JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **24**, No. 3, September 2011

MODULAR POLYNOMIALS FOR MODULAR CURVES $X_0^+(N)$

SoYoung Choi*

Abstract. We show that for all $N \geq 1$, the modular function field $K(X_0^+(N))$ is generated by $j(z)j(Nz)$ and $j(z)+j(Nz)$ over $\mathbb{C}$, where $j(z)$ is the modular invariant. Moreover we derive the defining equation of the the modular function field $K(X_0^+(N))$ from the classical modular polynomial $\Phi_N(X,Y)$.

1. Introduction

Let $\Gamma_0^+(N)$ be the group generated by the Hecke group $\Gamma_0(N)$ and the Fricke involution $W_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. Let $X_0(N)$ and $X_0^+(N)$ be the modular curves associated with the groups $\Gamma_0(N)$ and $\Gamma_0^+(N)$ respectively. Then the function field of $X_0(N)$ is generated by $j(z)$ and $j(Nz)$, where $j(z)$ is the modular invariant. The modular polynomial

$$\Phi_N(X, j(z)) = \prod_{\alpha \in \Delta_N^*} (X - j(\alpha z)) \in \mathbb{Z}[X, j]$$

of order $\psi(N)$ gives a relation between j and $j \circ N$, where $\psi(N)$ denotes the number of the set $\Delta_N^* = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) |\ (a,b,d) = 1,\ a > 0,\ ad = N,\ 0 \leq b < d\}$. Then the modular equation $\Phi_N(X,Y) = 0$ is an affine singular model of the modular curve $X_0(N)$. In this paper, we derive a defining equation of the modular curve $K(X_0^+(N))$ from the modular polynomial $\Phi_N(X,Y) = 0$. To do this we need the following property:

Proposition 1.1. *(1) $\Phi_N(X, j)$ is irreducible over $\mathbb{C}(j)$ and has the degree $\psi(N)$.*

Received June 01, 2011; Accepted August 25, 2011.
2010 Mathematics Subject Classification: Primary 11F03, 11F11.
Key words and phrases: modular invariant, modular polynomial.
This research was supported by Basic Science Research Program through the National Research Foundation(NRF)funded Ministry of Education, Science and Technology(2010-0003653).

(2) $\Phi_N(X, j) = \Phi_N(j, X)$

Proof. [1, Chap. 5, §2, Theorem 3.], $\square$

2. An affine singular model of the modular curve $X_0^+(N)$

THEOREM 2.1. *The function field of the modular curve* $X_0^+(N)$ *is* $\mathbb{C}(j(z)j(Nz), j(z) + j(Nz))$.

Proof. We consider the subfield $\mathbb{C}(j(z)j(Nz), j(z)+j(Nz))$ of $K(X_0^+(N))$, where $j(z)$ is the modular invariant. Since $K(X_0(N))$ is an algebraic extension of $K(X_0^+(N))$ of degree $[\overline{\Gamma_0^+(N)} : \overline{\Gamma_0(N)}]$ (see [2], p.31), we have $[K(X_0(N)) : K(X_0^+(N))] = 2$. Moreover, since $X^2 - (j(z) + j(Nz))X + j(z)j(Nz) = 0$ is the minimal polynomial of both $j(z)$ and $j(Nz)$ over $\mathbb{C}(j(z)j(Nz), j(z) + j(Nz))$, we have to get the equality

$$K(X_0^+(N)) = \mathbb{C}(j(z)j(Nz), j(z) + j(Nz))$$

for all $N \geq 1$ by virtue of the fact $K(X_0(N)) = \mathbb{C}(j(z), j(Nz))$ (see [2], Proposition 2.10). $\square$

Since the modular equation $\Phi_N(X, Y)$ is symmetric, there exist a polynomial $F_N(x, y) \in \mathbb{Z}[x, y]$ such that $\Phi_N(X, Y) = F_N(X + Y, XY)$. Then we have the following theorem.

THEOREM 2.2. $F_N(x, y)$ *gives an affine singular model of the modular curve* $X_0^+(N)$.

Proof. We know that $F_N(j(z)+j(Nz), j(z)j(Nz)) = \Phi_N(j(Nz), j(z)) = 0$. Assume that $F_N(x, y) = G(x, y)H(x, y)$ with $G(x, y)$, $H(x, y) \in \mathbb{C}[x, y]$. Then we have that $\Phi_N(X, Y) = G(X + Y, XY)H(X + Y, XY)$. Since $\Phi_N(X, Y)$ is an irreducible polynomial, either $G(X + Y, XY)$ or $H(X + Y, XY)$ is a constant and hence either $G(x, y)$ or $H(x, y)$ is constant. This implies that $F_N(x, y)$ gives a defining equation of the modular curve $X_0^+(N)$. $\square$

EXAMPLE 2.3. For $N = 2$ we have $\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 1488XY(X + Y) - 162000(X^2 + Y^2) + 40773375XY + 8748000000(X + Y) - 157464000000000$ which induces $F_2(x, y) = x^3 - 162000x^2 - y^2 + 1485xy + 8748000000x + 41097375y - 157464000000000$.

References

[1] S. Lang, *Elliptic Functions*, Springer-Verlag, 1987.
[2] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publ. Math. Soc. Japan, No. 11, Tokyo Prineton, 1971.

*
Department of Mathematics Education
Dongguk University
Gyeongju 780-714, Republic of Korea
E-mail: young@dongguk.ac.kr