Monatsh Math
https://doi.org/10.1007/s00605-018-1161-3

On a simple model of $X_0(N)$

Iva Kodrnja[1]

Received: 4 April 2017 / Accepted: 31 January 2018

Abstract We find plane models for all $X_0(N)$, $N \geq 2$. We observe a map from the modular curve $X_0(N)$ to the projective plane constructed using modular forms of weight 12 for the group $\Gamma_0(N)$; the Ramanujan function Δ, $\Delta(N\cdot)$ and the third power of Eisestein series of weight 4, E_4^3, and prove that this map is birational equivalence for every $N \geq 2$. The equation of the model is the minimal polynomial of $\Delta(N\cdot)/\Delta$ over $\mathbb{C}(j)$.

Keywords Modular forms · Modular curves · Birational equivalence · Modular polynomial

Mathematics Subject Classification 11F11 · 11F23

1 Introduction

The recent paper [13] by Muić presents a new method of finding defining equations for modular curves. As an application of the method one example was presented—a map from $X_0(N)$ to the projective plane defined by

$$\mathfrak{a}_z \mapsto \left(\Delta(z) : E_4^3(z) : \Delta(Nz)\right), \tag{1.1}$$

Communicated by A. Constantin.

The author acknowledges Croatian Science Foundation Grant No. 9364.

✉ Iva Kodrnja
ikodrnja@grad.hr

[1] Faculty of Civil Engineering, University of Zagreb, Kačićeva 26, 10000 Zagreb, Croatia

Published online: 07 February 2018

where

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

is the usual Eisenstein series and

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

is the Ramanujan delta function.

Modular curves are defined as quotient spaces of the action of a Fuchsian group [in the case of $X_0(N)$ the group is the congruence subgroup $\Gamma_0(N)$] on the complex upper half-plane and when compactified by adding cusps, they have the structure of a compact Riemann surface. This kind of objects are also (complex) algebraic curves. This connection for the modular curves, as well as their relation to elliptic curves is extensively studied in [4].

For a modular curve observed as a Riemann surface, the field of meromorphic functions is isomorphic to the field of modular functions for the subgroup defining this Riemann surface and we know that this field is transcendental over $\mathbb{C}$ of degree one and also isomorphic to the field of rational functions of the algebraic curve. One way to find the equation of the algebraic curve is to find the generators of the rational function field.

If there is more than one generator, we know that they are connected with a polynomial relation. This is true because if we choose one generator, say f, then all other generators are algebraic over the field $\mathbb{C}(f)$. This polynomial is then the equation of this algebraic curve. The standard method for computing this polynomial consists of computing the Fourier expansions of modular functions and solving a linear system of equations.

Hence, using modular functions in the presented way, we can find equations of modular curves. The first example is the standard model for $X_0(N)$, whose (affine) equation is the polynomial relation between the modular j function defined by

$$j(z) = \frac{E_4^3(z)}{\Delta(z)}, \tag{1.2}$$

which is also Hauptmodul (the sole generator) for the genus zero curve $X_0(1)$, and the modular function $j(N\cdot)$. This polynomial is called the classical modular polynomial or modular equation and is the minimal polynomial of $j(N\cdot)$ over $\mathbb{C}(j)$. It is canonical in the sense that it contains informations over the relations of $X_0(N)$ and elliptic curves, see [4].

Mathematician have also searched for other generators of modular function fields of various modular curves and used them to find their equations.

In [5,6], Ishida and Ishii find generators for function fields of $X(N)$ and $X_1(N)$. In the first case this generators are functions constructed using Klein forms, and in

the second case generators are derived using the Weierstrass $\wp$-function. We use their argument in proving Theorem 1.1.

We would also like to mention the paper [15] by Young which provides equations for $X_0(N)$ and as well for $X(N)$ and $X_1(N)$. Young uses the following claim; if we take two modular functions with relatively prime degrees of divisors of poles, then these two functions must generate the modular function field. He then proves that two such functions (with poles only at infinity) can always be found within a group of modular functions of $\Gamma_1(N)$ whose divisors are supported by the cusps lying above ∞ on $X_0(N)$. Furthermore, he proves that this group is precisely the group of certain products of generalized Dedekind eta-functions. His equations are the most simple and beautiful given they have the smallest degrees and smallest coefficients.

On the other hand, compact Riemann surfaces can always be embedded into some projective space and their image is then a projective curve. This embedding is canonically done using differentials, but given the relations between differentials on modular curves and modular forms of the underlaying Fuchsian group, it can also be done with modular forms, as we see in the example presented at the beginning.

Furthermore, given that modular curves are algebraic curves, we can use modular forms to construct maps into some projective space and then analyze whether the image curve and the modular curve are birational by analyzing their function fields.

The method for finding models of modular curves using modular forms on the defining group is developed by Muić in [11–13]. We give a short overview of this method in Sect. 2.

Let us return to the example. The image of the map (1.1) is an irreducible plane projective curve which we denote by $\mathcal{C}_N$. In ([13], Lemmas 5.4 and 5.5), it is proved that the curve $\mathcal{C}_p$ is birational to $X_0(p)$ for every prime number p and a question was posed whether the map is always birational.

We answer that question and prove that this is true for every number $N \geq 2$.

Theorem 1.1 *The curve $\mathcal{C}_N$ is birational to $X_0(N)$ for every $N \geq 2$.*

We will see that the modular forms defining the map are connected to the generators of the rational functions field of the image curve; these generators are their quotients. In this light, we can restate Theorem 1.1 in the following way:

Corollary 1.1 *Modular functions j and $\Delta(N\cdot)/\Delta$ generate $\mathbb{C}(X_0(N))$.*

These results give us simple models for all $X_0(N)$. In Sect. 3 we compute the degree of this model and see that it is equal to

$$\Psi(N) = N \prod_{p|N} (1 + 1/p), \tag{1.3}$$

which is also the index of the subgroup $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$. This is slightly better than the standard model, where $\Psi(N)$ is the degree in each of the two variables.

Some examples of equations (in affine versions) are in the end of Sect. 3 and even for very small values of N, these numbers are huge.

The classical modular equation is very hard to compute [3] and so are other modular polynomials for different modular functions (§7 of [3] or [1]) and this is also the case

for our polynomials. In Sect. 3 we explain the computations of equations and the limitations of the mentioned standard method for computing equations.

As computed in [2], the explicit bound for the logarithmic height of the modular polynomial of prime level l is

$$6l\log(l) + 18l.$$

It would be interesting to compute the height of our polynomials, and we believe that the bound would be very close to this one.

I would like to thank G. Muić for introducing me into this very interesting subject and for many useful conversations and advices.

2 Maps to projective plane

Let Γ be a Fuchsian group of first order. The quotient space of the complex upper half-plane $\mathbb{H}$ by the action of Γ is a Riemann surface which we will denote $X(\Gamma)$. This set can be compactified by adding orbits of cusps of Γ. For $\Gamma = \Gamma_0(N)$, this compact Riemann surface is denoted by $X_0(N)$ and called modular curve.

The main idea of [13] is to map $X(\Gamma)$ to the projective plane $\mathbb{P}^2$ using modular forms. It is achieved in the following way:

Select $k \geq 2$ such that $\dim M_k(\Gamma) \geq 3$. Take three linearly independent modular forms f, g and h in $M_k(\Gamma)$ and construct the map $X(\Gamma) \mapsto \mathbb{P}^2$ by defining it on the complement of points in $X(\Gamma)$ which are orbits of common zeros of f, g and h by

$$\mathfrak{a}_z \mapsto (f(z) : g(z) : h(z)). \tag{2.1}$$

The map defined in this way is uniquely determined holomorphic map from the Riemann surface $X(\Gamma)$ to $\mathbb{P}^2$. It is actually a rational (in fact regular because the domain is compact) map

$$\mathfrak{a}_z \mapsto (1 : g(z)/f(z) : h(z)/f(z)).$$

The image is an irreducible projective curve which we denote by $\mathcal{C}(f, g, h)$, whose degree is less or equal to $\dim M_k(\Gamma) + g(\Gamma) - 1$. This bound for $\deg(\mathcal{C}(f, g, h))$ equals the degree of integral divisors attached to modular forms f, g and h and can be shown by calculating the number of points in the intersection of $\mathcal{C}(f, g, h)$ with a line in general position (see [13], Lemma 2.2 (vi) for integral divisors).

The degree of the map (2.1) is defined as the degree of the field extension

$$\mathbb{C}(\mathcal{C}(f, g, h)) \subset \mathbb{C}(X(\Gamma)), \tag{2.2}$$

and we denote it by $d(f, g, h)$.

The field of rational functions $\mathbb{C}(\mathcal{C}(f, g, h))$ of the image curve is isomorphic to a subfield of $\mathbb{C}(X(\Gamma))$ generated over $\mathbb{C}$ by g/f and h/f. Therefore, the map (2.1) is birational equivalence if and only if g/f and h/f generate $\mathbb{C}(X(\Gamma))$.

In [13], the following formula for the degree of the image curve $\mathcal{C}(f, g, h)$ was proved (see [13], Corollary 1.5):

Theorem 2.1 *Assume that $k \geq 2$ is an integer such that $\dim(M_k(\Gamma)) \geq 3$. Let f, g, $h \in M_k(\Gamma)$ be three linearly independent modular forms. Then, we have the following:*

$$d(f, g, h) \deg \mathcal{C}(f, g, h) = \dim(M_k(\Gamma)) + g(\Gamma) - 1 - \sum_{\mathfrak{a} \in X(\Gamma)} \min\left(\mathfrak{c}'_f(\mathfrak{a}), \mathfrak{c}'_g(\mathfrak{a}), \mathfrak{c}'_h(\mathfrak{a})\right),$$

where $\mathfrak{c}'_f$, $\mathfrak{c}'_g$ and $\mathfrak{c}'_h$ are integral divisors attached to modular forms f, g and h.

3 Proof of Theorem 1.1

For a non-constant function $f \in \mathbb{C}(X(\Gamma))$, the degree of the subfield generated by f equals the degree of the divisor of poles of f (see [9], §6) which we will denote by

$$d(f) = \deg(\mathrm{div}_\infty(f)) = [\mathbb{C}(X(\Gamma)) : \mathbb{C}(f)]. \tag{3.1}$$

Returning to the map (2.1) we have an easy condition for birational equivalence:

Lemma 3.1 *The map (2.1) is a birational equivalence if*

$$\gcd(d(g/f), d(h/f)) = 1.$$

Proof The field of rational functions $\mathbb{C}(\mathcal{C}(f, g, h))$ is isomorphic to a subfield $\mathbb{C}(g/f, h/f) \subseteq \mathbb{C}(X_0(N))$ and the degree of this subfield is precisely $d(d, f, g)$. Birational equivalence means that $d(f, g, h) = 1$. Let us see that this is the case with given conditions. For the modular function g/f we have the following field extensions:

$$\mathbb{C}(g/f) \subseteq \mathbb{C}(g/f, h/f) \subseteq \mathbb{C}(X(\Gamma)),$$

where the second extension is of degree $d(f, g, h)$. From the definition (3.1) of $d(g/f)$ we have

$$d(f, g, h) | d(g/f).$$

The same is true for the function h/f. Hence, if $d(f, g, h)$ divides two relatively prime numbers, it must be equal to 1. □

The converse is not true. For the map (1.1) when $N > 2$ the degrees of divisors of poles of j and $\Delta(N\cdot)/\Delta$ are always divisible by 2.

But we can look at other functions in $\mathbb{C}(\mathcal{C}(f, g, h))$. This is an argument which is used in ([5], Lemma 2) to find generators of modular function fields for modular curves $X(N)$ and $X_1(N)$.

Lemma 3.2 *If there are two non-constant functions f_1 and f_2 in $\mathbb{C}(g/f, h/f)$ such that $\gcd(d(f_1), d(f_2)) = 1$, then the map (2.1) is a birational equivalence.*

Proof The map (2.1) is birational equivalence if $d(f, g, h) = 1$, where $d(f, g, h)$ is given by (2.2) and is also the degree of $\mathbb{C}(g/f, h/f) \subseteq \mathbb{C}(X(\Gamma))$. Since $f_1 \in \mathbb{C}(g/f, h/f)$, we have a sequence of fields

$$\mathbb{C}(f_1) \subseteq \mathbb{C}(g/f, h/f) \subseteq \mathbb{C}(X(\Gamma)).$$

The degree of

$$\mathbb{C}(f_1) \subseteq \mathbb{C}(X(\Gamma))$$

is $d(f_1)$, by definition (3.1). We conclude that $d(f, g, h)$ must divide $d(f_1)$.

The same holds for the function f_2, $d(f, g, h)$ must divide $d(f_2)$. Hence, $d(f, g, h)$ is a common divisor of two relatively prime numbers $d(f_1)$ and $d(f_2)$ and so must be equal to 1. □

We can now prove Theorem 1.1.

Proof We look at the following two non-constant functions in $\mathbb{C}\,(j, \Delta(N\cdot)/\Delta)$:

$$f_1 = j \quad \text{and} \quad f_2 = j^{N-2} + \left(\frac{\Delta(N\cdot)}{\Delta}\right)^{N-1}.$$

We compute $d(f_1)$ and $d(f_2)$ and show that these numbers are relatively prime.

First, we need the divisors of modular forms Δ, $\Delta(N\cdot)$ and E_4^3. They are computed in ([13], Lemma 4.3). For our purpose, it is important that E_4^3 has zeros in the $\Gamma_0(N)$-orbits of $(1 + \sqrt{(-3)})/2$ and that Δ and $\Delta(N\cdot)$ have zeros at cusps of $\Gamma_0(N)$ so supports of their divisors are disjoint.

The full set of representatives of cusps of $\Gamma_0(N)$ is the set of rational numbers c/d where d is a positive divisor of N, $\gcd(c, d) = 1$ and there are $\varphi(\gcd(d, N/d))$ representatives with denominator d, where φ denotes the Euler function(see [8], Proof of Theorem 4.2.7).

Divisors of Δ and $\Delta(N\cdot)$ are ([13], Lemma 4.2):

$$\operatorname{div}(\Delta) = \sum_{\substack{d|N \\ 1\le d\le N}} \frac{N}{d}\frac{1}{\gcd(d, N/d)}\mathfrak{a}_{c/d}$$

$$\operatorname{div}(\Delta(N\cdot)) = \sum_{\substack{d|N \\ 1\le d\le N}} \frac{d}{\gcd(d, N/d)}\mathfrak{a}_{c/d}.$$

Now, the divisor of poles of f_1 is minus the divisor of Δ and its degree is

$$d(f_1) = \sum_{\substack{d|N \\ 1\le d\le N}} \frac{N}{d}\frac{\varphi(\gcd(d, N/d))}{\gcd(d, N/d)} = \Psi(N). \tag{3.2}$$

where $\Psi(N)$ is the Dedekind Psi function defined in (1.3), (also see [13], end of Section 4).

Let us compute the degree of divisor of poles of f_2. We start with finding its divisor. Function $\Delta(N\cdot)/\Delta$ has poles at cusps where Δ has zero of greater order than $\Delta(N\cdot)$, and that happens precisely at the cusps c/d for $d - N/d < 0$, that is for $d < \sqrt{N}$. Therefore, we have

$$\operatorname{div}_\infty(\Delta(N\cdot)/\Delta) = \sum_{\substack{d|N \\ 1\le d\le \sqrt{N}}} \frac{N/d - d}{\gcd(d, N/d)}\mathfrak{a}_{c/d}.$$

The function j^{N-2} has poles at all cusps of $\Gamma_0(N)$ and we conclude that f_2 has poles at all cusps. In the cusps c/d where $d \ge \sqrt{N}$ the order of pole equals the order of pole of j^{N-2} whereas in the cusps c/d for $d < \sqrt{N}$ the order of pole is the greater of orders of poles of j^{N-2} and $(\Delta(N\cdot)/\Delta)^{N-1}$. Hence we have

$$\begin{aligned} d(f_2) = &\sum_{\substack{d|N \\ 1\le d\le \sqrt{N}}} \frac{\varphi(\gcd(d, N/d))}{\gcd(d, N/d)} \max\left(\frac{N}{d}(N-2), \left(\frac{N}{d} - d\right)(N-1)\right) \\ &+ \sum_{\substack{d|N \\ d\ge \sqrt{N}}} \frac{\varphi(\gcd(d, N/d))}{\gcd(d, N/d)}\frac{N}{d}(N-2). \end{aligned} \tag{3.3}$$

The maximum appearing in formula (3.3) equals $\frac{N}{d}(N-2)$ for $d > 1$ and for $d = 1$ the maximum is $(N-1)^2 = N(N-2) + 1$ and we have

$$d(f_2) = N(N-2) + 1 + \sum_{\substack{d|N \\ 1< d\le N}} \frac{\varphi(\gcd(d, N/d))}{\gcd(d, N/d)}\frac{N}{d}(N-2) = (N-2)d(f_1) + 1. \tag{3.4}$$

Since $\gcd(d(f_1), d(f_2)) = 1$, Lemma 3.2 implies that $d_N = 1$ and we have proved Theorem 1.1. □

We have shown that the degree of the map (1.1) is one, in other words this map is birational equivalence. We can now also compute the degree of the image curve $\mathcal{C}_N$ using the formula relating these values, that we presented in Theorem 2.1. The left hand-side of the formula is equal to this degree, and the right hand-side is equal to

$$\dim(M_{12}(\Gamma_0(N))) + g(\Gamma_0(N)) - 1,$$

given that the divisors of modular forms have disjunct supports as we have already seen.

This quantity can be computed using known formulas for the dimension of space of modular forms and genus of the modular curve which can be found [8], and it is equal to $\Psi(N)$.

At the end, we present some equations for our models, where the polynomials P_N are minimal polynomials of $\Delta(N\cdot)/\Delta$ over $\mathbb{C}(j)$.

If a homogeneous polynomial $\mathcal{P}_N$ is the defining (minimal) equation of the plane curve $\mathcal{C}_N$, then $\mathcal{P}_N(\Delta(z), E_4^3(z), \Delta(Nz))$ is also a modular form for $\Gamma_0(N)$ which is a null-form. We know that a null-form is determined by vanishing of a finite number of initial coefficients in its Fourier expansion. This gives us a linear system where the unknowns are coefficients of $\mathcal{P}_N$ and the coefficients are polynomial combinations of finite number of initial coefficients of modular forms $\Delta(z)$, $E_4^3(z)$, $\Delta(Nz)$. We have used *Sage* for our computations.

The problem in computing arises from the size of the linear system, which has dimensions

$$\frac{(d+1)(d+2)}{2} \times d\Psi(N) + 1,$$

where d is the degree of $\mathcal{P}_N$ which we know is $\Psi(N)$.

Polynomials P_N are affine (dehomogenized) forms of computed polynomials $\mathcal{P}_N$.

$$\begin{aligned}
P_2(x, y) &= 16777216y^3 - xy + 196608y^2 + 768y + 1\\
P_3(x, y) &= 150094635296999121y^4 - x^2y + 38263752\,xy^2 - 213516729579636\,y^3\\
&\quad + 1512\,xy + 10589493366\,y^2 - 177876\,y + 1\\
P_4(x, y) &= 3245185536584267267831560205762 56\,y^6 - 4096\,x^3y^2\\
&\quad + 6597069766656\,x^2y^3 - 2490310449950789468160\,xy^4\\
&\quad + 193118646128519322884263378944\,y^5 - x^3y + 1620049920\,x^2y^2\\
&\quad - 569986827839078400\,xy^3 + 383220040084871709091430 40\,y^4\\
&\quad + 2256\,x^2y + 9349606932480\,xy^2 + 2538589037956201185280\,y^3\\
&\quad - 1105920\,xy + 557658553712640\,y^2 + 40894464\,y + 1\\
P_5(x, y) &= 867361737988403547205962240695953369140625\,y^6 - x^4y\\
&\quad + 29296875000\,x^3y^2 - 246763229370117187500\,x^2y^3\\
&\quad + 54715201258659362792968750000 0\,xy^4\\
&\quad - 85798035343032097443938255310058593750\,y^5 + 3000\,x^3y\\
&\quad + 1243896484375000\,x^2y^2 + 1291394233703613281250000 0\,xy^3\\
&\quad + 28290287445997819304466247558593 75\,y^4\\
&\quad - 2587500\,x^2y + 1322387695312500000\,xy^2\\
&\quad - 3109516575932502746582031250 0\,y^3\\
&\quad + 587500000\,xy + 29664516448974609375\,y^2 - 9433593750\,y + 1
\end{aligned}$$

References

1. Blake, I., Csirik, J.A., Rubinstein, M., Seroussi, G.: On the computation of modular polynomials for elliptic curves. Technical. Report, Hewlett-Packard Laboratories. http://www.math.uwaterloo.ca/~mrubinst/publications/publications.html (1999). Accessed 11 Jan 2018
2. Bröker, R., Sutherland, A.V.: An explicit height bound for the classical modular polynomial. Ramanujan J. **22**, 293–313 (2010)
3. Bröker, R., Lauter, K., Sutherland, A.V.: Modular polynomials via isogeny volcanoes. Math. Comput. **81**, 1201–1231 (2012)
4. Diamond, F., Shurman, J.: A First Course in Modular Forms. Springer, New York (2005)
5. Ishida, N.: Generators and equations for modular function fields of principal congruence subgroups. Acta Arith. **85**(3), 197–207 (1998)
6. Ishida, N., Ishii, N.: Generators and defining equations of the modular function field of the group $\Gamma_1(N)$. Acta Arith. **101**(4), 303–320 (2002)
7. Ligozat, G.: Courbes modulaires de genre 1. Bull. Soc. Math. France (Memoire) **43**, 1–80 (1972)
8. Miyake, T.: Modular Forms. Springer, Berlin (2006)
9. Miranda, R.: Algebraic Curves and Riemann Surfaces. Graduate Studies in Mathematics, vol. 5. American Mathematical Society, Providence (1995)
10. Muić, G.: Modular curves and bases for the spaces of cuspidal modular forms. Ramanujan J. **27**, 181–208 (2012)
11. Muić, G.: On embeddings of curves in projective spaces. Monatsh. Math. **173**(2), 239–256 (2014)
12. Muić, G., Mikoč, D.: Birational maps of $X(1)$ into $\mathbb{P}^2$. Glasnik Matematicki **48**(2), 301–312 (2013)
13. Muić, G.: On degrees and birationality of the maps $X_0(N) \to \mathbb{P}^2$ constructed via modular forms. Monatsh. Math. **180**(3), 607–629 (2016)
14. Shimura, G.: 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 (1971)
15. Yifan, Y.: Defining equations of modular curves. Adv. Math. **204**, 481–508 (2006)