Metadata of the chapter that will be visualized online

Chapter Title	Revisiting the Complex Multiplication Method for the Construction of Elliptic Curves	
Copyright Year	2015	
Copyright Holder	Springer International Publishing Switzerland	
Author	Family Name	**Konstantinou**
	Particle	
	Given Name	**Elisavet**
	Suffix	
	Email	ekonstantinou@aegean.gr
Author	Family Name	**Kontogeorgis**
	Particle	
	Given Name	**Aristides**
	Suffix	
	Email	kontogar@math.uoa.gr
Abstract	In this article we give a detailed overview of the Complex Multiplication (CM) method for constructing elliptic curves with a given number of points. In the core of this method, there is a special polynomial called Hilbert class polynomial which is constructed with input a fundamental discriminant $d < 0$. The construction of this polynomial is the most demanding and time-consuming part of the method and thus the use of several alternative polynomials has been proposed in previous work. All these polynomials are called *class polynomials* and they are generated by proper values of modular functions called *class invariants*. Besides an analysis on these polynomials, in this paper we will describe our results about finding new class invariants using the Shimura reciprocity law. Finally, we will see how the choice of the discriminant can affect the degree of the class polynomial and consequently the efficiency of the whole CM method.	

Revisiting the Complex Multiplication Method for the Construction of Elliptic Curves

Elisavet Konstantinou and Aristides Kontogeorgis

Abstract In this article we give a detailed overview of the Complex Multiplication (CM) method for constructing elliptic curves with a given number of points. In the core of this method, there is a special polynomial called Hilbert class polynomial which is constructed with input a fundamental discriminant $d < 0$. The construction of this polynomial is the most demanding and time-consuming part of the method and thus the use of several alternative polynomials has been proposed in previous work. All these polynomials are called *class polynomials* and they are generated by proper values of modular functions called *class invariants*. Besides an analysis on these polynomials, in this paper we will describe our results about finding new class invariants using the Shimura reciprocity law. Finally, we will see how the choice of the discriminant can affect the degree of the class polynomial and consequently the efficiency of the whole CM method.

AQ1

1 Introduction

Complex Multiplication (CM) method is a well-known and efficient method for the construction of elliptic curves with a given number of points. In cryptographic applications, it is required that the order of the elliptic curves satisfies several restrictions and thus CM method is a necessary tool for them. Essentially, CM method is a way

The authors were partially supported by the Project "*Thalis, Algebraic modeling of topological and computational structures*". The Project "THALIS" is implemented under the Operational Project "Education and Life Long Learning"and is co-funded by the European Union (European Social Fund) and National Resources (ESPA).

AQ2

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

A. Kontogeorgis
Department of Mathematics, University of Athens, Panepistimioupolis, 15784 Athens, Greece
e-mail: kontogar@math.uoa.gr

N.J. Daras, M.Th. Rassias (eds.), *Computation, Cryptography, and Network Security*, DOI 10.1007/978-3-319-18275-9_12

to use elliptic curves defined over the field of complex numbers in order to construct elliptic curves defined over finite fields with a given number of points. Therefore, we will begin our article by giving a brief introduction to the theory of elliptic curves over a field K, which for our purposes will be either the finite field $\mathbb{F}_p$ or the field of complex numbers $\mathbb{C}$.

We describe the CM method using first the classical j-invariant and its corresponding Hilbert polynomial. Hilbert polynomial is constructed with input a fundamental discriminant $d < 0$. The disadvantage of Hilbert polynomials is that their coefficients grow very large as the absolute value of the discriminant $D = |d|$ increases and thus their construction requires high precision arithmetic and a huge amount of disk space to store and manipulate them.

Supposing that f is a modular function, such that $f(\tau)$ for some $\tau \in \mathbb{Q}(\sqrt{-D})$ generates the Hilbert class field of $\mathbb{Q}(\sqrt{-D})$, then its minimal polynomial can substitute the Hilbert polynomial in the CM method and the value $f(\tau)$ is called *class invariant*. These minimal polynomials are called *class polynomials*, their coefficients are much smaller than their Hilbert counterparts and their use can considerably improve the efficiency of the whole CM method. Some well-known families of class polynomials are: Weber polynomials [28], $M_{D,l}(x)$ polynomials [24], Double eta (we will denote them by $M_{D,p_1,p_2}(x)$) polynomials [7] and Ramanujan polynomials [20]. The logarithmic height of the coefficients of all these polynomials is smaller by a constant factor than the corresponding logarithmic height of the Hilbert polynomials and this is the reason for their much more efficient construction.

In what follows, we will present our contribution on finding alternative class invariants (instead of the classical j-invariant) which can considerably improve the efficiency of the CM method. Also we will see how the choice of the discriminant can affect the efficiency of the class polynomials' construction.

2 Preliminaries

The theory of elliptic curves is a huge object of study and the interested reader is referred to [2, 30] and references within for more information. An *elliptic curve* defined over a field K of characteristic $p > 3$ is the set of all points $(x, y) \in K \times K$ (in affine coordinates) which satisfy an equation

$$y^2 = x^3 + ax + b \tag{1}$$

where $a, b \in K$ satisfy $4a^3 + 27b^2 \neq 0$, together with at special point O_E which is called the point at infinity. The set $E(K)$ of all points can be naturally equipped with a properly defined addition operation and it forms an abelian group (see [3],38] for more details on this group).

AQ3

An elliptic curve $E(\mathbb{F}_q)$ defined over a finite field $\mathbb{F}_q$ is then a finite abelian group and as such it is isomorphic to a product of cyclic groups:

$$E(\mathbb{F}_q) \cong \prod_{i=1}^{s} \mathbb{Z}/n_i\mathbb{Z}.$$

The arithmetic complexity of this elliptic curve is reduced to the smallest cyclic factor of the above decomposition. For example, we can have an elliptic curve of huge order which is the product of a large amount of cyclic groups of order 2. The discrete logarithm problem is trivial for this curve. For cryptographic algorithms, we would like to have elliptic curves which do not admit small cyclic factors and even better elliptic curves which have order a large prime number. This forces the curve to consist of only one cyclic factor.

In order to construct an elliptic curve with a proper order, we can either generate random elliptic curves, compute their order and then check their properties or we can use a method which constructs elliptic curves with a given order which we known beforehand that satisfies our restrictions. In this article we will use the second approach and present the method of Complex Multiplication. This method uses the theory of elliptic curves defined over the field of complex numbers in order to construct elliptic curves over finite fields having the desired order.

Definition 1. A lattice L in the field of complex numbers is the set which consists of all linear $\mathbb{Z}$-combinations of two $\mathbb{Z}$-linearly independent elements $e_1, e_2 \in \mathbb{C}$.

Given a lattice L Weierstrass defined a function $\wp$ depending on the lattice L

$$\wp : \mathbb{C} \to \mathbb{C}$$

by the formula:

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\lambda \in L - \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

The function $\wp$ satisfies the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L).$$

Therefore the pair $(x, y) = (\wp(z), \wp'(z))$ parametrizes the elliptic curve

$$y^2 = 4x^3 - g_2(L)x - g_3(L).$$

Remark 1. The transcendental functions $(x, y) = (\sin(x), \cos(x)) = (\sin(x), \sin'(x))$ satisfy the equation $x^2 + y^2 = 1$, therefore they parametrise the unit circle.

The function $\wp$ is periodic with period the lattice L, i.e.

$$(\wp(z+\lambda), \wp'(z+\lambda)) = (\wp(z), \wp'(z)) \text{ for every } \lambda \in L.$$

At the level of group theory this means that

$$\frac{\mathbb{C}}{L} \cong E(\mathbb{C}).$$

From the topological viewpoint, this means that the fundamental domain of the lattice, i.e. the set

$$z = ae_1 + be_2 : 0 \le a, b < 1$$

covers the elliptic curve while the border is glued together giving to the elliptic curve the shape of a "donut".

The functions $g_2(L), g_3(L)$ depend on the lattice L, and are given by the formula

$$g_2(L) = 60 \sum_{\lambda \in L - \{0\}} \frac{1}{\lambda^4} \qquad g_3(L) = 140 \sum_{\lambda \in L - \{0\}} \frac{1}{\lambda^6}.$$

2.1 Algebraic Theory of the Equation $y^2 = x^3 + ax + b$

In this paragraph we will study certain invariants of the elliptic curve given by the equation:

$$y^2 = x^3 + ax + b.$$

For every polynomial of one variable $f(x)$ we can define the discriminant. This is a generalization of the known discriminant of a quadratic polynomial and is equal to zero if and only if the polynomial f has a double root.

For the special case of the cubic polynomial $x^3 + ax + b$ the discriminant is given by the formula: $-16(4a^3 + 27b^2)$. We observe that by definition all elliptic curves have non-zero discriminant.

The j-invariant of the elliptic curve is defined by:

$$j(E) = \frac{(4a)^3}{4a^3 + 27b^2} = -\frac{4a^3}{\Delta(E)}.$$

Proposition 1. *Two elliptic curves defined over an algebraically closed field are isomorphic if and only if have the same j-invariant.*

This proposition does not hold if the elliptic curves are considered over a non-algebraically closed field k. They became isomorphic over a quadratic extension of k.

Proposition 2. *For every integer $j_0 \in K$ there is an elliptic curve E defined over K with j-invariant equal to j_0.*

Proof. If $j \neq 0, 1728$, then the elliptic curve defined by

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

has discriminant

$$\Delta(E) = \frac{j_0^3}{(j_0 - 1728)^3} \text{ and } j(E) = j_0.$$

When $j_0 = 0$ we consider the elliptic curve:

$$E : y^2 + y = x^3, \text{ with } \Delta(E) = -27 \text{ and } j = 0$$

while for j_0 we consider the elliptic curve:

$$E : y^2 = x^3 + x, \text{ with } \Delta(E) = -64 \text{ and } j = 1728.$$

Proposition 3. *Every element in the finite field $\mathbb{F}_p$ is the j-invariant of an elliptic curve defined over $\mathbb{F}_p$. For $j \neq 0, 1728$ this elliptic curve is given by*

$$y^2 = x^3 + 3kc^2x + 2kc^3,$$

for $k = j/(1728-j)$ and c an arbitrary element in $\mathbb{F}_p$. There are two non-isomorphic elliptic curves E, E′ over $\mathbb{F}_p$ which correspond to different values of c. They have orders

$$|E| = p + 1 - t \text{ and } |E| = p + 1 + t.$$

In this section we consider the lattices generated by $1, \tau$, where $\tau = a + ib$ is a complex number with $b > 0$. The set of such τ's is called the hyperbolic plane and it is generated by $\mathbb{H}$. In this setting the Eisenstein series, the discriminant and the j-invariant defined above (which depend on L) can be seen as functions of τ.

Proposition 4. *The functions g_2, g_3, Δ, j seen as functions of $\tau \in \mathbb{H}$ remain invariant under transformations of the form:*

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

In particular these functions remain invariant under the transformation $\tau \mapsto \tau + 1$ so they are periodic. Hence they admit a Fourier expansion. In the coefficients of the Fourier expansion there is "hidden arithmetic information". For example, the Fourier expansion of the j-invariant function is given by:

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots,$$

where $q = e^{2\pi i \tau}$.

Definition 2. We will say that the function $f : E \to E$ is an endomorphism of the elliptic curve if it can be expressed in terms of rational functions and moreover $f(O_E) = O_E$, where O_E is the neutral element of the elliptic curve.

The set of endomorphisms will be denoted by $\mathrm{End}(E)$ and it has the structure of a ring where addition is the natural addition of functions and multiplication is composition of functions.

If we fix an integer $n \in \mathbb{Z}$, then we can define the endomorphism sending $P \in E$ to nP. In this way $\mathbb{Z}$ becomes a subring of $\mathrm{End}(E)$.

For most elliptic curves defined over fields of characteristic 0, $\mathrm{End}(E) = \mathbb{Z}$. For elliptic curves defined over the finite field $\mathbb{F}_q$, there is always an extra endomorphism the so-called Frobenious endomorphism ϕ, which is defined as follows:

The element $P \in E$ with coordinates (x, y) is mapped to the element $\phi(P)$ with coordinates (x^q, y^q). This endomorphism is interesting because we know that $x \in \bar{\mathbb{F}}_q$ is an element in $\mathbb{F}_q$ if and only if $x^q = x$. So the elements which remain invariant under the action of the Frobenious endomorphism are exactly the points of the elliptic curve over the finite field $\mathbb{F}_p$.

Proposition 5. *The Frobenious endomorphism Φ satisfies the relation*

$$\phi^2 - t\phi + q = 0, \tag{2}$$

where t is an integer called the "trace of Frobenious".

Theorem 1 (H. Hasse). *The trace of Frobenious satisfies*

$$|t| \leq 2\sqrt{q}.$$

Proposition 6. *For a general elliptic curve if there is an extra endomorphism ϕ then it satisfies an equation of the form:*

$$\phi^2 + a\phi + b = 0,$$

with negative discriminant (the term "complex multiplication" owes his name to this fact).

Remark 2. The bound of Hasse is equivalent to the fact that the quadratic equation (2) satisfied by Frobenious has negative discriminant.

Let $\tau \in \mathbb{H}$, for example the one which satisfies the relation

$$\tau^2 - t\tau + q = 0$$

for a negative discriminant D. The theorem of complex multiplication asserts that $j(\tau)$ satisfies an a polynomial $f(x) \in \mathbb{Z}[x]$ end that the elliptic curve E_τ, has j-invariant $j(\tau)$ end endomorphism ring $\mathrm{End}(E_\tau) = \mathbb{Z}[\tau]$.

Moreover, if we reduce the polynomial $f(x)$ modulo p, then the roots of the reduced polynomials are j-invariants which correspond to elliptic curves $\mathbb{F}_p$ with Frobenious endomorphisms ϕ satisfying $\phi^2 - t\phi + q = 0$.

K.F. Gauss in his work Disquisitiones Arithmeticae [9] studied the quadratic forms of discriminant D of the form

$$ax^2 + bxy + cy^2; b^2 - 4ac = -D, a, b, c \in \mathbb{Z} \;\; (a, b, c) = 1,$$

up to the following equivalence relation which in modern language can be defined as: two quadratic forms $f(x, y)$ and $g(x, y)$ are equivalent if there is a transformation $\tau \in \mathrm{SL}(2, \mathbb{Z})$ such that

$$\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } f(x, y) = g(ax + by, cx + dy).$$

For more information on this classical subject, we refer to [6].

A full set of representatives $\mathrm{CL}(D)$ of the equivalence classes are the elements (a, b, c) such that

$$|b| \le a \le \sqrt{\frac{D}{3}}, a \le c, (a, b, c) = 1, b^2 - 4ac = -D$$

if $|b| = a$ or $a = c$ then $b \ge 0$.

Theorem 2. *Consider $\tau \in \mathbb{H}$ which satisfies a monic quadratic polynomial in $\mathbb{Z}[x]$. Consider the elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ which has j-invariant $j(\tau)$.*

The complex number $j(\tau)$ satisfies an algebraic equation given by:

$$H_D(x) = \prod_{[a,b,c] \in \mathrm{CL(D)}} \left(x - j\left(\frac{-b + \sqrt{-D}}{2a} \right) \right) \in \mathbb{Z}[x].$$

Moreover a root of the reduction of the polynomial $H_D(x)$ modulo p corresponds to an elliptic curve with Frobenious endomorphism sharing the same characteristic polynomial with τ.

Example. For $D = 491$ we have compute the following equivalence classes for quadratic forms of discriminant -491

$$\mathrm{CL}(D) = [1, 1, 123], [3, \pm 1, 41], [9, \pm 7, 15], [5, \pm 3, 25], [11, \pm 9, 3].$$

For each of the above $[a, b, c]$ we compute the root

$$\rho = \frac{-b + i\sqrt{491}}{2s},$$

of positive imaginary part.

This computation is summarized to the following table:

$[a, b, c]$	Root	j-invariant
$[1, 1, 123]$	$\rho_1 = (-1 + i\sqrt{491})/2$	$-1.7082855E30$
$[3, 1, 41]$	$\rho_2 = (-1 + i\sqrt{491})/6$	5.977095 E9 + 1.0352632 E10I
$[3, -1, 41]$	$\rho_3 = (1 + i\sqrt{491})/6$	5.9770957 E9 − 1.0352632 E10I
$[9, 7, 15]$	$\rho_4 = (-7 + i\sqrt{491})/18$	−1072.7816 + 1418.3793I
$[9, -7, 15]$	$\rho_5 = (7 + i\sqrt{491})/18$	−1072.7816 −1418.3793I
$[5, 3, 25]$	$\rho_6 = (-3 + i\sqrt{491})/10)$	−343205.38 + 1058567.0I
$[5, -3, 25]$	$\rho_7 = (3 + i\sqrt{491})/10$	−343205.38 − 1058567.0I
$[11, 9, 13]$	$\rho_8 = (-9 + i\sqrt{491})/22$	6.0525190 + 170.50800I
$[11, -9, 13]$	$\rho_9 = (9 + i\sqrt{491})/22$	6.0525190 − 170.50800I

We can now compute the polynomial

$$f(x) = \prod_{i=1}^{9} (x - j(\rho_i))$$

with 100-digit precision and we arrive at

```
x^9 + (1708285519938293560711165050880.0 + 0.E-105*I)*x^8 +
(-20419995943814746224552691418802908299264.0 + 5.527 E-76*I)*x^7 +
(244104497665432748158715313783583130211556702289920.0 - 3.203 E-66*I)*x^6 +
(168061099707176489267621705337969352389335280404863647744.0 - 8.477 E-61*I)*x^5 +
(302663406228710339993356777425938984884433281603698934574743552.0 + 1.179E-53*I)*x^4 +
(645485900085616784926354786035581108920923697188375949395393249280.0 + 5.552 E-50*I)*x^3 +
(957041138046397870965520808576552949198885665738183643750394920697856.0 - 1.530 E-47*I)*x^2 +
(7322862871033784419236596129273250845529108502221762556507445472002048.0 + 4.458 E-45*I)*x +
(27831365943253888043128977216106999444228139865055751457267582234307592192.0 - 3.587 E-43*I)
```

which we recognize as a polynomial with integer coefficients (all complex coefficients multiplied by 10^{-40} or a smaller power are considered to be zero and are just floating point approximation garbage).

3 Complex Multiplication Method and Shimura Reciprocity Law

We would like to construct an elliptic curve defined over the finite field $\mathbb{F}_p$ with order $p + 1 - m$. For this case, we must construct the appropriate $j \in \mathbb{F}_p$. The bound of Hasse gives us that $Z := 4p - (p + 1 - m)^2 \geq 0$. We write $Z = Dv^2$ as a square v^2 times a number D which is squarefree.

The equation $4p = u^2 + Dv^2$ for some integer u satisfies $m = p + 1 \pm u$. The negative integer$-D$ is called the CM-discriminant for the prime p.

We have $x^2 - \mathrm{tr}(\phi)x + p \mapsto \Delta = \phi(F)^2 - 4p = -Dv^2$.

Algorithm:

1. Select a prime p. Select the least D together with $u, v \in \mathbb{Z}$ such that $4p = u^2 + Dv^2$.
2. If one of the values $p + 1 - u, p + 1 + u$ is a prime number, then we proceed to the next steps, otherwise we go back to step 1.
3. We compute the Hilbert polynomial $H_D(x) \in \mathbb{Z}[x]$ using floating approximations of the j-invariant.
4. Reduce modulo p and find a root of $H_D(x) mod p$. This root is the desired j-invariant. The elliptic curve corresponding to j-invariant $j \neq 0, 1728$ is

$$y^2 = x^3 + 3kc^2x + 2kc^3, k = j/(1728 - j), c \in \mathbb{F}_p.$$

To different values of c correspond two different elliptic curves E, E' which have orders $p + 1 \pm t$. One is

$$y^2 = x^3 + ax + b$$

and the other is

$$y^2 = x^3 + ac^2x + bc^3,$$

where c is a quadratic non-residue in $\mathbb{F}_p$. In order to select the elliptic curve with the correct order we choose a point P in one of them and we compute its order, i.e. the natural number n such that $nP = O_E$. This order should divide either $p + 1 - t$ or $p + 1 + t$.

The CM method for every discriminant D requires the construction of polynomial $H_D(x) \in \mathbb{Z}[x]$ (called the Hilbert polynomial)

$$H_D(x) = \prod_{\tau}(x - j(\tau)),$$

for all values $\tau = (-b + \sqrt{-D})/2a$ for all integers $[a, b, c]$ running over a set of representatives of the group of equivalent quadratic forms.

Let h be the order of $\mathrm{Cl}(D)$. It is known that the bit precision required of the generation of $H_D(x)$ (see [23]):

$$\mathrm{H-Prec}(D) \cong \frac{\ln 10}{\ln 2}(h/4 + 5) + \frac{\pi\sqrt{D}}{\ln(2)} \sum_{\tau} \frac{1}{a}.$$

The most demanding step of the CM-method is the construction of the Hilbert polynomial, as it requires high precision floating point and complex arithmetic. As the value of the discriminant D increases, the coefficients of the grow extremely large and their computation becomes more inefficient.

In order to overcome this difficulty, alternative class functions were proposed by several authors. It was known in the literature [14, 32, 33] that several other complex valued functions can be used in order to construct at special values the Hilbert class field. Usually one tries functions of the form

$$\frac{\eta(p\tau)}{\eta(\tau)} \text{ or } \frac{\eta(p\tau)\eta(q\tau)}{\eta(pq\tau)\eta(\tau)},$$

where η is the Dedekind zeta function defined by

$$\eta(\tau) = e^{2\pi i\tau/24} \prod_{n\geq 1}(1-q^n), \tau \in \mathbb{C}, \mathrm{Im}(\tau) > 0, q = e^{2\pi i\tau}.$$

All such constructions have the Shimura reciprocity law as ingredient or can be written in this language. This technique was proposed by Shimura [29], but it was Gee and Stevenhagen [10–12, 31] who put it in form suitable for applications. In order to define Shimura reciprocity law, we have to define some minimum amount of the theory of modular functions.

Consider the group $\mathrm{SL}(2,\mathbb{Z})$ consisted by all 2×2 matrices with integer entries and determinant 1. It is known that an element

$$\sigma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$$

acts on the upper complex plane $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ by Möbius transformations by

$$\sigma z = \frac{az+b}{cz+d}.$$

Moreover it is known that $\mathrm{SL}(2,\mathbb{Z})$ can be generated by the elements $S : z \mapsto -\frac{1}{z}$ and $T : z \mapsto z+1$. Let $\Gamma(N)$ be the kernel of the map $\mathrm{SL}(2,\mathbb{Z}) \mapsto \mathrm{SL}\,(2,\mathbb{Z}/N\mathbb{Z})$.

Let $\mathbb{H}^*$ be the upper plane $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. One can show that the quotient $\Gamma(N)\backslash\mathbb{H}^*$ has the structure of a compact Riemann surface which can be described as an algebraic curve defined over the field $\mathbb{Q}(\zeta_N)$, where ζ_N is a primitive N-th root of unity. We consider the function field F_N of this algebraic curve defined over $\mathbb{Q}(\zeta_N)$. The function field F_N is acted on by

$$\Gamma(N)/\{\pm 1\} \cong \mathrm{Gal}(F_N/F_1(\zeta_N)).$$

For an element $d \in \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^*$ we consider the automorphism $\sigma_d : \zeta_N \mapsto \zeta_N^d$. Since the Fourier coefficients of a function $h \in F_N$ are known to be in $\mathbb{Q}(\zeta_N)$, we consider the action of σ_d on F_N by applying σ_d on the Fourier coefficients of h. In this way we define an arithmetic action of

$$\mathrm{Gal}(F_1(\zeta_N)/F_1) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^*,$$

on F_N. We have an action of the group $\mathrm{GL}\left(2, \frac{\mathbb{Z}}{N\mathbb{Z}}\right)$ on F_N that fits in the following short exact sequence.

$$1 \to \mathrm{SL}\left(2, \frac{\mathbb{Z}}{N\mathbb{Z}}\right) \to \mathrm{GL}\left(2, \frac{\mathbb{Z}}{N\mathbb{Z}}\right) \xrightarrow{\det} \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^* \to 1.$$

The following theorem by A. Gee and P. Stevehagen is based on the work of Shimura:

Theorem 3. *Let $\mathcal{O} = \mathbb{Z}[\theta]$ be the ring of integers of an imaginary quadratic number field K of discriminant $d < -4$. Suppose that a modular function $h \in F_N$ does not have a pole at θ and $\mathbb{Q}(j) \subset \mathbb{Q}(h)$. Denote by $x^2 + Bx + C$ the minimum polynomial of θ over $\mathbb{Q}$. Then there is a subgroup $W_{N,\theta} \subset \mathrm{GL}\left(2, \frac{\mathbb{Z}}{N\mathbb{Z}}\right)$ with elements of the form:*

$$W_{N,\theta} = \left\{ \begin{pmatrix} t - Bs & -Cs \\ s & t \end{pmatrix} \in \mathrm{GL}\left(2, \frac{\mathbb{Z}}{N\mathbb{Z}}\right) : t\theta + s \in (\mathcal{O}/N\mathcal{O})^* \right\}.$$

The function value $h(\theta)$ is a class invariant if and only if the group $W_{N,\theta}$ acts trivially on h.

Proof. [10, cor. 4].

The above theorem can be applied in order to show that a modular function gives rise to a class invariant and was used with success in order to prove that several functions were indeed class invariants. Also A. Gee and P. Stevenhagen provided us with an explicit way of describing the Galois action of $\mathrm{Cl}(\mathcal{O})$ on the class invariant so that we can construct the minimal polynomial of the ring class field.

The authors have used in [19] this technique in order to prove a claim of S. Ramanujan that the function

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

gives rise to class invariants. Ramanujan managed somehow (we are only left with the final result written in his notebook) to compute the first class polynomials corresponding to this class invariant and many years later, Berndt and Chan [4] proved that these first polynomials where indeed class invariants and the class polynomials written by Ramanujan were correct. We would like to notice that these Ramanujan invariants proved to be one of the most efficient invariants for the construction of prime order elliptic curves [20, 21] if one uses the CM method.

We will present now an algorithm which will allow us not only to check that a modular function is a class invariant but also to find bases of vector spaces of them. Let V be a finite dimensional vector space consisting of modular functions of level N so that $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ acts on V.

Example 1 (Generalized Weber Functions). An example of such a vector space of modular form is given by the generalized Weber functions defined as:

$$\nu_{N,0} := \sqrt{N}\frac{\eta \circ \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}}{\eta} \text{ and } \nu_{k,N} := \frac{\eta \circ \begin{pmatrix} 1 & k \\ 0 & N \end{pmatrix}}{\eta}, 0 \leq k \leq N-1. \tag{3}$$

These are known to be modular functions of level $24N$ [11, th5. p.76]. Notice that $\sqrt{N} \in \mathbb{Q}(\zeta_N) \subset \mathbb{Q}(\zeta_{24 \cdot N})$ and an explicit expression of $\sqrt{N}$ in terms of ζ_N can be given by using Gauss sums [8, 3.14 p. 228].

The group $\mathrm{SL}(2, \mathbb{Z})$ acts on the $(N+1)$-th dimensional vector space generated by them. In order to describe this action we have to describe the action of the two generators S, T of $\mathrm{SL}(2, \mathbb{Z})$ given by $S : z \mapsto -\frac{1}{z}$ and $T : z \mapsto z + 1$. Keep in mind that

$$\eta \circ T(z) = \zeta_{24}\eta(z) \text{ and } \eta \circ S(z) = \zeta_8^{-1}\sqrt{iz}\eta(z).$$

We compute that (see also [11, p.77])

$$\nu_{N,0} \circ S = \nu_{0,N} \text{ and } \nu_{N,0} \circ T = \zeta_{24}^{N-1}\nu_{N,0},$$
$$\nu_{0,N} \circ S = \nu_{N,0} \text{ and } \nu_{0,N} \circ T = \zeta_{24}^{-1}\nu_{1,N},$$

for $1 \leq k < N - 1$ and N is prime

$$\nu_{k,N} \circ S = \left(\frac{-c}{n}\right) i^{\frac{1-n}{2}} \zeta_{24}^{N(k-c)} \text{ and } \nu_{k,N} \circ T = \zeta_{24}^{-1}\nu_{k+1,N},$$

where $c = -k^{-1} \mod N$. The computation of the action of S on η is the most difficult, see [14, eq. 8 p.443].

Notice that every element $a \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ can be written as $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$. The group $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ is generated by the elements S and T. The action of S on functions $g \in V$ is defined to be $g \circ S = g(-1/z) \in V$ and the action of T is defined $g \circ T = g(z+1) \in V$.

So in order to define the action of $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ we first use the decomposition based on Chinese remainder theorem:

$$\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) = \prod_{p|N} \mathrm{GL}(2, \mathbb{Z}/p^{v_p(N)}\mathbb{Z}),$$

where $v_p(N)$ denotes the power of p that appears in the decomposition in prime factors. Working with the general linear group over a field has advantages and one can use lemma 6 in [10] in order to express an element of determinant one in $\mathrm{SL}(2, \mathbb{Z}/p^{v_p(N)}\mathbb{Z})$ as word in elements S_p, T_p where S_p and T_p are 2×2 matrices which reduce to S and T modulo $p^{v_p(N)}$ and to the identity modulo $q^{v_q(N)}$ for prime divisors q of N, $p \neq q$.

This way the problem is reduced to the problem of finding the matrices S_p, T_p (this is easy using the Chinese remainder Theorem), and expressing them as products of S, T. For more details and examples, the reader is referred to the article of the second author [22].

The action of the matrix $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ is given by the action of the elements

$$\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$$

on the Fourier coefficients of the expansion at the cusp at infinity [10].

4 Class Invariants and Invariant Theory

Since every element in $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ can be written as a word in S, T we obtain a function ρ

$$\begin{tikzcd} \left(\frac{\mathscr{O}}{N\mathscr{O}}\right)^* \arrow[r, "\phi"] \arrow[rr, bend left, "\rho"] & \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \arrow[r] & \mathrm{GL}(V), \end{tikzcd} \tag{4}$$

where ϕ is the natural homomorphism given by Theorem 3.

The map ρ defined above is not a homomorphism but a cocycle. Indeed, if $e_1, \ldots, e_m$ is a basis of V, then the action of σ is given in matrix notation as

$$e_i \circ \sigma = \sum_{\nu=1}^{m} \rho(\sigma)_{\nu,i} e_\nu,$$

and then since $(e_i \circ \sigma) \circ \tau = e_i \circ (\sigma\tau)$ we obtain

$$e_i \circ (\sigma\tau) = \sum_{\nu,\mu=1}^{m} \rho(\sigma)_{\nu,i}^{\tau} \rho(\tau)_{\mu,\nu} e_\mu.$$

Notice that the elements $\rho(\sigma)_{\nu,i} \in \mathbb{Q}(\zeta_N)$ and $\tau \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ acts on them as well by the element $\sigma_{\det(\tau)} \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. So we arrive at the following:

Proposition 7. *The map ρ defined in Eq. (4) satisfies the cocycle condition*

$$\rho(\sigma\tau) = \rho(\tau)\rho(\sigma)^{\tau} \tag{5}$$

and gives rise to a class in $H^1(G, \mathrm{GL}(V))$, where $G = (\mathscr{O}/N\mathscr{O})^*$. The restriction of the map ρ in the subgroup H of G defined by

$$H := \{x \in G : \det(\phi(x)) = 1\}$$

is a homomorphism.

The basis elements $e_1, \dots e_m$ are modular functions. There is a natural notion of multiplication for them so we consider them as elements in the polynomial algebra $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]$. The group H acts on this algebra in terms of the linear representation ρ (recall that ρ when restricted to H is a homomorphism).

Classical invariant theory provides us with effective methods (Reynolds operator method,linear algebra method [17]) in order to compute the ring of invariants $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]^H$. Also there is a well-defined action of the quotient group $G/H \cong \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]^H$.

Define the vector space V_n of invariant polynomials of given degree n:

$$V_n := \{F \in \mathbb{Q}(\zeta_N)[e_1, \dots, e_m]^H : \deg F = n\}.$$

The action of G/H on V_n gives rise to a cocycle

$$\rho' \in H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_N))/\mathbb{Q}), \mathrm{GL}(V_n)).$$

The multidimensional Hilbert 90 theorem asserts that there is an element $P \in \mathrm{GL}(V_n)$ such that

$$\rho'(\sigma) = P^{-1}P^{\sigma}. \tag{6}$$

Let $v_1, \dots, v_\ell$ be a basis of V_n. The elements v_i are by construction H invariant. The elements $w_i := v_i P^{-1}$ are G/H invariant since

$$(v_i P^{-1}) \circ \sigma = (v_i \circ \sigma)(P^{-1})^{\sigma} = v_i \rho(\sigma)(P^{-1})^{\sigma} = v_i P^{-1} P^{\sigma} (P^{-1})^{\sigma} = v_i P^{-1}.$$

The above computation together with Theorem 3 allows us to prove

Proposition 8. *Consider the polynomial ring $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]$ and the vector space V_n of H-invariant homogenous polynomials of degree n. If P is a matrix such that Eq. (6) holds, then the images of a basis of V_n under the action of P^{-1} are class invariants.*

For computing the matrix P so that Eq. (6) holds one can use the probabilistic algorithm of Glasby-Howlett [13]. In this method one starts with the sum

$$B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^{\sigma}. \tag{7}$$

We have to find 2×2 matrix in $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ such that B_Q is invertible then $P := B_Q^{-1}$. Indeed, we compute that

$$B_Q^{\tau} = \sum_{\sigma \in G/H} \rho(\sigma)^{\tau} Q^{\sigma\tau}, \tag{8}$$

and the cocycle condition $\rho(\sigma\tau) = \rho(\sigma)^{\tau}\rho(\tau)$, together with Eq. (8) allows us to write:

$$B_Q^{\tau} = \sum_{\sigma \in G/H} \rho(\sigma\tau)\rho(\tau)^{-1} Q^{\sigma\tau} = B_Q \rho_{\tau}^{-1}$$

i.e.

$$\rho(\tau) = B_Q \left(B_Q^{\tau}\right)^{-1}.$$

We feed Eq. (8) with random matrices Q until B_Q is invertible. Since non invertible matrices form a Zariski closed subset in the space of matrices practice shows that we obtain an invertible B_Q almost immediately. For examples on this construction we refer to [22].

This method does not give us only some class invariants but whole vector spaces of them. For example for the space of the generalized Weber functions $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$ defined in the work of Gee in [11, p. 73] as

$$\mathfrak{g}_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)},\ \mathfrak{g}_1(\tau) = \zeta_{24}^{-1}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)},\ \mathfrak{g}_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)},\ \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)},$$

which are the functions defined in Example 1 for $N = 3$. We find first that the polynomials

$$I_1 := \mathfrak{g}_0\mathfrak{g}_2 + \zeta_{72}^6\mathfrak{g}_1\mathfrak{g}_3, \qquad I_2 := \mathfrak{g}_0\mathfrak{g}_3 + (-\zeta_{72}^{18} + \zeta_{72}^6)\mathfrak{g}_1\mathfrak{g}_2$$

are indeed invariants of the action of H. Then using our method

$$\begin{aligned} e_1 &:= (-12\zeta_{72}^{18} + 12\zeta_{72}^6)\mathfrak{g}_0\mathfrak{g}_3 + 12\zeta_{72}^6\mathfrak{g}_0\mathfrak{g}_3 + 12\mathfrak{g}_1\mathfrak{g}_2 + 12\mathfrak{g}_1\mathfrak{g}_3, \\ e_2 &:= 12\zeta_{72}^6\mathfrak{g}_1\mathfrak{g}_2 + (-12\zeta_{72}^{18} + 12\zeta_{72}^6)\mathfrak{g}_0\mathfrak{g}_3 + (-12\zeta_{72}^{12} + 12)\mathfrak{g}_1\mathfrak{g}_3 + 12\zeta_{72}^{12}\mathfrak{g}_1\mathfrak{g}_3 \end{aligned}$$

Table 1 Minimal polynomials using the $\mathfrak{g}_0, \ldots, \mathfrak{g}_3$ functions

Invariant	Polynomial
Hilbert	$t^5 + 400497845154831586723701480652800t^4 +$
	$818520809154613065770038265334290448384t^3 +$
	$4398250752422094811238689419574422303726895104t^2 -$
	$16319730975176203906274913715913862844512542392320t +$
	$15283054453672803818066421650036653646232315192410112$
e_1	$t^5 - 936t^4 - 60912t^3 - 2426112t^2 - 40310784t - 3386105856$
e_2	$t^5 - 1512t^4 - 29808t^3 + 979776t^2 + 3359232t - 423263232$

generate a $\mathbb{Q}$-vector space of class invariants. All $\mathbb{Q}$ linear combinations of the form $\lambda_1 e_1 + \lambda_2 e_2$ also provide class invariants. Finding the most efficient class invariant among them is a difficult problem which we hope to solve in the near future. For comparison we present in Table 1 the polynomials generating the Hilbert class field using the j invariant and the two class functions we obtained by our method.

5 Selecting the Discriminant

We have seen in the previous sections that the original version of the CM method uses a special polynomial called Hilbert class polynomial which is constructed with input a fundamental discriminant $d < 0$. A discriminant $d < 0$ is fundamental if and only if d is free of any odd square prime factors and either $-d \equiv 3 \pmod 4$ or $-d/4 \equiv 1, 2, 5, 6 \pmod 8$. The disadvantage of Hilbert class polynomials is that their coefficients grow very large as the absolute value of the discriminant $D = |d|$ increases and thus their construction requires high precision arithmetic.

According to the first main theorem of complex multiplication, the modular function $j(\theta)$ generates the Hilbert class field over K. However, the Hilbert class field can also be generated by modular functions of higher level. There are several known families of class polynomials having integer coefficients which are much smaller than the coefficients of their Hilbert counterparts. Therefore, they can substitute Hilbert class polynomials in the CM method and their use can considerably improve its efficiency. Some well-known families of class polynomials are: Weber polynomials [28], $M_{D,l}(x)$ polynomials [24], Double eta (we will denote them by $M_{D,p_1,p_2}(x)$) polynomials [7] and Ramanujan polynomials [20]. The logarithmic height of the coefficients of all these polynomials is smaller by a constant factor than the corresponding logarithmic height of the Hilbert class polynomials and this is the reason for their much more efficient construction.

A crucial question is which polynomial leads to the most efficient construction. The answer to the above question can be derived by the precision requirements of the polynomials or (in other words) the logarithmic height of their coefficients. There are asymptotic bounds which estimate with remarkable accuracy the precision requirements for the construction of the polynomials. The polynomials with the smallest (known so far) asymptotic bound are Weber polynomials constructed with discriminants d satisfying the congruence $D = |d| \equiv 7 \pmod 8$. Naturally, this leads to the conclusion that these polynomials will require less precision for their construction than all other class polynomials constructed with values D' close enough to the values of D.

In what follows, we will show that this is not really true in practice. Clearly, the degrees of class polynomials vary as a function of D, but we will see that on average these degrees are affected by the congruence of D modulo 8. In particular, we prove theoretically that class polynomials (with degree equal to their Hilbert counterparts) constructed with values $D \equiv 3 \pmod 8$ have three times smaller degree than polynomials constructed with comparable in size values of D that satisfy the congruence $D \equiv 7 \pmod 8$. Class polynomials with even discriminants (e.g., $D \equiv 0 \pmod 4$) have on average two times smaller degree than polynomials constructed with comparable in size values $D \equiv 7 \pmod 8$. This phenomenon can be generalized for congruences of D modulo larger numbers. This leads to the (surprising enough) result that there are families of polynomials which seem to have asymptotically larger precision requirements for their construction than Weber polynomials with $D \equiv 7 \pmod 8$, but they can be constructed more efficiently than them in practice (for comparable values of D).

The degree of every polynomial generating the Hilbert class field equals the class number h_D which for a fundamental discriminant $-D < 4$ is given by [25, p. 436]

$$h_D = \frac{\sqrt{D}}{2\pi} L(1, \chi) = \frac{\sqrt{D}}{2\pi} \prod_p \left(1 - \frac{\chi(p)}{p}\right)^{-1},$$

where χ is the quadratic character given by the Legendre symbol, i.e. $\chi(p) = \left(\frac{-D}{p}\right)$. Let us now consider the Euler factor

$$\left(1 - \frac{\chi(p)}{p}\right)^{-1} = \begin{cases} 1 & \text{if } p \mid D \\ \frac{p}{p-1} & \text{if } \left(\frac{-D}{p}\right) = 1 \\ \frac{p}{p+1} & \text{if } \left(\frac{-D}{p}\right) = -1. \end{cases} \tag{9}$$

Observe that smaller primes have a bigger influence on the value of h_D. For example, if $p = 2$, then we compute

$$\left(1 - \frac{\chi(2)}{2}\right)^{-1} = \begin{cases} 1 & \text{if } 2 \mid D \\ 2 & \text{if } D \equiv 7 \pmod 8 \\ \frac{2}{3} & \text{if } D \equiv 3 \pmod 8). \end{cases} \tag{10}$$

This leads us to the conclusion that on average the degree of a class polynomial with $D \equiv 3 \pmod 8$ will have three times smaller degree than a polynomial constructed with a comparable value of $D \equiv 7 \pmod 8$. Similarly, the degree of a polynomial constructed with even values of $D \equiv 0 \pmod 4$ will have on average two times smaller degree than a polynomial with $D \equiv 7 \pmod 8$.

Going back to Eq. (9), we can see that for discriminants of the same congruence modulo 8, we can proceed to the next prime $p = 3$ and compute

$$\left(1 - \frac{\chi(3)}{3}\right)^{-1} = \begin{cases} 1 & \text{if } 3 \mid D \\ \frac{3}{2} & \text{if } \left(\frac{-D}{3}\right) = 1 \\ \frac{3}{4} & \text{if } \left(\frac{-D}{3}\right) = -1. \end{cases}$$

This means that for values of D such that $\left(\frac{-D}{3}\right) = -1$ the value of h_D is on average two times smaller than class numbers corresponding to values with $\left(\frac{-D}{3}\right) = 1$. Consider for example, the cases $D \equiv 3 \pmod 8$ and $D \equiv 7 \pmod 8$. If we now include in our analysis the prime $p = 3$, then we can distinguish 6 different subcases $D \equiv 3, 11, 19 \pmod{24}$ and $D \equiv 7, 15, 23 \pmod{24}$. Having in mind the values $\left(1 - \frac{\chi(2)}{2}\right)^{-1}$ and $\left(1 - \frac{\chi(3)}{3}\right)^{-1}$, we can easily see, for example, that the polynomials with $D \equiv 19 \pmod{24}$ will have on average 6 times smaller degrees than the polynomials with $D \equiv 23 \pmod{24}$.

What happens if we continue selecting larger primes p? Equation (9) implies that if we select a discriminant $-D$ such that for all primes $p < N$ we have $\left(\frac{-D}{p}\right) = -1$ then the class number corresponding to D has a ratio that differs from other discriminants by a factor of at most

$$\prod_{p<N} \left(\frac{p-1}{p+1}\right) = \prod_{p<N} \left(1 - \frac{2}{p+1}\right). \tag{11}$$

Since the series $\sum_p \frac{2}{p+1}$ diverges (p runs over the prime numbers), the product in Eq. (11) diverges as well [1, p.192 th. 5]. Therefore, the product in Eq. (11) can have arbitrarily high values for sufficiently large values of N. This also means that if D is sufficiently big we can choose discriminants that correspond to class numbers that have an arbitrarily high ratio with respect to other discriminants of the same size.

6 Conclusions

In this paper, we have given a detailed overview of the CM method for the construction of elliptic curves. We have presented the necessary theoretical background and we have described our published results on finding new class invariants using the Shimura reciprocity law. The proper selection of a suitable discriminant D for the construction of class polynomials, combined with the above results, will hopefully lead us to more efficient constructions in the future using new families of class polynomials.

References

1. Ahlfors, L.V.: Complex Analysis. An introduction to the Theory of Analytic Functions of One Complex Variable, 3rd edn. International Series in Pure and Applied Mathematics. McGraw-Hill, New York (1978)
AQ5 2. Blake, I.F., Seroussi, G., Smart, N.P.: Elliptic Curves in Cryptography London Mathematical Society Lecture Note Series, vol. 165
AQ6 3. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**(3–4), 235–265 (1997)
4. Bruce, C., Berndt, H., Huat, C.: Ramanujan and the modular j-invariant. Can. Math. Bull. **42**(4), 427–440 (1999). MR MR1727340 (2002a:11035)
AQ7 5. Conrad, K.: Galois descent. Expository article on authors website http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/galoisdescent.pdf
6. David, A.C.: Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication. Wiley, New York (1989). MR MR1028322 (90m:11016)
7. Enge, A., Schertz, R.: Constructing elliptic curves over finite fields using double eta-quotients. J. Théor. Nombres Bordeaux **16**, 555–568 (2004). (MR2144957)
8. Fröhlich, A., Taylor, M.J.: Algebraic Number Theory. Cambridge Studies in Advanced Mathematics, vol. 27. Cambridge University Press, Cambridge (1993). xiv+355 pp. ISBN: 0-521-43834-9
9. Gauss, C.F.: Disquisitiones Arithmeticae. Traducida por Arthur A. Clarke. Yale University Press, New Haven and London (1966)
10. Gee, A.: Class invariants by Shimura's reciprocity law, J. Théor. Nombres Bordeaux **11**(1), 45–72 (1999) Les XXèmes Journées Arithmétiques (Limoges, 1997). MR MR1730432 (2000i:11171)
11. Gee, A.: Class fields by Shimura reciprocity, Ph.D. thesis, Leiden University available online at http://www.math.leidenuniv.nl/nl/theses/44
12. Gee, A., Stevenhagen, P.: Generating class fields using Shimura reciprocity. In: Buhler, J.P. (ed.) Algorithmic Number Theory (Portland, OR, 1998). Lecture Notes in Computer Science, vol. 1423, pp. 441–453. Springer, Berlin (1998). MR MR1726092 (2000m:11112)
13. Glasby, S.P., Howlett, R.B.: Writting representatations over minimal fields. Commun. Algebra **25**(6), 1703–1711 (1997)
14. Hart, W.B.: Schläfli modular equations for generalized Weber functions. Ramanujan J. **15**(3), 4352̌013468 (2008)
15. Hindry, M., Silverman, J.: Diophantine Geometry An Introduction. Graduate Texts in Mathematics. Springer, New York (2000)
16. Hindry, M., Silverman, J.: Diophantine Geometry An Introduction. Graduate Texts in Mathematics. Springer, New York (2000)
17. Kemper, G., Steel, A.: Some algorithms in invariant theory of finite groups. In: Dräxler, P., Michler, G.O., Ringel, C.M. (eds.) Computational Methods for Representations of Groups and Algebras, Euroconference in Essen. Progress in Mathematics, vol. 173. Birkhäuser, Basel (1997)
18. Konstantinou, E., Kontogeorgis, A., Stamatiou, Y.C., Zaroliagis, C.: Generating prime order elliptic curves: difficulties and efficiency considerations. In: International Conference on Information Security and Cryptology – ICISC 2004. Lecture Notes in Computer Science, vol. 3506, pp. 261–278. Springer, Berlin (2005)
19. Konstantinou, E., Kontogeorgis, A.: Computing polynomials of the Ramanujan t_n class invariants. Can. Math. Bull. **52**(4), 583–597 (2009). MR MR2567152
20. Konstantinou, E., Kontogeorgis, A.: Introducing Ramanujan's class polynomials in the generation of prime order elliptic curves. Comput. Math. Appl. **59**(8), 2901–2917 (2010)
21. Konstantinou, E., Kontogeorgis, A.: Ramanujan invariants for discriminants equivalent to 5 mod 24. Int. J. Number Theory **8**(1), 265–287
22. Kontogeorgis, A.: Constructing class invariants. Math. Comput. **83**(287), 1477–1488 (2014)

23. Lay, G.J., Zimmer, H.G.: Constructing elliptic curves with given group order over large finite fields. In: Algorithmic Number Theory Symposium I. Springer Lecture Notes in Computer Science. Springer, Berlin (1994)
24. Morain, F.: Modular curves and class invariants. preprint
25. Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers, 2nd edn. Springer, Berlin (1990)
26. Procesi, C.: A Primer of Invariant Theory. Notes by Giandomenico Boffi. Brandeis Lecture Notes, vol. 1. Brandeis University, Waltham, MA (1982)
27. Ramanujan, S.: Notebooks, vols. 1, 2. Tata Institute of Fundamental Research, Bombay (1957). MR MR0099904 (20 #6340)
28. Schertz, R.: Weber's class invariants revisited. J. Théor. Nombres Bordeaux **4**, 325–343 (2002). (MR1926005)
29. Shimura G.: 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)
30. Silverman, J.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106. Springer, New York (1986)
31. Stevenhagen, P.: Hilbert's 12th problem, complex multiplication and Shimura reciprocity. In: Class Field Theory—Its Centenary and Prospect (Tokyo, 1998). Advanced Studies in Pure Mathematics, vol. 30, pp. 161–176, Mathematical Society of Japan, Tokyo (2001). MR MR 18464571 (2002i:11110)

AQ8 32. Weber, H.: Lehrbuch der Algebra, Band III, 2nd edition, Chelsea reprint, original edition 1908
33. Yui, N., Zagier, Don.: On the singular values of Weber modular functions. Math. Comput. Am. Math. Soc. **66**(220), 1645–1662 (1997). MR MR1415803 (99i:11046)

AUTHOR QUERIES

AQ1. Please provide Keywords for this chapter.
AQ2. "Elisavet Konstantinou" has been set as corresponding author. Please check. and Please check the author affiliations are ok.
AQ3. kindly check this sentence Şabelian group (see [3],38] forŤ parenthesis missing in this line.
AQ4. Please check if the edit made to the sentence, "We find that..." is fine.
AQ5. Please update Refs. [2] and [24].
AQ6. References "[3, 5, 15, 16, 18, 26, 27]" are not cited in the text. Please provide the citation or delete them from the list.
AQ7. Please provide year for Refs. [5] and [11].
AQ8. Please provide publisher name and location for Ref. [32].