MATHEMATICS OF COMPUTATION
Volume 78, Number 267, July 2009, Pages 1767–1786
S 0025-5718(08)02201-1
Article electronically published on October 29, 2008

COMPUTING THE ℓ-POWER TORSION OF AN ELLIPTIC CURVE OVER A FINITE FIELD

J. MIRET, R. MORENO, A. RIO, AND M. VALLS

Abstract. The algorithm we develop outputs the order and the structure, including generators, of the ℓ-Sylow subgroup of the group of rational points of an elliptic curve defined over a finite field. To do this, we do not assume any knowledge of the group order. We are able to choose points in such a way that a linear number of successive ℓ-divisions leads to generators of the subgroup under consideration. After the computation of a couple of polynomials, each division step relies on finding rational roots of polynomials of degree ℓ. We specify in complete detail the case $\ell = 3$, when the complexity of each trisection is given by the computation of cubic roots in finite fields.

1. Introduction

Throughout this paper let $p > 2$ be a prime number, $\mathbb{F}$ a finite field of characteristic p (we will write $\mathbb{F}_p$ for the prime field) and $E/\mathbb{F}$ an elliptic curve defined over $\mathbb{F}$. There exist positive integers m_1, m_2 such that the group of the $\mathbb{F}$-rational points is $E(\mathbb{F}) \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_1m_2\mathbb{Z}$ with m_1 dividing $|\mathbb{F}| - 1$ (see [19]). The possible pairs (m_1, m_2) that may occur are classified in [17] and [15] or [22]. But when $|\mathbb{F}|$ is large, computing the group order $|E(\mathbb{F})|$, and the group structure, is a non-trivial task. Our aim is to determine the Sylow subgroups of $E(\mathbb{F})$ without assuming any knowledge of the group order, so that the unique data is an equation for E.

Given a prime number ℓ, we are interested in the computation of the ℓ-Sylow subgroup of $E(\mathbb{F})$, namely the subgroup of rational points having ℓ-power order. We will denote this subgroup $\mathcal{S}_\ell(E(\mathbb{F}))$. The case $\ell = 2$ was already developed in [12].

The Sylow subgroup $\mathcal{S}_\ell(E(\mathbb{F}))$ will be non-trivial if and only if there exists a rational point of order ℓ. If $\ell \neq p$, to check this condition we can argue on rational roots of the ℓ-division polynomial. If $\ell = p$, we can use Gunji's formulae (see [6]).

As for the structure, the p-Sylow subgroup of $E(\mathbb{F})$ is cyclic and for any $\ell \neq p$ the ℓ-Sylow subgroup is a product of at most two cyclic groups. In any case, we must determine integers $n \geq r \geq 0$ such that

$$\mathcal{S}_\ell(E(\mathbb{F})) = E[\ell^n](\mathbb{F}) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^r\mathbb{Z}\,.$$

Received by the editor March 30, 2005 and, in revised form, May 28, 2008.

2000 *Mathematics Subject Classification.* Primary 11G20.

The first, second and fourth authors were supported in part by grant MTM2007-66842-C02-02.

The third author was supported in part by grants MTM2006-15038-C02-01 and 2005SGR 00443.

After some consideration of the initial computation of the rational ℓ-division points, we begin the description of the inductive process which leads to the determination of $\mathcal{S}_\ell(E(\mathbb{F}))$ showing how we can make an appropriate choice of points to perform successive divisions. Once this is done, we devote to the existence and computation of rational *ℓ-divisors* of a given rational point, which are the preimages under the multiplication-by-ℓ isogeny.

After the general description, we provide full details of the case $\ell = 3$. We develop a polynomial-time algorithm that for each elliptic curve $E/\mathbb{F}$ returns the complete information about its 3-Sylow subgroup. Namely, it returns

- n_3, the maximum value for which E has $\mathbb{F}$-rational points of order 3^{n_3};
- r_3 such that $\mathcal{S}_3(E(\mathbb{F})) \cong \mathbb{Z}/3^{n_3}\mathbb{Z} \times \mathbb{Z}/3^{r_3}\mathbb{Z}$;
- two points in $E(\mathbb{F})$, of orders 3^{n_3} and 3^{r_3}, generating $\mathcal{S}_3(E(\mathbb{F}))$.

In the last section we provide some examples of the performance of the algorithm.

For general results or common terminology on elliptic curves used throughout this paper, we refer to [19] or [7].

2. Basics on ℓ-division

Let $E/\mathbb{F}$ be an elliptic curve and let ℓ be a prime integer. Then, it is said that a point $Q \in E(\mathbb{F})$ *ℓ-divides* if there exists another point $P \in E(\mathbb{F})$ such that $[\ell]P = Q$, where $[\ell]$ denotes the multiplication-by-ℓ isogeny . It can be said, as well, that P is an *ℓ-divisor* of Q or that the point Q is *divisible* by ℓ.

The kernel of the multiplication-by-ℓ isogeny, the set of ℓ-divisors of $\mathcal{O}_E$, is $\ker[\ell] = E[\ell]$, the ℓ-torsion subgroup, which consists of $\mathcal{O}_E$ and the points of E having order ℓ. The rational points of $E[\ell]$ are denoted by $E(\mathbb{F})[\ell]$. They will be initially computed by the algorithm for determining $\mathcal{S}_\ell(E(\mathbb{F}))$. Therefore, our first task is to determine when this is a non-trivial subgroup and then compute its elements.

If p is the characteristic of the ground field and the curve E is given by an equation $y^2 = f(x)$ with $f(x)$ a cubic polynomial, then the Hasse invariant of E is the coefficient of x^{p-1} in the polynomial $f(x)^{\frac{p-1}{2}}$. If the Hasse invariant is zero, then $E[p]$ is trivial and so is the p-Sylow subgroup. Otherwise, $E[p]$ is a cyclic group of order p and the Sylow subgroup may be trivial or cyclic, according to whether $E(\mathbb{F})[p]$ is trivial or not.

In [6] we can find expressions for the x-coordinates of the p-torsion points. We have that the p-th power of such a coordinate is given by a rational expression in the coefficients of f and a $\frac{p-1}{2}$-th root of the Hasse invariant. This expression involves the computation of determinants of tridiagonal matrices of size $\frac{p-1}{2}$. We should compute one of these x-coordinates and then check if it actually corresponds to a rational point of the curve, namely if x is rational and $f(x)$ is a square in $\mathbb{F}$.

For example, for $p = 3$ and $E/\mathbb{F}$ given by $y^2 = x^3 + x^2 + a$ the Hasse invariant is 1 and the points of order 3 have x-coordinate 0, so that $E(\mathbb{F})[3] = E[3] = \{\mathcal{O}_E, (0, \sqrt{a}\,), (0, -\sqrt{a}\,)\}$ if a is a square in $\mathbb{F}$ and $E(\mathbb{F})[3]$ is trivial otherwise. For $p = 5$ and $E/\mathbb{F}$ defined by $y^2 = x^3 + a_4x + a_6$, in order to have rational abscissas of the 5-torsion points, the Hasse invariant $2a_4$ should be a square in $\mathbb{F}^*$. If so, then such an abscissa is obtained from $x^5 = 14a_6a_4 - (9a_4^2 + 2a_6^2/a_4)\sqrt{2a_4}$ and the 5-Sylow subgroup is non-trivial if, and only if, $x^3 + a_4x + a_6$ is a square in $\mathbb{F}$.

Now we assume $\ell \neq p$. Hence, $P \in E[\ell]$ if, and only if, $x(P)$ is a root of the ℓ-division polynomial $\Psi_\ell(x)$, which has degree $(\ell^2 - 1)/2$. We should then compute rational roots of this polynomial and check that the corresponding ordinates are also rational.

If an elliptic curve has a point of order ℓ, then it has either $\ell - 1$ points of order ℓ and $E(\mathbb{F})[\ell]$ and $\mathcal{S}_\ell(E(\mathbb{F}))$ are cyclic groups, or it has $\ell^2 - 1$ points of order ℓ and $E(\mathbb{F})[\ell]$ and $\mathcal{S}_\ell(E(\mathbb{F}))$ are products of two cyclic groups. In the first case, $E(\mathbb{F})[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ and $\mathcal{S}_\ell(E(\mathbb{F})) \cong \mathbb{Z}/\ell^n\mathbb{Z}$, for a certain integer $n \geq 1$. In the second one, $E(\mathbb{F})[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, namely the full ℓ-torsion is rational, and $\mathcal{S}_\ell(E(\mathbb{F})) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^r\mathbb{Z}$ with $1 \leq r \leq n$.

In order to distinguish the two possibilities, one can compute the degree of the polynomial $\delta(x) = \gcd(\Psi_\ell(x), x^{|\mathbb{F}|} - x)$. If it has degree zero, then both groups $E(\mathbb{F})[\ell]$ and $\mathcal{S}_\ell(E(\mathbb{F}))$ are trivial. Otherwise, according to the factorization patterns studied in [20], this degree can be $(\ell - 1)/2$, $\ell - 1$ or $(\ell^2 - 1)/2$. The first two cases correspond to the cyclic Sylow subgroup; in the first one any root of $\delta(x)$ is the abscissa of a point of $E(\mathbb{F})[\ell]$ and in the second case just half of the roots of $\delta(x)$ give rise to points in this group. In the third case, $E(\mathbb{F})[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ and the roots of $\delta(x) = \Psi_\ell(x)$ are the abscissas of those rational ℓ-torsion points different from $\mathcal{O}_E$.

In order to avoid factorization of a degree $(\ell^2-1)/2$ polynomial and gain efficiency one can use the modular polynomial $\Phi_\ell(j_E, X)$, which has degree $\ell + 1$. If it has no rational roots, then the group $E(\mathbb{F})[\ell]$ is trivial. Otherwise, computing its rational roots and then proceeding *à la SEA* (see [2] and [3]) to determine the kernel of the corresponding degree ℓ-isogeny one ends up with polynomials of degree $(\ell - 1)/2$. Their rational roots provide the abscissas of the ℓ-torsion points different from $\mathcal{O}_E$.

3. ℓ-DIVISION TREES

We give here some algebraic and combinatorial properties of the group $\mathcal{S}_\ell(E(\mathbb{F}))$. We will define some trees with roots which play a crucial role in the design of our algorithm to compute the ℓ-Sylow subgroup of $E(\mathbb{F})$, since they show us how to choose good ℓ-division paths.

As we said, the group of rational points having ℓ-power order is

$$\mathcal{S}_\ell(E(\mathbb{F})) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^r\mathbb{Z},$$

with $0 \leq r \leq n$. The following lemmas, which are easy to prove, give the first basic information on how these points are organized, according to their order and behavior under ℓ-division.

Lemma 3.1. *Let $Q \in E(\mathbb{F})$ be a point which ℓ-divides and P an ℓ-divisor of Q, then the ℓ-divisors of Q are exactly the points $P + E(\mathbb{F})[\ell]$.*

Lemma 3.2. *Let n, r, k be integers such that $1 \leq r \leq n$ and $1 \leq k < n$.*

1. *The group $\mathbb{Z}/\ell^n\mathbb{Z}$ has $(\ell - 1)\ell^{k-1}$ elements of order ℓ^k, all divisible by ℓ.*
2. *If $G = \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^r\mathbb{Z}$, then:*
   - (a) *if $k < r$, then G has $(\ell^2 - 1)\ell^{2k-2}$ elements of order ℓ^k, and all of them are divisible by ℓ;*
   - (b) *if $k = r$, there are also $(\ell^2 - 1)\ell^{2k-2}$ elements of order ℓ^k, but only $(\ell - 1)\ell^{2k-2}$ of them are divisible by ℓ;*
   - (c) *if $k > r$, then there are $(\ell - 1)\ell^{k+r-1}$ elements of order ℓ^k, and only $(\ell - 1)\ell^{k+r-2}$ of them are divisible by ℓ.*

Now we define a combinational structure associated with the group $\mathcal{S}_\ell(E(\mathbb{F}))$. It is a *tree with root* which we denote $\mathcal{T}_\ell$. We put $\mathcal{T}_\ell = (V, A)$, where the set of vertices is $V = \mathcal{S}_\ell(E(\mathbb{F}))$ and the set of edges is

$$A = \{(Q, P) \in V \times V : \ [\ell]P = Q\}.$$

So we deal with a *digraph* or *oriented graph*, which we call the *ℓ-division tree* of the $\mathcal{S}_\ell(E(\mathbb{F}))$ group.

Let us assume that $\mathcal{S}_\ell(E(\mathbb{F}))$ is non-trivial and use the terminology of trees to give a first description of $\mathcal{T}_\ell$. If $\mathcal{S}_\ell(E(\mathbb{F}))$ is cyclic, then $\mathcal{T}_\ell$ has $\ell - 1$ children of the root vertex, which is $\mathcal{O}_E$, and in the $k \geq 1$ levels every internal vertex has ℓ children. If $\mathcal{S}_\ell(E(\mathbb{F}))$ is not cyclic, then the root vertex has $\ell^2 - 1$ children and the rest of the vertices, either have ℓ^2 children or none. In Figure 1 we show the trees $\mathcal{T}_3$ corresponding to these two cases.

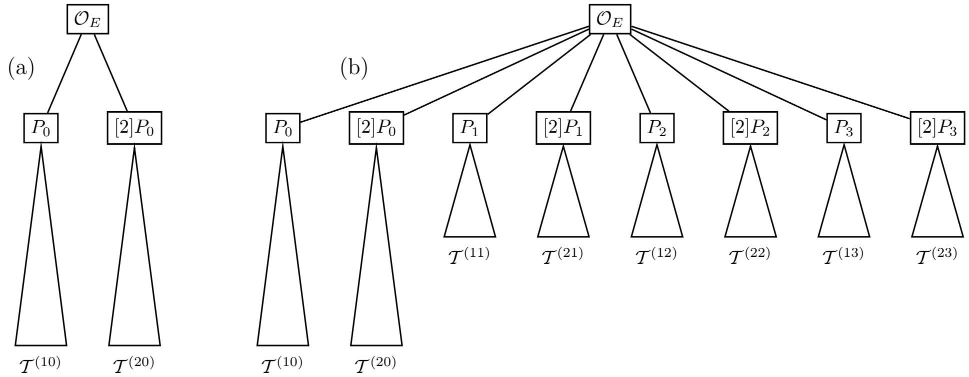

FIGURE 1. The trisection trees $\mathcal{T}_3$

Let $P_0 \in E(\mathbb{F})$ denote a point of order ℓ and $\{P_0, P_1\}$ a basis of $E[\ell]$, considered as a 2-dimensional vector space over the finite field of ℓ elements $\mathbb{F}_\ell$. Then, in the cyclic case $E(\mathbb{F})[\ell] = \langle P_0 \rangle = \{\mathcal{O}_E, [\pm j]P_0 : \ 1 \leq j \leq \frac{\ell-1}{2}\} \cong \mathbb{Z}/\ell\mathbb{Z}$ and in the non-cyclic case $E(\mathbb{F})[\ell] = \{[\varepsilon]P_0 + [\delta]P_1 : \ -\frac{\ell-1}{2} \leq \varepsilon, \delta \leq \frac{\ell-1}{2}\} \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. Here, we have $\ell + 1$ cyclic subgroups of order ℓ:

$$\langle P_0 \rangle, \quad \langle P_i = P_1 + [i-1]P_0 \rangle \quad i = 1 \ldots \ell.$$

The sets

$$\mathcal{T}^{(ji)} = \{P \in E(\mathbb{F}) : \ \exists\, h \geq 1 \text{ such that } [\ell^h]P = [j]P_i\},$$

with $-\frac{\ell-1}{2} \leq j \leq \frac{\ell-1}{2}$, $j \neq 0$, and $i \in \{0\}$ or $i \in \{0, 1, \ldots, \ell\}$, respectively, are the subtrees rooted at the rational points of order ℓ.

However, for our purposes it is enough to consider a simpler structure: instead of the tree $\mathcal{T}_\ell$ we will take a *representative tree* of the quotient tree $\mathbb{F}_\ell^* \backslash \mathcal{T}_\ell$ generated by the natural action of the multiplicative group $\mathbb{F}_\ell^*$ on the graph $\mathcal{T}_\ell$; see [18] for more details. Since for any j the diagram

$$\begin{tikzcd}
\mathcal{S}_\ell(E(\mathbb{F})) \arrow[r, "{[j]}"] & \mathcal{S}_\ell(E(\mathbb{F})) \\
\mathcal{S}_\ell(E(\mathbb{F})) \arrow[u, "{[\ell]}"] \arrow[r, "{[j]}"'] & \mathcal{S}_\ell(E(\mathbb{F})) \arrow[u, "{[\ell]}"']
\end{tikzcd}$$

is commutative, the scalar multiplication $[j]$ is an automorphism of $\mathcal{T}_\ell$. It maps the subtree $\mathcal{T}^{(i)}$ into $\mathcal{T}^{(ji)}$, and therefore these are isomorphic trees. We denote $\widetilde{\mathcal{T}}_\ell$ a representative tree of $\mathbb{F}_\ell^* \backslash \mathcal{T}_\ell$. All the information about ℓ-divisibility will be obtained from this representative tree, which we show in Figure 2 for $\ell = 3$.

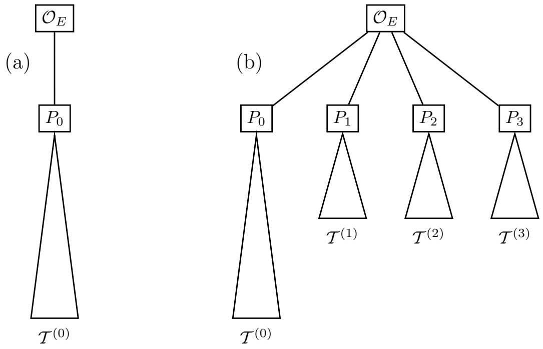

FIGURE 2. The representative trees $\widetilde{\mathcal{T}}_3$

Let us describe in further detail the structure of these representative trees. We recall that a *complete m-ary* tree is a tree with root in which all internal vertices have out-degree m and all the leaves are at the same height.

The simple structure of a cyclic group can be expressed in terms of the combinatorial structure of $\widetilde{\mathcal{T}}_\ell$: if $\mathcal{S}_\ell(E(\mathbb{F})) \cong \mathbb{Z}/\ell^n\mathbb{Z}$, then the subtree $\mathcal{T}^{(0)}$ is a complete ℓ-ary tree of height $n-1$.

In the non-cyclic case, namely when $\mathcal{S}_\ell(E(\mathbb{F})) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^r\mathbb{Z}$, with $1 \le r \le n$, the structure of $\widetilde{\mathcal{T}}_\ell$ is the following:

- If $r = n$, then the subtrees $\mathcal{T}^{(i)}$, where $i \in \{0, 1, \dots, \ell\}$, are all isomorphic. They are complete ℓ^2-ary trees of height $n-1$.
- If $1 \le r < n$, then ℓ of the subtrees $\mathcal{T}^{(i)}$ are ℓ^2-ary complete trees of height $r-1$. The remaining one, the subtree denoted as $\mathcal{T}^{(0)}$ in Figure 2(b), is also ℓ^2-ary and its height is $n-1$. But it is complete only until level r. From there on it has leaves, since, according to Lemma 3.2, in each level only one ℓ-th of the points are ℓ-divisible.

The strategy followed by the algorithm to determine the ℓ-Sylow subgroup $\mathcal{S}_\ell(E(\mathbb{F}))$ of $E(\mathbb{F})$ will consist of descending through the subtrees of the representative tree until reaching its leaves. This way, the values n and r will be obtained, as well as a couple of points $\{Q, R\}$, with respective orders ℓ^n and ℓ^r, which are generators of $\mathcal{S}_\ell(E(\mathbb{F}))$. In fact, due to this linear structure, the descending process can be restricted to only two subtrees[1]. Moreover, since these subtrees are complete until level r, each step will consist of finding just one ℓ-divisor of the present point. This way, from any pair of the root-points of the subtrees, for instance, P_0 and P_1, two lists of successive ℓ-divisors will be obtained:

$$\{P_0, P_{0,2}, P_{0,3}, \dots, P_{0,k}\} \text{ and } \{P_1, P_{1,2}, P_{1,3}, \dots, P_{1,k}\}.$$

When either one or none of the points $P_{0,k}, P_{1,k}$ do not ℓ-divide, then $r = k$. The point of order ℓ^r is one of the points that does not ℓ-divide. In case that none of

[1] We acknowledge Enric Nart (UAB, Spain) for his comments suggesting this approach [14].

them do, it should be checked whether some of the $\ell - 1$ points $P_{0,r} + [i]P_{1,r}$, for $i \in \{1, \dots, \ell - 1\}$, would ℓ-divide. If not, then $n = r$ and $\{Q = P_{0,n}, R = P_{1,n}\}$ would be the generators of $\mathcal{S}_\ell(E(\mathbb{F}))$. Otherwise, it holds that $n > r$, and we have identified the subtree of maximum height $n-1$. To compute n and a point of order ℓ^n, we should descend through this subtree, say $\mathcal{T}^{(0)}$, until we reach its height. The problem is that we may end up in an external node whose depth is not maximal, namely a point of order ℓ^k, with $r < k < n$, which cannot be ℓ-divided. To deal with this situation we consider the sets

$$\mathcal{Q}_{i,m} = \{Q \in \mathcal{T}^{(i)} : \operatorname{ord}(Q) = \ell^m\},$$

with $1 \le m \le n$ when $i = 0$ and $1 \le m \le r$ when $i \in \{1, \dots, \ell\}$.

Proposition 3.3. *Let us assume $\mathcal{S}_\ell(E(\mathbb{F})) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^r\mathbb{Z}$ with $1 \le r < n$. Let $r < k < n$, $Q \in \mathcal{Q}_{0,k}$ and $R \in \mathcal{Q}_{1,r}$. Then, exactly one of the points in the set $\{Q + [j]R : -\frac{\ell-1}{2} \le j \le \frac{\ell-1}{2}\}$ can be ℓ-divided.*

Proof. First, let us observe that ℓ-divisibility of two of the points in the set $\{Q + [j]R : -\frac{\ell-1}{2} \le j \le \frac{\ell-1}{2}\}$ would imply the ℓ-divisibility of R, which contradicts our assumption.

Let us assume that we cannot ℓ-divide the point Q. Since $k < n$, we know that there is some $Q' \in \mathcal{Q}_{0,k}$ which can be ℓ-divided: $Q' = [\ell]P'$. We have

$$\mathcal{Q}_{0,k} = \{[u]Q + [v]R : u \in \mathbb{Z}/\ell^k\mathbb{Z},\ u \equiv 1 \bmod \ell,\ v \in \mathbb{Z}/\ell^r\mathbb{Z}\}$$

and, hence, $Q' = [u]Q + [v]R$ with $u = \ell u' + 1$, for some $u' \in \{0, \dots, \ell^{k-1} - 1\}$, and $v = \ell v' + v''$, where $v' \in \{0, 1, \dots, \ell^{r-1}\}$ and $-\frac{\ell-1}{2} \le v'' \le \frac{\ell-1}{2}$, $v'' \ne 0$. Then, from

$$Q' = [\ell u']Q + [\ell v']R + Q + [v'']R = \ell P'$$

we get that $P' - ([u']Q + [v']R)$ is an ℓ-divisor of $Q + [v'']R$. □

4. ℓ-DIVIDING

In the previous sections we have been sketching the main ideas involved in the design of the algorithm presented in this paper. At this point, we face the problem that arises at each step of the algorithm: finding a point $P = (x, y) \in E(\mathbb{F})$ such that

$$[\ell]\, P = Q$$

for a given point $Q = (\xi, \zeta) \in E(\mathbb{F})$. Therefore, such a point P belongs to the preimage of Q by the multiplication-by-ℓ isogeny, and we can consider the following expression in terms of division polynomials:

$$x([\ell]P) = x(P) - \frac{\Psi_{\ell-1}(x,y)\Psi_{\ell+1}(x,y)}{\Psi_\ell^2(x,y)},$$

(for instance, see [2]), to obtain that the point (x, y) must be a root of

$$(x - \xi)\Psi_\ell^2(x,y) - \Psi_{\ell-1}(x,y)\Psi_{\ell+1}(x,y) = 0.$$

Now working modulo the equation of the elliptic curve, we are led to the one variable polynomial

$$f_{\xi,[\ell]}(x) = (x - \xi)\Psi_\ell^2(x) - \bar{\Psi}_{\ell-1}(x,y)\bar{\Psi}_{\ell+1}(x,y), \tag{4.1}$$

which is the polynomial associated to the ℓ-division of a point having abscissa ξ. Notice that its degree is ℓ^2, its *trace* is $\xi\ell^2$ and it has distinct roots whenever Q is taken not to be a 2-torsion point.

With this approach, in order to compute the ℓ-Sylow subgroup of $E(\mathbb{F})$ we use once the formula (4.1) to obtain the polynomial $f_{\xi,[\ell]}(x) \in \mathbb{F}[x,\xi]$. Then, starting with suitable rational points of order ℓ as explained in the previous section, at each ℓ-division step of the algorithm we have a given point $Q = (\xi, \zeta)$ and we should find a root in $\mathbb{F}$ of a degree ℓ^2 polynomial in $\mathbb{F}[x]$.

However, this computational cost can be improved if we take advantage of an isogeny decomposition

$$\begin{tikzcd} E \arrow[rr, "{[\ell]}"] \arrow[dr, "\mathcal{I}"'] & & E \\ & E' \arrow[ur, "\widehat{\mathcal{I}}"'] & \end{tikzcd} \qquad [\ell] = \widehat{\mathcal{I}} \circ \mathcal{I}$$

where $\mathcal{I}$ is an isogeny of degree ℓ and $\widehat{\mathcal{I}}$ denotes its dual. Then, to carry out the ℓ-division steps the above degree ℓ^2 polynomial can be replaced by a couple of polynomials of degree ℓ, associated to $\mathcal{I}$ and $\widehat{\mathcal{I}}$ respectively: first we consider the preimages of Q by $\widehat{\mathcal{I}}$, fix one of them $Q' = (X, Y)$ and then consider its preimage by $\mathcal{I}$.

In what follows we show how to consider an appropriate isogeny $\mathcal{I}$ of degree ℓ, compute the polynomials attached to $\mathcal{I}$ and its dual $\widehat{\mathcal{I}}$, and finally use them to find an ℓ-divisor.

In the context of our problem, there is an obvious candidate for the isogeny $\mathcal{I}$, since we are assuming from the beginning that the elliptic curve E has a rational point P_0 of order ℓ. Let $\mathcal{I}$ be the isogeny whose kernel is the cyclic group generated by this point. Hence,

$$\mathcal{I} :\ E \longrightarrow E' = E/\langle P_0 \rangle$$

is a separable isogeny of degree ℓ defined over $\mathbb{F}$. This situation corresponds also to the existence of a rational root of the modular polynomial $\Phi_\ell(x, j_E)$, which is the j-invariant of the curve E'. If we have followed the procedure explained at the end of Section 2, we already have such an isogeny $\mathcal{I}$ explicitly computed.

The isogeny equations provide the identities

$$\frac{N(x)}{D(x)} = X, \qquad \frac{\widehat{N}(X)}{\widehat{D}(X)} = \xi, \tag{4.2}$$

where $N(x), D(x), \widehat{N}(X), \widehat{D}(X)$ are polynomials with coefficients in $\mathbb{F}$. The SEA algorithm (cf. [13, 3]) efficiently determines polynomials $F_\ell(x)$ and $\widehat{F_\ell}(X)$, both of degree $(\ell-1)/2$, such that its roots are the abscissas of the non-trivial points in the kernel of the respective isogeny:

$$D(x) = F_\ell(x)^2, \qquad \widehat{D}(X) = \widehat{F_\ell}(X)^2.$$

The final computation of the abscissa can be done following Kohel [8, p. 14] or Dewaghe [4]:

$$\begin{aligned} N(x) = (4x^3 + b_2x^2 + 2b_4x + b_6)\left(F_\ell'(x)^2 - F_\ell''(x)F_\ell(x)\right) \\ - (6x^2 + b_2x + b_4)F_\ell'(x)F_\ell(x) + (\ell x - 2S_1)F_\ell(x)^2, \end{aligned} \tag{4.3}$$

where S_1 is the *trace coefficient* of F_ℓ, namely the first elementary symmetric polynomial in the distinct abscissas of the points in the kernel of the isogeny. The formula for $\widehat{N}(X)$ is analogous. As we said before, an ℓ-division step now involves first finding a root $X_0 \in \mathbb{F}$ of the degree ℓ polynomial $\widehat{N}(X) - \xi\, \widehat{D}(X) \in \mathbb{F}[X]$ and then a root of the degree ℓ polynomial $N(x) - X_0\, D(x) \in \mathbb{F}[x]$.

For the sake of completeness, we would like to mention a third way to perform an ℓ-division step in the context of a *small* prime ℓ and a rational order ℓ point P_0 explicitly known, so that the set of abscissas $\{x(P_0), x(2P_0), \ldots, x((\ell-1)P_0)\}$ is easy to obtain. In this case we are able to provide a purely algebraic description of the procedure.

In order to fix notation, for $E, E'/\mathbb{F}$ elliptic curves, $\mathcal{I} : E \to E'$ a non-constant isogeny and $Q \neq \mathcal{O}_{E'}$ a point on E', we call the *associated polynomial* for the isogeny $\mathcal{I}$ and the point Q the polynomial

$$f_{x(Q),\mathcal{I}}(x) = \prod_{\mathcal{I}(P)=Q} (x - x(P)) \in \overline{\mathbb{F}}[x]. \tag{4.4}$$

It is monic of degree $|G|$, where G is the kernel of $\mathcal{I}$. If Q is a rational point and G is $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-invariant, namely if the isogeny is defined over $\mathbb{F}$, then $f_{x(Q),\mathcal{I}}(x) \in \mathbb{F}[x]$.

We fix the isogeny $\mathcal{I}_0 :\ E \longrightarrow E' = E/\langle P_0\rangle$, which is defined over $\mathbb{F}$. As shown in [11], a generalization of Vélu's formulae [21] allows us to obtain the coefficients of the polynomial

$$f_{X,\mathcal{I}_0}(x) = \prod_{0\le\lambda\le\ell-1} (x - x(P + \lambda P_0)),$$

for $X = x(\mathcal{I}_0(P))$ and P a point on E,

$$f_{X,\mathcal{I}_0}(x) = \sum_{r=0}^{\ell} (-1)^r \Big(S_{r-1}X + S_r + \sum_{i=0}^{r-2} (-1)^i w_i S_{r-i-2}\Big) x^{|G|-r}, \tag{4.5}$$

where S_j is the j-th elementary symmetric polynomial in the abscissas of the points $P_0, 2P_0, \ldots (\ell-1)P_0$ and the w_i, the generalized Vélu parameters, are given by

$$w_i = (2i+3)S^{(i+2)} + \frac{(i+1)b_2}{2} S^{(i+1)} + \frac{(2i+1)b_4}{2} S^{(i)} + \frac{ib_6}{2} S^{(i-1)}, \tag{4.6}$$

where $S^{(j)}$ indicates the j-th power sum of the abscissas of the same set of points as before, with the b_i being the usual quantities defined in terms of the Weierstraß coefficients of E ([19]). Under our current hypothesis, using these formulas we are able to efficiently determine the polynomial $f_{X,\mathcal{I}_0}(x)$ in terms of $X = x(\mathcal{I}_0(P))$, which is still unknown. This is another way to obtain the polynomial $N(x) - X\, D(x)$ of the previous setting.

As for the polynomial attached to the dual isogeny, taking into account that $x(\widehat{\mathcal{I}}_0(\mathcal{I}_0(P))) = \xi$, this polynomial is

$$f_{\xi,\widehat{\mathcal{I}}_0}(x) = \prod_{T\in\ker\widehat{\mathcal{I}}_0} (x - x(\mathcal{I}_0(P) + T)). \tag{4.7}$$

The following lemma determines the kernel of the dual isogeny.

Lemma 4.1. *Let E be an elliptic curve, G a non-trivial subgroup of E, $n = |G|$ and $\mathcal{I}_G : E \to E/G$ the isogeny with kernel G. Then,*

$$\ker \widehat{\mathcal{I}}_G = \mathcal{I}_G(E[n]) \cong E[n]/G.$$

Proof. The claim follows from the exhaustivity of $\mathcal{I}_G$ and the fact that $\widehat{\mathcal{I}}_G \circ \mathcal{I}_G = [n]$. On the other hand, $\{\mathcal{O}_E\} \longrightarrow G \hookrightarrow E[n] \xrightarrow{\mathcal{I}_G} \mathcal{I}_G(E[n]) \xrightarrow{\widehat{\mathcal{I}}_G} \{\mathcal{O}_E\}$ is an exact sequence. □

Going back to our particular case, we let $\{P_0, P_1\}$ be a basis of $E[\ell]$ as an $\mathbb{F}_\ell$-vector space. Then, we have

$$\ker \widehat{\mathcal{I}}_0 = \langle \mathcal{I}_0(P_1) \rangle$$

and the points in the kernel of the dual isogeny $\widehat{\mathcal{I}}_0$ are not always rational.

The polynomial associated to the dual isogeny can be written as

$$f_{\xi,\widehat{\mathcal{I}}_0}(x) = \prod_{k=0}^{\ell-1} (x - x(\mathcal{I}_0(P) + [k]\mathcal{I}_0(P_1))) = \prod_{k=0}^{\ell-1} (x - x(\mathcal{I}_0(P + [k]P_1)))\,. \tag{4.8}$$

Notice that $X = x(\mathcal{I}_0(P))$ is one of the ℓ roots of this polynomial, which are

$$X_k = x(\mathcal{I}_0(P + [k]P_1)),\ k = 0, 1, \ldots, \ell - 1.$$

Over $\mathbb{F}(X_0, \ldots, X_{\ell-1})$, the splitting field of $f_{\xi,\widehat{\mathcal{I}}_0}(x)$, we have the factorization

$$f_{\xi,[\ell]}(x) = \prod_{k=0}^{\ell-1} f_{X_k,\mathcal{I}_0}(x). \tag{4.9}$$

Therefore, the rational values of the unknown X that we are looking for give rise to polynomials $f_{X,\mathcal{I}_0}(x)$ dividing $f_{\xi,[\ell]}(x)$. Let us show now that the resultant of $f_{\xi,[\ell]}(x)$ and $f_{X,\mathcal{I}_0}(x)$, both considered as polynomials over $\mathbb{F}(X)[x]$, is a power of the polynomial $f_{\xi,\widehat{\mathcal{I}}_0}(X) \in \mathbb{F}[X]$.

Proposition 4.2. *Let $E/\mathbb{F}$ be an elliptic curve, $\{P_0, P_1\}$ a basis of $E[\ell]$ as an $\mathbb{F}_\ell$-vector space with $P_0 \in E(\mathbb{F})[\ell]$, and $f_{\xi,[\ell]}(x), f_{X,\mathcal{I}_0}(x) \in \mathbb{F}[x]$ the polynomials associated to the isogenies $[\ell]$ and $\mathcal{I}_0 = \mathcal{I}_{\langle P_0 \rangle}$, respectively. Then*

$$\operatorname{Res}_x(f_{\xi,[\ell]}(x), f_{X,\mathcal{I}_0}(x)) = c\left(f_{\xi,\widehat{\mathcal{I}}_0}(X)\right)^\ell, \tag{4.10}$$

where $c \in \mathbb{F}^*$ and $f_{\xi,\widehat{\mathcal{I}}_0}(x)$ is the polynomial associated to the dual isogeny.

Proof. Consider the polynomial $f_{\xi,[\ell]}(x) \bmod f_{X,\mathcal{I}_0}(x)$ in $\mathbb{F}(X)[x]$. As a polynomial in X, it vanishes for the values X_k, $k \in \{0, 1, \ldots, \ell-1\}$, and it is therefore divisible by $f_{\xi,\widehat{\mathcal{I}}_0}(X) = \prod_{k=0}^{\ell-1}(X - X_k)$. We denote $r(X, x)$ as the quotient. Thus, from the properties of the resultant, it follows that

$$\begin{aligned}\operatorname{Res}_x(f_{\xi,[\ell]}(x), f_{X,\mathcal{I}_0}(x)) &= -\operatorname{Res}_x(f_{X,\mathcal{I}_0}(x), f_{\xi,[\ell]}(x) \bmod f_{X,\mathcal{I}_0}(x)) \\ &= -\operatorname{Res}_x(f_{X,\mathcal{I}_0}(x), r(X,x) f_{\xi,\widehat{\mathcal{I}}_0}(X)) \\ &= -\left(f_{\xi,\widehat{\mathcal{I}}_0}(X)\right)^\ell \operatorname{Res}_x(f_{X,\mathcal{I}_0}(x), r(X,x))\,.\end{aligned}$$

The resultant can be written as

$$\operatorname{Res}_x(f_{\xi,[\ell]}(x), f_{X,\mathcal{I}_0}(x)) = \prod_{j=1}^{\ell^2} f_{X,\mathcal{I}_0}(\alpha_j),$$

where $\alpha_j \in \overline{\mathbb{F}},\ j \in \{1, 2, \ldots, \ell^2\}$ are the roots of $f_{\xi,[\ell]}(x)$. Since $f_{X,\mathcal{I}_0}$ is linear in X, the resultant is a non-zero polynomial in $\mathbb{F}[X]$ of degree ℓ^2. Consequently, the factor $\operatorname{Res}_x(f_{X,\mathcal{I}_0}(x), r(X,x))$ belongs to $\mathbb{F}^*$. □

Putting this all together, this method consists of determining the degree ℓ^2 polynomial $f_{\xi,[\ell]}(x)$, depending on ξ, using (4.1); determining $f_{X,\mathcal{I}_0}(x)$, depending on

X, using (4.5) and, finally, we compute $f_{\xi,\widehat{\mathcal{I}}_0}(X)$, depending on ξ, using the resultant as in (4.10). Once this is done, in each ℓ-dividing step an abscissa ξ is fixed and we are faced as before with the computation of roots of two degree ℓ polynomials.

To avoid the computation of the resultant we can also use a hybrid method, determining the polynomial $f_{X,\mathcal{I}_0}(x)$ using the algebraic formulas in the abscissas of the multiples of the point P_0 and using the analytic formulas of the SEA algorithm to compute $f_{\xi,\widehat{\mathcal{I}}_0}(X) = \widehat{N}_0(X) - \xi\,\widehat{D}_0(X)$.

To finish this section, we provide an easy example for a 5-division procedure, by fixing a small field of definition: $\mathbb{F} = \mathbb{F}_p$ with $p = 1021$. From the family $y^2 + (t+1)xy + ty = x^3 + tx^2$ of elliptic curves having $(0,0)$ as a point of order 5 ([19, Exercise 8.13]), we take the elliptic curve corresponding to the value $t = 81$, namely

$$E/\mathbb{F}_{1021}:\; y^2 + 82xy + 81y = x^3 + 81x^2.$$

Its 5-division polynomial is

$$\begin{aligned}\Psi_5(x) = x(&5\,x^{11} + 526\,x^{10} + 272\,x^9 + 145\,x^8 + 525\,x^7 + 682\,x^6 + 698\,x^5\\ &+ 493\,x^4 + 950\,x^3 + 394\,x^2 + 888\,x + 45).\end{aligned}$$

Since $\gcd(\Psi_5(x), x^{1021} - x) = \Psi_5(x)$, we know that it splits completely over $\mathbb{F}$ and that $E(\mathbb{F})[5] \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. From expression (4.1) we obtain the polynomial $f_{\xi,[5]}(x)$ in terms of the abscissa ξ:

$$\begin{aligned}f_{\xi,[5]}(x) = x^{25} &+ 996\,\xi\,x^{24} + (746 + 866\,\xi)\,x^{23} + (631 + 358\,\xi)\,x^{22} + (137 + 328\,\xi)\,x^{21}\\ &+ (50 + 1014\,\xi)\,x^{20} + (373 + 125\,\xi)\,x^{19} + (689 + 141\,\xi)\,x^{18} + (389 + 493\,\xi)\,x^{17}\\ &+ (280 + 160\,\xi)\,x^{16} + (643 + 1014\,\xi)\,x^{15} + (337 + 773\,\xi)\,x^{14} + (380 + 351\,\xi)\,x^{13}\\ &+ (912 + 817\,\xi)\,x^{12} + (399 + 397\,\xi)\,x^{11} + (621 + 675\,\xi)\,x^{10} + (320 + 263\,\xi)\,x^9\\ &+ (394 + 307\,\xi)\,x^8 + (986 + 725\,\xi)\,x^7 + (141 + 2\,\xi)\,x^6 + (136 + 926\,\xi)\,x^5\\ &+ (916 + 964\,\xi)\,x^4 + (845 + 739\,\xi)\,x^3 + (129 + 17\,\xi)\,x^2 + 962\,x + 521.\end{aligned}$$

The cyclic subgroup of $E(\mathbb{F})[5]$ generated by the point $P_0 = (0,0)$, which is

$$\langle P_0\rangle = \{P_0 = (0,0), [2]P_0 = (940,435), [3]P_0 = (940,0), [4]P_0 = (0,940), \mathcal{O}_E\}\,,$$

is the kernel of the isogeny $\mathcal{I}_0$. The elementary symmetric polynomials on the abscissas of the points in $\langle P_0\rangle$ and the generalized Vélu parameters are

$$S_1 = 859,\; S_2 = 435,\; S_3 = 0, \quad w_0 = 430,\; w_1 = 594,$$

so that

$$f_{X,\mathcal{I}_0}(x) = x^5 + (1020\,X + 162)x^4 + (859\,X + 865)x^3 + (586\,X + 826)x^2 + 882\,x + 340.$$

Finally, computing the resultant, we determine the polynomial

$$\begin{aligned}f_{\xi,\widehat{\mathcal{I}}_0}(X) = X^5 &+ (996\xi + 211)X^4 + (696\xi + 59)X^3 + (624\xi + 163)X^2\\ &+ (584\xi + 281)X + 369\xi + 1008.\end{aligned}$$

The two polynomials of degree 5 we have computed are what we need to perform the 5-division of points. As an example, we show descent from $P_0 = (0,0)$ in the 5-division tree. Taking $\xi = 0$ in the second polynomial we obtain

$$f_{0,\widehat{\mathcal{I}}_0}(X) = X^5 + 211X^4 + 59X^3 + 163X^2 + 1007X + 1008,$$

which has rational roots $48, 491, 560, 871, 882$. Each one of them determines a polynomial $f_{X_k,\mathcal{I}_0}(x)$. Let us look for a rational root of the first one, which is

$$f_{48,\mathcal{I}_0}(x) = x^5 + 114x^4 + 236x^3 + 366x^2 + 882x + 340.$$

We obtain the root $x_1 = 201$ which is the abscissa of the points $P_{0,2} = (201, 261)$ and $-P_{0,2} = (201, 533)$. One of these points is a 5-divisor of P_0 and the other one a 5-divisor of $-P_0$. Let us continue with the 5-division of $P_{0,2} = (201, 261)$. Now we take $\xi = 201$ and we get

$$f_{201,\widehat{\mathcal{I}}_0}(X) = X^5 + 291X^4 + 78X^3 + 4X^2 + 976X + 644.$$

This polynomial has no rational roots and consequently the point $P_{0,2}$ is not divisible by 5.

Table 1 shows the average time in seconds to perform the ℓ-division of a point using this method. We have considered primes p between 90 and 190 bits and one hundred elliptic curves $E/\mathbb{F}_p$ to carry out ℓ-division for primes $3 \leq \ell \leq 19$. The calculations are due to J. Molgó, who executed a LiDIA [9] program over a Pentium IV 1.7 GHz.

Table 1. Average time of the ℓ-division

Bit length of prime p	ℓ						
	3	5	7	11	13	17	19
90	0.0032	0.0058	0.0076	0.0169	0.0289	0.2066	0.8254
110	0.0035	0.0075	0.0097	0.0218	0.0378	0.2539	1.0745
130	0.0048	0.0092	0.0135	0.0322	0.0444	0.3026	1.2118
150	0.0051	0.0082	0.0144	0.0328	0.0524	0.3459	1.4035
170	0.0070	0.0125	0.0186	0.0397	0.0664	0.4310	1.6776
190	0.0082	0.0134	0.0198	0.0438	0.0702	0.4543	1.7607

Now we work out the same example but proceeding as in the SEA algorithm to determine isogenies, so that computation of the degree ℓ^2 polynomial and the resultant are avoided. We consider the short Weierstraß equation

$$E/\mathbb{F}: \; y^2 = x^3 + 313x + 775.$$

The isomorphism between the two models is $(x, y) \xrightarrow{\varphi} (36x+724, 216y+688x+580)$ and $\varphi(0, 0) = (724, 580)$ is a point of order 5 in this second model.

The j-invariant is 953 and the modular polynomial $\Phi_5(x, 953) \mod 1021$ has root $j = 105$. The isogenous curve is

$$E'/\,\mathbb{F}: \; y^2 = x^3 + 222x + 497$$

and the equations of the isogeny $E \xrightarrow{\mathcal{I}} E', (x, y) \to (X, Y)$ are

$$\begin{aligned} X &= \frac{x^5 + 894x^4 + 801x^3 + 419x^2 + 858x + 15}{F_5(x)^2}, \\ Y &= \frac{(x^6 + 320x^5 + 185x^4 + 966x^3 + 247x^2 + 345x + 586)y}{F_5(x)^3}. \end{aligned}$$

where $F_5(x) = x^2+447x+647 = (x-724)(x-871)$ is the polynomial corresponding to the kernel. Therefore the polynomial $N(x) - X\,D(x)$ involved in the 5-division procedure is

$$x^5+(894+1020X)x^4+(801+127X)x^3+(419+34X)x^2+(858+489X)x+(15+X).$$

The corresponding equations for the dual isogeny, $(X,Y) \xrightarrow{\widehat{\mathcal{I}}} (\xi,\zeta)$, are

$$\begin{aligned} \xi &= \frac{776X^5+638X^4+914X^3+61X^2+271X+250}{\widehat{F}_5(X)^2}, \\ \zeta &= \frac{(972X^6+804X^5+686X^4+503X^3+630X^2+257X+875)Y}{\widehat{F}_5(X)^3}, \end{aligned}$$

where $\widehat{F}_5(X) = X^2+828X+293$. Therefore, $\widehat{N}(x) - \xi\,\widehat{D}(x)$, the second polynomial involved in the 5-division procedure, is

$$\begin{aligned} 776X^5+(1020\xi+638)X^4+(386\xi+914)X^3+(963\xi+61)X^2 \\ +(788\xi+271)X+(936\xi+250). \end{aligned}$$

Putting $\xi = 724$, we obtain a rational root $X = 22$. Substituting in the first polynomial we get a polynomial in $\mathbb{F}[x]$ having rational roots $146, 303, 326, 593$ and 823. If we go on with the 5-division procedure using the first one, namely $\xi = 146$, then we deal with the polynomial

$$776X^5+492X^4+94X^3+782X^2+967X+92.$$

Its rational roots X give rise to polynomials $N(x) - X\,D(x)$ without rational roots, which means that at the point $(146, 410)$ the 5-division descent stops.

5. Trisection

This section is devoted to develop the algorithm in full detail for $\ell = 3$. The main purpose is to show that we can reduce the trisection of points to computation of cubic roots in finite fields. We use this fact for the complexity analysis of the algorithm.

If E is an elliptic curve over a finite field $\mathbb{F}$ of characteristic $p > 3$, the abscissas of the points of order 3 are given by the roots of the 3-division polynomial, which is a quartic polynomial with coefficients in $\mathbb{F}$, explicitly computable in terms of the equation of $E/\mathbb{F}$. Therefore, to decide whether or not a rational point of order 3 exists, we compute the gcd of this polynomial and $x^{|\mathbb{F}|} - x$. In case of existence, the explicit determination of such a point may also require the computation of a root of the quartic polynomial in the finite field $\mathbb{F}$. Once we have done this, we can take the point of order 3 to the origin and work with a model

$$E/\mathbb{F}: \ y^2+3axy+by = x^3.$$

Its discriminant is $\Delta = 27(a^3-b)b^3$ and the discriminant of the equation, considered as a quadratic equation in y, is $d(x) = 4x^3+(3ax+b)^2 = 4x^3+9a^2x^2+6abx+b^2$. An element $x \in \mathbb{F}$ is the abscissa of a point in $E(\mathbb{F})$ if, and only if, $d(x) \in \mathbb{F}^2$.

Using this model, the 3-division polynomial of $E/\mathbb{F}$ is

$$\Psi_3(x) = 3x(x^3+3a^2x^2+3abx+b^2).$$

Proposition 5.1. *The polynomial $\psi_3(x) = x^3+3a^2x^2+3abx+b^2$:*

(1) *is irreducible in $\mathbb{F}[x]$ if, and only if, $\Delta \notin \mathbb{F}^{*\,3}$,*

(2) *splits completely in $\mathbb{F}[x]$ if, and only if, $\Delta \in \mathbb{F}^{*\,3}$ and $-3 \in \mathbb{F}^{*\,2}$.*

Proof. The roots of ψ_3 in $\overline{\mathbb{F}}$ are $x_j = -(\Delta_j^2 + a\Delta_j + a^2)$, where $\{\Delta_j\ ,\ j = 1,2,3\}$ are the cubic roots of $\Delta/27b^3$ in $\overline{\mathbb{F}}$. If $\omega \in \overline{\mathbb{F}}$ is a primitive cubic root of unity, we have $x_j = -(a - \omega\Delta_j)(a - \omega^2\Delta_j)$. □

If $|\mathbb{F}| \equiv -1 \bmod 3$, then $-3 \notin \mathbb{F}^{*\,2}$ and $\omega \notin \mathbb{F}$. Every element of $\mathbb{F}^*$ is a cube and has a unique cubic root in $\mathbb{F}^*$. In this case, ψ_3 has a unique root in $\mathbb{F}$. But it is not the abscissa of a rational point, since $d(x) = 4\psi_3(x) - 3(b + ax)^2$.

If $|\mathbb{F}| \equiv 1 \bmod 3$, then $\omega \in \mathbb{F}$. Only one third of the elements in $\mathbb{F}^*$ are cubes and each one of them has three cubic roots in $\mathbb{F}^*$.

Corollary 5.2. *If* $|\mathbb{F}| \equiv -1 \bmod 3$*, then* $\Psi_3(x) = x(x - x_1)\widetilde{\psi}_3(x)$ *and*

$$E(\mathbb{F})[3] = \{\mathcal{O}_E, (0,0), (0,-b)\} \cong \mathbb{Z}/3\mathbb{Z}.$$

If $|\mathbb{F}| \equiv 1 \bmod 3$*, then we have two possibilities for the factorization over* $\mathbb{F}$ *of the* 3*-division polynomial:*

(1) *if* Δ *is not a cube, then* $\Psi_3(x) = x\psi_3(x)$*;*
(2) *if* Δ *is a cube, then* $\Psi_3(x) = x(x - x_1)(x - x_2)(x - x_3)$*.*

In the first case $E(\mathbb{F})[3] = \{\mathcal{O}_E, (0,0), (0,-b)\} \cong \mathbb{Z}/3\mathbb{Z}$ *and in the second case*

$$\begin{aligned} E(\mathbb{F})[3] &= \{\mathcal{O}_E, (0,0), (0,-b), (x_i, b\omega + ax_i(\omega - 1)\,), (x_j, b\omega^2 + ax_j(\omega^2 - 1))\} \\ &= \{\mathcal{O}_E, (0,0), (0,-b), (x_j, -x_j^2 x_k/b) \textit{ with } j,k = 1,2,3 \textit{ and } j \neq k\} \\ &\cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}. \end{aligned}$$

From now on, let us denote $P_0 = (0,0)$ (rational 3-torsion point) and $P_1 = (x_1, -x_1^2 x_2/b)$. Then, $\{P_0, P_1\}$ is an $\mathbb{F}_3$-basis of $E[3]$.

Once we have determined the 3-torsion structure, we perform successive trisection steps until we reach the maximal 3-power torsion. Let us deal now with one of these trisection steps. That is, we assume that $Q = (\xi, \eta)$ is a point in $E(\mathbb{F})$ and we want to know if there exists $P = (x_P, y_P) \in E(\mathbb{F})$ such that $[3]P = Q$. This condition shows that x_P must be a root of the polynomial

$$\begin{aligned} f_{\xi,[3]}(x) &= x^9 - 9\xi x^8 - 18a(b + 3a\xi)x^7 - 3(9a^3 b + 8b^2 + 27a^4\xi + 18ab\xi)x^6 \\ &\quad -18b(3a^2 b + 9a^3\xi + b\xi)x^5 - 9ab^2(b + 15a\xi)x^4 + 3b^3(9a^3 + b - 18a\xi)x^3 \\ &\quad +9b^4(3a^2 - \xi)x^2 + 9ab^5 x + b^6. \end{aligned}$$

The roots of $f_{\xi,[3]}(x)$ are the x-coordinates of the points in the set $P + E[3] = \{P + \varepsilon P_0 + \delta P_1 :\ -1 \le \varepsilon, \delta \le 1\}$. Since P_0 is rational, the abscissas of the points $P,\ P + P_0$ and $P - P_0$ are defined over the same field extension of $\mathbb{F}$ and therefore the polynomial

$$(x - x_P)(x - x_{P+P_0})(x - x_{P-P_0}) = x^3 + \left(-\frac{b^2}{x_P^2} - \frac{3a\,b}{x_P} - x_P\right)x^2 + 3abx + b^2$$

divides $f_{\xi,[3]}(x)$ in $\mathbb{F}(x_P)$. Let us consider the polynomial

$$x^3 + Xx^2 + 3abx + b^2 \in \mathbb{F}(X)[x].$$

According to the values $S_0 = 1,\quad S_i = 0,\ i \ge 1,\quad w_0 = 3ab,\quad w_1 = b^2$, corresponding to the isogeny $\mathcal{I}_0$, with kernel $\langle P_0\rangle$, this polynomial is $f_{-X,\mathcal{I}_0}(x)$. Nevertheless, for the sake of notational simplicity, we change X by $-X$.

The trace value X has to be a rational root of the polynomial

$$f_{\xi,\hat{\mathcal{I}}_0}(X) = X^3 + 9\xi X^2 - 27a(2a\xi + b)X + 81a^4\xi + 27b(a^3 + b).$$

Therefore, in order to determine rational roots of the degree 9 polynomial $f_{\xi,[3]}(x)$, we can proceed in two cubic steps: compute rational roots of $f_{\xi,\hat{\mathcal{I}}_0}(X)$ and for each one of them compute rational roots of the corresponding $f_{X,\mathcal{I}_0}(x)$.

Since trisecting the point $P_0 = (0, 0)$ is equivalent to trisecting the opposite point $-P_0 = (0, -b)$, without loss of generality, we can assume that we start with $Q = (\xi, \eta)$ having $\eta \neq 0$. Then the roots of $f_{\xi,\hat{\mathcal{I}}_0}(X)$ in $\overline{\mathbb{F}}$ are

$$X_i = -3\left(\eta_i^2 - a\eta_i + \xi + \frac{a\xi}{\eta_i} + \frac{\xi^2}{\eta_i^2}\right),$$

where η_1, η_2, η_3 denote the three cubic roots of η in $\overline{\mathbb{F}}$.

Proposition 5.3. *If* $|\mathbb{F}| \equiv -1 \bmod 3$*, the polynomial* $f_{\xi,\hat{\mathcal{I}}_0}(X)$ *has a unique rational root, say* X_1*, and* $f_{\xi,[3]}(x) = f_{X_1,\mathcal{I}_0}(x)(f_{X_2,\mathcal{I}_0}(x)f_{X_3,\mathcal{I}_0}(x))$ *is a decomposition over* $\mathbb{F}$ *of type* $(\deg 3)(\deg 6)$*.*

If $|\mathbb{F}| \equiv 1 \bmod 3$*, either the polynomial* $f_{\xi,\hat{\mathcal{I}}_0}(X)$ *is irreducible (when* η *is not a cube) or splits completely. In the last case,* $f_{\xi,[3]}(x) = f_{X_1,\mathcal{I}_0}(x)f_{X_2,\mathcal{I}_0}(x)f_{X_3,\mathcal{I}_0}(x)$ *is a decomposition over* $\mathbb{F}$ *of type* $(\deg 3)(\deg 3)(\deg 3)$*.*

Now we are left with the factorization of polynomials $f_{X,\mathcal{I}_0}(x)$. We remark here that if $f_{X,\mathcal{I}_0}(x)$ splits completely and ξ'_1, ξ'_2, ξ'_3 denote its roots, then

$$(\xi'_j, -{\xi'_j}^2\xi'_k/b) \in E(\mathbb{F})$$

for $j \neq k$. Therefore, the roots of $f_{X,\mathcal{I}_0}(x)$ provide both coordinates of new rational points, which are necessary to keep descending in the trisection tree.

Let us see how to compute these roots ξ'_j. A necessary condition for the trisection of $Q = (\xi, \eta)$, with $\eta \neq 0$, is $\eta \in \mathbb{F}^{*\,3}$. Let $\eta_1 \in \mathbb{F}$ be a cubic root of η. Then $f_{\xi,\hat{\mathcal{I}}_0}(X)$ has a rational root X_1. The polynomial $f_{X_1,\mathcal{I}_0}(x)$ has a root in $\mathbb{F}$ if, and only if,

$$\mu = \frac{\eta_1 a - \omega\xi + \omega^2\eta_1^2}{\eta_1 a - \omega^2\xi + \omega\eta_1^2}$$

is a cube. This element has to be considered in $\mathbb{F}(\omega)$, which is either $\mathbb{F}$ or its quadratic extension. When this condition holds, if μ_1, μ_2, μ_3 are the cubic roots of μ in $\mathbb{F}(\omega)$, then the roots of $f_{X_1,\mathcal{I}_0}(x)$ are

$$\xi'_j = \frac{\nu\overline{\nu}}{\eta_1^2} + \lambda_j + \overline{\lambda}_j - a^2 \qquad j \in \{1, 2, 3\},$$

where

$$\nu = \eta_1 a - \omega\xi + \omega^2\eta_1^2, \qquad \lambda_j = \left(\frac{\xi}{\eta_1^2} - \omega\right)\mu_j\overline{\nu}$$

and ¯ denotes *conjugation* in $\mathbb{F}(\omega)$ (namely, replacement of ω by ω^2). We see that, if $f_{X_1,\mathcal{I}_0}(x)$ has a rational root, then it splits completely over $\mathbb{F}$.

When $f_{\xi,\hat{\mathcal{I}}_0}(X)$ splits completely, the corresponding formulae for X_2 and X_3 are obtained via the substitutions $\eta_1 \to \omega\eta_1$ and $\eta_1 \to \omega^2\eta_1$.

Algorithm: Trisection of points of the elliptic curve $E/\mathbb{F}:\ y^2+3axy+by=x^3$

```
INPUT: Point $Q=(\xi,\eta)\in E(\mathbb{F})$ with $\eta\neq 0$.
OUTPUT: Points $P\in E(\mathbb{F})$ such that $3P=\pm Q$.
    (1) If $\eta\notin\mathbb{F}^{*3}$, then return "$Q$ cannot be trisected"; else, compute cubic roots
        $\eta_i$ of $\eta$ in $\mathbb{F}^*$ (we can have $i\in\{1\}$ or $i\in\{1,2,3\}$).
    (2) Compute $\nu_i=\eta_i a-\omega\xi+\omega^2\eta_i^2$ and compute $\overline{\nu}_i$.
    (3) Compute $\mu_i=\nu_i/\overline{\nu}_i$. If $\mu_i\notin\mathbb{F}(\omega)^{*3}$ for all $i$, then return "$Q$ cannot be
        trisected"; else, compute three cubic roots $\mu_{ij}$ of $\mu_i$ in $\mathbb{F}(\omega)^*$.
    (4) Compute $\lambda_{ij}=(\xi\eta_i^{-2}-\omega)\mu_{ij}\overline{\nu_i}$ and compute $\overline{\lambda}_{ij}$.
    (5) Compute $\xi'_{ij}=(\nu_i\overline{\nu}_i)\eta_i^{-2}+(\lambda_{ij}+\overline{\lambda}_{ij})-a^2$.
    (6) Compute $\eta'_{ijk}=-{\xi'_{ij}}^2\xi'_{ik}/b$ for $k\neq j$.
    (7) Return the points $(\xi'_{ij},\eta'_{ijk})$ (either 6 or 18 points).
```

At this point we have shown that trisection of points in $E/\mathbb{F}$ reduces to computation of cubic roots in $\mathbb{F}^*$ and $\mathbb{F}(\omega)^*$. In a finite field with q elements, this computation can be done in $\mathrm{O}(\log^4 q)$ bit operations using a randomized algorithm (see [1, Theorem 7.3.2]). Assuming the *Extended Riemann Hypothesis*, a deterministic algorithm can be considered instead. In that case, the cost would be $\mathrm{O}(\log^5 q)$ (see [1, Theorem 7.8.2]).

Now, putting this all together it is easy to obtain a concrete statement of the procedure of successive trisection that we have described previously and that ends up describing completely the 3-Sylow subgroup of $E(\mathbb{F})$. Let us just remark that the above trisection algorithm has to be adapted to compute only one trisection point and not all of them. The cost of the whole algorithm is dominated by the repeated call (each time four calls at most) to this trisection algorithm, as many times as the height of the tree $\widetilde{\mathcal{T}}_3$, namely $\mathrm{O}(\log|\mathbb{F}|)$ times. Then, we finally get that with this algorithm the cost of computing group order and generators for the 3-Sylow subgroup of $E(\mathbb{F})$ is $\mathrm{O}((\log|\mathbb{F}|)^5)$. Again, assuming the *ERH* for the computation of cubic roots, the algorithm would be deterministic with cost $\mathrm{O}((\log|\mathbb{F}|)^6)$ bit operations.

6. Examples

The algorithm to compute the 3-Sylow subgroup of $E(\mathbb{F})$ presented in the above section has been implemented by J. Valera in `MAGMA`, [10], running over a Pentium IV 1.7 GHz. It has been used to test one million random elliptic curves

$$E/\mathbb{F}_p:\ y^2+3axy+by=x^3,$$

for a couple of 60-digit primes p. The average time of execution for a curve was 0.035 seconds when $p\equiv 1 \mod 3$ and 0.049 seconds when $p\equiv -1 \mod 3$. Some examples are shown in Table 2. They have been taken over a prime field $\mathbb{F}_p$ as well as over some of those extensions $\mathbb{F}_{p^k}$ where the size of the 3-Sylow subgroup increases. In the case $p\equiv 1 \mod 3$, the 3-Sylow subgroup grows only for extensions of degree divisible by 3 while for $p\equiv -1 \mod 3$ the 3-Sylow subgroup changes when considering extensions of degree divisible by 2 or 3. We provide also two examples of *big* 3-Sylow subgroups corresponding to a 100-digit prime p in Table 3.

Table 2. Structure of the 3-Sylow subgroup of curves over $\mathbb{F}_{p^k}$

	$\mathbf{p = 10^{60} + 13797}$			$\mathbf{p = 10^{60} + 13813}$		
a			1			2
b			114			4
k	1	3	9	1	2	3
(n_3, r_3)	(2,0)	(3,1)	(4,2)	(2,0)	(2,2)	(3,0)
time	0.02 sec	0.51 sec	1.66 sec	0.19 sec	0.90 sec	4.52 sec
a			53351884			2
b			5838033			3
k	1	3	9	1	2	3
(n_3, r_3)	(6,3)	(7,4)	(8,5)	(4,0)	(4,2)	(5,0)
time	0.21 sec	7.73 sec	167.48 sec	0.24 sec	1.23 sec	5.14 sec
a			82712312			99316564
b			45000893			36282433
k	1	3	9	1	2	3
(n_3, r_3)	(10,0)	(11,1)	(12,2)	(8,0)	(8,2)	(9,0)
time	0.14 sec	4.68 sec	162.60 sec	0.53 sec	2.23 sec	8.79 sec

Table 3. Structure of the 3-Sylow subgroup of curves over $\mathbb{F}_{10^{100}+267}$

	$\mathbf{p = 10^{100} + 267}$
a	76421267519872312497485277156867183786032284809439934 7\ 60791174480178130650934297942329858845005136 6
b	66041678618908011662232487897410795223626270478421613 4\ 08735028991776404414991621057707153719378046 14
(n_3, r_3)	(11,0)
time	0.48 sec
a	22887982063070410113159815109782303503102333850867955 6\ 49248348255150389866870549515617964341168050 78
b	27306879337764451605882350478137388784195052838836724 7\ 66701971453311964672083129592142578289247992 53
(n_3, r_3)	(10,1)
time	0.85 sec

Table 4. Distribution of the curves over $\mathbb{F}_{4483}$ according to their 3-Sylow subgroup

$n_3 + r_3$	(n_3, r_3)	Elliptic Curves	Isomorphism classes
1	(1,0)	8998362	2009
2	(2,0)	2985012	666
	(1,1)	4517856	252
3	(3,0)	887436	198
	(2,1)	1183248	66
4	(4,0)	430272	96
	(3,1)	573696	32
	(2,2)	233064	13
5	(5,0)	13446	3
	(4,1)	17928	1
	(3,2)	5976	1
7	(7,0)	80676	18
	(6,1)	107568	6
	(5,2)	35856	2
	(4,3)	17928	1

In order to compare performances, the group order of the first of the curves in Table 3 has been computed using `MAGMA`, which implements the SEA algorithm. The time to obtain

$$|E(\mathbb{F}_p)| = 3^{11} \cdot 5 \cdot 19 \cdot 5413097 \cdot q$$

where q is the prime 109773315961887140276574601976831947116686249194668952068232967554646936221117475309929, was 205.83 seconds. Taking $p = 10^{180} + 711$ and coefficients $a = 10^{100} + 2$ and $b = 10^{100} + 4$ for $E/\mathbb{F}_p$, the 3-Sylow subgroup $\mathbb{Z}/3^5\mathbb{Z}$ was computed in 0.51 seconds with our algorithm, while the computation of the group order, without factoring, took 5346.86 seconds in a first execution and 5244.24 seconds in another one.

Our algorithm has also been used to study the distribution of the curves $y^2 + 3axy + by = x^3$ over a prime field $\mathbb{F}_p$. In particular, the results obtained for the prime $p = 4483$ are summarized in Table 4. They are classified according to their 3-Sylow subgroup $\mathbb{Z}/3^{n_3}\mathbb{Z} \times \mathbb{Z}/3^{r_3}\mathbb{Z}$. Notice that, since there is no integer in Hasse's interval divisible by 3^6, the value $n_3 + r_3 = 6$ is not possible. The amount of curves for each pair (n_3, r_3) is given in the third column, while the corresponding isomorphism classes are counted in the last one.

The amount of isomorphism classes has been computed taking into account that elliptic curve isomorphisms

$$\begin{cases} x = u^2x' + v, \\ y = u^3y' + su^2x' + t \end{cases}$$

preserve the form $y^2+3axy+by = x^3$ of the equation when (v, t) are the coordinates of a rational 3-torsion point and s is the slope of the tangent line to the curve at

Table 5. Distribution of the curves over $\mathbb{F}_{4483}$ for some structures of the 2-Sylow and 3-Sylow subgroups

$n_3 + r_3$	(n_3, r_3)	(n_2, r_2)	Elliptic Curves	Isom. classes
2	(2,0)	(0,0)	1048788	234
		(1,0)	717120	160
		(2,0)	457164	102
		(1,1)	215136	48
		(3,0)	116532	26
		(2,1)	116532	26
		(4,0)	125496	28
		(3,1)	125496	28
		(9,0)	62748	14
		(8,1)	62748	14
	(1,1)	(0,0)	1505952	84
		(1,0)	1111536	62
		(2,0)	699192	39
		(1,1)	233064	13
		(3,0)	233064	13
		(2,1)	233064	13
		(4,0)	125496	7
		(3,1)	125496	7
		(9,0)	125496	7
		(8,1)	125496	7
7	(7,0)	(1,0)	80676	18
	(6,1)	(1,0)	107568	6
	(5,2)	(1,0)	35856	2
	(4,3)	(1,0)	17928	1

this point. In particular, the curve obtained while translating the origin to the 3-torsion point $(0, -b)$ is $y^2 - 3axy - by = x^3$.

If the curve $y^2 + 3axy + by = x^3$ has a cyclic 3-Sylow subgroup, its isomorphic curves have equation $y^2 + 3\gamma axy + \gamma^3 by = x^3$, with $\gamma \in \mathbb{F}_p^*$. Therefore, there are $p - 1$ curves in each isomorphism class, except when $a = 0$ and $p \equiv 1 \pmod 3$, in which case we have only $(p - 1)/3$ curves.

If the curve $y^2 + 3axy + by = x^3$ has a non-cyclic 3-Sylow subgroup, we have to add to its isomorphism class those curves obtained by translation of the origin to one of the other points of order 3. It turns out that an isomorphism class contains $4(p-1)$ curves, except when $a = 0$ or $b = 9a^3/8$, in which case it contains $4(p-1)/3$ curves. Notice that, since the elliptic curve $E : y^2 + 3axy + by = x^3$ has j-invariant

$$j_E = \frac{27\, a^3 \left(9\, a^3 - 8\, b\right)^3}{\left(a^3 - b\right)\, b^3},$$

the special cases correspond to $j_E = 0$.

It should also be noted that there are relations between the amounts listed in the last column, since they can be read in the context of the volcano structure of the 3-isogenies [5]. When $n_3 > 2$, the number of isomorphism classes having $(n_3, 0)$ is three times the number of isomorphism classes corresponding to $(n_3 - 1, 1)$. This responds to the fact that the curves with cyclic 3-Sylow subgroup are placed at the base of the volcano, whereas the ones with $(n_3 - 1, 1)$ are at the first level.

To finish with the examples, we combine the algorithm described here with the algorithm to compute the 2-Sylow subgroup given in [12]. We take the cases $n_3 + r_3 = 2$ and $n_3 + r_3 = 7$ of Table 4 and detail in Table 5 the distribution according to their 2-power torsion subgroup $\mathbb{Z}/2^{n_2}\mathbb{Z} \times \mathbb{Z}/2^{r_2}\mathbb{Z}$.

Looking at Hasse's interval $[4351, 4617]$ one realizes that all the curves having $n_3 + r_3 = 7$ and $(n_2, r_2) = (1, 0)$ have $|E(\mathbb{F}_p)|$ are not only divisible but equal to $2 \cdot 3^7$; and the same occurs when $n_3 + r_3 = 2$ and $n_2 + r_2 = 9$: all the curves in these cases have group order exactly $2^9 \cdot 3^2$.

References

[1] E. Bach and J. Shallit, *Algorithmic Number Theory. Vol. 1: Efficient Algorithms*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1996. MR1406794 (97e:11157)

[2] I. Blake, G. Seroussi and N. Smart, *Elliptic curves in cryptography*, London Math. Soc. Lecture Note Series, no. 265, Cambridge Unuversity Press, 1999. MR1771549 (2001i:94048)

[3] A. Bostan, B. Salvy, F. Morain and E. Schost, *Fast algorithms for computing isogenies between elliptic curves*, Math. Comp. 77 (2008), 1755–1778. MR2398793

[4] L. Dewaghe, *Isogénie entre courbes elliptiques*, Utilitas Mathematica (1999), no. 55, 123–127. MR1685678 (2000b:14034)

[5] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, in ANTS-V, C. Fieker and D.R. Kohel, eds., Lecture Notes in Computer Science, Vol. 2369, Springer-Verlag, Berlin-Heidelberg-New York, 2002, pp. 276–291. MR2041091 (2005c:11077)

[6] H. Gunji, *The Hasse invariant and p-division points of an elliptic curve*, Arch. Math., 27 (1976), pp. 148–158. MR0412198 (54:325)

[7] D. Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, Vol. 111, Springer-Verlag, Berlin-Heidelberg-New York, 1987. MR868861 (88h:11039)

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

[9] LiDIA-Group, LiDIA *Manual: A library for computational number theory*, Tech. Univ. Darmstadt, 2001. Available from `ftp.informatik.tu-darmstadt.de/pub/TI/systems/LiDIA`.

[10] Magma Group, *Handbook of Magma functions*, J. Canon and W. Bosma, eds. Available from `http://magma.maths.usyd.edu.au/`.

[11] J. Miret, R. Moreno, and A. Rio, *Generalization of Vélu's formulae for isogenies*, Proceedings of the Primeras Jornadas de Teoría de Números (Vilanova i la Geltrú, 2005) Publ. Mat. (2007), Vol. Extra, pp. 147–163.

[12] J. Miret, R. Moreno, A. Rio, and M. Valls, *Determining the* 2*-Sylow subgroup of an elliptic curve over a finite field*, Math. Comp., 74 (2005), pp. 411–427. MR2085900 (2005d:11090)

[13] F. Morain, *Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques*, Journal de Théorie des Nombres de Bordeaux (1995), no. 7, 255–282. MR1413579 (97i:11069)

[14] E. Nart, Personal communication, May 2005.

[15] H. G. Rück, *A note on elliptic curves over finite fields*, Math. Comp., 49 (1987), pp. 301–304. MR890272 (88d:11058)

[16] D. Sadornil, *A note on factorisation of division polynomials* Arxiv preprint arXiv:math/0606684v1 [math.NT], 2006.

[17] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A, 46 (1987), pp. 183–211. MR914657 (88k:14013)

[18] J. P. Serre, *Trees*, Springer Monographs in Mathematics, Springer-Verlag, Berlin-Heidelberg-New York, 2003. MR1954121 (2003m:20032)

[19] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, Berlin-Heidelberg-New York, 1986. MR817210 (87g:11070)

[20] H. Verdure, *Factorization patterns of division polynomials*, Proc. Japan Acad. Ser. A Math. Sci., Vol. 80 (2004), pp. 79–82. Correction in [16]. MR2062806 (2005b:11085)

[21] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Math. Acad. Sci. Paris, Série A, vol. 273 (1971), pp. 238–241. MR0294345 (45:3414)

[22] J. Voloch, *A note on elliptic curves over finite fields*, Bull. Soc. Math. France, 116 (1988), pp. 455–458. MR1005390 (90f:14012)

Department de Matemàtica, Universitat de Lleida, Jaume II 69, 25001-Lleida, Spain
E-mail address: miret@eps.udl.es

Department de Matemàtica, Universitat de Lleida, Jaume II 69, 25001-Lleida, Spain
E-mail address: ramiro@eps.udl.es

Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, Jordi Girona 1-3. 08034-Barcelona, Spain
E-mail address: ana.rio@upc.edu

Department de Matemàtica, Universitat de Lleida, Jaume II 69, 25001-Lleida, Spain
E-mail address: magda@eps.udl.es