Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Khashayar FILOM

The Belyi Characterization of a Class of Modular Curves

Tome 30, n° 2 (2018), p. 409-429.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_2_409_0>

Journal de Théorie des Nombres de Bordeaux **30** (2018), 409–429

The Belyi Characterization of a Class of Modular Curves

par Khashayar FILOM

Résumé. Une classe de courbes modulaires est caractérisée par l'existence de certains couples de fonctions de Belyi qui engendrent leurs corps des fonctions. Des applications à l'équation modulaire et au calcul de valeurs spéciales de la fonction j sont données.

Abstract. A class of modular curves is characterized by the existence of certain pairs of Belyi functions which generate their function fields. Applications to the modular equation and the computation of special values of the j-function are given.

1. Introduction

According to a theorem of Belyi, compact Riemann surfaces with models over $\bar{\mathbb{Q}}$ are precisely those admitting a non-trivial meromorphic function unramified outside of $\{0, 1, \infty\}$. Let $\mathbb{H}$ denote the upper half plane and $\Gamma(N)$ the principal congruence subgroup of level N. Realizing $\mathbb{C} - \{0, 1\}$ as $\Gamma(2)\backslash\mathbb{H}$, one deduces that curves defined over number fields contain Zariski open subsets that are uniformized by $\mathbb{H}$ modulo a finite index subgroup of $\Gamma(2)$. The main result of this note (Theorem 3.1) states that curves X admitting a pair of Belyi functions f and g with identical critical points, and generating the function field of X are precisely compactifications of curves of the form $\Gamma\backslash\mathbb{H}$ where $\Gamma = \Gamma(2) \cap \Gamma_0(2N)$. A partial extension of this result to the modular group $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ (replacing $\Gamma(2)$) is given in §4. This extension will be used to calculate (in principle) the modular equation for $X_0(N) = \Gamma_0(N)\backslash\mathbb{H}^*$ (Examples 4.3, 4.4 and 4.5) and certain special values of the j-function (see for example Corollary 4.6). An immediate generalization of our main theorem is to the case where the function field is generated by a number of Belyi functions with the same set of critical points. This is the content of Theorem 3.2. A straightforward argument establishes that all of the curves discussed in these two theorems can be defined over the rationals.

Manuscrit reçu le 22 août 2016, révisé le 4 novembre 2016, accepté le 2 décembre 2016.

2010 *Mathematics Subject Classification.* 14H57, 11F03, 14Q05.

Mots-clefs. dessins d'enfants, Belyi functions, modular curves, modular equation.

This work is part of author's Ph.D. thesis at Sharif University under co-advising of H. Fanai and M. Shahshahani.

The paper is organized as follows. In §2 the background material about Belyi functions on modular curves and two methods for their construction are discussed. The calculation of Belyi functions and dessins d'enfants for congruence subgroups appears in [3] and [5] in the particular case of dessins associated to torsion-free congruence subgroups of genus 0. In [7] cusp forms are utilized to embed modular curves in projective spaces and the defining equations of the curves are obtained by analyzing the q-expansions of these forms. In §3 the main result of the paper, Theorem 3.1, is proven. The fourth section is devoted to our primary example of a modular curve whose function field is generated by two Belyi functions, that is the modular curve $X_0(N)$ equipped with Belyi functions $[\tau] \mapsto \frac{1}{1728}j(\tau)$ and $[\tau] \mapsto \frac{1}{1728}j(N\tau)$. Having two Belyi functions in hand, comparing the corresponding dessins might reveal some new data and when they generate the function field, the algebraic dependence relation between them gives rise to equation of a plane curve whose normalization is our Riemann surface. For the sake of brevity, some details of calculations are omitted and the reader can consult [1] for a much lengthier treatment where other examples are also discussed.

We mainly follow notations of [6]: $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ denotes the upper half plane union cusps for $\Gamma(1)$ and Γ always indicates a finite index subgroup of $\Gamma(1)$. We denote the compact Riemann surface $\Gamma\backslash\mathbb{H}^*$ by $X(\Gamma)$. For $\Gamma = \Gamma(N)$ or $\Gamma_0(N)$, notations $X(N)$ and $X_0(N)$ are used instead. The point $\mathrm{e}^{\frac{\pi \mathrm{i}}{3}}$ of the upper half plane is denoted by ρ, and $[\tau]$ means the orbit of $\tau \in \mathbb{H}$ under the action of Γ and also the corresponding point in $X(\Gamma)$. Finally, $\bar{\Gamma}$ is the image of $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ in $\bar{\Gamma}(1) = \mathrm{PSL}_2(\mathbb{Z}) \subset \mathrm{Aut}(\mathbb{H})$, and we will work with Möbius transformations $T : \tau \mapsto \tau + 1$ and $S : \tau \mapsto \frac{-1}{\tau}$ (induced by $T = \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$) as a set of generators for $\mathrm{PSL}_2(\mathbb{Z})$.

2. Belyi Functions on Modular Curves

The purpose of this section is to discuss two ways for equipping modular curves with some natural Belyi functions. For a more comprehensive account of these two constructions and also more examples of them see §2, §3 in [1] where calculations have been carried out in full detail.

In the action of $\bar{\Gamma}(1)$ on $\mathbb{H}$, points with non-trivial stabilizer are exactly the elements of the orbits $\Gamma(1).\rho$ or $\Gamma(1).\mathrm{i}$ with stabilizers of orders three and two respectively. Thus branch values of the map $\Gamma\backslash\mathbb{H} \to \Gamma(1)\backslash\mathbb{H}$ are among $[\rho], [\mathrm{i}] \in \Gamma(1)\backslash\mathbb{H}$. Moreover, the point $[\tau] \in \Gamma\backslash\mathbb{H}$ where $\tau \in \Gamma(1).\rho$ (resp. $\tau \in \Gamma(1).\mathrm{i}$) is a ramification point of this map if and only if τ is not an elliptic point of Γ and in that case, the multiplicity of this point is three (resp. two). The only other ramification value that $\Gamma\backslash\mathbb{H}^* \to \Gamma(1)\backslash\mathbb{H}^*$ may possess is $[\infty]$ whose fiber is the set of orbits of cusps for Γ. Hence $\Gamma\backslash\mathbb{H}^* \to \Gamma(1)\backslash\mathbb{H}^*$ is a Belyi function if one identifies $X(1) = \Gamma(1)\backslash\mathbb{H}^*$ with $\mathbb{CP}^1$ in a way that the subset containing two elliptic orbits (points $[\rho], [\mathrm{i}] \in X(1)$) and one orbit of cusps (point $[\infty] \in X(1)$) bijects to $\{0, 1, \infty\}$. The multiple $\frac{1}{1728}j$ of the modular function $j : \mathbb{H} \to \mathbb{C}$ gives us such an identification since j has a simple pole at infinity and satisfies $j(\rho) = 0$ and $j(\mathrm{i}) = 1728$. Thus, for any Γ, the function $\frac{1}{1728}j : X(\Gamma) = \Gamma\backslash\mathbb{H}^* \to \mathbb{CP}^1$ is Belyi. The number of black or white vertices of the dessin associated with this Belyi function (that is, points of $f^{-1}(0)$ or $f^{-1}(1)$) is related to the number of inequivalent elliptic points of order three or two respectively. Let us denote these numbers by ν_3 and ν_2. There are also vertices corresponding to poles of the Belyi function which are marked by $\times$ in our pictures. They can be thought of as vertices located in centers of faces and the degree of such a vertex (the order of the pole that it represents) is half the number of edges of the corresponding face. The number of such vertices is the number of inequivalent cusps, denoted as ν_∞.

Proposition 2.1. *Notations as above, for a finite index subgroup* Γ *of* $\Gamma(1)$ *the function*

$$\begin{cases} f : X(\Gamma) = \Gamma\backslash\mathbb{H}^* \to \mathbb{CP}^1 \\ [\tau] \mapsto \frac{1}{1728}j(\tau) \end{cases}$$

is Belyi of degree $m := [\bar{\Gamma}(1) : \bar{\Gamma}]$. *In its dessin black (resp. white) vertices are* Γ*-orbits of points in* $\Gamma(1).\rho$ *(resp.* $\Gamma(1).\mathrm{i}$*) and centers of faces (*$\times$ *vertices) are orbits of cusps of* Γ. *The dessin has* ν_∞ *faces and among its black (resp. white) vertices, there are* $\frac{m-\nu_3}{3}$ *(resp.* $\frac{m-\nu_2}{2}$*) vertices of degree three (resp. two) and the rest, i.e.* ν_3 *(resp.* ν_2*) remaining black (resp. white) vertices, are all of degree one. Furthermore, the degree of a vertex* $[\tau]$ *of type* $\times$*, where* $\tau \in \mathbb{Q} \cup \{\infty\}$*, is the width of the cusp* τ *of* Γ.

For principal congruence subgroups $\Gamma(N)$ the Belyi function is a regular (or Galois or normal) ramified cover with $\bar{\Gamma}(1)/\bar{\Gamma} \cong \mathrm{PSL}_2(\mathbb{Z}_N)$ as its group of deck transformations. The corresponding dessin on $X(N)$ has many symmetries and exploiting them simplifies calculating this Belyi function as we shall see in the example below:

Example 2.2. For $N \geq 2$, $\Gamma(N)$ is torsion-free and hence according to Proposition 2.1, in the dessin on $X(N)$, $\bullet, \circ$ vertices are of degrees $3, 2$ respectively. Since $\Gamma(N) \trianglelefteq \Gamma(1)$ the width of any cusp (the degree of any $\times$ vertex) is the same as the width of the cusp ∞ for $\Gamma(N)$ which is N. There are $\mu_N := \left[\bar{\Gamma}(1) : \bar{\Gamma}(N)\right]$ edges along with $\frac{\mu_N}{3}$ black vertices of degree three, $\frac{\mu_N}{2}$ white vertices of degree two, and $\frac{\mu_N}{N}$ faces each with $2N$ edges. Computing the Euler characteristics yields the number $1 + \frac{N-6}{12N}\mu_N$ for the genus of $X(N)$.

For $N=2$, $\mu_2=6$ and the corresponding dessin on the sphere is displayed in Figure 2.1 whose Belyi function is

$$f(z)=\frac{4}{27}\frac{(z^2-z+1)^3}{(z^2-z)^2},\quad f(z)-1=\frac{4}{27}\frac{(z+1)^2(z-2)^2(z-\frac{1}{2})^2}{(z^2-z)^2}, \tag{2.1}$$

while when $N=3$, $\mu_3=12$ and the Belyi function is

$$f(z)=\frac{1}{64}\frac{z^3(z^3+8)^3}{(z^3-1)^3},\quad f(z)-1=\frac{1}{64}\frac{(z^6-20z^3-8)^2}{(z^3-1)^3}, \tag{2.2}$$

and the genus zero dessin is illustrated in Figure 2.2.[1] Both modular curves $X(2)$ and $X(3)$ are of genus zero and thus, as in (2.1) and (2.2), can be equipped with complex coordinates z which of course are modular functions for subgroups $\Gamma(2)$ and $\Gamma(3)$ respectively, cf. Remark 2.3.

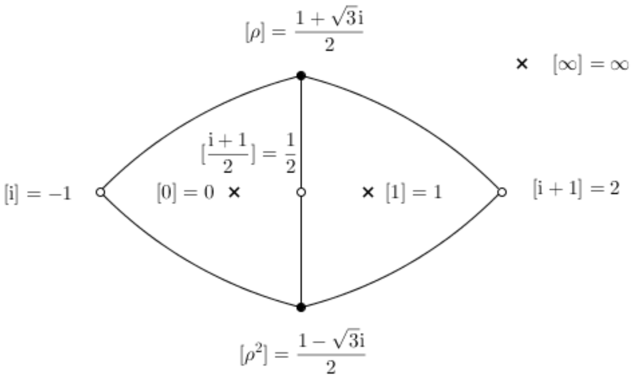

FIGURE 2.1. The dessin on $X(2)$.

The symmetries have been employed to obtain these dessins. In the case of $N=2$, the deck group $\mathrm{Deck}(f:\mathbb{CP}^1\to\mathbb{CP}^1)\cong\bar{\Gamma}(1)/\bar{\Gamma}(2)$ is isomorphic to S_3 via a map which takes cosets of S and T to transpositions. In Figure 2.1 vertices $[0],[1],[\infty]$ corresponding to cusps are fixed at the beginning and then transformations induced by S and T amount to automorphisms $z\mapsto\frac{1}{z}$ and $z\mapsto 1-z$ of the meromorphic function in (2.1). In the dessin on $X(3)\cong\mathbb{CP}^1$ in Figure 2.2, the deck transformation group $\bar{\Gamma}(1)/\bar{\Gamma}(3)$ is a version of the alternating group A_4 such that cosets of T and S correspond to a 3-cycle and a product of two disjoint transpositions in A_4, respectively. The dessin is drawn in a way that T is the 120° rotation about the origin whose fixed points are 0 and ∞, representing orbits $\left[\frac{2\rho-5}{\rho-2}\right]$ and $[\infty]$ respectively.

[1] In Proposition 2.1 edges of the dessin can be described as $\{[\gamma.\mathrm{e}^{\mathrm{i}\theta}]\mid\frac{\pi}{3}\leq\theta\leq\frac{\pi}{2},\gamma\in\mathrm{SL}_2(\mathbb{Z})\}$. For a torsion-free Γ there is a general method discussed in [3] for drawing the underlying graph of the dessin by relating it to the *Schreier coset graph* associated with the subgroup Γ of $\mathrm{PSL}_2(\mathbb{Z})$.

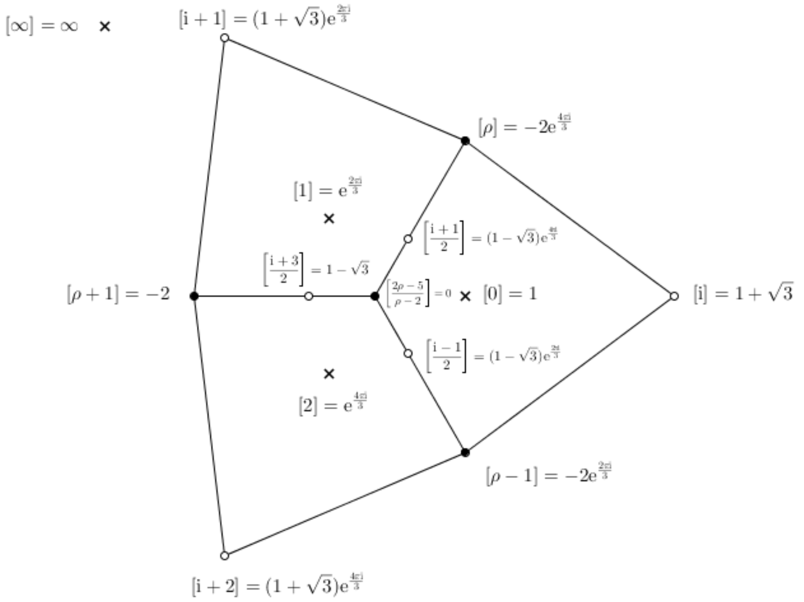

FIGURE 2.2. The dessin on $X(3)$.

Remark 2.3. The fact that $X(2)$ is of genus zero amounts to the existence of a modular function λ for $\Gamma(2)$ which identifies $X(2)$ with $\mathbb{CP}^1$ (a Hauptmodul) via inducing an isomorphism $\Gamma(2)\backslash\mathbb{H} \to \mathbb{C} - \{0,1\}$ that at cusps takes values $\lambda([0]) = 0, \lambda([1]) = 1, \lambda([\infty]) = \infty$. Then the Belyi function f in (2.1), that we will denote as $\alpha : \mathbb{CP}^1 \to \mathbb{CP}^1$ hereafter, is a degree six map which satisfies $\frac{1}{1728}j(\tau) = \alpha(\lambda(\tau))$ for any $\tau \in \mathbb{H}$. Interpreting $\Gamma(2)\backslash\mathbb{H}$ as the moduli space of elliptic curves in a Legendre form $y^2 = x(x-1)(x-\lambda)$ and $\Gamma(1)\backslash\mathbb{H}$ as the moduli space of elliptic curves, 1728α is just the description of the j-invariant in terms of the Legendre form. Our discussion on the deck transformation group of α in Example 2.2 translates to $\lambda(\frac{-1}{\tau}) = \frac{1}{\lambda(\tau)}$, $\lambda(\tau+1) = 1-\lambda(\tau)$. Hence applying an element of $\Gamma(1)$ to τ alters $\lambda(\tau)$ only up to the action of S_3 on $\mathbb{C} - \{0,1\}$ generated by $\lambda \mapsto 1-\lambda$, $\lambda \mapsto \frac{1}{\lambda}$.[2] These Möbius transformations generate the classical *anharmonic group*

Next, we propose a second method for constructing Belyi functions in which the monodromy representations are easy to describe. Let Γ be a finite index subgroup of $\Gamma(2)$. Here is the key point: there is not any elliptic point

[2]An alternative elementary method to derive the formula $j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{(\lambda^2-\lambda)^2}$ for the j-invariant of $y^2 = x(x-1)(x-\lambda)$ is to note that this is the unique degree 6 element of $\mathbb{C}(\lambda)$ invariant under $\lambda \mapsto 1-\lambda$, $\lambda \mapsto \frac{1}{\lambda}$ whose values at $\lambda = \mathrm{e}^{\frac{\pi\mathrm{i}}{3}}$ (the hexagonal elliptic curve) and $\lambda = -1$ (the square elliptic curve) are 0, 1728 respectively.

for $\Gamma(2)$ but there are exactly three inequivalent cusps:

$$[0]=\left\{\frac{a}{b}\,\middle|\,a\,\text{even},b\,\text{odd}\right\},\quad [1]=\left\{\frac{a}{b}\,\middle|\,a\,\text{odd},b\,\text{odd}\right\},$$
$$[\infty]=\left\{\frac{a}{b}\,\middle|\,a\,\text{odd},b\,\text{even}\right\}\cup\{\infty\}. \tag{2.3}$$

Fixing the identification of $X(2)=\Gamma(2)\backslash\mathbb{H}^*$ with $\mathbb{CP}^1$ in Figure 2.1, these orbits correspond to $0,1,\infty$ and so the quotient map $\mathbb{H}\to\Gamma(2)\backslash\mathbb{H}$ realizes the upper half plane $\mathbb{H}$ as the universal cover of $\mathbb{C}-\{0,1\}$, the space which is identified with $\Gamma(2)\backslash\mathbb{H}$ via the modular function λ of level 2 introduced in Remark 2.3. Then, for any finite index subgroup Γ of $\Gamma(2)$, the obvious map $X(\Gamma)=\Gamma\backslash\mathbb{H}^*\to X(2)=\Gamma(2)\backslash\mathbb{H}^*\cong\mathbb{CP}^1$ of degree $[\bar{\Gamma}(2):\bar{\Gamma}]$ may be assumed to be Belyi. The main advantage of working with this Belyi function rather than $X(\Gamma)\to X(1)\cong\mathbb{CP}^1$ introduced before, besides having lower degree that eases computations, is that the monodromy homomorphism of $X(\Gamma)\to X(2)\cong\mathbb{CP}^1$, which specifies the isomorphism class of the Belyi function, has a simple description in terms of the subgroup Γ because unlike the map $\mathbb{H}\to\Gamma(1)\backslash\mathbb{H}$, which is ramified, here $\mathbb{H}\to\Gamma(2)\backslash\mathbb{H}\cong\mathbb{C}-\{0,1\}$ is the universal covering map and it suffices to determine the monodromy around three punctures $[0]=0$, $[1]=1$ and $[\infty]=\infty$. Identifying $\bar{\Gamma}(2)$ with the free group on two generators $\pi_1(\mathbb{C}-\{0,1\})$ such that T^2 and ST^2S^{-1} correspond to homotopy classes of small counterclockwise loops around ∞ and 0 respectively (which is consistent with the identification of $\pi_1(\mathbb{C}-\{0,1\})$ with $\mathrm{Deck}(\mathbb{H}\to\Gamma(2)\backslash\mathbb{H})\cong\bar{\Gamma}(2)$), one gets, following notations of [2], σ_0, σ_∞ in the permutation representation $(\sigma_0,\sigma_1,\sigma_\infty)$ of this Belyi function.

Proposition 2.4. *Let Γ be a finite index subgroup of $\Gamma(2)$. Then the obvious map*

$$\begin{cases} f: X(\Gamma)=\Gamma\backslash\mathbb{H}^*\to X(2)=\Gamma(2)\backslash\mathbb{H}^*\overset{\cong}{\to}\mathbb{CP}^1\\ [\tau]\mapsto\lambda(\tau)\end{cases}$$

where $X(2)$ is identified with $\mathbb{CP}^1$ in the way that $[0]\mapsto 0$, $[1]\mapsto 1$ and $[\infty]\mapsto\infty$, is a Belyi function of degree $m:=[\bar{\Gamma}(2):\bar{\Gamma}]$. In its dessin black vertices, white vertices and vertices corresponding to faces are Γ-orbits of points in $\Gamma(2).0$, $\Gamma(2).1$ and $\Gamma(2).\infty$ respectively. The number of edges is m and the degree of a vertex $[\tau]\in X(\Gamma)$ is half the width of the cusp $\tau\in\mathbb{Q}\cup\{\infty\}$ of Γ. Moreover, the monodromy is specified by two permutations of the set of right cosets of $\bar{\Gamma}$ in $\bar{\Gamma}(2)$ induced by the right actions of T^2 and ST^2S^{-1}.

Remark 2.5. For Belyi functions $\Gamma\backslash\mathbb{H}^*\to\Gamma(1)\backslash\mathbb{H}^*\overset{\frac{1}{1728}j}{\cong}\mathbb{CP}^1$, introduced in Proposition 2.1, the monodromy representation has a more subtle description because $\mathbb{H}\to\Gamma(1)\backslash\mathbb{H}$ is ramified. After removing critical fibers to obtain the unramified cover

$$\Gamma\backslash\left(\mathbb{H}-\Gamma(1).\{\mathrm{i},\rho\}\right)\rightarrow\Gamma(1)\backslash\left(\mathbb{H}-\Gamma(1).\{\mathrm{i},\rho\}\right)\overset{\frac{1}{1728}j}{\cong}\mathbb{C}-\{0,1\}$$

and then switching to the identification of $\mathbb{C}-\{0,1\}$ with $\Gamma(2)\backslash\mathbb{H}$ through λ, one has to study the monodromy of the unramified cover

$$\Gamma\backslash\left(\mathbb{H}-\Gamma(1).\{\mathrm{i},\rho\}\right)\rightarrow\Gamma(2)\backslash\mathbb{H}:[\tau]\mapsto\left[\lambda^{-1}\left(\frac{1}{1728}j(\tau)\right)\right].$$

Since $\frac{1}{1728}j=\alpha\circ\lambda$, for two continuous curves $t\mapsto\gamma(t)$ and $t\mapsto\tilde{\gamma}(t)$ in $\mathbb{H}$, $t\mapsto[\gamma(t)]$ lifts to $t\mapsto[\tilde{\gamma}(t)]$ in the preceding unramified cover if and only if $\alpha(\lambda(\tilde{\gamma}(t)))=\lambda(\gamma(t))$. Thus everything boils down to the monodromy of α which was analyzed in Example 2.2 : in the regular ramified covering $\alpha:\mathbb{CP}^1\rightarrow\mathbb{CP}^1$ the deck transformations group is generated by Möbius transformations $z\mapsto 1-z$ and $z\mapsto\frac{1}{z}$ induced respectively by actions of T and S on $\Gamma(2)\backslash\mathbb{H}^*\cong\mathbb{CP}^1$. The action of $\pi_1(\mathbb{C}-\{0,1\},z_0)$ on a regular fiber $\alpha^{-1}(z_0)$ translates to the action of $\mathrm{Deck}(\alpha:\mathbb{CP}^1\rightarrow\mathbb{CP}^1)$ on this fiber once we identify $\mathrm{Deck}(\alpha:\mathbb{CP}^1\rightarrow\mathbb{CP}^1)$ with a quotient of $\pi_1(\mathbb{C}-\{0,1\},z_0)$ in the obvious way. Hence, having in mind the identification of $\pi_1(\mathbb{C}-\{0,1\})$ with $\bar{\Gamma}(2)$ as before, for any finite index subgroup Γ of $\Gamma(1)$ the ramified cover $\Gamma\backslash\mathbb{H}^*\rightarrow\Gamma(1)\backslash\mathbb{H}^*\cong\mathbb{CP}^1$ is isomorphic with $\Gamma'\backslash\mathbb{H}^*\rightarrow\Gamma(2)\backslash\mathbb{H}^*\cong\mathbb{CP}^1$ where Γ' is the stabilizer of the trivial coset in the action $\Gamma(2)$ on the set of right cosets of $\bar{\Gamma}$ in $\bar{\Gamma}(1)$ where the actions of T^2 and ST^2S^{-1} are by right multiplication at T and S (or any two other generator of $\bar{\Gamma}(1)$). Now Proposition 2.4 determines the monodromy representation of the previous covering and hence that of the original one $\Gamma\backslash\mathbb{H}^*\rightarrow\Gamma(1)\backslash\mathbb{H}^*$.[3]

3. Function Fields Generated by Two Belyi Functions

We now discuss our main theorem concerning a certain class of curves over $\bar{\mathbb{Q}}$.

Theorem 3.1. *Let X be a compact Riemann surface and f,g two Belyi functions on X with $f^{-1}(\{0,1,\infty\})=g^{-1}(\{0,1,\infty\})$ that generate the function field. Then there is an isomorphism $X\cong X(\Gamma)$ where $\Gamma=\Gamma(2)\cap\Gamma_0(2N)$ for some $N\in\mathbb{N}$ in which Belyi functions f and g, after possibly modifying them with an element of anharmonic group (cf. Remark 2.3), can be identified with $f:[\tau]\mapsto\lambda(\tau)$ (the Belyi function introduced in Proposition 2.4) and $g:[\tau]\mapsto\lambda(N\tau)$. Conversely, for any such subgroup*

[3]More generally, given (not necessarily torsion-free) Fuchsian groups $\Gamma_1<\Gamma$, in the ramified cover $\Gamma_1\backslash\mathbb{H}\rightarrow\Gamma\backslash\mathbb{H}$ the monodromy action of an element γ of Γ on a generic fiber identified with the set of right cosets of $\bar{\Gamma}_1$ in $\bar{\Gamma}$ is the obvious action of γ on the set of cosets, cf. [2, pp. 151, 232].

Γ *of* $\Gamma(2)$*, functions* $[\tau] \mapsto \lambda(\tau)$*,* $[\tau] \mapsto \lambda(N\tau)$ *on* $X(\Gamma)$ *are Belyi and generate its function field. Moreover, any such curve can be defined over the rationals.*

Proof. By identifying $\mathbb{C} - \{0,1\}$ with $\Gamma(2)\backslash\mathbb{H}$ just as before, there is a finite index subgroup Γ of $\Gamma(2)$ which uniformizes a Zariski open subset of X via $f : X \to \mathbb{CP}^1$. This implies that X is just $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$ and f is the natural map $X(\Gamma) \to X(2) \cong \mathbb{CP}^1$. But the same is true for $g : X \to \mathbb{CP}^1$ which yields the similar description $X(\Gamma') \to X(2) \cong \mathbb{CP}^1$ of this Belyi function for another finite index subgroup Γ'. Removing cusps, i.e. points in the fibers of f and g above $0, 1, \infty$, these functions restrict to unramified covers $\Gamma\backslash\mathbb{H} \to \Gamma(2)\backslash\mathbb{H}$ and $\Gamma'\backslash\mathbb{H} \to \Gamma(2)\backslash\mathbb{H}$. Hence $\Gamma\backslash\mathbb{H}$ and $\Gamma'\backslash\mathbb{H}$ are both isomorphic to this punctured surface obtained from X. But any isomorphism $\Gamma\backslash\mathbb{H} \to \Gamma'\backslash\mathbb{H}$ must be of the form $[\tau] \mapsto [u(\tau)]$ where $u \in \mathrm{GL}_2^+(\mathbb{R})$ due to the fact that $\mathrm{Aut}(\mathbb{H}) = \mathrm{PSL}_2(\mathbb{R})$. In order for this isomorphism to be well-defined, one should have $\Gamma' = u\Gamma u^{-1}$. Thus Γ is also contained in $u^{-1}\Gamma(2)u$. The group $\Gamma(2) \cap u^{-1}\Gamma(2)u$ coincides with its subgroup Γ: it just suffices to note that Belyi functions $f : [\tau] \mapsto \lambda(\tau)$ and $g : [\tau] \mapsto \lambda(u(\tau))$ on $X = X(\Gamma)$ actually can be defined on the curve $X(\Gamma(2) \cap u^{-1}\Gamma(2)u)$ corresponding to the bigger subgroup $\Gamma(2) \cap u^{-1}\Gamma(2)u$. But the function field of this curve is included in $\mathbb{C}(X) = \mathbb{C}(f, g)$. We conclude that there is an equality of the function fields and hence these subgroups of $\Gamma(2)$ are the same.

On the other hand, for any such Γ, functions f, g are Belyi. For f this is the content of Proposition 2.4 and for g this is due to the fact that $\Gamma\backslash\mathbb{H} \overset{\cong}{\to} \Gamma'\backslash\mathbb{H} \to \Gamma(2)\backslash\mathbb{H} \overset{\lambda}{\cong} \mathbb{C} - \{0,1\} : [\tau] \mapsto [u(\tau)]$ is unramified. Moreover, $\mathbb{C}(X(\Gamma)) = \mathbb{C}(f, g)$: the inclusion $\mathbb{C}(f, g) \hookrightarrow \mathbb{C}(X(\Gamma))$ defines a morphism $\beta : X(\Gamma) \to Y$ such that f, g descend to meromorphic functions on Y. After removing cusps from $X(\Gamma)$, f restricts to the unramified cover $\Gamma\backslash\mathbb{H} \to \Gamma(2)\backslash\mathbb{H}$. Hence by removing finitely many point from Y, we get a punctured surface isomorphic to $\tilde{\Gamma}\backslash\mathbb{H}$ for some suitable $\tilde{\Gamma}$ between Γ and $\Gamma(2)$ such that β is isomorphic with $\Gamma\backslash\mathbb{H} \to \tilde{\Gamma}\backslash\mathbb{H}$. But the function g induced by $[\tau] \mapsto [u(\tau)] \in \Gamma(2)\backslash\mathbb{H}$ must descend to a well-defined function on $\tilde{\Gamma}\backslash\mathbb{H}$ which is the case if and only if $\tilde{\Gamma}$ is contained in $u^{-1}\Gamma(2)u$ or equivalently $\tilde{\Gamma} = \Gamma$.

Next, we claim that up to a scalar multiple, elements u of $\mathrm{GL}_2^+(\mathbb{R})$ with $[\Gamma(2) : \Gamma(2) \cap u^{-1}\Gamma(2)u] < \infty$ are precisely integer matrices with positive determinant (that is to say, the *commensurator* of $\mathrm{PSL}_2(\mathbb{Z})$ in $\mathrm{PGL}_2^+(\mathbb{R})$ is the image of $\mathrm{GL}_2^+(\mathbb{Z})$). For any integer 2×2 matrix of determinant $M > 0$: $u\Gamma(2M)u^{-1} \subseteq \Gamma(2)$ and thus $\Gamma(2) \cap u^{-1}\Gamma(2)u$ contains the finite index subgroup $\Gamma(2M)$. One the other hand, if the index of $\Gamma(2) \cap u^{-1}\Gamma(2)u$ in $\Gamma(2)$ is finite, $\Gamma(2) \cap u^{-1}\Gamma(2)u$ must have elements in the form of $\left[\begin{smallmatrix} 1 & 2M \\ 0 & 1 \end{smallmatrix}\right]$

and $\left[\begin{smallmatrix}1 & 0\\ 2M & 1\end{smallmatrix}\right]$ for some suitable $M \in \mathbb{N}$. So $u\left[\begin{smallmatrix}1 & 2M\\ 0 & 1\end{smallmatrix}\right]u^{-1}$ and $u\left[\begin{smallmatrix}1 & 0\\ 2M & 1\end{smallmatrix}\right]u^{-1}$ lie in $\Gamma(2)$. Changing u by a scalar does not change the subgroup. Hence we may suppose $\det(u) = 1$. Writing u in the form of $\left[\begin{smallmatrix}x & y\\ z & w\end{smallmatrix}\right]$ where $xw - yz = 1$, we have:

$$u\begin{bmatrix}1 & 2M\\ 0 & 1\end{bmatrix}u^{-1} = \begin{bmatrix}1-2xzM & 2x^2M\\ -2z^2M & 1+2xzM\end{bmatrix};$$
$$u\begin{bmatrix}1 & 0\\ 2M & 1\end{bmatrix}u^{-1} = \begin{bmatrix}1+2ywM & -2y^2M\\ 2w^2M & 1-2ywM\end{bmatrix}.$$

The fact that the first matrix belongs to $\Gamma(2)$ indicates that x^2M, xzM, z^2M are integers. Therefore, denoting $\gcd(x^2M, z^2M)$ by k, real numbers x and z may be described respectively as $\alpha\sqrt{\frac{k}{M}}$ and $\gamma\sqrt{\frac{k}{M}}$ for suitable coprime integers α, γ. Similarly, since the second matrix above is again an element of $\Gamma(2)$, there are integers β, δ with $y = \beta\sqrt{\frac{k'}{M}}$ and $w = \delta\sqrt{\frac{k'}{M}}$. In conclusion, u must be in the form of

$$\begin{bmatrix}\alpha\sqrt{\frac{k}{M}} & \beta\sqrt{\frac{k'}{M}}\\ \gamma\sqrt{\frac{k}{M}} & \delta\sqrt{\frac{k'}{M}}\end{bmatrix}$$

with $\alpha, \beta, \gamma, \delta, k, k', M \in \mathbb{Z}$, $M, k, k' > 0$ and $\alpha\delta - \beta\gamma = \frac{M}{\sqrt{kk'}}$. Consequently, kk' is a perfect square and now multiplying at the scalar $\sqrt{Mk}$ transforms u to an integer matrix. The claim is proved.

Using the well-known Smith normal form, an integer matrix u of determinant $M > 0$ can be written as $v\left[\begin{smallmatrix}a & 0\\ 0 & d\end{smallmatrix}\right]w^{-1}$ with $v, w \in \mathrm{SL}_2(\mathbb{Z})$ and a, d positive integers with $d \mid a$, $ad = M$. Denoting $\frac{a}{d}$ by N, we have:

$$\begin{aligned}\Gamma(2) \cap u^{-1}\Gamma(2)u &= w\left(\Gamma(2) \cap \left(\begin{bmatrix}N & 0\\ 0 & 1\end{bmatrix}^{-1}\Gamma(2)\begin{bmatrix}N & 0\\ 0 & 1\end{bmatrix}\right)\right)w^{-1}\\ &= w\left(\Gamma(2) \cap \Gamma_0(2N)\right)w^{-1}.\end{aligned}$$

Therefore, applying the isomorphism

$$X = X(\Gamma) \xrightarrow{\cong} X(\Gamma(2) \cap \Gamma_0(2N)) : [\tau] \mapsto \left[w^{-1}(\tau)\right]$$

converts $f : [\tau] \mapsto \lambda(\tau)$ and $g : [\tau] \mapsto \lambda(u(\tau))$ to $f : [\tau] \mapsto \lambda(w(\tau))$ and $g : [\tau] \mapsto \lambda(u(w(\tau))) = \lambda(v(N\tau))$, respectively. Moreover, according to Remark 2.3, the elements v, w of $\mathrm{SL}_2(\mathbb{Z})$ change λ through composing it with an element of the anharmonic group.

For the last part, it suffices to show that the minimal polynomial of $\lambda(N\tau)$ over the field $\mathbb{C}(\lambda(\tau))$ is with rational coefficients. In a neighborhood of ∞ the modular function $\tau \mapsto \lambda(\tau)$ for $\Gamma(2)$ has a Laurent series expansion in terms of $q^{\frac{1}{2}} = \mathrm{e}^{\pi \mathrm{i}\tau}$ with rational coefficients. Hence the same is true for $\tau \mapsto \lambda(N\tau)$ as ∞ is a fixed point of $\tau \mapsto N\tau$. Now plugging these Laurent series of $q^{\frac{1}{2}}$ in the minimal polynomial indicates that coefficients of this polynomial are solution to a linear system with rational coefficients. The solution is unique as the minimal polynomial is unique and therefore it also lies in $\mathbb{Q}$. □

Arguments used in this proof immediately establish the following generalization to the case of more than two Belyi functions. Consider all $(k+1)$-tuples $(X, f_1, f_2, \ldots, f_k)$ where X is a compact Riemann surface, functions $f_i : X \to \mathbb{CP}^1$ $(1 \leq i \leq k)$ are Belyi with subsets $f_i^{-1}(\{0, 1, \infty\})$ identical and moreover $\mathbb{C}(f_1, \ldots, f_k) = \mathbb{C}(X)$.

Theorem 3.2. *Notations as above, such $(k+1)$-tuples can be classified up to isomorphism as $(X(\Gamma), [\tau] \mapsto \lambda(\tau), [\tau] \mapsto \lambda(u_2(\tau)), \ldots, [\tau] \mapsto \lambda(u_k(\tau)))$ where u_i's $(2 \leq i \leq k)$ are integer matrices of positive determinants, Γ is the finite index subgroup $\Gamma = \Gamma(2) \cap u_2^{-1}\Gamma(2)u_2 \cap \cdots \cap u_k^{-1}\Gamma(2)u_k$ of $\Gamma(2)$ and λ is the Hauptmodul for $\Gamma(2)$ that we fixed in Remark 2.3. Furthermore, any such Riemann surface X has a model over $\mathbb{Q}$.*

Proof. We only need to use what established in the proof of Theorem 3.1. There are finite index subgroups $\Gamma_1, \ldots, \Gamma_k$ of $\Gamma(2)$ such that $f_i : X \to \mathbb{CP}^1$ is isomorphic with $[\tau] \in X(\Gamma_i) = \Gamma_i \backslash \mathbb{H}^* \to \mathbb{CP}^1 : [\tau] \mapsto \lambda(\tau)$. For any $2 \leq i \leq k$ there is a $u_i \in \mathrm{SL}_2(\mathbb{R})$ which defines an isomorphism $X(\Gamma_1) \to X(\Gamma_i) : [\tau] \mapsto [u_i(\tau)]$ so the function $\tau \mapsto \lambda(u_i(\tau))$ is modular for Γ_1. This finite index subgroup of $\Gamma(2)$ thus is contained in $\Gamma(2) \cap u_i^{-1}\Gamma(2)u_i$. The preceding subgroup of $\Gamma(2)$ is of finite index if and only if u_i is a scalar multiple of an integer matrix of positive determinant. Since functions $f_1 : [\tau] \mapsto \lambda(\tau)$, $f_i : [\tau] \mapsto \lambda(u_i(\tau))$ $(2 \leq i \leq k)$ generate the function field of $X = X(\Gamma_1)$, Γ_1 must coincide with the larger group $\Gamma := \Gamma(2) \cap u_2^{-1}\Gamma(2)u_2 \cap \cdots \cap u_k^{-1}\Gamma(2)u_k$ because this is the largest subgroup of $\Gamma(2)$ for which all functions $\tau \mapsto \lambda(\tau)$, $\tau \mapsto \lambda(u_i(\tau))$ $(2 \leq i \leq k)$ are modular. Finally, note that there is a rational map $X = X(\Gamma) \dashrightarrow \mathbb{C}^k : [\tau] \mapsto (\lambda(\tau), \lambda(u_2(\tau)), \ldots, \lambda(u_k(\tau)))$ which away from cusps provides us with an embedding $X^* := \Gamma \backslash \mathbb{H} \hookrightarrow \mathbb{C}^k$. Any two components $\lambda(u_i(\tau))$ and $\lambda(u_j(\tau))$ $(1 \leq i, j \leq k$ distinct and $u_1 := I_2)$ satisfy an equation which is the algebraic dependence relation between $\lambda(\tau)$ and $\lambda(u_i u_j^{-1}(\tau))$. This is over $\mathbb{Q}$ because after multiplying $u_i u_j^{-1}$ at some suitable integer the result will be an integer matrix of positive determinant which, invoking Smith normal form, can be descibed as $v\left[\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right]w^{-1}$ where $v, w \in \mathrm{SL}_2(\mathbb{Z})$ and $a, d \in \mathbb{N}$ satisfy $d \mid a$. Then, denoting $\frac{a}{d}$ by $N \in \mathbb{N}$ and replacing τ in $\lambda(\tau)$ and $\lambda(u_i u_j^{-1}(\tau))$ with $w(\tau)$, we end up with the algebraic dependence relation between two functions which up to the action of anharmonic group are the same as $\lambda(\tau)$, $\lambda(N\tau)$ and now the q-expansion argument from the end of the proof of Theorem 3.1 indicates that this algebraic dependence is in fact over $\mathbb{Q}$. The equations over $\mathbb{Q}$ that functions

$\lambda(u_i(\tau))$, $\lambda(u_j(\tau))$ $(1 \leq i < j \leq k)$ satisfy define an affine algebraic curve in $\mathbb{C}^k$ birational to X. Hence X has a model over the rationals. □

Remark 3.3. In some sense the algebraic dependence between $\lambda(\tau), \lambda(N\tau)$ is the prototype of any algebraic relation that a function, modular for a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and its twist with an automorphism may satisfy. Rigorously speaking, let f be a non-constant modular function for the finite index subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, $\Phi(X, Y)$ a polynomial without multiple factors and $u \in \mathrm{PSL}_2(\mathbb{R})$ an automorphism of the upper half plane $\mathbb{H}$ such that $\Phi(f(\tau), f(u(\tau))) = 0$ for all $\tau \in \mathbb{H}$. When τ varies in a small enough neighborhood of a generic point of $\mathbb{H}$, it is possible to express $f(u(\tau))$ in terms of $f(\tau)$ as functions $\alpha_i(f(\tau))\, 1 \leq i \leq m$ where $m := \deg_Y \Phi$ and α_i's are holomorphic. There is a right action of Γ on these branches in which $\gamma \in \Gamma$ maps $f(u(\tau))$ to $f(u(\gamma(\tau)))$. We conclude that $f \circ u$ is modular for the finite index subgroup Γ' of Γ which is defined to be the kernel of the homomorphism $\Gamma \to \mathrm{S}_m$ arising from this action. Hence f is invariant under the action of the subgroup $u\Gamma' u^{-1}$ of $\mathrm{SL}_2(\mathbb{R})$ too. We claim that u is in the commensurator of $\bar{\Gamma}(1)$ in $\mathrm{PSL}_2(\mathbb{R})$ or equivalently (keeping in mind that $[\Gamma(1) : \Gamma'] < \infty$) $[\Gamma' : u^{-1}\Gamma(1)u \cap \Gamma'] < \infty$. Otherwise, there are infinitely many elements $\{w_i\}_{i\in\mathbb{N}}$ of $u\Gamma' u^{-1}$ such that $w_i w_j^{-1} \notin \Gamma(1)$ for $i \neq j$. Pick a point τ_0 of the upper half plane which is not fixed by any of countably many matrices in the subset $\bigcup_{i,j\in\mathbb{N}, i\neq j} w_i^{-1}\Gamma(1)w_j$ of $\mathrm{SL}_2(\mathbb{R}) - \{\pm I_2\}$. This implies that the orbits of points $w_i(\tau_0)$ comprise an infinite subset of the compact Riemann surface $X(\Gamma')$. But the non-trivial meromorphic function induced by f on $X(\Gamma')$ restricts to the constant function of value $f(\tau_0)$ on this subset since f is invariant under elements w_i of $u\Gamma' u^{-1}$. This contradiction establishes our claim. Now our discussion in the proof of Theorem 3.1 on the commensurator of $\bar{\Gamma}(1) = \mathrm{PSL}_2(\mathbb{Z})$ in $\mathrm{PGL}_2^+(\mathbb{R})$ combined with the existence of Smith normal form shows that u up to a scalar multiple is of the form $v\left[\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right]w^{-1}$ where $v, w \in \Gamma(1)$. Therefore, one can think of $\Phi(X, Y)$ as a polynomial relation between functions $\tau \mapsto f(w(\tau))$ and $\tau \mapsto f(v(N\tau))$ which are modular for a suitable finite index subgroup of the original group Γ. It might be possible to turn this into a polynomial equation in the form of $\tilde{\Phi}(f(\tau), f(N\tau)) = 0$ after a change of coordinates in the (X, Y)-plane. This is the case when $\Gamma'' := \{\gamma'' \in \Gamma(1) \mid f \circ \gamma'' = f\} \trianglelefteq \Gamma(1)$ so the function field $\mathbb{C}(f)$ is invariant under the right action of $\Gamma(1)$ which indicates that in the equation $\Phi(f(w(\tau)), f(v(N\tau))) = 0$ one can replace $f(w(\tau))$ and $f(v(N\tau))$ with functions of the form $\tau \mapsto \frac{af(\tau)+b}{cf(\tau)+d}$ and $\tau \mapsto \frac{a'f(N\tau)+b'}{c'f(N\tau)+d'}$. Then, by substituting X with $\frac{aX+bY}{cX+dY}$ and Y with $\frac{a'X+b'Y}{c'X+d'Y}$ in $\Phi(X, Y)$ and multiplying at a sufficiently large power of $(cX + dY)(c'X + d'Y)$ we get a non-zero polynomial $\tilde{\Phi}(X, Y)$ for which $\tilde{\Phi}(f(\tau), f(N\tau)) = 0$. Two examples of this situation are $f = \lambda, \Gamma'' = \Gamma(2)$, i.e. what mentioned in Theorem 3.1, and $f = j, \Gamma'' = \Gamma(1)$ which is the case of modular equations that we are going to study in the next section.

4. Dessins on $X_0(N)$ and Modular Equation

In this section we turn to a class of compact Riemann surfaces where the function field can be generated by two Belyi functions. It is well-known that $\tau \mapsto j(\tau)$ and $\tau \mapsto j(N\tau)$ are $\Gamma_0(N)$-invariant and generate the function field of $X_0(N)$. The minimal polynomial of $j(N\tau)$ over $\mathbb{C}(j(\tau))$ is the so called *modular equation.* Aside from the Belyi function $f : X_0(N) = \Gamma_0(N)\backslash\mathbb{H}^* \to X(1) = \Gamma(1)\backslash\mathbb{H}^* \cong \mathbb{CP}^1$ in Proposition 2.1, which is nothing but $\frac{1}{1728}j$, the modular function $g : X_0(N) \to \mathbb{CP}^1$ defined as $[\tau] \mapsto \frac{1}{1728}j(N\tau)$ is Belyi too. Hence $\mathbb{C}(X_0(N))$ coincides with the subfield $\mathbb{C}(f, g)$ generated by two Belyi functions.

It must be mentioned that the situation is slightly different from that of Theorem 3.1 in the sense that dessins of f and g need not to have the same set of vertices, one can only say that the vertices of type $\times$ at the centers of faces are the same, i.e. $f^{-1}(\infty) = g^{-1}(\infty)$ which is the set of cusp orbits for $\Gamma_0(N)$. But there are similarities: $\Gamma_0(N)$ can be written in the form of $\Gamma(1) \cap u^{-1}\Gamma(1)u$ where u is either $\left[\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right]$ or $\left[\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right]$. Moreover, aforementioned Belyi functions on $X_0(N)$ may be realized as maps $[\tau] \in \Gamma_0(N)\backslash\mathbb{H}^* \mapsto [\tau] \in \Gamma(1)\backslash\mathbb{H}^*$ and $[\tau] \in \Gamma_0(N)\backslash\mathbb{H}^* \mapsto [u(\tau)] \in \Gamma(1)\backslash\mathbb{H}^*$. Note that the second choice for u above induces the well-defined involution $[\tau] \mapsto [\frac{-1}{N\tau}]$ of $X_0(N)$. Summarizing this discussion:

Proposition 4.1. *The Belyi functions*

$$\begin{cases} f : X_0(N) \to \mathbb{CP}^1 \\ [\tau] \mapsto \frac{1}{1728}j(\tau), \end{cases} \qquad \begin{cases} g : X_0(N) \to \mathbb{CP}^1 \\ [\tau] \mapsto \frac{1}{1728}j(N\tau) \end{cases}$$

on the compact Riemann surface $X_0(N) = \Gamma_0(N)\backslash\mathbb{H}^*$ *generate the function field of* $X_0(N)$ *and transform to each other after composition with the holomorphic involution* $[\tau] \mapsto [\frac{-1}{N\tau}]$*. The minimal polynomial of* $1728g$ *over* $\mathbb{C}(f)$ *is symmetric and precisely the modular equation for* $\Gamma_0(N)$*.*

Proof. Proposition 2.1 implies that f is Belyi and it is straightforward to check that $[\tau] \mapsto [\frac{-1}{N\tau}]$ is a well-defined holomorphic involution of $X_0(N)$. So g must be Belyi as well, being the composition of the Belyi function f with an automorphism. The fact that $j(\tau)$ and $j(N\tau)$ generate the function field $\mathbb{C}(X_0(N))$ is standard. □

Remark 4.2. It is possible to transform the situation in Proposition 4.1 to that of Theorem 3.1 after replacing our curve with a finite cover. To be precise, in Theorem 3.1 we encountered the curve $\tilde{X}_0(N) := X(\Gamma(2) \cap \Gamma_0(2N))$ with the pair of Belyi functions $\tilde{f} : [\tau] \mapsto \lambda(\tau)$, $\tilde{g} : [\tau] \mapsto \lambda(N\tau)$

on it. This is a ramified covering of $X_0(N)$ in the obvious way and makes the following diagrams commute:

$$\begin{array}{ccc} \tilde{X}_0(N) & \xrightarrow{\tilde{f}} & \mathbb{CP}^1 \\ \pi\downarrow & & \downarrow\alpha \\ X_0(N) & \xrightarrow[f]{} & \mathbb{CP}^1 \end{array} \qquad \begin{array}{ccc} \tilde{X}_0(N) & \xrightarrow{\tilde{g}} & \mathbb{CP}^1 \\ \pi\downarrow & & \downarrow\alpha \\ X_0(N) & \xrightarrow[g]{} & \mathbb{CP}^1 \end{array}$$

Although subgroups $\Gamma_0(N)$ provide us with examples of function fields generated by a pair of Belyi functions with identical poles, yet these are not all such examples because, as Proposition 2.1 indicates, there are constraints on degrees of black and white vertices in dessins arising from finite index subgroups of $\Gamma(1)$. Even assuming conditions outlined in that proposition about the degrees is not enough. In other words, it is not possible to formulate an analogue of Theorem 3.1 for the case where $f, g : X \to \mathbb{CP}^1$ are Belyi functions with $\mathbb{C}(X) = \mathbb{C}(f, g)$ and $f^{-1}(\infty) = g^{-1}(\infty)$ with the property that in the corresponding dessins the degree of any black (resp. white) vertex is one or three (resp. one or two). For instance, $\Gamma_0(2)\backslash\mathbb{H}$ and $\Gamma_0(3)\backslash\mathbb{H}$ are both isomorphic to $\mathbb{C} - \{0\}$ as we shall see in Examples 4.3, 4.4 whereas these subgroups of $\Gamma(1)$ are not conjugate by an element of $\mathrm{PSL}_2(\mathbb{R})$ due to different orders of torsion elements and therefore the argument employed in the proof of Theorem 3.1 breaks down.

An essential ingredient of Theorem 3.1 is existence of an automorphism whose composition with the Belyi functions f is the Belyi function g. As the preceding example concerning $\Gamma_0(2)\backslash\mathbb{H}^*$ and $\Gamma_0(3)\backslash\mathbb{H}^*$ indicates, the weaker assumption $f^{-1}(\infty) = g^{-1}(\infty)$ is not enough to infer existence of such an automorphism. To illustrate the subtlety here, notice that even if –unlike the previous example –one assumes that moreover underlying graphs of dessins of f and g are isomorphic, still ramified coverings f and g need not to be isomorphic so there might not be any holomorphic automorphism carrying one of the dessins to the other. For instance, look at Figure 4.1 (adopted from [4, p. 92]) of two different embeddings of a tree on the Riemann sphere. In each dessin there is only one face whose center can be located at the point ∞, the point that will serve as the common unique pole of resulting Belyi functions. Thus the set of poles and the underlying graphs are the same but the corresponding dessins are not isomorphic (or even Galois conjugate).

Before starting to work with this pair of Belyi functions in examples, let us say a few words about the dessin of g. As mentioned before, just like the case of f, vertices of type $\times$ (poles of the Belyi function g) are orbits of cusps for $\Gamma_0(N)$. But the degrees might be different. For instance, according to Proposition 2.1, degrees of cusp orbits $[0], [\infty] \in X_0(N) = \Gamma_0(N)\backslash\mathbb{H}^*$ in

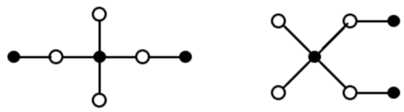

FIGURE 4.1. Dessins of two polynomial Belyi functions on $\mathbb{CP}^1$. The underlying graphs are the same whereas the dessins are not.

the dessin of f are specified by widths of these cusps of $\Gamma_0(N)$. These widths are N and 1 respectively. These degrees are reversed in the dessin of g: writing down the q-expansion and carefully analyzing charts around these points of $X_0(N)$, it is not hard to see that the orders of poles $[0]$ and $[\infty]$ of $[\tau] \in X_0(N) \mapsto j(N\tau)$ are 1 and N respectively. This fact will aid us in drawing the dessin of g in Examples 4.3, 4.4 (Figures 4.3, 4.5). Black (resp. white) vertices of the dessin of g correspond to $\Gamma_0(N)$-orbits of points τ in the upper half plane lying in the $\Gamma_0(N)$-invariant subset $\frac{1}{N}\Gamma(1).\rho$ (resp. $\frac{1}{N}\Gamma(1).\mathrm{i}$) where again, just as the dessin of f described in Proposition 2.1, the degree is either one or three (resp. one or two) with degree one occuring precisely when τ is an elliptic point of $\Gamma_0(N)$.[4] Again, we observe that unlike Theorem 3.1, in Proposition 4.1 the dessins of f and g may have different black or white vertices. Actually, the new vertices appearing in the dessin of g lead to some interesting results: suppose the equation of the Belyi function $f : X_0(N) \to \mathbb{CP}^1$ is calculated and its dessin is fixed both in the algebraic (in terms of the $\Gamma_0(N)$-orbits appearing as vertices) and the geometric (in the sense of coordinates on the Riemann surface $X_0(N)$) sense. One should consider how the dessin of the Belyi function g is positioned with respect to it. There are constraints because type $\times$ vertices whose coordinates have been fixed occur in the dessin of g too. If there are enough of these constraints (three constraints in the genus zero case, one constraint in the genus one case while no constraint necessary for higher genera) the coordinates of these new vertices are determined up to finitely many choices and evaluating the function $1728f$ at them (or the other way around, finding the values that $1728g$ attains at vertices of the dessin of f) results in values of the j-function on some new $\Gamma(1)$-orbits. Several j-values computed by this procedure are outlined in Corollary 4.6.

Example 4.3. When $N = 2$: $\bar{\Gamma}_0(2) = \langle T \rangle \bar{\Gamma}(2)$. In Example 2.2 the Belyi function $X(2) \cong \mathbb{CP}^1 \to X(1) \cong \mathbb{CP}^1$ was calculated as $z \mapsto \frac{4}{27}\frac{(z^2-z+1)^3}{(z^2-z)^2}$ (cf. (2.1)) whose dessin is shown in Figure 2.1. Here T induces the order two Möbius transformation $z \mapsto 1 - z$ with fixed points $\infty, \frac{1}{2}$. Therefore,

[4] In general, $\Gamma_0(N)$ has an elliptic point of order three if and only if N is odd and -3 is a quadratic residue modulo N and has an elliptic point of order two if and only if -1 is a quadratic residue modulo N.

any meromorphic function $\mathbb{CP}^1 \to \mathbb{CP}^1$ invariant under it factors via $z \mapsto (z-\frac{1}{2})^2$. Applying this map to coordinates of vertices in Figure 2.1, we arrive at the dessin of $f : X_0(2) \to \mathbb{CP}^1$ in Figure 4.2.

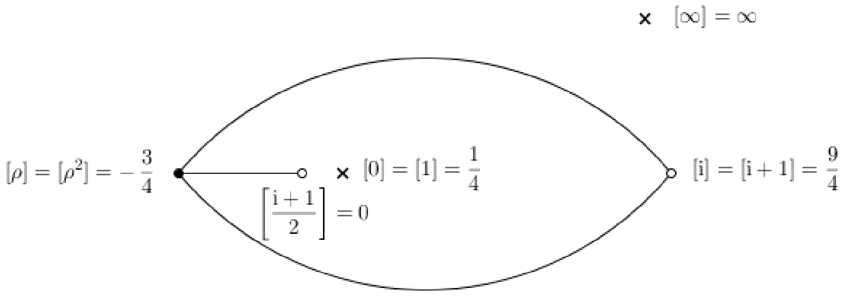

FIGURE 4.2. The dessin of the Belyi function $f : X_0(2) \to \mathbb{CP}^1$.

The Belyi function of this dessin is $f(z) = \frac{1}{27}\frac{(4z+3)^3}{(4z-1)^2}$ and satisfies $f(z) - 1 = \frac{1}{27}\frac{4z(4z-9)^2}{(4z-1)^2}$.

Let us switch to the second Belyi function $g : [\tau] \mapsto \frac{1}{1728}j(2\tau)$. There is only one black vertex, $[\frac{\rho}{2}]$, and the white vertices are $[\frac{\mathrm{i}}{2}]$ and $[\frac{\mathrm{i}+1}{2}]$. According to the dessin in Figure 4.2, $[\frac{\mathrm{i}+1}{2}]$ is the unique elliptic orbit of $\Gamma_0(2)$. Therefore, the degrees of these vertices are three, two and one respectively. Up to now, the dessin of g on $X_0(2) \cong \mathbb{CP}^1$ possesses three edges, one black vertex of degree three and two white vertices of degrees one and two which implies that there are two faces. But, as we observed before, points $[0]$ and $[\infty]$ are two vertices of type $\times$ and of degrees 1 and $N = 2$. The coordinates of $[\frac{\mathrm{i}+1}{2}], [0], [\infty]$ may be read off from the dessin of f in Figure 4.2 which implies that $g(z)$ must be in the form of $\frac{k(z-\alpha)^3}{z-\frac{1}{4}}$ while satisfies $g(z) - 1 = \frac{kz(z-\beta)^2}{z-\frac{1}{4}}$ where $\alpha = [\frac{\rho}{2}], \beta = [\frac{\mathrm{i}}{2}]$. Fixing three vertices of a dessin on $\mathbb{CP}^1$ rigidifies it so the unknowns α, β and k are readily determined: $k = \frac{1024}{27}, \alpha = \frac{3}{16}, \beta = \frac{9}{32}$. Thus $g(z) = \frac{1}{27}\frac{(16z-3)^3}{4z-1}$, $g(z) - 1 = \frac{1}{27}\frac{4z(32z-9)^2}{4z-1}$ and the dessin is illustrated in Figure 4.3. Our pair of Belyi functions is:

$$f(z) = \frac{1}{27}\frac{(4z+3)^3}{(4z-1)^2}, \quad g(z) = \frac{1}{27}\frac{(16z-3)^3}{4z-1}. \tag{4.1}$$

To derive the modular equation for $\Gamma_0(2)$ it suffices to find the algebraic dependence relation between $1728f = 64\frac{(4z+3)^3}{(4z-1)^2}$ and $1728g = 64\frac{(16z-3)^3}{4z-1}$. A simple observation helps us to accomplish this: changing z to $\frac{z+1}{4}$ in them yields new rational functions $64\frac{(z+4)^3}{z^2}$ and $64\frac{(4z+1)^3}{z}$ where the former transforms to the latter by substituting z with $\frac{1}{z}$. Hence any polynomial

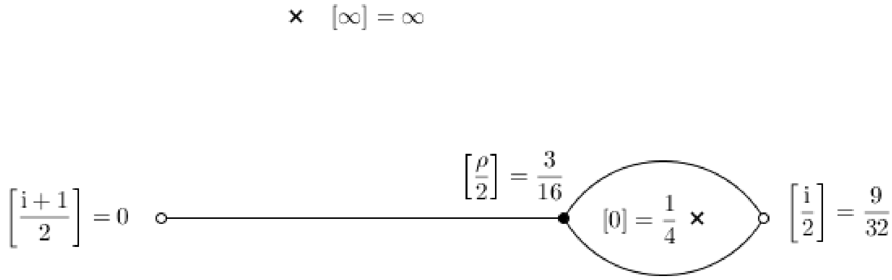

FIGURE 4.3. The dessin of the Belyi function $g : X_0(2) \to \mathbb{CP}^1$.

equation that $1728f$ and $1728g$ satisfy is symmetric and actually a polynomial relation between $64\frac{(z+4)^3}{z^2}+64\frac{(4z+1)^3}{z}$ and $(64\frac{(z+4)^3}{z^2})(64\frac{(4z+1)^3}{z})$ which are polynomials in $y := z + \frac{1}{z}$.

$$\begin{aligned}64\frac{(z+4)^3}{z^2}+64\frac{(4z+1)^3}{z} &= 4096\left(z^2+\frac{1}{z^2}\right)+3136\left(z+\frac{1}{z}\right)+1536\\ &= 4096y^2+3136y-6656\end{aligned}$$

$$\begin{aligned}&\left(64\frac{(z+4)^3}{z^2}\right)\left(64\frac{(4z+1)^3}{z}\right)\\ &\qquad= 262144\left(z^3+\frac{1}{z^3}\right)+3342336\left(z^2+\frac{1}{z^2}\right)\\ &\qquad\quad+14991360\left(z+\frac{1}{z}\right)+26808320\\ &\qquad= 262144y^3+3342336y^2+14204928y+20123648.\end{aligned}$$

One has to compute the algebraic dependence relation between the above quadratic and cubic in y and then in the derived equation replace them with $X+Y$ and XY respectively:

$$\begin{aligned}&X^3+Y^3-X^2Y^2+1488(X^2Y+XY^2)-162000(X^2+Y^2)\\ &\qquad+40773375XY+8748000000(X+Y)-157464000000000=0.\end{aligned}$$

Example 4.4. Let $N = 3$. In the coordinate system on $X(3) \cong \mathbb{CP}^1$ picked in Example 2.2, T acts as the rotation through 120° about the origin. Therefore, since $\bar{\Gamma}_0(3) = \langle T\rangle\bar{\Gamma}(3)$, factoring the degree twelve Belyi function in (2.2) via $z \mapsto z^3$ gives rise to the formula $z \mapsto \frac{1}{64}\frac{z(z+8)^3}{(z-1)^3}$ for the Belyi function $f : X_0(3) \to \mathbb{CP}^1$ whose dessin, illustrated in Figure 4.4, is obtained from applying $z \in \mathbb{CP}^1 \mapsto z^3 \in \mathbb{CP}^1$ to coordinates of vertices in Figure 2.2.

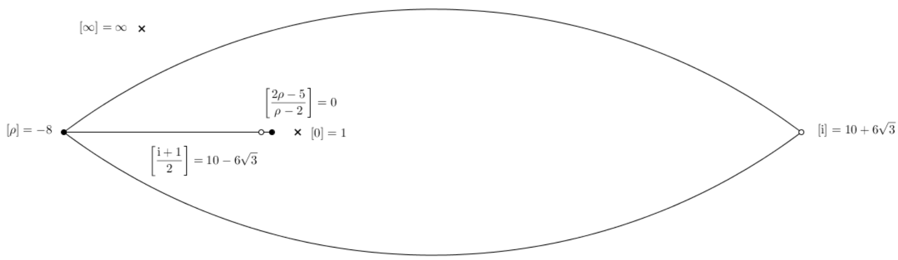

FIGURE 4.4. The dessin of the Belyi function $f : X_0(3) \to \mathbb{CP}^1$.

The dessin of the Belyi function $g : [\tau] \mapsto \frac{1}{1728} j(3\tau)$ is displayed in Figure 4.5 where the coordinates of $\left[\frac{2\rho-5}{\rho-2}\right], [0], [\infty]$ have been obtained from the dessin of f in Figure 4.4. Again, these three coordinates rigidify the dessin and the coordinates of unknown vertices $[\frac{\mathrm{i}}{3}]$, $[\frac{\mathrm{i}+1}{3}]$ and $[\frac{\rho}{3}]$ will be uniquely determined. We leave the details to the reader and just exhibit the final formula for our pair of Belyi functions on $X_0(3) \cong \mathbb{CP}^1$, cf. [1].

$$f(z) = \frac{1}{64} \frac{z(z+8)^3}{(z-1)^3}, \quad g(z) = \frac{1}{64} \frac{z(9z-8)^3}{z-1}. \tag{4.2}$$

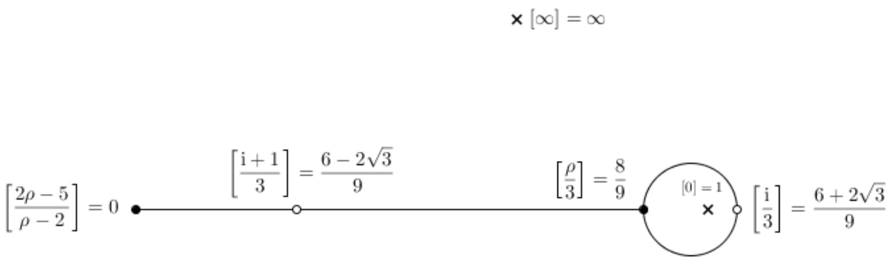

FIGURE 4.5. The dessin of the Belyi function $g : X_0(3) \to \mathbb{CP}^1$.

The next task is to compute the algebraic equation that meromorphic functions $1728f = 27\frac{z(z+8)^3}{(z-1)^3}$ and $1728g = 27\frac{z(9z-8)^3}{z-1}$ satisfy. Again, the pair (f, g) has a property that facilitates such a calculation: $f(\frac{z}{z-1}) = g(z)$ and following a procedure similar to the one explained in the previous example, we obtain the modular equation for $\Gamma_0(3)$ below:

$$\begin{aligned} &X^4 + Y^4 - X^3Y^3 + 2232(X^3Y^2 + X^2Y^3) + 2587918086X^2Y^2 \\ &-1069956(X^3Y + XY^3) + 36864000(X^3 + Y^3) + 8900222976000(X^2Y + XY^2) \\ &+ 452984832000000(X^2 + Y^2) - 770845966336000000XY \\ &+ 1855425871872000000000(X + Y) = 0. \end{aligned}$$

The existence of a relation such as $f(\frac{z}{4z-1})=g(z)$ in (4.1) or $f(\frac{z}{z-1})=g(z)$ in (4.2) that facilitated computing the algebraic dependence for either of these pairs is not accidental. Involutions $z\mapsto\frac{z}{4z-1}$ or $z\mapsto\frac{z}{z-1}$ of $X_0(2)\cong\mathbb{CP}^1$ or $X_0(3)\cong\mathbb{CP}^1$ are examples of the involution $[\tau]\mapsto[\frac{-1}{N\tau}]$ of $X_0(N)$ appeared in Proposition 4.1. It is interesting to find the values of $1728f=j$ at the fixed points of these involutions. When $N=2$, we have $[\tau]=[\frac{-1}{2\tau}]$ for $\Gamma_0(2)$-orbits of $\tau=\frac{\sqrt{2}\mathrm{i}}{2},\tau=\frac{\mathrm{i}-1}{2}$. The coordinates of these fixed points are $z=0,\frac{1}{2}$, i.e. fixed points of the involution $z\mapsto\frac{z}{4z-1}$. Since $\frac{\mathrm{i}-1}{2}$ is congruent with i under the action of $\Gamma(1)$: $j(\frac{\mathrm{i}-1}{2})=j(\mathrm{i})=1728$ which coincides with value of $1728\cdot f(z)=64\frac{(4z+3)^3}{(4z-1)^2}$ at $z=0$. So $j(\frac{\sqrt{2}\mathrm{i}}{2})=j(\sqrt{2}\mathrm{i})$ must be $1728\cdot f(\frac{1}{2})=20^3$. Similarly, when $N=3$ under the action of $\Gamma_0(3)$ the equality $[\tau]=[\frac{-1}{3\tau}]$ holds for $\tau=\frac{\sqrt{3}\mathrm{i}}{3}$ or $\tau=\rho$. These orbits have coordinates $z=0,2$ because they are fixed points of $z\mapsto\frac{z}{z-1}$. The j-function and $27\frac{z(z+8)^3}{(z-1)^3}$ vanish at ρ and $z=0$, respectively. Therefore, $1728\cdot f(2)=2\cdot 30^3$ must be equal to $j(\frac{\sqrt{3}\mathrm{i}}{3})=j(\sqrt{3}\mathrm{i})$.

Another interesting set of values of the modular j-function can be obtained by evaluating $1728f$ at vertices of the dessin of g. In the case of $N=2$ evaluating the Belyi function $f(z)=\frac{1}{27}\frac{(4z+3)^3}{(4z-1)^2}$ derived in (4.1) at vertices $[\frac{\rho}{2}]=\frac{3}{16}$ and $[\frac{\mathrm{i}}{2}]=\frac{9}{32}$ of the dessin illustrated in Figure 4.3 yields: $j(\frac{\rho}{2})=1728\cdot f(\frac{3}{16})=16\cdot 15^3$ and $j(\frac{\mathrm{i}}{2})=1728\cdot f(\frac{9}{32})=66^3$ while in Example 4.4 one should compute the values of $f(z)=\frac{1}{64}\frac{z(z+8)^3}{(z-1)^3}$ at points $[\frac{\rho}{3}]=\frac{8}{9}$, $[\frac{\mathrm{i}+1}{3}]=\frac{6-2\sqrt{3}}{9}$ and $[\frac{\mathrm{i}}{3}]=\frac{6+2\sqrt{3}}{9}$: $j(\frac{\rho}{3})=1728\cdot f(\frac{8}{9})=-3\cdot 160^3$, $j(\frac{\mathrm{i}+1}{3})=1728\cdot f(\frac{6-2\sqrt{3}}{9})=(18-6\sqrt{3})\cdot(82-54\sqrt{3})^3$ and $j(\frac{\mathrm{i}}{3})=1728\cdot f(\frac{6+2\sqrt{3}}{9})=(18+6\sqrt{3})\cdot(82+54\sqrt{3})^3$.

Example 4.5. The group $\Gamma_0(4)$ does not have any elliptic point and thus is a torsion-free genus zero congruence subgroup. One can check its dessin from [3, p. 277]. A better way to analyze this dessin, that also determines which vertex corresponds to which orbit, is to note that $\Gamma_0(4)$ is a normal subgroup of $\Gamma_0(2)$ with the quotient $\Gamma_0(2)/\Gamma_0(4)$ an order two group generated by the coset of the matrix $\left[\begin{smallmatrix}-1&1\\-2&1\end{smallmatrix}\right]$. This matrix generates the stabilizer of $\frac{\mathrm{i}+1}{2}$ in the action of $\Gamma_0(2)$ and maps 0 to 1, a point from the same $\Gamma_0(4)$-orbit. Hence the dessin of $f:[\tau]\in X_0(4)\mapsto\frac{1}{1728}j(\tau)$ is the pullback of the dessin on $X_0(2)$ illustrated in Figure 4.2 by a degree two map $X_0(4)\cong\mathbb{CP}^1\to X_0(2)\cong\mathbb{CP}^1$ branched over $[\frac{\mathrm{i}+1}{2}],[0]\in X_0(2)$. Such a dessin is displayed in Figure 4.6 below where points $[\frac{\mathrm{i}+1}{2}]$, [i] are fixed to be 0, 3 respectively and [0], the unique cusp of width $N=4$, is placed at infinity.

$$f(z) = \frac{(z^2-6)^3}{27(z^2-8)}, \quad f(z)-1 = \frac{z^2(z^2-9)^2}{27(z^2-8)}. \tag{4.3}$$

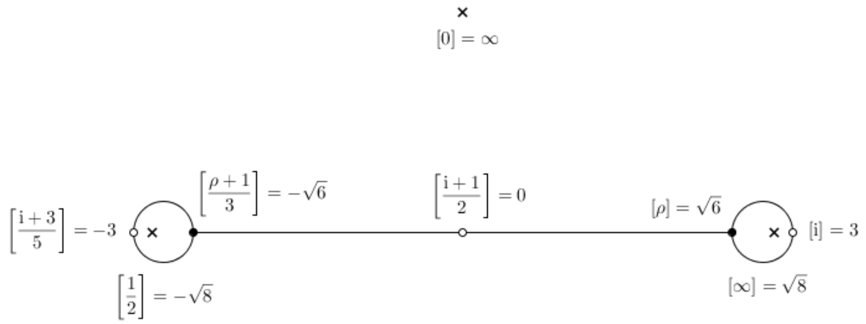

FIGURE 4.6. The dessin of the Belyi function $f : X_0(4) \to \mathbb{CP}^1$.

Unlike Examples 4.3, 4.4, here there are three cusps and since the involution $l : [\tau] \mapsto [\frac{-1}{4\tau}]$ of $X_0(4)$ permutes cusp orbits, the cusp coordinates in Figure 4.6 uniquely determine l: in this coordinate system on $X_0(4) \cong \mathbb{CP}^1$, the involution l swaps $[\infty] = \sqrt{8}$ with $[0] = \infty$ while fixes $[\frac{1}{2}] = -\sqrt{8}$ and thus is given by $z \mapsto \frac{\sqrt{8}z+24}{z-\sqrt{8}}$. Composing it with f yields the second Belyi function $g(z)$, the one which is induced by $[\tau] \mapsto \frac{1}{1728}j(4\tau)$:

$$\begin{aligned} g(z) &= \frac{(z^2+30\sqrt{8}z+264)^3}{216\sqrt{8}(z-\sqrt{8})^4(z+\sqrt{8})}, \\ g(z)-1 &= \frac{(z+3\sqrt{8})^2(z^2-66\sqrt{8}z-504)^2}{216\sqrt{8}(z-\sqrt{8})^4(z+\sqrt{8})}. \end{aligned} \tag{4.4}$$

The fixed points of l are $z = -\sqrt{8}$ and $z = 3\sqrt{8}$ that represent orbits $[\frac{1}{2}]$ and $[\frac{i}{2}]$. This yields the value $1728 \cdot f(3\sqrt{8}) = 66^3$ for $j(\frac{i}{2}) = j(2i)$ that coincides with what computed before. Evaluating $1728 \cdot g(z)$ at black and white vertices of Figure 4.6 yields: $j(\frac{4(i+1)}{2}) = 1728 \cdot g(0) = 66^3$, $j(4i) = 1728 \cdot g(3) = 27\sqrt{8} \cdot (3+\sqrt{8})^3 \cdot (91+30\sqrt{8})^3$, $j(\frac{4(i+3)}{5}) = 1728 \cdot g(-3) = -27\sqrt{8} \cdot (3-\sqrt{8})^3 \cdot (91-30\sqrt{8})^3$, $j(4\rho) = 1728 \cdot g(\sqrt{6}) = 13500 \cdot (30+17\sqrt{3})^3$ and $j(\frac{4(\rho+1)}{3}) = 13500 \cdot (30-17\sqrt{3})^3$.

The following corollary summarizes the special values of the modular j-function obtained in this paper. We have chosen representatives of $\Gamma(1)$-orbits with imaginary parts as big as possible in order to have fast convergence in the q-expansion so that the interested reader can verify these computations numerically only by writing down first few terms of the q-expansion. For instance, $\frac{4(\mathrm{i}+3)}{5}$ is replaced with $\mathrm{i}+\frac{1}{2}$ from the same orbit or $\frac{1+3\sqrt{3}\mathrm{i}}{2}$ is preferred to $\frac{\rho}{3}$.

Corollary 4.6. *We have:*

$$j(\sqrt{3}\mathrm{i}) = 16\cdot 15^3, \quad j(2\mathrm{i}) = 66^3, \quad j(\sqrt{2}\mathrm{i}) = 20^3,$$
$$j\left(\frac{1+3\sqrt{3}\mathrm{i}}{2}\right) = -3\cdot 160^3, \quad j(3\mathrm{i}) = \left(18+6\sqrt{3}\right)\cdot(82+54\sqrt{3})^3,$$
$$j\left(\frac{1+3\mathrm{i}}{2}\right) = \left(18-6\sqrt{3}\right)\cdot(82-54\sqrt{3})^3,$$
$$j(4\mathrm{i}) = 27\sqrt{8}\cdot(3+\sqrt{8})^3\cdot(91+30\sqrt{8})^3,$$
$$j\left(\mathrm{i}+\frac{1}{2}\right) = -27\sqrt{8}\cdot(3-\sqrt{8})^3\cdot(91-30\sqrt{8})^3,$$
$$j(2\sqrt{3}\mathrm{i}) = 13500\cdot\left(30+17\sqrt{3}\right)^3,$$
$$j\left(\frac{\sqrt{3}\mathrm{i}}{2}\right) = 13500\cdot\left(30-17\sqrt{3}\right)^3.$$

Let us finish with an example of a ramified cover of $X_0(N)$ whose function field is generated by three Belyi functions instead of two, the situation which is reminiscent of Theorem 3.2.

Example 4.7. Suppose that apart from Belyi functions $[\tau]\mapsto\frac{1}{1728}j(\tau)$ and $[\tau]\mapsto\frac{1}{1728}j(N\tau)$ on $X_0(N)$ introduced in Proposition 4.1, we also require $[\tau]\mapsto\frac{1}{1728}j(\frac{\tau}{N})$ to be a Belyi function. In order for this function to be well-defined, one has to pass to a ramified cover of $X_0(N)$ corresponding to a subgroup of $\Gamma_0(N)$ which is contained in $\Gamma(1)\cap(\left[\begin{smallmatrix}1&0\\0&N\end{smallmatrix}\right]^{-1}\Gamma(1)\left[\begin{smallmatrix}1&0\\0&N\end{smallmatrix}\right]) = \Gamma_0(N)^{\mathrm{t}}$. We can work with

$$\Gamma_0'(N) := \Gamma_0(N)\cap\Gamma_0(N)^{\mathrm{t}} = \left\{\left[\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right]\in\Gamma(1)\,\middle|\, N\mid b,c\right\}$$
$$= \Gamma(1)\cap\left(\left[\begin{smallmatrix}N&0\\0&1\end{smallmatrix}\right]^{-1}\Gamma(1)\left[\begin{smallmatrix}N&0\\0&1\end{smallmatrix}\right]\right)\cap\left(\left[\begin{smallmatrix}1&0\\0&N\end{smallmatrix}\right]^{-1}\Gamma(1)\left[\begin{smallmatrix}1&0\\0&N\end{smallmatrix}\right]\right).$$

Denote the corresponding curve by $X_0'(N) := X(\Gamma_0'(N))$. The same arguments indicate that the three Belyi functions $[\tau]\mapsto\frac{1}{1728}j(\tau)$, $[\tau]\mapsto\frac{1}{1728}j(N\tau)$ and $[\tau]\mapsto\frac{1}{1728}j(\frac{\tau}{N})$ generate the function field $\mathbb{C}(X_0'(N))$. The algebraic dependence relation between any two of them is a modular equation. We conclude that this curve has a model over $\mathbb{Q}$. It is worth mentioning that $X_0'(N)$ is just the quotient of $X(N)$ under the action of the group $\Gamma_0'(N)/\Gamma(N)$ of diagonal matrices over $\mathbb{Z}/N\mathbb{Z}$ and hence $X(N)\to X_0'(N)$ is a regular cover with $\Gamma_0'(N)/\Gamma(N)\cong(\mathbb{Z}/N\mathbb{Z})^*$ as its group of deck transformations. This is closely related to the standard fact that the modular curve $X(N)$ has a model over the cyclotomic field $\mathbb{Q}(\mathrm{e}^{\frac{2\pi \mathrm{i}}{N}})$ where the Galois group $\mathrm{Gal}(\mathbb{Q}(\mathrm{e}^{\frac{2\pi \mathrm{i}}{N}})/\mathbb{Q})$ is isomorphic with $(\mathbb{Z}/N\mathbb{Z})^*$ too.

References

[1] K. Filom & A. Kamalinejad, "Dessins on Modular Curves", https://arxiv.org/abs/1603.01693, 2016.

[2] E. Girondo & G. Gonzàlez-Diez, *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*, London Mathematical Society Student Texts, vol. 79, Cambridge University Press, 2012, xii+298 pages.

[3] Y.-H. He, J. McKay & J. Read, "Modular subgroups, dessins d'enfants and elliptic K3 surfaces", *LMS J. Comput. Math.* **16** (2013), p. 271-318.

[4] S. K. Lando & A. K. Zvonkin, *Graphs on Surfaces and Their Applications*, Encyclopaedia of Mathematical Sciences, vol. 141, Springer, 2004, xv+455 pages.

[5] J. McKay & A. Sebbar, "J-invariants of arithmetic semistable elliptic surfaces and graphs", in *Proceedings on Moonshine and related topics (Montréal, 1999)*, CRM Proceedings & Lecture Notes, vol. 30, American Mathematical Society, 2001, p. 119-130.

[6] J. S. Milne, "Modular Functions and Modular Forms (Elliptic Modular Curves)", http://www.jmilne.org/math/CourseNotes/MF.pdf, 2012.

[7] J. Sijsling & J. M. Voight, "On computing Belyi maps", *Publ. Math. Besançon, Algèbre Théor. Nombres* **2014** (2014), no. 1, p. 73-131.

Khashayar Filom
Department of Mathematical Sciences
Sharif University of Technology
Tehran, Iran
E-mail: khashayarfilom2014@u.northwestern.edu