JTN 2015
Universidad de Valladolid
June 29-July 3, 2015

On Singular Moduli for Picard Curves

K. Lauter[1], E. Lorenzo[2] (Charla presentada por la segunda autora)

[1] *Microsoft Research Cryptography group, Redmond, EEUU*
[2] *Universiteit Leiden, Leiden, Holanda, e.lorenzo.garcia@math.leidenuniv.nl*

En 1985, Gross y Zagier [6] prueban que el siguiente número es entero y calculan su factorización:

$$J(d_1,d_2)=\left(\prod_{disc(\tau_i)=d_i}(j(\tau_1)-j(\tau_2))\right)^{\frac{w_1w_2}{4}}, \tag{1}$$

donde d_1 y d_2 son discriminantes fundamentales de cuerpos cuadráticos imaginarios $K_i=\mathbf{Q}(\sqrt{d_i})$, el productorio recorre representantes τ_1 y τ_2 de elementos del semiplano superior con discriminante d_i modulo la acción de $\mathbf{SL}_2(\mathbf{Z})$, y w_i denota el número de raíces de la unidad en K_i.

Claramente, si d_1 y d_2 son diferentes, las diferentes curvas con j-invariante $j(\tau_1)$ y $j(\tau_2)$ no son isomorfas entre sí y el número $J(d_1,d_2)$ es no nulo. Ahora bien, módulo un número primo p que divida a $J(d_1,d_2)$, obtenemos que al menos dos de las reducciones de estas curvas modulo p si que son isomorfas. Más concretamente, $J(d_1,d_2)$ puede reinterpretarse como el número de isomorfismos entre la reducción de las curvas elípticas E_i asociadas a los elementos τ_i modulo diferentes primos mediante la siguiente expresión

$$v_p(j_1-j_2)=\frac{1}{2}\sum_n \#\mathbf{Isom}_n(E_1,E_2), \tag{2}$$

Donde el subíndice n indica el número de isomorfismo módulo p^n. Este número, también puede reinterpretarse como el número de embeddings

$$\iota:\mathbf{End}(E_2)\hookrightarrow \mathbf{B}_{p,\infty}, \tag{3}$$

satisfaciendo ciertas propiedades. Lauter y Viray generalizan este resultado para discriminantes arbitrarios en [9].

La siguiente generalización natural es el estudio del caso de género 2. En primer lugar debe sustituirse el $j-$inavariante por los invariantes de Igusa para superficies abelianas (o curvas de género 2). En este caso, los números que se obtienen no son enteros, aunque siguen siendo racionales. El estudio de los denominadores [2, 3, 4, 12, 13] tiene aplicaciones en criptografía [11] y está relacionado con el estudio del equivalente al embedding (3) en dimensión 2. También está relacionado con este embedding el estudio de los numeradores de estos números [5, 10], que a su vez están relacionados con el número de isomorfismos entre las reducciones de las jacobianas de curvas de género 2 con multiplicación compleja.

Por último, para género 3, no disponemos de invariantes equivalentes. Por ejemplo, los invariantes de Dixmier-Ohno para cuárticas planas lisas, i.e., curvas no hiperelípticas de género 3, no son modulares, luego no sirve para este propósito. Por tanto, tenemos que conformarnos con estudiar el problema de la existencia o no de ciertos embeddings de órdenes de cuerpos de multiplicación compleja de grado 6 en las matrices de tamaño 3 por 3 con entradas en el álgebra de quaterniones $\mathbf{B}_{p,\infty}$, [1, 8].

$$\iota:\mathscr{O}\subseteq K\hookrightarrow \mathscr{M}_3(\mathbf{B}_{p,\infty}). \tag{4}$$

Además de no disponer de invariantes equivalentes, en el caso de dimensión 3 aparecen nuevos incovenientes. Por ejemplo, hasta dimensión 2, la existencia de una solución al problema de embedding resulta equivalente a la mala

reducción módulo p de una de las curvas de partida, y además el tipo de mala reducción es único. En dimensión 3 esto ya no se cumple, con lo que tenemos que añadir restricciones en el tipo de mala reducción y en vez de un enunciado del tipo "si y sólo si", obtenemos una cota [1]:

Teorema 6.8**:** Sea C una curva de género 3 con multiplciación compleja por un cuerpo $K = \mathbf{Q}(\sqrt{\alpha})$ de grado 6 y que no contiene ningún cuerpo cuadrático imaginario. Entonces, los primos de mala reducción de C que dan lugar a 3 componentes irreducibles, están acotados por $4(\mathbf{Tr}(\alpha)/3)^6$.

La condición de que el cuerpo de multiplicación compleja K no contenga un cuerpo cuadrático imaginario surge de nuevo por una diferencia entre el caso de dimensión menor o igual que 2 y mayor o igual que 3. A partir de dimensión 3 la condición que un tipo de multiplicación compleja sea primitivo ya no es equivalente a que el cuerpo de multiplicación compleja contenga o no un cuerpo cuadrático imaginario. Por tanto debemos añadir esa condición extra. En el artículo [8], añadimos las condiciones necesarias a pedir al problema de embedding para que el hecho de que tenga solución sea equivalente a la mala reducción de la curva. Además, somo capaces de dar un resultado equivalente al teorema 6.8 arriba enunciado, en el que relajamos las condiciones sobre el tipo de reducción y la existencia o no de cuerpo cuadráticos imaginarios.

Como consecuencia de los resultados obtenidos en [8] y siguiendo la línea del árticulo original de Gross y Zagier [6], en esta charla estudiaremos la fórmula equivalente de la factorización del número (1) para curvas de Picard con multiplicación compleja. Estas curvas son un caso particular de curvas no hiperelípticas de género 3 con multiplicación compleja por un cuerpo que contiene a $\mathbf{Q}(\sqrt{-3})$. Además explicaremos como esta fórmula mejora el algoritmo descrito en [7].

Una curva de Picard es una curva trigonal cíclica de género 3. Una curva de Picard definida sobre un cuerpo k de característica diferente de 2 y 3 puede escribirse de la forma:

$$C : y^3 = x^4 + g_2x^2 + g_3x + g_4, \;\; g_i \in k. \tag{5}$$

Si $g_2g_3 \neq 0$, las clases de $\bar{k}$-isomorfismo están determinadas por los invariantes:

$$j_1 = \frac{g_3^2}{g_2^3}, \;\; j_2 = \frac{g_4}{g_2^2}. \tag{6}$$

En [7], Koike y Weng, escriben estos invariantes en término de las funciones theta (invariantes modulares) y dan un algoritmo para dado un cuerpo de multiplicación compleja de grado 6 de la forma $K = K_0(\sqrt{-3})$, construir una curva de Picard con multiplicación compleja por el anillo de enteros de dicho cuerpo. Para que el algoritmo funciones siempre se necesita una cota de los primos que aparecen en los denominadores de los invariantes j_1 y j_2, pues en cierto momento se debe hacer uso del algoritmo de fracciones continuas. Pero esta cota no es conocida.

En esta charla definimos los invariantes

$$j_3 = \frac{1}{j_1} \;\; j_4 = \frac{j_2^3}{j_1^2}, \tag{7}$$

para los que somos capaces de calcular una cota para los primos que aparecen en el denominador usando técnicas similares a las empleadas en el artículo original de Gross-Zagier. Uno de los resultados clave es el siguiente:

Proposición: Se tiene la siguiente igualdad

$$v_p(j_1 - j_1') = \sum_n i(n), \tag{8}$$

donde $i(n)$ se define como

$$i(n) = \frac{\#\mathbf{Isom}(C, C')}{3}, \tag{9}$$

y donde C, C' son curvas de Picard con multiplciación compleja por un cierto orden de cuerpos de multiplicación compleja dados.

De este modo podemos modificar ligeramente el algoritmo descrito en [7] de modo que siempre termine.

References

[1] I. Bouw, J. Cooley, K. Lauter, E. Lorenzo, M. Manes, R. Newton, E. Ozman, Bad reduction of genus 3 curves with complex multiplication, submitted, arXiv:1407.3589.

[2] J. Bruinier and T. Yang, CM-values of Hilbert modular functions, Invent. Math. 163 (2006).

[3] E. Goren and K. Lauter, Evil primes and superspecial moduli, Int. Math. Res. Not. (2006).

[4] ———, Class invariants for quartic CM fields, Ann. Inst. Fourier (Grenoble) 57 (2007).

[5] ———, A Gross-Zagier formula for quaternion algebras over totally real fields, Algebra Number Theory 7 (2013).

[6] B. Gross and D. Zagier, On singular moduli, J. Reine Angew. Math. 355 (1985).

[7] K. Koike, A. Weng, Construction of CM Picard curves, Mathematics of Computation 74 - 249 (2004).

[8] K. Lauter, E. Lorenzo, R. Newton, E. Ozman, Bad reduction of genus 3 curves with complex multiplication II, in preparation.

[9] K. Lauter, B. Viray, On singular moduli for arbitrary discriminants, arXiv:1206.6942.

[10] K. Lauter, B. Viray, An arithmetic intersection formula for denominators of Igusa class polynomials, to appear in American Journal of Mathematics.

[11] M. Streng, Computing Igusa Class Polynomials, Mathematics of Computation, Vol. 83 (2014).

[12] T. Yang, An arithmetic intersection formula on Hilbert modular surfaces, Amer. J. Math. 132 (2010).

[13] ———, Arithmetic intersection on a Hilbert modular surface and the Faltings height, Asian J. Math. 17 (2013).