Reunión Anual de la Unión Matemática Argentina - Bahía Blanca, 2016

Nicolás Sirolli

`Sage`, formas modulares y curvas elípticas

El objetivo de estos ejercicios es utilizar `Sage` para, experimentalmente, encontrar la "primer" curva elíptica de *rango* 1. Los contenidos teóricos involucran algunos conceptos profundos de la Teoría de Números. A no asustarse: no hace falta manejarlos para trabajar.

El *rango* de una curva elíptica E, según predice la conjetura de Birch y Swinnerton-Dyer[1], es el único entero no negativo r tal que

$$\prod_{p \leq x} \frac{N_p(E)}{p} \approx C \log^r(x), \qquad x \to +\infty. \tag{1}$$

Aquí, $N_p(E)$ denota la cantidad de puntos de la reducción $\overline{E}/\mathbb{F}_p$.

Ejercicio 1. Escribir un algoritmo que dada una curva elíptica E devuelva su rango r, utilizando (1).
Sugerencia: Aproveche el código del póster.

El *conductor* de una curva E es un entero positivo N divisible exactamente por los primos en los que E tiene mala reducción.

Eichler y Shimura exhibieron una construcción que, dada una forma modular cuspidal de nivel N, *nueva* y con coeficientes racionales, devuelve una curva elíptica $E/\mathbb{Q}$ de conductor N tal que para todo primo de buena reducción p de E se tiene

$$\lambda_p(f) = p + 1 - N_p(E). \tag{2}$$

Aquí, $\lambda_p(f)$ es el autovalor del p-ésimo operador de Hecke actuando en f.

Ejercicio 2. Escribir un algoritmo que dada una forma modular cuspidal f, nueva y con coeficientes racionales, devuelva el rango de la curva elíptica correspondiente, utilizando 2.
Sugerencia: Con `CuspForms(N)` se construye el espacio de formas cuspidales de nivel N. Analice los métodos de los que dispone esta clase.

Según probaron Wiles y otros, toda curva elíptica $E/\mathbb{Q}$ es modular. Esto es, la construcción de Eichler y Shimura es sobreyectiva. En particular, podemos obtener todas las curvas elípticas de conductor N a partir de todas las formas modulares cuspidales, nuevas y con coeficientes racionales, de nivel N.

Ejercicio 3. Escribir un algoritmo que encuentre el primer entero positivo N para el cual existe una curva elíptica $E/\mathbb{Q}$ de conductor N y rango 1.

La construcción de Eichler y Shimura se puede hacer efectiva, cosa que es deseable si queremos conocer explícitamente la curva recién hallada.

Ejercicio 4*. Escribir un algoritmo que, dada una forma modular cuspidal, nueva y con coeficientes racionales, devuelva la curva elíptica correspondiente.
Sugerencia: Ver el comienzo del capítulo XI del libro *Elliptic Curves*, de Anthony Knapp.

Ejercicio 5**. Explique por qué la cuenta de Twitter de William Stein, el creador de `Sage`, se llama `@wstein389`.

[1] Uno de los problemas del U$S 10^6 del Clay Mathematics Institute.