TOKYO J. MATH.
VOL. 18, NO. 2, 1995

Defining Equations of Modular Curves $X_0(N)$

Mahoro SHIMURA

Waseda University

(Communicated by T. Suzuki)

1. Introduction.

We have as a defining equation of the modular curve $X_0(N)$ the modular equation of level N, which has many good properties; e.g. it reflects the properties of $X_0(N)$ that is the coarse moduli space of the isomorphism classes of the generalized elliptic curves with a cyclic subgroup of order N. But its degree and coefficients are too large for its application to practical calculation on $X_0(N)$. While it is an important problem to determine the algebraic points on $X_0(N)$, we need a handier form of defining equation, which will also serve to solve other related problems.

In the present paper, we give a general method to explicitly calculate a system of defining equations of an arbitrary modular curve $X_0(N)$. In case of a hyperelliptic modular curve of genus two, a kind of normal form of defining equations is given by Murabayashi (cf. [M]). We generalize his method. We list defining equations of all modular curves $X_0(N)$ of genus two to six. One should note that our algorithm works for $X_0(N)$ of genus greater than six.

The form of our defining equations is as follows. If $X_0(N)$ is hyperelliptic or of genus three, then the number of our defining equations is one. If $X_0(N)$ is non-hyperelliptic and of genus greater than three, then our system of defining equations is given as the intersection of some quadratic and cubic hypersurfaces on $\boldsymbol{P}^{g-1}$. In particular, we list the defining equations of $X_0(N)$ ($N=34$, 43, 45, 64) which are non-hyperelliptic of genus three. We note that $X_0(64)$ is the Fermat curve of degree four.

In our method, we cannot have defining equations of modular curves of genus zero or one. But defining equations of some modular curves of genus one (i.e. $X_0(N)$, $N=14$, 20, 24) can be obtained by means of a covering from some $X_0(N)$. We can explicitly give covering maps between modular curves.

To get our equations, we use the Fourier expansions of certain cusp forms of weight 2 on $\Gamma_0(N)$. Their Fourier coefficients can be given by the Brandt matrix (cf.

Received June 6, 1994
Revised December 5, 1994