Canad. Math. Bull. Vol. **52** (4), 2009 pp. 583–597

# Computing Polynomials of the Ramanujan $t_n$ Class Invariants

Elisavet Konstantinou and Aristides Kontogeorgis

*Abstract.* We compute the minimal polynomials of the Ramanujan values $t_n$, where $n \equiv 11 \mod 24$, using the Shimura reciprocity law. These polynomials can be used for defining the Hilbert class field of the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$ and have much smaller coefficients than the Hilbert polynomials.

## 1 Introduction

In his third notebook, pages 392 and 393 in [10, vol. 2], Ramanujan defined the values

$$t_n := \sqrt{3} q_n^{1/18} \frac{f(q_n^{1/3}) f(q_n^3)}{f^2(q_n)} \tag{1}$$

where

$$q_n = \exp(-\pi\sqrt{n}).$$

The function $f$ is equal to:

$$f(-q) := \prod_{n=1}^{\infty} (1 - q^n) = q^{-1/24} \eta(\tau)$$

where $q = \exp(2\pi i \tau)$, $\tau \in \mathbb{H}$ and $\eta(\tau)$ denotes the Dedekind eta-function.

Without any further explanation on how he found them, Ramanujan gave the following table of polynomials $p_n(t)$ based on $t_n$ for five values of $n$:

| $n$ | $p_n(t)$ |
|---|---|
| 11 | $t - 1$ |
| 35 | $t^2 + t - 1$ |
| 59 | $t^3 + 2t - 1$ |
| 83 | $t^3 + 2t^2 + 2t - 1$ |
| 107 | $t^3 - 2t^2 + 4t - 1$ |

Bruce C. Berndt and Heng Huat Chan [2] proved that these polynomials indeed have roots the Ramanujan values $t_n$. Unfortunately, their method could not be applied for higher values of $n$, and they asked for an efficient way of computing the polynomials $p_n$ for every $n$. Moreover, the authors proved that if the class number of

Received by the editors May 26, 2006; revised July 4, 2006.
AMS subject classification: Primary: 11R29; secondary: 33E05, 11R20.

$K_n := \mathbb{Q}(\sqrt{-n})$ is odd and $n \in \mathbb{N}$ is squarefree such that $n \equiv 11 \bmod 24$, then $t_n$ is a real unit generating the Hilbert class field.

It is known that the Hilbert class field can also be constructed by considering the irreducible polynomial of the algebraic integer $j(\theta)$ where $\theta = -1/2 + i\sqrt{n}/2$. The minimal polynomial of $j(\theta)$ is called the Hilbert polynomial. It is interesting to point out that the coefficients of the polynomials $p_n$ have remarkably smaller size compared to the coefficients of the Hilbert polynomials. Therefore, finding an efficient and simple method for their construction is highly desirable and has a direct impact on applications where the explicit construction of class fields is needed. Problems such as primality testing/proving [1], the generation of elliptic curve parameters [7] and the representability of primes by quadratic forms [4] could be considerably improved if the polynomials $p_n$ could be constructed in an efficient and easily implemented way.

An explicit construction of the Hilbert class field has been given by N. Yui and D. Zagier [12] using the Weber functions. Yui and Zagier use a clever construction of a function on quadratic forms $ax^2 + bxy + cy^2$ that does not depend on the equivalence class of quadratic forms. The construction of a similar function in the case of $p_n$ polynomials seems very complicated, and it is clear that a different approach must be followed. Our construction came from the enforcement of the Shimura reciprocity law on the values $t_n$. The Shimura reciprocity law has been proven to be a very powerful tool for attacking similar problems [3, 5, 6] and can provide methods for systematically determining the instances when a given function yields a class invariant and for computing the minimum polynomial of a class invariant.

The contribution of this paper is twofold. First, we prove that the values $t_n$ constitute class invariants for all values of $n \equiv 11 \bmod 24$. Expanding the theorem in [2], we show that $t_n$ is a real unit generating the Hilbert class field not only in the case where the class number of $K_n$ is odd but also when it is even. Second, we provide an efficient method for constructing the irreducible polynomials $p_n$ from the Ramanujan values $t_n$ and thus answer the demand made in [2] for a direct and easily applicable construction method. Moreover, we have implemented our method in *gp-pari* [9], and we present all polynomials $p_n$ for all integers $107 < n \leq 1000$, where $n \equiv 11 \bmod 24$; see Table 1.

The rest of the paper is organized as follows. In the first section we fix the notation and give the Ramanujan $t_n$ values in terms of the Dedekind eta function. Next, we define six modular functions of level 72: $R, R_1, R_2, R_3, R_4, R_5$, and compute the action of the generators of the group $SL_2(\mathbb{Z})$ on them. In section 2 we prove that $t_n$ is indeed a class invariant for all values $n \equiv 11 \bmod 24$, and in final section we employ the Shimura reciprocity law in order to compute the conjugates of $t_n$ under the action of the class group and compute the minimal polynomial of $t_n$.

## 2 Notation

Let $SL_2(\mathbb{Z})$ be the group of matrices with integer entries and of determinant one. It is known [11, cor. 1.6] that the group $SL_2(\mathbb{Z})$ is generated by the matrices

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

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

*Table 1*: Polynomials $p_n$ for $107 \leq n < 1000$.

| $n$ | $p_n(t)$ |
|---|---|
| 107 | $x^3 - 2x^2 + 4x - 1$ |
| 131 | $x^5 + x^4 - x^3 - 3x^2 + 5x - 1$ |
| 155 | $x^4 + 2x^3 + 5x^2 + 4x - 1$ |
| 179 | $x^5 - 2x^4 + 5x^3 - x^2 + 6x - 1$ |
| 203 | $x^4 - 3x^3 + 7x - 1$ |
| 227 | $x^5 - 5x^4 + 9x^3 - 9x^2 + 9x - 1$ |
| 251 | $x^7 + 5x^6 + 6x^5 - 2x^4 - 4x^3 + 2x^2 + 9x - 1$ |
| 275 | $x^4 - x^3 + 6x^2 - 11x + 1$ |
| 299 | $x^8 + x^7 - x^6 - 12x^5 + 16x^4 - 12x^3 + 15x^2 - 13x + 1$ |
| 323 | $x^4 - x^3 + 4x^2 + 13x - 1$ |
| 347 | $x^5 + 7x^4 + 21x^3 + 27x^2 + 13x - 1$ |
| 371 | $x^8 + 9x^6 - 10x^5 + 14x^4 + 8x^3 - 23x^2 + 18x - 1$ |
| 395 | $x^8 - x^7 + 5x^6 + 16x^5 + 28x^4 + 24x^3 + 27x^2 + 17x - 1$ |
| 419 | $x^9 - 6x^8 + 12x^7 - 7x^6 + 12x^5 - 8x^4 + 31x^3 + 10x^2 + 20x - 1$ |
| 443 | $x^5 - 4x^4 - 3x^3 + 17x^2 + 22x - 1$ |
| 467 | $x^7 + 6x^6 + 7x^5 - 3x^4 + 3x^3 - 23x^2 + 26x - 1$ |
| 491 | $x^9 + x^8 + 16x^7 + 2x^6 + 37x^5 - 31x^4 + 44x^3 - 40x^2 + 29x - 1$ |
| 515 | $x^6 + 8x^5 + 32x^4 + 60x^3 + 68x^2 + 28x - 1$ |
| 539 | $x^8 - 6x^7 + 28x^6 - 56x^5 + 77x^4 - 56x^3 + 28x^2 - 34x + 1$ |
| 563 | $x^9 + 4x^8 + 6x^7 - 11x^6 + 44x^5 - 76x^4 + 91x^3 - 64x^2 + 38x - 1$ |
| 587 | $x^7 + x^6 + 16x^5 - 12x^4 + 20x^3 + 24x^2 + 39x - 1$ |
| 611 | $x^{10} - 8x^9 + 35x^8 - 62x^7 - x^6 + 116x^5 - 65x^4 - 100x^3 + 125x^2 - 46x + 1$ |
| 635 | $x^{10} - 11x^9 + 50x^8 - 121x^7 + 201x^6 - 192x^5 + 87x^4 + 51x^3 - 98x^2 + 49x - 1$ |
| 659 | $x^{11} - 7x^{10} + 7x^9 + 27x^8 + 19x^7 - 43x^6 - 5x^5 + 91x^4 + 157x^3 + 97x^2 + 49x - 1$ |
| 683 | $x^5 + 6x^4 - 5x^3 - 41x^2 + 56x - 1$ |
| 707 | $x^6 + 4x^5 + 30x^4 + 72x^3 + 108x^2 + 58x - 1$ |
| 731 | $x^{12} + 7x^{11} + 25x^{10} + 12x^9 + 41x^8 + 9x^7 +$ $+92x^6 + 73x^5 - 133x^4 + 216x^3 - 153x^2 + 67x - 1$ |
| 755 | $x^{12} - 2x^{11} + 18x^{10} + 50x^9 + 82x^8 + 182x^7 + 360x^6 + 522x^5 +$ $+598x^4 + 486x^3 + 262x^2 + 66x - 1$ |
| 779 | $x^{10} + 8x^9 + 24x^8 - 8x^7 - 11x^6 + 26x^5 + 81x^4 + 220x^3 + 98x^2 + 74x - 1$ |
| 803 | $x^{10} + 3x^9 + 26x^8 + 11x^7 - 65x^6 + 16x^5 + 7x^4 - 83x^3 + 150x^2 - 83x + 1$ |
| 827 | $x^7 - 7x^6 + 38x^5 - 54x^4 + 112x^3 - 146x^2 + 89x - 1$ |
| 851 | $x^{10} - 7x^9 - x^8 + 86x^7 + 69x^6 - 201x^5 - 219x^4 + 94x^3 + 103x^2 - 95x + 1$ |
| 875 | $x^{10} - 10x^9 + 25x^8 + 10x^7 + 15x^6 + 94x^5 - 35x^4 - 120x^3 + 85x^2 + 100x - 1$ |
| 899 | $x^{14} + 16x^{13} + 97x^{12} + 308x^{11} + 666x^{10} + 1086x^9 +$ $+1490x^8 + 1766x^7 + 1800x^6 + 1556x^5 + 998x^4 + 698x^3 + 229x^2 + 106x - 1$ |
| 923 | $x^{10} - x^9 + 30x^8 - 81x^7 - 29x^6 + 56x^5 + 211x^4 - 27x^3 - 110x^2 - 115x + 1$ |
| 947 | $x^5 + 5x^4 + 7x^3 - 103x^2 + 125x - 1$ |
| 971 | $x^{15} - x^{14} + 21x^{13} + 133x^{12} + 264x^{11} + 310x^{10} + 216x^9 +$ $+62x^8 - 100x^7 - 300x^6 + 152x^5 + 338x^4 + 79x^3 - 285x^2 + 135x - 1$ |
| 995 | $x^8 + 12x^7 + 59x^6 + 78x^5 + 12x^4 + 66x^3 + 289x^2 + 140x - 1$ |

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

Every matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of $SL_2(\mathbb{Z})$ induces an action on the upper half plane

$$\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}, \quad \text{by sending } z \mapsto \frac{az+b}{cz+d}.$$

Let $\eta$ denote the Dedekind function:

$$\eta(\tau) = \exp(2\pi i\tau/24)\prod_{n=1}^{\infty}(1-q^n), \text{ where } \tau \in \mathbb{H} \text{ and } q = \exp(2\pi i\tau). \tag{2}$$

The $\eta$-function is transformed by $S$ and $T$ as follows [11, prop. 8.3]:

$$\eta(\tau+1) = e^{2\pi i/24}\eta(\tau) \text{ and } \eta(-\frac{1}{\tau}) = \sqrt{-i\tau}\eta(\tau). \tag{3}$$

From equation (3) we can compute the action of every element $g$ of $SL_2(\mathbb{Z})$ on the $\eta$-function, since $g$ can be written as a word in $S, T$.

We denote by $H_n$ the Hilbert field of $K_n := \mathbb{Q}(\sqrt{-n})$, *i.e.*, the maximal Abelian unramified extension of $K_n$. The extension $H_n/K_n$ is Galois, with Galois group equal to the class group of fractional ideals modulo principal fractional ideals. For imaginary quadratic fields the class group can be represented as the space of binary quadratic forms $ax^2 + bxy + cy^2$ modulo an equivalence relation [4, Thm. 5.30]. We will denote by $[a, b, c]$ the quadratic form $ax^2 + bxy + cy^2$, and we will call two quadratic forms $[a_i, b_i, c_i]$ for $i = 1, 2$ equivalent if the corresponding roots $\tau_i \in \mathbb{H}$ are in the same orbit of $SL_2(\mathbb{Z})$ acting on $\mathbb{H}$. Using the identification of equivalence classes of quadratic forms with the ideal class group we can define the structure of an abelian group on the set of equivalence classes of quadratic forms.

Let $\ell_0 := (1, 1, \frac{1-d}{4})(d = -n \equiv 1 \mod 4, n \in \mathbb{N})$ be the zero element in this group. This element corresponds to the root

$$\tau_{\ell_0} = -\frac{1}{2} + i\frac{\sqrt{n}}{2}.$$

Set

$$q_n = \exp(-\pi\sqrt{n}) = -\exp(2\pi i\tau_{\ell_0}).$$

Then

$$\begin{aligned} f(q_n) &= f\big(-\exp(2\pi i\tau_{\ell_0})\big) = \exp(2\pi i\tau_{\ell_0})^{-1/24}\eta(\tau_{\ell_0}), \\ f(q_n^3) &= \exp(2\pi i\tau_{\ell_0})^{-3/24}\eta(3\tau_{\ell_0}), \\ f(q_n^{1/3}) &= (-1)^{1/18}\exp(2\pi i\tau_{\ell_0})^{-\frac{1}{3\cdot 24}}\eta\Big(\frac{\tau_{\ell_0}}{3}+\frac{2}{3}\Big). \end{aligned}$$

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

Taking equation (1) and all the above equations into consideration we arrive easily at the following Lemma.

***Lemma 2.1*** *The Ramanujan value $t_n$ is given by*

$$t_n = \sqrt{3}R_2(\tau_{\ell_0}),$$

*where*

$$R_2(\tau) = \frac{\eta(3\tau)\eta(\frac{1}{3}\tau + \frac{2}{3})}{\eta^2(\tau)}.$$

Now let $N \in \mathbb{N}$ and $\Gamma(N)$ be the group

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

The field of modular functions of level $N$ consists of the meromorphic functions $g$ of the upper half plane $\mathbb{H}$ that are invariant under the group $\Gamma(N)$, *i.e.*, $g(\gamma\tau) = g(\tau)$ for every $\tau \in \mathbb{H}$ and $\gamma \in \Gamma(N)$. Every modular function is periodic with period $N$ and thus it admits a Fourier expansion of the form

$$g(q) = \sum_{\nu=-i}^{\infty} a_\nu q^\nu,$$

where $q = \exp(2\pi i\tau/N)$. We will limit ourselves to modular functions where all coefficients of the Fourier expansions are elements of the field $\mathbb{Q}(\zeta_N)$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is isomorphic to the group $(\frac{\mathbb{Z}}{N\mathbb{Z}})^*$ by defining $\sigma_d(\zeta_N) = \zeta_N^d$ for every $(d, N) = 1$.

The action of the group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ can be extended to the field of modular functions of level $N$ with coefficients in $\mathbb{Q}(\zeta_N)$, as follows:

$$g(q)^{\sigma_d} = \sum_{\nu=-i}^{\infty} \sigma_d(a_\nu)q^\nu, \quad \sigma_d \in Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q}).$$

Moreover, the action of an element $A \in GL_2(\mathbb{Z})$ on modular functions $g(q)$ can be expressed as

$$g^A = (g^B)^{\sigma_{\det(A)}},$$

where $A = B \cdot \left(\begin{smallmatrix} 1 & 0 \\ 0 & \det(A) \end{smallmatrix}\right)$ and $B \in SL_2(\mathbb{Z})$.

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

***Lemma 2.2*** *The following are modular functions of level 72:*

$$R(\tau) = \frac{\eta(3\tau)\eta(\tau/3)}{\eta^2(\tau)},$$
$$R_1(\tau) = \frac{\eta(3\tau)\eta(\tau/3+1/3)}{\eta^2(\tau)},$$
$$R_2(\tau) = \frac{\eta(3\tau)\eta(\tau/3+2/3)}{\eta^2(\tau)},$$
$$R_3(\tau) = \frac{\eta(\tau/3)\eta(\tau/3+2/3)}{\eta^2(\tau)},$$
$$R_4(\tau) = \frac{\eta(\tau/3)\eta(\tau/3+1/3)}{\eta^2(\tau)},$$
$$R_5(\tau) = \frac{\eta(\tau/3+2/3)\eta(\tau/3+1/3)}{\eta^2(\tau)}.$$

*Moreover, the element $\sigma_d : \zeta_{72} \mapsto \zeta_{72}^d$ for $(d,n) = 1$ acts on them as follows:*

$$\sigma_d(R) = R,$$
$$\sigma_d(R_1) = \begin{cases} \zeta_{72}^{d-1} R_1 & \text{if } d \equiv 1 \bmod 3, \\ \zeta_{72}^{d-2} R_2 & \text{if } d \equiv 2 \bmod 3, \end{cases}$$
$$\sigma_d(R_2) = \begin{cases} \zeta_{72}^{2d-2} R_2 & \text{if } d \equiv 1 \bmod 3, \\ \zeta_{72}^{2d-1} R_1 & \text{if } d \equiv 2 \bmod 3, \end{cases}$$
$$\sigma_d(R_3) = \begin{cases} \zeta_{72}^{d-1} R_3 & \text{if } d \equiv 1 \bmod 3, \\ \zeta_{72}^{d-2} R_2 & \text{if } d \equiv 2 \bmod 3, \end{cases}$$
$$\sigma_d(R_4) = \begin{cases} \zeta_{72}^{2d-2} R_4 & \text{if } d \equiv 1 \bmod 3, \\ \zeta_{72}^{2d-1} R_3 & \text{if } d \equiv 2 \bmod 3, \end{cases}$$
$$\sigma_d(R_5) = \zeta_{72}^{3d-3} R_5. \tag{4}$$

**Proof** The fact that the above equations are indeed modular of level 72 is a direct computation using the transformations of the $\eta$-functions under the generators $T, S$ of $SL_2(\mathbb{Z})$ given in (3). The action of $\sigma_d$ given in (4) is computed by considering the Fourier expansions of the $\eta$-factors of the functions $R_i$. For instance let as compute the action of the element $\sigma_d$ on $R_2$. We begin by computing its action on $\eta(\tau/3+2/3)$:

$$\eta(\tau/3+2/3) = \exp\Big(\frac{2\pi i}{24}(\tau/3+2/3)\Big) \sum_{\nu=0}^{\infty} a_n \exp\Big(\frac{2\pi i\nu}{3}\tau + \frac{2\pi i\nu}{3}\Big) \tag{5}$$
$$= \exp\Big(\frac{2\pi i}{24}(\tau/3)\Big) \zeta_{72}^2 \sum_{\nu=0}^{\infty} \zeta_3^{2\nu} a_n \exp\Big(\frac{2\pi i\nu}{3}\tau\Big),$$

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

where $\zeta_3 = \zeta_{72}^{24}$ is a primitive third root of unity. The desired formulas of (4) follow from the definition of the action of $\sigma_d$ on $\zeta_{72}$ and arguing as above. For example (notice that from (2) the Fourier expansion for $\eta(\tau)$ has rational coefficients, so it is invariant under the action of $\sigma_d$),

$$\sigma_d(R_2) = \sigma_d\Big(\frac{\eta(3\tau)\eta(\tau/3+2/3)}{\eta^2(\tau)}\Big) = \frac{\eta(3\tau)}{\eta^2(\tau)}\sigma_d(\eta(\tau/3+2/3)).$$

By (5) we have that

$$\sigma_d(\eta(\tau/3+2/3)) = \exp\Big(\frac{2\pi i}{24}(\tau/3)\Big)\zeta_{72}^{2d}\sum_{\nu=0}^{\infty}\zeta_3^{2\nu d}a_n\exp\Big(\frac{2\pi i\nu}{3}\tau\Big).$$

If $d \equiv 1 \bmod 3$ then $\zeta_3^{2\nu d} = \zeta_3^{2\nu}$, thus

$$\sigma_d(R_2) = \zeta_{72}^{2d-2}R_2.$$

If $d \equiv 2 \bmod 3$ then $\zeta_3^{2\nu d} = \zeta_3^{\nu}$, and

$$\sigma_d(\eta(\tau/3+2/3)) = \eta(\tau/3+1/3))\zeta_{72}^{2d-1} \Rightarrow \sigma_d(R_2) = \zeta_{72}^{2d-1}R_1. \qquad \blacksquare$$

Later we will use some computer algebra programs in order to prove that $t_n$ is indeed a class invariant and find the minimal polynomials of $t_n$. For this reason it is convenient to have the actions of the elements $S, T, \sigma_d$ in matrix form. Using (3) we give the following matrix action of the elements $S, T, \sigma_d$ on the functions $R, R_1, \ldots, R_5$:

$$\text{(6)}\qquad \begin{pmatrix} R(\tau+1)\\ R_1(\tau+1)\\ R_2(\tau+1)\\ R_3(\tau+1)\\ R_4(\tau+1)\\ R_5(\tau+1)\end{pmatrix} = A_T\begin{pmatrix} R(\tau)\\ R_1(\tau)\\ R_2(\tau)\\ R_3(\tau)\\ R_4(\tau)\\ R_5(\tau)\end{pmatrix},\quad \begin{pmatrix} R(\frac{-1}{\tau})\\ R_1(\frac{-1}{\tau})\\ R_2(\frac{-1}{\tau})\\ R_3(\frac{-1}{\tau})\\ R_4(\frac{-1}{\tau})\\ R_5(\frac{-1}{\tau})\end{pmatrix} = A_S\begin{pmatrix} R(\tau)\\ R_1(\tau)\\ R_2(\tau)\\ R_3(\tau)\\ R_4(\tau)\\ R_5(\tau)\end{pmatrix},$$

$$\begin{pmatrix} \sigma_d R\\ \sigma_d R_1\\ \sigma_d R_2\\ \sigma_d R_3\\ \sigma_d R_4\\ \sigma_d R_5\end{pmatrix} = A_{\sigma_d}\begin{pmatrix} R\\ R_1\\ R_2\\ R_3\\ R_4\\ R_5\end{pmatrix},$$

where

$$\text{(7)}\qquad A_T := \begin{pmatrix} 0 & \zeta_{72}^3 & 0 & 0 & 0 & 0\\ 0 & 0 & \zeta_{72}^3 & 0 & 0 & 0\\ \zeta_{72}^6 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & \frac{1}{\zeta_{72}^3} & 0\\ 0 & 0 & 0 & 0 & 0 & \frac{1}{\zeta_{72}^6}\\ 0 & 0 & 0 & \frac{1}{\zeta_{72}^3} & 0 & 0\end{pmatrix},$$

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

$$A_S := \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{\zeta_{72}^3(-\zeta_{72}^{30}+\zeta_{72}^6)} & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{\zeta_{72}^3}{-\zeta_{72}^{30}+\zeta_{72}^6} & 0 \\ 0 & -\zeta_{72}^{33}+\zeta_{72}^9 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{-\zeta_{72}^{30}+\zeta_{72}^6}{\zeta_{72}^3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

and

$$A_{\sigma_d} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_{72}^{d-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_{72}^{2d-d} & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_{72}^{2d-2} & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_{72}^{d-1} & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_{72}^{3d-3} \end{pmatrix} \text{ if } d \equiv 1 \bmod 3,$$

$$A_{\sigma_d} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_{72}^{d-2} & 0 & 0 & 0 \\ 0 & \zeta_{72}^{2d-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_{72}^{2d-1} & 0 \\ 0 & 0 & 0 & \zeta_{72}^{d-2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_{72}^{3d-3} \end{pmatrix} \text{ if } d \equiv 2 \bmod 3,$$

## 3 The Shimura Reciprocity Law and $t_n$ Class Invariants

Let $K_n = \mathbb{Q}(\sqrt{-n})$ be an imaginary quadratic number field, $\mathcal{O}$ the ring of integers of $K_n$ and $\theta = \frac{1}{2} - i\frac{\sqrt{n}}{2}$. It is known that $j(\theta)$ is an algebraic integer that generates the Hilbert class field of $K_n$, and moreover that the conjugates $j(\theta)$ under the action of the class group are given by

$$j(\theta)^{[a,-b,c]} = j(\tau_{[a,b,c]}),$$

where $\tau_{[a,b,c]}$ is the unique root of $ax^2 + bx + c$ with positive imaginary part, *i.e.*,

$$\tau_{[a,b,c]} = \frac{-b + i\sqrt{-D}}{2a}.$$

There is an efficient algorithm for computing a set of non-equivalent quadratic forms and the minimal polynomial $f_D(x)$ of $j(\theta)$ can easily be computed from the floating point approximation of the values $j(\tau_{[a,b,c]})$:

$$f_D(x) = \prod_{[a,b,c] \in Cl(\mathcal{O})} (x - j(\tau_[a,b,c])).$$

For instance, the polynomial for the quadratic extension of discriminant $-107$ is

$$f_{-107}(x) = x^3 + 129783279616 \cdot 10^3 x^2 - 6764523159552 \cdot 10^6 x + 337618789203968 \cdot 10^9.$$

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

The disadvantage of using the above polynomials for the construction of the Hilbert class field is the very large size of their coefficients compared to the coefficients of the polynomials $p_n$. Notice that the polynomial $p_n$ for $n = 107$ is equal to $x^3-2x^2+4x-1$. In the literature there are alternative explicit constructions of the Hilbert class fields based on the Weber functions [12] or other modular functions [3, 5, 6]. In [2] the authors proved that the values $t_n$ can also generate the Hilbert class field, providing the following theorem.

***Theorem 3.1*** *If $n \equiv 11 \mod 24$ and the class group of $K_n$ is odd, then $t_n$ generates the Hilbert field.*

**Proof** See [2, Thm. 4.1]. ∎

The Shimura reciprocity law can be applied in order to compute the minimal polynomial of $t_n$ and give an alternative proof of Theorem 3.1 by removing the odd class number requirement.

In order to prove that $t_n$ is also a class invariant when the class group of $K_n$ is even, we will use the following construction.

***Theorem 3.2*** *Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of algebraic integers of the imaginary quadratic field $K$, and assume that $x^2 + Bx + C$ is the minimal polynomial of $\theta$. Let $N > 1$ be a natural number, $x_1, \ldots, x_r$ be generators of the abelian group $(\mathcal{O}/N\mathcal{O})^*$ and let $\alpha_i + \beta_i\theta \in \mathcal{O}$ be a representative of the class of the generator $x_i$. 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*

$$f(\theta) = f^{A_i}(\theta), \text{ and } \mathbb{Q}(j) \subset \mathbb{Q}(f), \tag{8}$$

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

**Proof** See [5, Cor. 4] ∎

We know by Lemma 2.1 that the Ramanujan invariant $t_n$ can be constructed by evaluating the modular function $\sqrt{3}R_2$ of level 72 at $\tau_{\ell_0}$. Thus, we begin by constructing the generators of $(\mathcal{O}/72\mathcal{O})^*$, as Theorem 3.2 dictates. Since $n \equiv 11 \mod 24$ we can take $\theta = \frac{1}{2} + \frac{1}{2}\sqrt{-n}$ as a generator of the ring of algebraic integers of $K = \mathbb{Q}(\sqrt{-n})$. The minimal polynomial of $\theta$ is $x^2 - x + \frac{n+1}{4}$, and thus $B$ and $C$ in Theorem 3.2 are equal to $-1$ and $\frac{n+1}{4}$ respectively. The form of the minimal polynomial implies that the prime $p = 2$ stays inert in the extension $K/\mathbb{Q}$ while the prime $p = 3$ splits.

In order to prove that $t_n := \sqrt{3}R_2(\theta)$ is indeed a class invariant, we have to prove that

$$\left(\sqrt{3}R_2\right)^{A_i} = \sqrt{3}R_2, \text{ for all matrices } A_i \text{ and for } n \equiv 11 \mod 24. \tag{9}$$

We observe that the structure of the group $(\frac{\mathcal{O}}{72\mathcal{O}})^*$ depends only on the value of $n \mod 72$, and there are exactly three equivalence classes $n \mod 72$ such that

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

$n \equiv 11 \mod 24$, namely $n = 11, 35, 59 \mod 72$. Thus, we are reduced to checking (9) for a finite number of $n$.

Using the Chinese remainder theorem we can express the group $(\frac{\mathcal{O}}{72\mathcal{O}})^*$ as a direct product

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

We will study the structure of the above two summands separately.

We compute that

$$\left(\frac{\mathcal{O}}{9\mathcal{O}}\right)^* \cong \frac{\mathbb{Z}}{6\mathbb{Z}} \times \frac{\mathbb{Z}}{6\mathbb{Z}}.$$

A selection of generators for this group is cumbersome to do by hand. We have used a brute force method, *i.e.*, we have checked all elements one by one if there are invertible and then we have computed their orders using the *magma* [8] algebra system in order to compute that for $C = \frac{n+1}{4} \in \{3, 9, 15\}$ a set of generators is given by $7\theta + 4, 5$. Moreover

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

and, we have computed the following selection of generators using *magma*.

| $n$ | $\frac{n+1}{4}$ | Generators |
|---|---|---|
| 11 | 3 | $\theta, 7, 4\theta + 7$ |
| 35 | 9 | $5\theta + 6, 7, 4\theta + 7$ |
| 59 | 15 | $\theta, 7, 4\theta + 7$ |

From the above generators and from the Chinese remainder theorem we can construct generators for the group $(\mathcal{O}/72\mathcal{O})^*$ and map them to the matrices $A_i$ defined in theorem 3.2. We have a total of 5 generators for the group $(\mathcal{O}/72\mathcal{O})^*$. The first two are generators of the group $(\mathcal{O}/9\mathcal{O})^*$ and, the last three are generators of the group $(\mathcal{O}/8\mathcal{O})^*$. In order to compute the term $f^{A_i}$ in (8), we have to consider any lift of $A_i$ in $GL_2(\mathbb{Z})$ and write it as a product $w_i(S, T)\mathrm{diag}(1, \det(A_i))$, where $w_i(S, T)$ is a word in $S, T$.

The following lemma gives us the decomposition of a matrix in $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ as a word in the generators of the group $SL_2(\mathbb{Z}/p^r\mathbb{Z})$. Therefore, we must consider the matrices $A_i$ modulo 8 or 9 and define $A_{i,8} \in GL_2(\mathbb{Z}/8\mathbb{Z})$ and $A_{i,9} \in GL_2(\mathbb{Z}/9\mathbb{Z})$, such that $A_i \equiv A_{i,8} \mod 8$ and $A_i \equiv A_{i,9} \mod 9$. Notice that $A_{i,8} \equiv \mathrm{Id} \mod 8$ for $i = 1, 2$, *i.e.*, the first two generators, and $A_{i,9} \equiv \mathrm{Id} \mod 9$ for $i = 3, 4, 5$, *i.e.*, the last three generators.

***Lemma 3.3*** *Let $p^r$ be a prime power and let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}/p^r\mathbb{Z})$ so that either $a$ or $c$ is invertible modulo $p^r$. Let $\bar{S}_{p^r} = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $\bar{T}_{p^r} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ be two generators of the group $SL_2(\mathbb{Z}/p^r\mathbb{Z})$. Set $y = (1+a)c^{-1} \mod p^r$ if $(c, p) = 1$, otherwise set $z = (1+c)a^{-1} \mod p^r$. Then*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{cases} \bar{T}_{p^r}^{y} \bar{S}_{p^r} \bar{T}_{p^r}^{c} \bar{S}_{p^r} \bar{T}_{p^r}^{dy-b} \mod p^r & \text{if } (c, p) = 1 \\ \bar{S}_{p^r} \bar{T}_{p^r}^{-z} \bar{S}_{p^r} \bar{T}_{p^r}^{-a} \bar{S}_{p^r} \bar{T}_{p^r}^{bz-d} \mod p^r & \text{if } (a, p) = 1. \end{cases}$$

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

**Proof** See [5, lemma 6]. ∎

The generators $\bar{S}_{p^r}, \bar{T}_{p^r}$ modulo $p^r = 8, 9$ are then lifted to elements $S_8, S_9$, $T_8, T_9 \in SL_2(\mathbb{Z})$ such that

$$S_8 \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \bmod 8, \text{ and } S_8 \equiv \mathrm{Id} \bmod 9,$$

$$S_9 \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \bmod 9, \text{ and } S_9 \equiv \mathrm{Id} \bmod 8,$$

$$T_8 \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \bmod 8, \text{ and } T_8 \equiv \mathrm{Id} \bmod 9,$$

$$T_9 \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \bmod 9, \text{ and } T_9 \equiv \mathrm{Id} \bmod 8.$$

Using the Chinese remainder theorem we compute that

$$S_8 = T^{-1}ST^{-10}ST^{-1}ST^{-162}, \quad T_8 = T^9, \tag{10}$$
$$S_9 = T^{-1}ST^{-65}ST^{-1}ST^{1096}, \quad T_9 = T^{-8}.$$

We observe that the elements $S_8, T_8$ commute with $S_9, T_9$ modulo 72.

The matrices $A_{i,p^r}$, $p^r = 8$ or 9 can be decomposed as products

$$A_{i,p^r} = B_{i,p^r} \begin{pmatrix} 1 & 0 \\ 0 & \det(A_{i,p^r}) \end{pmatrix},$$

where the matrices $B_{i,p^r}$ have determinant 1 mod $p^r$ and can be expressed, using Lemma 3.3, as words $w_{p^r}(S, T)$ in the generators $S, T$. The matrices of the form $A_i$ act on the field of modular functions of level 72 with coefficients in $\mathbb{Q}(\zeta_{72})$ as the product $w_8(S, T) \cdot w_9(S, T) \cdot \mathrm{diag}(1, d_i)$, where $d_i$ is the determinant of $A_i$, *i.e.*, the unique integer such that $d_i \equiv \det(A_{i,9}) \bmod 9$ and $d_i \equiv \det(A_{i,8}) \bmod 8$.

For instance the generator $7\theta + 4$ of $(\mathcal{O}/9\mathcal{O})^*$ for $C = 3$ corresponds to the matrix $A := \left(\begin{smallmatrix} 11 & -21 \\ 7 & 4 \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 2 & 6 \\ 7 & 4 \end{smallmatrix}\right) \bmod 9$ (and to the identity matrix modulo 8). This is a matrix of determinant 2 mod 9, and it is decomposed as

$$\begin{pmatrix} 2 & 6 \\ 7 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 7 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix},$$

where $B := \left(\begin{smallmatrix} 2 & 3 \\ 7 & 2 \end{smallmatrix}\right)$ is a matrix of determinant 1 mod 9. Using 3.3 we find that

$$B = \begin{pmatrix} 2 & 3 \\ 7 & 2 \end{pmatrix} = \bar{T}_9^3 \bar{S}_9 \bar{T}_9^7 \bar{S}_9 \bar{T}_9^3.$$

A lift of the elements $\bar{S}_9, \bar{T}_9$ in $SL_2(\mathbb{Z})$ is given by equation (10). This means that we replace each $\bar{S}_9$ of the above formula by $S_9 = T^{-1}ST^{-65}ST^{-1}ST^{1096}$ and each $\bar{T}_9$ by $T^{-9}$. This gives us the desired lift of $B$ to an element in $SL_2(\mathbb{Z})$. Using this lift and the

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

transformation matrices $A_S, A_T$ given in (7) we compute that the action of $A$ on the modular functions $R_i$ is given in terms of the following matrix:

$$E := \begin{pmatrix} 0 & 0 & 0 & \frac{-2\zeta_{72}^{18}}{3} + \frac{\zeta_{72}^{6}}{3} & 0 & 0 \\ 0 & 0 & \zeta_{72}^{15} - \zeta_{72}^{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{\zeta_{72}^{15}}{3} + \frac{\zeta_{72}^{3}}{3} \\ 0 & 0 & 0 & 0 & -\zeta_{72}^{9} & 0 \\ -2\zeta_{72}^{21} + \zeta_{72}^{9} & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_{72}^{18} + \zeta_{72}^{6} & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let $V$ be the $\mathbb{Q}(\zeta_{72})$-vector space of modular functions generated by the elements $R, R_1, R_2, R_3, R_4, R_5$. The vector space $V$ can be identified to the vector space $\mathbb{Q}(\zeta_{72})^6$, in terms of the map

$$V \to \mathbb{Q}(\zeta_{72})^6,$$
$$a_0R + a_1R_1 + \cdots + a_5R_5 \mapsto (a_0, a_1, \ldots, a_5), \quad a_i \in Hom(V, \mathbb{Q}(\zeta_{72}))$$

The space $V^* = \mathbb{Q}(\zeta_{72})^6$ is the dual space of $V$ and we have to see how the action of the elements $T, S, \sigma_d$ act on $V^*$. The elements $A_T, A_S$ defined in (7) act on $\mathbb{Q}(\zeta_{72})^6$ in terms of the transpose matrices $A_T^t, A_S^t$, while the action of $A_{\sigma_d}$ on $R, R_1, \ldots, R_5$ given on (7) acts on $\mathbb{Q}(\zeta_{72})^6$ in terms of the contragredient action, *i.e.*, by considering the transpose of the matrix $A_{\sigma_{-d}}$. By the Chinese remainder theorem we compute that the element $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ acts on $\mathbb{Q}(\zeta_{72})$ as the automorphism $\sigma_{65}\colon \zeta_{72} \mapsto \zeta_{72}^{65}$. Indeed, 65 is an integer $65 \equiv 2 \bmod 9$ and $65 \equiv 1 \bmod 8$.

Since $d = 65 \equiv 2 \bmod 3$ we compute that the vector $(0, 0, 1, 0, 0, 0)^t$ corresponding to the element $R_2$ is mapped to

$$A_{\sigma_{-65}} E^{\sigma_{-65}} (0, 0, 1, 0, 0, 0)^t = (0, 0, -1, 0, 0, 0),$$

where by $E^{\sigma_{-65}}$ we denote the matrix where all elements are acted on by $\sigma_{-d}$. Notice that $\sqrt{3} = \zeta_{72}^{6} - \zeta_{72}^{30}$. Indeed, the value $i\sqrt{3}$ can be expressed as a difference of two primitive 3-roots of unity $\zeta_3, \zeta_3^2$ since $i = \zeta_{72}^{18}$ and $\zeta_3 = \zeta_{72}^{24}$. Moreover, $\sigma_{-65}(\sqrt{3}) = \zeta_{72}^{-6\cdot 65} - \zeta_{72}^{-30\cdot 65} = -\sqrt{3}$ and thus $\sqrt{3}R_2$ is left invariant. Following the same procedure it can be proven that $\sqrt{3}R_2$ stays invariant for all matrices $A_i$.

***Theorem 3.4*** *The Ramanujan value $t_n$ is a class invariant for $n \equiv 11 \bmod 24$.*

**Proof** The condition $\mathbb{Q}(j) \subset \mathbb{Q}(f)$ of Theorem 3.2 is known [2, proof of Thm. 4.1]. By machine computation[1], it turns out that (9) holds for all matrices $A_i$ and thus $t_n$ is a class invariant for all $n \equiv 11 \bmod 24$. ∎

[1]The magma program used for this computation is available at http://eloris.samos.aegean.gr/papers.html

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

## 4 Computing the Polynomials $p_n$

In this section we provide a method for the construction of the minimal polynomial of $t_n$. Following the article of A. Gee [5, eq. 17] we give the following definition:

***Definition 4.1*** *Let $N \in \mathbb{N}$ and let $[a, b, c]$ 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 $D = b^2 - 4ac \equiv 1 \bmod 4$. We define the matrix*

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

*The Chinese remainder theorem implies that*

$$GL_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{p|N} GL_2(\mathbb{Z}/p^r\mathbb{Z}).$$

*We define $A_{[a,b,c]}$ as the unique element in $GL_2(\mathbb{Z}/N\mathbb{Z})$ that it is mapped to $A_{[a,b,c],p^r}$ modulo $p^r$. This matrix $A_{[a,b,c]}$ can be written uniquely as a product*

$$A_{[a,b,c]} = B_{[a,b,c]} \begin{pmatrix} 1 & 0 \\ 0 & d_{[a,b,c]} \end{pmatrix}, \tag{11}$$

*where $d_{[a,b,c]} = \det A_{[a,b,c]}$ and $B_{[a,b,c]}$ is a matrix with determinant* 1.

The Shimura reciprocity law gives us [5, lemma 20] the action of $[a, b, c]$ on $\sqrt{3}R_2(\theta)$ for $\theta = 1/2 - i\sqrt{n}/2$:

$$\left(\sqrt{3}R_2(\theta)\right)^{[a,-b,c]} = (\zeta_{72}^{6d_{[a,b,c]}} - \zeta_{72}^{30d_{[a,b,c]}}) R_2\left(\frac{\alpha_{[a,b,c]}\tau_{[a,b,c]} + \beta_{[a,b,c]}}{\gamma_{[a,b,c]}\tau_{[a,b,c]} + \delta_{[a,b,c]}}\right)^{\sigma_{d_{[a,b,c]}}},$$

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.

If we try to implement this method in order to compute the polynomial for $t_n$ we face a problem. Even though we can compute a floating point approximation of the conjugate $R_2(A_{[a,b,c]})$, it is not possible to use this approximation in order to compute the action of $\sigma_{d_{[a,b,c]}}$ on it. There is however a simple approach that we can follow and solve this problem. We can express the matrix $A_{[a,b,c]}$ as a product of a matrix $B_{[a,b,c]}$ as in (11) and then compute the expansion of $B_{[a,b,c]}$ as a word of the matrices $S, T$.

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

We begin our computation by computing a full set of representatives of equivalence classes $[a, b, c]$. Since $72 = 2^3 \cdot 3^2$, we have to compute matrices

$$A_{[a,b,c],p^r} \in GL_2(\mathbb{Z}/p^r\mathbb{Z}) \text{ for } p^r = 8, 9.$$

Then we compute the determinant $d_{[a,b,c],p^r}$ of the matrix $A_{[a,b,c],p^r}$, and we find a decomposition

$$A_{[a,b,c],p^r} = B_{[a,b,c],p^r} \begin{pmatrix} 1 & 0 \\ 0 & d_{[a,b,c],p^r} \end{pmatrix}.$$

The matrices $B_{[a,b,c],p^r}$ are elements of $SL_2(\mathbb{Z}/p^r\mathbb{Z})$ and can be written as words of $\bar{S}_{p^r}, \bar{T}_{p^r}$ using Lemma 3.3.

So if $B_{[a,b,c],8} = w(\bar{T}_8, \bar{S}_8)$ and $B_{[a,b,c],9} = w'(\bar{T}_9, \bar{S}_9)$ are the decompositions of $B_{[a,b,c],p^r}$ as words of $\bar{S}_{p^r}, \bar{T}_{p^r}$, we take the lift

$$B_{[a,b,c]} = w(T_8, S_8)w'(T_9, S_9) \in SL_2(\mathbb{Z})$$

and the corresponding action on the functions $R, R_1, \ldots, R_5$ is computed using (6).

The determinants $d_{[a,b,c],8} \in \mathbb{Z}/8\mathbb{Z}$ and $d_{[a,b,c],9} \in \mathbb{Z}/9\mathbb{Z}$ can be lifted to an element $d_{[a,b,c]}$ of $\mathbb{Z}/72\mathbb{Z}$ (so that it reduces to $d_{[a,b,c],8}$ mod 8 and $d_{[a,b,c],9}$ mod 9 respectively) by again using the Chinese remainder theorem.

The desired polynomial $p_n$ can then be computed:

$$p_n(t) = \prod_{[a,b,c]} \left( t - \left( \sqrt{3} R_2\left(\frac{-1 + i\sqrt{n}}{2}\right)\right)^{[a,-b,c]} \right).$$

We have used the *gp-pari* [2] program in order to perform this computation. The resulting polynomials $p_n$ for $107 \leq n < 1000$ are given in Table 1.

## References


[1] A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving.* Math. Comp. **61**(1993), no. 203, 29–68.

[2] B. C. Berndt and H. H. Chan, *Ramanujan and the modular $j$-invariant*. Canad. Math. Bull. **42**(1999), no. 4, 427–440.

[3] H. H. Chan, A. Gee, and V. Tan, *Cubic singular moduli, Ramanujan's class invariants $\lambda_n$ and the explicit Shimura reciprocity law.* Pacific J. Math. **208**(2003), no. 1, 23–37.

[4] David A. Cox, *Primes of the form $x^2 + ny^2$*. John Wiley & Sons Inc., New York, NY, 1989. Fermat, class field theory and complex multiplication.

[5] A. Gee, *Class invariants by Shimura's reciprocity law.* J. Théor. Nombres Bordeaux **11**(1999), no. 1, 45–72.

[6] A. Gee and P. Stevenhagen, *Generating class fields using Shimura reciprocity.* In: Algorithmic number theory, Lecture Notes in Comput. Sci., 1423, Springer, Berlin, 1998, pp. 441–453.

[7] E. Konstantinou, A. Kontogeorgis, Y. Stamatiou, and C. Zaroliagis, *Generating prime order elliptic curves: difficulties and efficiency considerations.* In: International Conference on Information Security and Cryptology, Lecture Notes in Comput. Sci. 3506, Springer, Berlin, 2005, pp. 261–278.

[8] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language.* J. Symbolic Comput. **24**(1997), no. 3-4, 235–265.

[9] Pari/GP Number Theory System. http://www.parigp-home.de]

[10] S. Ramanujan, *Notebooks.* Vols. 1, 2, Tata Institute of Fundamental Research, Bombay, 1957.


[2] The pari program used for this computation is available at http://eloris.samos.aegean.gr/papers.html.

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press

[11] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151, Springer-Verlag, New York, 1994.
[12] N. Yui and D. Zagier, *On the singular values of Weber modular functions*, Math. Comp. **66**(1997), no. 220, 1645–1662.

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

*Department of Mathematics, University of the Aegean, 83200 Karlovassi, Samos,Greece,*
*e-mail*: kontogar@aegean.gr

https://doi.org/10.4153/CMB-2009-058-6 Published online by Cambridge University Press