La conjetura de Watkins para torcimientos cuadráticos[1]

Héctor Pastén

Pontificia Universidad Católica de Chile

Seminario Latinoamericano de Teoría de Números

[1]Trabajo en conjunto con José A. Esparza-Lozano

Rango

Sea E una curva elíptica sobre $\mathbb{Q}$. El teorema de Mordell da

$$E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^{r(E)}$$

donde T es un grupo abeliano finito y $r(E) \geq 0$ es el rango de E.

- T se sabe calcular (Nagell-Lutz)
- $r(E)$ solo bajo conjetura. Pero se puede acotar incondicionalmente:

La demostración del teorema de Mordell construye una función inyectiva

$$E(\mathbb{Q})/2E(\mathbb{Q}) \simeq T[2] \oplus \mathbb{F}_2^{r(E)} \longrightarrow Sel_2(E) \simeq \mathbb{F}_2^{d(E)}$$

donde $Sel_2(E)$ es finito y calculable. Esto da

$$r(E) \leq r(E) + \dim_{F_2} T[2] \leq d(E).$$

(Teóricamente se puede usar $Sel_n(E)$, pero $n = 2$ es más práctico.)

Cotas calculables para $r(E)$

Un caso muy conveniente donde podemos acotar $Sel_2(E)$ para así acotar $r(E)$ es cuando $T[2] \neq (0)$.

Ahí se puede calcular $Sel_2(E)$ con un 2-descenso sobre $\mathbb{Q}$ obteniendo

$$r(E) \leq 2 \cdot \omega(\Delta_E) - 1$$

donde Δ_E es sl discriminante minimal de E y $\omega(n)$ es el número de factores primos de n.

Ejemplo. $E : y^2 = x^3 + x^2 + x + 1$ tiene $\Delta_E = -2^8$ por lo que

$$r(E) \leq 2 \cdot 1 - 1 = 1.$$

De hecho en este caso $r(E) = 1$.

Algunos problemas sobre $r(E)$

Probablemente, el problema más famoso sobre $r(E)$ es la **conjetura BSD** que predice

$$\mathrm{ord}_{s=1} L(E,s) = r(E).$$

Salvo ejemplos particulares con $r(E) \leq 3$, hasta ahora solo se sabe en casos donde alguno de los dos lados de la ecuación es 0 o 1.

Pero hay otros problemas interesantes:

- **Conjetura de Tate-Shafarevich**. $Sha_{2^\infty}(E)$ es finito. En particular, $r(E)$ es calculable.
- **Problema de los rangos acotados.** ¿Existen curvas elípticas E con $r(E)$ tan grande como se quiera? ¿Y si solo variamos en una familia de twists cuadráticos $E^{(D)}$?
- **Conjetura de Watkins.** Sea $m(E)$ el grado de una parametrización modular $X_0(N) \to E$ sobre $\mathbb{Q}$. Entonces $2^{r(E)}$ divide $m(E)$.

Más sobre la conjetura de Watkins

El teorema de modularidad de Wiles, Taylor-Wiles, Breuil-Conrad-Diamond-Taylor nos da una **parametrización modular**

$$\phi : X_0(N) \to E$$

definida sobre $\mathbb{Q}$, donde $N =$ conductor de E. No es única, pero la elegimos del menor grado posible. El **grado modular** es

$$m(E) = \deg(\phi).$$

Conjetura de Watkins ($\sim$ 2001). Tenemos que $2^{r(E)}$ divide a $\deg(\phi)$.

Ejemplo. $X_0(11)$ tiene género 1. Tomando $E = X_0(11)$ y $\phi : X_0(11) \to E$ la identidad, nos da $m(E) = 1$. La conjetura de Watkins implicaría

$$r(X_0(11)) = 0, \quad \text{lo que es correcto.}$$

Evidencia

- Montones de ejemplos calculados. De hecho, los ejemplos sugieren algo más cercano a " $2^{d(E)}|m(E)$ ", que sería más fuerte.
- **Trivial**: Si $r(E) = 0$ todo OK. Esto da infinitos ejemplos.
- **Heurística** (Dummigan): $Sel_2(E) \dashrightarrow Sel_2(Sym^2 E)$.
  Asumiendo "$R = \mathbb{T}$" 2-ádico, $\#Sel_2(Sym^2 E) = \eta_2 \sim_2 \deg(\phi)$.
- **Caso especial** (abierto): "Si $m(E)$ es impar entonces $r(E) = 0$".

  Gracias a Calegari-Emerton, Yazdani, y Kazalicki-Kohen se sabe una **versión débil de este caso especial**:

  Si el *número de congruencia* de E es impar, entonces $r(E) = 0$.

  Nota. Stein conjetura que hay hay infinitas E con $m(E)$ impar, pero no se sabe. Así que no sabemos si esto da infinitos ejemplos de la versión débil.

Resultado principal

Teorema (J. Esparzal-Lozano, H. Pasten '20)

Sea E con $E(\mathbb{Q})[2] \neq (0)$ y tal que su conductor N es minimal entre sus twists cuadráticos. Hay un cierto B_E que solo depende de E, tal que para cualquier discriminante fundamental D que cumpla $\omega(D) \geq B_E$, la curva $E^{(D)}$ satisface la conjetura de Watkins.

- B_E es explícito y efectivo.
- Obtenemos incondicionalmente infinitos ejemplos no-triviales.
- Concluimos que las excepciones a la conjetura de Watkins en una familia de twists cuadráticos son escasas (si es que hay):

$$\#\{|D| < x : E^{(D)} \text{ no cumple Watkins}\} \ll_E \frac{x(\log\log x)^{\kappa_E}}{\log x}.$$

Esto suponiendo que $E(\mathbb{Q})$ tiene 2-torsión no-trivial.

Plan de la demostración

- Fórmula analítica para $m(E)$.
- Estudiar como cambian las partes de esa fórmula analítica bajo twist cuadrático.
- Concluir que $v_2(m(E^D))$ crece cuando $\omega(D)$ crece.
- Acotar $r(E)$ en términos del número de factores primos de D. Esto es posible gracias a los grupos de Selmer.
- *Bajo la hipótesis que $E(\mathbb{Q})$ tenga 2-torsión no-trivial*, resulta que la cota superior de $r(E^{(D)})$ es $2\omega(D) + cte.$, mientras que la cota inferior de $v_2(m(E^D))$ es $3\omega(D) - cte.$ $\square$

El resto de la charla daremos los detalles de la demostración.

Altura de Faltings

Dada E curva elíptica sobre $\mathbb{Q}$ su diferencial global de Neron es ω_E (único salvo signo). La **altura de Faltings de** E es cierto grado de Arakelov que en este caso se puede escribir

$$h(E) = -\frac{1}{2}\log\left(\frac{i}{2}\int_{E(\mathbb{C})}\omega_E \wedge \overline{\omega_E}\right).$$

Silverman demostró

$$h(E) = \frac{1}{12}\left(\log|\Delta_E| - \log\left|\Delta(\tau_E)\Im(\tau)^6\right|\right) - \log(2\pi)$$

con $\Delta_E =$ discriminante minimal, $\tau_E \in \mathfrak{h}$ corresponde a E, y

$$\Delta(z) = q\prod_n (1-q^n)^{24} \in S_{12}(SL_2(\mathbb{Z})), \quad q = e^{2\pi i z}.$$

Variación de la altura de Faltings

Para medir la variación de la altura de Faltins definimos

$$\delta(E_1, E_2) = \exp(2h(E_1) - 2h(E_2)).$$

Lema

Si E_2 es un twist cuadrático de E_1 entonces $\delta(E_1, E_2) \in \mathbb{Q}^\times$ y se cumple

$$|v_2(\delta(E_1, E_2))| \leq 3.$$

Idea. Lo único que cambia bajo twist en la fórmula de Silverman

$$h(E) = \frac{1}{12}\left(\log|\Delta_E| - \log\left|\Delta(\tau_E)\Im(\tau)^6\right|\right) - \log(2\pi)$$

es el discriminante minimal Δ_E, y su variación bajo twist es conocida. □

Norma de Petersson

Para una forma cuspidal

$$f = a_1(f)q + a_2(f)q^2 + \ldots \in S_2(\Gamma_0(N))$$

su norma de Petersson (no normalizada) es

$$\|f\|_N = \left(\int_{\Gamma_0(N)\backslash\mathfrak{h}} |f(z)|^2 dx \wedge dy\right)^{1/2}, \quad z = x + iy.$$

Si f es una newform (con $a_1(f) = 1$), el método de desdoblamiento de Rankin-Selberg da la fórmula clásica (Shimura)

$$L(Sym^2_{imp} f, 1) = 8\pi^3 \cdot \frac{\|f\|_N^2}{N}.$$

donde usamos el cuadrado simétrico imprimitivo.

Variación de la norma de Petersson

Para una curva elíptica E, sea $f_E \in S_2(\Gamma_0(N))$ su forma modular asociada.

Lema

Sea E tal que su conductor N es minimal entre sus twists cuadráticos. Sea D discriminante fundamental y sea $N^{(D)}$ el conductor de $E^{(D)}$. Sea $\mathscr{P}(D,N) = \{p : p|D, p \nmid 2N\}$. Entonces $R := \|f_{E^{(D)}}\|^2_{N^{(D)}} / \|f_E\|^2_N \in \mathbb{Q}^\times$ y se cumple

$$v_2(R) + 1 \geq \sum_{p \in \mathscr{P}(D,N)} v_2\left((p-1)(p+1-a_p(E))(p+1+a_p(E))\right).$$

Idea. La fórmula de Shimura transforma el problema en un análisis del cambio de $L(Sym^2_{imp} f_E, s)$ bajo twist cuadrático de E
Esto es bien explícito: $L(Sym^2_{imp} f_E, s)$ pierde factores de Euler para $p \in \mathscr{P}(D,N)$ y otras modificaciones para $p|\mathrm{mcd}(D,N)$. Es engorroso, pero Delaunay ya calculó estos factores en detalle. $\square$

La constante de Manin

f_E se relaciona con E de varias maneras, por ejemplo, $L(f_E, s) = L(E, s)$. Hay una relación geométrica usando $\phi : X_0(N) \to E$:

$$\phi^*\omega_E = 2\pi i c_E f_E(z)dz$$

viendo $X_0(N) = \Gamma_0(N)\backslash\mathfrak{h}^*$.

Aquí, c_E es la **constante de Manin**: a priori es racional, y un análisis de modelos enteros (Edixhoven) muestra que $c_E \in \mathbb{Z}$.

Fórmula analítica para $m(E)$

De la ecuación

$$\phi^*\omega_E = 2\pi i c_E f_E(z)dz$$

por integración deducimos que

$$\deg(\phi)\cdot\frac{i}{2}\int_{E(\mathbb{C})}\omega_E\wedge\overline{\omega_E} = 4\pi c_E^2\|f_E\|_N^2.$$

Esto da una fórmula clásica estudiada por Frey, Silverman, Szpiro y otros:

$$\boxed{m(E) = 4\pi c_E^2\|f_E\|_N^2\exp(2h(E))}$$

Cota inferior para $v_2(m(E^{(D)}))$

Por la fórmula analítica tenemos

$$\frac{m(E^{(D)})}{m(E)} = \frac{c_{E^{(D)}}^2}{c_E^2} \cdot \frac{\|f_{E^{(D)}}\|_{N^{(D)}}^2}{\|f_E\|_N^2} \cdot \delta(E^{(D)}, E).$$

Del trabajo anterior y del hecho que $c_{E^{(D)}} \in \mathbb{Z}$, obtenemos

Lema

Si E es de conductor minimal entre sus twists cuadráticos, entonces

$$\begin{aligned} v_2(m(E^{(D)})) \geq & v_2(m(E)/c_E^2) - 4 \\ & + \sum_{p \in \mathscr{P}(D,N)} v_2\left((p-1)(p+1-a_p(E))(p+1+a_p(E))\right). \end{aligned}$$

El truco ahora es forzar que la sumatoria sea grande.
Veremos que cuando $E(\mathbb{Q})[2] \neq (0)$, cada sumando es ≥ 3.

Juntando todo cuando $E(\mathbb{Q})[2] \neq (0)$

Cuando $p \nmid 2N$ tenemos que $E(\mathbb{F}_p)$ contiene una copia de $E(\mathbb{Q})[2]$. Así que $E(\mathbb{Q})[2] \neq (0)$ implica

$$p + 1 - a_p = \#E(\mathbb{F}_p) \equiv 0 \bmod 2.$$

Pero $p + 1$ es par, así que a_p es par, obteniendo

$$p + 1 + a_p \equiv 0 \bmod 2.$$

Obviamente $p + 1$ es par, por lo tanto

$$v_2\left((p-1)(p+1-a_p(E))(p+1+a_p(E))\right) \geq 3.$$

De este modo el lema anterior da

$$\boxed{v_2(m(E^{(D)}) \geq 3\omega(D) + v_2(m(E)/c_E^2) - (7 + 3\omega(N))}.$$

Juntando todo cuando $E(\mathbb{Q})[2] \neq (0)$

Recordemos que cuando $E(\mathbb{Q})[2] \neq (0)$, la cota del 2-descenso para grupos de Selmer daba

$$r(E) \leq 2\omega(N) - 1.$$

Importante: $E^{(D)}[2] \simeq E[2]$ así que también obtenemos

$$r(E^{(D)}) \leq 2\omega(N^{(D)}) - 1 \leq 2\omega(ND^2) - 1 \leq 2\omega(D) + 2\omega(N) - 1.$$

Finalmente, cuando $\omega(D) \geq 6 + 5\omega(N) - v_2(m(E)/c_E^2)$ se cumple

$$\begin{aligned} r(E^{(D)}) &\leq 2\omega(D) + 2\omega(N) - 1 \\ &\leq 3\omega(D) + v_2(m(E)/c_E^2) - (7 + 3\omega(N)) \\ &\leq v_2(m(E^{(D)})). \end{aligned}$$

La cantidad $B_E = 6 + 5\omega(N) - v_2(m(E)/c_E^2)$ solo depende de E. $\square$

Comentarios finales

(1) En este caso obtenemos una versión fuerte de la conjetura de Watkins, porque usamos la cota superior de $r(E)$ que viene de $Sel_2(E)$.

(2) Nuestra cota inferior de $v_2(m(E))$ viene de un análisis de $L(Sym^2 E, s)$, y dicha cota inferior se combina con una cota superior para $Sel_2(E)$. Esto es curioso: en la heurística de Dummigan, $v_2(m(E))$ se controla con $Sel_2(Sym^2(E))$, y se usa como cota superior de $Sel_2(E)$.

(3) Que yo sepa, este es el primer resultado incondicional que da infinitos casos no-triviales de la conjetura de Watkins. Aún así, el artículo tiene 4 páginas, de las cuales la primera es introducción y la última bibliografía.

(4) Mi estudiante Jerson Caro recientemente demostró la versión fuerte de la conjetura de Watkins en varios casos nuevos, entre ellos, todas las curvas elípticas "congruentes" $y^2 = x^3 - n^2 x$.

Gracias por su atención