Primer Congreso Conjunto de Matemáticas RSME–SCM–SEIO–SEMA

MAT.ES 2005

Sesión Especial 25: "Teoría de números"

Organizadores: Javier Cilleruelo, Adolfo Quirós
(con el apoyo de la Universidad Autónoma de Madrid)

Jueves 3 de febrero, AULA 11

15:30-16:10 Fernando Chamizo (Universidad Autónoma de Madrid)
Sumas de cuadrados en anillos cuadráticos reales

16:10-16:30 Emilio Elizalde (CSIC)
Extensión del desarrollo de Chowla-Selberg para la función zeta de Epstein

16:30-16:50 Ángela Arenas (Universitat de Barcelona)
Formas modulares nuevas de Hilbert

16:50-17:30 Victor Rotger (Universitat Politècnica de Catalunya)
Formas y variedades modulares: conjeturas y resultados de finitud

17:30-18:00 DESCANSO

18:00-18:20 Daniel Sadornil y Juan Tena (U. de Salamanca / U. de Valladolid)
Tests deterministas de primalidad tipo Proth

18:20-18:40 I. Jiménez Calvo, J. Herranz y G. Sáez (CSIC / U. Politècnica de Catalunya)
Un nuevo algoritmo para buscar valores pequeños no nulos de $|x^3-y^2|$

18:40-19:20 Alain Plagne (École Polytechnique, Francia)
Old and new results on additive bases

19:20-19:40 Mario Pérez y Francisco J. Ruiz (Universidad de Zaragoza)
La ecuación diofántica $a^2+b^2=c^n$ y la función $\phi_n(z)=z^n$

19:40-20:00 J. C. Rosales, P. A. García Sánchez*, J. I. García García y J. M. Urbano Blanco (Universidad de Granada)
El conjunto de soluciones de una inecuación diofántica proporcionalmente modular

Viernes 4 de febrero, AULA 12

11:30-12:10 Fernando Pablos (Universidad de Salamanca)
Conmensurabilidad, Extensiones Centrales y Leyes de Reciprocidad

12:10-12:30 Fernando Holgado (Universidad Autónoma de Madrid)
Sobre módulos fuertemente divisibles

12:30-12:50 J. Guàrdia, E. Torres y M. Vela* (Universitat Politècnica de Catalunya)
Modelos estables de curvas elípticas, "ring class fields" y multiplicación compleja

12:50-13:30 Núria Vila (Universitat de Barcelona)
Representaciones de Galois y Grupos de Galois sobre Q

**** indica el autor que presentará la ponencia***

MAT.ES 2005 - Primer Congreso Conjunto de Matemáticas RSME-SCM-SEIO-SEMA

Sesión Especial 25. Teoría de Números.

Resúmenes de las Ponencias

Sumas de cuadrados en anillos cuadráticos reales

Fernando Chamizo

Departamento de Matemáticas, Universidad Autónoma de Madrid.

Consideramos $S = \sum_{n=1}^{N} \sum_{m=1}^{M} r(n + m\sqrt{k})$, donde $r(n + m\sqrt{k})$ es el número de representaciones de $n + m\sqrt{k}$ como suma de dos cuadrados en el anillo $\mathbb{Z}[\sqrt{k}]$ (con $k > 1$ libre de cuadrados). Mostramos que la teoría espectral de formas automorfas puede aplicarse provechosamente en ciertos rangos, para obtener la asintótica de S.

Extensión del desarrollo de Chowla-Selberg para la función zeta de Epstein

Emilio Elizalde

Consejo Superior de Investigaciones Científicas

La utilidad práctica del método de regularización zeta se apoya en la existencia de prolongaciones analíticas adecuadas de la correspondiente función zeta. Éstas no consisten tan solo en la fórmula de reflexión en cada caso (dado que su convergencia es extraordinariamente lenta cerca de la abscisa de convergencia), sino sobre todo en otras expresiones derivadas de la identidad de Jacobi para la función theta, las fórmulas de sumación de Poisson y de Plana, y el celebrado desarrollo de Chowla y Selberg (del que sus autores se han sentido siempre manifiestamente muy orgullosos).

Pero aún eso no resulta suficiente, ya que ocurre que tales herramientas están restringidas a casos bastante específicos: funciones zeta homogéneas y bidimensionales en el caso de Chowla-Selberg, y a sumas que se extienden sobre toda la lattice de números enteros. Presentaremos aquí extensiones de estas fórmulas a funciones zeta más generales, en dimensión arbitraria y abordaremos así mismo el problema mucho más complejo de la obtención de series asintóticas para los desarrollos truncados a la lattice de enteros positivos.

Formas modulares nuevas de Hilbert

Ángela Arenas
Departament d'Àlgebra i Geometria. Facultat de Matemàtiques.
Universitat de Barcelona, Gran Via 585, 08007 Barcelona.
angelaarenas@ub.edu

El objetivo de esta charla es determinar de manera natural el subespacio del espacio de formas nuevas de Hilbert de nivel $\mathfrak{n}$ que corresponden a formas propias de un álgebra de cuaterniones apropiada, en el sentido de tener los mismos valores propios respecto de los correspondientes operadores de Hecke. Este estudio puede verse como un caso particular de la correspondencia de Jacquet-Langlands.

Formas y variedades modulares: conjecturas y resultados de finitud

Víctor Rotger
Universitat Politènica de Catalunya

Dado un entero positivo $N \geq 1$, sea $X_1(N)/\mathbb{Q}$ la curva modular uniformizada analíticamente por el grupo de congruencia

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a \\ c \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mod N \right\}$$

y denotemos $J_1(N)/\mathbb{Q}$ la variedad Jacobiana de $X_1(N)$.

Una curva C proyectiva y lisa sobre $\mathbb{Q}$ es modular si existe un morfismo regular no constante $\Phi : X_1(N) \to C$ definido sobre $\mathbb{Q}$ para algún $N \geq 1$.

Una variedad abeliana A definida sobre $\mathbb{Q}$ es *modular* si es isógena sobre $\mathbb{Q}$ a una subvariedad abeliana de $J_1(N)$ para algún $N \geq 1$. Si A es irreducible, la modularidad de A sobre $\mathbb{Q}$ es equivalente a la existencia de una forma modular nueva normalizada $f \in S_2(\Gamma_1(N))$ tal que las series L asociadas a A y f respectivamente coinciden: $L(A/\mathbb{Q}, s) = L(f, s)$.

Esta charla prentende ofrecer una introducción a algunos de los resultados conocidos y a algunas de las cuestiones abiertas sobre curvas y variedades abelianas modulares: la conjectura de Shimura-Taniyama-Weil, la conjectura de finitud de curvas modulares de género acotado y la conjetura de finitud de álgebras de endomorfismos de variedades abelianas modulares de dimensión acotada

Tests deterministas de primalidad tipo Proth

Daniel Sadornil
Dpt. Matemáticas. Universidad de Salamanca. sadornil@agt.uva.es
Juan Tena
Dept. de Algebra, Geometría and Topología. Universidad de Valladolid.
tena@agt.uva.es

En el año 2002 Agrawal, Kayal y Saxena presentaron a la comunidad matemática un algoritmo, denominado AKS, que determina si un número n es primo o compuesto cuya complejidad computacional es polinómica. Hasta esa fecha, habían aparecido numerosos tests deterministas de primalidad de complejidad polinómica, pero que o bien tenían una componente probabilística (como puede ser la determinación de no residuos cuadráticos) o bien eran sólo aplicables a números particulares. Sin embargo, este algoritmo presenta varias limitaciones a la hora de su implementación y diversos autores han tratado de mejorar dicho algoritmo refinando los resultados del AKS. No obstante, y a pesar de ello, todavía tienen cabida los tests de primalidad para números particulares, pues además de ser deterministas, su complejidad es también polinómica y son fácilmente implementables.

El conocido teorema de Proth que determina la primalidad de un número $n = A2^s + 1$ puede generalizarse para números de la forma $n = Ar^s \pm \omega_s$, con r primo, $A < r^s$, $\omega_s < r^s$, $\omega_s^f \equiv 1 \bmod r^s$. En este caso, se trabajará en el anillo de enteros $Z[\zeta_r]$ con ζ_r una raíz primitiva de la unidad de orden r módulo n. El test de primalidad puede plantearse de la forma siguiente:

Teorema: n es primo si y sólo si $\alpha^{(n^f-1)/r}$ es una raíz primitiva de orden r de la unidad módulo n, donde $\alpha \in Z[\zeta_r]$ es un elemento que depende de r y n.

Sin embargo, es posible definir también dicho test de primalidad a partir de unas sucesiones recurrentes que permiten su implementación de manera más eficiente.

Un nuevo algoritmo para buscar valores pequeños no nulos de $|x^3 - y^2|$

I. Jiménez Calvo, J. Herranz y G. Sáez
Consejo Superior de Investigaciones Científicas, Instituto de Física Aplicada, C/Serrano 144, 28006–Madrid.
Universitat Politècnica de Catalunya, c/Jordi Girona, 1-3, 08034-Barcelona.

Marshall Hall conjeturó en 1971 que la diferencia no nula entre un cubo y un cuadrado, $k = |x^3 - y^2|$, es siempre superior a $Cx^{1/2}$ para cierta constante C. La conjetura original, probablemente falsa, se formula actualmente de la siguiente manera: *Para todo exponente* $e < 1/2$*, existe una constante* K_e *dependiente de* e*, tal que* $k > K_e x^e$. A. Baker demostró una cota inferior para k que posteriormente fue mejorada por H. M. Stark que la sitúa aproximadamente en el orden de $\log(x)$. Entre las soluciones paramétricas encontradas destaca la debida a L. V. Danilov, y posteriormente ajustada por Noam Elkies, que proporciona una familia infinita de soluciones tales que $k \approx 0{,}9966x^{1/2}$.

Hasta el momento, los trabajos computacionales realizados sobre el problema han permitido encontrar un total de 38 casos en los que $k < x^{1/2}$, lo que denominamos "buenos

ejemplos de la conjetura de Hall". Aparte de los encontrados por el mismo Marshall Hall, J. Gebel, A. Petho y H. G. Zimmer caracterizaron el grupo de puntos racionales de las curvas elípticas $x^3 - y^2 = k$ con $|k| \leq 100{,}000$ con lo que pudieron determinar la totalidad de los puntos enteros en ellas. De esta forma, encontraron 14 "buenos ejemplos de la conjetura de Hall" con $x < 10^{10}$. Posteriormente, en el año 2000, N. Elkies publicó un trabajo en el que dio cuenta de 12 casos más encontrados aplicando un método basado en los algoritmos de reducción de base de A.K. Lenstra, H. W Lenstra y L. Lovász (conocidos habitualmente como algoritmos LLL). Noam Elkies elevó la cota de búsqueda hasta $x = 10^{18}$ y encontró el valor más alto conocido en la relación $\sqrt{x}/k = 46,60$.

En este trabajo se presenta un nuevo algoritmo que ha proporcionado 12 casos más, el mayor con $x \approx 2 \cdot 10^{24}$. Está basado en la existencia de ciertas familias de polinomios que contienen todos los puntos enteros de la función $k(x) = x^3 - \lfloor x^{2/3} \rceil$. La selección de los polinomios más apropiados proporcionan los valores más bajos de $k(x)$. Así se ha podido ver que el número de "buenos ejemplos de la conjetura de Hall" para $x < X$ es aproximadamente $\ln(X)/1{,}5$.

Old and new results on additive bases

Alain Plagne
École Polytechnique, Francia.

Additive bases appear naturally in the context of some well known mathematical problems like Waring's or Goldbach's where one wants to show that a given, arithmetically defined, set is an additive basis.

In this talk, we will be concerned with some properties of additive bases of a combinatorial nature. More precisely, we will study what happens when one removes one element from an additive basis. Is the remaining set still a basis ? How often ? If so, what is its order ? How often is it large ?

La ecuación diofántica $a^2 + b^2 = c^n$ y la función $\Phi_n(z) = z^n$

Mario Pérez y Francisco J. Ruiz
Departamento de Matemáticas, Universidad de Zaragoza.
mperez@unizar.es, fjruiz@unizar.es

Investigamos la acción de la aplicación compleja $z \mapsto z^n$ sobre los puntos del retículo unidad. Los resultados nos llevan a una parametrización para las soluciones primitivas de la ecuación diofántica $a^2 + b^2 = c^n$. En particular, para $n = 2$ obtenemos una demostración geométrica simple de la parametrización de Diofanto de las ternas pitagóricas. Esta aproximación permite encontrar con facilidad ternas con alguna propiedad extra, como las consecutivas.

El conjunto de soluciones de una inecuación diofántica proporcionalmente modular

J. C. Rosales, P. A. García-Sánchez,
J. I. García-García, J. M. Urbano-Blanco
Departamento de Álgebra, Universidad de Granada, E-18071 Granada, España
jrosales@ugr.es, pedro@ugr.es, jigg@ugr.es, jurbano@ugr.es

Una *inecuación diofántica proporcionalmente modular* es una expresión de la forma $ax \bmod b \leq cx$, donde a, b y c son enteros positivos. El conjunto $\mathrm{S}(a,b,c)$ de soluciones enteras de la inecuación anterior es un semigrupo numérico. En esta charla presentamos un método para calcular el conjunto de soluciones de una inecuación proporcionalmente modular. El algoritmo que presentamos se basa en los siguientes hechos.

(1) La inecuación $ax \bmod b \leq cx$ tiene las mismas soluciones que la inecuación $(a \bmod b)x \bmod b \leq cx$. Además, si $c \geq a$, entonces $\mathrm{S}(a,b,c) = \mathbb{N}$. Por tanto, podemos suponer que $c < a < b$. Bajo esta hipótesis, se puede probar que $\mathrm{S}(a,b,c) = T \cap \mathbb{N}$, donde T es el submonoide de $(\mathbb{Q},+)$ generado por $[\frac{b}{a}, \frac{b}{a-c}]$ (el recíproco también es cierto: si a_1, a_2, b_1 y b_2 son enteros positivos tales que $\frac{a_1}{b_1} < \frac{a_2}{b_2}$ y T es el submonoide de $(\mathbb{Q},+)$ generado por $[\frac{a_1}{b_1}, \frac{a_2}{b_2}]$, entonces $T \cap \mathbb{N} = \mathrm{S}(a_2b_1, a_1a_2, a_2b_1 - a_1b_2)$).

(2) La secuencia de fracciones $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ es de *Bézout* si $a_1, \ldots, a_p, b_1, \ldots, b_p$ son enteros positivos y $a_{i+1}b_i - a_ib_{i+1} = 1$ para todo $i \in \{1, \ldots, p-1\}$. Dados a, b, c y d enteros positivos, mostramos cómo construir una secuencia de este tipo $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ de forma que $\frac{a}{b} = \frac{a_1}{b_1}$ y $\frac{c}{d} = \frac{a_2}{b_2}$.

(3) Se puede comprobar que si $\frac{a_1}{b_1} < \frac{a_2}{b_2} < \cdots < \frac{a_p}{b_p}$ es una secuencia de Bézout, entonces $\{a_1, \ldots, a_p\}$ es un sistema de generadores para el semigrupo numérico $T \cap \mathbb{N}$, donde T es el submonoide de $\mathbb{Q}$ generado por $[\frac{a_1}{b_1}, \frac{a_p}{b_p}]$.

(4) De esta forma, el método anunciado en (2), junto con la observación hecha en el punto (1), nos proporcionan el método para calcular un sistema de generadores del semigrupo $\mathrm{S}(a,b,c)$ y por tanto un algoritmo para determinar el conjunto de todas las soluciones enteras de la inecuación $ax \bmod b \leq c$.

Conmensurabilidad, Extensiones Centrales y Leyes de Reciprocidad

Fernando Pablos Romo
Departamento de Matemáticas, Universidad de Salamanca.

En 1968, J. Tate [6] introdujo la noción de conmensurabilidad de subespacios para dar una definición de los residuos de diferenciales de curvas algebraicas, a partir de trazas de operadores en espacios vectoriales de dimensión infinita, y para demostrar el Teorema de los Residuos como una consecuencia inmediata de la finitud de la cohomología de una curva completa.

Posteriormente, en 1989, E. Arbarello, C. de Concini y V.G. Kac [1], utilizaron la conmensurabilidad de subespacios para definir una extensión central de grupos cuyo conmutador coincide, salvo el signo, con el símbolo moderado de una curva algebraica [3] y, de nuevo, la ley de reciprocidad de este símbolo es deducida a partir de la finitud de la cohomología de una curva completa.

La conferencia pretende mostrar sucintamente el proceso de construcción de extensiones centrales de grupos a partir de subespacios conmensurables a fin de definir, utilizando el conmutador de cada extensión, símbolos aritméticos (el símbolo del residuo normado de Hilbert, el símbolo de Legendre, el símbolo de Contou-Carrère [2], el símbolo de Parshin en una superficie [5] o el símbolo moderado del grupo lineal del cuerpo de funciones de una curva [4]) y deducir, directamente de las propiedades del conmutador, leyes de reciprocidad para estos símbolos.

Referencias

[1] Arbarello, E.; de Concini, C.; Kac, V.G., *The Infinite Wedge Representation and the Reciprocity Law for Algebraic Curves*, Proc. of Symposia in Pure Mathematics, Volume **49,** Part I, A.M.S., (1989), 171-190.

[2] Contou-Carrère, C., *Jacobienne Locale, Groupe de Bivecteurs de Witt Universel et Symbole Modéré*, C.R. Acad. Sci. Paris, t. **318,** Série I (1994) 743-746.

[3] Milnor, J., *Introduction to Algebraic K-Theory*, Annals of Mathematics Studies, Princeton University Press, 1971.

[4] Muñoz Porras, J. M.; Pablos Romo, F., *Generalized Reciprocity Laws*, Preprint, Universidad de Salamanca (2004).

[5] Parshin, A. N., *Local Class Field Theory.*, Proc. Steklov Inst. Math. **3,** (1985) 157-185.

[6] Tate, J., *Residues of Differentials on Curves*, Ann. Scient. Éc. Norm. Sup., 4a série, t. **1,** (1968) 149-159.

Sobre módulos fuertemente divisibles

Fernando Holgado Cortés
Departamento de Matemáticas, Universidad Autónoma de Madrid.

Sea k un cuerpo perfecto de característica $p > 0$, $W = W(k)$ sus vectores de Witt, $K_0 = Frac(W)$, K una extensión finita totalmente ramificada de K_0 de grado e. Sea $\bar{K}$ una clausura algebraica de K y $G_K = Gal(\bar{K}/K)$ su grupo de Galois

Un (Φ, N)-módulo filtrado es un K_0-espacio vectorial de dimensión finita, D, con un automorfismo semilineal (Frobenius), Φ, y un operador lineal y nilpotente (monodromía), N, tal que $N\Phi = p\Phi N$ junto con una filtración decreciente, separada y exhaustiva en $D \otimes_{K_0} K$.

Fontaine y Colmez probaron [Invent. Math. **140** 2000] la conocida como Conjetura de Fontaine, es decir, que un (Φ, N)-módulo "débilmente admisible"(propiedad que depende de Frobenius y de la filtración) es en realidad "admisible"(propiedad que depende de las representaciones del Grupo de Galois G_K).

Antes de este prueba definitiva, los únicos resultados que se tenían imponían condiciones a la longitud de la filtración o al índice de ramificación, por ejemplo, que la longitud de la filtración y el índice de ramificación fuesen más peque?os que p, como en el artículo de C. Breuil [Invent. Math. **136** 1999]. Estas pruebas se basaban en la construcción de un retículo dentro de un módulo asociado a D que fuera "fuertemente divisible"(propiedad que relaciona la acción de Frobenius en la filtración con el retículo). La existencia de este retículo es equivalente al hecho de que el módulo sea "débilmente admisiblez usando este retículo se obtenía que el (Φ, N)-módulo era "admisible".

En este trabajo construimos retículos "fuertemente divisibles"sin limitación ninguna a la longitud de la filtración ni al índice de ramificación obteniendo que el módulo es débilmente admisible si y sólo si tiene un retículo "fuertemente divisible", obteniendo así una versión "entera"de la prueba de la conjetura de Fontaine.

Para ello, usamos las potencias divididas de nivel superior introducidas por P. Berthelot y construimos un anillo S_m, un S_m-módulo, $\mathcal{D}$, asociado a D y un módulo "fuertemente divisible", $\mathcal{M}$, de $\mathcal{D}$. La línea general de la demostración es la misma que la del artículo de C. Breuil antes citado, aunque para evitar limitaciones tenemos que tomar en consideración con más cuidado la acción de Frobenius.

Modelos estables de curvas elípticas, "ring class fields" y multiplicación compleja

Jordi Guàrdia, Eugenia Torres y Montserrat Vela
Universitat Politènica de Catalunya
guardia@mat.upc.es, eugenia@mat.upc.es, Montse.Vela@upc.es

En este trabajo introducimos un nuevo modelo para curvas elípticas sobre anillos de característica impar yestudiamos sus propiedades y su utilizaci ón en cálculos numéricos.

Son particularmente interesantes en el caso de curvas elípticas con multiplicación compleja, para las cuales proporcionan ecuaciones estables muy simples. Los invariantes asociados a estos modelos nos permiten la construcción de manera sencilla de ciertos "ring class fields" de órdenes cuadráticos imaginarios, con interesantes consecuencias teóricas y utilidad práctica en cálculos numéricos.

Representaciones de Galois y grupos de Galois sobre $\mathbb{Q}$

Núria Vila
Departament d'Àlgebra i Geometria. Facultat de Matemàtiques.
Universitat de Barcelona, Gran Via 585, 08007 Barcelona.

La acción del grupo de Galois absoluto del cuerpo de los racionales sobre ciertos objetos aritmético-geométricos da lugar a familias de representaciones de Galois p-ádicas y módulo p, p primo. El estudio de estas representaciones ha sido una herramienta clave para el tratamiento de problemas diofánticos y para la obtención de importantes resultados sobre propiedades aritméticas de objetos geométricos. En esta charla presentaremos representaciones de Galois geométricas y modulares para las que podemos tener un control efectivo de las imágenes de las representaciones modulo p, en el sentido de dar condiciones explícitas que nos garanticen que dichas imágenes son "tan grandes como es posible". Esto nos permite contribuir al problema inverso de la teoría de Galois al obtener realizaciones de nuevas familias de grupos lineales sobre cuerpos finitos como grupos de Galois sobre el cuerpo de los racionales.