I. Ingredients of Schoof's algorithm and its main idea

Let E be a projective elliptic curve over $\mathbb{F}_q$. By Hasse's theorem, $|E(\mathbb{F}_q)| = q - t + 1$, where $|t| \leq 2\sqrt{q}$. A related fact states that

$$\varphi^2 \ominus [t]\varphi \oplus [q] = \mathcal{O}, \tag{I.1}$$

where φ stands for the *Frobenius endomorphism* of E.

To explain the meaning of (I.1) let us start with the meaning of φ. If $P = (\alpha_1 : \alpha_2 : \alpha_3) \in E$, then $\varphi(P) = (\alpha_1^q : \alpha_2^q : \alpha_3^q) \in E$ too. To see this consider the equation, say $w(X_1, X_2, X_3) = 0$, that determines E. If $w(\alpha_1, \alpha_2, \alpha_3) = 0$, then $0 = \big(w(\alpha_1, \alpha_2, \alpha_3)\big)^q = w(\alpha_1^q, \alpha_2^q, \alpha_3^q)$. For example if E is given by a smooth Weierstraß curve $y^2 = x^3 + ax + b$ and $P = (\alpha, \beta) \in E$, then $\varphi(P) = (\alpha^q, \beta^q)$. Indeed $\beta^{2q} = (\beta^2)^q$ is equal to $\alpha^{3q} + a\alpha^q + b = (\alpha^3 + a\alpha + b)^q$, as $a^q = a$ and $b^q = b$.

The Frobenius endomorphism φ sends points of E upon the points of E. Equation (I.1) implicitly uses the fact that φ is also an endomorphism of the group $E(\bar{\mathbb{F}}_q)$, i.e. that $\varphi(P \oplus Q) = \varphi(P) \oplus \varphi(Q)$ for all $P, Q \in E$. This can be proved from the addition formulas. However, this is also a consequence of a more general fact that is explained below when introducing the notion of *isogeny*.

Equation (I.1) thus means that if three endomorphisms of $E(\bar{\mathbb{F}}_q)$, i.e., $P \mapsto \varphi^2(P)$, $P \mapsto [-t](\varphi(P))$ and $P \mapsto [q]P$, are summed up, then the result is the trivial endomorphism $P \mapsto \mathcal{O}$. This can also be expressed as

$$\varphi^2(P) \ominus [t]\varphi(P) \oplus [q]P = \mathcal{O} \text{ for every } P \in E. \tag{I.2}$$

In fact, the latter form occurs in literature more often than (I.1). However, it may be argued that the expression via (I.1) is more instructive since it conveys better the fact that we are dealing with a property of the group $E(\bar{\mathbb{F}}_q)$. This is important since the structure of the group does not change under birational equivalence.

It is usual to call $T^2 - tT + q$ the *characteristic polynomial of the Frobenius endomorphism* and t the *trace of the Frobenius endomorphism*. Here T stands for a variable and carries no specific meaning. Reasons for calling t a 'trace' will be explained at the end of this section.

If P is a $\mathbb{F}_q$-rational point of E, then $\varphi(P) = P$. In such a case (I.2) states that $[P] \ominus [t]P \oplus [q]P = [q - t + 1]P$ is equal to $\mathcal{O}$. This is true because $P \in E(\mathbb{F}_q) \leq E(\bar{\mathbb{F}}_q)$ and $|E(\mathbb{F}_q)| = q - t + 1$.

I.1. **Isogenies.** To understand Schoof's algorithm it is not completely necessary to absorb the content of this subsection. Its purpose is to set the endomorphisms occurring in (I.1) into a broader context. It explains the notion of morphism and the notion of isogeny, and states some of the basic properties that morphisms and isogenies fulfil. Morphisms and isogenies belong to central notions of elliptic curves theory, and are used in quite a few algorithms.

How to transfer the notion of a rational map to projective curves, say C and D? This question can be answered in several ways. Here we shall discuss, for the sake of simplicity, only the situation when both C and D are smooth. In that case every rational map from an affine part of C to an affine part of D may be extended to a *morphism* $C \to D$.

Suppose that $C = V_F$ and $D = V_G$. A morphism $\psi\colon C \to D$ is *represented* by $A = (A_1 : A_2 : A_3)$ if *the polynomials* $A_1, A_2, A_3 \in K[X_1, X_2, X_3]$ *are homogeneous and of the same degree and, with only finitely many exceptions, for each* $\alpha = (\alpha_1 : \alpha_2 : \alpha_3) \in C$ *at least one of* $A_1(\alpha)$, $A_2(\alpha)$ *and* $A_3(\alpha)$ *is nonzero, and* $(A_1(\alpha) : A_2(\alpha) : A_3(\alpha)) = \psi(\alpha) \in D$.

Triples $(A_1 : A_2 : A_3)$ and $(B_1 : B_2 : B_3)$ represent the same morphism if $A_iB_j - A_jB_i \in (F)$ whenever $1 \leq i < j \leq 3$. It can be proved that if $\alpha \in C$, and if $\psi\colon C \to D$ is a morphism, then there exists $(A_1 : A_2 : A_3)$ representing ψ such

that at least one of $A_i(\alpha)$ is not zero. This means that a **morphism $\psi\colon C \to D$ is defined everywhere**. This is the main theoretical advantage of morphisms when compared to rational maps.

Any constant mapping $C \to D$ is a morphism. Because of that (and for other reasons too) it is useful, while not necessary, to allow in the definition of morphism that one or two of A_is are zero polynomials.

If C is an elliptic curve over K, then any K-rational point of C may be chosen as the zero element $\mathcal{O}$ of the group $C(K)$. In fact, $C(K)$ is completely determined by C and the choice of $\mathcal{O}$. This is why some authors define an elliptic curve as a pair $(C, \mathcal{O})$. Here it is assumed that $\mathcal{O}$ is known from the context. By context we understand, e.g., the convention that $\mathcal{O} = \infty$ for a Weierstraß curve, and $\mathcal{O} = (0, 1)$ for a (twisted) Edwards curve. (Of course, choosing a different neutral element induces different addition formulas.)

Let C and D be smooth elliptic curves over K, and let $\mathcal{O}_C$ and $\mathcal{O}_D$ be the neutral elements. An *isogeny* $C \to D$ is any morphism $C \to D$ that sends $\mathcal{O}_C$ upon $\mathcal{O}_D$. It can be proved (and the proof is not completely easy) that **each isogeny is also a group homomorphism** $C(K) \to D(K)$. A related result states that **if ψ_1 and ψ_2 are isogenies $C \to D$, then $\psi_1 \oplus \psi_2$ is also an isogeny $C \to D$.** (The mapping $\psi_1 \oplus \psi_2$ sends a point $P \in C$ to $\psi_1(P) \oplus \psi_2(P) \in D$, the addition being performed in $D(\bar{K})$.) Note that if $n > 0$, then the mapping $P \mapsto [n]P$ can be expressed as $\mathrm{id}_C \oplus \cdots \oplus \mathrm{id}_C$, where id_C occurs n times. To prove that $P \mapsto [n]P$ is an isogeny thus does not require knowledge of formula (D.3).

An *endomorphism* of C is an isogeny $C \to C$. This is seemingly inconsistent with usual conventions since here an endomorphism of C is something different than a morphism $C \to C$. As an example of the latter take a point $Q \in C$. The *translation* $t_Q\colon P \mapsto P \oplus Q$ is a morphism $C \to C$, but not an endomorphism (unless $Q = \mathcal{O}$) since it maps $\mathcal{O}$ upon Q.

Without going into details let us justify the convention that an endomorphism of C has to be an isogeny by saying that endomorphisms of C are, in fact, assumed to be endomorphisms of $(C, \mathcal{O})$.

All endomorphisms of C form a ring. The ring is denoted by $\mathrm{End}(C)$. This ring contains a subring that is isomorphic to $\mathbb{Z}$ and consists of all mappings $[n]\colon P \to [n]P$. If $K = \mathbb{F}_q$, then $\mathrm{End}(C)$ also contains the Frobenius endomorphism φ.

As an example how to express a rational map (ρ_1, ρ_2) as a morphism represented by $(A_1 : A_2 : A_3)$ let us consider the doubling upon a smooth Weierstraß curve C given by $y^2 = x^3 + ax + b$. The strategy is always the same. Replace $r_i/s_i = r_i(x_1, x_2)/s_i(x_1, x_2)$ that represents ρ_i by $R_i(X_1, X_2, X_3)/S_i(X_1, X_2, X_3)$, where $\deg(R_i) = \deg(S_i)$, $\gcd(R_i, S_i) = 1$ and $R_i(X_1, X_2, 1)/S_i(X_1, X_2, 1) = r_i/s_i$, and then replace $(R_1/S_1 : R_2/S_2 : 1)$ by $(R_1S/S_1 : R_2S/S_2 : S) = (A_1 : A_2 : A_3)$, where $S = \mathrm{lcm}(S_1, S_2)$.

In our example we may proceed similarly as when expressing the doubling in projective coordinates, as done at the end of Section A. We have

$$\begin{aligned}
\frac{r_1(x_1, x_2)}{s_1(x_1, x_2)} &= \frac{(3x_1^2 + a)^2 - 8x_1x_2^2}{4x_2^2},\\
\frac{r_2(x_1, x_2)}{s_2(x_1, x_2)} &= \frac{(3x_1^2 + a)(12x_1x_2^2 - (3x_1^2 + a)^2) - 8x_2^4}{8x_2^3},\\
R_1(X_1, X_2, X_3) &= (3X_1^2 + aX_3^2)^2 - 8X_1X_2^2X_3,\\
S_1(X_1, X_2, X_3) &= 4X_2^2X_3^2,\\
R_2(X_1, X_2, X_3) &= (3X_1^2 + aX_3^2)(12X_1X_2^2X_3 - (3X_1^2 + aX_3^2)^2) - 8X_2^4X_3^2, \text{ and}\\
S_2(X_1, X_2, X_3) &= 8X_2^3X_3^3 = S(X_1, X_2, X_3).
\end{aligned}$$

This shows that the morphism $P \mapsto [2]P$ may be represented by $(A_1 : A_2 : A_3) = (2X_2X_3R_1(X_1, X_2, X_3) : R_2(X_1, X_2, X_3) : 8X_2^3X_3^3)$. Unlike the rational maps, morphisms are defined everywhere. To illustrate this assume that $P = (\alpha, \beta) = (\alpha : \beta : 1)$ is an involution. This means that $\beta = 0$. In such a case $(A_1 : A_2 : A_3)$ sends P upon $(0 : -(3\alpha^2 + a)^3 : 0) = (0 : 1 : 0) = \infty$, as expected. (Recall that $3\alpha^2 + a \neq 0$ since α is a simple root of $x^3 + ax + b$.)

I.2. **The idea of Schoof's algorithm.** Schoof's algorithm counts the number of $\mathbb{F}_q$-rational points upon an elliptic curve E. It will be assumed that E is given by $y^2 = x^3 + ax + b$ and that q is divisible by neither 2 nor 3.

While we shall be concerned only with Weierstraß curves, the general framework of Schoof's algorithm is clearly applicable to other forms of elliptic curves. Nevertheless, details of the algorithm are tightly bounded with the specific properties of Weierstraß curves. The algorithm may be adapted to normal forms in characteristics 2 and 3. However, the case of $y^2 = x^3 + ax + b$ is technically the least complicated.

Recall that the order of $E(K)$ does not change under a birational equivalence. Hence there is always a possibility of finding a Weierstraß curve that is birationally equivalent to a given curve E.

The complexity of Schoof's algorithm is $O(\log^8 q)$ bit operations. This is an upper estimate that has been confirmed by practical experience. Theoretical complexity that uses different estimates for the complexity of multiplication is somewhat lower.

More advanced counting algorithms by Elkies and Atkins develop Schoof's ideas further on. A complete understanding of the Schoof-Elkies-Atkins algorithm (the SEA algorithm) requires knowledge of *modular polynomials*.

We shall now give an overall description of Schoof's algorithm.

Denote by t the trace of the Frobenius endomorphism. By Hasse's theorem, $|t| \leq 2\sqrt{q}$. If $\ell_1 < \cdots < \ell_r$ are primes such that $\prod \ell_i > 4\sqrt{q}$ and $t \bmod \ell_i$ is known for each $i \in \{1, \ldots, r\}$, then the Chinese Remainder Theorem determines t uniquely.

Primes $\ell_1, \ldots, \ell_r$ are taken to be the first r primes for which $\prod \ell_i$ is big enough. The main part of Schoof's algorithm thus is to determine $t_\ell = t \bmod \ell$, where ℓ is a prime that is significantly smaller than q.

If $\ell = 2$, then $t_\ell = 0$ when $E(K)$ contains an involution, and $t_\ell = 1$ otherwise. Thus $t_2 = 1$ if and only if the polynomial $x^3 + ax + b$ is irreducible in $K[x]$. Note that the latter happens if and only if $x^3 + ax + b$ is coprime to $x^q - x$.

For the rest we may thus assume that ℓ is an odd prime.

Let us denote by $E[\ell]^*$ the nonzero elements of $E[\ell]$. Hence each $P \in E[\ell]^*$ is of order ℓ. Each such P fulfils (I.2). Since $[\ell]P = \mathcal{O}$, we have, in fact,

$$\varphi^2(P) \oplus [q_\ell]P = [t_\ell]\varphi(P), \text{ where } q_\ell = q \bmod \ell. \tag{I.3}$$

This holds for every $P \in E[\ell]^*$. Hence if we find $\tau \in \{0, 1, \ldots, \ell - 1\}$ such that for *some* $P \in E[\ell]^*$

$$\varphi^2(P) \oplus [q_\ell]P = [\tau]\varphi(P),$$

then there must be $\tau = t_\ell$. The algorithm proceeds by taking values of $\tau = 0, 1, \ldots, (\ell-1)/2$ one after another. For each such τ the algorithm tests the existence of $P \in E[\ell]^*$ such that

$$\varphi^2(P) \oplus [q_\ell]P = [\pm\tau]\varphi(P) \tag{I.4}$$

until it succeeds.

Imagine for a while that all points $P = (\alpha, \beta) \in E$ fulfilling (I.4) were at our disposal. In such a case the obvious step to do would be to test whether some of

them belongs to $E[\ell]$. Of course, $P \in E[\ell]$ if and only if $\psi_\ell(\alpha, \beta) = 0$, where ψ_ℓ is the ℓth division polynomial.

However, the algorithm does not run by finding all points P that fulfil (I.4). That would be difficult to achieve. What the algorithm does is to look for properties that such a point P has to fulfil, and to refute the incorrect values of τ when such a property is not fulfilled.

Suppose for a while that τ is fixed and that $\tau > 0$. Let us compare symbolically the first coordinate of $\varphi^2(P) \oplus [q_\ell]P$ (i.e., the x-coordinate) with the first coordinate of $[\tau]P$. It turns out that there exists a polynomial $h_X = h_{X,\tau} \in \mathbb{F}_q[x]$ such that **a point $P = (\alpha, \beta) \in E$ fulfils (I.4) if and only if** $h_X(\alpha) = 0$. To be exact, the "if and only if" relationship holds only for those P that do not belong to $E[q_\ell]^*$ or $E[\pm\tau]^*$. These exceptions cause no problem since the goal is to decide whether such a P can be found in $E[\ell]^*$. This is true if and only if $\gcd(\bar{f}_\ell, h_X) \neq 1$.

Suppose thus that $\bar{f}_\ell$ and h_X have a common root, say α. This means that $t_\ell \in \{-\tau, \tau\}$, and that there exists $\beta \in \bar{\mathbb{F}}_q$ such that $P = (\alpha, \beta)$ belongs to $E[\ell]^*$ and the point $\varphi^2(P) \oplus [q_\ell]P$ shares the first coordinate with $[\tau](\varphi(P))$. If these two points share also the second coordinate, then they are equal. In such a case $t_\ell = \tau$. If the points to not agree then $t_\ell = -\tau$. Hence the second coordinates either agree for all $P \in E[\ell]^*$, or for none $P \in E[\ell]^*$.

It turns out that if the second coordinates are compared, then the value of β may be cancelled out. Therefore there exists a polynomial h_Y such that $h_Y(\alpha) = 0$ if and only if the second coordinates agree, for any $P = (\alpha, \beta) \in E[\ell]^*$. If h_Y and $\bar{f}_\ell$ have a nontrivial common divisor, then $t_\ell = \tau$. Otherwise $t_\ell = -\tau$.

The construction of polynomials h_X and h_Y can be regarded as the computational core of Schoof's algorithm.

Because we are interested only in $\gcd(h_X, \bar{f}_\ell)$, the polynomial h_X may be actually computed modulo $\bar{f}_\ell$ all the time. This reduces the computational complexity. The degree of $\bar{f}_\ell$ is $\leq (\ell^2 - 1)/2$. The same reduction may be done for h_Y and other polynomials.

Polynomials h_X and h_Y are not computed when $t_\ell = 0$, and also in some other cases. What exactly are these exceptional cases and how they are handled is explained below.

While points $P = (\alpha, \beta) \in E[\ell]$ are considered throughout the description of the algorithm, neither α nor β is ever explicitly computed. All needed tests are turned into a polynomial form that involves α only, and we are asking if such a polynomial has a root in $E[\ell]^*$. Since any $P \in E \setminus E[2]$ belongs to $E[\ell]$ if and only if $\bar{f}_\ell(\alpha) = 0$, such a test may be performed by testing whether the polynomial and $\bar{f}_\ell$ possess a nontrivial common divisor.

I.3. **When the first coordinates coincide.** When starting to process an odd prime ℓ, the first step to be performed is to add $\varphi^2(P)$ and $[q_\ell]P$ under the assumption that $P \in E[\ell]^*$. But which formula to use? To decide that, the algorithm finds out whether there exists $P \in E[\ell]^*$ such that $\varphi^2(P) = [\pm q_\ell]P$. If $P = (\alpha, \beta) \in E \setminus E[q_\ell]$, then $[q_\ell](P)$ can be expressed by means of (D.3). Since $\varphi^2(P) = (\alpha^{q^2}, \beta^{q^2})$ it is easy to see that the first coordinates of both $\varphi^2(P)$ and $[q_\ell](P)$ depend only upon α. This yields a polynomial $\bar{s}_\ell \in \mathbb{F}_q[x]$ such that the first coordinates agree if and only if $\bar{s}_\ell(\alpha) = 0$. The existence of $P \in E[\ell]^*$ with $\varphi^2(P) = [\pm q_\ell]P$ is thus equivalent to $\gcd(\bar{s}_\ell, \bar{f}_\ell) \neq 1$. Let the latter be true.

Thus either $\varphi^2(P) = [q_\ell]P$ or $\varphi^2(P) = [-q_\ell]P$. In the latter case $t_\ell = 0$. To test whether $t_\ell = 0$ compare the second variables of $\varphi^2(P)$ and $[-q_\ell]P$. It turns out that by using $\beta^2 = \alpha^3 + a\alpha + b$ the value of β can be cancelled out from such an equation, and we get a polynomial in x. Now, $t_\ell = 0$ if and only if α is the root

of this polynomial for each $(\alpha, \beta) \in E[\ell]^*$, and that takes place if and only if this polynomial is a multiple of $\bar{f}_\ell$.

If the polynomial is coprime to $\bar{f}_\ell$, then $\varphi^2(P) = [q_\ell]P$ for some (but necessarily for all) $P \in E[\ell]^*$. This is a special case which differs from the cases considered above. Historically it is important since this has been the departing point for Elkies improvements.

The equality $\varphi^2(P) = [q_\ell]P$ does not yield immediately the value of t_ℓ. Replacing $\varphi^2(P)$ with $[q_\ell]P$ in (I.3) gives $[2q_\ell]P = [t_\ell]\varphi(P)$. Thus $\varphi(P) = [2q_\ell/t_\ell]P$ (the fraction is evaluated modulo ℓ) and

$$[q_\ell]P = \varphi^2(P) = \varphi([2q_\ell/t_\ell]P) = [(2q_\ell/t_\ell)^2]P.$$

Therefore $[t_\ell^2]P = [4q_\ell]P$ and $t_\ell^2 \equiv 4q_\ell \bmod \ell$. This gives two possible values for t_ℓ. Denote one of them by τ. We are asking whether $[2q_\ell]P = [\tau]\varphi(P)$ for some $P \in E[\ell]^*$. This can be written as $\varphi(P) = [\gamma]P$, where $\gamma = 2q_\ell/\tau$. A test for that can be devised similarly as the tests described earlier. If no such P exists, then $t_\ell = -\tau$.

I.4. **Comments on the SEA algorithm.** In Schoof's algorithm, when there is computed the gcd of a polynomial and $\bar{f}_\ell$, the polynomial is in most cases either coprime to $\bar{f}_\ell$ or a multiple of $\bar{f}_\ell$. This is because the equation (I.3) either holds for all $P \in E[\ell]^*$, or for none $P \in E[\ell]^*$. However the equation $\varphi^2(P) = [q_\ell]P$ may hold only for some $P \in E[\ell]^*$, and not for all of them. What is behind this phenomenon?

We have $E[\ell] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. This means that $(E[\ell], \oplus)$ can be regarded as a vector space of dimension 2 over $\mathbb{Z}_\ell$. The Frobenius endomorphism when restricted to this vector space is a linear automorphism, i.e., a linear transformation with trivial kernel. Denote this restriction by ψ. By Cayley-Hamilton Theorem, $\psi^2 - \mathrm{tr}(\psi)\psi + \det(\psi) = 0$. It is now clear why t is called the *trace of Frobenius endomorphism*.

The polynomial $T^2 - t_\ell T + q_\ell$ may have a root in $\mathbb{Z}_\ell$. If it does have a root, then ℓ is called an *Elkies prime*. If the polynomial is irreducible over $\mathbb{Z}_\ell$, then ℓ is called an *Atkin prime*.

Assume that ℓ is an Elkies prime. Then ψ possesses one or two eigenvalues. If λ is such an eigenvalue, then there exists $P \in E[\ell]^*$ such that $\varphi(P) = [\lambda]P$. We have encountered such a situation above, with $\lambda = 2q_\ell/t_\ell$. That is a special case. In the SEA algorithm an eigenvalue λ is determined for each Elkies prime ℓ.

Since we do not know t_ℓ in advance we also do not know in advance whether ℓ is an Elkies or Atkin prime. However, there exist methods using modular polynomials that allow to establish this without actually computing t_ℓ. Furthermore there exist methods involving modular polynomials and curves isogenous to E that allow, for each Elkies prime, to perform the testing for λ more efficiently. Once λ is known, we can use the existence of $P \in E[\ell]^*$ with $\varphi(P) = [\lambda]P$ to express (I.3) as $[\lambda^2](P) \oplus [q_\ell]P = [t_\ell\lambda]P$, which implies that $t_\ell = \lambda + q_\ell/\lambda$ (the fraction and the addition is evaluated modulo ℓ).

Another ingredient of the SEA algorithm is a method how to obtain, in case of an Atkin prime, a relatively small set T_ℓ such that t_ℓ has to belong to T_ℓ.

S. Schoof's algorithm

Let it be assumed that q is a prime power not divisible by 2 and 3, and that $a, b \in \mathbb{F}_q$ are such that $y^2 = x^3 + ax + b$ determines a smooth Weierstraß curve E. Polynomials h_X, h_Y and $\bar{s}_\ell$ are assumed to have the same meaning as in Section I. Here we shall explain how exactly they are computed.

Any polynomial in one variable that is computed in Schoof's algorithm may be immediately reduced modulo $\bar{f}_\ell$, where ℓ is the prime that is being processed. This fact is not being reflected in the ensuing description of Schoof's algorithm.

The description contains declarations of only those variables and procedures the meaning of which is not clear from the context. It skips declarations of procedures `equalx`, `nonequalx`, `tyzero` and `eigen` that are explained separately.

Procedure `equalx` is called when $\varphi^2(P)$ and $[q_\ell]P$ agree in the first variable for some $P \in E[\ell]^*$, while `noequalx` is used when $E[\ell]^*$ carries no such P.

```
Schoof's algorithm:
INPUT: q, a and b that determine a Weierstraß curve E.
OUTPUT: The order of E(F_q).

VARIABLES: B is the product of primes.
           M is the set of (ℓ, t_ℓ).
           r is the return value from nonequalx.

B = 2;
ℓ = 2;
if (gcd(x^q − x, x^3 + ax + b) = 1) then τ = 1 else τ = 0;
M = {(2, τ)};
while (B < 4√q) do:
      ℓ = nextprime(ℓ);
      B = B * ℓ;
      if (gcd(s̄_ℓ, f̄_ℓ) ≠ 1)
          then τ = equalx(ℓ)
          else do:
               τ = 0;
               do:
                    τ = τ + 1;
                    r = nonequalx(ℓ, τ);
               until (r ≠ 0);
               if (r = −1) then τ = −τ;
      M = M ∪ {(ℓ, τ)};
Recover t using the set M and the CRT.
Return q+1−t.
```

Suppose that $m \geq 2$ and that $P = (\alpha, \beta) \in E$. By (D.3) the first coordinate of $[m]P$ is equal to $\alpha - (\psi_{m-1}\psi_{m+1}\psi_m^{-2})(\alpha, \beta)$. Using the transformation of (D.5) this yields $\alpha - \bar{f}_{m-1}(\alpha)\bar{f}_{m+1}(\alpha)/4\beta^2\bar{f}_m^2(\alpha)$ if m is even, while for m odd we get $\alpha - \bar{f}_{m-1}(\alpha)\bar{f}_{m+1}(\alpha)4\beta^2/\bar{f}_m^2(\alpha)$. Therefore the first coordinate of $[m]P$, $m \geq 2$, is equal to

$$\begin{aligned} &\alpha - \frac{\bar{f}_{m-1}(\alpha)\bar{f}_{m+1}(\alpha)}{4(\alpha^3 + a\alpha + b)\bar{f}_m^2(\alpha)} && \text{if } m \text{ is even, and} \\ &\alpha - \frac{4(\alpha^3 + a\alpha + b)\bar{f}_{m-1}(\alpha)\bar{f}_{m+1}(\alpha)}{\bar{f}_m^2(\alpha)} && \text{if } m \text{ is odd.} \end{aligned} \tag{S.1}$$

Thus $\bar{s}_\ell(x) = x^{q^2} - x$ if $q_\ell = 1$,

$$\bar{s}_\ell(x) = 4(x^{q^2}-x)(x^3+ax+b)\bar{f}_{q_\ell}^2(x) + \bar{f}_{q_\ell-1}(x)\bar{f}_{q_\ell+1}(x) \text{ if } q_\ell \text{ is even, and}$$

$$\bar{s}_\ell(x) = (x^{q^2}-x)\bar{f}_{q_\ell}^2(x) + 4(x^3+ax+b)\bar{f}_{q_\ell-1}(x)\bar{f}_{q_\ell+1}(x) \text{ if } q_\ell > 1 \text{ is odd.}$$

From (D.3) there also may be derived a formula for the second coordinate of $[m]P$, $m \geq 2$:

$$\begin{cases} \beta\dfrac{\bar{f}_{m+2}(\alpha)\bar{f}_{m-1}^2(\alpha) - \bar{f}_{m-2}(\alpha)\bar{f}_{m+1}^2(\alpha)}{16(\alpha^3+a\alpha+b)^2 f_m^3(\alpha)} & \text{if } m \text{ is even, and} \\ \beta\dfrac{\bar{f}_{m+2}(\alpha)\bar{f}_{m-1}^2(\alpha) - \bar{f}_{m-2}(\alpha)\bar{f}_{m+1}^2(\alpha)}{\bar{f}_m^3(\alpha)} & \text{if } m \text{ is odd.} \end{cases} \tag{S.2}$$

The procedure `equalx` calls as a subprocedure the procedure `tyzero`(ℓ, m) with parameter m equal to q_ℓ. This procedure returns `TRUE` if there exists $P = (\alpha, \beta) \in E[\ell]^*$ such that $\varphi^2(P) = [-m]P$, under the assumption that there exists $P \in E[\ell]^*$ for which the first coordinates of $\varphi^2(P)$ and $[-m]P$ agree.

Let us now describe the content of `tyzero`. The procedure is concerned with the equality $-\beta^{q^2} = \beta r_m(\alpha)/s_m(\alpha)$, where $r_m, s_m \in \mathbb{F}_q[x]$ correspond to (S.2). Thus $r_m = \bar{f}_{m+2}\bar{f}_{m-1}^2 - \bar{f}_{m-2}\bar{f}_{m+1}^2$ if m is even, etc. Since $\beta^2 = \alpha^3+a\alpha+b$ and $\beta \neq 0$, the equality takes the form $(\alpha^3+a\alpha+b)^{(q^2-1)/2} = -r_m(\alpha)/s_m(\alpha)$. If $t_\ell = 0$, then each $\alpha \in E[\ell]^*$ fulfils this equality. That takes place if and only if $\bar{f}_\ell$ divides $s_m(x)(x^3+ax+b)^{(q^2-1)/2} + r_m(x)$.

The other procedure called by `equalx` is called `eigen`. The parameters are ℓ and m. The procedure returns `TRUE` if there exists $P \in E[\ell]^*$ such that $\varphi(P) = [m]P$. The procedure has two parts, the first part tests the first coordinate and produces a polynomial $g_\ell \in \mathbb{F}_q[x]$ that can be regarded as an input for the second part which tests the second coordinate. In Schoof's algorithm the first part may be skipped if $\gcd(\bar{s}_\ell, \bar{f}_\ell)$ is remembered, since at this point of the algorithm that polynomial coincides with g_ℓ (the exact meaning of g_ℓ is described below).

The first part is similar to the derivation of $\bar{s}_\ell$. The only difference is that the term $x^{q^2} - x$ is replaced by $x^q - x$. Indeed, we are asking whether there exists $(\alpha, \beta) \in E[\ell]^*$ such that $\alpha^q = \alpha - (\psi_{m-1}\psi_{m+1}\psi_m^{-2})(\alpha, \beta)$, and derive a polynomial in variable x for which α has to be a root. To see if there exists a root of such a polynomial that really belongs to $E[\ell]^*$ we compute the gcd of this polynomial with $\bar{f}_\ell$, and denote the gcd by g_ℓ. If $g_\ell = 1$, then the procedure returns `FALSE`. Assume that g_ℓ is nontrivial. There are some special situations when $g_\ell = \bar{f}_\ell$ (e.g. if λ is a double root of the characteristic polynomial induced by the Frobenius endomorphism). In the other situations the polynomial g_ℓ is of degree $(\ell-1)/2$. The points $(\alpha, \beta) \in E[\ell]^*$ that fulfil $g_\ell(\alpha) = 0$ form a subgroup of $E[\ell]^*$. For the second part of the test only these points are to be considered because these are the points from which the eigenspace, if it exists, is constructed.

We are thus asking whether β^q is equal to $\beta r_m(\alpha)/s_m(\alpha)$, where r_m and s_m are derived from (S.2) as in the procedure `tyzero`, and where $g_\ell(\alpha) = 0$. This is true if $g_\ell(x)$ divides $(x^3+ax+b)^{(q-1)/2}s_m(x) - r_m(x)$ (alternatively: if the latter two polynomials possess a nontrivial common divisor).

```
PROCEDURE equalx(ℓ)
INPUT: Prime ℓ for which there exists P ∈ E[ℓ]* such that there agree
x-coordinates of φ²(P) and [q_ℓ]P.
OUTPUT: The value of t_ℓ.
if (tyzero(ℓ, q_ℓ) = TRUE)
    return 0;
τ = sqrt(4q_ℓ) mod ℓ;
```

$\gamma = 2q_\ell/\tau \bmod \ell$;
if $(\texttt{eigen}(\ell, \gamma) = \texttt{TRUE})$
    return τ
else return $-\tau$;

The description of procedure `nonequalx` is short too. In this case the computational content is delegated to the description of polynomials h_X and h_Y (and not to subroutines).

PROCEDURE nonequalx(ℓ, τ)
INPUT: Prime ℓ such that the x-coordinates of $\varphi^2(P)$ and $[q_\ell]P$ differ for every $P \in E[\ell]^*$.
Positive $\tau < \ell/2$ that is a candidate for t_ℓ.
OUTPUT: 0 if $t_\ell \neq \pm\tau$, 1 if $t_\ell = \tau$, -1 if $t_\ell = -\tau$.
if $(\gcd(h_X, \bar{f}_\ell) = 1)$ return 0;
if $(\gcd(h_Y, \bar{f}_\ell) = 1)$ return -1;
return 1;

When `nonequalx` is invoked, then it is already known that the generic addition formula holds for $\varphi^2(P) \oplus [q_\ell]P$ whenever $P \in E[\ell]^*$. Put $m = q_\ell$ to spare some indices.

Write (S.1) and (S.2) in a compact form

$$[m](\alpha, \beta) = \left(\alpha - \frac{c_m(\alpha)}{d_m(\alpha)},\, \beta\frac{r_m(\alpha)}{s_m(\alpha)}\right). \tag{S.3}$$

Note that this can be used even for $m = 1$ if we set $d_1(x) = r_1(x) = s_1(x) = 1$ and $c_1(x) = 0$. With this notation $\varphi^2(P) \oplus [m]P = (\alpha^{q^2}, \beta^{q^2}) \oplus [m](\alpha, \beta)$ is equal to

$$\left(\lambda^2 - \alpha^{q^2} - \alpha + \frac{c_m(\alpha)}{d_m(\alpha)},\ \lambda\left(2\alpha^{q^2} - \lambda^2 + \alpha - \frac{c_m(\alpha)}{d_m(\alpha)}\right) - \beta^{q^2}\right), \text{ where}$$

$$\lambda = \frac{\beta^{q^2} - \beta r_m(\alpha)/s_m(\alpha)}{\alpha^{q^2} - \alpha + c_m(\alpha)/d_m(\alpha)} = \beta\frac{d_m(\alpha)}{s_m(\alpha)}\frac{(\alpha^3+a\alpha+b)^{(q^2-1)/2}s_m(\alpha) - r_m(\alpha)}{d_m(\alpha)(\alpha^{q^2} - \alpha) + c_m(\alpha)}.$$

Since in the first coordinate λ occurs only as a square, the occurrence of β may be completely eliminated from the expression of the first coordinate of $\varphi^2(P) \oplus [m]P$.

We have

$$[\tau]\varphi(P) = \varphi([\tau]P) = \left(\alpha^q - \frac{c_\tau(\alpha^q)}{d_\tau(\alpha^q)},\, \beta^q\frac{r_\tau(\alpha^q)}{s_\tau(\alpha^q)}\right).$$

Therefore comparing the first coordinate of $\varphi^2(P) \oplus [m]P$ with $\alpha^q - c_\tau(\alpha^q)/d_\tau(\alpha^q)$ results into a polynomial condition on α. This is how polynomial h_X is derived. The first coordinates thus agree if and only if $h_X(\alpha) = 0$, assuming $d_m(\alpha) \neq 0$, $s_m(\alpha) \neq 0$ and $d_\tau(\alpha) \neq 0$. The latter assumptions cause no difficulty since an element of $E[q_\ell]^*$ or $E[\tau]^*$ is never an element of $E[\ell]^*$.

Since β may be eliminated from λ^2 and since $\beta^{q^2} = \beta(\alpha^3 + a\alpha + b)^{(q^2-1)/2}$ and $\beta^q = \beta(\alpha^3 + a\alpha + b)^{(q-1)/2}$ we see that when comparing the second coordinate of $[\tau]\varphi(P)$ with the second coordinate of $\varphi^2(P) \oplus [m]P$ the value of β may be cancelled out. Therefore the equality of the second coordinates may be expressed via a polynomial in α too. This is the polynomial h_Y.