Tu, F.-T. and Yang, Y.
Osaka J. Math.
46 (2009), 105–113

DEFINING EQUATIONS OF $X_0(2^{2n})$

FANG-TING TU and YIFAN YANG

(Received February 1, 2007, revised November 21, 2007)

Abstract

In this note we will obtain defining equations of modular curves $X_0(2^{2n})$. The key ingredient is a recursive formula for certain generators of the function fields on $X_0(2^{2n})$.

1. Introduction and statements of results

Let Γ be a congruence subgroup of $SL_2(\mathbb{R})$ commensurable with $SL_2(\mathbb{Z})$. The modular curve $X(\Gamma)$ is defined as the quotient of the extended upper half-plane $\mathbb{H}^* = \{\tau \in \mathbb{C}\colon \operatorname{Im}\tau > 0\} \cup \mathbb{P}^1(\mathbb{Q})$ by the action of Γ. It has a complex structure as a compact Riemann surface (i.e., a non-singular irreducible projective algebraic curve), and the polynomials defining the Riemann surface are called *defining equations* of $X(\Gamma)$. The problem of explicitly determining the equations of modular curves has been addressed by numerous authors. For instance, Galbraith [5], Murabayashi [12], and Shimura [17] used the so-called canonical embeddings to find equations of $X_0(N)$ that are non-hyperelliptic. For hyperelliptic $X_0(N)$, we have results of Galbraith [5], González [6], Hibino [7], Hibino-Murabayashi [8], and Shimura [17]. In [16] Reichert used the fact that $X_1(N) = X(\Gamma_1(N))$ is the moduli space of isomorphism classes of elliptic curves with level N structure to compute equations of $X_1(N)$ for $N = 11, 13, \ldots, 18$. Furthermore, in [10] Ishida and Ishii proved that for each N two certain products of the Weierstrass σ-functions generate the function field on $X_1(N)$, and thus the relation between these two functions defines $X_1(N)$. A similar method was employed in [9] to obtain equations of $X(N) = X(\Gamma(N))$. Very recently, in [19] the second author of the present article devised a new method for obtaining defining equations of $X_0(N)$, $X_1(N)$, and $X(N)$, in which the required modular functions are constructed using the generalized Dedekind eta functions. (See [18] for the definition and properties of these functions.)

When Γ_1 and Γ_2 are two congruence subgroups such that Γ_2 is contained in Γ_1 and a defining equation of $X(\Gamma_1)$ is known, one may attempt to deduce an equation for $X(\Gamma_2)$ using the natural covering $X(\Gamma_2) \to X(\Gamma_1)$. Of course, the main difficulty in this approach lies at finding an explicit description of the covering map. In this note

2000 Mathematics Subject Classification. Primary 11F03; Secondary 11G05, 11G18, 11G30.

The authors were support by Grant 95-2115-M-009-005 of the National Science Council (NSC) of Taiwan.

we will prove a recursive formula for the coverings $X_0(2^{2(n+1)}) \to X_0(2^{2n})$, from which we easily obtain defining equations of $X_0(2^{2n})$ for positive integers n.

To state our result, we first recall the definition of the Jacobi theta functions

$$\theta_2(\tau) = \sum_{n\in\mathbb{Z}} q^{(2n+1)^2/8} = 2\frac{\eta(2\tau)^2}{\eta(\tau)},$$

$$\theta_3(\tau) = \sum_{n\in\mathbb{Z}} q^{n^2/2} = \frac{\eta(\tau)^5}{\eta(\tau/2)^2\eta(2\tau)^2},$$

and

$$\theta_4(\tau) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2/2} = \frac{\eta(\tau/2)^2}{\eta(\tau)},$$

where $q = e^{2\pi i\tau}$ and

$$\eta(\tau) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$$

is the Dedekind eta function. Now our main result can be stated as follows.

Theorem 1. *Let $P_6(x, y) = y^4 - x^3 - 4x$, and for $n \geq 7$ define polynomials $P_n(x, y)$ recursively by*

$$P_n(x, y) = P_{n-1}\left(\frac{\sqrt{x^2+4}}{\sqrt{x}}, \frac{y}{\sqrt{x}}\right)P_{n-1}\left(-\frac{\sqrt{x^2+4}}{\sqrt{x}}, \frac{y}{\sqrt{x}}\right)x^{2^{n-5}}.$$

Then $P_{2n}(x, y) = 0$ is a defining equation of the modular curve $X_0(2^{2n})$ for $n \geq 3$.

To be more precise, for $n \geq 1$, let

$$x_n = \frac{2\theta_3(2^{n-1}\tau)}{\theta_2(2^{n-1}\tau)}, \quad y_n = \frac{\theta_2(8\tau)}{\theta_2(2^{n-1}\tau)}.$$

Then,

(1) *for $n \geq 2$, we have $x_{n-1} = \sqrt{(x_n^2+4)/x_n}$ and $y_{n-1} = y_n/\sqrt{x_n}$;*

(2) *for $n \geq 6$, $P_n(x_n, y_n) = 0$, and $P_n(x, y)$ is irreducible over $\mathbb{C}$;*

(3) *when n is an even integer greater than 4, x_n and y_n are modular functions on $\Gamma_0(2^n)$ that are holomorphic everywhere except for a pole of order 2^{n-4} and $2^{n-4}-1$, respectively, at ∞. (Thus, they generate the field of modular functions on $\Gamma_0(2^n)$ and the relation $P_n(x_n, y_n) = 0$ between them is a defining equation for $X_0(2^n)$.)*

We remark that it can be easily shown by induction that $P_n(x, y)$ is contained in $\mathbb{Z}[x, y^8]$ for $n \geq 7$ and has a degree $2^{n-4}-1$ in x and a degree 2^{n-4} in y. We also

remark that when n is odd, the polynomial $P_n(x, y)$ fails to be a defining equation of $X_0(2^n)$ because in this case

$$y_n(\tau) = \frac{\eta(16\tau)^2\eta(2^{n-1}\tau)}{\eta(8\tau)\eta(2^n\tau)^2}$$

is not modular on $\Gamma_0(2^n)$. (When n is odd, y_n does not satisfy the conditions of Newman [13, Theorem I] for a product of Dedekind eta functions to be modular on $\Gamma_0(N)$. Indeed, one can show that when n is odd,

$$y_n\left(\frac{a\tau + b}{c\tau + d}\right) = \left(\frac{2}{d}\right)y_n(\tau), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(2^n),$$

where $\left(\frac{\cdot}{d}\right)$ is the Jacobi symbol.)

EXAMPLES. Using Theorem 1, we find that a defining equation of $X_0(256)$ is

$$y^{16} - 16x(x+2)^4(x^2+4)y^8 - x(x+2)^4(x-2)^8(x^2+4) = 0,$$

and an equation for $X_0(1024)$ is

$$\begin{aligned} &y^{64} - 2^{12}vy^{56} - 2^8 \cdot 241uvy^{48} - 2^9uv(11 \cdot 23u + 2^8 \cdot 7 \cdot 17v)y^{40} \\ &- 2^4uv(31 \cdot 149u^2 - 2^8 \cdot 2053uv + 2^{16} \cdot 7 \cdot 73v^2)y^{32} \\ &- 2^9uv(31u^3 + 2^7 \cdot 3^2 \cdot 31u^2v + 3 \cdot 2^{16}uv^2 + 2^{23}v^3)y^{24} \\ &- 2^5u^3v(47u^2 - 2^9 \cdot 5^4uv + 2^{15} \cdot 17 \cdot 31v^2)y^{16} \\ &- 2^6u^3v(u^3 + 2^7 \cdot 41u^2v + 2^{18} \cdot 5uv^2 + 2^{26}v^3)y^8 - u^7v = 0, \end{aligned}$$

where $u = (x-2)^8$ and $v = x(x+2)^4(x^2+4)$.

Our interest in the modular curves $X_0(2^{2n})$ stems from the following remarkable observation of Hashimoto. When $n = 3$, it is known that the curve $X_0(64)$ is non-hyperelliptic (see [14]) of genus 3. Then the theory of Riemann surfaces says that it can be realized as a plane quartic. Indeed, it can be shown that the space of cusp forms of weight 2 on $\Gamma_0(64)$ is spanned by

$$x = \eta(4\tau)^2\eta(8\tau)^2, \quad y = 2\eta(8\tau)^2\eta(16\tau)^2, \quad z = \frac{\eta(8\tau)^8}{\eta(4\tau)^2\eta(16\tau)^2},$$

and the map $X_0(64) \to \mathbb{P}^2(\mathbb{C})$ defined by $\tau \mapsto [x(\tau) : y(\tau) : z(\tau)]$ is an embedding. Then the relation

$$x^4 + y^4 = z^4$$

among x, y, z is a defining equation of $X_0(64)$ in $\mathbb{P}^2$. (The Fermat curve $X^4+Y^4=1$ is birationally equivalent to $y^4-x^3-4x=0$ in Theorem 1 via the map $X=(x-2)/(x+2)$, $Y=2y/(x+2)$.) Then Hashimoto pointed out the curious fact that the Fermat curve F_{2^n}: $x^{2^n}+y^{2^n}=1$ and the modular curve $X_0(2^{2n+2})$ have the same genus for all positive integer n. In fact, there are more similarities between these two families of curves. For instance, the obvious covering $F_{2^{n+1}} \to F_{2^n}$ given by $[x:y:z] \to [x^2:y^2:z^2]$ branches at $3\cdot 2^n$ points, each of which is of order 2. On the other hand, the congruence subgroup $\Gamma_0(2^{2n+2})$ is conjugate to

$$\Gamma_0^0(2^{n+1}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \colon 2^{n+1} \mid b,\, c \right\},$$

and the natural covering $X_0^0(2^{n+2}) \to X_0^0(2^{n+1})$ also branches at $3\cdot 2^n$ cusps of $X_0^0(2^{n+1})$. These observations naturally lead us to consider the problem whether the modular curve $X_0(2^{2n+2})$ is birationally equivalent the Fermat curve F_{2^n}. It turns out that this problem can be answered easily as follows.

According to [3, 11, 15], when a modular curve $X_0(N)$ has genus ≥ 2, any automorphism of $X_0(N)$ will arise from the normalizer of $\Gamma_0(N)$ in $SL_2(\mathbb{R})$, with $N=37, 63$ being the only exceptions. Now by [1, Theorem 8], for all $n \geq 7$, the index of $\Gamma_0(2^n)$ in its normalizer in $SL_2(\mathbb{R})$ is 128. Therefore, the automorphism group of $X_0(2^{2n+2})$ has order 128 for all $n \geq 3$. On the other hand, it is clear that the automorphism group of any Fermat curve contains S_3. Thus, we conclude that the modular curve $X_0(2^{2n+2})$ cannot be birationally equivalent to the Fermat curve F_{2^n} when $n \geq 3$. Still, it would be an interesting problem to study the exact relation between these two families of curves.

REMARK. After the paper was finished, Professor M. Zieve has kindly informed us that explicit equations for $X_0(2^n)$ have also been obtained by Elkies [2]. Using geometric arguments, Elkies showed that the curve $X_0(l^n)$ can be embedded in $X_0(l^2)^{n-1}$. When $l=2$, the curve $X_0(2^2)$ is of genus zero and thus possesses a Hauptmodul $\xi(\tau)$. Then the embedding is explicitly given as

$$\tau \mapsto (\xi(\tau), \xi(2\tau), \ldots, \xi(2^{n-2}\tau)),$$

and the equations of $X_0(2^n)$ are defined in terms of the relations between $\xi(2^{j-1}\tau)$ and $\xi(2^j\tau)$. Elkies' equations and ours are both recursive in nature. Note that, however, Elkies' method is a generalization of the classical modular equations where a defining equation for $X_0(N)$ is given in terms of $j(\tau)$ and $j(N\tau)$, while our method emphasizes on explicit construction of generators of the field of modular functions. Moreover, since our starting point is the genus 3 modular curve $X_0(64)$, our equations are more comparable to Elkies' equations for $X_0(6^n)$, where the starting point is the genus 1 modular curve $X_0(36)$.

2. Proof of Theorem 1

To prove $x_{n-1} = \sqrt{(x_n^2+4)/x_n}$, we first verify the case $n = 2$ by comparing the Fourier expansions for enough terms, and then the general case follows since $x_n(\tau)$ is actually equal to $x_1(2^{n-1}\tau)$. The proof of $y_{n-1} = y_n/\sqrt{x_n}$ is equally simple. We have

$$\frac{y_{n-1}^2}{y_n^2} = \frac{\theta_2(2^{n-1}\tau)^2}{\theta_2(2^{n-2}\tau)^2} = \frac{\eta(2^{n-2}\tau)^2\eta(2^n\tau)^4}{\eta(2^{n-1}\tau)^6} = \frac{\theta_2(2^{n-1}\tau)}{2\theta_3(2^{n-1}\tau)} = \frac{1}{x_n}.$$

This proves the recursion part of the theorem. We now show that when $n \geq 6$ is an even integer, x_n and y_n are modular functions on $\Gamma_0(2^n)$ that have a pole of order 2^{n-4} and $2^{n-4}-1$, respectively, at ∞ and are holomorphic everywhere.

By the criteria of Newman [13], a product

$$\prod_{k=0}^{n} \eta(2^k\tau)^{e_k}$$

of Dedekind eta functions is a modular function on $\Gamma_0(2^n)$ if the four conditions
(1) $\sum_k e_k = 0$,
(2) $\sum_k k e_k \equiv 0 \bmod 2$,
(3) $\sum_k e_k 2^k \equiv 0 \bmod 24$,
(4) $\sum_k e_k 2^{n-k} \equiv 0 \bmod 24$,
are satisfied. Now we have

$$x_n = \frac{\eta(2^{n-1}\tau)^6}{\eta(2^{n-2}\tau)^2\eta(2^n\tau)^4}, \quad y_n = \frac{\eta(16\tau)^2\eta(2^{n-1}\tau)}{\eta(8\tau)\eta(2^n\tau)^2}.$$

It is clear that when n is an even integer greater than 2, the four conditions are all satisfied for x_n and y_n. We now show that x_n and y_n have poles only at ∞ of the claimed order.

Still assume that $n \geq 4$ is an even integer. Since x_n and y_n are η-products, they have no poles nor zeros in $\mathbb{H}$. Also, it can be checked directly that x_n and y_n have a pole of order 2^{n-4} and $2^{n-4}-1$, respectively, at ∞. It remains to consider other cusps. For an odd integer a and $k \in \{0, 1, \ldots, n-1\}$, the width of the cusp $a/2^k$ is

$$h_{n,k} = \begin{cases} 1, & \text{if} \quad k \geq \dfrac{n}{2}, \\ 2^{n-2k}, & \text{if} \quad k < \dfrac{n}{2}. \end{cases}$$

Choosing a matrix $\sigma = \begin{pmatrix} a & b \\ 2^k & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$, a local parameter at $a/2^k$ is

$$e^{2\pi i \sigma^{-1}\tau/h_{n,k}}.$$

Therefore, the order of a function $f(\tau)$ at $a/2^k$ is the same as the order of $f(\sigma\tau)$ at ∞, multiplied by $h_{n,k}$.

Now recall that, for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, we have

$$\theta_2(\tau) \mid \alpha = \begin{cases} \epsilon q^{1/8} + \cdots, & \text{if} \quad 2 \mid c, \\ \epsilon + \cdots, & \text{if} \quad 2 \nmid c, \end{cases}$$

and

$$\theta_3(\tau) \mid \alpha = \begin{cases} \epsilon + \cdots, & \text{if} \quad 2 \mid ac, \\ \epsilon q^{1/8} + \cdots, & \text{if} \quad 2 \nmid ac, \end{cases}$$

where ϵ represents a nonzero complex number, but may not be the same at each occurence. (Up to multipliers, if α is congruent to the identity matrix or $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ modulo 2, then the action of α fixes θ_2. Any other matrices will send θ_2 to either θ_3 or θ_4. This explains the fact about θ_2. The fact about θ_3 can be explained similarly.) When $k = n - 1$, we have

$$2^{n-1}\begin{pmatrix} a & b \\ 2^{n-1} & d \end{pmatrix}\tau = \frac{a(2^{n-1}\tau) + 2^{n-1}b}{(2^{n-1}\tau) + d} = \begin{pmatrix} a & 2^{n-1}b \\ 1 & d \end{pmatrix}(2^{n-1}\tau)$$

and

$$8\begin{pmatrix} a & b \\ 2^{n-1} & d \end{pmatrix}\tau = \frac{a(8\tau) + 8b}{2^{n-4}(8\tau) + d} = \begin{pmatrix} a & 8b \\ 2^{n-4} & d \end{pmatrix}(8\tau).$$

It follows that

$$x_n\left(\begin{pmatrix} a & b \\ 2^{n-1} & d \end{pmatrix}\tau\right) = \frac{\epsilon_1 q^{2^{n-4}} + \cdots}{\epsilon_2 + \cdots} = \epsilon q^{2^{n-4}} + \cdots,$$

and

$$y_n\left(\begin{pmatrix} a & b \\ 2^{n-1} & d \end{pmatrix}\tau\right) = \frac{\epsilon_1 q + \cdots}{\epsilon_2 + \cdots} = \epsilon q + \cdots,$$

where ϵ, ϵ_1, and ϵ_2 are nonzero complex numbers. That is, x_n and y_n have a zero of order 2^{n-4} and 1, respectively, at $a/2^{n-1}$.

When $k = 4, \ldots, n-2$, we have

$$2^{n-1}\begin{pmatrix} a & b \\ 2^k & d \end{pmatrix}\tau = \begin{pmatrix} 2^{n-k-1}a & -1 \\ 1 & 0 \end{pmatrix}(2^{2k-n+1}\tau + 2^{k-n+1}d),$$

$$8\begin{pmatrix} a & b \\ 2^k & d \end{pmatrix}\tau = \frac{a(8\tau)+8b}{2^{k-3}(8\tau)+d} = \begin{pmatrix} a & 8b \\ 2^{k-3} & d \end{pmatrix}(8\tau).$$

Therefore,

$$x_n\left(\begin{pmatrix} a & b \\ 2^k & d \end{pmatrix}\tau\right) = \frac{\epsilon_1 + \cdots}{\epsilon_2 + \cdots} = \epsilon + \cdots,$$

and

$$y_n\left(\begin{pmatrix} a & b \\ 2^k & d \end{pmatrix}\tau\right) = \frac{\epsilon_1 q + \cdots}{\epsilon_2 + \cdots} = \epsilon q + \cdots,$$

where ϵ, ϵ_1, and ϵ_2 are nonzero complex numbers. In other words, x_n has no poles nor zeros at $a/2^k$ for $k = 4, \ldots, n-2$, while y_n has zeros of order $h_{n,k}$ at those points.

When $k = 0, \ldots, 3$, we have

$$2^{n-1}\begin{pmatrix} a & b \\ 2^k & d \end{pmatrix}\tau = \begin{pmatrix} 2^{n-k-1}a & -1 \\ 1 & 0 \end{pmatrix}(2^{2k-n+1}\tau + 2^{k-n+1}d),$$

$$8\begin{pmatrix} a & b \\ 2^k & d \end{pmatrix}\tau = \begin{pmatrix} 2^{3-k}a & -1 \\ 1 & 0 \end{pmatrix}(2^{2k-3}\tau + 2^{k-3}d),$$

and we find that x_n and y_n have no zeros nor poles at $a/2^k$, $k = 0, \ldots, 3$.

In summary, we have shown that x_n and y_n have a pole of order 2^{n-4} and $2^{n-4}-1$, respectively, at ∞ and are holomorphic at any other points. Since 2^{n-4} and $2^{n-4}-1$ are clearly relatively prime, x_n and y_n generate the field of modular functions on $X_0(2^n)$. It remains to show that P_n is irreducible over $\mathbb{Q}$ and $P_n(x_n, y_n) = 0$.

When $n = 6$, we verify by a direct computation that $y_6^4 - x_6^3 - 4x_6 = 0$. Then the recursive formulas for x_n and y_n implies that $P_n(x_n, y_n) = 0$ for all $n \geq 6$. Finally, by the theory of algebraic curve (see [4, p. 194]), the field of modular functions on $X_0(2^n)$ is an extension field of $\mathbb{C}(x_n)$ of degree 2^{n-4}. In other words, the minimal polynomial of y_n over $\mathbb{C}(x_n)$ has degree 2^{n-4}. Now it is easy to see that $P_n(x, y)$ is a polynomial of degree 2^{n-4} in y with leading coefficient 1. We therefore conclude that P_n is irreducible. This completes the proof of Theorem 1.

ACKNOWLEDGMENT. The authors would like to thank Professor Hashimoto of the Waseda University for drawing their attention to the family of modular curves $X_0(2^n)$ and for several enlightening conversations. The authors would also like to thank Professor M.L. Lang of the National University of Singapore for providing information about

normalizers of congruence subgroups. The authors are grateful to Professor M. Zieve for bringing Elkies' work to their attention. Finally, the authors would like to thank the anonymous referee for thorough reading of the manuscript. His suggestion makes the statement of Theorem 1 simpler.

References

[1] A.O.L. Atkin and J. Lehner: *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.
[2] N.D. Elkies: *Explicit modular towers*; in Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing, Univ. Illinois at Urbana-Champaign, 1998, 23–32, `http://arxiv.org/abs/math/0103107`.
[3] N.D. Elkies: *The automorphism group of the modular curve* $X_0(63)$, Compositio Math. **74** (1990), 203–208.
[4] W. Fulton: Algebraic Curves, Reprint of 1969 original, Addison-Wesley, Redwood City, CA, 1989.
[5] S.D. Galbraith: *Equations for modular curves*, Doctoral thesis, Oxford University, 1996,
[6] J. Gonzàlez Rovira: *Equations of hyperelliptic modular curves*, Ann. Inst. Fourier (Grenoble) **41** (1991), 779–795.
[7] T. Hibino: *Formulae for relating the modular invariants and defining equations of* $X_0(40)$ *and* $X_0(48)$, Tokyo J. Math. **22** (1999), 279–288.
[8] T. Hibino and N. Murabayashi: *Modular equations of hyperelliptic* $X_0(N)$ *and an application*, Acta Arith. **82** (1997), 279–291.
[9] N. Ishida: *Generators and equations for modular function fields of principal congruence subgroups*, Acta Arith. **85** (1998), 197–207.
[10] N. Ishida and N. Ishii: *Generators and defining equation of the modular function field of the group* $\Gamma_1(N)$, Acta Arith. **101** (2002), 303–320.
[11] M.A. Kenku and F. Momose: *Automorphism groups of the modular curves* $X_0(N)$, Compositio Math. **65** (1988), 51–80.
[12] N. Murabayashi: *On normal forms of modular curves of genus* 2, Osaka J. Math. **29** (1992), 405–418.
[13] M. Newman: *Construction and application of a class of modular functions*, II, Proc. London Math. Soc. (3) **9** (1959), 373–387.
[14] A.P. Ogg: *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462.
[15] A.P. Ogg: *Über die Automorphismengruppe von* $X_0(N)$, Math. Ann. **228** (1977), 279–292.
[16] M.A. Reichert: *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, Math. Comp. **46** (1986), 637–658.
[17] M. Shimura: *Defining equations of modular curves* $X_0(N)$, Tokyo J. Math. **18** (1995), 443–456.
[18] Y. Yang: *Transformation formulas for generalized Dedekind eta functions*, Bull. London Math. Soc. **36** (2004), 671–682.
[19] Y. Yang: *Defining equations of modular curves*, Adv. Math. **204** (2006), 481–508.

Fang-Ting Tu
Department of Applied Mathematics
National Chiao Tung University
Hsinchu 300
Taiwan
e-mail: ft.am95g@cc.nctu.edu.tw

Yifan Yang
Department of Applied Mathematics
National Chiao Tung University
Hsinchu 300
Taiwan
e-mail: yfyang@math.nctu.edu.tw