Canad. Math. Bull. Vol. **50** (3), 2007 pp. 334–346

Determination of Hauptmoduls and Construction of Abelian Extensions of Quadratic Number Fields

Hung-Jen Chiang-Hsieh and Yifan Yang

Abstract. We obtain Hauptmoduls of genus zero congruence subgroups of the type $\Gamma_0^+(p) := \Gamma_0(p) + w_p$, where p is a prime and w_p is the Atkin–Lehner involution. We then use the Hauptmoduls, along with modular functions on $\Gamma_1(p)$ to construct families of cyclic extensions of quadratic number fields. Further examples of cyclic extension of bi-quadratic and tri-quadratic number fields are also given.

1 Introduction

Let Γ be a congruence subgroup of $SL_2(\mathbb{R})$ commensurable with $SL_2(\mathbb{Z})$. The genus of Γ is defined to be the genus of the compact Riemann surface $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$, where $\mathbb{H}^* = \{\tau : \operatorname{Im}\tau > 0\} \cup \mathbb{Q} \cup \{\infty\}$. When the genus of a congruence subgroup Γ is zero, the function field on $X(\Gamma)$ can be generated by a single modular function. We call a generator of the function field a Hauptmodul if the modular function has a unique simple pole with residue 1 at infinity. For example, the classical modular j-function is a Hauptmodul of $SL_2(\mathbb{Z})$.

Since a Hauptmodul on a congruence subgroup of genus zero is periodic, a Hauptmodul has a Fourier expansion $q^{-1/k} + c_0 + c_1q^{1/k} + \cdots$, where $q = e^{2\pi i\tau}$ and k is the width of the cusp ∞. When the genus zero congruence subgroups contain $\Gamma_0(N)$, these Fourier coefficients have a surprising connection with the monster group, the largest sporadic finite simple group. This connection was conjectured in [1], and proved by Borcherds. In order to formulate the connection, Conway and Norton expressed Hauptmoduls of such subgroups using the classical Dedekind η-functions and the θ-series, from which the Fourier coefficients can be easily computed. (Note that the first fifty Fourier coefficients of Hauptmoduls have been calculated in [6].)

In this note we will give an alternative determination of Hauptmoduls of some of the genus zero congruence subgroups using the generalized Dedekind η-functions. (See Section 2 for the definition of these functions.) We are primarily concerned with genus zero congruence subgroups of the type $\Gamma_0^+(p) := \Gamma_0(p) + w_p$, where p are 11, 17, 19, 23, 29, 31, 41, 47, 59, 71, because they are the cases where there is no way to express the Hauptmoduls in terms of the Dedekind η-functions. (The values of the

Received by the editors April 28, 2005.

The first author was support by Grant 94-2115-M-194-005 of the National Science Council (NSC) of Taiwan. The second author was supported by Grant 93-2115-M-009-014 of the NSC and by the National Center for Theoretical Sciences (NCTS) of Taiwan.

AMS subject classification: Primary: 11F03; secondary: 11G16, 11R20.

©Canadian Mathematical Society 2007.

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

prime p are precisely those such that $X_0(p) := X(\Gamma_0(p))$ is elliptic or hyperelliptic, except 37.)

An application of interest is the construction of cyclic extensions of quadratic number fields. Our construction is an immediate generalization of the construction of cyclic extensions of $\mathbb{Q}$ described in Lecacheux [5], Washington [8], and Darmon [3]. Their basic idea is to use the fact that if f is a modular function on

$$\Gamma_1(N) = \{\gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod N\},$$

then any symmetric sum of product of $f|_\gamma$, where γ runs through a set of coset representatives of $\Gamma_0(N)/\Gamma_1(N)$, is a modular function on $\Gamma_0(N)$. Thus, the coefficients in

$$\prod_{\gamma \in \Gamma_0(N)/\Gamma_1(N)} (T - f\,\big|_\gamma)$$

are all modular functions on $\Gamma_0(N)$. When the genus of $\Gamma_0(N)$ is zero and H is its Hauptmodul, the coefficients are rational functions of H. If f is suitably chosen, then H and f will generate the function field of $\Gamma_1(N)\backslash\mathbb{H}^*$. More precisely, any other $f|_\gamma$ is in $\mathbb{Q}(H, f)$. Therefore, the above polynomial gives an abelian extension of $\mathbb{Q}(H)$ with the Galois group isomorphic to $\Gamma_0(N)/\Gamma_1(N) \simeq \mathbb{Z}_N^\times/\{\pm 1\}$, which in many cases are cyclic. For the cases where $\Gamma_0(N)\backslash\mathbb{H}^*$ is elliptic or hyperelliptic, we can show that the above idea yields families of cyclic extensions of quadratic number fields. The precise procedure will be described in Section 3.

Finally, we remark that our approach can also be applied to genus zero congruence subgroups of other types. However, given the main application we have in mind, we only consider $\Gamma_0^+(p)$ here. Nonetheless, we will give a few examples of other types of genus zero congruence subgroups in Section 4, where families of cyclic extension of bi-quadratic and tri-quadratic number fields will also be presented.

2 Hauptmoduls of $\Gamma_0^+(p)$

In this section we will obtain expressions for Hauptmoduls of $\Gamma_0^+(p)$. Throughout this section we assume that p is one of the primes 11, 17, 19, 23, 29, 31, 41, 47, 59, and 71. We first prove a lemma that makes Hauptmoduls explicit.

Lemma 1 *Let g be the genus of $\Gamma_0(p)$. Let $X(\tau)$ and $Y(\tau)$ be modular functions on $\Gamma_0(p)$ with a unique pole of order $g+1$ and $g+2$, respectively, at infinity. Let the Fourier expansions of X and Y at 0 be*

$$X(-1/(p\tau)) = a_0 + \sum_{n=1}^{\infty} a_n q^n \quad \textit{and} \quad Y(-1/(p\tau)) = b_0 + \sum_{n=1}^{\infty} b_n q^n,$$

where $q = e^{2\pi i\tau}$. Then the function $(Y + a_1 - b_0)/(X - a_0)$ is a Hauptmodul on $\Gamma_0^+(p)$.

Proof We first notice that the cusp ∞ is never a Weierstrass point on the compact Riemann surface $\Gamma_0(p)\backslash\mathbb{H}^*$ (see [7]). Therefore, the existence of such functions X

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

and Y is guaranteed. Now let H be a Hauptmodul on $\Gamma_0^+(p)$. Then H, considered as a modular function on $\Gamma_0(p)$, has two simple poles at ∞ and 0. It follows that $(X - a_0)H$ is a modular function with a pole of order $g + 2$ at infinity. Hence we have $H(X - a_0) = Y + c_1X + c_2$ for some constants c_1 and c_2. Thus, a Hauptmodul on $\Gamma_0^+(p)$ can be taken to be of the form $(Y - c)/(X - a_0)$ for some constant c. Now, taking the local behavior of the function $(Y - c)/(X - a_0)$ near ∞ and 0 into account, we see that the constant c must be $b_0 - a_1$. This completes the proof. ■

With the above lemma proven, the problem of determining Hauptmoduls reduces to finding functions with a pole of designated order at infinity. For this purpose we follow the approach of Yang [9].

Following the notation in Yang [10], we fix a positive integer N, and define two classes of generalized Dedekind η-functions by

$$E_{g,h}(\tau) = q^{B(g/N)/2} \prod_{m=1}^{\infty} (1 - e^{2\pi ih/N} q^{m-1+g/N})(1 - e^{-2\pi ih/N} q^{m-g/N})$$

for g and h not congruent to 0 modulo N simultaneously and

$$E_g(\tau) = q^{NB(g/N)/2} \prod_{m=1}^{\infty} (1 - q^{(m-1)N+g})(1 - q^{mN-g})$$

for g not congruent to 0 modulo N, where $B(x) = x^2 - x + 1/6$. Here we recall the properties of E_g relevant to our consideration.

Proposition 2 ([10, Theorem 1]) *The functions $E_{g,h}$ satisfy*

$$(1) \qquad E_{g+N,h} = E_{-g,-h} = -\zeta^{-h} E_{g,h}, \qquad E_{g,h+N} = E_{g,h}.$$

Moreover, let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. Then we have for $c = 0$,

$$E_{g,h}(\tau + b) = e^{\pi ibB(g/N)} E_{g,bg+h}(\tau),$$

and for $c \neq 0$, $E_{g,h}(\gamma\tau) = \epsilon(a, b, c, d)e^{\pi i\delta} E_{g',h'}(\tau)$, where

$$\epsilon(a, b, c, d) = \begin{cases} e^{\pi i(bd(1-c^2)+c(a+d-3))/6} & \text{if } c \text{ is odd}, \\ -ie^{\pi i(ac(1-d^2)+d(b-c+3))/6} & \text{if } d \text{ is odd}, \end{cases}$$

$$\delta = \frac{g^2ab + 2ghbc + h^2cd}{N^2} - \frac{gb + h(d-1)}{N},$$

$$(g'h') = (g\ h) \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).$$

Proposition 3 ([10, Corollary 2]) *The functions E_g satisfy*

$$(2) \qquad E_{g+N} = E_{-g} = -E_g.$$

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

Moreover, let $\gamma = \left(\begin{smallmatrix} a & b \\ cN & d \end{smallmatrix}\right) \in \Gamma_0(N)$. *We have for* $c = 0$,

$$E_g(\tau + b) = e^{\pi i b N B(g/N)} E_g(\tau),$$

and for $c \neq 0$,

$$E_g(\gamma\tau) = \epsilon(a, bN, c, d) e^{\pi i (g^2 ab/N - gb)} E_{ag}(\tau), \tag{3}$$

where

$$\epsilon(a, b, c, d) = \begin{cases} e^{\pi i (bd(1-c^2)+c(a+d-3))/6} & \text{if } c \text{ is odd}, \\ -ie^{\pi i (ac(1-d^2)+d(b-c+3))/6} & \text{if } d \text{ is odd}. \end{cases}$$

Proposition 4 ([10, Corollary 3]) *Consider the function* $f(\tau) = \prod_g E_g(\tau)^{e_g}$, *where* g *and* e_g *are integers. Suppose that one has*

$$\sum_g e_g \equiv 0 \bmod 12, \quad \sum_g g e_g \equiv 0 \bmod 2. \tag{4}$$

Then f *is invariant under the action of* $\Gamma(N)$. *Moreover, if in addition to* (4), *one also has*

$$\sum_g g^2 e_g \equiv 0 \bmod 2N, \tag{5}$$

then f *is a modular function on* $\Gamma_1(N)$.

Furthermore, for the cases where N *is a positive odd integer, the conditions* (4) *and* (5) *can be reduced to*

$$\sum_g e_g \equiv 0 \bmod 12 \quad \textit{and} \quad \sum_g g^2 e_g \equiv 0 \bmod N,$$

respectively.

Proposition 5 ([10, Lemma 2]) *The order of the function* E_g *at a cusp* a/c *with* $(a, c) = 1$ *is* $(c, N) P_2(ag/(c, N))/2$, *where* $P_2(x) = \{x\}^2 - \{x\} + 1/6$ *and* $\{x\}$ *denotes the fractional part of a real number* x.

Take $p = 11$, for example. The genus of $\Gamma_0(11)$ is 1. Thus, we need to find two functions X and Y with a unique pole of order 2 and 3, respectively, at infinity. By Propositions 3–5 we see that

$$X = \sum_{\gamma \in \Gamma_0(11)/\Gamma_1(11)} \frac{E_2 E_4^2}{E_1^3}\bigg|_\gamma = q^{-2} + 2q^{-1} + 4 + 5q + 8q^2 + q^3 + q^4 - 11q^5 + \cdots$$

and

$$Y = \sum_{\gamma \in \Gamma_0(11)/\Gamma_1(11)} \frac{E_5^4}{E_1^3 E_3}\bigg|_\gamma$$

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

are such functions. (See [9] for details on how we find such functions.)

To complete our determination of a Hauptmodul on $\Gamma_0^+(11)$ we notice that by Proposition 21 and the definition of E_g,

$$E_g(-1/(11\tau)) = E_{g,0}(-1/\tau) = e^{\pi i g/11} E_{0,g}(\tau). \tag{6}$$

It follows that

$$X(-1/(11\tau)) = 16 + 121q + 605q^2 + 2299q^3 + \cdots,$$
$$Y(-1/(11\tau)) = 59 + 726q + 4961q^2 + 25773q^3 + \cdots.$$

By Lemma 1, we see that the function

$$\frac{Y+62}{X-16} = q^{-1} + 1 + 17q + 46q^2 + 116q^3 + 252q^4 + 533q^5 + 1034q^6 + 1961q^7 + \cdots$$

is a Hauptmodul of $\Gamma_0^+(11)$. As a check on our computation we note that the above Fourier expansion agrees with that in [1, Table 4].

Hauptmoduls of other subgroups $\Gamma_0^+(p)$ can be obtained in the same way. We now summarize our finding in the following theorem. Here the notation $\sum_k \prod a^b$ represents $\sum_{\gamma\in\Gamma_0(p)/\Gamma} \prod E_a^b|_\gamma$, where Γ is the unique intermediate subgroup between $\Gamma_0(p)$ and $\Gamma_1(p)$ with $[\Gamma_0(p):\Gamma] = k$. We say a Hauptmodul is *normalized* if its constant term is zero.

Theorem 6 *Let X and Y be given as in Table* 1. *Then the function Y/X is the normalized Hauptmodul for their respective group $\Gamma_0^+(p)$.*

3 Construction of Cyclic Extensions of Quadratic Number Fields

In this section we will use the idea presented in the introduction to construct cyclic extensions of quadratic number fields.

Let Γ be an intermediate subgroup between $\Gamma_1(N)$ and $\Gamma_0(N)$. The following lemma gives sufficient conditions for the polynomial

$$\prod_{\gamma\in\Gamma_0(N)/\Gamma} (T - f|_\gamma)$$

to split in $K(f)$, where K denotes the subfield of modular functions on $\Gamma_0(N)$ whose Fourier coefficients are all rational numbers.

Lemma 7 *Let Γ be an intermediate subgroup between $\Gamma_1(N)$ and $\Gamma_0(N)$. Let f be a modular function on Γ such that f can be expressed in the form $\prod E_g^{e_g}$. Assume that Γ is the largest intermediate subgroup between $\Gamma_0(N)$ and $\Gamma_1(N)$ on which f is modular. Then the polynomial*

$$F(T) := \prod_{\gamma\in\Gamma_0(N)/\Gamma} (T - f|_\gamma)$$

splits in the field $K(f)$ with $\mathrm{Gal}(K(f)/K) \simeq \Gamma_0(N)/\Gamma$, *where K is the subfield of modular functions on $\Gamma_0(N)$ whose Fourier coefficients are all rational.*

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

p	X	Y
11	$\sum_{5} \frac{2 \cdot 4^2}{1^3} - 16$	$\sum_{5} \frac{5^4}{1^3 \cdot 3} - X + 62$
17	$\sum_{8} \frac{3 \cdot 8}{1 \cdot 2} - 11$	$\sum_{8} \frac{6^2 \cdot 8}{2^2 \cdot 3} + 22$
19	$\sum_{9} \frac{7 \cdot 8}{1 \cdot 6} - 8$	$\sum_{9} \frac{6^2 \cdot 8}{2 \cdot 3^2} + X + 8$
23	$\sum_{11} \frac{8 \cdot 10}{1 \cdot 5} - 15$	$\sum_{11} \frac{8 \cdot 10^2 \cdot 11^2}{4 \cdot 5^2 \cdot 6^2} + 4X + 85$
29	$\sum_{7} \frac{8 \cdot 9}{2 \cdot 5} - 4$	$\sum_{7} \frac{4 \cdot 6 \cdot 10 \cdot 14}{2 \cdot 3 \cdot 5 \cdot 7} + 2X + 25$
31	$\sum_{5} \frac{4 \cdot 7 \cdot 11}{1 \cdot 5 \cdot 6} - 10$	$\sum_{5} \frac{3 \cdot 13 \cdot 15}{1 \cdot 5 \cdot 6} + X + 20$
41	$\sum_{10} \frac{16 \cdot 20}{2 \cdot 18} - 16$	$\sum_{10} \frac{11 \cdot 17}{4 \cdot 5} + 2X + 32$
47	$\sum_{23} \frac{12 \cdot 17 \cdot 19 \cdot 21}{6 \cdot 10 \cdot 13 \cdot 15} - 17$	$\sum_{23} \frac{21 \cdot 22 \cdot 23}{6 \cdot 11 \cdot 13} + 3X + 102$
59	$\sum_{29} \frac{17 \cdot 19 \cdot 23}{1 \cdot 18 \cdot 21} - 38$	$\sum_{29} \frac{24 \cdot 25 \cdot 26 \cdot 28}{12 \cdot 13 \cdot 14 \cdot 21} + 2X + 102$
71	$2\sum_{35} \frac{30 \cdot 32}{2 \cdot 28} - \sum_{35} \frac{14 \cdot 22 \cdot 32}{7 \cdot 11 \cdot 16} - 68$	$\sum_{35} \frac{30 \cdot 32}{2 \cdot 28} + 2X + 110$

Table 1

Proof From the properties of E_g (see Proposition 3) we know that if $f = \prod E_g^{e_g}$ is modular on Γ, then $f|_\gamma = \epsilon \prod E_{ag}^{e_g}$ for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, where $\epsilon = \pm 1$. Thus, the Fourier coefficients of $f|_\gamma$ are all rational numbers. It follows that the coefficients in the polynomial $F(T)$ are all in K. Let $f_1, \dots, f_k$ denote the zeroes of $F(T)$. Then $K(f_1, \dots, f_k)$ is a finite extension of K. Moreover, if γ_1 and γ_2 are two distinct elements of $\Gamma_0(N)/\Gamma$, then we must have $f|_{\gamma_1} \neq f|_{\gamma_2}$. This is because if $f|_{\gamma_1} = f|_{\gamma_2}$, then f is fixed by the non-trivial element $\gamma_1\gamma_2^{-1}$ of $\Gamma_0(N)/\Gamma$, contradicting the assumption that Γ is the largest intermediate subgroup on which f is modular. Thus, the extension degree of $K(f_1, \dots, f_k)$ over K is at least $[\Gamma_0(N) : \Gamma]$.

Now we consider the Galois group G of $K(f_1, \dots, f_k)$ over K. Clearly, G has a subgroup H induced by the action of $\Gamma_0(N)/\Gamma$ on f_i. By the definition of a modular function, if an element h in $K(f_1, \dots, f_k)$ is fixed by H, then h is a modular function on $\Gamma_0(N)$. Moreover, every element in $K(f_1, \dots, f_k)$ has rational Fourier coefficients. Therefore, $h \in K$, and the fixed field of H is exactly K. By the Galois theory, this implies that the Galois group G is in fact equal to H, which is isomorphic to $\Gamma_0(N)/\Gamma$ because of the assumption that Γ is the largest intermediate subgroup on which f is modular. It follows that $F(T)$ splits in $K(f)$. This completes the proof. ■

Lemma 8 *Let $X_1, \dots, X_k$ be modular functions on a congruence subgroup Γ such that they generate the whole function field on Γ. Suppose that their Fourier expansions have rational coefficients. Then every modular function on Γ whose Fourier coefficients are rational is in the field $\mathbb{Q}(X_1, \dots, X_k)$.*

Proof Let f be a modular function on Γ whose Fourier coefficients are rational. We have $f = p_1/p_2$ for some polynomials p_1, p_2 in $\mathbb{C}[X_1, \dots, X_k]$. Writing out the Fourier expansion of $fp_2 = p_1$, we see that the coefficients of the polynomials p_1, p_2 satisfy a system of linear equations whose coefficients are all rational numbers. Therefore, they can be chosen to be rational. This completes the proof. ■

We now construct cyclic extensions of quadratic number fields as follows. Let X and Y be the modular functions on $\Gamma_0(p)$ listed in Theorem 6 such that $H := Y/X$ is the normalized Hauptmodul of $\Gamma_0^+(p)$. It is clear that $X + X|_{w_p}$ and $X \cdot X|_{w_p}$ are functions on $\Gamma_0^+(p)$. Therefore, they are zeroes of a quadratic polynomial over $\mathbb{Q}(H)$. In fact, because the only pole of X is at infinity, the polynomial is a monic polynomial over $\mathbb{Q}[H]$. That is, we have $X^2 + c_1(H)X + c_2(H) = 0$ for some $c_1, c_2 \in \mathbb{Q}[H]$. Moreover, since $Y = XH$, we also have $Y^2 + Hc_1(H)Y + H^2c_2(H) = 0$.

Let Γ be an intermediate group between $\Gamma_0(p)$ and $\Gamma_1(p)$ with $[\Gamma_0(p):\Gamma] = k$. Let $f = \prod E_g^{e_g}$ be a modular function on Γ such that Γ is the largest intermediate subgroup on which f is modular. By Lemmas 7 and 8, the coefficients of the polynomial

$$F(T) := \prod_{\gamma \in \Gamma_0(N)/\Gamma} (T - f|_\gamma)$$

are all in $\mathbb{Q}(X, Y)$, and the splitting field is $\mathbb{Q}(X, Y)(f)$ with Galois group isomorphic to $\Gamma_0(p)/\Gamma \simeq \mathbb{Z}_k$. Now suppose that H takes a rational value h. Then X and Y will be in the same quadratic number field $\mathbb{Q}(\sqrt{\Delta})$, where $\Delta = c_1(h)^2 - 4c_2(h)$. Thus, the above polynomial $F(T)$ defines a cyclic extension of degree k over $\mathbb{Q}(\sqrt{\Delta})$. (Of course, we sometimes get a cyclic extension of $\mathbb{Q}$ this way, not a quadratic number field. But this occurs only when (X, Y) is a rational point on the modular curve $X_0(p)$, and it is known that there are only finitely many of them. Also, it may happen that the value of f for certain rational numbers h is in an extension field of $\mathbb{Q}(\sqrt{\Delta})$ of degree strictly less than k, but we expect that this is not the case for a general h.)

We now give some examples.

Example 1 Take $p = 11$, for example. Let X and Y be given as in Theorem 6. Since the orders of poles of X and Y are relatively prime, X and Y generate the whole modular function field on $\Gamma_0(11)$. Furthermore, X and Y clearly have integer Fourier coefficients. Thus, by Lemma 8, every modular function on $\Gamma_0(11)$ that has rational Fourier coefficients is in the field $\mathbb{Q}(X, Y)$. Moreover, the quadratic relation between X and the Hauptmodul $H = Y/X$ is $X^2 - (H^2 + 2H - 46)X + (121H + 847) = 0$, and the discriminant is

$$H^4 + 4H^3 - 88H^2 - 668H - 1272 = (H + 6)(H^3 - 2H^2 - 76H - 212).$$

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

(We remark that the four zeroes of the above polynomial of H correspond to the four elliptic points of order 2 in $\Gamma_0^+(11)\backslash\mathbb{H}^*$. The fact that one of the zeroes is rational corresponds to the fact that the number of inequivalent classes of positive definite quadratic forms $11Ax^2 + Bxy + Cy^2$, $A, B, C \in \mathbb{Z}$, of discriminant -11 under the action of $\Gamma_0^+(11)$ is 1. In other words, -6 is the value of H at the elliptic point $(11 + \sqrt{-11})/22$, which is the root of $11z^2 - 11z + 3$ on the upper half-plane. On the other hand, the roots of $H^3 - 2H^2 - 76H - 212$ are the values of H at the three elliptic points corresponding to the three inequivalent classes of positive definite quadratic forms $11Ax^2 + Bxy + Cy^2$ of discriminant -44. See [2] for more discussion on the values of Hauptmoduls at elliptic points.)

Now choose $T = E_3E_4E_5/E_1^2E_2$. By Proposition 4, T is modular on $\Gamma_1(11)$. Moreover, we see from Proposition 3 that the action of $\Gamma_0(11)/\Gamma_1(11)$ on T results in T, $E_1E_3E_5/E_2^2E_4$, $-E_1E_2E_5/E_3E_4^2$, $E_1E_2E_4/E_5E_3^2$, and $E_2E_3E_4/E_1E_5^2$. This, in particular, shows that $\Gamma_1(11)$ is the largest intermediate subgroup between $\Gamma_0(11)$ and $\Gamma_1(11)$ on which T is modular, and T satisfies the assumption in Lemma 7 with $\Gamma = \Gamma_1(11)$. Furthermore, by Proposition 5, their divisors are supported at the cusps of the form $k/11$. Thus, any modular function on $\Gamma_0(11)$ formed by a symmetric sum of the above functions will have poles only at ∞, and hence must be expressible as a polynomial of X and Y. In fact, we find that f satisfies

$$(7) \qquad T^5 - (X + 18)T^4 + (2X + 35)T^3 - (X + 16)T^2 - 2T + 1 = 0.$$

The settings of $H = -10, -8, -6, -4, -2, 0, 2$, for example, give cyclic extensions of degree 5 of

$$\mathbb{Q}(\sqrt{163}),\ \mathbb{Q}(\sqrt{122}),\ \mathbb{Q},\ \mathbb{Q}(\sqrt{-2}),\ \mathbb{Q}(\sqrt{-19}),\ \mathbb{Q}(\sqrt{-318}),\ \text{and } \mathbb{Q}(\sqrt{-182}),$$

respectively.

Remark In [5] Lecacheux showed that the family of the sextic fields she constructed using the covering of modular curves $X_1(13) \mapsto X_0(13)$ have systems of fundamental units expressible in terms of values of modular functions. A similar phenomenon also appears in the family of quartic fields considered in [8]. A common feature of the above two families of cyclic extensions is that the modular functions used are the so-called modular units. That is, they are modular functions with divisors supported only at cusps. (See [4] for more information.) In our notation, they can be expressed as products of E_g or $E_{0,g}$. Since our construction of cyclic extensions of quadratic number fields also uses the modular units, one may ask whether systems of fundamental units for the fields under consideration can be expressed in terms of values of modular functions analogously. To be more precise, we would like to study the unit groups in $\mathbb{Q}(\sqrt{\Delta}, T)$, where H is an integer, $\Delta = (H + 6)(H^3 - 2H^2 - 76H - 212)$, and T is a root of (7). However, our investigation is not as satisfactory as that in [5] or that in [8].

From now on, we use the capital letters H and T to indicate that they are considered as modular functions, while the lowercase letters h and t will denote the assignment of an integer h to H and of a complex number t to the corresponding value of T.

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

We first deal with the case when Δ is a perfect square. These Δ correspond to rational points on $X_0(11)$, and it is well known that there are five rational points on $X_0(11)$. Among them, two are the cusps ∞ and 0, and the value of H at these two points is infinity. Moreover, since there are two choices for x for a given h in general, we conclude that there are only two finite values of h that make Δ a perfect square. Namely, they are $h = -6$, which gives $\Delta = 0$ and corresponds to the rational points $(X, Y) = (-11, 66)$, and $h = -7$, which gives $\Delta = 121$ and corresponds to $(0, 0)$ and $(-11, 77)$. When $X = -11$ and $X = 0$, the polynomial in (7) has discriminant 11^4 and 11^8, respectively. Thus the extension field $\mathbb{Q}(t)$ is $\mathbb{Q}(\cos(2\pi/11))$. (This can be seen from the conductor-discriminant formula and the fact that $\mathrm{Gal}(\mathbb{Q}(t)/\mathbb{Q})$ is of order 5.) Computing the regulators using the computer software PARI GP, we find that when $X = -11$, the roots of (7), along with ± 1, generate the whole unit group, and when $X = 0$, they generate a subgroup of index 11 of the unit group.

We next consider the case when Δ is not a perfect square. The minimal polynomial for the modular function T over $\mathbb{Q}(H)$ is of degree 10, and the conjugates of T are obtained by letting the right cosets of $\Gamma_1(11)$ in $\Gamma_0^+(11)$ act on T. The extension $\mathbb{Q}(H, T)$ over $\mathbb{Q}(H)$ is not normal because the Fourier coefficients of $T|_{w_{11}}$ are not in $\mathbb{Q}$. In fact, using property (6) of E_g and the fact that H and T generate the whole function field on $\Gamma_1(11)$, one sees that the splitting field is $\mathbb{Q}(H, T, \cos(2\pi/11))$. On the other hand, by Lemma 8, we have $T|_\gamma \in \mathbb{Q}(H, T)$ for all $\gamma \in \Gamma_0(11)/\Gamma_1(11)$. Thus, if h is an integer, then any conjugate of t induced by the action of $\Gamma_0(11)/\Gamma_1(11)$ is in $\mathbb{Q}(t)$, while the remaining conjugates are in $\mathbb{Q}(t, \cos(2\pi/11))$.

Now assume that h is an integer such that Δ is negative. That is, assume that h is one of the integers $-5, \dots, 10$. Then the rank of the unit groups is 4 because all of the conjugates of t are non-real. Since we are interested in the question of whether the unit group U is generated by values of modular functions, we naturally consider the subgroup U' generated by the conjugates of t induced by the action of $\Gamma_0(11)/\Gamma_1(11)$. Since there are only finitely many cases, we just use PARI GP to determine the index $[U : U']$ case by case. We find that when $h = -5, -4, -2, 10$, the index is 11. When $h = 1$, the index is 781, and when $h = -3, -1, 0, 2, \dots, 9$, we have $U = U'$.

For the remaining cases, where Δ is positive non-square, the field $\mathbb{Q}(t)$ is totally real, and the rank of the unit group is 9. Now among the conjugates of T over $\mathbb{Q}(H)$, only five of them are in $\mathbb{Q}(T, H)$, and the rest are in $\mathbb{Q}(T, H, \cos(2\pi/11))$. Thus, it seems to us that in these cases the values of modular units will not be able to generate the unit group of $\mathbb{Q}(t)$, and a result analogous to that of [5] or that of [8] is out of reach.

Example 2 Take $p = 23$, and let X, Y, and H be given as in Theorem 6. Then we have

$$X^2 - (H^3 + 2H^2 - 11H - 49)X + (69H^2 + 368H + 644) = 0,$$

whose discriminant, as a function of X, is

$$(H^3 - 2H^2 - 17H - 25)(H^3 + 6H^2 + 11H + 7).$$

(Again, we remark that the factor $H^3 + 6H^2 + 11H + 7$ corresponds to the three inequivalent classes of quadratic forms $23Ax^2 + Bxy + Cy^2$ of discriminant -23 under

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

the action of $\Gamma_0^+(23)$, while the other factor $H^3-2H^2-17H-25$ corresponds to those quadratic forms $23Ax^2+Bxy+Cy^2$ of discriminant -92.) Set $T=E_8E_{10}/(E_1E_5)$. We find

$$\begin{aligned}T^{11}&+(X+15)T^{10}+(Z+2X+18)T^9+(-Z+Y-X-22)T^8\\&+(-XY+3X^2-5Z-15Y+107X+968)T^7\\&+(2XY-7X^2+11Z+27Y-242X-2089)T^6\\&+(-XY+5X^2-6Z-15Y+166X+1442)T^5\\&+(-X^2-Z+5Y-35X-434)T^4+(Z-4Y+5X+177)T^3\\&+(Y-X-49)T^2+5T-1=0,\end{aligned}$$

where

$$\begin{aligned}Z&=\sum_{\gamma\in\Gamma_0(23)/\Gamma_1(23)}\frac{E_8^4}{E_1E_4^3}\Big|_\gamma=\frac{Y^2-XY-6X^2-69Y-129X}{X}\\&=q^{-5}+q^{-4}+q^{-3}+q^{-2}+2q^{-1}+8+3q+\cdots\end{aligned}$$

is a modular function on $\Gamma_0(23)$ with a pole of order 5 at infinity. Now the settings of $H=-5,-4,-3,-2,-1,0,1$, for instance, yield cyclic extensions of degree 11 of $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{265}]$, $\mathbb{Q}[\sqrt{-19}]$, $\mathbb{Q}[\sqrt{-7}]$, $\mathbb{Q}[\sqrt{-11}]$, $\mathbb{Q}[\sqrt{-7}]$, $\mathbb{Q}[\sqrt{-43}]$, respectively.

4 Further Examples

Example 3 Let $N=21$. The congruence subgroup $\Gamma_0(21)$ is of genus 1, while $\Gamma_0(21)+w_3$ is of genus 0. The normalized Hauptmodul for $\Gamma_0(21)+w_3$ can be expressed as $\eta(\tau)\eta(3\tau)/(\eta(7\tau)\eta(21\tau))+1$. Let

$$X=\frac{\eta(3\tau)^3\eta(7\tau)}{\eta(\tau)\eta(21\tau)^3}-1=q^{-2}+q^{-1}+1+2q^2+q^3+\cdots,$$

$$Y=\frac{\eta(3\tau)^6\eta(7\tau)^2}{\eta(\tau)^2\eta(21\tau)^6}-\frac{\eta(3\tau)\eta(7\tau)^7}{\eta(\tau)\eta(21\tau)^7}-2X-4=q^{-3}+q^{-2}-2+q+3q^2+2q^3+\cdots$$

be two modular functions on $\Gamma_0(21)$ with poles of orders 2 and 3 at ∞. Then we have the relations

$$Y=XH,\quad X^2-(H^2+H+3)X-(3H+3)=0.$$

The discriminant of the last quadratic equation is $(H^2+3H+3)(H^2-H+7)$, which we can verify that the zeroes of the factor H^2+3H+3 are the values of H at the two elliptic points of order 2 on $X_0(21)/w_3$, while H^2-H+7 corresponds to the two elliptic points of order 3 on $X_0(21)/w_3$. Now take a modular function $T=$

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

$E_8E_{10}/(E_1E_4) = q^{-3} + q^{-2} + q^{-1} + 1 + 2q + 2q^2 + \cdots$ on $\Gamma_1(21)$ whose divisors are supported at cusps of the form $k/21$ with $(k, 21) = 1$. We have

$$(8)\quad T^6 - YT^5 - (X^2 + 2Y)T^4 - (2X^2 + 2Y - 1)T^3 - (X^2 + 2Y)T^2 - YT + 1 = 0.$$

(We remark that the observation that the above equation of T is invariant under the substitution $T \mapsto 1/T$ can be explained using the fact that the action of one of the coset representative $\left(\begin{smallmatrix} 8 & 3 \\ 21 & 8 \end{smallmatrix}\right)$ of $\Gamma_0(21)/\Gamma_1(21)$ sends T to its reciprocal.) Now the setting of $H = -3, \dots, 3$ yields cyclic extensions of degree 6 of $\mathbb{Q}[\sqrt{57}]$, $\mathbb{Q}[\sqrt{13}]$, $\mathbb{Q}$, $\mathbb{Q}[\sqrt{21}]$, $\mathbb{Q}$, $\mathbb{Q}[\sqrt{13}]$, and $\mathbb{Q}[\sqrt{273}]$, respectively.

Example 4 Again let $N = 21$. The congruence subgroups $\Gamma_0(21)+w_3$, $\Gamma_0(21)+w_{21}$, and $\Gamma_0^+(21)$ are all of genus zero, where $\Gamma_0^+(21)$ denotes the congruence subgroup $\Gamma_0(21)$ plus all the Atkin–Lehner involutions. The normalized Hauptmoduls for the above three congruence subgroups are, respectively,

$$H_1 = \frac{\eta(\tau)\eta(3\tau)}{\eta(7\tau)\eta(21\tau)} + 1, \quad H_2 = \frac{\eta(3\tau)^2\eta(7\tau)^2}{\eta(\tau)^2\eta(21\tau)^2} - 2,$$

and

$$H = H_1 + \frac{7}{H_1 - 1} = H_2 + \frac{1}{H_2 + 2}.$$

They satisfy the quadratic relations

$$H_1^2 - (H+1)H_1 + (H+7) = 0, \qquad H_2^2 - (H-2)H_2 + (-2H+1) = 0.$$

Let $\Delta_1 = H^2 - 2H - 27$ and $\Delta_2 = H(H+4)$ denote the discriminants of the above quadratic polynomials. Now the functions X and Y in Example 3 satisfy

$$X + 1 = (H_1 - 1)(H_2 + 2), \quad Y = XH_1.$$

Thus, they are in the field $\mathbb{Q}[\sqrt{\Delta_1}, \sqrt{\Delta_2}]$. When H is a rational number, equation (8) yields a cyclic extension of degree 6 of $\mathbb{Q}[\sqrt{\Delta_1}, \sqrt{\Delta_2}]$. For example, the settings of $H = -3, -2, \dots, 3$ give cyclic extensions of $\mathbb{Q}[\sqrt{-3}]$, $\mathbb{Q}[\sqrt{-19}, i]$, $\mathbb{Q}[\sqrt{-3}, \sqrt{-6}]$, $\mathbb{Q}[\sqrt{-3}]$, $\mathbb{Q}[\sqrt{-7}, \sqrt{5}]$, $\mathbb{Q}[\sqrt{-3}, \sqrt{3}]$, $\mathbb{Q}[\sqrt{-6}, \sqrt{21}]$, respectively.

Example 5 Let $N = 30$. The groups $\Gamma_0(30) + \langle w_3, w_5\rangle$, $\Gamma_0(30) + \langle w_2, w_{15}\rangle$, and $\Gamma_0(30) + \langle w_5, w_6\rangle$ are of genus zero. Their normalized Hauptmoduls are

$$H_1 = \frac{\eta(\tau)\eta(3\tau)\eta(5\tau)\eta(15\tau)}{\eta(2\tau)\eta(6\tau)\eta(10\tau)\eta(30\tau)} + 1, \quad H_2 = \frac{\eta(3\tau)\eta(5\tau)\eta(6\tau)\eta(10\tau)}{\eta(\tau)\eta(2\tau)\eta(15\tau)\eta(30\tau)} - 1,$$

and

$$H_3 = \left(\frac{\eta(2\tau)\eta(3\tau)\eta(10\tau)\eta(15\tau)}{\eta(\tau)\eta(5\tau)\eta(6\tau)\eta(30\tau)}\right)^2 - 2,$$

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

respectively. Then the normalized Hauptmodul H for $\Gamma_0^+(30)$ is

$$H = H_1 + \frac{4}{H_1 - 1} = H_2 + \frac{1}{H_2 + 1} = H_3 + \frac{1}{H_3 + 2}.$$

Thus, H_1, H_2, and H_3 fall in the fields $\mathbb{Q}[\sqrt{\Delta_k}]$, $k = 1, 2, 3$ with

$$\Delta_1 = (H-5)(H+3), \quad \Delta_2 = (H-1)(H+3), \quad \Delta_3 = H(H+4).$$

Set

$$X = \frac{\eta(\tau)\eta(6\tau)^6\eta(10\tau)^2\eta(15\tau)^3}{\eta(2\tau)^2\eta(3\tau)^3\eta(5\tau)\eta(30\tau)^6} - 5 = q^{-4} - q^{-3} + q^{-2} + q^{-1} - 5 + q^2 + \cdots,$$

$$Y = \frac{\eta(6\tau)^3\eta(10\tau)^3\eta(15\tau)^6}{\eta(2\tau)\eta(5\tau)^2\eta(30\tau)^9} - \frac{\eta(\tau)\eta(2\tau)\eta(5\tau)\eta(6\tau)\eta(10\tau)\eta(15\tau)^3}{\eta(3\tau)\eta(30\tau)^7} - 5X - 20$$
$$= q^{-5} - 2q^{-4} + 3q^{-3} - 2q^{-2} - 2q^{-1} + 1 + q - q^2 + \cdots,$$

$$Z = \frac{\eta(6\tau)^3\eta(10\tau)^3\eta(15\tau)^6}{\eta(2\tau)\eta(5\tau)^2\eta(30\tau)^9} = q^{-6} + q^{-4} + 2q^{-2} + 2q^{-1} + 2q + 2q^2 + 4q^{-3} + \cdots,$$

$$W = \frac{\eta(\tau)\eta(5\tau)^2\eta(6\tau)\eta(10\tau)\eta(15\tau)^3}{\eta(30\tau)^8} = q^{-7} - q^{-6} - q^{-5} - q^{-2} + q^{-1} + 4 + q + \cdots.$$

By an argument analogous to that in the proof of Lemma 7, we can show that the functions X, Y, Z, and W are in an extension field of $\mathbb{Q}(H)$ with Galois group isomorphic to $\Gamma_0^+(30)/\Gamma_0(30) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. In other words, they are in

$$\mathbb{Q}\Big[\sqrt{\Delta_1}, \sqrt{\Delta_2}, \sqrt{\Delta_3}\Big].$$

Now choose

$$T = \frac{E_{11}E_{14}}{E_1E_4}.$$

We find

$$T^4 - (Y + 3X + 16)T^3 - (X^2 + 3W + 2Z + 5Y + 23X + 74)T^2 - (Y + 3X + 16)T + 1 = 0.$$

By Lemma 7, this equation defines a cyclic extension of degree 4 of the tri-quadratic field $\mathbb{Q}[\sqrt{\Delta_1}, \sqrt{\Delta_2}, \sqrt{\Delta_3}]$.

References

[1] J. H. Conway and S. P. Norton, *Monstrous moonshine.* Bull. London Math. Soc. **11**(1979), no. 3, 308–339.

[2] D. Cox, J. McKay, and P. Stevenhagen, *Principal moduli and class fields.* Bull. London Math. Soc. **36**(2004), no. 1, 3–12.

[3] H. Darmon, *Note on a polynomial of Emma Lehmer.* Math. Comp. **56**(1991), no. 194, 795–800.

[4] D. S. Kubert and Serge Lang, *Modular Units.* Grundlehren der Mathematischen Wissenschaften 244, Springer-Verlag, New York, 1981.

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press

[5] O. Lecacheux, *Unités d'une famille de corps cycliques réeles de degré* 6 *liés à la courbe modulaire* $X_1(13)$. J. Number Theory **31**(1989), no. 1, 54–63.

[6] J. McKay and H. Strauss, *The q-series of monstrous moonshine and the decomposition of the head characters.* Comm. Algebra **18**(1990), no. 1, 253–278.

[7] A. P. Ogg, *On the Weierstrass points of* $X_0(N)$. Illinois J. Math. **22**(1978), no. 1, 31–35.

[8] L. C. Washington, *A family of cyclic quartic fields arising from modular curves.* Math. Comp. **57**(1991), no. 196, 763–775.

[9] Y. Yang, *Defining equations of modular curves.* Adv. Math. **204**(2006), no. 2, 481–508.

[10] ———, *Transformation formulas for generalized Dedekind eta functions.* Bull. London Math. Soc. **36**(2004), no. 5, 671–682.

Department of Mathematics
National Chung Cheng University
Chiayi 621
Taiwan
e-mail: hchiang@math.ccu.edu.tw

Department of Applied Mathematics
National Chiao Tung University
Hsinchu 300
Taiwan
e-mail: yfyang@math.nctu.edu.tw

https://doi.org/10.4153/CMB-2007-032-1 Published online by Cambridge University Press