Turkish Journal of Mathematics

Volume 39 | Number 4 Article 10

1-1-2015

On the computation of generalized division polynomials

ÖMER KÜÇÜKSAKALLI

TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2015) 39: 547 – 555

doi:10.3906/mat-1410-29

On the computation of generalized division polynomials

Ömer KÜÇÜKSAKALLI*
Department of Mathematics, Middle East Technical University, Ankara, Turkey

Received: 12.10.2014 • **Accepted/Published Online:** 15.01.2015 • **Printed:** 30.07.2015

Abstract: We give an algorithm to compute the generalized division polynomials for elliptic curves with complex multiplication. These polynomials can be used to generate the ray class fields of imaginary quadratic fields over the Hilbert class field with no restriction on the conductor.

Key words: Complex multiplication, division polynomial, Hurwitz number

1. Introduction

A fundamental problem in algebraic number theory is to construct a polynomial that generates a given number field. Inspired by the Kronecker–Weber theorem, Hilbert's twelfth problem asks us to generate abelian extensions of number fields using singular values of analytical functions. There are two cases, namely the cyclotomic case and the elliptic case, for which this problem has an affirmative answer.

The cyclotomic case has been investigated deeply and there is a vast literature. On the other hand, our information for the elliptic case is limited. Unlike the cyclotomic case there is not even a formula for polynomials generating the simplest extensions, such as the extensions of prime conductor.

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$ and let $\mathfrak{f}$ be an ideal of $\mathcal{O}_K$. The fundamental theorem of complex multiplication states that the ray class field $K_{\mathfrak{f}}$ of conductor $\mathfrak{f}$ can be generated by the singular values of the j-function and Weber functions [9]. The first step of such a construction is to generate the Hilbert class field H using the j-function. Instead of the j-function one can use alternative functions and produce relatively smaller class polynomials, but there is no closed formula or recurrence relation producing such polynomials.

Generating $K_{\mathfrak{f}}$ over H is better understood. If $\mathfrak{f} = (f)$ for some integer f, then we can find the corresponding division polynomial recursively using the theory of elliptic curves [8]. Moreover, Satoh succeeded in generalizing this recursive construction for some elements $\alpha \in \mathcal{O}_K - \mathbf{Z}$. More precisely, if $\mathfrak{f} = (\alpha)$ for some *unbiased* $\alpha \in \mathcal{O}_K$, then Satoh recursively constructs the corresponding division polynomials generating the ray class field $K_{(\alpha)}$ over H [7].

In this paper we give an algorithm to compute the generalized division polynomials with no restriction on the conductor $\mathfrak{f}$. We are inspired by our previous results for cyclotomic fields [4] and the analogy between the cyclotomic and the elliptic cases. Our idea is to use the close connection between the sums of powers of certain elements and the coefficients of division polynomials via the Newton identities. We also use methods

*Correspondence: komer@metu.edu.tr
2010 *AMS Mathematics Subject Classification:* 11G15, 11G05.

of Robert [6] in order to compute the Hurwitz numbers, which are analogous to the Bernoulli numbers of the cyclotomic case. Our algorithm is easy to implement and performs only a few high-precision computations if the size of the class number of K is small.

In the first section, we define the generalized division polynomials and give the idea behind our algorithm. In Section 2, we describe how Hurwitz numbers attached to an elliptic curve $E : y^2 = x^3 + Ax + B$ can be computed in terms of A and B. In Section 3, we give our main result, which provides a formula for sums of powers of roots of the generalized division polynomials. Finally, in the last section, we give the algorithm described throughout the paper and an example to illustrate it.

2. Division polynomials

The assertions of this section can be found in [8] or [9] unless otherwise stated or proved. Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$ and let H be the Hilbert class field of K. Let E be an elliptic curve define over $H \cap \mathbf{R}$ admitting complex multiplication by $\mathcal{O}_K$. A classical method for constructing such a curve can be found in the work of Lang [5, p. 18]. Suppose that

$$E : y^2 = x^3 + Ax + B$$

for some A, B in the number field $H \cap \mathbf{R}$. We denote the Weierstrass $\wp$-function relative to the lattice Λ by $\wp(z, \Lambda)$. The uniformization theorem for elliptic curves enables us to find a lattice Λ parameterizing E. More precisely, we have a complex analytic isomorphism from $\mathbf{C}/\Lambda$ to E given by the map $z \mapsto (\wp(z, \Lambda), 2\wp'(z, \Lambda))$. The assumption that the coefficients A, B are real enables us to use the PARI command `ellinit` to produce a basis of the lattice Λ.

Given a point P on E, denote its x-coordinate by $x(P)$. If S is a subset of points of E, we set $S_x = \{x(P) : P \in A\}$. Let O be the point at infinity. For any ideal $\mathfrak{f} \subset \mathcal{O}_K$, the group of $\mathfrak{f}$-torsion points of E is defined by

$$E[\mathfrak{f}] = \{P \in E : [\alpha]P = O \text{ for all } \alpha \in \mathfrak{f}\}.$$

Notice that the definition of $E[\mathfrak{f}]$ depends on the isomorphism $\mathcal{O}_K \cong \mathrm{End}(E)$. We always use the isomorphism $[\cdot] : \mathcal{O}_K \to \mathrm{End}(E)$ such that for any invariant differential ω_E of E, $[\alpha]^*\omega_E = \alpha\omega_E$ for all $\alpha \in \mathcal{O}_K$.

Since there is no infinite prime, we can consider any modulus of K as an ideal of $\mathcal{O}_K$. Given an ideal $\mathfrak{f} \subset \mathcal{O}_K$, the ray class field $K_\mathfrak{f}$ of conductor $\mathfrak{f}$ can be generated over H by the division points $E[\mathfrak{f}]$. More precisely, we have the following fundamental theorem of complex multiplication:

$$K_\mathfrak{f} = H(E[\mathfrak{f}]_x).$$

Definition 2.1 *The generalized division polynomial attached to the ideal $\mathfrak{f} \subset \mathcal{O}_K$ is defined by the following product, which is taken over all $\mathfrak{f}$-division points except the point at infinity:*

$$\mathcal{P}_\mathfrak{f}(t) := \prod_{P \in E[\mathfrak{f}]}{}' (t - x(P)).$$

The polynomial $\mathcal{P}_\mathfrak{f}(t)$ is of degree $N(\mathfrak{f}) - 1$ and its coefficients are elements of the Hilbert class field H. In this paper we give an algorithm to compute $\mathcal{P}_\mathfrak{f}(t)$ with no restriction on the conductor $\mathfrak{f}$.

Our strategy is to reduce the problem of determining the polynomial $\mathcal{P}_{\mathfrak{f}}(t)$ to the problem of computing the sum of mth power of x-coordinates of division points

$$p_m(E,\mathfrak{f}) := \sum_{P\in E[\mathfrak{f}]}{}' x(P)^m.$$

The sums $p_m(E,\mathfrak{f})$ are closely related with the division polynomials. To see this, suppose that $\mathcal{P}_{\mathfrak{f}}(t) = \sum_{j=0}^{n}(-1)^j s_j(E,\mathfrak{f})t^{n-j}$ where $s_0(E,\mathfrak{f}) = 1$. The Newton identities play an important role in the theory of symmetric functions by providing a recursive method to switch between two fundamental bases [2]. More precisely, for each $m \in \{1,\dots n\}$, we have

$$ms_m(E,\mathfrak{f}) = \sum_{j=1}^{m}(-1)^{j+1}p_j(E,\mathfrak{f})s_{m-j}(E,\mathfrak{f}). \tag{2.1}$$

3. Hurwitz numbers

In order to provide a formula for $p_m(E,\mathfrak{f})$, we will use Hurwitz numbers and an invariant depending on $\mathfrak{f}$; see Theorem 4.4. In this section, we describe how Hurwitz numbers can be computed in terms of A and B.

Recall that the Weierstrass $\wp$-function (relative to Λ) is defined by the series

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda}{}'\left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right),$$

where the sum is taken over all nonzero elements of Λ. The Eisenstein series of index $2k$ is given as

$$G_{2k}(\Lambda) = \sum_{\lambda\in\Lambda}{}'\frac{1}{\lambda^{2k}},$$

where the sum is taken over all nonzero elements. The series above converges absolutely for $k \geq 2$. The numbers $G_{2k}(\Lambda)$ are also called Hurwitz numbers in an analogous fashion to Bernoulli numbers [6] and appear in the Laurent series expansion of $\wp(z,\Lambda)$. Indeed, we have

$$\wp(z,\Lambda) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}(\Lambda)z^{2k}.$$

A classical corollary of this formula is the following well-known equation:

$$D_z(\wp(z,\Lambda))^2 = 4\wp(z,\Lambda)^3 - 60G_4(\Lambda)\wp - 140G_6(\Lambda). \tag{3.1}$$

The coefficients $G_{2k}(\Lambda)$ can be written in terms of $G_4(\Lambda)$ and $G_6(\Lambda)$ by using the recurrence relation

$$G_k(\Lambda) = \frac{6}{(k-6)(k^2-1)}\sum_{\substack{j=4\\ j \text{ even}}}^{k-4}(j-1)(k-j-1)G_j(\Lambda)G_{k-j}(\Lambda).$$

For example, $G_8(\Lambda) = 3G_4(\Lambda)^2/7, G_{10}(\Lambda) = 5G_6(\Lambda)G_4(\Lambda)/11$. One can prove this recurrence relation by comparing the coefficients in the equation

$$D_z^2(\wp(z,\Lambda)) = 6\wp(z,\Lambda)^2 - 30G_4(\Lambda).$$

See the work of Robert [6].

Recall that we have a complex analytic isomorphism from $\mathbf{C}/\Lambda$ to $E : y^2 = x^3 + Ax + B$ given by the map $z \mapsto (\wp(z,\Lambda), 2\wp'(z,\Lambda))$. Combining this with equation (3.1), we see that $G_4(\Lambda) = -A/15$ and $G_6(\Lambda) = -B/35$. It follows by the above recurrence relation that $G_{2k}(\Lambda)$ is a polynomial in variables A and B with coefficients from rational numbers for all integers $k \geq 2$.

4. Sums of powers

Now we start computing $p_m(E,\mathfrak{f})$. Recall that $p_m(E,\mathfrak{f})$ is defined by a sum over $\mathfrak{f}$-division points. Alternatively we can write this sum as follows:

$$p_m(E,\mathfrak{f}) = \sum_{\omega \in \mathfrak{f}^{-1}\Lambda} \wp(\omega,\Lambda)^m.$$

Note that this sum is weight-$2m$ invariant under the action of $\mathrm{SL}_2(\mathbf{Z})$.

For simplicity let us focus on the case $m = 1$. The basic quasi-period η_2 attached to the Weierstrass $\wp$-function is very close to being a modular function of weight 2 [1]. Given a complex number τ in the upper half plane, set $q = \exp(2\pi i\tau)$. We have

$$\eta_2(\tau) = (2\pi i)^2 \left[\frac{1}{12} - 2\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n} \right].$$

See the work of Lang [5, Chap. 18]. Since $\eta_2(\tau)$ has a q-expansion, it is true that $\eta_2(\tau+1) = \eta_2(\tau)$. On the other hand, one can think of $\eta_2(\tau)$ as the Eisenstein series of weight 2 and write

$$\eta_2(\tau) = \sum_{c \in \mathbf{Z}} \sum_{d \in \mathbf{Z}'_c} \frac{1}{(c\tau + d)^2}$$

where $\mathbf{Z}'_c = \mathbf{Z} - \{0\}$ if $c = 0$ and $\mathbf{Z}'_c = \mathbf{Z}$ otherwise [3]. This double sum is not absolutely convergent and as a result we have

$$\eta_2(-1/\tau) = \tau^2\eta_2(\tau) - 2\pi i\tau.$$

See the work of Apostol [1].

In order to understand $p_1(E,\mathfrak{f})$ in terms of the Eisenstein series, a normalization must be done. Suppose that Λ has a basis $[w_1, w_2]$ with w_1 real and $\tau = w_2/w_1$ in the upper half plane. Given a complex number $z = a + bi$, we set $\mathbf{Im}(z) = b$. The reader is cautioned that the notation G_2 is used for η_2 in [1] and [3]. We follow Robert's notation [6] and define

$$G_2(\Lambda) = \frac{\eta_2(\tau) - \pi/\mathbf{Im}(\tau)}{w_1^2}.$$

The normalized function $G_2(\Lambda)$ is no longer meromorphic; however, it is a weight-2 function invariant under the action of $\mathrm{SL}_2(\mathbf{Z})$ [3]. Moreover, Robert [6] showed that

$$p_1(E,\mathfrak{f}) = G_2\left(\mathfrak{f}^{-1}\Lambda\right) - N(\mathfrak{f})G_2(\Lambda). \tag{4.1}$$

Now we start computing $p_m(E,\mathfrak{f})$ for $m \geq 2$ with the following lemma. Recall that $E : y^2 = x^3 + Ax + B$ is an elliptic curve with $A = -15G_4(\Lambda)$ and $B = -35G_6(\Lambda)$. For simplicity we use $\wp$ instead of $\wp(z,\Lambda)$.

Lemma 4.1 *For any integer* $m \geq 1$,

$$\wp^{m+1} = \frac{D_z^2(\wp^m)}{(2m)(2m+1)} - A\frac{2m-1}{2m+1}\wp^{m-1} - B\frac{2m-2}{2m+1}\wp^{m-2}.$$

Proof The chain and product rules of the derivative give

$$\begin{aligned} D_z^2(\wp^m) &= D_z(m\wp^{m-1}D_z(\wp)) \\ &= m(m-1)\wp^{m-2}D_z(\wp)^2 + m\wp^{m-1}D_z^2(\wp). \end{aligned}$$

Recall that $D_z(\wp)^2 = 4\wp^3 + 4A\wp + 4B$ and $D_z^2(\wp) = 6\wp^2 + 2A$. Taking these polynomial expressions into account and solving for $\wp^{m+1}$, we obtain the above identity. □

We denote the nth derivative of $\wp(z,\Lambda)$ with respect to z by $\wp^{(n)}$. If $n=0$, then $\wp^{(0)}$ is the function $\wp$ itself. We omit the use of Λ below and write G_{2k} instead of $G_{2k}(\Lambda)$. Using Lemma 4.1, we find that

$$\begin{aligned} \wp^0 &= 1, \\ \wp^1 &= \wp^{(0)}/1! + 0, \\ \wp^2 &= \wp^{(2)}/3! + 5G_4, \\ \wp^3 &= \wp^{(4)}/5! + 9G_4\wp^{(0)}/1! + 14G_6, \\ \wp^4 &= \wp^{(6)}/7! + 12G_4\wp^{(2)}/3! + 20G_6\wp^{(0)}/1! + (375/7)G_4^2, \\ \wp^5 &= \wp^{(8)}/9! + 15G_4\wp^{(4)}/5! + 25G_6\wp^{(2)}/3! + 105G_4^2\wp^{(0)}/1! + 280G_4G_6. \end{aligned}$$

Let us denote the constant term appearing in the above expressions by a_m, which depends on Λ. For example, $a_0 = 1, a_1 = 0, a_2 = 5G_4$ and so forth. A consequence of Lemma 4.1 is the fact that a_m satisfies the following recurrence relation for all $m \geq 2$:

$$a_{m+1} = -A\frac{2m-1}{2m+1}a_{m-1} - B\frac{2m-2}{2m+1}a_{m-2}. \tag{4.2}$$

Now our purpose is to give a formula expressing $\wp^m$ as a sum of its derivatives. Inspired by the construction in our previous paper [4], let us define c_{2j}^m as follows:

$$(z^2\wp(z,\Lambda))^m = \sum_{j=0}^{\infty} c_{2j}^m z^{2j}.$$

This definition is possible thanks to fact that $\wp(z,\Lambda)$ is an even function with a pole of order 2 at $z=0$. For example $c_0^1 = 1, c_2^1 = 0$ and $c_{2j}^1 = (2j-1)G_{2j}$ for $j \geq 2$. In general, for $m \geq 1$, we have

$$c_{2j}^{m+1} = \frac{(2j-2m)(2j-2m-1)}{(2m)(2m-1)}c_{2j}^m - A\frac{2m-1}{2m+1}c_{2j-4}^{m-1}B\frac{2m-2}{2m+1}c_{2j-6}^{m-2}, \tag{4.3}$$

which is another consequence of Lemma 4.1. Using the coefficients c_{2j}^m, we can express $\wp^m$ as follows.

Lemma 4.2 *For all $m \geq 1$, we have*

$$\wp^m = a_m + \sum_{k=1}^{m} \frac{c_{2m-2k}^m \wp^{(2k-2)}}{(2k+1)!}.$$

Proof If we subtract the sum above from the function $\wp^m$, we obtain a doubly periodic function with no poles at all. Therefore, it must be a constant by Liouville's theorem. This constant is precisely a_m by definition. □

This lemma reduces the problem of computing $p_m(E, \mathfrak{f})$, to the problem of computing the sum of singular values of derivatives. Indeed we have

$$\sum_{\omega \in \mathfrak{f}^{-1}\Lambda} \frac{\wp^{(2k-2)}(\omega, \Lambda)}{(2k+1)!} = \sum_{\omega \in \mathfrak{f}^{-1}\Lambda}{}' \sum_{\lambda \in \Lambda} \frac{1}{(\omega - \lambda)^{2k}}$$

for $k \geq 2$. It is easy to see that the latter sum is equal to $G_{2k}(\mathfrak{f}^{-1}\Lambda) - G_{2k}(\Lambda)$. Combining this with (4.1), we obtain the following.

Lemma 4.3

$$\sum_{\omega \in \mathfrak{f}^{-1}\Lambda} \frac{\wp^{(2k-2)}(\omega, \Lambda)}{(2k+1)!} = \begin{cases} G_2(\mathfrak{f}^{-1}\Lambda) - N(\mathfrak{f})G_2(\Lambda) \text{ if } k = 1 \\ G_{2k}(\mathfrak{f}^{-1}\Lambda) - G_{2k}(\Lambda) \text{ if } k \geq 2 \end{cases}.$$

The computation of $G_{2k}(\mathfrak{f}^{-1}\Lambda)$ is easy if $\mathfrak{f}$ is principal. Indeed, we have

$$G_{2k}(\alpha^{-1}\Lambda) = \alpha^{2k} G_{2k}(\Lambda)$$

for every integer $k \geq 1$. Moreover, Robert showed in general that

$$G_{2k}(\mathfrak{f}^{-1}\Lambda) = \vartheta(\mathfrak{f}, \Lambda)^{2k} \cdot G_{2k}(\Lambda)^{\sigma_{\mathfrak{f}}}$$

for some $\vartheta(\mathfrak{f}, \Lambda) \in H$ [6]. Here $\sigma_{\mathfrak{f}}$ is the automorphism in $\mathrm{Gal}(H/K)$ corresponding to the ideal class of $\mathfrak{f}$. If $\mathfrak{f}$ is a principal ideal generated by $\alpha \in \mathcal{O}_K$, then we trivially have $\vartheta(\mathfrak{f}, \Lambda)^2 = \alpha^2$. For some nontrivial examples, see Robert's computations focusing on imaginary quadratic fields of class number two [6].

Theorem 4.4 *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve admitting complex multiplication by $\mathcal{O}_K$ and let $\mathfrak{f}$ be an ideal of $\mathcal{O}_K$. Then for each integer $m \geq 1$, we have*

$$p_m(E, \mathfrak{f}) = (a_m - c_{2m-2}^m G_2)(N(\mathfrak{f}) - 1) + \sum_{k=1}^{m} c_{2m-2k}^m \left(G_{2k}^{\sigma_{\mathfrak{f}}} \vartheta^{2k} - G_{2k} \right)$$

where $G_{2k} = G_{2k}(\Lambda)$ and $\vartheta^2 = \vartheta(\mathfrak{f}, \Lambda)^2$.

For example, if we list the first few values of p_m for $m \in \{1, 2, 3\}$ restricted to the case $\mathfrak{f} = (\alpha)$ for some $\alpha \in \mathcal{O}_K$, we see that

$$p_1(E, (\alpha)) = G_2(\alpha^2 - N(\alpha)),$$
$$p_2(E, (\alpha)) = G_4(\alpha^4 + 5N(\alpha) - 6),$$
$$p_3(E, (\alpha)) = G_6(\alpha^6 + 14N(\alpha) - 15) + 9G_4G_2(\alpha^2 - N(\alpha)).$$

In general, for integers $m \geq 1$ we have

$$p_m(E,(\alpha)) = (a_m - c_{2m-2}^m G_2)(N(\alpha)-1) + \sum_{k=1}^{m} c_{2m-2k}^m (\alpha^{2k}-1)G_{2k}.$$

Using the Newton identities (2.1) we can find $s_i(E,(\alpha))$, the coefficients of the generalized division polynomial $\mathcal{P}_{(\alpha)}(t)$, in terms of A, B, G_2, and α. Moreover if $\mathfrak{f} = (f)$ for some integer f, then the G_2 terms vanish and coefficients of $\mathcal{P}_{(f)}(t)$ can be written in terms of A, B over $\mathbf{Q}$.

If $\mathfrak{f}$ is not principal, we can express each $s_i(E,\mathfrak{f})$ algebraically in terms of a basis of H over $\mathbf{Q}$. For this purpose we compute the numerical value of $\vartheta(\mathfrak{f},L)^2$ by the equality

$$\vartheta(\mathfrak{f},\Lambda)^2 = \frac{G_2(\mathfrak{f}^{-1}\Lambda)}{G_2(\Lambda)^{\sigma_{\mathfrak{f}}}}$$

with high precision. Once we choose a basis for H over $\mathbf{Q}$, we can use the PARI command `lindep` in order find a linear dependence between $\vartheta(\mathfrak{f},\Lambda)^2$ and the basis elements.

5. An example and the algorithm

In this section, we provide an example to illustrate the algorithm described throughout the paper. We give the algorithm at the end.

Example 5.1 Let K be the quadratic field with discriminant $d_K = -139$. The class number of K is 3. Set $w = (\sqrt{-139}-1)/2$. Note that $\mathcal{O}_K = \mathbf{Z}[w]$. In order to generate the Hilbert class field over K, one can use the j-invariant of $\mathcal{O}_K$. However, this invariant turns out to be very big. Instead, one can use other functions to generate the same extension. For example, using the PARI command `quadhilbert` we find a root of the polynomial $x^3 - 4x^2 + 6x - 1 = 0$ that generates H over K. Let γ be the unique real root of this polynomial. We have

$$\gamma \approx 0.18946428623386322598.$$

Moreover, $H = K(\gamma) = \mathbf{Q}(w,\gamma)$. There are several ways to obtain a Weierstrass model defined over $H \cap \mathbf{R} = \mathbf{Q}(\gamma)$, which admits complex multiplication by $\mathcal{O}_K$. For example, see [5, p. 18]. We choose $E : y^2 = x^3 + Ax + B$ with

$$A = -580464\gamma^2 + 2211768\gamma - 3063560,$$

$$B = 364736000\gamma^2 - 1389839872\gamma + 1925091898.$$

Comparing $j(w)$ and $j(E)$, one can verify that this elliptic curve E admits complex multiplication by $\mathcal{O}_K = \mathbf{Z}[w]$. Suppose that a basis for the corresponding lattice Λ is given by $[w_1, w_2]$ with w_1 real $\tau = w_2/w_1$ in the upper half plane. Such a lattice can be found by the PARI command `ellinit` since A, B are both real. Moreover, we find that

$$G_2(\Lambda) = -172\gamma^2 + 656\gamma - 908$$

by using the command `lindep`. One can obtain G_{2k}^{σ} in terms of γ and w for $i \in \{1,2,3\}$ and $\sigma \in \mathrm{Gal}(H/K)$. All we need to to is to determine $\sigma(\gamma)$ for $\sigma \in \mathrm{Gal}(H/K)$. This finishes the computations for the ground field.

Now we start computing a generalized division polynomial attached to a conductor $\mathfrak{f}$. Suppose that $\mathfrak{f} = (13, w-5)$, a prime ideal that is not principal. Consider the basis $\{1, \gamma, \gamma^2, w, w\gamma, w\gamma^2\}$ for H over $\mathbf{Q}$. One can show that

$$\sigma_{\mathfrak{f}}(\gamma) = \frac{-2\gamma^2 - 54\gamma + 260 - w(4\gamma^2 - 31\gamma + 36)}{139}$$

where $\sigma_{\mathfrak{f}}$ is the automorphism in $\mathrm{Gal}(H/K)$ corresponding to the ideal class of $\mathfrak{f}$. Note that $\mathbf{Q}(\gamma)$ is not a Galois extension. Thus, it is reasonable to expect that conjugates of γ cannot be written in terms of γ only. We compute $\vartheta(\mathfrak{f}, \Lambda)^2$ with high precision and using the command `lindep` we find that

$$\vartheta(\mathfrak{f}, \Lambda) = \pm\frac{397\gamma^2 - 1652\gamma + 2600 + w(-40\gamma^2 + 171\gamma - 221)}{139}.$$

Now we consider the part of our algorithm that takes the most time if the norm of the conductor $N(\mathfrak{f})$ is large. Using the recurrence relations (4.2) and (4.3), we find the values of all necessary a_i and c_{2i}^m respectively in terms of G_2, G_4, and G_6. Using Theorem 4.4, we find $p_i(E, \mathfrak{f})$ for $0 \le i \le N(\mathfrak{f})$. Afterwards we apply the Newton identities (2.1) and obtain $s_i(E, \mathfrak{f})$ for $0 \le i \le N(\mathfrak{f})$ as well. Therefore, we obtain $\mathcal{P}_{\mathfrak{f}}(t)$ by providing its coefficients in terms of γ and w. Since this polynomial is too big to exhibit here, we only give the first two terms and the last term. We have

$$\mathcal{P}_{\mathfrak{f}}(t) = t^{12} + \left(-16w\gamma^2 + 2296\gamma^2 + 76w\gamma - 8644\gamma - 88w + 11796\right)t^{11} + \ldots$$
$$+ \frac{1}{\vartheta(\mathfrak{f}, \Lambda)^2}\begin{pmatrix} -16457377034724544662283150797648199 68w\gamma^2 \\ -42785375983691544817594335105139875 84\gamma^2 \\ +62711422945732520303528776617641287 68w\gamma \\ +16303520321276858703501503860336459 776\gamma \\ -86862687221224143591603620902223462 40w \\ -22582290749444922390830898249523351552 \end{pmatrix}.$$

The algebraic expression of the constant term of $\mathcal{P}_{\mathfrak{f}}(t)$ would have been very difficult to obtain if we had tried to use the PARI command `lindep` with its numerical value from the beginning. Observe also that if the class number of K gets bigger, it will be harder to obtain $G_2(\Lambda)$ and $\vartheta(\Lambda, \mathfrak{f})$ in terms of γ and w.

We finish our paper by giving the algorithm described throughout the paper.

Algorithm I: Computation of generalized division polynomials

Input: An ideal $\mathfrak{f}$ of an imaginary quadratic field K.
Output: A polynomial $\mathcal{P}_{\mathfrak{f}}(t) \in H[t]$ generating the ray class field $K_{\mathfrak{f}}$ over H.

- **First part** (Computations that are independent from the conductor.)

  1. Find a real element $\gamma \in H$ such that $H = K(\gamma)$.
  2. Find an elliptic curve $E : y^2 = x^3 + Ax + B$ defined over $\mathbf{Q}(\gamma)$ admitting complex multiplication by $\mathcal{O}_K = \mathbf{Z}[w]$.
  3. Compute G_{2i}^{σ} in terms of γ, w for $1 \le i \le 3$ and $\sigma \in \mathrm{Gal}(H/K)$.

- **Second part** (Computations that depend on the conductor.)

  1. Compute a_m and c_{2j}^m for $0 \leq m \leq N(\mathfrak{f})$ and $0 \leq j \leq m$.
  2. Compute $\vartheta(\mathfrak{f},\Lambda)^2$ in terms of γ and w.
  3. Compute the values $p_i(E,\mathfrak{f})$ using Theorem 4.4 for $1 \leq i \leq N(\mathfrak{f})$.
  4. Compute $s_i(E,\mathfrak{f})$ using the Newton identities (2.1) for $1 \leq i \leq N(\mathfrak{f})$.
  5. Return $\mathcal{P}_{\mathfrak{f}}(t) = \sum_{j=0}^{n}(-1)^j s_j(E,\mathfrak{f})t^{n-j}$.

References

[1] Apostol TM. Modular Functions and Dirichlet Series in Number Theory. Graduate Texts in Mathematics 41. 2nd ed. Berlin, Germany: Springer-Verlag, 1990.

[2] Cox DA, Little J, O'Shea D. Ideals, Varieties, and Algorithms. New York, NY, USA: Springer-Verlag, 1997.

[3] Diamond F, Shurman J. A First Course in Modular Forms. Graduate Texts in Mathematics 228. Berlin, Germany: Springer-Verlag, 2005.

[4] Küçüksakallı Ö. A recurrence relation for Bernoulli numbers. Hacet J Math Stat 2013; 42: 319–329.

[5] Lang S. Elliptic Functions. Graduate Texts in Mathematics 112. 2nd ed. Berlin, Germany: Springer-Verlag, 1987.

[6] Robert G. Unités elliptiques. Bulletin de la Societe Mathematique de France Memoire 36. Paris, France: Societe Mathematique de France, 1973 (in French).

[7] Satoh T. Generalized division polynomials. Math Scand 2004; 94: 161–184.

[8] Silverman JH. The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 106. Berlin, Germany: Springer-Verlag, 1986.

[9] Silverman JH. Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 151. Berlin, Germany: Springer-Verlag, 1994.