XXI CLA - Session S13
Number Theory

S13 - July 25, 15:00 – 15:40

Sharp lower bounds for regulators of small-degree number fields

Eduardo Friedman
Universidad de Chile, Santiago
friedman@uchile.cl

Minimal discriminants of number fields are presently known for 22 signatures. Using a combination of analytic and geometric techniques, for 20 of these we are able to find the minimal regulator. Except in the totally complex case, in each signature we find that the field with the minimal discriminant has the minimal regulator.

Joint work with Sergio Astudillo (Weston Academy, Quilicura, Chile) and Francisco Diaz y Diaz (U. Bordeaux, retired).

S13 - July 25, 15:50 – 16:20

Waldspurger formulas for Hilbert modular forms

Nicolás Sirolli
Universidad de Buenos Aires, Argentina
nsirolli@dm.uba.ar

Computing central values of L-functions attached to modular forms is interesting because of the arithmetic information they encode. These values are related to Fourier coefficients of half-integral weight modular forms and the Shimura correspondence, as shown in great generality by Waldspurger.

In this talk we will show an explicit Waldspurger type formula for Hilbert modular forms, which is valid under rather mild hypotheses.

Joint work with Gonzalo Tornaría (Universidad de la República).

S13 - July 25, 16:25 – 16:55

The Mahler measure of elliptic curves

Matilde Lalín
Université de Montréal, Canada
mlalin@dms.umontreal.ca

The Mahler measure of a multivariable polynomial or rational function P is given by the integral of $\log|P|$ where each of the variables moves on the unit circle and with respect to the Haar measure. In 1998 Boyd made a systematic numerical study of the Mahler measure of many polynomial families and found interesting conjectural relationships to special values of L-functions of elliptic curves. We will discuss some recent advances on Boyd's conjectures.

S13 - July 25, 17:30 – 18:00

Heegner point constructions

Daniel Kohen
Universidad de Buenos Aires- IMAS, Argentina
kohendaniel@gmail.com

In this talk we will show how to construct certain special points on rational elliptic curves in situations where the so-called "Heegner hypothesis" does not hold. More concretely, given a rational elliptic curve with conductor divisible by the square of a prime p, we show how to construct points associated to an imaginary quadratic field K regardless of the factorization of p in K.

Joint work with Ariel Pacetti (Universidad de Buenos Aires-Warwick).

S13 - July 25, 18:05 – 18:35

Overconvergent Eichler-Shimura isomorphisms for Shimura curves

Daniel Barrera Salazar
CRM, Montreal, Canada
danielbarreras@hotmail.com

We will discuss the p-adic variation of the Eichler-Shimura isomorphism in the context of Shimura curves. In particular, we describe the finite slope part of the space of overconvergent modular symbols in terms of the finite slope part of the space of overconvergent modular forms. As an application we will explain how to attach Galois representations to certain overconvergent modular forms.

Joint work with Shan Gao (Concordia University).

S13 - July 25, 18:40 – 19:10

Large images of reducible Galois representations

Aftab Pande
Universidade Federal do Rio de Janeiro, Brasil
aftab.pande@gmail.com

Ramakrishna showed that one could deform a 2 dimensional mod p representation to a power series ring in infinitely many variables over the p-adics. We extend his results for the residually reducible case by modifying the primes that one adds to the level.

S13 - July 26, 15:00 – 15:40

La criba de Eratóstenes en menos espacio

Harald Helfgott
Georg-August Universitaet Goettingen/CNRS, Alemania/Francia
harald.helfgott@gmail.com

Digamos que queremos una lista de todos los números primos de 1 hasta N, o factorizar todos los enteros del 1 hasta N. Muchos aprendimos la criba de Eratóstenes en la primaria. Con ciertos trucos estándar, esta criba puede hacerse en espacio aproximadamente $\sqrt{N}$, en vez de N. Veremos cómo modificar la criba de Eratóstenes para que funcione en espacio $N^{1/3}(\log N)^{2/3}$ y tiempo aun esencialmente linear en N.

La inspiración principal viene de trabajos de índole combinatoria (Voronoi-Sierpinski) sobre el método del circulo; hay en esto una conexión con la versión de Galway (2000) de la criba de Atkin, que también utiliza espacio esencialmente $N^{1/3}$. La ventaja de la criba de Eratóstenes es que se puede utilizar para factorizar o para calcular diversas funciones aritméticas, y no sólo para producir números primos.

S13 - July 26, 15:50 – 16:20

Bounding the argument of zeta on the Riemann hypothesis

Emanuel Carneiro
IMPA, Brazil
carneiro@impa.br

Let $S(t)$ denote the argument of the Riemann zeta-function at the point $1/2 + it$. Let $S_n(t)$ be the n-th antiderivative of $S(t)$ (adding a suitable constant c_n at each step). In 1924, J. Littlewood established, under the Riemann hypothesis, that

$$S_n(t) \ll \frac{logt}{(\log logt)^{n+1}}$$

and this estimate has never been improved in its order of magnitude over the last 92 years. The efforts have focused in improving the implicit constant in this estimate. In this talk we will show how to obtain the best (up to date) form of all of these estimates. This involves the use of certain special entire functions of exponential type.

S13 - July 26, 16:25 – 16:55

Equidistribución p-ádica de órbitas de Hecke y aplicaciones diofantinas

Ricardo Menares
Pontificia Universidad Católica de Valparaíso, Chile
ricardo.menares@pucv.cl

Es sabido que las órbitas por correspondencias de Hecke en la curva modular de nivel 1 se equidistribuyen con respecto a la medida hiperbólica. Recientemente, Habegger ha utilizado este principio para establecer que el conjunto de valores del invariante j de curvas elípticas con multiplicación compleja ("singular moduli") que son unidades algebraicas es finito.

En esta charla explicaremos un análogo p-ádico del resultado de equidistribución de órbitas de Hecke. Si el tiempo lo permite, explicaremos también cómo adaptar la estrategia de Habegger para establecer que, dado un conjunto finito de primos S que satisfacen ciertas congruencias, el conjunto de los singular moduli que son S-unidades es finito.

Joint work with Sebastián Herrero (Pontificia Universidad Católica de Chile, Chile) and Juan Rivera-Letelier (Rochester University, EEUU).

S13 - July 26, 17:30 – 18:00

CM-points on straight lines

Amalia Pizarro Madariaga
Universidad de Valparaíso, Chile
amalia.pizarro@uv.cl

A CM-point (or special point) is a point of the form $(j(\tau_1), j(\tau_2))$ where both τ_1, τ_2 are imaginary quadratic numbers. In this talk we will show that, with "obvious" exceptions, a CM-point cannot belong to a straight line in $\mathbb{C}^2$ defined over $\mathbb{Q}$.

Joint work with Bill Allombert (Université de Bordeaux) and Yuri Bilu (Université de Bordeaux).

S13 - July 26, 18:05 – 18:35

Weak Arithmetic equivalence

Guillermo Mantilla-Soler
Universidad de los Andes, Colombia
g.mantilla691@uniandes.edu.co

Inspired by the invariant of a number field given by its zeta function we define the notion of weak arithmetic equivalence and show that for certain families of number fields, e.g., semistable(having fundamental discriminant), this equivalence determines the local root numbers of the number field. This is analogous to the fact that for semistable rational elliptic curves the local root numbers are determined by the bad part of the L-function of the curve.

S13 - July 26, 18:40 – 19:10

On the paramodular conjecture

Gonzalo Tornaría
Universidad de la República, Uruguay
tornaria@cmat.edu.uy

In this talk we will recall the statement of the paramodular conjecture by Brumer and Kramer, and we will show recent work with Brumer and Pacetti which proves the first known examples.

Joint work with Armand Brumer (Fordham University) and Ariel Pacetti (Universidad de Buenos Aires).

S13 - Poster

Conjuntos de Sidon en intervalos

Brady Miliwska Ali Medina
Universidad Nacional de San Agustín , Perú
bradyalimedina@hotmail.com

Un conjunto $\mathbb{A}$ en un grupo abeliano (G,+) es un conjunto de Sidon si todas las diferencias no nulas a-a', con a,a' $\in \mathbb{A}$ son distintas. Nos preguntamos ¿Cuál es el mayor tamaño que puede tener un conjunto de

Sidon en [1:n]?. En este trabajo se presenta una respuesta asintótica al problema planteado en 1932 por el analista Simón Sidon. Además, damos a conocer algunos de los problemas sin resolver sobre los conjuntos de Sidon en intervalos. Por último, presentamos algunas de las aplicaciones que tienen los conjuntos de Sidon en el área de las telecomunicaciones.

Joint work with Mijael Hancco(Universidad Nacional de San Agustin) and Jhon Huarachi(Universidad Nacional de San Agustin).

S13 - Poster

Propiedades de las p-extensiones elementales abelianas sobre $\mathbb{F}_{p^r}(T)$

Jonny Fernando Barreto Castañeda
Centro de Investigación y de Estudios Avanzados del I.P.N., México
jfbarretoc@unal.edu.co

Se presentan varias propiedades para una p-extensión elemental abeliana sobre el cuerpo de funciones racionales $k = \mathbb{F}_{p^r}(T)$ con $\mathbb{F}_{p^r}$ el cuerpo finito de p^r elementos, p un entero primo. Entre las propiedades a presentar están la ramificación, la inercia y la descomposición de los lugares asociados al cuerpo k, el cálculo de índice de ramificación de dichos lugares utilizando las técnicas de Q. Wu y R. Scheidler en su artículo 'The ramification groups and different of a compositum of Artin-Schreier extensions' y de A. Garcia y de H. Stichtenoth en 'Elementary Abelian p-extensions of algebraic function fields'. También se presentan varios ejemplos que ilustran los resultados presentados.

Joint work with Martha Rzedowski Calderón (Centro de Investigación y de Estudios Avanzados del I.P.N.).

S13 - Poster

Primos de Wilson, Mersenne y Wieferich en el anillo $\mathbb{F}_q[T]$

Jonny Fernando Barreto Castañeda
Centro de Investigación y de Estudios Avanzados del I.P.N., México
jfbarretoc@unal.edu.co

En el 2011, D. Thakur en su artículo "Binomial and factorial congruences for $\mathbb{F}_q[T]$" presentó tres formas diferentes de definir factorial y coeficiente binomial para el anillo $\mathbb{F}_q[T]$. Además, demostró que existen ciertos análogos a los bien conocidos teoremas de Lucas y de Wilson. Este último teorema permite definir una familia de primos llamados primos de Wilson para $\mathbb{F}_p[T]$ para p un primo entero. La caracterización de estos primos no se realizó por completo para cualquier anillo de polinomios con coeficientes en un cuerpo finito. Tiempo después el mismo D. Thakur en su artículo "Differential characterization of Wilson primes for $\mathbb{F}_q[T]$ " presenta una caracterización completa de dichos primos utilizando la derivada usual. Con estos dos artículos como referencia, en el 2014 Dong Quan en el artículo " Carlitz module analogues of Mersenne primes, Wieferich primes, and certain prime elements in cyclotomic function fields" presenta, en la misma dirección que D. Thakur, una nueva familia de primos de Mersenne y Wieferich para el módulo de Carlitz.

En este trabajo se pretende presentar algunos conceptos y los argumentos utilizados por los autores citados anteriormente, para comprender los artículos. Algunos de éstos son: el módulo de Carlitz, los cuerpos de funciones ciclotómicos y los análogos a los teoremas de Lucas y de Wilson en el anillo $\mathbb{F}_q[T]$. También se harán algunas observaciones y se sugerirán trabajos futuros en esta línea de investigación.

Joint work with Martha Rzedowski Calderón (Centro de Investigación y de Estudios Avanzados del I.P.N.).

S13 - Poster

Formas Cuadráticas y el teorema de los 15

Juanita Duque
Universidad de los Andes, Colombia
j.duque10@uniandes.edu.co

Una forma cuadrática entera es un polinomio $f(x_1, \ldots, x_n) \in \mathbb{Z}[x]$, homogéneo y de grado 2. Diremos que $f(x_1, \ldots, x_n)$ representa a un entero m si existe $\vec{a} \in \mathbb{Z}^n$ tal que $f(\vec{a}) = m$. Nuestro objetivo será explicar con detalle una demostración del *"teorema de los 15" de Conway-Schneeberger* (1993). Explicaremos los detalles de la prueba publicada por Bhargava (2000). El teorema afirma: *si una forma cuadrática entera definida positiva representa a todo entero positivo hasta 15, entonces representa a todos los enteros positivos.* Una forma que cumpla esto último se denomina *universal*.

A partir de este punto, el término forma cuadrática se referirá a una forma cuadrática definida positiva. Para demostrar el teorema se utilizará la relación que existe entre retículos y formas cuadráticas. Denote como *ausente* al mínimo entero que una forma cuadrática no universal no representa. Una *escalada* de un retículo no universal L es el retículo generado por L y un vector de norma el ausente de L. Un *retículo escalado* es una sucesión de escaladas partiendo del retículo cero dimensional. Se mostrará que todo retículo escalado de dimensión cinco es universal, hallando directamente todos los retículos escalados de dimensión menor o igual a 5. Después, se probará que toda forma cuadrática es universal si y solo si posee un subretículo escalado cuatro o cinco dimensional universal. Luego, toda forma cuadrática es universal si representa a los ausentes de los retículos escalados de dimensión 0 hasta 4. El nombre del teorema se debe a que estos ausentes son menores o iguales que 15.

Joint work with Yacir Ramirez (Universidad de los Andes, Colombia).
