INTEGRAL MODELS OF $X_0(N)$ AND THEIR DEGREES

GORAN MUIĆ

Abstract. In this paper we give a formula for the total degree i.e., the degree considered as a polynomial of two variables of the classical modular polynomial (or the degree of the canonical model of $X_0(N)$). The result is a consequence of our second main result in which we compute the degree of a curve which is the image of a mapping $z \mapsto (f(z): g(z): h(z))$ constructed out of three linearly independent modular forms of the same even weight $\geq 4$ into $\mathbb{P}^2$. We prove that in most cases this map is a birational equivalence and defined over $\mathbb{Z}$. We use this to construct models of $X_0(N)$, $N \geq 2$, using modular forms in $M_{12}(\Gamma_0(N))$ with integral $q$-expansion. The models have degree equal to $\psi(N)$ (a classical Dedekind psi function). When genus is at least one, we show the existence of models constructed using cuspidal forms in $S_4(\Gamma_0(N))$ of degree $\leq \psi(N)/3$ and in $S_6(\Gamma_0(11))$ of degree 4.

1. Introduction

Let $N \geq 2$. The modular curves $X_0(N)$ have canonical plane models constructed by Hauptmoduln $j$ [3]. More precisely, its function field over $\mathbb{C}$ is generated by $j$ and $j(N\cdot)$. The classical modular polynomial $\Phi_N \in \mathbb{Z}[x, y]$ is the minimal polynomial of $j(N\cdot)$ over $\mathbb{C}(j)$. It is symmetric in $x$ and $y$ i.e., $\Phi_N(x, y) = \Phi_N(y, x)$ and it has a degree in $x$ or $y$ equal to the Dedekind psi function

$$\psi(N) = N \prod_{p|N} \left( 1 + \frac{1}{p} \right).$$

It is also irreducible as a polynomial in $x$ as an element of $\mathbb{C}(y)[x]$ or in $y$ as an element of $\mathbb{C}(x)[y]$. But then it is irreducible in $\mathbb{C}[x, y]$. This polynomial is rather mysterious and difficult to compute [1]. In this paper we prove the following formula for the degree of $\Phi_N$ considered as a polynomial of two variables $x$ and $y$:

**Theorem 1-1.** Let $N \geq 2$. Then, the total degree of $\Phi_N$ is given by

$$\dim S_{24}(\Gamma_0(N)) + g(\Gamma_0(N)) - 1 = 2\psi(N) - \sum_{d>0, d|N} \phi((d, N/d)), $$

where $S_{24}(\Gamma_0(N))$ is the space of all cusp forms of weight 24 for $\Gamma_0(N)$, $g(\Gamma_0(N))$ is the genus of $X_0(N)$, $\phi$ is the Euler function, and $(\cdot, \cdot)$ denotes the largest common factor.

2000 Mathematics Subject Classification. 11F11, 11F23.

Key words and phrases. modular forms, modular curves, birational equivalence, modular polynomial.
Let us explain the proof of the theorem. Let

\[ E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n \]

be the usual Eisenstein series, and let

\[ \Delta(z) = q + \sum_{n=2}^{\infty} \tau(n)q^n \]

be the Ramanujan delta function. Then, \( j = E_4^3 / \Delta \). Since \( E_4^3(N \cdot) \), \( \Delta(N \cdot) \) \( \in M_{12}(\Gamma_0(N)) \), the fact that the function field over \( \mathbb{C} \) is generated by \( j \) and \( j(N \cdot) \) means that the holomorphic map

\[
\mathfrak{a}_z \mapsto (1 : j(z) : j(Nz)) = (\Delta(z)\Delta(Nz) : E_4^3(z)\Delta(Nz) : E_4^3(Nz)\Delta(z))
\]

is a birational uniformization by \( S_{24}(\Gamma_0(N)) \). The image, say \( C \), is an irreducible projective curve (Lemma 3-1). Since \( \Phi_n \) is irreducible in \( \mathbb{C}[x,y] \), the homogenization

\[ x_0^{\deg \Phi_N} \Phi(x_1/x_0, x_2/x_0) \]

is an irreducible homogeneous polynomial of total degree \( \deg \Phi_N \). Its locus is \( C \). By definition, the degree of \( C \) is the total degree of this irreducible polynomial. A classical geometric interpretation of the degree of \( C \) is the number of intersection of \( C \) with a generic line \( l \subset \mathbb{P}^2 \). We use this fact along with the following general Theorem 1-3 to prove Theorem 1-1.

We start more generally from any Fuchsian group of the first kind \( \Gamma \) (see [4]). For an even integer \( m \geq 4 \), we denote the space cuspidal forms by \( S_m(\Gamma) \) and the space of all modular forms by \( M_m(\Gamma) \) of weight \( m \). Let \( g(\Gamma) \) be the genus of \( \mathfrak{H}_\Gamma \).

We select three linearly independent modular forms \( f, g, \) and \( h \) in \( M_m(\Gamma) \), and construct the holomorphic map \( \mathfrak{H}_\Gamma \rightarrow \mathbb{P}^2 \) given by

\[
\mathfrak{a}_z \mapsto (f(z) : g(z) : h(z)).
\]

The image is an irreducible projective plane curve which we denote by \( \mathcal{C}(f,g,h) \) of degree \( \leq \dim M_m(\Gamma) + g(\Gamma) - 1 \). The details about this map can be found in the proof of Lemma 3-1. If the curve \( \mathcal{C}(f,g,h) \) has no singularities, then it is itself a compact Riemann surface, and one can define the degree \( \deg (\varphi) \) of the map \( \varphi \) as usual (a number of preimages of a point counted with multiplicities). But \( \mathcal{C}(f,g,h) \) is rarely non-singular, and one needs to modify this standard definition in order get the correct definition of \( \deg (\varphi) \). This is achieved in Lemma 3-4. In our definition, \( \deg (\varphi) \) is the number of preimages of a non-singular point counted with multiplicities. This definition is the one that behaves well as we explain in the proof of the main theorem (see Lemma 3-11). For \( f \in M_m(\Gamma) \), \( f \neq 0 \), we attach an integral effective divisor \( \mathfrak{c}_f \) by subtracting from its rational effective divisor \( \text{div}(f) \) necessary contribution at elliptic points (see Lemma 2-1 (vi)). The degree of this divisor is \( \dim M_m(\Gamma) + g(\Gamma) - 1 \). In addition, if \( f \in S_m(\Gamma) \), then we subtract necessary contribution from \( \mathfrak{c}_f \) at cusps, and get a divisor \( \mathfrak{c}_f \) which has degree \( \dim S_m(\Gamma) + g(\Gamma) - 1 \). The second main result of the paper is the following theorem (see Theorem 3-5).
Theorem 1-3. Assume that \( m \geq 4 \) is an even integer such that \( \dim M_m(\Gamma) \geq 3 \). Let \( f, g, h \in M_m(\Gamma) \) be linearly independent. Then, we have the following:

\[
\deg (\varphi) \cdot \deg C(f, g, h) = \dim M_m(\Gamma) + g(\Gamma) - 1 - \sum_{a \in \mathcal{R}_T} \min (c'_f(a), c'_g(a), c'_h(a)).
\]

Moreover, if \( f, g, h \in S_m(\Gamma) \), then

\[
\deg (\varphi) \cdot \deg C(f, g, h) = \dim S_m(\Gamma) + g(\Gamma) - 1 - \sum_{a \in \mathcal{R}_T} \min (c_f(a), c_g(a), c_h(a)).
\]

In particular, if \( \varphi \) is birational, then \( \deg (\varphi) = 1 \) (since it is generically injective), and we have in either case a simple formula for the degree of \( \deg C(f, g, h) \) in terms of \( f, g, \) and \( h \).

The proof of the theorem uses fine points of the theory of compact Riemann surfaces and algebraic curves. Preliminaries about divisors attached to cuspidal modular forms are stated in Section 2. The proof of the theorem is given in Section 3 in a series of Lemmas. In Section 4, we prove Theorem 1-1 using Theorem 1-3.

As we see, the canonical model of \( X_0(N) \) is obtained using cusp forms of weight 24. In Section 4, we show that this model is just one in the series of birational models constructed using cusp forms (this is not essential). To state the main result of Section 4 (see Theorem 4-7), we introduce some notation.

Let \( m \geq 4 \) be an even integer and let \( W \subset M_m(\Gamma) \) be a non–zero linear subspace. Then, we say that \( W \) generates the field of rational functions \( \mathbb{C}(\mathcal{R}_T) \) if \( \dim W \geq 2 \), and there exists a basis \( f_0, \ldots, f_{s-1} \) of \( W \), such that the holomorphic map \( \mathcal{R}_T \rightarrow \mathbb{P}^{s-1} \) given by \( a \mapsto (f_0(z) : \cdots : f_{s-1}(z)) \) is birational. Clearly, this notion does not depend on the choice of the basis used. It is also obvious that this is equivalent with the fact that \( \mathbb{C}(\mathcal{R}_T) \) is generated over \( \mathbb{C} \) with the quotients \( f_i/f_0, 1 \leq i \leq s - 1 \). We need one more definition. We say that \( W \not\subset S_m(\Gamma) \) (resp., \( W \subset S_m(\Gamma) \)) separates the points on \( \mathcal{R}_T \) if for each \( a \in \mathcal{R}_T \) there exists \( f \in W, f \neq 0 \), such that \( c'_f(a) = 0 \) (resp., \( c_f(a) = 0 \)). The geometric meaning of this assumption is that the complete linear system attached to the divisor of above holomorphic map into \( \mathbb{P}^{s-1} \) has no base points (see the proof of Lemma 4-3). Now, we are ready to state the main result of Section 4 (see Theorem 4-7).

Theorem 1-4. Assume that \( m \geq 4 \) is an even integer. Let \( W \subset M_m(\Gamma), \dim W \geq 3, \) be a subspace which generates the field of rational functions \( \mathbb{C}(\mathcal{R}_T) \), and separates the points on \( \mathcal{R}_T \). For example, if \( \dim S_m(\Gamma) \geq \max (g(\Gamma) + 2, 3) \), then we can take \( W = S_m(\Gamma) \). Let \( f, g \in W \) be linearly independent. Then there exists a non–empty Zariski open set \( \mathcal{U} \subset W \) such that for any \( h \in \mathcal{U} \) we have the following:

(i) \( \mathcal{R}_T \) is birationally equivalent to \( C(f, g, h) \), and

(ii) \( C(f, g, h) \) has degree equal to \( \dim M_m(\Gamma) + g(\Gamma) - 1 \) (resp., \( \dim S_m(\Gamma) + g(\Gamma) - 1 \) if \( W \not\subset S_m(\Gamma) \), resp., \( W \subset S_m(\Gamma) \)).

In Section 4 we prove the following corollary (see Corollary 4-1):

Corollary 1-5. Assume that \( N \not\in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\} \) (so that the genus \( g(\Gamma_0(N)) \geq 1 \)). Assume that \( m \geq 4 \) (if \( N = 23 \)) and \( m \geq 6 \) (if \( N = 25 \)) is an even integer. Let \( f, g \in S_m(\Gamma_0(N)) \) be linearly independent with integral \( q \)-expansions. Then,
there exists infinitely many $h \in S_m(\Gamma_0(N))$ with integral $q$-expansion such that we have the following:

(i) $X_0(N)$ is birationally equivalent to $\mathcal{C}(f, g, h)$,

(ii) $\mathcal{C}(f, g, h)$ has degree equal to $\dim S_m(\Gamma_0(N)) + g(\Gamma_0(N)) − 1$ (this number can be easily explicitly computed using Lemma 2-1(v) and (5-4)); if $N = 11$, then the minimal possible degree achieved (for $m = 6$) is 4, and if $N \neq 11$, then the minimal possible degree achieved (for $m = 4$) is

$$\frac{1}{3}\psi(N) - \frac{1}{3} \nu_3 - \sum_{d>0, d|N} \phi((d, N/d)),$$

where $\nu_3$ is the number of elliptic elements of order three on $X_0(N)$, $\nu_3 = 0$ if $9|N$, and $\nu_3 = \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right)$, otherwise.

(iii) the equation of $\mathcal{C}(f, g, h)$ has integral coefficients.

As an example to Theorem 1-4, we consider the subspace $W \subset M_{12}(\Gamma_0(N))$ which basis is $\Delta, E_3^4, \Delta(N\cdot), \text{ and } E_3^3(N\cdot)$ (see Lemma 7-1). It satisfies the requirement stated in Theorem 1-4, and a direct application of Theorem 1-4 is stated in Corollary 7-3. But the following result is an improvement with a similar proof (see Theorem 7-4):

**Theorem 1-6.** Let $N \geq 2$. Then, there exists infinitely many pairs $(\alpha, \beta) \in \mathbb{Z}^2$ such that $X_0(N)$ is birational with $\mathcal{C}(\Delta, E_3^3, \alpha\Delta(N\cdot) + \beta E_3^3(N\cdot))$, and

$$\deg \mathcal{C}(\Delta, E_3^3, \alpha\Delta(N\cdot) + \beta E_3^3(N\cdot)) = \psi(N).$$

In closing the introduction we should mention several other works which construct plane models of modular curves ([2], [3], [9], [10]). They use strategies which are quite different than ours.

I would like to thank M. Kazalicki and G. Savin for some useful discussion about integral structure on the spaces of cusp forms.

2. Preliminaries

In this section we recall from ([4], 2.3) some notions related to the theory of divisors of modular forms and state a preliminary result.

Let $m \geq 2$ be an even integer and $f \in M_m(\Gamma) - \{0\}$. Then $\nu_{z-\xi}(f)$ the order of the holomorphic function $f$ at $\xi$. For each $\gamma \in \Gamma$, the functional equation $f(\gamma z) = j(\gamma, z)^m f(z)$ shows that $\nu_{z-\xi}(f) = \nu_{z-\xi'}(f)$, where $\xi' = \gamma \cdot \xi$. Also, if we let

$$e_\xi = \#(\Gamma_\xi / \Gamma \cap \{\pm1\}),$$

then $e_\xi = e_{\xi'}$. The point $\xi$ is elliptic if $e_\xi > 1$. Next, following ([4], 2.3), we define

$$\nu_{\xi}(f) = \nu_{z-\xi}(f) / e_\xi.$$

Clearly, $\nu_{\xi} = \nu_{\xi'}$, and we may let

$$\nu_{\alpha\xi}(f) = \nu_{\xi}(f),$$
MODELS OF $X_0(N)$

where

$$a_ξ \in R_Γ$$

is a projection of $ξ$ to $R_Γ$, a notation we use throughout this paper.

If $x \in R ∪ \{∞\}$ is a cusp for $Γ$, then we define $ν_x(f)$ as follows. Let $σ ∈ SL_2(R)$ such that $σ.x = ∞$. We write

$$\{±1\}σΓxσ^{-1} = \{±1\}\left\{ \begin{pmatrix} lh' + l & 1 \\ 0 & 1 \end{pmatrix} \right\} ; \ l ∈ Z,$$

where $h' > 0$. Then we write the Fourier expansion of $f$ at $x$ as follows:

$$(f|_mσ^{-1})(σ.z) = ∑_{n=1}^{∞} a_n e^{2π√-1nσ.z/h}.$$ 

We let

$$ν_x(f) = N ≥ 0,$$

where $N$ is defined by $a_0 = a_1 = · · · = a_{N-1} = 0, a_N ≠ 0$. One easily see that this definition does not depend on $σ$. Also, if $x' = γ.x$, then $ν_x(f) = ν_{x'}(f)$. Hence, if $b_x ∈ R_Γ$ is a cusp corresponding to $x$, then we may define

$$ν_{b_x} = ν_x(f).$$

Put

$$\text{div}(f) = ∑_{a ∈ R_Γ} ν_a(f)a ∈ Q ⊗ \text{Div}(R_Γ),$$

where $\text{Div}(R_Γ)$ is the group of (integral) divisors on $R_Γ$.

Using ([4], 2.3), this sum is finite i.e., $ν_a(f) ≠ 0$ for only a finitely many points. We let

$$\deg(\text{div}(f)) = ∑_{a ∈ R_Γ} ν_a(f).$$

Let $d_i ∈ Q ⊗ \text{Div}(R_Γ), i = 1, 2$. Then we say that $d_1 ≥ d_2$ if their difference $d_1 − d_2$ belongs to $\text{Div}(R_Γ)$ and is non–negative in the usual sense.

**Lemma 2-1.** Assume that $m ≥ 4$ is an even integer. Assume that $f ∈ M_m(Γ), f ≠ 0$. Let $t$ be the number of inequivalent cusps for $Γ$. Then we have the following:

(i) For $a ∈ R_Γ$, we have $ν_a(f) ≥ 0$.

(ii) For a cusp $a ∈ R_Γ$, we have that $ν_a(f) ≥ 1$ is an integer.

(iii) If $a ∈ R_Γ$ is not an elliptic point or a cusp, then $ν_a(f) ≥ 0$ is an integer. If $a ∈ R_Γ$ is an elliptic point, then $ν_a(f) − m/2(1 − 1/e_a)$ is an integer.

(iv) Let $g(Γ)$ be the genus of $R_Γ$. Then

$$\deg(\text{div}(f)) = m(g(Γ) − 1) + ∑_{a ∈ R_Γ, \ \text{elliptic}} m/2 \left( t + ∑_{a ∈ R_Γ, \ \text{elliptic}} (1 − 1/e_a) \right).$$
(v) Let \( [x] \) denote the largest integer \( \leq x \) for \( x \in \mathbb{R} \). Then

\[
\dim S_m(\Gamma) = (m - 1)(g(\Gamma) - 1) + \left( \frac{m}{2} - 1 \right) t + \sum_{a \in \mathfrak{M}_\Gamma, \text{elliptic}} \left[ \frac{m}{2}(1 - 1/e_a) \right]
\]

\[
\dim M_m(\Gamma) = \dim S_m(\Gamma) + t.
\]

(vi) There exists an integral divisor \( \mathcal{C}_f' \geq 0 \) of degree \( \dim M_m(\Gamma) + g(\Gamma) - 1 \) such that

\[
\text{div}(f) = \mathcal{C}_f' + \sum_{a \in \mathfrak{M}_\Gamma, \text{elliptic}} \left( \frac{m}{2}(1 - 1/e_a) - \left[ \frac{m}{2}(1 - 1/e_a) \right] \right) a.
\]

Proof. The claims (i)–(v) are standard ([4], 2.3, 2.5). The claim (vi) follows from (iii), (iv), and (v) (see Lemma 4-1 in [6]). \( \square \)

If \( f \in S_m(\Gamma) \), we can define an integral divisor \( \mathcal{C}_f' \geq 0 \) of degree \( \dim S_m(\Gamma) + g(\Gamma) - 1 \) by

\[
\mathcal{C}_f \overset{\text{def}}{=} \mathcal{C}_f' - \sum_{b \in \mathfrak{M}_\Gamma, \text{cusp}} b.
\]

3. A proof of the formula for the degree

In this section \( \Gamma \) is an arbitrary Fuchsian group of the first kind. We introduce the objects of our study in the following lemma:

**Lemma 3-1.** Assume that \( m \geq 4 \) is an even integer such that \( \dim M_m(\Gamma) \geq 3 \). Let \( f, g, h \in M_m(\Gamma) \) be linearly independent. Then, the image of the map \( \varphi : \mathfrak{M}_\Gamma \to \mathbb{P}^2 \) given by

\[
\mathbf{a}_z \mapsto (f(z) : g(z) : h(z))
\]

is an irreducible projective curve which we denote by \( \mathcal{C}(f, g, h) \). The degree of \( \mathcal{C}(f, g, h) \) (i.e., the degree of \( P \)) is \( \leq \dim M_m(\Gamma) + g(\Gamma) - 1 \). Moreover, if \( f, g, \) and \( h \) are selected to be cusp forms, then the degree is \( \leq \dim S_m(\Gamma) + g(\Gamma) - 1 \).

Proof. Note that \( g/f \) and \( h/h \) are rational functions on \( \mathfrak{M}_\Gamma \) considered as a smooth irreducible projective curve over \( \mathbb{C} \). Thus, the meromorphic map \( \mathbf{a}_z \mapsto (f(z) : g(z) : h(z)) \) is actually a rational map

\[
\mathbf{a}_z \mapsto (1 : g(z)/f(z) : h(z)/g(z)).
\]

Hence, it is regular since \( \mathfrak{M}_\Gamma \) is smooth. The image of the map is clearly not constant. Hence, it is an irreducible curve in \( \mathbb{P}^2 \).

Let \( l \) be the line in \( \mathbb{P}^2 \) in general position with respect to \( \mathcal{C}(f, g, h) \). Then, it intersects \( \mathcal{C}(f, g, h) \) in different points a number of which is the degree of \( \mathcal{C}(f, g, h) \). We can change the coordinate system so that the line \( l \) is \( x_0 = 0 \). In new coordinate system, the map \( \mathbf{a}_z \mapsto (f(z) : g(z) : h(z)) \) is of the form

\[
\mathbf{a}_z \mapsto (F(z) : G(z) : H(z)),
\]
where \( F, G, H \) are again linearly independent. In particular, \( F, G, H \neq 0 \).

We write this map in the form
\[
a_z \mapsto (1 : G(z)/F(z) : H(z)/F(z)).
\]

By Lemma 2-1 (vi), we can write
\[
div(G/F) = div(G) - div(F) = \mathcal{c}_G' - \mathcal{c}_F',
\]
\[
div(H/F) = div(H) - div(F) = \mathcal{c}_H' - \mathcal{c}_F'.
\]

We remark that the divisors \( \mathcal{c}_F', \mathcal{c}_G', \) and \( \mathcal{c}_H' \) are integral divisors of degree \( \text{dim } M_m(\Gamma) + g(\Gamma) - 1 \) (see Lemma 2-1 (vi)).

Now, we intersect \( \mathcal{C}(f,g,h) \) with the line \( x_0 = 0 \). The intersection points of intersection are contained among the points in the support of \( \mathcal{c}_F' \). The claim about the degree follows since the support can not have more than \( \text{dim } M_m(\Gamma) + g(\Gamma) - 1 \) points. If we deal with the cusps forms, then we can slightly improve the last argument using (2-2). This proves the last claim of the lemma.

Next, we define the degree of the covering map \( \varphi : \mathfrak{R}_\Gamma \rightarrow \mathcal{C}(f,g,h) \) (see Lemma 3-4 below). This would be a standard fact (see page 31 of [4] for the summary) if \( \mathcal{C}(f,g,h) \) would have no singularities. We follow and modify the standard way of defining the degree of the map as explained in [5].

First, we observe

**Lemma 3-2.** Maintaining the assumptions of Lemma 3-1, the preimage \( \varphi^{-1}(q) \) is finite for any \( q \in \mathcal{C}(f,g,h) \).

**Proof.** Let \( q = (x_0 : x_1 : x_2) \). Without loss of generality we may assume that \( x_2 \neq 0 \). Then, \( h \) is not identically zero. Since \( f, g, \) and \( h \) are linearly independent, the quotient \( f/h \) is not constant. Now, by the standard theory of compact Riemann surfaces (see for example summary on pages 30–31 in [4]), the regular map \( \mathfrak{R}_\Gamma \rightarrow \mathbb{P}^1 \) defined by \( f/h \) has finite preimages.

We let \( V \) be the complement of finitely many points in \( \mathcal{C}(f,g,h) \) where this curve is singular. We let \( U \) be the preimage of \( V \) in \( \mathfrak{R}_\Gamma \). By Lemma 3-2, it is a complement of finitely many points which maps to the set of singular points in \( \mathcal{C}(f,g,h) \). Thus, both \( U \) and \( V \) are open Riemann surfaces and we have a holomorphic surjective map \( \varphi|_U : U \rightarrow V \).

The multiplicity \( \text{mult}_p(\varphi|_U) \) of \( p \in U \) of \( \varphi|_U \) is defined in the usual way: using suitable local coordinates, in a neighborhood of \( p \), the map \( \varphi|_U \) is of the form \( w \mapsto w^{\text{mult}_p(\varphi|_U)} \) (\( w = 0 \) corresponds to \( p \)). As usual, following [5], we let

\[
(3-3) \quad \deg_q(\varphi|_U) = \sum_{p \in \varphi^{-1}(q)} \text{mult}_p(\varphi|_U), \quad q \in U.
\]
The following lemma is a variant of the standard argument (i.e., the case when $C(f, g, h)$ has no singularities)

**Lemma 3.4.** The map $q \mapsto \deg_q(\varphi|_U)$ is constant on $U$. In this way we define a degree of $\varphi$ (since $U$ is uniquely determined by $\varphi$), and we denoted by $\deg(\varphi)$.

**Proof.** First, $C(f, g, h)$ is connected since it is a continuous image of the connected set $\mathfrak{R}_\Gamma$. Then, since $U$ is a complement of finitely many points in $C(f, g, h)$, $U$ is connected. Thus, it is enough to show that $q \mapsto \deg_q(\varphi|_U)$ is locally constant.

Let us show that $q \mapsto \deg_q(\varphi|_U)$ is locally constant. Let us fix $q \in U$. For each of finitely many points $p \in \varphi^{-1}(q)$, we select a neighborhood (charts) $U_p$ of $p$, and a neighborhood $W$ of $q$ such that $\varphi(U_p) \subset W$, and $\varphi$ is of the form $w_p \mapsto w_p^{\mult_p(\varphi|_U)}$ ($w_p = 0$ corresponds to $p$). By shrinking $U_p$, we may assume that they are all disjoint. Then, for each $q' \in W - \{q\}$, there are $\mult_p(\varphi|U)$ different points in $U_p$ which maps to $q'$. Thus, there are $\deg_q(\varphi|U) = \sum_{p \in \varphi^{-1}(q)} \mult_p(\varphi|U)$ different points from the union $\cup_{p \in \varphi^{-1}(q)} U_p$ which maps to $q'$.

We may think that the chart $W$ is given by an open circle $|u| < r$, $u = 0$ corresponds to $q$, and we may define neighborhoods $W_p$, $p < r$, of $p$ which corresponds to open circles $|u| < \rho$. We show that for suitable small $\rho$, none of the preimages is left out i.e., for each $q' \in W_p - \{q\}$ we have $\varphi^{-1}(q) \subset \cup_{p \in \varphi^{-1}(q)} U_p$. If not, then there is a sequence of points such that $q_n \rightarrow q$, and there is a sequence of points $p_n \in U - \cup_{p \in \varphi^{-1}(q)} U_p$ such that $\varphi(p_n) = q_n$.

The key point is the fact that the sequence $p_n$ belongs to the complement of $\cup_{p \in \varphi^{-1}(q)} U_p$ in $\mathfrak{R}_\Gamma$. But $\mathfrak{R}_\Gamma$ is compact so the sequence $p_n$ has a convergent subsequence; we may assume that $p_n$ itself is a convergent. Let $\lim_n p_n = p'$. Then, $\varphi(p') = q$ and $p' \notin \cup_{p \in \varphi^{-1}(q)} U_p$. This is clearly a contradiction.

Thus, for suitable small $\rho$, preimages of $q' \in W_p - \{q\}$ consist of exactly $\deg_q(\varphi|U)$ different points. Clearly, in a neighborhood of them the map is of the form $w \mapsto w$, which implies

$$\deg_{q'}(\varphi|U) = \deg_q(\varphi|U),$$

or otherwise there would exist a point $q' \in W_p - \{q\}$, and a preimage $p'$ of $q'$ in some $U_p$ such that the map is in the neighborhood of $p'$ is of the form $q \mapsto q' + l$, $l \geq 1$. Then, for $q'' \in W_p - \{q\}$ near $q'$, in the neighborhood of $p'$ the point $q''$ would have at least two preimages. This would result in at least $\mult_p(\varphi|_U) + 1$ of preimages of $q'$ in $U_p$ which is impossible. This proves the lemma.

Now, we state and prove the main result of the present section.

**Theorem 3.5.** Assume that $m \geq 4$ is an even integer such that $\dim M_m(\Gamma) \geq 3$. Let $f, g, h \in M_m(\Gamma)$ be linearly independent. Then, we have the following:

$$\deg(\varphi) \cdot \deg C(f, g, h) = \dim M_m(\Gamma) + g(\Gamma) - 1 - \sum_{a \in \mathfrak{R}_\Gamma} \min (c'_f(a), c'_g(a), c'_h(a)).$$

Moreover, if $f, g, h \in S_m(\Gamma)$, then

$$\deg(\varphi) \cdot \deg C(f, g, h) = \dim S_m(\Gamma) + g(\Gamma) - 1 - \sum_{a \in \mathfrak{R}_\Gamma} \min (c_f(a), c_g(a), c_h(a)).$$
In particular, if \( \varphi \) is birational, then \( \deg(\varphi) = 1 \) (since it is generically injective), and we have in either case a simple formula for the degree of \( \deg C(f, g, h) \) in terms of \( f, g, \) and \( h \).

**Proof.** The formula in the case \( f, g, h \in S_m(\Gamma) \) follows at once from the general case using (2-2). We consider the general case \( f, g, h \in M_m(\Gamma) \).

In the first step of the proof, we associate the linear system to the map \( \varphi \). Assume that \( k \in M_m(\Gamma) \) is non–zero. We write the map in the form

\[
\varphi(a_z) = (f(z) : g(z) : h(z)) = (F(z) : G(z) : H(z)),
\]

where \( F = f/k, \ G = g/k, \) and \( H = h/k. \) Then, we define the divisor \( d_k \) in the usual way using

\[
d_k(a) = -\min(\text{div}(F)(a), \text{div}(G)(a), \text{div}(H)(a)), \quad a \in \mathcal{R}_{\Gamma}.
\]

Using Lemma 2-1 (vi), we compute

\[
d_k = -\sum_{a \in \mathcal{R}_{\Gamma}} \min(c_f(a) - c_{h}(a), c_g(a) - c_{h}(a), c_h(a) - c_{h}(a))a
\]

(3-6)

\[
= c_f - \sum_{a \in \mathcal{R}_{\Gamma}} \min(c_f(a), c_g(a), c_h(a))a.
\]

The computation in (3-6) shows that different \( k \)'s determine the same linear system \( |d_k| \). We shall select \( k = h \) in the sequel, and let

\[
d = d_h.
\]

Let \( l \subset \mathbb{P}^2 \) be a line. Let us write \( \varphi^*(l) \) be the hyperplane divisor of the map \( \varphi : \mathcal{R}_{\Gamma} \to C(f, g, h) \). By definition, if we write the equation of the line \( l \) as follows: \( a_0x_0 + a_1x_1 + a_2x_2 = 0 \), then

\[
\varphi^*(l) = \text{div}(a_0F + a_1G + a_2) + d.
\]

(3-8)

If \( C(f, g, h) \) is smooth (i.e., an embedded Riemann surface), then one would define the intersection divisor \( \text{div}(l) \) of a line \( l \) as follows. Let \( q \in l \cap C(f, g, h) \). We select a coordinate function \( x_i \) which does not vanish at \( q \) and let \( \text{div}(l)(q) = \text{ord}_q(l/x_i) \). This is independent of the coordinate function used. We have

\[
\text{div}(l) = \sum_{q \in l \cap C(f, g, h)} \text{div}(l)(q)q.
\]

Still assuming that \( C(f, g, h) \) is smooth, we have

\[
\deg(\text{div}(l)) = \deg C(f, g, h),
\]

(3-9)

and

\[
\deg(d) = \deg(\varphi^*(l)) = \deg(\varphi) \cdot \deg(\text{div}(l)).
\]

(3-10)
Of course, in general $C(f, g, h)$ can have singularities outside $V$ (introduced before the statement of Lemma 3-4). So, we modify the proof of above formulas such that they hold in generality we need. First of all, we restrict ourselves to the lines such that $l \cap C(f, g, h) \subset V$. Then, we may define $\text{div}(l)$ as before.

**Lemma 3-11.** Let $l \subset \mathbb{P}^2$ be any line such that $l \cap C(f, g, h) \subset V$. Then, (3-9) and (3-10) hold. Moreover, we can select a line $l \subset \mathbb{P}^2$ such that $l \cap C(f, g, h) \subset V$ and $l \cap C(f, g, h)$ consists of $\deg C(f, g, h)$ different points.

**Proof.** With the aid of Lemma 3-4 we easily adapt the proof of ([5], Proposition 4.23) to prove (3-10). We leave details to the reader.

To show (3-9), we adapt the classical argument with resultants. We may assume $(0 : 0 : 1) \not\in C(f, g, h)$. We look at the family of lines $l_\lambda$ given by $x_0 - \lambda x_1 = 0$ that pass through this point. Since there are just finitely many points in $C(f, g, h) - V$, for all but finitely many $\lambda$’s we have the following: $l_\lambda \cap C(f, g, h) \subset V$.

We observe that $x_0 - \lambda x_1$ and $x_1$ never vanish simultaneously on $C(f, g, h)$ since $(0 : 0 : 1) \not\in C(f, g, h)$. Thus, $\text{div}(x_0 - \lambda x_1)$ is determined by $x_0/x_1 - \lambda$ at any point of intersection of $l_\lambda$ and $C(f, g, h)$.

The intersection of $x_0 - \lambda x_1$ with $C(f, g, h)$ is of the form $(\lambda : 1 : \mu)$. If we let $P$ be the irreducible homogeneous polynomial which locus is $C(f, g, h)$, then the equation for $\mu$ is given by $P(\lambda, 1, \mu) = 0$. Since $(0 : 0 : 1) \not\in C(f, g, h)$, we may write (up to a non–zero constant depending on $P$ only)

$$P(\lambda, 1, \mu) = \mu^{\deg C(f, g, h)} + \sum_{i=0}^{\deg C(f, g, h)-1} a_i(\lambda)\mu^i,$$

where $a_i$ is polynomial in $\lambda$. The discriminant of $P$ with respect to $\mu$ (that is, a resultant of $P(\lambda, 1, \mu)$ and $\frac{\partial}{\partial \mu} P(\lambda, 1, \mu)$) is a polynomial of $\lambda$ which does not vanish identically.

At all but finitely many points $\lambda$, we have that the equation for $\mu$

$$(3-12) \quad P(\lambda, 1, \mu) = \mu^{\deg C(f, g, h)} + \sum_{i=0}^{\deg C(f, g, h)-1} a_i(\lambda)\mu^i = 0,$$

satisfies

$$P(\lambda, 1, \mu) = 0 \implies \frac{\partial}{\partial x_2} P(\lambda, 1, \mu) \neq 0.$$

This means that for such $\lambda$, we have $\deg C(f, g, h)$ different solutions for $\mu$. By the Implicit function theorem, $\frac{\partial}{\partial x_2} P(\lambda, 1, \mu) \neq 0$ means that near the point $(\lambda : 1 : \mu)$, the local coordinate is $x_0/x_1$. Hence,

$$\text{ord}_{(\lambda; 1; \mu)}(x_0 - \lambda x_1) = 1.$$
Finally, for \( \lambda \) which makes the discriminant non–vanishing, we have
\[
\text{div}(x_0 - \lambda x_1) = \sum_{(\lambda:1:\mu)} (\lambda:1:\mu),
\]
where \( \mu \) runs over all solutions of \((3-12)\). This implies
\[
\text{deg} (\text{div}(x_0 - \lambda x_1)) = \text{deg} C(f, g, h).
\]
This proves the claim about the degree. \( \square \)

Having completed the proof of Lemma \(3-11\), the proof of Theorem \(3-5\) is easy to complete. Let \( \ell \subset \mathbb{P}^2 \) be any line. Then, by Lemma \(3-11\), \((3-9)\) and \((3-10)\) hold. So, if we combine them with \((3-6)\) (with \( k = h \)), we obtain
\[
\text{deg} (\varphi) \cdot \text{deg} C(f, g, h) = \text{deg} \left( c'_h - \sum_{a \in \mathcal{B}_1} \min (c'_f(a), c'_g(a), c'_h(a)) a \right)
\]
\[
= \text{deg} (c'_h) - \sum_{a \in \mathcal{B}_1} \min (c'_f(a), c'_g(a), c'_h(a))
\]
\[
= \dim M_m(\Gamma) + g(\Gamma) - 1 - \sum_{a \in \mathcal{B}_1} \min (c'_f(a), c'_g(a), c'_h(a)).
\]
The last equality follows by Lemma \(2-1\) (vi). \( \square \)

4. A GENERIC CONSTRUCTION OF BIRATIONAL MAPS

In this section, we let \( t_m = \dim S_m(\Gamma) \). The goal of this section is to construct various models of the curve \( \mathcal{R}_\Gamma \), where \( \Gamma \) is any Fuchsian group of the first kind.

**Lemma 4-1.** Let \( m \geq 4 \) be an even integer such that \( t_m \geq g(\Gamma) + 2 \). Then, the field of rational functions \( \mathbb{C}(\mathcal{R}_\Gamma) \) is generated over \( \mathbb{C} \) by the rational functions \( f_i/f_0, 1 \leq i \leq t_m - 1 \), where \( f_0, \ldots, f_{t_m-1} \) is a basis of \( S_m(\Gamma) \).

**Proof.** This is \((7)\), Corollary 3-7). Let us sketch the proof. For \( f \in S_m(\Gamma) \), we consider \( L(\mathcal{C}_f) \) which is by definition the space of all \( F \in \mathbb{C}(\mathcal{R}_\Gamma) \) such that \( \text{div}(F) + \mathcal{C}_f \geq 0 \). In \((7)\), Proposition 2-10) we show that \( L(\mathcal{C}_f) = \{ g/f; \ g \in S_m(\Gamma) \} \) assuming only that \( m \geq 4 \) and \( t_m \geq 1 \). The proof of this is similar to the proof of \((6)\), Theorem 4-15) using computations on pages 17 and 18 of \(6\). Then, we construct the embedding \( \mathcal{R}_\Gamma \hookrightarrow \mathbb{P}^{t_m-1} \) using the holomorphic map
\[
a_z \mapsto (f_0(z) : \cdots : f_{t_m-1}(z)) = (f_0(z)/f(z) : \cdots : f_{t_m-1}(z)/f(z)).
\]
A computation similar to that in \((3-6)\) shows that this map is attached to the linear system \(|\mathcal{C}_f|\) as we demonstrate this in \((7)\), Theorem 3-3). If \( t_m \geq g(\Gamma) + 2 \), then \( \mathcal{C}_f \) is very ample. So, the map is an embedding. The claim of the lemma is an obvious consequence of this. \( \square \)
Lemma 4-2. Let \( \xi \in X \) or let \( \xi \) be a cusp for \( \Gamma \). Let \( m \geq 4 \) be an even integer such that \( t_m \geq g(\Gamma) + 1 \). Then, there exists \( f \in S_m(\Gamma) \) such that \( c_f(a_\xi) = 0 \).

Proof. This is ([7], Lemma 2-9). The proof of this lemma is a straightforward generalization of computations made in ([6], Section 4, pages 17 and 18).

Lemma 4-3. Assume that \( m \geq 4 \) is an even integer. Let \( W \not\subset S_m(\Gamma) \) be a subspace which separates the points of \( \mathcal{R}_\Gamma \). Select a basis \( f_0, \ldots, f_{s-1} \) for \( W \). Then, for each \( \xi \in X \) or a cusp for \( \Gamma \), there exists \( i \) such that \( c_{f_i}(a_\xi) = 0 \).

Proof. Let \( f \in W, f \neq 0 \), be an arbitrary form. Consider the linear space

\[
L(c'_{f_i}) = \{ F \in \mathbb{C}(\mathcal{R}_\Gamma); \ \text{div}(F) + c'_{f} \geq 0 \}.
\]

Then, it contains a linear subspace \( W_1 \) consisting of all quotients \( g/f, g \in W \). This is so, since, for \( g \neq 0 \), by Lemma 2-1 (vi) we obtain

\[
\text{div} \left( \frac{g}{f} \right) + c'_{f} = \text{div}(g) - \text{div}(f) + c'_{f} = c'_{g} - c'_{f} + c'_{f} = c'_{g} \geq 0.
\]

Assume that the claim of the lemma is not true, then for all \( i \) we have \( c'_{f_i}(a_\xi) \geq 1 \). So, we have

\[
\text{div} \left( \frac{f_i}{f} \right) + c'_{f_i} - a_\xi = \text{div}(f_i) - \text{div}(f) + c'_{f_i} = c'_{f_i} - c'_{f} + c'_{f} - a_\xi = c'_{f_i} - a_\xi \geq 0.
\]

Thus, \( f_i/f \in L(c'_{f_i} - a_\xi) \). This implies that \( W_1 \subset L(c'_{f_i} - a_\xi) \). But there exists \( g \in W \) such that \( c'_{g}(a_\xi) = 0 \). Then \( c'_{g} - a_\xi \geq 0 \) is clearly not true.

Lemma 4-4. Assume that \( m \geq 4 \) is an even integer. Let \( W \subset S_m(\Gamma) \) be a subspace which separates the points of \( \mathcal{R}_\Gamma \). Select a basis \( f_0, \ldots, f_{s-1} \) for \( W \). Then, for each \( \xi \in X \) or a cusp for \( \Gamma \), there exists \( i \) such that \( c_{f_i}(a_\xi) = 0 \).

Proof. In view of [22], this has the same proof as the previous lemma.

Lemma 4-5. Assume that \( m \geq 4 \) is an even integer. Let \( W \subset M_m(\Gamma), \dim W \geq 3 \), be a subspace which generates the field of rational functions \( \mathbb{C}(\mathcal{R}_\Gamma) \), and separates the points of \( \mathcal{R}_\Gamma \). Then there exists a non-empty Zariski open set \( \mathcal{U} \subset W \) such that for any \( h \in \mathcal{U} \), we have that the field of rational functions \( \mathbb{C}(\mathcal{R}_\Gamma) \) is generated over \( \mathbb{C} \) by the rational functions \( g/f \) and \( h/f \), and \( \text{supp}(c_f) \cap \text{supp}(c_h) = \emptyset \) if \( W \subset S_m(\Gamma) \) or \( \text{supp}(c_f) \cap \text{supp}(c_h) = \emptyset \) if \( W \not\subset S_m(\Gamma) \).

Proof. For the matter of notation, we consider the case \( W \subset S_m(\Gamma) \). In the other case, one needs to replace all \( \xi \) with \( c' \).

We select a basis \( f_0, \ldots, f_{s-1} \) of \( W \), \( \dim W = s \geq 3 \) such that \( f = f_0 \) and \( g = f_1 \). By the assumption on \( W \), the field of rational functions \( \mathbb{C}(\mathcal{R}_\Gamma) \) is generated over \( \mathbb{C} \) by all \( f_i/f_0 \), \( 1 \leq i \leq s \). We let

\[
K = \mathbb{C}(f_1/f_0),
\]
and
\[ L = \mathbb{C}(R_T) = \mathbb{C}(f_1/f_0, \ldots, f_{s-1}/f_0) = K(f_2/f_0, \ldots, f_{s-1}/f_0). \]

By Lemma 3-1, \( f_2/f_0, \ldots, f_{s-1}/f_0 \) are all algebraic over \( K \). Thus, the field \( L \) is a finite algebraic extension of \( K \). It is also obviously separable. Hence, by a variant of a proof of Primitive Element Theorem there exists \( \lambda_2, \ldots, \lambda_{s-1} \in \mathbb{C} \) such that
\[ L = K((\lambda_2 f_2 + \cdots + \lambda_{s-1} f_{s-1})/f_0) = \mathbb{C}(f_1/f_0, \lambda_2 f_2 + \cdots + \lambda_{s-1} f_{s-1})/f_0). \]

Now, we explain the systematic way to get them all. For \( (\lambda_2, \ldots, \lambda_{s-1}) \in \mathbb{C}^{s-2} \), we consider the characteristic polynomial
\[ P(X, \lambda_2, \ldots, \lambda_{s-1}) = \det \left( X \cdot Id_L - T(f_{2} + \cdots + \lambda_{s-1} f_{s-1})/f_0 \right), \]
where \( T_x : L \to L \), is an \( \mathbb{K} \)-endomorphism given by \( T_x(y) = xy \), and \( Id_L \) is identity on \( L \). The resultant \( R \) with respect to the variable \( X \) of the polynomial \( P(X, \lambda_2, \ldots, \lambda_{s-1}) \) and its derivative \( \frac{\partial}{\partial X} P(X, \lambda_2, \ldots, \lambda_{s-1}) \) is a polynomial in \( \lambda_2, \ldots, \lambda_{s-1} \).

If \( R(\lambda_2, \ldots, \lambda_{s-1}) \neq 0 \), then \( (\lambda_2 f_2 + \cdots + \lambda_{s-1} f_{s-1})/f_0 \) generate \( L \) over \( K \). Indeed, the characteristic polynomial \( P(X, \lambda_2, \ldots, \lambda_{s-1}) \) has no multiple roots in the algebraic closure of \( L \). It also has the same roots as the minimal polynomial of \( (\lambda_2 f_2 + \cdots + \lambda_{s-1} f_{s-1})/f_0 \).

Thus, they are equal. Since the degree of the characteristic polynomial is equal to \([L : K]\), this element must be primitive. The first part of the proof assures that the resultant is not identically zero so that these considerations make sense.

Hence, primitive elements for the extension \( K \subset L \) are constructed from the set of all
\[ h = \lambda_2 f_2 + \cdots + \lambda_{s-1} f_{s-1} \in \mathbb{C} f_2 \oplus \cdots \oplus \mathbb{C} f_{s-1} \]
which belong to the Zariski open set defined by
\[ R(\lambda_2, \ldots, \lambda_{s-1}) \neq 0. \]

It does not affect the thing if we enlarge \( h \) to be
\[ h = \lambda_0 f_0 + \lambda_1 f_1 + \lambda_2 f_2 + \cdots + \lambda_{s-1} f_{s-1}, \]
where \( \lambda_0, \lambda_1 \) are arbitrary complex numbers. This means that \( h \) can be selected from the Zariski open subset of \( W \) given by \([1-6]\), where we consider the resultant \( R \) as a polynomial of all variables \( \lambda_0, \ldots, \lambda_{s-1} \) but which does not depend on the first two variables.

Now, we prove the last part of the lemma. By the second assumption on \( W \) and Lemma [4-4] for each \( a \in \text{supp}(c_{f_0}) \) there exists \( a_i \in \{1, \ldots, s-1\} \) such that \( a \not\in \text{supp}(c_{f_i}) \). Then, the rational functions \( f_i/f_{i_a} \) are defined at \( a \) since we have the following (see Lemma [2-1] (vi))
\[ \text{div} \left( \frac{f_i}{f_{i_a}} \right) = \text{div}(f_i) - \text{div}(f_{i_a}) = c_f - c_{f_a}, \]
where the right–most difference consists of effective divisors, so that the point \( a \) does not belong to the divisors of poles because of \( a \not\in \text{supp}(c_{f_i}) \).

Now, we can form the following product of non–zero linear forms in \( (\lambda_0, \ldots, \lambda_{s-1}) \in \mathbb{C}^s \)
\[ \prod_{a \in \text{supp}(c_{f_0})} \left( \frac{\lambda_0 f_0(f_a)}{f_{i_a}}(a) + \lambda_1 f_1(f_a) + \cdots + \lambda_{s-1} f_{s-1}(a) \right). \]
For $\sum_{i=0}^{s-1} \lambda_i f_i$ in a Zariski open subset of $W$, defined by making this product not equal to zero, neither of $a \in \text{supp}(c_{f_0})$ belong to the divisor of zeroes $\text{div}_0 \left( \frac{\sum_{i=0}^{s-1} \lambda_i f_i}{f_a} \right)$ of the corresponding rational function. Since $a \notin \text{supp}(c_{f_0})$ and $\text{div}_0 \left( \frac{\sum_{i=0}^{s-1} \lambda_i f_i}{f_a} \right) = \text{div}_\infty \left( \frac{\sum_{i=0}^{s-1} \lambda_i f_i}{f_a} \right) = c_{\sum_{i=0}^{s-1} \lambda_i f_i} - c_{f_a},$

where the right most expression is a difference of two effective divisors, we get

$a \in \text{supp}(c_{f_0}) \Rightarrow a \notin \text{supp}(c_{\lambda_0 f_0 + \lambda_1 f_1 + \cdots + \lambda_{s-1} f_{s-1}}).

Combining this with (4-6), we complete the proof of the lemma.

\begin{theorem}
Assume that $m \geq 4$ is an even integer. Let $W \subset M_m(\Gamma)$, $\dim W \geq 3$, be a subspace which generates the field of rational functions $\mathbb{C}(\mathcal{R}_\Gamma)$, and separates the points of $\mathcal{R}_\Gamma$. For example, if $\dim S_m(\Gamma) \geq \max (g(\Gamma) + 2, 3)$, then we can take $W = S_m(\Gamma)$. Let $f, g \in W$ be linearly independent. Then there exists a non–empty Zariski open set $U \subset W$ such that for any $h \in U$ we have the following:

(i) $\mathcal{R}_\Gamma$ is birationally equivalent to $\mathbb{C}(f, g, h)$, and

(ii) $\mathbb{C}(f, g, h)$ has degree equal to $\dim M_m(\Gamma) + g(\Gamma) - 1$ (resp., $\dim S_m(\Gamma) + g(\Gamma) - 1$) if $W \notin S_m(\Gamma)$ (resp., $W \subset S_m(\Gamma)$).

\begin{proof}
First of all, Lemmas 4-1 and 4-2 assure that $W = S_m(\Gamma)$ generates the field of rational functions $\mathbb{C}(\mathcal{R}_\Gamma)$, and separates the points of $\mathcal{R}_\Gamma$ whenever $\dim S_m(\Gamma) \geq \max (g(\Gamma) + 2, 3)$.

Now, go back to the general subspace which satisfies these conditions. We select the set $U \subset W$ given by Lemma 4-5. Since, by Lemma 4-5, the field of rational functions $\mathbb{C}(\mathcal{R}_\Gamma)$ is generated over $\mathbb{C}$ by the rational functions $g/f$ and $h/f$, we immediatelly get that the map given by Lemma 3-1 is birational equivalence. This proves (i).

Now, we prove (ii). Since, $\varphi$ is birational, by Theorem 3-5 we get $\deg(\varphi) = 1$, and, if $W \notin S_m(\Gamma)$, then

$$\deg \mathbb{C}(f, g, h) = \deg(\varphi) \cdot \deg \mathbb{C}(f, g, h) = \dim M_m(\Gamma) + g(\Gamma) - 1 - \sum_{a \in \mathcal{R}_\Gamma} \min (c'_f(a), c'_g(a), c'_h(a))$$

$$= \dim M_m(\Gamma) + g(\Gamma) - 1,$$

since $\text{supp}(c'_f) \cap \text{supp}(c'_h) = \emptyset$. The case $W \subset S_m(\Gamma)$ is treated similarly.

\end{proof}

5. APPLICATION TO MODULAR EQUATION

In this section we complete the proof of Theorem 1-1 following the approach explained in the introduction. We start the proof with the following well–known lemma:
Lemma 5-1. Assume that $\Gamma = SL_2(\mathbb{Z})$. Then, we have the following:

$$\text{div}(\Delta) = a_\infty$$

$$\text{div}(E_4) = \frac{1}{3}a_{(1+\sqrt{-3})/2}$$

$$\text{div}(E_4^3) = a_{(1+\sqrt{-3})/2}.$$  

Proof. By Lemma 2-1 (iv), we get $\deg(\text{div}(\Delta)) = 1$. Since $\Delta$ is a cusp form, the first formula follows. Again, by Lemma 2-1 (iv), we get $\deg(\text{div}(E_4)) = 1/3$. Set $\epsilon = (1 + \sqrt{-3})/2$ and $\gamma = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. Then $\gamma \epsilon = \epsilon$, and we have

$$E_4(\epsilon) = E_4(\gamma \epsilon) = j(\gamma, \epsilon)^4 E_4(\epsilon) \implies E_4(\epsilon) = 0,$$  

since $j(\gamma, \epsilon)^4 = \epsilon^4 = -\epsilon \neq 1$. Thus, by the preliminary considerations in Section 2, we obtain the second formula. The third formula is a direct consequence of the second. □

In the remainder of this section we let $\Gamma = \Gamma_0(N)$ and assume that $N \geq 2$. We warn the reader that we compute div with respect to $\Gamma_0(N)$, not with respect to $SL_2(\mathbb{Z})$ as in the previous lemma.

Lemma 5-2. Assume that $\Gamma = \Gamma_0(N)$ and $N \geq 2$. Set $\epsilon = (1 + \sqrt{-3})/2$. Then, by considering $\Delta, E_4^3 \in M_{12}(\Gamma_0(N))$, we have the following:

$$\text{div}(\Delta) = \sum_{\gamma \in \Gamma_0(N) \setminus SL_2(\mathbb{Z})/SL_2(\mathbb{Z})_\infty} a_{\gamma, \infty} = \sum_{b \in X_0(N), \text{cusp}} b$$

$$\text{div}(E_4^3) = \sum_{\gamma \in \Gamma_0(N) \setminus SL_2(\mathbb{Z})/SL_2(\mathbb{Z})_c} m_{\gamma} a_{\gamma, \epsilon}$$

$$\text{div}(E_4^3(N \cdot)) = \sum_{\gamma \in \Gamma_0(N) \setminus \{ \frac{1}{N} \gamma \epsilon; \gamma \in SL_2(\mathbb{Z}) \}} m_{\gamma} a_{\gamma, \epsilon},$$

where $m_{\gamma} \geq 1$ in both cases. Finally, for $\Delta(N \cdot) \in S_{12}(\Gamma_0(N))$, $\text{div}(\Delta(N \cdot))$ has support among the cuspidal points.

Proof. The first formula follows from the construction of the divisor explained in Section 2 and the first formula of Lemma 5-1. For the second and third formula, we observe that Lemma 5-1 implies that $SL_2(\mathbb{Z})$–orbit of $\epsilon$ are only zeroes of $E_4$. Some of them are elliptic for $\Gamma_0(N)$ and some are not. But, since elliptic among them are of order 3 and $m = 12$, we see that by Lemma 2-1 (vi) we have $\epsilon_{E_4^3} = \text{div}(E_4^3)$. This immediately implies the second formula. For the third, only zeroes of $E_4^3(N \cdot)$ are in the set $\{ \frac{1}{N} \gamma \epsilon; \gamma \in SL_2(\mathbb{Z}) \}$, and the claim follows. The last claim is obvious from Lemma 5-1. □

We remark that $\Delta(N \cdot) \Delta, E_4^3(N \cdot) \Delta \in S_{24}(\Gamma_0(N))$. So, the divisors $c_{\Delta(N \cdot)\Delta}$ and $c_{E_4^3(N \cdot)\Delta}$ are well–defined (see (2-2)).
Lemma 5-3. Maintaining the assumptions of Lemma 5-2, have that the support of \( c_{E_4^3(N)\Delta} \) is \( \{ a_{\gamma,\epsilon} : \gamma \in \Gamma_0(N) \setminus \{ \frac{1}{N}\gamma,\epsilon ; \gamma \in SL_2(\mathbb{Z}) \} \} \), and and \( c_{\Delta(N)\Delta} \) has support among the cuspidal points.

Proof. By the previous lemma, we have

\[
\text{div}(E_4^3(N)\Delta) = \text{div}(E_4^3(N)) + \text{div}(\Delta) = \sum_{\gamma \in \Gamma_0(N) \setminus \{ \frac{1}{N}\gamma,\epsilon ; \gamma \in SL_2(\mathbb{Z}) \}} m_{\gamma} a_{\gamma,\epsilon} + \sum_{b \in X_0(N), \text{cusp}} b.
\]

Since any elliptic point of \( \Gamma_0(N) \) has order 2 or 3, Lemma 2-1 (vi) applied to \( m = 24 \) implies that

\[
c'_{E_4^3(N)\Delta} = \text{div}(E_4^3(N)\Delta).
\]

Thus, the claim follows from (2-2). Similarly, we prove the last claim of the lemma. \( \square \)

Having Lemma 5-3, it is easy to complete the proof of Theorem 1-1. We consider the regular map given by (1-2). As we indicated in the introduction this map is birational. Thus, by Theorem 3-5, we have the following formula for the degree of the corresponding curve which is the same as the degree of \( N \)-th modular polynomial \( \Phi_N \)

\[
\deg (\Phi_N) = \dim S_{24}(\Gamma_0) + g(X_0(N)) - 1 - \sum_{a \in X_0(N)} \min \left( c_{\Delta(N)\Delta}(a), c_{E_4^3(N)\Delta}(a), c_{E_4^3(N)\Delta}(a) \right).
\]

But, Lemma 5-3 implies that

\[
\min \left( c_{\Delta(N)\Delta}(a), c_{E_4^3(N)\Delta}(a), c_{E_4^3(N)\Delta}(a) \right) = 0
\]

holds for \( a \in X_0(N) \) since the supports of \( c_{\Delta(N)\Delta} \) and \( c_{E_4^3(N)\Delta} \) are disjoint.

Now, let us write \( \nu_2(\Gamma_0(N)) \), \( \nu_3(\Gamma_0(N)) \), and \( \nu_\infty(\Gamma_0(N)) \) for the number of inequivalent elliptic points of order 2, inequivalent elliptic points of order 3, and inequivalent cusps for \( \Gamma_0(N) \), respectively. Then, inserting explicit formulas for \( \dim S_{24}(\Gamma_0(N)) \) (see Lemma 2-1 (v)), and recalling that elliptic points of \( \Gamma_0(N) \) are of order 2 or 3, we obtain

\[
\deg (\Phi_N) = 24(g(\Gamma_0(N)) - 1) + 11\nu_\infty(\Gamma_0(N)) + 6\nu_2(\Gamma_0(N)) + 8\nu_3(\Gamma_0(N)).
\]

Since (see [1], Theorem 4.2.11)

\[
g(\Gamma_0(N)) = 1 + \frac{1}{12} [SL_2(\mathbb{Z}) : \Gamma_0(N)] = \frac{\nu_2(\Gamma_0(N))}{4} - \frac{\nu_3(\Gamma_0(N))}{3} - \frac{\nu_\infty(\Gamma_0(N))}{2},
\]

we find

\[
\deg (\Phi_N) = 2[SL_2(\mathbb{Z}) : \Gamma_0(N)] - \nu_\infty(\Gamma_0(N)).
\]

Combining with ([1], Theorems 4.2.5 and 4.2.7), we find the second formula in the theorem. This completes the proof of Theorem 1-1.
6. Existence of Integral models

The goal of this section is to prove the following corollary to Theorem 4-7 (stated as Theorem 1-4 in the Introduction):

**Corollary 6-1.** Assume that \( N \not\in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\} \) (so that the genus \( g(\Gamma_0(N)) \geq 1 \)). Assume that \( m \geq 4 \) (if \( N \neq 11 \)) and \( m \geq 6 \) (if \( N = 11 \)) is an even integer. Let \( f, g \in S_m(\Gamma_0(N)) \) be linearly independent with integral \( q \)-expansions. Then, there exists infinitely many \( h \in S_m(\Gamma_0(N)) \) with integral \( q \)-expansion such that we have the following:

(i) \( X_0(N) \) is birationally equivalent to \( C(f, g, h) \),

(ii) \( C(f, g, h) \) has degree equal to \( \dim S_m(\Gamma_0(N)) + g(\Gamma_0(N)) - 1 \) (this number can be easily explicitly computed using Lemma 2-1(v) and (5-4)); if \( N = 11 \), then the minimal possible degree achieved (for \( m = 6 \)) is 4, and if \( N \neq 11 \), then the minimal possible degree achieved (for \( m = 4 \)) is

\[
\frac{1}{3} \psi(N) - \frac{1}{3} \nu_3 - \sum_{d > 0, d \mid N} \phi((d, N/d)),
\]

where \( \nu_3 \) is the number of elliptic elements of order three on \( X_0(N) \), \( \nu_3 = 0 \) if \( 9 \mid N \), and \( \nu_3 = \prod_{p \mid N} \left(1 + \left(\frac{-3}{p}\right)\right) \) otherwise.

(iii) the equation of \( C(f, g, h) \) has integral coefficients.

**Proof.** First, by Eichler–Shimura theory, for each even integer \( m \geq 2 \) the space of cusp forms \( S_m(\Gamma) \) has a basis as a complex vector space consisting of forms which have integral \( q \)-expansions. So, if we \( f \) and \( g \) with integral coefficients in their \( q \)-expansions, then we can select infinitely many \( h \) which also have integral coefficients in their \( q \)-expansions. This is because \( \mathbb{Z}^l \) and a complement of finite subset of it are Zariski dense in \( \mathbb{C}^l \), for any \( l \geq 1 \). As a consequence, since the polynomial equation of \( C(f, g, h) \), after inserting the \( q \)-expansions for \( f, g, \) and \( h \), produces a homogeneous system with integral coefficients which has the coefficients of the polynomial as a unique solution up to a scalar, the coefficients can be taken to be integral as well. At the end, to apply Theorem 4-7 so that above discussion is valid, we need to assure that \( \dim S_m(\Gamma_0(N)) \geq \max \left(g(\Gamma_0(N)) + 2, 3\right) \). Since we assume that \( g(\Gamma_0(N)) \geq 1 \), we only require that \( \dim S_m(\Gamma_0(N)) \geq g(\Gamma_0(N)) + 2 \). Using Lemma 2-1(v), and the notation introduced at the end of Section 5, we obtain

\[
\dim S_m(\Gamma_0(N)) = (m - 1)(g(\Gamma_0(N)) - 1) + \left(\frac{m}{2} - 1\right) \nu_\infty(\Gamma_0(N)) + \\
+ \left[\frac{m}{4}\right] \nu_2(\Gamma_0(N)) + \left[\frac{m}{3}\right] \nu_3(\Gamma_0(N)).
\]

By (4, Theorem 4.2.7), we have

\[
\nu_\infty(\Gamma_0(N)) = \sum_{d > 0, d \mid N} \phi((d, N/d)) \geq 3
\]
unless $N$ is prime number in which case $\nu_\infty(\Gamma_0(N)) = 2$. Next, unless $\nu_2(\Gamma_0(N)) = \nu_3(\Gamma_0(N)) = 0$, above formula shows that for $m = 4$ we have
\[
\dim S_4(\Gamma_0(N)) \geq 3(g(\Gamma_0(N)) - 1) + 2 \left( \frac{4}{2} - 1 \right) + 1 = 3g(\Gamma_0(N)) \geq g(\Gamma_0(N)) + 2,
\]
since we assume that $g(\Gamma_0(N)) \geq 1$. Similarly we have if $\nu_2(\Gamma_0(N)) = \nu_3(\Gamma_0(N)) = 0$ but $N$ is not prime. It remains to consider the case $N$ is prime and $\nu_2(\Gamma_0(N)) = \nu_3(\Gamma_0(N)) = 0$. In this case
\[
\dim S_4(\Gamma_0(N)) = 3g(\Gamma_0(N)) - 1 \geq g(\Gamma_0(N)) + 2
\]
if and only if $g(\Gamma_0(N)) \geq 2$. It remains to consider the case $N$ is prime, $\nu_2(\Gamma_0(N)) = \nu_3(\Gamma_0(N)) = 0$, and $g(\Gamma_0(N)) = 1$. In this case (5.1) gives us $[SL_2(\mathbb{Z}) : \Gamma_0(N)] = 12$. Applying (4.2.5), we see that $\psi(N) = N + 1 = 12$ since $N$ is prime. Hence, $N = 11$. In this case, we use (4.2.5) to check that we indeed have $\nu_2(\Gamma_0(11)) = \nu_3(\Gamma_0(11)) = 0$ and $g(\Gamma_0(N)) = 1$. This gives us $\dim S_4(\Gamma_0(11)) = 2$ and $\dim S_6(\Gamma_0(11)) = 4$. In this case is $\dim S_6(\Gamma_0(11)) + g(\Gamma_0(11)) - 1 = 4$.

Apart from this case, we can use $m = 4$, which gives us the formula
\[
\dim S_4(\Gamma_0(N)) + g(\Gamma_0(N)) - 1 = \frac{1}{3} \psi(N) - \frac{1}{3} \nu_3(\Gamma_0(N)) - \nu_\infty(\Gamma_0(N)).
\]
Now, we apply (5.1, Theorem 4.2.5) to complete the proof of the corollary. \hfill \Box

7. AN IMPROVEMENT OF THEOREM 4-7

The goal of this section is to prove a corollary to Theorem 4-7 (stated as Theorem 1-4 in the Introduction) and its improvement. We prove necessary lemmas first.

**Lemma 7-1.** Let $N \geq 2$. Then, $\Delta, E_4^3, \Delta(\cdot \cdot)$, and $E_4^3(\cdot \cdot)$ are linearly independent.

**Proof.** We write their $q$–expansions
\[
\Delta = q - 24q^2 + 252q^3 + \cdots
\]
\[
E_4^3 = 1 + 720q + 172800q^2 + 13824000q^3 + \cdots
\]
\[
\Delta(\cdot \cdot) = q^{-N} - 24q^{2N} + 252q^{3N} + \cdots
\]
\[
E_4^3(\cdot \cdot) = 1 + 720q^N + 172800q^{2N} + 13824000q^{3N} + \cdots.
\]

Now, assume that for $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ we have
\[
\alpha \Delta + \beta E_4^3 + \gamma \Delta(\cdot \cdot) + \delta E_4^3(\cdot \cdot) = 0.
\]

Inserting $q$–expansions in that expression, the coefficients of $q^0$ and $q$ must be equal to zero i.e., $\beta + \delta = 0$ and $\alpha + 720\beta = 0$. If $N > 2$, then $-24\alpha + 172800\beta = 0$ is a coefficient of $q^2$. If $N = 2$, then $252\alpha + 13824000\beta = 0$ is a coefficient of $q^3$. In either case, we get immediately $\alpha = \beta = \gamma = \delta = 0$. \hfill \Box

**Lemma 7-2.** Let $N \geq 2$. Then, by considering $\Delta$ and $E_4^3$ as modular forms of $\Gamma_0(N)$, we have $\text{supp}(\mathcal{C}_\Delta) \cap \text{supp}(\mathcal{C}_{E_4^3}) = \emptyset$. In particular, a four–dimensional subspace $W \subset M_{12}(\Gamma_0(N))$ spanned by $\Delta, E_4^3, \Delta(\cdot \cdot)$, and $E_4^3(\cdot \cdot)$ separates points on $X_0(N)$.
Proof. We use the expressions for $\text{div}(\Delta)$ and $\text{div}(E_4^3)$ from Lemma 5-2, and the definition of $c'_\Delta$ and $c'_{E_4^3}$ Lemma 2-1 (vi) to see that $\text{supp}(c'_\Delta) \cap \text{supp}(c'_{E_4^3}) = \emptyset$. 

Corollary 7-3. Let $N \geq 2$. Then, there exists infinitely many $(\alpha, \beta, \gamma, \delta) \in \mathbb{Z}^4$ such that $X_0(N)$ is birational with $C(\Delta, E_4^3, \alpha \Delta + \beta E_4^3 + \gamma \Delta(N:\cdot) + \delta E_4^3(N:\cdot))$, and

$$\deg C(\Delta, E_4^3, \alpha \Delta + \beta E_4^3 + \gamma \Delta(N:\cdot) + \delta E_4^3(N:\cdot)) = \psi(N).$$

Proof. We observe that $W \not\subset S_{12}(\Gamma_0(N))$. Next, $W$ separates points on $X_0(N)$ by Lemma 7-2. It also generates the field of rational functions on $X_0(N)$ (see the Introduction). This shows that we can apply Theorem 4-7. We just observe that $\mathbb{Z}^4$ is Zariski dense in $\mathbb{C}^4$, and that the same holds for a complement of a finite subset in $\mathbb{Z}^4$. The curves are of degree $\dim M_{12}(\Gamma_0(N)) + g(\Gamma_0(N)) - 1$. Finally, we compute $\dim M_{12}(\Gamma_0(N)) + g(\Gamma_0(N)) - 1$ using similar computations to those made at the end of Section 5. We leave details to the reader. 

The following result is an improvement of Theorem 4-7.

Theorem 7-4. Let $N \geq 2$. Then, there exists infinitely many pairs $(\alpha, \beta) \in \mathbb{Z}^2$ such that $X_0(N)$ is birational with $C(\Delta, E_4^3, \alpha \Delta(N:\cdot) + \beta E_4^3(N:\cdot))$, and

$$\deg C(\Delta, E_4^3, \alpha \Delta(N:\cdot) + \beta E_4^3(N:\cdot)) = \psi(N).$$

Proof. For $W$ defined by Lemma 7-2 we let $f_0 = \Delta$, $f_1 = E_4^3$, $f_2 = \Delta(N:\cdot)$, $f_3 = E_4^3(N:\cdot)$. This is a basis of $W$ in the notation of the proof of Lemma 4-5. In our case the resultant $R(\lambda_2, \lambda_3)$ from the proof of Lemma 4-5 is used to secure that $(\lambda_2 f_2 + \lambda_3 f_3)/f_0$ is a primitive element of appropriate extension if and only if $R(\lambda_2, \lambda_3) \neq 0$ (see (4-6)). The remainder of the proof of Lemma 4-5 is not relevant for us since we have the first claim of Lemma 7-2 at our disposal: $\text{supp}(c'_\Delta) \cap \text{supp}(c'_{E_4^3}) = \emptyset$. With this in hand, the proof of Theorem 4-7 is easy to modify so that with the help of arguments in the proof of Corollary 7-3 we can complete the proof. 

References

[1] R. Bröker, K. Lauter, A. V. Sutherland, Modular polynomials via isogeny volcanoes, Mathematics of Computation 81 (2012), 1201–1231.
[2] B. Cho, N. M. Kim, J. K. Koo, Affine models of the modular curves $X(p)$ and its application, Ramanujan J. 24 (2011), no. 2, 235-257.
[3] S. Galbraith, Equations for modular curves, Ph.D. thesis, Oxford 1996.
[4] T. Miyake, Modular forms, Springer-Verlag (2006).
[5] R. Miranda, Algebraic Curves and Riemann Surfaces, Graduate Studies in Mathematics 5 (1995).
[6] G. Muić, Modular curves and bases for the spaces of cuspidal modular forms, Ramanujan J. 27 (2012), 181-208.
[7] G. Muić, On embeddings of curves in projective spaces, preprint [http://web.math.pmf.unizg.hr/~gmuic/papers.html].
[8] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Kan Memorial Lectures, No. 1. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971.
[9] M. Shimura, *Defining Equations of Modular Curves* $X_0(N)$, Tokyo J. Math. Vol. 18, No. 2, 1995.
[10] Y. Yifan, *Defining equations of modular curves*, Advances in Mathematics 204 (2006) 481-508.

Department of Mathematics, University of Zagreb, Blijenička 30, 10000 Zagreb, Croatia
E-mail address: gmuic@math.hr