COMPUTING THE CARDINALITY OF CM ELLIPTIC CURVES USING TORSION POINTS

F. MORAIN

Abstract. Let $\mathcal{E}$ be an elliptic curve having complex multiplication by a given quadratic order of an imaginary quadratic field $\mathbf{K}$. The field of definition of $\mathcal{E}$ is the ring class field Ω of the order. If the prime p splits completely in Ω, then we can reduce $\mathcal{E}$ modulo one the factors of p and get a curve E defined over $\mathbb{F}_p$. The trace of the Frobenius of E is known up to sign and we need a fast way to find this sign. For this, we propose to use the action of the Frobenius on torsion points of small order built with class invariants *à la* Weber, in a manner reminiscent of the Schoof-Elkies-Atkin algorithm for computing the cardinality of a given elliptic curve modulo p. We apply our results to the Elliptic Curve Primality Proving algorithm (ECPP).

1. Introduction

Let $\mathbf{K}$ be an imaginary quadratic field of discriminant $-D$. For any integer t, let $\mathcal{O}_t$ be the order of conductor t of $\mathbf{K}$, $\Delta_t = -t^2 D$ its discriminant, and $h_t = h(\Delta_t)$ its class number. We denote by Ω_t the ring class field modulo t over $\mathbf{K}$. By class field theory, the extension $\Omega_t/\mathbf{K}$ can be constructed using the minimal polynomial of the modular function j over a set of representatives $\{\mathfrak{i}_1, \mathfrak{i}_2, \ldots, \mathfrak{i}_{h_t}\}$ of the class group $Cl(\mathcal{O}_t)$. An elliptic curve $\mathcal{E}$ of invariant $j(\mathfrak{i}_r)$ is defined over Ω_t and has complex multiplication (CM) by $\mathcal{O}_t$. We denote by $H_{\Delta_t}[j](X)$ the minimal polynomial of the j's, namely

$$H_{\Delta_t}[j](X) = \prod_{r=1}^{h_t} (X - j(\mathfrak{i}_r))$$

which is known to have rational integer coefficients.

Let p be a rational prime number which splits completely in Ω_t, or equivalently which is the norm of an integer of Ω_t (that is $p = (U^2 + Dt^2V^2)/4$ for rational integers U and V). Then we can reduce $\mathcal{E}$ modulo a prime divisor $\mathfrak{P}$ of p to get an elliptic curve $E/\mathbb{F}_p$ having CM by $\mathcal{O}_t$. If π denotes the Frobenius of E, then it can be viewed as an element of $\mathcal{O}_t$ of norm p, that is (assuming that $\Delta_t \notin \{-3, -4\}$):

$$\pi = (\pm U \pm tV\sqrt{-D})/2. \tag{1}$$

The cardinality of $E(\mathbb{F}_p)$ is the norm of $\pi - 1$, or more simply $p + 1 \mp U$.

The j-invariant of $E/\mathbb{F}_p$ is the reduction of one of the $j(\mathfrak{i}_r)$'s modulo p, that is a root of $H(X) = H_{\Delta_t}[j](X)$ modulo p. Building E is done as follows: find a root j of $H(X)$, and deduce from that the equation of E. When $j \notin \{0, 1728\}$, we may take any equation $E(j, c)$:

$$Y^2 = X^3 + a_4(j)c^2X + a_6(j)c^3$$

Date: October 11, 2002.

Key words and phrases. Elliptic curves, complex multiplication, modular curves, class invariants, ECPP algorithm, SEA algorithm.

The author is on leave from the French Department of Defense, Délégation Générale pour l'Armement.

where c is any element of $\mathbb{F}_p$ and

$$a_4(j) = \frac{3j}{1728-j}, \quad a_6(j) = \frac{2j}{1728-j}. \tag{2}$$

We will note $E(j)$ for $E(j,1)$. If its cardinality is $p+1-a$, then a curve $E(j,c)$ has cardinality $p+1-\left(\frac{c}{p}\right)a$ (where $\left(\frac{a}{b}\right)$ stands for the Legendre symbol). A curve with $\left(\frac{c}{p}\right) = -1$ is a twist of $E(j)$. The problem is now to compute $\#E(j)$ modulo p, or equivalently, fix the sign of U in equation (1).

In the course of implementing the ECPP algorithm [3] or for cryptographic reasons, it is important to compute this cardinality rapidly. We could of course try both signs of U yielding cardinalities m, find some random points P on $E(j)$ and check whether $[m]P = O_E$ on E. This approach is somewhat probabilistic and we prefer deterministic and possibly faster solutions.

In the case where D is fundamental and prime to 6, the solution is to use Stark's approach [29], together with tricks described in [20]. This method is efficient, provided we can afford some precomputations. Note that in the special case where $h_t = 1$, which includes $j = 0, 1728$, one already knows the answer (see [3, 13, 23] and the references given therein). For $D = 20$, we have the isolated result of [16] (see also section 6.2 below).

Our approach consists in computing the action of the Frobenius of the curve on torsion points of small order, using the techniques of the SEA algorithm [25]. These points are obtained using singular values of functions on $X_0(\ell)$ for small prime ℓ. This will give us algorithmic solutions to our motivating problem when $\left(\frac{-D}{\ell}\right) \neq -1$.

Section 2 describes properties of the modular equations defining $X_0(\ell)$ for prime ℓ and their relations to complex multiplication over $\overline{\mathbb{Q}}$. In Section 3, we briefly describe the necessary results used in the SEA algorithm. Section 4 contains our main contribution. We treat the special cases $\ell = 3$ in Section 5 and $\ell = 5$ in Section 6. Section 7 describes the very interesting case of $\ell = 7$ and for the sake of completeness that of $\ell = 11$. Section 8 is devoted to the particular case $\ell = 2$. We provide numerical examples for each case. We conclude with remarks on the use of our results in our implementation of ECPP.

The books [8, 27] are a good introduction to all the material described above.

2. Modular curves and class invariants

2.1. **Modular equations.** Let ℓ be a prime number. The curve $X_0(\ell)$ parametrizes the cyclic isogenies of degree ℓ associated to an elliptic curve E defined over a field $\mathbf{k}$. In brief, there exists a polynomial (called a modular polynomial), $\Phi_\ell(X,Y) \in \mathbb{Z}[X,Y]$ such that the roots of $\Phi_\ell(X, j(E))$ over $\mathbf{k}$ are the invariants of the curves that are ℓ-isogenous to E over $\mathbf{k}$. Among all the properties satisfied by these polynomials, note that they have rational integer coefficients and are monic for prime ℓ; moreover $\Phi_\ell(X,Y) = \Phi_\ell(Y,X)$ and the degree in X is $\ell+1$. For instance:

$$\Phi_2(X,Y) = X^3 + Y^3 - 162000(X^2+Y^2) - X^2Y^2 + 1488XY(X+Y) + 40773375XY$$
$$+8748000000(X+Y) - 157464000000000.$$

In fact, one can build a modular equation for any modular function f invariant under $\Gamma^0(\ell)$, often obtained from Dedekind's η function:

$$\eta(\tau) = q^{1/24} \prod_{m \geq 1} (1 - q^m)$$

where $q = \exp(2i\pi\tau)$. In the case $\ell = 2$, we may use Weber's functions defined by:

$$\mathfrak{f}_1(\tau) = \frac{\eta(\tau/2)}{\eta(\tau)}, \quad \mathfrak{f}(\tau) = \zeta_{48}^{-1}\, \frac{\eta((\tau+1)/2)}{\eta(\tau)}, \quad \mathfrak{f}_2(\tau) = \sqrt{2}\, \frac{\eta(2\tau)}{\eta(\tau)}.$$

The functions $\mathfrak{f}^{24}$, $-\mathfrak{f}_1^{24}$ and $-\mathfrak{f}_2^{24}$ are the three roots of the modular equation:

$$\Phi_2^c(X,J) = (X+16)^3 - JX.$$

For larger ℓ's, one classical way of doing this is via η-products [21, 22]. For instance, let

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

and $s = 12/\gcd(12, \ell-1)$. The function $\mathfrak{w}_\ell^{2s}$ is a modular function for $\Gamma^0(\ell)$ and is related to $j(z)$ via a modular equation $\Phi_\ell^c(F,J)$ such that $\Phi_\ell^c(\mathfrak{w}_\ell^{2s}(z), j(z)) = 0$ (the c refers to Atkin's denomination of *canonical* modular equations [19]). The equations for small prime values of ℓ are given in Table 1. Note that $\mathfrak{w}_2 = \mathfrak{f}_1$.

ℓ	Φ_ℓ^c
2	$(X+16)^3 - JX$
3	$(X+27)(X+3)^3 - JX$
5	$\left(X^2+10\,X+5\right)^3 - JX$
7	$\left(X^2+13\,X+49\right)\left(X^2+5\,X+1\right)^3 - JX$

TABLE 1. Table of modular equations $\Phi_\ell^c(X,J)$.

2.2. **Class invariants.** View the class group $Cl(\Delta_t)$ as a set of reduced quadratic primitive binary forms of discriminant Δ_t, say $Cl(\Delta_t) = \{(A,B,C), B^2-4AC = \Delta_t\}$ with h_t forms in it. For a given $Q = (A,B,C)$, let $\tau_Q = (-B+\sqrt{\Delta_t})/(2A)$. Then $j(\tau_Q)$ is an algebraic integer that generates $\Omega_t/\mathbf{K}$. Moreover, the associated curve E_Q of invariant $j(\tau_Q)$ has CM by $\mathcal{O}_t$.

Suppose $j(\tau) \in \Omega_t$. Then the roots of $\Phi_\ell(X, j(\tau))$ are algebraic integers. They generate an extension of Ω_t of degree dividing $\ell+1$. The striking phenomenon, known for a long time, is that sometimes these roots lie in Ω_t itself.

Let us give an example. Substituting $Y = -3375 = j((-1+\sqrt{-7})/2)$ in $\Phi_2(X,Y)$, we get:

$$\Phi_2(X,-3375) = (X-16581375)\,(X+3375)^2\,.$$

This remark carries over to other functions, such as $\mathfrak{w}_\ell$, or the classical functions of Weber:

$$\gamma_2(z) = \sqrt[3]{j(z)} = \frac{\mathfrak{f}_1(\tau)^{24}+16}{\mathfrak{f}_1(\tau)^8}, \quad \gamma_3(z) = \sqrt{j(z)-1728}.$$

We will note $\Phi[u](X,J)$ for the modular equation relating $u(z)$ and $j(z)$ and $H_{\Delta_t}[u](X)$ for the minimal polynomial of the invariant u.

We take the following from [24]. Suppose α is a quadratic integer with minimal polynomial

$$A\alpha^2 + B\alpha + C = 0$$

such that $\gcd(A,B,C) = 1$ and $B^2 - 4AC = \Delta_t$.

Definition 2.1. *Let N be a natural integer. Let $\mathcal{S} = \{(A_i,B_i,C_i)\}_{1\le i\le h_t}$ be a system of representatives of $Cl(\Delta_t)$. If $(A_i,N)=1$ and $B_r \equiv B_s \bmod (2N)$ for all $1 \le r,s \le h_t$, then $\mathcal{S}$ is called an N-system mod t.*

Schertz then proceeds to show that an N-system always exists for any N and Δ_t. Using this definition, he then gives new proofs of old theorems.

Theorem 2.1. *Let $\Delta_t = -4m = -t^2D$ and let $\mathcal{S} = \{(A_i, B_i, C_i)\}$ be a 32-system such that $B_i \equiv 0 \bmod 32$ and $\alpha_i = (-B_i + \sqrt{\Delta_t})/(2A_i)$. Then*

$$H_{\Delta_t}[X] = \prod_{i=1}^{h_t}(X - g(\alpha_i))$$

is the minimal polynomial of $g(\alpha_1)$ for the following functions (A is any of the A_i's):

$$\left(\left(\frac{2}{A}\right)\frac{1}{\sqrt{2}}\mathfrak{f}^2\right)^3, \text{ if } m \equiv 1 \bmod 8,$$

$$\mathfrak{f}^3, \text{ if } m \equiv 3 \bmod 8,$$

$$\left(\frac{1}{2}\mathfrak{f}^4\right)^3, \text{ if } m \equiv 5 \bmod 8,$$

$$\left(\left(\frac{2}{A}\right)\frac{1}{\sqrt{2}}\mathfrak{f}\right)^3, \text{ if } m \equiv 7 \bmod 8,$$

$$\left(\left(\frac{2}{A}\right)\frac{1}{\sqrt{2}}\mathfrak{f}_1^2\right)^3, \text{ if } m \equiv 2 \bmod 4,$$

$$\left(\left(\frac{2}{A}\right)\frac{1}{2\sqrt{2}}\mathfrak{f}_1^4\right)^3, \text{ if } m \equiv 4 \bmod 8.$$

Moreover, if $3 \nmid \Delta_t$, then the preceding theorem can be improved by forgetting the outer exponent 3 and requiring $3 \mid B$ and $\mathcal{S}$ be a $3 \cdot 32$-system for Δ_t.

We will also need:

Theorem 2.2. *Suppose $\alpha = (-B + \sqrt{\Delta_t})/(2A)$ where $3 \nmid A$, $3 \mid B$. Then*

$$\mathbb{Q}(\gamma_2(\alpha)) = \begin{cases} \mathbb{Q}(j(\alpha)) & \text{if } 3 \nmid \Delta_t, \\ \mathbb{Q}(j(3\alpha)) & \text{if } 3 \mid \Delta_t. \end{cases}$$

Moreover, if $3 \nmid \Delta_t$, then the conjugates of $\gamma_2(\alpha)$ are obtained from a 3-system modulo t.

A companion result is:

Theorem 2.3. *Suppose $\alpha = (-B + \sqrt{\Delta_t})/(2A)$ where $2 \nmid A$. We assume that*

$$B \equiv \begin{cases} 0 \bmod 4 & \text{if } 2 \mid \Delta_t, \\ 1 \bmod 4 & \text{if } 2 \nmid \Delta_t. \end{cases}$$

Then

$$\mathbb{Q}(\sqrt{-D}\gamma_3(\alpha)) = \mathbb{Q}(j(\alpha)), \quad \text{if } 2 \nmid \Delta_t,$$

$$\mathbb{Q}(\gamma_3(\alpha)) = \mathbb{Q}(j(2\alpha)), \quad \text{if } 2 \mid \Delta_t.$$

If $2 \nmid \Delta_t$, then the conjugates are obtained from a 2-system modulo t.

From [11], we extract the following Theorem.

Theorem 2.4. *Let ℓ be an odd prime and Δ_t a quadratic discriminant such that $\left(\frac{\Delta_t}{\ell}\right) \neq -1$. Choose the power $\mathfrak{w}_\ell^e$ and the natural number N, a multiple of ℓ, depending on $\Delta_t \bmod 6$ as specified in the table below. Assume that $Q = (A, B, C)$ is a primitive quadratic form of discriminant Δ_t with $\gcd(A, N) = 1$, $B^2 \equiv \Delta_t \pmod{4\ell}$ and B satisfying the additional congruences modulo 3 or 4* *as given in the table. If* $\tau_Q = \frac{-B+\sqrt{\Delta_t}}{2A}$ *is the root of* Q *in the upper complex half plane, then* $\mathfrak{w}_\ell^e(\tau_Q) \in \Omega_t$ *and its minimal polynomial has coefficients in* $\mathcal{O}_K$*.*

$\ell \bmod 12$	Δ_t	invariant	N	B
$\ell = 3$	—	$\mathfrak{w}_3^{12}$	3	—
	$2 \nmid \Delta_t$	$\mathfrak{w}_3^{6}$	6	$B \equiv 1 \pmod 4$
1	—	$\mathfrak{w}_\ell^{2}$	ℓ	—
5	—	$\mathfrak{w}_\ell^{6}$	ℓ	—
	$3 \nmid \Delta_t$	$\mathfrak{w}_\ell^{2}$	3ℓ	$3 \mid B$
7	—	$\mathfrak{w}_\ell^{4}$	ℓ	—
	$2 \nmid \Delta_t$	$\mathfrak{w}_\ell^{2}$	2ℓ	$B \equiv 1 \pmod 4$
11	—	$\mathfrak{w}_\ell^{12}$	ℓ	—
	$2 \nmid \Delta_t$	$\mathfrak{w}_\ell^{6}$	2ℓ	$B \equiv 1 \pmod 4$
	$3 \nmid \Delta_t$	$\mathfrak{w}_\ell^{4}$	3ℓ	$3 \mid B$
	$\gcd(\Delta_t, 6) = 1$	$\mathfrak{w}_\ell^{2}$	6ℓ	$B \equiv 9 \pmod{12}$

If furthermore $\ell | \Delta_t$ *and the table does not specify any restriction for* $B \bmod 4$*, then* $H_{\Delta_t}[\mathfrak{w}_\ell^e] \in \mathbb{Z}[X]$*.*

2.3. **Explicit factors of division polynomials.** Let $E[n]$ denote the group of n-torsion points of E (over $\overline{\mathbb{Q}}$). We let $f_n(X)^E$ (or simply $f_n(X)$) denote the n-th division polynomial whose roots are the abscissae of the n-torsion points of E. See [26] for its definition and properties. For instance for the curve $E : Y^2 = X^3 + aX + b$, the first values are:

$$f_0(X) = 0, f_1(X) = 1, f_2(X) = 1,$$

$$f_3(X) = 3\,X^4 + 6\,a\,X^2 + 12\,b\,X - a^2,$$

$$f_4(X) = 2\,X^6 + 10\,a\,X^4 + 40\,b\,X^3 - 10\,a^2X^2 - 8\,a\,b\,X - 2\,a^3 - 16\,b^2.$$

Recurrence relations for computing f_n are given by:

$$f_{2n} = f_n(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2),$$

$$f_{2n+1} = \begin{cases} f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1}(16(X^3+aX+b)^2) & \text{if } n \text{ is odd,} \\ 16(X^3+aX+b)^2 f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1} & \text{if } n \text{ is even.} \end{cases}$$

Once we have a root of $\Phi_\ell(X, J)$, Vélu's formulas [30] enable us to compute a factor $g_\ell^{E(j)}(X)$ of $f_\ell^{E(j)}(X)$. This property is at the heart of the improvements of Elkies and Atkin to Schoof's algorithm for computing the cardinality of curves over finite fields [1, 25, 10] (see also [19] for technicalities related to the actual computations).

In the table below, for prime ℓ, we suppose v_ℓ is a root of $\Phi_\ell^c(X, j)$ and we give the factor of $f_\ell^{E(j)}$ that can be obtained in Table 2.

ℓ	factor
2	$(v_2-8)\,X+v_2+16,$
3	$\left(v_3^2+18\,v_3-27\right)X+v_3^2+30\,v_3+81,$
5	$\left(v_5^2+4\,v_5-1\right)^2\left(v_5^2+22\,v_5+125\right)X^2$ $+2\,\left(v_5^2+4\,v_5-1\right)\left(v_5^2+10\,v_5+5\right)\left(v_5^2+22\,v_5+125\right)X$ $+\left(v_5^2+22\,v_5+89\right)\left(v_5^2+10\,v_5+5\right)^2,$
7	$\left(v_7^4+14\,v_7^3+63\,v_7^2+70\,v_7-7\right)^3X^3$ $+3\,\left(v_7^2+13\,v_7+49\right)\left(v_7^2+5\,v_7+1\right)\left(v_7^4+14\,v_7^3+63\,v_7^2+70\,v_7-7\right)^2X^2$ $+3\,\left(v_7^2+13\,v_7+33\right)\left(v_7^2+13\,v_7+49\right)\left(v_7^2+5\,v_7+1\right)^2$ $\times\left(v_7^4+14\,v_7^3+63\,v_7^2+70\,v_7-7\right)X$ $+\left(v_7^2+13\,v_7+49\right)\left(v_7^2+5\,v_7+1\right)^3\left(v_7^4+26v_7^3+219v_7^2+778v_7+881\right)$

TABLE 2. Factors of $f_\ell^{E(j)}$.

3. The foundations of the SEA algorithm

What we have just described over $\overline{\mathbb{Q}}$ has an impact on what happens modulo p, when we reduce a CM curve E modulo a prime p of good reduction that splits completely in Ω_t. We take the following result from [1] (see also [25]). Let ℓ and p be two distinct primes, and $E/\mathbb{F}_p$ an elliptic curve. Put $\#E=p+1-U$, $\mathcal{D}=4p-U^2$. We denote the splitting type of a squarefree polynomial $P(X)$ by the degrees of its factors. For instance, a polynomial of degree 4 having two linear factors and one quadratic factor will be said to have splitting type (1)(1)(2).

Theorem 3.1. *Put $\Psi_\ell(X)\equiv\Phi_\ell(X,j(E)) \bmod p$.*
If $\left(\frac{-\mathcal{D}}{\ell}\right)=0$, then Ψ_ℓ splits as $(1)(\ell)$ or $(1)\cdots(1)$.
If $\left(\frac{-\mathcal{D}}{\ell}\right)=+1$, then Ψ_ℓ splits as $(1)(1)(r)\cdots(r)$ where $r\mid\ell-1$ and $r>1$ if $\ell\neq 2$.
If $\left(\frac{-\mathcal{D}}{\ell}\right)=-1$, then Ψ_ℓ splits as $(r)\cdots(r)$ where $r>1$ and $r\mid\ell+1$.
If k denotes the number of factors of Ψ_ℓ, then $(-1)^k=\left(\frac{p}{\ell}\right)$.

We can make precise the first part of the theorem as follows:

Theorem 3.2. *Let $p=(U^2+DV^2)/4$. If $\ell\mid V$, then $\Psi_\ell(X)$ has $\ell+1$ roots modulo p.*

Proof: See Kohel's thesis [14]. □

We briefly summarize Elkies's idea [10]. Let π be the Frobenius of the curve, sending any point $P=(x,y)$ of $E(\overline{\mathbb{F}_p})$ to (x^p,y^p).

Theorem 3.3. *Let $\chi(X)=X^2-UX+p$ denote the characteristic polynomial of the Frobenius π of the elliptic E of cardinality $p+1-U$. When $\left(\frac{-\mathcal{D}}{\ell}\right)\neq-1$, the restriction of π to $E[\ell]$ (denoted by $\pi|_{E[\ell]}$) has at least one eigenvalue. To each eigenvalue λ of $\pi|_{E[\ell]}$ corresponds a factor of degree $(\ell-1)/2$ of f_ℓ. We deduce that $U\equiv\lambda+p/\lambda \bmod \ell$.*

We will note $g_{\ell,\lambda}(X)$ the factor of $f_\ell^{E(j)}(X)$ associated to the eigenvalue λ. Let ω denote the order of λ modulo ℓ and $\sigma=\omega/2$ if ω is even and ω otherwise. With these notations, one can show the following result:

Proposition 3.1. *The splitting type of $g_{\ell,\lambda}(X) \bmod p$ is $(\sigma)(\sigma)\cdots(\sigma)$ with κ factors such that $(\ell-1)/2=\kappa\sigma$.*

From this, we deduce:

Corollary 3.1. *The polynomial $g_{\ell,\lambda}(X)$ splits completely modulo p if and only if $\lambda = \pm 1 \bmod \ell$.*

Note also the following result of Dewaghe [9] in the formulation of [17].

Proposition 3.2. *Let $r = \mathrm{Resultant}(g_{\ell,\lambda}(X), X^3 + a_4(j)X + a_6(j))$. Then*

$$\left(\frac{\lambda}{\ell}\right) = \left(\frac{r}{p}\right)$$

Classically, this enables us to fix the sign of λ when $\ell \equiv 3 \bmod 4$.

4. A general framework

Let us state more formally our problem. We are given some root j_0 of some class polynomial $H_{-D}[j](X) \bmod p$, and we want to compute $\#E(j_0)$ defined by the formula (2). We know that $4p = U_0^2 + DV_0^2$ and $\#E(j_0) = p + 1 \pm U_0$. Again, we let $\mathcal{D} = DV_0^2$. Suppose that $\ell \neq p$ is an odd prime (the case $\ell = 2$ will be dealt with later) and $\left(\frac{-D}{\ell}\right) \neq -1$. In that case, Theorem 3.3 applies and if we can find one eigenvalue λ, we can find $U \bmod \ell$. If $U_0 \not\equiv 0 \bmod \ell$, then we can find the sign of $U = \pm U_0$. Note that if $\ell \mid D$, then $U_0 \not\equiv 0 \bmod \ell$.

The most favorable case is when $\ell \mid \mathcal{D}$, because then there is only one eigenvalue λ (it can be a double one) and $\lambda \equiv U/2 \bmod \ell$. Having λ gives us immediately the sign of U. A very favorable case is when $\ell \equiv 3 \bmod 4$, using Dewaghe's idea.

Apart from this, there is another interesting sub-case, when we can find a rational root x_0 of $g_{\ell,\lambda}^E$, using for instance some class invariant. In that case, we can form $y_0^2 = x_0^3 + ax_0 + b \bmod p$ and test whether y_0 is in $\mathbb{F}_p$ or not. If it is, then $\lambda = 1$, since (x_0, y_0) is rational and $\pi(P) = P$. Otherwise, $\lambda = -1$.

Our idea is then to use the general framework for some precise values of ℓ, and use rational roots of $g_{\ell,\lambda}$ obtained via class invariants. When $\ell = 3$, we are sure to end with a rational root of $f_3^{E(j)}(X)$, as is the case for $\ell = 2$ and $f_4^{E(j)}$. Moreover, we can use some invariant that give us the torsion points directly. We also give examples for $\ell = 5, 7, 11$.

We end this section with the typical algorithm for solving our general problem.

procedure BuildEWithCM(D,p)

1. For some ℓ and some invariant u, compute the minimal polynomial $H_D[u](X)$.
2. Find a root x_0 of $H_D[u](X)$ modulo p.
3. Solve $\Phi[u](x_0, J)$ for a root j and deduce from this $E(j)$.
4. Use x_0 to compute the cardinality of $E(j)$.

5. The case $\ell = 3$

We suppose that $4p = U^2 + DV^2$. The first subsection makes precise the above results.

5.1. Using 3-torsion points.

We begin with an easy lemma that can be proved by algebraic manipulations:

Lemma 5.1. *Let v be any root of $\Phi_3^c(X, j) = 0$. Then a root of $f_3^{E(j)}(X)$ is given by*

$$x_3 = -\frac{(v + 27)(v + 3)}{v^2 + 18v - 27}.$$

Proposition 5.1. *Let p be a prime representable as $4p = U_0^2 + DV_0^2$, for which $3 \mid DV_0^2$ and $\#E = p + 1 - U$. Suppose $P = (x_3, y_3)$ is a 3-torsion point on $E(j)$ for which x_3 is rational. Let $s = x_3^3 + a_4(j)x_3 + a_6(j) \bmod p$. Then $U \equiv 2\left(\frac{s}{p}\right) \bmod 3$.*

Proof: This is a simple application of Theorem 3.3. □

5.2. Solving the equation $\Phi_3^c(X, j(E)) = 0$.

5.2.1. *The case* $\left(\frac{-D}{3}\right) \neq -1$. A solution of this equation is given by $\mathfrak{w}_3^{12}$, which lies in Ω_1 with the hypothesis made on D.

Numerical examples. Let $H_{-15}[\mathfrak{w}_3^{12}] = X^2 + 81\,X + 729$, $p = 109$, $4p = 14^2 + 15 \times 4^2$, $v_3 = 3$, $x_3 = 104$, $E : Y^2 = X^3 + 94X + 99$; $U = \pm 14$. Since $\lambda = 1 \bmod 3$, we conclude that $U = 14$ and E has $109 + 1 - 14$ points.

Take $D = 20$ and $p = 349$. We find $(U, V) = (\pm 26, \pm 6)$. We compute:

$$H_{-20}[\mathfrak{w}_3^{12}] = X^2 + (70 - 22\sqrt{-20})X - 239 - 154\sqrt{-20}.$$

Using $\sqrt{-20} = 237 \bmod p$, a root of this polynomial is $v_3 = 257$, from which $j = 224$ and $E(j) : Y^2 = X^3 + 45X + 30$. Now $\lambda = -1$, which gives us that $\#E = 349 + 1 + 26$.

5.2.2. *The case* $\left(\frac{-D}{3}\right) = -1$. We may solve the degree 4 equation $\Phi_3^c(X, j(\alpha)) = 0$ directly.

In Skolem's approach [28], to compute the roots of a general quartic (with a_1 and a_3 not both zero)

$$P(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4$$

one uses the four roots X_i of P to define

$$\left\{\begin{array}{rcl} z_1 & = & X_1 + X_2 - X_3 - X_4, \\ z_2 & = & X_1 - X_2 + X_3 - X_4, \\ z_3 & = & X_1 - X_2 - X_3 + X_4. \end{array}\right. \tag{3}$$

Writing $y_i = z_i^2$, the y_i's are roots of

$$R(y) = y^3 + b_1y^2 + b_2y + b_3 \tag{4}$$

in which

$$\left\{\begin{array}{rcl} b_1 & = & 8a_2 - 3a_1^2, \\ b_2 & = & 3a_1^4 - 16a_1^2a_2 + 16a_1a_3 + 16a_2^2 - 64a_4, \\ b_3 & = & -(a_1^3 - 4a_1a_2 + 8a_3)^2. \end{array}\right. \tag{5}$$

Conversely, if the y_i's are the roots of R and if the z_i's are chosen in such a way that

$$-z_1z_2z_3 = a_1^3 - 4a_1a_2 + 8a_3,$$

then the X_i's defined by (3) (together with $X_1 + X_2 + X_3 + X_4 = -a_1$) are the roots of P.

In our case, we find that

$$R(Y) = Y^3 - 1728Y^2 - 576(j(\alpha) - 1728)Y - 64(j(\alpha) - 1728)^2$$

and the compatibility relation is $z_1z_2z_3 = 8(j(\alpha) - 1728)$. Since we suppose that $3 \nmid D$, we replace $j(\alpha)$ by $\gamma_2(\alpha)^3$. In that case, the roots of $R(Y)$ are

$$4(\zeta_3^{2i}\gamma_2(\alpha)^2 + 12\zeta_3^i\gamma_2(\alpha) + 144)$$

for $i = 0, 1, 2$. Studying the roots of these numbers as class invariants could probably be done. The function

$$\sqrt{\gamma_2(\alpha)^2 + 12\gamma_2(\alpha) + 144}$$

has been introduced via a different route by Birch in [4] and the theorems proven there could be used in our context, though we refrain from doing so in this article.

Let us summarize the algorithm to find the roots of $\Phi_3^c(X, j(E))$ modulo p when $3 \nmid D, 3 \mid V$ (which implies $p \equiv 1 \bmod 3$):

1. compute $\gamma_2 \bmod p$;
2. compute the values $y_i = 4(\zeta_3^{2i}\gamma_2(\alpha)^2 + 12\zeta_3^i\gamma_2(\alpha) + 144) \bmod p$ for $i = 1, 2$;

3. compute $z_i = \sqrt{y_i} \bmod p$ for $i = 1, 2$ and $z_3 = 8(\gamma_2^3 - 1728)/(z_1 z_2)$ from which $X_1 = z_1 + z_2 + z_3 - 36$ is a root of $\Phi_3^c(X, j)$.

Notice that $\zeta_3 \bmod p$ can be computed as follows (see [2] for more on this sort of ideas): since $3 \mid p-1$, we can find a such that $a^{(p-1)/3} \not\equiv 1 \bmod p$. Put $\zeta_3 = a^{(p-1)/3}$. It satisfies $\zeta_3^2 + \zeta_3 + 1 \equiv 0 \bmod p$. Therefore, finding a root costs two squareroots and one modular exponentiation, once γ_2 is known.

Numerical examples. Consider $(D, p, U, V) = (40, 139, \pm 14, \pm 3)$. A root of $H_{-40}[\gamma_2](X) = X^2 - 780\,X + 20880$ modulo p is 110. Using $\zeta_3 = 96$, we compute $v_3 = 109$ and $x_3 = 135$. Then $E : Y^2 = X^3 + 124X + 129$ has $\lambda = 1$ and $U = 14$.

6. The case $\ell = 5$

6.1. **Using $\mathfrak{w}_5$.** We assume here that $\left(\frac{-D}{5}\right) \neq -1$ and $5 \mid DV^2$. In that case, we can use some power of $\mathfrak{w}_5$ as invariant to get a root v_5 of $\Phi_5^c(X, j)$, thus yielding a factor $g_5^{E(j)}$ of $f_5^{E(j)}$. Writing:

$$A = v_5^2 + 22v_5 + 125, B = v_5^2 + 4v_5 - 1, C = v_5^2 + 10v_5 + 5,$$

one has:

$$g_5^{E(j)}(X) = X^2 + 2(C/B)X + (1 - 36/A)(C/B)^2.$$

Putting $Y = (B/C)X$ leads us to $(Y+1)^2 - 36/A$. At this point, since

$$j = \frac{(v_5^2 + 10\,v_5 + 5)^3}{v_5}$$

we also have:

$$j - 1728 = \frac{\left({v_5}^2 + 22\,v_5 + 125\right)\left({v_5}^2 + 4\,v_5 - 1\right)^2}{v_5}$$

or $A = v_5(j - 1728)/B^2$.

6.1.1. *The case $U \equiv \pm 2 \bmod 5$.* We deduce that $p \equiv 1 \bmod 5$ and $g_5^{E(j)}(X)$ has two rational roots.
Examples. Take $D = 35$ for which

$$H_{-35}[\mathfrak{w}_5^6](X) = X^2 + 50X + 125.$$

Take $(p, U, V) = (281, \pm 33, \pm 1)$. We first use $v_5 = 163$ to compute $E(j) : Y^2 = X^3 + 32X + 115$ and $g_5^{E(j)}(X) = X^2 + 245X + 198$. From this, we get $x_5 = 227$ and find that $x_5^3 + a_4(j)x_5 + a_6(j)$ is a square in $\mathbb{F}_p$, so that $\#E(j) = p + 1 + 33$.

Consider now $D = 91$ for which $\left(\frac{-91}{5}\right) = +1$. We find:

$$H_{-91}[\mathfrak{w}_5^6] = X^2 + (130 - 40\sqrt{-91})X - 99 - 8\sqrt{-91}.$$

Taking $(p, U, V) = (571, \pm 3, \pm 5)$, we use $\sqrt{-91} = 342 \bmod p$, find $v_5 = 216$ from which $j = 533$ and $E(j) : Y^2 = X^3 + 181X + 311$. Then $g_5^{E(j)}(X) = X^2 + 213X + 412$ which has a root $x_5 = 315$. We find that $\lambda = -1$ and $U = 3$.

6.1.2. *The case* $U \equiv \pm 1 \bmod 5$. One has $p \equiv 4 \bmod 5$ and $g_5^{E(j)}(X)$ is irreducible; the eigenvalue is $\lambda = U/2 \equiv \pm 2 \bmod 5$. We can compute it using the techniques of SEA, that is test the identity

$$(X^p, Y^p) = [\pm 2](X, Y) \bmod g_5^{E(j)}(X).$$

(Actually, checking the equality on the ordinates is enough.) Depending on the implementation, this can cost more than testing $[m]P$ on E.

Example. Consider $(D, p, U, V) = (35, 109, \pm 11, \pm 3)$. One computes $v_5 = 76$ and $g_5^{E(j)}(X) = X^2 + 13X + 13$. We compute

$$(X^p, Y^p) \equiv (108X + 96, Y(72X + 43)) = [2](X, Y).$$

Therefore, $U = -11$.

Consider $(D, p, U, V) = (91, 569, \pm 1, \pm 5)$. We find $E(j) : Y^2 = X^3 + 558X + 372$, $g_5^{E(j)}(X) = X^2 + 100X + 201$ and

$$(X^p, Y^p) \equiv [2](X, Y)$$

so that $U = -1$.

6.2. **A remark on the case** $D = 20$. We will take a route different from that in [16]. Write $p = a^2 + 5b^2$. Let $\varepsilon_0 = (1 + \sqrt{5})/2$ be the fundamental unit of $\mathbb{Q}(\sqrt{5})$. We have

$$a_4 = -\frac{162375}{87362} - \frac{89505\sqrt{5}}{174724}, \quad a_6 = -\frac{54125}{43681} - \frac{29835\sqrt{5}}{87362}$$

and $f_5(X)$ has the factor:

$$X^2 + \left(\frac{695}{418} + \frac{225\sqrt{5}}{418}\right) X + \frac{129925}{174724} + \frac{45369\sqrt{5}}{87362}$$

of discriminant:

$$\Delta = \frac{3^2}{11^2 \cdot 19^2} \left(\frac{7 + \sqrt{5}}{2}\right)^4 \left(\frac{9 + \sqrt{5}}{2}\right)^2 \frac{\sqrt{5}}{\varepsilon_0^5}$$

which is congruent to $\varepsilon_0\sqrt{5}$ modulo squares. Now, by [15], we have

$$\left(\frac{\varepsilon_0\sqrt{5}}{p}\right) = \left(\frac{p}{5}\right)_4.$$

When $p \equiv 1 \bmod 20$, Δ is a square modulo p and there are two abscissas in $\mathbb{F}_p$. Now, $a \equiv \pm 1 \bmod 5$ and thus

$$\#E(j) \equiv 1 + 1 \pm 2 \bmod 5.$$

We can distinguish the two cases by computing y_5: It is in $\mathbb{F}_p$ if and only if $m \equiv 0 \bmod 5$.

7. Numerical examples for $\ell \equiv 3 \bmod 4$

7.1. The case $\ell = 7$.

Lemma 7.1. *Let* v_7 *be a root of* $\Phi_7^c(X, j)$ *and put*

$$A(v_7) = v_7^4 + 14\,v_7^3 + 63\,v_7^2 + 70\,v_7 - 7.$$

Then

$$\mathrm{Resultant}(g_{7,\lambda}^{E(j)}(X), X^3 + a_4(j)X + a_6(j)) = -3jv_7A(v_7)S(v_7)^2$$

for some rational fraction S *with integer coefficients.*

Proof: using MAPLE, we compute:

$$\mathrm{Resultant}(g_{7,\lambda}, X^3 + a_4(j)X + a_6(j)) = -2^{12} \cdot 3^9 \cdot \left({v_7}^2 + 13\,v_7 + 49\right)^3 \left({v_7}^2 + 5\,v_7 + 1\right)^9 / A^9$$

from which the result follows. □

Take $D = 91$ for which

$$H_{-91}[\mathfrak{w}_7^4] = X^2 + 77X + 49.$$

Take $(p, U, V) = (107, \pm 8, \pm 2)$. We find $v_7 = 62$ from which $g_7^{E(j)}(X) = X^3 + 104X^2 + 44X + 73$. Using $E(j) : Y^2 = X^3 + 101X + 103$, we find $r = 13$ and $\left(\frac{13}{p}\right) = 1$ and therefore $U = 8$.

For $(D, p, U, V) = (20, 569, \pm 36, \pm 7)$, we compute:

$$H_{-20}[\mathfrak{w}_7^4](X) = X^2 + (15 - \sqrt{-20})X + 41 - 6\sqrt{-20}$$

one of which roots modulo p is $v_7 = 195$ (taking $\sqrt{-20} = 320$). Then $E(j) : Y^2 = X^3 + 289X + 3$ has $g_7^{E(j)}(X) = X^3 + 111X^2 + 185X + 94$ from which $U = 36$.

7.2. **The case $\ell = 11$.** In that case, the modular equation is quite large. However, if we restrict to the case where $3 \nmid D$, we can use the modular equation relating $\mathfrak{w}_{11}^4$ and γ_2:

$$X^{12} - 1980\,X^9 + 880\,\gamma_2 X^8 + 44\,\gamma_2^2 X^7 + 980078\,X^6 - 871200\,\gamma_2 X^5 + 150040\,\gamma_2^2 X^4$$
$$+ \left(47066580 - 7865\,\gamma_2^3\right) X^3 + \left(154\,\gamma_2^4 + 560560\,\gamma_2\right) X^2 + \left(1244\,\gamma_2^2 - \gamma_2^5\right) X + 121.$$

Consider $(D, p, U, V) = (88, 103, \pm 18, \pm 1)$. First, we find:

$$H_{-88}[\mathfrak{w}_{11}^4](X) = X^2 - 66X + 121$$

a root of which is $w_{11} = 21$. Plugging this into the modular equation, we find $\gamma_2 = 63$, from which $j = 66$ and $E(j) : Y^2 = X^3 + 73X + 83$. Using the techniques of SEA, we find that

$$g_{11} = X^5 + 81X^4 + 22X^3 + 55X^2 + 99X + 15$$

and the resultant is 98, so that $U = 18$.

Note that the techniques needed to compute g_{11} are probably too heavy to make this case useful. However, we provide it as a non-trivial example.

8. THE CASE $\ell = 2$

The points of 2-torsion cannot be used in our context, since they have ordinate 0. So we must try to use 4-torsion points instead. We suppose that $-D$ is fundamental.

8.1. **Splitting $f_4^{E(j)}$.** Curves having rational 2-torsion are parametrized by $X_0(2)$, or equivalently, $j(E) = (u + 16)^3/u$. Notice that:

$$j - 1728 = \gamma_3^2 = \frac{(u + 64)\,(u - 8)^2}{u}. \tag{6}$$

Using algebraic manipulations (and MAPLE), $f_4^{E(j)}(X)$ factors as $P_2(X)P_4(X)$ where:

$$P_2(X) = X^2 + 2\,\frac{u + 16}{u - 8}X + \frac{(u - 80)\,(u + 16)^2}{(u - 8)^2\,(u + 64)},$$

$$P_4(X) = X^4 - 2\,\frac{u + 16}{u - 8}X^3 - 12\,\frac{(u + 16)^2}{(u + 64)\,(u - 8)}X^2 - 2\,\frac{(7\,u + 16)\,(u + 16)^3}{(u + 64)\,(u - 8)^3}X$$
$$- \frac{\left(5\,u^2 + 640\,u - 256\right)(u + 16)^4}{(u + 64)^2\,(u - 8)^4}.$$

The polynomial P_2 has discriminant:

$$\Delta_2(u) = 12^2 \, \frac{(u+16)^2}{(u-8)^2\,(u+64)}.$$

The polynomial P_4 has the following property. If $(u+64)/u = v^2$, then it splits as a product of two quadratic polynomials:

$$G_a(X) = X^2 + 2\,\frac{\left(v^2+3\right)}{v\,(v+3)}X + \frac{\left(v^2+12\,v-9\right)\left(v^2+3\right)^2}{(v+3)^2\,(v-3)^2\,v^2},$$

$$G_b(X) = X^2 + 2\,\frac{\left(v^2+3\right)}{v\,(v-3)}X + \frac{\left(v^2-12\,v-9\right)\left(v^2+3\right)^2}{(v+3)^2\,(v-3)^2\,v^2}.$$

8.2. **CM theory.**

Proposition 8.1. *Let $4p = U^2 + Dt^2V^2$. If α belongs to a N-system for $u(\alpha)$, then $j(\alpha) - 1728$ is a square modulo a factor of p in Ω_t in the following cases:*
(i) D odd;
(ii) $4 \mid D$ and $2 \mid V$.

Proof:
(i) We know from Theorem 2.3 that $\sqrt{-D}\gamma_3(\alpha)$ is a class invariant, which means that $H_{-D}[\sqrt{-D}\gamma_3]$ splits modulo p.
(ii) Theorem 2.3 tells us that $\mathbb{Q}(\gamma_3(\alpha)) = \mathbb{Q}(j(2\alpha))$. But p splits in the order $\mathcal{O}_{2t}$ and therefore in Ω_{2t}, which shows that the minimal polynomial of γ_3 splits modulo p, proving the result. $\square$

Proposition 8.2. *Suppose that (D, p, V) satisfies one of the conditions of Proposition 8.1 and that u is a square. Then P_2 splits modulo p.*

Proof: Equation (6) tells us that $u(u+64)$ is a square modulo p, which implies that $\Delta_2(u)$ is also a square. $\square$

Notice that generally, at least one of the roots of $\Phi_2^c(X, j)$, denoted by u, will be the square of some Weber function, see Theorem 2.1.

8.3. **Eigenvalues modulo 2^k.**

Our idea is to use the roots of the characteristic polynomial $\chi(X) = X^2 - UX + p$ modulo powers of 2 and deduce from this the sign of U when possible. This subsection is devoted to properties of these roots.

Since $p \equiv 1 \bmod 2$, $\chi(X)$ has roots modulo 2 if and only if $U \equiv 0 \bmod 2$. Modulo 4, $\chi(X)$ has roots if and only if $U \equiv (p+1) \bmod 4$, which we suppose from now on. It is not enough to look at this case, since we have $U \equiv 0 \bmod 4$ or $U \equiv 2 \bmod 4$ and in both cases, and we cannot deduce from this alone the sign of U. We will need to look at what happens modulo 8. We list below the cases where $\chi(X)$ has roots modulo 8 and then relate this with the splitting of p.

Lemma 8.1. *The solutions of $X^2 \equiv 4 \bmod 8$ are ± 2.*

Lemma 8.2. *Write $\varepsilon = \pm 1$. We give in the following table the roots of $\chi(X)$ modulo 8:*

$p \bmod 8 \backslash U \bmod 8$	0	2ε	4
1	$\emptyset$	$\{\varepsilon, \varepsilon+4\}$	$\emptyset$
3	$\emptyset$	$\emptyset$	$\{\pm 1, \pm 3\}$
5	$\emptyset$	$\{-\varepsilon, -\varepsilon+4\}$	$\emptyset$
7	$\{\pm 1, \pm 3\}$	$\emptyset$	$\emptyset$

Proposition 8.3. *Let $4p = U^2 + DV^2$. The polynomial $\chi(X)$ has roots modulo 8 exactly in the following cases:*
(i) $4 \mid D$ and $2 \mid V$;
(ii) $4 \nmid D$ and [($4 \mid V$) or ($2 \,||\, V$ and $D \equiv 7 \bmod 8$)].

Proof:
(i) If V is even, we deduce that $U^2 \equiv 4p \equiv 4 \bmod 8$, $\chi(X)$ is one of $X^2 - 2\varepsilon X + 1$ or $X^2 - 2\varepsilon X + 5$ by Lemma 8.1. The result follows from Lemma 8.2.

What can be said when V is odd? When $4 \,||\, D$, this means that $p = (U/2)^2 + (D/4)V^2$, implying that $U \equiv 0 \bmod 4$ and $p \equiv 1 \bmod 4$ (since $-D$ is fundamental, $D/4 \equiv 1 \bmod 4$), but then $U \not\equiv p + 1 \bmod 4$.

When $8 \mid D$, then $p = (U/2)^2 + (D/4)V^2$ with $U \equiv \pm 2 \bmod 8$, but $p \equiv 3 \bmod 4$ and again $U \not\equiv p + 1 \bmod 4$.

(ii) In that case, U and V have the same parity. If U and V are odd, this implies $m = p+1-U$ is odd, so that we do not have 2-torsion points. If U and V are even, so is m and $p = (U/2)^2 + D(V/2)^2$.

If $V/2$ is even of the form $2V'$, then $p = (U/2)^2 + 4DV'^2$; $U/2$ must be odd and $p \equiv 1 \bmod 4$ and we conclude as in case (i).

If $V/2$ is odd, then $p = (U/2)^2 + DV'^2$ with V' odd, which implies $U/2$ even, that is $U \equiv 0 \bmod 8$ or $U \equiv 4 \bmod 8$. One has $p \equiv (U/2)^2 + D \bmod 8$. If $D \equiv 7 \bmod 8$, then $(U, p) = (0, 7) \bmod 8$ or $(4, 3) \bmod 8$ and the two characteristic polynomials have four roots modulo 8. If $D \equiv 3 \bmod 8$, then $(U, p) = (0, 3)$ or $(4, 7)$ modulo 8 and $\chi(X)$ has no roots. □

8.4. **Computing the cardinality of CM-curves.** This section makes use of the theory of isogeny cycles described in [7, 6].

With the notations of the preceding section, we suppose we are in the case where $U = 2\varepsilon \bmod 8$, or equivalently $4 \mid D$ and $2 \mid V$, or $4 \nmid D$ and $4 \mid V$.

From Proposition 8.2, we know that the factor $P_2(X)$ of $f_4^{E(j)}$ has at least two roots modulo p. If x_4 is one of these and $s = x_4^3 + ax_4 + b$, we let $y_4 = \sqrt{s}$ (*a priori* in $\mathbb{F}_{p^2}$) and $P = (x_4, y_4)$. Now $\pi(P) = \pm P$ according to the fact that s is a square or not. We have our eigenvalue $\lambda_4 \equiv \pm 1 \bmod 4$. By the theory of isogeny cycles, the eigenspace C_4 generated by P can be lifted to an eigenspace C_8 of $E[8]$ associated to the eigenvalue λ_8 which is congruent to λ_4 modulo 4. Since $U = 2\varepsilon \bmod 8$, we know from Lemma 8.2 that only one of the possible values of λ_8 reduces to a given λ_4, which gives us ε.

In practice, x_4 is relatively inexpensive to use when u is the square of a Weber function, which happens in the case $4 \mid D$ or $D \equiv 7 \bmod 8$ (for this, one uses an invariant for $-4D$ instead of $-D$, and both class groups have the same class number, see [3]). When $D \equiv 3 \bmod 4$, $h_t = 3h_1$, which is not as convenient; still, a root of $\Phi_2^c(X, j)$ exists, since it is in Ω_2 and p splits in it.

Examples. First take $(D, p, U, V) = (20, 29, \pm 6, \pm 2)$. We find $u = 7$, $j = 23$ and $E(j) : Y^2 = X^3 + 3X + 2$. From this, P_2 has a root $x_4 = 7$ and $\lambda_8 = -1$, so that $U = -6$.

Now take $(D, p, U, V) = (40, 41, \pm 2, \pm 2)$. We compute $u = 16$, $j = 39$, $E(j) : Y^2 = X^3 + 30X + 20$, $x_4 = 19$ and $\lambda_8 = -1$ implying $U = -2$.

Let us turn to odd D's. Take $(D, p, U, V) = (15, 409, \pm 26, \pm 8)$. Then $u = 102$, $j = 93$, $E : Y^2 = X^3 + 130X + 223$, $x_4 = 159$ yielding $\lambda_8 = -1$ and $U = -26$.

8.5. **The case D odd.** In that case, $\Phi_2^c(X, J)$ will have three roots in $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, that we can compute directly. This could be useful for the cases not treated by the the preceding section.

Let us try to solve the equation

$$\Phi_2^c(X, J) = X^3 + 48\,X^2 + 768\,X - JX + 4096 = 0$$

directly. As in [5] (already used in [18]), we first complete the cube letting $Y = X + 16$ to get:

$$Y^3 - JY + 16\,J = 0. \tag{7}$$

We look for α and β such that this equation can be rewritten:

$$Y^3 - 3\alpha\beta Y + \alpha\beta(\alpha+\beta) \equiv 0.$$

The coefficients α and β are solutions of

$$W^2 - 48W + J/3 = 0$$

whose discriminant is $\Delta = (-4/3)(J - 1728)$. Having α and β (in $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$), we solve

$$z^3 = \frac{\alpha}{\beta}$$

and we get a root

$$Y = \frac{\beta z - \alpha}{z - 1}$$

of (7).

Since D is odd, $\sqrt{-D}\gamma_3$ is an invariant, so that we can write:

$$\Delta = -\frac{4}{3}\left(\frac{\sqrt{-D}\gamma_3}{\sqrt{-D}}\right)^2.$$

The computation of the roots then depends on $\left(\frac{-3}{p}\right) = 1$. It is not clear that the above mentionned approach is really faster than the naive one.

9. Applications to ECPP and conclusion

In ECPP, the situation is as follows. We are given j and $m = p + 1 - U$ for some known U. We have to build an elliptic curve E having invariant j and cardinality m. We use the results of the preceding sections in the following way. We build a candidate E and compute its cardinality m'. If $m' = m$, then E is the correct answer, otherwise, we have to twist it.

In [12], a comparison of all possible class invariants for a given D was made using the height of their minimal polynomial. Though it is clear that it is easier to use invariants of small height, the results of the present article show that we might as well favor those invariants that give us a fast way of computing the right equation instead.

For instance, if $(D, 6) = 1$, using Stark's ideas whenever possible is a good thing. When $3 \mid D$ or $7 \mid D$, $\mathfrak{w}_3$ or $\mathfrak{w}_7$ should be preferred since we have a fast answer. Note now a new phenomenon. If we are interested in a prescribed p, we should use an invariant which depends on D, but also on p, or more precisely on the small factors of V. For instance, if $3 \mid V$, we can use the direct solution of $\Phi_3^c(X, J)$. If not, we may use some case where $\left(\frac{-D}{\ell}\right) = +1$, and $\ell \mid V$.

The present work has enlarged the set of D's for which the corresponding E's are easy to find. Nevertheless, there are cases which are badly covered (for instance odd primes which are non quadratic residues modulo 8, 3, 5, 7, such as $D = 163$) and that will require new ideas to be treated.

Acknowledgments. The author wants to thank A. Enge for his careful reading of the manuscript and suggesting many improvements.

References

[1] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime (II). Draft. Available on `http://listserv.nodak.edu/archives/nmbrthry.html`, 1992.

[2] A. O. L. Atkin. Probabilistic primality testing. In P. Flajolet and P. Zimmermann, editors, *Analysis of Algorithms Seminar I*. INRIA Research Report XXX, 1992. Summary by F. Morain.

[3] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, July 1993.

[4] B. J. Birch. Weber's class invariants. *Mathematika*, 16:283–294, 1969.

[5] C. Cailler. Sur les congruences du troisième degré. *Enseign. Math.*, 10:474–487, 1902.

[6] J.-M. Couveignes, L. Dewaghe, and F. Morain. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Research Report LIX/RR/96/03, LIX, April 1996. Available at `http://www.lix.polytechnique.fr/Labo/Francois.Morain/`.

[7] J.-M. Couveignes and F. Morain. Schoof's algorithm and isogeny cycles. In L. Adleman and M.-D. Huang, editors, *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 43–58. Springer-Verlag, 1994. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[8] D. A. Cox. *Primes of the form* $x^2 + ny^2$. John Wiley & Sons, 1989.

[9] L. Dewaghe. Remarks on the Schoof-Elkies-Atkin algorithm. *Math. Comp.*, 67(223):1247–1252, July 1998.

[10] N. D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In D. A. Buell and J. T. Teitelbaum, editors, *Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A. O. L. Atkin*, volume 7 of *AMS/IP Studies in Advanced Mathematics*, pages 21–76. American Mathematical Society, International Press, 1998.

[11] A. Enge and F. Morain. Further investigations of the generalized weber functions. Preprint, July 2001.

[12] A. Enge and F. Morain. Comparing invariants for class fields of imaginary quadratic fields. In C. Fieker and D. R. Kohel, editors, *Algorihmic Number Theory*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 252–266. Springer-Verlag, 2002. 5th International Symposium, ANTS-V, Sydney, Australia, July 2002, Proceedings.

[13] A. Joux and F. Morain. Sur les sommes de caractères liées aux courbes elliptiques à multiplication complexe. *J. Number Theory*, 55(1):108–128, November 1995.

[14] D. Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California at Berkeley, 1996.

[15] E. Lehmer. On some special quartic reciprocity law. *Acta Arith.*, XXI:367–377, 1972.

[16] F. Leprévost and F. Morain. Revêtements de courbes elliptiques à multiplication complexe par des courbes hyperelliptiques et sommes de caractères. *J. Number Theory*, 64:165–182, 1997.

[17] M. Maurer and V. Müller. Finding the eigenvalue in Elkies' algorithm. *Experiment. Math.*, 10(2):275–285, 2001.

[18] F. Morain. *Courbes elliptiques et tests de primalité.* Thèse, Université Claude Bernard–Lyon I, September 1990.

[19] F. Morain. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux*, 7:255–282, 1995.

[20] F. Morain. Primality proving using elliptic curves: an update. In J. P. Buhler, editor, *Algorithmic Number Theory*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 111–127. Springer-Verlag, 1998. Third International Symposium, ANTS-III, Portland, Oregon, june 1998, Proceedings.

[21] M. Newman. Construction and application of a class of modular functions. *Proc. London Math. Soc.*, 3(7):334–350, 1957.

[22] M. Newman. Construction and application of a class of modular functions (II). *Proc. London Math. Soc.*, 3(9):373–387, 1959.

[23] R. Padma and S. Venkataraman. Elliptic curves with complex multiplication and a character sum. *J. Number Theory*, 61:274–282, 1996.

[24] R. Schertz. Weber's class invariants revisited. To appear in J. Théor. Nombres Bordeaux, 2001.

[25] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7:219–254, 1995.

[26] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts in Math.* Springer, 1986.

[27] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Grad. Texts in Math.* Springer-Verlag, 1994.

[28] Th. Skolem. The general congruence of 4th degree modulo p, p prime. *Norsk. Mat. Tidsskr*, 34:73–80, 1952.

[29] H. M. Stark. Counting points on CM elliptic curves. *Rocky Mountain J. Math.*, 26(3):1115–1138, 1996.

[30] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 273:238–241, July 1971. Série A.

Laboratoire d'Informatique de l'École polytechnique (LIX), F-91128 Palaiseau Cedex, France
E-mail address, F. Morain: morain@lix.polytechnique.fr