Journal de Théorie des Nombres
de Bordeaux **16** (2004), 555–568

Constructing elliptic curves over finite fields using double eta-quotients

par ANDREAS ENGE et REINHARD SCHERTZ

RÉSUMÉ. Nous examinons une classe de fonctions modulaires pour $\Gamma^0(N)$ dont les valeurs engendrent des corps de classes d'anneaux d'ordres quadratiques imaginaires. Nous nous en servons pour développer un nouvel algorithme de construction de courbes elliptiques à multiplication complexe. Vu que le genre des $X_0(N)$ associées n'est pas zéro, le calcul de la courbe se fait à l'aide de certains polynômes modulaires.

Étant un produit de quatre fonctions η, les fonctions modulaires proposées peuvent être vues comme une généralisation naturelle des fonctions traitées par Weber et généralement utilisées pour construire des courbes elliptiques à multiplication complexes. Contrairement au cas des fonctions de Weber, les valeurs des fonctions examinées ici engendrent tous les corps de classes d'anneaux de n'importe quel ordre quadratique imaginaire sans tenir compte des congruences satisfaites par leur discriminant modulo des puissances de 2 ou 3.

ABSTRACT. We examine a class of modular functions for $\Gamma^0(N)$ whose values generate ring class fields of imaginary quadratic orders. This fact leads to a new algorithm for constructing elliptic curves with complex multiplication. The difficulties arising when the genus of $X_0(N)$ is not zero are overcome by computing certain modular polynomials.

Being a product of four η-functions, the proposed modular functions can be viewed as a natural generalisation of the functions examined by Weber and usually employed to construct CM-curves. Unlike the Weber functions, the values of the examined functions generate any ring class field of an imaginary quadratic order regardless of the congruences modulo powers of 2 and 3 satisfied by the discriminant.

Manuscrit reçu le 8 avril 2003.

1. Introduction

Over the past decades, elliptic curves over finite fields have become an important ingredient for different number theoretic algorithms. They are used, for instance, to construct secure public key cryptosystems [17, 21], factor integers [20] or prove the primality of an integer [13, 1]. For at least two of these applications it is necessary to construct curves whose orders satisfy certain constraints. The order of an elliptic curve suitable for cryptography must have a large prime factor to exploit to the maximum the security potential of the key space. To show that an integer q is prime, one may construct an elliptic curve over $\mathbb{Z}/q\mathbb{Z}$ and a point on the curve of order larger than $(\sqrt[4]{q}+1)^2$ and recursively show that this order is prime.

The theory of complex multiplication yields an attractive approach to the construction of elliptic curves with a suitable number of points over a finite field. It allows to first determine the relevant parameters and then to tailor the elliptic curve to one's needs. Furthermore, it can be used to construct many non-isomorphic (albeit isogenous) curves at the same time. For obtaining the curves it is necessary to explicitly determine the ring class field of an imaginary-quadratic order. Classically, this involves singular values of certain modular functions, whose minimal polynomials have to be computed during the algorithm. A nice feature of the functions described in the literature is that they generate a rational extension of the field $\mathbb{C}(j)$ of modular functions for the full modular group. Thus, it is easy to deduce the j-invariant of the curve and finally the curve itself. On the other hand, some of these functions lead to minimal polynomials with prohibitively large coefficients, which limits their applicability to small discriminants. Others are suited for discriminants of a special type only. In particular, the commonly employed Weber functions cannot be used directly for discriminants divisible by 96 or congruent to 5 modulo 8.

In this article, we propose a new family of modular functions whose singular values allow to construct the ring class field of *any* imaginary-quadratic order, thus permitting a unified approach regardless of the discriminant. Moreover, their associated class polynomials have comparatively small coefficients and can thus be computed in a reasonable amount of time. In Section 2, we give a concise introduction to the theory of complex multiplication and the algorithms proposed in the literature, before presenting our alternative modular functions in Section 3. In general, these functions do not generate a rational function field over $\mathbb{C}(j)$ any more. Hence the actual computation of the j-invariant corresponding to a singular value of a such a function (and thus of the complex multiplication curve itself) becomes a problem. In Section 4, we propose a solution by factoring the modular polynomial relating our functions and j. We conclude by presenting a few examples in Section 5.

2. Complex multiplication

2.1. Orders, class fields, and curves. Complex multiplication of elliptic curves is the study of their endomorphism rings, which turn out to be orders in imaginary-quadratic number fields. We introduce the notation used throughout this article and recall a few basic facts; for a more comprehensive account of quadratic orders, see [2, Chapter 2.7] or [3].

Let $d < 0$ be a *fundamental discriminant*, $D = f^2 d$ and $K = \mathbb{Q}(\sqrt{d})$ the imaginary-quadratic field of discriminant d. Denote by $\mathcal{O}_1$ its *maximal order* and by $\mathcal{O}_f$ the order of discriminant D and *conductor* f. The elements of the *ideal class group* $\mathfrak{H}_f$ of the order $\mathcal{O}_f$ are conveniently (for the sake of computations) represented by *quadratic forms*: to the ideal $\mathfrak{a} = [\alpha_1, \alpha_2]$ of $\mathcal{O}_f$ we associate its *basis quotient* $\alpha = \frac{\alpha_1}{\alpha_2}$, where we suppose that the numbering is such that $\alpha \in \mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. In turn, α is the root of a primitive quadratic form $[A, B, C] = AX^2 + BX + C$ of discriminant D, that is, $A > 0$, $\gcd(A, B, C) = 1$ and $D = B^2 - 4AC$. The $h_f = h(D)$ elements of $\mathfrak{H}_f$ are in bijective correspondence with certain quadratic forms of discriminant D, called *reduced*, which are easily enumerated.

Concerning elliptic curves, the standard reference is [26], a more elementary (and far less comprehensive) introductory book is [7].

Over the complex numbers, the endomorphism ring of an ordinary elliptic curve is either $\mathbb{Z}$ or an imaginary quadratic order $\mathcal{O}_f$; in the latter case, the curve is said to have *complex multiplication* by $\mathcal{O}_f$ or D. There are exactly $h(D)$ isomorphism classes of such curves. They are characterised by their j-invariant being a *singular value* of the absolute modular invariant j, that is, a value $j(\alpha)$ where α is the root of a primitive quadratic form of discriminant D, or equivalently the basis quotient of a proper ideal of $\mathcal{O}_f$. The singular values of j have the algebraic property that they generate the *ring class field* K_f over $K = \mathbb{Q}(\sqrt{d})$. By class field theory, the Galois group of K_f/K is canonically isomorphic to $\mathfrak{H}_f$: if $j(\mathfrak{a})$ is the singular value associated to the ideal $\mathfrak{a}$, then the automorphism $\sigma(\mathfrak{b})$ corresponding to an ideal class $\mathfrak{b}$ acts on K_f by $j(\mathfrak{a})^{\sigma(\mathfrak{b})} = j(\mathfrak{a}\mathfrak{b}^{-1})$.

Ordinary elliptic curves over finite fields $\mathbb{F}_q$ have necessarily complex multiplication by some imaginary-quadratic order $\mathcal{O}_f$. Deuring's lifting and reduction theorem [5, p. 202–203] states that any such curve is obtained as the reduction of an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_f$ (so that in fact the complex curve is defined over K_f). More precisely, if $q = p^m$ with p prime, then p splits in $\mathcal{O}_f$ as $p = \mathfrak{p}\overline{\mathfrak{p}}$, and $\mathfrak{p}$ is of order m in $\mathfrak{H}_f$. By class field theory, the ideals above $\mathfrak{p}$ in the ring of integers of K_f are of inertia degree m, and the curve over $\mathbb{F}_q$ is obtained by reducing a complex multiplication curve over K_f modulo a prime ideal above $\mathfrak{p}$. The

order of $\mathfrak{p}$ being m implies that $q = p^m$ can be written as

$$4q = u^2 + |D|v^2 \text{ with } u,\, v \in \mathbb{Z}.$$

If $D \notin \{-3, -4\}$, then the number of $\mathbb{F}_q$-rational points on the reduced curve is given by $q + 1 + u$ or $q + 1 - u$.

2.2. Classical complex multiplication constructions. The results mentioned in the previous section imply a conceptually simple way of constructing elliptic curves with complex multiplication. For a suitable combination of $q = p^m$ and D, compute the minimal polynomial $H_D[j]$, called the *class polynomial*, of a singular value of j as follows: enumerate a system $[A_i, B_i, C_i]$, $i = 1, \ldots, h(D)$, of reduced quadratic forms of discriminant D and compute complex approximations of the singular values $j(\alpha_i) = j\left(\frac{-B_i+\sqrt{D}}{2A_i}\right)$ and of the class polynomial

$$H_D[j](X) = \prod_{i=1}^{h(D)} (X - j(\alpha_i)).$$

In fact, $H_D[j]$ has rational integral coefficients, and if the complex approximations are sufficiently accurate, the coefficients can be obtained by rounding. Over $\mathbb{F}_q$, this polynomial splits completely, and its roots $\overline{j}$ are precisely the j-invariants of the elliptic curves over $\mathbb{F}_q$ with complex multiplication by D. An elliptic curve equation is then given by simple formulae (which we provide for $D \neq \{-3, -4\}$):

- If $\operatorname{char} \mathbb{F}_q = 2$, let $E : Y^2 + XY = X^3 + \overline{j}^{-1}$.
- If $\operatorname{char} \mathbb{F}_q = 3$, let $E : Y^2 = X^3 - j^{|\mathbb{F}|/3}X^2 + 1$.
- If $\operatorname{char} \mathbb{F}_q \geq 5$, let $c = \frac{\overline{j}}{1728-\overline{j}}$, and $E : Y^2 = X^3 + 3cX + 2c$.

Any elliptic curve with j-invariant $\overline{j}$ is then isomorphic over $\mathbb{F}_q$ either to E or to its quadratic twist.

Unfortunately, the coefficients of $H_D[j]$ grow very fast with D. Consider the logarithmic height of $H_D[j]$, i.e. the logarithm of the largest absolute value of its coefficients. Obviously, the conjugates $j(\alpha_i)$ have to be approximated to a precision of at least this height so that the coefficients may be rounded properly. In practice, it suffices to increase the accuracy by only a few digits to account for numerical errors. Thus, the time needed to determine $H_D[j]$ is closely correlated to its height, and it is desirable to devise equivalent polynomials with smaller coefficients which may play the role of class equations. In order to not loose the elliptic curves out of sight, it appears hereby reasonable to remain close to j, and thus to the ring class field K_f generated by the singular values of j. This motivates the following definition, cf. [27].

Definition. Let $\mathfrak{w}$ be a non-constant modular function and α the root of a primitive quadratic form of discriminant $D = f^2 d$. If the singular value $\mathfrak{w}(\alpha)$ lies in the ring class field K_f, we call it a *class invariant* for D. The characteristic polynomial $H_D[\mathfrak{w}]$ of the singular value with respect to K_f/K is called a *class polynomial.*

A few such modular functions have been investigated in the literature [27, 1, 19, 24], all of which are suited only for specific types of discriminants.

Denote by $q = e^{2\pi i z}$ the Fourier transform of a complex variable z, and let $q^{1/24} = e^{(2\pi i z)/24}$. We introduce Dedekind's η–function [4]

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1-q^n) = q^{1/24} \left(1 + \sum_{n=1}^{\infty} (-1)^n \left(q^{n(3n-1)/2} + q^{n(3n+1)/2} \right) \right).$$

The simple η quotients are given by

$$\mathfrak{w}_\ell(z) = \frac{\eta(z/\ell)}{\eta(z)}$$

for some integer ℓ (often chosen as a prime). Weber examined the function $f_1 = \mathfrak{w}_2$ and the further functions f and f_2, obtained in a similar fashion as a quotient of η by applying a modular transformation of level 2 and normalising suitably: $f = e^{-\pi i/24} \frac{\eta\left(\frac{z+1}{2}\right)}{\eta(z)}$ and $f_2 = \sqrt{2}\, \frac{\eta(2z)}{\eta(z)}$. Certain powers of these functions turn out to be class invariants for some discriminants D, where the main constraint is that 2 be not inert in $\mathbb{Q}(\sqrt{D})$. The exact exponents depend on the congruences of D satisfied modulo powers of 2 and modulo 3; for modern proofs, see [24].

These results have been generalised to powers of $\mathfrak{w}_\ell$ for primes ℓ such that $\ell - 1 | 24$, see [1], under essentially the same condition that ℓ be not inert in $\mathbb{Q}(\sqrt{D})$.

Hence there are discriminants for which this finite family of functions is not suited. Moreover, the higher the additional exponent, the larger the height of the class polynomial, see [8]. Thus even in cases where these functions are actually class invariants, they need not be a good choice from a computational point of view.

3. Double η quotients as class invariants

In this section, we examine a class of functions that can be seen as a natural generalisation of the simple η quotients as described in the previous section. Being defined for an infinite combination of parameter values, they yield invariants for any discriminant. For two prime numbers p_1 and p_2,

define the double η quotient of level $N = p_1 p_2$ by

$$\mathfrak{w}_{p_1,p_2}(z) = \frac{\mathfrak{w}_{p_1}(z)}{\mathfrak{w}_{p_1}(z/p_2)} = \frac{\mathfrak{w}_{p_2}(z)}{\mathfrak{w}_{p_2}(z/p_1)} = \frac{\eta\left(\frac{z}{p_1}\right)\eta\left(\frac{z}{p_2}\right)}{\eta(z)\eta\left(\frac{z}{p_1 p_2}\right)}.$$

Here we do not exclude the cases that $p_1 = p_2$ or that p_1, $p_2 \in \{2, 3\}$. In fact, letting $p_1 = p_2 = 2$ shows an interesting connection to Weber's functions: the well-known identity $f f_1 f_2 = \sqrt{2}$, already proved in [16], implies that

$$f\left(\frac{z}{2}\right) = \frac{\eta\left(\frac{z}{2}\right)^2}{\eta(z)\eta\left(\frac{z}{4}\right)} = \mathfrak{w}_{2,2}(z).$$

Let $s = 24/\gcd(24, (p_1 - 1)(p_2 - 1))$ be the integer measuring how far $(p_1 - 1)(p_2 - 1)$ is from being divisible by 24. Then the functions we are interested in are the $\mathfrak{w}_{p_1,p_2}^s$. (We mention that an infinite family of class invariants may also be obtained from simple η quotients of arbitrary level, as examined in [9].)

As can be seen by examining the behaviour of η under unimodular transformations, $\mathfrak{w}_{p_1,p_2}^s$ is a modular function for $\Gamma^0(N) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : N|b\right\}$, see [22]. Furthermore, it is invariant under the Fricke–Atkin–Lehner involution of level N by [10], Theorem 2, and an element of $\mathcal{F}_N$, the field of modular functions of level N whose q-expansions at any cusp lie in the N-th cyclotomic field, by Theorem 7 of [10].

Our first aim is to determine under which conditions the singular values of $\mathfrak{w}_{p_1,p_2}^s$ lie in the ring class field K_f, which places them close to the singular values of j. In Section 4, we discuss how to obtain the corresponding elliptic curves with complex multiplication by $\mathcal{O}_f$. The properties of $\mathfrak{w}_{p_1,p_2}^s$ allow to apply the following result, which is Theorem 4 of [24].

Theorem 3.1. *Let $\mathfrak{w} \in \mathcal{F}_N$ be a modular function for $\Gamma^0(N)$ such that $\mathfrak{w}(z)$ and $\mathfrak{w}\left(\frac{-1}{z}\right)$ have rational q-expansions. Let $D < 0$ be a quadratic discriminant. Assume that there is a quadratic form $[A_1, B_1, C_1] = A_1X^2 + B_1X + C_1$ of discriminant $B_1^2 - 4A_1C_1 = D$ such that $\gcd(A_1, N) = 1$ and $N|C_1$, and let α_1 be its root in $\mathbb{H}$. If α_1 is not a pole of $\mathfrak{w}$, then $\mathfrak{w}(\alpha_1) \in K_f$.*

The conjugates of $\mathfrak{w}(\alpha_1)$ under $\mathrm{Gal}(K_f/K)$ are given by the $\mathfrak{w}(\alpha_i)$, where α_i varies over the roots in $\mathbb{H}$ of an N-system for D, that is a complete system of inequivalent quadratic forms $[A_i, B_i, C_i]$ of discriminant D such that

$$\gcd(A_i, N) = 1 \text{ and } B_i \equiv B_1 \pmod{2N}. \tag{3.1}$$

It is not difficult to show that an N-system can always be obtained effectively by applying unimodular transformations to any system of representatives of the class group (cf. [24], Proposition 3). Notice also that (3.1) implies the divisibility by N of all the C_i.

Theorem 3.2. *Let $D = f^2 d$ with $d < 0$ a fundamental discriminant, $N = p_1 p_2$ with p_1, p_2 prime, satisfying furthermore the following condition:*

- *If $p_1 \neq p_2$, then $\left(\frac{D}{p_1}\right), \left(\frac{D}{p_2}\right) \neq -1$;*
- *if $p_1 = p_2 = p$, then either $\left(\frac{D}{p}\right) = 1$ or $p | f$.*

Then there is a primitive quadratic form $[A_1, B_1, C_1]$ of discriminant D with $\gcd(A_1, N) = 1$ and $N | C_1$. Let α_1 be its root in $\mathbb{H}$. The singular value $\mathfrak{w}^s_{p_1,p_2}(\alpha_1)$ lies in K_f. The conjugates of $\mathfrak{w}^s_{p_1,p_2}(\alpha_1)$ are the $\mathfrak{w}^s_{p_1,p_2}(\alpha_i)$, where the α_i vary over the roots of an N-system as defined in Theorem 3.1.

Proof. The existence of the quadratic form $[A_1, B_1, C_1]$ amounts to the existence of B_1 such that $4N | D - B_1^2$, which can readily be shown to be equivalent to the given conditions on p_1 and p_2.

The remaining assertions are a direct consequence of Theorem 3.1. The main point we have not yet verified is the rationality of the different q-expansions. For $\mathfrak{w}^s_{p_1,p_2}$ itself this follows directly from the rationality of the q-expansion of η. The invariance of $\mathfrak{w}^s_{p_1,p_2}$ under the Fricke–Atkin–Lehner involution $z \mapsto \frac{-N}{z}$ associated to $\Gamma^0(N)$ implies that $\mathfrak{w}^s_{p_1,p_2}\left(-\frac{1}{z}\right) = \mathfrak{w}^s_{p_1,p_2}(Nz)$, which clearly has a rational q-expansion. Finally, as η has neither zeroes nor poles in $\mathbb{H}$, also $\mathfrak{w}^s_{p_1,p_2}$ has no poles in $\mathbb{H}$. □

Remark. It can be shown that depending on the congruences satisfied by D modulo 12, lower powers of $\mathfrak{w}_{p_1,p_2}$ may yield singular values in the ring class field. Indeed, Satz 4 of [23] states that $(\gamma_2\gamma_3)^{\frac{(p_1-1)(p_2-1)}{4}} \mathfrak{w}_{p_1,p_2}$ has singular values in K_f if N is coprime to $6f$. Depending on D modulo 12, the singular values of γ_2 and γ_3 may lie in K_f themselves, so the same holds already for $\mathfrak{w}_{p_1,p_2}$. We do not pursue this issue any further here, as the incurred technicalities would rather obscure the following discussions.

The singular values of $\mathfrak{w}^s_{p_1,p_2}$ are algebraic integers and in many cases even units, for which there is a simple proof in the case $p_1 \neq p_2$.

Theorem 3.3. *Under the conditions of Theorem 3.2, the number $\mathfrak{w}^s_{p_1,p_2}(\alpha_1)$ is an algebraic integer. If $p_1 \neq p_2$, or $p_1 = p_2 = p$ and $\left(\frac{D}{p}\right) = 1$, then they are units.*

Proof. Consider the modular polynomial Φ_{p_1,p_2} relating $\mathfrak{w}^s_{p_1,p_2}$ and j; this is the monic polynomial $\Phi_{p_1,p_2}(X, j)$ of degree $\psi(N) = N \prod_{p|N,\, p \text{ prime}} \left(1 + \frac{1}{p}\right)$ in X such that $\Phi_{p_1,p_2}(\mathfrak{w}^s_{p_1,p_2}, j) = 0$. It is shown in Theorem 7 of [10] that

Φ_{p_1,p_2} is an element of $\mathbb{Z}[j,X]$. Specialising in the singular values yields that $\Phi_{p_1,p_2}(X,j(\alpha_1))$ is a monic polynomial with coefficients in $\mathbb{Z}[j(\alpha_1)]$ and with $\mathfrak{w}^s_{p_1,p_2}(\alpha_1)$ as a root. As $j(\alpha_1)$ is an algebraic integer, this implies that also $\mathfrak{w}^s_{p_1,p_2}(\alpha_1)$ is an integer.

For $p_1 \neq p_2$, Theorem 9 of [10] states that the constant coefficient of Φ_{p_1,p_2} is 1. Hence, the specialised reciprocal polynomial $\Phi^*_{p_1,p_2}(X,j(\alpha_1))$ is monic with root $\left(\mathfrak{w}^s_{p_1,p_2}(\alpha_1)\right)^{-1}$ and with integral coefficients, so that $\mathfrak{w}^s_{p_1,p_2}(\alpha_1)$ is indeed a unit.

If $p_1 = p_2 = p$, then the constant coefficient of the modular polynomial is a proper power of p, so that the preceding argument does not apply. In this case, the prime ideal decomposition of the singular values given in [6], § 22, provides a proof. □

The previous two theorems yield a simple algorithm to compute the class polynomial $H_D[\mathfrak{w}^s_{p_1,p_2}]$ of $\mathfrak{w}^s_{p_1,p_2}(\alpha_1)$. The algorithm consists of enumerating an N-system, computing complex approximations of the conjugates $\mathfrak{w}^s_{p_1,p_2}(\alpha_i)$ and of $H_D[\mathfrak{w}^s_{p_1,p_2}](X) = \prod_{i=1}^{h(D)} \left(X - \mathfrak{w}^s_{p_1,p_2}(\alpha_i)\right) = X^{h(D)} + \sum_{i=0}^{h(D)-1} a_i X_i$. The coefficients a_i are elements of the principal order $\mathcal{O}_1$, and choosing an integral basis $[1,\omega]$ of $\mathcal{O}_1$ and separating the real and the imaginary parts of the a_i allows to recognise them as algebraic integers.

The following theorem shows that under mild additional constraints, this algorithm can be simplified, since the class polynomials are actually elements of $\mathbb{Z}[X]$. So the conjugates are either real or come in complex-conjugate pairs, which saves about half of the work, as only one conjugate in each pair needs to be computed.

Theorem 3.4. *Under the assumptions of Theorem 3.1, suppose furthermore that* $\mathfrak{w}$ *is invariant under the Fricke–Atkin–Lehner involution, that is,* $\mathfrak{w}\left(-\frac{1}{z}\right) = \mathfrak{w}(Nz)$ *for* $z \in \mathbb{H}$. *Assume that* $C_1 = N$. *Denote by* $\mathfrak{a}_i = \left[A_i, \frac{-B_i+\sqrt{D}}{2}\right]_{\mathbb{Z}}$ *the ideal corresponding to the quadratic form* $[A_i,B_i,C_i]$. *If* $\mathfrak{a}_i\mathfrak{a}_l$ *is equivalent to* $\mathfrak{a}_1$, *then* $\mathfrak{w}(\alpha_i) = \overline{\mathfrak{w}(\alpha_l)}$. *In particular,* $H_D[\mathfrak{w}] \in \mathbb{Q}[X]$.

Proof. Denote the complex conjugation by κ. We consider first the special case $i = 1$ with $N = C_1 = \frac{B_1^2-D}{4A_1}$ and $l = 0$, where α_0 is defined as the basis quotient of $\mathfrak{a}_0 = \mathcal{O}_f = \left[1, \frac{-B_1+\sqrt{D}}{2}\right]$. Since $\mathfrak{w}(z)$ is supposed to have a rational q-expansion, i.e. it can be written as a Laurent series with rational coefficients in $q^{1/n} = e^{2\pi iz/n}$ for some $n \in \mathbb{N}$, and since $(q^{1/n})^\kappa = e^{2\pi i(-\overline{z})/n}$,

we have $\mathfrak{w}(z)^\kappa = \mathfrak{w}(-z^\kappa)$. Now

$$\begin{aligned}\mathfrak{w}(\alpha_1) &= \mathfrak{w}\left(\frac{-B_1+\sqrt{D}}{2A_1}\right) = \mathfrak{w}\left(\frac{B_1^2-D}{2A_1(-B_1-\sqrt{D})}\right)\\ &= \mathfrak{w}\left(\frac{2N}{-B_1-\sqrt{D}}\right) = \mathfrak{w}\left(\frac{B_1+\sqrt{D}}{2}\right) = \mathfrak{w}\left(\frac{-B_1+\sqrt{D}}{2}\right)^\kappa\\ &= \mathfrak{w}(\alpha_0)^\kappa.\end{aligned}$$

Let now $\mathfrak{a}_i$ and $\mathfrak{a}_l$ be arbitrary. We are going to use the action of $\mathrm{Gal}(K_f/\mathbb{Q})$ on the singular values of $\mathfrak{w}$ to reduce this case to the previously considered one. For a proper ideal $\mathfrak{a} = \left[A, \frac{-B+\sqrt{D}}{2}\right]_{\mathbb{Z}}$ of $\mathcal{O}_f$ we have

$$j(\mathfrak{a})^\kappa = j\left(\frac{-B+\sqrt{D}}{2}\right)^\kappa = j\left(\frac{B+\sqrt{D}}{2}\right) = j(\mathfrak{a}^{-1}) \in K_f,$$

so κ is an automorphism of $K_f/\mathbb{Q}$.

If $\mathfrak{b}$ is a second proper ideal of $\mathcal{O}_f$, then

$$j(\mathfrak{a})^{\kappa\sigma(\mathfrak{b})\kappa} = j(\mathfrak{a}^{-1})^{\sigma(\mathfrak{b})\kappa} = j(\mathfrak{a}^{-1}\mathfrak{b}^{-1})^\kappa = j(\mathfrak{a}\mathfrak{b}) = j(\mathfrak{a})^{\sigma(\mathfrak{b}^{-1})}.$$

Since $K_f = \mathbb{Q}(\sqrt{D}, j(\mathfrak{a}))$, we have $\mathrm{Gal}(K_f/\mathbb{Q}) = \langle\kappa\rangle \ltimes \sigma(\mathfrak{H}_f)$ with $\kappa\sigma(\mathfrak{b})\kappa = \sigma(\mathfrak{b}^{-1})$.

Notice that $\mathfrak{w}(\alpha_i) = \mathfrak{w}(\alpha_0)^{\sigma(\mathfrak{a}_i^{-1})}$ (cf. the proof of Theorem 7 in [24], used for the proof of Theorem 3.1), whence

$$\begin{aligned}\mathfrak{w}(\alpha_i) &= \mathfrak{w}(\alpha_0)^{\sigma(\mathfrak{a}_i^{-1})} = \mathfrak{w}(\alpha_1)^{\kappa\sigma(\mathfrak{a}_i^{-1})} = \mathfrak{w}(\alpha_0)^{\sigma(\mathfrak{a}_1^{-1})\kappa\sigma(\mathfrak{a}_i^{-1})}\\ &= \mathfrak{w}(\alpha_0)^{\sigma(\mathfrak{a}_1^{-1}\mathfrak{a}_i)\kappa}\\ &= \mathfrak{w}(\alpha_0)^{\sigma(\mathfrak{a}_l^{-1})} \text{ since } \mathfrak{a}_1^{-1}\mathfrak{a}_i \text{ is in the same class as } \mathfrak{a}_l^{-1}\\ &= \mathfrak{w}(\alpha_l)^\kappa.\end{aligned}$$

□

Corollary 3.1. *With the notations of Theorem 3.2, suppose that the following conditions hold:*

- *If $p_1 \neq p_2$, then $\left(\frac{D}{p_1}\right), \left(\frac{D}{p_2}\right) \neq -1$, and $p_1, p_2 \nmid f$;*
- *if $p_1 = p_2 = p \neq 2$, then $\left(\frac{D}{p}\right) = 1$ or $p|f$;*
- *if $p_1 = p_2 = 2$, then $\left(\frac{D}{2}\right) = 1$, or $2|f$, but $D \not\equiv 4 \pmod{32}$.*

Then there is a primitive quadratic form $[A_1, B_1, C_1]$ of discriminant D with $\gcd(A_1, N) = 1$ and $C_1 = N$. The assertions of Theorem 3.2 hold, and the class polynomial $H_D[\mathfrak{w}^s_{p_1,p_2}](X)$ is an element of $\mathbb{Z}[X]$. If $\sim$ denotes

equivalence of ideals, the class polynomial can be computed as

$$\prod_{i:\mathfrak{a}_i^2\sim\mathfrak{a}_1}\left(X-\mathfrak{w}^s_{p_1,p_2}(\alpha_i)\right)\prod_{i:\mathfrak{a}_i\mathfrak{a}_{l(i)}\sim\mathfrak{a}_1,\,l(i)>i}\left(X^2-\mathrm{Tr}(\mathfrak{w}^s_{p_1,p_2}(\alpha_i))X+\mathrm{N}(\mathfrak{w}^s_{p_1,p_2}(\alpha_i))\right),$$

where Tr *resp.* N *denote the complex trace resp. norm.*

Proof. For $p_1\neq p_2$, the existence of the quadratic form with $C_1=N$ is equivalent to the existence of B_1 such that $p_1,p_2\parallel\frac{D-B_1^2}{4}$. For $p_1=p_2$, it is equivalent to the existence of B_1 such that $N\parallel\frac{D-B_1^2}{4}$. It is readily verified that this situation is captured by exactly the conditions of the corollary. The assertion now follows directly from Theorem 3.4. □

Remark. The additional constraint of the corollary in the case $p_1=p_2=2$, when compared to Theorem 3.2, is in fact no serious restriction: If $D\equiv 4 \pmod{32}$, then $f=2$ and $\left(\frac{d}{2}\right)=1$. One may then use the double η quotient for the fundamental discriminant d to construct the Hilbert class field K_1, which in this special case equals the ring class field K_2 associated to D.

4. Retrieving j

As observed in the previous sections, an elliptic curve over a finite field $\mathbb{F}$ having complex multiplication by the discriminant $D=df^2$ can be obtained via the ring class field K_f. Using some class invariant $\mathfrak{w}$, the approach consists of computing the class polynomial $H_D[\mathfrak{w}]$ as an element of $\mathbb{Z}[X]$ or $\mathcal{O}_1[X]$ and of reducing it modulo the characteristic of $\mathbb{F}$. If $\mathbb{F}$ has been chosen such that the desired complex multiplication curve exists, then the reduced class polynomial splits completely over $\mathbb{F}$, and one determines a root $\overline{\mathfrak{w}}$. Writing down an explicit equation for the elliptic curve is now equivalent to determining the corresponding value $\overline{j}$ of its j-invariant, cf. the formulae in Section 2.2.

In the classical case where $\mathfrak{w}$ is one of the Weber functions, this task is easily accomplished: there is a rational expression for j in terms of $\mathfrak{w}$, with coefficients in $\mathbb{Z}$, so that reducing to $\mathbb{F}$ yields a rational expression for $\overline{j}$ in terms of $\overline{\mathfrak{w}}$. However, this approach can only be possible when the associated modular curve is of genus zero. This is the case for the Weber functions, which are functions on $X_0(2)$. A rational expression still exists for the simple η-quotients $\mathfrak{w}_\ell$ with $\ell\in\{3,4,5,7,9,13,25\}$. All other modular curves $X_0(N)$ are not rational, whence there is no possibility of obtaining j directly. For $\mathfrak{w}^s_{p_1,p_2}$ of level 4, 9 or 25, moreover, the function field extension $\mathbb{C}(\mathfrak{w}^s_{p_1,p_2},j)/\mathbb{C}(\mathfrak{w}^s_{p_1,p_2})$ is of degree 2; otherwise said, $\mathbb{C}(\mathfrak{w}^s_{p_1,p_2})$ is not a rational model for the function field of $X_0(N)$.

However, in any case $\mathfrak{w}^s_{p_1,p_2}$ and j are still related by the modular polynomial $\Phi_{p_1,p_2}(X,j)\in\mathbb{Z}[X,j]$, which already played a role in the proof of Theorem 3.3, and which is studied more thoroughly in [10]. Here, it

suffices to recall that $\Phi_{p_1,p_2}(X,j)$ is a polynomial in $\mathbb{Z}[X,j]$ such that $\Phi_{p_1,p_2}(\mathfrak{w}^s_{p_1,p_2},j) = 0$. Hence, the desired value $\overline{j}$ is among the roots of $\Phi_{p_1,p_2}(\overline{\mathfrak{w}},J)$ in $\mathbb{F}$.

In general, there will be several roots $\overline{j}_1,\ldots,\overline{j}_k$ leading to several elliptic curves $E_1,\ldots,E_k$ (and their quadratic twists), and it remains to test which of them has complex multiplication by D. As the cardinality of the target curve is known, a quick check consists of taking a random point on each curve and testing whether it has torsion by this cardinality. This test will rule out most (in particular the quadratic twists), but not necessarily all of the candidates.

In certain applications (construction of elliptic curve cryptosystems, elliptic curve primality proving), one is not necessarily interested in the complex multiplication discriminant itself, but rather in the curve having a point of large, known prime order, which can be checked easily. In the case that $4|\mathbb{F}| = u^2 + |D|v^2$ with $v \neq 1$, one might then end up with a curve having complex multiplication by Df_1^2 with $f_1|v$ and $f_1 \neq 1$; if one has started with $D = df^2$ of non-trivial conductor f, one might also end up with complex multiplication by D/g^2 for some $g|f$. Unfortunately, $v \neq 1$ happens systematically for $D \equiv 1 \pmod 8$ and $|\mathbb{F}|$ odd, where $2|v$ and the curves with complex multiplication by D and by $4D$ have the same cardinality. If one wants to be sure to have complex multiplication by the given discriminant, one needs to use Kohel's algorithm [18, 12] for computing the exact endomorphism rings of the constructed curves.

Of course, the approach sketched here for deriving the j-invariant and thus the complex multiplication curve from a root of some class polynomial is not limited to $\mathfrak{w}^s_{p_1,p_2}$: it can be used for $\mathfrak{w}_\ell$ or any other class invariant whose modular polynomial is an element of $\mathbb{Z}[X,j]$.

5. Examples and discussion

We implemented the computation of ring class fields and elliptic curves over prime fields via double η-quotients in C, using `gmp`, `mpfr` and `mpc` for the computation of class polynomials and `ntl` for their factorisation [14, 15, 11, 25]. For more details and implementational tricks, see [8].

As a first small example, computable "by hand", consider $D = -23$ with $h(D) = 3$, $p_1 = 3$ and $p_2 = 13$. Let q be the smallest prime larger than 1000 such that the resulting curve over $\mathbb{F}_q$ has order $C = cQ$ with Q prime and $c \in \{1,2,3,4\}$. Then $q = 1117$ and $C = 1084 = 4 \cdot 271$.

A (partial) 39-system is given by $[1,-61,936]$, leading to the pair of complex conjugates $0.87 \pm 0.75i$, and $[2,-61,468]$, leading to the real conjugate -0.75. Hence, the class polynomial is $H_{-23}[\mathfrak{w}_{3,13}] = X^3 - X^2 + 1$. A root modulo q is given by 176. The modular polynomial $\Phi_{3,13}$ is of degree 2

in j, see [10], and its specialisation has the two roots 946 and 88; an elliptic curve with j-invariant 946 and 1084 points over $\mathbb{F}_{1117}$ is obtained as $E : Y^2 = X^3 + 455X + 1048$.

For larger examples, it is useful to know the required precision for the complex approximations. This precision depends essentially on the largest coefficient of the computed class polynomial. The logarithm of its absolute value is the logarithmic height of the polynomial. An estimate for the height is provided in [8]. For $H_D[j]$, the heuristic estimate is $\pi\sqrt{|D|}\sum\frac{1}{A}$, where the sum is taken over all reduced quadratic forms $[A, B, C]$ of discriminant D. For other class invariants, the height is proved to asymptotically change by a constant factor, given by the quotient of the degrees of the modular polynomial in the different variables, $\frac{\deg_j(\Phi(X,j))}{\deg_X(\Phi(X,j))}$. In our case, by Theorem 9 of [10], the factor is

$$\frac{s(p_1-1)(p_2-1)}{12(p_1+1)(p_2+1)} \text{ for } p_1 \neq p_2 \text{ and } \frac{s(p-1)^2}{12p(p+1)} \text{ for } p_1 = p_2 = p,$$

which is always smaller than 1. Its smallest value $1/28$ is obtained for $\mathfrak{w}_{3,13}$. The size of this factor allows to set up a hierarchy of class invariants, ordered corresponding to the precision required to carry out the computations and thus ultimately according to the efficiency of the computations.

Providing an example of cryptographic size, let $D = -78641219$ with $h(D) = 5000$, and let q be the smallest 192-bit prime leading to an elliptic curve with a prime number of points. Then

$$q = 313855086769334038191789471160383320805117772223240439559 3,$$

and the cardinality is

$$313855086769334038191789471166285758924009425342259032254 3.$$

We may choose $p_1 = 3$ and $p_2 = 61$. Using the above estimate for the height of the class polynomial (and adding a few bits to allow for rounding errors), we compute all approximations to complex numbers with a precision of 14793 bits. In fact, the largest coefficient of the class polynomial turns out to have 13050 bits.

On an Athlon 64 with 2.4 GHz, the timings for the different steps of the curve computation are as follows:

0.3	s	for the class group and an N-system
94	s	for the conjugates
58	s	to derive the minimal polynomial from the conjugates
29	s	for the root $\overline{\mathfrak{w}}$ modulo p
0.1	s	for factoring $\Phi_{3,61}(\overline{\mathfrak{w}}, j)$ and constructing the curve

While the degree of the modular polynomial $\Phi_{3,61}$ in j is 10 by Theorem 9 of [10], actually only 2 of its roots are elements of $\mathbb{F}_q$. An elliptic curve over

$\mathbb{F}_q$ having complex multiplication by D is given by the j-invariant

$$\overline{j} = 6121488206998830709788057876479356182485440428601649820 6$$

and finally the curve equation $E : Y^2 = X^3 + aX + b$ with

$$a = 3115836233330800492041622286815602160980719047690489875548$$
$$b = 2016651797253760621691021725108451981799256233015221196912$$

Acknowledgements. We are grateful to François Morain for his helpful comments on a previous version of this article. The first author was supported by a grant of the German Academic Exchange Service (DAAD).

References

[1] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving.* Mathematics of Computation, **61(203)** (July 1993), 29–68.

[2] Z. I. Borevich, I. R. Shafarevich, *Number Theory.* Pure and Applied Mathematics, Academic Press, New York, 1966.

[3] David A. Cox, *Primes of the Form $x^2 + ny^2$ — Fermat, Class Field Theory, and Complex Multiplication.* John Wiley & Sons, New York, 1989.

[4] R. Dedekind, *Erläuterungen zu den vorstehenden Fragmenten.* In R. Dedekind and H. Weber, editors, Bernhard Riemann's gesammelte mathematische Werke und wissenschaftlicher Nachlaß, pages 438–447. Teubner, Leipzig, 1876.

[5] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abhandlungen aus dem mathematischen Seminar der hamburgischen Universität **14** (1941), 197–272.

[6] Max Deuring, *Die Klassenkörper der komplexen Multiplikation.* In Enzyklop. d. math. Wissenschaften, volume I 2 Heft 10. Teubner, Stuttgart, 2 edition, 1958.

[7] Andreas Enge, *Elliptic Curves and Their Applications to Cryptography — An Introduction.* Kluwer Academic Publishers, 1999.

[8] Andreas Enge, François Morain, *Comparing invariants for class fields of imaginary quadratic fields.* In Claus Fieker and David R. Kohel, editors, Algorithmic Number Theory — ANTS-V, volume 2369 of Lecture Notes in Computer Science, pages 252–266, Berlin, 2002. Springer-Verlag.

[9] Andreas Enge, François Morain, *Further investigations of the generalised Weber functions.* In preparation, 2005.

[10] Andreas Enge, Reinhard Schertz, *Modular curves of composite level.* To appear in Acta Arithmetica, 2005.

[11] Andreas Enge, Paul Zimmermann, `mpc` — *a library for multiprecision complex arithmetic with exact rounding.* Version 0.4.3, available from http://www.lix.polytechnique.fr/Labo/Andreas.Enge/Software.html.

[12] Mireille Fouquet, François Morain, *Isogeny volcanoes and the SEA algorithm.* In Claus Fieker and David R. Kohel, editors, Algorithmic Number Theory — ANTS-V, volume 2369 of Lecture Notes in Computer Science, pages 276–291, Berlin, 2002. Springer-Verlag.

[13] Shafi Goldwasser, Joe Kilian. *Almost all primes can be quickly certified.* In Proc. 18th Annual ACM Symp. on Theory of Computing, pages 316–329, 1986.

[14] Torbjörn Granlund et. al., `gmp` — *GNU multiprecision library.* Version 4.1.4, available from http://www.swox.com/gmp.

[15] Guillaume Hanrot, Vincent Lefèvre, Paul Zimmermann et. al., `mpfr` — *a library for multiple-precision floating-point computations with exact rounding.* Version 2.1.0, available from http://www.mpfr.org.

[16] Carl Gustav Jacob Jacobi, *Fundamenta nova theoriae functionum ellipticarum.* In Gesammelte Werke, pages 49–239. Chelsea, New York, 2 (1969) edition, 1829.

[17] NEAL KOBLITZ *Elliptic curve cryptosystems.* Mathematics of Computation **48(177)** (January 1987), 203–209.

[18] DAVID KOHEL *Endomorphism Rings of Elliptic Curves over Finite Fields.* PhD thesis, University of California at Berkeley, 1996.

[19] GEORG-JOHANN LAY, HORST G. ZIMMER, *Constructing elliptic curves with given group order over large finite fields.* In Leonard M. Adleman and Ming-Deh Huang, editors, Algorithmic Number Theory, volume 877 of Lecture Notes in Computer Science, pages 250–263, Berlin, 1994. Springer-Verlag.

[20] H. W. LENSTRA JR., *Factoring integers with elliptic curves.* Annals of Mathematics **126** (1987), 649–673.

[21] VICTOR S. MILLER, *Use of elliptic curves in cryptography.* In Hugh C. Williams, editor, Advances in Cryptology — CRYPTO '85, volume 218 of Lecture Notes in Computer Science, pages 417–426, Berlin, 1986. Springer-Verlag.

[22] MORRIS NEWMAN, *Construction and application of a class of modular functions (II).* Proceedings of the London Mathematical Society 3rd Series **9** (1959), 373–387.

[23] REINHARD SCHERTZ, *Zur expliziten Berechnung von Ganzheitsbasen in Strahlklassenkörpern über einem imaginär-quadratischen Zahlkörper.* Journal of Number Theory **34(1)** (January 1990), 41–53.

[24] REINHARD SCHERTZ, *Weber's class invariants revisited,* Journal de Théorie des Nombres de Bordeaux **14(1)** (2002), 325–343.

[25] VICTOR SHOUP, `ntl` — *a library for doing number theory.* Version 5.3.2, available from http://www.shoup.net/ntl/.

[26] JOSEPH H. SILVERMAN, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.

[27] HEINRICH WEBER, *Lehrbuch der Algebra,* volume 3. Chelsea Publishing Company, New York, 3rd edition, 1908.

Andreas ENGE
INRIA Futurs & LIX (CNRS/UMR 7161)
École polytechnique
91128 Palaiseau cedex, France
E-mail : `enge@lix.polytechnique.fr`
URL: `http://www.lix.polytechnique.fr/Labo/Andreas.Enge/`

Reinhard SCHERTZ
Institut für Mathematik
Universität Augsburg
86135 Augsburg, Deutschland
E-mail : `schertz@math.uni-augsburg.de`