International Journal of Number Theory
Vol. 8, No. 1 (2012) 265–287
© World Scientific Publishing Company
DOI: 10.1142/S1793042112500157

World Scientific
www.worldscientific.com

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

RAMANUJAN INVARIANTS FOR DISCRIMINANTS CONGRUENT TO 5 (mod 24)

ELISAVET KONSTANTINOU

Department of Information and Communication Systems Engineering
University of the Aegean, 83200 Karlovassi, Samos, Greece
ekonstantinou@aegean.gr

ARISTIDES KONTOGEORGIS

Department of Mathematics, University of Athens
Panepistimioupolis Zografou 15784, Athens, Greece
kontogar@math.uoa.gr

Received 11 January 2011
Accepted 30 June 2011
Published 27 January 2012

Dedicated to Professor Jannis A. Antoniadis on the occasion of his 60th birthday

In this paper we compute the minimal polynomials of Ramanujan values $27t_n^{-12}$ for discriminants $D \equiv 5 \pmod{24}$. Our method is based on Shimura Reciprocity Law as which was made computationally explicit by Gee and Stevenhagen in [Generating class fields using Shimura reciprocity, in *Algorithmic Number Theory*, Lecture Notes in Computer Science, Vol. 1423 (Springer, Berlin, 1998), pp. 441–453; MR MR1726092 (2000m:11112)]. However, since these Ramanujan values are not class invariants, we present a modification of the method used in [Generating class fields using Shimura reciprocity, in *Algorithmic Number Theory*, Lecture Notes in Computer Science, Vol. 1423 (Springer, Berlin, 1998), pp. 441–453; MR MR1726092 (2000m:11112)] which can be applied on modular functions that do not necessarily yield class invariants.

Keywords: Explicit class field theory; Shimura reciprocity; elliptic curve cryptography.

Mathematics Subject Classification 2010: 11R29, 11G15

1. Introduction

It is known that the ring class field of imaginary quadratic orders can be generated by evaluating the j-invariant at certain algebraic integers. Several other modular functions, like the Weber functions [17] can also be used for the generation of the ring class field. In [6, 8] Gee and Stevenhagen developed a method based on Shimura reciprocity theory, in order to check whether a modular function gives rise to a class invariant and in the case it does, they provided a method for the efficient computation of the corresponding minimal polynomial. This method was generalized further in [16] to handle the ring class fields case as well. Shimura reciprocity law relates

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

the Galois group of the ray class field $H_{N,\mathcal{O}}$ of conductor N over the ring class field $H_{\mathcal{O}}$ of the order $\mathcal{O}$, to the group $G_N = (\mathcal{O}/N\mathcal{O})^*/\mathcal{O}^*$. In our study we encounter modular functions of level 72, and the structure and order of the group G_{72} depends on the decomposition of $2\mathcal{O}, 3\mathcal{O}$ as product of prime ideals in $\mathcal{O}$. If the ideals $2, 3$ do not remain inert simultaneously then a variety of modular functions like the Weber functions, double eta functions, etc. can be used for constructing the ring class field.

Let $K_n = \mathbb{Q}(\sqrt{-n})$ be an imaginary quadratic number field such that $n \equiv 19 \pmod{24}$ and assume that $\mathcal{O} \subset K$. If n is squarefree then $D = -n$ is a fundamental discriminant of K_n. In this paper we will treat the case when $2, 3$ both remain inert, i.e. $2\mathcal{O}$ and $3\mathcal{O}$ are prime ideals of $\mathcal{O}$. In this article we are interested in the $-n \equiv 1 \pmod 4$ case so we set $\theta_n = \frac{1}{2} + i\frac{\sqrt{n}}{2}$ and we consider the order $\mathcal{O} = \mathbb{Z}[\theta_n]$ which is a maximal order if n is squarefree. Notice that the case $n \equiv 19 \pmod{24}$ is the only case where $2, 3$ remain inert.

The authors used the method of Gee and Stevenhagen [9, 10] in order to construct the minimal polynomials of the Ramanujan values t_n for $n \equiv 11 \pmod{24}$ proposed by Ramanujan in his third notebook [13, Vol. 2, pp. 392 and 393]. For a definition of t_n, see Sec. 3, Eq. (3.3). The values t_n were proven to be class invariants for $n \equiv 11 \pmod{24}$ by Berndt and Chan in [2]. However, for $n \equiv 19 \pmod{24}$ the values t_n are no longer class invariants and Ramanujan proposed the use of the values $H_n = 27t_n^{-12}$ [13, p. 317].

In this paper, we will prove that H_n values are still not class invariants since $K(H_n)$ is a quadratic extension of the ring class field. This is clearly an obstacle for the construction of the minimal polynomials of H_n values, since Gee and Stevenhagen method can no longer be applied. Therefore, we propose a modification of their method that allows us to study the case of modular functions which do not give class invariants and then we proceed to the study of H_n.

We explicitly describe a method for the construction of their minimal polynomials and examine some interesting properties of these polynomials. Finally, we propose the use of values $A_n = 27t_n^{-12} + t_n^{12}/27$ that are class invariants and generate the ring class field. Unfortunately, A_n are algebraic integers which are not units.

We also study the relation with the modular functions $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$ introduced by Gee in [7, p. 73]. In Remark 14 we see how the Ramanujan values A_n are naturally introduced as generators of the invariant ring $\mathbb{Q}[\mathfrak{g}_0^{12}, \mathfrak{g}_1^{12}, \mathfrak{g}_2^{12}, \mathfrak{g}_3^{12}]$, under the action of a cyclic permutation τ of order 4. Notice that $\mathfrak{g}_0^6(\theta)$, $\mathfrak{g}_1^6(\theta)$, $\mathfrak{g}_2^6(\theta)$, $\mathfrak{g}_3^6(\theta)$ are inside the ray class field $H_{3,\mathcal{O}}$ and we are able to find their minimal polynomials over the ring class field. We believe that this method of formalizing the search of class invariants in terms of invariant theory can be applied to many other cases as well.

This method allows us to handle the case $n \equiv 3 \pmod{24}$. In Sec. 4 we define some new class invariants and compute their polynomials using the methods developed in the previous sections.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Finally, we give an example of using the A_n class invariant in order to construct an elliptic curve over the finite field $\mathbb{F}_p$,

$$p = 2912592100297027922366637171900365067697538262949$$

of prime order

$$m = 2912592100297027922366635123877214056291799441739.$$

2. Class Field Theory

Gee and Stevenhagen provided us with a method to check whether a modular function is a class invariant. We will follow the notation of [6, 14, Chap. 6; 16]. It is known that the modular curve $X(N)$ can be defined over $\mathbb{Q}(\zeta_N)$. Let $\mathcal{F}_N$ be the function field of $X(N)$ over $\mathbb{Q}(\zeta_N)$, i.e. the field of meromorphic functions on $X(N)$ with Fourier coefficients in $\mathbb{Q}(\zeta_N)$. Observe that $\mathcal{F}_1 = \mathbb{Q}(j)$. The automorphic function field $\mathcal{F}$ is defined as $\mathcal{F} = \bigcup_{N\geq 1} \mathcal{F}_N$.

For the convenience of the reader we repeat here some elements of the adelic formulation of class field theory and the relation to modular functions. For more information about these subjects we refer to [14, Secs. 5.2 and 6.4] and to the articles of Gee and Stevenhagen (see [6, 8, 16]).

Fix an imaginary quadratic field K and an order $\mathcal{O} = \mathbb{Z}[\theta]$ in K. Let K^{ab} be the maximal abelian extension of K. For each rational prime $p \in \mathbb{Z}$ we consider $K_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} K$ and $\mathcal{O}_p = \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}$. We will denote by $\hat{\mathbb{Z}} = \lim_{\leftarrow n} \mathbb{Z}/n\mathbb{Z}, \hat{\mathcal{O}} = \mathcal{O} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} = \lim_{\leftarrow n} \mathcal{O}/n\mathcal{O} = \hat{\mathbb{Z}}\theta + \hat{\mathbb{Z}}$ the profinite completions of the rings $\mathbb{Z}, \mathcal{O}$. Notice that $\hat{\mathcal{O}}^* = \prod_p \mathcal{O}_p^*$. We consider the group

$$J_K^f = \prod_p{}' K_p^*$$

of finite idèles of K. The restricted product is taken with respect to the subgroups $\mathcal{O}_p^* \subset K_p^*$. We denote by $[\sim, K]$ the Artin map on J_K^f. There is a map g_θ which connects the two short exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & \mathcal{O}^* \arrow[r] & \prod_p \mathcal{O}_p^* \arrow[r, "{[\sim,K]}"] \arrow[d, "g_\theta"] & \mathrm{Gal}(K^{\mathrm{ab}}/K(j(\theta))) \arrow[r] & 1, \\
1 \arrow[r] & \{\pm 1\} \arrow[r] & \mathrm{GL}_2(\hat{\mathbb{Z}}) \arrow[r] & \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1) \arrow[r] & 1
\end{tikzcd}$$

such that the image of $f(\theta)^x$ of a modular function f evaluated at θ under the Artin symbol of $x \in \mathcal{O}^*$ is given by

$$f(\theta)^x = f^{g_\theta(x^{-1})}(\theta). \tag{2.1}$$

The morphism g_θ is described as follows: Every idèle $x \in \hat{\mathcal{O}}^*$ corresponds to a 2×2 matrix representing the linear action of θ on $\hat{\mathbb{Z}}\theta + \hat{\mathbb{Z}}$ by multiplication. If $x^2 + Bx + C$

is the irreducible polynomial of θ then the matrix for $x = s\theta + t$ is computed to be

$$g_\theta(x) = \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix}.$$

Theorem 1. *Let $h \in \mathcal{F}$ which does not have a pole at θ and suppose that $\mathbb{Q}(j) \subset \mathbb{Q}(h)$. The function value $h(\theta)$ is a class invariant if and only if every element of the image $g_\theta\big(\prod_p \mathcal{O}_p^*\big) \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$ acts trivially on h.*

Proof. See [6, Corollary 3]. □

Now we will consider the non-class invariant case. We have the following tower of fields:

$$\begin{tikzcd} K^{\mathrm{ab}} \arrow[d, dash, "H_1"] \arrow[dd, dash, bend right=60, "H=\hat{\mathcal{O}}^*/\mathcal{O}^*"'] \\ K(h(\theta)) \arrow[d, dash] \\ K\big(j(\theta)\big) \end{tikzcd} \cdot$$

Consider the open subgroup

$$\mathrm{Stab}_{\mathbb{Q}(h)} = \{\alpha \in \mathrm{GL}_2(\hat{\mathbb{Z}}) : h^\alpha = h\}.$$

The preimage $g_\theta^{-1}(\mathrm{Stab}_{\mathbb{Q}(h)})$ contains $\mathcal{O}^* = \{\pm 1\}$ and $g_\theta^{-1}(\mathrm{Stab}_{\mathbb{Q}(h)}) \subset \prod_p \mathcal{O}_p^*$. Notice that $h(\theta)$ is a class invariant if and only if $g_\theta^{-1}(\mathrm{Stab}_{\mathbb{Q}(h)}) = \prod_p \mathcal{O}_p^*$. Let $H_1 = \mathrm{Gal}(K^{\mathrm{ab}}/K(h(\theta)))$. We can write H as a disjoint union of the cosets $H = \bigcup \sigma_i H_1$, and if $h(\theta)$ is not a class invariant then there is more than one coset.

Now we will write the Shimura reciprocity law in full generality taking into account the full automorphism group of the function field $\mathcal{F}$. We consider the following two short exact sequences, connected with morphism $g_\theta : J_K^f \to \mathrm{GL}_2(A_{\mathbb{Q}}^f)$:

$$\begin{tikzcd} 1 \arrow[r] & K^* \arrow[r] & J_K^f \arrow[r, "{[\sim,K]}"] \arrow[d, "g_\theta"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[r] & 1 \\ 1 \arrow[r] & \mathbb{Q}^* \arrow[r] & \mathrm{GL}_2(A_{\mathbb{Q}}^f) \arrow[r] & \mathrm{Aut}(\mathcal{F}) \arrow[r] & 1. \end{tikzcd} \tag{2.2}$$

The map g_θ is the $\mathbb{Q}$-linear extension of the map g_θ given in Eq. (2.1) which is a homomorphism $J_K^f \to \mathrm{GL}_2(A_{\mathbb{Q}}^f)$. The action of $z \in \mathrm{GL}_2(A_{\mathbb{Q}}^f)$ on $\mathcal{F}$ is given by writing $z = u\alpha$ where $u \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ and $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$. The group $\mathrm{GL}_2(\mathbb{Q})^+$ consists of rational 2×2 matrices with positive determinant and acts on $\mathbb{H}$ via linear fractional transformations. Then we define $f^{u\cdot\alpha} = (f^u)^\alpha$. For more details on this construction we refer to [16, p. 6].

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

The Shimura reciprocity theorem states the following.

Theorem 2. *For $h \in \mathcal{F}$ and $x \in J_K^f$ we have*

$$h(\theta)^{[x^{-1},K]} = h^{g_\theta(x)}(\theta).$$

The following proposition will be useful for us.

Proposition 3. *If $\mathcal{F}/\mathbb{Q}(h)$ is Galois then*

$$h(\theta)^x = h(\theta) \Leftrightarrow h^{g_\theta(x)} = h.$$

Proof. See [16, Eq. (3.5)]. $\square$

From now on we will focus on functions $h \in \mathcal{F}$ such that $\mathcal{F}/\mathbb{Q}(h)$ is Galois. Notice that if $\mathbb{Q}(j) \subset \mathbb{Q}(h)$ then $\mathcal{F}/\mathbb{Q}(h)$ is Galois since $\mathcal{F}/\mathbb{Q}(j)$ is.

We have the following tower of fields:

$$\begin{tikzcd}
K^{\mathrm{ab}} \arrow[d, dash, "H_1"] \arrow[dd, dash, bend right=60, "H"'] \arrow[ddd, dash, bend left=60, "G"] \\
K(h(\theta)) \arrow[d, dash] \\
K(j(\theta)) \arrow[d, dash, "\mathrm{Cl}(\mathcal{O})"'] \\
K
\end{tikzcd}$$

where $H = \mathrm{Gal}(K^{\mathrm{ab}}/K(j(\theta)))$, $G = \mathrm{Gal}(K^{\mathrm{ab}}/K)$, $H_1 = \mathrm{Gal}(K^{\mathrm{ab}}/K(h(\theta)))$ and $G/H \cong \mathrm{Cl}(\mathcal{O})$, where $\mathrm{Cl}(\mathcal{O})$ denotes the class group of the order $\mathcal{O}$. We now form the following short exact sequence:

$$1 \to \frac{H}{H_1} \to \frac{G}{H_1} \to \frac{G}{H} \to 1. \tag{2.3}$$

Notice that $H/H_1 \cong \mathrm{Gal}(K(h(\theta))/K(j(\theta)))$.

Suppose that $h(\theta)$ is an algebraic integer. The class group of $\mathcal{O}$ is identified with the set of primitive forms $[a, b, c]$ of discriminant D. We also set $\tau_{[a,b,c]} = \frac{-b+\sqrt{d}}{2a}$. Proposition 4 will provide us a method to compute its minimal polynomial in $\mathbb{Z}[x]$.

For every element $[a, b, c] \in \mathrm{Cl}(\mathcal{O}) = G/H$ we fix a representative $\sigma_{[a,b,c]} \in G$ such that $[a, b, c] = \sigma_{[a,b,c]}H$. Notice that the selection of the representative does not matter when one is acting on $K(j(\theta)) = (K^{\mathrm{ab}})^H$ since H acts trivially on $K(j(\theta))$.

The situation changes if we try to act with $\sigma_{[a,b,c]}$ on the field $K(h(\theta))$ which is the fixed field of H_1 with $H_1 < H$. The class $\sigma_{[a,b,c]}H$ gives rise to $[H : H_1]$ classes in G/H_1, namely $\sigma_{[a,b,c]}\sigma_i H_1$, where $\sigma_1, \ldots, \sigma_s$ are some coset representatives of H_1 in H and $s = [H : H_1]$. The action of the representative $\sigma_{[a,b,c]}\sigma_i = \sigma_i\sigma_{[a,b,c]}$ on

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

$K(h(\theta))$ is now well defined. Notice also that when $[a,b,c]$ runs over G/H and i runs over $1,\dots,s$ then $\sigma_i\sigma_{[a,b,c]}$ runs over G/H_1.

Proposition 4. *Assume that $h(\theta)\in\mathbb{R}$ and $h(\theta)$ is algebraic. Let H_1 be the subgroup of G that stabilizes the field $K(h(\theta))$ and let H be the subgroup corresponding to the ring class field $K(j(\theta))$ of K. We consider the elements $h(\theta)^{\sigma_i\sigma_{[a,b,c]}}$. The polynomial*

$$p_{h(\theta)} := \prod_{i=1}^{s} \prod_{[a,b,c]\in\mathrm{Cl}(\mathcal{O})} (x-(h(\theta)^{\sigma_i\sigma_{[a,b,c]}})) \tag{2.4}$$

is a polynomial in $\mathbb{Z}[x]$.

Proof. We have already observed that the product in Eq. (2.4) runs over all elements in $\mathrm{Gal}(K(h(\theta))/K(j(\theta)))$. We have the following tower of field extensions

$$\begin{tikzcd}
 & K(h(\theta)) \arrow[dl, dash, "H/H_1"'] \arrow[dr, dash, "G_1"] & \\
K(j(\theta)) \arrow[d, dash, "\mathrm{Cl}(\mathcal{O})"] \arrow[drr, dash, "G_2"] & & \mathbb{Q}(h(\theta)) \arrow[d, dash, "H/H_1"] \\
K \arrow[dr, dash, "\mathrm{Gal}(K/\mathbb{Q})"'] & & \mathbb{Q}(j(\theta)) \arrow[dl, dash, "\mathrm{Cl}(\mathcal{O})"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

where G_1, G_2 are lifts of $\mathrm{Gal}(K/\mathbb{Q})$. From the diagram above we deduce that $\mathrm{Gal}(\mathbb{Q}(h(\theta))/\mathbb{Q}) = \mathrm{Gal}(K(h(\theta))/K)$. This proves that the polynomial $p_{h(\theta)}$ defined in Eq. (2.4) is the defining polynomial of the extension $\mathbb{Q}(h(\theta))/\mathbb{Q}$. Moreover the coefficients of $p_{h(\theta)}$ are algebraic integers in $\mathbb{Q}$ therefore $p_{h(\theta)}\in\mathbb{Z}[x]$. $\square$

Remark 5. The assumption $h(\theta)\in\mathbb{R}$ is essential as one sees in Sec. 4, where we compute the minimal polynomial of the class invariant $\mathfrak{g}_2^6(\theta)$.

The above construction becomes practical if $h\in\mathcal{F}_N$ is a modular function of level N. Then the value $h(\theta)$ is known to be inside the ray class field modulo N and the action of $\hat{\mathcal{O}}^*$ can be computed in terms of a finite quotient $(\mathcal{O}/N\mathcal{O})^*$. Here it is important to assume also that $\mathbb{Q}(j)\subset\mathbb{Q}(h)$ so Proposition 3 is applicable. More precisely we can replace Eq. (2.2) with the exact sequence:

$$\begin{tikzcd}
\mathcal{O}^* \arrow[r] & (\mathcal{O}/N\mathcal{O})^* \arrow[r] \arrow[d, "\bar{g}_\theta"'] & \mathrm{Gal}\big(K(\mathcal{F}_N(\theta))/K(j(\theta))\big) \arrow[r] & 1 \\
\{\pm 1\} \arrow[r] & \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \arrow[r] & \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \arrow[r] & 1,
\end{tikzcd}$$

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

where we have considered the reduction of all rings and maps modulo N. The strategy for the computations is the following: compute generators $x_1, \ldots, x_k$ for the group $(\mathcal{O}/N\mathcal{O})^*$ and map them to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ using $\bar{g}_\theta$. If each matrix $g(x_i) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts trivially on h then $h(\theta)$ is a class invariant. If not we can consider the subgroup $A \subset \bar{g}_\theta((\mathcal{O}/N\mathcal{O})^*)$ that acts trivially on h. The Galois group of $K(h(\theta))/K(j(\theta))$ equals

$$\mathrm{Gal}(K(h(\theta)))/K(j(\theta)) = \frac{(\mathcal{O}/N\mathcal{O})^*/\mathcal{O}^*}{\bar{g}_\theta^{-1}(A)}.$$

We will now give an applicable approach to Proposition 4 by working modulo N. Following the article of Gee [6, Eq. 17] we give the next definition. This will allow us to compute the action of the images of generators of G_{72} on the modular functions of level 72.

Definition 6. Let $N \in \mathbb{N}$ and $[a, b, c]$ be a representative of the equivalence class of an element in the class group. Let p be a prime number and p^r be the maximum power of p that divides N. Assume that the discriminant $D = b^2 - 4ac \equiv 1 \pmod 4$. The following matrix definition is motivated by the explicit writing of the idèle that locally generates $[a, b, c]$ for all primes p, see [8, Sec. 4]. Define the matrix

$$A_{[a,b,c],p^r} = \begin{cases} \begin{pmatrix} a & \dfrac{b-1}{2} \\ 0 & 1 \end{pmatrix} & \text{if } p \nmid a, \\ \begin{pmatrix} \dfrac{-b-1}{2} & -c \\ 1 & 0 \end{pmatrix} & \text{if } p \mid a \text{ and } p \nmid c, \\ \begin{pmatrix} \dfrac{-b-1}{2} - a & \dfrac{1-b}{2} - c \\ 1 & -1 \end{pmatrix} & \text{if } p \mid a \text{ and } p \mid c. \end{cases}$$

The Chinese Remainder Theorem implies that

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{p \mid N} \mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}).$$

We define $A_{[a,b,c]}$ as the unique element in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that it is mapped to $A_{[a,b,c],p^r} \pmod{p^r}$ for all $p \mid N$. This matrix $A_{[a,b,c]}$ can be written uniquely as a product

$$A_{[a,b,c]} = B_{[a,b,c]} \begin{pmatrix} 1 & 0 \\ 0 & d_{[a,b,c]} \end{pmatrix}, \tag{2.5}$$

where $d_{[a,b,c]} = \det A_{[a,b,c]}$ and $B_{[a,b,c]}$ is a matrix with determinant 1. We will denote by $\sigma_{d_{[a,b,c]}}$ the automorphism of $\mathbb{Q}(\zeta_N)$ sending $\zeta_N \mapsto \zeta_N^{d_{[a,b,c]}}$.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Let $\lambda \in \mathbb{Q}(\zeta_N)$. Shimura reciprocity law gives us [6, Lemma 20] the action of $[a,b,c]$ on $\lambda h(\theta)$ for $\theta = 1/2 + i\sqrt{n}/2$:

$$(\lambda h(\theta))^{[a,-b,c]} = \lambda^{\sigma_{d_{[a,b,c]}}} h\left(\frac{\alpha_{[a,b,c]}\tau_{[a,b,c]} + \beta_{[a,b,c]}}{\gamma_{[a,b,c]}\tau_{[a,b,c]} + \delta_{[a,b,c]}}\right)^{\sigma_{d_{[a,b,c]}}},$$

where $\begin{pmatrix} \alpha_{[a,b,c]} & \beta_{[a,b,c]} \\ \gamma_{[a,b,c]} & \delta_{[a,b,c]} \end{pmatrix} = A_{[a,b,c]}$ and $\tau_{[a,b,c]}$ is the (complex) root of $az^2 + bz + c$ with positive imaginary part.

Theorem 7. *Let $\mathcal{O} = \mathbb{Z}[\theta]$ be an order of the imaginary quadratic field K, and assume that $x^2 + Bx + C$ is the minimal polynomial of θ. Let $N > 1$ be a natural number, $x_1, \ldots, x_r$ be generators of the abelian group $(\mathcal{O}/N\mathcal{O})^*$ and $\alpha_i + \beta_i\theta \in \mathcal{O}$ be a representative of the class of the generator x_i. For each representative we consider the matrix:*

$$A_i := \begin{pmatrix} \alpha_i - B\beta_i & -C\beta_i \\ \beta_i & \alpha_i \end{pmatrix}.$$

If f is a modular function of level N and if for all matrices A_i it holds that

$$f(\theta) = f^{A_i}(\theta), \quad \text{and} \quad \mathbb{Q}(j) \subset \mathbb{Q}(f) \tag{2.6}$$

then $f(\theta)$ is a class invariant.

Proof. See [6, Corollary 4] for the maximal order case and [16, Sec. 5] for the general case. □

3. Ramanujan Invariants

We would like to find the minimal polynomial in $\mathbb{Z}[x]$ of the Ramanujan invariants $H_n = 27/t_n^{12}$ for values $n \equiv 19 \pmod{24}$. In [9] the authors introduced the modular functions $R, R_1, \ldots, R_5$ of level $N = 72$ in order to study t_n. Stevenhagen pointed to us that the functions R_i can be expressed in terms of the generalized Weber functions $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$ defined in the work of Gee in [7, p. 73] as

$$\mathfrak{g}_0(\tau) = \frac{\eta\left(\frac{\tau}{3}\right)}{\eta(\tau)}, \quad \mathfrak{g}_1(\tau) = \zeta_{24}^{-1}\frac{\eta\left(\frac{\tau+1}{3}\right)}{\eta(\tau)},$$

$$\mathfrak{g}_2(\tau) = \frac{\eta\left(\frac{\tau+2}{3}\right)}{\eta(\tau)}, \quad \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)},$$

where η denotes the Dedekind eta function:

$$\eta(\tau) = e^{2\pi i\tau/24}\prod_{n\geq 1}(1-q^n) \quad \tau \in \mathbb{H}, q = e^{2\pi i\tau}.$$

Proposition 8. *The functions* $\mathfrak{g}_i^{12}$ *satisfy the polynomial*:

$$X^4 + 36X^3 + 270X^2 + (756 - j)X + 3^6 = 0.$$

In particular $\mathbb{Q}(h) \subset \mathbb{Q}(\mathfrak{g}_i)$ *and* $\mathcal{F}/\mathbb{Q}(\mathfrak{g}_i)$ *is Galois.*

Proof. This is a classical result see [7, Eq. 5, p. 73; 18, p. 255]. □

Here will need only the $R_2(\tau)$ and $R_4(\tau)$ defined by

$$R_2(\tau) = \frac{\eta(3\tau)\eta(\tau/3 + 2/3)}{\eta^2(\tau)} = \sqrt{3}^{-1}\mathfrak{g}_2(\tau)\mathfrak{g}_3(\tau), \tag{3.1}$$

$$R_4(\tau) = \frac{\eta(\tau/3)\eta(\tau/3 + 1/3)}{\eta^2(\tau)} = \zeta_{24}\mathfrak{g}_0(\tau)\mathfrak{g}_1(\tau). \tag{3.2}$$

The six modular functions R_i defined in [9] correspond to the $\binom{4}{2} = 6$ different products $\mathfrak{g}_i\mathfrak{g}_j$ we can make from $\mathfrak{g}_i$, $i = 0, \ldots, 3$.

The Ramanujan value can be expressed in terms of the above modular functions as

$$t_n = \sqrt{3}R_2\left(-\frac{1}{2} + i\frac{\sqrt{n}}{2}\right) = (\mathfrak{g}_2\mathfrak{g}_3)\left(-\frac{1}{2} + i\frac{\sqrt{n}}{2}\right). \tag{3.3}$$

Notice also that $\sqrt{3} = \zeta_{72}^6 - \zeta_{72}^{30}$. The Ramanujan invariants for $D \equiv 5 \pmod{24}$ are

$$H_n := \frac{27}{t_n^{12}}$$

and we also define the values

$$A_n := H_n + \frac{1}{H_n} = \frac{27}{t_n^{12}} + \frac{t_n^{12}}{27}.$$

Denote by S the involution $\tau \mapsto -\frac{1}{\tau}$ and by T the map $\tau \mapsto \tau + 1$. The elements S, T generate the group $\mathrm{SL}(2, \mathbb{Z})$. We will use the following lemma.

Lemma 9. *The action of* $S : z \mapsto -1/z$ *on* $\mathfrak{g}_i$ *is given by*

$$(\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3)\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & \zeta_{72}^6 & 0 \\ 0 & \zeta_{72}^{-6} & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

and the action of $T : z \mapsto z + 1$ *on* $\mathfrak{g}_i$ *is given by*

$$(\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3)\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & \zeta_{72}^{-6} & 0 & 0 \\ 0 & 0 & 0 & \zeta_{72}^6 \end{pmatrix}.$$

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

The action of σ_d on $\mathfrak{g}_i$ is given in terms of the following matrix

$$(\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \zeta_{72}^{-2d+2} & 0 & 0 \\ 0 & 0 & \zeta_{72}^{2d-2} & 0 \\ 0 & 0 & 0 & \frac{\zeta_{72}^{6d}-\zeta_{72}^{30d}}{\zeta_{72}^{6}-\zeta_{72}^{30}} \end{pmatrix} \quad \textit{if } d \equiv 1 \pmod 3$$

and

$$(\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & \zeta_{72}^{2d+2} & 0 \\ 0 & \zeta_{72}^{-2d-2} & 0 & 0 \\ 0 & 0 & 0 & \frac{\zeta_{72}^{6d}-\zeta_{72}^{30d}}{\zeta_{72}^{6}-\zeta_{72}^{30}} \end{pmatrix} \quad \textit{if } d \equiv 2 \pmod 3.$$

Proof. The action of S, T follows by using the transformation formulas of the η-function [15]:

$$\eta(\tau+1) = e^{2\pi i\tau/24}\eta(\tau) \quad \text{and} \quad \eta\left(-\frac{1}{\tau}\right) = \sqrt{-i\tau}\,\eta(\tau).$$

For the action of σ_d observe for example that

$$\begin{aligned}\eta\left(\frac{\tau}{3}+\frac{1}{3}\right) &= \exp\left(\frac{2\pi i}{24}\left(\frac{\tau}{3}+\frac{1}{3}\right)\right)\sum_{\nu=0}^{\infty} a_\nu \exp\left(\frac{2\pi i\nu}{3}\tau + \frac{2\pi i\nu}{3}\right) \\ &= \exp\left(\frac{2\pi i}{24}\frac{\tau}{3}\right)\zeta_{72}\sum_{\nu=0}^{\infty}\zeta_3^{\nu} a_\nu \exp\left(\frac{2\pi i\nu}{3}\tau\right).\end{aligned}$$

The element $\sigma_d : \zeta_{72} \mapsto \zeta_{72}^d$ sends ζ_3^ν to $\zeta_3^{d\nu} = \zeta_3$ if $d \equiv 1 \pmod 3$ and to $\zeta_3^{2\nu}$ if $d \equiv 2 \pmod 3$. Therefore

$$\sigma_d(\mathfrak{g}_1(\tau)) = \sigma_d\left(\zeta_{24}^{-1}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)}\right) = \begin{cases}\zeta_{72}^{-2d+2}\mathfrak{g}_1 & \text{if } d \equiv 1 \pmod 3, \\ \zeta_{72}^{-2d-2}\mathfrak{g}_2 & \text{if } d \equiv 2 \pmod 3.\end{cases}$$ □

Remark 10. We have a representation

$$\rho : \mathrm{SL}(2,\mathbb{Z}) \to \langle \mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3\rangle_{\mathbb{R}} = V.$$

This representation gives rise to the representation $\mathrm{Sym}^2 V$, where the space $\mathrm{Sym}^2 V$ has dimension $\binom{4}{2} = 6$ and it is generated by the elements $\mathfrak{g}_i\mathfrak{g}_j$, $1 \le i < j \le 4$. The representation $\mathrm{Sym}^2 V$ was an alternative way to express the action given in [9] in terms of the modular functions R_i.

We first study the group $(\mathcal{O}/72\mathcal{O})^*$ for the values $n = 19, 43, 67$. Using Chinese Remainder Theorem we compute first that

$$\left(\frac{\mathcal{O}}{72\mathcal{O}}\right)^* \cong \left(\frac{\mathcal{O}}{9\mathcal{O}}\right)^* \times \left(\frac{\mathcal{O}}{8\mathcal{O}}\right)^*.$$

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Notice that the assumptions we put force $2\mathcal{O}, 3\mathcal{O}$ to be prime ideals. The structure of the group $\left(\frac{\mathcal{O}}{P^k\mathcal{O}}\right)^*$ for a prime ideal of $\mathcal{O}$ is given by the following.

Theorem 11. *Let P be a prime ideal of $\mathcal{O}$ of inertia degree f over the field of rationals, i.e. if p is the generator of the principal ideal $P \cap \mathbb{Z}$ then $N(P) = p^f$ and assume that the ramification index $e(P/p) = 1$. The group $\left(\frac{\mathcal{O}}{P^k\mathcal{O}}\right)^*$ is isomorphic to the direct product $\left(\frac{\mathcal{O}}{P\mathcal{O}}\right)^* \times \frac{1+P}{1+P^k}$. The group $\left(\frac{\mathcal{O}}{P\mathcal{O}}\right)^*$ is cyclic of order $p^f - 1$. If $p \geq \min\{3, k\}$ then the group $\frac{1+P}{1+P^k}$ is isomorphic to $\left(\frac{\mathbb{Z}}{p^{k-1}\mathbb{Z}}\right)^f$. If $p = 2$ and $k = 3$ then $\frac{1+P}{1+P^3}$ is isomorphic to $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2 \times \left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)^{f-1}$.*

Proof. The group $\left(\frac{\mathcal{O}}{P^k\mathcal{O}}\right)^*$ is isomorphic to the direct product $\left(\frac{\mathcal{O}}{P\mathcal{O}}\right)^* \times \frac{1+P}{1+P^k}$ by [5, Proposition 4.2.4]. For $e(P/p) = 1$ and $p \geq \min\{3, k\}$ the P-adic logarithmic function defines an isomorphism of the multiplicative group $\frac{1+P}{1+P^k}$ to the additive group P/P^k which in turn is isomorphic to $\mathcal{O}/P^{k-1}$ by [5, Lemma 4.2.9]. The condition $p \geq \min\{3, k\}$ is put so that the logarithmic function converges. By [5, Theorem 4.2.10] we have

$$\frac{\mathcal{O}}{P^{k-1}} \cong \left(\frac{\mathbb{Z}}{p^q\mathbb{Z}}\right)^{(r+1)f} \times \left(\frac{\mathbb{Z}}{p^{q-1}\mathbb{Z}}\right)^{(e-r-1)f}$$

where $k + e - 2 = eq + r$, $0 \leq r < e$. If $e = 1$ then the last formula becomes:

$$\frac{\mathcal{O}}{P^{k-1}} \cong \left(\frac{\mathbb{Z}}{p^{k-1}\mathbb{Z}}\right)^f.$$

The case $p = 2$ and $k = 3$ is studied in [5, Proposition 4.2.12]. $\square$

By applying Theorem 11 we find the structure of the multiplicative groups

$$\left(\frac{\mathcal{O}}{9\mathcal{O}}\right)^* \cong \frac{\mathbb{Z}}{8\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \cong \frac{\mathbb{Z}}{24\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$$

and

$$\left(\frac{\mathcal{O}}{8\mathcal{O}}\right)^* \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2 \times \frac{\mathbb{Z}}{4\mathbb{Z}} \cong \frac{\mathbb{Z}}{12\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2.$$

For finding the generators of these groups one can use the P-adic logarithmic function in order to pass from the multiplicative group $\frac{1+P}{1+P^k}$ to the additive group $\mathcal{O}/P^{k-1}\mathcal{O}$. This method does work only for large primes (so that the logarithmic function is convergent) and not for the case $p = 2$, $k = 3$.

In order to find the generators we proceed as follows: We exhaust all units in $\mathcal{O}/9\mathcal{O}$ until we find one unit U_1 of order 24 then we remove this unit and all its powers from the set of possible units and we try again in order to find a unit U_2 of order 3. For the units in $\mathcal{O}/8\mathcal{O}$ we work similarly. We first find a unit V_1 of maximal order 12 remove all its powers from the set of units and we try again in order to find a unit V_2 of order 2. We remove all products of powers of U_1 and U_2 and then

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

we search on the remaining units for the third generator V_3. Finally we lift these units to units of the ring $\mathcal{O}/72\mathcal{O}$ using the Chinese Remainder Theorem. This way we arrived to the following generators of the group $(\mathcal{O}/72\mathcal{O})^*$: $5\theta+7$, $6\theta+7$, $7\theta+7$, $4\theta+7$, $4\theta+1$. The orders of the generators of the group $(\mathcal{O}/72\mathcal{O})^*$ are given in the following table:

Generator	$5\theta+7$	$6\theta+7$	$7\theta+7$	$4\theta+7$	$4\theta+1$
Order	24	3	12	2	2

These generators will be mapped to matrices A_i defined in Theorem 7.

For example, the generator $5\theta+7$ in $(\mathcal{O}/9\mathcal{O})^*$ corresponds to the matrix

$$\begin{pmatrix} 3 & 8 \\ 5 & 16 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 8 \end{pmatrix},$$

where $M = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$ is a matrix of determinant $1 \pmod 9$. Let

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The matrix M can be decomposed according to [8] as $\bar{T}_9^8 \bar{S}_9 \bar{T}_9^5 \bar{S}_9 \bar{T}_9^6$ where

$$\bar{S}_9 = T^{-1}ST^{-65}ST^{-1}ST^{1096} \quad \text{and} \quad \bar{T}_9 = T^{-9}$$

according to [9]. The action of the generators on the elements $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$ is computed by magma and it is given in Table 1.

Lemma 12. *The quantities $\mathfrak{g}_i(\theta)^6$ are in the ray class field of conductor* 3.

Proof. There is the following diagram with exact rows for every N (here we will use the values $N = 72, 3$:

$$\begin{tikzcd}
\mathcal{O}^* \arrow[r] & (\mathcal{O}/N\mathcal{O})^* \arrow[r] \arrow[d, "\bar{g}_\theta"] & \mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}}) \arrow[r] & 1 \\
\{\pm 1\} \arrow[r] & \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \arrow[r] & \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \arrow[r] & 1,
\end{tikzcd}$$

where $H_{N,\mathcal{O}}$ denotes the ray class field of conductor N. The epimorphism of the upper row is induced by the Artin map and allows us to see elements in $(\mathcal{O}/N\mathcal{O})^*$ as elements in $\mathrm{Gal}(H_{N,\mathcal{O}}/H_{\mathcal{O}})$.

Table 1. Orders and generators of the group $(\mathcal{O}/72\mathcal{O})^*$.

	$5\theta+7$	$6\theta+7$	$7\theta+7$	$4\theta+7$	$4\theta+1$
$\mathfrak{g}_0$	$(-\zeta_{72}^{18}+\zeta_{72}^{6})\mathfrak{g}_2$	$\zeta_3\mathfrak{g}_0$	$\mathfrak{g}_0$	$-\mathfrak{g}_0$	$\mathfrak{g}_0$
$\mathfrak{g}_1$	$\zeta_{72}^{12}\mathfrak{g}_3$	$\zeta_3\mathfrak{g}_1$	$-\mathfrak{g}_1$	$-\mathfrak{g}_1$	$\mathfrak{g}_1$
$\mathfrak{g}_2$	$-\mathfrak{g}_1$	$-\zeta_{72}^{12}\mathfrak{g}_2$	$-\mathfrak{g}_2$	$-\mathfrak{g}_2$	$\mathfrak{g}_2$
$\mathfrak{g}_3$	$(-\zeta_{72}^{18}+\zeta_{72}^{6})\mathfrak{g}_0$	$-\zeta_{72}^{12}\mathfrak{g}_3$	$-\mathfrak{g}_3$	$-\mathfrak{g}_3$	$\mathfrak{g}_3$

The ray class field $H_{3,\mathcal{O}}$ of conductor 3 is an extension of degree 4 of the ring class field, as one computes looking at $(\mathcal{O}/3\mathcal{O})^*/\mathcal{O}^*$. Indeed, the group $(\mathcal{O}/3\mathcal{O})^*$ is isomorphic to a cyclic group of order 8 by Theorem 11 and by taking the quotient of $\mathcal{O}^* = \{\pm 1\}$ we arrive at a group of order 4.

The element $5\theta + 7$ generates a subgroup of order 24 in $(\mathcal{O}/72\mathcal{O})^*$. This means that the ray class field of conductor 3 is the fixed field of $\langle (5\theta+7)^4 \rangle$ and all other generators $6\theta + 7, 7\theta + 7, 4\theta + 7, 4\theta + 1$.

We compute that the action of $(5\theta + 7)^4 = 3\theta + 8$ on $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$ is given by

$$(\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3) \mapsto \left((-\zeta_{72}^{12} + 1)\mathfrak{g}_0, (-\zeta_{72}^{12} + 1)\mathfrak{g}_1, \zeta_{72}^{12}\mathfrak{g}_2, \zeta_{72}^{12}\mathfrak{g}_3 \right).$$

Since $\zeta_{72}^{12}, (\zeta_{72}^{12} - 1)$ are sixth roots of unity we see that $(5\theta + 7)^4$, indeed leaves $\mathfrak{g}_0^6, \mathfrak{g}_1^6, \mathfrak{g}_2^6, \mathfrak{g}_3^6$ invariant. On the other hand, looking at Table 1 we see that all other generators leave also $\mathfrak{g}_0^6, \mathfrak{g}_1^6, \mathfrak{g}_2^6, \mathfrak{g}_3^6$ invariant.

Notice that the Galois group $\mathrm{Gal}(H_{n,\mathcal{O}}/K)$ is cyclic of order 4 generated by $5\theta + 7$ and the action is given by

$$(\mathfrak{g}_0^6, \mathfrak{g}_1^6, \mathfrak{g}_2^6, \mathfrak{g}_3^6) \mapsto (-\mathfrak{g}_2^6, \mathfrak{g}_3^6, -\mathfrak{g}_1^6, -\mathfrak{g}_0^6). \qquad \square$$

Remark 13. Notice that we have a polynomial action of the permutation group $\langle (0,2,1,3) \rangle$[a] on the polynomial ring $\mathbb{Q}[\mathfrak{g}_0^{12}, \mathfrak{g}_1^{12}, \mathfrak{g}_2^{12}, \mathfrak{g}_3^{12}]$. The ring of invariants of this action can be computed to be the polynomial ring generated by the polynomials

$$\mathfrak{g}_0^{12} + \mathfrak{g}_1^{12} + \mathfrak{g}_2^{12} + \mathfrak{g}_3^{12}, \quad \mathfrak{g}_0^{24} + \mathfrak{g}_1^{24} + \mathfrak{g}_2^{24} + \mathfrak{g}_3^{24},$$
$$\mathfrak{g}_0^{12}\mathfrak{g}_1^{12} + \mathfrak{g}_2^{12}\mathfrak{g}_3^{12}, \quad \mathfrak{g}_0^{48} + \mathfrak{g}_1^{48} + \mathfrak{g}_2^{48} + \mathfrak{g}_3^{48}.$$

Of course $\mathfrak{g}_0^{12} + \mathfrak{g}_1^{12} + \mathfrak{g}_2^{12} + \mathfrak{g}_3^{12} = -36$ is an invariant of the linear action but not an interesting one. All these (and their combinations) will give class invariants. Notice that the class invariant A_n introduced later in this paper comes from the third one $\mathfrak{g}_0^{12}\mathfrak{g}_1^{12} + \mathfrak{g}_2^{12}\mathfrak{g}_3^{12}$.

Remark 14. Every polynomial expression given in Remark 13 gives rise to a class invariant. What are the relations of these class invariants? Set $Y_i = \mathfrak{g}_i^{12}$. We know that Y_i satisfy equation

$$Y_i^4 + 36Y_i^3 + 270Y_i^2 + (756 - j)Y_i + 3^6 = 0, \tag{3.4}$$

by Proposition 8. The first invariant given in Remark 13 is just 36. We then have

$$36^2 = \left(\sum_{i=0}^{3} Y_i \right)^2 = \left(\sum_{i=0}^{3} Y_i^2 \right) + 2 \sum_{0 \le i < j \le 3} Y_i Y_j = \left(\sum_{i=0}^{3} Y_i^2 \right) - 540.$$

[a]Here in order to be compatible with the enumeration of $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$ we allow 0 as a number in the permutations.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Therefore,

$$\sum_{i=0}^{3} Y_i^2 = 36^2 + 540 = 1836.$$

We compute that

$$\begin{aligned} 36^3 = \left(\sum_{i=0}^{3} Y_i\right)^3 &= \sum_{i=0}^{3} Y_i^3 + 6\sum_{i,j,k} Y_i Y_j Y_k + 3\sum_{i\neq j} Y_i Y_j^2 \\ &= \sum_{i=0}^{3} Y_i^3 + 6(756 - j) + 3\sum_{i\neq j} Y_i Y_j^2. \end{aligned} \tag{3.5}$$

We now compute

$$1836 \cdot 36 = \left(\sum_{i=0}^{3} Y_i\right)\left(\sum_{j=0}^{3} Y_i^2\right) = \sum_{i=0}^{3} Y_i^3 + \sum_{i\neq j} Y_i Y_j^2. \tag{3.6}$$

By combining Eqs. (3.5) and (3.6) we obtain

$$2\sum_{i=0}^{3} Y_i^3 = 151632 + 6(756 - j).$$

Finally, we compute that the last invariant given in Remark 13 is given by Eq. (3.4)

$$\sum_{i=0}^{3} Y_i^4 = -36\sum_{i=0}^{3} Y_i^3 - 270\sum_{i=0}^{3} Y_i^2 - (756 - j)\sum_{i=0}^{3} Y_i - 3^6.$$

This means that the invariants of Remark 13 are either constant or linear combinations of j (and these would give polynomials with the same growth as the Hilbert polynomials) and $Y_0Y_1 + Y_2Y_3$ which gives by evaluation at θ the A_n class invariants.

Remark 15. Notice that Eq. (3.4) allows us to find the minimal polynomials (over the ring class field) of the quantities $Z_i := \mathfrak{g}_i(\theta)^6$, just by replacing Y_i by Z_i^2.

Remark 16. Notice that using only powers of the $\mathfrak{g}_i$ modular functions we can only construct an extension of the ring class field of order 4. The Ramanujan invariants H_n allow us to construct a quadratic extension of the ring class field.

We return now to the study of Ramanujan invariants. Using magma and the above computations we compute that $5\theta + 7$ sends $(1/R_2)^{12}$ to $-3^6/R_4^{12}$. Therefore H_n is not a class invariant. Similarly we compute that all other generators of $\left(\frac{\mathcal{O}}{72\mathcal{O}}\right)^*$ act trivially on $(1/R_2)^{12}$. The field generated by the class invariant H_n is a quadratic extension of the ring class field of K.

On the other hand the above computation allows us to compute the minimal polynomial $p_n \in \mathbb{Z}[x]$ of $H(n)$ by using the formula

$$p_n(x) = \prod_{[a,b,c]\in \mathrm{Cl}(\mathcal{O})} \left(x - 3^{-3}R_2(\tau_0)^{-12[a,-b,c]}\right)\left(x + 3^3 R_4(\tau_0)^{-12[a,-b,c]}\right), \tag{3.7}$$

Table 2. Polynomials p_n for $19 \leq n \leq 451$, $n \equiv 19 \pmod{24}$.

n	C.N.	$p_n(x)$
19	1	$x^2 - 302x + 1$
43	1	$x^2 - 33710x + 1$
67	1	$x^2 - 1030190x + 1$
91	2	$x^4 - 17590492x^3 + 148475718x^2 + -17590492x + 1$
115	2	$x^4 - 210267100x^3 + 424646982x^2 - 210267100x + 1$
139	3	$x^6 - 1960891530x^5 - 13943617329x^4 - 30005622092x^3 - 13943617329x^2$ $- 1960891530x + 1$
163	1	$x^2 - 15185259950x + 1$
187	2	$x^4 - 101627312860x^3 + 1102664076102x^2 - 101627312860x + 1$
211	3	$x^6 - 604100444298x^5 + 20137792248015x^4 - 414952590867788x^3$ $+ 20137792248015x^2 - 604100444298x + 1$
235	2	$x^4 - 3253104234460x^3 + 47263043424582x^2 - 3253104234460x + 1$
259	4	$x^8 - 16106786824376x^7 - 810131323637348x^6 - 9925794993033992x^5$ $+ 26425093196592454x^4 - 9925794993033992x^3 - 810131323637348x^2$ $- 16106786824376x + 1$
283	3	$x^6 - 74167114012170x^5 - 119654555118897x^4 - 3009681130315340x^3$ $- 119654555118897x^2 - 74167114012170x + 1$
307	3	$x^6 - 320508447128970x^5 - 1963936794491697x^4 - 5740503875332940x^3$ $- 1963936794491697x^2 - 320508447128970x + 1$
331	3	$x^6 - 1309395837485706x^5 + 113317118488006863x^4 - 115566485199414254847x^3$ $+ 113317118488006863x^2 - 1309395837485706x + 1$
355	4	$x^8 - 5087640031882040x^7 + 583328538578918044x^6 - 16479665770932342920x^5$ $+ 172809183517820572486x^4 - 16479665770932342920x^3$ $+ 583328538578918044x^2 - 5087640031882040x + 1$
379	3	$x^6 - 18895199824010634x^5 - 4124999225954564913x^4 - 27450136968814231022 0x^3$ $- 4124999225954564913x^2 - 18895199824010634x + 1$
403	2	$x^4 - 67361590779141340x^3 + 361802623368357702x^2 - 67361590779141340x + 1$
427	2	$x^4 - 231347688320676700x^3 + 2519902537964728902x^2 - 231347688320676700x + 1$
451	6	$x^{12} - 767819046799630740x^{11} + 161913605740919729922x^{10}$ $- 6645802964147706691 1812x^9 - 1654687781430584516238609x^8$ $- 338755376410852686511117096x^7$ $+ 818792581063463562471434 52x^6 - 338755376410852686511117096x^5$ $- 1654687781430584516238609x^4 - 66458029641477066911812x^3$ $+ 161913605740919729922x^2 - 767819046799630740x + 1$

with $\tau_0 = \frac{-1+i\sqrt{n}}{2}$. The results of these computations for some values $n = 19 + 24i$, $i = 0, \ldots, 18$, are shown in Table 2. We have used gp-pari [12] in order to compute them. We will now prove some properties for the minimal polynomials. We will need the following lemma.

Lemma 17. *The following identity holds*:

$$(R_2(\tau)R_4(\tau))^{12} = -1.$$

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Proof. Gee in [7, p. 73] observes that $\mathfrak{g}_0\mathfrak{g}_1\mathfrak{g}_2\mathfrak{g}_3 = \sqrt{3}$. The result follows by Eqs. (3.1) and (3.2). □

Lemma 18. *Consider a monic polynomial $f(x) = x^n + \sum_{\nu=0}^{n-1} a_\nu x^\nu$, with n even. Consider the set of roots $\Sigma = \{\rho_1, \ldots, \rho_n\}$ of f and assume that f has no multiple roots. If the transformation $x \mapsto 1/x$ sends the above defined set of roots Σ to Σ then $a_0 = 1$ and $a_\nu = a_{n-\nu}$.*

Proof. Write $f = \prod_{i=1}^{n}(x - \rho_i)$. By the assumption all roots $\rho_i \neq 0$. The result follows from the fact that the "reverse polynomial" $x^n f(1/x)$ is the polynomial $\prod_{i=1}^{n}(1 - \rho_i X)$ having the reciprocals of ρ_i as roots. □

Proposition 19. *The minimal polynomials $p_n(x) = x^{2h} + \sum_{\nu=0}^{2h-1} a_\nu x^\nu$ of $H(n)$ are palindromic, i.e. $a_\nu = a_{2h-\nu}$. The constant coefficient a_0 equals* 1.

Proof. From Eq. (3.7) we have that whenever

$$H(n)^{[a,-b,c]} = 3^{-3} R_2(\tau_0)^{-12[a,-b,c]}$$

is a root then $-3^3 R_4(\tau_0)^{-12[a,-b,c]}$ is a root. But Lemma 17 implies that

$$-3^3 R_4(\tau_0)^{-12[a,-b,c]} = 3^{-3} R_2^{12[a,-b,c]} = 1/H_n.$$

The desired result now follows by Lemma 18. □

Corollary 20. *The values $H(n)$ are real units.*

Proof. This is clear since $H(n)$ is real and the product of all roots of p_n is $a_0 = 1$. □

Corollary 21. *The polynomials $p_n(x)$ have the following simplified form*:

$$p_n(x) = \prod_{[a,b,c]\in \mathrm{Cl}(\mathcal{O})} (x - 3^{-3} R_2(\tau_0)^{-12[a,-b,c]})(x - 3^3 R_2(\tau_0)^{12[a,-b,c]}).$$

We have seen that H_n is not a class invariant. But the quantity $A_n = H_n + \frac{1}{H_n}$ is a class invariant as we can verify using Theorem 7. This new invariant is not a unit anymore.

The minimal polynomial $q_n \in \mathbb{Z}[x]$ of A_n is given by

$$q_n(x) = \prod_{[a,b,c]\in \mathrm{Cl}(\mathcal{O})} (x - 3^{-3} R_2(\tau_0)^{-12[a,-b,c]} - 3^3 R_2(\tau_0)^{12[a,-b,c]}).$$

In Table 3 we give minimal polynomials q_n for $19 \leq n \leq 451$, $n \equiv 19 \pmod{24}$.

Observe that if $p_n = \sum_{\nu=0}^{2h} a_\nu x^\nu$ and $q_n = \sum_{\nu=0}^{h} b_\nu x^\nu$ then $b_\nu = a_{h+\nu}$ as one can prove using the Vieta formulæ.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Table 3. Polynomials q_n for $19 \le n \le 451$, $n \equiv 19 \pmod{24}$.

n	C.N.	$p_n(x)$
19	1	$x - 302$
43	1	$x - 33710$
67	1	$x - 1030190x$
91	2	$x^2 - 17590492x + 148475718$
115	2	$x^2 - 210267100x + 424646982$
139	3	$x^3 - 1960891530x^2 - 13943617329x - 30005622092$
163	1	$x - 15185259950$
187	2	$x^2 - 101627312860x + 1102664076102$
211	3	$x^3 - 604100444298x^2 + 20137792248015x - 414952590867788$
235	2	$x^2 - 3253104234460x + 47263043424582$
259	4	$x^4 - 16106786824376x^3 - 810131323637348x^2 - 9925794993033992x$ $+ 26425093196592454$
283	3	$x^3 - 74167114012170x^2 - 119654555118897x - 3009681130315340$
307	3	$x^3 - 320508447128970x^2 - 1963936794491697x - 5740503875332940$
331	3	$x^3 - 1309395837485706x^2 + 113317118488006863x - 115566485199414254847$
355	4	$x^4 - 5087640031882040x^3 + 583328538578918044x^2 - 1647966577093234292 0x$ $+ 1728091835178205724 86$
379	3	$x^3 - 18895199824010634x^2 - 4124999225954564913x - 274501369688142310220x^3$
403	2	$x^2 - 67361590779141340x + 361802623368357702$
427	2	$x^2 - 231347688320676700x + 2519902537964728902$
451	6	$x^6 - 767819046799630740x^5 + 161913605740919729922x^4$ $- 6645802964147706691 1812x^3 - 1654687781430584516238609x^2$ $- 33875537641085268651117096x + 81879258106346356247143452$

3.1. *Some unit computations*

Professor Stevenhagen proposed to us the study of the following situation: Consider the field $R_n := \mathbb{Q}(H_n) \subset \mathbb{R}$. The field R_n is an abelian extension of degree $2h$ of $\mathbb{Q}$ where h is the class number of the order $\mathbb{Z}[\theta_n]$. If $h = 1$, i.e. when $n = 19, 43, 67, 163$ then R_n is a real quadratic extension of $\mathbb{Q}$ and we can verify using magma that H_n is a fundamental unit.

The field R_n has $\mathbb{Q}(\sqrt{3n})$ as a subfield and we might ask if $\mathrm{N}_{R_n/\mathbb{Q}(\sqrt{3n})}H_n$ is a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{3n})$. Using magma [4], we compute that this is not always the case. In the following table we give the index of the subgroup generated by $\mathrm{N}_{R_n/\mathbb{Q}(\sqrt{3n})}H_n$ inside the group generated by the fundamental unit:

N	19	43	67	91	115	139	163	187	211	235
Index	1	1	1	2	2	1	1	2	1	2

N	259	283	307	331	355	379	403	427	451	475
Index	4	1	1	3	2	1	2	2	2	8

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

The authors could not find an obvious pattern for the behavior of the index. Professor Antoniadis pointed to us the following pattern: If the index is one then N is prime but not vice versa since 331 gives index 3. We have checked that this is correct for all values of $N < 1000$.

4. Computing Class Invariants for the 3 (mod 24) Case

In this case the prime 2 remains inert in $\mathcal{O}$ while 3 ramifies. We compute first the structure of the group $(\mathcal{O}/72\mathcal{O})^*$. Modulo 72 we have the following values $n = 3, 27, 51$ that are equivalent to 3 (mod 24). The structure of the group $(\mathcal{O}/72\mathcal{O})^*$ is computed to be the following:

n	$(\mathcal{O}/9\mathcal{O})^*$	$(\mathcal{O}/8\mathcal{O})^*$
3	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
27	$\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
51	$\mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

The actions of the generators τ_i of each direct cyclic summand on the elements $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$ for each case is computed to be:

$\boldsymbol{n = 3}$ $(\mathrm{mod}\,\mathbf{72})$

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
$\tau(\mathfrak{g}_0)$	$\mathfrak{g}_0$	$-\mathfrak{g}_0$	$\mathfrak{g}_0$	$(-\zeta^{18}+\zeta^6)\mathfrak{g}_1$	$-\zeta^{12}\mathfrak{g}_0$	$(\zeta^{12}-1)\mathfrak{g}_0$
$\tau(\mathfrak{g}_1)$	$-\mathfrak{g}_1$	$-\mathfrak{g}_1$	$\mathfrak{g}_1$	$(-\zeta^{12}+1)\mathfrak{g}_3$	$-\zeta^{12}\mathfrak{g}_1$	$-\zeta^{12}\mathfrak{g}_1$
$\tau(\mathfrak{g}_2)$	$-\mathfrak{g}_2$	$-\mathfrak{g}_2$	$\mathfrak{g}_2$	$-\mathfrak{g}_2$	$\mathfrak{g}_2$	$-\zeta^{12}\mathfrak{g}_2$
$\tau(\mathfrak{g}_3)$	$-\mathfrak{g}_3$	$-\mathfrak{g}_3$	$\mathfrak{g}_3$	$-\zeta^{18}\mathfrak{g}_0$	$-\zeta^{12}\mathfrak{g}_3$	$(\zeta^{12}-1)\mathfrak{g}_3$

$\boldsymbol{n = 27}$ $(\mathrm{mod}\,\mathbf{72})$

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
$\tau(\mathfrak{g}_0)$	$\mathfrak{g}_0$	$-\mathfrak{g}_0$	$\mathfrak{g}_0$	$\zeta^6\mathfrak{g}_1$	$-\zeta^{12}\mathfrak{g}_0$	$(\zeta^{12}-1)\mathfrak{g}_0$
$\tau(\mathfrak{g}_1)$	$-\mathfrak{g}_1$	$-\mathfrak{g}_1$	$\mathfrak{g}_1$	$\zeta^{12}\mathfrak{g}_3$	$-\zeta^{12}\mathfrak{g}_1$	$-\zeta^{12}\mathfrak{g}_1$
$\tau(\mathfrak{g}_2)$	$-\mathfrak{g}_2$	$-\mathfrak{g}_2$	$\mathfrak{g}_2$	$-\mathfrak{g}_2$	$\mathfrak{g}_2$	$-\zeta^{12}\mathfrak{g}_2$
$\tau(\mathfrak{g}_3)$	$-\mathfrak{g}_3$	$-\mathfrak{g}_3$	$\mathfrak{g}_3$	$-\zeta^{18}\mathfrak{g}_0$	$-\zeta^{12}\mathfrak{g}_3$	$(\zeta^{12}-1)\mathfrak{g}_3$

$\boldsymbol{n = 51}$ $(\mathrm{mod}\,\mathbf{72})$

	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6
$\tau(\mathfrak{g}_0)$	$\mathfrak{g}_0$	$-\mathfrak{g}_0$	$\mathfrak{g}_0$	$\zeta^{18}\mathfrak{g}_1$	$-\zeta^{12}\mathfrak{g}_0$	$(\zeta^{12}-1)\mathfrak{g}_0$
$\tau(\mathfrak{g}_1)$	$-\mathfrak{g}_1$	$-\mathfrak{g}_1$	$\mathfrak{g}_1$	$-\mathfrak{g}_3$	$-\zeta^{12}\mathfrak{g}_1$	$-\zeta^{12}\mathfrak{g}_1$
$\tau(\mathfrak{g}_2)$	$-\mathfrak{g}_2$	$-\mathfrak{g}_2$	$\mathfrak{g}_2$	$-\mathfrak{g}_2$	$\mathfrak{g}_2$	$-\zeta^{12}\mathfrak{g}_2$
$\tau(\mathfrak{g}_3)$	$-\mathfrak{g}_3$	$-\mathfrak{g}_3$	$\mathfrak{g}_3$	$\zeta^{18}\mathfrak{g}_0$	$-\zeta^{12}\mathfrak{g}_3$	$(\zeta^{12}-1)\mathfrak{g}_3$

Now if we raise the $\mathfrak{g}_i$ functions to 12 we observe that $(\mathcal{O}/72\mathcal{O})^*$ acts like a 3-cycle on $\mathfrak{g}_i^{12}$ leaving $\mathfrak{g}_2^6$ invariant. Therefore $\mathfrak{g}_2^{12}$ gives rise to a class invariant but also the functions $\mathfrak{g}_0^{12} + \mathfrak{g}_1^{12} + \mathfrak{g}_3^{12}$ give rise to class invariants but since their sum

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Table 4. Polynomials for the invariant $\mathfrak{g}_2^{12}$, $n \equiv 3 \pmod{24}$.

n	C.N.	Polynomials
3	1	$x + 27$
27	1	$x + 243$
51	2	$x^2 + 1817x + 63408$
75	2	$x^2 + 8694x + 729$
99	2	$x^2 + 33538x + 675212$
133	2	$x^2 + 110682x + 3982527$
147	2	$x^2 + 326646x + 729$
171	4	$x^4 + 885577x^3 + 75449123x^2 + 1878791197x + 9480040943$
195	4	$x^4 + 2243057x^3 + 134435463x^2 + 2044439302x + 4021471722$
219	4	$x^4 + 5374182x^3 + 177358410x^2 + 3337735739x + 452759$
243	3	$x^3 + 12288753x^2 - 36669429x + 129140163$
267	2	$x^2 + 27000090x + 972001215$
291	4	$x^4 + 57302460x^3 + 6191231603x^2 + 190393837000x + 2422188$
315	4	$x^4 + 117966740x^3 + 5465452595x^2 - 18078266775x - 2283511958571$
339	6	$x^6 + 236380194x^5 + 16297323547x^4 + 865456023300x^3 + 28951950717535x^2 + 379087533199695x + 3423896293014081$
363	4	$x^4 + 462331692x^3 + 22863777174x^2 + 337039803468x + 531441$
387	4	$x^4 + 884736829x^3 + 65027878839x^2 + 1219285304855x + 878209991853$
411	6	$x^6 + 1659823938x^5 + 299376470893x^4 + 17714533511043x^3 + 122181573194844x^2 - 5409428705176675x + 70928211329527433$

is -36 the $\mathfrak{g}_2^{12}$ is more interesting (it involves computation of only one modular function). In Table 4 we present some small class polynomials for the invariant $\mathfrak{g}_2^{12}$. Notice that $\mathfrak{g}_2^{6}$ is a also a class invariant but its minimal polynomial does not have coefficients in $\mathbb{Z}$. In Table 5 we present some of the minimal polynomials of $\mathfrak{g}_2^{6}$ that are in $\mathbb{Z}[\sqrt{D'}][x]$, where D' is the core discriminant of D, i.e. the non-square part of D.

5. An Application to Elliptic Curve Generation

An important application of class invariants is that their minimal polynomials can be used for the generation of elliptic curves over finite fields. In particular, a method called *Complex Multiplication* or *CM method* is used being raised from the theory of Complex Multiplication (CM) of elliptic curves over the rationals [1, 3, 11]. In the case of prime fields $\mathbb{F}_p$, the CM method starts with the specification of a discriminant value D, the determination of the order p of the underlying prime field and the order m of the elliptic curve (EC). It then computes the Hilbert polynomial, which is uniquely determined by D and locates one of its roots modulo p. This root can be used to construct the parameters of an EC with order m over the field $\mathbb{F}_p$.

Alternative classes of polynomials can be used in the CM method as long as there is a transformation of their roots modulo p to the roots of the corresponding Hilbert

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

Table 5. Polynomials for the invariant $\mathfrak{g}_2^6$, $n \equiv 3 \pmod{24}$.

D	C.N.	Polynomials
-3	1	$x - 3\sqrt{D'}$
-27	1	$x - 9\sqrt{D'}$
-51	2	$x^2 - 6\sqrt{D'}x - 27$
-75	2	$x^2 - 54\sqrt{D'}x - 27$
-99	2	$x^2 - 54\sqrt{D'}x + 729$
-123	2	$x^2 - 30\sqrt{D'}x - 27$
-147	2	$x^2 - 330\sqrt{D'}x - 27$
-171	4	$x^4 - 216\sqrt{D'}x^3 - 486x^2 - 19683$
-195	4	$x^4 - 108\sqrt{D'}x^3 - 15714x^2 + 2916\sqrt{D'}x + 729$
-219	4	$x^4 - 156\sqrt{D'}x^3 + 22302x^2 + 4212\sqrt{D'}x + 729$
-243	3	$x^3 - 2025\sqrt{D'}x^2 - 6561x + 6561\sqrt{D'}$
-267	2	$x^2 - 318\sqrt{D'}x - 27$
-291	4	$x^4 - 444\sqrt{D'}x^3 - 32130x^2 + 11988\sqrt{D'}x + 729$
-315	4	$x^4 - 1836\sqrt{D'}x^3 - 7290x^2 - 78732\sqrt{D'}x + 531441$
-339	6	$x^6 - 834\sqrt{D'}x^5 + 293355x^4 + 123444\sqrt{D'}x^3 - 7920585x^2 - 607986\sqrt{D'}x - 19683$
-363	4	$x^4 - 12420\sqrt{D'}x^3 - 218754x^2 + 335340\sqrt{D'}x + 729$
-387	4	$x^4 - 4536\sqrt{D'}x^3 - 486x^2 - 19683$

polynomials. Clearly, polynomials q_n can be used in the CM method. However, firstly we have to find a relation between the j-invariant and the values A_n. Using [10, Lemma 3] we obtain the following relation between the j-invariant j_n and the Ramanujan values t_n:

$$j_n = (t_n^6 - 27t_n^{-6} - 6)^3. \tag{5.1}$$

If we set $C = t_n^6 - 27t_n^{-6}$ then we easily observe that

$$C^2 = 27(A_n - 2). \tag{5.2}$$

Remark 22. An other way to obtain a formula that relates the values H_n, t_n is working with Eq. (3.4) that relates $\mathfrak{g}_i^{12}$ to j. We compute the coefficients of the polynomial $\prod_{0\le i<j\le 3}(X - \mathfrak{g}_i^{12}\mathfrak{g}_j^{12})$. These are symmetric polynomials in the variables $\mathfrak{g}_i^{12}$ and can be expressed as polynomials on the elementary symmetric polynomials which up to sign are the coefficients of the polynomial in Eq. (3.4). Using this approach with magma [4] we arrive at

$$\begin{aligned} G(Y,j) = {} & Y^6 - 270\,Y^5 + (-36\,j + 26487)Y^4 \\ & + (-j^2 + 1512\,j - 1122660)Y^3 + (-26244\,j + 19309023)Y^2 \\ & -143489070\,Y + 387420489. \end{aligned}$$

We arrive at the same polynomial if we eliminate t_n^6 from Eq. (5.1) and the definition of H_n.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

If we wish to construct an EC over a prime field $\mathbb{F}_p$ using the q_n polynomials, we have to find one of their roots modulo p and then transform it to a root of the corresponding Hilbert polynomial j_n. The root j_n can be acquired using Eq. (5.2) and the relation $j_n = (C-6)^3$.

Let us give a brief example on how q_n polynomials can be used in the CM method. Suppose that we wish to generate an EC over the prime field $\mathbb{F}_p$ where $p = 2912592100297027922366637171900365067697538262949$ and we choose to use a discriminant equal to $n = 259$. Initially, the CM method having as input the values p and n constructs the order of the EC which is equal to a prime number

$$m = 2912592100297027922366635123877214056291799441739.$$

Then, the polynomial $q_{259}(x)$ is constructed

$$q_{259}(x) = x^4 - 16106786824376x^3 - 810131323637352x^2$$
$$-9877474632560864x + 28045355843867152.$$

This polynomial has four roots modulo p. Every such root can be transformed to a root j_n using Eq. (5.2) and the relation $j_n = (C-6)^3$. Equation (5.2) will result to two values C and this means that for every root modulo p of the $q_{259}(x)$ polynomial we will have two roots j_{259}. However, only one of these two roots gives rise to an EC with order m. The correct choice is made easily: we follow the steps of the CM method, construct an EC having as input a value j_{259} and then check whether the resulted curve (or its twist) has indeed order m. If the answer is negative, then this value is rejected.

For example, one root modulo p of the $q_{259}(x)$ polynomial is equal to

$$r = 2920001438693564712339432846235267368992567584 97.$$

Using Eq. (5.2), we compute the two solutions

$$C_1 = 1555795526891231123931549739786994193545044932499$$

and

$$C_2 = 1356796573405796798435087432113370874152493330450$$

and therefore the two possible values of the j-invariant are

$$j_1 = 2662539171725102375366109856465433412332472450493$$

and

$$j_2 = 1859938916666171899538097507602720023646246323886.$$

Selecting the first value j_1, we construct the EC $y^2 = x^3 + ax + b$ where

$$a = 1545339657951389136173847270246016180230953846699$$

and

$$b = 593624052019167833270191228638890975881231434 83.$$

In order to check if this EC (or its twist) has order m, we choose a point P at random in it and we compute the point $Q = mP$. If this point is equal to the point at infinity then the EC has order m. Making the necessary computations for the above EC, we see that this is the case and our construction is finished. Thus, we conclude that we have chosen the correct j-invariant and the second value j_2 is rejected.

Acknowledgments

We would like to thank Professor Heng Huat Chan for suggesting the study of the Ramanujan class invariant for the $-D \equiv 19 \pmod{24}$ case. We would also like to thank Professor Peter Stevenhagen for making a lot of valuable comments on a previous version of the article and for pointing us to the relation between the A_n and to the modular functions $\mathfrak{g}_i$. We also thank Professor Jannis Antoniadis for observing a pattern for the behavior of the index given in Sec. 3.1. Finally, we would like to thank the magma algebra team for providing us with a free extension of the license to their system.

References

[1] A. O. L. Atkin and F. Morain, Elliptic curves and primality proving, *Math. Comp.* **61**(203) (1993) 29–68; MR MR1199989 (93m:11136).

[2] B. C. Berndt and H. H. Chan, Ramanujan and the modular j-invariant, *Canad. Math. Bull.* **42**(4) (1999) 427–440; MR MR1727340 (2002a:11035).

[3] I. F. Blake, G. Seroussi and N. P. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society Lecture Note Series, Vol. 265 (Cambridge University Press, Cambridge, 1999).

[4] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24**(3–4) (1997) 235–265.

[5] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, Vol. 193 (Springer-Verlag, New York, 2000); MR 1728313 (2000k:11144).

[6] A. Gee, Class invariants by Shimura's reciprocity law, *J. Théor. Nombres Bordeaux* **11**(1) (1999) 45–72, *Les XXèmes Journées Arithmétiques* (Limoges, 1997); MR MR1730432 (2000i:11171).

[7] ———, Class fields by Shimura reciprocity, Ph.D. thesis, Leiden University, http://www.math.leidenuniv.nl/nl/theses/44.

[8] A. Gee and P. Stevenhagen, Generating class fields using Shimura reciprocity, in *Algorithmic Number Theory*, Lecture Notes in Computer Science, Vol. 1423 (Springer, Berlin, 1998), pp. 441–453; MR MR1726092 (2000m:11112).

[9] E. Konstantinou and A. Kontogeorgis, Computing polynomials of the Ramanujan t_n class invariants, *Canad. Math. Bull.* **52**(4) (2009) 583–597; MR MR2567152.

[10] ———, Introducing Ramanujan's class polynomials in the generation of prime order elliptic curves, *Comput. Math. Appl.* **59**(8) (2010) 2901–2917.

[11] E. Konstantinou, A. Kontogeorgis, Y. Stamatiou and C. Zaroliagis, Generating prime order elliptic curves: Difficulties and efficiency considerations, in *Int. Conf. Information Security and Cryptology — ICISC 2004*, Lecture Notes in Computer Science, Vol. 3506 (Springer, 2005), pp. 261–278.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.

[12] Pari/GP Number theory system, http://www.parigp-home.de/.

[13] S. Ramanujan, *Notebooks*, Vols. 1, 2 (Tata Institute of Fundamental Research, Bombay, 1957); MR MR0099904 (20 #6340).

[14] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publications of the Mathematical Society of Japan, Vol. 11 (Princeton University Press, Princeton, NJ, 1994), Reprint of the 1971 original, Kano Memorial Lectures, 1; MR MR1291394 (95e:11048).

[15] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Vol. 151 (Springer-Verlag, New York, 1994); MR MR1312368 (96b:11074).

[16] P. Stevenhagen, Hilbert's 12th problem, complex multiplication and Shimura reciprocity, in *Class Field Theory — Its Centenary and Prospect*, Advanced Studies in Pure Mathematics, Vol. 30 (Mathematical Society of Japan, Tokyo, 2001), pp. 161–176; MR MR 18464571 (2002i:11110).

[17] N. Yui and D. Zagier, On the singular values of Weber modular functions, *Math. Comp.* **66**(220) (1997) 1645–1662; MR MR1415803 (99i:11046).

[18] H. Weber, *Lehrbuch der Algebra*, Band III, 2nd edn. (Braunschweig, 1908); Reprinted by Chelsea, New York.

Int. J. Number Theory 2012.08:265-287. Downloaded from www.worldscientific.com
by UNIVERSITY OF THE AEGEAN LIBRARY on 09/18/12. For personal use only.