RSME-SMM-2012 17-20 ene 2012, Torremolinos

S21. Teoría de Números. SALA M3

Coordinada por: **Javier Cilleruelo**, UAM e ICMAT; **Adolfo Quirós**, UAM; **Wilson Zúñiga**, CINVESTAV.

PROGRAMA

mar17 15:00-15:40 →MOUBARIZ GARAEV, UNAM
Concentración de puntos en funciones polinomiales, curvas elípticas e hiperelípticas en cuerpos primos y aplicaciones.

mar17 15:40-16:20 →JORDI GUÀRDIA, U. Politécnica Catalunya
El ADN de los polinomios p-ádicos.

mar17 16:20-17:00 →WILSON ZÚÑIGA, CINVESTAV
Formas Cuadráticas, Funciones Zeta Locales y la Ecuación del Calor sobre los p-ádicos.

mar17 17:00-17:40 →LUIS NAVAS, U. Salamanca
El comportamiento asintótico de los polinomios de Apostol-Bernoulli.

mié18 15:00-15:40 →EDUARDO DUÉÑEZ, U. Texas
Matrices Aleatorias y Ceros de Funciones-L de Twists Cuadráticos de Curvas Elípticas.

mié18 15:40-16:20 →JESÚS GÓMEZ AYALA, U. País Vasco
Fantasías y variaciones en torno al teorema de Hilbert-Speiser.

mié18 16:20-17:00 →TIMOTHY GENDRON, UNAM
El Grupo de Aproximaciones Diofantinas y el Invariante Modular Cuántico.

mié18 17:00-17:40 →JAVIER CILLERUELO, UAM e ICMAT
Puntos de coordenadas enteras sobre circunferencias y números de Fibonacci.

RESÚMENES

Ponente: MOUBARIZ GARAEV UNAM

Título: *Concentración de puntos en funciones polinomiales, curvas elípticas e hiperelípticas en cuerpos primos y aplicaciones*

Hora: (M3) mar17 15:00-15:40

Resumen: Sea $\mathbb{F}_p$ el cuerpo de las clases residuales módulo un primo p y sean I_1, I_2 intervalos en $\mathbb{F}_p$ de longitud M. Para un polinomio $f \in \mathbb{F}_p[X]$, consideremos las congruencias $y \equiv f(x) \pmod p$, $y^2 \equiv f(x) \pmod p$, donde $(x, y) \in I_1 \times I_2$. En esta plática voy a hablar sobre nuevas cotas superiores para el número de soluciones de dichas congruencias y presentaré algunas nuevas aplicaciones de estas estimaciones.
Es un trabajo conjunto con M.-C. Chang, J. Cilleruelo, J. Hernández, I. Shparlinski y A. Zumalacárregui.

[1] J. Cilleruelo and M. Z. Garaev, *Concentration of points on two and three dimensional modular hyperbolas and applications*, Geom. and Func. Anal. **21** (2011), 892–904.

[2] J. Cilleruelo, M.Z. Garaev, A. Ostafe, and I. Shparlinski, *On the concentration of points of polynomial maps and applications*, Math. Zeitschrift, 1–18, to appear.

[3] J. Cilleruelo, I. Shparlinski, and A. Zumalacárregui, *Isomorphism classes of elliptic curves over a finite field in some thin families*, Math. Res. Lett., 1–13, to appear.

[4] T. H. Chan and I. Shparlinski, *On the concentration of points on modular hyperbolas and exponential curves*, Acta Arith. **142** (2010), 59–66.

[5] M.-C. Chang, *Expansions of quadratic maps in prime fields*, preprint (2011), 1–11.

garaev@matmor.unam.mx

Ponente: JORDI GUÀRDIA U. Politécnica Catalunya

Título: *El ADN de los polinomios p-ádicos*

Hora: (M3) mar17 15:40-16:20

Resumen: Los polinomios a coeficientes p-ádicos son un objeto de naturaleza mixta: juegan un papel importante en muchos problemas de la teoría de números algebraica, pero a la práctica deben manipularse con técnicas numéricas. En la charla mostraremos cómo esta dualidad confiere a los polinomios p-ádicos una estructura algebraica subyacente, que da lugar simultáneamente a nuevas representaciones eficientes (su ”ADN”) y a potentes técnicas numéricas para la resolución de problemas clásicos de la teoría de números computacional.

guardia@ma4.upc.edu

Ponente: WILSON ZÚÑIGA CINVESTAV

Título: *Formas Cuadráticas, Funciones Zeta Locales y la Ecuación del Calor sobre los p-ádicos*

Hora: (M3) mar17 16:20-17:00

Resumen: La conexiones entre el análisis p-ádico y la física matemática han recibido una fuerte atención en los últimos, debido principalmente a la aparición de nuevos modelos modelos matemáticos envolviendo números p-ádicos. Uno de los más interesantes, la versión p-ádica de la ecuación del calor, describe una caminata aleatoria sobre los p-ádicos. En la conferencia discutiremos las conexiones entre las ecuaciones funcionales para las funciones zeta locales asociadas a ciertas formas cuadráticas y la solución del problema de Cauchy de ciertas ecuaciones parabólicas.

wazuniga@gmail.com

Ponente: LUIS NAVAS U. Salamanca

Título: *El comportamiento asintótico de los polinomios de Apostol-Bernoulli*

Hora: (M3) mar17 17:00-17:40

Resumen: Trabajo conjunto con Francisco José Ruiz Blasco y Juan Luis Varona Malumbres.

Apostol introdujo los polinomios de Apostol-Bernoulli $\mathscr{B}_n(x;\lambda)$ en [1] para generalizar la relación entre los valores de la función zeta de Riemann en los enteros negativos y los números de Bernoulli, expresada por $\zeta(-n) = -\frac{B_{n+1}}{n+1}$. Dicha generalización relaciona, mediante una fórmula análoga, los valores de la función zeta de Lerch con esta nueva familia de polinomios.

Recientemente ([2, 5]) se han estudiado las series de Fourier de los polinomios de Apostol-Bernoulli, usando métodos de variable compleja, algunos de hecho ya empleados con anterioridad en [4], y que generalizan el desarrollo de Fourier de los polinomios de Bernoulli, descubierta por Hurwitz ya en 1890. En principio, una limitación de la serie de Fourier es que su convergencia es sobre el intervalo real $[0,1]$. En [3] y en [7], utilizando métodos diferentes, se abordaba la cuestión particular del comportamiento asintótico de los polinomios de Bernoulli sobre el plano complejo. Finalmente, en [8] se extienden los resultados anteriores, mostrando que la serie de Fourier, aun cuando deja de ser convergente, sigue siendo válida como serie asintótica sobre el plano complejo.

En esta charla haremos una introducción general a los polinomios de Apostol-Bernoulli, repasaremos los resultados anteriores y expondremos el último de ellos sobre el desarrollo asintótico de los polinomios de Apostol-Bernoulli. De la técnica de demostración empleada veremos que se obtienen también resultados sobre el grado de aproximación. Comentaremos algunos casos particulares de los parámetros que dan lugar a fenómenos oscilatorios en el comportamiento asintótico, resultantes de ciertas relaciones con la aproximación diofántica.

[1] T. M. Apostol, *On the Lerch zeta function*, Pacific J. Math. **1** (1951), 161–167.

[2] A. Bayad, *Fourier expansions for Apostol-Bernoulli, Apostol-Euler and Apostol-Genocchi polynomials*, Math. Comp. **80** (2011), 2219–2221.

[3] K. Dilcher, *Asymptotic behaviour of Bernoulli, Euler, and generalized Bernoulli polynomials*, J. Approx. Theory **49** (1987), 321–330.

[4] A. Erdélyi, W. Magnus, F. Oberhettinger, and F. Tricomi, *Higher Transcendental Functions*, Vol. I, McGraw-Hill, New York, 1953.

[5] Q.-M. Luo, *Fourier expansions and integral representations for the Apostol-Bernoulli and Apostol-Euler polynomials*, Math. Comp **78** (2009), 2193–2208.

[6] Q.-M. Luo and H. M. Srivastava, *Some relationships between the Apostol-Bernoulli and Apostol-Euler polynomials*, Comput. Math. Appl. **51** (2006), 631–642.

[7] L. M. Navas, F. J. Ruiz, and J. L. Varona, *The Möbius inversion formula for Fourier series applied to Bernoulli and Euler polynomials*, J. Approx. Theory **163** (2011), 22–40.

[8] ______, *Asymptotic estimates for Apostol-Bernoulli and Apostol-Euler polynomials*, Math. Comp., to appear.

navas@usal.es

Ponente: EDUARDO DUÉÑEZ U. Texas

Título: *Matrices Aleatorias y Ceros de Funciones-L de Twists Cuadráticos de Curvas Elípticas*

Hora: (M3) mié18 15:00-15:40

Resumen: Trabajo conjunto con D.K. Huynh, J.P. Keating, S.J. Miller, y N.C. Snaith.

En 2006, S.J. Miller [3] observó cierto comportamiendo de los ceros críticos en familias uniparamétricas de funciones-L pares de curvas elípticas: a saber, una repulsión de los mismos alejándolos del punto central de la línea crítica. Esta repulsión es sumamente inesperada porque va en contra de la filosofía de Katz-Sarnak [2], la cual predice (al menos en el límite cuando el conductor tiende a infinito) que tales ceros críticos deberían obedecer el comportamiento estadístico de los eigenvalores cerca de $+1$ de matrices aleatorias ortogonales $\mathrm{SO}(2N)$ conforme $N \to \infty$. Sin embargo, el eigenvalor $+1$ de matrices en $\mathrm{SO}(2N)$ no repele eigenvalores cercanos sino que cualitativamente los atrae.

Proponemos un modelo (descrito en [1]) para el comportamiento estadístico de los ceros críticos de la familia de twists cuadráticos pares $E \otimes \chi_d$ de una curva elíptica $E/\mathbb{Q}$ fija como aquél de los eigenvalores de una *familia de matrices ortogonales "extraídas"*. La construcción de esta familia imita la discretización de valores centrales de funciones-L implicada por las fórmulas de Waldspurger y Kohnen-Zagier, y el estudio de las propiedades estadísticas de sus eigenvalores es posible aplicando resultados sobre familias de matrices aleatorias de Jacobi. Los eigenvalores de matrices en la familia ortogonal extraída exhiben una repulsión cualitativamente idéntica a la observada por Miller. También realizamos algunos experimentos numéricos para juzgar cuantitativamente la bondad del ajuste estadístico entre las distribuciones de ceros y eigenvalores.

[1] E. Duéñez, D.K. Huynh, J.P. Keating, S.J. Miller, and N.C. Snaith, *A Random Matrix Model for Elliptic Curve L-Functions of Finite Conductor*, available at arXiv:1107.4426v2[math.NT].

[2] N.M. Katz and P. Sarnak, *Zeros of zeta functions and symmetry*, Bull. Amer. Math. Soc. **36** (1999), 1–26.

[3] S.J. Miller, *Investigations of zeros near the central point of elliptic curve L-functions*, Experiment. Math. **15** (2006), no. 3, 257–279.

eduenez@math.utsa.edu

Ponente: JESÚS GÓMEZ AYALA U. País Vasco

Título: *Fantasías y variaciones en torno al teorema de Hilbert-Speiser*

Hora: (M3) mié18 15:40-16:20

Resumen: El teorema de Hilbert-Speiser afirma que si E es una extensión finita abeliana y moderadamente ramificada del cuerpo de los números racionales $\mathbf{Q}$, con grupo de Galois G, el anillo de los enteros $\mathfrak{O}_E$ de E posee una base normal sobre $\mathbf{Z}$, esto es, existe un elemento α de $\mathfrak{O}_E$ tal que él y sus conjugados forman una base de $\mathfrak{O}_E$ como $\mathbf{Z}$-módulo; dicho de otro modo, $\mathfrak{O}_E$ es un $\mathbf{Z}[G]$-módulo libre de rango uno. Este resultado fue probado por Hilbert en algunos casos particulares en su famoso *Zahlbericht*, y posteriormente Speiser lo demostró con toda generalidad. El teorema de Hilbert-Speiser es el resultado clásico por excelencia de lo que hoy se conoce como la teoría de la estructura galoisiana de los anillos de enteros, desarrollada principalmente por Albrecht Fröhlich y su escuela. En esta charla se tratará de situar el teorema de Hilbert-Speiser en su contexto, dentro de la teoría general de la estructura galoisiana de los anillos de enteros, y de exponer algunas de las diversas versiones, variaciones o intentos de generalización a que ha dado lugar en los últimos años.

eugeniojesus.gomez@ehu.es

Ponente: TIMOTHY GENDRON UNAM

Título: *El Grupo de Aproximaciones Diofantinas y el Invariante Modular Cuántico*

Hora: (M3) mié18 16:20-17:00

Resumen: El propósito de esta plática es

- $\boxed{\text{Introducir el grupo de aproximaciones diofantinas } {}^*\mathbb{Z}(\theta) \text{ de } \theta \in \mathbb{R}.}$

  El grupo ${}^*\mathbb{Z}(\theta)$ es una generalización para cualquier $\theta \in \mathbb{R}$ del concepto de ideal principal generado por el denominador de un número racional. Indicaremos como puede ser utilizado para formular una teoría de números que une la teoría transcendente con la teoría algebraica. Referencias: [1],[2],[3].

- $\boxed{\text{Usar } {}^*\mathbb{Z}(\theta) \text{ para definir un invariante-} j \text{ del toro cuántico } \mathbb{T}(\theta) = \mathbb{R}/\langle 1,\theta\rangle.}$

  Definiremos el invariante modular $j(\theta) = j(\mathbb{T}(\theta))$ usando ideas de análisis no estandar donde ${}^*\mathbb{Z}(\theta)$ juega el papel de el latiz en la definición clásica de j. Terminaremos con una discusión de $j(\varphi)$ donde φ = la razón aurea, dando una fórmula explícita para $j(\varphi)$ que involucra una generalización de la función de Rodgers-Ramanujan. La esperanza es que el invariante modular cuántico definido aquí, pueda ser usado para encontrar una solución de el programa de Multiplicación Real de Yu. Manin. Referencias: [4],[5].

[1] T.M. Gendron, *Real algebraic number theory I: Diophantine approximation groups.*

[2] ______, *Real algebraic number theory II: Growth-decay arithmetic.*

[3] ______, *Real algebraic number theory III: Galois Theory.*

[4] C. Castaño Bernard and T.M. Gendron, *Modular invariant of quantum tori I: A Definition via Diophantine Approximation Groups.*

[5] ______, *Modular invariant of quantum tori II: Quadratic units of norm* −1.

tim@matcuer.unam.mx

Ponente: JAVIER CILLERUELO UAM e ICMAT

Título: *Puntos de coordenadas enteras sobre circunferencias y números de Fibonacci*

Hora: (M3) mié18 17:00-17:40

Resumen: El número y la distribución de los puntos de coordenadas enteras sobre la circunferencia $x^2 + y^2 = n$ dependen de las propiedades aritméticas de n. Se presentarán distintos resultados del autor sobre la distribución de estos puntos y otros resultados, en colaboración con A. Córdoba y A. Granville, sobre la ubicación de estos puntos en arcos pequeños de circunferencias.
Por último presentaremos un resultado, en colaboración con F. Luca, sobre la distribución de los puntos sobre las circunferencia $x^2 + y^2 = F_n$, donde los F_n son números de Fibonacci.

[1] J. Cilleruelo, *The distribution of lattice points on circles*, Journal of Number Theory **43** (1993), no. 2.

[2] ______, *Lattice points on circles*, Journal Australian Math. Soc. **72** (2002).

[3] J. Cilleruelo and A. Córdoba, *Lattice points on ellipses*, Duke Math. J. **76** (1993).

[4] J. Cilleruelo and A. Granville, *Close Lattice points*, Canadian Journal of Mathematics **61** (2009), no. 6.

[5] J. Cilleruelo and F. Luca, *Fibonacci lattice points*, The Ramanujan Journal **22** (2010), no. 3.

franciscojavier.cilleruelo@uam.es