The moduli scheme $Y_{\mathrm{ns}}^{+}(7)$ and the class number one problem

Jürgen Böhm

December 11, 2007

Contents

Abstract

For the moduli scheme $X_{\mathrm{ns}}^{+}(7)/\mathbb{Z}[1/7]$ of elliptic curves with a certain level 7 structure an explicit description as a finite cover of $\mathbb{P}^1_{\mathbb{Z}[1/7]}$ is computed. To achieve this, methods from computer–algebra (gröbner–bases and algorithms for computing with fundamental domains of congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$) and algebraic geometry are combined.

Using the explicit knowledge of the finite cover, a diophantine equation of Thue–type is derived, which has as integral solutions 12 pairs of numbers describing 12 different $\mathbb{Z}[1/7]$–integral points on $X_{\mathrm{ns}}^{+}(7)/\mathbb{Z}[1/7]$, that arise from certain elliptic curves. The j–invariants of these curves are computed and it is checked if the curves have complex–multiplication.

All but finitely many imaginary quadratic fields of class number one give rise to $\mathbb{Z}[1/7]$–integral points on $Y_{\mathrm{ns}}^{+}(7)$. These are all different and correspond to elliptic curves with complex multiplication. So finally the classical result that the number of these fields is finite is recovered.

1 Introduction

1.1 Preliminary remark

In this article methods of [4] are used to study the moduli scheme $X_{\mathrm{ns}}^{+}(7)$ instead of the moduli scheme $X_{\mathrm{ns}}^{+}(5)$ considered there.

The goal is to give an explicit presentation of $X_{\mathrm{ns}}^{+}(7)$ and then to find the $\mathbb{Z}[1/7]$–integral points of its open subscheme $Y_{\mathrm{ns}}^{+}(7)$. Knowing these points allows us to give a new proof of the finiteness of the number of fields $\mathbb{Q}(\sqrt{-d})$ with class number $h = 1$ and $d > 0$.

1.2 Basic notions

Elliptic curves An elliptic curve E over a scheme S is given by a smooth proper map $E \xrightarrow{p} S$ of relative dimension 1 and with geometrically connected fibers of genus 1 together with a section $O : S \to E$ with $p \circ O = \mathrm{id}_S$

An elliptic curve E/S carries the structure of an abelian group scheme over S with the section O playing the role of a zero in the abelian group $E(S)$. As E is an abelian group scheme, there exists a morphism $[N] : E \to E$, which is multiplication by the integer N. The kernel of this morphism is the subgroup scheme of *N–division points* and shall be denoted $E[N]$ ($N \geqslant 2$). For its properties see [7, Theorem 2.3.1].

An *elliptic curve E/S with a full level N–structure* is a pair

$$(E/S, \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N](S)),$$

where the induced homomorphisms $\alpha_s : (\mathbb{Z}/N\mathbb{Z})^2 \to E[N](k(s))$ are isomorphisms for all $s \in S$.

Equivalently α can be regarded as giving an isomorphism of group schemes over S: $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \times S \xrightarrow{\sim} E[N]$.

Elliptic curves with full level N–structures can be considered as a category with morphisms

$$f : (E \xrightarrow{p} S, \alpha) \to (E' \xrightarrow{p'} S', \alpha')$$

being morphisms $f : E \to E'$ and $g : S \to S'$ which fulfill $p' \circ f = g \circ p$ and $f \circ \alpha(w) = \alpha'(w) \circ g$.

If $(E/S, \alpha)$ together with a morphism $g : S' \to S$ is given, there is a canonical level N–structure α' on the elliptic curve $E'/S' = S' \times_S E/S'$. It is $\alpha'(w) = g^*(\alpha(w))$ defined by $p'_S(\alpha'(w)) = \mathrm{id}_{S'}$ and $p_E(\alpha'(w)) = \alpha(w) \circ g$.

Taking all together, we have a morphism $(E'/S', \alpha') \to (E/S, \alpha)$ in the category of elliptic curves with full N–structure. The pair $(E'/S', \alpha')$ we call *induced from* $(E/S, \alpha)$ by g.

Moduli schemes For elliptic curves $(E/S, \alpha)$ with full level N–structure ($N \geqslant 3$) for which S is a $\mathbb{Z}[1/N]$–scheme there exists a so called *fine moduli scheme* over $\mathbb{Z}[1/N]$.

In accordance with [7, Corollary 4.7.2] I call this scheme $Y(N)$. It is a smooth affine curve over $\mathbb{Z}[1/N]$.

The property of being a fine moduli scheme has the following meaning: There is a *universal elliptic curve with full N–structure* over $Y(N)$, which I call $(\mathbf{E}/Y(N), \alpha)$. Now for every elliptic curve $(E/S, \alpha)$ over a scheme S on which N is invertible, there is a unique morphism $g : S \to Y(N)$ and a commutative diagram

$$\begin{array}{ccc} (E, \alpha) \cong (S \times_{Y(N)} \mathbf{E}, \alpha') & \longrightarrow & (\mathbf{E}, \alpha) \\ \downarrow & & \downarrow \\ S & \xrightarrow{\quad g \quad} & Y(N) \end{array}$$

representing morphisms in the category of elliptic curves with N–structure. The isomorphism $(E,\alpha) \cong (\mathbf{E} \times_{Y(N)} S, \alpha')$ is uniquely determined.

Using this property the scheme $Y(N)$ is endowed with an operation

$$\rho_g : Y(N) \to Y(N)$$

of $G = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, defined over $\mathbb{Z}[1/N]$, which stems from the operation

$$\rho_g : (E/S, \alpha) \mapsto (E/S, \alpha \circ g^{\mathrm{t}})$$

for a $g \in G$.

There is a complex–analytical isomorphism

$$Y(N)(\mathbb{C}) \cong \Gamma(N)\backslash\mathfrak{H} \times (\mathbb{Z}/N\mathbb{Z})^* \tag{1}$$

Therein $\mathfrak{H}$ stands for the upper half plane $\{z \in \mathbb{C} \mid \Im z > 0\}$, and $\Gamma(N)$ is the group of matrices from $\mathrm{SL}_2(\mathbb{Z})$, congruent to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ modulo N. This group $\Gamma(N)$ is called *principal congruence subgroup of level N*

The isomorphism (1) results from the *modular interpretation* of both sides of the isomorphism.

The term "modular interpretation", as used here, stands for associating a given set canonically with a certain set of isomorphism classes of elliptic curves, possibly with an additional structure, for example a full N–structure.

The left side of (1) corresponds to the isomorphism classes of elliptic curves with full level N–structure over $\mathbb{C}$. The right side of (1) has the modular interpretation

$$(\tau, m) \mapsto (\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), (\alpha(1,0) = \tau/N, \alpha(0,1) = m/N)) = (E_\tau/\mathbb{C}, \alpha_{\tau,m})$$

where the elliptic curve $E_\tau/\mathbb{C}$ is defined by the lattice $\mathbb{Z}+\tau\mathbb{Z} \subset \mathbb{C}$ and $\alpha_{\tau,m}$ is a well–defined full level N–structure on $E_\tau/\mathbb{C}$.

It is a theorem, that both sets are in one-to-one correspondance.

The group $\mathrm{SL}_2(\mathbb{Z})$ operates canonically on $\mathfrak{H}$ ($\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z = \frac{az+b}{cz+d}$). This operation gives rise to an operation of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\Gamma(N)\backslash\mathfrak{H}$. Additionally there is the canonical operation of $(\mathbb{Z}/N\mathbb{Z})^*$ on itself.

Together an operation ρ'_g of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\Gamma(N)\backslash\mathfrak{H} \times (\mathbb{Z}/N\mathbb{Z})^*$ results, which makes the diagram

$$\begin{array}{ccc} Y(N)(\mathbb{C}) & \xrightarrow{\cong} & \Gamma(N)\backslash\mathfrak{H} \times (\mathbb{Z}/N\mathbb{Z})^* \\ \downarrow{\scriptstyle \rho_g(\mathbb{C})} & & \downarrow{\scriptstyle \rho'_g} \\ Y(N)(\mathbb{C}) & \xrightarrow{\cong} & \Gamma(N)\backslash\mathfrak{H} \times (\mathbb{Z}/N\mathbb{Z})^* \end{array}$$

commute.

The scheme $Y(N)$ can be completed to a scheme $X(N)$ over $\mathbb{Z}[1/N]$, in which it is contained as an open subscheme. For details see [7, (8.6)] or [5, section 4.]. We will need the following facts:

The operation of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $Y(N)$ extends itself to $X(N)$.

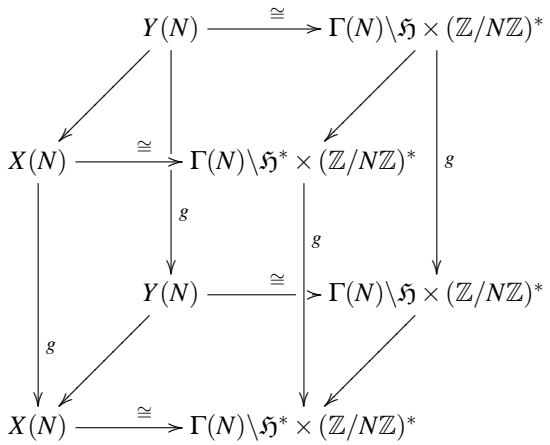
There is a complex–analytical isomorphism

$$X(N)(\mathbb{C}) \cong \Gamma(N)\backslash\mathfrak{H}^* \times (\mathbb{Z}/N\mathbb{Z})^*,$$

where $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$ is the upper half plane together with the so called *cusps*.

The operation of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathfrak{H}$ extends itself naturally on $\mathfrak{H}^*$, and therefore also the operation of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ extends on $\Gamma(N)\backslash\mathfrak{H}^* \times (\mathbb{Z}/N\mathbb{Z})^*$.

Again there is a commutative diagram expressing compatibility of operations:



The classical modular curves The connection of the abovely used terminology with the classical use of the term "modular curve" is the following: Classically one starts from an observation, that the points of a suitable quotient $\Gamma_H\backslash\mathfrak{H} = Y(\Gamma_H)$ are in one to one correspondence with the isomorphism classes over $\mathbb{C}$ of elliptic curves carrying some additional structure.

If the structure is a full level N–structure α with the extra condition, that

$$e_n(\alpha(1,0),\alpha(0,1)) = \exp(2\pi i/N) = \zeta_N$$

where e_n is the Weil pairing, then $\Gamma_H = \Gamma(N)$ and the quotient $\Gamma(N)\backslash\mathfrak{H}$ is called $Y(N)$ and its completion with the cusps added $X(N)$. At first hand $X(N)$ is defined over $\mathbb{C}$, but by suitable constructions one can get a model defined over $\mathbb{Q}(\zeta_N)$. It is even true, that for every congruence subgroup $\Gamma_H \subseteq \mathrm{SL}_2(\mathbb{Z})$ a model of $\Gamma_H\backslash\mathfrak{H}$ over an algebraic number field k_{Γ_H} can be constructed ([10, 6.7]).

Now the model $Y(N)/\mathbb{Q}(\zeta_N)$ introduced in the preceding paragraph is nothing else but the base extension $Y(N)_{\mathbb{Q}(\zeta_N)}$ of the modular scheme $Y(N)/\mathbb{Z}[1/N]$ as both have the same modular interpretation of the sets $Y(N)(K)$ for an algebraic number field $K \supseteq \mathbb{Q}(\zeta_N)$.

Quotients of moduli schemes Let a subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be given. Then call $\tilde{\Gamma}_H$ its preimage under $\mathrm{GL}_2(\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and set $\Gamma_H = \tilde{\Gamma}_H \cap \mathrm{SL}_2(\mathbb{Z})$. Now the quotient schemes

$$Y(N)^H$$
$$X(N)^H$$

can be formed.

Their complex valued points are

$$Y(N)^H(\mathbb{C}) \cong \Gamma_H\backslash\mathfrak{H} \times ((\mathbb{Z}/N\mathbb{Z})^*/(\det H)) \tag{2}$$
$$X(N)^H(\mathbb{C}) \cong \Gamma_H\backslash\mathfrak{H}^* \times ((\mathbb{Z}/N\mathbb{Z})^*/(\det H)) \tag{3}$$

Definition 1.1 *We now define a pre-H–structure on an elliptic curve E/S as H-orbit $[\alpha]_H$ of N–structures $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N](S)$ under the operation $\alpha \mapsto \alpha \circ h^t$ for a $h \in H$.*

Then a H–structure on an elliptic curve E/S can be defined as follows

Definition 1.2 *A H–structure on E/S is given by a set $[\alpha_\kappa]_H$ of pre-H–structures on the elliptic curves E_κ/S_κ, where $(S_\kappa \to S)_\kappa$ is an etale covering family of S and $E_\kappa = E \times_S S_\kappa$. Furthermore it is required that for every κ_1, κ_2 there has to exist an etale covering family $(S_{\lambda\kappa_1\kappa_2} \to S_{\kappa_1} \times_S S_{\kappa_2})$ such that the pullbacks of $[\alpha_{\kappa_1}]_H$ and $[\alpha_{\kappa_2}]_H$ to $E_{\lambda\kappa_1\kappa_2}/S_{\lambda\kappa_1\kappa_2}$ agree as pre-H-structures on $E_{\lambda\kappa_1\kappa_2}/S_{\lambda\kappa_1\kappa_2}$.*

One notes, that for $S = \mathrm{spec}(L)$, with L an algebraically closed field, a H–structure on E/L is identical to a pre-H–structure.

Then the variety of points $Y(N)^H(L)$ for any algebraically closed field L with $N \in L^*$ parameterizes the set of elliptic curves $(E/\mathrm{spec}(L), [\alpha]_H)$ with H–structure. The scheme $Y(N)^H$ is then called a *coarse moduli scheme* for elliptic curves with H–structure. A fine moduli scheme for elliptic curves with H–structure does not exist in general.

The moduli schemes $Y^+_{\mathbf{ns}}(p)$ and $X^+_{\mathbf{ns}}(p)$ In what follows, we will consider specifically the groups

$$\bar{H}^0_p(l) = \left\{ \begin{pmatrix} a & bl \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \right\} \cup \left\{ \begin{pmatrix} a & bl \\ -b & -a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \right\} \tag{4}$$
$$l \in \mathbb{Z}/p\mathbb{Z}, \quad l \text{ quadratic non-residue}$$

It is $\det \bar{H}^0_p = (\mathbb{Z}/p\mathbb{Z})^*$ and therefore $X(p)^{\bar{H}^0_p}(\mathbb{C}) \cong H_p \backslash \mathfrak{H}^*$, where H_p shall be a short notion for the group, that had to be called $\Gamma_{\bar{H}^0_p}$ following the convention explicated in the preceding paragraph.

Furthermore we write, following [4], $Y^+_{\mathrm{ns}}(p)$ and $X^+_{\mathrm{ns}}(p)$ for $Y(p)^{\bar{H}^0_p}$ and $X(p)^{\bar{H}^0_p}$.

Now let $K/\mathbb{Q}$ be an imaginary–quadratic number field with associated elliptic curve $E_{(K)}/\mathbb{C}$, defined by the period lattice $\mathcal{O}_K$, that is, the principal order in K. The j–invariant of $E_{(K)}$ is equal to the j–invariant of the lattice $\mathcal{O}_K$, so non–isomorphic K give rise to different j–invariants of the associated elliptic curves.

Definition 1.3 *For an integer N and an elliptic curve $E/\mathbb{C}$ the image of $\mathrm{End}(E)$ in $\mathrm{End}(E[N](\mathbb{C}))$ is a subring of $\mathrm{End}(E[N](\mathbb{C}))$, which we will call $B_N(E)$.*

Since now we write $B(E)$ for $B_p(E)$. Now the following holds:

Proposition 1.1 *One can choose a fixed subring $R_{p,i} \subseteq Mat(2, \mathbb{F}_p)$ in such a way, that for all K, in which p is inert, $B(E_{(K)}) = \alpha \circ R_{p,i} \circ \alpha^{-1}$ holds for suitable chosen full p–structures $\alpha : (\mathbb{Z}/p\mathbb{Z})^2 \xrightarrow{\sim} E_{(K)}[p](\mathbb{C})$ on $E_{(K)}$.*

Generally, two p–structures, α_1, α_2 on an elliptic curve E satisfying

$$B(E) = \alpha_j \circ R_{p,i} \circ \alpha_j^{-1}$$

are related by $\alpha_1 = \alpha_2 \circ h^t$ with $h \in \bar{H}^0_p$.

In [5, section 1.] a generalization of this proposition is shown, but to be independent of this reference, I give a shortened proof here: The p–division points $E_{(K)}[p](\mathbb{C})$ are $\frac{1}{p}\mathcal{O}_K/\mathcal{O}_K \cong \mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_{p^2}$. They form a one dimensional $\mathbb{F}_{p^2}$–module.

Now the map $\psi : \mathrm{End}(E_{(K)}) \to \mathrm{End}(E_{(K)}[p](\mathbb{C}))$ corresponds to $\mathcal{O}_K \to \mathrm{End}_{\mathbb{F}_{p^2}}(\mathbb{F}_{p^2}) = \mathbb{F}_{p^2}$ with $z \mapsto (w \mapsto \bar{z}w)$, wherein $w \in \mathbb{F}_{p^2}$ and $\bar{z}$ is the image of $z \in \mathcal{O}_K$ in $\mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_{p^2}$.

Setting $\lambda = \sqrt{l}$ with l a quadratic non–residue in $\mathbb{F}_p$ one has an $\mathbb{F}_p$–basis $(1, \lambda)$ of $\mathbb{F}_{p^2}$. Because of $\mathbb{F}_{p^2} \cong E_{(K)}[p](\mathbb{C})$ this basis can be regarded as giving a level p–structure α on $E_K/\mathbb{C}$.

Now the image of ψ is equal to $\mathbb{F}_{p^2} \cong \mathrm{End}_{\mathbb{F}_{p^2}}(E_{(K)}[p])$. Using the basis $(1, \lambda)$ of $\mathbb{F}_{p^2} \cong E_{(K)}[p]$ one gets an imbedding $\mathrm{End}_{\mathbb{F}_{p^2}}(E_{(K)}[p]) \cong \mathbb{F}_{p^2} \cong R \subseteq \mathbb{F}_p^{2\times 2}$. The ring R is $\mathbb{F}_p[u]$ with $u = \left(\begin{smallmatrix} 0 & l \\ 1 & 0 \end{smallmatrix}\right)$.

One can put $R_{p,\mathrm{i}} = R$ by choosing α defined through the basis $(1,\lambda)$ of $\mathbb{F}_{p^2} \cong E_{(K)}[p](\mathbb{C})$.

To prove the second part of the proposition note that the condition

$$gRg^{-1} = R \tag{5}$$

with $g \in \mathrm{GL}_2(\mathbb{F}_p)$ expresses that the level p-structures $\alpha_1 = \alpha$ and $\alpha_2 = \alpha \circ g$ both satisfy the relation $B(E) = \alpha_j \circ R_{p,\mathrm{i}} \circ \alpha_j^{-1}$ from the proposition.

As R is the group of matrices $\left(\begin{smallmatrix} p & ql \\ q & p \end{smallmatrix}\right)$, which is visibly a subgroup of $\bar{H}_p^0(l)$, the condition (5) means, that g is from the normalizer of this subgroup. Now it is known (and can be easily proved by a direct calculation with the equations expressing (5)), that this normalizer is $\bar{H}_p^0(l)$, so α_1 and α_2 are related by $\alpha_1 = \alpha_2 \circ g$ with $g \in \bar{H}_p^0(l)$, which is equivalent to $g^{\mathrm{t}} \in \bar{H}_p^0(1/l)$. (See also [4, p.4], where the fact is mentioned that $\bar{H}_p^0$ equals N_z, the normalizer of a so called non–split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. This explains the choice of the name of the index in $X_{\mathrm{ns}}^+(p)$). QED.

Let in the following H stand for $\bar{H}_p^0$ and $L/\mathbb{Q}$ for an algebraic extension field.

Now let E/L be an elliptic curve with $[\alpha_{B(E)}]_H$ an H–structure, fulfilling $B(E) = \alpha_{B(E)} \circ R_{p,i} \circ \alpha_{B(E)}^{-1}$. Then $(E_{\mathbb{C}}, [\alpha_{B(E)}]_H)$ corresponds to a point $r_E : \mathrm{spec}(\mathbb{C}) \to Y_{\mathrm{ns}}^+(p)$.

Next consider an automorphism $\theta : \mathbb{C} \to \mathbb{C}$ and the corresponding cartesian square

$$\begin{array}{ccc} E' = E \times_{\mathbb{C}} \mathbb{C} & \xrightarrow{f_\theta} & E \\ \downarrow & & \downarrow \\ \mathbb{C} & \xrightarrow{\theta^*} & \mathbb{C} \end{array} \tag{6}$$

Now there is a corresponding $[\alpha_{B(E')}]_H$ for E' with $B(E') = \alpha_{B(E')} \circ R_{p,i} \circ \alpha_{B(E')}^{-1}$. It fulfills the relation

$$f_\theta \circ \alpha_{B(E')} = \alpha_{B(E)}.$$

The pair $(E'_{\mathbb{C}}, [\alpha_{B(E')}]_H)$ gives rise to a point $r_{E'} : \mathrm{spec}(\mathbb{C}) \to Y_{\mathrm{ns}}^+(p)$. Together the two points satisfy

$$r_E \circ \theta^* = r_{E'} \tag{7}$$

If one chooses θ fixing the subfield L, then $E' = E$, $B(E) = B(E')$, $f_\theta = \mathrm{id}$ and $[\alpha_{B(E)}]_H = [\alpha_{B(E')}]_H$. So $r_E = r_{E'}$. Now $Y_{\mathrm{ns}}^+(p) = \mathrm{spec}(C^H)$ and (7) can be expressed as $\theta \circ \eta_E = \eta_{E'}$, where $\eta_E : C^H \to \mathbb{C}$ and $\eta_{E'} : C^H \to \mathbb{C}$ are the ring homomorphisms corresponding to r_E and $r_{E'}$. As $\eta_E = \eta_{E'}$ and θ is arbitrary only subject to the condition to fix L, this entrains $\eta_E(C^H) \subseteq L$. So the pair $(E/L, [\alpha_{B(E)}]_H)$ corresponds to a point $Y_{\mathrm{ns}}^+(p)(L)$.

So we have, as $E_{(K)}$ is defined already over $L = \mathbb{Q}$:

Proposition 1.2 *We can interpret the $B(E_{(K)})$ as $\bar{H}_p^0$–structures $[\alpha]_{\bar{H}_p^0}$ on the elliptic curves $E_{(K)}$ which stem from imaginary quadratic fields K in which p is inert.*

Any such curve $(E_{(K)}/\mathbb{C}, [\alpha]_{\bar{H}_p^0})$ therefore gives rise to a point P_K in $Y_{ns}^+(p)(\mathbb{Q})$.

In [5, 5.4.2] a stronger statement is shown:

Proposition 1.3 *For $K/\mathbb{Q}$, imaginary quadratic with class number 1 in $\mathcal{O}_K$, the point P_K stems from a point P'_K in $Y_{ns}^+(\mathbb{Z}[1/p])$.*

The proof there goes as follows: The point P_K corresponds to a morphims $\eta : C^H \to \mathbb{C}$, where $\mathrm{spec}(C) = Y(p)$. The rings C and C^H are integral over the subring $\mathbb{Z}[1/p, j]$ and $\eta(j)$ is equal to the classical j–invariant j_K of $E_{(K)}$ over $\mathbb{C}$. But in the special case of K imaginary quadratic and of class number one, this j_K is in $\mathbb{Z}$. So first, $\eta(C^H)$ is integral over $\mathbb{Z}[1/p]$ and secondly $\eta(C^H) \subseteq \mathbb{Q}$ holds because of the previous proposition. Together $\eta(C^H) = \mathbb{Z}[1/p]$ follows. QED.

1.3 Purpose of this article

In this article we will single out the case $p = 7$ and settle some questions that remained open in [5, section 6.].

Especially we study the covering

$$\pi : X_{\mathrm{ns}}^{+}(7) \to X(1) \tag{8}$$

over $\mathbb{Z}[1/7]$, where $X(1)$ shall stand for $X(7)^{\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})}$, which corresponds to the coarse moduli scheme for elliptic curves without additional structure. The map π corresponds, interpreted modularly, to "forgetting" the $\bar{H}_7^0$–structure.

The scheme $X(1)$ is exactly known:

Proposition 1.4 *There is an isomorphism:* $X(1) \cong \mathbb{P}^1_{\mathbb{Z}[1/7]}$.

Going over to complex–valued points, and restricting to $Y(1) \stackrel{\mathrm{def}}{=} Y(7)^{\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})}$, this isomorphism maps an elliptic curve $E/\mathbb{C}$ to its j–invariant.

Furthermore the following is true:

Proposition 1.5 *There is an isomorphisms* $\kappa : X_{ns}^{+}(7) \cong \mathbb{P}^1_{\mathbb{Z}[1/7]}$ *of* $\mathbb{Z}[1/7]$*–schemes.*

For reasons of space, I can only sketch the proof given in [5, section 6.3]: First one uses that $X_{\mathrm{ns}}^{+}(7)$ is projective over $\mathbb{Z}[1/7]$ together with the fact that $X_{\mathrm{ns}}^{+}(7)_{\mathbb{Q}}$ is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ to conclude that for every $t \in \mathrm{spec}(\mathbb{Z}[1/7])$ there is an isomorphism $X_{\mathrm{ns}}^{+}(7)_t \cong \mathbb{P}^1_{k(t)}$. For this step the Riemann–Roch theorem and the semicontinuity theorems of cohomology are used.

In a second step the existence of a section $s : \mathrm{spec}(\mathbb{Z}[1/7]) \to X_{\mathrm{ns}}^{+}(7)$ is used to construct the line bundle $\mathcal{L} = (\ker(\mathcal{O}_{X_{\mathrm{ns}}^{+}(7)} \to s_* \mathcal{O}_{\mathbb{Z}[1/7]}))^{-1}$ on $X_{\mathrm{ns}}^{+}(7)$. Then two everywhere generating sections T_0, T_1 of this bundle are proven to exist. They give a morphism $\kappa : X_{\mathrm{ns}}^{+}(7) \to \mathbb{P}^1_{\mathbb{Z}[1/7]}$ over $\mathbb{Z}[1/7]$ which is an isomorphism. QED.

Now in [5] the question is raised, if κ can be so chosen that the covering $\mathbb{P}^1_{\mathbb{Z}[1/7]} \to \mathbb{P}^1_{\mathbb{Z}[1/7]}$ induced from (8) can be described in a certain, explicit way. We will answer this question in the affirmative.

Following that, there is the question to find the solutions of a certain diophantic equation of Thue–type, that originates from the explicit description of (8).

Thanks to newer results in this field we can determine all solutions with the help of computer–algebra systems (MAGMA, KASH). As a consequence all points $Y_{\mathrm{ns}}^{+}(7)(\mathbb{Z}[1/7])$ are explicitly known as pairs of integers.

Using the explicit description of (8) we can then compute the value of the j–invariant belonging to each of these pairs.

There exist 12 points $Y_{\mathrm{ns}}^{+}(7)(\mathbb{Z}[1/7])$, of which 6, as one can verify by looking up their j-invariant in suitable tables, come from imaginary quadratic fields K of class number 1 and discriminant $-d \geqslant -163$ in the abovely discussed way. The remaining 6 belong to elliptic curves, that either do not admit complex multiplication, or are not defined through the principal order of an imaginary quadratic field or stem from the principal order in an imaginary quadratic field, in which $p = 7$ is not inert.

An application to the problem of determining all number fields $K = \mathbb{Q}(\sqrt{-d})$ with class number 1 results from the observation, that for all those with discriminant $-d < -163$ the prime number $p = 7$ is inert in K. These K would therefore produce additional $\mathbb{Z}[1/7]$–valued points on $Y_{\mathrm{ns}}^{+}(7)$ (note, that the points must be different, because their j–invariant would be different).

As such points do not exist, it can be concluded (independently of former proofs of this fact) that there are no further imaginary quadratic fields with class number one, apart from those known with discriminant $-d \geqslant -163$.

2 Algorithms

Let Γ and Γ_1 be two level N congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ (that is, preimages of subgroups of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ under the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ given by $\mathbf{A} \mapsto \mathbf{A} \mod N$) with $\Gamma \subseteq \Gamma_1$, which are concretely given by their images $\overline{\Gamma}$ and $\overline{\Gamma}_1$ under $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

In this section I will specify algorithms to compute a fundamental domain for $\Gamma\backslash\mathfrak{H}^*$, to describe the covering $\Gamma\backslash\mathfrak{H}^* \to \Gamma_1\backslash\mathfrak{H}^*$, and to analyze the ramification of $\Gamma\backslash\mathfrak{H}^* \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$.

Before expounding the algorithms in detail, I want to explain some terms used in this connexion. The reader who already has an idea, what to understand by a *list* as an abstract datastructure, can skip the following subsection.

2.1 Lists

1. A *list list* of length $n \in \mathbb{N}_0$ with values from a set V is a mapping $list : \{i \in \mathbb{N} \mid 1 \leqslant i \leqslant n\} \to V$. A list of length 0 is called *empty* and will be represented by []. The expression $list[i]$ shall mean $list(i)$ and is called *i-th element of list*.
2. On lists operate the functions append, map, select.

   Now for a list *list* of length n with values in V and v from V, append$(list, v)$ is a list of length $n+1$, which on $\{i \mid 1 \leqslant i \leqslant n\}$ agrees with *list* and whose $(n+1)$-th element is v.

   The function map$(z \mapsto g(z), list)$ returns for a given map $g : V \to W$ and a list *list* with values in V a list $list_1$ of the same length as *list* with $list_1[i] = g(list[i])$.

   The function select$(z \mapsto h(z), list)$ returns for a map $h : V \to \{\text{TRUE}, \text{FALSE}\}$ and a list *list* with values in V and of length n a list $list_1$ of length m, so that a bijection $\psi : \{1, \ldots, m\} \to \{i \mid 1 \leqslant i \leqslant n, h(list[i]) = \text{TRUE}\}$ exists for which $\psi(i) < \psi(j)$ for $i < j$ and $list_1[i] = list[\psi(i)]$ holds.
3. The expression $[v_1, \ldots, v_n]$ shall represent the list $list : \{1, \ldots, n\} \to V$ with $list[i] = v_i$.
4. By $v \in list$ we mean $\exists i : v = list[i]$.
5. It is first$(list) \stackrel{\text{def}}{=} list[1]$ for all non–empty lists.
6. For a list *list* of length n the function rest is defined by rest$(list) \stackrel{\text{def}}{=} [list[2], \ldots, list[n]]$. The cases $n = 1$ and $n = 0$ are allowed and have the empty list as return value.

2.2 The algorithms

The first two functions are trivial auxiliary functions:

The function IN-SUBGROUP$(\mathbf{M}, \overline{\Gamma})$ answers the question, whether a matrix $\mathbf{M}$ from $\mathrm{SL}_2(\mathbb{Z})$ lies in the subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ that is given by its image $\overline{\Gamma}$ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, considered as a set or list of matrices.

The function GET-INDEX$(\mathbf{M}, patches, \overline{\Gamma})$ determines an index i, such that $\mathbf{M} \sim_\Gamma patches[i]$ holds, where $\mathbf{M}$ and $\overline{\Gamma}$ have the same meaning as in the previous paragraph and *patches* is a list of matrices from $\mathrm{SL}_2(\mathbb{Z})$. The notation $\mathbf{M} \sim_\Gamma patches[i]$ shall stand for $\mathbf{M}\,(patches[i])^{-1} \in \Gamma$.

For technical reasons, which will become clear below, in case of $\mathbf{M} = patches[i]$ the value $-i$ is returned, the negative value serving merely as a "marking" of the special case.

The value i of course need not be determined uniquely, but in the cases where GET-INDEX is called, it will always be.

IN-SUBGROUP($\mathbf{M}, \overline{\Gamma}$)

$\triangleright$ It is $\overline{\Gamma} \subseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.
$\triangleright$ It is $\mathbf{M} \in \mathrm{SL}_2(\mathbb{Z})$.
if $\mathbf{M} \mod N \in \overline{\Gamma}$
  then
    return TRUE
  else
    return FALSE

GET-INDEX($\mathbf{M}, patches, \overline{\Gamma}$)

1 **if** $\mathbf{M} = patches[i]$
2 **then return** $-i$
3 **elseif** IN-SUBGROUP($\mathbf{M}\,(patches[i])^{-\mathbf{1}}, \overline{\Gamma}$)
4 **then return** i
5 **else return** NIL

2.2.1 Computation of a fundamental domain

The following algorithm computes a fundamental domain $\mathcal{F}_\Gamma$ for $\Gamma\backslash\mathfrak{H}^*$. Additionally we require that $\mathcal{F}_\Gamma$ shall be connected.

An algorithm for computing such a $\mathcal{F}_\Gamma$ can be found in [11], the algorithm delineated below is a simplified version of the method described in that article and pays no consideration to a good graphical representability of $\mathcal{F}_\Gamma$.

For use further below the following terms are useful:

Notation 2.1 *With $\overline{\mathcal{F}}$ shall be meant the closure of a fundamental domain of $SL_2(\mathbb{Z})\backslash\mathfrak{H}^*$ that is given by $\{z \in \mathfrak{H} \mid |z| \geqslant 1, -\frac{1}{2} \leqslant \Re z \leqslant \frac{1}{2}\} \cup \{\infty\}$.*

Notation 2.2 *With $\mathbf{T}$, $\mathbf{T^{-1}}$, $\mathbf{S}$ shall be denoted the matrices $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}1 & -1\\ 0 & 1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$ from $SL_2(\mathbb{Z})$.*

Notation 2.3 *For $\mathbf{A}$ from $\{\mathbf{T}, \mathbf{T^{-1}}, \mathbf{S}\}$ the $\mathbf{A}$–side of $\overline{\mathcal{F}}$ shall be defined to be $s_\mathbf{A} = \overline{\mathcal{F}} \cap \mathbf{A}\,\overline{\mathcal{F}}$. Analogously $\mathbf{M}s_\mathbf{A}$ shall be the $\mathbf{A}$-side of $\mathbf{M}\overline{\mathcal{F}}$ for an arbitrary $\mathbf{M}$ from $SL_2(\mathbb{Z})$.*

It then follows, that $\mathbf{M}\overline{\mathcal{F}}$ and $\mathbf{MA}\,\overline{\mathcal{F}}$ have the $\mathbf{A}$–side of $\mathbf{M}\overline{\mathcal{F}}$ in common, or, amounting to the same, that $\mathbf{MT}\overline{\mathcal{F}}$, $\mathbf{MT^{-1}}\overline{\mathcal{F}}$, $\mathbf{MS}\overline{\mathcal{F}}$ are the three neighbouring triangles of $\mathbf{M}\overline{\mathcal{F}}$ as much as $\mathbf{T}\overline{\mathcal{F}}$, $\mathbf{T^{-1}}\overline{\mathcal{F}}$, $\mathbf{S}\overline{\mathcal{F}}$ are those of $\overline{\mathcal{F}}$.

Phrasing the above, I have regarded the fundamental domain closure $\overline{\mathcal{F}}$ as a "triangle" with the "sides" $\overline{\infty\rho}$, $\overline{\rho\,(\mathbf{T}\rho)}$, $\overline{(\mathbf{T}\rho)\,\infty}$ where $\rho = e^{2\pi i/3}$.

Remark 2.1 *The mapping $\mathbf{M}\overline{\mathcal{F}} \to \mathbf{PM}\overline{\mathcal{F}}$ for $\mathbf{P} \in SL_2(\mathbb{Z})$ maps the $\mathbf{T}$, $\mathbf{T^{-1}}$, $\mathbf{S}$–side of $\mathbf{M}\overline{\mathcal{F}}$ to the corresponding side of $\mathbf{PM}\overline{\mathcal{F}}$.*

Remark 2.2 *The following algorithms all require, that $\overline{\Gamma}$ (or $\overline{\Gamma}_1$) contains $\left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)$, because the identity $\mathbf{P}\overline{\mathcal{F}} = -\mathbf{P}\overline{\mathcal{F}} = \mathbf{M}\overline{\mathcal{F}}$ shall be recognizable by the condition $(\mathbf{P}^{-1}\mathbf{M}) \in \overline{\Gamma}$ mod N.*

In our concrete application of the algorithms, this prerequisite will be always satisfied.

FUNDAMENTAL-DOMAIN($\overline{\Gamma}$)

▷ It is $\overline{\Gamma} \subseteq \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

```
1  patches ← [Id]
2  frontier ← patches
3  while frontier ≠ ∅
4       do
5          P ← first(frontier)
6          frontier ← rest(frontier)
7          for A through [T, T^-1, S]
8               do
9                  M ← PA
10                 if ∃ R ∈ patches : IN-SUBGROUP(RM^-1, Γ̄) = TRUE
11                   then next
12                 patches ← append(patches, M)
13                 if M ∉ frontier
14                   then frontier ← append(frontier, M)
15 res ← COMPUTE-CONNECT-RELS(patches, Γ̄)
16 return res
```

COMPUTE-CONNECT-RELS($patches, \overline{\Gamma}$)

```
1  res ← []
2  for P through patches
3       do
4          i_1 ← GET-INDEX(PT, patches, Γ̄)
5          i_2 ← GET-INDEX(PT^-1, patches, Γ̄)
6          i_3 ← GET-INDEX(PS, patches, Γ̄)
7          indices ← [i_1, i_2, i_3]
8          res-element ← [P, indices]
9          res ← append(res, res-element)
10 return res
```

The result of FUNDAMENTAL-DOMAIN($\overline{\Gamma}$) is a list *res* of lists $[\mathbf{M}, [i_1, i_2, i_3]]$ with $\mathbf{M}$ from $\mathrm{SL}_2(\mathbb{Z})$ and i_ν from $\mathbb{Z}$, such that $\bigcup_{1 \leqslant j \leqslant \mathrm{length}(res)} \mathbf{M}_j \overline{\mathcal{F}} = \overline{\mathcal{F}}_\Gamma$ with $\mathbf{M}_j = res[j][1]$ forms a connected fundamental domain for $\Gamma \backslash \mathfrak{H}^*$, if one carries out suitable identifications on the border of $\overline{\mathcal{F}}_\Gamma$.

These identifications are described by the indices i_1, i_2, i_3.

In detail, the indices have the following interpretation:

1. If $i_1 = res[j][2][1] > 0$ the $\mathbf{T}$–side of $\mathbf{M}_j \overline{\mathcal{F}}$ will be identified with the $\mathbf{T^{-1}}$–side of $\mathbf{M}_{i_1} \overline{\mathcal{F}}$, specifically setting $\mathbf{M}_j \mathbf{T} x \sim \mathbf{M}_{i_1} x$, for all x from the $\mathbf{T^{-1}}$–side of $\overline{\mathcal{F}}$.

2. If $i_2 = res[j][2][2] > 0$ the $\mathbf{T^{-1}}$–side of $\mathbf{M}_j \overline{\mathcal{F}}$ will be identified with the $\mathbf{T}$–side of $\mathbf{M}_{i_2} \overline{\mathcal{F}}$, specifically setting $\mathbf{M}_j x \sim \mathbf{M}_{i_2} \mathbf{T} x$, for all x from the $\mathbf{T^{-1}}$–side of $\overline{\mathcal{F}}$.

3. If $i_3 = res[j][2][3] > 0$ the $\mathbf{S}$–side of $\mathbf{M}_j \overline{\mathcal{F}}$ will be identified with the $\mathbf{S}$–side of $\mathbf{M}_{i_3} \overline{\mathcal{F}}$, specifically setting $\mathbf{M}_j \mathbf{S} x \sim \mathbf{M}_{i_3} x$, for all x from the $\mathbf{S}$–side of $\overline{\mathcal{F}}$.

A negative value i_1 (resp. i_2, i_3) indicates the same kind of identification as the corresponding positive value, with the difference that the $\mathbf{T}$–side (resp. the $\mathbf{T^{-1}}$–side, $\mathbf{S}$–side) of $\mathbf{M}_j \overline{\mathcal{F}}$ is an inner side of the constructed fundamental domain $\overline{\mathcal{F}}_\Gamma$.

The list *res* is build up by the program in two stages. First (line 1–14) a list *patches* of matrices $[\mathbf{M}_1, \ldots, \mathbf{M}_r]$ with $\mathbf{M}_i$ from $\mathrm{SL}_2(\mathbb{Z})$ is constructed, so that $\bigcup \mathbf{M}_j \overline{\mathcal{F}} = \overline{\mathcal{F}}_\Gamma$. The routine COMPUTE-CONNECT-RELS then computes the associated gluing–data.

The procedure of construction of *patches* is that of a breadth–first search in a directed graph, controlled by the list *frontier*, which is used as a queue. The graph has as nodes the matrices $\mathbf{M}$ from $\mathrm{SL}_2(\mathbb{Z})$ and for each node $\mathbf{M}$ exactly three outgoing edges, which lead to $\mathbf{MT}$, $\mathbf{MT^{-1}}$, $\mathbf{MS}$. We call them *edges in* $\mathbf{T}$–, $\mathbf{T^{-1}}$–, $\mathbf{S}$–*direction*. On identifying the node $\mathbf{M}$ with the triangle $\mathbf{M}\overline{\mathcal{F}}$ the neighbouring nodes of $\mathbf{M}$ correspond to the neighbouring triangles of $\mathbf{M}\overline{\mathcal{F}}$.

The search starts at $\mathbf{M} = \mathbf{Id}$ (line 1) and proceeds from the first element of *frontier* successively into the $\mathbf{T}$–, $\mathbf{T^{-1}}$– and $\mathbf{S}$–direction as long as the list *frontier*, which contains the triangles not yet taken into account as starting points, is not empty (line 3).

The $\mathbf{T}$–, $\mathbf{T^{-1}}$– or $\mathbf{S}$–neighbour $\mathbf{M}$ of $\mathbf{P}$ which was found in that way is checked in line 10 if it is equivalent modulo Γ to a node already accumulated in the list *patches*.

If yes, the **for**–loop will be advanced (**next** in line 11) and thereby prevented, that two different elements of *patches* are equivalent modulo Γ.

If no, $\mathbf{M}$ will be added to the list *patches* of accumulated nodes, and, if not yet present in *frontier*, appended at its end. This guarantees, that in line 3 all elements of *frontier* are members of *patches*.

As one is proceeding in line 7 always to a $\mathbf{T}$, $\mathbf{T^{-1}}$ or $\mathbf{S}$–neighbour of $\mathbf{P}$, it can be asserted that $\bigcup \mathbf{M}_j \overline{\mathcal{F}}$ will be connected.

The first stage terminates, as all $\mathbf{M}_j$ from *patches* are pairwise inequivalent modulo Γ and $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is well–defined and finite. For that reason the list *frontier* at some point has to become empty, because line 14, in which *frontier* is extended, can be reached only a finite number of times, since each time line 12 had to be reached too.

During the second stage COMPUTE-CONNECT-RELS establishes the gluing–data by considering for each matrix $\mathbf{P}$ from *patches* the $\mathbf{T}$–, $\mathbf{T^{-1}}$– and $\mathbf{S}$–neighbours and finding to each of these neighbours an equivalent or identical matrix lying in *patches*. The existence of such a matrix is clear, because of the termination of the graph–search in the first stage. The matrix is also unique, as $\mathbf{PT} \sim_\Gamma \mathbf{M}_{j_1}$ and $\mathbf{PT} \sim_\Gamma \mathbf{M}_{j_2}$ with $\mathbf{M}_{j_\nu} = \mathit{patches}[j_\nu]$ would imply $\mathbf{M}_{j_1} \sim_\Gamma \mathbf{M}_{j_2}$ in contradiction to the pairwise inequivalence of the matrices from *patches*. That the computed indices have their abovely described meaning follows from 2.1.

2.2.2 Computation of the covering of two fundamental domains

The next algorithm to consider, FUNDAMENTAL-DOMAIN2, computes for two congruence subgroups $\Gamma \subseteq \Gamma_1$ of level N with images $\overline{\Gamma} \subseteq \overline{\Gamma}_1$ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ a description of the covering $\Gamma\backslash\mathfrak{H}^* \to \Gamma_1\backslash\mathfrak{H}^*$.

The invocation has the form FUNDAMENTAL-DOMAIN2$(\mathit{reslist}, \overline{\Gamma}_1)$, where *reslist* is the result of FUNDAMENTAL-DOMAIN$(\overline{\Gamma})$.

The result is a two–element list $[\mathit{res}, \mathit{proj\text{-}list}]$. Therein *res* has the structure of a list returned by FUNDAMENTAL-DOMAIN and describes a fundamental domain $\overline{\mathcal{F}}_{\Gamma_1}$ of $\Gamma_1\backslash\mathfrak{H}^*$ in the way illustrated in the description of FUNDAMENTAL-DOMAIN.

The list *proj-list* is a list of natural numbers $[i_1, \ldots, i_n]$, where n equals the length of *reslist*. The value i_ν has to be interpreted as stating, that under the canonical projection $\Gamma\backslash\mathfrak{H}^* \to \Gamma_1\backslash\mathfrak{H}^*$ the triangle $\mathit{reslist}[\nu][1]\overline{\mathcal{F}}$ from fundamental domain $\overline{\mathcal{F}}_\Gamma$ is mapped to the triangle $\mathit{res}[i_\nu][1]\overline{\mathcal{F}}$ from fundamental domain $\overline{\mathcal{F}}_{\Gamma_1}$.

In that way the result of FUNDAMENTAL-DOMAIN2 describes $\Gamma_1\backslash\mathfrak{H}^*$ as well as $\Gamma\backslash\mathfrak{H}^* \to \Gamma_1\backslash\mathfrak{H}^*$ completely and explicitly.

```
FUNDAMENTAL-DOMAIN2(reslist, Γ̄_1)
    ▷ It is Γ̄ ⊆ Γ̄_1 ⊆ SL_2(ℤ/Nℤ).
    ▷ The list reslist is the result of FUNDAMENTAL-DOMAIN(Γ̄).
 1  patches ← [first(reslist)]
 2  frontier ← patches
 3  while frontier ≠ ∅
 4      do
 5          patch-elem ← first(frontier)
 6          frontier ← rest(frontier)
 7          for i through patch-elem[2]
 8              do
 9                  if i > 0
10                    then next
11                  new-elem ← reslist[−i]
12                  if ∃ j : IN-SUBGROUP((new-elem[1]) (patches[j][1])^{-1}, Γ̄_1)
13                    then next
14                  patches ← append(patches, new-elem)
15                  if new-elem ∉ frontier
16                    then frontier ← append(frontier, new-elem)
17  patches-1 ← map(z ↦ z[1], patches)
18  res ← COMPUTE-CONNECT-RELS(patches-1, Γ̄_1)
19  proj-list ← []
20  for res-elem through reslist
21      do
22          i ← GET-INDEX(res-elem[1], patches-1, Γ̄_1)
23          i ← abs(i)
24          proj-list ← append(proj-list, i)
25  return [res, proj-list]
```

The actual proceeding of FUNDAMENTAL-DOMAIN2 corresponds in the lines 1 to 18 wholly to the proceeding of FUNDAMENTAL-DOMAIN, with the difference, that the graph–search in this case does not advance inside the graph described above, formed by all matrices of $\mathrm{SL}_2(\mathbb{Z})$ as nodes, but inside the subgraph embedded in it which is given by *reslist*. Therein $reslist[i][1]$ corresponds to the node and $j_\nu = reslist[i][2][\nu]$ for $\nu = 1,2,3$ and $j_\nu < 0$ to the $\mathbf{T}$,$\mathbf{T}^{-1}$,$\mathbf{S}$–edges, which go out from this node. The case $j_\nu > 0$ on the contrary stands for a gluing of the respective triangles modulo Γ on the border of the fundamental domain and shall not contribute an edge.

The check in line 9 therefore asserts, that while searching *reslist* only passages to neighbouring nodes are taken into account and gluings modulo Γ are suppressed.

Line 17 in FUNDAMENTAL-DOMAIN2 is only necessary to get from the list *patches* consisting of lists $[\mathbf{M}, [i_1, i_2, i_3]]$ to a list *patches-1* consisting only of matrices. The gluings modulo Γ_1 are established in line 18.

The loop from line 20 to 24 finally constructs *proj-list*, by determining for each $\mathbf{M} =$ *res-elem*$[1]$ the position of the matrix in *patches-1* equivalent to $\mathbf{M}$ modulo Γ_1. As the elements of *patches-1* are inequivalent modulo Γ_1, the i computed in line 22 is uniquely determined.

2.2.3 Computation of the ramification behaviour

As a third problem it remains to give an algorithm for analyzing the ramification behaviour of the covering $\psi : \Gamma\backslash\mathfrak{H}^* \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$. Again, Γ shall designate a congruence subgroup of level N, represented by its image $\overline{\Gamma}$ in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The fundamental domain $\overline{\mathcal{F}}_\Gamma$ shall be described by *reslist*, the result of FUNDAMENTAL-DOMAIN$(\overline{\Gamma})$.

Since the mapping ψ can ramify only above the points $\rho = e^{2\pi i/3}$, $i = \sqrt{-1}$ and ∞ (with ramification indices over ρ resp. i only 3 resp. 2 being possible) it suffices to compute the ramification behaviour over these points.

The algorithms used for that purpose

- COMPUTE-RHO-COVERING
- COMPUTE-I-COVERING
- COMPUTE-INFINITY-COVERING

have much in common and can all be formulated as special cases of COMPUTE- COVERING.

```
COMPUTE-COVERING(reslist, val, select-list)
    ▷ It is reslist the result of FUNDAMENTAL-DOMAIN(Γ̄)
    ▷ It is val ∈ ℂ ∪ {∞}
    ▷ It is select-list a list with values from {1,2,3}
 1  rels ← COMPUTE-RELS(val, select-list, reslist)
 2  rels ← SYMMETRIC-REFLEXIVE-CLOSURE(rels)
 3  elem-followers ← TRANSITIVE-CLOSURE(rels)
 4  equivs ← {}
 5  for equiv-class through elem-followers
 6       do
 7          equivs ← equivs ∪ {equiv-class}
 8  val-images ← COMPUTE-IMAGES(val, reslist)
 9  ergl ← []
10  for equiv-class ∈ equivs
11       do
12          point ← select(z → z[1] ∈ equiv-class, val-images)
13          ergl ← append(ergl, point)
14  return ergl
```

```
COMPUTE-RHO-COVERING(reslist)
    ▷ It is reslist the result of FUNDAMENTAL-DOMAIN(Γ̄)
1   return COMPUTE-COVERING(reslist, ρ, [1,2,3])
```

```
COMPUTE-I-COVERING(reslist)
    ▷ It is reslist the result of FUNDAMENTAL-DOMAIN(Γ̄)
1   return COMPUTE-COVERING(reslist, i, [3])
```

```
COMPUTE-INFINITY-COVERING(reslist)
    ▷ It is reslist the result of FUNDAMENTAL-DOMAIN(Γ̄)
1   return COMPUTE-COVERING(reslist, ∞, [1,2])
```

The idea behind the working of COMPUTE-COVERING is quite straightforward:

For a given *val* from ρ, i, ∞ the images $w_j = \mathbf{M}_j\, val$ for all $\mathbf{M}_j = reslist[j][1]$ are considered. If for a certain image $w = w_j$ exactly e values $j_1, \ldots, j_e$ with $w_{j_\nu} \sim w$ exist, then w represents in the fundamental domain $\overline{\mathcal{F}}_\Gamma$ a point of ramification index e over *val*. The equivalence $w_{j_\nu} \sim w$ shall denote that the two points are equal in $\overline{\mathcal{F}}_\Gamma$, with identifications on the border being taken into account.

The only complications that can arise in this procedure come from the identifications on the borders of $\overline{\mathcal{F}}_\Gamma$.

COMPUTE-RELS To allow for these identifications, in COMPUTE-RELS a relation R among the elements $E_\rho = \{\mathbf{M}_j\,\rho\}_j \cup \{\mathbf{M}_j\,\mathbf{T}\,\rho\}_j$ for $val = \rho$ (resp. the elements $E_i = \{\mathbf{M}_j\sqrt{-1}\}_j$ for $val = i = \sqrt{-1}$, resp. the elements $E_\infty = \{\mathbf{M}_j\,\infty\}_j$ for $val = \infty$) will be computed, so that two elements from E_ρ (resp. E_i, resp. E_∞) are equivalent modulo the symmetric, reflexive and transitive closure R^* of R, if and only if they are identical as elements of $\overline{\mathcal{F}}_\Gamma$, taking the gluings on the border described by *reslist* into account. Concretely given is R by the list *rels* of pairs (w_1, w_2) with w_i from $\mathbb{C} \cup \{\infty\}$, where (w_1, w_2) stands for $w_1 R w_2$.

In particular, from line 9 to 12 of COMPUTE-RELS a possible identification at the **T**–side of *res-el*$[1]\,\overline{\mathcal{F}}$ will be expressed as a relation–pair *rel-1*. This case is relevant for $val = \rho$ and $val = \infty$ and will therefore be selected in COMPUTE-RHO-COVERING, COMPUTE-INFINITY-COVERING by appropriately setting *select-list*.

Analogously from line 14 to 17 of COMPUTE-RELS a possible identification at the $\mathbf{T}^{-\mathbf{1}}$–side of *res-el*$[1]\,\overline{\mathcal{F}}$ will be expressed as a relation–pair *rel-2*. This case too is relevant for $val = \rho$ and $val = \infty$ and so the above remark about setting *select-list* applies.

Finally the possible identification at the **S**–side of *res-el*$[1]\,\overline{\mathcal{F}}$ is treated from line 19 to 24, here the relation–pairs *rel-3a* and *rel-3b* are generated. This case is relevant for $val = \rho$ and $val = i = \sqrt{-1}$ and will be chosen by appropriately setting *select-list* in COMPUTE-RHO-COVERING, COMPUTE-I-COVERING.

COMPUTE-COVERING The relation R, represented by *rels* and obtained by the abovely described method will be closed reflexive, symmetric and transitive by COMPUTE- COVERING in the lines 2 and 3, that is the minimal equivalence relation R^* will be determined, which is given by the list *elem-followers* (in the way explained at the end of the listing of TRANSITIVE-CLOSURE).

The lines 5 to 7 in COMPUTE-COVERING transform these equivalence relation R^* into a set *equiv* of sets of elements $\mathbb{C} \cup \{\infty\}$, each consisting of elements equivalent under R^*.

In line 8 a list called *val-images* is computed which is of the form $[[w_1, 1], \ldots, [w_n, n]]$, where n is the length of *reslist* and $w_j = reslist[j][1] \cdot val \in \mathbb{C} \cup \{\infty\}$.

Among the elements of *val-images* for every equivalence class *equiv-class* from *equiv* those $[[w_{j_1}, j_1], \ldots, [w_{j_e}, j_e]]$ are picked out, for which $w_{j_\nu} \in$ *equiv-class* holds (line 12).

As the relation R^*, from which *equiv-class* was constructed, represents exactly the gluing–data underlying $\overline{\mathcal{F}}_\Gamma$, applied to the *val* from ρ, i, ∞ which has been considered, it follows from the introductory remarks on the principle of operation used by COMPUTE-COVERING that the length e of the list *point* is really the ramification index of the point of $\overline{\mathcal{F}}_\Gamma$ lying over *val* and represented by an arbitrary w_{j_ν} with $[w_{j_\nu}, j_\nu] \in$ *point*

The list *ergl* finally is a list of all points over *val*, its length equals $|\psi^{-1}(val)|$.

COMPUTE-RELS$(val, select\text{-}list, reslist)$

▷ It is $val \in \mathbb{C} \cup \{\infty\}$
▷ It is *select-list* a list with values from $\{1,2,3\}$
▷ It is *reslist* the result of FUNDAMENTAL-DOMAIN(Γ)

```
1  rels ← {}
2  for res-el through reslist
3       do
4            w ← MÖBIUS(res-el[1], val)
5            rel-0 ← (w, w)
6            rels ← append(rels, rel-0)
7            ilist ← res-el[2]
8            i_1 ← ilist[1]
9            if i_1 > 0 and 1 ∈ select-list
10             then
11                  rel-1 ← (MÖBIUS((res-el[1]) · T, val), MÖBIUS(reslist[i_1][1], val))
12                  rels ← append(rels, rel-1)
13           i_2 ← ilist[2]
14           if i_2 > 0 and 2 ∈ select-list
15             then
16                  rel-2 ← (MÖBIUS(res-el[1], val), MÖBIUS((reslist[i_2][1]) · T, val))
17                  rels ← append(rels, rel-2)
18           i_3 ← ilist[3]
19           if i_3 > 0 and 3 ∈ select-list
20             then
21                  rel-3a ← (MÖBIUS((res-el[1]) · S, val), MÖBIUS(reslist[i_3][1], val))
22                  rel-3b ← (MÖBIUS(res-el[1], val), MÖBIUS((reslist[i_3][1]) · S, val))
23                  rels ← append(rels, rel-3a)
24                  rels ← append(rels, rel-3b)
25 return rels
```

COMPUTE-IMAGES$(val, reslist)$

▷ It is $val \in \mathbb{C} \cup \{\infty\}$
▷ It is *reslist* the result of FUNDAMENTAL-DOMAIN$(\overline{\Gamma})$

```
1  erg-list ← []
2  cnt ← 0
3  for res-el through res-list
4       do
5            cnt ← cnt + 1
6            M ← res-el[1]
7            w ← MÖBIUS(M, val)
8            erg-list ← append(erg-list, [w, cnt])
9  return erg-list
```

TRANSITIVE-CLOSURE(R)

▷ R is a relation, given by a set of pairs (r_1, r_2).
1 *elems* $\leftarrow \bigcup_{(r_1,r_2)\in R}\{r_1, r_2\}$
2 **for** $e \in$ *elems*
3 **do** *elem-followers*$[e] \leftarrow \emptyset$
4 **for** $(r_1, r_2) \in R$
5 **do**
6 *elem-followers*$[r_1] \leftarrow$ *elem-followers*$[r_1] \cup$ *elem-followers*$[r_2] \cup \{r_2\}$
7 **for** $e \in$ *elems*
8 **do**
9 **if** $r_1 \in$ *elem-followers*$[e]$
10 **then** *elem-followers*$[e] \leftarrow$ *elem-followers*$[e] \cup$ *elem-followers*$[r_1]$
11 **return** *elem-followers*

▷ The list *elem-followers* encodes the transitive closure
▷ R^* of R as $R^* = \{(r_1, r_2) | r_1 \in elems, r_2 \in$ *elem-followers*$[r_1]\}$.

MÖBIUS($\mathbf{M}, val$)

▷ The canonical operation of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{C}\cup\{\infty\}$, also called Möbius–transformation
▷ $\mathbf{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$
▷ $val \in \mathbb{C}\cup\{\infty\}$
1 **return** $\frac{(a\ val+b)}{(c\ val+d)}$

2.3 An example: The covering of $X_{\mathbf{ns}}^{+}(7)(\mathbb{C})$ over $\mathbf{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$

As described in section 1, it is $X_{\mathrm{ns}}^{+}(7)(\mathbb{C}) \cong X(7)^{\bar{H}_7^0}(\mathbb{C})$ and $X(7)^{\bar{H}_7^0}(\mathbb{C}) \cong H_7\backslash\mathfrak{H}^*$ with

$$\bar{H}_p^0 = \left\{ \begin{pmatrix} a & bl \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \right\} \cup \left\{ \begin{pmatrix} a & bl \\ -b & -a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \right\} \tag{9}$$

$$\bar{H}_p = \bar{H}_p^0 \cap \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \tag{10}$$

$l \in \mathbb{Z}/p\mathbb{Z}$, $\quad l$ quadratic non–residue

and the preimage H_7 of $\bar{H}_7$ under $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$.

If one calls D_7 the preimage under $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z})$ of the group denoted $7D^0$ in [9], and designates by $\bar{D}_7$ the image of D_7 under $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ one can check by direct computation that

$$\bar{H}_7 = \bar{\mathbf{P}}\,\bar{D}_7\,\bar{\mathbf{P}}^{-1} \tag{11}$$

for $\mathbf{P} = \left(\begin{smallmatrix} 7 & 3 \\ 9 & 4 \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and $\bar{\mathbf{P}}$ its image in $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ so that furthermore $i : \mathbf{M} \mapsto \mathbf{P}\mathbf{M}\mathbf{P}^{-1}$ due to

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma(7) & \longrightarrow & D_7 & \longrightarrow & \bar{D}_7 & \longrightarrow & 1 \\ & & \downarrow \cong & & \downarrow i & & \downarrow \cong & & \\ 1 & \longrightarrow & \Gamma(7) & \longrightarrow & H_7 & \longrightarrow & \bar{H}_7 & \longrightarrow & 1 \end{array}$$

induces an isomorphism $D_7 \xrightarrow{\sim} H_7$.

As a consequence the horizontal arrow in

$$\begin{array}{ccc} H_7\backslash\mathfrak{H}^* & \longrightarrow & D_7\backslash\mathfrak{H}^* \\ & \searrow \quad \swarrow & \\ & \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^* & \end{array} \qquad z \mapsto \mathbf{P}^{-1}z \tag{12}$$

is an isomorphism over $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$.

In particular, the ramification behaviour of $H_7\backslash\mathfrak{H}^*$ is the same as that of $D_7\backslash\mathfrak{H}^*$, which we will now study.

For that we use, as we will need it later on, the information from [9] that there exists a chain of subgroups

$$D_7 \subset 7A^0 \subset \mathrm{SL}_2(\mathbb{Z}) \tag{13}$$

where the image of D_7 in $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ is generated by the matrices

$$\begin{bmatrix} 0 & 3 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 4 & 6 \end{bmatrix}\begin{bmatrix} 2 & 5 \\ 6 & 5 \end{bmatrix}\begin{bmatrix} 6 & 0 \\ 0 & 6 \end{bmatrix} \tag{14}$$

from $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ and the image of $7A^0$ in $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ is generated by the matrices above and the two additional matrices

$$\begin{bmatrix} 4 & 0 \\ 6 & 2 \end{bmatrix}\begin{bmatrix} 6 & 6 \\ 2 & 1 \end{bmatrix} \tag{15}$$

It then holds that

$$[\mathrm{SL}_2(\mathbb{Z}) : 7A^0] = 7 \tag{16}$$
$$[\mathrm{SL}_2(\mathbb{Z}) : D_7] = 21 \tag{17}$$

Therefore we can factorize the covering $D_7\backslash\mathfrak{H}^* \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$ as

$$D_7\backslash\mathfrak{H}^* \xrightarrow{\phi} 7A^0\backslash\mathfrak{H}^* \xrightarrow{\psi} \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^* \tag{18}$$

where ϕ is of degree 3 and ψ of degree 7.

A fundamental domain for $D_7\backslash\mathfrak{H}^*$ is described by the list *reslist*:

$$\begin{array}{lll}
[[\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, [-2,-3,-4]], & [\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, [-5,-1,-6]], & [\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, [-1,-7,-8]], \\
[\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, [-9,-10,1]], & [\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, [-11,-2,-12]], & [\begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}, [-13,-14,2]], \\
[\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}, [-3,-15,7]], & [\begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}, [-16,9,3]], & [\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, [8,-4,9]], \\
[\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, [-4,-17,13]], & [\begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}, [15,-5,17]], & [\begin{bmatrix} 2 & -1 \\ 1 & 0 \end{bmatrix}, [-18,13,5]], \\
[\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, [12,-6,-10]], & [\begin{bmatrix} 1 & -2 \\ 1 & -1 \end{bmatrix}, [-6,-19,18]], & [\begin{bmatrix} 1 & -3 \\ 0 & 1 \end{bmatrix}, [-7,11,16]], \\
[\begin{bmatrix} -1 & -2 \\ 1 & 1 \end{bmatrix}, [-20,-8,15]], & [\begin{bmatrix} 0 & -1 \\ 1 & -2 \end{bmatrix}, [-10,20,11]], & [\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, [-21,-12,-14]], \\
[\begin{bmatrix} 1 & -3 \\ 1 & -2 \end{bmatrix}, [-14,21,19]], & [\begin{bmatrix} -1 & -3 \\ 1 & 2 \end{bmatrix}, [17,-16,20]], & [\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}, [19,-18,21]]]
\end{array} \tag{19}$$

as the result of FUNDAMENTAL-DOMAIN(D_7).

With FUNDAMENTAL-DOMAIN2($reslist, 7A^0$) one computes a fundamental domain $7A^0\backslash\mathfrak{H}^*$ in the form of $reslist_1$.

$$\begin{array}{lll}
[[\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, [-2,-3,-4]], & [\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, [-5,-1,2]], & [\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}, [-1,-6,3]], \\
[\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, [6,-7,1]], & [\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, [7,-2,7]], & [\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}, [-3,4,6]], \\
[\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, [-4,5,5]]] & &
\end{array} \tag{20}$$

As a second result one gets the mapping under the covering map ϕ of the triangles of *reslist* to those of $reslist_1$ according to the following table

From	To	From	To	From	To
1	1	8	3	15	4
2	2	9	6	16	1
3	3	10	7	17	5
4	4	11	7	18	4
5	5	12	7	19	3
6	2	13	5	20	2
7	6	14	1	21	6

(21)

The ramification behaviour of ψ and $\psi \circ \phi$ over ρ, i, ∞, as well as that of ϕ, can be summarized in the following diagrams:

Figure 1: Ramification over ρ

$$\begin{array}{ccccc} & [[15,17,20]] & & [[14,19,21]] & & [[1,8,9]] \\ [[2,4,13]] & & [2,4,5] & & [1,3,6] & & [7] \\ & [[5,6,18]] & & [[3,7,16]] & & [[10,11,12]] \end{array} \tag{22}$$

Figure 2: Ramification over i

$$\begin{array}{cccccc} [[10,13]] & [[11,17]] & [[14,18]] & [[15,16]] & & [[7]] \\ [5,7] & [1,4] & [2] & [3] & [6] & [[9]] \\ & & & & & [[21]] \\ [[5,12]] & [[1,4]] & [[20]] & [[2,6]] & [[19]] & [[3,8]] \end{array} \tag{23}$$

Figure 3: Ramification over ∞

$$\begin{array}{ccc} [[1,2,3,5,7,11,15]] & [[6,12,13,14,18,19,21]] & [[4,8,9,10,16,17,20]] \\ & [1,2,3,4,5,6,7] & \end{array} \tag{24}$$

Therein $[j_1,\ldots,j_e]$ denotes a point of $7A^0\backslash\mathfrak{H}^*$ that is ramified of index e over its image in $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$, with $[j_1,\ldots,j_e]$ representing as a short form the result–form $[[w_{j_1},j_1],\ldots,[w_{j_e},j_e]]$ described in the explanation of COMPUTE-COVERING.

Analogously $[[j_1,\ldots,j_e]]$ denotes a point of $D_7\backslash\mathfrak{H}^*$ which is e times ramified over $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$. The arrows describe the mapping ϕ.

3 Determination of an uniformizer of $X^+_{\mathbf{ns}}(7)/\mathbb{Z}[1/7]$

3.1 Preliminary considerations

In the following subsection let $A=\mathbb{Z}[\frac{1}{7}]$, let X_S be $X\times_{\mathrm{spec}(R)}\mathrm{spec}(S)$ for commutative rings $R\to S$ and a scheme X/R and let furthermore f_S be $f\times_{\mathrm{id}_{\mathrm{spec}(R)}}\mathrm{id}_{\mathrm{spec}(S)}$ for $f:X\to Y$ and schemes X/R and Y/R.

We know from [5] and section 1 that

i) there exists an isomorphism $X^+_{\mathrm{ns}}(7)\cong\mathbb{P}^1_A$.

ii) there exists a morphism $\pi: X^+_{\mathrm{ns}}(7)\to X(1)$ over A that corresponds in the modular interpretation over algebraically closed fields to forgetting the 7–structure.

iii) there exists a morphism $j: X(1)\to\mathbb{P}^1_A$ over A for which $j_{\mathbb{C}}: X(1)_{\mathbb{C}}\to\mathbb{P}^1_{\mathbb{C}}$ agrees with $j_{\mathrm{ell}}:\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*\to\mathbb{P}^1_{\mathbb{C}}$. Therein j_{ell} is the usual meromorphic j–function from the theory of elliptic functions and the isomorphism $X(1)_{\mathbb{C}}\cong\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$ is given by the modular interpretation of both sides.

If now a commutative diagram

$$\begin{array}{ccc} X^+_{\mathrm{ns}}(7) & \xrightarrow{\eta} & \mathbb{P}^1_A \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle p} \\ X(1) & \xrightarrow{j} & \mathbb{P}^1_A \end{array} \tag{25}$$

of morphisms over $\mathrm{spec}(A)$ exists, in which the horizontal morphisms are isomorphisms, we will call η a *uniformizer* of $X^+_{\mathrm{ns}}(7)$ over A.

If one performs a base extension $\mathrm{spec}(\mathbb{C})\to\mathrm{spec}(A)$ in (25) and calls $\pi_{\mathbb{C}}$, $\eta_{\mathbb{C}}$, $j_{\mathbb{C}}$, $p_{\mathbb{C}}$ the extensions of π, η, j, p, the diagram

$$\begin{array}{ccccc} X^+_{\mathrm{ns}}(7)_{\mathbb{C}}(\mathbb{C}) & & \xrightarrow{\text{mod.}} & & H_7\backslash\mathfrak{H}^* \\ & \searrow^{\eta_{\mathbb{C}}} & & \swarrow_{\tilde\eta} & \\ \downarrow{\scriptstyle\pi_{\mathbb{C}}} & & \mathbb{P}^1_{\mathbb{C}}(\mathbb{C}) & & \downarrow{\scriptstyle\text{can.}} \\ & & \downarrow{\scriptstyle p_{\mathbb{C}}} & & \\ X(1)_{\mathbb{C}}(\mathbb{C}) & & \xrightarrow{\text{mod.}} & & \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^* \\ & \searrow_{j_{\mathbb{C}}} & & \swarrow^{j_{\mathrm{ell}}} & \\ & & \mathbb{P}^1_{\mathbb{C}}(\mathbb{C}) & & \end{array} \tag{26}$$

results.

The horizontal morphisms in it are isomorphisms and arise through the modular interpretation of both sides as coarse moduli schemes of elliptic curves over $\mathbb{C}$ with suitable 7–structures ($X^+_{\mathrm{ns}}(7)_{\mathbb{C}}$) resp. without such structures ($X(1)_{\mathbb{C}}$).

We will now take an isomorphism $\tilde\eta$ in (26) as given and determine $\eta_{\mathbb{C}}$ by $\tilde\eta$ so that it will remain to prove, that $\eta_{\mathbb{C}}$ really arises from a diagram of the form of (25).

The morphism $\tilde\eta$ we will determine in the next subsection in the way that

$$j_{\mathrm{ell}}=\frac{P(\tilde\eta)}{Q(\tilde\eta)}=\frac{(2\tilde\eta+3)^3(5\tilde\eta^2+8\tilde\eta-1)^3(2\tilde\eta^2-\tilde\eta+1)^3(\tilde\eta^2+3\tilde\eta+4)^3}{(\tilde\eta^3+\tilde\eta^2-2\tilde\eta-1)^7} \tag{27}$$

is fulfilled with $P,Q\in\mathbb{Z}[T]$ therefore being polynomials of degree $d=21$.

The relation (27) gives rise to a finite morphism

$$p : \mathbb{P}^1_A(E_0, E_1) \to \mathbb{P}^1_A(J_0, J_1) \tag{28}$$

where $E_0, E_1 \in \mathcal{O}_{\mathbb{P}^1_A}(1)(\mathbb{P}^1_A)$ and $J_0, J_1 \in \mathcal{O}_{\mathbb{P}^1_A}(1)(\mathbb{P}^1_A)$ are the canonical sections and $p^*(J_0) = Q(E_1/E_0)E_0^{21}$ as well as $p^*(J_1) = P(E_1/E_0)E_0^{21}$.

The morphism $p_{\mathbb{C}}$ in (26) is the base extension of this morphism.

The left square in (26) yields a diagram

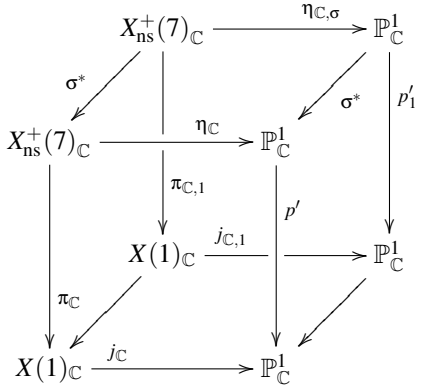
$$\begin{array}{ccc} X^+_{\mathrm{ns}}(7)_{\mathbb{C}} & \xrightarrow{\eta_{\mathbb{C}}} & \mathbb{P}^1_{\mathbb{C}} \\ \downarrow{\scriptstyle \pi_{\mathbb{C}}} & & \downarrow{\scriptstyle p_{\mathbb{C}}} \\ X(1)_{\mathbb{C}} & \xrightarrow{j_{\mathbb{C}}} & \mathbb{P}^1_{\mathbb{C}} \end{array} \tag{29}$$

But there is even a $\eta_{\mathbb{Q}}$ for which

$$\begin{array}{ccc} X^+_{\mathrm{ns}}(7)_{\mathbb{Q}} & \xrightarrow{\eta_{\mathbb{Q}}} & \mathbb{P}^1_{\mathbb{Q}} \\ \downarrow{\scriptstyle \pi_{\mathbb{Q}}} & & \downarrow{\scriptstyle p_{\mathbb{Q}}} \\ X(1)_{\mathbb{Q}} & \xrightarrow{j_{\mathbb{Q}}} & \mathbb{P}^1_{\mathbb{Q}} \end{array} \tag{30}$$

commutes, and for which $\eta_{\mathbb{C}} = \eta_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C}$ holds.

To see this, we consider the diagram



(31)

that originates from (29) through a base extension $\mathrm{spec}(\mathbb{C}) \to \mathrm{spec}(\mathbb{C})$, coming from an automorphism $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$.

In it $j_{\mathbb{C},1}$, p'_1, $\pi_{\mathbb{C},1}$ are respectively equal to $j_{\mathbb{C}}$, $p' = p_{\mathbb{C}}$, $\pi_{\mathbb{C}}$ as these morphisms are already defined over $\mathbb{Q}$.

If we could now prove that $\gamma_\sigma = \sigma^* \circ \eta_{\mathbb{C}} \circ {\sigma^*}^{-1} \circ {\eta_{\mathbb{C}}}^{-1}$ as an automorphism of (the upper, right, frontal) $\mathbb{P}^1_{\mathbb{C}}$ equals $\mathrm{id}_{\mathbb{P}^1_{\mathbb{C}}}$ for all σ, it would follow from general theory of descent, that $\eta_{\mathbb{C}}$ really stems from a $\eta_{\mathbb{Q}}$, that makes (30) commute.

Now γ_σ definitely is of the form

$$E \mapsto \frac{aE+b}{cE+d} \quad \text{with} \quad a,b,c,d \in \mathbb{C}, \quad ad-bc \neq 0 \tag{32}$$

where we call $E = E_1/E_0$ the affine coordinate in $\mathbb{P}^1_{\mathbb{C}}$.

Because of the commutation relations in (31) the morphism γ_σ is an automorphism of every fiber ${p_{\mathbb{C}}}^{-1}(j)$, especially of the fibers over $j = 0$ and $j = \infty$ (j being regarded as the affine coordinate in the frontal, lower, right $\mathbb{P}^1_{\mathbb{C}}$). But these fibers are, expressed

with E as affine coordinate nothing else but $P(E) = 0$ and $Q(E) = 0$. The corresponding splitting fields of $P(E)$ and $Q(E)$ are $L_1 = \mathbb{Q}(\sqrt{7})\,\mathbb{Q}(\sqrt{3})$ and $L_2 = \mathbb{Q}(\zeta)$ with $R(\zeta) = 0$ and $R(E)^7 = Q(E)$. Both fibers contain at least three points and therefore suffice to determine the projective automorphism γ_σ. Computing the values a, b, c, d from the mappings in the fibers, one can conclude that they have to lie in L_1 as well as in L_2 and hence in $\mathbb{Q}$ as $L_1 \cap L_2 = \mathbb{Q}$.

Since inside the fibers over $j = j(1)$, $j = j(2)$, $j = j(3)$ the rational points $E = 1$, $E = 2$, $E = 3$ are the only rational points, and are therefore mapped onto themselves under γ_σ it is $\gamma_\sigma = \mathrm{id}_{\mathbb{P}^1_{\mathbb{C}}}$ as requested.

After having now descended to the definition ring $\mathbb{Q}$, we can even find a morphism η that makes the diagram (25) commute and for which $\eta_{\mathbb{Q}} = \eta \otimes_A \mathbb{Q}$ holds.

For this we make use of the following

Proposition 3.1 *Let X, Y be schemes over a principal ideal domain R and $K = Q(R)$ the quotient field. There shall be isomorphisms $X \cong Y \cong \mathbb{P}^1_R$. Additionally a morphism $f' : X_K \to Y_K$ shall be given.*

Then $f' = f_K$ for a uniquely determined morphism $f : X \to Y$ over $spec(R)$.

Proof. At first f' can be extended to a morphism

$$f'' : X_{D(r)} \to Y_{D(r)} \to Y, \quad r \in R, \quad \text{suitably chosen}$$

This follows from [6, Théorème (8.8.2)], if one puts $S_0 = S_\alpha = \mathrm{spec}(R)$, $X_\alpha = X$, $Y_\alpha = Y$ and chooses as projective system S_λ the system given by the open subsets $D(r)$ of $\mathrm{spec}(R)$.

As X and Y are normal and smooth schemes, the rational map f'' can be extended to a maximal domain of definition $U \subset X$, for which $\mathrm{codim}_X(X - U) = 2$. So $X - U$ only consists of finitely many closed points in closed fibers of X over R.

We now have a diagram

$$\begin{array}{ccccccc} \Gamma_{f''} & \longrightarrow & \bar{\Gamma}_{f''} & \hookrightarrow & X \times_R Y & & \\ & \swarrow^{p_1''} \quad \swarrow^{p_1'} & & \swarrow^{p_1} & & \searrow^{p_2} & \\ U & \hookrightarrow & X & = & X & & Y \\ & & & & \searrow & \swarrow & \\ & & & & \mathrm{spec}(R) & & \end{array} \tag{33}$$

where $\Gamma_{f''}$ denotes the graph of f'' and $\bar{\Gamma}_{f''}$ its scheme–theoretic closure in $X \times_R Y$.

In this diagram p_1 and therefore p_1' is proper. As p_1' is quasi–finite it is, using Zariskis Main Theorem, even finite. Additionally p_1'' is an isomorphism and consequently p_1' is a birational morphism, so that for the function fields $K(\bar{\Gamma}_{f''}) = K(X)$ holds.

Locally on ring level p_1' is therefore described by diagrams

$$\begin{array}{ccc} C' & \longrightarrow & K(\bar{\Gamma}_{f''}) \\ \uparrow & & \| \\ C & \longrightarrow & K(X) \end{array} \tag{34}$$

where C' is integral over C. As X is normal, C is integrally closed in $K(X)$, and so $C = C'$ follows. But this means, that p_1' is an isomorphism and therefore determines a morphism $f = p_2 \circ (p_1')^{-1}$. This f is the sought for morphism of the proposition.

Its uniqueness follows from the construction and the fact that a morphism from a reduced into a separated scheme is determined by its restriction to any open dense subscheme. □

As the base extension $\mathrm{spec}(\mathbb{Q}) \to \mathrm{spec}(A)$ of (25) equals (30), the map η can be obtained as the extension of $\eta_{\mathbb{Q}}$ over the whole of $\mathrm{spec}(A) = \mathrm{spec}(\mathbb{Z}[\frac{1}{7}])$ which exists and is uniquely determined by proposition 3.1.

The commutativity of (25) then follows from those of (30) and the uniqueness assertion in proposition 3.1. That the schemes considered fulfill the assumptions of proposition 3.1 follows from Proposition 1.5 for $X_{\mathrm{ns}}^{+}(7)$ from Proposition 1.4 for $X(1)$ and trivially for $\mathbb{P}^1_A$.

3.2 The uniformization over $\mathbb{C}$

As remarked in the previous subsection, the problem remains to be solved, to explicitly uniformize the covering $H_7\backslash\mathfrak{H}^* \to \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$ that is, to find an η for which

$$\begin{array}{ccc} H_7\backslash\mathfrak{H}^* & \xrightarrow{\eta} & \mathbb{P}^1_{\mathbb{C}} \\ \downarrow & & \downarrow p \\ \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^* & \xrightarrow{j_{\mathrm{ell}}} & \mathbb{P}^1_{\mathbb{C}} \end{array} \tag{35}$$

commutes and p is explicitly known (we write η in this subsection instead of $\tilde{\eta}$ in the previous one).

In [4] a general procedure to solve this problem is given that can be formulated in abstract terms as follows:

Proposition 3.2 *Let $X \xrightarrow{\pi} Y$ be a covering of Riemann surfaces of genus 0 with explicitly known ramification behaviour. Additionally for an isomorphism $Y \xrightarrow{f} \mathbb{P}^1_{\mathbb{C}}$ the values $f(R_i)$ shall be known for all $R_i \in Y$ above which π ramifies ($i = 1,\ldots,s$). Furthermore, let R_0 and R_∞ be the points from Y with $f(R_0) = 0$ and $f(R_\infty) = \infty$.*

Then one can explicitly construct a morphism $p : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ for which an isomorphism $g : X \to \mathbb{P}^1_{\mathbb{C}}$ exists, so that

$$\begin{array}{ccc} X & \xrightarrow{g} & \mathbb{P}^1_{\mathbb{C}} \\ \pi\downarrow & & \downarrow p \\ Y & \xrightarrow{f} & \mathbb{P}^1_{\mathbb{C}} \end{array} \tag{36}$$

commutes.

Proof. Let $P_1,\ldots,P_d \in X$ be the points above R_0 and $Q_1,\ldots,Q_d \in X$ the points above R_∞, where d is the degree of the covering $X \xrightarrow{\pi} Y$ and multiply occurring P_i or Q_i are allowed according to possible ramification of π.

Then

$$f = \lambda \frac{(g-g(P_1))\cdot\cdots\cdot(g-g(P_d))}{(g-g(Q_1))\cdot\cdots\cdot(g-g(Q_d))} = \frac{P(g)}{Q(g)}, \quad \lambda \in \mathbb{C} \tag{37}$$

holds, as one can see immediately by comparing divisors left and right.

Therein we identify f from the function field $K(Y)$ with its image $\pi^*(f)$ in $K(X)$ under $\pi^* : K(Y) \to K(X)$. A value $g(P_i) = \infty$ or $g(Q_i) = \infty$ leads to the omission of the corresponding factor.

To obtain now relations for actually determining the λ, $g(P_i)$, $g(Q_i)$, we draw on the $R_i \neq R_0, R_\infty \in Y$, above which π ramifies in a known way.

Let R be such an R_i, and let $S_1,\ldots,S_d$ be the points above it, with repetitions because of the ramification.

Then

$$(f-f(R))(R) = 0 \qquad\qquad (f-f(R))(R_\infty) = \infty \tag{38}$$

holds and therefore by comparison of divisors

$$f - f(R) = \mu \frac{(g - g(S_1)) \cdot \cdots \cdot (g - g(S_d))}{(g - g(Q_1)) \cdot \cdots \cdot (g - g(Q_d))} = \frac{T_R(g)}{Q(g)}, \quad \mu \in \mathbb{C} \tag{39}$$

Using (37) one gets from that

$$\lambda P(g) - f(R)\, Q(g) = \mu (g - g(S_1)) \cdot \cdots \cdot (g - g(S_d)) = T_R(g) \tag{40}$$

By comparing coefficients of corresponding powers of g in (40) a set Σ_R of $d+1$ polynomial relations between λ, μ, $g(P_i)$, $g(Q_i)$, $g(S_i)$ results. With every new $R = R_i$ the number of unknowns grows, but also the number of relations until finally only $R \in Y$ are available for forming relations over which π does not ramify and for which (40) allows as many degrees of freedom (that is $d+1$) as it provides relations. By solving the simultaneous relations Σ_{R_i} for all $R_i \neq R_0, R_\infty$, one obtains with every solution an expression

$$f = \lambda \frac{P(g)}{Q(g)} \tag{41}$$

with explicitly known λ, P, Q and g, which is uniquely determined by its values at three points. This g is the one requested in (36), the mapping p is explicitly known as $p(g) = \lambda P(g)/Q(g)$. □

To construct η and p in (35), we first recall the remarks from the beginning of subsection 2.3. We have introduced there the inner automorphism $i : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z})$ with $\mathbf{M} \mapsto \mathbf{P}\mathbf{M}\mathbf{P}^{-1}$ and $\mathbf{P} = \left(\begin{smallmatrix} 7 & 3 \\ 9 & 4 \end{smallmatrix}\right)$ that maps the subgroup D_7 isomorphically onto H_7. Defining the image $7\tilde{A}^0 \stackrel{\text{def}}{=} i(7A^0)$ it holds that

$$H_7 \subset 7\tilde{A}^0 \subset \mathrm{SL}_2(\mathbb{Z}) \tag{42}$$

Accordingly, the chain of coverings (18) becomes, under the isomorphisms of quotients of $\mathfrak{H}^*$ induced by i, a chain of coverings

$$H_7 \backslash \mathfrak{H}^* \xrightarrow{\phi} 7\tilde{A}^0 \backslash \mathfrak{H}^* \xrightarrow{\psi} \mathrm{SL}_2(\mathbb{Z}) \backslash \mathfrak{H}^* \tag{43}$$

where we gave the new covering maps the old names ϕ and ψ. Obviously the structure of ramification in (43) is the same as in (18), so we can, mutatis mutandis, carry over the ramification structure depicted in (22), (23), (24) to the situation in (43).

To keep the computation manageable, we use the chain (43) and construct an uniformizer ξ of $7\tilde{A}^0 \backslash \mathfrak{H}^*$ over j first, and secondly an uniformizer η of $H_7 \backslash \mathfrak{H}^*$ over ξ.

So let, with the notations of proposition 3.2, $X = 7\tilde{A}^0 \backslash \mathfrak{H}^*$ and $Y = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathfrak{H}^*$ as well as $\pi = \psi$. As the function f, we choose $j = j_{\mathrm{ell}}$, the usual j–function on $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathfrak{H}^*$.

Then the points $R_1 = \rho$, $R_2 = i$, $R_3 = \infty$ are the branch points and $R_0 = R_1$ because of $j(\rho) = 0$ as well as $R_\infty = R_3$ because of $j(\infty) = \infty$. The value $j(R_2) = j(i) = 1728$ is known.

For abbreviation we denote the points called $[2,4,5]$ and $[1,3,6]$ in (22) by $\tilde{P}_1 = P_1 = P_2 = P_3$ and $\tilde{P}_2 = P_4 = P_5 = P_6$ respectively. The point called $[7]$ we denote by $\tilde{P}_3 = P_7$ and furthermore the point called $[1,2,3,4,5,6,7]$ in (24) by $Q = Q_1 = \ldots = Q_7$.

The isomorphism g from proposition 3.2 we call ξ and dispose over its values such that $\xi(Q) = \infty$ and $\xi(\tilde{P}_3) = 0$.

The product $(\xi - \xi(\tilde{P}_1))(\xi - \xi(\tilde{P}_2))$ we write as $\xi^2 + A\xi + B$, so that equation (37) becomes

$$j = \lambda (\xi^2 + A\xi + B)^3 \xi \tag{44}$$

Above the point $R_2 = i$ lie, according to figure (23) the points $S_1 = S_2 = [5,7]$, $S_3 = S_4 = [1,4]$, $S_5 = [2]$, $S_6 = [3]$, $S_7 = [6]$ (bracketed lists referring to notation in (23)).

Introducing the equations $(\xi-\xi(S_1))(\xi-\xi(S_3))=\xi^2+C\xi+D$ and $(\xi-\xi(S_5))(\xi-\xi(S_6))=\xi^2+E\xi+F$ as well as $\xi(S_7)=G$, the equation (40) for $R=R_2$ takes the form

$$1728-\lambda(\xi^2+A\xi+B)^3\xi=\mu(\xi^2+C\xi+D)^2(\xi^2+E\xi+F)(\xi-G) \tag{45}$$

Equating coefficients of like powers ξ^k one obtains the system of expressions required to vanish

$$\begin{gathered}
1728+\mu D^2FG,\\
-\lambda B^3-\mu D^2F+(\mu D^2E+2\mu DCF)G,\\
-3\lambda B^2A-\mu D^2E-2\mu DCF+(\mu D^2+2\mu DCE+\mu(2D+C^2)F)G,\\
-\lambda-\mu,\\
-3\lambda A-2\mu C-\mu E+\mu G,\\
-\lambda(3B+3A^2)-\mu(2D+C^2)-2\mu CE-\mu F+(2\mu C+\mu E)G,\\
-\lambda(4BA+A(2B+A^2))-2\mu DC-\mu(2D+C^2)E-2\mu CF\\
+(\mu(2D+C^2)+2\mu CE+\mu F)G,\\
-\lambda(B(2B+A^2)+2A^2B+B^2)-\mu D^2-2\mu DCE-\mu(2D+C^2)F\\
+(2\mu DC+\mu(2D+C^2)E+2\mu CF)G
\end{gathered} \tag{46}$$

A Gröbner base of these polynomials in lexicographical term ordering $E>F>G>C>D>\mu>B>A>\lambda$ is

$$\begin{gathered}
86812553324672+\lambda^2A^{14}+10706059\lambda A^7,\\
161414428B-\lambda A^9-37059435A^2,\\
\lambda+\mu,\\
1129900996D-\lambda A^9-37059435A^2,\\
7C-4A,\\
7909306972G^3+14688712948AG^2+133G\lambda A^9+9287094411GA^2\\
+108\lambda A^{10}+2134623456A^3,\\
1129900996F-1129900996G^2-2098387564AG-19\lambda A^9-1326727773A^2,\\
-13A+7E-7G
\end{gathered} \tag{47}$$

One notices, upon trying to solve the equations from top to bottom, that one degree of freedom remains, which corresponds with the fact, that we have disposed over the values of ξ at two, but not at three places.

So we set arbitrarily $\lambda=1$ and solve (47), from which we obtain for the quantities relevant for determining the relation between j and ξ

$$\lambda=1, \tag{48a}$$

$$B=-\frac{35}{2}+\frac{7}{2}i\sqrt{7}, \tag{48b}$$

$$A=\frac{7}{2}+\frac{7}{2}i\sqrt{7} \tag{48c}$$

Therewith p from proposition 3.2 is determined for the mapping ψ.

The remaining values of the same solution system are

$$\begin{aligned} C &= 2+2i\sqrt{7}, \\ D &= -\frac{5}{2}+\frac{1}{2}i\sqrt{7} \\ E &= 2+4i\sqrt{7}, \\ F &= -27 \\ G &= -\frac{9}{2}-\frac{5}{2}i\sqrt{7}, \\ \mu &= -1, \end{aligned} \tag{49}$$

As we will need the values $t_1 = \xi(S_5)$ and $t_2 = \xi(S_6)$ later on, we determine them from the equation $(\xi - \xi(S_5))(\xi - \xi(S_6)) = \xi^2 + E\,\xi + F$ given above, to be

$$t_1 = -\alpha - 2 - 4i\sqrt{7}, \tag{50a}$$

$$t_2 = \alpha \tag{50b}$$

with α being an arbitrary, fixed root of

$$\alpha^2 + (2+4i\sqrt{7})\,\alpha - 27 = 0 \tag{51}$$

In the second step we set $X = H_7\backslash\mathfrak{H}^*$ and $Y = 7\tilde{A}^0\backslash\mathfrak{H}^*$ as well as $\pi = \phi$. The function f then becomes ξ, the function g we call η, it is the η searched in (35).

To distinguish the newly appearing points below from the former ones, we will mark the new ones with a prime.

It is then $R'_0 = \tilde{P}_3$, $R'_\infty = Q$ and $R'_2 = S_5$, $R'_3 = S_6$ with the point–names from above.

Above R'_0 lies, according to figure (22) the 3–fold point $P' = [[10,11,12]]$, so it is $P'_1 = P'_2 = P'_3 = P'$. Therewith one can put $R'_1 = R'_0$.

Above R'_∞ lie the three cusps Q'_1, Q'_2, Q'_3. We dispose over the values $\eta(Q'_i)$ such, that

$$\left(\eta - \eta(Q'_1)\right)\left(\eta - \eta(Q'_2)\right)\left(\eta - \eta(Q'_3)\right) = \eta^3 + \eta^2 - 2\eta - 1 \tag{52}$$

So the equation for ξ and η corresponding to equation (37) is

$$\xi = \lambda_1 \frac{(\eta - d)^3}{\eta^3 + \eta^2 - 2\eta - 1} \tag{53}$$

with $d = \eta(P')$

The relations flowing from the ramification as explicated in equation (40) are for R'_2 because of $\xi(R'_2) = \xi(S_5) = t_1$ and (23)

$$\lambda_1 (\eta - d)^3 - t_1 (\eta^3 + \eta^2 - 2\eta - 1) = -\mu_{21} (\eta - A_1)^2 (\eta - B_1) \tag{54}$$

and for R'_3 because of $\xi(R'_3) = \xi(S_6) = t_2$ and (23)

$$\lambda_1 (\eta - d)^3 - t_2 (\eta^3 + \eta^2 - 2\eta - 1) = -\mu_{22} (\eta - A_2)^2 (\eta - B_2) \tag{55}$$

Suitably simplified (54) becomes

$$\begin{aligned} &(-\alpha - 4i\sqrt{7} - \lambda_1 - 2 - \mu_{21})\,\eta^3 \\ &+(3\lambda_1 d - 2 - 4i\sqrt{7} - \alpha + 2\mu_{21} A_1 + \mu_{21} B_1)\,\eta^2 \\ &+(-\mu_{21} {A_1}^2 - 2\mu_{21} A_1 B_1 - 3\lambda_1 d^2 + 4 + 8i\sqrt{7} + 2\alpha)\,\eta \\ &+\mu_{21} {A_1}^2 B_1 + 4i\sqrt{7} + \lambda_1 d^3 + \alpha + 2 = 0 \end{aligned} \tag{56}$$

and (55) becomes

$$\begin{aligned}(\alpha-\lambda_1-\mu_{22})\,\eta^3\\ +(\alpha+3\,\lambda_1\,d+2\,\mu_{22}\,A_2+\mu_{22}\,B_2)\,\eta^2\\ +(-\mu_{22}\,{A_2}^2-2\,\mu_{22}\,A_2\,B_2-2\,\alpha-3\,\lambda_1\,d^2)\,\eta\\ +\mu_{22}\,{A_2}^2\,B_2-\alpha+\lambda_1\,d^3=0\end{aligned}\tag{57}$$

Introducing the variables z with $z^2=-7$ and $w=\alpha$ with $w^2+(2+4\,z)\,w-27=0$ the system of expressions obtained from extracting coefficients of η^k in (56) and (57) can be regarded as a system of generators of an ideal $\mathfrak{a}$ in $\mathbb{Q}[\lambda_1,\mu_{21},\mu_{22},A_1,B_1,A_2,B_2,z,d,w]$.

By computing a Gröbner base for $\mathfrak{a}$ with respect to an elimination term–ordering (for what I have used the CAS–system MAGMA), one obtains a base for the ideal $\mathfrak{b}=\mathfrak{a}\cap\mathbb{Q}[\lambda_1,d,z,w]$ as

$${\lambda_1}^3+\frac{89831}{21866}\,{\lambda_1}^2\,z+\frac{2265}{754}\,\lambda_1\,d\,z-\frac{176535}{21866}\,d^2\,z+\frac{22456}{10933}\,{\lambda_1}^2+\frac{3}{13}\,\lambda_1\,d\\ -\frac{285383}{21866}\,d^2+\frac{22}{29}\,\lambda_1\,z-\frac{146605}{21866}\,d\,z-44\,\lambda_1-\frac{833}{841}\,d-\frac{55241}{1682}\,z+\frac{114044}{10933},\tag{58a}$$

$${\lambda_1}^2\,d+\frac{55}{29}\,\lambda_1\,d\,z+\frac{97}{58}\,d^2\,z+\frac{127}{58}\,{\lambda_1}^2+\frac{55}{58}\,\lambda_1\,d-\frac{679}{58}\,d^2\\ +\frac{182}{29}\,\lambda_1\,z+\frac{14}{29}\,d\,z+\frac{91}{29}\,\lambda_1-\frac{875}{58}\,d-\frac{195}{29}\,z-\frac{2219}{58},\tag{58b}$$

$$\lambda_1\,d^2-\frac{1}{10933}\,{\lambda_1}^2\,z-\frac{105}{21866}\,d^2\,z+\frac{1}{21866}\,{\lambda_1}^2\\ +\frac{643}{754}\,\lambda_1\,d-\frac{49}{21866}\,d^2+\frac{761}{10933}\,d\,z-\frac{2}{29}\,\lambda_1+\frac{805}{21866}\,d-\frac{10807}{10933}\,z-\frac{10885}{21866},\tag{58c}$$

$$d^3+\frac{23}{754}\,{\lambda_1}^2\,z-\frac{495}{3016}\,\lambda_1\,d\,z+\frac{1}{8}\,d^2\,z+\frac{161}{754}\,{\lambda_1}^2+\frac{231}{3016}\,\lambda_1\,d-\frac{505}{3016}\,d^2\\ +\frac{135}{232}\,\lambda_1\,z+\frac{1123}{1508}\,d\,z-\frac{63}{232}\,\lambda_1+\frac{1093}{1508}\,d-\frac{3689}{3016}\,z-\frac{6215}{3016},\tag{58d}$$

$$w^3+4\,w^2+108\,z+89\,w-54,\tag{58e}$$

$$z^2+7,\tag{58f}$$

$$z\,w+\frac{1}{4}\,w^2+\frac{1}{2}\,w-\frac{27}{4}\tag{58g}$$

With the CAS–system MAPLE one possible solution of this system can be found to be

$$d=-\frac{3}{2}+\frac{1}{2}\,i\sqrt{7},\tag{59a}$$

$$\lambda_1=-1,\tag{59b}$$

$$w=-1-2\,i\sqrt{7}+2\,\sqrt{i\sqrt{7}},\tag{59c}$$

$$z=i\sqrt{7}\tag{59d}$$

Since the ideal $\mathfrak{b}$ is zero–dimensional, there is really a solution of $\mathfrak{a}$ above (59).

If one substitutes the λ_1 and d found thus into (53) and further substitutes the ξ so obtained together with the values from (48a)-(48c) into (44) the final result is

$$j=\frac{(2\,\eta+3)^3\,(5\,\eta^2+8\,\eta-1)^3\,(2\,\eta^2-\eta+1)^3\,(\eta^2+3\,\eta+4)^3}{(\eta^3+\eta^2-2\,\eta-1)^7}\tag{60}$$

So η from (35) is determined, p is given explicitly by (60).

3.3 Summary

In the diagram

$$\begin{array}{ccc} X_{\mathrm{ns}}^{+}(7) & \xrightarrow{\eta} & \mathbb{P}^1_{\mathbb{Z}[1/7]} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle p} \\ X(1) & \xrightarrow{j} & \mathbb{P}^1_{\mathbb{Z}[1/7]} \end{array} \tag{61}$$

we have constructed an isomorphism η in such a way, that, calling $E = E_1/E_0$ the affine coordinate of the "upper" $\mathbb{P}^1$ and $J = J_1/J_0$ the affine coordinate of the "lower" $\mathbb{P}^1$, the map p is given by

$$J = \frac{(2E+3)^3\,(5E^2+8E-1)^3\,(2E^2-E+1)^3\,(E^2+3E+4)^3}{(E^3+E^2-2E-1)^7} \tag{62}$$

So the questions 1 and 2 of [5, 6.4.4] are answered in the affirmative, the denominator polynomial called $Q_?(T_0,T_1)$ there corresponds to the (E^3+E^2-2E-1) appearing in (62).

As described in [5, 6.4] we have the isomorphism $\eta : Y_{\mathrm{ns}}^{+}(7) \xrightarrow{\sim} p^{-1}(D_+(J_0)) = D_+(E_1^3 + E_1^2E_0 - 2E_1E_0^2 - E_0^3)$ with E_0, E_1 as the projective coordinates of $\mathbb{P}^1_{\mathbb{Z}[1/7]}$.

4 Determination of $Y_{\mathbf{ns}}^{+}(7)(\mathbb{Z}[1/7])$

By virtue of the results of the last section it is

$$Y_{\mathrm{ns}}^{+}(7) \cong \mathrm{D}_+\left(Q_0(E_0,E_1)\right) \subset \mathbb{P}^1_{\mathbb{Z}[1/7]}(E_0,E_1) \tag{63}$$

$$\text{with} \qquad Q_0(E_0,E_1) = E_1^3 + E_1^2E_0 - 2E_1E_0^2 - E_0^3 \tag{64}$$

As further explicated in [5, 6.4.5] the points $Y_{\mathrm{ns}}^{+}(7)(\mathbb{Z}[1/7])$ correspond to the integer solutions of the diophantine equations $Q_0(E_0,E_1) \in \{1,7\}$, which are both of Thue–type.

For equations of this type effective and practically feasible solution algorithms exist ([1]), which are implemented for example in the CA–system MAGMA([2]).

A computation yields as complete solution system of $Q_0(E_0,E_1) = 1$

(E_1,E_0)	j
$(-9,5)$	$-2^{18}3^3 5^3 23^3 29^3$
$(-1,-1)$	$-2^{18}3^3 5^3$
$(-1,1)$	-2^{15}
$(-1,2)$	$-2^{15}3^3 5^3 11^3$
$(0,-1)$	$2^6 3^3$
$(1,0)$	$2^6 5^3$
$(2,-1)$	$2^3 3^3 11^3$
$(4,-9)$	$2^9 17^6 19^3 29^3 149^3$
$(5,4)$	$2^6 11^3 23^3 149^3 269^3$

(65)

and of $Q_0(E_0,E_1) = 7$

(E_1,E_0)	j
$(-3,2)$	0
$(1,-3)$	$2^{15}7^5$
$(2,1)$	$2^3 5^3 7^5$

(66)

5 Application to the class number $h = 1$ problem

The following table contains imaginary quadratic number fields $K = \mathbb{Q}(\sqrt{-d})$ together with orders $\mathcal{O}_{K,f} \subset K$ with conductor f, such that the class number h of $\mathcal{O}_{K,f}$ equals 1. The class number is in every special case explicitly computable, suitable algorithms are implemented for example in the CA–system MAGMA.

In the last column the j–invariant of the elliptic curve $E_{(K,f)}$, which is defined by the lattice $\mathcal{O}_{K,f} \subset \mathbb{C}$, is given. Equating $\mathcal{O}_{K,f} = \mathbb{Z} + \mathbb{Z}\tau$ this is the value $j(\tau)$ of the classical j–function.

The value $j(\tau)$ here has to be always in $\mathbb{Z}$, as, firstly, the galois group $\mathrm{Gal}(K(j(\tau))/K)$ equals the Picard group of $\mathcal{O}_{K,f}$. As these is trivial, it follows $K(j(\tau)) = K$. Secondly it is $[\mathbb{Q}(j(\tau)) : \mathbb{Q}] = [K(j(\tau)) : K]$ and thirdly $j(\tau)$ is an algebraic integer, so consequently $j(\tau) \in \mathbb{Z}$. For proofs of these facts, see [10, Theorem 4.14; Theorem 5.7]

Therefore we can compute $j(\tau)$ in every single case numerically with sufficient precision, and from that infer its true value in $\mathbb{Z}$.

K	f	$\mathcal{O}_{K,f}$	j
$\mathbb{Q}(\sqrt{-1})$	1	$\mathbb{Z}+\mathbb{Z}\sqrt{-1}$	$2^6 3^3$
$\mathbb{Q}(\sqrt{-1})$	2	$\mathbb{Z}+\mathbb{Z}2\sqrt{-1}$	$2^3 3^3 11^3$
$\mathbb{Q}(\sqrt{-2})$	1	$\mathbb{Z}+\mathbb{Z}\sqrt{-2}$	$2^6 5^3$
$\mathbb{Q}(\sqrt{-3})$	1	$\mathbb{Z}+\mathbb{Z}\frac{-1+\sqrt{-3}}{2}$	0
$\mathbb{Q}(\sqrt{-11})$	1	$\mathbb{Z}+\mathbb{Z}\frac{-1+\sqrt{-11}}{2}$	-2^{15}
$\mathbb{Q}(\sqrt{-43})$	1	$\mathbb{Z}+\mathbb{Z}\frac{-1+\sqrt{-43}}{2}$	$-2^{18} 3^3 5^3$
$\mathbb{Q}(\sqrt{-67})$	1	$\mathbb{Z}+\mathbb{Z}\frac{-1+\sqrt{-67}}{2}$	$-2^{15} 3^3 5^3 11^3$
$\mathbb{Q}(\sqrt{-163})$	1	$\mathbb{Z}+\mathbb{Z}\frac{-1+\sqrt{-163}}{2}$	$-2^{18} 3^3 5^3 23^3 29^3$

(67)

On comparing the j–invariants in (67) with those in (65) and (66), one notices, that 8 of the points in (65) and (66) correspond to elliptic curves with complex multiplication, thereof are 6 with complex multiplication in the principal order $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{-d})$ and $p = 7$ inert in $\mathcal{O}_K$. The cases are $d = 1, 2, 11, 43, 67, 163$, and, following the considerations in section 1, the corresponding points come from an $\bar{H}_7^0$–structure on the elliptic curve $E_{(K,1)}$.

These results agree with those of [8], up to a misprint there, giving the case $d = -67$ the wrong sign for j.

5.1 Criteria for complex multiplication with given j

After all, 4 points from the lists (65) and (66) remain to be examined for their potential origin from elliptic curves with complex multiplication.

For this, we use the following proposition [3, Theorem 6.3]

Proposition 5.1 *Let E/K be an elliptic curve defined over an algebraic number field $K/\mathbb{Q}$.*

With $E[N](\overline{\mathbb{Q}})$ shall be denoted the set of N–division points, and with $k(P)$ the field of definition of a point $P \in E(\overline{\mathbb{Q}})$.

If E has complex multiplication and $L = \mathbb{Q}(\sqrt{-d})$ is the imaginary quadratic field whose order equals End(E)*, the extension of fields*

$$L^{div}K = L\left((k(P))_{P\in E[N](\overline{\mathbb{Q}})}\right) K/LK$$

is abelian for all $N \geqslant 1$.

Corollary 5.1 *Let E be as above, with complex multiplication, but explicitly given by a Weierstraß equation $y^2 = x^3 + ax + b$ in $\mathbb{A}^2_K$. For $P \in E(\overline{\mathbb{Q}})$ let $x(P)$ and $y(P)$ be the x– and y–coordinate of P.*

Then the extension $K\left((x(P))_{P\in E[N](\overline{\mathbb{Q}})-\{\bar{0}\}}\right)/K$ *is solvable.*

Now one can, for an E as in the corollary and for every $N \geqslant 1$, explicitly give a polynomial $\psi_N(x;a,b)$, so that the x_0 with $\psi_N(x_0;a,b) = 0$ are exactly the $x(P)$ with $P \in E[N](\overline{\mathbb{Q}}) \cap \mathbb{A}^2_K(\overline{\mathbb{Q}})$. This polynomial has, for $N \geqslant 3$ and N odd, the degree $(N^2-1)/2$ in x and is called *division polynomial of order N*. Together with the Weierstraß equation itself, it describes the affine part of the subgroup scheme $E[N]$ of N–division points of E.

So we can for the remaining 4 points

(E_1,E_0)	j
$(4,-9)$	$2^9 17^6 19^3 29^3 149^3$
$(5,4)$	$2^6 11^3 23^3 149^3 269^3$
$(1,-3)$	$2^{15} 7^5$
$(2,1)$	$2^3 5^3 7^5$

(68)

construct initially a Weierstraß equation $y^2 = x^3 + ax + b$ over $\mathbb{Q}$, so that the corresponding elliptic curve has the prescribed j–invariant. Subsequently, we compute for a suitably chosen $N \geqslant 3$ the division polynomial $\psi_N(x;a,b)$ and then the Galois group $\mathrm{Gal}(F/\mathbb{Q})$ of the splitting field $F/\mathbb{Q}$ of $\psi_N(x;a,b)$. If this group is not solvable, the elliptic curve with the given j–invariant can not have complex multiplication.

As the intermediate results, especially the division polynomials, become very huge, I do not present them here, but instead give only the MAGMA command sequence to execute the computation:

```
jj:=2^9*17^6*19^3*29^3*149^3;
ec:=EllipticCurveFromjInvariant(jj);
ec1:=MinimalModel(ec);
pol:=DivisionPolynomial(ec1,5);
g:=GaloisGroup(pol);
IsSoluble(g);
```

The j–invariant here is the one of the first point in (68), for the other points only the value jj in the first line has to be changed. In any case the Galois group turns out as not solvable, so to all 4 remaining points belong elliptic curves without complex multiplication, which again agrees with [8]

5.2 The class number $h = 1$ problem

As already explained in the introduction, every imaginary quadratic number field K of class number 1, in which $p = 7$ is inert, gives rise to a point in $Y^+_{\mathrm{ns}}(7)(\mathbb{Z}[1/7])$, to which corresponds an elliptic curve with complex multiplication in K.

We have found 12 points $Y^+_{\mathrm{ns}}(7)(\mathbb{Z}[1/7])$ and discussed their possible origin from those number fields exhaustively. It follows, that additional imaginary quadratic number fields K with class number 1 and p inert in K can not exist, since they would produce points in $Y^+_{\mathrm{ns}}(7)(\mathbb{Z}[1/7])$, that are different from each other and from those already found, because their j–invariant would differ.

So additional imaginary quadratic number fields with $h = 1$ could only exist, if $p = 7$ would not be inert in them. But this can be excluded for $\mathbb{Q}(\sqrt{-d})$ with $d > 163$ by the following lemma:

Lemma 5.1 *Let* $K = \mathbb{Q}(\sqrt{-d})$ *be an imaginary quadratic number field with class number* $h = 1$. *Let* $d > 4p$ *for a prime number p. Then p is inert in K.*

Proof. By making an ansatz $(m + n\tau)(m + n\bar{\tau}) = p$ with $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\tau$ and direct computation. □

Since for $1 \leqslant d \leqslant 163$ all imaginary quadratic number fields with class number 1 are known, therewith all of these are known.

References

[1] Yuri Bilu and Guillaume Hanrot. Solving Thue equations of high degree. *J. Number Theory*, 60(2):373–392, 1996.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I: The user language. *J. Symb. Comput.*, 24(3-4):235–265, 1997.

[3] Denis Xavier Charles. Complex multiplication of elliptic curves. available at `http://www.cs.wisc.edu/~cdx/ComplexMult.pdf`.

[4] Imin Chen. On Siegel's modular curve of level 5 and the class number one problem. *J. Number Theory*, 74(2):278–297, 1999.

[5] Ulrich Everling and Bent Behnke. Eine bestimmte Art von Niveaustrukturen elliptischer Kurven und die Kompaktifizierung der Modulschemata. Diplomarbeit, Rheinische Friedrich-Wilhelms-Universität Bonn, 1986.

[6] A. Grothendieck. Éléments de géométrie algébrique. IV: Étude locale des schemas et des morphismes de schemas. (Troisieme partie). 1966.

[7] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves.* Annals of Mathematics Studies, 108. Princeton, New Jersey: Princeton University Press. XIV, 514 p., 1985.

[8] M. A. Kenku. A note on the integral points of a modular curve of level 7. *Mathematika*, 32:45–48, 1985.

[9] Sebastian Pauli and Chris Cummins. Congruence subgroups of psl(2,z) of genus up to 24. *Experimental Mathematics*, 12, 2003. tabulated results available at `http://www.math.tu-berlin.de/~pauli/congruence/`.

[10] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions. Repr. of the 1971 orig.* Publications of the Mathematical Society of Japan. Kanô Memorial Lectures. 11 (1). Princeton, NJ: Princeton Univ. Press., 1994.

[11] H. A. Verrill. Algorithm for drawing fundamental domains. 2001. available at `http://hverrill.net`.