# Bad reduction of genus 3 curves with Complex Multiplication

Elisa Lorenzo García
Universiteit Leiden

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

October 1, 2015

# Index

# Gross-Zagier g=1

Let be $\mathcal{O}_1$, $\mathcal{O}_2$ be two different orders of discriminant $d_i$ in $\mathbb{Q}(\sqrt{d_i})$. We wonder whenever there are two elliptic curves $E_i/\mathbb{C}$ with CM by $\mathcal{O}_i$ and a prime $\mathfrak{p}$ such that $E_1 \simeq E_2 \bmod \mathfrak{p}$. In order to answer it, Gross and Zagier defined the number:

# Gross-Zagier g=1

Let be $\mathcal{O}_1$, $\mathcal{O}_2$ be two different orders of discriminant $d_i$ in $\mathbb{Q}(\sqrt{d_i})$. We wonder whenever there are two elliptic curves $E_i/\mathbb{C}$ with CM by $\mathcal{O}_i$ and a prime $\mathfrak{p}$ such that $E_1 \simeq E_2 \bmod \mathfrak{p}$. In order to answer it, Gross and Zagier defined the number:

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

where the $\tau_i$ run over equivalence classes, and $w_i$ is the number of units in $\mathcal{O}_i$.

# Gross-Zagier g=1

Let be $\mathcal{O}_1$, $\mathcal{O}_2$ be two different orders of discriminant $d_i$ in $\mathbb{Q}(\sqrt{d_i})$. We wonder whenever there are two elliptic curves $E_i/\mathbb{C}$ with CM by $\mathcal{O}_i$ and a prime $\mathfrak{p}$ such that $E_1 \simeq E_2 \bmod \mathfrak{p}$. In order to answer it, Gross and Zagier defined the number:

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

where the $\tau_i$ run over equivalence classes, and $w_i$ is the number of units in $\mathcal{O}_i$.

- 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

Let be $\mathcal{O}_1$, $\mathcal{O}_2$ be two different orders of discriminant $d_i$ in $\mathbb{Q}(\sqrt{d_i})$. We wonder whenever there are two elliptic curves $E_i/\mathbb{C}$ with CM by $\mathcal{O}_i$ and a prime $\mathfrak{p}$ such that $E_1 \simeq E_2 \bmod \mathfrak{p}$. In order to answer it, Gross and Zagier defined the number:

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

where the $\tau_i$ run over equivalence classes, and $w_i$ is the number of units in $\mathcal{O}_i$.

- 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].

**Remark**

$J(d_1, d_2) = Res(H_{d_1}, H_{d_2})$ *(Hilbert polynomials $\Rightarrow$ CM-method)*

# Gross-Zagier g=1

Roughly speaking,

$$\left\{ \begin{array}{c} \text{factorization} \\ J(d_1, d_2) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting} \\ \mathrm{Isom}_n(E_1, E_2) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting} \\ \text{embeddings} \\ \iota : \mathrm{End}(E_2) \hookrightarrow B_{p,\infty} \end{array} \right\}$$

# Gross-Zagier g=1

Roughly speaking,

$$\left\{ \begin{array}{c} \text{factorization} \\ J(d_1, d_2) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting} \\ \mathrm{Isom}_n(E_1, E_2) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting} \\ \text{embeddings} \\ \iota : \mathrm{End}(E_2) \hookrightarrow B_{p,\infty} \end{array} \right\}$$

They prove

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

# Gross-Zagier g=1

Roughly speaking,

$$\left\{ \begin{array}{c} \text{factorization} \\ J(d_1, d_2) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting} \\ \mathrm{Isom}_n(E_1, E_2) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting} \\ \text{embeddings} \\ \iota : \mathrm{End}(E_2) \hookrightarrow B_{p,\infty} \end{array} \right\}$$

They prove

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

## Idea

*If* $\mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$, *we need* $End^0(\bar{E}_i) \simeq B_{p,\infty}$.

$$\iota : End(E_2) \hookrightarrow End(\bar{E}_2) \to End(\bar{E}_1) \simeq B_{p,\infty}$$

# Gross-Zagier g=2

Generalizations $g = 2$:

- Igusa invariants: $i_i : \mathcal{M}_2 \hookrightarrow \mathcal{A}_2 \to \mathbb{C}$, $i \in \{1, 2, 3\}$

# Gross-Zagier g=2

Generalizations $g = 2$:

- Igusa invariants: $i_i : \mathcal{M}_2 \hookrightarrow \mathcal{A}_2 \to \mathbb{C}$, $i \in \{1, 2, 3\}$
- For $C_1$, $C_2$ curves with CM by orders $\mathcal{O}_1$, $\mathcal{O}_2$ in quartic CM-fields, we want to define

$$J(\mathcal{O}_1, \mathcal{O}_2) = \text{g.c.d}(i_1 - i_1', i_2 - i_2', i_3 - i_3')$$

# Gross-Zagier g=2

Generalizations $g = 2$:

- Igusa invariants: $i_i : \mathcal{M}_2 \hookrightarrow \mathcal{A}_2 \to \mathbb{C}$, $i \in \{1, 2, 3\}$
- For $C_1$, $C_2$ curves with CM by orders $\mathcal{O}_1$, $\mathcal{O}_2$ in quartic CM-fields, we want to define

$$J(\mathcal{O}_1, \mathcal{O}_2) = \text{g.c.d}(i_1 - i_1', i_2 - i_2', i_3 - i_3')$$

**PROBLEM!!** the invariants are not integer numbers any more!! but, still rational ....

# Gross-Zagier g=2

Generalizations $g = 2$:

- Igusa invariants: $i_i : \mathcal{M}_2 \hookrightarrow \mathcal{A}_2 \to \mathbb{C}$, $i \in \{1, 2, 3\}$
- For $C_1$, $C_2$ curves with CM by orders $\mathcal{O}_1$, $\mathcal{O}_2$ in quartic CM-fields, we want to define

$$J(\mathcal{O}_1, \mathcal{O}_2) = \text{g.c.d}(i_1 - i_1', i_2 - i_2', i_3 - i_3')$$

**PROBLEM!!** the invariants are not integer numbers any more!! but, still rational ....

Numerators: (Gross-Zagier formula) Goren and Lauter.

$$\{\text{factorization}\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting} \\ \text{Isomorphisms} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting embeddings} \\ \iota : \text{End}(C_2) \hookrightarrow B_{p,\infty} \otimes L \end{array} \right\}$$

# Gross-Zagier g=2

Generalizations $g = 2$:

- Igusa invariants: $i_i : \mathcal{M}_2 \hookrightarrow \mathcal{A}_2 \to \mathbb{C}$, $i \in \{1, 2, 3\}$
- For $C_1$, $C_2$ curves with CM by orders $\mathcal{O}_1$, $\mathcal{O}_2$ in quartic CM-fields, we want to define

$$J(\mathcal{O}_1, \mathcal{O}_2) = \text{g.c.d}(i_1 - i_1', i_2 - i_2', i_3 - i_3')$$

**PROBLEM!!** the invariants are not integer numbers any more!! but, still rational ....

Numerators: (Gross-Zagier formula) Goren and Lauter.

$$\{\text{factorization}\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting} \\ \text{Isomorphisms} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting embeddings} \\ \iota : \text{End}(C_2) \hookrightarrow B_{p,\infty} \otimes L \end{array} \right\}$$

Denominators: (Cryptographic purposes) Goren & Lauter, Bruinier & Yang, Lauter & Viray, Streng.

$$\{\text{factorization}\} \leftrightarrow \left\{ \begin{array}{c} \text{Bad} \\ \text{Reduction} \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Counting embeddings} \\ \iota : \text{End}(C_2) \hookrightarrow \mathcal{M}_2(B_{p,\infty}) \end{array} \right\}$$

# Gross-Zagier g=2

**Theorem (Lauter-Viray)**

*$p$ divides denominators ($\chi_{10}$) $\Leftrightarrow$ Bad Reduction $\Leftrightarrow$ Solution to emb. prob.*

**Igusa invariants:** $i_j = \frac{\text{some modular form}}{\chi_{10}}$, $p \mid \chi_{10} \Leftrightarrow \bar{J}$ decomposable.

**Bad reduction:** $\Leftrightarrow \bar{C} = C_1 \cup C_2$

# Gross-Zagier g=2

**Theorem (Lauter-Viray)**

*$p$ divides denominators ($\chi_{10}$) $\Leftrightarrow$ Bad Reduction $\Leftrightarrow$ Solution to emb. prob.*

**Igusa invariants:** $i_i = \frac{\text{some modular form}}{\chi_{10}}$, $p \mid \chi_{10} \Leftrightarrow \bar{J}$ decomposable.

**Bad reduction:** $\Leftrightarrow \bar{C} = C_1 \cup C_2$

**Idea**

*If $\mathfrak{p}$ is a prime of bad reduction, then $\bar{C} = C_1 \cup C_2$ and $\bar{J} = J(C_1) \times J(C_2)$ $\Rightarrow \bar{J} \simeq E \times F \Rightarrow \bar{J} \sim E^2 \Rightarrow \iota : \mathcal{O} \hookrightarrow \mathcal{M}_2(B_{p,\infty})$*

We will look for a bound, so we don't care about the other direction of the implication.

# Gross-Zagier g=3

**PROBLEM:** there are not invariants!!

# Gross-Zagier g=3

**PROBLEM:** there are not invariants!!

but ..., we can still study the embedding problem!

$$\iota : \mathcal{O} \hookrightarrow \mathcal{M}_3(B_{p,\infty})$$

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

# Gross-Zagier g=3

**PROBLEM:** there are not invariants!!

but ..., we can still study the embedding problem!

$$\iota : \mathcal{O} \hookrightarrow \mathcal{M}_3(B_{p,\infty})$$

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

**Conditions:**

- Optimal
- Rosati involution given by complex conjugation

$$\gamma \to \gamma^\dagger = \lambda^{-1} \cdot \gamma^\vee \cdot \lambda$$

# Abelian Varieties with CM

## Proposition

*If $A$ is an abelian variety defined over a number field $M$ and with CM, then it has potentially good reduction everywhere.*

## Proposition (Lang)

*Let $A$ be an abelian variety with CM by $K$ and defined over a field of characteristic zero. The CM-type $(K, \varphi)$ is primitive if and only if the abelian variety $A$ is simple.*

# Abelian Varieties with CM

**Proposition**

*If $A$ is an abelian variety defined over a number field $M$ and with CM, then it has potentially good reduction everywhere.*

**Proposition (Lang)**

*Let $A$ be an abelian variety with CM by $K$ and defined over a field of characteristic zero. The CM-type $(K, \varphi)$ is primitive if and only if the abelian variety $A$ is simple.*

If $g = 2$: $(K, \varphi)$ 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 $K_1$.

# Abelian Varieties with CM

## Proposition

*If $A$ is an abelian variety defined over a number field $M$ and with CM, then it has potentially good reduction everywhere.*

## Proposition (Lang)

*Let $A$ be an abelian variety with CM by $K$ and defined over a field of characteristic zero. The CM-type $(K, \varphi)$ is primitive if and only if the abelian variety $A$ is simple.*

If $g = 2$: $(K, \varphi)$ 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 $K_1$.

If $g = 2$: in the previous setting, we have that $\lambda$ is given by a diagonal matrix.

(R2) **Restriction 2:** we still assume that $\lambda$ is diagonal.

# Curves with CM

Let $C$ be a genus 3 curve with CM by $K$. We denote by $J$ its Jacobian.

## Proposition

*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

Let $C$ be a genus 3 curve with CM by $K$. We denote by $J$ its Jacobian.

## Proposition

*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

*If $\overline{J}$ is not simple, then $\overline{J}$ is isogenous to $E^3$. In particular, if $C$ has bad reduction, then $\overline{J} \sim E^3$.*

# The main Theorem

We are ready to state the main theorem in our paper:

**Theorem**

*Let $C$ be a genus 3 curves with CM by a CM-field $K$ (with a primitive CM-type). Write $K = \mathbb{Q}(\sqrt{\alpha})$ for some totally negative element $\alpha \in K^+/\mathbb{Z}$ with $\sqrt{\alpha} \in \mathcal{O} = End(J(C))$. Assume further that we are under restrictions $(R1)$ and $(R2)$.*
*Then any prime $\mathfrak{p} \mid p$ for which there is a solution to the embedding problem, in particular, for primes 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

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

such that complex conjugation on the LHS corresponds to the Rosati involution on the RHS.
Recall that $K = \mathbb{Q}(\sqrt{\alpha})$ and $K^+ = \mathbb{Q}(\alpha)$ with $\alpha$ a totally negative element. Let us call $\gamma = \iota(\alpha)$. Then (using R2)

$$0 > \mathrm{Tr}(\alpha) = -\mathrm{Tr}(\gamma\gamma^\dagger) = -\mathrm{Tr}(\gamma\lambda\gamma^\vee\lambda^{-1}) = -\sum \mathrm{Nr}(\gamma_{ij})$$

Goren & Lauter's Lemma about small norm elements implies that we have an embedding $\iota : K \hookrightarrow \mathcal{M}_3(K_1)$ with $K_1$ an at most degree 2 CM-field. (R1) $\Rightarrow K_1 = \mathbb{Q}$. This gives us a contradiction with $[\mathbb{Q}(\sqrt{\alpha}) : \mathbb{Q}] = 6$. □

1. Motivation
   - Gross-Zagier Formula
   - Gross-Zagier g=2
   - Gross-Zagier g=3
2. Set up
   - Abelian Varieties with CM
   - Bad reduction
3. Main Theorem
   - The statement
   - The Proof
4. Removing the assumptions

# Restrictions

How can we remove the restrictions??

**(R1) Restriction 1:** we need to use more fine arguments, not only dimension ones. We still didn't use the primitivity of the CM-type. The reduction of the CM-type is not well-defined, we have to work with the Lie type, and prove that if $\mathbb{Q}(\sqrt{-d}) \subseteq K$, then $\iota(-\sqrt{d})$ is a matrix equivalent to

$$\pm\sqrt{-d}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

# Restrictions

How can we remove the restrictions??

**(R1) Restriction 1:** we need to use more fine arguments, not only dimension ones. We still didn't use the primitivity of the CM-type. The reduction of the CM-type is not well-defined, we have to work with the Lie type, and prove that if $\mathbb{Q}(\sqrt{-d}) \subseteq K$, then $\iota(-\sqrt{d})$ is a matrix equivalent to

$$\pm\sqrt{-d}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

**(R2) Restriction 2:** We need to study the case in which $\overline{C}$ has an irreducible component of genus 1 and one of genus 2. That is, consider the case in which the polarization may be given by

$$\lambda = \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}, \ A \in \mathcal{M}_2(B_{p,\infty})$$

Thank you!