MATHEMATICS OF COMPUTATION
Volume 74, Number 249, Pages 411–427
S 0025-5718(04)01640-0
Article electronically published on March 4, 2004

DETERMINING THE 2-SYLOW SUBGROUP OF AN ELLIPTIC CURVE OVER A FINITE FIELD

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

ABSTRACT. In this paper we describe an algorithm that outputs the order and the structure, including generators, of the 2-Sylow subgroup of an elliptic curve over a finite field. To do this, we do not assume any knowledge of the group order. The results that lead to the design of this algorithm are of inductive type. Then a right choice of points allows us to reach the end within a linear number of successive halvings. The algorithm works with abscissas, so that halving of rational points in the elliptic curve becomes computing of square roots in the finite field. Efficient methods for this computation determine the efficiency of our algorithm.

1. INTRODUCTION

The goal of this paper is the determination of the order and structure of the 2-Sylow subgroup of an elliptic curve over a finite field $\mathbb{F}_q$, avoiding the previous computation of the group order. We assume that the characteristic of $\mathbb{F}_q$ is greater than 2. For some related results in characteristic 2 one can see [6].

A priori we know that for any elliptic curve $E/\mathbb{F}_q$ and any m prime to the characteristic of $\mathbb{F}_q$, the m-torsion group $E[m](\overline{\mathbb{F}}_q)$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$. Therefore, the subgroup under consideration has rank at most 2 and our problem consists in the determination of integers $n \geq r \geq 0$ such that the 2-Sylow subgroup of $E(\mathbb{F}_q)$ is

$$S_2(E(\mathbb{F}_q)) = E[2^n](\mathbb{F}_q) \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}\,.$$

We are dealing with a rationality question and, from now on, even if it is not explicitly mentioned, each time we refer to a point of the elliptic curve we implicitly mean a rational point.

Some results concerning the whole group structure of $E(\mathbb{F}_q)$ provide some extra pieces of information. For nonsupersingular elliptic curves, from the description in [10] and [13] it follows that $r \leq v_2(q-1)$, where v_2 denotes the 2-adic valuation. For supersingular elliptic curves, Schoof ([11]) shows that the group $E(\mathbb{F}_q)$ is cyclic or isomorphic to $\mathbb{Z}/_{(\sqrt{q}-1)}\mathbb{Z}\times\mathbb{Z}/_{(\sqrt{q}-1)}\mathbb{Z}$, $\mathbb{Z}/_{(\sqrt{q}+1)}\mathbb{Z}\times\mathbb{Z}/_{(\sqrt{q}+1)}\mathbb{Z}$ or $\mathbb{Z}/\frac{q+1}{2}\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, the last structure being possible only when $q \equiv 3 \pmod 4$. Therefore, supersingular curves have cyclic 2-Sylow subgroup except when q is an even power of the characteristic or when $q \equiv 3 \pmod 4$. In the first case we can have

Received by the editor March 5, 2003 and, in revised form, May 3, 2003.
2000 *Mathematics Subject Classification.* Primary 11G20.
The first, second and fourth authors were supported in part by grant BFM2000-1113-C02-02.
The third author was supported in part by grant BFM2000-0794-C02-02.

$n = r = v_2(\sqrt{q}-1)$ or $v_2(\sqrt{q}+1)$ and in the second case we can have $n = v_2(q+1)-1$ and $r = 1$.

In order to carry out the inductive process which leads to the determination of $S_2(E(\mathbb{F}_q))$, from the very beginning we will distinguish between those curves with either one or three rational points of order two. Namely, between the cyclic and noncyclic case.

In general, we provide conditions to decide whether, given the abscissa of a rational point of order 2^k, there exist rational points of order 2^{k+1}. Such conditions follow from the study of the solvability of a quartic equation over the finite field.

Combining these results with an appropriate choice of points, we can give an algorithm that for each elliptic curve, $E/\mathbb{F}_q$ returns, in $\mathrm{O}(\log q)$ steps, the complete information about its 2-Sylow subgroup. Namely, it returns

- n, the maximum value for which E has $\mathbb{F}_q$-rational points of order 2^n,
- r such that $S_2(E(\mathbb{F}_q)) \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$,
- two points in $E(\mathbb{F}_q)$, of orders 2^n and 2^r, generating $S_2(E(\mathbb{F}_q))$.

For general results or common terminology on elliptic curves used in this paper, we refer to [12] or [5].

2. First step: 2-torsion points

If an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic $p > 2$ is given by an equation $y^2 = x^3 + ax^2 + bx + c$, the rational points of order 2 are determined by the roots of the cubic polynomial $x^3 + ax^2 + bx + c$ in the field. Therefore, to decide whether or not such a rational point exists, we can compute the $\gcd(x^3 + ax^2 + bx + c, x^q - x)$. When it is not 1, with this computation, we can also decide, according to the degree of the result, if there are one or three rational points of order 2; namely if the structure of $E[2](\mathbb{F}_q)$ is $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In the first case, since the computation of the gcd provides a factor $x - \xi$ of the cubic polynomial, we also determine the rational point $P = (\xi, 0)$ of order 2. In the noncyclic case, the explicit determination of such a point requires the computation of a root of the cubic polynomial. Once we have done this, we can take the point of order 2 to the origin and work with a model

$$y^2 = x(x^2 + \alpha x + \beta)$$

of the elliptic curve.

Then, the quadratic character of the discriminant $\rho = \alpha^2 - 4\beta$ distinguishes the two possible cases we have mentioned. If χ denotes the unique nontrivial quadratic character in $\mathbb{F}_q^*$, then

- $\chi(\rho) = -1$ corresponds to $(0,0)$ being the unique point of order 2 and $E[2](\mathbb{F}_q) \cong \mathbb{Z}/2\mathbb{Z}$; therefore, $S_2(E(\mathbb{F}_q))$ is cyclic.
- $\chi(\rho) = 1$ corresponds to the case of three rational points of order 2:

$$(0,0), \quad \left(-\frac{\alpha+\sqrt{\rho}}{2}, 0\right), \quad \text{and} \quad \left(-\frac{\alpha-\sqrt{\rho}}{2}, 0\right). \tag{1}$$

It follows that $E[2](\mathbb{F}_q) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $S_2(E(\mathbb{F}_q))$ have rank 2.

If we want to establish a parametric setting, we can approach the subject using modular curves. The modular curve $X_1(N)$ parametrizes isomorphism classes of pairs (E, P), where E is an elliptic curve and P is a point of E of exact order N. The modular curve $X_0(N)$ parametrizes isomorphism classes of pairs (E, C),

where E is an elliptic curve and C is a cyclic subgroup of E of order N. Let us observe that for $N = 2$ both modular curves coincide and recall that the field of definition of a point of a modular curve indicates that there is a representative of the corresponding isomorphism class which is defined over this field. The forgetful morphism from a modular curve to the projective line maps each point to the j-invariant of *the* corresponding elliptic curve.

Since the genus of the modular curves increases, we do not expect to solve the problem in this way, but we consider it as an alternative for the input data of the algorithm.

The modular curve $X_0(2)$ has genus zero and a model $uv = 2^{12}$ with forgetful morphism

$$(u, v) \mapsto \frac{(u + 16)^3}{u}$$

(cf. [8]). If $uv = 2^{12}$, then $j_u = (u + 16)^3/u$, and $j_v = (v + 16)^3/v$ are j-invariants of elliptic curves linked by an isogeny of degree 2. Namely, $\Phi_2(j_u, j_v) = 0$, where Φ_2 denotes the modular polynomial.

- If $\chi(u(u + 64)) = -1$, then $(u, 2^{12}/u)$ is the unique pre-image of j_u under the forgetful morphism. That means that *the* elliptic curve having this j-invariant has a unique rational point of order 2.
- If $\chi(u(u + 64)) = 1$, then j_u has three pre-images under the forgetful morphism. This corresponds to an elliptic curve having three rational points of order 2.

Note that for a given elliptic curve $E/\mathbb{F}_q$, if we compute the j-invariant j_E, deciding if there is a rational point of order 2 amounts to deciding if the equation

$$(x + 16)^3 - j_E\, x = 0$$

has a rational solution and therefore to the computation of a gcd. Again, in the cyclic case this computation provides an explicit solution, and in the noncyclic case we should solve a cubic equation in the finite field.

The parametric family of j-invariants

$$j_u = \frac{(u + 16)^3}{u} \quad (u \neq -64, -16, 0, 8)$$

corresponds to the family of elliptic curves with j-invariant $\neq 0, 1728$ having a rational point of order 2. For such a curve, we can take the model

$$y^2 = x^3 + \frac{x^2}{4} - \frac{36}{j - 1728}x - \frac{1}{j - 1728}$$

with discriminant $\Delta = j^2/4(j - 1728)^3$, or its twist by a nonquadratic residue. Then, we deal with the family of elliptic curves

$$c\, y^2 = x^3 + \frac{x^2}{4} - \frac{36u}{(u + 64)(u - 8)^2}x - \frac{u}{(u + 64)(u - 8)^2}\,, \tag{2}$$

with $c \in \mathbb{F}_q^*/\mathbb{F}_q^{*\,2}$.

The zeroes of the cubic polynomial determine the points of order 2, and we have:

- if $\chi(u(u + 64)) = -1$, the unique rational point of order 2 is

$$\left(\frac{2}{u - 8}, 0\right);$$

- if $\chi(u(u+64))=1$, there are three rational points of order 2

$$\left(\frac{2}{u-8},0\right),\quad \left(-\frac{r+(u+16)\sqrt{r}}{8(u-8)(u+64)},0\right),\quad \text{and}\ \left(-\frac{r-(u+16)\sqrt{r}}{8(u-8)(u+64)},0\right),$$

  where $r=u(u+64)$.

As before, we end up with an explicit point of order 2 that we can translate to the origin in order to work with a model $y^2=x(x^2+\alpha x+\beta)$.

3. Successive halving

On one hand, assuming the existence of a rational point of order 2^k, we look for conditions granting the existence of a rational point of order 2^{k+1}. On the other hand, we want to reach points of maximal 2-power order performing as few successive halvings as possible.

The basis for the first step of these inductive processes has been set above. According to the arguments given there, we can work with a model

$$y^2=x(x^2+\alpha x+\beta)$$

of the elliptic curve E over $\mathbb{F}_q$. From now on we will denote

$$\rho=\alpha^2-4\beta.$$

Recall that the quadratic character of this discriminant determines the structure of the 2-torsion subgroup $E[2](\mathbb{F}_q)$.

Assume that a given curve E has points of order 2^k, with $k\geq 1$. Obviously, this curve would have a point of order 2^{k+1} if and only if some point $Q=(\xi,\zeta)$ of order 2^k is in the image of multiplication by 2. If $Q=2P$, we say that Q has a *half* point P. If we denote $P=(x,y)$, such a condition is equivalent to

$$\xi = x(2P)=\frac{(x^2-\beta)^2}{4y^2}, \tag{3}$$

$$y^2 = x(x^2+\alpha x+\beta). \tag{4}$$

Obviously, one gets the following:

Lemma 1. *Let $E/\mathbb{F}_q:\ y^2=x(x^2+\alpha x+\beta)$ and $Q=(\xi,\zeta)\in E(\mathbb{F}_q)\setminus\{\mathcal{O}\}$. A necessary condition for the existence of a half point of Q is that ξ is a square in $\mathbb{F}_q$. Furthermore, since $\zeta^2=\xi\delta_\xi$, with $\delta_\xi=\xi^2+\alpha\,\xi+\beta$, it follows that δ_ξ should also be a square in $\mathbb{F}_q$.*

On the other hand, from equations (3) and (4), we get the quartic equation over $\mathbb{F}_q$

$$x^4-4\,\xi\,x^3-2\,(2\,\alpha\,\xi+\beta)\,x^2-4\,\beta\,\xi\,x+\beta^2=0. \tag{5}$$

Its solvability can be deduced from the following considerations:

- The quartic polynomial in (5), which will be denoted by f_ξ, can be transformed into a palindromic polynomial. Therefore, it factorizes $f_\xi=f_{1,\xi}\,f_{2,\xi}$, where

$$\begin{aligned} f_{1,\xi}(x) &= x^2-2\,(\xi-\sqrt{\delta_\xi}\,)\,x+\beta,\\ f_{2,\xi}(x) &= x^2-2\,(\xi+\sqrt{\delta_\xi}\,)\,x+\beta. \end{aligned}$$

- The discriminants of f_ξ and its factors $f_{i,\xi}$ are

$$\begin{aligned} D_\xi &= \operatorname{disc}(f_\xi) = 2^{12}\,\beta^2\,\xi^2\,\delta^2\,\rho, \\ \operatorname{disc}(f_{i,\xi}) &= 4\xi\left(\alpha + 2\xi + (-1)^i\,2\sqrt{\delta}\right), \text{ for } i = 1, 2. \end{aligned}$$

  Notice that

$$\operatorname{disc}(f_{1,\xi})\operatorname{disc}(f_{2,\xi}) = 2^4\,\xi^2\,\rho.$$

According to this, in the halving process we distinguish the following cases:

- If $D_\xi = 0$, the equation (5) has two double roots. We will be in this situation when $\xi = 0$ or $\delta_\xi = 0$ (only possible if $\chi(\rho) = 1$). This means that the point we are trying to halve is a point of order 2.
- If $\xi \neq 0$ and $\chi(\rho) = -1$, then only one of the polynomials $f_{i,\xi}$ factorizes into two (different) linear factors.
- If $\xi \neq 0$ and $\chi(\rho) = 1$, then either both quadratic polynomials $f_{i,\xi}$ factorize into two (different) linear factors or none of them does.

3.1. **The cyclic case.** In this section we make more specific the inductive process over k mentioned above, for the curves $E/\mathbb{F}_q:\ y^2 = x(x^2+\alpha x+\beta)$, whose 2-Sylow subgroup is cyclic:

$$S_2(E(\mathbb{F}_q)) = E[2^n](\mathbb{F}_q) \cong \mathbb{Z}/2^n\mathbb{Z}\,,$$

namely those with $\chi(\rho) = -1$.

In this situation, to check the existence of points of order 2^{k+1}, we can take any point of order 2^k and check the existence of a half point. In case of an affirmative answer, in order to go on in this way it is enough to compute one of the points of order 2^{k+1} (see Figure 1). Such a process actually begins with a characterization of the existence of points of order 4.

Lemma 2. *A curve $E/\mathbb{F}_q:\ y^2 = x(x^2+\alpha x+\beta)$ with $\chi(\rho) = -1$ has a point of order 4 if and only if $\chi(\beta) = 1$.*

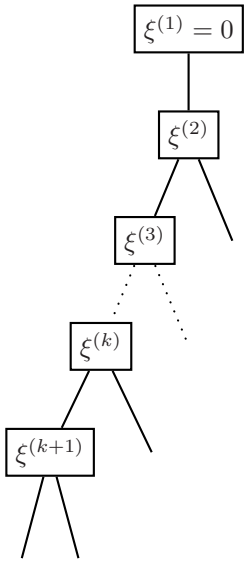


FIGURE 1. Tree of abscissas in the cyclic case

Proof. In this case, $Q = (0, 0)$ is the unique rational point of order two. If a point of order 4 exists, it should be a half of Q. Therefore, the corresponding quartic equation (5) has a solution. This equation is now $(x^2 - \beta)^2 = 0$ and therefore β should be a square in $\mathbb{F}_q^*$.

On the other way round, if $\chi(\beta) = 1$, then one of $x = \pm\sqrt{\beta}$ is a solution of (5) and corresponds to the abscissa of a point in $E(\mathbb{F}_q)$. Indeed, for these values of x, the computation of $x(x^2 + \alpha x + \beta)$ gives $y_1 = \beta(\alpha + 2\sqrt{\beta}\,)$ and $y_2 = \beta(\alpha - 2\sqrt{\beta}\,)$. Since $y_1 y_2 = \beta^2\rho$, one of them will be a square in $\mathbb{F}_q^*$ and the claim follows. □

Remark 1. If $\chi(\rho) = -1$ and $\chi(\beta) = 1$, the points of order 4 are one of the following pairs:

$$\left(\sqrt{\beta}, \pm\sqrt{\beta(\alpha + 2\sqrt{\beta})}\right) \text{ or } \left(-\sqrt{\beta}, \pm\sqrt{\beta(\alpha - 2\sqrt{\beta})}\right).$$

The inductive step in this cyclic case is completed with the following result, which characterizes the existence of points of order 2^{k+1}.

Proposition 1. *Let $E/\mathbb{F}_q :\ y^2 = x(x^2 + \alpha x + \beta)$ with $\chi(\rho) = -1$. Let us assume that $Q = (\xi, \zeta)$ is a point of $E(\mathbb{F}_q)$ of order 2^k with $k > 1$. Then there exists a half point of Q if and only if $\chi(\xi) = 1$.*

Proof. The necessity has already been established in Lemma 1. Let us see the sufficiency. We are in the case $\xi \neq 0$, since we are considering $k \geq 2$, and $\chi(\rho) = -1$. Therefore, one of the polynomials $f_{i,\xi}$ breaks into linear factors. Its roots are the possible abscissas of the half point. If x denotes one of them, we have to see that it really corresponds to the abscissa of a point on $E(\mathbb{F}_q)$, namely that $x(x^2 + \alpha x + \beta)$ is a square in $\mathbb{F}_q^*$.

Assuming that the polynomial that factorizes is $f_{1,\xi}$, then we have $x^2 = 2(\xi - \sqrt{\delta_\xi}\,)\, x - \beta$ and, consequently,

$$x(x^2 + \alpha x + \beta) = x^2(\alpha + 2\xi - 2\sqrt{\delta_\xi}\,) = \frac{x^2 \operatorname{disc}(f_{1,\xi})}{4\xi}$$

is a square in $\mathbb{F}_q^*$. □

Remark 2. In the proof of Proposition 1 it is shown how to compute explicitly the abscissa of a point of order 2^{k+1} in the case $\chi(\rho) = -1$ and $\chi(\xi) = 1$.

To summarize, due to the group structure, the cyclic case is treated considering, in each step, the abscissa $\xi^{(k)}$ of a point of order 2^k and checking whether it is a square. If it is so, then $\xi^{(k+1)}$ is computed from one of the quadratic polynomials $f_{i,\xi^{(k)}}$, and the same process is repeated. The initial conditions are established from the coefficients of the curve and Lemma 2.

3.2. **The noncyclic case.** Now we consider curves $E/\mathbb{F}_q :\ y^2 = x(x^2 + \alpha x + \beta)$, whose 2-Sylow subgroup is not cyclic:

$$S_2(E(\mathbb{F}_q)) = E[2^n](\mathbb{F}_q) \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z} \quad (n \geq r \geq 1)\,,$$

namely those with $\chi(\rho) = 1$.

Now, the subgroup of 2-torsion points is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the subgroup of 4-torsion is

$$\begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{if none of the points of order 2 has a half point;} \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & \text{if only one of the points of order 2 has a half point;} \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, & \text{if the three points of order 2 have a half point.} \end{cases}$$

Let us begin with the computational characterization of these cases.

Lemma 3. *Let $E/\mathbb{F}_q:\ y^2 = x(x^2+\alpha x+\beta)$ with $\chi(\rho)=1$ and $(0,0)$, $(\xi_1,0)$, $(\xi_2,0)$ its rational points of order 2. Then, E has rational points of order 4 if and only if one of the following conditions holds:*

(1) $\chi(\beta)=1$ *and* $\chi(\alpha-2\sqrt{\beta}\,)=1$;
(2) $\chi(\xi_1)=\chi(2\xi_1+\alpha)=1$;
(3) $\chi(\xi_2)=\chi(2\xi_2+\alpha)=1$.

If only one of them holds, then $E[4](\mathbb{F}_q)\cong\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. If two of them hold, then the third one does also and $E[4](\mathbb{F}_q)\cong\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

According to these conditions, the abscissas of the points of order 4 are:

(1) *The roots of $X^2-\beta$;*
(2) *The roots of $X^2-2\xi_1 X+\beta$;*
(3) *The roots of $X^2-2\xi_2 X+\beta$.*

Proof. If we consider the point $(0,0)$, the argument goes as in Lemma 2, but now both values $\beta(\alpha+2\sqrt{\beta}\,)$ and $\beta(\alpha-2\sqrt{\beta}\,)$ could be nonsquares.

If we consider a point $(\xi,0)$, then the polynomials $f_{i,\xi}$ of the halving process are both $X^2-2\xi X+\beta$, having discriminant $4\xi^2-4\beta=4\xi(2\xi+\alpha)$. If it is a square and x is one of the roots of the polynomial, then

$$x(x^2+\alpha x+\beta)=x(2\xi x+\alpha x)=x^2(2\xi+\alpha).$$

Finally, since $(\xi_1,0)+(\xi_2,0)=(0,0)$, if two of these points can be halved, then the third one can also. □

Remark 3. Since $\xi_1+\xi_2=-\alpha$, the second and third conditions in Lemma 3 can be restated as

$$\chi(\xi_1)=\chi(\xi_1-\xi_2)=1\quad\text{and}\quad\chi(\xi_2)=\chi(\xi_2-\xi_1)=1\,,$$

respectively.

Remark 4. Since

$$(2\xi_1+\alpha)(2\xi_2+\alpha)=-\rho=-(\xi_1-\xi_2)^2,$$

if all the conditions in Lemma 3 hold, we must have $-1\in\mathbb{F}_q^{*\,2}$. Therefore,

$$q\equiv 3\pmod 4\Rightarrow E[4](\mathbb{F}_q)\ncong\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}\,.$$

As we already mentioned in the introduction, $q\equiv 3\pmod 4\Rightarrow r=1$ in the noncyclic case.

As before, in order to continue the halving process, first we need the characterization of the image of multiplication by 2.

Proposition 2. *Let $E/\mathbb{F}_q:\ y^2=x(x^2+\alpha x+\beta)$ with $\chi(\rho)=1$. Let us assume that $Q=(\xi,\zeta)$ is a point of $E(\mathbb{F}_q)$ of order 2^k, with $k>1$. Then, there exists a half point of Q if and only if*

$$\chi(\xi)=1\quad\text{and}\quad\chi\left(2\xi+\alpha+2\sqrt{\delta_\xi}\right)=1\,,\tag{6}$$

where $\delta_\xi=\xi^2+\alpha\xi+\beta$.

Proof. We argue as in the proof of Proposition 1. The condition corresponds now to the factorization of (both) $f_{i,\xi}$ into two (different) linear factors giving abscissas of points of $E(\mathbb{F}_q)$. If x is a root of $f_{i,\xi}$, then

$$x(x^2+\alpha x+\beta) = x^2\left(2\xi+\alpha+(-1)^i\,2\sqrt{\delta_\xi}\right) = \frac{x^2\,\mathrm{disc}(f_{i,\xi})}{4\xi}. \qquad \square$$

Remark 5. If we write $x(x^2+\alpha x+\beta) = x(x-\xi_1)(x-\xi_2)$, then

$$\mathrm{disc}(f_{i,\xi}) = 4\,\xi\left((\xi-\xi_1)+(\xi-\xi_2)+(-1)^i\,2\sqrt{(\xi-\xi_1)(\xi-\xi_2)}\right).$$

The condition in Proposition 2 is equivalent to

$$\xi,\ (\xi-\xi_1),\ \text{ and } (\xi-\xi_2)\ \text{ are squares,}$$

which is the condition stated in Theorem 1(4.1) of [5].

Remark 6. Let us assume that the condition in Proposition 2 holds. If a root x of $f_{i,\xi}$ is the abscissa of a point $P\in E(\mathbb{F}_q)$, then the other root of $f_{i,\xi}$, namely β/x, is the abscissa of $P+(0,0)$.

If a root x of one of the polynomials $f_{i,\xi}$ is the abscissa of $P\in E(\mathbb{F}_q)$, then the abscissa of $P+(\xi_1,0)$, namely $\xi_1(x-\xi_2)/(x-\xi_1)$, is a root of the other polynomial.

Up to now, we have well-established initial conditions, an effective way to check if a point can be halved and an effective method to compute a half point when it exists. In order to prove that this can be used in an efficient algorithm, it remains to show that we do not need too many checkings/computations to move down the layers of points of 2-power order until we reach the deepest.

Let us denote by

$$Q_0=(0,0),\quad Q_1=(\xi_1,0),\quad \text{and } Q_2=(\xi_2,0)$$

the points of order 2, and

$$\mathcal{T}_j=\{P\in E(\mathbb{F}_q)\mid \exists\ \ell\geq 0 \text{ such that } 2^\ell P=Q_j\}$$

for $j\in\{0,1,2\}$. Each $\mathcal{T}_j$ is a tree with root in Q_j, and the maximum n such that E has $\mathbb{F}_q$-rational points of order 2^n is

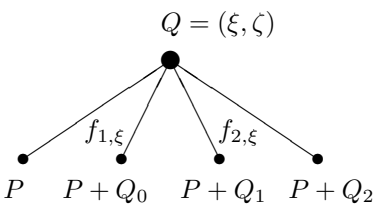
$$n=\max_j\{\mathrm{depth}(\mathcal{T}_j)\}+1\,.$$

As we will observe, the value of r such that $S_2(E(\mathbb{F}_q))$ has order 2^{n+r} is

$$r=\min_j\{\mathrm{depth}(\mathcal{T}_j)\}+1\,.$$

We have pointed out before that if $q\equiv 3 \pmod 4$, then two of these trees have depth 0 and we have $r=1$.

In these trees $\mathcal{T}_j$, if a vertex has children, then it has four.



According to Remark 6, the abscissas of the left pair are the roots of one of the polynomials $f_{i,\xi}$ and those of the right pair are the roots of the other one.

If we are in the case $E[4](\mathbb{F}_q) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, then the children of the root point Q_j, for $j \in \{0,1,2\}$, are

$$P_j, \quad P_j + Q_0 = P_j + 2P_0, \quad P_j + Q_1 = P_j + 2P_1, \quad P_j + Q_2 = P_j + 2P_2.$$

It is clear then that either the four points can be halved or none of them can. At most, we need three checkings, one in each tree, to determine the structure of $E[8](\mathbb{F}_q)$.

We have the same situation as long as $E[2^k](\mathbb{F}_q) \cong \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$: the known part of each $\mathcal{T}_j$ is a full quaternary tree with $k-1$ levels. Therefore, in $E[2^k](\mathbb{F}_q)$ we have $3 \cdot 4^{k-1}$ points of order 2^k, but three checkings of condition (6) are enough to determine $E[2^{k+1}]$. Since this condition depends only on the abscissa of the point, three computations of a root of a quadratic polynomial are enough to continue the process (see Figure 2).

Remark 7. If $E[2^k](\mathbb{F}_q) \cong \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$, every point of order 2^k in $\mathcal{T}_2$ can be written as a sum of a point of order 2^k in $\mathcal{T}_0$ and a point of order 2^k in $\mathcal{T}_1$. Therefore, if the checkings in $\mathcal{T}_0$ and $\mathcal{T}_1$ give affirmative answers, we already know that $E[2^{k+1}](\mathbb{F}_q) \cong \mathbb{Z}/2^{k+1}\mathbb{Z} \times \mathbb{Z}/2^{k+1}\mathbb{Z}$ and can proceed directly to the computation of the three new abscissas.

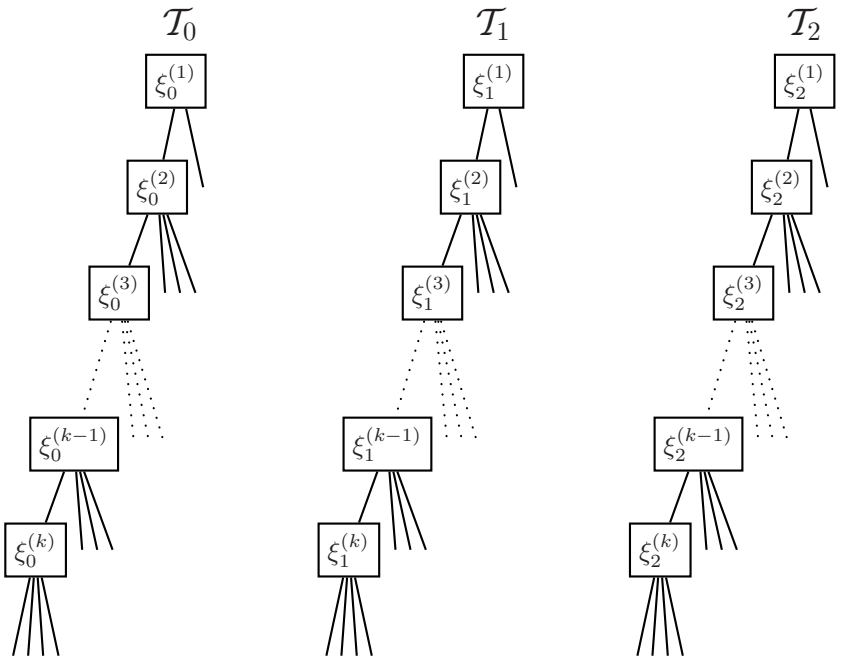


FIGURE 2. Forest of abscissas when $E[2^k](\mathbb{F}_q) \overset{\sim}{=} \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^k\mathbb{Z}$

We will continue in the way we have just described until we find that condition (6) fails, say at level ℓ. Then we set $r = \ell + 1$. This value will be an output of the algorithm.

If the halving condition fails in two of the points under consideration and it holds in the other one, then $E[2^{r+1}] \cong \mathbb{Z}/2^{r+1}\mathbb{Z} \times Z/2^r\mathbb{Z}$, which has 4^r points of order 2^{r+1}. Therefore, not only the point we have computed but all the points in its tree can be halved. And we can be sure that if the halving condition fails for the three points at the same level, then $S_2(E(\mathbb{F}_q))$ is $E[2^r](\mathbb{F}_q) \cong \mathbb{Z}/2^r\mathbb{Z} \times Z/2^r\mathbb{Z}$. Any two of these three points can be taken as generators of the Sylow subgroup.

Let us see how we reach the end when condition (6) fails for two points in different trees and it holds for the point in the tree $\mathcal{T}_i$. The algorithm outputs

$$\begin{aligned} r &= \ell + 1 = \operatorname{depth}(\mathcal{T}_j) + 1 \quad (j \neq i) \\ R, &\quad \text{a point of order } 2^r \text{ such that } 2^{r-1}R = Q_j \quad (j \neq i), \end{aligned}$$

and from the point in $\mathcal{T}_i$ we get a point of order 2^{r+1}. But from now on it is not enough to check the halving of a single point (see Figure 3).

Since $\mathbb{Z}/2^{r+2}\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$ has $2 \cdot 4^r$ points of order 2^{r+2}, either none of the points of $E[2^{r+1}](\mathbb{F}_q)$ can be halved or only half of them can. At most we need two points to check the halving condition. We will have this situation as long as $E[2^k](\mathbb{F}_q) \cong \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$: from the 2^{k-1+r} points of order 2^k, one half is 2-divisible and the other half is not. The only remaining question is to ensure that in each level we are able to take a point in each half. We reach the end when none of the abscissas of these two points satisfies condition (6).

Trivially, if P is a point of order 2^k, with $k > r$, such that $2^{k-1}P = Q_i$ and R is a point such that $2^{r-1} = Q_j$, with $j \neq i$, then P and $P + R$ are points of order 2^k that cannot both be halved, since R is a point of order 2^r and has not a half point.

Proposition 3. *Let $E/\mathbb{F}_q : y^2 = x(x^2 + \alpha x + \beta)$ with $\chi(\rho) = 1$, and Q_0, Q_1, Q_2 its rational points of order 2. Assume that one of these points, say Q_i, is 2^r divisible and the other two are not.*

Let P be a rational point of order 2^k, with $k > r$, such that $2^{k-1}P = Q_i$. Let R be a rational point such that $2^{r-1}R = Q_j$, with $j \neq i$. If $E(\mathbb{F}_q)$ has points of order 2^{k+1}, then either P or $P + R$ has a half point.

Proof. For any $j \in \{0, 1, 2\}$ and $m \geq 1$, let us denote

$$\begin{aligned} \mathcal{T}_{j,m} &= \{Q \in \mathcal{T}_j \text{ of order } 2^m\}, \\ \mathcal{T}^h_{j,m} &= \{Q \in \mathcal{T}_{j,m} \text{ having a half point}\}, \\ \mathcal{T}^{nh}_{j,m} &= \{Q \in \mathcal{T}_{j,m} \text{ not having a half point}\}. \end{aligned}$$

We are assuming that $P \in \mathcal{T}_{i,k}$, with $k > r$, and $R \in \mathcal{T}_{j,r}$, with $j \neq i$.

The points in the following (disjoint) sets have the same behavior as P with respect to the halving:

$$\begin{cases} P + E[2^{r-1}](\mathbb{F}_q) & (4^{r-1} \text{ points}), \\ P + \mathcal{T}_{i,r} & (4^{r-1} \text{ points}), \\ P + \mathcal{T}^h_{i,m} \text{ with } r+1 \leq m \leq k-1 & (2^{m-r} \cdot 4^{r-1} \text{ points}). \end{cases}$$

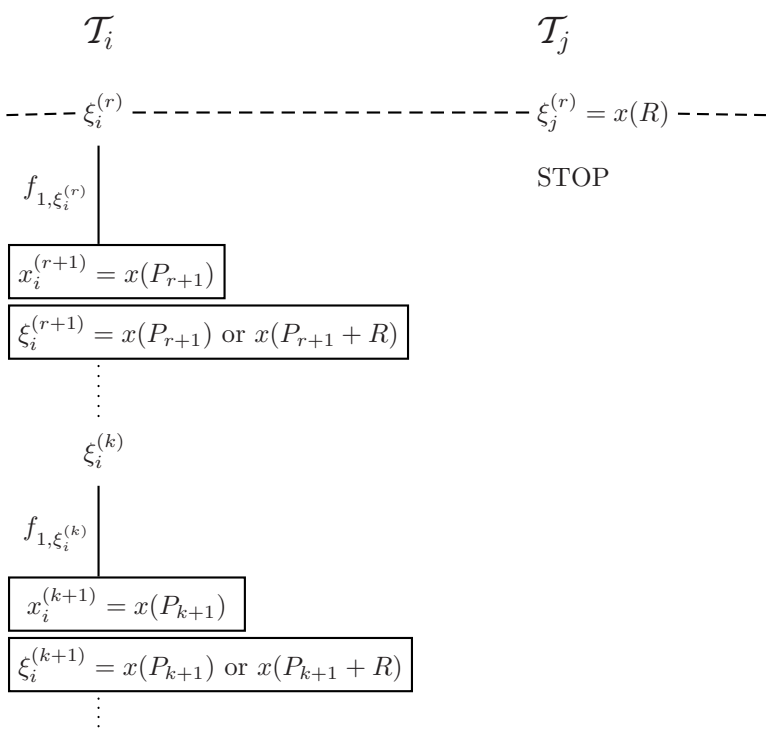


FIGURE 3. Halving process when $E[2^k](\mathbb{F}_q) \overset{\sim}{=} \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$

On the other hand, P and a point in one of the following (disjoint) sets cannot both be halved:

$$\begin{cases} P + \mathcal{T}_{j,r} \text{ with } j \neq i & (2 \cdot 4^{r-1} \text{ points}), \\ P + \mathcal{T}_{i,m}^{nh} \text{ with } r+1 \leq m \leq k-1 & (2^{m-r} \cdot 4^{r-1} \text{ points}). \end{cases}$$

We have described the set of 2^{k-1+r} points of order 2^k in such a way that if one of them has a half point, then this is the partition according to the halving condition. Since P and $P + R$ are in different parts, the claim follows. □

To summarize, in the noncyclic case we can have two different processes. At the beginning, in each step we have abscissas $\xi_0^{(k)}, \xi_1^{(k)}, \xi_2^{(k)}$ of points of order 2^k projecting over the three points of order 2, and $\xi_j^{(k+1)}$ is computed from the quadratic polynomial $f_{1,\xi_j^{(k)}}$ (or from $f_{2,\xi_j^{(k)}}$). If at some level we must continue from just one $\xi_i^{(r)}$, then we set R a point with abscissa $\xi_j^{(r)}$, with $j \neq i$. We compute a root $x_i^{(k+1)}$ of $f_{1,\xi_i^{(k)}}$. If the halving condition holds for this abscissa, then we take it as $\xi_i^{(k+1)}$. If not, $\xi_i^{(k+1)}$ is the abscissa of $P_{k+1} + R$, where P_{k+1} is a point with abscissa $x_i^{(k+1)}$. We repeat this until we find that neither P_n nor $P_n + R$ can be halved.

Remark 8. If $r = 1$, then $R = Q_j$, one of the points of order 2 not having a half point. Therefore, P and $P + R$ always have the same image under multiplication by 2, namely they are children of the same vertex. Since the abscissas of these two

points can be computed from the quadratic polynomials $f_{1,\xi}, f_{2,\xi}$, we do not need to perform any addition in the elliptic curve. We recall that this is always the case when $q \equiv 3 \pmod 4$.

According to Remark 6, to iterate the halving process, if the 4-divisible point is $(0,0)$, then from the first level we have to consider a root of $f_{1,\xi}$ and a root of $f_{2,\xi}$, else we have to consider the two roots of one of these polynomials.

4. Twists

If we want the input for our algorithm to be just a j-invariant, we have to consider couples of twisted elliptic curves (equations as in (2) to start with). Let $E_c/\mathbb{F}_q$ be a twist of $E/\mathbb{F}_q$, where $c \in \mathbb{F}_q^*$ is a quadratic nonresidue.

First of all, let us observe that the rank of the 2-Sylow subgroup is the same for both curves, since the distinction between the cyclic and the noncyclic case is given by the amount of rational points of order 2, and $E_c[2](\mathbb{F}_q) \cong E[2](\mathbb{F}_q)$.

Now, let us see what information concerning the order and structure of 2-Sylow subgroups can be obtained from the relation

$$|E(\mathbb{F}_q)| + |E_c(\mathbb{F}_q)| = 2(q+1) \tag{7}$$

between the group orders. We denote

$$\begin{aligned} \mu &= v_2(q+1), \\ \nu &= n + r = v_2(\,|E(\mathbb{F}_q)|\,), \\ \nu_c &= n_c + r_c = v_2(\,|E_c(\mathbb{F}_q)|\,). \end{aligned}$$

Then, it follows from (7) that

(1) $\nu \le \mu \Rightarrow \nu_c = \nu$;
(2) $\nu > \mu + 1 \Rightarrow \nu_c = \mu + 1$;
(3) $\nu = \mu + 1 \Rightarrow \nu_c > \mu + 1$.

Using that $r_c = 0$ if and only if $r = 0$, we see that in the first and second cases the output (n, r) of the algorithm provides not only the order ν_c but also the structure (n_c, r_c) of the 2-Sylow subgroup of the twisted curve:

- If $\mu \ge 2$, we have $q \equiv 3 \pmod 4$ and then $r_c = r \in \{0, 1\}$.
- If $\mu = 1$, namely $q \equiv 1 \pmod 4$, in the first case above we have $r_c = r = 0$ and $\nu_c = n_c = n = \nu = 1$. In the second case, $\nu_c = 2$ gives only two possible structures, $(2, 0)$ and $(1, 1)$, which are distinguished according to the value of r.

In brief, except for one critical value, $\nu = \mu + 1$, the computation of $S_2(E(\mathbb{F}_q))$ gives us $S_2(E_c(\mathbb{F}_q))$.

5. Algorithm

We devote this section to a concrete statement of the procedure of successive halving that we have described in the previous sections. In the cyclic case, the algorithm involves only computations of quadratic character and solving of quadratic equations in the finite field. In the noncyclic case, we may also need a translation map in the group of points of the elliptic curve.

We restrict to groups $E(\mathbb{F}_q)$ of even order and take as input the finite field $\mathbb{F}_q$ and the coefficients of an equation $y^2 = x(x^2 + \alpha x + \beta)$ for $E/\mathbb{F}_q$. As we have pointed in Section 2, to work in full generality, using a Weierstraß equation or just

a j-invariant, we have to add a gcd computation to decide if $E(\mathbb{F}_q)$ has even order, and if it is so, at most we have to solve a cubic equation to get a point of order 2. By translating it to the origin, we find a model as the one used here.

INPUT: : An odd prime power q and coefficients α and β of a model

$$y^2 = x(x^2 + \alpha x + \beta)$$

of E over $\mathbb{F}_q$, namely $(\alpha, \beta) \in \mathbb{F}_q \times \mathbb{F}_q^*$ such that $\alpha^2 - 4\beta \neq 0$.

OUTPUT: : Integers n, r such that $S_2(E(\mathbb{F}_q)) \cong \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$ and abscissas X_1, X_2 of points of order 2^n and 2^r, respectively, generating this Sylow subgroup.

---

(1) **If** $\chi\left(\alpha^2 - 4\beta\right) = -1$ compute, if it exists, the abscissa $\xi^{(2)}$ of the two points of order 4 (Lemma 2). If $\nexists\ \xi^{(2)}$, then $n = 1$, $r = 0$, $X_1 = 0$, $X_2 = \infty$ and **end** of the algorithm.
   (a) $k := 2$ and $\xi^{(k)} := \xi^{(2)}$.
   (b) **While** $\chi(\xi^{(k)}) = 1$ **do** $k := k + 1$; compute $\xi^{(k)}$ (Proposition 1).
   (c) **Return** $n = k$, $r = 0$, $X_1 = \xi^{(k)}$, $X_2 = \infty$ and **end** of the algorithm.

(2) **If** $\chi\left(\alpha^2 - 4\beta\right) = 1$ compute the roots ξ_1, ξ_2 of $x^2 + \alpha x + \beta$ and compute, if they exist, abscissas $\xi_i^{(2)}$, $i = 0, 1, 2$, of half points of the three points of order 2 (Lemma 3). If none of them exists, then $n = r = 1$, $X_1 = 0$, $X_2 = \xi_1$ and **end** of the algorithm.
   (a) $k := 2$; $h = 1$.
   (b) **While** $\exists\ \xi_i^{(k)}$ for all $i = 0, 1, 2$ and all of them verify the halving condition (Proposition 2) **do** $k := k + 1$; $h := k$; compute $\xi_i^{(k)}$ for all $i = 0, 1, 2$.
   (c) **If** $\nexists\ \xi_i^{(k)}$ for any $i = 0, 1, 2$, then **return** $n = r = h$, $X_1 = \xi_0^{(h)}$ and $X_2 = \xi_1^{(h)}$.
   (d) **If** $\exists\ \xi_i^{(k)}$ for some $i = 0, 1, 2$, and $\nexists\ \xi_j^{(k)}$ with $j \neq i$, then **do**
      (i) **If** $h = 1$, then **do**
         (A) Let X_2 the abscissa of one of the points of order 2 that has not a half point.
         (B) Select $\xi^{(k)}$ in $\{\xi_i^{(k)}, \xi_1(\xi_i^{(k)} - \xi_2)/(\xi_i^{(k)} - \xi_1)\}$ or $\{\xi_i^{(k)}, \beta/\xi_i^{(k)}\}$ (Remark 8).
         (C) **While** $\xi^{(k)}$ satisfies the halving condition (Proposition 2) **do** $k := k + 1$; compute ${\xi_i}^{(k)}$ and select $\xi^{(k)}$.
      (ii) **Else do**
         (A) $X_2 = \xi_j^{(h)}$. Select $\xi^{(k)} = \xi_i^{(k)}$ or $x(P^{(k)} + R)$, where the ordinates of the points $R = (X_2, Y_2)$ and $P^{(k)} = (\xi^{(k)}, \zeta^{(k)})$ are computed from the equation of the curve.
         (B) **While** $\xi^{(k)}$ satisfies the halving condition (Prop. 2) **do**
            B.1 $k := k + 1$; compute $\xi^{(k)}$.
            B.2 **If** $\xi^{(k)}$ does not satisfy the halving condition then **do** compute the point $P^{(k)} = (\xi^{(k)}, \zeta^{(k)})$ from the equation of the curve; $\xi^{(k)} = x(P^{(k)} + R)$.
   (e) **Return** $n = k$, $r = h$, $X_1 = \xi^{(k)}$ and X_2 and **end** of the algorithm.

The number of steps of this algorithm is bounded by $v_2(|E(\mathbb{F}_q)|)$, which is $\mathrm{O}(\log q)$. To analyze the cost of each step, we remark that the quadratic character in $\mathbb{F}_q$ may be evaluated in $\mathrm{O}(\log^2 q)$ bit operations, but any known method for computing square roots in finite fields has higher complexity. Therefore, this computation determines the running time of our algorithm.

Given a square in $\mathbb{F}_q^*$, the randomized algorithm of Cipolla returns a square root in expected running time $\mathrm{O}(\log^3 q)$ bit operations, which would give $\mathrm{O}(\log^4 q)$ for our algorithm. Nevertheless, there are other options to implement this computation which may be more convenient depending on the ground field. For a complete discussion on this subject we refer to Chapter 7 of [1]. As for the deterministic complexity, assuming the *Extended Riemann Hypothesis*, quadratic equations over $\mathbb{F}_q$ can be solved using $\mathrm{O}(\log^4 q)$ bit operations, which would give $\mathrm{O}(\log^5 q)$ for our algorithm.

We end this section with some brief comments aimed to place this algorithm in context:

- In elliptic curves with a *big* 2-Sylow subgroup, the ECDLP (Elliptic Curve Discrete Logarithm Problem) can be attacked using the Pohlig–Hellman method. With the algorithm presented, one could reject weak curves in the setup of cryptographic protocols based on the ECDLP.
- The existing algorithms (for instance, in library `LiDIA`, [7]) to compute the group structure of $E(\mathbb{F}_q)$ require costly subalgorithms to compute the group order and its factorization. With this algorithm, some information about this structure is leaked at a low cost.
- In the context of the SEA (Schoof–Elkies–Atkin) algorithm to compute the order of $E(\mathbb{F}_q)$ [2], it is necessary to compute $\tau \equiv t \pmod{\ell^n}$, where t is the trace of π, the Frobenius endomorphism, and ℓ is a primer number. Lately, Fouquet and Morain [4, 3] have extended the concept of the cycle graph of isogenies to the more general one of *volcano* graph. If the characteristic polynomial of the Frobenius endomorphism has a double root, i.e., $t^2-4q \equiv 0 \pmod{\ell}$, the method they present gives the ℓ-adic valuation

$$\nu = v_\ell(t^2 - 4q) = v_\ell(g^2 d_{\mathbb{K}}),$$

  where g is the conductor of the order $\mathbb{Z}[\pi]$, and $d_{\mathbb{K}}$ is the discriminant of the ring of integers $\mathcal{O}_{\mathbb{K}}$ of the imaginary quadratic field $\mathbb{K}$. When $\ell = 2$, $v_2(d_{\mathbb{K}})$ is not completely determined. Our algorithm could provide the value $v_2(|E(\mathbb{F}_q)|)$.

6. Some examples

The algorithm presented in the previous section has been implemented by A. Albajes in `LiDIA`, running over a Pentium IV with 1.7 GHz. It has been used to test one million random elliptic curves $E/\mathbb{F}_p$, for a couple of primes $p \approx 10^{60}$. The average time of execution for a curve was 0.01 seconds. We show some examples in Table 1.

We also provide two examples of *big* 2-Sylow subgroups corresponding to elliptic curves over $\mathbb{F}_p$, for a prime $p \approx 10^{100}$ in Table 2.

TABLE 1.

$\mathbf{p = 10^{60} + 3201}$	
α	234820398740293874092183470923740912374092384723
β	282370498273409827340987234098723098472309874092387 4
(n, r)	(1,0)
time	0.001 sec
α	63756814922387767694762229599315800444043404524720384773611
β	71699534277638901252704184433863155118707525941936400731125
(n, r)	(5,5)
time	0.08 sec
α	624244459916739411596415277576380974012824140892827008373162
β	48728557733801145957038989661215962911684332416416325433913 6
(n, r)	(17,0)
time	0.11 sec
α	804515977734860566494239770982282063895480484302363715494873
β	58477222160363286666568232289929714179318825200067425666207 1
(n, r)	(16,1)
time	0.13 sec

TABLE 2.

$\mathbf{p = 10^{100} + 13057}$	
α	627150165013081253030994054442804209234173351359015667297 22\ 391403729542696618483017975454652703999830
β	104760847526076775657639968093829764240798496900075038382 56\ 285520419480733828706532243068843293963 36
(n, r)	(7,4)
time	0.31 sec
α	6369288812394634484923439349628752492876927557605470188657 8\ 609470354767781904006642623542972510153 7
β	2826724025325719096445419599987395530037612819013666916774 0\ 529649301278049357372327726172030028848 02
(n, r)	(19,0)
time	0.37 sec

Moreover, the algorithm has also been used to study the distribution of the curves $y^2 = x(x^2 + \alpha x + \beta)$ over $\mathbb{F}_p$. In particular, the results obtained for the Fermat prime $p = 257$ are summarized in Table 3. They are classified according to their 2-Sylow subgroup $\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$. Notice that, since there is no integer in

Table 3.

$n+r$	(n,r)	EC's	Isom. class.
1	(1,0)	16512	130
2	(2,0)	8192	64
	(1,1)	16320	43
3	(3,0)	4096	32
	(2,1)	6144	16
4	(4,0)	2560	20
	(3,1)	3840	10
	(2,2)	2304	6
5	(5,0)	512	4
	(4,1)	768	2
	(3,2)	384	1
8	(8,0)	1024	8
	(7,1)	1536	4
	(6,2)	768	2
	(5,3)	384	1
	(4,4)	192	1

Hasse's interval $[226, 290]$ with a factor either 2^6 or 2^7, there exists no curve with $n+r=6$ or $n+r=7$.

The amount of curves for each pair (n,r) is given in the third column and the number of their isomorphism classes in the last one. The isomorphisms $x = ux' + v$ and $y = u^3y' + su^2x' + t$, which we denote (u,v,s,t), preserving the form $y^2 = x(x^2+\alpha x+\beta)$ of the equation have $s = t = 0$ and v an abscissa of a rational 2-torsion point. Hence, the isomorphisms are $(u,0,0,0)$ when $\chi(\rho) = -1$, or $(u,0,0,0)$, $(u, \frac{-\alpha+\sqrt{\rho}}{2}, 0, 0)$ and $(u, \frac{-\alpha-\sqrt{\rho}}{2}, 0, 0)$ when $\chi(\rho) = 1$. Then, since $(u,0,0,0)$ and $(-u,0,0,0)$ lead to the same isomorphic curve, there will exist either $(p-1)/2$ or $3(p-1)/2$ curves in each isomorphism class, respectively. Nevertheless, notice that when $j = 1728$ and -1 is a quadratic residue, only half of them can be accounted for. Then, the last column of the table can be obtained by combining these results with the ones presented in [9], which provide the number of isomorphism classes with $j = 1728$.

In Table 3, we observe some relations already predicted in Section 4. Since $\mu = v_2(258) = 1$,

- the number of curves obtained for $(2,0)$ is the sum of the ones obtained for $(n,0)$ with $n \geq 3$: each elliptic curve with cyclic 2-Sylow subgroup of order $\nu = 2$ has a twisted curve with cyclic 2-Sylow subgroup of order $\nu_c > 2$, and vice versa.
- the number corresponding to $(1,1)$ is the sum of the ones corresponding to (n,r) with $n \geq 2$ and $r \geq 1$: the analogue to the above statement is true in the noncyclic case.

Finally, it should be remarked that other relations between the amounts in the last column can be read in the context of the volcano structure of the 2-isogenies (see [4]). For instance, the number of isomorphism classes with $(n, 0)$, when $n > 2$, doubles the one corresponding to $(n-1, 1)$. This responds to the fact that the curves with cyclic 2-Sylow subgroup are placed at the base of the volcano, whereas the ones with $(n-1, 1)$ are in the first level.

References

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

[2] J. M. Couveignes and F. Morain, *Schoof algorithm and isogeny cycles*, ANTS-I (L. Adleman and M.D. Huangs, eds.), LNCS, no. 877, Springer-Verlag, 1994, pp. 43–58. MR **95m:**11147

[3] M. Fouquet, *Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques*, Ph.D. thesis, École Polytechnique, Paris, 2001.

[4] M. Fouquet and F. Morain, *Isogeny volcanoes and the SEA algorithm*, ANTS-V (C. Fieker and D.R. Kohel, eds.), LNCS, no. 2369, Springer-Verlag, 2002, pp. 276–291.

[5] D. Husemöller, *Elliptic curves*, GTM, no. 111, Springer-Verlag, 1987. MR **88h:**11039

[6] E. W. Knudsen, *Elliptic scalar multiplication using point halving*, Advances in Cryptology–ASIACRYPT'99 (K.Y. Lam, E. Okamoto, and C. Xing, eds.), LNCS, no. 1716, Springer-Verlag, 1999, pp. 135–149. MR **2001d:**94016

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

[8] J. F. Mestre, *La méthode des graphes. Exemples et applications*, Proc. Int. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, Japan), 1986, pp. 217–242. MR **88e:**11025

[9] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls, *Isomorphism classes of elliptic curves with even order over a finite field*, Int. Math. Journal **2** (2002), no. 9, 931–942. MR **2003e:**11066

[10] H. G. Rück, *A note on elliptic curves over finite fields*, Math. of Comp. **49** (1987), no. 179, 301–304. MR **88d:**11058

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

[12] J. H. Silverman, *The arithmetic of elliptic curves*, GTM, no. 106, Springer-Verlag, 1986. MR **87g:**11070

[13] J. Voloch, *A note on elliptic curves over finite fields*, Bull. Soc. Math. France (1988), no. 116, 455–458. MR **90f:**14012

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

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

Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, Pau Gargallo 5, 08028-Barcelona, Spain
E-mail address: `ana.rio@upc.es`

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