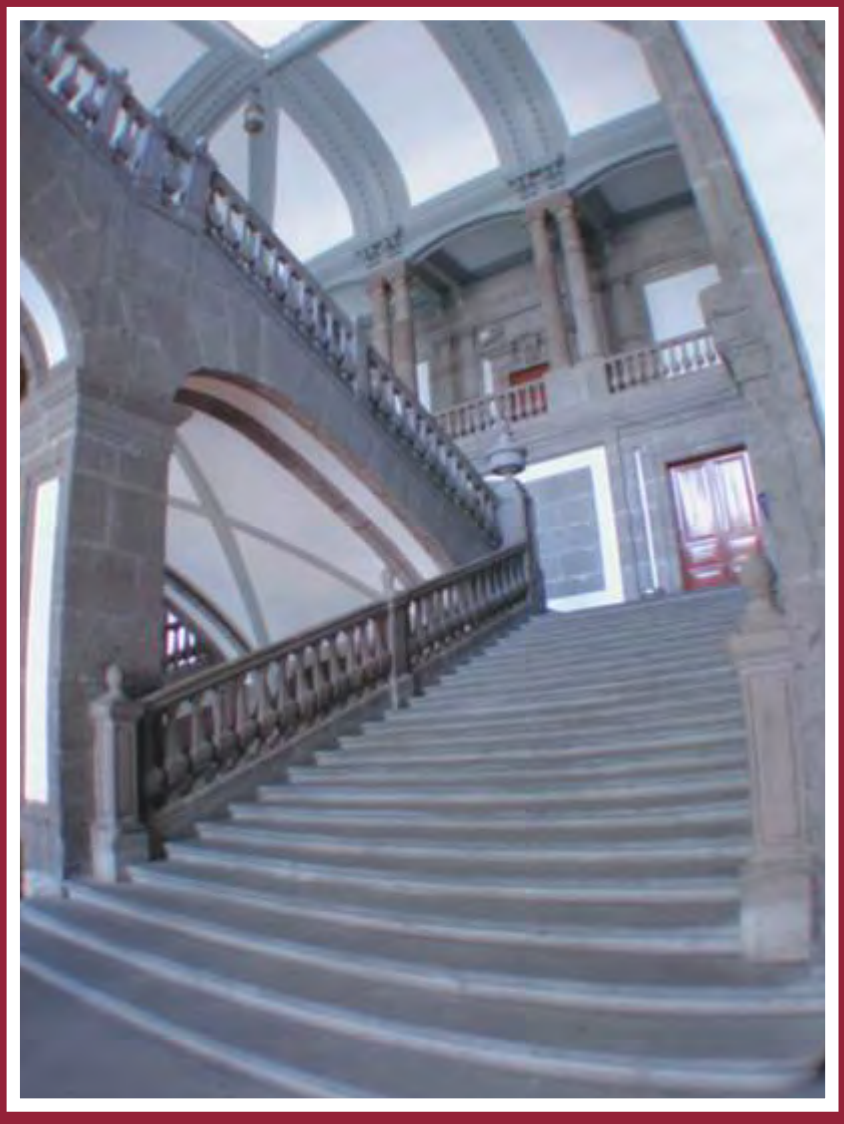
CARTA INFORMATIVA

Abril 2003



Sexagésimo Aniversario

Sociedad Matemática Mexicana

Palacio de Minería 27 de junio 2003

Raymundo Bautista Ramos
Aprendiendo a vencer la flojera

Rita Esther Zuazua Vega
Unidad Morelia del Instituto de Matemáticas de la UNAM
(zuazua@matmor.unam.mx)

Raymundo Bautista Ramos, nació en la ciudad de Puebla, en marzo de 1943. Desde muy joven (quizás desde sus estudios de primaria) se empeñó en ser matemático.

Siendo el mayor de once hermanos, a su familia no le agradó mucho su decisión. Las matemáticas eran una carrera a la que no se le veía ningún futuro (hablando en plata), por lo cual entró a estudiar a la normal para ser maestro de primaria (1960). No duró mucho su obediencia, en menos de dos meses, Raymundo desertaría. Entonces se hizo un pacto: "estudias lo que quieras porque te gusta, pero primero te inscribes en una carrera que sirva para algo". Raymundo decidió entrar a ingeniería química (1961) e inscribirse simultáneamente en la carrera de físico-matemáticas de la Universidad de Puebla. Empezaron nuevamente los problemas, la carrera era más de física, no había profesores que impartieran las materias de matemáticas y la ingeniería química era demasiado real y al mismo tiempo muy imprecisa, había que hacer ciertos experimentos y tomar mediciones y luego pues a ojo de buen cubero afinar el asunto para que todo saliera bien. Ayudado por su profesor de matemáticas, el Ing. Joaquín Ancona Albertos, Raymundo consigue obtener una beca de la Universidad de Puebla para irse a la Facultad de Ciencias de la UNAM (1963), a terminar su carrera de matemático (1966), con la tesis titulada "Anillos factoriales", bajo la dirección de Emilio Lluis Riera. Su primer trabajo como matemático fue en la Escuela de Altos Estudios de la Universidad de Sonora. Después regresaría a la Facultad de Ciencias para realizar sus estudios de maestría (1969) y doctorado (1970), obteniendo el grado con la tesis titulada "Cohomología relativa de grupos finitos", bajo la dirección de Humberto Cárdenas.

De 1966 a 1970, Raymundo ocuparía una plaza de Investigador adjunto en el Instituto de Matemáticas de la UNAM (IM-UNAM). Después de una estancia durante un año como investigador en la Escuela de Ciencias Físico-Matemáticas de la Universidad Autónoma de Puebla (1971-72), ingresó como Investigador Titular al IM-UNAM, posición que ha ocupado hasta la fecha. Entre las áreas en las que ha trabajado podemos mencionar de manera muy breve: representaciones de grupos y cohomología de grupos, representaciones de álgebras y problemas matriciales y físico-matemática.

A todo lo largo de su carrera académica, Raymundo ha realizado visitas como investigador invitado a múltiples universidades en los cuatro puntos cardinales, impartiendo conferencias y realizando trabajos conjuntos. Por poner sólo algunos, mencionaremos Universidades de USA, Alemania, Polonia, Suiza, Noruega, la antigua URSS, Brasil, Argentina, China, Inglaterra, etc.

La labor docente de Raymundo ha sido continua desde los años setentas, iniciando en la Facultad de Ciencias de la UNAM, hasta la Escuela de Ciencias Físico-Matemáticas de la Universidad Michoacana, donde actualmente imparte cursos. Ha dirigido un total de 22 tesis, de las cuales 8 son de licenciatura, 9 de maestría y 5 de doctorado.

Raymundo Bautista Ramos

De sus más de setenta artículos publicados, Raymundo tiene más de 400 citas, lo cual nos da una muy buena idea del impacto de sus trabajos.

Además de su labor docente y de investigación, Raymundo ha sobresalido en nuestra comunidad por el desempeño de altos puestos académicos y administrativos como son: Director del Instituto de Ciencias de la Universidad Autónoma de Puebla (1981-82); miembro de la Comisión Evaluadora del Sistema Nacional de Investigadores en Ciencias Físico-matemáticas (1985-89), presidente de esta comisión durante 1988-89; Secretario y Vicepresidente de la Sociedad Matemática Mexicana (1980-81 y 1981-82, respectivamente); Director del Instituto de Matemáticas de la UNAM, durante los

periodos 1984-1990 y 1990-1994. Actualmente Raymundo es el Jefe de la Unidad Morelia del Instituto de Matemáticas de la UNAM.

Con respecto a la organización de eventos académicos nacionales e internacionales y participación en Comités Editoriales podemos mencionar, entre los más importantes, la Tercera y Séptima Conferencia Internacional de Teoría de Representaciones de Álgebra ICRA, (1980, Puebla; 1994 Cocoyoc), el Encuentro Latinoamericano de Álgebra y Geometría Algebraica (1992, Guanajuato y Morelia), la Sesión Especial de Teoría de Representaciones de Álgebras (1993, Reunión Conjunta AMS-SMM, Mérida), Whorkshop on Algebra (1995, Morelia).

Desde 1977 Raymundo también ha dirigido un gran número de seminarios en el IM-UNAM, actualmente dirige, junto con Humberto Cárdenas, el seminario de álgebra de la Unidad Morelia.

Como alumna de Raymundo he tenido la oportunidad de ver el reconocimiento que a nivel internacional ha recibido. Recuerdo que en 1997, en una reunión en Ukrania el organizador del evento, Y. Drozd, decidió hacer cambios en el programa para que el profesor Bautista dispusiera no sólo de una hora sino de todo el tiempo que considerara necesario para impartir su conferencia. También el impacto de la plática plenaria que Raymundo presentó en Bielefeld, Alemania 1998 durante el ICRA, aunque por su nerviosismo, Raymundo olvidó apretar el botón que hacia que los pizarrones subieran y bajaran y decidió hacerlo manualmente, teniendo que hacer un gran esfuerzo físico, cuando finalmente Raymundo escuchó la recomendación de hacerlo electrónicamente, su comentario sencillamente fue: yo soy un matemático del tercer mundo (aunque no sus matemáticas).

En cierta ocasión, cuando Raymundo terminó su último periodo de director, por lo cual no era muy conocido entre los nuevos estudiantes, impartimos un curso conjunto en la Facultad de Ciencias, después de un par de semanas, los estudiantes se acercaron preocupados a preguntarme quién era Raymundo Bautista, ¿por qué se viste de traje?, ¿es matemático? Raymundo y yo nos reímos mucho con esta anécdota. Esto no nos extraña a quienes lo conocemos, quizá una de las características que más admiro de él es su modestia como matemático, pero también su gran ambición y tenacidad, he visto trabajar a Raymundo durante diez años en un problema, sin que en ningún momento decaiga su ánimo. Para Raymundo no hay matemáticas o problemas de moda, cuando algo logra llamar su atención se convertirá en un reto para él entenderlo, desmenuzarlo y volverlo a armar aportando nuevas ideas.

El estilo de Raymundo como matemático, no es fácil de describir, le gusta crear teorías, puede empezar con un problema a primera vista simple, pero siempre tratará de ir más y más lejos, generalizando cosas, tomando otras teorías y tratando de unirlas, dando lugar a unas matemáticas muy creativas y originales, por lo que muchas veces resulta muy difícil convencerlo de ponerle punto final a un trabajo. Si nos permitieran ver a Raymundo haciendo matemáticas a través de un espejo, nos sería muy complicado adivinar su nacionalidad, veríamos la pasión del latino, mezclada con la fuerza de un vikingo, la minuciosidad de un relojero suizo y la disciplina de un japonés.

Si quisiéramos decir cuál es su mejor sentido, me atrevería a afirmar que el olfato, su intuición natural aunada a tantos años de trabajo y conocimientos en las matemáticas en general y no sólo en su área, lo hace percibir de manera inmediata problemas fundamentales y las técnicas par atacarlos.

Hablando con Rudyd, su esposa, le comenté que al principio de mi trabajo con Raymundo, me sorprendía mucho que cada vez que terminaba un congreso él se enfermaba. Rudyd me lo explicó; ese es su mecanismo de sobrevivencia, trabajar sin descanso, hasta que se enferma, entonces puede relajarse y dejar de trabajar sin dejar de sentir remordimientos, así que su cuerpo aprendió rápidamente eso y ésta será la única manera en que veamos a Raymundo descansando. En sus primeros años de matrimonio, su compañera se sorprendía por su capacidad de trabajo, así que alguna vez le preguntó: "¿es que a ti nunca te da flojera?", a lo que él contestó: "claro que sí, pero el chiste es vencer a la flojera". Con esta filosofía es que Raymundo ha enfrentado a nuestro sistema, habiendo logrado alcanzar las máximas categorías académicas en nuestro país.

En una conversación cotidiana, fuera de las matemáticas, el cine no es un buen tema, Raymundo dice con gran orgullo que la última película que vio fue "Allá en el Rancho Grande". Sin embargo, es un apasionado lector, desde Sócrates hasta Saramago. Quizás el amor de Raymundo por los libros tenga su origen en el hecho de que su familia poseía una imprenta en la cual Raymundo tuvo su primer trabajo, como corrector de estilo y ortografía.

Sin lugar a dudas la mayor debilidad de Raymundo es su familia. Su esposa y sus hijos, quienes reciben su apoyo incondicional en todas sus decisiones. Raymundo no es un hombre de consejos, es un hombre que escucha y muestra el panorama general con todos sus senderos, pero que cree en la libertad de la toma de decisiones y el derecho de asumir las consecuencias sobre nuestros actos.

Después de largas conversaciones con Rudyd, mi visión al final es que Raymundo es como un globo que tiende a ir al cielo, Rudyd tiene la cuerda que lo sujeta y en muchas ocasiones tiene que dar un gran jalón para mantenerlo en la tierra. He aquí una de sus historias favoritas:

Cuando Raymundo y Rudyd eran novios, fueron al cine, Rudyd tenia sed pero le daba pena decirlo, por lo que usando la filosofía femenina (existe, pero no es única), comentó: "qué calor esta haciendo", gran error, Raymundo le dijo que sí, hacía mucho calor, porque las ondas... y la película se convirtió en una clase de física. Moraleja, Con Raymundo hay que llamar al pan, pan y al vino, vino.

Para terminar, quiero agradecerle a Rudyd su asesoría para escribir este artículo como muestra de gratitud y cariño hacia mi maestro y amigo con motivo de su sesenta aniversario. ¡Felicidades!

Tejiendo destellos: Imágenes de la vida de Sylvia de Neymet

Ma. de la Paz Álvarez Scherer
Facultad de Ciencias, UNAM.
mpas@hp.fciencias.unam.mx

El siguiente texto es una adaptación del leído en el homenaje que la Facultad de Ciencias dedicó a Sylvia de Neymet. Todas las historias fueron contadas por ella misma en deliciosas conversaciones al calor de un café. Hoy, a casi un mes de su fallecimiento, quisiera compartir la inmensa nostalgia de su ausencia.

I.

La mamá de Sylvia quedó huérfana de padre, siendo muy joven, durante la Revolución. Su madre la impulsó a estudiar en la normal. El primer trabajo que tuvo fue en un pueblo, hoy comido por la ciudad, llamado Santiaguito al cual llegaba todos los días tomando un tren que salía del Zócalo. Ádemás de ser maestra tenía grandes inquietudes artísticas y estudió en La Esmeralda, dedicándose a la escultura. Sus trabajos son orgullo de sus hijos y nietos. La abuela paterna de Sylvia fue maestra muy reconocida del Colegio de las Vizcaínas. Sylvia proviene, pues, de una estirpe de mujeres singulares de principio del siglo pasado: mujeres cultas, mujeres trabajadoras, mujeres artistas.

El papá era ingeniero civil. Para llegar a su primer trabajo tomaba, todos los días, el mismito tren en el Zócalo. Y así, tras largas jornadas viajeras, el ingeniero, delgado, formal, siempre de sombrero, conquistó a la joven maestra. Desde entonces, vivieron en San José Insurgentes-Mixcoac, en una casa llena de arte, de plantas y de pláticas interesantes. Así crecieron Sylvia y sus hermanos.

Estando Sylvia en primaria, pocas cosas la desconcertaron más que el día que su mamá intentó ayudarle en la tarea de aritmética. El problema era de los típicos: "si 15 manzanas cuestan 7 pesos, ¿cuánto cuestan 23 manzanas?" Y ahí estaba Sylvia a punto de empezar a talachear cuando su mamá le pregunta "a ver, dime, ¿es más o menos?

El asombro de Sylvia fue mayúsculo: "¿Cómo?"

—"¿Cuestan más o menos?" volvió a preguntar su mamá.

Sylvia no pudo más y le dijo, "Mamá, en la escuela nos piden resultados EXACTOS, ¡no más o menos!"

La mamá comprendió que nunca había discutido la maestra ninguna forma de razonamiento, que sólo había enseñado procedimientos sin ton ni son y, pacientemente, volvió a formular la pregunta conduciendo la discusión.

II.

Esta situación cambió radicalmente y para bien en la secundaria. Sylvia entró a la Universidad Femenina y su maestra de trigonometría, la que le mostró el placer de razonar fue, ni más ni menos, que nuestra querida Manuela Garín. Más tarde, en la preparatoria, la extraordinaria profesora Ma. Teresa Sánchez de Padilla, que también daba clases en la ENP, culminó el proceso que enamoró a Sylvia de las matemáticas. Por cierto, el libro de Cálculo que llevaron fue el Vázquez-Barros Sierra, mismo que sería su libro de texto en la Facultad de Ciencias de la UNAM.

Vale la pena mencionar aquí que la Universidad Femenina, fundada y dirigida por la Sra. Obregón Santacilia se convirtió en un centro de desarrollo intelectual muy profundo. Las veladas culturales de los viernes incluían a personajes como Juan José Arreola, Nabor Carrillo, etc. El arte, la ciencia y la cultura en boca de sus creadores, difundiendo entre estas jóvenes las ideas más actuales de la época. En esta escuela y desde la secundaria, tuvo Sylvia a una de sus más queridas amigas, Alejandra Jaidar, de entrañable memoria en la UNAM.

Sylvia de Neymet

Y así, en 1955, llega Sylvia a la nuevecita Facultad de Ciencias. Ciudad Universitaria llevaba dos años funcionando. Sus maestros del primer año fueron, ni más ni menos que los pioneros: Barajas, Torres, Nápoles Gándara, Graef y Vázquez. Además cursó Temas Selectos de Física con Oyarzábal. El laboratorio de esta materia lo daba Lozano. En este laboratorio, Sylvia rompió un record: Para un experimento de probabilidad, Lozano le pidió a Sylvia, anunciándola como "una mano inocente", que echara volados. La tal "mano santa" en TODOS los tiros sacó puras águilas.... para envidia de cualquier vendedor de buñuelos.

¿Alguien puede pensar en Sylvia de Neymet como una domadora de fieras? Pues ahí donde ven, así fue. Resulta que cuando Sylvia estaba en 4º año, es decir, cuando era una jovencita de 19 años, el entonces director de la Facultad, Nápoles Gándara, le propone dar clases en la preparatoria. A Sylvia le parece una gran oportunidad y sin preguntar más, acepta.

La sorpresa es que las clases eran de Geometría Analítica para los chavos de la prepa 3. Esto, a los jóvenes de hoy puede no decirles nada...pero los menos jóvenes recordamos que la prepa 3 era, ni más ni menos, que la prepa 1, en San Ildefonso, en la tarde-noche. Y ahí va Sylvia a darle clases a los jóvenes de la nocturna.

Cuando llegó, lo primero que supo fue que sus futuros alumnos acababan de correr, mediante una huelga, a su antecesor. Y la mismita tarde que habló con el director sobre la clase, así, sin más preámbulos, la mandaron a dar su materia. Lo primero que recibió de los chavos fue un reclamo por haber intercambiado, rumbo a la clase, el salón de la planta baja que tenían asignado por otro en el primer piso de un profesor con problemas para caminar. Hay que decir que casi todos sus alumnos eran mayores que Sylvia. Así que todas las tardes ella se ponía el más serio ropaje que encontrara y llegaba a dar su clase. En su casa se reían de su disfraz de maestra seria.

Ese año, 1958, hubo muchas huelgas importantes en México. En particular, hubo una huelga estudiantil contra el alza de precio del transporte. Los chavos de la prepa 3 organizaron brigadas, hicieron propaganda y convocaron a una manifestación al Zócalo. Desde luego, invitaron a su querida profesora: "nosotros vamos por usted y la cuidamos toda la marcha, maestra".

Al acercarse el final del curso, los alumnos le pidieron a Sylvia que les diera Cálculo el año siguiente. Pero ella estaba a punto de irse a París y no podía hacerlo. El día del último examen llegaron todos los alumnos trajeados, guapísimos. Al final le dijeron a Sylvia que la invitaban a echarse un taquito. Ellos, los más bravos, los de la fama de groseros y de vándalos, le tenían reservada una mesa a su maestra y habían contratado un mariachi para despedirla. ¿Ahora si ven a la domadora de fieras? Si lo gentil no quita lo valiente...

Dicen por ahí que Lefschetz no era precisamente una persona fácil... pero, si los chavos de la prepa cayeron ante la gentileza de Sylvia, ¿cómo iba a resistirse el gran maestro? Y así se convirtió en su alumna de tesis. Él venía los veranos. Sylvia se recibió en 1961.

III.

Antes de recibirse, ya con la tesis hecha, se fue dos años a París becada por el gobierno francés. El primer año vivió en la Alianza Francesa y el 2º en la Casa de México de la Ciudad Universitaria de París. Estudió en el Instituto Henri Poincaré de la Sorbona. Llevó cursos con el Prof. Ehresaman de Topología Diferencial (rama de las matemáticas que estaba naciendo), Topología Algebraica y Categorías. Participó en el seminario de Cartan. Entre sus compañeros estaba Adrien Douady, el famoso y estrambótico –desde entonces- matemático francés, y Shu-Bei-Shu, un gran topólogo chino.

De regreso a México, pasó por Princeton donde además de visitar a su maestro, conoce a Fox, Milnor, Papakyriakopoulos. Nada más para que se den una idea de la época de la que hablamos, Princeton era EXCLUSIVAMENTE para hombres y este discriminatorio hecho era parte de su orgullo.

Quizá nos parezca totalmente natural, como le parece a Sylvia, esta historia. A ver, sitúense en 1958, piensen en una jovencita y pregunto ¿de verdad les parece natural? ¿a cuántas chavitas más de esa época conocen que lo hicieran? De esta característica de Sylvia, de hacer pasar por natural lo extraordinario, hablaré más tarde.

Al regresar de Francia, Sylvia se recibe. Era abril de 1961. Durante este año da clases, como maestra por horas, en la Facultad de Ciencias.

De la estancia en París, Sylvia ganó en profundidad matemática, en experiencia de la vida y.... en el amor. Y así, en abril de 1962 se casa con Michel Christ, joven médico que prendado de la matemática y con el espíritu aventurero que lo caracteriza, deja su país en pos de ELLA. Juntos compartirán aventuras de todo tipo: pesca, buceo, radioafición y la más comprometida de todas las aventuras: tener hijos.

IV.

Por estas mismas fechas se produce un cambio importante en el medio matemático: se abre el CINVESTAV. A él se incorporan dos jóvenes recién doctorados en Princeton: José Adem y Samuel Gitler. El CINVESTAV abre su maestría y doctorado y entre sus primeros alumnos están Francisco Tomás y, claro, Sylvia. En esa época imparte clases en la Escuela de Físco-Matemáticas del IPN a la 1ª generación (que iba en 4º año) de Álgebra Homológica y Análisis Matemático.

Al año siguiente, presenta los exámenes generales y nace su hija Simone. Hace su tesis de doctorado con Samuel Gitler y nace Lorraine. En 1966, Sylvia es la primera mujer mexicana que se recibe de doctorado. Se incorpora a la Facultad de Ciencias y nace Pierre. Aunque la historia no lo registra, también en ese año fue la 1ª reunión conjunta de la AMS y la SMM. La ponencia de Sylvia sobre una parte de su tesis doctoral es expuesta por Gitler.

Y ese mismo año, 1966, Sylvia es nombrada profesora de Tiempo Completo del Depto. de Matemáticas. Los únicos tres tiempos completos eran Sylvia, Víctor Neumann y Arturo Fregoso.

De entonces a la fecha, ha enseñado en más de 50 cursos de la Facultad, ha dirigido tesis de licenciatura y maestría, ha sido sinodal (en exámenes profesionales, de maestría y de doctorado), ha dado conferencias en congresos nacionales e internacionales, ha participado en comisiones del departamento de Matemáticas, del CONACYT, ha sido miembro de la Junta Directiva de la Sociedad Matemática Mexicana, ha impartido cursos en universidades de provincia, ha publicado artículos de investigación y, a últimas fechas, ha dedicado su esfuerzo a la redacción de un libro sobre acciones de grupos que muy pronto será editado por la Sociedad Matemática Mexicana.

V.

Para terminar quiero platicar de mi relación con Sylvia.
De una u otra forma, aunque en la licenciatura Sylvia no fue mi maestra, siempre estuvo presente: Sylvia, cuando te saluda, no está siendo "amable" en el sentido formal de la palabra: te saluda a ti. Cuando te pregunta cómo estás, cómo van las cosas, las materias, cómo te va en tu nueva ayudantía, cómo va tu embarazo, cómo están tus bebés, te está diciendo que lo comparte, que aunque nunca hayas platicado con ella, está contigo.

Fue más tarde, en la maestría, que realmente conocí y desde entonces he disfrutado a Sylvia. Es la más entusiasta y apasionada de la geometría, la topología, de los ejemplos bonitos, me tocó verla

enloquecer con las acciones de grupo (ya veía acciones de grupo hasta en la sopa de letritas), el seminario de geometría hiperbólica en el que participamos la entusiasmaba enormemente. Ahí descubrí otra parte de su personalidad; su identidad secreta: Sylvia es "el gis más rápido del Oeste"... ninguna demostración se le para enfrente... una hora es más que suficiente para desenredar los más terribles secretos de teorema alguno... es muy difícil discernir que va más rápido: el gis, sus palabras, las ideas o el implacable borrador... es impresionante y agotador. Saliendo de seminario sólo cabía compartir un café t-r-a-n-q-u-i-l-o.

El momento crucial de nuestra amistad fue el congreso en Guanajuato de 1990. Viajamos Pilar Martínez, Sylvia, Mariana Saiz y yo en el coche de Sylvia. Ahí se rompió cualquier hielo y descubrimos que detrás de lo serio y formal, Sylvia escondía a una mujer divertida, alegre, dicharachera. Recuerdo que Mariana todavía le habló de "usted" a Sylvia... hasta la 1ª caseta de la carretera a Querétaro. Sylvia y yo compartimos habitación... y noches enteras de la más deliciosa plática... eran las 2 de la mañana y nos decíamos "bueno, ya. Mañana seguimos platicando" apagábamos la luz... y bastaba con que una dijera "pero..." para que la luz se encendiera, y la plática continuara hora tras hora. Las dos vivimos ese congreso con grandes ojeras, bostezos que intentábamos fueran discretos y felices... de ese mismo congreso salió una declaración de la Sociedad Matemática Mexicana (por cierto, muy poco difundida) que, en esas noches de desvelos, Sylvia ayudó a matizar. Nos gustó tanto, que en Morelia y en Guanajuato, una segunda vez, volvimos a hacerlo: madrugadas llena de buena plática, días de intenso trabajo, cenas departiendo con otros colegas... para reiniciar la madrugada platicando....

Sylvia es gentil, es alegre, entusiasta, Sylvia sabe oír y sabe decirte... Sylvia se sabe la historia de la Facultad de Ciencias; no sólo se la sabe, ha sido partícipe importantísima de ella. Como lo gentil no quita lo valiente, siempre ha tomado posición y ha defendido sus puntos de vista implacable pero gentilmente.

VI.

Sylvia se siente apabullada cuando uno le habla de lo excepcional de ella y de su vida. Recuerdo que en el congreso de Aguascalientes, cuando me tocó presentarla para una conferencia magistral, lo único que me pidió fue que no dijera nada que sonara extraordinario. Le parece "cualquier cosa" ser:

— La "domadora" de la prepa
— La alumna de Lefschetz,
— La primera mujer con doctorado en matemáticas
— La primer mujer que fue maestra de tiempo completo del Departamento de Matemáticas de la Facultad de Ciencias
— La mamá-maestra de tiempo completo
— La maestra que le ha dado su vida a la facultad.

No se da cuenta plena de cómo ella y mujeres como ella desbrozaron el camino para las que vinimos después. Le parece lo natural, lo que había que hacer...y eso es parte de lo que la hace tan especial. Algún día se tendrá que escribir la historia bien, poniendo a Sylvia, a todas estas grandes mujeres, en el lugar que les corresponde.

Quiero acabar parafraseando a Bertold Brecht:

Hay profesores que están un día y son buenos
Hay profesores que están muchos días y son muy buenos
Pero hay profesores que están toda la vida;
ésos son los imprescindibles

A Sylvia, extraordinaria mujer, extraordinaria matemática, entrañable amiga, imprescindible maestra, un ramo de flores con todo cariño:

19 de septiembre del 2002
Amoxcalli, Facultad de Ciencias, UNAM.

Proyecto EMAT: una esperanza para la enseñanza de las Matemáticas. Experiencias y resultados en Coahuila

Francisco Javier Cepeda Flores
Facultad de Matemáticas y CIMA
Universidad Autónoma de Coahuila
fcepeda@cima.uadec.mx

Es tradicional y actualmente está de moda, la problemática que existe en la enseñanza de las matemáticas en México. También es generalizada la queja sobre las dificultades y alta reprobación en esta materia. Muchas quejas, muchas voces, muchos fantasmas estereotipados sobre las matemáticas; sin embargo pocas propuestas y menos soluciones. Los maestros de matemáticas llevan a cabo todo tipo de acciones para mejorar sus cátedras, pero son iniciativas aisladas, la mayoría lejos de la sistematización, con poco o nulo apoyo institucional.

Por eso, el Programa Enseñanza de las Matemáticas Asistidas por Tecnología, EMAT, es uno de los pocos esfuerzos institucionales más serios y prometedores a nivel nacional. El objetivo de esta nota es compartir con la comunidad la experiencia de su aplicación masiva en Coahuila. Quizá para algunos pueda parecer que nos gana el entusiasmo por los resultados positivos y porque no hablaremos de un proyecto sino de algo realizado masivamente y con buenos resultados; sin embargo, de ninguna manera se pretende decir que el programa es una panacea, porque cualquier especialista del área sabe que en enseñanza de las matemáticas no hay panaceas.

Antecedentes y coyuntura

Con raíces internacionales y como producto de años de investigación de los académicos del Departamento de Matemática Educativa del Centro de Investigación y Estudios Avanzados del IPN (CINVESTAV), encabezados por las doctoras Teresa Rojano y Sonia Ursini, se diseñó y probó el EMAT en una decena de lugares en el país, a nivel piloto, con buenos resultados.

Al incorporarse Coahuila a este esfuerzo, en 1999, se presentó un conjunto de afortunadas acciones que conformaron una coyuntura favorable para aplicar masivamente este programa en todas las escuelas secundarias estatales. El Gobierno del Estado compró computadoras para todas ellas, formó laboratorios de cómputo en las mismas, creó el Centro de Informática Educativa Siglo XXI, para garantizar y promover el uso de la computadora en la educación. A esto se sumó el interés de la Facultad de Matemáticas y el Centro de Investigación en Matemáticas Aplicadas de la Universidad de Coahuila, por investigar el problema de enseñanza de las matemáticas e impulsar su enseñanza con nuevas tecnologías. En la Universidad, a propuesta del CINVESTAV, se integró un grupo de especialistas, dirigidos por el Doctor Humberto Madrid y el autor de estas líneas, para diseñar un proyecto de aplicación del nuevo método al sistema educativo coahuilense.

Bajo un Convenio entre la SEP Federal, la SEP Coahuila, el CINVESTAV, el Instituto Latinoamericano de Comunicación Educativa (ILCE), el Centro Siglo XXI mencionado y la Universidad Autónoma de Coahuila, se inició en 1999 el programa de investigación y la expansión masiva de la enseñanza de las matemáticas usando calculadoras y computadoras. Era la primera vez en nuestro país y representaba todo un reto.

Este proyecto se basa en el modelo conocido entre los pedagogos como *constructivista*, porque se aprende a través de la acción al mismo tiempo que se estructura el pensamiento racional, a través de las posibilidades del micro mundo de la computadora. Se usan programas especiales y generales como Excel, Cabri, Derive, Stella, Sim Calc, etc. Además, el Departamento de Matemática Educativa del CINVESTAV generó más de 100 hojas de trabajo para los temas del Programa Oficial de Secundarias que plantean situaciones didácticas e inducen el raciocinio matemático.

Todos los elementos estaban presentes, faltaba convertirlo en realidad para aprovechar la coyuntura y lograr la masificación del programa hacia el mejoramiento de la enseñanza de las matemáticas. Sin embargo, al inicio de 1999, faltaba mucho trabajo y particularmente, una gran movilización para capacitar a los profesores de secundaria y hasta sensibilizar a los niveles directivos. Al organizar el grupo de especialistas entre el Departamento de Matemática Educativa y la Facultad de Matemáticas, se preparan los materiales y se organizan las acciones conjuntamente con la SEP Coahuila y el Centro de Informática Siglo XXI.

Después de pasar una y mil peripecias para lograr la distribución de las computadoras por todo el amplio territorio coahuilense; y la operación de los laboratorios de cómputo en las 256 escuelas secundarias del Estado, se inició la capacitación.

Con cursos iniciales y posteriores de reforzamiento, se capacitaron alrededor de 50 instructores y 800 maestros en activo del nivel secundaria. En total fueron 7 cursos a instructores, reproducidos por ellos en 265 cursos a profesores de todo el estado; además, de 14 sesiones de sensibilización a directivos. También aquí se presentaron las dificultades propias del trabajo masivo y de las condiciones precarias por recursos escasos.

Desde agosto de 1999 se inició la expansión masiva frente a los grupos de alumnos, para lo cual se editaron 165 mil cuadernillos con hojas de trabajo y manuales de EMAT. Durante tres generaciones se alcanzó un máximo de expansión de 98 % de escuelas, 85% de alumnos y 90% de profesores. En casos específicos la aplicación fue deficiente; y no siempre se ha mantenido el mismo nivel.

Evaluación y resultados

Para llevar a cabo el seguimiento se levantaron reportes bimestrales, evaluaciones iniciales y evaluaciones al final del curso. Con todo esto, a nivel masivo, se obtuvieron del orden de 5,000 gráficas sobre el impacto del uso de la computadora en el aprendizaje de los alumnos (totales, por región, tipo de escuela y por género).

En esta fase de evaluación, después de aplicarlo por ciclos escolares a cada generación, se trataba de determinar cuál era el impacto del uso de la computadora, los nuevos materiales, y cambios en la didáctica de las matemáticas. Se aplicó una Evaluación inicial, Reportes Bimestrales, Entrevistas directas, visitas de observación a clases, reuniones de evaluación con profesores y una evaluación final a cada generación durante tres años consecutivos. Una vez que se procesaron los millones de datos, el resultado es ampliamente favorable y muy esperanzador. Algunas cifras obtenidas se explican a continuación, aunque se cuenta con bancos de datos muy amplios que respaldan las afirmaciones y que están a disposición de la comunidad. De hecho, este programa ha convertido al Estado en un gran laboratorio sobre enseñanza de las matemáticas.

Entre los diversos cuestionarios de encuesta que se aplicaron, se pudo detectar que tanto para profesores, alumnos y directivos, EMAT fue bueno o muy bueno en porcentajes que alcanzaron el 75% y, en todos los caso, fue mayoritaria la aprobación.

En otro instrumento, aproximadamente el 70 % de los profesores respondieron que mejora el interés por las matemáticas, cerca del 80% aprende computación y más del 50% respondió que contribuye a razonar y explorar más y que propicia la creatividad, entre otras cosas. Los procesos lógicos se ejercitan al basar el aprendizaje en la acción al mismo tiempo que se estructura el pensamiento.

El uso de la exploración para resolver problemas en el micromundo que ofrece la computadora, manipulando los objetos matemáticos, simulando la realidad, prepara y forma a los alumnos en el análisis, comparación, identificación de regularidades y patrones, sucesiones funcionales, reversibilidad y recursividad de los procesos, capacidad de abstracción, entre otros aspectos. La amplia posibilidad del cálculo numérico fácil, permite construir sucesiones de números que representen fenómenos reales y se pueda ver su comportamiento al manipular cantidades deseadas; o que se manipule un objeto geométrico relacionando el comportamiento con la expresión algebraica. Por ejemplo, la representación a través de los años de la población de algún lugar, hacia adelante o hacia él; o una recta movida en el marco de los ejes cartesianos, relacionándola con su expresión algebraica. El uso creativo de la computadora y la calculadora, también ofrece la posibilidad de usar diferentes representaciones como la graficación a colores y dinámica que permiten fortalecer la comprensión de las abstracciones del álgebra y su comportamiento recursivo numérico y geométrico.

Para los alumnos, a los cuales se les preguntó sobre el método tradicional y el usado con base en la computadora, en alrededor del 70% de los casos les gusta más este último método para aprender matemáticas y no les parece nada aburrido; opinando que con el método tradicional las matemáticas son muy aburridas.

Otro tipo de resultados directamente relacionados con temas y conceptos de matemáticas, también fueron interesantes:

- Se detectó claramente que las sucesiones de números naturales son fácilmente identificadas a diferencia de cuando intervienen el cero y los números negativos.
- En el caso de la proporcionalidad, las grandes posibilidades de cálculo numérico que aporta Excel, le permiten a los alumnos aprender este concepto que no tienen claro.
- Para los diferentes aspectos de la preálgebra, EMAT se reveló muy útil, con fuerte impacto en el aprendizaje. Específicamente se cambia el uso del lenguaje oral en la resolución de problemas, para acceder al uso de técnicas, instrucciones y lenguaje prealgebraico, dando un salto en su estructura racional.
- En el caso de la probabilidad se evidenció que su enseñanza es deficiente, que estos conceptos tienen dificultad en sus fundamentos y que se requiere mayor énfasis en este tema.

Sin ser las únicas, con las anteriores observaciones, se puede afirmar que EMAT permite atacar aquellos problemas de aprendizaje detectados y ampliar el uso de la computadora con secuencias didácticas en aquellos temas del programa en que se obtuvieron resultados positivos como los descritos.

Un aspecto interesante, es que todos estos resultados coinciden con los obtenidos en las pruebas piloto llevadas a cabo por el personal del Departamento de Matemática Educativa del CINVESTAV en varios estados de la República.

Los resultados anteriores que se encuentran en bancos de información del orden de los seis millones de datos, permiten continuar estudios comparativos por temas, áreas, regiones, tipos de escuelas y por género. Estas acciones actualmente están en proceso.

Los buenos resultados obtenidos en la masificación de EMAT en Coahuila, permiten diseñar programas y metodologías de expansión para el resto del país. De hecho, ya se trabaja para lograr la organización de las Escuelas de Matemáticas, a través del Comité respectivo de la SMM, con el fin de emprender la enorme tarea de aplicar este esperanzador programa cuya viabilidad y bondades ha sido demostrada. La tarea es tan grande que lograr una movilización nacional no está siendo fácil pero al menos ya existe una esperanza, con programas concretos y probados, que tienden a superar los aspectos críticos de la enseñanza de las matemáticas en nuestro país.

Por supuesto que debe considerarse que en la fase piloto se dieron condiciones favorables de laboratorio que no siempre se presentan. Aunque en el caso de la expansión masiva fueron condiciones muy apegadas a las existentes regularmente porque se trabajó en el sistema instituido con todas sus fortalezas y debilidades. Sin embargo, también hubo esfuerzos adicionales como la fuerte inversión en equipo, la creación de unidades específicas para atender la operatividad y la participación de especialistas de la Universidad, así como la concurrencia interinstitucional, a nivel nacional e internacional. Es decir, se presentaron varios elementos sin los cuales el programa se degradaría o no sería posible.

Ciertamente, una de las dificultades mayores que hacen peligrar estos programas, sobre todo cuando son masivos, son los problemas logísticos por insuficiente comprensión de algunos niveles de autoridad o mandos medios. Falta consolidar la cultura de operación, man-

tenimiento y desarrollo de equipo y programas de computadora; así como programas de formación y actualización del personal docente y administrativo.

De cualquier forma, en Coahuila fue posible llevarlo a cabo y los resultados fueron buenos y pueden serlo en cualquier lugar en que se garanticen las condiciones mínimas según la experiencia obtenida. Por eso se afirma que el programa no es una panacea, pero sí una esperanza; porque se demostró que es posible en el mundo real, aunque tenga sus limitaciones y condiciones mínimas para tener éxito. La esperanza no debe ser un sentimiento idealizado, sino un proyecto que se construye, una meta que se conquista transformando la realidad.

Incluso, desde una perspectiva más amplia, debe prevalecer la prudencia e inteligencia necesaria para no adoptar acríticamente la tecnología; estar alertas para enfrentar los riesgos de ésta, como por ejemplo lo inconveniente que resulta *"acceder al transistor sin haber pasado por el alfabeto",* como lo señala un distinguido intelectual mexicano.

La tarea es grande y las dificultades también, pero ya se tienen propuestas concretas serias, derivadas de la investigación, con probada viabilidad como se demuestra en Coahuila, que permiten tener esperanzas de superar los problemas prácticos y, en unos años, ver mejores resultados en la enseñanza de las matemáticas.

Ahora sí podremos decir que ante las visiones catastrofistas, existen alternativas que se van convirtiendo en realidad. Los matemáticos debemos impulsar todas estas posibilidades y abandonar la tradicional contemplación ante un rechazo social hacia nuestra disciplina. La esperanza existe, hagámosla realidad; construyamos el futuro.

Se notifica a todos los miembros de la Sociedad Matemática Mexicana que ha quedado conformado el Comité Electoral en vista de la próxima elección de Junta Directiva de la Sociedad Matemática Mexicana. Los integrantes son:

- Flor de María Aceff
- Eugenio Garnica Vigil
- Bertha Madrid Núñez
- Lourdes Palacios Fabila
- Lino F. Reséndis Ocampo

La Junta Directiva actual y este Comité Electoral abren la convocatoria al registro de planillas para la próxima Junta Directiva, bienio 2004-2005, y del correspondiente Consejo Consultivo para sus miembros no permanentes. Los registros se deben hacer llegar por escrito a la dirección de la Sociedad Matemática Mexicana:

Apdo. Postal 70-450
04510 México, D.F.

El escrutinio de los votos se llevará a cabo en la sede del XXXVI Congreso Nacional de la SMM, en la **Ciudad de Pachuca, Hidalgo, el Jueves 16 de Octubre a las 12:00 hrs.**

Asimismo se informa que el Comité Organizador de la Olimpiada Mexicana de Matemáticas será también renovado en dicho periodo.

Reducción de Cuota de Inscripción

A las Instituciones de Educación Superior,
a la Comunidad Matemática del país:

La Sociedad Matemática Mexicana pone a disposición de la comunidad matemática un número limitado de reducciones en la cuota de inscripción al XXXVI Congreso Nacional para las personas que estén interesadas en asistir pero que tengan una fuerte restricción presupuestal. La cuota especial será de $250.00 por persona y habrá reducción solamente para 10 personas por estado de la república.

Para tramitar esta cuota especial, los interesados deberán enviar su nombre e institución de procedencia a la dirección electrónica cuotaespecial@smm.org.mx antes del 10 de junio. La SMM publicará en su página Web www.smm.org.mx , entre el 30 de junio y el 4 de julio, la lista de personas que se hicieron acreedoras a estas cuotas especiales.

Junta Directiva de la Sociedad Matemática Mexicana

Corrección y Seguridad de la Información (Segunda parte: Criptografía)

Horacio Tapia-Recillas
Departamento de Matemáticas
Universidad Autónoma Metropolitana, Iztapalapa
(htr@xanum.uam.mx)

En la primera parte de esta nota se introdujeron algunas ideas sobre la detección y corrección de errores que se adquieren durante la transmisión de la información por cualquier canal de comunicación. Esto se hizo por *medio de los llamados códigos lineales detectores-correctores de errores*. En esta segunda parte se introducirán algunas ideas básicas para proteger la información por medio de la *criptografía*, también conocida como *cifrado de datos*, sin importar el medio de comunicación que se use para su transmisión.

Introducción

La *criptografía*, cuyas raíces vienen de **kryptos**: *esconder* y **graphos**: *escritura*, a la cual algunas personas llaman la *ciencia de la información secreta* no es nueva, ya que por ejemplo los romanos usaban técnicas para "esconder" su información. Durante muchos siglos y en diversos contextos se usó la criptografía, en un buen número de casos vinculados con cuestiones bélicas y de seguridad nacional (por ejemplo México estuvo vinculado con el telegrama Zimmermann durante la Primera Guerra Mundial, [10], [21]). Lo cierto es que hoy en día existen muchas otras aplicaciones interesantes en diversas áreas de la vida cotidiana, como son: seguridad informática, comercio y banca electrónica, licitaciones electrónicas, firma y ensobretado digital, tarjetas inteligentes, votación electrónica, entre otras. Se puede decir que actualmente cualquier sistema de seguridad para salvaguardar la información tiene entre sus componentes un módulo criptográfico. En las siguientes líneas se presentarán algunas ideas básicas sobre la *criptografía*, también conocida como *cifrado de datos*. Existe un gran número de libros, revistas y direcciones en internet sobre este tema, el lector interesado en profundizar en esta línea de investigación puede consultar por ejemplo [5], [11], [13], [17], [20], [22].

Esquema de cifrado

Supóngase que una entidad **A** (persona, oficina, etc.) desea enviar información confidencial, por cualquier medio de comunicación convencional (radio, red, teléfono, etc.), a otra entidad **B**. Antes de enviar la información original, conocida también como *texto llano* o *texto en claro*, la entidad **A** la "transforma" usando un sistema de cifrado (una "caja negra"), es decir, le aplica una función de cifrado e_{K_1}, la cual depende de una *llave*, $\mathbf{K_1}$ (que puede ser por ejemplo, un número, una palabra o frase, las cuales se transforman en una colección de bits). Este sistema produce el *texto cifrado o encriptado*, el cual se envía a la contraparte. Para que la entidad **B** pueda recuperar el texto original, el texto cifrado se hace pasar por un sistema de descifrado (otra "caja negra"), es decir, le aplica una función d_{K_2} al texto cifrado, la cual también depende de una *llave* $\mathbf{K_2}$ de tal manera que la composición $d_{K_2} \circ e_{K_1}$ es la función identidad. Existe la posibilidad de que al enviar la información ésta pueda ser interceptada por un "enemigo o intruso" **E**, quien por supuesto desea conocer la información original. En general, la forma o método de cifrado es público y la robustez de un sistema de cifrado radica en el hecho de que no sea fácil obtener la información original a partir del texto cifrado sin conocer las llaves, tanto para cifrar como para descifrar, es decir, que el sistema de cifrado resista un *criptoanálisis*.

La siguiente figura muestra un esquema de cifrado/descifrado.

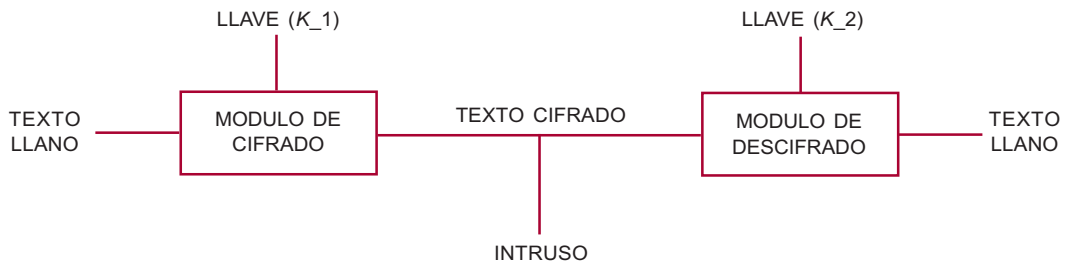


Fig. 1. Esquema de cifrado

Sistemas de cifrado

Un sistema de cifrado se dice que es de *llave secreta*, también conocido como *cifrados simétricos*, si $\mathbf{K_1} = \mathbf{K_2}$, y es de *llave pública* o *asimétrico* si $\mathbf{K_1} \neq \mathbf{K_2}$.

Los sistemas de cifrado más usados a través de la Historia han sido de llave secreta y muchos de ellos fueron bastante robustos para su época. Entre estos sistemas se cuentan el de Julio César, el Vigenère (que tardó más de dos siglos en que se pudiera "romper"), la Máquina Enigma, el sistema DES ([6]), y más recientemente, el sistema AES (Advanced Encription Standard, [4]). Varios de los sistemas de llave secreta, como los mencionados anteriormente usan permutaciones en su diseño, además de otros conceptos matemáticos. Por ejemplo, el sistemas DES usa resultados de las llamadas funciones *Booleanas* y las cajas de substitución (*S*-boxes); el sistema AES usa entre otras cosas la estructura y aritmética de los campos finitos.

Cabe mencionar que la criptografía de llave pública es bastante reciente y data de mediados de la década de 1970, cuando Diffie y Hellman introdujeron este concepto ([8]). Actualmente este tipo de cifrado tiene una gran cantidad de aplicaciones como la firma y ensobretado digital. Entre los sistemas de cifrado de llave pública más comunes, se puede mencionar al RSA (Rivest-Shamir-Adleman, 1975, [19]), el cual usa resultados básicos de Teoría de Números como los Teoremas de Fermat y Euler, la función ϕ de Euler y residuos cuadráticos, entre otros. La robustez de este sistema radica, sobre todo, en el hecho de que computacionalmente no es factible determinar en un tiempo razonable si un número entero, del orden de 150-200 dígitos es primo, y si éste es compuesto, determinar sus factores. Recientemente ha circulado un algoritmo (denominado PRIME) que detecta en tiempo polinomial si un entero es o no un número primo ([1]).

El otro sistema de llave pública que ha estado tomando gran impulso en los últimos años es el basado en el grupo de puntos racionales de una curva elíptica definida sobre un campo finito, el cual fue introducido en forma independiente por N. Koblitz ([12] y V. Miller [18]) a mediados de la década de 1980. La robustez de este sistema de cifrado radica principalmente en la dificultad de resolver el Problema del Logaritmo Discreto sobre curvas elípticas ([17]). Como es obvio inferir, la geometría algebraica y campos finitos, juegan un papel muy importante en este sistema de cifrado.

En las siguientes secciones se darán algunos ejemplos de sistemas de cifrado y se describirá brevemente una aplicación de la criptografía de llave pública.

¿Qué ofrece la criptografía?

Una de las características de la criptografía es proporcionar los siguientes servicios en el manejo y seguridad de la información:

1. *Privacidad o confidencialidad*: mantener el contenido de la información fuera del alcance de las entidades no autorizadas.
2. *Integridad*: la información no debe ser alterada por entidades no autorizadas.
3. *Autenticación*: determinar la validez de la información así como la legitimidad del emisor.
4. *No-repudiación*: prevenir la negación de un compromiso o acción realizada.

A partir de los objetivos mencionados anteriormente se derivan otros, entre los que se pueden mencionar:

- Firma digital
- Autorización
- Validación
- Control de acceso
- Certificación
- Anonimato
- Revocación

Ejemplos

A continuación, a manera de ilustración se presentan dos ejemplos sencillos de sistemas de cifrado de llave secreta, uno de ellos muy elemental para nuestros días, pero que en su época fue muy robusto y usado por Julio César, y el sistema Vigenère el cual estuvo vigente por dos siglos. Brevemente se describirá el sistema de cifrado de llave pública RSA, basado en resultados clásicos de Teoría de Números tales como aritmética modular, función de Euler, Teoremas de Fermat y Euler, entre otros.

Cifrado de Julio César

Para comenzar sea $A = \{A, B, C,..., X, Y, Z\}$ el alfabeto usual para escribir el texto normal (en este caso de 26 letras), y sea $C = \{a, b, c,..., x, y, z\}$ el alfabeto que se usará para cifrar. Los elementos de ambos alfabetos se numeran del 0 al 25, es decir, se establece una biyección con los enteros módulo 26, $\mathbb{Z}_{26}$. Si $0 \leq k \leq 25$ se define:

$$E_k : A \to C,\ E_k(\alpha) = \alpha + k$$

La Historia dice que Julio César usó este cifrado con $k = 3$ ([10]). Así, por ejemplo, si se desea cifrar la letra C con este método se tiene: $E_3(C) = 2 + 3 = 5$, es decir,

$$E_3(C) = f$$

Por consiguiente el texto "GRACIAS" queda cifrado como "judfldv".

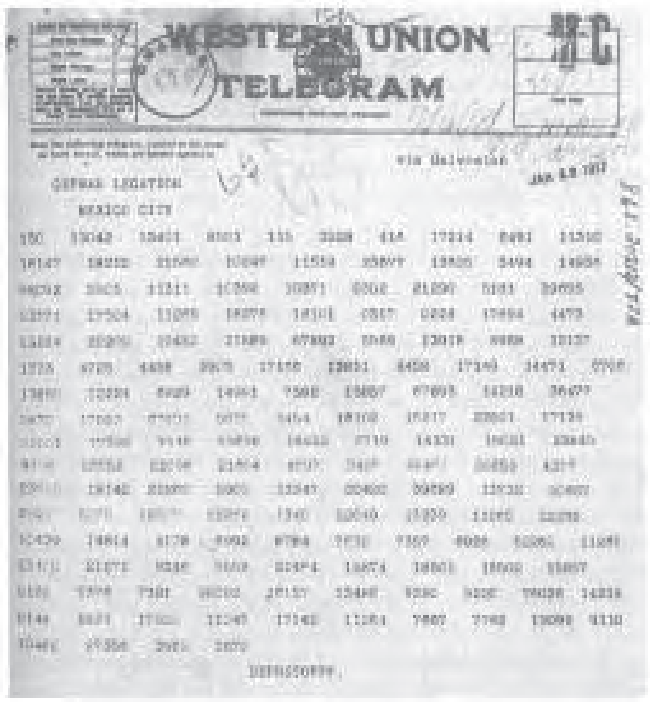


Fig. 2. The Zimmermann telegram, as forwarded by von Bernstorff, the German Ambassador in Washington, to Eckhardt, the German Ambassador in Mexico City.

Como es de esperarse, la aritmética se realiza módulo 26. Por ejemplo la letra "Z" quedará cifrada como "c" ya que $E_3(25) = 25 + 3 = 2$ módulo 26.

Si ahora se toma la llave $k = 17$, el texto "GRACIAS" queda cifrado como "vhprxph".

El cifrado de Julio César es un ejemplo de cifrado *monoalfabético*. Un ejemplo de cifrado *polialfabético* es el Vigenère (Siglo XVI), el cual se ilustra a continuación (el lector interesado puede ver más detalles en [17], [21], [22]).

Cifrado de Blaise Vigenère

Dado un entero m, se elige una llave K con m caracteres cada uno de ellos correspondiendo a un alfabeto, y se cifran m caracteres del texto original a la vez. Veamos un ejemplo:

Sea $m = 6$ y sea K= "MEXICO" la llave que corresponde, con la asignación que se hizo al alfabeto, a la colección (12, 4, 23, 8, 2, 14). Supóngase que se desea cifrar el texto "AL NORTE DE MEXICO". A este texto se le asocian los números de acuerdo con la asignación que se hizo al alfabeto y se agrupa en bloques de 6 caracteres (sin contar los espacios en blanco):

0	11	13	14	17	19
4	3	4	12	4	23
8	2	14			

A cada renglón del arreglo anterior se le suma la colección (12, 4, 23, 8, 2, 14) que corresponde a la llave K, ("coordenada por coordenada" y reduciendo módulo 26), obteniéndose:

12	15	10	22	19	7
23	7	1	20	6	11
20	6	11			

Por lo tanto, el texto cifrado es: "mpkwt hxhbu glugl"

En general, se puede decir lo siguiente: si $\mathbf{K} = (k_1, k_2, \cdots, k_m)$ es la llave de longitud m, el texto original se agrupa en bloques de longitud m. Cada bloque $\mathbf{T} = (a_1, a_2, \cdots, a_m)$ del texto original se cifra de la siguiente manera:

$$e_K(T) = (k_1 + a_1,\ k_2 + a_2,\ \cdots,\ k_m + a_m)$$

con la aritmética (modular) de $\mathbb{Z}_{26}$. Para descifrar, se realiza la operación inversa ("resta"):

$$d_K(b_1,\ b_2,\ \cdots,\ b_m) = (b_1 - k_1,\ b_2 - k_2,\ \cdots,\ b_m - k_m).$$

Un bonito ejercicio es realizar un criptoanálisis del sistema de cifrado Vigenère, es decir, a partir de un texto cifrado con este método, recuperar el texto original.

El cifrado RSA

El sistema de cifrado RSA, toma el nombre de las iniciales de las personas que lo diseñaron: Rivest, R., Shamir, A., Adleman, L.N. Es un sistema de llave pública y hasta la fecha el más popular, el cual se usa en prácticamente todas las aplicaciones donde se requiere un sistema de esta naturaleza. Para mayores detalles sobre este sistema el lector puede consultar el trabajo original de Rivest-Shamir-Adleman ([19]) o bien, [5], [17], [20], [22], entre otros.

Si $n > 1$ es un entero, $\mathbb{Z}_n$ denota al anillo de enteros módulo n y $\mathbb{Z}_n^*$ a su grupo (multiplicativo) de unidades cuyo orden es $\varphi(n)$, la función *phi* de Euler. En general cuando uno piensa en el anillo $\mathbb{Z}_n$, el entero n es "pequeño". Para construir el sistema de cifrado RSA, el entero n debe ser "grande", del orden de 150-200 dígitos.

A continuación se proporcionan, en forma general, los elementos necesarios para el sistema de cifrado RSA.

1. Sea $n = pq$ con p y q dos primos distintos (para cuestiones prácticas, éstos son del orden de 150-200 dígitos).
2. Sea $e \in \mathbb{Z}_n^*$ una unidad en el anillo de enteros modulares $\mathbb{Z}_n$, es decir, e y n son primos relativos (o cualquier representante de e), y sea $d \in \mathbb{Z}_n^*$ el inverso (multiplicativo) de e. Obsérvese que debido a la unicidad del inverso, la pareja (e, d) es única.
3. Considerando que la información a cifrar se ha identificado con elementos del anillo $\mathbb{Z}_n$, la función de cifrado (encriptamiento) es la siguiente:

$$E_e : \mathbb{Z}_n \to \mathbb{Z}_n$$
$$E_e(M) = M^e$$

4. Para recuperar la información original, se usa el entero d, la otra parte de la llave, y se aplica la función $D_d x = x^d$ al mensaje cifrado M, es decir,

$$D_d(m) = D_d(E_e(M)) = M^{ed} = M$$

dado que d es el inverso de e, las funciones E_e y D_d son inversas una de la otra.

En este caso se hacen públicos n y d. La entidad emisora **A** guarda en secreto la llave para cifrar e. Si una entidad **B** desea enviar información cifrada a la entidad **A**, **B** cifra el texto original con la llave pública, d, de **A** y debido a que la pareja (e, d) es única, sólo la entidad **A** puede recuperar el texto original usando su llave privada e.

A continuación se dará un ejemplo sencillo para ilustrar el funcionamiento del sistema RSA. Para este propósito el entero n se tomará "pequeño" de tal manera que el lector pueda efectuar las operaciones sin necesidad de hacer uso de una computadora, basta con una calculadora de bolsillo.

Sean $p = 71$, $q = 167$ y por lo tanto $n = pq = 11{,}857$. Supóngase que el mensaje que se desea cifrar es SI, el cual usando la identificación natural del alfabeto con los enteros módulo 26, la letra S se identifica con 19 y la letra I con 9. Por consiguiente, SI se identifica con $19(26) + 9 = 503$, usando base 26.

Sea $e = 117 \in \mathbb{Z}_{11{,}857}^*$, la llave para cifrar y $d = 9{,}733 \in \mathbb{Z}_{11{,}857}^*$ el inverso (multiplicativo) de e, la llave para descifrar. La entidad emisora envía:

$$(\mathrm{SI})^e = (503)^{117} \mathrm{mod}.n = 3702 = 5(26)^2 + 12(26) + 10 = \text{"EJL"}.$$

La entidad receptora recupera el mensaje original realizando las siguientes operaciones:

$$(\mathrm{ELJ})^d = (3702)^{9733} \mathrm{mod}.n = 503 = \text{"SI"}.$$

Cabe mencionar que la seguridad del sistema RSA radica principalmente en el hecho de que computacionalmente es difícil determinar la factorización de un número entero (grande). En las últimas décadas varios grupos de investigadores se han dado a la tarea de resolver este problema ([15]). Recientemente ha circulado un algoritmo que asegura determinar si un entero racional es primo, en tiempo polinomial ([1]).

Otro de los problemas difíciles de resolver computacionalmente es el llamado Problema del Logaritmo Discreto (PLD):

Si G es un grupo cíclico finito con generador g y $x \in G$, determinar el entero α tal que $x = g^{\alpha}$.

Otro de los sistemas de cifrado interesantes es el de ElGamal ([9], [17]) cuya seguridad está basada en el Problema del Logaritmo Discreto sobre campos finitos. El sistema de cifrado definido sobre el grupo de puntos racionales de curvas elípticas definidas en campos finitos también basa su seguridad en este problema ([11], [17]).

Una de las desventajas del sistema RSA es que debido a su lentitud por la aritmética que tiene que realizar, no se usa para cifrar grandes volúmenes de información. En situaciones prácticas, los sistemas de cifrado que se usan son *híbridos*, es decir, uno de llave secreta (por ejemplo DES, triple DES, AES, etc.) y uno de llave pública (por ejemplo RSA o bien el de curvas elípticas). El sistema de cifrado de llave pública se usa por ejemplo para comunicar llaves de sesión y el de llave secreta para cifrar los volúmenes de información.

Cifrado sobre curvas elípticas

Las curvas elípticas han jugado un papel muy importante en diversas áreas de la Matemáticas entre las que se incluyen Variable Compleja, Teoría de Números, Topología y Geometría Algebraica, entre otras. A mediados de la década de los años 80, N. Koblitz ([12]) y en forma independiente V. Miller ([18]) introdujeron ideas sobre el uso del grupo de puntos racionales de dichas curvas sobre campos finitos, para definir un sistema de cifrado de llave pública. A partir de esas aportaciones varios grupos de trabajo de la comunidad internacional se han dedicado a un estudio más profundo de las curvas elípticas definidas sobre diversos tipos de campos finitos y a la aplicación de dichos sistemas de cifrado en diversos contextos, como es la comunicación inalámbrica y tarjetas inteligentes, entre otros. Cabe mencionar que este sistema, debido a sus ventajas como la longitud de sus llaves, está siendo un gran competidor del sistema RSA.

Debido a la falta de espacio y por requerir de algunos otros elementos, sobre todo matemáticos no definidos hasta el momento, no profundizaremos en la descripción de tales sistemas de cifrado. El lector interesado puede consultar, por ejemplo, [11], [12], [16], [18], [17].

Cabe mencionar que para implementaciones y usos prácticos de los sistemas de cifrado, tanto de llave secreta como de llave pública, es muy importante conocer la matemática detrás de ellos; sin embargo no es lo único, ya que la computación también es importante, entre otras cosas, para tener programas de cómputo que realicen en forma óptima los algoritmos de dichos sistemas. Para implementaciones en "hardware" también es importante la colaboración de personal en el área de electrónica.

Como el lector puede observar, hay varios elementos matemáticos, en particular de Teoría de Números y Curvas Elípticas, que intervienen de manera explícita e importante en el diseño de sistemas de cifrado de llave pública y que tienen aplicaciones interesantes en las actividades cotidianas. Desde este punto de vista también se puede decir que éstas son Matemáticas Aplicadas.

Algunas aplicaciones de la criptografía

Actualmente hay varias aplicaciones de la criptografía en diversas actividades de la vida cotidiana, como es por ejemplo en la banca y comercio electrónico, licitaciones públicas, declaración de impuestos por medio de internet, y en general donde hay necesidad de tener seguridad en el manejo de la información y que ésta no deba ser utilizada por entidades no autorizadas. A continuación se presentarán en forma breve algunas ideas generales sobre una aplicación de la criptografía de llave pública: la *firma digital*. Los lectores interesados en más detalles pueden consultar [17], [23], entre otros.

Supongamos que dos usuarios **A** y **B** desean intercambiar información usando un sistema de cifrado de llave pública (por ejemplo el sistema RSA o el de curvas elípticas). Sea $(K_{pu}(A), K_{pr}(A))$ el par de llaves del usuario **A**. Recordemos que esta pareja de llaves es única, es decir, hay una y sólo una llave $K_{pr}(A)$) que corresponde a $K_{pu}(A)$.

La firma digital de un texto es un bloque de información de tamaño fijo que se obtiene a partir del documento que se desea firmar por un procedimiento llamado "hashing" ([17]). Algunos autores suelen llamar "huella digital" a este bloque de información. Una de las características importantes de este bloque es que es único del documento, es decir, a la menor alteración que se le haga a dicho documento, por ejemplo cambiar un sólo "bit", su huella es totalmente distinta a la del documento antes de ser alterado. Otra de las propiedades de la "huella digital" es que la probabilidad de que haya otro documento con la misma huella es prácticamente cero. Si una entidad **A** desea enviar un documento firmado digitalmente a una contraparte **B**, la entidad **A** cifra la huella del documento con su llave privada y envía a la entidad **B** el texto y la huella cifrada. La entidad B recupera la huella usando la llave pública de la entidad **A** y aplicando el mismo procedimiento que usó **A** para obtener la huella del documento ("hashing"), si ambas huellas coinciden entonces se puede concluir la autenticidad del firmante y la integridad del documento.

Una de las aplicaciones de la firma digital es en la *autenticidad de las llaves públicas* por medio de las autoridades certificadoras así como también en los llamados *sobres digitales*, los cuales por falta de espacio no se describen en esta nota. Los lectores interesados pueden consultar [17], [23].

Conclusión

En el desarrollo de la Humanidad siempre ha sido importante tener seguridad en el manejo de la información. Actualmente, y sobre todo en los próximos años, esto será aún más importante. La *criptografía* o *cifrado de datos* es una herramienta que proporciona dicha seguridad. Los sistemas de cifrado que se usan actualmente, tanto de llave secreta como de llave pública, están fundamentados en resultados matemáticos muy interesantes de áreas como la Teoría de Números, Campos Finitos, Curvas Algebraicas, Álgebra Conmutativa, Combinatoria y funciones Booleanas, entre otros. De esta manera se puede decir que la criptografía, así como los códigos lineales detectores-correctores de errores, son Matemáticas Aplicadas. Otra dirección que está tomando mucho interés es la teoría de la información, computación, códigos y criptografía cuántica. En el manejo de la seguridad de la información convergen varias disciplinas como son la Matemática, Computación e Ingeniería Electrónica. A pesar de que los sistemas de cifrado se están usando en nuestro país en varias partes con diversas aplicaciones, entre las que se cuentan la banca y comercio electrónico, votación electrónica, declaración de impuestos, etc., aún no se tienen los suficientes recursos humanos altamente capacitados en esta línea de investigación y su parte operativa. Se comienzan a dar los primeros pasos en esta dirección y actualmente algunas instituciones académicas ya contemplan temas relevantes en sus planes de estudio. Esperemos que en un corto plazo el número de colegas interesados en esta área aumente y se consoliden aquellos grupos de trabajo que se están iniciando.

Referencias

[1] Agrawal, M., Kayal, N. Saxena, N. PRIMES is in P. http:// www.cse.iitk.ac.in/news/primality.html

[2] Ángel-Ángel J., Criptografía y Curvas Elípticas, Tesis (Maestría), Dpto. de Matemáticas, UAM-I, 1998.
[3] Bautista-Osorno M., Implementación de un sistema de cifrado de llave pública basado en el problema del logaritmo discreto para curvas elípticas, Tesis (Maestría), Posgrado en Ciencias e Ingeniería de la Computación, UNAM, 2002.
[4] Daemen, J., Rijmen, V., *The Design of Rijndael: The AES-Advanced Encryption Standard*, Information Security and Cryptography, Texts and Monographs, Springer Verlag, 2001.
[5] Denning, D.E.R. *Cryptography and Data Security*, Addison-Wesley, 1982.
[6] Data Encryption Standard. FIPS Publ.46-I. National Bureau of Standards, Washington, D.C., 1987.
[7] Díaz-Santiago, S. El sistema criptográfico RSA, Proyecto de Investigación, Dpto. de Matemáticas, UAM-I, 1998.
[8] Diffie, W. and Hellman, M. New directions in cryptography. *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644-654, 1976.
[9] ElGamal, T. A public key cryptosystem and signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, vol. IT-31, pp. 469-472, 1985.
[10] Kahn, D. *The Codebreakers*, Scribner, New York, 1996.
[11] Koblitz, N. *Algebraic Aspects of Cryptography*, Algorithms and Computation in Mathematics, vol. 3, Springer Verlag, 1998.
[12] Koblitz, N. Elliptic curve cryptosystem, *Math. Comp.* 48, pp.203-209, 1987.
[13] Koblitz, N. *A Course in Number Theory and Cryptography*, 2nd. ed., Springer Verlag, 1994.
[14] Koblitz, N., Menezes, A., Vanstone, S.A., The state of elliptic curve cryptography, *Designs, Codes and Cryptography*, 19, pp. 173-193, 2000.
[15] Lenstra, A.K., Manasse, M.S., Factoring with two large primes, *Mathematics of Computation*, 63, pp. 785-798, 1994.
[16] Menezes, A. *Elliptic Curve Public Key Cryptosystem*, Kluwer Academic Publ., 1993.
[17] Menezes, A., van Oorschot, P., Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, 1996.
[18] Miller, V. Uses of elliptic curves in cryptography, *Lecture Notes in Computer Sciences* (Advances in Cryptology-CRYPTO'85), 218, pp. 417-426, 1986.
[19] Rivest, R., Shamir, A., Adleman, L.N., A method for obtaining digital signature and public-key cryptosystems, *Communications of the ACM*, 21, pp. 120-126, 1978.
[20] Schneider, B. *Applied Cryptography*, John Wiley & Sons, New York, 1996.
[21] Singh, S. *The code book*, Anchor Books, Random House, Inc. 1999.
[22] Stinson, D.R. *Cryptography: Theory and Practice*, CRC Press, 1995.
[23] Vega, G. Firmas digitales, *Enter@te*, Internet, Cómputo y Telecomunicaciones, DGSCA, Suplemento mensual de Gaceta UNAM, Número 12, Sept. 2002.
[24] Algunos sitios de interés:

http:/www.rsa.com
http://www.ftech.net/ monark/crypto
http://www.dean.usma.edu/math/resource/pubs/cryptolo
http://www.qubit.org
http://theory.lcs.mit.edu/ rivest
http://www.iacr.org
http://www.certicom.com
http://www.digicash.com
http://www.cryptography.com
http://www.nist.gov/aes

A la Comunidad Matemática del país, a los colegas responsables de Proyectos de Investigación

El XXXVI Congreso Nacional de la Sociedad Matemática Mexicana se llevará a cabo en la Universidad Autónoma del Estado de Hidalgo en la ciudad de Pachuca, Hidalgo, durante los días 12 al 17 de octubre. Aunque consideramos que es un congreso de buen nivel académico, la Junta Directiva de nuestra sociedad está buscando mecanismos para elevarlo aún más. Uno de los factores que impactan el nivel de una sesión es contar con conferencias impartidas por especialistas reconocidos mundialmente. La Sociedad no tiene recursos suficientes para invitar conferencistas extranjeros en un buen número para cubrir todas las áreas. Por tal motivo les hacemos una invitación a que consideren dentro de la programación de sus Proyectos de Investigación, incluir a uno o varios de sus invitados en el mes de octubre y promover que participen en el Congreso Nacional de la SMM.

Esperamos que esta recomendación les parezca razonable y apoyen las actividades académicas de nuestra Sociedad.

Junta Directiva de la Sociedad Matemática Mexicana

Richard Gordon Wilson: Semblanza de un matemático

Mikhail Tkachenko
Universidad Autónoma Metropolitana, Iztapalapa.
mich@xanum. uam.mx

Me acuerdo perfectamente bien del verano del 1993, fue la primera vez que ví a Richard Wilson en persona, buscándome entre la multitud, en el aeropuerto internacional de la Ciudad de México. Ya la primera impresión me decía que íbamos a trabajar con una persona muy cortés, respetable y eficiente. En aquel entonces no podía ni imaginar que casi diez años después tuviera el honor de aceptar la invitación de la Sociedad Matemática Mexicana de escribir unas líneas sobre mi querido colega y amigo. Estos diez años me regalaron la valiosa posibilidad de conocer a Richard mucho mejor y disfrutar de las charlas con él tanto de matemáticas como "de la vida".

Al parecer nada predecía que Richard Wilson se establecería en México. Nació en Liverpool, Inglaterra, y bien podría ser cuate de los Beatles, si no fuera por su vocación por las Ciencias Exactas. Al terminar la maestría en su ciudad natal (con honores de primera clase), Richard optó por continuar sus estudios en la Universidad de Texas, en Austin, donde obtuvo el grado de doctor en Filosofía. Al inicio, el escogió la Física como su especialidad, estudiando la teoría de la relatividad, pero pronto se dio cuenta de que lo atraían mucho más las matemáticas puras, especialmente la Topología. Ahí mismo, Richard inició su carrera como profesor. El año siguiente, después de doctorarse, trabajó como profesor asociado en la Carleton University en Ottawa, Canadá. En aquel entonces Richard ya estaba casado y según Elda Alva de Wilson, la elegante y muy hospitalaria esposa de Richard, "los Wilson" recuerdan dos hechos inolvidables en Canadá: el nacimiento de su hija y mucha, muchísima nieve, hasta los techos.

El siguiente cambio de residencia acerca al matrimonio a la tierra natal de Elda, México. Al terminar el año académico en Canadá, Richard obtiene un nuevo puesto en la Universidad de Puerto Rico en Mayagüez. Ahí, creo, Richard tuvo sus primeras lecciones de español, aunque daba las clases en inglés.

En 1973, por decreto gubernamental se crea una nueva institución de educación superior en México, la Universidad Autónoma Metropolitana, más conocida como la UAM. Richard recibe la invi-

Richard Wilson

tación para formar parte de la UAM, acepta y se incorpora a la planta académica de la Unidad Iztapalapa en el año 1974. Desde entonces empieza para Richard Wilson un incansable trabajo, sin interrupción alguna, en el Departamento de Matemáticas de la UAM-Iztapalapa; el próximo año la UAM, tendrá oportunidad de celebrar el trigésimo aniversario de la permanencia de uno de sus más destacados profesores.

Muchos académicos y estudiantes conocen a Richard Wilson por su impecable desempeño como profesor del Departamento de Matemáticas (¿cuántos alumnos habrán asistido a sus clases?), coordinador de la Maestría en Matemáticas o, mirando hacia atrás, coordinador del Doctorado en Ciencias de la División de Ciencias Básicas e Ingeniería, Jefe del Departamento de Matemáticas, etc. En cada uno de sus puestos, Richard Wilson ha mostrado su entrega y honestidad, cualidades que son notables y reconocidas en su persona.

Sin embargo, las labores cotidianas del Profesor Wilson en la UAM-Iztapalapa no se limitan sólo a las actividades de docencia y administración. Es muy reconocida su trayectoria científica: Richard Wilson es miembro del Sistema Nacional de Investigadores, nivel III, a partir del año 1993. La producción científica de Richard Wilson es amplia y profunda, el es autor o coautor de más de cincuenta artículos de investigación y un libro de texto.

Las áreas de interés científico de Richard Wilson son la Topología General y aplicaciones de métodos topológicos a las gráficas en computación, la cual es una combinación muy interesante y con un gran potencial de desarrollo. Los resultados científicos obtenidos por él se publican, en su mayoría, en revistas internacionales de prestigio (basta mencionar algunas: Proceedings of American Mathematical Society, Journal of the London Mathematical Society, Mathematische Zeitschrift, Canadian Mathematical Bulletin, Topology and its Applications, Discrete and Computational Geometry, etc.). En uno de sus artículos más elaborados [1], escrito junto con otro matemático distinguido del Instituto de Matemáticas de la UNAM, Víctor Neumann-Lara, Richard presentó un método muy sutil de reordenamiento de espacios linealmente ordenados que permite evitar "los huecos" en el espacio. En 1993, junto con el famoso matemático canadiense Steven Watson, Richard empezó la investigación de los espacios que admiten extensiones densas y conexas. Desde entonces, el tema se ha enriquecido con más de veinte artículos y, más de la mitad de ellos, son el resultado de la colaboración de Richard Wilson con otros matemáticos mexicanos y extranjeros. La importancia del tema se puede explicar en pocas palabras. Las dos propiedades básicas de los espacios topológicos son la compacidad y la conexidad (sin olvidarnos de la metrizabilidad). Uno de los teoremas de más impacto en la Topología General dice que cualquier espacio completamente regular admite una compactación, es decir, se encaja como subespacio denso en un espacio compacto Hausdorff. Si uno sustituye la compacidad por conexidad, surge el problema de encontrar una caracterización de los espacios que admiten una "conectificación". A pesar de los esfuerzos de varios especialistas, la solución del problema aún está lejos.

También es muy importante la investigación de Richard Wilson en la dirección de aplicar los métodos topológicos a la computación teórica y a la geometría computacional. En este tema, colabora con Ralph Kopperman, un reconocido matemático de Nueva York. Los resultados obtenidos por Richard y Ralph gozan de buena aceptación por los investigadores del área y muestran la creciente tendencia de mayor interacción entre las ramas de matemáticas "puras" y "aplicadas".

Otro rasgo muy importante de Richard Wilson es su habilidad de animar a la gente y establecer contactos científicos duraderos. Él fundó el Área de Topología del Departamento de Matemáticas, y fue el primer Jefe de ésta durante los años 1980-1987. En el año 1997, el Área de Topología ganó el premio de la División de CBI por los mejores resultados en la investigación y en la formación de recursos humanos. El profesor Richard colabora en tareas de investigación con matemáticos de Brasil, Estados Unidos de América, Canadá, Italia, Rusia y, por supuesto, de México. La reputación científica de Richard Wilson se refleja bastante bien en el hecho de haber realizado nueve estancias de investigación en el extranjero (Italia, Puerto Rico, EE.UU., Brasil, Nueva Zelanda). Además, ha presentado más de veinte ponencias en congresos internacionales e impartido 25 conferencias en otras instituciones.

La misión principal de cualquier Universidad es la acumulación y divulgación del conocimiento. Ya hemos visto la contribución de Richard Wilson en este campo. Por lo tanto, ahora es importante subrayar su labor en la formación de recursos humanos. Tres alumnos de Richard han obtenido bajo su supervisión, el grado de doctor en Matemáticas, y dos más el grado de maestro. Uno de ellos, Angel Tamariz Mascarúa de la UNAM, es ya un investigador internacionalmente reconocido.

Richard Wilson sigue siendo muy activo en los campos de investigación y formación de recursos humanos. En los últimos cinco años publicó quince artículos de investigación. La calidad de sus resultados es altamente reconocida por la comunidad internacional: Richard Wilson fue conferencista principal en la III Reunión Conjunta de American Mathematical Society y la Sociedad Matemática Mexicana en el año 1997. Durante el mismo periodo, dos alumnos de Richard Wilson presentaron sus tesis doctorales y, reciente y actualmente tiene un alumno en el programa doctoral.

Sería imperdonable no mencionar otra vocación de Richard Wilson: la observación de aves. En cada uno de sus viajes, aunque sea por razones matemáticas, él trata de encontrar tiempo y lugar para ampliar sus conocimientos del mundo de los pájaros. Más aún, Richard es autor del único libro dedicado a las aves del Distrito Federal [3]. En varias ocasiones yo tuve la suerte de acompañar a Richard en sus excursiones y escuchar sus explicaciones acerca de la peculiaridad y diversidad de los pájaros, aunque tengo que confesar que no he progresado mucho en esta área. Espero disponer de tiempo y de la paciencia de Richard para compartir esta especialidad.

Referencias

[1] V. Neumann-Lara y R. Wilson, When is a *LOTS* densely orderable?, *Topology and its Applications* **30** (1988) 225-235.

[2] S. Watson y R. Wilson, Embedding in connected spaces, *Houston J. Math.* **19** (1993) 469-481.

[3] R. Wilson, *The birds of Mexico City: An annotated check-list and bird-finding guide,* BBC Printing graphics, Hamilton, Ontario, Canadá, 1993.

BOLETÍN

BOLETIN DE LA SOCIEDAD MATEMATICA MEXICANA
TERCERA SERIE

INFORME 1995 - 2002

Desde el inicio de la tercera serie del Boletín de la Sociedad Mexicana a la fecha he desempeñado el cargo de Editora General de esa revista. Ha sido un honor y un placer colaborar con éste, que considero uno de los proyectos más importantes de la comunidad matemática mexicana. La calidad de nuestra revista es un reflejo fiel de la madurez de nuestra comunidad.

Hoy, después de ocho años de labor intensa, considero que es tiempo de que otro miembro de la comunidad me sustituya en el cargo y le dé un nuevo impulso a nuestra revista. Por ello tomé la decisión de presentar mi renuncia.

Este informe pretende dejar constancia de la labor realizada por todos los involucrados con el quehacer del Boletín durante estos ocho años.

LOS ORÍGENES

LA TERCERA SERIE DEL BOLETÍN DE LA SOCIEDAD MATEMÁTICA MEXICANA inicia en 1995 a iniciativa del entonces presidente de la Sociedad Matemática Mexicana, el Dr. José Carlos Gómez Larrañaga.

El objetivo era dar un nuevo impulso a esa publicación a fin de que la comunidad matemática mexicana contara con una revista de investigación de calidad y circulación internacional, que incluyera a todas las áreas de matemáticas puras y aplicadas, y que reflejara los avances de dicha comunidad en su conjunto. Aspectos importantes de este proyecto eran lograr que el Boletín apareciera de manera regular, con una periodicidad de dos números por año, y asegurar la eficacia en la calidad y en los tiempos del proceso de arbitraje.

Para ello se nombró un Consejo Editorial integrado por investigadores mexicanos que representaran a buena parte de los campos de las Matemáticas que se cultivan en México. Dicho Consejo se subdividió en subcomités, cada uno de ellos con un coordinador. Los subcomités son los siguientes:

1) Álgebra, teoría de los números, geometría algebraica y álgebra numérica.
2) Análisis real, análisis complejo, análisis armónico y análisis funcional.
3) Ecuaciones diferenciales, sistemas dinámicos, análisis nolineal, métodos numéricos y teoría del control.
4) Topología algebraica, topología en dimensiones bajas y geometría.
5) Probabilidad, estadística y control óptimo.
6) Fundamentos, lógica y teoría de la computación, gráficas, combinatoria y topología general.

Los coordinadores de los subcomités han sido, sucesivamente, en el Subcomité 1: José Antonio de la Peña, Raymundo Bautista, Rafael Villarreal y Luis Verde, en el Subcomité 2: Michael Porter y Salvador Pérez Esteva, en el Subcomité 3: Jorge Ize, en el Subcomité 4: Francisco González Acuña, José Seade y Adolfo Sánchez Valenzuela, en el Subcomité 5: Luis Gorostiza, y en el Subcomité 6: Víctor Neumann y Richard Wilson.

Como editores generales hemos compartido la responsabilidad Enrique Ramírez de Arellano y Mónica Clapp.

LOS LOGROS

LA TERCERA SERIE DEL BOLETÍN DE LA SOCIEDAD MATEMÁTICA MEXICANA

- Aparece puntualmente desde su primer número (abril de 1995).
- Cuenta con el reconocimiento de la comunidad matemática nacional e internacional, lo cual se refleja en el número de artículos sometidos a publicación (véanse Tablas 1 y 2).

- Desde el año 2000 la revista aparece incluida en los listados del Science Citation Index del Institute for Scientific Information.
- Está incluida en el Índice de Revistas Mexicanas de Excelencia Científica y Tecnológica del CONACYT, lo que le ha permitido contar con un apoyo financiero de dicha institución.
- Los artículos enviados a consideración son sometidos a un estricto proceso de arbitraje por especialistas nacionales e internacionales.
- El proceso de arbitraje se desarrolla en un tiempo promedio de 6.5 meses.

Todo esto ha sido posible gracias al apoyo decidido de las sucesivas Juntas Directivas de la Sociedad Matemática Mexicana y de las instituciones patrocinadoras, especialmente del Instituto de Matemáticas de la UNAM, del CINVESTAV del IPN, de la UAM-Iztapalapa y del CONACYT, al trabajo serio y comprometido de los sucesivos Consejos Editoriales, especialmente de los coordinadores y de Enrique Ramírez de Arellano con quien he compartido el cargo de Editor General, y al apoyo profesional de nuestro equipo de edición técnica. Pero lo logrado hasta ahora es fruto sobre todo de la confianza depositada por los matemáticos mexicanos que han enriquecido nuestra revista con excelentes artículos. A todos, muchas gracias. Ha sido, como dije al principio, un placer y un honor colaborar con el Boletín de la Sociedad Matemática Mexicana.

27 de enero de 2003
Mónica Clapp

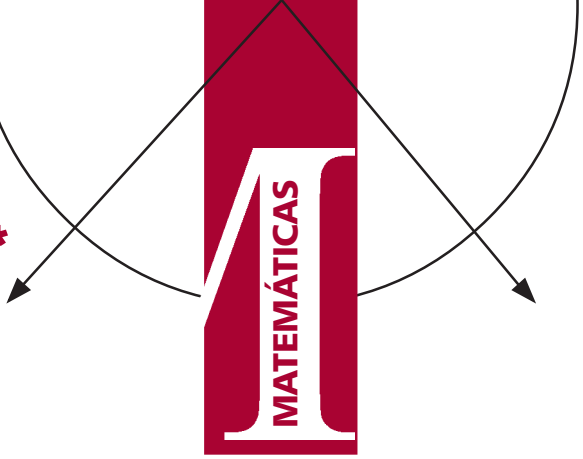
Tabla 1. Volúmenes y artículos publicados.

Año	Volumen	Número	Páginas	Artículos de Invest.	Artículos Panorámicos	De autores nacionales
1995	1	1	85	4	1	2
1995	1	2	61	6	0	3
1996	2	1	64	5	0	3
1996	2	2	81	8	0	4
1997	3	1	192	11	1	8
1997	3	2	162	14	0	8
1998	4	1	158	9	0	3
1998	4	2	132	11	6	6
1999	5	1	222	14	2	9
1999	5	2	212	12	2	5
2000	6	1	150	8	1	7
2000	6	2	130	11	0	7
2001	7	1	136	11	0	5
2001	7	2	124	6	1	2
2002	8	1	116	11	0	4
2002	8	2	126	10	0	9

Tabla 2. Artículos recibidos por subcomité por año en los últimos 4 años.

	Subcomité 1	Subcomité 2	Subcomité 3	Subcomité 4	Subcomité 5	Subcomité 6	Total	De autores nacionales
1999								
Recibidos	9	7	6	2	10	7	41	26
Aceptados	7	3	2	2	8	4	26	15
Rechazados	2	4	4	0	2	3	15	11
2000								
Recibidos	6	11	3	2	3	4	29	14
Aceptados	4	1	0	1	3	2	11	6
Rechazados	2	10	3	1	0	2	18	8
2001								
Recibidos	8	9	4	3	7	5	36	11
Aceptados	3	6	0	0	3	4	16	8
Rechazados	5	3	4	3	2	1	18	3
En proceso	0	0	0	0	2	0	2	0
2002								
Recibidos	10	12	2	9	14	4	51	25
Aceptados	3	3	0	7	3	0	20	12
Rechazados	4	4	0	2	1	1	12	5
En proceso	3	5	2	0	10	3	19	8

Una flor que no se seca y que su aroma convence,* es la reina de las ciencias en la región hidalguense



Orlando Ávila Pozos
Director del Área Académica de Matemáticas
Universidad Autónoma del Estado de Hidalgo
avilap@uaeh.reduaeh.mx

Antecedentes

Enclavada en la parte septentrional de Mesoamérica, la región que hoy ocupa el Estado de Hidalgo presenció el florecimiento del imperio fundado por los toltecas, herederos directos de la cultura teotihuacana, y de su capital Tula. El gran esplendor alcanzado por los toltecas se manifiesta en sus bellos estilos arquitectónicos y escultóricos y en la gran influencia que éstos tuvieron sobre el desarrollo de la mayor parte de los pueblos mesoamericanos. No tenemos conocimiento del grado de complejidad que alcanzaron las matemáticas teotihuacanas y toltecas pero, siendo las matemáticas un buen índice para conocer el avance de cualquier sociedad, nos parece muy difícil imaginar el gran desarrollo social, económico y artístico que lograron esas civilizaciones, sin un desarrollo matemático de la misma magnitud.

En la época colonial, destaca la obra del científico hidalguense fray Diego Rodríguez (1596-1668), nacido en Atitalaquia, población del actual Estado de Hidalgo. Entre las principales obras de fray Diego Rodríguez se encuentra una *Geometría*, un *Tratado de las Equaciones,* y un tratado *De los Logaritmos y Aritmética,* en donde elabora sus propias tablas de logaritmos de funciones trigonométricas –las primeras en México de que se tiene conocimiento– independientemente de las tablas que Edmund Gunter publicó por primera vez en 1620. Cabe mencionar que fray Diego participó en la solución de varios de los problemas que originaba la construcción del desagüe de la ciudad de México y que en 1638 determinó la longitud del valle de México, en relación al meridiano de París, con mayor precisión que Alejandro de Humboldt en 1803. Según Trabulse [T], "*el florecimiento científico en México del último cuarto del siglo XVII y cuyo más preclaro representante es Sigüenza y Góngora tuvo su origen, en buena medida, en la obra del padre Rodríguez".*

La Universidad Autónoma del Estado de Hidalgo

Las raíces de la Universidad Autónoma del Estado de Hidalgo (UAEH) se encuentran en el Instituto Literario y Escuela de Artes y Oficios del Estado de Hidalgo (ILEH), fundado en la ciudad de Pachuca en febrero de 1869 [B] con el propósito de llenar el gran hueco educativo que dejó el Instituto Literario de Toluca, al fundarse el Estado de Hidalgo en enero de ese mismo año. La matrícula durante el primer año del ILEH fue de treinta y cinco alumnos y las primeras carreras profesionales que se ofrecieron fueron las de agrimensor, mecánico, minero, agricultor, veterinario, farmacéutico, comerciante, maestro de obras y estudios preparatorios en medicina y abogacía. Diez años después se ofrecieron también las ingenierías en topografía y minas. En 1890 el ILEH adoptó el nombre de Instituto Científico y Literario del Estado de Hidalgo (ICL), el cual, de 1921 a 1925, pasó a formar parte de la Universidad de Hidalgo, institución que incluía además a las escuelas: Normal, de Comercio, de Artes y Oficios, de Jurisprudencia y de Ingenieros. En 1925 la Universidad de Hidalgo desaparece y el ICL se desliga de las otras instituciones transformándose en la Universidad Autónoma del Estado de Hidalgo el 3 de marzo de 1961, por decreto oficial.

Para atender la creciente demanda educativa de la comunidad hidalguense, la UAEH ha incrementado significativamente sus programas académicos y actualmente tiene una matrícula cercana a treinta mil estudiantes, distribuidos en cuatro preparatorias y seis institutos: Artes, Ciencias Agropecuarias, Ciencias Básicas e Ingeniería (ICBI), Ciencias de la Salud, Ciencias Económico-Administrativas y Ciencias Sociales y Humanidades, que se encuentran ubicados en quince campus, con una oferta educativa de un bachillerato general, treinta y cinco licenciaturas, dieciocho maestrías y tres doctorados. Aunado a lo anterior, la UAEH ha dado recientemente un gran impulso a la investigación básica y aplicada; por ejemplo, en el ICBI se hace investigación en ciencias biológicas, ciencias computacionales, ciencias de la tierra, ciencias de los materiales y ciencias químicas, así como en ingeniería industrial y en matemáticas.

Actividad Matemática en la UAEH

Maestría en Matemática Educativa

Con el propósito de organizar el Programa Nacional de Formación y Actualización de Profesores de Matemáticas (PNFAPM) en el estado de Hidalgo, en 1985 se creó en la UAEH el Subnodo Regional de Matemática Educativa, encabezado por el M. en C. Juan Alberto Acosta Hernández, con base en un convenio tripartita entre la Universidad sede, la Secretaría de Educación Pública y el Centro de

* Del son "El Hidalguense" de Nicandro Castillo.

Investigación de Estudios Avanzados del IPN. En 1986 el PNFAPM tenía ochenta profesores de matemáticas inscritos: sesenta y uno de la UAEH y el resto de otras instituciones del estado. Los trabajos del PNFAPM originaron el proyecto de la Especialidad en la Enseñanza de las Matemáticas que se aprobó en septiembre de 1989, el cual derivó en el plan de estudios de la Maestría en Ciencias con Orientación en Educación Matemática, aprobado por el H. Consejo Universitario en enero de 1992. Esta maestría se modificó en 1998 y tomó el nombre de Maestría en Ciencias con Orientación en la Enseñanza de las Matemáticas. Hasta diciembre de 2002, las actividades de investigación del subnodo se concentraron en las siguientes líneas: desarrollo conceptual del cálculo, visualización en la matemática, desarrollo de modelos explicativos y uso de la tecnología educativa en la enseñanza de las matemáticas.

Licenciatura en Matemáticas Aplicadas

En junio de 2000 se creó el Área de Matemáticas Aplicadas del ICBI y su primera misión consistió en elaborar el Proyecto de la Licenciatura en Matemáticas Aplicadas (LIMA). Este proyecto fue aprobado por el H. Consejo Universitario en octubre de 2000. La primera generación de la LIMA inició sus actividades con cincuenta y ocho alumnos en julio de 2001. El plan de estudios de la LIMA es de nueve semestres y una de las características sobresalientes es su carácter interdisciplinario. En el tercer semestre los estudiantes eligen una de las cuatro subespecialidades siguientes: computación, economía, finanzas y biología.

Para incorporar estudiantes a la LIMA de la UAEH, el Área de Matemáticas Aplicadas ha difundido esta licenciatura en el Estado de Hidalgo, por medio de la radio y la televisión, así como de un intenso programa de conferencias que sus profesores imparten en los principales centros hidalguenses de enseñanza del nivel medio superior. Como resultado, cada una de las dos primeras generaciones ha tenido más de sesenta aspirantes. Por otro lado, para fortalecer las perspectivas académicas y de desarrollo profesional de los estudiantes de la LIMA, el Área de Matemáticas Aplicadas ha desarrollado un programa quincenal de conferencias de divulgación que, hasta la fecha, ha contado con la participación de más de treinta conferencistas procedentes de importantes centros académicos y de servicios tales como Banca BITAL, el Centro de Investigación y Docencia Económica, el CIMAT, el CINVESTAV, el Instituto Nacional de Salud Pública, el ITESM, la UAMI, la UDLA-P, la UNAM, la Universidad de Bath, la Universidad de California en Irvine, la Universidad de Princeton y la Universidad Veracruzana.

Investigación en Matemáticas

En diciembre de 2002 el H. Consejo Universitario aprobó la creación del Centro de Investigación en Matemáticas (CIMA) de la UAEH, el cual ha integrado al Área de Matemáticas Aplicadas y al Subnodo Regional de Matemática Educativa. Actualmente el CIMA cuenta con dieciocho profesores, nueve con doctorado, que desarrollan investigaciones en economía matemática, educación matemática, física matemática, teoría de números y teoría de operadores.

Es pertinente mencionar que, en virtud de que el CIMA seguirá creciendo, la UAEH ofrece una excelente oportunidad para aquellos matemáticos con grado de doctor, preferentemente miembros del SNI, que deseen desarrollarse de manera equilibrada tanto en la docencia como en la investigación y aplicación de las matemáticas.

Conclusión

Aunque el CIMA de la UAEH aún está en proceso de consolidar sus grupos de investigación y sus programas educativos de licenciatura y postgrado, los logros alcanzados en años recientes por el Área Académica de Matemáticas, no habrían sido posibles sin el apoyo decidido de sus autoridades universitarias, muy especialmente, del Lic. Juan Manuel Camacho Bertrán, actual Rector de nuestra Casa de Estudios.

Este es el escenario en el que la UAEH se prepara para dar una cordial bienvenida y ofrecer una estancia productiva y placentera a la comunidad matemática mexicana, durante la celebración en Pachuca de su XXXVI Congreso Nacional en octubre de 2003.

Referencias

[T] Trabulse, E. *El círculo roto*. Lecturas Mexicanas. No. 54. Fondo de Cultura Económica.

[B] Ballesteros, Víctor Manuel. *Breve Historia de la Universidad Autónoma del Estado de Hidalgo.* Raíces Hidalguenses. Editorial de la UAEH.

ANUNCIOS

II Congreso Internacional de Teoría de los Continuos
Facultad de Ciencias Físico Matemáticas
Benemérita Universidad Autónoma de Puebla

Julio 3 al 5 de 2003

Informes:

Raúl Escobedo (escobedo@fcfm.buap.mx)
Alejandro Illanes (illanes@matem.unam.mx)

The Aritmetic, Geometry and Topology of Algebraic Cycles.
IM-UNAM, Morelia, México

Junio 15–Julio 4, 2003

Informes:

Information: cycles@math.unam.mx

III Escuela de Matemáticas de América Latina y el Caribe
IM-UNAM, Morelia, México.

19–28 de agosto del 2003

Informes:

www.matmor.unam.mx/eventos/emalca/default.html

IV Escuela de Verano del Instituto de Matemáticas de la UNAM, Unidad Morelia

11 al 15 de agosto de 2003

Informes:

http://www.matmor.unam.mx/eventos/escuela

CARTA INFORMATIVA

SOCIEDAD MATEMÁTICA MEXICANA

Número 36,
Abril de 2003

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
syg@att.net.mx

PORTADA

Escalera Monumental, Palacio de Minería

SEGUNDA DE FORROS

Santa María Regla, Hgo.

TERCERA DE FORROS

Los prismas basálticos, San Miguel Regla; Molango, Hgo.