**.** *Sea n un número entero impar con factorización $\prod p_i^{e_i}$. Entonces el* símbolo de Jacobi

Input: $n \geq 3$
Output: A decision whether n is PRIME or COMPOSITE
1.- Choose randomly $a \in \{1,2,\ldots,n-1\}$.
2.- If $\gcd(a,n) \neq 1$ then COMPOSITE; stop else
3.- If $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \bmod n$ then COMPOSITE; stop
4.- else PRIME.

Cuadro 5: Algoritmo *Aleatorio de Solovay-Strassen*

de un entero a, respecto a n, es $\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right)$, donde para cada primo p_i, $\left(\frac{a}{p_i}\right)$ es el símbolo de Legendre*: vale 1, si a es un residuo cuadrático módulo p_i y vale -1 en otro caso.*

El *criterio de Euler* consiste en que si p es un número primo impar y a es un entero tal que $\text{mcd}\,(a,p) = 1$ entonces a es un residuo cuadrático módulo p siempre que $a^{(p-1)/2} \equiv 1 \bmod p$ y no lo es si $a^{(p-1)/2} \equiv -1 \bmod p$.

Definición 9. *Se define el grupo de* falsos testigos *de Euler, para un entero n, como*

$$E(n) = \left\{ a \in \mathbb{Z}_n^* | \left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \bmod n \right\}.$$

Por ejemplo $E(65) = \{1, 8, 14, 18, 47, 51, 57, 64\}$.

Lema 2. *Sea n un número entero impar mayor que 1. Entonces n es primo si y sólo si $E(n) = \mathbb{Z}_n^*$.*

Ahora estamos listos para probar el lema 1.

Si n es un primo impar, el primer condicional "If" en el algoritmo no se satisfará nunca. En ese caso, de la definición del símbolo de Legendre este paso regresará siempre PRIME.

Si n es un número compuesto impar, entonces si $\text{mcd}(a,n) \neq 1$, el primer condicional regresa COMPOSITE, en caso contrario $a \in \mathbb{Z}_n^*$, y por el lema anterior $E(n) \neq \mathbb{Z}_n^*$. Pero como $E(n)$ es un subgrupo de $\mathbb{Z}_n^*$, entonces $E(n)$ debe ser un subgrupo propio. Por lo tanto,

$$|E(n)| \leq \frac{|\mathbb{Z}_n^*|}{2} = \frac{\phi(n)}{2} \leq \frac{(n-1)}{2} \leq \frac{n}{2}.$$

Y con probabilidad mayor o igual a $1/2$, a ha de ser un falso testigo de Euler para la composición de n, con el cual el algoritmo regresa COMPOSITE.

Por otro lado se sabe que para el cálculo de $\left(\frac{a}{n}\right)$ se toma un tiempo $O((\log n)^2)$, mientras que el cálculo de $a^{(n-1)/2} \bmod n$ requiere $O((\log n)^3)$. Esto termina la demostración. □

El algoritmo de Solovay-Strassen puede reescribirse para convertirlo en un algoritmo no-aleatorio, según se puede ver en la Tabla 6. La diferencia de los dos algoritmos se encuentra en la elección de a: el primero lo hace aleatoriamente y el segundo por medio de un ciclo "For" desde $a = 2$ hasta $2(\log n)^2$. Los siguientes resultados nos permitirán ver que esta variación del algoritmo es correcta.

Definición 10. *Para cada entero positivo n, sea*

$$G(n) = \text{mín}\left\{x | \mathbb{Z}_n^* \text{ es generado por primos } \leq x\right\}.$$

Teorema 2 (Ankeny)**.** *Suponiendo verdadera la HER, entonces $G(n) = O((\log n)^2)$, y para cada subgrupo H no trivial de $\mathbb{Z}_n^*$ se puede encontrar un $a \in \mathbb{Z}_n^* - H$ en tiempo $O((\log n)^2)$.*

Input: $n \geq 3$ **Output:** A decision whether n is PRIME or COMPOSITE
1.- For $a = 2$ to $2(\log n)^2$ do 2.- If mcd $(a, n) \neq 1$ then COMPOSITE else 3.- If $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} (\text{mod} n)$ then COMPOSITE 4.- PRIME

Cuadro 6: Algoritmo *No-aleatorio de Solovay-Strassen*

En diversas situaciones, se requiere encontrar un número fuera de cierto subgrupo propio de $\mathbb{Z}_n^*$. Por el teorema de Ankeny y la generalización de Bach, tales números son fáciles de ser encontrados y lo son mediante una búsqueda directa en lugar de una aleatoria. El teorema de Ankeny implica el siguiente, el cual finalmente nos permitirá llegar al objetivo que nos hemos planteado.

Teorema 3. *Suponiendo vedadera la HER, si n es un número entero impar compuesto, entonces existe un entero positivo $a \leq 2(\log n)^2$, para el cual se cumple una de las dos relaciones siguientes:* mcd $(a, n) \neq 1$ *o* $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \bmod n$.

En efecto, sea n es un número entero impar compuesto. Por el lema anterior, $E(n)$ es un subgrupo propio no-trivial de $\mathbb{Z}_n^*$. Por el teorema de Ankeny, se puede localizar un elemento $a \in \mathbb{Z}_n - E(n)$ en tiempo $O((\log n)^2)$, puesto que el complemento $\mathbb{Z}_n - E(n)$ es un subgrupo no-trivial de $\mathbb{Z}_n^*$. La cota específica en tiempo es $2(\log n)^2$. Si $a \notin \mathbb{Z}_n^*$ entonces mcd $(a, n) \neq 1$. Si $a \in \mathbb{Z}_n^*$, entonces $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \bmod n$ puesto que a no está en $E(n)$. □

Finalmente:

Teorema 4. *Suponiendo verdadera la HER, la versión no-aleatoria del algoritmo de Solovay-Strassen, regresa* PRIME *si y sólo si n es primo, y lo hace en tiempo polinomial.*

En efecto, por el teorema 3, si n es compuesto, uno de los dos "If" del algoritmo regresa COMPOSITE. En caso contrario, n debe ser primo. Ya que sólo se está probando hasta $2(\log n)^2$ valores de a, el tiempo polinomial es prácticamente una consecuencia de que el algoritmo original corre también en tiempo polinomial. □

5. Algoritmo de Miller Rabin

De manera similar al algoritmo de Solovay-Strassen, el de Miller-Rabin, el cual se bosqueja en la Tabla 7, es un algoritmo aleatorio que puede evitar esa aleatoriedad bajo la suposición de la HER.

Teorema 5. *Si n es un número primo impar, entonces el algoritmo de Miller-Rabin regresa siempre* PRIME. *si n es compuesto entonces el algoritmo regresa* COMPOSITE, *para al menos $3/4$ de todos los a's tales que $1 \leq a \leq n-1$. El algoritmo tiene una complejidad de tiempo $O((\log n)^3)$.*

Bajo la suposición de la HER, una vez más, el cambio del algoritmo para suprimir la aleatoriedad está en sustituir la instrucción

Choose a at random from $\{1, 2, \ldots, n-1\}$

por la instrucción

Input: $n \geq 3$ **Output:** A decision whether n is PRIME or COMPOSITE
1.- Choose a at random from $\{1, 2, \ldots, n-1\}$ 2.- Express $n - 1 = 2^s t$, t odd. 3.- Compute successively $a_0 = a^t \bmod n$, $a_1 = a_0^2 \bmod n, \ldots, a_k = a_{k-1}^2 \bmod n$ until $k = s$ or $a_k \equiv 1 \bmod n$ 4.- If $(k = s)$ and $a_k \not\equiv 1$ then COMPOSITE 5.- else If $(k = 0)$ then PRIME 6.- else If $(a_{k-1} \not\equiv -1)$ then COMPOSITE 7.- else PRIME

Cuadro 7: Algoritmo *Aleatorio de Miller-Rabin*

For $a = 1$ to $2(\log n)^2$ do .

Se sugiere para propósitos de implementación elegir el algoritmo de Miller-Rabin (MR) en vez del algoritmo de Solovay-Strassen (SS). En primer lugar porque en SS hay que evaluar el símbolo de Jacobi y en segundo, la probabilidad de error en SS es 1/2, mientras que en MR es 1/4.

6. Otras aplicaciones de la conjetura de Riemann

Como vemos, una de las más importantes conjeturas es la HER. En esta sección simplemente mencionaremos algunos resultados en diferentes áreas, que bajo la suposición de que la HER es válida, ellos también son válidos. Existen cientos de aplicaciones y las aquí enlistadas forman una pequeña muestra, repetimos, siempre suponiendo la HER.

1. En la versión de campos numéricos algebraicos, se ha demostrado la conjetura original de Artin [5].
2. Se tiene una diversidad de algoritmos para campos finitos [10].
3. Se tiene un algoritmo para factorizar polinomios en $\mathbb{F}_p[X]$ [9].
4. Existe un algoritmo para calcular el número de clase h_Δ del grupo de clase C_Δ, además de otros algoritmos para el mismo grupo [6].
5. Existe un método que garantiza la *suavidad* de ciertos números, es decir, el que estos números puedan factorizarse con primos acotados por un b adecuado [6].

En [2] se puede encontrar una gran cantidad de resultados de la Teoría de Números apoyados en la suposición de la HER. Otro de los campos abundantes en aplicaciones de la HER es la Física, particularmente en aplicaciones relativas al movimiento browniano, osciladores armónicos, ruido, caos y, en general, mecánica estadística. También en la existencia de ciertos esquemas de compartición de secretos en criptografía.

Bibliografía

[1] N. C. Ankeny, "The Least Quadratic Non Residue" *Annals of Mathematics*, Vol. 55, No. 1, January 1952

[2] E. Bach, J. Shallit, *"Algorithmic Number Theory, Efficient Algorithms"*, Vol 1., The MIT Press. Cambridge Massachusetts. 1996

[3] D. J. Bernstein, "Distinguishing prime numbers from composite numbers: the state of the art in 2004", Draft. University of Illinois at Chicago. http://cr.yp.to/primetests/prime2004-20041223.pdf

[4] E. Bombieri, "Problems of the Millennium: The Riemann Hypothesis," http://www.claymath.org/millennium/Riemann_Hypothesis/Official_Problem_Description.pdf

[5] C. Hooley, "On Artin's conjecture," *J. Reine and Angew. Math.* 225, pp. 209-220.

[6] A.K. Lenstra, H.W. Lenstra, "Algorithms in Number Theory," *Handbook of Theoretical Computer Science*, Chapter 12., Elsevier Science Publisher B.V. 1990.

[7] Andrew Odlyzko, "Tables of zeros of the Riemann zeta function". http://www.dtc.umn.edu/~odlyzko/zeta_tables/index.html

[8] Ronald L. Rivest, "Finding Four Million Large Random Primes", CRYPTO90 Lecture Notes in Computer Science No. 537, pp. 625–626, 1991. http://theory.lcs.mit.edu/~rivest/Rivest-FindingFourMillionLargeRandomPrimes.ps

[9] V. Shop, "Smoothness and Factoring Polynomials over Finite Fields", CSD University of Toronto, 1996.

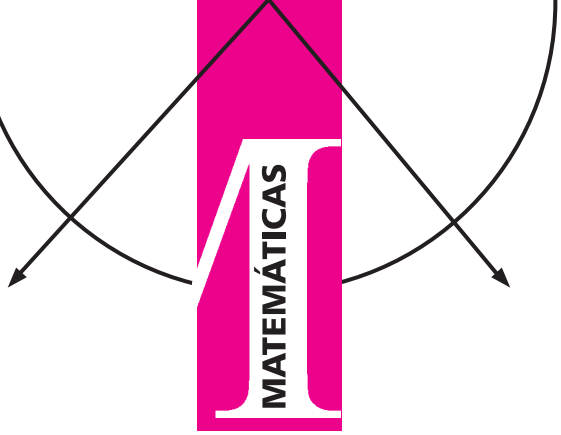
[10] I. E. Shparlinski, *"Finite fields: theory and computation"*, Kluwer Acad. Publ. Dordrecht 1999.

[11] Matthew R. Watkins, "Proposed proofs of the Riemann Hypothesis". http://www.secamlocal.ex.ac.uk/people/staff/mrwatkin/zeta/RHproofs.htm

[12] Eric W. Weisstein, "Riemann Zeta Function Zeros". From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/RiemannZetaFunctionZeros.html

[13] J Wojciechowski, "The Extended Riemann Hypothesis and its Application to Computation", January 2003. http://wonka.hampshire.edu/~jason/math/comp2/final_paper.pdf

Semigrupos de Operadores y su Relación con la Ecuación de Calor



Oswaldo González Gaxiola
UAM-Cuajimalpa

Resumen

En este trabajo hacemos una breve revisión de los conceptos y principales resultados de la teoría de *semigrupos de operadores* y en particular de *semigrupos fuertemente continuos* en un espacio de Banach. Además estableceremos una relación entre la teoría de *semigrupos* y una de las ecuaciones clásicas de la física-matemática: la ecuación de calor, cuya solución se modela por medio de un *semigrupo de convolución*.

Preliminares

Definición 3. *Sea $(E, ||\cdot||)$ un espacio normado. Si la métrica correspondiente d es completa, diremos que $(E, ||\cdot||)$ es un espacio de Banach. Si $(E, \langle\cdot,\cdot\rangle)$ es un espacio con producto interno cuya correspondiente métrica es completa, diremos que $(E, \langle\cdot,\cdot\rangle)$ es un espacio de Hilbert.*

En lo sucesivo, X, Y seran espacios de Banach sobre el campo $\mathbb{C}$. Denotaremos indistintamente por $||\cdot||$ la norma en X y en Y y $\mathcal{H}$ será un espacio de Hilbert sobre el mismo campo.

Definición 4. *Sea D subespacio vectorial de X. Una función $A : D \to Y$ es un operador lineal, o simplemente operador, de X en Y si D es denso en X y A es lineal; i.e.*

- $\overline{D} = X$.
- $\forall \alpha \in \mathbb{C}$, $f, g \in D$, $A(\alpha f + g) = \alpha A(f) + A(g)$.

Al conjunto de operadores de X en Y con dominio D lo denotaremos por $\mathcal{L}(D;Y)$ y para simplificar, denotaremos $\mathcal{L}(X;X) = \mathcal{L}(X)$.

Diremos que un operador $A \in \mathcal{L}(X;Y)$ es *acotado* si

$$\sup_{f\in X;||f||=1} ||Af|| < \infty,$$

en cuyo caso escribiremos

$$||A|| := \sup_{f\in X;||f||=1} ||Af||.$$

Al conjunto de los operadores acotados de X en Y lo denotaremos por $\mathcal{B}(X;Y)$ y denotaremos $\mathcal{B}(X;X) = \mathcal{B}(X)$.
Se tienen las siguientes propiedades:

(a) $\mathcal{L}(X;Y)$ es un espacio vectorial y $\mathcal{B}(X;Y)$ es subespacio de $\mathcal{L}(X;Y)$.

(b) $||\cdot||$ es una norma en $\mathcal{B}(X;Y)$.

(c) $\forall f \in X$, $||Af|| \leq ||A||||f||$.

(d) Si D es denso en X y $A \in \mathcal{B}(D;Y)$, entonces A se puede extender a todo X.

Proposición 1. *Si $A \in \mathcal{L}(X;Y)$, son equivalentes:*

(i) *A es acotado;*

(ii) *A es continuo; y*

(iii) *A es continuo en algún $x_0 \in X$.*

Principio de Acotación Uniforme: Sean $A \in \mathcal{B}(X;Y)$ y $\{A_n\}_{n\in\mathbb{N}} \subseteq \mathcal{B}(X;Y)$ tal que $A_n f \to Af$, $\forall f \in X$; entonces $\exists M > 0$ tal que $||A_n|| \leq M$, $\forall n \in \mathbb{N}$.

Breve Introducción a la Teoría de Semigrupos de Operadores

Fue A. Cauchy [1] quien en 1821 preguntó en su *Cours dÁnalyse* sin mayor motivación, lo siguiente:

" Déterminer la fonction $\varphi(x)$ de manière quélle reste continue entre deux limites réelles quelconques de la variable x, et que lón ait pour toutes les valeurs réelles des variables x et y

$$\varphi(x+y) = \varphi(x)\varphi(y)."$$

Usando notación moderna, reescribimos el requerimiento de Cauchy, omitiendo por el momento el requisito de continuidad, de la siguiente forma:

Problema

Encontrar todas las funciones $U_{(\cdot)} : \mathbb{R}_+ \to \mathbb{C}$ tales que satisfagan la siguiente ecuación funcional (EF),

$$\begin{cases} U_{t+s} = U_t U_s & \text{para cada} \quad t, s \geq 0, \\ U_0 = I. \end{cases}$$

Evidentemente, las funciones exponenciales

$$t \mapsto e^{at} \quad \text{para cualquier} \quad a \in \mathbb{C},$$

satisfacen la (EF). Con su pregunta, Cauchy sugiere que estas soluciones canónicas deberían ser todas las soluciones de la (EF).
Antes de dar respuesta al problema, analizaremos un poco a las funciones exponenciales y observaremos que además de satisfacer la identidad algebraica de la (EF), también tienen algunas propiedades analíticas importantes.

Proposición 2. *Sea $U_t := e^{at}$ para alguna $a \in \mathbb{C}$ y para todo $t \geq 0$. Entonces la función $U_{(\cdot)}$ es diferenciable y satisface el problema de valor inicial (PVI),*

$$\begin{cases} \frac{d}{dt}U_t = aU_t \quad \text{para cada} \quad t \geq 0, \\ U_0 = I. \end{cases}$$

Inversamente, dada $a \in \mathbb{C}$ la función $U_{(\cdot)} : \mathbb{R}_+$[1] $\to \mathbb{C}$ definida por $U_t = e^{at}$ es la única función diferenciable que satisface el (PVI). Finalmente, observemos que $a = \frac{d}{dt}U_t|_{t=0}$.

Demostración Demostraremos solamente la afirmación concerniente a la unicidad. Sea $S_{(\cdot)} : \mathbb{R}_+ \to \mathbb{C}$ otra función diferenciable que satisface el (PVI), fijemos $t > 0$, entonces la nueva función $Q_{(\cdot)} : [0, t] \to \mathbb{C}$ definida por

$$Q_s := U_s S_{t-s} \quad \text{para cada} \quad 0 \leq s \leq t$$

es diferenciable, con derivada $\frac{d}{ds}Q_s \equiv 0$. Así hemos demostrado que

$$U_t = Q_t = Q_0 = S_t \quad \text{para cada} \quad t > 0.$$

La existencia es fácil de verificar. ■

Consideremos ahora la siguiente proposición que, combinada con la anterior resolverá nuestro problema.

Proposición 3. *Sea $U_{(\cdot)} : \mathbb{R}_+ \to \mathbb{C}$ una función continua que satisface la (EF). Entonces $U_{(\cdot)}$ es diferenciable, y existe una única $a \in \mathbb{C}$ tal que se satisface el (PVI).*

Demostración Como $U_{(\cdot)}$ es una función continua en $\mathbb{R}_+$, entonces la función $V_{(\cdot)}$ definida por

$$V_t := \int_0^t U_s ds, \qquad t \geq 0,$$

es diferenciable con derivada $\dot{V}(t) = U_t$[2]. Esto implica que

$$\lim_{t \to 0^+} \frac{1}{t} V_t = \dot{V}_0 = U_0 = I.$$

Por lo tanto, V_{t_0} es diferente de cero, para algún $t_0 > 0$ pequeño. La (EF) ahora se puede escribir como,

$$U_t = V_{t_0}^{-1} V_{t_0} U_t = V_{t_0}^{-1} \int_0^{t_0} U_{t+s} ds$$

$$= V_{t_0}^{-1} \int_t^{t+t_0} U_s ds = V_{t_0}^{-1}(V_{t+t_0} - V_t)$$

para cada $t \geq 0$. Por lo tanto, $U_{(\cdot)}$ es diferenciable con derivada

$$\frac{d}{dt}U_t = \lim_{h \to 0^+} \frac{U_{t+h} - U_t}{h} = \lim_{h \to 0^+} \frac{U_h - U_0}{h} U_t$$

$$= \dot{U}_0 U_t \quad \text{para cada} \quad t \geq 0;$$

lo cual prueba que $U_{(\cdot)}$ satisface el (PVI) con $a := \dot{U}_0$. ■

La combinación de los dos resultados anteriores da una respuesta satisfactoria al problema de Cauchy escrito de manera moderna, lo cual enunciamos de manera formal en el teorema siguiente.

Teorema 1. *Sea $U_{(\cdot)} : \mathbb{R}_+ \to \mathbb{C}$ una función continua que satisface la (EF). Entonces existe una única $a \in \mathbb{C}$ tal que*

$$U_t = e^{at} \quad \text{para todo} \quad t \geq 0.$$

[1] $\mathbb{R}_+$ denota los números reales no negativos.

[2] estamos denotando por $\dot{v}$ la derivada $\frac{d}{dt}v(t)$

Lo anterior, lo hemos puesto aquí como una breve introducción a la teoría de *semigrupos* de operadores.

Definición 5. *Una familia 1-paramétrica $\{U_t\}_{t \geq 0} \subseteq \mathcal{B}(X)$ es un semigrupo de operadores acotados (o simplemente semigrupo) si:*
(i) $U_0 = I$, donde I es el operador identidad en $\mathcal{B}(X)$.
(ii) $U_{s+t} = U_s U_t$ para cada $s, t \geq 0$ (propiedad de semigrupo).
Si un semigrupo $\{U_t\}_{t \geq 0}$ satiface además
(iii) $lim_{t \to 0^+} ||U_t - I|| = 0$, decimos que es un semigrupo uniformemente continuo.
(iv) Si la propiedad en (ii) se cumple para cada par $s, t \in \mathbb{R}$, la familia $\{U_t\}_{t \in \mathbb{R}}$ es llamada grupo de operadores en $\mathcal{B}(X)$.

Definición 6. *Un semigrupo $\{U_t\}_{t \geq 0}$, de operadores en $\mathcal{B}(X)$ es un semigrupo fuertemente continuo si*

$$\lim_{t \to 0^+} U_t f = f \qquad \text{para cada } f \in X.$$

Definición 7. *El operador A en $\mathcal{L}(X)$ definido por*

$$D(A) = \{f \in X : \quad \lim_{t \longrightarrow 0^+} \frac{U_t f - f}{t} \quad existe\}$$

y

$$Af = \lim_{t \to 0^+} \frac{U_t f - f}{t} = \frac{d^+ U_t f}{dt}|_{t=0} \qquad \text{para } f \in D(A)$$

es el generador infinitesimal del semigrupo U_t, $D(A)$ es el dominio de A.

Tenemos el siguiente teorema, cuya demostración se puede hallar en [3]

Teorema 2. *Sea $\{U_t\}_{t \geq 0}$ un semigrupo fuertemente continuo en $\mathcal{B}(X)$, entonces existen constantes $\omega \geq 0$ y $M \geq 1$ tales que*

$$\|U_t\| \leq M e^{\omega t} \qquad \text{para} \quad t \geq 0.$$

Ejemplo 1. ***(Semigrupo de Traslaciones)*** *Sea X el espacio de Banach que consiste de las funciones acotadas y uniformemente continuas en $\mathbb{R}$ con la norma del supremo, $\|f\|_\infty = \sup_{x \in \mathbb{R}}\{|f(x)|\}$. Para $f \in X$ definimos U_t para cada $t \geq 0$ por $(U_t f)(x) = f(x + t)$;*

1. *Para $t = 0$ tenemos $U_0 = I$.*
2. *Para $s, t \geq 0$, y para $f \in X$, $U_t((U_s f)(x)) = (U_t f)(x + s) = f(x + s + t) = (U_{s+t} f)(x)$, luego $\{U_t\}_{t \geq 0}$ es un semigrupo sobre $\mathcal{B}(X)$*
3. *Como $f \in X$ es uniformemente continua en $\mathbb{R}$ entonces $\{U_t\}_{t \geq 0}$ es un semigrupo fuertemente continuo.*

El generador infinitesimal del semigrupo $\{U_t\}_{t \geq 0}$ está definido en

$$D(A) = \{f : \ f \in X, \ f' \ existe, \ f' \in X\}$$

por

$$(Af)(x) = f'(x).$$

Ahora expondremos el siguiente ejemplo, el cual está directamente relacionado con el objetivo principal del presente trabajo, que es ilustrar de manera simple la relación entre la teoría básica de semigrupos y la ecuación de calor.

Ejemplo 2. ***(El semigrupo de Gauss-Weierstrass en*** $\mathbb{R}$.*)*
Consideremos el espacio $\mathcal{H} = L^p(\mathbb{R})$, $1 \leq p < \infty$, *para* $t > 0$ *definamos* U_t *para* $f \in L^p(\mathbb{R})$ *por*

$$(U_t f)(x) = \frac{1}{\sqrt{4\pi t}} \int_{\mathbb{R}} exp(\frac{-(x-y)^2}{4t}) f(y) dy.$$

Podemos ver que $U_t f = G_t * f$, *(*$*$ *denota convolución) donde* $G_t(x) = \frac{1}{\sqrt{4\pi t}} exp(\frac{-x^2}{4t})$. *Como* $G_t \in L^1(\mathbb{R})$, *entonces* $U_t f \in L^p(\mathbb{R})$ *cuando* $f \in L^p(\mathbb{R})$.
Además

$$\|U_t f\|_p = \|G_t * f\|_p \leq \|G_t\|_1 \|f\|_p.$$

Como

$$\|G_t\|_1 = \frac{1}{\sqrt{4\pi t}} \int_{-\infty}^{\infty} exp(\frac{-x^2}{4t}) dx = 1,$$

entonces $\|U_t\| \leq 1$, *es decir,* U_t *es acotado sobre* $L^p(\mathbb{R})$ *para cada* $t > 0$.

Ahora, hagamos $U_0 = I$; *luego si* $t = 0$ *o bien* $s = 0$ *tenemos claramente que* $U_{t+s} = U_t U_s$. *Ahora, para el caso general consideremos el espacio de Schwartz*

$$\mathcal{S}(\mathbb{R}) = \{f \in C^\infty(\mathbb{R}) : \ \forall\, \alpha, \beta \in \mathbb{N}, \ \sup_x |x^\alpha D^\beta f(x)| < \infty\}$$

el cual es un subespacio denso de $L^p(\mathbb{R})$. *Para* $f \in \mathcal{S}(\mathbb{R})$, *por la asociatividad de la convolución para* $s, t > 0$ *se tiene* $(U_s U_t) f = G_s * (G_t * f) = (G_s * G_t) * f$; *haciendo cálculos tenemos*

$$(G_s * G_t)(x) = \frac{1}{4\pi\sqrt{st}} \int_{-\infty}^{\infty} exp(\frac{-(x-y)^2}{4s}) exp(\frac{-y^2}{4t}) dy$$

$$= \frac{1}{4\pi\sqrt{st}} \int_{-\infty}^{\infty} exp(\frac{-t(x-y)^2 - sy^2}{4st}) dy$$

$$= \frac{1}{4\pi\sqrt{st}} \int_{-\infty}^{\infty} exp[-\{\frac{(s+t)y^2 - 2txy + tx^2}{4st}\}] dy$$

$$= \frac{1}{4\pi\sqrt{st}} \int_{-\infty}^{\infty} exp[-(\frac{s+t}{4st})\{(y - \frac{tx}{s+t})^2 + (\frac{t}{s+t} - \frac{t^2}{(s+t)^2}) x^2\}] dy$$

$$= \frac{1}{4\pi\sqrt{st}} \int_{-\infty}^{\infty} exp[-(\frac{s+t}{4st}) Y^2] exp[-\frac{(s+t)}{4st} \cdot \frac{st}{(s+t)^2} x^2] dY$$

$$= \frac{1}{2\pi\sqrt{s+t}} exp(-\frac{x^2}{4(s+t)}) \int_{-\infty}^{\infty} e^{-z^2} dz \quad (z = \sqrt{\frac{s+t}{4st}} Y)$$

$$= \frac{1}{2\pi\sqrt{s+t}} exp(-\frac{x^2}{4(s+t)}) \sqrt{\pi}$$

$$= \frac{1}{\sqrt{4\pi(s+t)}} exp\{\frac{-x^2}{4(s+t)}\} = G_{s+t}(x)$$

luego $(U_s U_t) f = G_{s+t} * f = U_{s+t} f$ *para cada* $f \in \mathcal{S}(\mathbb{R})$; *por la densidad de este subespacio en* $L^p(\mathbb{R})$ *el resultado se puede extender a todo* $L^p(\mathbb{R})$.
Ahora usando resultados de la teoría de funciones de prueba tenemos que $G_t * f \longrightarrow f$ *cuando* $t \to 0^+$. *Por lo tanto* $\{U_t\}_{t \geq 0}$ *es un semigrupo fuertemente continuo sobre* $L^p(\mathbb{R})$.

La Relación con la Ecuación de Calor

En el ejemplo anterior, el semigrupo de Gauss-Weierstrass está dado por el núcleo

$$G_t(x) = \frac{1}{\sqrt{4\pi t}} exp(\frac{-x^2}{4t}).$$

Haciendo $G_t(x) = G(x,t)$ obtenemos la solución fundamental de la ecuación de calor $\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2}$ en la recta; lo cual significa que $u(x,t) = (G_t * f)(x) = (U_t f)(x)$ es solución del problema de valor inicial

$$\begin{cases} \frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2} \quad \text{para} \quad x \in \mathbb{R}, \ t > 0, \\ u(x,0) = f(x) \end{cases}$$

bajo condiciones apropiadas. En el caso n-dimensional, la solución de la ecuación de difusión de calor $\frac{\partial u}{\partial t} = \triangle u$ ($\triangle$ denota el Laplaciano n-dimensional) puede ser tratada de manera similar haciendo uso de la solución fundamental

$$G_n(x,t) = (4\pi t)^{-\frac{n}{2}} exp(-\frac{||x||^2}{4t}) \quad x \in \mathbb{R}^n, \quad t > 0.$$

Este es sólo un ejemplo de una teoría más general, la teoría de ecuaciones de evolución, en la cual los semigrupos y el análisis funcional juegan un papel fundamental, el objetivo principal del presente artículo, es invitar al lector a estudiar algunos temas del análisis funcional (teoría de semigrupos de operadores) como una herramienta fundamental para el estudio de algunos temas de ecuaciones en derivadas parciales.

Bibliografía

[1] Cauchy, A.L. *Cours dÁnalyse* de lÉcole Royale Polytechnique, première Partie, Analyse Algébrique, 1821

[2] Haberman Richard *Ecuaciones en Derivadas Parciales; Con Series de Fourier y Problemas de Contorno*; Prentice Hall, Madrid, 2003.

[3] Klaus-Jochen E. Rainer Nagel; *One-parameter semigroups for linear evolution equations*; Springer, New York, 1999.

[4] Mc Bride A. C. *Semigroup of Linear Operator: An Introduction*; Longman Scientific and Technical, New York, 1987.

[5] M. Reed and Barry Simon, W. *Methods of Modern Mathematical Physics*; Vol I, Academic Press, New York, 1970.

[6] Pazy, A. *Semigroups of Linear Operator and Applications to Partial Differential Equations*, Applied Mathematical Sciences; Springer-Verlag: New York, 1983.

[7] Weidmann, J. *Linear operators in Hilbert spaces*; Graduate texts in mathematics **68**, Springer-Verlag: New York, 1980.

XL Congreso Nacional de la Sociedad Matemática Mexicana

Relación de Hoteles con los que se llevó a cabo algún convenio y respetarán precios

Hotel Courtyard by Marriot San Jerónimo (SEDE) Av. San Jerónimo 1012, Col. San Jerónimo C.P. 64640 Tel: 01 (81) 8389 7900 Fax: 01 (81) 8389 7910 **Habitación Sencilla o Doble: $936.00 (impuestos incluidos)** Referencia: Sociedad Matemática Mexicana 2007	***Hotel Hampton Inn Norte (SEDE)*** Av. Universidad 501 Norte, San Nicolás, México 66450 Tel: 01 (81) 8305 2400 Fax: 01 (81) 8305 2410 **Habitación Sencilla o Doble: $819.00 (impuestos y desayuno buffet incluidos)**
Hotel 88 Inn Av. Lerdo de Tejada 767 Fracc. Tabachines C.P. 66450 Tel. 01 (81) 8305 9988 Lada sin costo 01 800 834 88 00 **Habitación Sencilla o Doble: $556.00 (Impuestos incluidos)** ***Tarifa sujeta a 10 habitaciones del grupo***	***Hotel Holiday Inn Norte*** Av. Universidad 101 Nte. San Nicolás de los Garza, C.P. 66450 Tel. (01) 81-8158-0000 Fax. (01) 81-8158-0017 **Habitación Sencilla o Doble: $1,013.22 (impuestos y desayuno buffet incluido)**
Fiesta Inn Av. Fidel Velazquez 3000.Col. Central C.P. 64270 Monterrey, N.L. Tel. 01 (81) 8389 8989 Fax. 01 (81) 8389 8900 Lada sin costo 01 800 504 50 00 **Habitación Sencilla o Doble: $970.77 (Impuestos y desayuno continental incluidos)** Clave de grupo: GHHVI	***Hotel Son Mar*** Av. Alfonso Reyes No. 1211 Norte. Col. Sarabia C.P. 64490 Monterrey N.L. Tel. 01 (81) 8126 1300 x. 513 y 502 Fax. 01 (81) 8372 5077 e-mail reservaciones@sonmar.com.mx **Habitación Sencilla o Doble: $585.00 (Impuestos incluidos)** **Persona Extra: $117.00 (Impuestos incluidos)**
Hotel Plaza del Arco Av. Pino Suárez # 935 Norte Col. Centro, Monterrey, N.L. Tel. 01 (81) 8372 4050 **Habitación Sencilla o Doble $650.00** **Habitación $700.00** **Hab. Cuádruple $750.00 (Impuestos y desayuno americano incluidos)**	***Hotel Plaza del Arco Express*** Av. Madero # 309 Pte. Col. Centro , Monterrey, N.L. Tel. 01 (81) 8125 2646 **Habitación Sencilla o Doble $600.00** **Habitación Triple $650.00** **Habitación Cuádruple $700.00 (Impuestos y desayuno americano incluidos)**
Best Western Madero Av. Madero #123 Oriente Col. Centro C.P. 06400 Tel. 01 (81) 8375 0750 **Habitación Sencilla: $550.00** **Habitación Doble: $600.00** **Habitación Triple: $650.00** **Habitación Cuadruple: $700.00 (Impuestos y desayuno buffet incluidos)**	***Best Western Plaza Monterrey*** Av. Madero No. 250 Ote. Col. Centro C.P. 64000 Monterrey, N.L. **Habitación Sencilla: $643.00** **Habitación Doble: $760.00 (Impuestos y desayuno continental incluidos)**
Safi centro Pino Suárez No. 444 Sur. Monterrey, N.L. C.P. 64000 Tel. 01 (81) 8399 7000 Fax. 01 (81) 8399 7020 Lada sin costo. 01 800 8399 7000 **Habitación Sencilla: $760.50 (incluye impuestos)** **Habitación Sencilla: $842.40 (incluye impuestos)**	***Novotel Monterrey Valle*** Av. Lázaro Cárdenas No. 3000. Esq. Dr. Atl. Col del Valle. San Pedro Garza García N.L. Tel. 01 (81) 8133 8133 Fax. 01 (81) 8133 8134 **Habitación Sencilla o Doble: $930.15 (incluye impuestos)**
Holiday Inn Monterrey Centro Padre Mier No. 194 Poniente Col. Centro C.P. 64000 Monterrey, N.L. Tel. 01 (81) 8228 6000 Lada sin costo 01 800 223 6870 Fax. 01 (81) 8228 6020 e-mail: rmtycentro@hotelesmilenium.com **Habitación Sencilla o Doble: $877.50 (impuestos incluidos)** **Habitación Triple: $1,053.00 (impuestos incluidos)**	***Holiday Inn Express Monterrey Galerias-San Jerónimo*** Av. San Jerónimo No. 1082 Pte. Col. San Jerónimo C.P. 64640 Monterrey, N.L. Tel. 01 (81) 8389 6000 Lada sin costo. 01 800 711 9158 Fax. 01 (81) 8389 6020 e-mail santiago.fraga@hotelesmilenium.com **Habitación Sencilla o Doble: $918.00** **Habitación Triple: $1,110.33 (impuestos, desayuno ejecutivo y llamadas locales incluidas)**
Hotel Fastos Av. Colón No. 956 Pte. Esq. Con Villagran. C.P. 64000 Monterrey, N.L. Tel. 01 (81) 1233 3500 y 3529 Lada sin costo 01 800 839 2400 **Habitación Sencilla o Doble: $ 503.10** **Habitación Triple: $ 600.00** **Hab. Cuádruple $ 690.30 (impuestos, desayuno continental y llamadas locales incluidas)**	

SMM-Fundación Kovalévskaia
CONVOCATORIA 2007

Objetivo: Promover la participación de las mujeres en la investigación matemática en México.

I. Dirigido a:

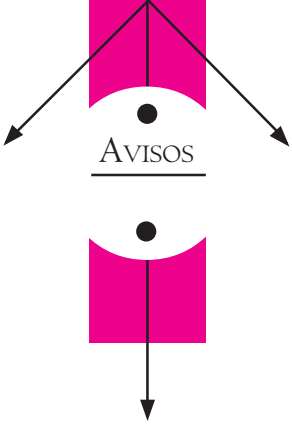
a) Mujeres mexicanas que realizan estudios de doctorado en cualquier campo de la matemática.
b) Mujeres que realizan investigación en matemáticas, que están adscritas a una institución de educación superior o a una institución pública de investigación en México, y que obtuvieron el grado de doctor dentro de los cinco años previos a la fecha de emisión de esta convocatoria

II. Características: Otorgar un apoyo económico complementario para:

- La conclusión del proyecto doctoral y la obtención del grado.
- Llevar a cabo un proyecto de investigación.

Los apoyos serán individuales y no de grupo.

Fecha límite: 31 de agosto del 2007.
Requisitos e informes:
http://www.smm.org.mx



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

CARTA INFORMATIVA

SOCIEDAD MATEMÁTICA MEXICANA

Número 53,
Julio de 2007

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

Premiación de la Olimpiada Mexicana de Matemáticas