Computation of the cover of Shimura curves $X_0(2) \to X(1)$ for the cyclic cubic field of discriminant $13^2$

Emmanuel HALLOUIN*

February 1, 2008

**Summary** — We compute the canonical model of the cover of Shimura curves $X_0(2) \to X(1)$ for the cubic field of discriminant $13^2$ described at the end of Elkies’ paper [Elk06]. Last, we list the coordinates of some rational CM points on $X(1)$.

**Introduction**

In [Elk06], Noam D. Elkies computes explicit algebraic models of some Shimura curves associated with quaternion algebras whose center is a cubic cyclic totally real field and whose ramification data consists in exactly two of the infinite places of the center. The examples of $K_7$ and $K_9$, the cubic fields of discriminant $49 = 7^2$ and $81 = 9^2$ respectively, are studied in details. Then the case of the center $K = K_{13}$, the cubic field of discriminant $13^2$, is described. Elkies shows that $X(1)$ has genus zero and that the cover $X_0(2) \to X(1)$ is a degree 9 cover with four branch points and with Galois group equal to $PSL_2(F_8)$. But the explicit computation of the canonical model remains to be done.

It turns out that this cover belongs to a family of degree 9 covers of $\mathbb{P}^1_C$ with Galois group $PSL_2(F_8)$, that I have computed in [Hal05]. The strategy followed to compute the cover $X_0(2) \to X(1)$ is though very simple. First gathering enough data’s about the cover of Shimura curves (see [1]), secondly putting these conditions into equations in order to compute the parameter corresponding to the expected element (see [2]).

One of the key properties of $X_0(2)$ is that it has an involution $w_2$. Once we know explicitly the map $X_0(2) \to X(1)$ and this involution $w_2$, it is an easy task to deduce the coordinates of some CM points on $X(1)$. We obtain, this way, some rational CM points on $X(1)$.

*Institut de Mathmatiques de Toulouse (Laboratoire Émile Picard), University of Toulouse II, France.
1 The cover of Shimura curves $X_0(2) \to X'(1)$

Let $K$ be the unique cyclic cubic field of discriminant $13^2$, which can be obtained by adjoining to $\mathbb{Q}$ a root $\theta$ of $x^3 + x^2 - 4x + 1 \in \mathbb{Q}[x]$. Its narrow class group $\text{Cl}^+(K)$, and thus its class group $\text{Cl}(K)$, are trivial. We denote by $\sigma_i$, $1 \leq i \leq 3$, the three real embeddings of $K$ into $\mathbb{R}$.

Let $B$ be the unique (up to $K$-isomorphisms) quaternion algebra over $K$ ramified at $\sigma_2$ and $\sigma_3$ and nowhere else. The embedding $\sigma_1$ being unramified in $B$, we know that $B \otimes_{K,\sigma_1} \mathbb{R} \simeq M_2(\mathbb{R})$ (the notation $\otimes_{K,\sigma_1} \mathbb{R}$ means that $\mathbb{R}$ is considered as a $K$-algebra via the embedding $K \otimes_{K,\sigma_1} \mathbb{R}$). This allows us to fix an embedding $i_\infty : B \to M_2(\mathbb{R})$ which restricts to $\sigma_1$ on $K$. We also fix $\mathcal{O}$ one of the maximal orders of $B$; since $\text{Cl}^+(K)$ is trivial, all these maximal orders are known to be conjugate. We denote by $\mathcal{O}^+$ the set of invertible elements of $\mathcal{O}$ whose reduce norm equals $1$. Then the group $\Gamma(1) \overset{\text{def.}}{=} i_\infty(\mathcal{O}^+)$ is an arithmetic Fuchsian group (cf. [Kat92]), and in particular a discrete subgroup of $\text{PSL}_2(\mathbb{R})$ (I denote the same way a subgroup of $\text{PSL}_2(\mathbb{R})$ and its image in the quotient $\text{PSL}_2(\mathbb{R})$).

Let $\mathcal{H}$ be the usual upper half-plane with the action of $\text{PSL}_2(\mathbb{R})$. The quotient $\Gamma(1) \backslash \mathcal{H}$, denoted by $X(1)_\mathbb{C}$, is a compact Riemann surface, called the Shimura curve associated to $B$. It has a structure of complex algebraic curve.

The (inert) prime $2$ in $K$ being unramified in $B$, we know that $B \otimes_K \mathbb{Q}_8 \simeq M_2(\mathbb{Q}_8)$. We can fix an embedding $i_2 : B \to M_2(\mathbb{Q}_8)$ in such a way that $i_2(\mathcal{O}) = M_2(\mathbb{Z}_8)$. As for the classical modular curves case, we consider the subgroups $\Gamma_0(2), \Gamma_1(2)$ and $\Gamma(2)$ of $\Gamma(1)$. For example, $\Gamma_0(2)$, which is the subgroup we will focus on, is the image by $i_\infty$ of:

$$\left\{ \omega \in \mathcal{O}^+, \ i_2(\omega) \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod 2M_2(\mathbb{Z}_8) \right\}.$$

They are also discrete subgroups of $\text{PSL}_2(\mathbb{R})$ and the quotients of $\mathcal{H}$ by these subgroups, respectively denoted by $X_0(2)_\mathbb{C}$, $X_1(2)_\mathbb{C}$ and $X(2)_\mathbb{C}$, are complex algebraic curves. We have the tower:

$$X(2)_\mathbb{C} \to X(1)_\mathbb{C} \to X_0(2)_\mathbb{C} \to X_1(2)_\mathbb{C} \to \mathcal{H}.$$

The cover $X(2)_\mathbb{C} \to X(1)_\mathbb{C}$ is the Galois closure of the cover $X_0(2)_\mathbb{C} \to X(1)_\mathbb{C}$. Moreover, the curve $X_0(2)_\mathbb{C}$ has an involution $w_2$ which comes from a trace-zero element of $B$ of norm $2$.

More precisely, in [Elk06] pages 314-315, thanks to Shimizu’s area formula, Elkies proves that $\Gamma(1)$ has four elliptic points, one of order $3$, $P_0$, three of order $2$, $P_1$, $P_2$, $P_3$ and that the curve $X(1)$ has genus zero. The map $X_0(2)_\mathbb{C} \to X(1)_\mathbb{C}$ is a cover of degree $9 = \#F_9 + 1$, with geometric Galois group $\text{PSL}_2(\mathbb{F}_9)$ (acting on the nine points of $\mathbb{P}_9^1$) and is ramified at the elliptic points $P_0, P_1, P_2, P_3$. Since elements of order $3$ and $2$ in $\text{PSL}_2(\mathbb{F}_9)$ have cycle shapes $3^3$ and $2^3 \cdot 1$ respectively, the ramification data of this cover must be $(3^3, 2^4, 1, 2^4, 1, 2^4, 1)$. 

2
We denote by $Q_1, Q_2, Q_3$ the there unramified points on $X_0(2)_{\mathbb{C}}$ above $P_1, P_2, P_3$ respectively.

Apart from elliptic points, Shimura curves also contains CM-points who are associated to CM-fields over $K$. Let $L/K$ be a CM-field and $\mathcal{O}_L$ its ring of integers. The field $L$ can be embed in $B$ by $i : L \hookrightarrow B$. The ring $i^{-1}(i(L) \cap \mathcal{O})$ is an order of $\mathcal{O}_L$ and the embedding $i$ is called optimal if and only this order is $\mathcal{O}_L$ itself. Then all the elements of $i_\infty \circ i(L)$ share the same fixed point $\tau \in \mathcal{H}$. The point $\tau \mod \Gamma(1) \in X(1)_{\mathbb{C}}$ is called a CM-point on $X(1)_{\mathbb{C}}$ by the CM-order $i^{-1}(i(L) \cap \mathcal{O})$ or by $L$ if the embedding $i$ is optimal. One can show that two embeddings $i$ and $i'$, whose associated orders are equal, give rise to the same CM-point on $X(1)_{\mathbb{C}}$ if and only if they are conjugate by a invertible element of $\mathcal{O}$.

Shimura’s results. Thanks to a modular interpretation, Shimura proved that the curve $X(1)_{\mathbb{C}}$ have a canonical model defined over the narrow class field of $K$, namely $K$ itself here.

**Theorem 1 (Shimura, [Shi67], §3.2, Main Theorem I)** There exists an algebraic curve $X(1)$ and a holomorphic map $j : \mathcal{H} \to X(1)$ satisfying the following conditions.

1. The curve $X(1)$ is defined over $K$.

2. The map $j$ yields an analytic isomorphism from $\Gamma(1) \setminus \mathcal{H}$ to $X(1) \otimes_K \mathbb{C}$.

3. Let $L$ be a CM-field over $K$ which optimally embeds in $B$ and whose class number is denoted by $h_L$. Then there are exactly $h_L$ CM-points $\tau_1, \ldots, \tau_{h_L}$ by $L$ on $X(1)$. The values $j(\tau_i)$, for $1 \leq i \leq h_L$, form a complete set of conjugates over $K$ and for each $i$, one has $L^{\text{hab.}} = L \cdot K(j(\tau_i))$.

As in the classical case, computing the modular polynomial relying the functions $j$ and $j \circ w_2$, one can prove that the curve $X_0(2)$ is also defined over $K$.

As for the curve $X(2)$, Shimura proves that it admits a canonical model which is defined over the strict 2-ray class field of $K$ (i.e. unramified outside 2 and the real places), namely $K$ another time since $\text{Cl}^+(K, 2)$ is also trivial.

Galois descent to $\mathbb{Q}$. In fact, as in [Elk98] (page 38) or [Voi06] §6, Galois descent to $\mathbb{Q}$ is possible. Nevertheless, the proofs of this fact contained in these two papers should be adapted since, here, the group $\Gamma(1)$ is no more a triangle group.

The $K$-model of $X(1)_{\mathbb{C}}$ is strongly connected to the CM-points; the elliptic points play a crucial role in the fact that this model also descents to $K$.

The elliptic point $P_0$ of order 3 is CM by $K(\sqrt{-3})$ which has class number 1. Thanks to Shimura’s result, the point $P_0$ is defined over $K$.

The elliptic points $P_1, P_2, P_3$ of order 2 are CM by $K(\sqrt{-1})$ which has class number equal to 3. Due to Shimura’s result, these points must be conjugate to each other over $K$. 

3
Proposition 2 The curve $\mathcal{X}(1)$ is defined over $\mathbb{Q}$, in such a way that:

1. the unique elliptic point $P_0$ of order 3, which is CM by $K(\sqrt{-3})$, is rational over $\mathbb{Q}$;

2. the three elliptic points $P_1, P_2, P_3$ of order 2, who are CM by $K(\sqrt{-1})$, are conjugate to each others over $\mathbb{Q}$.

Proof — The proposition follows from the fact that, not only the complete curve $\mathcal{X}(1)$, but also the curve $\mathcal{X}(1) \setminus \{P_0\} \cup \{P_1, P_2, P_3\}$ descents to $\mathbb{Q}$ (the point $P_0$ is “colored”, while the three others $P_1, P_2, P_3$ are “uncolored”). The key point is that the cubic field $K$, we start with, is a Galois extension of $\mathbb{Q}$.

By functoriality, for each $\sigma \in \text{Gal}(K/\mathbb{Q})$, the curve $\mathcal{X}(1)^\sigma$ is nothing else that the Shimura curve corresponding to the algebra $B^\sigma$ which is ramified at $\sigma_2 \circ \sigma$ and $\sigma_3 \circ \sigma$ and nowhere else.

The algebras $B$ and $B^\sigma$ are $\sigma$-isomorphic, meaning that there exists a $\mathbb{Q}$-isomorphism $\theta_\sigma : B \rightarrow B^\sigma$ which restricts to $\sigma$ on $K$. Let us denote by $\Gamma(1)_{\sigma}$ (I put $\sigma$ in subscript to emphasize the fact $\Gamma(1)$ is the group $\Gamma(1)$ whose coefficient are twisted by $\sigma$; this would not make any sense) the arithmetic group corresponding to $B^\sigma$; it follows form the choice of a maximal order $\mathcal{O}^\sigma$ of $B^\sigma$ and an embedding of $B^\sigma$ in $M_2(\mathbb{R})$. Since $\theta_\sigma^{-1}(\mathcal{O}^\sigma)$ is also a maximal order of $B$, it must be conjugate to $\mathcal{O}$ by an element of $B$. Concerning the groups $\Gamma(1)$ and $\Gamma(1)_{\sigma}$, this means that there exists $\gamma \in \text{PSL}_2(\mathbb{R})$ such that $\Gamma(1)_{\sigma} = \gamma \Gamma(1) \gamma^{-1}$. Then there exists an isomorphism of Riemann surfaces between $\mathcal{X}(1)_C$ and $\mathcal{X}(1)^\sigma_C$ which yields an isomorphism $\varphi_\sigma : \mathcal{X}(1) \rightarrow \mathcal{X}(1)^\sigma$ of algebraic curves over $K$.

It is easy to verify that these isomorphisms map an elliptic point of a given order to an elliptic point of the same order. So they are isomorphisms between the curve $\mathcal{X}(1) \setminus \{P_0\} \cup \{P_1, P_2, P_3\}$ and its twist $\mathcal{X}(1)_{\sigma} \setminus \{P_0, P_1, P_2, P_3\}$, for $\sigma \in \text{Gal}(K/\mathbb{Q})$.

To show that the $\varphi_\sigma$’s give a sufficient data for the Galois descent to $\mathbb{Q}$, it suffices to prove that the curve $\mathcal{X}(1) \setminus \{P_0\} \cup \{P_1, P_2, P_3\}$ and its conjugates do not have any non trivial automorphism. Such an automorphism is an automorphism of genus zero curve which must fix the point $P_0$ and permute $P_1, P_2, P_3$. So its order is 2 or 3, depending on the fact that it fixes or not one of the $P_i$’s for $i \geq 1$. The cross ratios $[P_0, P_1, P_2, P_3]$ is then equal to $[\infty, 0, 1, -1]$ or $[\infty, 1, j, j^2]$ (where $j = e^{i \pi/3}$). On the other hand, since $P_0$ is rational over $K$ and since the $P_i$’s for $i \geq 1$ are conjugate to each others over $K$ and such that $K(\sqrt{-1}) \cdot K(P_i) = K(\sqrt{-1})^{\text{hilb}}$, the cross ratio $[P_0, P_1, P_2, P_3]$ must satisfy:

$$K([P_0, P_1, P_2, P_3]) \cdot K(\sqrt{-1}) = K(\sqrt{-1})^{\text{hilb}}.$$

Neither $[\infty, 0, 1, -1]$ nor $[\infty, 1, j, j^2]$ satisfies this, therefore the curve $\mathcal{X}(1) \setminus \{P_0\} \cup \{P_1, P_2, P_3\}$ do not have any non trivial automorphism.

In this case, the Weil descent criterion is automatically satisfied. □
Proposition 3  The curve $X_0(2)$ is defined over $\mathbb{Q}$ and the three elliptic points $Q_1, Q_2, Q_3$ of order 2 are conjugate to each others over $\mathbb{Q}$ and fixed by the involution $w_2$.

Proof — The key point to prove the decent is that the prime 2 of $K$ is $\text{Gal}(K/\mathbb{Q})$-invariant. Indeed, keeping the notation of the preceding proof, this permit to show that the groups $\Gamma_0(2)$ and $\Gamma_0(2)_\sigma$ are also conjugate to each other by the same $\gamma$. Then the isomorphism $\varphi_\sigma$ from $X(1)$ to $X(1)^\sigma$ lifts to an isomorphism form $X_0(2)$ to $X_0(2)^\sigma$.

On the other hand, since $\text{PSL}_2(\mathbb{F}_8)$ is self-centralizing in the group of permutations of the points of $\mathbb{P}^1_{\mathbb{F}_8}$, the cover $X_0(2) \to X(1)$ and its conjugates do not have any non trivial automorphism. Therefore the previous isomorphisms between $X_0(2)$ and its conjugate give a sufficient conditions to the descent to $\mathbb{Q}$.

The construction of the involution $w_2$ being Galois-invariant, this function must be defined over $\mathbb{Q}$. Moreover, since $w_2$ permutes elliptic points of same order, it permutes the $Q_i$’s. So $w_2$ must fix one of them. By Galois conjugation, it fixes all of them. □

2 Selecting the good element in the family

In [Hal05], I have computed an algebraic model of the universal family of degree 9 covers of $\mathbb{P}^1_{\mathbb{C}}$ with Galois group $\text{PSL}_2(\mathbb{F}_8)$, with ramification type $(3^3, 2^4 \cdot 1, 2^4 \cdot 1, 2^4 \cdot 1)$ and such that the first branch point is rational while the three others are conjugate to each other. The final result (proposition 9) consists in a total degree 3 polynomial of $\mathbb{Q}(T)[f, g]$ which is an equation of a genus 1 curve $E$ over $\mathbb{Q}(T)$, and a function $\varphi \in \mathbb{Q}(T)(E)$. This function is such that the map $E \to \mathbb{P}^1_{\mathbb{Q}(T)}$ is a degree 9 cover, with (geometric) Galois group $\text{PSL}_2(\mathbb{F}_8)$, with four branch points: the point of type $3^3$ is at $\varphi = \infty$, the three points of type $2^4 \cdot 1$ have $\varphi$-coordinate equal to the three roots of $x^3 + H(T)(x + 1)$, where $H \in \mathbb{Q}(T)$ is explicit. The divisor of the degree 3 function $f$ is related to the ramification points as follows: its zeros are three unramified points on $E$ over the three branch points of type $2^4 \cdot 1$ while its poles are the three ramification points of index 3.

The variable $T$ is a coordinate on $\mathcal{H}$, the (absolute) Hurwitz space parameterizing this family, which thus is $\mathbb{Q}$-isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$. Besides this space, I also have computed the (inner) Hurwitz space $\mathcal{H}_{\text{PSL}_2(\mathbb{F}_8)}$ parameterizing the $\text{PSL}_2(\mathbb{F}_8)$-Galois covers. It is $\mathbb{Q}$-isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$, with parameter $S$, and it covers $\mathcal{H}$ by an explicit degree 3 map (see proposition 10, loc. cit.).

The specializations of this family at rational values of the parameter $T$ yield $\text{PSL}_2(\mathbb{F}_8)$ covers of $\mathbb{P}^1_{\mathbb{Q}}$ defined over $\mathbb{Q}$, with four branch points and expected ramification data.

It turns out that the cover $X_0(2) \to X(1)$ is such a specialization. Which one? That is the question!

Proposition 4  The cover $X_0(2) \to X(1)$ corresponds to the specialization at the value $T = -1$ of our family.
Proof — First of all, the cover $X_0(2) \to \mathcal{X}(1)$ is truly a member of our family. Indeed the ramification data, the Galois group do correspond and we know that the unique elliptic point of order three on $\mathcal{X}(1)$ is rational and that the three others of order 2 are conjugate to each others.

Let $E$ be the specialization we are looking for. We know that $E$ is defined over $\mathbb{Q}$ and that there exists an involution $w_2$ of $E$ also defined over $\mathbb{Q}$ that fix the three unramified points $P_1, P_2, P_3$ the three elliptic points of $\mathcal{X}(1)$ of order 2. Extending the scalars to $\mathbb{Q}(Q_1)$, the genus 1 curve $E$ becomes an elliptic curve whose origin can be chosen to be equal to $Q_1$. Then $w_2$ is nothing else that $P \mapsto -P$ and the 2-torsion consists in the $Q_i$’s plus the point $Q_2 + Q_3$. Therefore one has the relations $2Q_1 = 2Q_2 = 2Q_3$.

These conditions completely determine the parameter $T$ corresponding to the cover $X_0(2) \to \mathcal{X}(1)$. To show this fact, let us go back on the generic curve $E$. We choose the same notation for the unramified points above the branch points of type $2 \cdot 1$, namely $Q_1, Q_2, Q_3$. They are conjugate to each others over $\mathbb{Q}(T)$ since they are the zeros of the degree-3 function $f \in \mathbb{Q}(T)(E)$. We extend the scalars to $\mathbb{Q}(T)(\mathcal{X})$ the splitting field of $\mathbb{Q}(T)(Q_1)$ the field of definition of the $Q_i$’s; this is a degree 6 extension over $\mathbb{Q}(T)$. We choose the point $Q_1$ as the origin of $E$ over $\mathbb{Q}(T)(\mathcal{X})$ and we compute the $(f, g)$-coordinates of the points $2Q_2$ and $2Q_3$; they are unfortunately too huge to figure in this paper. The parameter $T_0 \in \mathbb{Q}$, we are looking for, must be such that these two points specialized at $T_0$ are equal. This leads to many polynomials in $T$ who must have $T_0$ as a common zero. But the gcd of these polynomials is equal to $T + 1$.

Since we know an algebraic model of the universal family $\varphi : E \to \mathbb{P}^1_{\mathbb{Q}(T)}$ (see [Hal05] §3.4, proposition 9), it is very easy to compute the specialization $\varphi_{-1} : E_{-1} \to \mathbb{P}^1_{\mathbb{Q}}$. We deduce an explicit algebraic model of $X_0(2) \to \mathcal{X}(1)$.

Elkies notes that the equation simplifies somewhat by taking $(43754 \varphi_{-1} + 687)/2061$ in place of $\varphi_{-1}$.

**Corollary 5** The curve $X_0(2)$ has equation:

$$f^3 - f^2g - f^2 - \frac{25}{147}f + \frac{40}{147}g + \frac{625}{147}g^3 + \frac{50}{147}g - \frac{649}{147} = 0$$

and the cover $X_0(2) \to \mathcal{X}(1)$ is given by the function:

$$\varphi = -\frac{241129}{192}f^2g - \frac{30309}{128}f^2 + \frac{1715}{3}f^2g^2 + \frac{22009}{30}fg - \frac{637}{2048}f - \frac{1715}{3f}g^3 + \frac{1225}{96}g^2 - \frac{17048}{96}g - \frac{1001}{96}.$$ 

It is a degree 9 cover ramified at $\varphi = \infty$ and at the three roots of $x^3 - x^2 - 992x - 20736$. The ramification data is $(3^3, 2^4 \cdot 1, 2^4 \cdot 1, 2^4 \cdot 1)$ and the (geometric) Galois group is equal to $\text{PSL}_2(\mathbb{F}_9)$.

Knowing this model, one can now check some easy facts.

- Since $w_2$ is defined over $\mathbb{Q}$, the fix points divisor $Q_1 + Q_2 + Q_3 + [Q_2 + Q_3]$ is rational; but the $Q_i$’s being conjugate to each others, necessarily the point $Q_2 + Q_3$ must be rational. It does and it has $(f, g)$-coordinates equal...
to \((\frac{16}{21}, 0)\). Thus \(X_0(2)\) is an elliptic curve which, as suggested by Watkins (see §4 in [Elk06]), is \(\mathbb{Q}\)-isomorphic to the elliptic curve \([1, -1, 1, -65773, -6478507]\).

• The involution \(w_2\) of \(\mathbb{Q}(f, g)\) is given by:

\[
\begin{align*}
w_2(f) &= \frac{733824f^2 - 733824fg - 454272f + 1715000g^3 - 218400g + 133120}{4501875g^3 + 733824g + 279552}, \\
w_2(g) &= -\frac{91728f^2g + 91728fg^2 + 56784fg + 62244g^2 - 3328g}{214375g^3 + 34944g + 13312}.
\end{align*}
\]

It does fix the \(Q_i\)’s and the rational point \((\frac{16}{21}, 0)\).

• Last, we recall that the Galois closure \(X(2)\) of the cover \(X_0(2) \to X(1)\) is known to be defined over \(K\) (since \(\text{Cl}^+(K, 2)\) is trivial). Therefore \(K\) must be the field of definition of the pre-image of the point \(T = -1\) by the cover \(\mathcal{H}_{PSL_2(F_8)} \to \mathcal{H}\); hopefully, it does! As in the context of triangle groups where J.Voight has shown in the claim following theorem 6.2 of [Voi06], that the curve \(X(2)\) may have a model defined over \(\mathbb{Q}\). Nevertheless, the automorphisms of the Galois cover \(X(2) \to X(1)\) are certainly not defined over \(\mathbb{Q}\).

### 3 Rational CM-points on \(X(1)\)

Before listing rational CM points, we come back over the three elliptic points \(P_1, P_2, P_3\) of order 2 on \(X(1)\). They are CM by \(K(\sqrt{-1})\) and thanks to Shimura’s result, we must have:

\(K(\sqrt{-1})^\text{hilb} = K(\sqrt{-1}) \cdot K(P_1)\).

Hopefully, this is true. Indeed, the field of definition of the \(P_i\)’s is the cubic field \(\mathbb{Q}(\theta_1)\) with \(\theta_1^3 - \theta_1^2 - 4\theta_1 + 12\) whose discriminant is equal to \(2^7 3^2\) and one can check that \(K(\sqrt{-1})^\text{hilb} = K(\sqrt{-1}, \theta_1)\).

Following Elkies, the rational CM points on \(X(1)\) must come from a CM-fields \(K(\sqrt{-D})\) for \(D \in \mathbb{Q}_+\) such that \(\mathbb{Q}(\sqrt{-D})\) is principal. An easy computation shows that only \(D = 2, 3, 7\) can appear.

**Proposition 6** On \(X(1)\) there are CM points who are defined over \(\mathbb{Q}\):

1. the pole of \(\varphi\), namely the unique elliptic point of order 3, which is CM by \(K(\sqrt{-3})\),
2. the point with \(\varphi\)-coordinate equal to \(\frac{2^{3} 3^{3} 11}{3^{3}}\) which is CM by \(K(\sqrt{-7})\),
3. the point with \(\varphi\)-coordinate equal to \(\frac{23549}{3^{3}}\) which is CM by \(K(\sqrt{-2})\).

**Proof** — The unique pole of \(\varphi\) is known to be CM by \(K(\sqrt{3})\). In order to calculate some other rational CM-points, we compute the “modular polynomial” \(\Phi_2(X, Y)\) which is the algebraic relation between \(\varphi\) and \(\varphi \circ w_2\). It is a
symmetric polynomial of bi-degree $(9,9)$. The polynomial $\Phi_2(X, X)$ factorizes into:

$$\Phi_2(X, X) = (X - \frac{4752}{125})^2 (X + \frac{23549}{125}) \left(X^3 - X^2 - 992X - 20736 \right) \times$$

$$\left(X^3 + \frac{95568}{125}X^2 - \frac{1212672}{125}X - \frac{23493376}{125}\right)^2 \times$$

$$\left(X^3 - \frac{16752}{125}X^2 - \frac{2291028}{15625}X + \frac{112619296}{15625}\right).$$

Necessarily, the two rational roots of this polynomial are rational CM points on $X(1)$.

On $X_0(2)$ there is a point $Q$, defined over $\mathbb{Q}(\sqrt{-7})$, such that $\varphi(Q) = \varphi(w_2(Q)) = \frac{4752}{125}$. This means that the point $\varphi = \frac{4752}{125}$ is CM by $K(\sqrt{-7})$.

Above the point $\varphi = -\frac{23549}{125}$ on $X_0(2)$, there are eight points conjugate to each other over $\mathbb{Q}$, and whose field of definition is a degree eight number field $M$ such that $K(\sqrt{-2}) \cdot M$ corresponds to the 2-ray class field of $K(\sqrt{-2})$. Thus, the point $\varphi = -\frac{23549}{125}$ is necessarily CM by $K(\sqrt{-2})$. □

References

[Elk98] Noam D. Elkies. Shimura curve computation. In Joe P. Buhler, editor, *Proceedings of ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 1–47. Springer, 1998.

[Elk06] Noam D. Elkies. Shimura curves for level-3 subgroups of the $(2,3,7)$ triangle group and some other examples. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 302–316. Springer, 2006.

[Hal05] Emmanuel Hallouin. Study and computation of a Hurwitz space and totally real $PSL_2(\mathbb{F}_8)$-extensions of $\mathbb{Q}$. *Journal of Algebra*, 292:259–281, 2005.

[Kat92] Svetlana Katok. *Fuchsian Groups*. Chicago Lectures in Mathematics. University of Chicago Press, 1992.

[Shi67] Goro Shimura. Construction of class fields and zeta functions of algebraic curves. *Annals of Mathematics*, 85:58–159, 1967.

[Voi06] John Voight. Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 406–420. Springer, 2006.

8