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 $\mathrm{SL}_2(\mathbf{Z})$. 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 $X_0(N)/\langle w_d \mid d \mid N\rangle$, 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 $h_1, \dots, h_g$ of $S_2(\Gamma_0(N))$ with the following Fourier expansions:

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

Table Ⅰ. Data on $X_0(N)$

N	$f(x)$	$d,\ (w_d^* x,\ w_d^* y)$
22	$2(x^3+4x^2+4x+2)(2x^3+4x^2+4x+1)$	$2,\ \left(\frac{1}{x},\ -\frac{y}{x^3}\right);\ 11,\ (x,\ -y)$
26	$x^6-8x^5+8x^4-18x^3+8x^2-8x+1$	$2,\ \left(\frac{1}{x},\ \frac{y}{x^3}\right);\ 26,(x,\ -y)$
33	(x^2+x+3) $(x^6+7x^5+28x^4+59x^3+84x^2+63x+27)$	$3,\ \left(\frac{3}{x},\ -\frac{9y}{x^4}\right);\ 11,\ (x,\ -y)$
35	$(x^2+x-1)(x^6-5x^5-9x^3-5x-1)$	$7,\ \left(-\frac{1}{x},\ -\frac{y}{x^4}\right);\ 35,\ (x,\ -y)$
39	$(x^4+x^3-x^2+x+1)(x^4-7x^3+11x^2-7x+1)$	$3,\ \left(\frac{1}{x},\ \frac{y}{x^4}\right);\ 39,\ (x,\ -y)$
46	$(x^3+x^2+2x+1)(x^3+4x^2+4x+8)$ $(x^6+5x^5+14x^4+25x^3+28x^2+20x+8)$	$2,\ \left(\frac{2}{x},\ -\frac{8y}{x^6}\right);\ 23,\ (x,\ -y)$
30	$(x^2+x-1)(x^2+4x-1)(x^4+x^3+2x^2-x+1)$	$2,\ \left(\frac{x+1}{x-1},\ -\frac{4y}{(x-1)^3}\right);$ $5,\ \left(-\frac{1}{x},\ \frac{y}{x^4}\right);\ 15,\ (x,\ -y)$

where $q=e^{2\pi\sqrt{-1}\,z}$ and the coefficients $s_k^{(i)}$ are rational numbers. By the assumption of the hyperellipticity, we may write a defining equation of $X_0(N)$ of the type

$$y^2=f(x), \tag{2.1}$$

where f is a polynomial over $\mathbf{Q}$. We put $x=\dfrac{h_2(z)}{h_1(z)}=q^{-1}+\cdots$. Then x defines a covering map from $X_0(N)$ to the projective line of degree two (cf. [7]). Now we put $y=\dfrac{q}{h_1(z)}\dfrac{dx}{dq}=-q^{-(g+1)}+\cdots$. Then x and y satisfy an equation of the form (2.1), which can be viewed as a defining equation of $X_0(N)$, and we can determine recursively the coefficients of $f(x)$ by observing the Fourier expansions of x and y.

Denote by $\mathbf{Q}(X_0(N))$ the function field of $X_0(N)$ defined over $\mathbf{Q}$. From the action of w_d on $S_2(\Gamma_0(N))$, we explicitly describe the action of w_d^* on the generators x and y of $\mathbf{Q}(X_0(N))$. To construct families of $\mathbf{Q}$-curves defined over number fields with degree 4 and 8, we consider the case where the level N is a composite number, namely

$$N=22,\ 26,\ 30,\ 33,\ 35,\ 39 \text{ and } 46.$$

Then we obtain the following result:

Proposition 2.1. *A defining equation of $X_0(N)$ and the action of w_d^* on x and y are given as in Table* Ⅰ.

Using this result, we find an expression of the covering map j in terms of x and y; For a positive integer M which gives the hyperelliptic involution w_M, *i.e.* $w_M^*x=x$ and $w_M^*y=-y$, we put $j_M=w_M^*j$. Then $j+j_M$ and $\dfrac{j-j_M}{y}$ are w_M^*-invariant, so they are rational functions of x, which are determined explicitly by observing the pole divisors and the values at the cusps of x, y, j and j_M, and also by comparing the Fourier expansions. Since the size of the expression is rather large, we shall give the covering map j only for $N=22$ and 30 in Table Ⅲ.

3. Results. Next we consider a parameterization of the $\mathbf{Q}$-rational points on $X_0^*(N)$ by using the function x of $\mathbf{Q}(X_0(N))$. We define an element t of $\mathbf{Q}(X_0(N))$ by a 'trace'

$$t=k_N\cdot\sum_{d\mid N}w_d^*(x), \tag{3.2}$$

where k_N is a rational constant.

Lemma 3.1. *If $k_N\neq 0$, then t parameterizes the $\mathbf{Q}$-rational points on $X_0^*(N)$.*

Proof. We see that the function field $\mathbf{Q}(X_0(N))$ of $X_0(N)$ is a $(2,\cdots,2)$-extension of degree 2^n over $\mathbf{Q}(X_0^*(N))$, since the Galois group of the extension is generated by the set of the automorphisms $\{w_d^*\mid d\mid N\}$. Since the pole divisor $(x)_\infty$ of x is equal to $\overline{\sqrt{-1}\,\infty}+w_M(\overline{\sqrt{-1}\,\infty})$, it follows that

$$(t)_\infty=\frac{1}{2}\sum_{d\mid N}w_d((x)_\infty)=\sum_{d\mid N}w_d(\overline{\sqrt{-1}\,\infty}).$$

Table II. Data on parameterization of $X_0(N)$

N	k_N	$x(r)$	$y(r)$
22	$\frac{1}{4}$	$r+\sqrt{r^2-1}$	$\left((2r-1)\sqrt{r+1}+(2r+1)\sqrt{r-1}\right)\sqrt{16r^3+48r^2+44r+13}$
26	$\frac{1}{4}$	$r+\sqrt{r^2-1}$	$\left((2r-1)\sqrt{r+1}+(2r+1)\sqrt{r-1}\right)\sqrt{4r^3-16r^2+5r-1}$
33	$\frac{1}{4}$	$r+\sqrt{r^2-3}$	$\left(2r^2-3+2r\sqrt{r^2-3}\right)\sqrt{(2r+1)(8r^3+28r^2+38r+17)}$
35	$\frac{1}{4}$	$r+\sqrt{r^2+1}$	$\left(2r^2+1+2r\sqrt{r^2+1}\right)\sqrt{(2r+1)(8r^3-20r^2+6r-19)}$
39	$\frac{1}{4}$	$r+\sqrt{r^2-1}$	$\left(2r^2-1+2r\sqrt{r^2-1}\right)\sqrt{(4r^2-14r+9)(4r^2+2r-3)}$
46	$\frac{1}{4}$	$r+\sqrt{r^2-2}$	$\left(r(2r^2-3)+(2r^2-1)\sqrt{r^2-2}\right)\sqrt{(8r^3+20r^2+8r+1)(8r^3+20r^2+16r+5)}$
30	$\frac{1}{8}$	$r+\sqrt{r^2-1}-\sqrt{r^2+r+\sqrt{r^2-r}}$	$2\sqrt{(4r+1)(4r+5)}\left((8r^2-5)r+(8r^2+4r-2)\sqrt{r^2-r}+(-8r^2+4r+2)\sqrt{r^2+r}+(-8r^2+1)\sqrt{r^2-1}\right)$

Clearly t is a non-constant rational function and $[\mathbf{Q}(X_0(N)):\mathbf{Q}(t)]=\deg((t)_\infty)=2^n$. Therefore t generates $\mathbf{Q}(X_0^*(N))$ over $\mathbf{Q}$. This completes the proof. □

Conversely, we parameterize the points on $X_0(N)$ which are $\mathbf{Q}$-rational points on $X_0^*(N)$ by considering the fibre of the convering map $X_0(N)\to X_0^*(N)$, $x\mapsto t$. We specialize the function t by a rational number r. Then we obtain the following result:

Proposition 3.2. *Let k_N, $x(r)$ and $y(r)$ be as in Table* II. *Then the point $P_r=(x(r),y(r))$ on $X_0(N)$ is a unique point of the fibre of the $\mathbf{Q}$-rational point represented by r on $X_0^*(N)$ up to conjugacy.*

Proof. From Proposition 2.1 and Lemma 3.1, we can check that P_r is one of the points on the modular curve $X_0(N)$ which belong to the fibre of the point represented by r on $X_0^*(N)$. This completes the proof of the proposition. □

Let K_r be the extension over $\mathbf{Q}$ generated by $x(r)$ and $y(r)$. Then we remark that K_r is a $(2,\dots,2)$-extension which is defined independently of the choice of P_r and there exist infinitely many rational numbers r such that $[K_r:\mathbf{Q}]=2^n$ by Hilbert's irreducibility theorem. We put $j_r=j(x(r),y(r))$ and define an elliptic curve E_r with j-invariant j_r by

$$E_r:\begin{cases} Y^2+Y=X^3 & \text{if } j_r=0,\\ Y^2=X^3+X & \text{if } j_r=1728,\\ Y^2+XY=X^3-\dfrac{36}{j_r-1728}X-\dfrac{1}{j_r-1728} & \text{otherwise.}\end{cases}$$

Our main result is the following:

Theorem 3.3. *For any rational number r, E_r is a $\mathbf{Q}$-curve of degree N defined over K_r. Moreover every non-CM $\mathbf{Q}$-curve of degree N is isogenous to E_r over $\bar{\mathbf{Q}}$.*

Proof. We use the following result of Elkies [1]: any elliptic curve corresponding to the $\mathbf{Q}$-rational point of $X_0^*(N)$ is a $\mathbf{Q}$-curve of degree N, and conversely any non-CM $\mathbf{Q}$-curve of degree N corresponds to a $\mathbf{Q}$-rational point of $X_0^*(N)$. Therefore the assertion is clear. □

Remark 3.4. In the case where N is a prime number, we can also construct a similar family of $\mathbf{Q}$-curves of degree N over quadratic fields.

Our families have the following interesting application:

Remark 3.5. In the case $N=22$, we can prove the following claim using Theorem C in [4]: *If the denominator of r is prime to* 11 *and r is congruence to neither* 1 *nor* 9 *modulo* 11, *then the elliptic curve E_r is a modular $\mathbf{Q}$-curve defined over K_r.*
The proof will be given in another paper ([6]).

Table Ⅲ. Data on j ($N = 22, 30$)

$N = 22$	$j = (A(x) + B(x)y)/(2x^{22})$
$A(x)$	$x^{33} + 22x^{32} + 11\cdot 19x^{31} + 2^3 11\cdot 13x^{30} + 2^4 11\cdot 23x^{29}$ $+ 2\cdot 11\cdot 443x^{28} + 2^6 11\cdot 23x^{27} + 2^7 11\cdot 13x^{26} + 2^6 11\cdot 19x^{25}$ $+ 2^9 11x^{24} + 2^{10}x^{23} + 2^9 3x^{22} + 2^{16} 3x^{21} + 2^{17} 7\cdot 23x^{20}$ $+ 2^{16} 11\cdot 23\cdot 47x^{19} + 2^{19} 11\cdot 2663x^{18} + 2^{20} 3\cdot 11\cdot 5591x^{17}$ $+ 2^{17} 11\cdot 1189553x^{16} + 2^{22} 11\cdot 401\cdot 613x^{15} + 2^{23} 5\cdot 11\cdot 125899x^{14}$ $+ 2^{22} 11\cdot 107\cdot 151\cdot 317x^{13} + 2^{25} 3\cdot 11\cdot 337\cdot 2081x^{12} + 2^{26} 31050451x^{11}$ $+ 2^{25} 3\cdot 7\cdot 11\cdot 13\cdot 45587x^{10} + 2^{32} 11\cdot 13\cdot 41\cdot 331x^9 + 2^{33} 3\cdot 11\cdot 53\cdot 827x^8$ $+ 2^{32} 11\cdot 320107x^7 + 2^{35} 11\cdot 39341x^6 + 2^{36} 1115359x^5$ $+ 2^{36} 11\cdot 9283x^4 + 2^{40} 3^2 11\cdot 29x^3 + 2^{41} 11\cdot 41x^2 + 2^{44} 11x + 2^{44}$
$B(x)$	$(x + 1)(x + 2)(x + 4)(x^2 + 16)(x^2 + 3x + 4)(x^2 + 4x + 8)$ $(x^2 + 6x + 4)(x^3 - 8x^2 + 16x + 16)(x^3 + 4x^2 + 16x + 16)$ $(x^3 - 16x - 32)(x^4 - 4x^3 + 8x^2 + 32x + 64)$ $(x^6 + 4x^5 + 16x^4 + 96x^3 + 320x^2 + 512x + 256)$

$N = 30$	$j = (A(x) + B(x)y)/(2(x - 1)^{30}x^5(x + 1)^{10})$
$A(x)$	$x^{60} - 5x^{59} - 30x^{58} + 235x^{57} + 25x^{56} - 3726x^{55} + 7620x^{54}$ $+ 20940x^{53} - 96255x^{52} + 21785x^{51} + 473942x^{50} - 695985x^{49}$ $- 1002775x^{48} + 3161780x^{47} + 419176x^{46} - 8205664x^{45}$ $+ 2472933x^{44} + 36683843x^{43} + 418878642x^{42} + 4934156855x^{41}$ $+ 33020966525x^{40} + 139304348910x^{39} + 392406277628x^{38}$ $+ 738615506700x^{37} + 853857680085x^{36} + 358521497865x^{35}$ $- 558814702826x^{34} - 1010196638005x^{33} - 481353378819x^{32}$ $+ 297255387224x^{31} + 372811349680x^{30} - 40731416160x^{29}$ $- 78597010813x^{28} + 91186120441x^{27} + 76990681110x^{26}$ $- 58178746527x^{25} - 107557876085x^{24} + 153414048430x^{23}$ $- 167568580740x^{22} + 184073373604x^{21} - 183406038941x^{20}$ $+ 156351681587x^{19} - 109878375758x^{18} + 66498621453x^{17}$ $- 35422847525x^{16} + 16250713012x^{15} - 6333882520x^{14}$ $+ 2042556352x^{13} - 541480745x^{12} + 131915465x^{11}$ $- 32472234x^{10} + 7220541x^9 - 1378785x^8 + 267314x^7$ $- 73404x^6 + 27524x^5 - 8825x^4 + 1963x^3 - 286x^2 + 25x - 1$
$B(x)$	$(x^2 - 4x - 1)(x^2 + 2x - 1)(x^3 + x^2 + x - 1)$ $(x^3 + x^2 + 3x - 1)(x^3 + 3x^2 - x + 1)(x^4 + 6x^2 + 1)$ $(x^4 + 4x^3 - 1)(x^6 + 5x^4 + 16x^3 - 5x^2 - 1)$ $(x^6 - 4x^5 + 5x^4 + 24x^3 - 5x^2 - 4x - 1)$ $(x^6 - 2x^5 + 7x^4 + 12x^3 + 23x^2 - 10x + 1)$ $(x^8 - 4x^7 - 4x^6 + 6x^5 + 38x^4 - 28x^3 + 28x^2 - 4x + 1)$ $(x^9 - 5x^8 - 4x^7 + 24x^6 + 62x^5 + 14x^4 - 4x^3 - 32x^2 + 9x - 1)$

Similar results can be obtained for $N = 33$ and 46.

4. Examples All the calculations in the following were done by a program with GNU C and PARI-library, ver. 1.39.

Example. 4.1. Let $N = 22$ and $r = 11/5$. Then $K_r = \mathbf{Q}(\sqrt{6}, \sqrt{29})$ has class number one. The elliptic curve E_r has j-invariant

$$\frac{1}{5^{22}}(998269691281725129260266540119630470 4 - 40754189488135321090109133597561154 56\sqrt{6} + 18537402791159630521518878692955412 48\sqrt{29} - 75678629992478957693784269242729267 2\sqrt{174}).$$

And the quadratic twist E of E_r by

$$\beta = 1585084727553 - \frac{1248019557557}{2}\sqrt{6} - 989865700341\sqrt{29} + \frac{826800325581}{2}\sqrt{174}$$

has the following global minimal model:

$$
\begin{aligned}
E : y^2 = x^3 &+ \left(9 + \frac{1}{2}\sqrt{6} + \frac{1}{2}\sqrt{174}\right)x^2 \\
&+ (-383506419653 - 156534506597\sqrt{6} \\
&+ 71201118525\sqrt{29} + 29073539873\sqrt{174})x \\
&- 182798829223792711 \\
&\quad - 74627160360067580\sqrt{6} \\
&\quad + 33944822557919841\sqrt{29} \\
&\quad + 13857943481193026\sqrt{174}.
\end{aligned}
$$

Then E has discriminant

$$
\begin{aligned}
\Delta(E) = &\ 770987498697389702212257965120 \\
&+ 314754328312196256240261626880\sqrt{6} \\
&- 143168784300891113577113736960\sqrt{29} \\
&- 58448411438624093585994387840\sqrt{174},
\end{aligned}
$$

$$(\Delta(E) = \mathfrak{p}_2^{12}\cdot\mathfrak{p}_5^{2}\cdot(\mathfrak{p}_5^{\sigma})^{11}\cdot(\mathfrak{p}_5^{\tau})\cdot(\mathfrak{p}_5^{\sigma\tau})^{22},$$

and conductor

$$\mathrm{cond}(E) = \mathfrak{p}_2^4\cdot\mathfrak{p}_5\cdot(\mathfrak{p}_5^{\sigma})\cdot(\mathfrak{p}_5^{\tau})\cdot(\mathfrak{p}_5^{\sigma\tau}) = 2^2\cdot 5,$$

where $\mathfrak{p}_2 = (-2+\sqrt{6})$, $\mathfrak{p}_5 = \left(\frac{1}{2} + \sqrt{6} + \frac{1}{2}\sqrt{29}\right)$ and $\mathrm{Gal}(K_r/\mathbf{Q}) = \langle \sigma, \tau \mid \sigma^2 = \tau^2 = 1\rangle$. E is a modular $\mathbf{Q}$-curve from Remark 3.5.

Acknowledgements. The authors express sincere thanks to Prof. Fumiyuki Momose for his kind and warm encouragement during the preparation of this paper. They thank Yuji Hasegawa for the access to his preprint.

References

[1] N. Elkies: Remarks on elliptic K-curves (1993) (preprint).

[2] B. Gross: Arithmetic on Elliptic Curves with Complex Multiplication. LNM 776, Springer-Verlag. New York-Berlin-Heidelberg (1980).

[3] Y. Hasegawa: $\mathbf{Q}$-curves over quadratic fields. Manuscripta Math., **94**, 347–364 (1997).

[4] Y. Hasegawa, K. Hashimoto, and F. Momose: Modular Conjecture for $\mathbf{Q}$-curves and **QM**- curves (1996)(preprint).

[5] T. Hibino and N. Murabayashi: Modular equations of hyperelliptic $X_0(N)$ and an application. Acta Arith., **82**, no. 3, 279–291 (1997).

[6] T. Hibino and A. Umegaki: A family of elliptic $\mathbf{Q}$-curves defined over biquadratic fields and their modularity (1997) (submitted).

[7] M. Shimura: Defining equations of modular curves $X_0(N)$. Tokyo J. Math., **18**, no. 2, 443–456 (1995).

[8] A. Umegaki: A construction of everywhere good $\mathbf{Q}$-curves with p-isogeny (1996)(submitted).