Equations for arithmetic $(1; e)$-curves

Jeroen Sijsling

Universiteit Utrecht

Intercity Seminar, December 4, 2009

Universiteit Utrecht

(1; e)-curves

Definition

Let $\mathfrak{H}$ be the complex upper half plane. Let Γ be a discrete subgroup of $\mathrm{PGL}_2^+(\mathbf{R}) \cong \mathrm{PSL}_2(\mathbf{R}) \cong \mathrm{Aut}(\mathfrak{H})$. The quotient

$$\mathfrak{H} \longrightarrow \Gamma\backslash\mathfrak{H} = X(\Gamma)$$

is called a *(1;e)-curve* if it is of signature $(1; e)$, that is, if it is compact, of genus one and branched above one point only, with ramification index e.

$(1; e)$-curves

Definition

Let $\mathfrak{H}$ be the complex upper half plane. Let Γ be a discrete subgroup of $\mathrm{PGL}_2^+(\mathbf{R}) \cong \mathrm{PSL}_2(\mathbf{R}) \cong \mathrm{Aut}(\mathfrak{H})$. The quotient

$$\mathfrak{H} \longrightarrow \Gamma\backslash\mathfrak{H} = X(\Gamma)$$

is called a *(1;e)-curve* if it is of signature $(1; e)$, that is, if it is compact, of genus one and branched above one point only, with ramification index e.

The preimage of Γ in $\mathrm{SL}(2, \mathbf{R})$ has a presentation

$$\langle \alpha, \beta, \gamma \mid \gamma = [\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta,\ \gamma^e = -1 \rangle.$$

Γ is determined up to conjugacy by the triple $(\mathrm{Tr}(\alpha), \mathrm{Tr}(\beta), \mathrm{Tr}(\alpha\beta))$.

Groups from quaternion algebras

Let F be a totally real field, and let B be a quaternion algebra over F. We suppose that

$$B \otimes_{\mathbf{Q}} \mathbf{R} \cong M_2(\mathbf{R}) \times \mathbf{H}^{d-1},$$

where $\mathbf{H}$ is the Hamilton algebra. We set D_B (the *discriminant* of B) equal to the product of those finite primes $\mathfrak{p}$ of F such that $B_{\mathfrak{p}}|F_{\mathfrak{p}}$ is a division algebra.

Groups from quaternion algebras

Let F be a totally real field, and let B be a quaternion algebra over F. We suppose that

$$B \otimes_{\mathbf{Q}} \mathbf{R} \cong M_2(\mathbf{R}) \times \mathbf{H}^{d-1},$$

where $\mathbf{H}$ is the Hamilton algebra. We set D_B (the *discriminant* of B) equal to the product of those finite primes $\mathfrak{p}$ of F such that $B_{\mathfrak{p}}|F_{\mathfrak{p}}$ is a division algebra.

Let $\mathcal{O}$ be an order of B. Then the group of units of positive norm $\mathcal{O}^+$ in the factor $M_2(\mathbf{R})$ forms a discrete subgroup $\mathcal{O}^+$ of $\mathrm{GL}^+(\mathbf{R})$. As such, it gives rise to an algebraic curve $X(\mathcal{O}^+)$ over $\mathbf{C}$.

Groups from quaternion algebras

Let F be a totally real field, and let B be a quaternion algebra over F. We suppose that

$$B \otimes_{\mathbf{Q}} \mathbf{R} \cong M_2(\mathbf{R}) \times \mathbf{H}^{d-1},$$

where $\mathbf{H}$ is the Hamilton algebra. We set D_B (the *discriminant* of B) equal to the product of those finite primes $\mathfrak{p}$ of F such that $B_{\mathfrak{p}}|F_{\mathfrak{p}}$ is a division algebra.

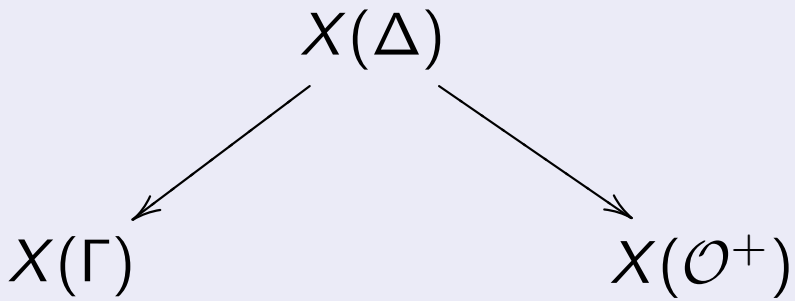
Let $\mathcal{O}$ be an order of B. Then the group of units of positive norm $\mathcal{O}^+$ in the factor $M_2(\mathbf{R})$ forms a discrete subgroup $\mathcal{O}^+$ of $\mathrm{GL}^+(\mathbf{R})$. As such, it gives rise to an algebraic curve $X(\mathcal{O}^+)$ over $\mathbf{C}$.

These curves are examples of *Shimura curves*. Shimura proved that they have canonical models over certain abelian extensions of F.

Arithmetic $(1; e)$-curves

Definition

A $(1; e)$-curve is called *arithmetic* if there is a diagram of finite morphisms

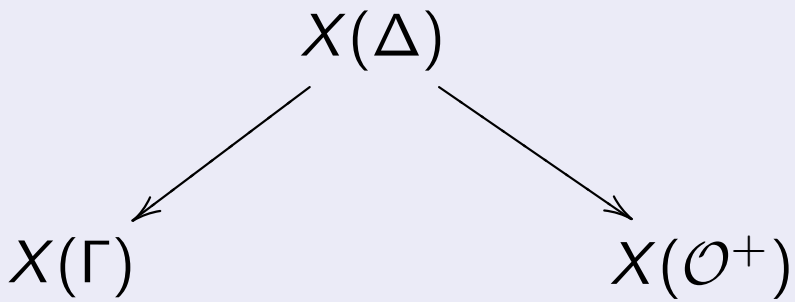


induced by inclusions of subgroups of $\mathrm{PGL}_2^+(\mathbf{R})$.

Arithmetic $(1;e)$-curves

Definition

A $(1;e)$-curve is called *arithmetic* if there is a diagram of finite morphisms



induced by inclusions of subgroups of $\mathrm{PGL}_2^+(\mathbf{R})$.

Kisao Takeuchi classified all $(1;e)$-curves in 1983. He proved that there are finitely many (72) such curves, and that one can take $\Delta = \Gamma^{(2)}$ above, where $\Gamma^{(2)} = \langle \gamma^2 : \gamma \in \Gamma \rangle$.

Motivation

Suppose the $(1; e)$-curve X is given by an equation $y^2 = p(x)$ with $\deg(p) = 3$ and that the elliptic point is the point at infinity. On X there lives the following Lamé equation:

$$\left[(\sqrt{p(x)}\frac{\mathrm{d}}{\mathrm{d}x})^2 - (n(n+1)x + B)\right] u = 0,$$

where $n = (1/2e) - (1/2)$ and B is the so-called *accessory parameter*.

Motivation

Suppose the $(1; e)$-curve X is given by an equation $y^2 = p(x)$ with $\deg(p) = 3$ and that the elliptic point is the point at infinity. On X there lives the following Lamé equation:

$$\left[(\sqrt{p(x)}\frac{\mathrm{d}}{\mathrm{d}x})^2 - (n(n+1)x + B)\right] u = 0,$$

where $n = (1/2e) - (1/2)$ and B is the so-called *accessory parameter*.
The quotient of two solutions of this equation gives the (multi-valued) inverse map $X \to \mathfrak{H}$.

Motivation

Suppose the $(1; e)$-curve X is given by an equation $y^2 = p(x)$ with $\deg(p) = 3$ and that the elliptic point is the point at infinity. On X there lives the following Lamé equation:

$$\left[(\sqrt{p(x)}\frac{\mathrm{d}}{\mathrm{d}x})^2 - (n(n+1)x + B)\right] u = 0,$$

where $n = (1/2e) - (1/2)$ and B is the so-called *accessory parameter*.
The quotient of two solutions of this equation gives the (multi-valued) inverse map $X \to \mathfrak{H}$.
One seeks to determine p and B for the curves in Takeuchi's list.
These are interesting because for Lamé equations coming from arithmetic $(1; e)$-groups, the coefficients of the power series solutions have very tame growth behavior.

The goal

This talk will show some techniques for determining equations of these curves over their canonical fields of definition.

The goal

This talk will show some techniques for determining equations of these curves over their canonical fields of definition.

Three tools have proved especially useful: Belyi maps, modularity of elliptic curves over $\mathbf{Q}$, and the computation of Hecke traces. This talk focuses on the first two techniques.
Partial results were found previously by Chudnovsky and Chudnovsky, without proof, and by Victor Rotger when the quaternion algebra is defined over $\mathbf{Q}$.

Belyi maps

Definition

A *Belyi map* is a finite morphism

$$f : X \longrightarrow \mathbf{P}^1_{\mathbf{C}}$$

where X is a complete non-singular algebraic curve over $\mathbf{C}$, and whose branch locus is contained in $\{0, 1, \infty\}$.

Belyi maps

Definition

A *Belyi map* is a finite morphism

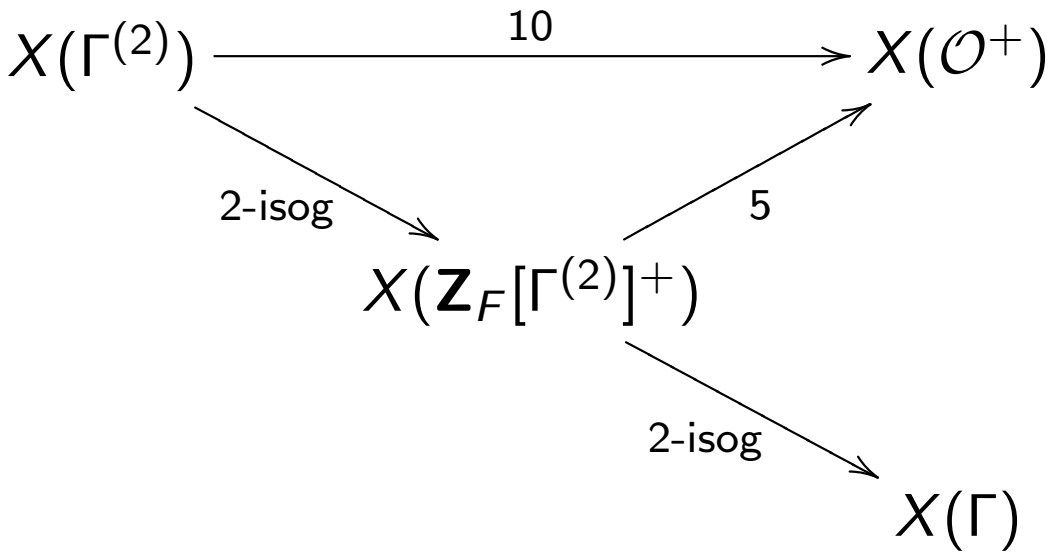
$$f : X \longrightarrow \mathbf{P}^1_{\mathbf{C}}$$

where X is a complete non-singular algebraic curve over $\mathbf{C}$, and whose branch locus is contained in $\{0, 1, \infty\}$.

Giving a Belyi map of degree n is the same as giving a simultaneous conjugacy class of triples $(\sigma_0, \sigma_1, \sigma_\infty)$ in S_n whose product is trivial. These permutations specify the ramification of the map.

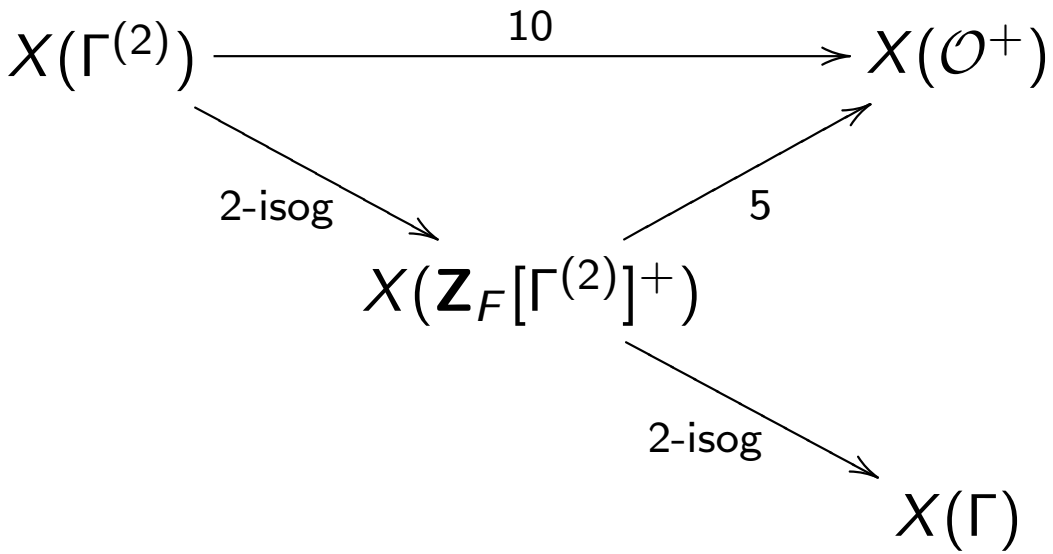
A cover from a $(1;3)$-curve

We take $F = \mathbf{Q}(w_5)$, $w_5 = (1+\sqrt{5})/2$, and trace triple $(\sqrt{2w_5+2}, \sqrt{6w_5+4}, \sqrt{8w_5+5})$. The algebra B has $D_B = \mathfrak{p}_3 = (3)$, and we have a diagram



A cover from a $(1;3)$-curve

We take $F = \mathbf{Q}(w_5)$, $w_5 = (1+\sqrt{5})/2$, and trace triple $(\sqrt{2w_5+2}, \sqrt{6w_5+4}, \sqrt{8w_5+5})$. The algebra B has $D_B = \mathfrak{p}_3 = (3)$, and we have a diagram



$\mathbf{Z}_F[\Gamma^{(2)}]^+$ is easier to calculate with than $\Gamma^{(2)}$ because membership testing is easy.

Eichler orders

$\mathbf{Z}_F[\Gamma^{(2)}]$ turns out to be an *Eichler order* (an intersection of maximal orders) of *level* $\mathfrak{p}_2 = (2)$ and index 4 in $\mathcal{O}$. This means that its localizations at finite primes are maximal, except at $\mathfrak{p}_2$, where this localization is conjugate to the order

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset M_2(\mathbf{Z}_{F,\mathfrak{p}_2}).$$

$\mathcal{O}$ itself is of course a level (1) Eichler order.

Eichler orders

$\mathbf{Z}_F[\Gamma^{(2)}]$ turns out to be an *Eichler order* (an intersection of maximal orders) of *level* $\mathfrak{p}_2 = (2)$ and index 4 in $\mathcal{O}$. This means that its localizations at finite primes are maximal, except at $\mathfrak{p}_2$, where this localization is conjugate to the order

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \subset M_2(\mathbf{Z}_{F,\mathfrak{p}_2}).$$

$\mathcal{O}$ itself is of course a level (1) Eichler order.

The signatures of $X(\mathbf{Z}_F[\Gamma^{(2)}]^+)$ and $X(\mathcal{O}^+)$ can be calculated using Eichler's theory of optimal embeddings for the special orders $\mathbf{Z}_F[\zeta_{2n}]$. It turns out that these equal $(1; 3, 3)$ and $(0; 3, 5, 5)$, respectively. So the cover $X(\mathbf{Z}_F[\Gamma^{(2)}]^+) \to X(\mathcal{O}^+)$ is a Belyi map, and one can recover $X(\Gamma)$ by identifying the elliptic points of $X(\mathbf{Z}_F[\Gamma^{(2)}]^+)$.

Atkin-Lehner involutions

We use one more trick. The normalizers of $\mathbf{Z}_F[\Gamma^{(2)}]^+$ and $\mathcal{O}^+$ in $\mathrm{PGL}_2^+(\mathbf{R})$ are of index 2 over the original groups. (They can be obtained by adjoining an element of $\mathbf{Z}_F[\Gamma^{(2)}]^+$ of norm 3.)

Atkin-Lehner involutions

We use one more trick. The normalizers of $\mathbf{Z}_F[\Gamma^{(2)}]^+$ and $\mathcal{O}^+$ in $\mathrm{PGL}_2^+(\mathbf{R})$ are of index 2 over the original groups. (They can be obtained by adjoining an element of $\mathbf{Z}_F[\Gamma^{(2)}]^+$ of norm 3.)
This gives a diagram

$$\begin{array}{ccc} X(\mathbf{Z}_F[\Gamma^{(2)}]^+) & \xrightarrow{2} & X(N(\mathbf{Z}_F[\Gamma^{(2)}]^+)) \\ \downarrow 5 & & \downarrow 5 \\ X(\mathcal{O}^+) & \xrightarrow{2} & X(N(\mathcal{O}^+)) \end{array} \qquad \begin{array}{ccc} (1;3,3) & \xrightarrow{2} & (0;2,2,6,6) \\ \downarrow 5 & & \downarrow 5 \\ (0;3,5,5) & \xrightarrow{2} & (0;2,5,6) \end{array}$$

We need only determine the Belyi map on the right. It has ramification type $((2,2,1),(5),(3,1,1))$, and by using permutations, one sees that this property determines the map.

Calculating the geometric map

We put the elliptic points of order $2, 5, 6$ of $X(N(\mathcal{O}^+))$ at $1, \infty, 0$ respectively. Then we have to solve:

$$a(x - p_0^1)^3(x^2 + p_1^2 x + p_0^2) - b(x - q_0^1)^5 = c(x^2 + r_1^1 x + r_0^1)^2(x - r_0^2).$$

Calculating the geometric map

We put the elliptic points of order $2, 5, 6$ of $X(N(\mathcal{O}^+))$ at $1, \infty, 0$ respectively. Then we have to solve:

$$a(x - p_0^1)^3(x^2 + p_1^2 x + p_0^2) - b(x - q_0^1)^5 = c(x^2 + r_1^1 x + r_0^1)^2(x - r_0^2).$$

After setting $p_0^1 = 0$, $q_0^1 = \infty$, $r_0^2 = 1/4$, there is a unique solution up to scalars, which can be calculated using Gröbner bases. It is given by

$$4z^3(36z^2 + 15z + 10) - 1 = (6z^2 + 2z + 1)^2(4z - 1).$$

and corresponds to the Belyi map

$$f : z \mapsto 4z^3(36z^2 + 15z + 10).$$

Recovering $X(\Gamma)$

$X(\mathbf{Z}[\Gamma^2]^+)$ is isomorphic to the $2:1$ cover of $\mathbf{P}^1_{\mathbf{C}}$ ramified doubly over the zeroes of $(36z^2+15z+10)$, z and $(4z-1)$. This gives the equation

$$y^2 = x(4x-1)(36x^2+15x+10).$$

Recovering $X(\Gamma)$

$X(\mathbf{Z}[\Gamma^2]^+)$ is isomorphic to the $2:1$ cover of $\mathbf{P}^1_{\mathbf{C}}$ ramified doubly over the zeroes of $(36z^2+15z+10)$, z and $(4z-1)$. This gives the equation

$$y^2 = x(4x-1)(36x^2+15x+10).$$

$X(\Gamma)$ can be recovered by identifying the points on the x-axis whose coordinates are the zeroes of $36x^2+15x+10$. This gives the elliptic curve of j-invariant $7949^3/2^5 3^{10}$ over $\mathbf{C}$.

The canonical model

Shimura guarantees us the existence of a canonical model of our curve over the ray class field $F(w_3)$, $w_3 = (1 + \sqrt{-3})/2$ of F, which has conductor $\mathfrak{p}_2\infty_1\infty_2$, and Carayol proved that this curve has semistable reduction, multiplicative exactly above the aforementioned finite primes. The elliptic point is a rational point on this curve.

The canonical model

Shimura guarantees us the existence of a canonical model of our curve over the ray class field $F(w_3)$, $w_3 = (1+\sqrt{-3})/2$ of F, which has conductor $\mathfrak{p}_2\infty_1\infty_2$, and Carayol proved that this curve has semistable reduction, multiplicative exactly above the aforementioned finite primes. The elliptic point is a rational point on this curve.

The only curve that qualifies has global minimal Weierstrass model

$$y^2 + xy + (1 - 2w_3 + 3w_5 - 3w_3w_5)y$$

$$=$$

$$x^3 + (-1 - 2w_5 + 3w_3w_5)x^2 + (-830 - 1327w_5 - w_3w_5)x$$

$$+(-16093 - 1323w_3 - 26019w_5 - 2150w_3w_5).$$

A more complicated map

In general, the ramification type does not determine the Belyi map. One $(1;e)$ -curve gives rise to ramification type $((4,4,1,1),(2,2,2,2,1,1),(5,5))$. There are 5 such maps.

A more complicated map

In general, the ramification type does not determine the Belyi map. One $(1;e)$ -curve gives rise to ramification type $((4,4,1,1),(2,2,2,2,1,1),(5,5))$. There are 5 such maps. The particular one under consideration is distinguished by its monodromy group, which can be explicitly calculated as the image of

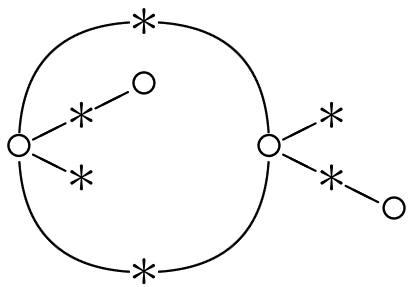
$$N(\mathcal{O}^+) \longrightarrow \mathrm{Sym}(N(\mathcal{O}^+)/N(\mathbf{Z}_F[\Gamma^{(2)}]^+)).$$

A more complicated map

In general, the ramification type does not determine the Belyi map. One $(1; e)$ -curve gives rise to ramification type $((4, 4, 1, 1), (2, 2, 2, 2, 1, 1), (5, 5))$. There are 5 such maps. The particular one under consideration is distinguished by its monodromy group, which can be explicitly calculated as the image of

$$N(\mathcal{O}^+) \longrightarrow \mathrm{Sym}(N(\mathcal{O}^+)/N(\mathbf{Z}_F[\Gamma^{(2)}]^+)).$$

For the cognoscenti, the dessin d'enfant is given in this case by



Using modularity

Now let $F = \mathbf{Q}(w_{17})$, $w_{17} = (1 + \sqrt{17})/2$. The trace triple $(\sqrt{w_{17} + 2}, \sqrt{6w_{17} + 10}, \sqrt{7w_{17} + 11})$ gives rise to an algebra B with $D_B = \mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$. We have $X(\Gamma) = X(\mathcal{O}^1)$.

Using modularity

Now let $F = \mathbf{Q}(w_{17})$, $w_{17} = (1 + \sqrt{17})/2$. The trace triple $(\sqrt{w_{17} + 2}, \sqrt{6w_{17} + 10}, \sqrt{7w_{17} + 11})$ gives rise to an algebra B with $D_B = \mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$. We have $X(\Gamma) = X(\mathcal{O}^1)$.
By Shimura, the canonical model of $X(\Gamma)$, call it E, is defined over the ray class field of conductor $\infty_1\infty_2$, which is just F itself. It has a rational point (the elliptic point) and conductor $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$ by Carayol.

Using modularity

Now let $F = \mathbf{Q}(w_{17})$, $w_{17} = (1 + \sqrt{17})/2$. The trace triple $(\sqrt{w_{17} + 2}, \sqrt{6w_{17} + 10}, \sqrt{7w_{17} + 11})$ gives rise to an algebra B with $D_B = \mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$. We have $X(\Gamma) = X(\mathcal{O}^1)$.
By Shimura, the canonical model of $X(\Gamma)$, call it E, is defined over the ray class field of conductor $\infty_1\infty_2$, which is just F itself. It has a rational point (the elliptic point) and conductor $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$ by Carayol.

By a result of Doi and Naganuma, the stability of D_B under the $\mathrm{Gal}(F|\mathbf{Q})$ implies that $X(\Gamma)$ is defined over $\mathbf{Q}$. Note that this does *not* imply that the canonical model of $X(\Gamma)$ is defined over $\mathbf{Q}$.

Candidate curves

So E is the twist over F of an elliptic curve E_0 defined over $\mathbf{Q}$. Since E has conductor $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$ and the extension $F|\mathbf{Q}$ is ramified over 17 only, it is in fact a twist of an E_0 whose conductor is of the form $2^i\,3\,17^k$.

Candidate curves

So E is the twist over F of an elliptic curve E_0 defined over $\mathbf{Q}$. Since E has conductor $\mathfrak{p}_2\mathfrak{p}_2'\mathfrak{p}_3$ and the extension $F|\mathbf{Q}$ is ramified over 17 only, it is in fact a twist of an E_0 whose conductor is of the form $2^i\,3\,17^k$.

Using Cremona's tables, we get 4 possible curves. They are distinguished by the denominator of their j-invariants, which equal $2^{10}3^2$, $2^5 3^4$, $2^2 3^{10}$ and $2^1 3^{20}$ respectively.

Dual graphs

Let F be a totally real field of narrow class number 1, B a quaternion algebra over F, $\mathcal{O}_B$ a maximal order of B, and let $\mathfrak{p}$ be a prime dividing D_B. Let X_F be the canonical model of $X(\mathcal{O}^+)$. Let H be a quaternion algebra satisfying

$$H \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{H}^d$$

and $D_H\mathfrak{p} = D_B$. Choose a maximal order $\mathcal{O}_H$ of H.

Dual graphs

Let F be a totally real field of narrow class number 1, B a quaternion algebra over F, $\mathcal{O}_B$ a maximal order of B, and let $\mathfrak{p}$ be a prime dividing D_B. Let X_F be the canonical model of $X(\mathcal{O}^+)$. Let H be a quaternion algebra satisfying

$$H \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{H}^d$$

and $D_H\mathfrak{p} = D_B$. Choose a maximal order $\mathcal{O}_H$ of H.

A extension by Boutot/Zink of the results by Cerednik-Drinfel'd now implies the following.

Theorem

There exists a model of X_F over $\mathbf{Z}_{F,\mathfrak{p}}$ for which the dual graph with weights G of the special fiber has the following properties:

- *The vertices of G are given by two disjoint copies of the set $Pic_l(\mathcal{O}_H)$ of left ideal classes of $\mathcal{O}_H$, the elements I of which are weighed by $\mathcal{O}_H^r(I)^+/\mathbf{Z}_F^\times$;*

Theorem

There exists a model of X_F over $\mathbf{Z}_{F,\mathfrak{p}}$ for which the dual graph with weights G of the special fiber has the following properties:

- *The vertices of G are given by two disjoint copies of the set $Pic_l(\mathcal{O}_H)$ of left ideal classes of $\mathcal{O}_H$, the elements I of which are weighed by $\mathcal{O}_H^r(I)^+/\mathbf{Z}_F^\times$;*
- *The edges of G are given by the set $Pic_l(\mathcal{O}_H)$ of left ideal classes of $\mathcal{O}_H$, the elements I of which are weighed by $\mathcal{O}_H^r(I)^+/\mathbf{Z}_F^\times$;*

Theorem

There exists a model of X_F over $\mathbf{Z}_{F,\mathfrak{p}}$ for which the dual graph with weights G of the special fiber has the following properties:

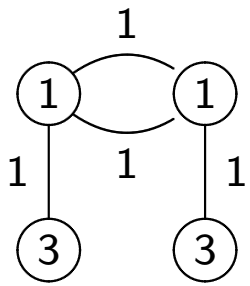
- *The vertices of G are given by two disjoint copies of the set $Pic_l(\mathcal{O}_H)$ of left ideal classes of $\mathcal{O}_H$, the elements I of which are weighed by $\mathcal{O}_H^r(I)^+/\mathbf{Z}_F^\times$;*
- *The edges of G are given by the set $Pic_l(\mathcal{O}_H)$ of left ideal classes of $\mathcal{O}_H$, the elements I of which are weighed by $\mathcal{O}_H^r(I)^+/\mathbf{Z}_F^\times$;*
- *For every vertex v, there is a sum formula*

$$\sum_{e \text{ through } v} \frac{w(v)}{w(e)} = \mathrm{Nm}(\mathfrak{p}) + 1.$$

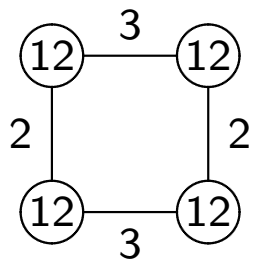
Dual graphs

Algorithms by John Voight allow us to explicitly determine the dual graphs of these integral models. These are displayed below.

Above 2 :

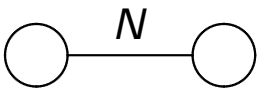


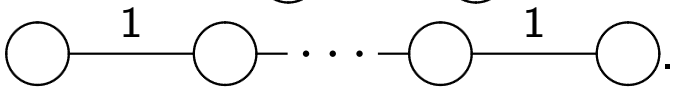
Above 3 :



Minimal models

The dual graph of a minimal model at the preceding primes can easily be recovered by a combinatorial process:

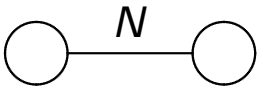
- (Blowing up) Replace every edge 

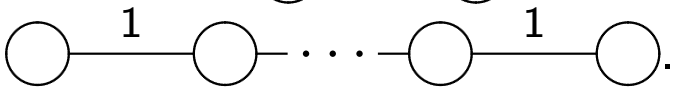
by a concatenation of edges 

.

Minimal models

The dual graph of a minimal model at the preceding primes can easily be recovered by a combinatorial process:

- (Blowing up) Replace every edge 

by a concatenation of edges 

.
- (Contraction) Contract the edges that end in a vertex through which only this edge passes.

Performing this reduction in our case, we get I_2-configurations above 2 and an I_{10}-configuration above 3.

The correct curve

The preceding implies that the j-invariant of our canonical model E has an order 2 pole at the primes above 2 and an order 10 pole at the prime above 3. Since $F|\mathbf{Q}$ is unramified above 2 and 3, this implies that the denominator of $j(E)$ is given by $2^2 3^{10}$. This determines the canonical model among the four curves mentioned previously.

The correct curve

The preceding implies that the j-invariant of our canonical model E has an order 2 pole at the primes above 2 and an order 10 pole at the prime above 3. Since $F|\mathbf{Q}$ is unramified above 2 and 3, this implies that the denominator of $j(E)$ is given by $2^2 3^{10}$. This determines the canonical model among the four curves mentioned previously.
A global minimal Weierstrass model for E is given by the equation

$$y^2 + xy + w_{17}y$$

$$=$$

$$x^3 - w_{17}x^2 + (-19694w_{17} - 30770)x + (-2145537w_{17} - 3350412).$$

Using modular curves

The final techique proceeds as follows. For simplicity, suppose $X(\Gamma) = X(\mathcal{O}^+)$.

- Calculate Hecke traces using Eichler-Shimura and fundamental domain algorithms;

Using modular curves

The final techique proceeds as follows. For simplicity, suppose $X(\Gamma) = X(\mathcal{O}^+)$.

- Calculate Hecke traces using Eichler-Shimura and fundamental domain algorithms;
- Conjecture the existence of the existence of an F-rational N-torsion point on $\mathrm{Jac}(X(\Gamma))$ for, say, $N = 5$;

Using modular curves

The final techique proceeds as follows. For simplicity, suppose $X(\Gamma) = X(\mathcal{O}^+)$.

- Calculate Hecke traces using Eichler-Shimura and fundamental domain algorithms;
- Conjecture the existence of the existence of an F-rational N-torsion point on $\mathrm{Jac}(X(\Gamma))$ for, say, $N = 5$;
- Calculate the valuations of $j(X(\Gamma))$ at prime of multiplicative reduction using Boutot/Zink;

Using modular curves

The final techique proceeds as follows. For simplicity, suppose $X(\Gamma) = X(\mathcal{O}^+)$.

- Calculate Hecke traces using Eichler-Shimura and fundamental domain algorithms;
- Conjecture the existence of the existence of an F-rational N-torsion point on $\mathrm{Jac}(X(\Gamma))$ for, say, $N = 5$;
- Calculate the valuations of $j(X(\Gamma))$ at prime of multiplicative reduction using Boutot/Zink;
- Using all this information, perform a guided search of $X_0(N)(F)$;

Using modular curves

The final techique proceeds as follows. For simplicity, suppose $X(\Gamma) = X(\mathcal{O}^+)$.

- Calculate Hecke traces using Eichler-Shimura and fundamental domain algorithms;
- Conjecture the existence of the existence of an F-rational N-torsion point on $\mathrm{Jac}(X(\Gamma))$ for, say, $N = 5$;
- Calculate the valuations of $j(X(\Gamma))$ at prime of multiplicative reduction using Boutot/Zink;
- Using all this information, perform a guided search of $X_0(N)(F)$;
- Prove correctness of this curve using results of Skinner/Wiles and Dieulefait.