Journal of Number Theory **72**, 13–31 (1998)
Article No. NT982259

Rational and Elliptic Parametrizations of Q-Curves

Josep González and Joan-C. Lario*

Facultat de Matemàtiques i Estadística, Universitat Politecnica de Catalunya, Pan Gargallo 5, E-08028 Barcelona, Spain

Communicated by A. C. Woods

Received January 21, 1997; revised June 30, 1997

We describe explicit parametrizations of the rational points of $X^*(N)$, the algebraic curve obtained as quotient of the modular curve $X_0(N)$ by the group $B(N)$ generated by the Atkin–Lehner involutions, whenever N is square-free and the curve is rational or elliptic. By taking into account the moduli interpretation of $X^*(N)$, along with a standard "boundedness" conjecture, we obtain all the $\bar{\mathbf{Q}}$-isogeny classes of $\mathbf{Q}$-curves except for a finite set.

1. INTRODUCTION

Let C be an elliptic curve defined over $\bar{\mathbf{Q}}$. The curve C is said to be a **Q**-curve if it is isogenous to all its Galois conjugates C^σ, with $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. The interest in **Q**-curves has recently been increasing with the aim of generalizing the Shimura–Taniyama–Weil conjecture for elliptic curves defined over number fields. See footnote 24 in [10] and also [13].

As Elkies first noticed, every **Q**-curve without complex multiplication is isogenous over $\bar{\mathbf{Q}}$ to a **Q**-curve attached to a rational point of the algebraic curve $X^*(N) = X_0(N)/B(N)$, where $B(N)$ is the automorphism group generated by the Atkin–Lehner involutions and N is square-free [5]. Every non-cusp rational point in $X^*(N)$ lifts to $X_0(N)$ giving **Q**-curves defined over abelian extensions of **Q** of type (2, ..., 2).

The only primes p for which the modular curve $X_0(p)$ has genus zero are $p = 2, 3, 5, 7$, and 13. For these values of p, the function

$$F(z) = \left(\frac{\eta(z)}{\eta(pz)}\right)^{24/(p-1,\,12)}$$

* Research of the authors was partially supported by DGICYT Grant PB96-0970-C02-02.

0022-314X/98 $25.00

is a Hauptmodul on $X_0(p)$ with $\operatorname{div}(F) = (0) - (i\infty)$, and the functions $j(z)$, $j(pz)$ are in $\mathbf{Z}(F)$. Given a quadratic field K, to certain values of $F(z)$ in K correspond values $j(z)$, $j(pz)$ which are conjugate and provide **Q**-curves defined over K, the isogeny being of degree p. Instead, we parametrize the elementary symmetric functions $J_1(z) = j(z) + j(pz)$ and $J_2(z) = j(z)\, j(pz)$ by means of a rational Hauptmodul on $X^*(p)$.

Our aim is to generalize the above procedure to parametrize the **Q**-curves arising from the rational points of $X^*(N)$ whenever this curve has genus zero or one. We first determine the complete list of such values of N. In the rational cases, we show how to construct a Hauptmodul on $X^*(N)$ and, once the Hauptmodul is normalized and has integral q-expansion, we obtain families of **Q**-curves over quadratic, biquadratic and triquadratic extensions. In the elliptic cases, we find explicit modular parametrizations of a reduced Néron model of $X^*(N)$ and give a method to retrieve the **Q**-curves parametrized by its Mordell-Weil group. In this situation we obtain families of **Q**-curves defined over quadratic, biquadratic, triquadratic and tetraquadratic extensions.

It is worth noting that there is a natural boundedness conjecture for this moduli problem. Namely, if N is large enough, then $X^*(N)$ should not contain rational points other than cusps or CM points [5]. Taking all this into account, along with the celebrated theorem of Faltings concerning the finiteness of rational points on algebraic curves, it can be concluded that the parametric families of **Q**-curves described in the present paper should exhaust all the $\bar{\mathbf{Q}}$-isogeny classes of **Q**-curves except for a finite (though non-empty, see [5]) set.

2. PARAMETRIC FAMILIES OF Q-CURVES

Let $N > 1$ be an integer. The number of cusps of $X_0(N)$ is $\sum_{d \mid N} \varphi((d, N/d))$, where φ denotes the Euler function. A system of representatives of the cusps is given by the fractions a/d, where d is a positive divisor of N and $a \in (\mathbf{Z}/f_d\mathbf{Z})^*$, with $f_d = (d, N/d)$, $(a, d) = 1$. In this way, $0 \equiv 1$, $i\infty \equiv 1/N$.

Given a divisor $1 < N_1 \mid N$ such that $(N_1, N/N_1) = 1$, the Atkin–Lehner involution w_{N_1} acts as a permutation on the set of cusps. Moreover, a cusp with denominator d is sent to a cusp with denominator $N_1\, d/(N_1, d)^2$. With no risk of confusion, we still denote by w_{N_1} the permutation on the set of positive divisors of N induced by the corresponding involution: $w_{N_1}(d) = N_1\, d/(N_1, d)^2$.

Now, assume that N is square-free and let $N = p_1 \cdots p_n$ its prime decomposition. Let $B(N)$ denote the group generated by the Atkin–Lehner involutions of $X_0(N)$. As it is shown in [8], the automorphism group of

$X_0(N)$ is $B(N)$ whenever the genus of $X_0(N)$ is at least 2, except for the case $N=37$. We have

$$B(N)=\langle w_{p_1}\rangle \oplus \cdots \oplus \langle w_{p_n}\rangle = \{w_{N_1}\colon N_1 \mid N\},$$

where $w_1=\mathrm{id}$. Since N is square-free, $X_0(N)$ has 2^n cusps and the set $\{1/d\colon d \mid N\}$ is a system of representatives of them. For $0<d$, $N_1 \mid N$, we have $w_{N_1}(1/d)=1/w_{N_1}(d)$. One can easily check that $B(N)$ acts transitively on the set of cusps.

Let $X^*(N)=X_0(N)/B(N)$ and let $\pi\colon X_0(N)\to X^*(N)$ denote the natural projection. The functions (differentials) on $X^*(N)$ are the functions (differentials) on $X_0(N)$ invariant under the action of $B(N)$. For each positive divisor $d \mid N$, we consider the functions $j_d(z)=j(dz)$. A straightforward computation shows that $j_d \mid w=j_{w(d)}$ for all $w\in B(N)$, so that the elementary symmetric functions

$$J_1=\sum_d j_d, \qquad J_2=\sum_{d_1<d_2} j_{d_1} j_{d_2}, \ldots, \qquad J_{2^n}=\prod_d j_d$$

are functions on $X^*(N)$ with an unique pole at $\pi(i\infty)$. More precisely, the function J_i has a pole at $\pi(i\infty)$ of order $\sum_{j=1}^{i} N/d_j$, where $1=d_1<\cdots<d_{2^n}=N$ are the positive divisors of N.

A non-cusp rational point in $X^*(N)$ lifts to a Galois stable set of points in $X_0(N)$ which is an orbit under the action of $B(N)$. The j-invariants of the corresponding elliptic curves are j_d where d runs the positive divisors of N, and the polynomial $J^*(x)=\prod_{d\mid N}(x-j_d)$ has coefficients in $\mathbf{Q}$. Note that if $J^*(x)$ is $\mathbf{Q}$-irreducible, then there is an isomorphism $B(N)\simeq \mathrm{Gal}(K/\mathbf{Q})$ where $K=\mathbf{Q}(j_1)$. Observe also that if $J^*(x)$ has repeated roots, then the $\mathbf{Q}$-curves attached to these roots are CM elliptic curves.

The Rational Case

Whenever $X^*(N)$ has genus zero, given a non-cusp point P of $X_0(N)$, there is a unique function F on $X_0(N)$ invariant under $B(N)$ such that

$$\mathrm{div}(F)=\sum_{w\in B(N)} (w(P))-(w(i\infty))$$

with a normalized Fourier q-expansion: $F(q)=1/q+\cdots$. The function F is then a Hauptmodul on $X^*(N)$ with a simple pole at $\pi(i\infty)$, and changing the base point P modifies F in an additive constant. In Section 4, we present a method to construct this Hauptmodul on $X^*(N)$.

In this case, the functions J_i can be expressed as polynomials in F of degree $\sum_{j=1}^{i} N/d_j$. In fact, we will show that $J^*(x)$ has coefficients in $\mathbf{Z}[F]$, due to the fact that we can always find a normalized Hauptmodul F with integral q-expansion.

The Elliptic Case

Whenever the curve $X^*(N)$ has genus one, it can be viewed as an elliptic curve over $\mathbf{Q}$ by considering the rational point $\pi(i\infty) \in X^*(N)(\mathbf{Q})$ as the origin. In section 6, we determine the $\mathbf{Q}$-isomorphism class of $X^*(N)$ and make the modular parametrization $\pi\colon X_0(N) \to X^*(N)$ explicit. In other words, we find modular functions U and V on $X_0(N)$ satisfying a minimal Weierstrass equation of $X^*(N)$. Then, the Riemann–Roch theorem allows us to express the symmetric functions J_i as polynomials of the functions U and V. Indeed, for $m \geqslant 2$ the $\mathbf{C}$-vector space of modular functions of $X^*(N)$ with a unique pole at $\pi(i\infty)$ of order $\leqslant m$ has dimension m, and a basis is given by $\{U^i, U^jV\}$ with $0 \leqslant i \leqslant [m/2]$, $0 \leqslant j \leqslant [(m-3)/2]$. It turns out that $J_i(U, V) \in \mathbf{Z}[U, V]$ and, since the Mordell–Weil group of $X^*(N)$ has rank one in all the cases, we do parametrize $\mathbf{Q}$-curves for such values of N.

We conclude with the process of extracting the $\mathbf{Q}$-curves parametrized by $X^*(N)(\mathbf{Q})$ under our genus assumptions.

3. THE GENUS OF $X^*(N)$

As before, let $N = p_1 \cdots p_n$ be square-free. In this section we give a formula for the genus g^* of $X^*(N)$, and determine all the cases for which g^* is either zero or one.

Let g be the genus of $X_0(N)$. The Hurwitz formula applied to the morphism $\pi\colon X_0(N) \to X^*(N)$ yields $2g-2 = \deg(\pi)(2g^*-2) + \sum (e(P)-1)$, where $e(P)$ denotes the ramification index of π at the point $P \in X_0(N)$. A point P of $X_0(N)$ is ramified if and only if it is fixed by some non-trivial Atkin–Lehner involution $w_d \in B(N)$. In this case, P is not a cusp and corresponds to an elliptic curve with complex multiplication by $\mathbf{Q}(\sqrt{-d})$. Since N is square-free, it turns out that w_d is the only Atkin–Lehner involution that fixes P. Thus, for all cases $e(P) \leqslant 2$.

For a positive divisor d of N, let $v_d(N)$ be the number of fixed points in $X_0(N)$ by w_d. We refer to [7] and [1, Table 7] for an explicit formula to compute this number. It can be concluded that

$$2g-2 = 2^n(2g^*-2) + \sum_{1<d\mid N} v_d(N).$$

Remark 3.1. Let B be any subgroup of $B(N)$. The genus g_B of $X_0(N)/B$ can be computed from the equation

$$2g-2=|B|\,(2g_B-2)+\sum_{w_d\in B\setminus\{\mathrm{id}\}} \nu_d(N),$$

where $|B|$ denotes the order of the subgroup B.

Remark 3.2. If $P\in X_0(N)$ is a ramified point of $\pi\colon X_0(N)\to X^*(N)$, then the polynomial $J^*(x)$ attached to $\pi(P)$ has repeated roots although the converse is not true in general. E.g., in the case $N=2$ we find that $J^*(x)$ has repeated roots for the following three values of j: 1728, 8000, and -3375. The elliptic curves corresponding to j-invariants 1728, 8000 provide the two ramification points of π. The point $(j_1, j_2)=(-3375, -3375)$ is a singularity of the affine curve defined by the modular equation $\Phi_2(x, y)=0$.

As we are interested in the cases $g^*=0$ and 1, the following two lemmas added to the formula above allow us to determine the finite list of values N for which $X^*(N)$ is rational or elliptic.

LEMMA 3.3. *Let N be an integer, and p be a prime with $(N, p)=1$. The genus of $X^*(Np)$ is at least as large as the genus of $X^*(N)$.*

Proof. Let us assume that the genus g^* of $X^*(N)$ is >0, if not there is nothing to prove. Let $\{f_i\}_{1\leqslant i\leqslant g^*}$ be a basis of $S_2(\Gamma_0(N))^{B(N)}$. The cusp forms $f_i\,|\,B_p=f_i(pz)$ are in $S_2(\Gamma_0(Np))$. Since $f_i\,|\,w_p=p(f_i\,|\,B_p)$ and $(f_i\,|\,B_p)|w_d=(f_i\,|\,w_d)|B_p$ for all $(d, p)=1$ and $1\leqslant i\leqslant g^*$, it follows that $h_i=f_i+p(f_i\,|\,Bp)$ are non-zero cusp forms fixed by $B(Np)$. As $S_2(\Gamma_0(N))\cap B_p(S_2(\Gamma_0(N)))=\{0\}$, we conclude that $\{h_i\}_{1\leqslant i\leqslant g^*}$ are linearly independent and, hence, the assertion holds. ∎

LEMMA 3.4. *Let us assume that N is an odd integer and let n be the number of prime divisors of N. Let $\psi(N)=N\prod_{p\,|\,N}(1+1/p)$.*

(i) *If $X^*(N)$ has genus zero, then $\psi(N)/2^n\leqslant 48$.*

(ii) *If $X^*(N)$ has genus one, then $\psi(N)/2^n\leqslant 96$.*

Proof. We outline the proof of (i). Since N is odd, the curve $X_0(N)$ has good reduction at 2. The argument in [12] shows that $X_0(N)(\mathbf{F}_4)$ has at least $2^n+\psi(N)/12$ points. Now, let B' be a subgroup of $B(N)$ of index 2 and consider the quotient $X'=X_0(N)/B'$. The curve X' also has good reduction at 2 and it is a hyperelliptic curve; therefore, $X'(\mathbf{F}_4)$ has at most $10=2(4+1)$ points. Since the reduction of the map $\pi'\colon X_0(N)\to X'$ is étale over $\mathbf{F}_4$ and has degree 2^{n-1}, we get $2^n+\psi(N)/12\leqslant 10.2^{n-1}$. The argument for (ii) is similar, but one simply uses instead the fact that $X^*(N)(\mathbf{F}_4)$ has at most 9 points and the morphism $X_0(N) \to X^*(N)$ has degree 2^n. ∎

Combining the two lemmas above we obtain the following results:

PROPOSITION 3.1. *There are exactly* 43 *square-free values of* $N > 1$ *such that* $X^*(N)$ *has genus zero. Namely,*

N	
p	2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, 71
$p.q$	6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 62, 69, 87, 94, 95, 119
$p.q.r$	30, 42, 66, 70, 78, 105, 110.

PROPOSITION 3.2. *There are exactly* 38 *square-free values of* N *such that* $X^*(N)$ *has genus one. Namely,*

N	
p	37, 43, 53, 61, 79, 83, 89, 101, 131
$p.q$	57, 58, 65, 74, 77, 82, 86, 91, 111, 114, 118, 123, 142, 143, 145, 155, 159
$p.q.r$	102, 114, 130, 138, 174, 182, 190, 195, 222, 231, 238
$p.q.r.s$	210.

Proof. The procedure for determining all the values follows by induction on the number of prime factors of N. We limit ourselves to Proposition 3.1, and the proof of Proposition 3.2 is similar. Start with the case $N = p$ prime. If the genus of $X^*(p)$ is zero, then $X_0(p)$ must be a hyperelliptic curve and Ogg has determined the 15 possible values [12]. If $N = p.q$ and $X^*(N)$ has genus zero, then the first step, along with Lemmas 1 and 2, forces N to be in an explicit finite set. After computing g^* for these candidates, we collect a further 21 new values. Next, we deal similarly with the case $N = p.q.r$ and get 7 more values. The process ends since the finite set of candidates with four prime factors having $g^* = 0$ is the empty set. ∎

Remark 3.5. The primes involved in the first row of Proposition 3.1 are exactly those dividing the order of the Monster group [2, 5, 16].

4. THE RATIONAL CASE

Let $G(z) = \prod_{d \mid N} \eta(dz)^{r_d}$ where $\eta(z)$ is the Dedekind function and $r_d \in \mathbf{Z}$. As is well-known [9, 11], $G(z)$ is a function on $X_0(N)$ if and only if the following three statements hold:

(i) $\sum_{d \mid N} r_d = 0$,

(ii) $\prod_{d \mid N} d^{r_d}$ is a square in $\mathbf{Q}^*$,

(iii) $A_N \cdot r \equiv 0 \pmod{24}$.

Here $A_N = (a_d^{d'})_{d, d' \mid N}$ is the matrix defined by $a_d^{d'} = N(d, d')^2/(dd'(d', N/d'))$, and r is the array $(r_d)_{d \mid N}$.

A function $G(z)$ satisfying these conditions has its zeros and poles at the cusps of $X_0(N)$, and the order at a cusp with denominator d is the dth component of $A_N \cdot r/24$. Let $\mathscr{G}_N$ denote the multiplicative group of functions on $X_0(N)$ generated by this procedure. We call $\mathscr{G}_N$ the Newman group of level N. As shown in [6], the group $\mathbf{Q} \otimes \mathscr{G}_N$ is stable under the Atkin–Lehner action, and every function $G(z)$ on $X_0(N)$ with neither zeros nor poles in the upper half plane and with the same order at all the cusps represented by the same denominator satisfies $G(z)^n \in \mathbf{C} \otimes \mathscr{G}_N$ for some positive integer n.

We shall need an auxiliary function on $X_0(N)$ lying in the Newman group that will help us to construct the Hauptmodul F on $X^*(N)$ whenever it exists. The next proposition generalizes Theorem 4 in [12].

PROPOSITION 4.1. *Let $N = p_1 \cdots p_n$ be square-free and B' be a subgroup of $B(N)$ of index 2. Let*

$$G_{B'}(z) = \left(\frac{\prod_{w \in B(N) \backslash B'} \eta(w(N)\, z)}{\prod_{w \in B'} \eta(w(N)\, z)} \right)^{r_{B'}}.$$

Here $r_{B'} = 24/(N-1, 12)$ if N is prime, or $24/(\prod_{i=1}^n (p_i + \delta_i), 24)$ otherwise, with $\delta_i = 1$ if $w_{p_i} \in B'$ and $\delta_i = -1$ if $w_{p_i} \notin B'$. Then,

(i) *$G_{B'}$ is a function on $X_0(N)$ with*

$$\operatorname{div} G_{B'} = m_{B'} \left(\sum_{w \in B(N) \backslash B'} (1/w(N)) - \sum_{w \in B'} (1/w(N)) \right),$$

where $m_{B'} = r_{B'}/24 \prod_{i=1}^n (p_i + \delta_i)$.

(ii) *For all integers $m > 1$, $G_{B'}^{1/m}$ is not a function on $X_0(N)$.*

Proof. Since B' has index 2 in $B(N)$, there is a prime $p \mid N$ such that $w_p \notin B'$; without loss of generality we can assume $p = p_n$ and, therefore, $B(N) = B' \oplus \langle w_{p_n} \rangle$. In particular, $B(N) \backslash B' = w_{p_n} B'$.

Let us consider the array $\bar{r} = (\bar{r}_d)_{d \mid N}$ with $\bar{r}_d = -1$ if $d = w(N)$ for some $w \in B'$ and $\bar{r}_d = 1$ otherwise. Let $\bar{n} = A_N \cdot \bar{r}$. On the one hand, the Newman matrix satisfies $a_d^{d'} = a_{w(d)}^{w(d')}$ for all $w \in B(N)$ and $\bar{r}_d = \bar{r}_{w(d)}$ for all $w \in B'$, hence $\bar{n}_d = \bar{n}_{w(d)}$ for all $w \in B'$. On the other hand, since $\sum_d \bar{r}_d = 0$ and for every divisor d one has $\sum_{d' \mid N} a_d^{d'} = \psi(N)$, we obtain $\sum_d \bar{n}_d = 0$. Therefore,

$$\bar{n}_d = \begin{cases} \bar{n}_N & \text{if} \quad d = w(N) \qquad \text{for some} \quad w \in B', \\ -\bar{n}_N & \text{otherwise.} \end{cases}$$

We also have $\bar{n}_N = \sum_{w \in B(N) \setminus B'} w(N) - \sum_{w \in B'} w(N) = \sum_{w \in B'} w(N/p_n) - w(N)$. Let us show that $\bar{n}_N = -\prod_{i=1}^{n} (p_i + \delta_i)$ by induction on the number n of prime divisors of N. The case $n = 1$ being obvious, we assume $n > 1$. Let $\mathscr{D}' = \{d : d \mid N, w_d \in B'\}$. If $B' = \langle w_{p_1}, ..., w_{p_{n-1}} \rangle$, then $\mathscr{D}' = \{d : d \mid N/p_n\}$ and

$$\bar{n}_N = \sum_{d \in \mathscr{D}'} N/dp_n - \sum_{d \in \mathscr{D}'} N/d = \sum_{d \in \mathscr{D}'} d - \sum_{d \in \mathscr{D}'} dp_n = (1 - p_n) \prod_{i=1}^{n-1} (p_i + 1).$$

If $B' \neq \langle w_{p_1}, ..., w_{p_{n-1}} \rangle$, then we consider $B'' = \{w_d \in B' : (d, p_n) = 1\}$ which is a subgroup of index 2 in B' and also in $B(N/p_n)$. In this case, we have

$$\begin{aligned} \bar{n}_N &= \sum_{w \in B''} w(N/p_n) + \sum_{w \in B' \setminus B''} w(N/p_n) - \sum_{w \in B''} w(N) - \sum_{w \in B' \setminus B''} w(N) \\ &= (1 - p_n) \sum_{w \in B''} w(N/p_n) + (p_n - 1) \sum_{w \in B(N/p_n) \setminus B''} w(N/p_n). \end{aligned}$$

With the induction hypothesis on N/p_n, we conclude that

$$\bar{n}_N = (1 - p_n) \prod_{i=1}^{n-1} (p_i + \delta_i).$$

Finally, observe that the product $\prod_{w \in B'} w(N/p_n)^{-1} w(N)$ is equal to $p_n^{2^{n-1}}$ if $B' = \langle w_{p_1}, ..., w_{p_{n-1}} \rangle$ or, otherwise, to 1. Thus, $\prod_{w \in B'} w(N/p_n) \, w(N)^{-1}$ is a square in $\mathbf{Q}$ if and only if N is not a prime. Now, the first claim follows from considering the properties of the functions in the Newman group $\mathscr{G}_N$. The second claim follows as in [12, Lemma on p. 458]. ∎

We also need the following result:

PROPOSITION 4.2. *Let N and B' be as in the previous proposition. The logarithmic differential of $G_{B'}$, $\omega = (dG_{B'}/dz)/G_{B'}$, is invariant under B' and satisfies $\omega \mid w = -\omega$ for all $w \in B(N) \setminus B'$.*

Proof. Since $\operatorname{div} G_{B'}$ is invariant under B', we see that $G_{B'}$ is an eigenvector of every $w \in B'$; so $G_{B'} \mid w = \pm G_{B'}$. Therefore, $G_{B'}^2$ is a function on $X_0(N)/B'$ and its logarithmic differential is a differential on $X_0(N)/B'$. Let

$w \in B(N) \backslash B'$. Since div $G_{B'} \mid w = -$div $G_{B'}$, there is a constant $a \in \mathbf{Q}^*$ such that $G_{B'} \mid w = a/G_{B'}$. Finally,

$$\left(\frac{G'_{B'}(z)}{G_{B'}(z)}\right) \mid w = \frac{G'_{B'}(w(z))}{G_{B'}(w(z))}\, w'(z) = -a\, \frac{G'_{B'}(z)/G_{B'}(z)^2}{a/G_{B'}(z)} = -\frac{G'_{B'}(z)}{G_{B'}(z)}. \quad \blacksquare$$

From now on, we assume that $X^*(N)$ has genus zero. Fix a subgroup B' of $B(N)$ of index 2. Let $X' = X_0(N)/B'$ and $G(z) = G_{B'}(z)$. Let us consider the projection $\pi'\colon X_0(N) \to X'$ and let g' denote the genus of X'. The vector space of regular differentials on $X_0(N)$ invariant under B' has dimension g'. If $g' > 0$, then for each $w \in B(N) \backslash B'$ these differentials are eigenvectors of w with eigenvalue -1 since $X'/\langle w \rangle$ has genus zero. Next, we describe how to find a Hauptmodul on $X^*(N)$ with a simple pole at $\pi(i\infty)$ according to the values of g'.

(1) Case $g' = 0$. If N is prime, then $N = 2$, 3, 5, 7 or 13. Otherwise, due to Proposition 4.1 (i), we have that $\prod_{i=1}^{n} (p_i + \delta_i) \mid 24$; so, the only values are $N \in \{2 \cdot 3,\ 2 \cdot 5,\ 2 \cdot 7,\ 2 \cdot 11,\ 2 \cdot 13,\ 2 \cdot 23,\ 3 \cdot 5,\ 3 \cdot 7,\ 3 \cdot 11,\ 3 \cdot 13,\ 5 \cdot 7,\ 5 \cdot 7,\ 2 \cdot 3 \cdot 5,\ 2 \cdot 3 \cdot 7,\ 2 \cdot 3 \cdot 11,\ 2 \cdot 3 \cdot 13\}$. In these cases, the function $F = G + G \mid w$ (any $w \notin B'$) is invariant under $B(N)$ and has a simple pole at $\pi(i\infty)$. It turns out that F has integral q-expansion, since $G \mid w = a/G$ where $a \in \mathbf{Z}$. More precisely, we find $a = p_n^{r_{B'} 2^{n-1}}$ if B' is of the form $\langle w_{p_1}, ..., w_{p_{n-1}} \rangle$, or $a = \pm 1$ otherwise.

(2) Case $g' = 1$. Let ω be a non-zero regular differential on $X_0(N)$ invariant under B'. Let us consider the function $F = (q\,dG/dq)/(G\omega)$. Proposition 4.2 tells us that F is invariant under $B(N)$, and it is easily seen that it has a simple pole at each cusp of $X_0(N)$. Since ω can be chosen to be normalized and with integral q-expansion, it is easy to see that $F(q) = -m_{B'}/q + a_0 + m_{B'} \sum a_n q^n$ with $a_i \in \mathbf{Z}$. Thus, the normalized Hauptmodul $-(F(q) - a_0)/m_{B'}$ has integral q-expansion.

(3) Case $g' > 1$. Let $\omega_1, ..., \omega_{g'}$ be a basis of the regular differentials on $X_0(N)$ invariant under B'. Take $w \in B(N) \backslash B'$. Since w is the hyperelliptic involution of X' and $\pi'(i\infty)$ is not fixed by w, it follows that $\pi'(i\infty)$ is not a Weierstrass point of X'. Therefore, the differentials ω_i can be chosen so that $\omega_i \equiv q^i \pmod{q^{g'+1}}$ The function $F = \omega_{g'-1}/\omega_{g'}$ is then a Hauptmodul on $X^*(N)$ with a simple pole at $\pi(i\infty)$. In every case one checks that $\omega_{g'}$ and $\omega_{g'-1}$ can be chosen with integral q-expansion, so that F is normalized and has integral q-expansion as well.

In the Appendix below we provide the genus g' attached to each possible subgroup B' for the 43 values of N such that $X^*(N)$ has genus zero.

Remark 4.1. The polyquadratic extensions of $X^*(N)$ containing the conjugates of j implicitly give the equations for $X_0(N)$ as a polyquadratic cover of $X^*(N)$. For other (non-implicit) equations of $X_0(N)$ we refer to [14].

5. RATIONAL EXAMPLES

Here we present some examples of parametric families of $\mathbf{Q}$-curves obtained accordingly to the previous results. They come from the curves $X^*(6)$, $X^*(11)$, $X^*(23)$, and $X^*(30)$.

• Case $X^*(6)$. By taking $B' = \langle w_2 \rangle$, we obtain $G(z) = (\eta(z)\,\eta(2z)/\eta(3z)\,\eta(6z))^4$. Let $t = G(z) + 81/G(z)$. The symmetric functions J_i are:

$$J_1 = 1730592 + 472644t - 19412t^2 - 8415t^3 - 234t^4 + 24t^5 + t^6,$$

$$J_2 = 986038273296 + 250882570080t + 24676194456t^2 + 1173557080t^3 + 27120609t^4 + 108792t^5 - 15624t^6 - 102t^7 + 37t^8 + t^9,$$

$$J_3 = (18+t)^3\,(-132914433600 - 41568310944t - 547226496t^2 + 326343744t^3 + 17402940t^4 + 173310t^5 + 1054t^6 - 9t^7 + t^8),$$

$$J_4 = (18+t)^3\,(32328 + 2700t + 246t^2 + t^3)^3.$$

The polynomial $P(x) = (x - j_1)(x - j_2)(x - j_3)(x - j_6)$ defines a biquadratic extension of $\mathbf{Q}(t)$. By computing the roots $(j_1 + j_2)(j_3 + j_6)$, $(j_1 + j_3)(j_2 + j_6)$, and $(j_1 + j_6)(j_2 + j_3)$ of a cubic resolvent of $P(x)$, it is shown that the splitting field of $P(x)$ is the compositum of the quadratic fields:

$$\mathbf{Q}(\sqrt{(t+18)(t-18)}), \qquad \text{and} \qquad \mathbf{Q}(\sqrt{(t+14)(t+18)}).$$

For instance, by taking $t = 0$ we obtain a $\mathbf{Q}$-curve with j-invariant:

$$j = 432648 - 243810i + 163674\sqrt{7} - 92232i\sqrt{7}.$$

The field $K = \mathbf{Q}(j)$ satisfies $\mathrm{Gal}(K/\mathbf{Q}) \simeq B(6)$, by identifying $w_6\colon i \mapsto -i$, and $w_2\colon \sqrt{7} \mapsto -\sqrt{7}$.

• Case $X^*(11)$. Let $B' = \{\mathrm{id}\}$, $G(z) = (\eta(z)/\eta(11z))^{12}$, and $\omega = \eta(z)^2\,\eta(11z)^2$. In this case, we take $F(z) = (q\,dG/dq)/(G\omega)$. Let us consider $t = -(F(z) + 22)/5$ so that t is a normalized Hauptmodul with integral q-expansion. We obtain

$$J_1 = 8720000 + 19849600t + 8252640t^2 - 1867712t^3 - 1675784t^4$$
$$- 184184t^5 + 57442t^6 + 11440t^7 - 506t^8 - 187t^9 + t^{11},$$
$$J_2 = (38800 + 21920t + 4056t^2 + 248t^3 + t^4)^3.$$

The polynomial $P(x) = (x - j_1)(x - j_{11}) = x^2 - J_1 x + J_2$ has discriminant $J_1^2 - 4J_2 = (6 + t)(t^3 - 2t^2 - 76t - 212) \bmod \mathbf{Z}[t]^2$.

- Case $X^*(23)$. The only subgroup of $B(23)$ with index 2 is $B' = \{\mathrm{id}\}$. The curve $X^*(23)$ has genus 0, and $X' = X_0(23)$ has genus $g' = 2$. Performing our algorithm, we get a Hauptmodul $t = 1/q + 4q + 7q^2 + 13q^3 + 19q^4 + \cdots$ on $X^*(23)$ and also the symmetric functions J_i:

$$J_1 = 33162750 + 160117560t + 181569843t^2 - 352943487t^3$$
$$- 1221122187t^4 - 1353267468t^5 - 414060444t^6 + 539366445t^7$$
$$+ 630176770t^8 + 197662552t^9 - 82673546t^{10} - 83684166t^{11}$$
$$- 15573852t^{12} + 8030680t^{13} + 4070172t^{14} + 64354t^{15} - 329912t^{16}$$
$$- 52992t^{17} + 11799t^{18} + 3381t^{19} - 161t^{20} - 92t^{21} + t^{23},$$
$$J_2 = (65025 + 209304t + 289980t^2 + 222984t^3 + 102214t^4$$
$$+ 27752t^5 + 4092t^6 + 248t^7 + t^8)^3,$$

$$J_1^2 - 4J_2 = t^2(t-3)^2\,(t-1)^2\,(t+1)^2\,(t+2)^2\,(t+3)^2\,(-9-4t+t^2)^2$$
$$\times(-17-2t+t^2)^2\,(-25-17t-2t^2+t^3)(-19-13t-t^2+t^3)^2$$
$$\times(-9-9t-t^2+t^3)^2\,(7+11t+6t^2+t^3)(-17-16t+4t^3+t^4)^2.$$

- Case $X^*(30)$. Let $B' = \langle w_3, w_5\rangle$ and

$$G(z) = \frac{\eta(z)\,\eta(3z)\,\eta(5z)\,\eta(15z)}{\eta(2z)\,\eta(6z)\,\eta(10z)\,\eta(30z)}.$$

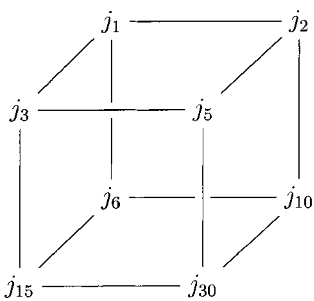
A normalized Hauptmodul is $t = G(z) + 4/G(z) + 1$, and the symmetric functions J_i are huge polynomials in the variable t. We simply write down the generic triquadratic extension obtained which is the compositum of the quadratic fields

$$\mathbf{Q}(\sqrt{t(t+4)}), \qquad \mathbf{Q}(\sqrt{(t-1)(t+3)}) \qquad \text{and} \qquad \mathbf{Q}(\sqrt{(t-5)(t+3)}).$$

In the particular case $t = 2$, the quadratic fields are: $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{3})$ and $\mathbf{Q}(\sqrt{5})$. We obtain a triquadratic $\mathbf{Q}$-curve which j-invariant is a root of an explicit irreducible polynomial of degree 8. After performing some resolvent computations we get a root

$$\begin{aligned} j_1 = \left(\frac{3}{4} + \frac{3i}{4}\right) & (-1520448042 - 9908421603i \\ & + (-877849349 - 5720577044i)\sqrt{3} \\ & + (679965303 + 4431181206i)\sqrt{5} \\ & + (392585740 + 2558319455i)\sqrt{15}). \end{aligned}$$

The following figure describes the graph which vertices are the eight conjugate j-invariants and the edges are the corresponding isogenies. The degree of each isogeny $(j_d, j_{d'})$ is $dd'/(d, d')^2$. We note that the involutions w_2, w_6, and w_{30} act as the Galois automorphims $\sqrt{3} \mapsto -\sqrt{3}$, $\sqrt{5} \mapsto -\sqrt{5}$, and $i \mapsto -i$, respectively.



6. THE ELLIPTIC CASE

In this section we assume that $X^*(N)$ has genus one. As alluded before, $E = (X^*(N), \pi(i\infty))$ is an elliptic curve over $\mathbf{Q}$. Our purpose is to determine E up to $\mathbf{Q}$-isomorphism and to describe explicitly the morphism $\pi: X_0(N) \to X^*(N)$. In other words, we are looking for a modular parametrization of E.

The first step is to detect the $\mathbf{Q}$-isogeny class of E. Let $f \in S_2(\Gamma_0(N))$ be the only normalized cusp form invariant under $B(N)$. There is a unique newform $h \in S_2(\Gamma_0(N'))$ with $N' \mid N$ which is invariant under $B(N')$. This h satisfies $f = \sum_{d \mid N/N'} dh \mid B_d$. The conductor of E is N', and h determines E up to $\mathbf{Q}$-isogeny. In fact, we find $h = f$ except for the values

N	74 111 222	86	159	174	130 195	231	182
N'	37	43	53	58	65	77	91

In the next proposition we determine the **Q**-isomorphism class of E.

Proposition 6.1. *The* **Q**-*isomorphism class of E is the strong Weil curve in its* **Q**-*isogeny class.*

Proof. Except for $N \in \{58, 65, 82, 102, 138, 238\}$, there is nothing to prove since the **Q**-isogeny class of E contains only one **Q**-isomorphism class. In the remaining six cases, the conductor of E is N. Let $\tilde{\pi}$: $X_0(N) \to \tilde{E}$ be the parametrization of the strong Weil curve in the isogeny class of E. Hence, a **Q**-morphism λ: $\tilde{E} \to E$ exists such that $\pi = \lambda \circ \tilde{\pi}$. By using that $\mathbf{C}(X_0(N))/\mathbf{C}(E)$ is an abelian extension with Galois group isomorphic to $B(N)$, one checks that none of the proper subgroups of $B(N)$ give an elliptic quotient of $X_0(N)$ (it is sufficient to check this for the subgroups of $B(N)$ of index 2). It follows that λ has degree one, so it is an isomorphism. ▮

Proposition 6.2. *Let* $R(x, y) = y^2 + a_1 yx + a_3 y - (x^3 + a_2 x^2 + a_4 x + a_6)$ *such that* $R(x, y) = 0$ *is a reduced Néron model of* $E = (X^*(N), \pi(i\infty))$ *over* **Q**. *Let U and V be functions on* $X_0(N)$ *invariant under* $B(N)$ *with* $R(U, V) = 0$. *Let* $f \in S_2(\Gamma_0(N))$ *be as above, and denote* $\omega = dU/(2V + a_1 U + a_3)$ *the invariant differential on E. Then,* $\pi^*(\omega) = \pm f(q)\, dq/q$.

Proof. If f is a newform, then the result follows from the fact that the Manin constant is ± 1 for the strong Weil parametrizations under consideration. For the other cases, let N' dividing N be the conductor of E, and let h be as before; so that we have $f = \sum_{d \mid N/N'} h \mid w_d$. Let pr: $X_0(N) \to X_0(N')$, π': $X_0(N') \to X^*(N')$ be the natural projections. Consider the composition

$$J_0(N) \xrightarrow{W} J_0(N) \xrightarrow{\mathrm{pr}_*} J_0(N') \xrightarrow{\pi'_*} X^*(N),$$

where $W = \sum_{d \mid N/N'} w_d$, and $J_0(N)$, $J_0(N')$ denote the jacobians of $X_0(N)$, $X_0(N')$. Since this morphism is invariant under $B(N)$, it factors through π_*. The fact that the elliptic curve E is non-CM ensures the existence of an integer m such that

$$\pi'_* \circ \mathrm{pr}_* \circ W = [m]\, \pi_*.$$

Therefore, $(\pi'_* \circ \mathrm{pr}_* \circ W)^* (\omega) = \pm f(q)\, dq/q$ and $(\pi_*)^* (\omega) = \pm f(q)\, dq/(mq)$. The arguments used by Edixhoven in Proposition 2 of [4] apply to this case, showing that $\pm 1/m \in \mathbf{Z}$. ∎

As a result, there are functions U and V on $X_0(N)$ satisfying $R(U, V) = 0$ and

$$U = 1/q^2 + \sum_{n \geqslant -1} b(n)\, q^n, \qquad V = -\left(\frac{q\, dU/dq}{f} + a_1 U + a_3\right)\Big/ 2.$$

The first coefficients $b(n)$ can be computed recursively from the above relations. At the same time, we determine the first coefficients of the q-expansion $V = 1/q^3 + \sum_{n \geqslant -2} c(n)\, q^n$. In all cases, it turns out that the Fourier coefficients $b(n)$ and $c(n)$ are in $\mathbf{Z}$. Finally, the Riemann–Roch theorem allows us to express the elementary symmetric functions J_i as polynomials in U and V: $J_i(z) = J_i(U, V)$, with $J_i(u, v) \in \mathbf{Z}[u, v]$.

In the Appendix we provide Cremona's code for the 38 values of N such that $X^*(N)$ has genus one. By looking at the functional equation, one realizes that $X^*(N)$ must have odd analytic rank, due to the fact that $h \mid w_{N'} = h$. In fact, in all cases the rank turns out to be one.

7. ELLIPTIC EXAMPLES

Here we present some examples from the curves $X^*(37)$, $X^*(74)$, and $X^*(82)$.

- Cases $X^*(37)$ and $X^*(74)$. We have the (non-commutative) diagram

$$\begin{tikzcd} X_0(74) \arrow[r, two heads] \arrow[d] & X_0(37) \arrow[d] \\ X^*(74) \arrow[r, "\simeq"] & X^*(37), \end{tikzcd}$$

and $\mathbf{Q}$-isomorphisms $X^*(37) \simeq X^*(74) \simeq E$, where E: $v^2 + v = u^3 - u$ is the elliptic curve 37A1 in Cremona's code. Let h denote the newform attached to E. As for $X^*(37)$, we find the modular parametrization $\pi_{37} : X_0(37) \to X^*(37) \simeq E$ given by

$$U = 1/q^2 + 2/q + 5 + 9q + 18q^2 + 29q^3 + 51q^4 + 82q^5 + 131q^6 + \cdots$$

$$V = 1/q^3 + 3/q^2 + 9/q + 20 + 46q + 92q^2 + 180q^3 + 329q^4 + 593q^5 + \cdots$$

satisfying $2V = -(qdU/dq)/f - 1$, where $f = h$ is the only newform of level 37 invariant under $B(37)$. On the other hand, as for $X^*(74)$, we find the modular parametrization π_{74}: $X_0(74) \to X^*(74) \simeq E$ given by

$$U = 1/q^2 + 2 + q + 4q^2 + 3q^3 + 7q^4 + 6q^5 + 13q^6 + 13q^7 + 22q^8 + \cdots$$
$$V = 1/q^3 + 3/q + 1 + 7q + 6q^2 + 17q^3 + 16q^4 + 35q^5 + 38q^6 + \cdots$$

satisfying $2V = -(qdU/dq)/f - 1$, where $f = h + 2h \mid B_2$ is the only normalized cusp form of level 74 invariant under $B(74)$.

At this point, it is easy to write down the polynomials

$$\begin{aligned} J(37)^*\,(x) &= (x - j(z))(x - j(37z)) \\ &= x^2 - J_1(u, v)\,x + J_2(u, v), \\ J(74)^*\,(x) &= (x - j(z))(x - j(2z))(x - j(37z))(x - j(74z)) \\ &= x^4 - \tilde{J}_1(u, v)\,x^3 + \tilde{J}_2(u, v)\,x^2 - \tilde{J}_3(u, v)\,x + \tilde{J}_4(u, v), \end{aligned}$$

although we omit the explicit symmetric functions lying in $\mathbf{Z}[u, v]$ due to reasons of space. Instead, we prefer to remark on some facts related to the discriminants of $J(37)^*$ and $J(74)^*$. Define δ_{37}: $E(\mathbf{Q}) \to \mathbf{Q}$ by $\delta_{37}(P) =$ discr$(J(37)^*\,(P)(x))$. That is, we first substitute u and v in $J(37)^*\,(x)$ by the coordinates of $P = (u, v)$ and then evaluate the discriminant of the resulting polynomial. The product $\delta_{37}(P)\,\delta_{37}(-P)$ is an even function on the elliptic curve E and thus it can be written as a polynomial in the variable u of $P = (u, v)$. We find $\delta_{37}(P)\,\delta_{37}(-P) = u^4(u+1)^4\,(u-1)^4\,(u-2)^4\,(u-6)^2$ $(u^2 - 30u + 77)\,Q(u)^2$, where $Q(u) \in \mathbf{Z}[u]$ does not have rational roots.

The elliptic curve E has no torsion points other than the origin, and the rational point $P = (0, 0)$ is a generator of its Mordell-Weil group. The only integral points not on the identity component are $\pm P$ and $\pm 3P = \pm(-1, -1)$. After computing the points

$$\begin{aligned} 2P &= (1, 0) & 4P &= (2, -3) \\ 6P &= (6, 14) & 8P &= (21/25, -69/125) \\ 12P &= (1357/841, 28888/24389) \end{aligned}$$

we deduce that $\pm P$, $\pm 2P$, $\pm 3P$, $\pm 4P$ and $\pm 6P$ are the only integer points on E (see Exercise IX.9.13 in [15]). We note that they are zeros of $\delta_{37}(\,*\,)\,\delta_{37}(-\,*\,)$. All of them are zeros of δ_{37} (and hence provide CM points), except for $-6P$ which gives rise to an isogeny of degree 37 between rational elliptic curves with j-invariants -7.11^3 and $-7.137^3.2083^3$. Analogously, define δ_{74} by using the polynomial $J(74)^*\,(x)$. Now, the ten integer points of E are zeros of δ_{74}, so they parametrize CM elliptic curves defined either over **Q** or over a quadratic field. We observe that the discriminant δ_{111} does not vanish at $4P$ and $-6P$.

- Case $X^*(82)$. In this example the parametrization $\pi : X_0(82) \rightarrow X^*(82)$ is given by

$$U = 1/q^2 + 1/q + 2 + 2q + 4q^2 + 3q^3 + 6q^4 + 7q^5 + 11q^6 + 11q^7 + \cdots$$
$$V = 1/q^3 + 2/q^2 + 4/q + 6 + 9q + 12q^2 + 19q^3 + 24q^4 + 38q^5 + \cdots,$$

and a Weierstrass model of $X^*(82)$ is $v^2 - uv - v = u^3 - 2u$. The Mordell–Weil group is $\langle Q \rangle + \langle P \rangle$, where $Q = (1, 1)$ is of order 2 and $P = (0, 0)$ of infinite order. Again the integral points $\pm P$, $\pm 2P$, Q, $\pm(P+Q)$, $\pm(2P+Q)$ and $\pm(4P+Q)$ are zeros of the norm discriminant $\delta_{82}(\,*\,)\,\delta_{82}(-\,*\,)$.

In these cases the integer points coincide with the rational zeros of the norm discriminant $\delta_N(\,*\,)\,\delta_N(-\,*\,)$, although not all of them need provide CM points.

APPENDIX

Rational Case

Next, we provide three tables according to the number of prime factors of $N > 1$ (square-free) such that $X^*(N)$ has genus 0. The genus of $X_0(N)$ is denoted by g. The other columns are labeled with generators of the different subgroups B' of index 2 in $B(N)$ and contain the genus g' of $X' = X_0(N)/B'$.

$N=p$	g	w_1
2	0	0
3	0	0
5	0	0
7	0	0
11	1	1
13	0	0
17	1	1
19	1	1
23	2	2
29	2	2
31	2	2
41	3	3
47	4	4
59	5	5
71	6	6

$N=p.q$	g	w_p	w_q	w_{pq}
$6=2.3$	0	0	0	0
$10=2.5$	0	0	0	0
$14=2.7$	1	1	0	0
$15=3.5$	1	1	0	0
$21=3.7$	1	0	1	0
$22=2.11$	2	1	0	1
$26=2.23$	2	1	1	0
$33=3.11$	3	2	0	1
$34=2.17$	3	1	1	1
$35=5.7$	3	1	2	0
$38=2.19$	4	2	1	1
$39=3.13$	3	1	2	0
$46=2.23$	5	3	0	2
$51=3.17$	5	3	1	1
$55=5.11$	5	3	1	1
$62=2.31$	7	4	1	2
$69=3.23$	7	4	1	2
$87=3.29$	9	5	2	2
$94=2.47$	11	6	1	4
$95=5.19$	9	5	3	1
$119=7.17$	11	6	4	1

$N=p.q.r$	g	w_p, w_q	w_p, w_r	w_q, w_r	w_p, w_{qr}	w_q, w_{pr}	w_r, w_{pq}	w_{pq}, w_{pr}
$30=2.3.5$	3	1	1	0	0	1	0	0
$42=2.3.7$	5	1	1	1	1	0	1	0
$66=2.3.11$	9	2	1	1	1	2	0	2
$70=2.5.7$	9	2	2	1	1	1	2	0
$78=2.3.13$	11	3	2	1	1	1	2	0
$105=3.5.7$	13	3	3	1	1	1	3	1
$110=2.5.11$	15	4	3	1	1	3	1	2

Elliptic Case

The columns of the following tables contain: the values of N (square-free) such that $X^*(N)$ has genus 1; the genus of $X_0(N)$ denoted by g; and the third column displays the elliptic curves $X^*(N)$ according to the terminology of [3]. In the last column, T stands for the order of the torsion subgroup of the Mordell–Weil group.

$N=p$	g	$X^*(N)$	T
37	2	$37A1$	1
43	3	$43A1$	1
53	4	$53A1$	1
61	4	$61A1$	1
79	6	$79A1$	1
83	7	$83A1$	1
89	7	$89A1$	1
101	8	$101A1$	1
131	11	$131A1$	1

$N=p.q$	g	$X^*(N)$	T
$58=2.29$	6	$58A1$	1
$74=2.37$	8	$37A1$	1
$82=2.41$	9	$82A1$	2
$86=2.43$	10	$43A1$	1
$118=2.59$	14	$118A1$	1
$142=2.71$	17	$142B1$	1
$57=3.19$	5	$57A1$	1
$111=3.37$	11	$37A1$	1
$123=3.41$	13	$123B1$	1
$141=3.47$	15	$141D1$	1
$159=3.53$	17	$53A1$	1
$65=5.13$	5	$65A1$	2
$145=5.29$	13	$145A1$	2
$155=5.31$	15	$155C1$	1
$77=7.11$	7	$77A1$	1
$91=7.13$	7	$91A1$	1
$143=11.13$	13	$143A1$	1

$N=p.q.r$	g	$X^*(N)$	T
$102=2.3.17$	15	$102A1$	2
$114=2.3.19$	17	$57A1$	1
$138=2.3.23$	21	$138A1$	2
$174=2.3.29$	27	$58A1$	1
$222=2.3.37$	35	$37A1$	1
$130=2.5.13$	17	$65A1$	2
$190=2.5.19$	27	$190B1$	1
$182=2.7.13$	25	$91A1$	1
$238=2.7.17$	33	$238B1$	2
$195=3.5.13$	25	$65A1$	2
$231=3.7.11$	29	$77A1$	1

$N = p.q.r.s$	g	$X^*(N)$	T
$210 = 2.3.5.7$	41	$210A1$	2

ACKNOWLEDGMENT

The authors thank the referee for suggesting several improvements to an earlier version of the manuscript.

REFERENCES

1. P. Bayer and A. Travesa, Eds., "Corbes modulars: Taules," Notes del Seminari de Teoria de Nombres de Barcelona, UB-UAB-UPC, Barcelona, 1992.
2. J. H. Conway and S. P. Norton, Monstrous moonshine, *Bull. London Math. Soc.* **11** (1979), 308–339.
3. J. E. Cremona, "Algorithms for Modular Elliptic Curves," Cambridge Univ. Press, Cambridge, UK, 1992.
4. S. B. Edixhoven, On the Manin constants of modular elliptic curves, *in* "Arithmetic and Algebraic Geometry," Progr. Math., Vol. 89, pp. 25–39, Birkhäuser, 1991.
5. N. Elkies, Remarks on elliptic K-curves, preprint 1993.
6. J. González, Equations of hyperelliptic modular curves, *Ann. Inst. Fourier* **41** (1991), 779–795.
7. P. G. Kluit, On the normalizer of $\Gamma_0(N)$, *in* "Modular Functions of One Variable V," Lecture Notes in Mathematics, Vol. 601, pp. 239–246, Springer-Verlag, Berlin/New York, 1976.
8. M. A. Kenku and F. Momose, Automorphism groups of the modular curves $X_0(N)$, *Comp. Math.* **65** (1988), 51–80.
9. G. Ligozat, Courbes modulaires de genre 1, *Bull. Soc. Math. France, Mém.* **43** (1975).
10. B. Mazur, Number theory as gadfly, *Am. Math. Monthly* **98** (1991), 593–610.
11. M. Newman, Construction and application of a class of modular functions, II, *Proc. London Math. Soc.* (1959), 373–387.
12. A. P. Ogg, Hyperelliptic modular curves, *Bull. Soc. Math. France* **102** (1974), 449–462.
13. K. Ribet, Abelian varieties over **Q** and modular forms, *in* "1992 Proceedings of KAIST Mathematics Workshop," pp. 53–79, Korea Advanced Institute of Science and Technology, Taejon, 1992.
14. M. Shimura, Defining equations of modular curves $X_0(N)$, *Tokyo J. Math.* **18** (1995), 443–456.
15. J. H. Silverman, "The Arithmetic of Elliptic Curves," Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, Berlin/New York, 1986.
16. N. Yui, The Monster, Thompson series, and applications, preprint 1996.