ALGUNAS TENDENCIAS ACTUALES EN MATEMATICA

Leopoldo Bertossi*

Doctor en Matemática. Universidad Católica de Chile.
Profesor e investigador de la Facultad de Matemática de esta Universidad.

Grandes tendencias de investigación en matemáticas son causadas por la aparición de *conjeturas*, es decir, de presuntos *teoremas* que exigen de la comunidad matemática una *demostración* o una refutación. Cuando se presentan, usualmente planteadas explícitamente por un matemático, muchos investigadores se ponen a trabajar incesantemente para resolverlas. Conjeturas y problemas abiertos han originado, a través de su solución o intentos de solución, grandes áreas de la matemática; y muchas ideas y técnicas desarrolladas con ese fin han adquirido vida propia, formando áreas importantísimas y consolidadas de ésta. El ejemplo más notorio es el de la conjetura de Fermat, aún no resuelta desde el siglo XVII, que ha motivado el desarrollo de muchos temas del álgebra abstracta.

No sólo famosas conjeturas causan grandes tendencias de investigación matemática; también nuevos resultados y el establecimiento de relaciones insospechadas entre distintas áreas de la matemática (o de la matemática con otras disciplinas del conocimiento) permiten descubrir vetas riquísimas de investigación en las cuales comienzan a trabajar de inmediato muchos matemáticos de todo el mundo. Es de esta manera que en matemática, tal como en las otras disciplinas científicas, se producen "modas". Sin embargo, por la naturaleza del conocimiento matemático estas teorías puestas de moda en algún momento no serán invalidadas en el futuro; se incorporarán al cúmulo de conocimientos matemáticos universalmente aceptados; y, en el peor de los casos, serán abandonadas como campo de trabajo de gran parte de la comunidad matemática cuando la parte medular de la veta se agote o permanezca invisible. No obstante, una eventual aplicación inesperada de esta teoría en hibernación podría hacerla revivir con pleno vigor.

A continuación veremos algunas tendencias de investigación matemática que, con seguridad, estarán vigentes por mucho tiempo y que se originaron —como expresamos— en nuevos resultados o en el descubrimiento de relaciones interdisciplinarias. Ellas fueron escogidas dentro del ámbito del interés matemático del autor: los fundamentos de la matemática, la computación teórica y la lógica matemática.

* *El autor agradece los valiosos comentarios de los profesores René Peralta, José López T., Javier Pinto y Darío Rodríguez.*

Análisis no estándar

En el siglo pasado, Cauchy y otros matemáticos dieron fundamentos sólidos al cálculo al eliminar de importantes conceptos de la matemática (como el de "límite") el uso de los número infinitesimales (números infinitamente pequeños) y de los números infinitamente grandes. Sin embargo, hasta hace poco se recurría —si es que no todavía— a textos de cálculo que hacían uso y hablaban de estos infinitesimales de naturaleza algo esotérica y de existencia no claramente compatible con las leyes (no discutidas) del cálculo. Esto se debía no sólo a la tradición, sino especialmente a que, a pesar de las objeciones que con fundamentos se les hacía, estos infinitesimales eran fácilmente intuibles por el matemático y proporcionaban a éste una poderosa herramienta heurística. Podemos decir, entonces, que la fundamentación del cálculo sin infinitesimales hecha por Cauchy fue correcta, pero no logró el propósito de erradicar de la práctica matemática el uso de éstos.

Fue en la década de los 60 que Abraham Robinson, usando resultados de la lógica matemática, creó el "análisis no estándar", el cual tenía fundamentos lógicos sólidos, permitía hacer cálculo como antes (permanecían las leyes indiscutidas) y, además, admitía la existencia y uso de infinitesimales y de números infinitamente grandes. Podemos hablar entonces de un cálculo enriquecido y lógicamente correcto.

Muchos matemáticos comenzaron a estudiar más en detalle este nuevo cálculo, y muchos otros comenzaron a buscar sus aplicaciones en áreas como la teoría de probabilidades, la física matemática, la economía matemática, etc. Los avances y éxitos fueron enormes: el análisis no estándar tenía más elementos y técnicas y, también, toda la fuerza heurística que aportaban los infinitesimales.

La aplicación del análisis no estándar en muchas áreas de la matemática ofrece un amplio campo de investigación, y es justificado esperar con optimismo grandes éxitos en este terreno.

Teoría de números y algoritmos

Un problema enfrentado por todos en algún momento de la educación básica es el de detección de primalidad de números

enteros positivos, es decir, el de, dado un número n, determinar si existen números enteros r y s distintos de uno, tales que n = r*s. Por supuesto, si el número n es "primo", la respuesta será negativa: sus únicos divisores son él mismo y uno. El problema de encontrar número r y s factor de n (y no sólo determinar su existencia) se llama "problema de factorización".

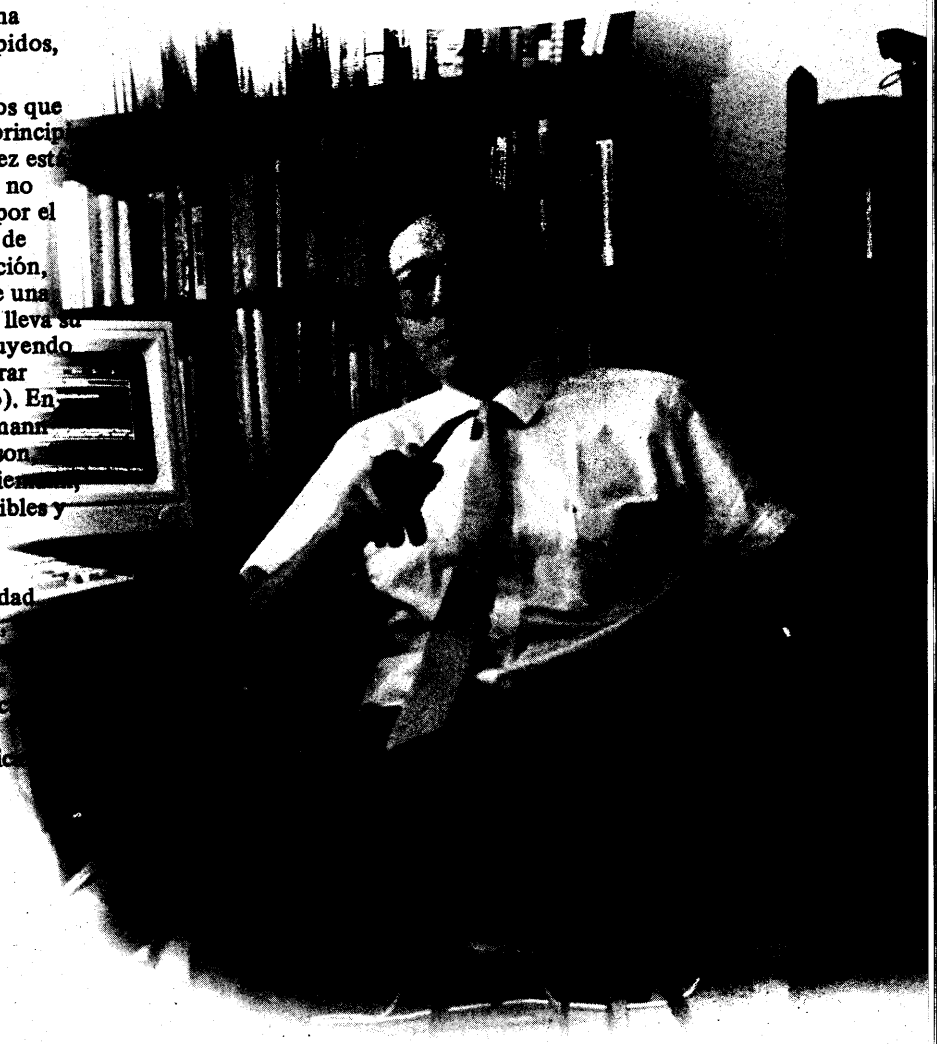
Actualmente no se conoce un algoritmo "rápido"** para resolver el problema de detección de primalidad; sólo se ha encontrado algoritmos "lentos". Sin embargo, existen "algoritmos rápidos probabilísticos" para resolver nuestro problema. Estos algoritmos probabilísticos, en una parte determinada de la ejecución, "eligen" al azar, digamos, 100 números enteros y los emplean en el resto de ella hasta responder sí o no a la pregunta sobre el número n. La respuesta la dan en tiempo corto. Estos algoritmos se pueden equivocar en la respuesta, pero la probabilidad de que lo hagan es más o menos $1/2^{100}$. A pesar de esta bajísima probabilidad de error, tendríamos aquí algoritmos rápidos, pero no infalibles

Hay modificaciones de estos algoritmos probabilísticos que los convierten en deterministas e infalibles, pero, en princip lentos. Sin embargo, en forma sorprendente, su rapidez est relacionada con un importante problema matemático no resuelto desde el siglo pasado, cuando fue planteado por el gran matemático alemán B. Riemann. En un artículo de 1859, Riemann formula una conjetura sobre la ubicación, en el plano de los números complejos, de las raíces de una cierta función de variable compleja (que actualmente lleva su nombre). Desde esa fecha, grandes matemáticos, incluyendo al propio Riemann, han tratado, sin éxito, de demostrar la conjetura (por supuesto, tampoco se la ha refutado). En 1976, G. Miller demostró que: si la conjetura de Riemann es verdadera, entonces estos algoritmos modificados son en realidad, rápidos. Si fuera válida la conjetura de Rie tendríamos, entonces, algoritmos deterministas, infalibles y rápidos para detectar primalidad.

Curiosamente, el problema de factorización es computacionalmente más complejo que el de primalidad Todos los algoritmos para resolverlo son lentísimos y hecho, ni siquiera hay algoritmos rápidos probabilíst la búsqueda de algoritmos para factorizar enteros má rápidos que los existentes, H. Lenstra, en 1984, conec manera inesperada este problema con la antigua y relativamente abandonada "teoría de las curvas elípti dando un nuevo auge a esta última.

La criptografía moderna –aquella basada en la teoría de números– es de indudable importancia práctica, pues tiene que ver con la codificación y decodificación numérica de información secreta. La seguridad de la mayoría de los método criptográficos modernos se basa en la presunta inexistencia de algoritmos rápidos para factorización de enteros. Vemos así otro aspecto relevante de la factorización rápida de enteros.

La importancia propia de estos temas y sus conexiones con la desafiante conjetura de Riemann y la teoría de las curvas elípticas han convertido a la teoría de números aplicada a la computación teórica y a la criptografía, en particular, en uno de los campos de investigación matemática más efervescentes; y es así como los expertos en teoría de números, por décadas postergados, están actualmente entre los matemáticos más cotizados.



*** Los conceptos de "algoritmo" ("algoritmo rápido" y "algoritmo lento") tienen una definición matemática precisa. Sin embargo, nos limitaremos a usarlos en forma intuitiva.*

Lógica matemática e inteligencia artificial

Uno de los propósitos de la inteligencia artificial es la creación de sistemas expertos computacionales que, tal como su nombre lo indica, se comporten como una persona experta en un tema. Esto comprende, para el sistema, las capacidades para almacenar información asequible, para hacer deducciones lógicas a partir de su base de conocimientos con el fin de responder a preguntas que se le formulen, para hacer uso del "sentido común", para aprender incorporando nueva información al sistema, para descubrir nuevos hechos.

En resumen, se espera que el sistema experto aprenda y razone como lo haría un ser humano en un área, posiblemente muy restringida, del conocimiento. Es claro que aquí surge un problema epistemológico fundamental: ¿cómo aprende, cómo razona, cómo descubre nuevos hechos una persona? Distintas posiciones filosóficas y científicas con respecto a estas preguntas conducirán a distintas concepciones de sistema experto; y, por lo tanto, el tema es inagotable.

En algunas áreas del conocimiento existen actualmente sistemas computacionales expertos que funcionan sobre la base de lenguajes de programación especialmente diseñados para hacer deducciones lógicas, a partir de una base de conocimientos que incluye datos propiamente tales y reglas lógicas de comportamiento del sistema (aquí surge el problema de representación lógica del conocimiento). Uno de estos lenguajes es el Prolog (programmation en logique). La lógica subyacente a éste y a otros lenguajes similares es la lógica de predicados de primer orden usual, que es la más popular y estudiada dentro de la lógica matemática (su capacidad para hacer demostraciones mecánicas —que es lo que hará un computador después de todo— y también su relativamente alto nivel de expresividad son especialmente útiles en nuestro contexto). Sin embargo, también hay otras lógicas creadas y estudiadas por lógicos matemáticos que extienden a la lógica usual o pueden coexistir con ésta (p.e., lógicas modales, lógica difusa, lógicas no monótonas, etc.), y que serán de gran importancia para el diseño de sistemas expertos en inteligencia artificial. Algunas de estas lógicas, además de las buenas propiedades deductivas de la lógica usual, permiten formalizar, en parte, el razonamiento con "sentido común" e incorporan cierta capacidad heurística, la capacidad de plantear conjeturas; en fin, capacidades que darían al sistema experto la posibilidad de descubrir nuevos hechos.

El estudio matemático y filosófico más profundo de estas lógicas, la creación de sistemas expertos computacionales que funcionen sobre la base de éstas y la aplicación de la lógica matemática en otras áreas de la inteligencia artificial —como el "planning" y la implementación computacional de lenguajes naturales— serán, sin duda, por mucho tiempo, campos de intensa investigación científica.