IV Congreso de Jóvenes Investigadores
Real Sociedad Matemática Española
Valencia, 4-8 de septiembre de 2017

Primos de mala reducción de curvas de género 3 con CM

E. Lorenzo García*

Saber construir curvas sobre cuerpos finitos con un número de puntos dado es importante por ejemplo para la criptografía. Un método para construir este tipo de curvas es el método de la multiplicación compleja. Este método permite construir una curva sobre los números complejos cuya reducción módulo p tiene el número de puntos buscado.

Para género 1 y género 2 este método es una realidad y está implementado en SAGE. Para implementar este método en género 3 necesitamos acotar los denominadores de unos números racionales asociados a invariantes de estas curvas, de este modo, por aproximación numérica y con una precisión adecuada podemos calcular los valores exactos. En ciertos casos de interés, los primos que aparecen en estos denominadores resultan ser primos de mala reducción de las curvas. En esta charla mostraremos como calcular una cota para estos primos siguiendo los artículos [1] y [2]. Además, mostratremos como determinar los exponentes con los que aparecen estos primos con las estrategias en [3].

Las curvas de género 3 son las curvas de género más pequeño con un comportamiento genérico y extrapolable a curvas de cualquier género, de ahí su interés.

Referencias

[1] I. Bouw, J. Cooley, K. Lauter, E. Lorenzo García, M. Manes, R. Newton, E. Ozman. *Bad reduction of genus 3 curves with complex multiplication*. Women in Numbers Europe, research Directions in Number Theory, Springer (2015), 109-151.

[2] P. Kılıçer, K. Lauter, E. Lorenzo García, R. Newton, E. Ozman, M. Streng. *A bound on the primes of bad reduction of CM curves of genus 3*. Envíado.

[3] S. Ionica, P. Kılıçer, K. Lauter, E. Lorenzo García, A. Manzateanu, M. Massierer, C. Vincent. *Towards a formula for denominators of class invariants in genus 3*. Envíado.

*IRMAR, Université de Rennes 1, Campus de Beaulieu, bât. 22-23, 35420, Rennes, Francia. Email: elisa.lorenzogarcia@univ-rennes1.fr