MATHEMATICS OF COMPUTATION
Volume 79, Number 272, October 2010, Pages 2371–2386
S 0025-5718(10)02332-X
Article electronically published on April 16, 2010

# EQUATIONS FOR THE MODULAR CURVE $X_1(N)$ AND MODELS OF ELLIPTIC CURVES WITH TORSION POINTS

HOURIA BAAZIZ

Abstract. We describe an algorithm for constructing plane models of the modular curve $X_1(N)$ and discuss the resulting equations when $N \leq 51$.

## Introduction

Let $N \geq 2$ be an integer. Recall that the modular curve $X_1(N)$ (with cusps removed) parametrizes isomorphism classes of pairs $(E, P)$ where $E$ is an elliptic curve and $P$ a torsion point of order $N$ on $E$. Two such pairs $(E, P)$ and $(E', P')$ are isomorphic if there exists an isomorphism $\phi : E \to E'$ such that $\phi(P) = P'$. Reichert [8] gave equations for $X_1(N)$ when $N = 11$ and $13 \leq N \leq 18$. Lecacheux [6] and Washington [10] gave equations for $X_1(13)$ and $X_1(16)$, respectively, in connection with the construction of families of cyclic extensions of $\mathbb{Q}$. In [2], Darmon discusses $X_1(25)$ from a similar point of view. However, their methods do not easily generalize to arbitrary values of $N$. Ishida and Ishii [3] developed methods to find equations for $X_1(N)$ for abritrary $N$ by explicitly constructing two modular functions that together generate the function field of $X_1(N)$; they list the equations obtained when $N \leq 20$. Yang [9] gave a method for constructing generators of function fields by using products constructed from generalized Dedekind $\eta$ functions. In his paper, Yang gives explicit models for $X_1(N)$ when $N = 11$ and $13 \leq N \leq 22$. However, apart from Reichert, these authors do not show how to recover an explicit model for the pair $(E, P)$ from the corresponding point on their model of $X_1(N)$.

The purpose of this paper is to present a new algorithm for obtaining equations for $X_1(N)$ which at the same time enables one to keep track explicitly of the corresponding pairs $(E, P)$. Our approach is similar to that of Reichert, in that we use division polynomials to characterize elliptic curves with the equation

$$(E) \qquad y^2 + (a_1x + a_3)y = x^3 + a_2x^2$$

on which the point $(0, 0)$ is torsion and of given order $N \geq 4$. As is well known, division polynomials can be calculated quickly by a recursive procedure, a variant of which is recalled in §2. It turns out that these division polynomials are divisible by

Received by the editor August 29, 2008 and, in revised form, July 17, 2009.
2010 *Mathematics Subject Classification.* Primary 11F03; Secondary 11G05, 11G18 11G30.
*Key words and phrases.* Modular curves, elliptic curves, torsion points.
This work was done at the Laboratoire de Mathématiques Nicolas Oresme of the University of Caen. I am deeply indebted to Professor John Boxall for advice and encouragement during my stay at the University of Caen. I am grateful to all members of the Laboratory for their reception and for the provision of facilities. Finally, I would like to thank the referee for his helpful comments on an earlier version of the paper.

high powers of $a_3$, which is also a factor of the discriminant of the elliptic curve, and removing this power of $a_3$ results in considerable simplification (see Lemma 2.3). Every elliptic curve of the form $(E)$ is isomorphic to one with model

$$y^2 + ((1+g)x + f)y = x^3 + fx^2$$

via an isomorphism taking $(0,0)$ to $(0,0)$ (see Proposition 1.3). When $(0,0)$ is of order $N$, the coefficients $f$ and $g$ can be viewed as modular forms on $\Gamma_1(N)$ and one shows that they generate the field of modular functions $\mathbb{C}(X_1(N))$ on $X_1(N)$ (see §3, and in particular equations (3.1) and (3.2), for explicit formulae for $f$ and $g$ in terms of Weierstrass $\wp$-functions). Simplifying the division polynomials gives a first equation $\Phi_N^{(f,g)}(f,g) = 0$ for $X_1(N)$. The fact that the division polynomials satisfy recurrence relations implies that the polynomials $\Phi_N^{(f,g)}$ can also be calculated using recursive formulae and this is explained in detail in the second half of §3. However, these equations are of considerably larger degree than those already given by previous authors. In §4, we define, in terms of $f$ and $g$, two other pairs of modular functions $\{s,t\}$ and $\{q,r\}$ on $\Gamma_1(N)$ each of which generates $\mathbb{C}(X_1(N))$ and results in an equation of smaller degree. All these equations have rational coefficients, which we normalize (up to sign) by assuming they have integral coefficients that are mutually coprime. Table 1 enables one to compare the resulting equations for $N \leq 15$. The pair $\{q,r\}$ gives the best results and, when $N \leq 22$, can be compared with the equations given by Ishida and Ishii [3] (pp. 316–317) and Yang [9] (page 506). In general, our equations would appear to be of smaller degree than theirs in the two variables individually but of slightly higher total degree. However it seems interesting to have equations which are of small degree in one of the functions, as this gives a better upper bound on the gonality of the curve (see the end of §5).

We have calculated the resulting equations for all $N \leq 51$. As we shall see, this can easily be done using recursive procedures based on using the recurrence relations (2.3), (2.4), and (2.5) below. (Alternatively one could use (3.7) and (3.8) and (2.5).) Since the equations quickly become large, it seems pointless to present the equations written out in full. When $N$ approaches 50, each of the equations obtained would occupy roughly a page. When $N = 50$, the equation in terms of $q$ and $r$ is of degree 23 in $r$ and 32 in $q$ and of total degree 48 (see Table 3) and the absolute value of the largest coefficient is 109037417.

The remaining table, Table 2, presents some particularly simple equations for $X_1(N)$ for $11 \leq N \leq 20$ and expresses the functions $u$ and $v$ used in terms $s$ and $t$.

## 1. Some elliptic functions

Let $K$ be a field and let $E$ be an elliptic curve over $K$. Then $E$ has a Weierstrass model

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K, \quad i \in \{1,2,3,4,6\}. \tag{1.1}$$

Suppose that $E(K)$ contains a point $P = (a,b)$ other than the origin $O$. Then, replacing $x$ by $x - a$ and $y$ by $y - b$, we can suppose that $P = (0,0)$. This implies that $a_6 = 0$. Thus, every pair $(E,P)$ consisting of an elliptic curve $E$ over $K$ and a point $P \in E(K)$ other than the origin can be represented as

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x, \qquad P = (0,0). \tag{1.2}$$

**Lemma 1.1.** *Suppose that* (1.2) *defines an elliptic curve and that $P$ is a torsion point.*

(1) *If $P$ is of order $N \geq 3$, then $a_3 \neq 0$ and, after a change of coordinates, we can suppose that $a_4 = 0$.*
(2) *If $a_3 \neq 0$ and $a_4 = 0$, then $P$ is of order 3 if and only if $a_2 = 0$.*

*Proof.* (1) Let $Q \neq O$ be a point with $x(Q) = 0$. Then $y(Q)^2 + a_3 y(Q) = 0$, so that if $a_3 = 0$, then $Q = P$ and so $x$ has no zero other than $P$. Thus $x$ must have a zero of order 2 at $P$ and therefore $P$ is of order 2, contrary to our hypothesis. Hence $a_3 \neq 0$, and one checks easily that substituting $y + \frac{a_4}{a_3}x$ for $y$ leads to a model with $a_4 = 0$.

(2) Suppose that $a_4 = 0$. Let $Q \neq O$ be a point with $y(Q) = 0$. Then $x(Q)^3 + a_2 x(Q)^2 = 0$, so $a_2 = 0$ if and only if the only possibility for $Q$ is $P$. Hence $P$ is of order 3 if and only if $a_2 = 0$. □

From now on, we consider pairs $(E, P)$ represented by

$$y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2, \qquad a_2 a_3 \neq 0, \qquad P = (0, 0). \tag{1.3}$$

Lemma 1.1 implies that if $P = (0, 0)$ is a point of order $N \geq 4$, then $(E, P)$ is isomorphic to a pair of the form (1.3). The discriminant of this model is

$$\Delta(E) = a_3^2(-a_2 a_1^4 + a_3 a_1^3 - 8a_2^2 a_1^2 + 36 a_3 a_2 a_1 - 16 a_2^3 - 27 a_3^2).$$

We always tacitly suppose (1.3) does define an elliptic curve, so that $\Delta(E) \neq 0$.

**Lemma 1.2.** *Let $(E, P)$ and $(E', P')$ be the pairs with equations*

$$(E) : y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2, \qquad a_2 a_3 \neq 0, \qquad P = (0, 0), \qquad \text{and} \tag{1.4}$$

$$(E') : y^2 + (a_1' x + a_3')y = x^3 + a_2' x^2, \qquad a_2' a_3' \neq 0, \qquad P' = (0, 0). \tag{1.5}$$

*Then $(E, P)$ and $(E', P')$ are $K$-isomorphic if and only if there exists $\lambda \in K^\times$ such that $a_i' = \lambda^i a_i$ for every $i \in \{1, 2, 3\}$. When this is the case, $\lambda$ is unique.*

*Proof.* If such a $\lambda$ exists, then $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$ is an isomorphism from $(E, P)$ to $(E', P')$. A $K$-isomorphism $\phi$ from the elliptic curve $E$ to $E'$ sends $(x, y)$ to $(\lambda^2 x + r, \lambda^3 y + ux + v)$, for some $\lambda \in K^\times$, $u, v \in K$. Since we want $\phi(0, 0) = (0, 0)$, we must have $r = v = 0$. Since the coefficients of $x$ in $E$ and $E'$ vanish, we must have $u = 0$. Thus $\phi$ must be of the form $(x, y) \mapsto (\lambda^2 x, \lambda^3 y)$. This implies that $a_i' = \lambda^i a_i$ for $i \in \{1, 2, 3\}$. Since $a_2' = \lambda^2 a_2$ and $a_3' = \lambda^3 a_3$ and $a_2 a_3 a_2' a_3' \neq 0$, we must have $\lambda = a_3' a_2 / a_3 a_2'$. Hence $\lambda$ is unique. □

**Proposition 1.3.** *Suppose that $N \geq 4$. Then every $K$-isomorphism class of pairs $(E, P)$ with $E$ an elliptic curve over $K$ and $P \in E(K)$ a torsion point of order $N$ contains a unique model of the form*

$$y^2 + ((1 + g)x + f)y = x^3 + f x^2, \qquad P = (0, 0), \tag{1.6}$$

*with $f \in K^\times$, $g \in K$.*

*Proof.* If we put $f = a_2^3/a_3^2$, $g = (a_1 a_2 - a_3)/a_3$, then $y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2$ becomes isomorphic to $y^2 + ((1 + g)x + f)y = x^3 + f x^2$, via $x \mapsto (a_2/a_3)^2 x$, $y \mapsto (a_2/a_3)^3 y$. Since $a_2 a_3 \neq 0$, we have $f \neq 0$.

If the isomorphism class also contains $\big(y^2 + ((1 + g')x + f')y = x^3 + f' x^2, (0, 0)\big)$ with $f' \in K^\times$ and $g' \in K$, then, considering the coefficients of $y$ and of $x^2$,

Lemma 1.2 implies that there exists $\lambda \in K^\times$ such that $f' = \lambda^2 f$ and $f' = \lambda^3 f$. Since $f \neq 0$, we deduce that $\lambda = 1$. □

For the rest of this section we suppose that $K = \mathbb{C}$. Our purpose is to parametrize the model (1.3) using elliptic functions associated to the lattice $\Omega = \{\int_\gamma \frac{dx}{2y+a_1x+a_3} \mid \gamma \in H_1(E(\mathbb{C}), \mathbb{Z})\}$. To be more precise, fixing $z_0 \in \mathbb{C}/\Omega$, we want to describe explicitly the isomorphism $\xi : \mathbb{C}/\Omega \to E(\mathbb{C})$ such that $\xi(z_0) = P$. If $\Omega$ is any lattice in $\mathbb{C}$, we recall the Weierstrass elliptic function

$$\wp(z) = \wp(z, \Omega) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Omega \\ \omega \neq 0}} \Big( \frac{1}{(z-\omega)^2} + \frac{1}{\omega^2} \Big). \tag{1.7}$$

It satisfies the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \tag{1.8}$$

where

$$g_2 = g_2(\Omega) = 60 \sum_{\substack{\omega \in \Omega \\ \omega \neq 0}} \frac{1}{\omega^4}, \quad g_3 = g_3(\Omega) = 140 \sum_{\substack{\omega \in \Omega \\ \omega \neq 0}} \frac{1}{\omega^6} \tag{1.9}$$

are the usual Eisenstein series, as well as the duplication formula

$$\wp(2z) = -2\wp(z) + \frac{1}{4} \frac{\wp''(z)^2}{\wp'(z)^2}. \tag{1.10}$$

Completing the square of the equation (1.3), we get

$$Y^2 = 4x^3 + (4a_2 + a_1^2)x^2 + 2a_1a_3x + a_3^2$$

with $Y = 2(y + \frac{1}{2}(a_1x + a_3))$. Replacing $x$ by $X - \frac{1}{12}(a_1^2 + 4a_2)$, we get

$$Y^2 = 4X^3 - g_2X - g_3, \qquad g_2^3 - 27g_3^2 \neq 0 \tag{1.11}$$

and this curve is parametrized by $X = \wp(z)$, $Y = \wp'(z)$.

It is useful to write

$$a = \frac{1}{12}(a_1^2 + 4a_2), \tag{1.12}$$

so that

$$\begin{aligned} g_2 &= \frac{1}{12}(a_1^4 + 8a_1^2a_2 - 24a_1a_3 + 16a_2^2) = 12a^2 - 2a_1a_3, \\ g_3 &= -(2^3a^3 - 2a_1a_3a + a_3^2). \end{aligned} \tag{1.13}$$

The point $P = (0, 0)$ corresponds to the point $(a, a_3)$ on the curve $Y^2 = 4X^3 - g_2X - g_3$, so that the condition $\xi(z_0) = P$ means that

$$a = \wp(z_0), \qquad a_3 = \wp'(z_0). \tag{1.14}$$

Since $a_3 \neq 0$, the first equation of (1.13) implies

$$a_1 = \frac{12a^2 - g_2}{2a_3} = \frac{12\wp(z_0)^2 - g_2}{2\wp'(z_0)} = \frac{\wp''(z_0)}{\wp'(z_0)}, \tag{1.15}$$

where the last equation follows by differentiating (1.8) and replacing $z$ by $z_0$. These equations together with (1.12) enable one to determine $a_2$.

Summing up the previous discussion, we obtain the following result.

**Theorem 1.4.** *Let $\Omega$ be a lattice in $\mathbb{C}$ and let $z_0 \in \mathbb{C}$ be such that $2z_0 \notin \Omega$. Define the elliptic functions*

$$a_1(z) = \frac{\wp''(z)}{\wp'(z)}, \quad a_2(z) = 3\wp(z) - \frac{1}{4}\frac{\wp''(z)^2}{\wp'(z)^2}, \quad a_3(z) = \wp'(z), \tag{1.16}$$

*so that $\wp(z) = (a_1(z)^2 + 4a_2(z))/12$. Then the elliptic curve*

$$y^2 + (a_1(z_0)x + a_3(z_0))y = x^3 + a_2(z_0)x^2 \tag{1.17}$$

*is parametrized by the elliptic functions*

$$x(z) = \wp(z) - \wp(z_0), \qquad y(z) = \frac{1}{2}\big(\wp'(z) - a_1(z_0)x(z) - a_3(z_0)\big) \tag{1.18}$$

*and we have $\big(x(z_0), y(z_0)\big) = (0,0)$.*

*Conversely, any pair of the form* (1.3) *can be parametrized in this way using the lattice $\Omega = \{\int_\gamma \frac{dx}{2y+a_1x+a_3} \mid \gamma \in H_1(E(\mathbb{C}),\mathbb{Z})\}$, the point $z_0$ being the unique solution* (mod $\Omega$) *of* (1.14).

Recall that the divisor of a non-zero elliptic function $f$ with period lattice $\Omega$ is the formal sum $\sum_{x\in\mathbb{C}/\Omega} v_x(f)[x]$, where $v_x(f)$ is the order of the zero (or of the pole counted negatively) of $f$ at any $z \in \mathbb{C}$ whose class (mod $\Omega$) is $x$. (Since $\mathbb{C}/\Omega$ is compact, $v_x(f)$ vanishes outside a finite set.) The order of $f$ is the non-negative integer $\sum_x \max(v_x(f), 0)$.

**Proposition 1.5.** *The divisors of the functions $a_2$, $a_3$, and $a_1a_2 - a_3$ are given by*

$$\operatorname{div}(a_2) = \sum_{\substack{3x=0\\ x\neq 0}} [x] - 2\sum_{2x=0}[x], \qquad \operatorname{div}(a_3) = \sum_{\substack{2x=0,\\ x\neq 0}} [x] - 3[0],$$

$$\operatorname{div}(a_1a_2 - a_3) = \sum_{\substack{4x=0\\ 2x\neq 0}} [x] - 3\sum_{2x=0}[x].$$

*Proof.* The case of $a_3(z) = \wp'(z)$ is well known. In the case $a_2(z)$, we use the duplication formula (1.10) to obtain

$$a_2(z) = -\wp(2z) + \wp(z), \tag{1.19}$$

from which the result follows easily since $\wp(z)$ is an even function. Similarly, a calculation using (1.8) and (1.10) shows that

$$a_1(z)a_2(z) - a_3(z) = \wp'(2z) \tag{1.20}$$

from which the last result follows. □

**Corollary 1.6.** *Let $F$ and $G$ be the elliptic functions defined by*

$$F(z) = F(z,\Omega) = \frac{a_2(z)^3}{a_3(z)^2}, \qquad G(z) = G(z,\Omega) = \frac{a_1(z)a_2(z) - a_3(z)}{a_3(z)}.$$

*Then*

$$\operatorname{div}(F) = 3\sum_{\substack{3x=0\\ x\neq 0}} [x] - 8\sum_{\substack{2x=0\\ x\neq 0}} [x], \tag{1.21}$$

$$\operatorname{div}(G) = \sum_{\substack{4x=0\\ 2x\neq 0}} [x] - 4\sum_{\substack{2x=0\\ x\neq 0}} [x]. \tag{1.22}$$

## 2. Division polynomials

We return to the model (1.3), viewing $x$, $a_1$, $a_2$, and $a_3$ as indeterminates, and work in the ring $A = \mathbb{Z}[x, a_1, a_2, a_3, y]$ where $y$ satisfies the equation

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2.$$

By Euclidian division, every element of $A$ can be written uniquely in the form $P + Qy$, with $P$, $Q \in \mathbb{Z}[x, a_1, a_2, a_3]$. For every integer $n \geq 1$, we consider the $n$-division element $\psi_n$ of $A$ defined recursively by

$$\begin{aligned}
&\psi_1 = 1, \qquad \psi_2 = a_1x + a_3 + 2y,\\
&\psi_3 = 3x^4 + (4a_2 + a_1^2)x^3 + 3a_1a_3x^2 + 3a_3^2x + a_3^2a_2,\\
&\psi_4 = \psi_2(2x^6 + (a_1^2 + 4a_2)x^5 + 5a_3a_1x^4 + 10a_3^2x^3 + 10a_3^2a_2x^2\\
&\qquad\qquad + (a_3^2a_2a_1^2 - a_3^3a_1 + 4a_3^2a_2^2)x + a_3^3a_2a_1 - a_3^4),
\end{aligned}$$

and

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \text{ if } n \geq 2, \tag{2.1}$$

$$\psi_2\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \text{ if } n \geq 3. \tag{2.2}$$

Furthermore, define $\phi_n$ and $\omega_n$ by

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \qquad 2\psi_n\omega_n = \psi_{2n} - \psi_n^2(a_1\phi_n + a_3\psi_n^2).$$

One checks by induction that $\psi_n$, $\omega_n$, $\phi_n \in A$ for all $n$.

**Theorem 2.1.** *Let $E$ be an elliptic curve of model* (1.3). *The point $P = (x_0, y_0)$ on $E$ is of order dividing $n$ if and only if $\psi_n(x_0, y_0) = 0$. If this is not the case, we have $nP = \Big(\dfrac{\phi_n(x_0, y_0)}{\psi_n(x_0, y_0)^2}, \dfrac{\omega_n(x_0, y_0)}{\psi_n(x_0, y_0)^3}\Big)$.*

*Furthermore, if we assign to $x$, $y$, $a_1$, $a_2$, and $a_3$, respectively, the weights* 2, 3, 1, 2, *and* 3 *and view $\mathbb{Z}[x, y, a_1, a_2, a_3]$ as a graded ring, then $\psi_n$, $\phi_n$, and $\omega_n$ are homogeneous with respective weights $n^2 - 1$, $2n^2$, and $3n^2$.*

*Proof.* This is a variant of the well-known formulae for curves of the form $y^2 = x^3 + Ax + B$, which are discussed for example in Cassels [1]. See also Lercier and Morain [7]. □

We shall only be interested in this result when $P = (0, 0)$ and from now on, we write $\psi_n$ for $\psi_n(0, 0)$ and similarly for $\phi_n$ and $\omega_n$. Thus $\psi_n$, $\phi_n$, and $\omega_n$ are homogeneous elements of $\mathbb{Z}[a_1, a_2, a_3]$ of respective weights $n^2 - 1$, $2n^2$, and $3n^2$.

We find

$$\psi_1 = 1, \quad \psi_2 = a_3, \quad \psi_3 = a_3^2a_2, \quad \psi_4 = a_3^4(a_1a_2 - a_3), \tag{2.3}$$

as well as the relations

$$\begin{aligned}
&\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \text{ if } n \geq 2,\\
&a_3\psi_{2n} = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2), \text{ if } n \geq 3.
\end{aligned} \tag{2.4}$$

Furthermore, for all $n \geq 2$ we have,

$$\phi_n = -\psi_{n+1}\psi_{n-1}, \qquad 2\psi_n\omega_n = \psi_{2n} - \psi_n^2(a_1\phi_n + a_3\psi_n^2). \tag{2.5}$$

**Corollary 2.2.** *Let $P$ be the point $(0,0)$ on the elliptic curve (1.3) and let $n \geq 2$ be an integer. Then $nP = O$ if and only if $\psi_n = 0$. When this is not the case, we have $nP = \left(\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3}\right)$.*

The relations (2.3), (2.4), and (2.5) are easy to implement and enable one to calculate $\psi_n$ and the coordinates of $nP$ quickly by induction. In practice, it is useful to be able to substitute various polynomials for $a_1$, $a_2$, and $a_3$. The following lemma shows that $\psi_n$ is divisible by a high power of $a_3$, and we can improve the implementation by removing it.

**Lemma 2.3.** *Let $v_{a_3}(n)$ be the exponent of the power of $a_3$ dividing $\psi_n$. Then*

$$v_{a_3}(n) = \begin{cases} \frac{n^2}{4}, & n \text{ even}, \\ \frac{n^2-1}{4}, & n \text{ odd}. \end{cases} \tag{2.6}$$

*Proof.* When $n \leq 4$, this is clear from (2.3). In general, write $\zeta_n = a_3^{-v^*_{a_3}(n)}\psi_n$, where $v^*_{a_3}(n)$ is defined to be the right hand side of (2.6). Then, from (2.4):

$$\zeta_{2n+1} = \begin{cases} a_3\zeta_{n+2}\zeta_n^3 - \zeta_{n-1}\zeta_{n+1}^3 & \text{if } n \text{ is even}, \\ \zeta_{n+2}\zeta_n^3 - a_3\zeta_{n-1}\zeta_{n+1}^3 & \text{if } n \text{ is odd} \end{cases} \tag{2.7}$$

for all $n \geq 2$ while, if $n \geq 3$, then

$$\zeta_{2n} = \zeta_n(\zeta_{n+2}\zeta_{n-1}^2 - \zeta_{n-2}\zeta_{n+1}^2). \tag{2.8}$$

Since $\zeta_1 = \zeta_2 = 1$, $\zeta_3 = a_2$, and $\zeta_4 = a_1a_2 - a_3$, we deduce by induction that $\zeta_n \in \mathbb{Z}[a_1, a_2, a_3]$ for all $n$, in other words that $v_{a_3}(n) \geq v^*_{a_3}(n)$ for all $n$. To prove equality, it suffices to prove that the constant term $\zeta_n(0)$ of $\zeta_n$, when viewed as a polynomial in $a_3$ with coefficients in $\mathbb{Z}[a_1, a_2]$, is non-zero. In fact, writing $\epsilon_n = (-1)^{n(n-1)/2}$, we find that

$$\zeta_{2n+1}(0) = \epsilon_n a_2^{n(n+1)/2}, \quad \text{for all } n \geq 0.$$

and, when $n \geq 1$, that $\zeta_{2n}(0)$ is of the form

$$\zeta_{2n}(0) = \epsilon_{n-1} \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} c_{n,i} a_1^{n-1-2i} a_2^{n(n-1)/2+i},$$

where the $c_{n,i}$ lie in $\mathbb{Z}$ and $c_{n,0} = 1$ for all $n$. Again, this can be checked by induction using the equations obtained by substituting $a_3 = 0$ in (2.7) and (2.8). □

Since $a_3$ is of weight 3, we see that $\zeta_n$ is of weight $\frac{1}{4}n^2 - 1$ or $\frac{n^2-1}{4}$ according as to whether $n$ is even or odd. This represents a considerable improvement. For example, $a_3^{625}$ divides $\psi_{50}$, while $\zeta_{50}$ is of weight 624 and therefore of degree at most 208 in $a_3$. Thus, it is better to implement (2.7) and (2.8) rather than (2.4). Using (2.5), one can calculate the power of $a_3$ dividing $\phi_n$ and $\omega_n$ and speed up the computation of $nP$ when $nP \neq O$.

However, as we shall see in the next section, further simplification is possible in the case needed for calculating equations for $X_1(N)$.

## 3. A first equation for $X_1(N)$

Fix an integer $N \geq 4$. Let $\mathcal{H}$ denote the upper half plane $\{\tau \in \mathbb{C} \mid \Im(\tau) > 0\}$. If $\tau \in \mathcal{H}$, we denote by $\Omega_\tau$ the lattice in $\mathbb{C}$ with basis $(\tau, 1)$. When $i \in \{1, 2, 3\}$, we write $a_i(\tau)$ for $a_i(1/N, \Omega_\tau)$ where $z \mapsto a_i(z, \Omega)$ is the elliptic function used in Theorem 1.4. We write $f(\tau) = F(1/N, \Omega_\tau)$ and $g(\tau) = G(1/N, \Omega_\tau)$, where $F$ and $G$ are the functions defined in Corollary 1.6. Thus by (1.19) and (1.20),

$$f(\tau) = \frac{(\wp(1/N, \Omega_\tau) - \wp(2/N, \Omega_\tau))^3}{\wp'(1/N, \Omega)^2}, \tag{3.1}$$

$$g(\tau) = \frac{\wp'(2/N, \Omega_\tau)}{\wp'(1/N, \Omega_\tau)}. \tag{3.2}$$

**Lemma 3.1.** *Let $\psi_n \in \mathbb{Z}[a_1, a_2, a_3]$ be the homogeneous polynomial introduced in §2. Then*

$$\psi_N\big(a_1(\tau), a_2(\tau), a_3(\tau)\big) = 0 \quad \textit{for all } \tau \in \mathcal{H}. \tag{3.3}$$

*Proof.* This follows from Theorem 1.4 and Corollary 2.2. □

**Theorem 3.2.** *Let $N \geq 4$ be an integer.*

1. *The functions $f$ and $g$ are modular functions on $\Gamma_1(N)$ and generate the field of all modular functions on $\Gamma_1(N)$.*
2. *We have*

$$\psi_N(1 + g, f, f) = 0. \tag{3.4}$$

*Proof.* It is well known that the functions $\tau \mapsto \wp(1/N, \Omega_\tau)$, $\tau \mapsto \wp'(1/N, \Omega_\tau)$, and $\tau \mapsto \wp''(1/N, \Omega_\tau)$ are modular forms on $\Gamma_1(N)$ of weights 2, 3, and 4. It follows that $a_i(\tau)$, $i \in \{1, 2, 3\}$, is an (*a priori* meromorphic) modular form of weight $i$. Hence $f$ and $g$ are modular functions on $\Gamma_1(N)$. To see that $f$ and $g$ generate $\mathbb{C}(X_1(N))$, we think of meromorphic functions on the compact Riemann surface $X_1(N)$. Recall that if $X$ is any compact Riemann surface and $S$ a subset of the field $\mathbb{C}(X)$ of meromorphic functions on $X$, then $S$ generates $\mathbb{C}(X)$ if and only if there exists a non-empty open subset $U$ of $X$ such that whenever $P$ and $Q$ are two points of $U$ such that $\varphi(P) = \varphi(Q)$ for all $\varphi \in S$, then $P = Q$. We apply this by taking $X = X_1(N)$ and $U = X_1(N)$ with the cusps removed, $S = \{f, g\}$; the assertion now follows from Proposition 1.3. This proves (1), and (2) follows from Lemma 3.1 and Proposition 1.3. □

*Remark* 3.3. As the referee pointed out to us, the functions $a_i(\tau)$ are in fact everywhere holomorphic modular forms (i.e., including at the cusps). To see this, we use the well-known fact that the functions $\tau \mapsto \big(\wp^{(k)}(z, \Omega_\tau)\big)_{z=1/N}$ are holomorphic for all $k \geq 0$. Since $a_3(\tau) = \wp'(1/N, \Omega_\tau)$, this already implies that $a_3$ is holomorphic. To prove that $a_1$ and $a_2$ are holomorphic, one notes that

$$3\wp(1/N, \Omega_\tau) - \tfrac{1}{4}a_1(\tau)^2 = a_2(\tau) = \wp(1/N, \Omega_\tau) - \wp(2/N, \Omega_\tau),$$

where the second equality follows from (1.19). This implies that $a_2$ and $a_1^2$ are holomorphic. Since $a_1$ is meromorphic and its square is holomorphic, we conclude that $a_1$ is itself holomorphic.

We can use Theorem 3.2 to obtain a plane affine model of $X_1(N)$ as follows. We know that if $y^2+((1+g)x+f)y = x^3+fx^2$ is an elliptic curve and $P=(0,0)$, then $NP = O$ if and only if $\psi_N(1+g,f,f)=0$. The discriminant of the elliptic curve is $-f^3(16f^2+(8g^2-20g-1)f+g(g+1)^3)$. Hence we can remove from $\psi_N(1+g,f,f)$ any common factor with this discriminant. Write $\Psi_N^{(f,g)} \in \mathbb{Z}[f,g]$ for the polynomial thus obtained, normalizing it up to sign by supposing the coefficients to be coprime. Also, if $M$ divides $N$, then $MP = O$ implies $NP = O$, so that $\Psi_M^{(f,g)}$ divides $\Psi_N^{(f,g)}$. Thus $\Psi_N^{(f,g)}$ has a factorisation

$$\Psi_N^{(f,g)} = \prod_{M|N} \Phi_M^{(f,g)}, \tag{3.5}$$

where $\Phi_M^{(f,g)}(f,g)$ vanishes if and only if the order of $(0,0)$ is exactly $M$. Then Theorem 3.2 implies that $\Phi_N^{(f,g)} = 0$ is the equation of an affine plane model of $X_1(N)$.

By Lemma 2.3, we know that $f^{v_{a_3}(\psi_n)}$ divides $\psi_n(1+g,f,f)$. In fact, we can do better than this.

**Theorem 3.4.** *Let*

$$v_f^*(n) = \begin{cases} 3k^2 & \text{if} \quad n = 3k, \\ 3k^2+2k & \text{if} \quad n = 3k+1, \\ 3k^2+4k+1 & \text{if} \quad n = 3k+2. \end{cases} \tag{3.6}$$

*Then for all $n \geq 1$, we have $\Psi_n^{(f,g)} = f^{-v_f^*(n)}\psi_n(1+g,f,f)$ (up to sign).*

*Proof.* Let $\theta_n = f^{-v_f^*(\psi_n)}\psi_n(1+g,f,f)$. We have to show that $\Psi_n^{(f,g)} = \theta_n$ for all $n \geq 1$. Using (2.3) and (2.4), we find that

$$\theta_1 = \theta_2 = \theta_3 = 1, \quad \theta_4 = g, \quad \theta_5 = g - f \tag{3.7}$$

and, when $N \geq 6$, that

$$\theta_N = \begin{cases} \theta_{3n}(\theta_{3n+2}\theta_{3n-1}^2 - \theta_{3n-2}\theta_{3n+1}^2) & \text{if} \quad N = 6n, \\ f\theta_{3n+2}\theta_{3n}^3 - \theta_{3n-1}\theta_{3n+1}^3 & \text{if} \quad N = 6n+1, \\ \theta_{3n+1}\big(f\theta_{3n+3}\theta_{3n}^2 - \theta_{3n-1}\theta_{3n+2}^2\big) & \text{if} \quad N = 6n+2, \\ \theta_{3n+3}\theta_{3n+1}^3 - \theta_{3n}\theta_{3n+2}^3 & \text{if} \quad N = 6n+3, \\ \theta_{3n+2}\big(\theta_{3n+4}\theta_{3n+1}^2 - f\theta_{3n}\theta_{3n+3}^2\big) & \text{if} \quad N = 6n+4, \\ \theta_{3n+4}\theta_{3n+2}^3 - f\theta_{3n+1}\theta_{3n+3}^3 & \text{if} \quad N = 6n+5. \end{cases} \tag{3.8}$$

We deduce that $\theta_n \in \mathbb{Z}[f,g]$ for all $n$. Indeed, if $n \leq 5$, this follows from (3.7), and for larger values of $n$ it follows from (3.8) by induction.

To conclude, we need to show that $\theta_n$ is prime to the discriminant

$$-f^3(16f^2+(8g^2-20g-1)f+g(g+1)^3)$$

of the elliptic curve

$$y^2+((1+g)x+f)y = x^3+fx^2$$

and that the coefficients of $\theta_n$ are coprime. We first show that $f$ does not divide $\theta_n$ by showing that the constant term $\theta_n(0)$ of $\theta_n$, viewed as a polynomial in $f$ with

coefficients in $\mathbb{Z}[g]$, is non-zero (compare with the proof of Lemma 2.3). In fact, we find

(3.9)
$$\theta_N(0) = \begin{cases} \epsilon_m \sum_{i=1}^{m} (-1)^i g^{m(m+1)/2-i} = \epsilon_{m-1} g^{m(m-1)/2} \dfrac{g^m+1}{g+1} & \text{if } N = 3m, \\ \epsilon_m g^{m(m+1)/2} \quad \text{if } N = 3m+1 \text{ or if } N = 3m+2, \end{cases}$$

where again $\epsilon_m = (-1)^{m(m-1)/2}$. This can be proved by induction on $N$ using the formulae obtained by substituting $f = 0$ in (3.7) and (3.8).

To see that $16f^2 + (8g^2 - 20g - 1)f + g(g+1)^3$ does not divide $\theta_n$, we observe that if it did, then $g(g+1)^3$ would divide $\theta_n(0)$, which is not the case as follows from (3.9). Finally, (3.9) also shows that $\pm 1$ appears as a coefficient in $\theta_n$ and this concludes the proof. □

It follows from this discussion that the relations (3.7) and (3.8) give a recursive procedure enabling one to calculate $\Psi_N^{(f,g)}$, and hence $\Phi_N^{(f,g)}$, in principle for any $N \geq 1$. The first column of Table 1 shows $\Phi_N^{(f,g)}$ for all $N$, $4 \leq N \leq 15$.

## 4. Improving the equation for $X_1(N)$

It is natural to ask whether other choices of generators of $\mathbb{C}(X_1(N))$ give rise to simpler equations, say of lower degree than $\Phi_N^{(f,g)}$. In general, if two elements $x$ and $y$ of $\mathbb{C}(X_1(N))$ generate $\mathbb{C}(X_1(N))$, we denote by $\Phi_N^{(x,y)}$ a polynomial of smallest degree such that $\Phi_N^{(x,y)}(x,y) = 0$ (this is defined only up to a non-zero constant multiple). In particular, if $x$ and $y$ generate $\mathbb{C}(X_1(N))$, then $\Phi_N^{(x,y)} = 0$ is a plane affine model of $X_1(N)$.

In particular, one can ask whether such generators can be defined in terms of $f$ and $g$ in a uniform way, say by formulae that are independent of $N$. That this is the case was first observed experimentally, and we know of no really satisfactory explanation for why the following choices work or why they produce simpler equations than similar substitutions that were tried.

Before going further, we record the following lemma.

**Lemma 4.1.** *Let $F$ and $G$ denote the elliptic functions used in Corollary* 1.6*. Then*

$$\begin{aligned} \operatorname{div}(G - F) &= \sum_{\substack{5x=0 \\ x\neq 0}} [x] - 8 \sum_{\substack{2x=0 \\ x\neq 0}} [x], \\ \operatorname{div}(G^2 - G + F) &= \sum_{\substack{6x=0 \\ 2x\neq 0, 3x\neq 0}} [x] - 8 \sum_{\substack{2x=0 \\ x\neq 0}} [x], \\ \operatorname{div}(G^3 - GF + F^2) &= \sum_{\substack{7x=0 \\ x\neq 0}} [x] - 16 \sum_{\substack{2x=0 \\ x\neq 0}} [x], \\ \operatorname{div}((F+1)G^2 - 3FG + 2F^2) &= \sum_{\substack{8x=0 \\ 4x\neq 0}} [x] - 16 \sum_{\substack{2x=0 \\ x\neq 0}} [x]. \end{aligned}$$

*Proof.* By Corollary 1.6, the polar divisor of a monomial $F^kG^\ell$ ($k \geq 0$, $\ell \geq 0$ integers) is $(8k+4\ell)\sum_{\substack{2x=0\\ x\neq 0}}[x]$. Consider for example the case of $G^2-G+F$. By what has just been said, the polar divisor of this function is supported by the three points $x_1$, $x_2$, $x_3$ of order 2 and is of the form $a[x_1]+b[x_2]+c[x_3]$ with $a$, $b$, and $c$ positive and not exceeding 8. Hence $G^2-G+F$ is of order at most 24. On the other hand, $G^2-G+F$ vanishes at the points of order 6 on $\mathbb{C}/\Omega$. This can be deduced from the fact that $\Phi_6^{(f,g)} = g^2-g+f$ (see Table 1). Since there are 24 points of order 6, we deduce that the order of $G^2-G+F$ is at least 24. Hence there are no other zeros or poles and $\operatorname{div}(G^2-G+F)$ is as stated in the lemma. A similar argument works in the other cases. □

We return to our discussion of equations of $X_1(N)$. Suppose that $N \geq 6$. Then the lemma implies that $g-f$ does not vanish identically on $X_1(N)$ and the same is true for $g$ by Corollary 1.6. Hence $t = f/g$ and $s = g^2/(f-g)$ are well-defined functions on $X_1(N)$ and we can solve for $f$ and $g$ to obtain $f = t(t-1)s$ and $g = (t-1)s$. Thus $s$ and $t$ generate $\mathbb{C}(X_1(N))$ when $N \geq 6$.

The second column of Table 1 gives $\Phi_N^{(s,t)}$ for all $N$, $6 \leq N \leq 15$.

Further calculations suggested another choice of generators. Let

$$r = \frac{t-1}{s+1}, \qquad q = \frac{(s+1)(t-1)}{t+s}. \tag{4.1}$$

In terms of $f$ and $g$, we have

$$r = \frac{(f-g)^2}{g(g^2-g+f)}, \qquad q = \frac{(g^2-g+f)(f-g)}{g^3-fg+f^2}. \tag{4.2}$$

Using Lemma 4.1, we see that $q$ and $r$ are well-defined whenever $N \geq 8$, and we can solve for $t$ and $s$ to obtain $t = q(r+1)+1$ and $s = q(r+1)/r - 1$. Thus $q$ and $r$ are a set of generators of $\mathbb{C}(X_1(N))$ whenever $N \geq 8$. We find that

$$f = \frac{q(1+r)(1+q+qr)(q+qr-r)}{r}, \qquad g = \frac{(q^2-q)r^2+(2q^2-q)r+q^2}{r},$$

which enables one to write down the equation of the corresponding elliptic curve.

Again, the right hand column of Table 1 gives the polynomial $\Phi_N^{(q,r)}$ for $N$, $8 \leq N \leq 15$.

*Remark* 4.2. As indicated above, we have no complete explanation as to why the pairs of generators $\{f,g\}$, $\{s,t\}$, and $\{q,r\}$ give rise successively to simpler equations for $X_1(N)$. We remark that, as in the work of most previous authors, the modular functions appearing in the equations have their divisor supported by the cusps and are therefore modular units (see for example [4]). Also, simple combinations of our functions are modular units. For example, $s$, $t$, and also $s+1$, $t-1$, and $s+t$ are modular units when $N \geq 8$ and we have $r = (t-1)/(s+1)$, $q = (s+1)(t-1)/(t+s)$. Then $q+1$ and $r-q$ are also modular units when $N \geq 10$. All this can be checked using Lemma 4.1.

## 5. Comments on the tables

We present three tables giving information concerning the equations for $X_1(N)$ that we have obtained. In each of the tables, the first column indicates the value of $N$ under consideration and the second, headed $g$, recalls the genus of $X_1(N)$.

To find the equations, we first computed $\psi_N(1+g,f,f)$ using the recurrence relations (2.3), (2.4), and (2.5) together with the relations $-\frac{N}{2}P = \frac{N}{2}P$ when $N$ is even and $-\frac{N-1}{2}P = \frac{N+1}{2}P$ when $N$ is odd. (An alternative would have been to implement (3.7) and (3.8) and then use (2.5).) From this we determined $\Phi_N^{(f,g)}$ by removing common factors with $\psi_M(1+g,f,f)$ when $M$ is a proper divisor of $N$ and with the discriminant of the curve. We then calculated $\Phi_N^{(s,t)}$ by substituting $f = t(t-1)s$, $g = (t-1)s$ in $\Phi_N^{(f,g)}$ and removing redundant factors. We obtained $\Phi_N^{(q,r)}$ from $\Phi_N^{(s,t)}$ in a similar manner. Note that it is extremely important to remove the redundant factors from $\psi_N(1+g,f,f)$ before substituting. For example, by Theorem 3.4, we know that $f^{833}$ divides $\psi_{50}(1+g,f,f)$, so that substituting $f = t(t-1)s$ would result in a useless factor of $(t-1)^{833}$ which, when expanded, would competely swamp $\Phi_{50}^{(f,g)}(1+(t-1)s, t(t-1)s, t(t-1)s)$.

As already indicated, the three final columns of Table 1 give the equations for $X_1(N)$ for the sets of generators $\{f,g\}$, $\{s,t\}$, and $\{q,r\}$ for those values of $N$ between 4 and 15 for which both members of the set are defined, an empty entry indicating that this is not the case. It shows clearly, for the values of $N$ indicated, the simplification obtained in passing from the set $\{f,g\}$ to the set $\{s,t\}$ and then on to $\{q,r\}$. Further calculations reveal similar simplifications for larger values of $N$.

The third column of Table 2 lists models of $X_1(N)$, $11 \le N \le 20$, most of which are well known. These equations are given in terms of two functions $u$ and $v$; the last two columns give $s$ and $t$ in terms of $u$ and $v$. These equations were mostly found by trial and error by trying various subtitutions in $\Phi_N^{(s,t)}$. Substituting for $s$ and $t$ in the coefficients of the elliptic curve $y^2+(1+(t-1)sx+t(t-1)s)y = x^3+t(t-1)sx^2$ gives the equation of the corresponding elliptic curve in terms of $u$ and $v$.

Since the polynomials $\Phi_N^{(q,r)}$ are obtained by a recursive procedure as explained above and which is easy to implement and since they quickly become large as $N$ grows, it seems pointless to present tables of them here. So, in Table 3, we list the degrees $\deg_r \Phi_N^{(q,r)}$ and $\deg_q \Phi_N^{(q,r)}$ as well as the total degree $\deg_{\text{total}} \Phi_N^{(q,r)}$ of $\Phi_N^{(q,r)}$ for every $N$ from 16 to 51.

Recall that the gonality of an irreducible projective algebraic curve $X$ is the smallest degree of a surjective morphism from $X$ to the projective line. It is also the smallest possible value of the degree in terms of one of the variables of a plane affine equation of $X$. In particular, if $\gamma(N)$ denotes the gonality of $X_1(N)$, then $\min\left(\deg_r \Phi_N^{(q,r)}, \deg_q \Phi_N^{(q,r)}\right)$ is an upper bound for $\gamma(N)$. However this bound is not always the best possible; for example the degrees in $u$ and $v$ of the equations in Table 2 are also upper bounds, and these are sometimes smaller.

TABLE 1. The polynomials $\Phi_N^{(f,g)}$, $\Phi_N^{(t,s)}$, $\Phi_N^{(q,r)}$, $4 \le N \le 15$.

| $N$ | $g$ | $\Phi_N^{(f,g)}$ | $\Phi_N^{(t,s)}$ | $\Phi_N^{(q,r)}$ |
|---|---|---|---|---|
| 4 | 0 | $g$ | | |
| 5 | 0 | $g - f$ | | |
| 6 | 0 | $g^2 - g + f$ | $s + 1$ | |
| 7 | 0 | $g^3 - fg + f^2$ | $t + s$ | |
| 8 | 0 | $(f+1)g^2 - 3fg + 2f^2$ | $(s+2)t - 1$ | $q + 1$ |
| 9 | 0 | $g^5 - g^4 + (f+1)g^3$<br>$-3fg^2 + 3f^2g - f^3$ | $t - (s^2 + s + 1)$ | $r - q$ |
| 10 | 0 | $g^5 + fg^4 - 3fg^3$<br>$+(3f^2 + f)g^2 - 2f^2g + f^3$ | $(s^2 + 3s + 1)t + s^2$ | $(q^2 + q - 1)r$<br>$+q(q+2)$ |
| 11 | 1 | $fg^7 - (3f+1)g^6 + 3f(f+2)g^5$<br>$-9f^2g^4 + f^2(4f-1)g^3$<br>$+3f^3g^2 - 3f^4g + f^5$ | $t^2 + s(s^2 + 3s + 4)t - s$ | $r^2 + q^2r + (q^2 + q)$ |
| 12 | 0 | $g^6 - (f-1)g^4 - 5fg^3$<br>$+f^2(f+10)g^2 - 9f^3g + 3f^4$ | $(s+3)t^2 + (s-3)t$<br>$+s^2 + 1$ | $(q+2)r + 1$ |
| 13 | 2 | $g^{10} + f^2g^9 - 6f(f+1)g^8$<br>$+f(5f^2 + 21f + 3)g^7$<br>$-f(24f^2 + 13f + 1)g^6$<br>$+3f^2(f+2)(3f+1)g^5$<br>$-15f^3(f+1)g^4 + 4f^4(f+5)g^3$<br>$-15f^5g^2 + 6f^6g - f^7$ | $t^3 -$<br>$(s^4 + 5s^3 + 9s^2 + 4s + 2)t^2$<br>$+(s^3 + 6s^2 + 3s + 1)t + s^3$ | $r^2 - (q^3 + q^2 - 1)r$<br>$-q(q+1)^2$ |
| 14 | 1 | $fg^9 - 3fg^8 + (4f^2 + 6f + 1)g^7$<br>$-f(f^2 + 17f + 10)g^6$<br>$+f(16f^2 + 30f + 1)g^5$<br>$-5f^2(f^2 + 8f + 1)g^4$<br>$+5f^3(5f+2)g^3 - 2f^4(3f+5)g^2$<br>$+f^5(5g - f)$ | $(s^3 + 5s^2 + 6s + 1)t^2$<br>$-(s^4 + 3s^3 + 6s^2 + 7s + 1)t$<br>$+s$ | $(q^3 + 2q^2 - q - 1)r^2$<br>$+q(3q+2)r$<br>$-q^2(q+1)$ |
| 15 | 1 | $g^{13} + (f-1)g^{12} + (f^2 - 3f + 1)g^{11}$<br>$-(3f^2 + 2f + 1)g^{10}$<br>$+(7f^3 + 19f^2 + 8f + 1)g^9$<br>$-f(36f^2 + 37f + 9)g^8$<br>$+f^2(18f^2 + 73f + 36)g^7 - 2f^3(31f + 37)g^6$<br>$+f^3(19f^2 + 81f - 1)g^5 - 5f^4(9f - 1)g^4$<br>$+10f^5(f-1)g^3 + 10f^6g^2 - 5f^7g + f^8$ | $t^3 +$<br>$s(s^4 + 7s^3 + 18s^2 + 19s + 10)t^2$<br>$+s(s^4 + 4s^3 - 5s - 5)t$<br>$+s(s^4 + s^3 + s^2 + s + 1)$ | $r^2 +$<br>$q(q-1)(q^2 + 3q + 3)r$<br>$+q^2(q^2 + 3q + 3)$ |

TABLE 2. The polynomials $\Phi_N^{(u,v)}$, $11 \leq N \leq 20$.

| $N$ | $g$ | $\Phi_N^{(u,v)}$ | $t$ | $s$ |
|---|---|---|---|---|
| 11 | 1 | $v^2 - v - u^3 + u^2$ | $v$ | $-\dfrac{v+u-1}{u}$ |
| 12 | 0 | $v^2 + 2uv + u$ | $\dfrac{v^2+v+u}{u}$ | $\dfrac{v-u+1}{u}$ |
| 13 | 2 | $u^2 - (v^3 + v + 1)u - v^4(v+1)$ | $\dfrac{v}{u^4} + 1$ | $\dfrac{(1-u)v+u^4}{vu-u^4}$ |
| 14 | 1 | $v^2 + uv - (u^3 - 3u^2 + 2u)$ | $\dfrac{v^4+3uv^3-u^2(u-6)v^2-u^3(2u-7)v-u^4(u-2)}{(uv^3+5u^2v^2+6u^3v+u^4)}$ | $\dfrac{v}{u}$ |
| 15 | 1 | $v^2 + (u+1)v - u^2(u+1)$ | $\dfrac{u^6+u^5-vu^4-2v^2u^3+v^3u+v^4}{u^5}$ | $\dfrac{v^2-u^3-u^2}{u^2+vu}$ |
| 16 | 2 | $v^2 + (u-1)(u^2-2u-1)v - u^2(u-1)(u^2-2u-1)$ | $-\dfrac{v^2-(u-1)(2u+1)v+u^4-u^3}{v}$ | $\dfrac{v-u^2+1}{u-1}$ |
| 17 | 5 | $v^4 + (2u^2-3u-3)v^3 + (u^4-4u^3+6u+3)v^2$ $-(u^5-2u^4-u^3+u^2+4u+1)v+u$ | $\dfrac{v+u^2-u}{v}$ | $\dfrac{2u-v-u^2}{v-u}$ |
| 18 | 2 | $v^2 - (u^3+2u^2+3u+1)v + u(u+1)^2$ | $\dfrac{(u+1)^2+uv}{(u+1)^2+(2u+1)v-v^2}$ | $-\dfrac{(u+1)^2-v}{v^2-uv-(u+1)^2}$ |
| 19 | 7 | $v^5 + (u^6+4u^5+3u^4-5u^3-4u^2+2)v^4$ $+(2u^6+11u^5+18u^4-u^3-12u^2-4u+1)v^3$ $+u(u^5+7u^4+21u^3+15u^2-2u-3)v^2$ $-u^2(u+1)(u^2-4u-3)v - u^3(u+1)^2$ | $\dfrac{v^3+v^2-(u-1)v+(u-1)^2}{(v^2+u-1)(u-1)}$ | $\dfrac{v^2+v-u+1}{u-1}$ |
| 20 | 3 | $v^3 - u(2u-3)v^2 + (u-1)(u^3-2u^2-u-1)v$ $+u(u-1)(u^2-u-1)$ | $\dfrac{(u^2-u+1)v+u^2}{v(u-1)^2}$ | $\dfrac{-uv-2u+1}{(u-1)(v+1)}$ |

TABLE 3. Degree in $r$, in $q$ and total degree of $\Phi_N^{(q,r)}$, $16 \leq N \leq 51$.

| $N$ | $g$ | $\deg_r \Phi_N^{(q,r)}$ | $\deg_q \Phi_N^{(q,r)}$ | $\deg_{\text{total}} \Phi_N^{(q,r)}$ | $N$ | $g$ | $\deg_r \Phi_N^{(q,r)}$ | $\deg_q \Phi_N^{(q,r)}$ | $\deg_{\text{total}} \Phi_N^{(q,r)}$ |
|---|---|---|---|---|---|---|---|---|---|
| 16 | 2 | 3 | 3 | 5 | 34 | 21 | 11 | 16 | 23 |
| 17 | 5 | 4 | 5 | 8 | 35 | 25 | 15 | 21 | 32 |
| 18 | 2 | 3 | 4 | 6 | 36 | 17 | 11 | 16 | 23 |
| 19 | 7 | 5 | 6 | 10 | 37 | 40 | 18 | 24 | 37 |
| 20 | 3 | 3 | 5 | 6 | 38 | 28 | 14 | 20 | 29 |
| 21 | 5 | 5 | 7 | 11 | 39 | 33 | 18 | 24 | 37 |
| 22 | 6 | 4 | 7 | 11 | 40 | 25 | 16 | 20 | 32 |
| 23 | 12 | 7 | 9 | 14 | 41 | 51 | 22 | 30 | 45 |
| 24 | 5 | 6 | 7 | 11 | 42 | 25 | 15 | 20 | 30 |
| 25 | 12 | 8 | 11 | 16 | 43 | 57 | 24 | 33 | 49 |
| 26 | 10 | 7 | 9 | 15 | 44 | 36 | 19 | 25 | 39 |
| 27 | 13 | 8 | 12 | 17 | 45 | 41 | 23 | 31 | 47 |
| 28 | 10 | 7 | 10 | 15 | 46 | 45 | 21 | 29 | 44 |
| 29 | 22 | 11 | 15 | 22 | 47 | 70 | 29 | 39 | 59 |
| 30 | 9 | 8 | 9 | 15 | 48 | 37 | 19 | 28 | 41 |
| 31 | 26 | 13 | 17 | 26 | 49 | 69 | 31 | 42 | 64 |
| 32 | 17 | 10 | 14 | 21 | 50 | 48 | 23 | 32 | 48 |
| 33 | 21 | 12 | 17 | 26 | 51 | 65 | 30 | 41 | 62 |

## REFERENCES


1. J. W. S. Cassels. *Lectures on elliptic curves*. London Mathematical Society. Student Texts 24, Cambridge University Press, 1991. MR1144763 (92k:11058)
2. H. Darmon. Note on a polynomial of Emma Lehmer. Math. Comp. **56**, nº 194 (1991), 795–800. MR1068821 (91i:11149)
3. N. Ishida, N. Ishii. *Generators and defining equation of the modular function field of the group* $\Gamma_1(N)$. Acta Arithmetica **101**, nº 4 (2002), 303–320. MR1880045 (2003a:11069)
4. D. S. Kubert, S. Lang. *Modular units*. Springer-Verlag. New York, Heidelberg, Berlin, 1981. MR648603 (84h:12009)
5. S. Lang. *Elliptic Functions*. Addison-Wesley Publishing Company, INC. Advanced Book Program, 1973. MR0409362 (53:13117)
6. O. Lecacheux. *Unités d'une famille de corps cycliques réels de degré* 6 *liés à la courbe modulaire* $X_1(13)$. J. Number Theory **31** (1989), 54–63. MR978099 (90i:11062)
7. R. Lercier and F. Morain. *Counting points on elliptic curves over* $\mathbb{F}_{p^n}$ *using Couveignes's algorithm*. Rapport de Recherche LIX/RR/95/09, Ecole Polytechnique, septembre 1995. ftp://lix.polytechnique.fr/pub/submissions/morain/Preprints/seacgfpn.960125.ps.Z. MR1367512 (96h:11060)
8. M. A. Reichert. *Explicit determination of non-trivial torsion structures of elliptic curves over quadratic number fields*. Math. Comput. **46**, nº 174 (1986), 637–658. MR829635 (87f:11039)

9. Y. Yang. *Defining equations of modular curves.* Advances in Math. **204** (2006), 481–508. MR2249621 (2007e:11068)
10. L. C. Washington. *A family of cyclic quartic fields arising from modular curves.* Math. Comp. **57**, n$^{o}$ 196 (1991), 763–775. MR1094964 (92a:11120)

USTHB Faculté de Mathématiques, BP 32 El Alia Bab Ezzouar Alger, 16111 Algeria
*E-mail address*: houriarz@yahoo.com