V-Encuentro de Teoría de Números
Octubre 11, 2023

CONFERENCISTAS

Valuation of sequences

Víctor Moll
(Tulane University)

Given an integer x and a prime p, the p-adic valuation of x is the highest power of p dividing x. It is denoted by $\nu_p(x)$. The goal of this talk is to present a variety of questions that have appeared in our of study of a fundamental question:

> *Given a prime p and a sequence of integers a_n, describe the sequence of valuations $\{\nu_p(a_n)\}$.*

An elementary formula of Legendre gives the p-adic valuation of factorials

$$\nu_p(n!) = \tfrac{1}{p-1}(n - s_p(n)),$$

where $s_p(n)$ is the sum of the integers of n in base p. From here, one can establish properties of the central binomial coefficients $\binom{2n}{n}$ (this is elementary) as well as those Catalan numbers $\frac{1}{n+1}\binom{2n}{n}$ (parts of this project are still open questions). The talk will present a collection of examples illustrating some of the techniques used as well as a variety of open questions.

Introducción a los grupos algebraicos y sus compactificaciones proyectivas

Pedro Montero
(Universidad Técnica Federico Santa María)

Un grupo G es un conjunto (no-vacío) dotado de una ley de composición interna asociativa y tal que existe un elemento neutro e inversos. Al agregarle una estructura geométrica adicional a dicho conjunto y a las funciones asociadas a la multiplicación e inversión, se obtienen grupos interesantes. Por ejemplo, si G es un espacio topológico (resp. variedad diferenciable) y las funciones son continuas (resp. diferenciables) entonces decimos que G es un grupo topológico (resp. grupo de Lie).

En esta charla, introduciremos rápidamente el concepto de variedad algebraica (afín o proyectiva) y luego la correspondiente noción de grupo algebraico. El resto de la charla estará dedicada a dar ejemplos de dichos objetos y de acciones de grupos algebraicos en variedades algebraicas. Finalmente, me concentraré en dos tipos especiales de grupos algebraicos que aparecen frecuentemente en problemas de investigación actual: los toros algebraicos y los grupos vectoriales. En ambos casos, daremos una idea de cómo lucen sus compactificaciones proyectivas.

Curvas algebraicas y seguridad en la red

Amalia Pizarro
(Universidad de Valparaíso)

En esta charla, revisaremos parte del impacto que han tenido (y siguen teniendo) las curvas elípticas e hiperelípticas en criptografía y algunas alternativas que se esperan, sean resistentes al ataque con procesadores cuánticos.

SESIÓN DE CHARLAS CORTAS

Métodos computacionales para la clasificación de polítopos de Fano suaves y aditivos

Fabián Levicán
(Pontificia Universidad Católica de Valparaíso)

Sean K un cuerpo algebraicamente cerrado, $\mathbb{G}_a^n$ su grupo aditivo, y X una variedad algebraica irreducible de dimensión n sobre K. Una acción aditiva es una acción (efectiva, regular) del grupo conmutativo unipotente $\mathbb{G}_a^n$ con una órbita abierta, y decimos que X es aditiva si admite una acción aditiva.

Las variedades de Fano suaves y aditivas [Hassett y Tschinkel, 1999] poseen propiedades aritméticas muy deseables. Si bien son difíciles de construir, existe un criterio reciente que permite hacerlo usando geometría tórica. La clasificación de estas variedades por métodos geométricos ha sido completada hasta dimensión 3, pero no en dimensiones superiores, debido a las limitaciones de los métodos teóricos. Existe otro criterio reciente que permite decidir si una acción aditiva sobre X es única (módulo isomorfismo con una acción normalizada) o no. Ambos criterios son, en esencia, combinatorios, y permiten diseñar algoritmos para obtener esta clasificación.

Describiremos brevemente estos algoritmos, que se pueden utilizar para clasificar estas variedades en dimensión arbitraria. También presentaremos una extensión que incluye estas funcionalidades en el paquete de geometría algebraica computacional *Macaulay2*.

Criptografía post-cuántica basada en isogenias

Odalis Ortega
(Doctorado en Consorcio de Valparaíso)

La criptografía basada en isogenias tiene considerables ventajas como lo compacto de claves. En esta charla veremos CSIDH: An Efficient Post-Quantum Commutative Group Action, el cual es un protocolo de intercambio de clave pública basado en isogenias.

Tríos Pitagóricos

Gonzalo Riquelme
(Pontificia Universidad Católica de Valparaíso)

Desde tiempos antiguos, incluso desde antes del propio Pitágoras, se conoce el teorema que lleva su nombre. En particular, se han reconocido, con especial interés, los triángulos rectángulos cuyos lados tienen medida entera. Estos tripletes de números reciben el nombre de "tríos pitagóricos".

En esta charla daremos luces sobre ciertos argumentos de tipo algebraico y geométrico para abordar el problema de fondo: ¿cómo determinar todos los tríos pitagóricos?