Bull. Korean Math. Soc. **44** (2007), No. 2, pp. 379–383

AN AFFINE MODEL OF $X_0(mn)$

SoYoung Choi and Ja Kyung Koo*

Abstract. We show that the modular equation $\Phi_m^{T_n}(X,Y)$ for the Thompson series T_n corresponding to $\Gamma_0(n)$ gives an affine model of the modular curve $X_0(mn)$ which has better properties than the one derived from the modular j invariant. Here, m and n are relative prime. As an application, we construct a ring class field over an imaginary quadratic field K by singular values of $T_n(z)$ and $T_n(mz)$.

1. Introduction

Let mn be a product of coprime positive integers. In [1], Chen and Yui constructed the modular polynomial $\Phi_m^{T_n}(X,Y) \in \mathbb{Z}[X,Y]$ for the Thompson series $T_n(z)$ and investigated their properties.

In this article, we shall show that the modular polynomial $\Phi_m^{T_n}(X,Y)$ gives an affine model of the modular curve $X_0(nm)$ defined over $\mathbb{Q}$ (Theorem 2.2) which has better properties, than the usual one as in [4]. Here we note that $\Phi_m^{T_n}(X,Y)$ has much smaller degrees and coefficients than the usual one derived from the modular j invariant.

Asymptotically optimal curves yield excellent linear error-correcting codes over a finite field. Indeed, all the known asymptotically optimal towers of curves are related to reductions of (classical elliptic, Shimura, Drinfeld) modular curves ([2, 3]). In order to construct and use these Goppa codes one needs explicit equations for such curves with enough rational points. Thus the modular equations for the Thompson series can have practical applications to the construction of asymptotically optimal towers of curves.

As an application of the modular equation $\Phi_m^{T_n}(X,Y)$, we shall construct the ring class fields over an imaginary quadratic field K by singular values of the generators of the function field of $X_0(nm)$ (Theorem 3.3).

Throughout this article, we adopt the following notations:

- $\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) |\ c \equiv 0 \ mod\ N\}$ for any positive integer N

Received November 28, 2006.
2000 *Mathematics Subject Classification.* 11F11, 14H50.
Key words and phrases. modular curve, modular equation, class field.
* He was supported by Korea Research Foundation Grant (KRF-2002-070-C00003).

- $\mathfrak{H}$: the complex upper half-plane
- $\mathfrak{H}^*$: the extended complex upper half-plane
- $X_0(N)$: the modular curve $\Gamma_0(N)\backslash\mathfrak{H}^*$
- $K(X_0(N))$: the function field of $X_0(N)$ over $\mathbb{C}$
- T_n : the fundamental Thompson series corresponding to $\Gamma_0(n)$
- m : a positive integer coprime to n,

where we always assume that m and n are both > 1.

2. An affine model of $X_0(mn)$

Let $\Omega(m) = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad = m,\ a > 0,\ 0 \le b < d\}$ and $\Phi_m^{T_n}(X, T_n)$ be the modular equation for T_n defined by

$$\Phi_m^{T_n}(X, T_n) = \prod_{w \in \Omega(m)} (X - T_n \circ w).$$

Then $\Phi_m^{T_n}(X, T_n) \in \mathbb{Z}[X, T_n]$ and, as is shown in [1], it is irreducible over $\mathbb{C}(T_n)[X]$.

Theorem 2.1. $K(X_0(mn)) = \mathbb{C}(T_n(z), T_n(mz))$.

Proof. It is easy to show that $T_n(z)$ and $T_n(mz)$ are contained in $K(X_0(mn))$. From the definition of $\Phi_m^{T_n}(X, T_n)$ we know that $T_n(mz)$ is a root of $\Phi_m^{T_n}(X, T_n)$. Also $\Phi_m^{T_n}(X, T_n)$ is irreducible over $\mathbb{C}(T_n)$ of degree $|\Omega(m)|$. We can easily show that $[K(X_0(mn)) : K(X_0(n))] = [\Gamma_0(mn) : \Gamma_0(n)] = |\Omega(m)|$. Since $K(X_0(n))$ is equal to $\mathbb{C}(T_n)$, the result follows. □

By the fact $\Phi_m^{T_n}(T_n(mz), T_n(z)) = 0$ and Theorem 2.1, we have the following theorem.

Corollary 2.2. *The modular equation $\Phi_m^{T_n}(X, Y)$ gives an affine model of a modular curve $X_0(mn)$.*

Example 2.3. The following equations can be obtained by using the computer algebra system MAPLE.

$$\begin{aligned}\Phi_2^{T_3}(X, Y) = {} & X^3 + (-Y^2 + 108)X^2 + (-153Y + 2268)X \\ & + (Y^3 + 108Y^2 + 2268Y - 46224)\end{aligned}$$

gives an affine model of $X_0(6)$. Note that the degree of the highest X-term and Y-term of the usual modular equation derived from the modular j invariant is 12.

$$\begin{aligned}\Phi_3^{T_5}(X, Y) = {} & X^4 + (-Y^3 + 27Y + 30)X^3 + (-90Y^2 + 288Y + 1728)X^2 \\ & + (27Y^3 + 288Y^2 - 3745Y + 5406)X \\ & + (Y^4 + 30Y^3 + 1728Y^2 + 5406Y - 101124)\end{aligned}$$

gives an affine model of $X_0(15)$. Note that the degree of the highest X-term and Y-term of the usual one is 24.

Let p be a prime not dividing 15 and $N(X_0(15)(\mathbb{F}_{p^r}))$ be the number of $\mathbb{F}_{p^r}$-rational points of the curve $X_0(15)$ mod p ($\mathbb{F}_{p^r}$ is a finite field of p^r elements). We see from [7] that the genus of $X_0(15)$ is 1. Hence the equation for $X_0(15)$ has many rational points by the fact ([5, 6]) that

$$p^r + 1 - [2\sqrt{p^r}] \leq N(X_0(15)(\mathbb{F}_{p^r})) \leq p^r + 1 + [2\sqrt{p^r}],$$

where $[x]$ is the largest integer less than or equal to x. Therefore, one can use it to construct and use Goppa code.

3. Application to class fields

Since the modular equation $\Phi_n^{T_m}(X, Y)$ gives an affine model of the modular curve $X_0(mn)$, there exists an isomorphism

$$\varphi : \Gamma_0(mn)\backslash\mathfrak{H} - \varphi^{-1}(Sing(V_{mn})) \longrightarrow V_{mn} - Sing(V_{mn}),$$

where V_{mn} is the affine algebraic curve defined by $\Phi_m^{T_n}(X,Y) = 0$ and $Sing(V_{mn})$ is the singular locus of V_{mn}. In this section, we construct a ring class field over an imaginary quadratic field K by using a nonsingular point $(T_n(m\alpha), T_n(\alpha))$ in V_{mn}.

To this end we need the following well known results.

Proposition 3.1. *Let $\mathfrak{F}_N$ be the field of modular functions of level N rational over $\mathbb{Q}(e^{2\pi i/N})$, and let K be an imaginary quadratic field. Let $\mathcal{O}_K$ be the maximal order of K and $\mathfrak{a}$ be an $\mathcal{O}_K$-ideal such that $\mathfrak{a} = [z_1, z_2]$ and $\alpha = z_1/z_2 \in \mathfrak{H}$. Then the field $K\mathfrak{F}_N(\alpha)$ generated over K by all values $f(\alpha)$ with $f \in \mathfrak{F}_N$ and f defined at α, is the ray class field $K_{(N)}$ over K with modulus $N\mathcal{O}_K$.*

Proof. [4, Ch. 10. Corollary of Theorem 2]. □

Proposition 3.2. *$\mathbb{Q}(T_n(z), T_n(mz))$ $(z \in \mathfrak{H})$ is the field of all modular functions in $K(X_0(mn))$ whose Fourier coefficients with respect to $q = e^{2\pi iz}$ belong to $\mathbb{Q}$.*

Proof. We can show the assertion by using the linear disjointness property adopted in [7, p. 141]. □

Now we have the following theorem, whose proof uses Chen-Yui's ideas from [1].

Theorem 3.3. *Let α be a root in $\mathfrak{H}$ of a quadratic equation $az^2 + bz + c = 0$ such that $a > 0, (a, b, c) = 1$, and $b^2 - 4ac = r^2 d_K < 0\,(r > 0)$. Let $K = \mathbb{Q}(\alpha)$ and $\mathcal{O}\,(= \mathbb{Z}[a\alpha])$ be an order in K of discriminant $r^2 d_K$. We suppose that $(T_n(m\alpha), T_n(\alpha))$ does not belong to $Sing(V_{mn})$. Then $K(T_n(m\alpha), T_n(\alpha))$ is the ring class field of an imaginary quadratic order $\mathcal{O}'$ of discriminant $f^2 d_K$, where $f = rmn/(a, mn)$ and d_K is the discriminant of K.*

Proof. By Proposition 3.2 $j(z) \in \mathbb{Q}(T_n(z), T_n(mz))$. Hence $K(T_n(\alpha), T_n(m\alpha))$ is a finite extension of the ring class field $K(j(\alpha))$ of $\mathcal{O}$. Note that $K(T_n(\alpha), T_n(m\alpha))$ is a subfield of the ray class field $K_{(nm)}$ by Proposition 3.1. Thus, it follows that the fixing group of $\mathbb{Q}(T_n(z), T_n(mz))$ is contained in the group $P(\mathcal{O})$, where $P(\mathcal{O})$ is the group generated by all principal ideals of $\mathcal{O}$. Let (β) be a principal ideal of $\mathcal{O}$ relatively prime to mn. Write $\beta = xa\alpha + y \in \mathbb{Z}\cdot a\alpha + \mathbb{Z}(= \mathcal{O})$. Let $\mathcal{A}_\beta$ be an element of $SL_2(\mathbb{Z})$ whose image in $SL_2(\mathbb{Z}/mn\mathbb{Z})$ is equal to $\begin{pmatrix} -bx+y & -cx \\ axN(\beta)^{-1} & yN(\beta)^{-1} \end{pmatrix}$. Let $SL_2(\mathbb{Q})_\alpha$ be the isotropy subgroup of α in $SL_2(\mathbb{Q})$. Then we have

$$\begin{aligned}(\beta) \text{ fixes } T_n(\alpha) \text{ and } T_n(m\alpha) &\Leftrightarrow T_n(\alpha)^{[(\beta),\ K_{ab}/K]} = T_n(\alpha) \text{ and} \\ &\quad T_n(m\alpha)^{[(\beta),\ K_{ab}/K]} = T_n(m\alpha) \\ &\Leftrightarrow T_n(\mathcal{A}_\beta\alpha) = T_n(\alpha) \text{ and } T_n(m\mathcal{A}_\beta\alpha) = T_n(m\alpha) \\ &\Leftrightarrow \mathcal{A}_\beta \in \pm\Gamma_0(mn)SL_2(\mathbb{Q})_\alpha.\end{aligned}$$

Here the statement that $T_n(\mathcal{A}_\beta\alpha) = T_n(\alpha)$ and $T_n(m\mathcal{A}_\beta\alpha) = T_n(m\alpha)$ implies $\mathcal{A}_\beta \in \pm\Gamma_0(mn)SL_2(\mathbb{Q})_\alpha$ due to the fact that $(T_n(m\alpha), T_n(\alpha))$ is a nonsingular point. We know that $SL_2(\mathbb{Z})_\alpha$ is trivial unless α is $SL_2(\mathbb{Z})$-equivalent to $e^{2\pi i/h}$ with $h \in \{3, 4\}$. Assuming $SL_2(\mathbb{Z})_\alpha = \{\pm 1\}$, we see that $\mathcal{A}_\beta \in \pm\Gamma_0(mn)$ if and only if $mn|ax$. Therefore the principal ideals in $\mathcal{O}$ which fix $T_n(\alpha)$ and $T_n(m\alpha)$ are of the form (β) with $\mathrm{disc}(\beta)$ dividing $(rmn/(a, mn))^2 d_K$. But these principal ideals are all in $P(\mathcal{O}')$. The cases α is $SL_2(\mathbb{Z})$-equivalent to $e^{2\pi i/h}$ with h=3 or 4 can be treated similarly. These prove our assertion. □

Example 3.4. In Example 2.3 we have shown that

$$\begin{aligned}\Phi_3^{T_5}(X, Y) = {} & X^4 + (-Y^3 + 27Y + 30)X^3 + (-90Y^2 + 288Y + 1728)X^2 \\ & + (27Y^3 + 288Y^2 - 3745Y + 5406)X \\ & + (Y^4 + 30Y^3 + 1728Y^2 + 5406Y - 101124)\end{aligned}$$

gives an affine model of $X_0(15)$. By approximating $T_5(3i)$ and $T_5(i)$ with the aid of a computer, we know that $(T_5(3i), T_5(i)) \approx (0.1523507, 535.4916562)$ and

$$\frac{\partial \Phi_3^{T_5}}{\partial Y}(T_5(3i), T_5(i)) \approx -304191454 \cdot 10^{22}.$$

Thus $T_5(3i)$ and $T_5(i)$ generate the ring class field of the imaginary quadratic order of discriminant $(15)^2 d_K$ over $K = \mathbb{Q}(i)$.

References

[1] I. Chen and N. Yui, *Singular values of Thompson series*, Groups, difference sets, and the Monster (Columbus, OH, 1993), 255–326, Ohio State Univ. Math. Res. Inst. Publ., 4, de Gruyter, Berlin, 1996.

[2] N. D. Elkies, *Explicit towers of Drinfeld modular curves*, European Congress of Mathematics, Vol. II (Barcelona, 2000), 189–198, Progr. Math., 202, Birkhauser, Basel, 2001.

[3] E. U. Gekeler, *Asymptotically optimal towers of curves over finite fields*, Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), 325–336, Springer, Berlin, 2004.
[4] S. Lang, *Elliptic functions*, With an appendix by J. Tate. Second edition. Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987.
[5] K. Lauter, *The maximum or minimum number of rational points on genus three curves over finite fields*, With an appendix by Jean-Pierre Serre. Compositio Math. **134** (2002), no. 1, 87–111.
[6] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algebrique sur un corps fini*, C. R. Acad. Sci. Paris Ser. I Math. **296** (1983), no. 9, 397–402.
[7] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kano Memorial Lectures, No. 1. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971.

SoYoung Choi
School of Mathematics
Korea Institute for Advanced Study (KIAS)
Seoul 130-722, Korea
E-mail address: young@kias.re.kr

Ja Kyung Koo
Department of Mathematics
Korea Advanced Institute of Science and Technology
Daejon 305-701, Korea
E-mail address: jkkoo@math.kaist.ac.kr