MINISTERIO DE ECONOMIA Y COMPETITIVIDAD

Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia

Áreas Temáticas

Área temática de gestión: Matemáticas
Subárea temática de Matemáticas
Área ANEP preferente Matemáticas
Área ANEP secundaria
Código NABS: 120122 - I+D relativa a la Ingeniería financiada con FGU
Clasificaciones Unesco: 1201 - ALGEBRA
1204 - GEOMETRIA
1205 - TEORIA DE NUMEROS
1210 - TOPOLOGIA

Información Proyecto

Título:
GEOMETRÍA, TOPOLOGÍA, ÁLGEBRA Y CRIPTOGRAFÍA EN SINGULARIDADES Y SUS APLICACIONES
Title:
GEOMETRY, TOPOLOGY, ALGEBRA AND CRIPTOGRAPHY OF SINGULARTIES AND THEIR APLICATIONS
Acrónimo: SING2016
Tipo de proyecto: Tipo B
Duración (años): 4

Modalidad: Coordinado **Tipo de proyecto coordinado:** Coordinador
Id. del proyecto: 345576886-76886-4-16
Régimen de subvención: Costes Marginales
¿Considera que su proyecto tiene un marcado carácter multidisciplinar? SI
Explique que áreas
GEOMETRÍA,TOPOLOGÍA,ÁLGEBRA,CRIPTOGRAFIA

Palabras clave:
Singularidades, Arcos, Polinomio-Bernstein, Orbifolds, Geometría dimensión-1-2, monodromía, criptografía post-cuántica

Key words:
Singularities, Arc spaces, Berstein polynomial, Orbifolds, low dimensional geometry, monodromy, post-quantum criptography.

Resumen:
El proyecto de investigación que aquí presentamos gira en torno a diversos aspectos que consideramos muy relevantes de la Teoría de Singularidades en su carácter más transversal. El propósito de este proyecto es doble: por una parte la resolución

de problemas bien conocidos que puedan tener una interpretación o un posible abordaje desde la Teoría de Singularidades, y por otra parte la indagación sobre las relaciones profundas entre las diversas áreas de conocimiento en torno a la Teoría de Singularidades.
Los problemas que se plantean son teóricos, pero también y de manera cada vez más dominante, lo son prácticos, efectivos y de computación. Por ejemplo, esto queda patente tanto en nuestra aproximación a la Criptografía, a la Teoría de Grupos (grupos de trenzas, grupos de Artin), la Topología de Variedades Algebraicas, la Geometría de baja dimensión o los problemas relacionados con el recuento de puntos enteros en polígonos racionales.
Seguimos desarrollando nuestros vínculos con grupos de investigación nacionales e internacionales, que actualmente agrupan a investigadores de más de 15 universidades y centros de investigación con los cuales hemos tenido colaboraciones en los últimos años que se han traducido por ejemplo en estancias, en publicaciones y en la organización de congresos y otras reuniones internacionales.
Este enfoque ha demostrado su eficacia en los proyectos anteriores que hemos desarrollado y nos permite avanzar en el conocimiento, en la excelencia y en la formación de investigadores para el futuro.
Los problemas se agrupan brevemente en las siguientes líneas generales:
1. Teoría local de singularidades. Nos centramos en el estudio local de singularidades de curvas, de superficies, de hipersuperficies (conjetura de la monodromía), de funciones polinómicas (fibra de Milnor), de la modificación de Nash, de familias equisingulares y de espacios de arcos.
2. Aspectos globales de singularidades. En esta línea se incluye el estudio de aplicaciones polinómicas y foliaciones, configuraciones de hiperplanos y conjetura de Terao, clasificación de curvas racionales cuspidales.
3. Topología de Variedades Algebraicas y de baja dimensión. Aquí incluimos aspectos topológicos de complementarios de hipersuperficies proyectivas y de variedades casi-proyectivas en superficies tipo del Pezzo, conjetura del K(pi,1), casi-proyectividad de grupos de Artin, escisiones de Heegaard explícitas de variedades de grafo
4. Geometría birracional y de baja dimensión. Estudiamos desde el punto de vista algebraico series generatrices de variedades y aplicaciones de la estructura de potencias desde el punto de vista geométrico (estructuras geométricas) y desde el punto de vista topológico (cirugía de Dehn).

Summary:
The project we present here revolves around different aspects we consider very relevant of Singularity Theory from a transversal perspective. Our purpose is twofold: on the one hand, the resolution of well-known problems which can be interpreted or addressed from Singularity Theory, and on the other hand the understanding of the deep relations the different areas of knowledge around Singularity Theory.
Such problems are theoretical, but they are also, and in an increasing way, practical, related to effectiveness and computational. For instance, this is especially evident in our approach to Cryptography, to Group Theory (braid groups, Artin groups), the Topology of Algebraic Varieties, low-dimensional Geometry or Combinatorial problems such as lattice-point counting on rational polytopes.
We continue to intensify our ties to national and international research groups, bringing together over 15 universities and other research institutions, with which we have collaborations in the recent years. These collaborations have resulted into research stays, publications, conference organization, and organization of other international meetings.
This perspective has shown to be fruitful in previous research projects lead by our team and it allows us to progress in the knowledge of the problems, to advance in the achievement of excellence, and to prepare young researchers for the continuation of this direction.
The different questions are organized as follows:
1. Local theory of singularities. We focus our interest in the study of curve, surface, and hypersurface singularities (monodromy conjecture), singularities of polynomial maps (Milnor fiber), properties of the Nash modification, arc spaces and equisingular families.
2. Global aspects of singularities. This approach includes the study of polynomial maps and foliations, hyperplane arrangements and Terao's conjecture, as well as classification of rational cuspidal curves.
3. Topology of Algebraic Varieties and in low dimension. Topological aspects of complements to projective hypersurfaces are included here,a s well as quasi-projective surfaces in del Pezzo surfaces, K(pi,1) conjecture, quasi-projectivity problem for Artin groups, explicit Heegaard splittings of graph manifolds, generating series for varieties and applications of the power structure, and orbifold pencils.
4. Birational and low-dimensional geometry. We consider from an algebraic point of view generating series for varieties and applications of the power structure; from a geometric point of view (geometric structures); and from a topological point of view (Dehn surgery).
5. Applications to Group Theory, such as the study of the homology groups of kernels of Artin groups, and quasi-projectivity of link groups.
6. Applications to Cryptography, including Post-quatum cryptography with multivariate systems (MS), new multivariate cryptographic primitives, and MS-cryptoanalysis using Gröbner bases.
7. Other Applications, such as counting lattice points in rational polytopes, and library developing in SAGE for coordinate components, braid monodromy, knot invariants, zeta functions, Bernstein polynomials, Alexander modules, and representations of infinite groups.