Bad reduction of genus 3 curves with Complex Multiplication

Elisa Lorenzo García
Universiteit Leiden

Joint work with Bouw, Cooley, Lauter, Manes, Newton, Ozman.

January 28, 2015

Index

Gross-Zagier g=1

Given coprime imaginary discriminants d_i, Gross and Zagier [GZ85] define

$$J(d_1, d_2) = \left(\prod_{\substack{[\tau_1], [\tau_2] \\ \mathrm{disc}(\tau_i) = d_i}} (j(\tau_1) - j(\tau_2)) \right)^{\frac{8}{w_1 w_2}},$$

The τ_i run over equivalence classes, and w_i is the number of units in $\mathbb{Q}(\sqrt{d_i})$.

Under some assumptions, GZ show that $J(d_1, d_2) \in \mathbb{Z}$, and their main result gives a formula for its factorization.

Lauter and Viray generalize the result for other disc. [LV14].

Gross-Zagier g=1

The **factorization of the integer** $J(d_1, d_2)$, may be reinterpreted as a formula for the **number of isomorphisms between reductions** of elliptic curves E_i corresponding to the τ_i.

$$v_l(j_1 - j_2) = \frac{1}{2} \sum_n \#\mathrm{Isom}_n(E_1, E_2).$$

That is equivalent to counting elements of $\mathrm{End}(E_2)$ of fix degree and traces, or to **counting embeddings** of

$$\iota : \mathrm{End}(E_2) \hookrightarrow B_{p,\infty}$$

satisfying certain properties.

Gross-Zagier g=2

Goren and Lauter [GL12], Bruinier and Yang [BY06],[Y10] and Lauter and Viray [LV15] prove generalization of the result of Gross–Zagier for genus 2 curves with CM.

The j-invariant is replaced by the **absolute Igusa invariants.** The function J is not anymore an integer number, but still rational.

Some of the results concern the factorization of the numerators (bad reduction, embedding problem) and others of the denominators (cryptography purposes).

Gross-Zagier g=3

- MAIN PROBLEM: there are not invariants!

Gross-Zagier g=3

- MAIN PROBLEM: there are not invariants!
- We will focus on the **embedding problem** (related with bad reduction and the **numerator** of the invariants)

$$\iota : K = \mathrm{End}^0(J(C)) \hookrightarrow \mathrm{End}^0(\overline{J(C)}) \hookrightarrow \mathcal{M}_3(B_{p,\infty})$$

Bad reduction $\Rightarrow \overline{J(C)}) \sim E^3$ with E supersingular $\Rightarrow$ we have a solution to the embedding problem

CM fields and types

Definition

A complex multiplication (CM) field K is an imaginary quadratic extension of a totally real field K^+.

Let K be a CM-field. The complex embeddings $K \hookrightarrow \mathbb{C}$ come in pairs $\{\psi, \rho \circ \psi\}$, where ρ denotes complex conjugation.

Definition

- A CM-type φ is a choice of one embedding from each of these pairs.
- A CM-type is called *primitive* if it is not induced from a CM-type on any proper CM-subfield of K.

Abelian Varieties with CM

Definition

Let A be an abelian variety and let K be a CM-field with $[K : \mathbb{Q}] = 2\dim(A)$. We say that A has *complex multiplication (CM) by K* if the endomorphism algebra

$$\mathrm{End}^0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$$

contains K. We say that a curve C has *CM by K* if its Jacobian has CM by K. If $\mathrm{End}(A)$ is an order $\mathcal{O}$ in a CM-field K with $[K : \mathbb{Q}] = 2\dim(A)$, we say that A has *CM by $\mathcal{O}$*.

Abelian Varieties with CM

Proposition (Lang)

Let A be an abelian variety with CM by K and defined over a field of characteristic zero. There is a way of defining a CM-type (K, φ) for A. The CM-type (K, φ) is primitive if and only if the abelian variety A is simple.

Abelian Varieties with CM

Proposition (Lang)

Let A be an abelian variety with CM by K and defined over a field of characteristic zero. There is a way of defining a CM-type (K, φ) for A. The CM-type (K, φ) is primitive if and only if the abelian variety A is simple.

If $g = 2$: (K, φ) primitive iff K does not contain any imaginary quadratic subfield K_1. This is not true any more if $g = 3$.

(R1) Restriction 1: we assume that K does not contain any K_1.

Curves with CM

Proposition

Let C be a genus 3 curve with CM by K. One of the following three possibilities holds for the irreducible components of $\overline{C}$ of positive genus:

(i) *(good reduction) $\overline{C}$ is a smooth curve of genus 3,*
(ii) *$\overline{C}$ has three irreducible components of genus 1,*
(iii) *$\overline{C}$ has an irreducible component of genus 1 and one of genus 2.*

Curves with CM

Proposition

Let C be a genus 3 curve with CM by K. One of the following three possibilities holds for the irreducible components of $\overline{C}$ of positive genus:

(i) *(good reduction) $\overline{C}$ is a smooth curve of genus 3,*

(ii) *$\overline{C}$ has three irreducible components of genus 1,*

(iii) *$\overline{C}$ has an irreducible component of genus 1 and one of genus 2.*

Theorem

With notation above. If $\overline{J}$ is not simple, then $\overline{J}$ is isogenous to E^3.

The main Theorem

(R2) Restriction 2: we are in case (*ii*) in previous proposition.

The main Theorem

(R2) Restriction 2: we are in case (*ii*) in previous proposition.

Theorem

Let C be a genus 3 curves with CM by a CM-field K. Write $K=\mathbb{Q}(\sqrt{\alpha})$ for some totally negative element $\alpha \in K^+/\mathbb{Z}$ with $\sqrt{\alpha} \in \mathcal{O} = End(J)$. Assume further that we are under restrictions $(R1)$ and $(R2)$.
Then any prime $\mathfrak{p} \mid p$ of bad reduction is bounded by

$$p \leq 4\,Tr_{K^+/\mathbb{Q}}(\alpha)^6/3^6.$$

Sketch of the proof

Proof (Sketch).

If p is a prime of bad reduction, then there exists an embedding

$$\iota : K = \mathrm{End}^0(J) \hookrightarrow \mathrm{End}^0(\bar{J}) = \mathcal{M}_3(B_{p,\infty})$$

such that complex conjugation on the LHS corresponds to the Rosati involution on the RHS. By inspecting the image by this embedding of $\sqrt{\alpha}$ we conclude that for enough big primes p the entries of $\iota(\sqrt{\alpha})$ are in fact in $\mathbb{Q}$ (since elements in an order of $B_{p,\infty}$ with "small norm" commute). This gives us a contradiction with $[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] = 6$. □

Restrictions

(R1) Restriction 1: we assume that K does not contain any K_1.

We need to introduce the concept of Lie types: work in progress ....

(R2) Restriction 2: $\overline{C}$ has an irreducible component of genus 1 and one of genus 2.

Ruled out! But we get a bigger bound.

Thank you!