Families of elliptic Q-curves defined over number fields with large degrees

By Takeshi HIBINO and Atsuki UMEGAKI

Department of Mathematics, School of Science and Engineering, Waseda University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1998)

Abstract: An elliptic curve E defined over $\bar{\mathbf{Q}}$ is called a $\mathbf{Q}$-curve, if E and E^σ are isogenous over $\bar{\mathbf{Q}}$ for any σ in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Many examples of $\mathbf{Q}$-curves defined over quadratic fields have already been known. In this paper, we will give families of $\mathbf{Q}$-curves defined over quartic and octic number fields.

1. Introduction. Definition 1.1. Let E be an elliptic curve defined over $\bar{\mathbf{Q}}$. Then E is called a $\mathbf{Q}$-*curve* if E and its Galois conjugate E^σ are isogenous over $\bar{\mathbf{Q}}$ for any σ in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Moreover we call a $\mathbf{Q}$-curve E *of degree* N if E has an isogeny to its conjugate E^σ with degree dividing N for any σ in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$.

In Gross [2], E was assumed to have complex multiplication, but we do not assume that in this paper.

$\mathbf{Q}$-curves are deeply connected with a modularity problem for a certain class of high dimensional abelian varieties over $\mathbf{Q}$. The following conjecture, which is known as a generalized Taniyama-Shimura conjecture, elucidates the relation of $\mathbf{Q}$-curves to the problem:

Conjecture 1.2 (Ribet). Every $\mathbf{Q}$-curve is modular, namely it is isogenous over $\bar{\mathbf{Q}}$ to a factor of the jacobian variety of the modular curve $X_1(N)$ for a positive integer N.

Recently many examples of $\mathbf{Q}$-curves defined over quadratic fields have been constructed in [3], [4] and [8], and the validity of this conjecture have been confirmed in these cases. Thus we are interested in finding non-trivial examples of $\mathbf{Q}$-curves defined over number fields whose degrees are greater than two.

In his paper [3], Hasegawa has given families of $\mathbf{Q}$-curves of prime degree p under the condition that the modular curve $X_0(p)$ has genus zero. In the present paper we obtain families of $\mathbf{Q}$-curves of degree N over quartic and octic number fields, by dealing with the case where the modular curve $X_0(N)$ is hyperelliptic and N is a square-free positive integer.

2. Data on the modular curve $X_0(N)$. Let $N=\prod_{i=1}^n p_i$ be a square-free positive integer. We denote by $X_0(N)$ the modular curve corresponding to the congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\boldsymbol{Z})$. For a positive integer $d \neq 1$ dividing N, we define the Atkin-Lehner involution w_d on $X_0(N)$, and denote by $X_0^*(N)$ the quotient curve $X_0(N)/\langle w_d \mid d|\, N\rangle$, where w_1 means the identity morphism over $X_0(N)$. From now on we assume that $X_0(N)$ is a hyperelliptic curve with genus g. In order to state our main result, we need some basic data about the modular curve $X_0(N)$, i.e. a defining equation of $X_0(N)$ over $\mathbf{Q}$, the action of the Atkin-Lehner involutions w_d, $d|N$, $d \neq 1$, on $X_0(N)$ and a certain formula for the covering map j from $X_0(N)$ to the projective j-line. We can calculate these by using the method of [5]. In the following, we sketch this method which is based on the computation of the Fourier coefficients of some modular forms.

Let $S_2(\Gamma_0(N))$ be the vector space over $\mathbf{C}$ of cusp forms of weight two for $\Gamma_0(N)$. We note that there is a natural isomorphism:

$$H^0(X_0(N),\ \Omega^1_{X_0(N)/\mathbf{C}}) \cong S_2(\Gamma_0(N)).$$

From the assumption that N is square-free and $X_0(N)$ is hyperelliptic, any automorphism w_d, $d|N$, has no fixed cuspidal points, so $\overline{\sqrt{-1}\,\infty}$ is not a Weierstrass point, where $\overline{\sqrt{-1}\,\infty}$ is the point of $X_0(N)$ represented by $\sqrt{-1}\,\infty$. Therefore we can choose a basis $h_1, \ldots, h_g$ of $S_2(\Gamma_0(N))$ with the following Fourier expansions:

$$\begin{aligned} h_1(z) &= q^g + s_1^{(g+1)} q^{g+1} + \cdots + s_1^{(i)} q^i + \cdots, \\ h_2(z) &= q^{g-1} + s_2^{(g)} q^g + \cdots + s_2^{(i)} q^i + \cdots, \\ &\vdots \\ h_g(z) &= q + s_g^{(2)} q^2 + \cdots + s_g^{(i)} q^i + \cdots, \end{aligned}$$