ON SIEGEL'S MODULAR CURVE OF LEVEL 5 AND THE CLASS NUMBER ONE PROBLEM

IMIN CHEN

Abstract. Another derivation of an explicit parametrisation of Siegel's modular curve of level 5 is obtained with applications to the class number one problem.

1. Introduction

In a not so well-known paper [14], Siegel obtained an explicit parametrisation of the modular curve $X_{\rm ns}^+(5)/\mathbb{Q}$ by constructing a uniformiser out of η-functions (see the end of Section 3 for a brief description of the modular curves $X_{\rm ns}^+(p)/\mathbb{Q}$). In modern terms, he then applied this to solve the class number one problem as follows.

Let $\overline{\mathbb{Q}}$ be the field of algebraic numbers of $\mathbb{C}$. The modular curves $X_{\rm ns}^+(p)/\mathbb{Q}$ classify isomorphism classes of elliptic curves with a certain type of "non-split" level p structure. Now, to every order $\mathcal{O}$ of class number one in an imaginary quadratic field K, there is an associated elliptic curve $E_{\mathcal{O}}/\mathbb{Q}$, unique up to $\overline{\mathbb{Q}}$-isomorphism, with the property that $E_{\mathcal{O}}/\mathbb{Q}$ has complex multiplication by $\mathcal{O}$. When p is inert in $\mathcal{O}$, the properties of $E_{\mathcal{O}}$ imply that $E_{\mathcal{O}}$ has one or more of the above "non-split" level p structures which are defined over $\mathbb{Q}$. Thus, by the modular interpretation of $X_{\rm ns}^+(p)/\mathbb{Q}$ above, $E_{\mathcal{O}}$ gives rise to one or more $\mathbb{Q}$-rational points of $X_{\rm ns}^+(p)/\mathbb{Q}$ if p is inert in $\mathcal{O}$. The case $p = 3$ is special because the weaker condition that p is not ramified in $\mathcal{O}$ is sufficient to imply that $E_{\mathcal{O}}$ has a "non-split" level p structure.

It is well-known and not too difficult to check that the imaginary quadratic orders with discriminant $d_{\mathcal{O}} = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$ have class number one and that these are the only ones for $d_{\mathcal{O}} \geq -163$ (see for instance Appendix A.2. of [13]). From this list of imaginary quadratic orders of class number one, those with discriminant $d_{\mathcal{O}} = -7, -8, -28, -43, -67, -163$ have the property that 3 is unramified and 5 is inert in $\mathcal{O}$. These imaginary quadratic orders therefore give rise to at least 6 distinct $\mathbb{Q}$-rational points on $X_{\rm ns}^+(3)/\mathbb{Q}$ and $X_{\rm ns}^+(5)/\mathbb{Q}$.

An explicit parametrisation of $X_{\rm ns}^+(3)/\mathbb{Q}$ shows that an elliptic curve E/K defined over a field $K \subset \overline{\mathbb{Q}}$ gives rise to a $\mathbb{Q}$-rational point on $X_{\rm ns}^+(3)$ (i.e. has a "non-split" level p structure defined over $\mathbb{Q}$) if and only if $j(E)$ is a cube in $\mathbb{Q}$. This is a folklore fact, but we shall prove this later for completeness (see Appendix A.6. of [13], Section 5.3(b) of [12], and [6]). In the case that E/K has complex multiplication, then E/K gives rise to a $\mathbb{Q}$-rational point on $X_{\rm ns}^+(3)/\mathbb{Q}$ if and only if $j(E)$ is an integer cube since one knows in such a case that $j(E)$ is an algebraic integer.

Date: 1 August 1998.

This research was supported by an NSERC postdoctoral fellowship.

Thus, the imaginary quadratic orders above give rise to at least 6 $\mathbb{Q}$-rational points on $X_{\mathrm{ns}}^+(5)/\mathbb{Q}$ whose j-invariant is an integer cube.

By considering the explicit parametrisation of $X_{\mathrm{ns}}^+(5)/\mathbb{Q}$ he obtained (strictly speaking, he obtained an explicit parametrisation for $X_{\mathrm{ns}}^+(5)/\mathbb{Q}(\sqrt{5})$), Siegel was able to deduce that there are only 8 $\mathbb{Q}$-rational points of $X_{\mathrm{ns}}^+(5)/\mathbb{Q}$ whose j-invariant is an integer cube. This explicit parametrisation also reveals that the 6 imaginary quadratic orders above each give rise to a *unique* $\mathbb{Q}$-rational point on $X_{\mathrm{ns}}^+(5)/\mathbb{Q}$ whose j-invariant is an integer cube, and that the 2 extra points arise from $E_{\mathcal{O}_{-3}}$ where $\mathcal{O}_{-3}$ is the imaginary quadratic order with discriminant -3 . This solves the class number one problem for if $\mathcal{O}$ is an imaginary quadratic order of class number one with $d_K < -163$, then it is easily seen that both 3 and 5 are inert in $\mathcal{O}$ (in fact, $d_{\mathcal{O}} < -20$ implies this property). Hence, such an order $\mathcal{O}$ must give rise to a $\mathbb{Q}$-rational point on $X_{\mathrm{ns}}^+(5)/\mathbb{Q}$ whose j-invariant is an integer cube and which is distinct from the complete list determined by Siegel. This is a contradiction so that the list of imaginary quadratic orders of class number one listed above is in fact complete.

One should add that Siegel did not use the above modular interpretation of $X_{\mathrm{ns}}^+(5)/\mathbb{Q}$ explicitly in his arguments, rather, he deduced it from the properties of the uniformiser he constructed. Heegner's original proof was similiar in nature, except that he considered a modular curve of level 24 and required some class field theory to show $E_{\mathcal{O}}$ gave rise to a $\mathbb{Q}$-rational point on this curve.

In this paper, we derive another explicit parametrisation of the modular curve $X_{\mathrm{ns}}^+(5)/\mathbb{Q}$ using little more than the geometry of its complex points $X_{\mathrm{ns}}^+(5)(\mathbb{C}) = \Gamma_{\mathrm{ns}}^+(5)\backslash\mathfrak{H}^*$ as a riemann surface and some elementary algebra. Our normalisation of uniformiser differs from Siegel's in that it yields a uniformiser which is defined over $\mathbb{Q}$.

As an application, we obtain a proof of the class number one problem which, though certainly not new, requires little theory once the modular interpretation of $X_{\mathrm{ns}}^+(p)/\mathbb{Q}$ is established. Even though this requires some work to do rigorously [4], using modular interpretations provides a good conceptual framework for Siegel's proof.

A good account of the class number one problem from this and other points of view can be found in the appendix to [13]. A related paper to this one is [8] where the modular curves $X_{\mathrm{ns}}^+(N)$ for $N = 7$ and $N = 9$ are used to give separate solutions to the class number one problem.

2. Acknowledgements

I would like to thank the Department of Mathematics at UC Berkeley for their hospitality during my stay there in 1996-97. I would also like to thank B.J. Birch and S.J. Edixhoven for many useful discussions and suggestions, in particular to the latter for rekindling my interest on this topic.

3. Non-split Cartan modular curves

Let $X(N)$ be the modular curve which classifies isomorphism classes of elliptic curves with level N structure. The natural construction of $X(N)$ as an algebraic object and the precise manner in which it has the above property requires a technical definition of level N structure and indeed even of an elliptic curve [5] [7].

However, in the setting which concerns us, the elliptic curves E/K under consideration will be usual elliptic curves defined over a field $K \subset \overline{\mathbb{Q}}$. A level N structure on such an E/K is then an isomorphism of abelian groups $\phi : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \to E[N](\overline{\mathbb{Q}})$. Finally, the modular curve $X(N)$ has the structure of a non-singular projective curve which is defined over $\mathbb{Q}$, and geometrically has $\phi(N) = \#\left(\mathbb{Z}/N\mathbb{Z}^{\times}\right)$ components. Each of the geometric components of $X(N)/\mathbb{Q}$ is canonically isomorphic as a riemann surface to $\Gamma(N)\backslash\mathfrak{H}^*$, where $\Gamma(N)$ is the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ whose elements are congruent to the identity matrix modulo N, $\mathfrak{H}$ is the complex upper half plane, and $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$. The modular curve $X(N)/\mathbb{Q}$ classifies isomorphism classes of elliptic curves with level N structure in the following sense.

Theorem 3.1. *Let $K \subset \overline{\mathbb{Q}}$ be a field. Denote by $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}|K)$ the absolute galois group of K. There is an open subset $Y(N)/\mathbb{Q}$ of $X(N)/\mathbb{Q}$ such that $Y(N)(K)$ is in bijection with the set of isomorphism classes over $\overline{\mathbb{Q}}$ of pairs $(E/K, \phi/K)$, where E/K is an elliptic curve defined over K and ϕ/K is a level N structure invariant under the action of G_K.*

Proof. c.f. [5, IV-3]. □

The modular curve $X(N)/\mathbb{Q}$ has an action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which is defined over $\mathbb{Q}$. For each subgroup H of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the quotient $X_H/\mathbb{Q} = X(N)/H$ exists as a projective non-singular curve defined over $\mathbb{Q}$, and geometrically has $\phi_H(N) = \#\left(\mathbb{Z}/N\mathbb{Z}^{\times}/\det(H)\right)$ components. Each of these geometric components is canonically isomorphic as a riemann surface to $\Gamma_H\backslash\mathfrak{H}^*$, where Γ_H is the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ whose elements are congruent modulo N to an element in $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. The modular curves $X_H/\mathbb{Q}$ classify isomorphism classes of elliptic curves with certain level N structures in the following sense.

Theorem 3.2. *Let $K \subset \overline{\mathbb{Q}}$ be a field. Denote by $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}|K)$ the absolute galois group of K. For H a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, there is an open subset Y_H of X_H such that $Y_H(K)$ is in bijection with the set of isomorphism classes over $\overline{\mathbb{Q}}$ of pairs $(E/K, [\phi]_H/K)$, where E/K is an elliptic curve defined over K and $[\phi]_H/K$ is a H-equivalence class of level N structures (of which ϕ is a member) invariant under the action of G_K (level N structures are H-equivalent if they are related by a transformation in H).*

Proof. c.f. [5, IV-3]. □

There is a natural morphism $\pi_H/\mathbb{Q} : X_H/\mathbb{Q} \to X(1)/\mathbb{Q}$ whose modular interpretation is to forget the level structure imposed. Also, the open subset $Y_H(\mathbb{C})$ of $X_H(\mathbb{C})$ is precisely $X_H(\mathbb{C}) = \Gamma_H\backslash\mathfrak{H}^*$ with its cusps removed, that is $Y_H(\mathbb{C}) = \Gamma_H\backslash\mathfrak{H}$.

Let E/K be an elliptic curve with K as above. The absolute galois group G_K acts naturally on $E[N](\overline{\mathbb{Q}})$. Fixing a level N structure ϕ, one obtains a *mod N representation* $\rho_N^{\phi} : G_K \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by the relation $\phi^{\sigma} = \phi \circ \rho_N^{\phi}(\sigma)$ for $\sigma \in G_K$. The mod N representation associated to a pair $(E/K, [\phi]_H/K)$ has image lying in H so that the K-rational points of $X_H(N)$ can also be interpreted as the $\overline{\mathbb{Q}}$-isomorphism classes of pairs $(E/K, [\phi]_H)$ with the property that ρ_N^{ϕ} has image lying in H.

For any choice of points, $x \neq y \in \mathbb{P}^1(\mathbb{F}_p)$ and $z \in \mathbb{P}^1(\mathbb{F}_{p^2}), \notin \mathbb{P}^1(\mathbb{F}_p)$, the stabilisers C_z and $C_{x,y}$ in $\mathrm{GL}_2(\mathbb{F}_p)$ of (z, z^p) and (x, y), respectively, are called

a *non-split Cartan subgroup* and a *split Cartan subgroup*, respectively. The stabiliser N_z of $\{z, z^p\}$ gives the normaliser of the non-split Cartan subgroup C_z where $[N_z : C_z] = 2$. Similarly, the stabiliser $N_{x,y}$ of $\{x, y\}$ gives the normaliser of the split Cartan subgroup $C_{x,y}$ where $[N_{x,y} : C_{x,y}] = 2$. Since $\mathrm{GL}_2(\mathbb{F}_p)$ acts transitively on the set of objects, (z, z^p), (x, y), $\{z, z^p\}$, and $\{x, y\}$, respectively, we see there is only one conjugacy class of each type of subgroup C_z, $C_{x,y}$, N_z, and $N_{x,y}$, respectively.

We note for computational purposes that the normaliser of a non-split Cartan subgroup H can be conjugated to have the form

$$H = \left\{ \begin{pmatrix} \alpha & \lambda\beta \\ \beta & \alpha \end{pmatrix} \right\} \bigcup \left\{ \begin{pmatrix} \alpha & \lambda\beta \\ -\beta & -\alpha \end{pmatrix} \right\}$$

where $\lambda \in \mathbb{F}_p$ is a quadratic non-residue and $(\alpha, \beta) \neq (0, 0) \in \mathbb{F}_p \times \mathbb{F}_p$ (i.e. we regard $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{\lambda})$; then $H = N_z$ for $z = [\sqrt{\lambda} : 1] \in \mathbb{P}^1(\mathbb{F}_{p^2}), \notin \mathbb{P}^(\mathbb{F}_p)$ is in the above form).

Lemma 3.3. *Let p be an odd prime and suppose that $E/\mathbb{Q}$ is an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K. Then the mod p representation of $G_\mathbb{Q}$ associated to $E/\mathbb{Q}$ lies in the normaliser of a non-split or split Cartan subgroup accordingly as p is inert or split in $\mathcal{O}$.*

Proof. This result follows from the fact that $E[p](\overline{\mathbb{Q}})$ is a rank one $\mathcal{O}/p$-module on which G_K acts, c.f. [13, A.5.]; see also [9] for technical details relating to general orders in an imaginary quadratic field (as opposed to the maximal order). □

Fix a point $z \in \mathbb{P}^1(\mathbb{F}_{p^2}), \notin \mathbb{P}^1(\mathbb{F}_p)$ (for instance, $z = \sqrt{\lambda}$ where $\lambda \in \mathbb{F}_p$ is a quadratic non-residue). With $H = C_z$, we make the definition

Definition 3.4.

$$X_{ns}(p)/\mathbb{Q} = X_H/\mathbb{Q} \tag{1}$$

$$\Gamma_{ns}(p)/\mathbb{Q} = \Gamma_H/\mathbb{Q} \tag{2}$$

$$\pi_{ns}(p)/\mathbb{Q} = \pi_H/\mathbb{Q} \tag{3}$$

Similarly, with $H = N_z$, we make the definition

Definition 3.5.

$$X^+_{ns}(p)/\mathbb{Q} = X_H/\mathbb{Q} \tag{4}$$

$$\Gamma^+_{ns}(p)/\mathbb{Q} = \Gamma_H/\mathbb{Q} \tag{5}$$

$$\pi^+_{ns}(p)/\mathbb{Q} = \pi_H/\mathbb{Q} \tag{6}$$

See also p. 194-195 of [13] where these classes of modular curves are described and denoted by X_C and $X_{\tilde{C}}$, respectively, with C and $\tilde{C}$ of "non-split type" and $N = p$. Note that there is a natural morphism $\omega/\mathbb{Q} : X_{\mathrm{ns}}(p)/\mathbb{Q} \to X^+_{\mathrm{ns}}(p)/\mathbb{Q}$ of degree two, whose modular interpretation is to regard a C_z equivalence class of level p structures as a N_z equivalence class of level p structures.

Let $\mathcal{O}$ be an imaginary quadratic order of class number one and denote by $E_\mathcal{O}$ the unique (up to $\overline{\mathbb{Q}}$-isomorphism) elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}$. By Lemma 3.3, if p is an odd prime which is inert in $\mathcal{O}$, then by a suitable choice of level p structure ϕ, the mod p representation ρ_p^ϕ has image lying in N_z. The choice of such ϕ is not necessarily unique. To analyse this, one

needs to determine the image of the mod p representation (it is unique for instance if the image is all of N_z). We shall not require such information for the application to the class number one problem.

It follows that $E_{\mathcal{O}}$ gives rise to one or more $\mathbb{Q}$-rational points on $X^+_{\rm ns}(p)$ if p is inert in $\mathcal{O}$. In the case of $p = 3$, we note that the normaliser of a split Cartan subgroup lies in the normaliser of a non-split Cartan subgroup (see Appendix A.6. of [12] and the remark on p. 280 of [12]) so that $E_{\mathcal{O}}$ also gives rise to one or more $\mathbb{Q}$-rational points on $X^+_{\rm ns}(p)$ if p is split in $\mathcal{O}$.

4. Fundamental domains

The method used in this paper to obtain an explicit parametrisation of $X^+_{\rm ns}(3)/\mathbb{Q}$ and $X^+_{\rm ns}(5)/\mathbb{Q}$ requires information about the ramification structure of the covering $\pi^+_{\rm ns}(p)/\mathbb{C} : X^+_{\rm ns}(p)/\mathbb{C} \to X(1)/\mathbb{C}$ of riemann surfaces. We obtain this information in a classical way by constructing a fundamental domain for $\Gamma^+_{\rm ns}(p)$. It is also possible to obtain this information by using the modular interpretation of $X^+_{\rm ns}(p)/\mathbb{Q}$ discussed in Section 3, but we do not pursue this here as it is necessary to give a modular interpretation to all points of $X^+_{\rm ns}(p)/\mathbb{Q}$ in order to determine the ramification behaviour above $\infty \in \Gamma(1)\backslash\mathfrak{H}^* = X(1)/\mathbb{C}$. This requires a treatment of generalised elliptic curves and Tate curves [5] [7].

Let Γ be a fuchsian group, that is, a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$. By a fundamental domain for Γ, we shall mean a closed connected set $\mathcal{F}$ of $\mathfrak{H}^*$, together with certain identifications of segments of its boundary by elements in Γ, having the property that every point in $\Gamma\backslash\mathfrak{H}^*$ corresponds to a unique point in $\mathcal{F}$, up to the given boundary identifications.

For example, consider the case of $\Gamma = \Gamma(1)$. Let $S, T \in \Gamma$ be the elements

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then the standard fundamental domain for Γ is $\mathcal{F} = \{z \in \mathfrak{H} : |\Re(z)| \leq \frac{1}{2}, |z| \geq 1\}$, where the line $a = \{z \in \mathfrak{H}^* : \Re(z) = -\frac{1}{2}, |z| \geq 1\}$ is identified with the line $b = \{z \in \mathfrak{H}^* : \Re(z) = \frac{1}{2}, |z| \geq 1\}$ via $T \in \Gamma$ and the arc $c = \{z \in \mathfrak{H}^* : -\frac{1}{2} \leq \Re(z) \leq 0, |z| = 1\}$ is identified with the arc $d = \{z \in \mathfrak{H}^* : 0 \leq \Re(z) \leq \frac{1}{2}, |z| = 1\}$ via $S \in \Gamma$.

One can construct a fundamental domain $\mathcal{F}'$ for $\Gamma \subset \Gamma(1)$ of finite index by gluing together copies of the fundamental domain $\mathcal{F}$ for $\Gamma(1)$ (see [11]). We illustrate this process for $\Gamma = \Gamma^+_{\rm ns}(3)$ using the concrete description of $\Gamma^+_{\rm ns}(p)$ given at the end of Section 3.

We start by considering the copies of $\mathcal{F}$ adjacent to $\mathcal{F}$, that is to say, $T^{-1}\mathcal{F}$, $S\mathcal{F}$, and $T\mathcal{F}$. Since $S \in \Gamma^+_{\rm ns}(3)$, we see that the arc c is identified with the arc d via $S \in \Gamma^+_{\rm ns}(3)$. On the other hand, $T^{-1}\Gamma^+_{\rm ns}(3), T\Gamma^+_{\rm ns}(3) \neq \Gamma^+_{\rm ns}(3)$ and $T^{-1}\Gamma^+_{\rm ns}(3) \neq T\Gamma^+_{\rm ns}(3)$, so we glue $T^{-1}\mathcal{F}$ and $T\mathcal{F}$ to the sides of $\mathcal{F}$.

We continue by considering the copies of $\mathcal{F}$ adjacent $T^{-1}\mathcal{F} \cup \mathcal{F} \cup T\mathcal{F}$ not yet considered, namely, $T^{-2}\mathcal{F}$, $T^{-1}S\mathcal{F}$, $TS\mathcal{F}$, and $T^2\mathcal{F}$. Now, $T^{-2}\Gamma^+_{\rm ns}(3) = T\Gamma^+_{\rm ns}(3)$ so the line $T^{-1}a$ is identified with the line Tb via $T^3 = (T^{-2})^{-1}T \in \Gamma^+_{\rm ns}(3)$. Similarly, $T^2\Gamma^+_{\rm ns}(3) = T^{-1}\Gamma^+_{\rm ns}(3)$ yields the inverse identification. Finally, $T^{-1}S\Gamma^+_{\rm ns}(3) = T^{-1}\Gamma^+_{\rm ns}(3)$ so that the arc $T^{-1}c$ is identified with the arc $T^{-1}d$ via $S^{-1} = (T^{-1}S)^{-1}T^{-1} \in \Gamma^+_{\rm ns}(3)$. Similarly, $TS\Gamma^+_{\rm ns}(3) = T\Gamma^+_{\rm ns}(3)$ so that the arc Tc is identified with the arc Td via $S^{-1} = (TS)^{-1}T \in \Gamma^+_{\rm ns}(3)$.

Since there were no new copies of $\mathcal{F}$ added in the previous step, the process ends, and the desired fundamental domain for $\Gamma^+_{\rm ns}(3)$ is $\mathcal{F}' = T^{-1}\mathcal{F} \cup \mathcal{F} \cup T\mathcal{F}$, where $T^{-1}a$ is identified with Tb via T^3, $T^{-1}c$ is identified with $T^{-1}d$ via S^{-1}, c is identified with d via S, Tc is identified with Td via S^{-1}. Note that the elements which transform $\mathcal{F}$ to the different copies of $\mathcal{F}$ which one glues together to obtain $\mathcal{F}'$ form a complete set of inequivalent representatives for $\Gamma/\Gamma^+_{\rm ns}(3)$: $\{T^{-1}, 1, T\}$.

In what is to follow, we will often regard a point $z \in \mathfrak{H}^*$ as lying in possibly different riemann surfaces $\Gamma\backslash\mathfrak{H}^*$ by the projection $\mathfrak{H}^* \to \Gamma\backslash\mathfrak{H}^*$.

The fundamental domain for $\Gamma \subset \Gamma(1)$ of finite index yields information about covering $\pi : \Gamma\backslash\mathfrak{H}^* \to \Gamma(1)\backslash\mathfrak{H}^*$. In particular, one can determine how π ramifies above the points $\rho, i, \infty \in \Gamma(1)\backslash\mathfrak{H}^*$ (the only points where ramification may occur for such Γ).

For example, consider the case of $\Gamma = \Gamma^+_{\rm ns}(3)$. By following a small circular path around the point $\rho \in \Gamma^+_{\rm ns}(3)\backslash\mathfrak{H}^*$ (taking into account the boundary identifications), we find that $\rho \in \Gamma^+_{\rm ns}(3)\backslash\mathfrak{H}^*$ is a point of ramification index 3 lying above $\rho \in \Gamma(1)\backslash\mathfrak{H}^*$ since three copies of $\mathcal{F}$ meet at $\rho \in \Gamma^+_{\rm ns}(3)\backslash\mathfrak{H}^*$. A similar consideration shows that $i-1, i, i+1$ are unramified points lying above i, and ∞ is a point of ramification index 3 lying above ∞.

We note that a fundamental domain for $\Gamma \subset \Gamma(1)$ of finite index provides slightly more information than the ramification behaviour of the covering $\pi : \Gamma\backslash\mathfrak{H}^* \to \Gamma(1)\backslash\mathfrak{H}^*$. Indeed, if one were only interested in the ramification behaviour of π at ρ, i, ∞, this can already be deduced from how the $\Gamma(1)$ conjugacy classes of the elements ST, S, T break up into Γ conjugacy classes, respectively [1]. However, for the purposes of calculating an explicit parametrisation for $X^+_{\rm ns}(5)/\mathbb{Q}$, it will be necessary to keep track of ramification points in different covers. The additional information provided by fundamental domains will be useful for this purpose (see Section 6 for more details).

5. Covering relations

Let $X/\mathbb{Q}$ be a projective non-singular algebraic curve defined over $\mathbb{Q}$ which has genus zero (as a curve over $\mathbb{C}$ say) and at least one $\mathbb{Q}$-rational point. In such a case, there exists an isomorphism defined over $\mathbb{Q}$

$$t/\mathbb{Q} : X/\mathbb{Q} \to \mathbb{P}^1/\mathbb{Q} \tag{7}$$

which is unique up to an automorphism of $\mathbb{P}^1/\mathbb{Q}$. We call $t/\mathbb{Q}$ a *uniformiser* for $X/\mathbb{Q}$.

For example, the modular curves $X(1)/\mathbb{Q}$ and $X^+_{\rm ns}(p)/\mathbb{Q}$ for $p = 3, 5, 7$ have genus zero and at least one $\mathbb{Q}$-rational point, so applying the above, there exist uniformisers $j/\mathbb{Q}$ and $\eta^+_{\rm ns}(p)/\mathbb{Q}$ of these curves, respectively.

Suppose now that we have a non-constant morphism $\pi/\mathbb{Q} : X/\mathbb{Q} \to X(1)/\mathbb{Q}$ of curves defined over $\mathbb{Q}$. Fixing uniformisers $j/\mathbb{Q}$ and $t/\mathbb{Q}$, we obtain a diagram

$$\begin{array}{ccc} X/\mathbb{Q} & \xrightarrow{t/\mathbb{Q}} & \mathbb{P}^1/\mathbb{Q} = \operatorname{Proj}\mathbb{Q}[T] \\ {\scriptstyle \pi/\mathbb{Q}}\downarrow & & \downarrow{\scriptstyle \phi/\mathbb{Q}} \\ X(1)/\mathbb{Q} & \xrightarrow{j/\mathbb{Q}} & \mathbb{P}^1/\mathbb{Q} = \operatorname{Proj}\mathbb{Q}[J], \end{array} \tag{8}$$

where J and T are indeterminates. The morphism $\phi/\mathbb{Q} : \operatorname{Proj}\mathbb{Q}[T] \to \operatorname{Proj}\mathbb{Q}[J]$ in affine coordinates is given by a relation of the form

$$J = \lambda \frac{P(T)}{Q(T)} \tag{9}$$

where $\lambda \in \mathbb{Q}$, and $P(T)$, $Q(T) \in \mathbb{Q}[T]$ are monic polynomials. Such a relation is called a *covering relation* for $t/\mathbb{Q}$ with respect to $j/\mathbb{Q}$.

Alternatively, the function fields of $X(1)/\mathbb{Q}$ and $X/\mathbb{Q}$ can be identified with $\mathbb{Q}(j)$ and $\mathbb{Q}(t)$, respectively. The morphism $\pi/\mathbb{Q} : X^+_{\mathrm{ns}}(p)/\mathbb{Q} \to X(1)/\mathbb{Q}$ induces an embedding of the field $\pi/\mathbb{Q} : \mathbb{Q}(j) \to \mathbb{Q}(t)$. Thus,$\pi(j)$ can be expressed as

$$\pi(j) = \lambda \frac{P(t)}{Q(t)} \tag{10}$$

where λ, P and Q are the coincide with quantities in the covering relation of $t/\mathbb{Q}$ with respect to $j/\mathbb{Q}$.

The covering relation above characterises the uniformiser $t/\mathbb{Q}$ relative to the uniformiser $j/\mathbb{Q}$. By an *explicit parametrisation* for $X/\mathbb{Q}$, we shall roughly mean fixing uniformisers $t/\mathbb{Q}, j/q$ and determining explicitly the covering relation for $t/\mathbb{Q}$ relative to $j/\mathbb{Q}$. We note that discussion above concerning uniformisers and covering relations remains valid upon replacing $\mathbb{Q}$ by $\mathbb{C}$.

Suppose that there exists a fuchsian group $\Gamma \subset \Gamma(1)$ of finite index such that $X/\mathbb{C} = \Gamma\backslash\mathfrak{H}^*$ as a compact riemann surface and the morphism $\pi/\mathbb{C} : X/\mathbb{C} \to X(1)/\mathbb{C}$ corresponds to the natural covering map $\pi/\mathbb{C} : \Gamma\backslash\mathfrak{H}^* \to \Gamma(1)\backslash\mathfrak{H}^*$. Considering diagram 8 over $\mathbb{C}$, we obtain a diagram

$$\begin{array}{ccc} \Gamma\backslash\mathfrak{H}^* & \xrightarrow{t/\mathbb{C}} & \mathbb{P}^1(\mathbb{C}) \\ {\scriptstyle \pi/\mathbb{C}}\downarrow & & {\scriptstyle \phi/\mathbb{C}}\downarrow \\ \Gamma(1)\backslash\mathfrak{H}^* & \xrightarrow{j/\mathbb{C}} & \mathbb{P}^1(\mathbb{C}). \end{array} \tag{11}$$

From here on, we choose $j/\mathbb{C}$ to be the unique uniformiser of $X(1)/\mathbb{C}$ which takes on the values $0, 12^3, \infty$ on the three distinct points $\rho = \exp^{2\pi i/3}, i = \sqrt{-1}, \infty \in \Gamma(1)\backslash\mathfrak{H}^*$. This uniformiser arises from a uniformiser $j/\mathbb{Q}$ since the points $\rho, i, \infty \in X(1)(\mathbb{C})$ are in fact $\mathbb{Q}$-rational points by the modular interpretation of $X(1)/\mathbb{Q}$ (i.e. this choice of uniformiser of $X(1)/\mathbb{Q}$ coincides with the function which assigns to an isomorphism class of elliptic curves its j-invariant).

The embedding $\pi : \mathbb{C}(j) \to \mathbb{C}(t)$ identifies the function $j/\mathbb{C}$ on $X(1)/\mathbb{C}$ with a function $\pi(j)$ on $X/\mathbb{C}$. However, if we consider j as a function on $\mathfrak{H}$, then this identification is to simply regard j, apriori a modular function for $\Gamma(1)$, as a modular function for Γ. Hence, the covering relation for $t/\mathbb{C}$ with respect to $j/\mathbb{C}$ is in fact a veritable relation (as modular functions for Γ)

$$j = \lambda \frac{P(t)}{Q(t)}$$

where $\lambda \in \mathbb{C}$ and $P(T), Q(T) \in \mathbb{C}[T]$ are monic polynomials. If one chooses the uniformiser $t/\mathbb{C}$ so that it arises from a uniformiser $t/\mathbb{Q}$, then in fact $\lambda \in \mathbb{Q}$ and $P(T), Q(T) \in \mathbb{Q}[T]$, as the covering relation for $t/\mathbb{C}$ with respect to $j/\mathbb{C}$ then coincides with the covering relation for $t/\mathbb{Q}$ with respect to $j/\mathbb{Q}$. Furthermore, in

terms of riemann surfaces, we see that

$$P(T) = \prod_{z\in\pi^{-1}(\rho)} (T - t(z))^{e(z)} \tag{12}$$

$$Q(T) = \prod_{z\in\pi^{-1}(\infty)} (T - t(z))^{e(z)} \tag{13}$$

$$\lambda = j(z_0) \cdot Q(z_0)/P(z_0) \tag{14}$$

where $\pi/\mathbb{C} : \Gamma\backslash\mathfrak{H}^* \to \Gamma(1)\backslash\mathfrak{H}^*$ and $e(z)$ is the ramification index of $z \in \Gamma\backslash\mathfrak{H}^*$ and $z_0 = t^{-1}(\infty)$.

Information about how the covering $\pi/\mathbb{C} : \Gamma\backslash\mathfrak{H}^* \to \Gamma(1)\backslash\mathfrak{H}^*$ branches above the points $\rho, i, \infty \in \Gamma\backslash\mathfrak{H}^*$ is in principle sufficient to determine the relation between $j/\mathbb{C}$ and $t/\mathbb{C}$. We illustrate this by deriving a covering relation for a uniformiser $t/\mathbb{Q} = \eta^+_{\mathrm{ns}}(3)/\mathbb{Q}$ of $X/\mathbb{Q} = X^+_{\mathrm{ns}}(3)/\mathbb{Q}$ with respect to $j/\mathbb{Q}$ using information from the fundamental domain we obtained for $\Gamma = \Gamma^+_{\mathrm{ns}}(3)$.

Since $\rho, \infty \in \Gamma^+_{\mathrm{ns}}(3)\backslash\mathfrak{H}^*$ are the unique points lying above $\rho, \infty \in \Gamma(1)\backslash\mathfrak{H}^*$, it follows that $t(\rho), t(\infty) \in \mathbb{P}^1(\mathbb{Q})$. By an automorphism of $\mathbb{P}^1/\mathbb{Q}$, we can therefore assume that $t(\rho) = 0$ and $t(\infty) = \infty$. This determines t up to scaling by $\mathbb{Q}$ so that the relation between j and t has the form $j = \lambda t^3$ where $\lambda \in \mathbb{Q}$ is determined up to a cube in $\mathbb{Q}$. However, it is easy to see that λ must be a cube and hence without loss of generality equal to 1. This follows from the fact that $j(E_{\mathcal{O}_{-4}}) = 12^3$ and $t(E_{\mathcal{O}_{-4}}) \in \mathbb{Q}$ as the prime 3 is inert in $\mathcal{O}_{-4}$ where $\mathcal{O}_{-4}$ is the imaginary quadratic order with discriminant -4.

We have thus proved

Proposition 5.1. *There exists a choice of uniformiser $t/\mathbb{Q} = \eta^+_{ns}(3)/\mathbb{Q} : X^+_{ns}(3)/\mathbb{Q} \to \mathbb{P}^1/\mathbb{Q}$ such that $t(0) = 0$, $t(\infty) = \infty$ and the relation between $j/\mathbb{Q}$ and $t/\mathbb{Q}$ is*

$$j = t^3. \tag{15}$$

Corollary 5.2. *An elliptic curve E/K with $K \subset \overline{\mathbb{Q}}$ gives rise to a $\mathbb{Q}$-rational point on $X^+_{ns}(3)/\mathbb{Q}$ if and only if $j(E)$ is a cube in $\mathbb{Q}$.*

6. An explicit parametrisation for $X^+_{\mathrm{NS}}(5)/\mathbb{Q}$

In this section, let $\eta/\mathbb{Q} = \eta^+_{\mathrm{ns}}(5)/\mathbb{Q}$ denote a uniformiser of $X^+_{\mathrm{ns}}(5)/\mathbb{Q}$. From the fundamental domain for $\Gamma^+_{\mathrm{ns}}(5)$, we see that the points $\rho, \rho+1, \rho+2, \rho+3 \in \Gamma^+_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ lie above the point $\rho \in \Gamma(1)\backslash\mathfrak{H}^*$ with ramification index $3, 3, 3, 1$, respectively. The points $i-1, i, i+1, i+2, \frac{i-1}{2}, \frac{i+1}{2} \in \Gamma^+_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ lie above the point $i \in \Gamma(1)\backslash\mathfrak{H}^*$ with ramification index $2, 2, 2, 2, 1, 1$, respectively. Finally, the cusps $1, \infty \in \Gamma^+_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ lie above the cusp $\infty \in \Gamma(1)\backslash\mathfrak{H}^*$ with ramification index 5.

The field of definition of the two galois conjugate cusps $1, \infty$ is $\mathbb{Q}(\sqrt{5})$, [13, A.5.]. Thus, by an automorphism of $\mathbb{P}^1/\mathbb{Q}$, we may assume that $\eta(1), \eta(\infty)$ are roots of $X^2 - 5$. Furthermore, since $\rho + 3 \in \Gamma^+_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ is the uniquely unramified point above $\rho \in \Gamma(1)\backslash\mathfrak{H}^*$, we have $\eta(\rho+3) \in \mathbb{P}^1(\mathbb{Q})$, which by an automorphism of $\mathbb{P}^1/\mathbb{Q}$ fixing the roots of $X^2 - 5$, we may assume $\eta(\rho+3) = 0$. This specifies the choice of η (unique up to sign) we will use in the subsequent calculation.

The relation between j and η has the form

$$j = \lambda \frac{\eta(\eta - A)^3(\eta^2 - B\eta + C)^3}{(\eta^2 - 5)^5} \tag{16}$$

where $A = \eta(\rho+2)$, $B = \eta(\rho) + \eta(\rho+1)$, $C = \eta(\rho) \cdot \eta(\rho+1)$.

In principle, one can determine the quantities λ, A, B, C by the same method used in the previous section. However, this requires solving a system of 10 equations in 10 unknowns, a daunting task even for a computer. To make the calculation of λ, A, B, C tractable, we shall compute the desired relation using intermediate coverings.

We note that once we have the covering relation, it is easy though unilluminating to verify it is correct by checking if it gives the unique (up to symmetries of the normalisation of η) solution to the above equations. In choosing a suitable normalisation of η, some properties of the modular curve $X_{\mathrm{ns}}^{+}(5)/\mathbb{Q}$ were required above, in particular, the field of definition of its two cusps. This is again unnecessary once we have the covering relation since we can verify that we have the correct model over $\mathbb{Q}$ by showing the existence of three $\mathbb{Q}$-rational j-invariants of elliptic curves with complex multiplication, each of which give rise via the covering relation to a $\mathbb{Q}$-rational value of η, for instance, $j = -15^3, 20^3, 255^3$ (refer to [3] for a complete list of $\mathbb{Q}$-rational j-invariants of elliptic curves with complex multiplication).

Although there is no intermediate subgroup between $\Gamma_{\mathrm{ns}}^{+}(5) \subset \Gamma(1)$, there is an intermediate subgroup Γ_5 between $\Gamma_{\mathrm{ns}}(5) \subset \Gamma(1)$ which can be described as follows: There exists a subgroup $A_4 \subset \mathrm{GL}_2(\mathbb{F}_5)$ whose projective image is isomorphic to A_4 and which lies between $C' \cap \mathrm{SL}_2(\mathbb{F}_5) \subset \mathrm{GL}_2(\mathbb{F}_5)$. Then Γ_5 is the subgroup of elements of $\Gamma(1)$ which reduce modulo p to an element in A_4.

The methods of Section 4 reveal that the points $\rho, \rho+1, \rho+3 \in \Gamma_5\backslash\mathfrak{H}^*$ lie above the point $\rho \in \Gamma(1)\backslash\mathfrak{H}^*$ with ramification index $1, 3, 1$, respectively. The points $i, i+1, i+2 \in \Gamma_5\backslash\mathfrak{H}^*$ lie above the point $i \in \Gamma(1)\backslash\mathfrak{H}^*$ with ramification index $2, 1, 2$, respectively. Finally, the cusp $\infty \in \Gamma_5\backslash\mathfrak{H}^*$ lies above the cusp $\infty \in \Gamma(1)\backslash\mathfrak{H}^*$ with ramification index 5.

Let $\xi/\mathbb{C} : \Gamma_5\backslash\mathfrak{H}^* \to \mathbb{P}^1(\mathbb{C})$ be a uniformiser such that $\xi(\rho+1) = 0$, $\xi(\infty) = \infty$. It is not too hard to see that up to scaling ξ, the quantity λ in the covering relation for $\xi/\mathbb{C}$ with respect to $j/\mathbb{C}$ can be assumed to be 1. The relation between j and ξ then has the form

$$j = \xi^3(\xi^2 - A\xi + B). \tag{17}$$

where $A = \xi(\rho)+\xi(\rho+3)$, $B = \xi(\rho)\cdot\xi(\rho+3)$. From the way $\pi_{A_4} : \Gamma_5\backslash\mathfrak{H}^* \to \Gamma(1)\backslash\mathfrak{H}^*$ branches above $i \in \Gamma(1)\backslash\mathfrak{H}^*$, we see that the polynomial

$$\xi^3(\xi^2 - A\xi + B) - 12^3 - (\xi - C)(\xi^2 - D\xi + E)^2 \in \mathbb{C}[\xi] \tag{18}$$

is zero, where $C = \xi(i+1)$, $D = \xi(i) + \xi(i+2)$, $E = \xi(i)\cdot\xi(i+2)$. This yields the equations

$$2D + C - A = 0 \tag{19}$$

$$-D^2 - 2E - 2CD + B = 0 \tag{20}$$

$$2DE + 2CE + CD^2 = 0 \tag{21}$$

$$-E^2 - 2CDE = 0 \tag{22}$$

$$CE^2 = 12^3. \tag{23}$$

By eliminating $C = 12^3/E^2$ from equation 22, we obtain $D = -E^3/2\cdot 12^3$. Eliminating C and D from equation 21 yields $E^5 = 24^5$ so $E = 24$ is one solution. The remaining unknowns are then easily determined as $A = -5$, $B = 40$, $C = 3$, $D = -4$.

Proposition 6.1. *There exists a choice of uniformiser $\xi/\mathbb{C} : \Gamma_5\backslash\mathfrak{H}^* \to \mathbb{P}^1(\mathbb{C})$ such that $\xi(\rho+1) = 0$, $\xi(\infty) = \infty$, and the relation between $j/\mathbb{C}$ and $\xi/\mathbb{C}$ is*

$$j = \xi^3(\xi^2 + 5\xi + 40). \tag{24}$$

Consider the two coverings

$$\Gamma_{\mathrm{ns}}(5)\backslash\mathfrak{H}^* \xrightarrow[\omega/\mathbb{C}]{} \Gamma^+_{\mathrm{ns}}(5)\backslash\mathfrak{H}^* \xrightarrow[\pi^+_{\mathrm{ns}}(5)/\mathbb{C}]{} \Gamma(1)\backslash\mathfrak{H}^*.$$

Recall the points $\rho, \rho+1, \rho+2, \rho+3 \in \Gamma^+_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ lie above the point $\rho \in \Gamma(1)\backslash\mathfrak{H}^*$, the points $i-1, i, i+1, i+2, \frac{i-1}{2}, \frac{i+1}{2}$ lie above the point $i \in \Gamma(1)\backslash\mathfrak{H}^*$, and the points $1, \infty$ lie above the point $\infty \in \Gamma(1)\backslash\mathfrak{H}^*$. For $z \in \Gamma^+_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ one of the above points, we denote the two (not necessarily distinct) points in $\omega^{-1}(z)$ by $z, \widetilde{z} \in \Gamma_{\mathrm{ns}}\backslash\mathfrak{H}^*$.

The covering $\pi : \Gamma_{\mathrm{ns}}(5)\backslash\mathfrak{H}^* \to \Gamma_5\backslash\mathfrak{H}^*$ is branched as follows: The points $\rho, \widetilde{\rho+3} \in \Gamma_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ lie above the point $\rho \in \Gamma_5\backslash\mathfrak{H}^*$ with ramification index $3, 1$, respectively. The points $\rho+3, \widetilde{\rho+1} \in \Gamma_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ lie above the point $\rho+3 \in \Gamma_5\backslash\mathfrak{H}^*$ with ramification index $1, 3$, respectively. The points $i+1, \widetilde{i-1} \in \Gamma_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ lie above the point $i+1 \in \Gamma_5\backslash\mathfrak{H}^*$ with ramification index 2.

Let $\chi/\mathbb{C} : \Gamma_5\backslash\mathfrak{H}^* \to \mathbb{P}^1(\mathbb{C})$ be the uniformiser such that $\chi(\rho) = 0$, $\chi(\rho+3) = \infty$, and the expansion of χ at ∞ has constant term 1. It is easily seen that

$$\chi = \frac{\xi - \xi(\rho)}{\xi - \xi(\rho+3)}. \tag{25}$$

Let $\gamma : \Gamma_{\mathrm{ns}}(5)\backslash\mathfrak{H}^* \to \mathbb{P}^1(\mathbb{C})$ be the uniformiser such that $\gamma(\rho) = 0$, $\gamma(\rho+3) = \infty$, the quantity λ is 1 in the covering relation for $\gamma/\mathbb{C}$ with respect to $\chi/\mathbb{C}$. The relation between χ and γ has the form

$$\chi = \frac{\gamma^3(\gamma - U)}{(\gamma - V)^3} \tag{26}$$

where $U = \gamma(\widetilde{\rho+3})$, $V = \gamma(\widetilde{\rho+1})$.

From how π branches above $i+1 \in \Gamma_5\backslash\mathfrak{H}^*$, we see that the polynomial

$$\gamma^3(\gamma - U) - e(\gamma - V)^3 - (\gamma^2 - X\gamma + Y)^2 \in \mathbb{C}[\gamma] \tag{27}$$

is zero, where $e = \chi(i+1)$, $X = \gamma(i+1) + \gamma(\widetilde{i-1})$, $Y = \gamma(i+1) \cdot \gamma(\widetilde{i-1})$. This yields the system of equations

$$-U - e + 2X = 0 \tag{28}$$

$$3eV - 2Y - X^2 = 0 \tag{29}$$

$$-3eV^2 + 2XY = 0 \tag{30}$$

$$eV^3 - Y^2 = 0 \tag{31}$$

which can be solved as follows. From equations 30, 31, we get

$$9e^2V^4 = 4X^2Y^2$$
$$eV^3 = Y^2.$$

Dividing the first equation by the second yields $9eV = 4X^2$ so that $X^2 = \frac{9}{4}eV$. Using equation 29, we obtain $3eV - 2Y - \frac{9}{4}eV = 0$ so that $V = \frac{8}{3e}Y$. Substituting this into equation 31 yields $Y = \frac{3^3}{8^3}e^2$. It then follows that $V = \frac{3^2}{8^2}e$, $X = \frac{3^2}{4^2}e$ from equation 30, and $U = \frac{1}{8}e$ from equation 28.

We determine the quantity U more explicitly. Using the relation between χ and ξ, plus the fact that $\xi(i+1)=3$, we obtain $e=\chi(i+1)=\frac{3-x}{3-\overline{x}}$, where $x=\xi(\rho)$ is a root of $X^2+5X+40=0$. It follows that $e=-\frac{1}{8^2}(11x+31)$ satisfies $8^2e^2+7e+8^2=0$ and $U=\frac{e}{8}$ satisfies $8^3U^2+7U+8=0$.

At this point, we have related $j/\mathbb{C}$ to $\xi/\mathbb{C}$, $\chi/\mathbb{C}$ to $\xi/\mathbb{C}$, and $\chi/\mathbb{C}$ to $\gamma/\mathbb{C}$. The final step is to find the relation between $\gamma/\mathbb{C}$ and $\eta/\mathbb{C}$. Consider the covering $\omega:\Gamma_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*\to\Gamma^+_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$. The points $\rho+3,\widetilde{\rho+3}\in\Gamma_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ lie above the point $\rho+3\in\Gamma^+_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$. Since $\eta(\rho+3)=0$, $\gamma(\rho+3)=U$, and $\gamma(\widetilde{\rho+3})=\infty$, we see such a relation has the form

$$\eta=\lambda\frac{\gamma-U}{\gamma^2-u\gamma+v}.$$

The isomorphism η was chosen so that $\eta(1),\eta(\infty)$ are roots of X^2-5. The cusps $0,1,\in\Gamma_{\mathrm{ns}}\backslash\mathfrak{H}^*$ lie above the cusp $1\in\Gamma^+_{\mathrm{ns}}\backslash\mathfrak{H}^*$, and the cusps $\frac{1}{2},\infty\in\Gamma_{\mathrm{ns}}(5)\backslash\mathfrak{H}^*$ lie above the cusp $\infty\in\Gamma^+_{\mathrm{ns}}\backslash\mathfrak{H}^*$. Furthermore, $\gamma(0),\gamma(1),\gamma(\frac{1}{2}),\gamma(\infty)$ satisfy $\gamma^3(\gamma-U)-(\gamma-V)^3=0$, since $\chi(\infty)=1$. Therefore, $\eta^2-5=0$ implies $\gamma^3(\gamma-U)-(\gamma-V)^3=0$.

We use the above fact to determine λ,u,v by requiring the polynomial

$$\lambda^2(\gamma-U)^2-5(\gamma^2-u\gamma+v)^2+5(\gamma^3(\gamma-U)-(\gamma-V)^3)\in\mathbb{C}[\gamma] \tag{32}$$

to be zero. This yields the system of equations

$$10u-5U-5=0 \tag{33}$$

$$\lambda^2-5u^2-10v+15V=0 \tag{34}$$

$$-2\lambda^2U+10uv-15V^2=0 \tag{35}$$

$$\lambda^2U^2-5v^2+5V^3=0. \tag{36}$$

From equation 33, we obtain immediately that $u=\frac{U+1}{2}$. Also, we have $V=\frac{9}{8}U$. We can therefore regard the remaining three equations in λ,v as having coefficients in the quadratic field $\mathbb{Q}[U]$, which we now work in.

Multiplying equation 34 by $2U$ and adding it to equation 35 yields

$$v(1-3U)=2Uu^2-6UV+3V^2. \tag{37}$$

and hence

$$v=\frac{3^2}{2^3\cdot 11}(-4U^2+5U). \tag{38}$$

Using equation 34, we obtain

$$\lambda^2=\frac{3^6}{2^2\cdot 11^2}(3U-1)^2 \tag{39}$$

and hence

$$\lambda=\pm\frac{3^3}{2\cdot 11}(3U-1). \tag{40}$$

At this point, we can compute the quantity

$$\eta(\rho)=-\lambda U/v \tag{41}$$

$$=\frac{2^2}{3^2\cdot 11}(128U-61) \tag{42}$$

Since $\eta(\rho+1)=\overline{\eta(\rho)}$, we see that $B=\mp 5$ and $C=20/3$.

To determine λ, A, consider the direct relation between ξ and η. This relation has the form

$$a(\eta)\xi^2 + b(\eta)\xi + c(\eta) = 0 \tag{43}$$

where $a(X), b(X), c(X)$ are quartic polynomials in $\mathbb{Q}[X]$ and $a(X)$ is monic.

To the point $\rho+1 \in \Gamma_5\backslash\mathfrak{H}^*$ corresponds the points $\rho, \rho+1, \rho+2 \in \Gamma_{\mathrm{ns}}^+(5)\backslash\mathfrak{H}^*$ with ramification index $1, 1, 2$, respectively. Since $\xi(\rho+1) = 0$, this implies that $c(X) = \beta(X-A)^2(X^2 - BX + C)$ for some $\beta \in \mathbb{Q}$. To the cusp $\infty \in \Gamma_5\backslash\mathfrak{H}^*$ corresponds the cusps $1, \infty \in \Gamma_{\mathrm{ns}}^+(5)\backslash\mathfrak{H}^*$ with ramification index 2. Thus, $a(X) = (X^2-5)^2$. On the other hand, if $\eta^2 - 5 = 0$, the relation must be such that $\xi = \infty$ is the only solution. This forces $X^2 - 5$ to divide $b(X)$. Similarly, when $\eta^2 - B\eta + C = 0$, the relation must be such that $\xi = 0$ is the only solution. Thus, $X - A$ divides $b(X)$ so that $b(X) = (X-A)(X^2-5)(\alpha X - \delta)$ for some $\alpha, \delta \in \mathbb{Q}$.

Therefore, the relation between ξ and η has the more specific form

$$\xi^2(\eta^2-5)^2 + \xi(\eta - A)(\eta^2-5)(\alpha\eta - \delta) + \beta(\eta - A)^2(\eta^2 - B\eta + C) = 0. \tag{44}$$

If $\eta = 0$, then relation 44 reads

$$5^2\xi^2 - 5A\delta\xi + \beta A^2 C = 0. \tag{45}$$

However, the corresponding ξ satisfies $\xi^2 + 5\xi + 40 = 0$, so we obtain the equations

$$-A\delta = 5^2 \tag{46}$$

$$\beta A^2 C = 5^2 \cdot 40. \tag{47}$$

If $\eta^2 - B\eta + C = 0$, then relation 44 reads

$$\xi^2(\eta^2-5)^2 + \xi(\eta - A)(\eta^2-5)(\alpha\eta - \delta) = 0. \tag{48}$$

so that

$$\xi = 0 \text{ or } \xi = -\frac{(\eta - A)(\alpha\eta - \delta)}{\eta^2 - 5}. \tag{49}$$

In the latter case, the corresponding ξ satisfies $\xi^2 + 5\xi + 40 = 0$ so that $\xi = \mp 9\eta - 25, \pm 9\eta + 20$ (where the signs depend on the choice of $B = \pm 5$) and hence we have

$$(\mp 9\eta - 25), (\pm 9\eta + 20) = \xi = -\frac{(\eta - A)(\alpha\eta - \delta)}{\eta^2 - 5}. \tag{50}$$

This gives a quadratic relation for η, which must be a $\mathbb{Q}$-scalar multiple of $\eta^2 - B\eta + C = 0$. The resulting equations in the case $\xi = \mp 9\eta - 25$ allow us to solve for $\alpha = \mp 5$, $A = \pm 1$, $\delta = \pm 25$, $\beta = 150$. The other case is not solvable and hence does not occur.

Finally, to obtain λ, we use the fact that when $\eta = \infty$, $j = \lambda$. Since $\eta = \infty$ implies that $\xi^2 + \alpha\xi + \beta = 0$, we see that $\xi = \frac{\pm 5 \pm \sqrt{-23}}{2}$ and hence $j = \xi^3(\xi^2 + 5\xi + 40) = 3^3 \cdot 10^4$.

Proposition 6.2. *There exists a choice of uniformiser $\eta/\mathbb{Q} = \eta_{ns}^+(5)/\mathbb{Q} : X_{ns}^+(5)/\mathbb{Q} \to \mathbb{P}^1/\mathbb{Q}$ such that $\eta(1), \eta(\infty)$ are roots of $X^2 - 5$ and $\eta(\rho+3) = 0$. The relation between $j/\mathbb{Q}$ and $\eta/\mathbb{Q}$ is*

$$j = 10^4 \frac{\eta(\eta \pm 1)^3(3\eta^2 \pm 15\eta + 20)^3}{(\eta^2 - 5)^5}. \tag{51}$$

Corollary 6.3. *There exists a choice of uniformiser $\eta/\mathbb{Q} = \eta^+_{ns}(5)/\mathbb{Q} : X^+_{ns}(5)/\mathbb{Q} \to \mathbb{P}^1/\mathbb{Q}$ such that $\eta(1), \eta(\infty)$ are roots of $X^2 + X - 1$ and $\eta(\rho + 3) = 0$. The relation between $j/\mathbb{Q}$ and $\eta/\mathbb{Q}$ is*

$$j = 5^3 \frac{\eta(2\eta \pm 1)^3(2\eta^2 \pm 7\eta + 8)^3}{(\eta^2 + \eta - 1)^5}. \tag{52}$$

Proof. The map $z \mapsto \frac{2z}{z+5}$ fixes 0 and sends the roots of $X^2 - 5$ to the roots of $X^2 + X - 1$. Hence, substituting $\eta = \frac{5\eta}{-\eta+2}$ into the covering relation given in Proposition 6.2 yields the desired result. □

Remark 6.4. *The covering relation in the above corollary is somewhat better in the sense that it is defined over $\mathbb{Z}[\frac{1}{5}]$, rather than $\mathbb{Z}[\frac{1}{10}]$, however obtaining the covering relation for η as normalised in the proposition is easier because the equations in 34–36 have no terms in λ.*

The above covering relations for $\eta^+_{\mathrm{ns}}(5)/\mathbb{Q}$ with respect to $j/\mathbb{Q}$, as well as a similar one for $\eta^+_{\mathrm{ns}}(7)/\mathbb{Q}$ with respect to $j/\mathbb{Q}$, can be found in [2].

7. Reduction to a genus 2 curve

Let $t/\mathbb{Q} = \eta^+_{\mathrm{ns}}(3)/\mathbb{Q}$ and $\eta/\mathbb{Q} = \eta^+_{\mathrm{ns}}(5)/\mathbb{Q}$ be normalised so that their relations with $j/\mathbb{Q}$ are

$$j = t^3 \tag{53}$$

$$j = 5^3 \frac{\eta(2\eta + 1)^3(2\eta^2 + 7\eta + 8)^3}{(\eta^2 + \eta - 1)^5}. \tag{54}$$

as given in Proposition 5.1 and Corollary 6.3.

Suppose that $E_{\mathcal{O}}/\mathbb{Q}$ is the elliptic curve associated to an imaginary quadratic order $\mathcal{O}$ of class number one in which 3 is unramified and 5 is inert. Then $E_{\mathcal{O}}/\mathbb{Q}$ gives rise to one or more values of (t, η) such that $t = m \in \mathbb{Z}$, $j(E_K) = m^3$ is a cube, and $\eta = x/y \in \mathbb{Q}$ where $x, y \in \mathbb{Z}$ and $(x, y) = 1$. If we let

$$u(x, y) = 5^3 \frac{x(2x + y)^3(2x^2 + 7xy + 8y^2)^3}{(x^2 + xy - y^2)^5}, \tag{55}$$

then

$$m^3 = u(x, y). \tag{56}$$

Thus, $E_{\mathcal{O}}$ gives rise to an integer solution (x, y, m) of 56 with $(x, y) = 1$. We now analyse such solutions by elementary considerations.

Let (x, y, m) be an integer solution to 56 with $(x, y) = 1$. Note that if (x, y, m) is a solution to 56, so is $(-x, -y, m)$. If $m = 0$, then the only solutions are $(x, y, m) = \pm(0, 1, 0), \pm(-1, 2, 0)$. We now assume that $m \neq 0$.

Lemma 7.1. *Let l be a prime. Suppose there exists $z \in \mathbb{Z}$ such that*

$$\begin{cases} z^2 + z - 1 & \equiv 0 \pmod{l} \\ 2z + 1 & \equiv 0 \pmod{l}. \end{cases}$$

Then $l = 5$.

Proof. Since $z^2 + z - 1 \equiv 0 \pmod 2$ has no solution, we may assume $l \neq 2$. Substituting $z \equiv -1/2 \pmod l$ into the first equation, we obtain that $-5 \equiv 0 \pmod l$. Thus, $l = 5$. □

Lemma 7.2. *Let l be a prime. Suppose that there exists $z \in \mathbb{Z}$ such that*

$$\begin{cases} z^2 + z - 1 & \equiv 0 \pmod{l} \\ 2z^2 + 7z + 8 & \equiv 0 \pmod{l}. \end{cases}$$

Then $l = 5$.

Proof. A simple check shows that $l \neq 2, 3$. By the quadratic formula, z is simultaneously $(-1 \pm \sqrt{5})/2 \pmod{l}$ and $(-7 \pm \sqrt{-15})/4 \pmod{l}$. As 2 and 3 are invertible $\pmod{l}$, we have

$$\begin{aligned} & (-1 \pm \sqrt{5})/2 \equiv (-7 \pm \sqrt{-15})/4 \pmod{l} \\ \iff & -2 \pm 2\sqrt{5} \equiv -7 \pm \sqrt{-15} \pmod{l} \\ \iff & \pm 2\sqrt{5} \pm \sqrt{-15} \equiv 5 \pmod{l} \\ \iff & \pm 5\sqrt{-3} \equiv 0 \pmod{l}. \end{aligned}$$

Hence, $l = 5$. □

Lemma 7.3. *The equation $z^2 + z - 1 \equiv 0 \pmod{5^2}$ does not have a solution in $\mathbb{Z}$.*

Suppose that $x^2 + xy - y^2 \equiv 0 \pmod{l}$ for some prime l. First note that $x \not\equiv 0 \pmod{l}$ since this would imply that $y \equiv 0 \pmod{l}$, contradicting $(x, y) = 1$. On the other hand, since $u(x, y)$ is an integer, we see that $5^3(2x+y)^3(2x^2+7xy+8y^2)^3 \equiv 0 \pmod{l}$. By Lemmas 7.1 and 7.2 it follows that $l = 5$, and by Lemma 7.3 we must in fact have $x^2 + xy - y^2 = \pm 5$. This contradicts $u(x, y)$ being a cube.

We have therefore shown that any solution (x, y, m) to 56 must satisfy $x^2 + xy - y^2 = \pm 1$. In addition, we see that x must be a cube. Now, the solutions of $x^2 + xy - y^2 = \pm 1$ are nothing but the solutions of $N_L(x + y\epsilon) = \pm 1$ where $\epsilon = (-1 + \sqrt{5})/2$ and $L = \mathbb{Q}(\epsilon)$. Thus, (x, y) is a solution of $x^2 + xy - y^2 = \pm 1$ exactly when $x + y\epsilon$ is a unit in the ring of integers of L, $\mathcal{O}_L = \mathbb{Z}[\epsilon]$. It is well-known that the units of $\mathcal{O}_L$ are given by $\pm\epsilon^n$ for some $n \in \mathbb{Z}$ and that

$$\pm\epsilon^n = \pm(x_n + y_n\epsilon) \tag{57}$$

where $x_n = (-1)^{n+1}F_n$, $y_n = (-1)^n F_{n+1}$, and F_n is the n-th Fibonacci number.

Theorem 7.4. *The only Fibonacci cubes are $F_1 = F_2 = 1^3, F_6 = 2^3$.*

Proof. There are numerous articles in the Fibonacci Quarterly journal concerning this fact, the first concrete result being [10]. A problem which is easily seen to be equivalent is to find the integer solutions of $Y^2 = 5X^6 \pm 4$, which is in fact what Siegel does in his paper [14]. □

Corollary 7.5. *The only solutions (x, y, m) to 56 satisfy $|x| \leq 2^3$ and all arise from an imaginary quadratic field of class number one. The complete list of solutions*

with $y > 0$ is

$$\begin{aligned}
(0,1,0) &\qquad (K = \mathbb{Q}(\sqrt{-3})) \\
(-1,2,0) &\qquad (K = \mathbb{Q}(\sqrt{-3})) \\
(-1,1,-15) &\qquad (K = \mathbb{Q}(\sqrt{-7})) \\
(1,0,20) &\qquad (K = \mathbb{Q}(\sqrt{-8})) \\
(1,1,255) &\qquad (K = \mathbb{Q}(\sqrt{-28})) \\
(1,2,-960) &\qquad (K = \mathbb{Q}(\sqrt{-43})) \\
(-8,5,-5280) &\qquad (K = \mathbb{Q}(\sqrt{-67})) \\
(8,13,-640320) &\qquad (K = \mathbb{Q}(\sqrt{-163})).
\end{aligned}$$

(To identify the imaginary quadratic order(s) corresponding to each solution, we made use of the list of $\mathbb{Q}$-rational j-invariants of elliptic curves with complex multiplication given in [3]*)*

References

[1] A.O.L. Aktin and H.P.F. Swinnerton-Dyer. Modular forms on noncongruence subgroups. In *Combinatorics (Univ. California, Los Angeles, Calif. 1968)*, volume XIX of *Proc. Sympos. Pure Math.*, pages 1–25, Providence, R.I., 1971. American Mathematical Society.

[2] I. Chen. *The Jacobian of Modular Curves Associated to Cartan Subgroups*. PhD thesis, University of Oxford, 1996.

[3] D.A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. John Wiley & Sons, Inc., 1989.

[4] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In P. Deligne and W. Kuyk, editors, *Modular Functions of One Variable II*, number 349 in Lecture Notes in Mathematics, pages 143–316. Springer-Verlag, 1972.

[5] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In P. Deligne and W. Kuyk, editors, *Modular Functions of One Variable II*, number 349 in Lecture Notes in Mathematics, pages 143–316. Springer-Verlag, 1972.

[6] B. Gross and D.B. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.

[7] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Number 108 in Annals of Mathematics Studies. Princeton University Press, 1985.

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

[9] S. Lang. *Elliptic functions*, volume 112 of *GTM*. Springer-Verlag, 1987.

[10] H. London and R. Finkelstein. On Fibonacci and Lucas numbers which are perfect powers. *Fibonacci quarterly*, 5:476–481, 1969.

[11] R.A. Rankin. *Modular forms and functions*. Cambridge University Press, 1977.

[12] J.P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15:259–331, 1972.

[13] J.P. Serre. *Lectures on the Mordell-Weil Theorem*. Number E15 in Aspects of Mathematics. Friedr, Vieweg & Sohn, Braunschweig, 1989.

[14] C.L. Siegel. Zum Beweise des Starkschen Satzes. *Inventiones Mathematicae*, 5:180–191, 1968.

Department of Mathematics and Statistics, McGill University, Montreal, Quebec, Canada, H3A 2K6

E-mail address: chen@math.mcgill.ca