Curvas elípticas e integrales multiplicativas sobre campos no arquimedianos

Yamidt Bermúdez Tobón
Interdisciplinary Center for Scientific Computing (IWR)
Universidad de Heidelberg, Heidelberg, Alemania
e-mail: yamidt.bermudez-tobon@iwr.uni-heidelberg.de

Universidad del Valle, Departamento de Matemáticas
Agosto de 2014

Resumen

En la primera parte de la conferencia introduzco las curvas elípticas, las cuales son una de las áreas más estudiadas en teoría de números. Estas son curvas algebraicas para las que existe un simple método que permite construir un tercer punto a partir de dos iniciales, además permiten definir una estructura de grupo sobre ellas. Los cálculos con curvas elípticas arrojan muchas conjeturas interesantes, entre ellas la de *Birch y Swinnerton-Dyer*. En las últimas décadas estas han ganado bastante terreno en aplicaciones como la factorización de enteros y la criptografía.

En la segunda parte de la conferencia presentaré los resultados de mi tesis doctoral, realizada bajo la supervisión del Prof. Dr. Gebhard Boeckle y el Dr. Juan Marcos Cerviño. El objetivo de mi trabajo fue listar todas las curvas elípticas de complejidad baja sobre un campo global. Aquí la complejidad se mide por medio del conductor. Los campos globales más simples son los números racionales $\mathbb{Q}$ y para cada número primo p el campo $\mathbb{F}_q(T)$ (el campo de cocientes de polinomios con coeficientes en el campo finito $\mathbb{F}_q$). Existen teoremas sorprendentes que relacionan curvas elípticas de un conductor dado con curvas modulares del nivel del conductor. Sobre los racionales estos teoremas se deben a varios autores, entre ellos *Andrew Wiles* y *Richard Taylor*, el cual fue el punto clave en la demostración de *el último teorema de Fermat*. Sobre $\mathbb{F}_q(T)$ el resultado relaciona curvas elípticas con curvas modulares de *Drinfeld*. Las curvas modulares tienen una estructura analítica compleja y las formas modulares de *Drinfeld* una descripción analítica π-ádica, donde π es el uniformizador en el infinito $1/T$. La pregunta es como pasar del lado analítico al lado algebraico de la curva elíptica deseada cuyos coeficientes son enteros en el

caso $\mathbb{Q}$ o polinomios en el caso $\mathbb{F}_q(T)$. Para el caso de los números racionales existe un algoritmo que se conoce desde los años 70. Para el caso de $\mathbb{F}_q(T)$ nosotros desarrollamos un algoritmo efectivo que permite encontrar las ecuaciones en tiempo polinomial. En nuestro caso la complejidad radica en las integrales multiplicativas.

Palabras claves

Curvas elípticas, Formas modulares, Arboles de Bruhat-Tits y Funciones Theta.

Referencias

[1] Darmon, Henri. Rational Points on Modular Elliptic Curves. American Mathematical Soc. Heidelberg, 2004.

[2] Gekeler, Ernst-Ulrich. Analytical construction of Weil curves over function fields. J. Théor. Nombres Bordeaux, 7(1):27-49, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).

[3] Reversat, M; Gekeler, E.-U. Jacobians of Drinfeld modular curves. Journal für die reine und angewandte Mathematik, 476:27-94, 1996.

[4] Greenberg, Matthew. An introduction to group rings. Heegner points and rigid analytic modular forms. PhD thesis, Mcgill University, February. 2006