Schoof-Elkies-Atkin Algorithm

Ben Galin[*]
bengalin@stanford.edu

Senior Thesis
Department of Mathematics
Stanford University

December 12, 2007

[*] The author would like to express his sincere gratitude to his thesis advisor, Prof. Gunnar Carlsson, and his degree advisor, Prof. Dan Bump.

1 Introduction

Following a timeworn naming convention, we assume that two people, Alice and Bob, would like to communicate in a secure manner through an insecure channel. Their cryptographic goals can be summarized as follows [16]:

1. *Confidentiality*: the content of the message is unknown to any third-party.

2. *Data integrity*: no third-party can change the content of the message in an undetected manner.

3. *Authentication*: a recipient of a message can detect the origin of the message.

4. *Non-repudiation*: a sender of a message cannot later deny the origin or content of a message.

If Alice and Bob can agree somehow on a secret key, they may be able to encrypt their messages such that if Eve, an eavesdropper, is intercepting the communication, she would be unable to recover the original message or alter its content in an undetectable manner. This would satisfy the first two goals above. Assuming that this secret key is only known to Alice and Bob, it's a small stretch of the imagination to see how the other two goals can be satisfied.

A cryptosystem based on the property above is called *symmetric-key cryptography.* This is to be contrasted with *public-key cryptography.* Public-key cryptography owes it origin to the 1976 article by Diffie and Hellman [8]. It is based on the idea that each participant generates two keys, one private and one public. The public key P_A of Alice is used by her partner, Bob, to encrypt a message he wishes to send to Alice. When Alice receives the ciphertext, she uses her private key p_A to decrypt the message.

One of the main advantages of public-key cryptography is obvious: in a system of n users, there is no need to distribute securely—and maintain the security of—$(n^2 - n)/2$ symmetric keys. Instead, each participant only needs access to the $n - 1$ public keys of the other parties. However, one notable disadvantage of public-key cryptography in comparison to symmetric-key cryptography is that the latter allows a much faster encryption and decryption of messages [16].

In Section 2, we provide the essential background information to a specific type of a public-key cryptosystem, known as the *Elliptic Curve Cryptography (ECC).* The overview in that section is not meant to be comprehensive by any means; a reader with background in ECC would find the material insufficient and simplified. Instead, one should view Section 2 as a motivation to the rest of the discussion.

The focus of this paper is on the `SEA` algorithm, which is one of the leading algorithms for point-counting, a concept that will be defined later. In Section 3, we introduce and build on the mathematical foundation needed in discussing point-counting in general and the `SEA` algorithm in particular. The theory behind elliptic curves is rich and complex. Therefore, we find it essential to refer the reader to other sources when elementary proofs cannot be found.

Section 4 includes the main exposition of this paper. It introduces Schoof's algorithm to determine the number of points on a curve, and then expands on this algorithm with Atkin's and Elkies' improvements. Once again, we shall occasionally encounter concepts that are beyond the scope of this paper and provide sources where proofs can be obtained. As elsewhere in modern cryptography, the mathematical theory is used to develop algorithms so that computations will be carried out by computers. To assist the reader in following this transition, we will work out a number of simple examples in an algorithmic fashion. We will conclude this section with a pseudo-code version of the `SEA` algorithm itself.

2 Overview of Elliptic Curve Cryptography

In this section we present an overview of ECC. We start by defining the Weierstrass equation of an elliptic curve and the group structure of the K-rational points of an elliptic curve, where K is a finite field. We then introduce the *discrete logarithm problem (DLP)* cryptographic primitive and show how it is applied to ECC. To conclude, we present an implementation example, the *Elliptic Curve Digital Signature Algorithm (ECDSA).*

2.1 Group structure

Let K be a finite field, K^* be its multiplicative group, and $\overline{K}$ be its algebraic closure. Our goal in this section is to first define elliptic curves and then construct a cyclic group G corresponding to a given elliptic curve E/K. The group elements are a subset of the so-called K-rational points. Using projective coordinates, we shall see that an elliptic curve E has one point of infinity, which we shall denote by $\mathcal{O}$. We will endow the set of points on the curve with a group operation $\oplus$, such that $\mathcal{O}$ is the identity element. Lastly, we will show that the K-rational points form a subgroup.

Following the treatment in [9], we define an *elliptic curve E over K* as follows:

Definition 1. An *elliptic curve E over a field K* is given by the affine Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ , \tag{1}$$

where the coefficients a_i are in the underlying field K, and for each point $(x_1, y_1) \in \overline{K}$ satisfying Equation (1), the partial derivatives $3x_1^2 + 2a_2x_1 + a_4 - a_1y_1$ and $2y_1 + a_1x_1 + a_3$ do not vanish simultaneously.

We write E/K for an elliptic curve E over K. When the underlying field is understood from the context, we may simply write E.

Let E/K be an elliptic curve with a Weierstrass equation (1). Write its equation with homogeneous coordinates in the projective plane $\mathbb{P}^2(\overline{K})$ by setting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \ . \tag{2}$$

With these homogeneous coordinates, the line of infinity is $Z = 0$. Thus, the intersection of the line of infinity with the elliptic curve E yields the equation $X^3 = 0$ and a single point of infinity $[0, 1, 0]$. We denote this point of infinity by $\mathcal{O}$. Note that the partial derivative of Equation (2) with respect to Z is $a_2X^2 + 2a_4XZ + 3a_6Z^2 - Y^2 - a_1XY - 2a_3YZ$, which does not vanish at $[0, 1, 0]$.

We say that a point $P = (x, y)$ is on an elliptic curve E/K if its coordinates are a solution to the Weierstrass equation of E, which implies that x and y are in the algebraic closure $\overline{K}$ of K. Our next goal is to separate points P on E with coordinates in K from the rest of the points.

Definition 2. Let E/K be an elliptic curve. For any field L with $K \subseteq L \subseteq \overline{K}$, an ordered pair (x, y) is called an *L-rational point of E* if x and y lie in the field L and (x, y) is a solution to the Weierstrass equation of E. In addition, we define the point of infinity $\mathcal{O}$ to be an L-rational point.

The set of all L-rational points of E is denoted by $E(L)$, and its cardinality is denoted by $|E(L)|$. We shall be mainly interested in K-rational points (that is, the case $L = K$).

Next, we define a group operation $\oplus$ on an elliptic curve E/K. First, we let $\mathcal{O}$ be the identity element, so $\mathcal{O} \oplus P = P \oplus \mathcal{O} = P$ and $P \oplus -P = \mathcal{O}$ for point P on E. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E. Then $P_1 \oplus P_2 = (x_3, y_3)$ with

$$\begin{aligned} -P_1 &= (x_1, -y_1 - a_1x_1 - a_3) \,, \\ P_1 \oplus P_2 &= \left(\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3\right) \text{ , where} \\ \lambda &= \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } P_1 \neq \pm P_2 \,, \\[2ex] \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } P_1 = P_2 \,. \end{cases} \end{aligned}$$

Proving that $(E/K, \oplus)$ is indeed a group is a straightforward process, albeit a tedious one. The associative rule, in particular, is painful. The group $(E/K, \oplus)$ is, in fact, abelian: Let $P_2 \oplus P_1 = (x_4, y_4)$ and observe that $\frac{y_1 - y_2}{x_1 - x_2} = \frac{y_2 - y_1}{x_2 - x_1}$, so λ is invariant. Then

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 = x_4 \,, \\ y_3 &= \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3 = \lambda(x_2 - x_3) + \lambda(x_1 - x_2) - y_1 - a_1x_3 - a_3 \\ &= \lambda(x_2 - x_3) - y_2 - a_1x_3 - a_3 = y_4 \,. \end{aligned}$$

We have defined a group operation on the entire set of points P on an elliptic curve E/K. However, we shall be mainly interested in K-rational points. From the definition of $\oplus$, it is clear that if P_1 and P_2 are K-rational points, then so are $P_1 \oplus P_2$ and $-P_1$, so $(E(K), \oplus)$ is indeed a subgroup of $(E/K, \oplus)$.

Henceforth, we shall write E/K and $E(K)$ in favor of $(E/K, \oplus)$ and $(E(K), \oplus)$, respectively, for the groups.

2.2 Discrete logarithm problem

In this section we begin relating the concepts defined above with the field of elliptic curve cryptography. The following definition is the cornerstone of ECC.

Definition 3. Let E/K be an elliptic curve. We define the *scalar multiplication by n*, where n is a positive integer, as a function

$$\begin{aligned} [n] : E/K &\to E/K \\ P &\mapsto [n]P = \underbrace{P \oplus \cdots \oplus P}_{n \text{ times}}. \end{aligned}$$

We extend this definition to all integers n by defining $[0]P = \mathcal{O}$ and $[n]P = [-n](-P)$ for $n < 0$. Note that if P is a K-rational point, than so is $[n]P$. Thus, the restriction of $[n]$ to the subgroup of K-rational points $E(K)$, yields a map $[n] : E(K) \to E(K)$.

We build on Definition 3 to introduce the district log problem, which is most commonly applied on cyclic groups of prime order. Note however that the group of K-rational points $E(K)$ need not be a cyclic group. In the remainder, we will let G be a cyclic subgroup of $E(K)$ of some prime order l.

Definition 4. Let $G \leq E(K)$ be a group of prime order l, and let $P, Q \in G$ with $P \neq \mathcal{O}$. Then the *discrete logarithm of Q with respect to P* is an integer n such that $Q = [n]P$.

Note that computing the discrete logarithm n can be done, and is unique, modulo l. The problem of finding the discrete logarithm of Q with respect to P for an arbitrary pair of elements $P, Q \in G$ is called the *discrete logarithm problem (DLP) in G*.

As explained by Avanzi [2], the complexity of solving the DLP in G is determined by the structure and representation of G. For instance, Lagrange's theorem asserts that there is only one group, up to isomorphism, of prime order l, so the DLP in G can be transformed to the one in $(\mathbb{Z}/l\mathbb{Z}, +)$. On the other hand, G can be embedded into the multiplicative group of $\mathbb{F}_r$ as the group of l-th roots of unity, where l divides $r - 1$. However, Avanzi [2] shows that the DLP in this group is harder than in $(\mathbb{Z}/l\mathbb{Z}, +)$.

In general, the DLP is considered a hard problem to solve for many finite cyclic groups of large order, though much care should be practiced in choosing the exact group. As such, the DLP is used as a *cryptographic primitive*, and a number of DLP-based cryptosystems have emerged. Examples of such cryptosystems are the ElGamal encryption, the Diffie-Hellman key exchange, and the elliptic curve digital signature algorithm systems. The last systems is discussed in some more detail in Section 2.4.

2.3 Security of ECC

With a careful choice of an elliptic curve E, an underlying field K, and the cyclic subgroup $G \leq E(K)$, the corresponding elliptic curve cryptosystem can provide the same level of security as the integer-factorization based system RSA, while allowing significantly smaller key sizes [23].

A standard way of assessing the level of security provided by a cryptosystem is to determine complexity of the best known attack algorithm against it [3]. Here, complexity is defined as follows:

Definition 5. Let `Alg` be an algorithm depending on N. Define

$$L_N(\alpha, c) = \exp\left(c(\ln N)^{\alpha}(\ln\ln N)^{1-\alpha}\right) ,$$

where $0 \leq \alpha \leq 1$ and $c > 0$. Then `Alg` is said to be *exponential in* N if its running time is bounded from above by a function proportional to $L_N(1, c)$; it is *polynomial in* N if its running time is bounded from above by a function proportional to $L_N(0, c)$; and it is *subexponential in* N if its running time is bounded from above by a function proportional to $L_N(\alpha, c)$ for $\alpha < 1$.

Note that the designation *exponential* refers to exponential in the *logarithm* of the order. In other words, an exponential algorithm in the group order $|G|$ is one that requires no more than $|G|^C$ group compositions, where C is a positive constant. It is known [2], that for any cyclic group we have $C \leq 1/2$.

As discussed in [2], [16], and [15], at present there are no generic subexponential algorithms to solve the DLP, where a generic algorithm is defined to be one which only performs composition, inversion, and equality checking. Examples of generic algorithms are the Chinese remainder theorem (CRT), Pollard's rho method, and the baby-step/giant-step (BSGS) algorithm. We will see an algorithm related to the BSGS algorithm in Section 4.6.

For curves with additional properties, some of which will be described later, there are subexponential algorithms that may be used to solve the DLP, such as the index calculus attack and Weil descent. We invite the reader to refer to the excellent surveys by Avanzi and Thériault [4] and Frey and Lange [10] for more details about different algorithms, as well as additional references.

In Table 1, adapted from the National Institute of Standards and Technology publication [5], we provide a comparison of key sizes between (i) finite field cryptography (FFC), such as Diffie-Hellmand key exchange and DSA; (ii) integer-factorization cryptography (IFC), such as RSA; and (iii) elliptic curve cryptography (ECC), such as ECDSA, which will be explained in Section 2.4.

Bits of security	FFC	IFC	ECC
80	1024 for public, 160 for private	1024	160–223
112	2048 for public, 224 for private	2048	224-255
128	3072 for public, 256 for private	3072	256–383
192	7680 for public, 384 for private	7680	384–511
256	15360 for public, 512 for private	15360	512+

Table 1: Comparison of key sizes

The reason for the striking difference in key sizes between ECC and the other two leading cryptosystems is that there are known subexponential algorithms to break FFC and IFC systems (see [3] and [15]). Therefore, in order to achieve the same level of security, one needs shorter keys when using an ECC-based system in comparison to RSA or non ECC-based DLP systems. This represents a significant advantage of ECC over other systems when hardware resources are limited.

2.4 Implementation example: ECDSA

In this section we provide an example for an elliptic curve cryptosystem implementation. Specifically, we describe the *Elliptic Curve Digital Signature Algorithm (ECDSA)*, which is an ElGamal-like digital signature algorithm, based on ECC. A digital signature algorithm is comprised of two separate algorithms, one for signing a message by the sender and the other for verifying the signature by the recipient. In the first algorithm, Alice, the sender, appends to a message m a signature (r, s) that depends on her private key p_A and the content of the message itself. Bob, the recipient, verifies the signature, using the knowledge of Alice's public key P_A.

In the context of elliptic curve cryptosystems, we define the following tuple of domain parameters $D = (q, FR, a_4, a_6, P, l, c)$:

- q is the field characteristic;
- FR is a field representation of $\mathbb{F}_q$;
- a_4 and a_6 are the coefficients of the short Weierstrass equation of E, an elliptic curve over $\mathbb{F}_q$;
- $P = (x_P, y_P)$ is an $\mathbb{F}_q$-rational base point;
- l is the order of a prime cyclic subgroup of $\mathbb{F}_q$, which contains P; and
- $c = |E(\mathbb{F}_q)|/l$.

We shall assume that the domain parameters are known to all parties and possibly to intruders, as well.

We present the digital signature algorithm in the context of ECC, as adapted from [15]. A simple key generation algorithm is presented in Figure 1. This algorithm is based on the difficulty to solve the discrete log problem in the group of $\mathbb{F}_q$-rational points. The algorithm in Figure 2 describes the signature procedure of ECDSA, and the algorithm in Figure 3 illustrates the verification procedure. We assume that both parties have agreed on a hash function h, where we recall from [3] that a hash function $h : S \to T$ is a function that is

1. *Pre-image resistant*, in the sense that for almost all $t \in T$ it is computationally infeasible to find $s \in S$ such that $h(s) = t$;

2. *Second pre-image resistant*, in the sense that for any $s_1 \in S$ it is computationally infeasible to find $s_2 \in S$ such that $h(s_1) = h(s_2)$; and

3. *Collusion resistant*, in the sense that it is computationally infeasible to find distinct $s_1, s_2 \in S$ such that $h(s_1) = h(s_2)$.

It is important to note that the algorithms we present are not ready for use as-is. For instance, in the key generation algorithm we allow $p_A = 1$, which is clearly not desirable. A comprehensive specification can be obtained from the ANSI X9.62 standard [1].

```
GenerateKey($D$)
Input: The domain parameters $D$.
Output: A private key $p_A$ and a public key $P_A$.

1.  select a random integer $p_A \in [1, l-1]$
2.  $P_A \leftarrow [p_A]P$
3.  return $p_A$ and $P_A$
```

Figure 1: ECC key generation

```
SignatureECDSA($D, h, p_A, m$)
Input: The domain parameters $D$, a hash function $h$, the sender's private key $p_A$, and
a message $m$.
Output: A signature $(r, s)$ on the message $m$.

1.  select a random integer $k \in [1, l-1]$
2.  $(x_1, y_1) \leftarrow [k]P$
3.  $r \leftarrow x_1 \mod l$
4.  if $r = 0$ then go to step 1
5.  $s \leftarrow k^{-1}(h(m) + p_A r)) \mod l$
6.  if $s = 0$ then go to step 1
7.  return $(r, s)$
```

Figure 2: ECDSA signature

```
VerificationECDSA$(D, h, P_A, m, (r, s))$
Input: The domain parameters $D$, a hash function $h$, the sender's public key $P_A$, a message $m$, and a signature $(r, s)$ on $m$.
Output: true if $(r, s)$ is a valid signature of $m$, false otherwise.

if $r, s \notin [1, l-1]$ then return false
$(x_1, y_1) \leftarrow [h(m)s^{-1}]P \oplus [rs^{-1}]P_A$
if $x_1 \equiv r \pmod{l}$ then return true
return false
```

Figure 3: ECDSA verification

The verification algorithm return the correct resolution, as can be verified by

$$\begin{aligned}(x_1, y_1) &= [h(m)s^{-1}]P \oplus [rs^{-1}]P_A = \left[\tfrac{h(m)k}{h(m)+p_A r}\right] P \oplus \left[\tfrac{rk}{h(m)+p_A r}\right] P_A \\ &= \left[\tfrac{h(m)k}{h(m)+p_A r}\right] P \oplus \left[\tfrac{p_A rk}{h(m)+p_A r}\right] P = \left[\tfrac{k(h(m)+p_A r)}{h(m)+p_A r}\right] P = [k]P\ ,\end{aligned}$$

as needed.

3 Arithmetic of Elliptic Curves

In this section we examine properties of elliptic curves that are essential in the development of the SEA algorithm. Our first step is to introduce a shorter form of the Weierstrass equation. To that end, we will define curve isomorphisms and survey some of their properties. Curve isomorphism and the scalar multiplication maps are special cases of curve isogenies, which we shall introduce next. Towards the end of this section, we will take a detour into the beautiful theory of complex analysis as a prelude to defining the division and modular polynomials. This will equip us with all the necessary tools before taking a stab at the SEA algorithm.

3.1 Isomorphism and short Weierstrass equations

Let K be a finite field and E/K be an elliptic curve with the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ . \tag{1}$$

We wish to associate to E two constants: the discriminant and the absolute invariant (also called the j-invariant). To that end, it is useful to introduce the following constants:

$$\begin{aligned} &b_2 = a_1^2 + 4a_2 \ , \quad b_4 = 2a_4 + a_1a_3 \ , \quad b_6 = a_3^2 + 4a_6 \ , \\ &b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 = (b_2b_6 - b_4^2)/4 \ , \\ &c_4 = b_2^2 - 24b_4 \ , \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \ . \end{aligned} \tag{3}$$

Then we have the following definition:

Definition 6. Let E be an elliptic curve with a Weierstrass equation (1). The *discriminant* of E is $\Delta_E = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$. If $\Delta_E = 0$ we say that E is *singular*. Otherwise, we define the *absolute invariant*, or *j-invariant*, of E to be $j(E) = j_E = c_4^3/\Delta_E$.

In the context of the SEA algorithm, we are particularly interested in fields of characteristic greater than 3. Note that by definition we have

$$\begin{aligned} c_4^3 &= b_2^6 - 72b_2^4b_4 + 1728b_2^2b_4^2 - 13824b_4^4 \ , \\ c_6^2 &= b_2^6 - 72b_2^4b_4 + 1296b_2^2b_4^2 + 432b_2^3b_6 - 15552b_2b_4b_6 + 46656b_6^2 \ . \end{aligned}$$

So when the field characteristic is prime to 6 we may divide by $2^6 3^3 = 1728$ and write

$$\Delta_E = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = \frac{c_4^3 - c_6^2}{1728} \ .$$

The definition of the j-invariant leads us to the closely related notion of elliptic curve isomorphism. We shall call two curves isomorphic (over a certain field) if there is an admissible change of variables from one curve to the other. More specifically, we have

Definition 7. Let L be a field extension $K \subseteq L \subseteq \overline{K}$. Two elliptic curves E_1/K (with variables x_1 and y_1) and E_2/K (with variables x_2 and y_2) are said to be *isomorphic elliptic curves over L* (or *L-isomorphic*) if there exists an element $(r, s, t, u) \in L^3 \times L^*$, such that the change of variable maps

$$x_1 \mapsto u^2 x_2 + r \ , \qquad y_1 \mapsto u^3 y_2 + u^2 s x_2 + t \ , \qquad \mathcal{O}_1 \mapsto \mathcal{O}_2$$

transform E_1/K to E_2/K. Such transformations are called *admissible change of variables*, or *L-isomorphisms*. By convention, we take the transformation $\mathcal{O}_1 \mapsto \mathcal{O}_2$ for granted and do not mention it explicitly.

Note that these transformations are invertible with the inverse transformations being

$$\begin{aligned} &x_2 \mapsto \left(u^{-1}\right)^2 x_1 + \left[-\left(u^{-1}\right)^2 r\right] \quad \text{and} \\ &y_2 \mapsto \left(u^{-1}\right)^3 y_1 + \left(u^{-1}\right)^2 \left[u^{-1} s\right] x_1 + \left[\left(u^{-1}\right)^3 (sr - t)\right] \ . \end{aligned}$$

Thus, we have shown that isomorphism of curves is a symmetric relation. Furthermore, it is also a transitive relation: suppose we have $(r_1, s_1, t_1, u_1), (r_2, s_2, t_2, u_2) \in K^3 \times K^*$, such that the change of variable maps

$$x_i \mapsto u_i^2 x_{i+1} + r \qquad \text{and} \qquad y_i \mapsto u_i^3 y_{i+1} + u_i^2 s_i x_{i+1} + t_i$$

transform E_i/K to E_{i+1}/K, $i = 1, 2$. Then

$$\begin{aligned} &x_1 = (u_1 u_2)^2 x_3 + \left[u_1^2 r_2 + r_1\right] \quad \text{and} \\ &y_1 = (u_1 u_2)^3 y_3 + (u_1 u_2)^2 \left[u_1 s_2 + s_1\right] x_3 + \left[u_1^3 t_2 + u_1^2 s_1 r_2 + t_1\right] \end{aligned}$$

transform E_1/K to E_3/K. Since reflexivity is trivial, we have established that isomorphism of curves is an equivalence relation.

Before we continue with more results regarding elliptic curve isomorphism, we find the next detour beneficial. Recall the Weierstrass equation

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ . \tag{1}$$

It is desirable to transform this equation to a simpler form. This is admissible using elliptic curve isomorphisms, as defined in Definition 7. The final form, however, depends on the characteristic of the underlying field K. The following lemma deals with the case of $\mathrm{char}(K) = p > 3$. There exist similar statements for the cases $p = 2$ and $p = 3$, but since the `SEA` algorithm is mostly used over large prime fields, the following suffices to our purpose.

Lemma 1. *Let K be a finite field with $\mathrm{char}\, K = p > 3$, and let E/K be an elliptic curve with a Weierstrass equation given in* (1)*. There exists an K-isomorphic curve E'/K (in variables x' and y') to E with the following short Weierstrass equation*

$$E' : (y')^2 = (x')^3 + \tilde{a}_4 x' + \tilde{a}_6 \ ,$$

where the coefficients $\tilde{a}_4$ and $\tilde{a}_6$ are in K.

Proof. Consider the following transformation:

$$x \mapsto x' - \left(\frac{a_1^2 + 4a_2}{12}\right) , \qquad y \mapsto y' - \left(\frac{a_1}{2}\right) x' + \left(\frac{a_1^3 + 4a_1a_2 - 12a_3}{24}\right) .$$

Then the Weierstrass equation of E' becomes

$$(y')^2 = (x')^3 - \left(\frac{a_1^4 + 8a_1^2a_2 - 24a_1a_3 + 16a_2^2 - 48a_4}{48}\right) x' + \left(\frac{a_1^6 + 12a_1^4a_2 - 36a_1^3a_3}{864}\right)$$
$$+ \left(\frac{48a_1^2a_2^2 - 72a_1^2a_4 - 144a_1a_2a_3 + 64a_2^3 - 288a_2a_4 + 216a_3^2 + 864a_6}{864}\right) ,$$

as needed. □

For simplicity, we shall immediately change notation and write the short Weierstrass equation as

$$E : y^2 = x^3 + a_4x + a_6 . \tag{4}$$

Through the remainder of this paper, we will only treat elliptic curves in their short Weierstrass equation form. This form allows much simpler expressions for the discriminant, j-invariant, and group law associated with an elliptic curve. We start by writing the constants in Equation (3) in terms of the coefficients of the short Weierstrass equation:

$$\begin{aligned} &b_2 = 0 , \quad b_4 = 2a_4 , \quad b_6 = 4a_6 , \quad b_8 = -a_4^2 , \\ &c_4 = -48a_4 , \quad c_6 = -864a_6 . \end{aligned}$$

Consequently, the discriminant of E is $\Delta_E = -64a_4^3 - 432a_6^2$ and the j-invariant of E is

$$j_E = 1728 \left(\frac{4a_4^3}{4a_4^3 + 27a_6^2}\right) . \tag{5}$$

The group law of an elliptic curve given by a short Weierstrass equation becomes

$$\begin{aligned} -P_1 &= (x_1, -y_1) , \\ P_1 \oplus P_2 &= (x_3, y_3) = \left(\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1\right) \text{ , where} \\ \lambda &= \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } P_1 \neq \pm P_2 , \\[2ex] \dfrac{3x_1^2 + a_4}{2y_1} & \text{if } P_1 = P_2 . \end{cases} \end{aligned} \tag{6}$$

In addition, the only admissible changes of variables that preserve the short Weierstrass form are

$$x_1 \mapsto u^2x_2 \qquad \text{and} \qquad y_1 \mapsto u^3y_2$$

for some $u \in \overline{K}^*$.

We continue our discussion with more results related to elliptic curve isomorphism. The following important proposition shows that j-invariants of curves E/K classify the isomorphism classes over the algebraic closure $\overline{K}$.

Proposition 1. *Let E/K and E'/K be two elliptic curves. If E and E' are isomorphic over K then they have the same j-invariant. Conversely, if E and E' have the same j-invariants then the two curves are isomorphic over $\overline{K}$.*

Proof. We shall prove the theorem only for the case $\mathrm{char}(K) = p > 3$, which is the only case where the `SEA` algorithm is applied in practice. Let E/K be an elliptic curve given by the short Weierstrass equation

$$E/K : y_1^2 = x_1^3 + a_4 x_1 + a_6 \, .$$

Suppose that there exists a K-isomorphism given by $x_1 \mapsto u^2 x_2$ and $y_1 \mapsto u^3 y_2$, where $u \in K^*$, from E/K to an isomorphic elliptic curve

$$\tilde{E}/K : y_2^2 = x_2^3 + \tilde{a_4} x_2 + \tilde{a_6} \, .$$

Then one sees that $\tilde{a_4} = a_4/(u^4)$ and $\tilde{a_6} = a_6/(u^6)$. Consequently, we have $\tilde{c_4} = c_4/(u^4)$ and $\tilde{c_6} = c_6/(u^6)$. It follows that $\Delta_{\tilde{E}} = \Delta_E/(u^{12})$, so that the two curves have the same j-invariant, as needed.

Conversely, suppose the curve E/K and $\tilde{E}/K$ have the same j-invariant. That is, we have

$$1728 \left(\frac{4a_4^3}{4a_4^3 + 27a_6^2} \right) = 1728 \left(\frac{4\tilde{a_4}^3}{4\tilde{a_4}^3 + 27\tilde{a_6}^2} \right) \, .$$

Therefore, $a_4^3 \tilde{a_6}^2 = \tilde{a_4}^3 a_6^2$. We consider three cases:

1. $a_4 = 0$. Then since $\Delta_E \neq 0$ we must have $a_6 \neq 0$. It follows that $\tilde{a_4} = 0$ and $\tilde{a_6} \neq 0$. Let $u = (a_6/\tilde{a_6})^{1/6}$ and note that the admissible change of variables $x_1 \mapsto u^3 x_2$ and $y_1 \mapsto u^2 y_2$ takes E to $\tilde{E}$.

2. $a_6 = 0$. Then similar to before we have $a_4 \neq 0$, $\tilde{a_6} = 0$ and $\tilde{a_4} \neq 0$. Let $u = (a_4/\tilde{a_4})^{1/4}$ and again the admissible change of variables $x_1 \mapsto u^3 x_2$ and $y_1 \mapsto u^2 y_2$ takes E to $\tilde{E}$.

3. $a_4 a_6 \neq 0$. Then, also using $\Delta_{\tilde{E}} \neq 0$, we must have $\tilde{a_4}\tilde{a_6} \neq 0$. Let $u = (a_4/\tilde{a_4})^{1/4} = (a_6/\tilde{a_6})^{1/6}$, so the admissible change of variables $x_1 \mapsto u^3 x_2$ and $y_1 \mapsto u^2 y_2$ takes E to $\tilde{E}$.

This concludes the proof. □

In the context of ECC, the above definition of isomorphism over K of curves would have been of little significance if this isomorphism did not respect the group operation on the K-rational points. The following proposition establishes that if E/K and E'/K are isomorphic curves, then $E(K)$ and $E'(K)$ are indeed homomorphic as groups.

Proposition 2. *Let E/K and E'/K be K-isomorphic curves. Then the groups of K-rational points $E(K)$ and $E'(K)$ are homomorphic.*

Proof. We prove the proposition only for the case $\mathrm{char}(K) = p > 3$. Let

$$E : y^2 = x^3 + a_4 x + a_6 \qquad \text{and} \qquad \tilde{E} : \tilde{y}^2 = \tilde{x}^3 + \tilde{a_4}\tilde{x} + \tilde{a_6}$$

be K-isomorphic curves, where the isomorphism θ is given by $x \mapsto u^2\tilde{x}$ and $y \mapsto u^3\tilde{y}$ for some $u \in K^*$. By a slight abuse of notation, we overload θ and let it act on points on the curve E, as well as expressions involving the variables x and y. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two K-rational points of E. We clearly have

$$\theta(-P_1) = \theta(x_1, -y_1) = (u^2\tilde{x_1}, -u^3\tilde{y_1}) = -\theta(P_1)\ .$$

Define $\tilde{\lambda}$ for $\tilde{E}$ in analogous way to Equation (6). Then manipulating the expression for $\tilde{\lambda}$, we see that $\theta(\lambda) = u\tilde{\lambda}$, regardless of whether $P_1 = P_2$ or not. It follows that

$$\begin{aligned} \theta(P_1 \oplus P_2) &= \theta\left(\lambda^2 - x_1 - x_2\ , \lambda\left(2x_1 + x_2 - \lambda^2\right) - y_1\right) \\ &= \left(u^2\left[\left(\tilde{\lambda}\right)^2 - \tilde{x_1} - \tilde{x_2}\right]\ , u^3\left[\tilde{\lambda}\left(2\tilde{x_1} + \tilde{x_2} - \left(\tilde{\lambda}\right)^2\right) - \tilde{y_1}\right]\right) \\ &= \theta(P_1) \oplus \theta(P_2)\ . \end{aligned}$$

This proves the proposition. □

3.2 Isogenies

In Proposition 2 we showed that K-isomorphic curves have homomorphic groups of K-rational points. However, isomorphism of elliptic curves is a much more restrictive notion than homomorphism of the respective groups of K-rational points. In this section we define isogenies and survey some of their properties, not the least of which is preserving the group structure of the K-rational points. Given the rich theory in which isogenies arise, we only state basic results in this section and do not provide proofs. An excellent introduction to isogenies, focusing on elliptic curves, is Silverman [20]. More information can be found in Cassels' study [7].

We start with a few definitions.

Definition 8. Let E/K and E'/K be two elliptic curves.

1. A *morphism* from E to E' is a rational map with coefficients in K which is regular at every point of E.

2. An *isogeny* from E to E' is a morphism $\psi : E \to E'$ that is (i) a nonconstant morphism mapping $\mathcal{O}_E$ to $\mathcal{O}_{E'}$, or (ii) the zero-morphism $P \mapsto \mathcal{O}_{E'}$ for all $P \in E$. Two elliptic curves E/K and E'/K are said to be *isogenous* if such an isogeny $\psi : E \to E'$ exists. The *degree* of an isogeny ψ is the cardinality of its kernel.

3. An isogeny ψ from E to itself is called an *endomorphism* of E. The set of all endomorphism of E is denoted by $\mathrm{End}_K(E)$, or simply $\mathrm{End}(E)$ when the field is understood from the context.

In fact, the notion of an isogeny is not new to us; curve isomorphisms are the simplest type of isogenies between curves, and the scalar multiplication maps we saw in Definition 3 are isogenies from a curve to itself. However, the theory of general isogenies is deeper, owing much of its beauty to the following observation: if ψ is an isogeny of curves from E_1/K to E_2/K, then it induces an injection of function fields $\psi^* : \overline{K}(E_2) \hookrightarrow \overline{K}(E_1)$. The degree of ψ—as well as the definition of whether ψ is separable, inseparable, or purely inseparable—are determined by the field extension $\overline{K}(E_1)/\psi^*\overline{K}(E_2)$. This observation leads to the following important theorem:

Theorem 1. *Let E/K and E'/K be isogenous elliptic curves over K under the isogeny ψ. Then ψ is a group homomorphism from $E(K)$ to $E'(K)$.*

Proof. See [20, pages 75–76]. □

Like curve isomorphism, curve isogeny is also an equivalence relation. We don't provide the details here, but only state that the symmetric property is given by the so-called dual isogeny. This and other basic properties of isogenies are given in the next proposition.

Proposition 3. *Let $\psi : E_1/K \to E_2/K$ be a non-constant isogeny of degree m.*

1. *For every $P \in E_2$, we have $|\psi^{-1}(P)| = \deg_s \psi$, where $\deg_s \psi$ is the separable degree of ψ.*

2. *There is a unique dual isogeny $\hat{\psi} : E_2/K \to E_1/K$ such that $\hat{\psi} \circ \psi = [m]$ on E_1 and $\psi \circ \hat{\psi} = [m]$ on E_2. Here, $\circ$ is the composition of morphisms operation. We extend this to the case that ψ is the constant (zero) isogeny by taking $\hat{\psi}$ to also be the constant isogeny.*

3. $\deg \psi = \deg \hat{\psi}$.

Let n be an integer

4. *The degree of the endomorphism $[n]$ is n^2.*

5. *Suppose $n \neq 0$ and n is prime to $\mathrm{char}(K)$. Then $[n]$ is a separable endomorphism.*

Proof. See [20, pages 76–77, 83, 86–87]. □

Another important property that holds in general for all abelian varieties (and thus also specifically for elliptic curves) is that the number of K-rational points characterizes the isogeny equivalence classes.

Proposition 4. *Let E/K and E'/K be two elliptic curves defined over a finite field. Then E and E' are isogenous over K if and only if $|E(K)| = |E'(K)|$.*

Proof. See [7, pages 242–243]. □

3.3 Frobenius endomorphism

Let E/K be an elliptic curve. We saw that the scalar multiplication maps $[n]$ on E are endomorphisms. If we endow the set $\mathrm{End}_K(E)$ with an addition $+$ defined by $(\phi + \psi)(P) = \phi(P) \oplus \psi(P)$ for all $\phi, \psi \in \mathrm{End}_K(E)$, then we see that $\mathrm{End}_K(E)$ is in fact a ring. Thus, we have $\mathbb{Z} \subseteq \mathrm{End}_K(E)$, where the inclusion is of subrings. If the inclusion is strict, then we say that E has complex multiplication. It turns out that this is always the case when the underlying field K is finite, as Theorem 2 shows.

Before we state and prove Theorem 2, we need to distinguish between two types of curves: supersingular and ordinary (or non-supersingular). Recall that the goal of the `SEA` algorithm is to determine the number of $\mathbb{F}_p$-rational points $|E(\mathbb{F}_p)|$, where $\mathbb{F}_p$ is prime field with a characteristic $p > 3$. We define supersingular curves over $\mathbb{F}_p$ to be curves for which $|E(\mathbb{F}_p)| = p + 1$. Clearly, this definition means that we shall mainly be concerned with ordinary curves in this paper. It is important to note that this is not the usual treatment in the literature, where supersingular curves are defined as those satisfying one of the cases in Proposition 5 and our definition arises as a property of those curves.

Theorem 2. *Let $E/\mathbb{F}_p$ be a non-supersingular curve, where $\mathbb{F}_p$ is a prime field of characteristic $p > 3$. Define*

$$\begin{aligned} \phi_p : E(\overline{\mathbb{F}}_p) &\to \{\overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p\} \cup \mathcal{O} \\ (x, y) &\mapsto (x^p, y^p) \\ \mathcal{O} &\mapsto \mathcal{O}\,. \end{aligned}$$

Then ϕ_p is an endomorphism and is different from $[n]$ for all integers n.

Proof. Suppose $E/\mathbb{F}_p$ is given by the short Weierstrass equation $y^2 = x^3 + a_4 x + a_6$. Then, recalling that $a_4, a_6 \in \mathbb{F}_p$, we have

$$\begin{aligned} (y^p)^2 = \left(y^2\right)^p = \left(x^3 + a_4 x + a_6\right)^p &= \left(x^3\right)^p + a_4^p\,(x^p) + a_6^p \\ &= (x^p)^3 + a_4\,(x^p) + a_6\,. \end{aligned}$$

Thus, (x^p, y^p) satisfies the Weierstrass equation of E, so ϕ_p is an endomorphism.

Suppose toward a contradiction that $\phi_p = [n]$ for some integer n. By definition of ϕ_p, we can immediately dismiss the case $n = 0$. From Proposition 3(1), $\deg_s \phi_p = |\phi_p^{-1}(\mathcal{O})| = |\{\mathcal{O}\}| = 1$, so ϕ_p is purely inseparable. It can be shown (see [20, page 30]) that this implies that $\deg \phi_p = p$. But then we immediately see from Proposition 3(4) that $\phi_p \neq [n]$ for any integer n, as needed. □

Definition 9. Let $E/\mathbb{F}_p$ be a non-supersingular curve. We call ϕ_p in Theorem 2 the *Frobenius endomorphism.*

The Frobenius endomorphism is critical to the development of Schoof's algorithm, and we shall revisit it many times throughout this paper. We now turn to a closer examination of the other endomorphisms of a curve: the scalar multiplication maps.

3.4 Torsion points

Recall the scalar multiplication maps in Definition 3. We now introduce the kernel, or torsion group, of scalar multiplications in the following definition.

Definition 10. Let E/K be an elliptic curve and n an integer. The *kernel of* $[n]$, denoted $E[n]$ satisfies $E[n] = \{P \in E(\overline{K}) \mid [n]P = \mathcal{O}\}$. An element $P \in E[n]$ is called an *n-torsion point.*

The kernels of scalar multiplications are used extensively in the development of Schoof's algorithm. The following proposition shows that these groups are of very simple forms.

Proposition 5. *Let $E/\mathbb{F}_p$ be an elliptic curve over a prime field of characteristic $p > 3$. Let n an integer. If p is prime to n then*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\,.$$

Otherwise, if $n = p^r$, then either

$$E[p^r] = \{\mathcal{O}\},\ \textit{for all } r \geq 1 \qquad \textit{or} \qquad E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z},\ \textit{for all } r \geq 1\,.$$

Proof. Suppose first that p is prime to n. From Proposition 3, we know that $|E[n]| = |[n]^{-1}(\mathcal{O})| = \deg_s[n] = \deg[n] = n^2$. Furthermore, for any integer d dividing n we have $|E[d]| = d^2$. Let $n = p_1^{e1} \cdots p_k^{ek}$ be the prime factorization of n. Then on the one hand $E[p_i^{e_i}]$ does not contain any element of order greater than $p_i^{e_i}$. On the other hand, it must contain an element of order $p_i^{e_i}$ or else $|E[p_i^c]| > (p_i^c)^2$ for some $c < e_i$. It follows that $E[p_i^{e_i}] \cong \mathbb{Z}/(p_i^{e_i})\mathbb{Z} \times \mathbb{Z}/(p_i^{e_i})\mathbb{Z}$. It follows immediately that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Now suppose $n = p^r$. Let ϕ_p be the Frobenius endomorphism. Then from Proposition 3, and since we already showed that ϕ_p is purely inseparable,

$$|E[p^r]| = \deg_s[p^r] = (\deg_s(\hat{\phi_p} \circ \phi_p))^r = (\deg_s \hat{\phi_p})^r\,.$$

We also know from the same proposition and the proof of Theorem 2 that $\deg \hat{\phi}_p = \deg \phi_p = p$. It follows that we need to consider two cases: $\deg_s \hat{\phi}_p = 1$ and $\deg_s \hat{\phi}_p = p$. In the first case, $|E[p^r]| = 1$ for all r, implying that $E[p^r] = \{\mathcal{O}\}$. In the second case, $|E[p^r]| = p^r$ for all r, which clearly means that $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$. This completes the proof of the proposition. □

The standard way of introducing supersingular curves over a prime field of characteristic p is defining them to be those for which the only p-torsion point is the point of infinity. Since the groups of rational points for these curves have known cardinalities (*i.e.*, $p+1$), we shall focus our interest on ordinary curves, instead.

A consequence of Proposition 5 is the next corollary, which will be instrumental in Atkin's and Elkies' improvements to Schoof's algorithm.

Corollary 1. *Let E be an elliptic curve over a prime field $\mathbb{F}_p$ of characteristic $p > 3$. Let $l < p$ a prime. Then $E[l] \cong \mathbb{F}_l \times \mathbb{F}_l$, and $E[l]$ has exactly $l+1$ cyclic subgroups C_i of order l, where $1 \leq i \leq l+1$.*

Proof. The first statement is just Proposition 5, for the case $n = l < p$ a prime. Therefore, we know that $E[l]$ is generated by two points P_1 and P_2, and that $|\langle P_1 \rangle| = |\langle P_2 \rangle| = l$. For $i = 3, \ldots, l+1$ define $P_i = [i-2]P_1 \oplus P_2$, and note that we necessarily have $P_i \neq \mathcal{O}$.

We claim that the $l+1$ cyclic subgroups C_i are precisely the $\langle P_i \rangle$ we defined. First, note that $[l]P_i = [i-2][l]P_1 \oplus [l]P_2 = \mathcal{O}$. Since l is a prime, it follows that $|\langle P_i \rangle| = l$. Next, we show that $\langle P_i \rangle \neq \langle P_j \rangle$ for $i \neq j$. Clearly, this is the case if $i = 1$. Let $i, j > 1$ and suppose $P_i = [m]P_j$ for some m. Then,

$$[i-2]P_1 \oplus [-m][j-2]P_1 = [m-1]P_j \ ,$$

and it follows that $m = 1$ and $i = j$, to prove that the groups are pairwise different. Since the groups are all of prime order, they intersect trivially, and a counting argument shows that we have all of them. □

3.5 Detour into complex analysis

The theory of elliptic curves is exceptionally rich over the complex field. In this section we state a few fundamental complex-analytic results. The theory relies on the observation that an elliptic curve corresponds uniquely to a lattice in the complex field (and thus, equivalently, to a torus). A moderately comprehensive development of the theory can be found in Silverman [20], from which we take a few important results.

Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, where $\omega_1, \omega_2 \in \mathbb{C}$ are $\mathbb{R}$-linearly independent, be a lattice. We define the Weierstrass $\wp$-function corresponding to Λ.

Definition 11. Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function (relative to Λ) is defined by the series

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \, . \tag{7}$$

For simplicity we write $\wp(z)$ in place of $\wp(z;\Lambda)$ when the lattice has been fixed.

It can be shown (see [20, pages 153–154]) that a Weierstrass $\wp$-function relative to $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ is a doubly periodic function with periods ω_1 and ω_2, which we call the basis of Λ. Clearly, the choice of a basis in not unique (for instance, $\omega_1' = \omega_1 + \omega_2$ and $\omega_2' = \omega_2$ will do), and one can choose, as is conventional, ω_1 and ω_2 such that $\tau = \omega_1/\omega_2$ lies in the upper half-plane $\mathcal{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ of the complex plane. We call such a basis *homogeneous.* The following lemma states that the homogeneous bases are characterized by elements of $\mathrm{SL}_2(\mathbb{Z})$.

Lemma 2. *Let Λ be a lattice with a homogeneous basis $\Omega = \{\omega_1, \omega_2\}$. Then for any transformation $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, the action of σ on Ω by a linear fractional transformation yields another homogeneous basis of Λ. Conversely, if Ω_1 and Ω_2 are two homogeneous bases of Λ then there exists a transformation $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ such that the action of σ on Ω_1 results in Ω_2.*

Proof. See [12, pages 29–30]. □

The next important theorem establishes a bijection between points on an elliptic curve over the complex field and points on the complex plain modulo a suitable lattice Λ.

Theorem 3. *Let $E/\mathbb{C}$ be an elliptic curve given by a Weierstrass equation* (1) *over the complex field. There exists a lattice $\Lambda \subset \mathbb{C}$ such that the map*

$$\begin{aligned} \mathbb{C}/\Lambda &\to E \\ z + \Lambda &\mapsto \begin{cases} (x_\Lambda, (\wp'(z) - a_1 x_\Lambda - a_3)/2) \ , & z \notin \Lambda \, , \\ \mathcal{O} \, , & z \in \Lambda \, , \end{cases} \end{aligned}$$

where $x_\Lambda = \wp(z) - b_2/12$, is a bijection. Conversely, given a lattice Λ, there exists a unique curve $E/\mathbb{C}$ such that the map above exists.

Proof. See [20, page 161]. □

A special case of Theorem 3 is when $E : y^2 = x^3 + a_4 x + a_6$. Then we have

$$z + \Lambda \mapsto (\wp(z), \wp'(z)/2) \, , \quad z \notin \Lambda \, .$$

In such a case, the coefficients of the short Weierstrass equation are $a_4 = -g_2/\sqrt[3]{4}$ and $a_6 = -g_3$, where

$$g_2 = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}\,, \qquad\qquad g_3 = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}\,.$$

Let $\Lambda \subset \mathbb{C}$ be a lattice with homogenous basis $\{\omega_1, \omega_2\}$ such that $\tau = \omega_1/\omega_2 \in \mathcal{H}$. Theorem 3 associates to Λ a curve $E/\mathbb{C}$, which we will denote by E_Λ. Let $q = e^{2\pi i \tau} \in \mathbb{C}$ and define $j(q)$ to be the j-invariant of E_Λ. Recall that j-invariants classify isomorphism classes over $\mathbb{C}$ (we showed this in Proposition 1 for the closure of a finite field $\overline{K}$, but the result holds in general). Note that if $\Lambda' \subset \mathbb{C}$ is a lattice with the homogenous basis $\{c\omega_1, c\omega_2\}$ for some nonzero $c \in \mathbb{C}$, then $(c\omega_1)/(c\omega_2) = \omega_1/\omega_2 = \tau$. Therefore, we would expect the elliptic curves corresponding to Λ and Λ' to be isomorphic. The following proposition ensures that this is indeed the case. It also plays a role in the `SEA` algorithm when we discuss how to construct a special polynomial from a kernel of an isogeny.

Proposition 6. *Let $\Lambda, \Lambda' \subset \mathbb{C}$ be two lattices. The elliptic curves corresponding to Λ and Λ' are isomorphic if and only if $\Lambda = c\Lambda'$ for some nonzero $c \in \mathbb{C}$.*

Proof. See [20, page 161]. □

For any $\tau \in \mathcal{H}$, we define the following lattice: $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$. A direct consequence of Proposition 6 is that for any lattice $\Lambda \subset \mathbb{C}$ we can find a nonzero $c \in \mathbb{C}$ such that $c\Lambda = \Lambda_\tau$ for some $\tau \in \mathcal{H}$. In Proposition 7 we will improve this result even further, but first we would like to motivate the discussion by recalling the j-invariants of curves.

In the discussion above, we defined $j(q)$ indirectly, in terms of the corresponding elliptic curve E. It turns out we can define $j(q)$ directly in terms of q. Such a procedure would be well-defined only if we can show that $j(q)$ is independent of the choice of $\tau = \omega_1/\omega_2$. From Lemma 2 we know that it suffices to show that for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, we have $j(q) = j(q_\sigma)$ where $q_\sigma = e^{2\pi i \sigma\{\omega_1, \omega_2\}}$. The proposition below uses this fact to show that we can pick τ in the standard fundamental region $\mathcal{F} = \{\tau \in \mathbb{C} \mid \Im(\tau) > 0, -1/2 \le \Re(\tau) < 1/2, |\tau| \ge 1\}$.

Proposition 7. *Let $\Lambda \subset \mathbb{C}$ be a lattice. Then there exists a nonzero $c \in \mathbb{C}$ such that $c\Lambda = \Lambda_\tau$ for some $\tau \in \mathcal{F}$.*

Proof. See [20, page 343]. □

We now show how to define $j(q)$ directly. To that end, let $\mathbb{Z}[\![q]\!]$ be the ring of formal power series over the integers in the variable q. Define in $\mathbb{Z}[\![q]\!]$ the following series:

$$E_2(q) = 1 - 24\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n}\ , \qquad E_4(q) = 1 + 240\sum_{n=1}^{\infty} \frac{n^3q^n}{1-q^n}\ ,$$
$$E_6(q) = 1 - 504\sum_{n=1}^{\infty} \frac{n^5q^n}{1-q^n}\ .$$

We define two more formal power series, this time in $\mathbb{Z}[\zeta, \frac{1}{\zeta(1-\zeta)}][\![q]\!]$:

$$x(\zeta;q) = \frac{1}{12} - 2\sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} + \sum_{n\in\mathbb{Z}} \frac{\zeta q^n}{(1-\zeta q^n)^2}\ ,$$
$$y(\zeta;q) = \frac{1}{2}\sum_{n\in\mathbb{Z}} \frac{\zeta q^n(1+\zeta q^n)}{(1-\zeta q^n)^3}\ .$$

Then with the above power series, the following proposition can be established:

Proposition 8. *The following equalities of power series hold:*

$$y^2 = x^3 - \frac{E_4(q)}{48}x + \frac{E_6(q)}{864}\ , \tag{8}$$
$$p_1 = \sum_{\zeta\in\mu_l, \zeta\neq 1} x(\zeta;q) = \frac{1}{12}l\left(E_2(q) - lE_2(q^l)\right)\ , \tag{9}$$

where $x = x(\zeta;q)$, $y = y(\zeta;q)$, and μ_l is the set of complex l-th roots of unity.

Proof. See [19, page 245]. □

Schoof (in [19] and further examined by others in [6]) notes that $E_4(q)$ and $E_6(q)$ are integers in some number field K, with a ring of integers $\mathcal{O}_K$. Furthermore, $\mathcal{O}_K$ contains a prime ideal $\mathfrak{B}$ with residue field $\mathbb{F}_p$ such that $E_4(q)$ and $E_6(q)$ modulo $\mathfrak{B}$ are elements of $\mathbb{F}_p$.

Let $E/\mathbb{C}$ be an elliptic curve with a j-invariant $j_E \notin \{0, 1728\}$. In Equation (4) we introduced the short Weierstrass equation of an elliptic curve over a field of prime characteristic greater than 3. Later, in Equation (5), we derived the j-invariant of such a curve. Both of these results also hold for fields of characteristic zero, such as the complex field. Thus, we can assume E is given by the short Weierstrass equation (4). Equation (8) establishes that

$$E_4(q) \equiv -48a_4 \pmod{\mathfrak{B}} \qquad \text{and} \qquad E_6(q) \equiv 864a_6 \pmod{\mathfrak{B}} \tag{10}$$

Thus, if we substitute the value q associated with an elliptic curve E into the formal series

$$j(q) = 1728\left(\frac{E_4(q)^3}{E_4(q)^3 - E_6(q)^2}\right) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots\ , \tag{11}$$

then the resultant value is the j-invariant j_E.

3.6 Division polynomials

Through the remainder of this section, let p a prime greater than 3.

Consider an elliptic curve $E/\mathbb{F}_p$ over a prime field of characteristic p. We wish to associate to this curve a set of multivariate polynomials and a related set of univariate polynomials, both called division polynomials. These polynomials arise from the complex analytic structure that we explored in the previous section. We present two important results in this section. The first is that the nontrivial torsion points are precisely the roots of corresponding division polynomials, as we shall see in Theorem 4. The second result we discuss in this section is Theorem 5, where we find that the division polynomials are intimately related to the scalar multiplications endomorphisms. Both of these results will be used in Schoof's algorithm.

Definition 12. Let $E/\mathbb{F}_p$ be an elliptic curve given by a short Weierstrass equation (4). Define recursively the *m-th division polynomial* $\psi_m \in \mathbb{F}_p[x, y]$ as

$$\begin{aligned}
\psi_0 &= 0\,,\\
\psi_1 &= 1\,,\\
\psi_2 &= 2y\,,\\
\psi_3 &= 3x^4 + 6a_4x^2 + 12a_6x - a_4^2\,,\\
\psi_4 &= 4y\left(x^6 + 5a_4x^4 + 20a_6x^3 - 5a_4^2x^2 - 4a_4a_6x - 8a_6^2 - a_4^3\right)\,,\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3\,, \quad m \geq 2\,,\\
\psi_{2m} &= \frac{\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right)\psi_m}{2y}\,, \quad m > 2\,.
\end{aligned}$$

where for simplicity we suppress the arguments of ψ_m.

First, we claim that the numerator of ψ_{2m}, where $m > 2$, is divisible by $4y^2$. Thus, in particular the numerator is divisible by the denominator $2y$, so the definition of ψ_{2m} makes sense. We have

$$\begin{aligned}
\psi_6 &= \frac{(\psi_5\psi_2^2 - \psi_1\psi_4^2)\psi_3}{4y^2}\\
&= \frac{4y^2\left(\psi_5 - 4\left(x^6 + 5a_4x^4 + 20a_6x^3 - 5a_4^2x^2 - 4a_4a_6x - 8a_6^2 - a_4^3\right)^2\right)\psi_3}{4y^2}\,,
\end{aligned}$$

so the claim holds in this case. If m is even, then so are $m+2$ and $m-2$. Otherwise, m is odd, so both $m-1$ and $m+1$ are even. It follows by induction that regardless of whether m is even or odd, the numerator of ψ_{2m} is divisible by $4y^2$, and the claim follows.

The evaluation of ψ_m is always taken at points on the curve. Therefore, we may write the division polynomials modulo the Weierstrass equation of the elliptic curve. In particular, it follows that the degree of ψ_m in y is never greater than one.

Furthermore, we already know that ψ_{2m} is divisible by $2y$. This observation gives rise to the first statement in the following important theorem, which ties the m-th division polynomial with the subgroup of m-torsion points $E[m]$.

Theorem 4. *Let m be a nonnegative integer. Define a polynomial f_m in the polynomial ring $\mathbb{F}_p[x, y]$ as follows:*

$$f_m(x, y) = \begin{cases} \psi_m(x, y) & m \text{ odd,} \\ \psi_m(x, y)/2y & m \text{ even.} \end{cases}$$

1. *f_m depends only on x.*
2. *The degree of f_m in x is at most $(m^2-1)/2$ if m is odd, and at most $(m^2-4)/2$ if m is even. The degrees are exact if p does not divide m for an odd m, or $m/2$ for an even m.*
3. *Let $P \neq \mathcal{O}$ be a point on the elliptic curve $E/\mathbb{F}_p$ such that $[2]P \neq \mathcal{O}$, and let $m \geq 1$. Then $P = (x, y) \in E[m]$ if and only if $f_m(x) = 0$.*
4. *If m is an odd prime not equal to p, then f_m has no other root in any extension of $\mathbb{F}_l$.*

Proof. We already know that ψ_{2m} is divisible by $2y$, so that the definition of f_m makes sense. We now prove that f_m depends only on x by induction. This clearly holds for $0 \leq m \leq 4$. We have $f_{2k+1} = \psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3$. It follows that

$$f_{2k+1} = \begin{cases} f_{k+2}f_k^3 - 16(x^3 + a_4x + a_6)^2 f_{k-1}f_{k+1}^3 & k \text{ is odd,} \\ 16(x^3 + a_4x + a_6)^2 f_{k+2}f_k^3 - f_{k-1}f_{k+1}^3 & k \text{ is even.} \end{cases}$$

In addition,

$$f_{2k} = \frac{\psi_{2k}}{2y} = \frac{(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2)\psi_k}{4y^2} = (f_{k+2}f_{k-1}^2 - f_{k-2}f_{k+1}^2)f_k\ ,$$

regardless of whether k is odd or even. By induction, f_m depends only on x, to prove the first statement. By abuse of notation, we will consider f_m as a univariate polynomial in the ring $\mathbb{F}_p[x]$.

The second and third statements follow from the way the division polynomials are introduced in the context of a complex plane modulo a suitable lattice. See Lang [11, pages 33–34] for more details.

If m a prime not equal to p, then by Proposition 5 there are $m^2 - 1$ nontrivial m-torsion points. If we further assume that m is odd, then there are $(m^2 - 1)/2$ different x-coordinates of the nontrivial m-torsion points. Furthermore, from the second statement, the degree of f_m is also $(m^2 - 1)/2$. The last statement of the theorem follows immediately. □

We now proceed to proving the second important result of this section. We show that the scalar multiplication endomorphisms can be expressed in terms of the division polynomials.

Theorem 5. *Let $E/\mathbb{F}_p$ be an elliptic curve. Let m be a positive integer and $P = (x, y) \in E(\overline{\mathbb{F}}_p)$ a point with $[m]P \neq \mathcal{O}$. Then*

$$[m]P = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y\psi_m^3} \right) . \tag{12}$$

Proof. We assume the curve is given by the short Weierstrass equation (4). There are two observations to be made here. The first is that under the equivalence we showed in Section 3.5 between curves and lattices in the complex plain, if $z \in \mathbb{C} \setminus \Lambda$ corresponds to a point $(\wp(z), \wp'(z)/2)$ on the curve of order not dividing m, then mz corresponds to a point $[m](\wp(z), \wp'(z)/2) = (\wp(mz), \wp'(mz)/2)$. This result holds whenever E is considered over a field of characteristic not equal to 2 or 3. With some squinting, this result seems plausible, and we refer the reader to Lang's [11] treatment for the necessary details.

The second observation, proven in [11, pages 34–36], is that for $u, v \in \mathbb{C}$ with $u - v \not\equiv 0 \pmod{\Lambda}$ we have

$$\wp(mz) = \wp(z) - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2} \quad \text{and} \quad \wp(u+v) - \wp(u-v) = -\frac{\wp'(u)\wp'(v)}{(\wp(u) - \wp(v))^2} .$$

Substituting $u = mz$ and $v = z$ (which is legal when P is not an m-torsion point) and rearranging, we find

$$\begin{aligned} \wp(z)\wp'(mz) &= -\Big(\wp\big((m+1)z\big) - \wp\big((m-1)z\big)\Big)\big(\wp(mz) - \wp(z)\big)^2 \\ &= \left(\frac{\psi_m\psi_{m+2}}{\psi_{m+1}^2} - \frac{\psi_{m-2}\psi_m}{\psi_{m-1}^2} \right) \left(\frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2} \right)^2 \\ &= \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{\psi_m^3} . \end{aligned}$$

From here the proof is immediate. If $P = (x, y) = (\wp(z), \wp'(z)/2)$ is a point such that $[m]P \neq \mathcal{O}$, then

$$[m]P = (\wp(mz), \wp'(mz)/2) = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y\psi_m^3} \right) ,$$

as needed. □

3.7 Modular polynomials

We conclude our survey of the arithmetic of elliptic curves by introducing the modular polynomials. These polynomials will be used extensively in our description of the Elkies and Atkin procedures.

Recall from the Section 3.5 that we can associate to each elliptic curve $E/\mathbb{C}$ an invariant $\tau \in \mathcal{F}$, unique up to isomorphism of curves. We also defined $q = e^{2\pi i \tau} \in \mathbb{C}$ and found that we can express the j-invariant of E in terms of a formal series $j(q)$. For simplicity, we change notation in this section from the previous one and define $j(\tau) = j_E$.

For any positive integer n, define

$$S_n^* = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| \, a, b, d \in \mathbb{Z}, 0 \leq b < d, ad = n, \gcd(a, b, d) = 1 \right\} .$$

For $\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in S_n^*$, we define the map

$$j \circ \alpha(\tau) = j\left(\frac{a\tau + b}{d}\right) .$$

Then, we can define the modular polynomials as follows:

Definition 13. Let n be a positive integer. Then the *n-th modular polynomial* is given by the equation

$$\Phi_n(x, j) = \prod_{\alpha \in S_n^*} (x - j \circ \alpha) .$$

The following lemma derives the relation between modular polynomials and isogenous elliptic curves over $\mathbb{C}$.

Lemma 3. *Let $E_1/\mathbb{C}$ and $E_2/\mathbb{C}$ be two elliptic curves with j-invariants j_{E_1} and j_{E_2}, respectively. Then $\Phi_n(j_{E_1}, j_{E_2}) = 0$ if and only if there is an isogeny from E_1 to E_2 whose kernel is cyclic of degree n.*

Proof. This is adopted from an exercise in [21, page 182]. □

The next theorem establishes an analogous statement for curves over finite fields. Its result is instrumental in Atkin's classification of primes. We shall also encounter this theorem in the context of constructing factors of divisional polynomials.

Theorem 6. *Let l be a prime, $\mathbb{F}_p$ be a finite field with $p \neq l$, and E an elliptic curve over $\mathbb{F}_p$. Then the $l+1$ zeros $\tilde{j} \in \overline{\mathbb{F}}_p$ of the polynomial $\Phi_l(x, j(E)) = 0$ are precisely the j-invariants of the isogenous curves $\tilde{E} = E/C$ with C one of the $l+1$ cyclic subgroups of $E[l]$.*

Proof. See [17, pages 44–46]. □

As has become customary with introductory texts to elliptic curve cryptography, we provide the modular polynomials for $l = 3$ and $l = 5$. The following are taken from [6] and the excellent SAGE code [22].

$$\begin{aligned}\Phi_3(x,y) = {}& x^4 - x^3y^3 + y^4\\ &+ 2232(x^3y^2 + x^2y^3)\\ &- 1069956(x^3y + xy^3)\\ &+ 36864000(x^3 + y^3)\\ &+ 2587918086x^2y^2\\ &+ 8900222976000(x^2y + xy^2)\\ &+ 452984832000000(x^2 + y^2)\\ &- 770845966336000000xy\\ &+ 1855425871872000000000(x + y)\ ,\end{aligned}$$

and

$$\begin{aligned}\Phi_5(x,y) = {}& x^6 - x^5y^5 + y^6\\ &+ 3720(x^5y^4 + x^4y^5)\\ &- 4550940(x^5y^3 + x^3y^5)\\ &+ 2028551200(x^5y^2 + x^2y^5)\\ &- 246683410950(x^5y + xy^5)\\ &+ 1963211489280(x^5 + y^5)\\ &+ 1665999364600x^4y^4\\ &+ 107878928185336800(x^4y^3 + x^3y^4)\\ &+ 383083609779811215375(x^4y^2 + x^2y^4)\\ &+ 128541798906828816384000(x^4y + xy^4)\\ &+ 1284733132841424456253440(x^4 + y^4)\\ &- 441206965512914835246100x^3y^3\\ &+ 26898488858380731577417728000(x^3y^2 + x^2y^3)\\ &- 192457934618928299655108231168000(x^3y + xy^3)\\ &+ 280244777828439527804321565297868800(x^3 + y^3)\\ &+ 5110941777552418083110765199360000x^2y^2\\ &+ 36554736583949629295706472332656640000(x^2y + xy^2)\\ &+ 6692500042627997708487149415015068467200(x^2 + y^2)\\ &- 264073457076620596259715790247978782949376xy\\ &+ 53274330803424425450420160273356509151232000(x + y)\\ &+ 141359947154721358697753474691071362751004672000\ .\end{aligned}$$

As is evident from these examples, the coefficient of the modular polynomials increase rapidly. Luckily, there exist other polynomials that satisfy similar properties as in Theorem 6. We will allude to this fact when we discuss the `SEA` algorithm.

4 SEA Algorithm

Throughout this section we assume that E is an elliptic curve of a prime field $\mathbb{F}_p$ of characteristic $p > 3$.

In Section 2.3 we showed that the security of an elliptic curve cryptosystem depends on the order of the group of rational points $E(\mathbb{F}_p)$. Therefore, it is of great interest to be able to determine the order of $E(\mathbb{F}_p)$ in an efficient manner. As discussed in [6], there are methods of constructing elliptic curves $E/\mathbb{F}_p$ for which the order of the group $E(\mathbb{F}_p)$ is easily determined. However, these methods impose additional structure on the curve. Thus, non-generic algorithms may leverage this additional structure in solving the DLP in this curves.

The Schoof-Elkies-Atkin (SEA) algorithm, however, does not assume any structural properties of the underlying elliptic curve, as long as it is an ordinary curve. Coupled with its efficient implementation over fields of large prime characteristic, the algorithm is the preferred method of determining the order of the group of rational points of an arbitrary elliptic curve [13].

In the following sections, we first present an important result by Hasse (which was later generalized by Weil) tying the order of $E(\mathbb{F}_p)$ to the one of $\mathbb{F}_p$. Next, we explain in some detail the original Schoof algorithm, in which we consider the trace of the Frobenius endomorphism (to be explained later) modulo different primes. This algorithm, while of polynomial complexity in the logarithm of the field characteristic, is still very slow in practice. We then turn our attention to Atkin's and Elkies' improvements to the algorithm, which resulted in a very practical running time. The first result, due to Atkin, is the classification of different primes into two groups: Atkin primes and Elkies primes. In the case of Atkin primes, further analysis of the Frobenius endomorphism as an element of $\mathrm{PGL}_2(\mathbb{F}_l)$ would prove useful. In the case of Elkies primes, we will be able to invoke complex analytic results to help us compute the group order.

4.1 Schoof's algorithm

Consider an elliptic curve E over $\mathbb{F}_p$. The following theorem, proven by Hasse, states that the number of $\mathbb{F}_p$-rational points of E is roughly equal to the number of elements in the field $\mathbb{F}_p$ plus one. There is an intuitive reasoning explaining this result: each of the p possible values of x gives rise to two values of y if $x^3 + a_4x + a_6$ is a square, and no value of y if it is not a square. Assuming that the distribution of the possible $x^3 + a_4x + a_6$ values is nearly "uniform," we would expect half of these values to be squares. We add to this number the point of infinity, which is by definition rational, to arrive at the expected number of $p + 1$ rational points.

Theorem 7 (Hasse)**.** *Let E be an elliptic curve defined over $\mathbb{F}_p$. Then*

$$|E(\mathbb{F}_p)| = p + 1 - t\,, \tag{13}$$

where $|t| \leq 2\sqrt{p}$.

Proof. See [20, page 131]. □

The error term t is intimately related to the Frobenius endomorphism described in Theorem 2. The missing link is the characteristic polynomial which we define next.

Definition 14. Let ϕ_p be the Frobenius endomorphism as in Theorem 2. We call the polynomial

$$\chi(T) = T^2 + tT + p$$

the *characteristic polynomial of the Frobenius endomorphism*, where t is the error term, also called the *trace of the Frobenius endomorphism*, as in Theorem 7.

The relation between the Frobenius endomorphism and Hasse's Theorem is thus realized in the following theorem.

Theorem 8. *The Frobenius endomorphism ϕ_p satisfies*

$$\chi(\phi_p) = \phi_p^2 - [t]\phi_p + [p] = [0] \,, \tag{14}$$

where t is the trace of the Frobenius endomorphism and $[n]$ is the scalar multiplication by n.

Proof. See [20, pages 135–136]. □

Hasse's theorem assures us that the trace of the Frobenius endomorphism t satisfies $|t| \leq 2\sqrt{p}$. Furthermore, it asserts that if we can find t then we can determine the number of $\mathbb{F}_p$-rational points of $E/\mathbb{F}_p$. Therefore, it suffices to find t modulo some integer greater than $4\sqrt{p}$. Schoof's approach to the problem of finding the trace t was to determine t modulo primes $l_1, \ldots, l_r$ satisfying $\prod_{i=1}^{r} l_i > 4\sqrt{p}$. Then, using the Chinese remainder theorem, one could easily find t.

To determine t modulo a small prime l, we first consider the case $l = 2$. Since p is an odd prime, we know from Hasse's theorem that $|E(\mathbb{F}_p)| = p + 1 - t \equiv t \pmod 2$. Clearly, $\mathcal{O} \in E(\mathbb{F}_p)$, and if $P = (x, y) \in E(\mathbb{F}_p)$ then $-P = (x, -y) \in E(\mathbb{F}_p)$. Thus, if E has no nontrivial points of order 2, then we have found that $t \equiv 1 \pmod 2$. Otherwise, E may have either one or three points of order 2, in which case $t \equiv 0 \pmod 2$.

Note that determining that a curve $E : y^2 = x^3 + a_4x + a_6$ has a nontrivial point of order 2 is equivalent to determining that $x^3 + a_4x + a_6$ is reducible in $\mathbb{F}_p$, which is in turn equivalent to finding nontrivial factor of $x^3 + a_4x + a_6$ and $x^p - x$.

Now consider the case l is an odd prime. Recall from Theorem 8 that the Frobenius endomorphism ϕ_p satisfies Equation (14). We restrict the characteristic polynomial of ϕ_p to the group of l-torsion points $E[l]$ to yield the equation

$$\phi_p^2 - [t_l]\phi_p + [p_l] = [0]$$

in $\operatorname{End}(E)$, where $t_l \equiv t \pmod{l}$, $p_l \equiv p \pmod{l}$ and $0 \leq t_l, q_l < l$. Thus, the problem of finding t_l amounts to finding an integer $0 \leq \tau < l$ such that

$$\phi_p^2(P) \oplus [p_l]P = [\tau]\phi_p(P) \tag{15}$$

for all nontrivial l-torsion points $P \in E[l] \setminus \{\mathcal{O}\}$. Note that τ is unique: if τ_1 and τ_2, with $0 \leq \tau_1, \tau_2 < l$, both satisfy (15), then we have $[\tau_1]\phi_p(P) = [\tau_2]\phi_p(P)$. Equivalently, $[\tau_d]\phi_p(P) = [0]$, where $\tau_d = |\tau_1 - \tau_2|$ for all nontrivial l-torsion points P. Since $P \neq \mathcal{O}$, also $\phi_p(P) \neq \mathcal{O}$ and it follows that $\tau_d \mid l$. But then, since l is a prime and $0 \leq \tau_1, \tau_2 < l$, we must have $\tau_1 = \tau_2$, to establish uniqueness.

The heart of Schoof's algorithm lies in the fact that we need not compute the coordinates of the points $\phi_p^2(P) = (x^{p^2}, y^{p^2})$ and $\phi_p(P) = (x^p, y^p)$. Computing these coordinates would indeed be very expensive. However, in Theorem 4 we showed that the nontrivial l-torsion points are precisely the roots of the l-th division polynomial f_l. Furthermore, to compute $[p_l](x, y)$ and $[\tau](x^p, y^p)$ we may also use the polynomials f_l, as shown in Theorem 5. Thus, our computations can be carried out in the polynomial ring $\mathbb{F}_p[x, y]/(f_l(x), E(x, y))$, where $E(x, y) = y^2 - x^3 - a_4x - a_6$ is the short Weierstrass equation (4).

We explain the algorithm in more detail, following the original introduction of the algorithm by Schoof in [18] and further discussion by Blake, Seroussi, and Smart in [6]. Let l be an odd prime, and let $P = (x, y)$ be a nontrivial l-torsion point, where we treat the coordinates as indeterminate. Our first main goal is to compute and compare the x-coordinates of $(x^{p^2}, y^{p^2}) \oplus [p_l](x, y)$ and $[\tau](x^p, y^p)$ for $0 \leq \tau < l$. In fact, since the x-coordinates of $[\tau](x^p, y^p)$ and its inverse $[l - \tau](x^p, y^p)$ are identical, it suffices to check $0 \leq \tau \leq (l - 1)/2$.

We distinguish between two cases. In the first case, $\phi_p^2(Q) \neq \pm[p_l]Q$ for all nontrivial l-torsion points Q. In particular, this means that $t_l \neq 0$, and that $\phi_p^2(Q)$ and $\pm[p_l]Q$ have different x-coordinates. In the second case, there exists a nontrivial l-torsion point $P = (x, y)$ for which $\phi_p^2(P) = [p_l]P$ or $\phi_p^2(P) = -[p_l]P$. Note that in this case the x-coordinates of $\phi_p^2(P)$ and $\pm[p_l]P$ are the same. That is, we have

$$x^{p^2} = x - \frac{\psi_{p_l-1}\psi_{p_l+1}}{\psi_{p_l}^2}\,.$$

Using the results of Theorem 4, we see that such a point P exists if and only if we have $\gcd(\psi_{p_l}^2(x^{p^2} - x) + \psi_{p_l-1}\psi_{p_l+1}, \psi_l) \neq 1$, so there is a simple test to separate the cases. In practice, we shall transform the expressions above and compute the greatest common divisor with the univariate division polynomials f_i.

Case 1: Here, $\phi_p^2(Q) \neq \pm[p_l]Q$ for all nontrivial l-torsion points Q. Using Equations (6) and (12), we have

$$\begin{aligned}&\left(x^{p^2}, y^{p^2}\right) \oplus [p_l](x, y)\\ &\qquad = \left(\lambda^2 - x^{p^2} - x + \frac{\psi_{p_l-1}\psi_{p_l+1}}{\psi_{p_l}^2}, \lambda\Big(2x^{p^2} - \lambda^2 + x - \frac{\psi_{p_l-1}\psi_{p_l+1}}{\psi_{p_l}^2}\Big) - y^{p^2}\right),\end{aligned}$$

where

$$\lambda = \frac{4y^{p^2+1}\psi_{p_l}^3 - \psi_{p_l+2}\psi_{p_l-1}^2 + \psi_{p_l-2}\psi_{p_l+1}^2}{4y\psi_{p_l}\left(\psi_{p_l}^2(x^{p^2}-x) + \psi_{p_l-1}\psi_{p_l+1}\right)} \,.$$

If $p_l = 1$, then ψ_{p_l-2} is not defined. However, in this case we need to compute $(x^{p^2}, y^{p^2}) \oplus (x, y)$, which is easy.

Thus, after finding a common denominator, we can write the x-coordinate of $(x^{p^2}, y^{p^2}) \oplus [p_l](x, y)$ as h_1/h_2 for some $h_1, h_2 \in \mathbb{F}_l[x, y]$. The x-coordinate of $[\tau](x, y)$ is written similarly as h_3/h_4 for some $h_3, h_4 \in \mathbb{F}_l[x, y]$. We will be computing $[\tau](x, y)$ for potentially many values of τ, so it may be preferred to write this expression leaving τ indeterminate.

Of course, the whole point of the algorithm is that we can make the computations considerably easier by reducing modulo the curve equation and the division polynomial f_l. Thus, we can and will reduce all powers of y greater than one and all powers of x greater than the degree of f_l, which is of the order $O(l^2)$. We equate the two resultant expressions, and by clearing denominators we obtain an expression of the form $a(x) - yb(x) = 0$ for $a, b \in \mathbb{F}_l[x]$. Substituting into the curve equation yields an expression $h_X(x) = 0$ for $h_X \in \mathbb{F}_l[x]$.

We need to determine if there exists one (and thus all) nontrivial l-torsion point $P = (x, y)$ for which $h_X(x) = 0$. As indicated in Theorem 4, a necessary and sufficient condition for the existence of such a point is that x is a root of f_l. Hence, if $\gcd(h_X, f_l) = 1$ then such a point does not exist and another value of τ should be tried. Otherwise, a nontrivial l-torsion point P satisfying Equation (15) exists for either τ or $l - \tau$, and it remains to find which of the two holds. This can be done by similarly computing and comparing the y-coordinates of $(x^{p^2}, y^{p^2}) \oplus [p_l](x, y)$ and $[\tau](x^p, y^p)$. If the two are equal, then we take $t_l = \tau$. Otherwise, we take $t_l = l - \tau$. Note that if in the computation of $[\tau](x, y)$ we have not left τ as indeterminate, then we in fact have $h_X \equiv 0 \pmod{f_l}$ whenever nontrivial l-torsion points satisfy Equation (15) with $t_l = \pm\tau$.

Case 2: Here, there exists a nontrivial l-torsion point P for which $\phi_p^2(P) = \pm[p_l]P$. Note that if $\phi_p^2(P) = [p_l]P$ then we must have $[2p_l]P = [t_l]\phi_p(P)$. Equivalently, $\phi_p(P) = [\frac{2p_l}{t_l}]P$. We apply the Frobenius endomorphism on both sides to find

$$[p_l]P = \phi_p^2(P) = \phi_p\left(\left[\frac{2p_l}{t_l}\right]P\right) = \left[\frac{4p_l^2}{t_l^2}\right]P \,.$$

Therefore, in this case $t^2 \equiv 4p_l \pmod{l}$ and thus p_l is a square in $\mathbb{F}_l$, say with $p_l \equiv \omega^2 \pmod{l}$ for some $\omega \in \mathbb{F}_l$. Note that in this case either ω or $-\omega$ is an eigenvalue of the Frobenius endomorphism: $\phi_p(P) = [\omega]P$ or $\phi_p(P) = [-\omega]P$.

This suggests the following treatment of Case 2. First we check if $\left(\frac{p_l}{l}\right) = -1$. If this is the case, then $\phi_p^2(P) = -[p_l]P$ and we conclude that $t_l = 0$. Otherwise, we can find a square root ω of p_l in $\mathbb{F}_l$. Next we check whether ω or $-\omega$ is an eigenvalue of the Frobenius endomorphism. This test is similar to the test which separated Case 1 and Case 2 above: if $\gcd(\psi_\omega^2(x^p - x) + \psi_{\omega-1}\psi_{\omega+1}, \psi_l) = 1$, then neither ω nor $-\omega$ is an eigenvalue and again we have $t_l = 0$. Otherwise, we need to check the y-coordinates. The y-coordinate of $[\omega](x, y)$ is

$$\frac{\psi_{\omega+2}\psi_{\omega-1}^2 - \psi_{\omega-2}\psi_{\omega+1}^2}{4y\psi_\omega^3} \, ,$$

so if $\gcd(4y^{p+1}\psi_\omega^3 - \psi_{\omega+2}\psi_{\omega-1}^2 + \psi_{\omega-2}\psi_{\omega+1}^2, \omega_l) = 1$, then $-\omega$ is eigenvalue and $t \equiv -2\omega \pmod{l}$. Otherwise, ω is an eigenvalue and $t \equiv 2\omega \pmod{l}$.

We illustrate this method with the following example. The curve and underlying field in the example were chosen to make computations easy. Clearly, such a curve would make an extremely poor choice for a cryptosystem. However, it is illustrative, and we shall make use of this curve later as well, when we discuss Elkies and Atkin primes.

Example 1. Let $E_1 : y^2 = x^3 + x + 2$ be an elliptic curve, taken over $\mathbb{F}_{17}$. It is easy to compute by hand that

$$\begin{aligned} E_1(\mathbb{F}_{17}) = \{&\mathcal{O}, (0, \pm 6), (1, \pm 2), (3, \pm 7), (4, \pm 6), (5, \pm 8), (9, \pm 3), \\ &(10, \pm 3), (11, \pm 1), (12, \pm 5), (13, \pm 6), (15, \pm 3), (16, 0)\} \, , \end{aligned}$$

so $|E_1(\mathbb{F}_{17})| = 24$. We would like to verify this using Schoof's algorithm. We need to determine the trace modulo $4\sqrt{17} \sim 16.5$, so it suffices to consider the primes 2, 3, and 5.

Consider first the case $l = 2$. We know that $t_2 = 0$ if and only if E_1 has a nontrivial point of order 2. Since $x^3 + x + 2 = (x + 1)(x^2 - x + 2)$ is reducible in $\mathbb{F}_{17}$, we conclude that there exists a nontrivial point of order 2, namely $(-1, 0) = (16, 0)$, and $t_2 = 0$.

Now consider the case $l = 3$, so that $p_3 = 17 \equiv 2 \pmod{3}$. Let $P = (x, y)$ be a nontrivial 3-torsion point with indeterminate coordinates. First, we compute the coordinates of $\phi_{17}(P)$ and $\phi_{17}^2(P)$ in $\mathbb{F}_{17}[x, y]/(f_3(x), E_1(x, y))$:

$$\begin{aligned} x^{17} &= -8x^3 - 2x^2 - 6x + 1, & x^{17^2} &= x, \\ y^{17} &= y\left(4x^3 - 8x^2 - 8x - 2\right), & y^{17^2} &= y. \end{aligned}$$

So in evaluating the test that separates Case 1 from Case 2 we see that

$$\gcd\left(\psi_2^2\left(x^{17^2} - x\right) + \psi_1\psi_3, \psi_3\right) = \gcd(\psi_3, \psi_3) = \psi_3 \neq 1 \, .$$

Since also p_3 is not a square in $\mathbb{F}_3$, we mush have $t_3 = 0$. Of course, in this case, even without computing the gcd, we can immediately see that $\phi_{17}^2(P) = P = -[2]P$, so $\phi_{17}^2(P) \oplus [2]P = \mathcal{O}$ and $t_3 = 0$. It is important to note that in general, for large primes p, the reductions of x^p, y^p, x^{p^2}, and y^{p^2} would require a very significant computational effort.

Lastly, we consider the case $l = 5$. Computations here are more involved than in the previous case. To help the reader follow the algorithm, we omit many non-trivial computations. As a compensation, we provide some relevant SAGE source code to the reader in Figure 6 in the appendix.

We have $p_5 = 17 \equiv 2 \pmod 5$. Similar to before, let $P = (x, y)$ be a nontrivial 5-torsion point with indeterminate coordinates. Note that after reducing by the curve equation $E_1(x, y)$, the univariate 5th division polynomial evaluates to

$$f_5(x) = 5x^{12} - 6x^{10} - 5x^9 - 3x^8 + 4x^7 - 2x^6 + 2x^5 - 2x^4 - 6x^3 - 7x^2 + x - 7 \,.$$

Again, we find the coordinates of $\phi_{17}(P)$ and $\phi_{17}^2(P)$ in $\mathbb{F}_{17}[x, y]/(f_5(x), E_1(x, y))$:

$$\begin{aligned}
x^{17} &= -4x^{11} - 7x^{10} + x^9 - 2x^8 + 7x^7 + 5x^6 + 5x^5 - 5x^4 + 5x^2 - x + 7,\\
x^{17^2} &= -4x^{11} + 6x^{10} + 7x^9 - 3x^8 - 7x^7 + x^6 - 4x^5 - 6x^4 + 8x^3 + x^2 + 6,\\
y^{17} &= y\left(3x^{11} + 6x^{10} + 6x^9 - 6x^8 - 3x^7 - 7x^6 + 5x^5 - 6x^4 + 2x^3 + 6x^2 + 2x + 4\right),\\
y^{17^2} &= y\left(x^{11} + 5x^{10} + 6x^9 + 4x^8 + 3x^7 - 7x^6 + 7x^5 - 5x^4 - 3x^3 + 2x^2 + 5x + 7\right).
\end{aligned}$$

Next, we evaluate and find

$$\gcd\left(\psi_2^2\left(x^{17^2} - x\right) + \psi_1\psi_3, \psi_5\right) = 1 \,,$$

so we know that Case 1 applies. Hence, we need only consider $0 < \tau \leq (5-1)/2 = 2$. Using Equation (12), we find that

$$\begin{aligned}
[p_5]P = [2]P &= \left(x - \frac{\psi_1\psi_3}{\psi_2^2}, \frac{\psi_4\psi_1^2 - \psi_0\psi_3^2}{4y\psi_2^3}\right)\\
&= \left(x - \frac{3x^4 + 6x^2 + 24x - 1}{4y^2}, \frac{x^6 + 5x^4 + 40x^3 - 5x^2 - 8x - 33}{8y^3}\right) \,,
\end{aligned}$$

For simplicity define $\phi_{17}^2(P) = (x_3, y_3)$, $[2]P = (x_4, y_4)$, and $(x_3, y_3) \oplus (x_4, y_4) = (x_5, y_5)$. From Equation (6) we know that $x_5 = \lambda^2 - x_3 - x_4$, where $\lambda = (y_3 - y_4)/(x_3 - x_4)$. In $\mathbb{F}_{17}[x, y]/(f_5(x), E_1(x, y))$, this resolves to

$$\lambda = y\left(-8x^{11} - 3x^{10} - 3x^9 - 3x^8 - 2x^7 - 5x^6 + x^5 - 2x^4 - 7x^3 - 8x^2 + 4x + 6\right).$$

Since there are only two values of τ to check, we choose to set $\tau = 1$ and explicitly compute the x-coordinate equality $x_5 = \tau x^{17}$. After clearing denominators, we find that in $\mathbb{F}_{17}[x, y]/(f_5(x), E_1(x, y))$ the resultant expression is $h(x) \equiv 0$. Therefore, we can conclude that $t_5 = \pm 1$, and it remains to see which of the two options holds. We compute

$$y_5 = y\left(-3x^{11} - 6x^{10} - 6x^9 + 6x^8 + 3x^7 + 7x^6 - 5x^5 + 6x^4 - 2x^3 - 6x^2 - 2x - 4\right),$$

so we see immediately that $y_5 = -y^{17}$. We conclude that $t_5 = -1$.

Next we combine the above information. We have found that $t_2 = t_3 = 0$ and $t_5 = 4$. Therefore, we can uniquely determine that $t \equiv 24 \pmod{30}$. On the other hand, we know from Theorem 7 that $|t| \leq 2 \cdot \sqrt{17} < 9$. Thus, we must have $t = -6$. It follows that $|E_1(\mathbb{F}_{17})| = 17 + 1 - (-6) = 24$, as needed. $\diamond$

The complexity of Schoof's algorithm is in the order $O(\log^{2+3\mu} p)$ bit operations [13]. Schoof [19] notes that although the algorithm is of polynomial running time in the logarithm of p, it is extremely slow and impractical. The reason for such a slow running time is due to the rapid growth in the degree of the division polynomial. For instance, Schoof [19] finds that if $l > 250$, then one element in the reduced polynomial ring will take more than 1.5 megabytes of memory to store.

4.2 Atkin's classification

As noted above, Schoof's algorithm is fairly inefficient because of the exponential growth in the degree of the division polynomial f_l. Atkin and Elkies sought to improve the efficiency of Schoof's algorithm by first analyzing how the restricted characteristic polynomial $\chi_l(T) = T^2 - t_l T + p_l$ of the Frobenius endomorphism splits over $\mathbb{F}_l$. The polynomial $\chi_l(T)$ has a root in $\mathbb{F}_l$ if and only if the (still unknown) discriminant $\Delta_\chi = t^2 - 4p \equiv t_l^2 - 4p_l \pmod{l}$ is a square in $\mathbb{F}_l$. Otherwise, the roots are elements of $\mathbb{F}_l[\sqrt{\Delta_\chi}] \cong \mathbb{F}_{l^2}$.

Definition 15. Let $\Delta_\chi = t^2 - 4p$ be the discriminant of $\chi(T)$, the characteristic polynomial of the Frobenius endomorphism. If Δ_χ is a square in $\mathbb{F}_l$, we say that l is an *Elkies prime*. Otherwise, we call l an *Atkin prime*.

Atkin was able to show how the l-th modular polynomial Φ_l can be used to determine whether l is an Elkies prime or an Atkin prime. He then proceeded to describe how to compute the order of the Frobenius endomorphism ϕ_p in $\mathrm{PGL}_2(\mathbb{F}_l)$. In the case of l an Atkin prime, the order of ϕ_p is useful to determine possible values of the reduced trace t_l. In the case of l an Elkies prime, Elkies was able to show how the division polynomial can be replaced by a polynomial of degree $(l-1)/2$.

The main result of this section is the classification theorem in Theorem 9. In order to prove the classification theorem, the following Proposition 9 will be extremely useful. Let C_i, with $1 \leq i \leq l+1$, be the cyclic subgroups of order l of $E[l]$. Recall from Theorem 6 that the zeros of $\Phi_l(x, j(E))$ are precisely the j-invariants of isogenous curves $\tilde{E}/C_i$ to E. The following theorem establishes the necessary links between the zeros of $\Phi_l(x, j(E))$ in some field extension $\mathbb{F}_{p^r}$, the map ϕ_p^r, and the cyclic subgroups C_i.

Proposition 9. *Let E be an ordinary elliptic curve over $\mathbb{F}_p$ with j-invariant $j \neq 0$ or 1728. Then*

1. *The polynomial $\Phi_l(x, j)$ has a zero $\tilde{\jmath} \in \mathbb{F}_{p^r}$ if and only if the kernel C of the corresponding isogeny $E \to E/C$ is a one-dimensional eigenspace of ϕ_p^r in $E[l]$, with ϕ_p the Frobenius endomorphism of E.*

2. *The polynomial $\Phi_l(x, j)$ splits completely in $\mathbb{F}_{p^r}[x]$ if and only if ϕ_p^r acts as a scalar matrix on $E[l]$.*

Proof. See [19, pages 236–238]. □

In the center of the SEA algorithm stands the following classification theorem.

Theorem 9 (Atkin)**.** *Let E be an ordinary elliptic curve defined over $\mathbb{F}_p$ with j-invariant $j \neq 0$ or 1728. Let $\Phi_l(x, j) = h_1 h_2 \cdots h_s$ be the factorization of $\Phi_l(x, j) \in \mathbb{F}_p[x]$ as a product of irreducible polynomials. Then there are the following possibilities for the degrees of $h_1, \ldots, h_s$:*

1. *$(1, 1, \ldots, 1)$ or $(1, l)$. In either case we have $t^2 - 4p \equiv 0 \pmod{l}$. In the former case we set $r = 1$ and in the latter case $r = l$.*

2. *$(1, 1, r, r, \ldots, r)$. In this case $t^2 - 4p$ is a square module l, r divides $l - 1$, and ϕ_p acts on $E[l]$ as a diagonal matrix $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ with $\lambda, \mu \in \mathbb{F}_l^*$.*

3. *$(r, r, \ldots, r)$ for some $r > 1$. In this case $t^2 - 4p$ is a nonsquare modulo l, r divides $l + 1$, and the restriction of ϕ_l to $E[l]$ has an irreducible characteristic polynomial over $\mathbb{F}_l$.*

In all cases, r is the order of ϕ_p in the projective general linear group $\mathrm{PGL}_2(\mathbb{F}_l)$ *and the trace t of the Frobenius satisfies*

$$t^2 \equiv p(\zeta + \zeta^{-1})^2 \pmod{l}, \tag{16}$$

for some primitive r-th root of unity $\zeta \in \overline{\mathbb{F}}_l$. Furthermore, the number of irreducible factors s satisfies

$$(-1)^s = \left(\frac{p}{l}\right). \tag{17}$$

Proof. Write the reduced characteristic polynomial

$$\chi_l(T) = T^2 - t_l T + p_l = T^2 - (\lambda + \mu)T + \lambda\mu = (T - \lambda)(T - \mu). \tag{18}$$

In particular, we see that $\lambda\mu \equiv p \pmod{l}$ and $\lambda + \mu \equiv t \pmod{l}$. It follows that $\Delta_\chi \equiv t^2 - 4p \equiv (\lambda + \mu)^2 - 4\lambda\mu \equiv (\lambda - \mu)^2 \pmod{l}$.

From Proposition 9, we know that the Frobenius endomorphism ϕ_p acts on $E[l]$ as A, a 2×2 matrix over $\mathbb{F}_l$ with a characteristic equation $\phi_p^2 - t\phi_p + p = 0$. We consider the following cases:

1a. A is diagonalizable and has a double eigenvalue $\lambda \in \mathbb{F}_l^*$. Then A is similar to a scalar matrix $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$, which in $\mathrm{PGL}_2(\mathbb{F}_l)$ reduces to the identity matrix. Therefore, the degree of ϕ_p in $\mathrm{PGL}_2(\mathbb{F}_l)$ is 1, and $\Phi_l(x, j)$ splits completely in $\mathbb{F}_p$. This case corresponds to the first possibility in Theorem 9, with a splitting type $(1, 1, \ldots, 1)$. Since $\lambda = \mu$, it is clear that $\Delta_\chi \equiv t^2 - 4p \equiv (\lambda - \lambda)^2 \equiv 0 \pmod{l}$, as needed.

1b. A is not diagonalizable and has eigenvalues $\lambda, \mu \in \mathbb{F}_l^*$. Then it must be the case that $\lambda = \mu$, or else A is diagonalizable. It follows that A is similar to a matrix $\left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$. Then the degree of ϕ_p in $\mathrm{PGL}_2(\mathbb{F}_l)$ is l. This case also corresponds to the first possibility in Theorem 9, but here the splitting type is $(1, l)$. Here, too, $\Delta_\chi \equiv t^2 - 4p \equiv (\lambda - \lambda)^2 \equiv 0 \pmod{l}$.

2. A is diagonalizable and has two distinct eigenvalues $\lambda, \mu \in \mathbb{F}_l^*$. In particular, $\lambda^{l-1} = \mu^{l-1} = 1$. Then A is similar to the matrix $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$, and the order of ϕ_p in $\mathrm{PGL}_2(\mathbb{F}_l)$ divides $l - 1$. This corresponds to the second possibility in Theorem 9. In addition, since $\Delta_\chi \equiv t^2 - 4p \equiv (\lambda - \mu)^2 \pmod{l}$ and $\lambda - \mu \in \mathbb{F}_l$, we conclude that Δ_χ is a square modulo l.

3. A is not diagonalizable and has two conjugate eigenvalues $\lambda, \mu \in \mathbb{F}_{l^2} - \mathbb{F}_l$. Here, A is similar to the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -\lambda\mu & \lambda+\mu \end{smallmatrix}\right)$. If instead we consider the action of the Frobenius endomorphism as $\tilde{A}$, a 2×2 matrix with coefficients in $\mathbb{F}_{l^2}$, then $\tilde{A}$ is similar to the matrix $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$.

   We claim that $\mu = \lambda^l$. To see why, let d be some non-square modulo l. Then we can write $\lambda = \alpha + \beta\sqrt{d}$ and $\mu = \alpha - \beta\sqrt{d}$ for some $\alpha, \beta \in \mathbb{F}_l$. On the one hand we have $(\sqrt{d})^{2l} = (\sqrt{d})^2$, and on the other hand we have $(\sqrt{d})^l \neq \sqrt{d}$. It follows that $(\sqrt{d})^l = -\sqrt{d}$. Thus, $\lambda^l = (\alpha + \beta\sqrt{d})^l = \alpha^l + \beta^l(\sqrt{d})^l = \alpha - \beta\sqrt{d} = \mu$, as needed. Similarly, $\lambda = \mu^l$.

   Let $r > 1$ be the smallest integer such that $\lambda^r \in \mathbb{F}_l^*$, and note that $\mu^r = (\lambda^l)^r = (\lambda^r)^l = \lambda^r$, with the last equality given since $\lambda^r \in \mathbb{F}_l$. In particular, r is also the smallest integer such that $\mu^r \in \mathbb{F}_l^*$. Therefore, $\tilde{A}^l$ is a scalar matrix with coefficients in $\mathbb{F}_l$, and we conclude that the order of the order of the Frobenius endomorphism is r. The order r divides $l^2 - 1$ but does not divide $l - 1$. It follows that r divides $l + 1$.

   In addition, since $\Delta_\chi \equiv t^2 - 4p \equiv (\lambda - \mu)^2 \equiv 4\beta^2 d \pmod{l}$ and d is a non-square in $\mathbb{F}_l$, we conclude that Δ_χ is also not a square modulo l. This corresponds to the third and final possibility in Theorem 9.

We now prove Equation (16). From the discussion above we know that r is the smallest integer such that $\lambda^r = \mu^r$. Recall that $\lambda\mu \equiv p \pmod{l}$ and $\lambda + \mu \equiv t \pmod{l}$. Then $\lambda^{2r} \equiv p^r \pmod{l}$, so that $\lambda^2 \equiv \zeta p \pmod{l}$ for some primitive r-th root of unity $\zeta \in \overline{\mathbb{F}}_l$. Furthermore,

$$\begin{aligned} t^2 &\equiv (\lambda+\mu)^2 \equiv (\lambda + p/\lambda)^2 \equiv \lambda^2 + 2p + p^2\lambda^{-2} \equiv \zeta p + 2p + \zeta^{-1}p \\ &\equiv p(\zeta+\zeta^{-1})^2 \pmod{l}\ , \end{aligned}$$

as needed.

Lastly, for the proof of Equation (17), see [19, page 240]. □

Note that Theorem 9 is indeed a classification theorem. For each prime l with $l \neq p$, we first determine the splitting type of $\Phi_l(x,j)$ by computing the degree of $g(x) = \gcd(\Phi_l(x,j), x^p - x)$. By the theorem above, the degree of $g(x)$ can only be 0, 1, 2, or l. If the $g(x)$ is a constant, l is an Atkin prime. Otherwise it is an Elkies prime.

Example 2. Recall the elliptic curve $E_1/\mathbb{F}_{17}$ from the previous example. The j-invariant of E_1 is 1. The case of $l = 2$ is most easily treated by looking for points of order 2, as we did in the previous example. We shall check which for the primes 3 and 5 if they are Atkin primes or Elkies primes. Relevant SAGE source code is provided in Figure 7 in the appendix.

Let $l = 3$. We consider the modular polynomial $\Phi_3(x,1)$ in the polynomial ring $\mathbb{F}_{17}[x]$. Using Section 3.7, direct computation reveals that

$$\begin{aligned} \Phi_3(x,1) &= x^4 + 2618675x^3 + 461887642896318x^2 + 18546550348058859060044x \\ &\quad + 18554263248568356864 01 \\ &\equiv x^4 - 5x^3 + 4x^2 - x + 5 \pmod{17}\ . \end{aligned}$$

We use the Euclidean division algorithm to find $\gcd\left(\Phi_3(x,1), x^{17}-x\right)$, where the Euclidean domain in which we work is of course the polynomial ring $\mathbb{F}_{17}[x]$. The division algorithm shows that

$$\Phi_3(x,1) = \left(x^3 + 7x^2 + 3x + 1\right)(x+5)\ .$$

Thus, we have found a linear factor of $\Phi_3(x,1)$, so we conclude that 3 is an Elkies prime.

Now let $l = 5$. Again from Section 3.7, the modular polynomial $\Phi_5(x,1)$ is given by

$$\begin{aligned} \Phi_5(x,1) = x^6 & \\ &+ 1718552082309x^5 \\ &+ 141365812323862726855 7935x^4 \\ &+ 280052346791868251027764047829968560x^3 \\ &+ 672905989018062337944240333947218196 1775x^2 \\ &+ 530102939008919308692993536888323369267276 74x \\ &+ 141413228178305070529031327599431299228189982721 \\ \equiv x^6 &+ 6x^5 - 2x^4 + 3x^3 - 7x^2 - 6x - 8 \pmod{17}. \end{aligned}$$

Here, the Euclidean division algorithm reveals that $\gcd\big(\Phi_5(x,1), x^{17}-x\big) = 1$. Hence, 5 in an Atkin prime. $\diamond$

In the following sections we describe how the knowledge of whether l is an Atkin or an Elkies prime can be used to compute the reduced trace t_l.

4.3 Atkin primes

We now turn our attention to the case of l an Atkin prime and follow the treatment in [13], [6], and [19].

Our first goal is compute the degree r of ϕ_p in $\mathrm{PGL}_2(\mathbb{F}_l)$. The approach Atkin took was to determine the smallest integer $i > 1$ such that

$$\gcd\left(\Phi_l(x,j), x^{p^i} - x\right) = \Phi_l(x,j)\,. \tag{19}$$

Thus, $\mathbb{F}_{p^i}$ is the smallest field extension of $\mathbb{F}_p$ which contains all the roots of $\Phi_l(x,j)$. From the second statement of Proposition 9, we conclude that $i = r$ is the degree of ϕ_p. From Theorem 9 we know that it suffices to check only integers i that divide $l+1$ and that satisfy $(-1)^{(l+1)/i} = \left(\frac{p}{l}\right)$. The possible values of i are tried with the greatest common divisor computed each time using the Euclidean algorithm.

Once the order r of ϕ_p is determined, we need to compute the restriction modulo l of the trace t. We shall construct a set T_l of such possible values t_l. Equation (16) is the main result we use here. There are $\phi_{\mathrm{Eul}}(r)$ options for the r-th roots of unity ζ, where ϕ_{Eul} is Euler's totient function. By symmetry, there are $\phi_{\mathrm{Eul}}(r)/2$ possible values for $\zeta+\zeta^{-1}$, and from Equation (16) the same is true for $t^2 \pmod{l}$. It follows that there T_l includes at most $\phi_{\mathrm{Eul}}(r)$ possible values of t_l.

Note that the primitive r-th roots of unity are elements of $\mathbb{F}_{l^2}$. To see why, let ζ be a primitive r-th root unity. Since $r \mid (l+1)$, say with $ar = l+1$ for some integer a, we know that $\zeta^{l^2-1} = \zeta^{(l+1)(l-1)} = \zeta^{ar(l-1)} = 1$, so $\zeta \in \mathbb{F}_{l^2}$. Let $\lambda, \mu \in \mathbb{F}_{l^2} - \mathbb{F}_l$ be the two eigenvalues of ϕ_p. From Proposition 9, we know that r is the smallest positive integer for which $\lambda^r = \mu^r$. It follows that $\lambda/\mu = \gamma$ is a primitive r-th root of unity. From the discussion above we conclude that $\gamma \in \mathbb{F}_{l^2}$. Furthermore, once we write $\mathbb{F}_{l^2} \cong \mathbb{F}_l[\sqrt{d}]$ for some nonsquare $d \in \mathbb{F}_l$, we can enumerate all the possible $\phi_{\mathrm{Eul}}(r)$ values of γ as follows: let g be a generator for the multiplicative group of $\mathbb{F}_{l^2}$; then $\gamma = g^{(l^2-1)/r}$ is a primitive r-th root of unity, as well as any $\gamma_i = \gamma^i$ where i is relatively prime to r and satisfying $1 \le i < r$.

Our next goal is to determine the members of T_l using the different γ_i. From Equation (18) we know that $t \equiv \lambda + \mu \pmod{l}$ and $p \equiv \lambda\mu \pmod{l}$. Using the same nonsquare $d \in \mathbb{F}_l$ as above, we have $\lambda = x_1 + x_2\sqrt{d}$ and $\mu = x_1 - x_2\sqrt{d}$ for some (still unknown) $x_i \in \mathbb{F}_l$. Similarly, we have $\gamma_i = g_{i_1} + g_{i_2}\sqrt{d}$, but here $g_{i_1}, g_{i_2} \in \mathbb{F}_l$

can be computed. Additionally,

$$\begin{aligned} g_{i_1} + g_{i_2}\sqrt{d} = \gamma_i = \frac{\lambda}{\mu} = \frac{\lambda^2}{\lambda\mu} &= \frac{x_1^2 + dx_2^2 + 2x_1x_2\sqrt{d}}{p} \\ &= \frac{x_1^2 + dx_2^2}{p} + \frac{2x_1x_2}{p}\sqrt{d}\,. \end{aligned}$$

Solving for the first coordinate, we have $pg_{i_1} \equiv x_1^2 + dx_2^2 \pmod{l}$. Also, $p \equiv \lambda\mu = x_1^2 - dx_2^2 \pmod{l}$. Thus, it follows that $x_1^2 = p(g_{i_1}+1)/2$. If x_1^2 is not a square in $\mathbb{F}_l$, then we discard γ_i and move on to the next one. Otherwise, since $t \equiv \lambda + \mu = 2x_1 \pmod{l}$, add to T_l the values $2x_1$ and $-2x_1$. We illustrate this procedure with the following example.

Example 3. Consider again the elliptic curve $E_1/\mathbb{F}_{17}$. We found in the previous example that 5 is an Atkin prime. Next, we need to compute the order r of the Frobenius endomorphism ϕ_p in $\mathrm{PGL}_2(\mathbb{F}_l)$. That is, we need to find the smallest integer $i > 1$ such that Equation (19) holds.

From Theorem 9 we know that we need only consider $i \mid (l+1)$. In other words, $i = 2$, $i = 3$, or $i = 6$. Furthermore, $17 \equiv 2 \pmod{5}$ is not a square in $\mathbb{F}_5$, so from Equation 17, we know that $6/i$ must be odd. It follows that $i \neq 3$. The very first step in the Euclidean algorithm reveals that $\Phi_5(x,1)$ does not divide $x^{17^2} - x$. In fact, $\gcd\left(\Phi_5(x,1), x^{17^2} - x\right) = 1$. Therefore, we must have $r = i = 6$.

Next, we need to find the primitive 6th roots of unity in $\overline{\mathbb{F}}_5$. We know that these are elements in $\mathbb{F}_{5^2} \cong \mathbb{F}_5[\sqrt{2}]$, so we start by finding a generator g for the multiplicative group $\mathbb{F}_5[\sqrt{2}]^*$. This group has only 24 elements, and one soon finds that $g = 3 + \sqrt{2}$ is a generator. Thus, one primitive 6th root of unity is $\gamma = g^4 = 3 + 2\sqrt{2}$ and the other is $\gamma^5 = 3 - 2\sqrt{2}$. Note that in practice, the restriction of finding $l_1, \ldots, l_r$ satisfying $\prod_{i=1}^r l_i > 4\sqrt{p}$ means that we would only evaluate small primes, say with $l_i < 1000$. Thus, it is easy to pre-compute and store generators of the multiplicative groups $\mathbb{F}_{l_i}[\sqrt{k_i}]^*$, where k_i is a nonsquare in $\mathbb{F}_{l_i}$.

The two primitive 6th roots of unity are conjugates and share the same "real" part $g_{1_1} = g_{5_1} = 3$. So in either case, we find that $x_1^2 = 17(3+1)/2 \equiv 4 \pmod{5}$. Clearly, $2^2 \equiv 3^2 \equiv 4 \pmod{5}$, so $x_1 = \pm 2$. Thus, we add the two possible traces $\pm 2x_1 = \{1, 4\}$ to T_5. ◇

As mentioned above, in reality one does not use the modular polynomial Φ_l in the computations, but instead would use a related polynomial. Lercier, Lubicz, and Vercauteren [13] discuss the so-called canonical modular polynomials as one example. Schoof [19] notes that working with modular polynomials can be done with a practical polynomial running time.

4.4 Elkies primes

We know turn out attention to Elkies primes. Elkies showed that if $t^2 - 4p$ is a square modulo the prime l, then we may substitute the division polynomial f_l of degree $(l^2-1)/2$ with a factor F_l of it of degree $(l-1)/2$. This represents a very significant reduction in computation time. We now trace this procedure.

Let $E/\mathbb{F}_p$ be the elliptic curve under consideration and l be an Elkies prime with $l \neq p$. Recall from Corollary 1 that $E[l]$ is the union of $l+1$ cyclic subgroups of order l, with a pair-wise intersection at the identity element. Since l is an Elkies prime, we can write the restricted characteristic polynomial of the Frobenius endomorphism over $\mathbb{F}_l$ as

$$\chi_l(T) = T^2 - t_l T + p_l = (T-\lambda)(T-\mu)\,. \tag{20}$$

Note that $t_l \equiv \lambda + \mu = \lambda + p_l/\lambda \pmod{l}$, so it suffices to find λ.

Suppose first that $\lambda = \mu$. Then $t_l \equiv 2\lambda \equiv 2\sqrt{p_l} \pmod{l}$. This corresponds to Case 2 in explanation of Schoof's algorithm in Page 32, where we found that $\phi_p(P_1) = [\sqrt{p_l}]P_1 = [\lambda]P_1$ for some nontrivial point $P_1 \in E[l]$. That is, λ is an eigenvalue of the Frobenius endomorphism. Let $C_1 = \langle P_1 \rangle$ be the cyclic subgroup of order l generated by P_1. Then we have just found that C_1 is stable under the action of the Frobenius endomorphism: $\phi_p(C_1) = C_1$.

Now suppose that $\lambda \neq \mu$. Then from Theorem 9, we know that there exist nontrivial points $P_1, P_2 \in E[l]$ such that $\phi_p(P_1) = [\lambda]P_1$ and $\phi_p(P_2) = [\mu]P_2$. Let $C_1 = \langle P_1 \rangle$ and $C_2 = \langle P_2 \rangle$, and note that $C_1 \neq C_2$. We with the previous case, it follows immediately that both C_1 and C_2 are stable under the action of the Frobenius endomorphism: $\phi_p(C_1) = C_1$ and $\phi_p(C_2) = C_2$.

We shall describe in Section 4.5 how this information allows for a construction of a polynomial

$$F_l(x) = \prod_{\pm P \in C_1 \setminus \{\mathcal{O}\}} (x - (P)_X)\,, \tag{21}$$

where $(P)_X$ denotes the x-coordinate of P. Note that only one point in each pair $\pm P$ is taken, as both share the same x-coordinate. The degree of F_l is thus $(l-1)/2$, and it is a factor of f_l.

From here, the algorithm proceeds in a similar way to Schoof's algorithm. We know that there exists a nonzero $\lambda \in \mathbb{F}_l^*$ such that for any nontrivial point $P = (x,y) \in C_1 \setminus \{\mathcal{O}\}$ the equation $\phi_p(P) = [\lambda]P$ holds. Moreover, since l is a prime, λ is unique. Note that for such a point P we necessarily have

$$x^p = x - \frac{\psi_{\lambda-1}\psi_{\lambda+1}}{\psi_\lambda^2}\,.$$

Let $h = \psi_\lambda^2(x^p - x) + \psi_{\lambda-1}\psi_{\lambda+1}$. We shall make h into a univariate equation $h_X = 0$ by reducing modulo, and substituting into, the curve equation. Then, it remains to find a value λ such that $\gcd(h_X, F_l) \neq 1$.

As with Schoof's algorithm, it suffices to check only values $1 \leq \lambda \leq (l-1)/2$ and then test the y-coordinate to separate λ from $l - \lambda$. Furthermore, we can also use the results of Theorem 9 to narrow down further the possibilities for λ.

Example 4. We continue to analyze $E_1/\mathbb{F}_{17}$. Recall that 3 is an Elkies prime for this curve. The only two values we need to check are $\lambda = 1$ and $\lambda = 2$. We take the case $\lambda = 1$ first. In Example 5 we shall see that $F_3 = x - 2$. Therefore, we have $h = \psi_1^2(x^{17} - x) + \psi_0\psi_2 \equiv 0 \pmod{F_3}$, so indeed the correct value of λ is 1. Then, $t = \lambda + p/\lambda \equiv 0 \pmod 3$, as needed. ◇

4.5 Factors of division polynomials

In this section we describe how to construct the polynomial F_l given in Equation (21). We shall approach this problem in two steps. First we find the first coefficient of F_l (which is the sum of the roots of F_l, with the sign inverted). Then we use the first coefficient to compute the other coefficients of F_l. Throughout this section we assume that l is an Elkies prime different from p, the characteristic of the underlying field. The discussion follows closely the ones in [6] and [19], though here we omit many details that are beyond the scope of this work.

Given a non-supersingular elliptic curve in a short Weierstrass equation $E/\mathbb{F}_p : y^2 = x^3 + a_4x + a_6$, we first compute the j-invariant as described in Equation (5):

$$j = j_E = 1728\left(\frac{4a_4^3}{4a_4^3 + 27a_6^2}\right) \tag{5}$$

Since l is an Elkies prime, we know from Theorem 9 that the degree of the polynomial $g(x) = \gcd(\Phi_l(x, j), x^p - x)$ is greater than zero, and that the roots of $g(x)$ are in $\mathbb{F}_p$. Find one of the roots and denote it by $\tilde{j}$. By Theorem 6, there exists an isogenous curve $\tilde{E} : y^2 = x^3 + \tilde{a_4}x + \tilde{a_6}$ to E with j-invariant $\tilde{j}$. Furthermore, the kernel of the isogeny is C, one of the $l + 1$ cyclic groups of order l of $E[l]$. Our immediate goal is to find $\tilde{a_4}$ and $\tilde{a_6}$, given the knowledge of a_4, a_6, j, and $\tilde{j}$. This will allow us to compute the first coefficient of F_l.

Recall from Section 3.5 that any elliptic curve E (with coefficients considered as integers) is characterized by a complex number $q = e^{2\pi i\tau}$. Furthermore, for an elliptic curve E corresponding to the parameter q as above, we have $j(q) = j_E$, where the expression on the left is from Equation (11) and the one on the right is from Equation (5). In fact, the choice for the notation in Section 3.1, where the constants in Equation (3) were introduced, stems from the reach theory of modular forms, from which the formal sum $j(q)$ is derived. This fact gives rise to the analytical treatment we develop in this section.

For any Laurent series $f(q) = \sum_n a_nq^n$ we define $f'(q)$ to be $q\frac{\mathrm{d}f}{\mathrm{d}q} = \sum_n na_nq^n$. Then we have the following result.

Proposition 10. *The following hold in* $\mathbb{Z}[\![q]\!]$*:*

$$\begin{aligned} \frac{j'}{j} &= -\frac{E_6}{E_4}\,, \qquad \frac{j'}{j-1728} = -\frac{E_4^2}{E_6}\,, \\ \frac{j''}{j'} &= \frac{1}{6}E_2 - \frac{1}{2}\frac{E_4^2}{E_6} - \frac{2}{3}\frac{E_6}{E_4}\,. \end{aligned} \tag{22}$$

Proof. See [19, page 244] □

Note that the assumption that $E/\mathbb{F}_p$ is an ordinary curve over a field of large characteristic ensures that the polynomials above do not vanish for the parameter q associated with E.

The crucial observation here is that we already know from Equation (10) that $E_4(q) \equiv -48a_4 \pmod{\mathfrak{B}}$ and $E_6(q) \equiv 864a_6 \pmod{\mathfrak{B}}$, where $\mathfrak{B}$ is as defined in Section 3.5. Thus, we can easily find j'. Furthermore, we can now express E_2 in terms of the ratio j''/j'. Clearly, analogous relations exist for the (still unknown) isogenous curve $\tilde{E} : y^2 = x^3 + \tilde{a_4}x + \tilde{a_6}$, and the next theorem provides the important missing link between the invariants of both curves. It relies on the following observation: given a curve with a j-invariant $j(q)$, there exists an isogenous curve with a j-invariant $j(q^l)$ and the degree of the isogeny is l. As mentioned by Lercier and Morain in [14], it is possible that this isogenous curve is not the one we were looking for. That is, it is possible that $\tilde{\jmath} \neq j(q^l)$, in which case we may have to discard the curve.

Theorem 10. *Let l be a prime and $\Phi_l(x, y) \in \mathbb{Z}[x, y]$ be the l-th modular polynomial. Let $\tilde{\jmath}(q) = j(q^l)$. Then $\Phi_l(j(q), \tilde{\jmath}(q)) = 0$. Furthermore, the following identities of power series hold:*

$$\tilde{\jmath}' = -\frac{j'\Phi_x(j, \tilde{\jmath})}{l\Phi_y(j, \tilde{\jmath})} \,, \tag{23}$$

$$\frac{j''}{j'} - l\frac{\tilde{\jmath}''}{\tilde{\jmath}'} = -\frac{j'^2\Phi_{xx}(j, \tilde{\jmath}) + 2lj'\tilde{\jmath}'\Phi_{xy}(j, \tilde{\jmath}) + l^2\tilde{\jmath}'^2\Phi_{yy}(j, \tilde{\jmath})}{j'\Phi_x(j, \tilde{\jmath})} \,, \tag{24}$$

where the subscripts x and y denote partial derivatives of Φ_l with respect to those variables.

Proof. See [19, page 246]. □

When computing the invariants in Equations (23) and (24), one must make sure that the partial derivatives do not vanish. In [19], Schoof explains that this happens if $(j, \tilde{\jmath})$ is a singular point of $\Phi_l(x, y)$ over $\mathbb{F}_p$, the likelihood of which is extremely low for large values of p. In the case where $(j, \tilde{\jmath})$ is such a singular point, the curve has to be discarded and a new curve must be picked.

Equation (23) is used to find $\tilde{\jmath}'$. Then, we use the first two equalities in Equation (22), as well as Equation (8) to find $\tilde{a_4}$, $\tilde{a_6}$, and $E_4(q^l), E_6(q^l) \pmod{\mathfrak{B}}$. Namely, we have

$$\begin{gathered}
\tilde{a_4} = -\frac{1}{48}\frac{\tilde{\jmath}'^2}{\tilde{\jmath}(\tilde{\jmath} - 1728)} \,, \qquad \tilde{a_6} = -\frac{1}{864}\frac{\tilde{\jmath}'^3}{\tilde{\jmath}^2(\tilde{\jmath} - 1728)} \,, \\
E_4(q^l) \equiv -48\tilde{a_4} \pmod{\mathfrak{B}} \,, \quad E_6(q^l) \equiv 864\tilde{a_6} \pmod{\mathfrak{B}} \,,
\end{gathered} \tag{25}$$

where

$$\tilde{j}' = -\frac{j'\Phi_x(j,\tilde{j})}{l\Phi_y(j,\tilde{j})} \, .$$

Next, we find p_1 using Equations (9) and (24):

$$\begin{aligned} p_1 &= \sum_{\zeta \in \mu_l, \zeta \neq 1} x(\zeta; q) \\ &= \frac{l}{2}\left(\frac{j''}{j'} - l\frac{\tilde{j}''}{\tilde{j}'}\right) + \frac{l}{4}\left(\frac{E_4^2(q)}{E_6(q)} - l\frac{E_4^2(q^l)}{E_6(q^l)}\right) + \frac{l}{3}\left(\frac{E_6(q)}{E_4(q)} - l\frac{E_6(q^l)}{E_4(q^l)}\right) \, . \end{aligned} \tag{26}$$

Recall that our first step in computing F_l is to find its first coefficient, the negated sum of its roots. Reducing p_1 modulo $\mathfrak{B}$, we have the sum of the x-coordinates of points in the kernel of the isogeny. But the x-coordinates are precisely the roots of F_l. Hence, we conclude that the first coefficient is $-p_1/2$.

There are two important remarks to be made here. The first is that even though the development above was complex analytic in nature, all of the computations can in fact be carried out in $\mathbb{F}_p$. The second remark is that in practice one does not use the modular polynomials Φ_l, as their coefficients grow rapidly. There are alternative polynomials that have similar properties to the modular polynomials while having less and smaller coefficients. One example is Müller's modular polynomials $G_l(x, y)$ [6].

The second step is to find the rest of the coefficients of F_l, using the knowledge of p_1. Recall from Section 3.5 that an elliptic curve E corresponds to a lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ for some $\omega_1, \omega_2 \in \mathbb{C}$. Let $\Lambda_1 = \omega_1\mathbb{Z} + l\omega_2\mathbb{Z}$ and consider the map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_1$ given by $z \mapsto lz$. Taking this modulo the prime ideal $\mathfrak{B}$, we obtain the l-isogeny $E \to \tilde{E}$ discussed in Page 43.

However, Schoof finds it easier to work with a different isogeny. Define $\Lambda_2 = \frac{1}{l}\omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ and consider the map $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_2$ given by $z \mapsto z$. Reducing this map modulo $\mathfrak{B}$, we now have an isogeny $E \to E'$ for some elliptic curve E'. Note that $\Lambda_1 = l\Lambda_2$, so by Proposition 6, the two curves $\tilde{E}$ and E' are isomorphic. Thus, the two isogenies have the same kernel, so the computation of p_1 is unchanged. From the equations of g_2 and g_3 in Theorem 3 we find that $E' : y^2 = x^3 + l^4\tilde{a}_4 x + l^6\tilde{a}_6$.

Let $\wp(z)$ be the Weierstrass $\wp$-function associated with Λ and write

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k}$$

for the Laurent series of $\wp$ at infinity. The coefficients c_k are given by the following recursion:

$$c_1 = -\frac{a_4}{5} \, , \quad c_2 = -\frac{a_6}{7} \, , \quad c_k = \frac{3}{(k-2)(2k+3)} \sum_{j=1}^{k-2} c_j c_{k-1-j} \, , \quad k \geq 3 \, . \tag{27}$$

We make similar computations for the Weierstrass $\wp$-function of Λ_2 and find the corresponding coefficients $\tilde{c_i}$.

Lastly, we have this final theorem that allows us to obtain all the coefficients of F_l in an efficient way.

Theorem 11. *Let l be prime and F_l be the polynomial that vanishes on the x-coordinates of the points in the kernel of the isogeny $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_2$ with lattices as defined above. Then*

$$z^{l-1}F_l(\wp(z)) = \exp\left(-\frac{1}{2}p_1z^2 - \sum_{k=1}^{\infty}\frac{\tilde{c_k} - lc_k}{(2k+1)(2k+2)}z^{2k+2}\right) . \tag{28}$$

Proof. See [19, page 252] □

By expanding the expressions on both sides of Equation (28), we can find the coefficients of $F_l(x) = x^{(l-1)/2} + a_{(l-3)/2}x^{(l-3)/2} + \cdots + a_0$. We give here the first three:

$$\begin{aligned}
a_{(l-3)/2} &= -\frac{p_1}{2} , \\
a_{(l-5)/2} &= \frac{p_1^2}{8} - \frac{\tilde{c_1} - lc_1}{12} - \frac{l-1}{2}c_1 , \\
a_{(l-7)/2} &= -\frac{p_1^3}{48} - \frac{\tilde{c_2} - lc_2}{30} + \frac{\tilde{c_1} - lc_1}{24}p_1 - \frac{l-1}{2}c_2 + \frac{l-3}{4}c_1p_1 .
\end{aligned}$$

Schoof [19] remarks that the denominators in the expressions for a_i are products of small primes. Thus, over a large prime field there is no risk that the denominators will vanish.

Example 5. We continue with the same curve $E_1/\mathbb{F}_{17}$ as in the previous examples. In this example we find F_3. We recall the following facts: (i) 3 is an Elkies prime for this curve; (ii) the j-invariant of E_1 is 1; and (iii) $\gcd(\Phi_3(x,1), x^{17} - x) = x + 5$. Note that the degree of F_3 is $(3-1)/2 = 1$, so only one coefficient, $-p_1/2$, needs to be found.

First we use Equations (8) and (22) to find

$$E_4(q) \equiv 3 \pmod{\mathfrak{B}} , \qquad E_6(q) \equiv -6 \pmod{\mathfrak{B}} , \qquad j' = 2 .$$

From the gcd above, we know that we must set $\tilde{\jmath} = -5$. Next, we compute

$$\Phi_x(j, \tilde{\jmath}) \equiv -1 \pmod{17} , \qquad \Phi_y(j, \tilde{\jmath}) \equiv 2 \pmod{17} .$$

Using Equation (23) and then (25), we find

$$\tilde{\jmath}' \equiv 6 \pmod{17} , \qquad E_4(q^l) \equiv 3 \pmod{\mathfrak{B}} , \qquad E_6(q^l) \equiv 7 \pmod{\mathfrak{B}} .$$

In particular, the isogenous curve is $\tilde{E} : y^2 = x^3 + x - 8$.

The next step is to find $j''/j' - l\tilde{\jmath}''/\tilde{\jmath}'$ using Equation (24). We first compute

$$\Phi_{xx}(j, \tilde{\jmath}) \equiv 6 \pmod{17}\,, \quad \Phi_{xy}(j, \tilde{\jmath}) \equiv -2 \pmod{17}\,, \quad \Phi_{yy}(j, \tilde{\jmath}) \equiv -1 \pmod{17}\,.$$

It follows that

$$\frac{j''}{j'} - l\frac{\tilde{\jmath}''}{\tilde{\jmath}'} \equiv -1 \pmod{17}\,.$$

To assist in the computations above, some relevant SAGE source code is provided in Figure 8 in the appendix.

Now we can find $p_1 = 4$ using Equation (26). Therefore, $F_3 = x - 2$. ◇

4.6 Combining information

The final step in the algorithm is to combine the information given to us by the Atkin and Elkies procedures. Unlike Schoof's original algorithm, the Chinese remainder theorem does not suffice here. The reason is that Atkin's procedure provides us with a *set* T_l of possible traces for each Atkin prime l, rather than a unique trace. Therefore another approach must be taken.

One possibility is to consider more primes l_i than the minimum needed by the condition $\prod_{i=1}^{r} l_i > 4\sqrt{p}$ until there are sufficiently many primes to recover the trace t. However, in practice a variant of the so-called *baby-step/giant-step (BSGS)* algorithm is taken, which allows to compute t modulo the product of the Atkin primes.

The BSGS algorithm, due to Shanks, is a time/space tradeoff algorithm and is one of the generic methods of solving the DLP. As explained in [6], the algorithm's running time is in the order of $O(\sqrt{n})$, where n is the order of the underlying abelian group. In this algorithm, one first computes a set of values (baby steps) and stores them in a table. With the running time assumption as above, the space needed for the table is also in the order of $O(\sqrt{n})$. Next one computes another set of values (giant steps), each time comparing the current value with the ones stored in table. When a match is found, the algorithm terminates and the DLP can be solved. The variant used in the `SEA` algorithm is explained in much more detail below.

We follow the discussion in [6]. To find the trace t, we first compute the trace t_E modulo the product m_E of the Elkies primes. This is done using the Chinese remainder theorem. Next, we split the set of Atkin primes into two, one with a product m_1 and the other with a product m_2. Using the Chinese remainder theorem on each of these sets, we construct two sets S_1 and S_2 such that

$$t \equiv t_1 \pmod{m_1} \text{ with } t_1 \in S_1\,, \qquad t \equiv t_2 \pmod{m_2} \text{ with } t_2 \in S_2\,.$$

We choose the sets such that the each one has approximately the same number of possible traces modulo the corresponding product m_1 or m_2.

Therefore, we can write

$$t = t_E + m_E(m_1 r_2 + m_2 r_1) \tag{29}$$

for some integers r_1 and r_2. Taking the above equation modulo m_1, we see that $t_1 \equiv t_E + m_E m_2 r_1 \pmod{m_1}$. Similarly we can reduce modulo m_2 and find that

$$r_1 \equiv \frac{t_1 - t_E}{m_E m_2} \pmod{m_1}\,, \quad r_2 \equiv \frac{t_2 - t_E}{m_E m_1} \pmod{m_2}\,. \tag{30}$$

Of course, the exact values of t_1 and t_2 is not yet known. The procedure henceforth is to determine r_1 and r_2 and the recover t using Equation (29). This procedure is reasonably fast due to the following lemma, which establishes a bound on the sizes of r_1 and r_2.

Lemma 4. *Consider Equation* (29)*. If we choose* $0 \leq t_E < m_E$ *and* $|r_1| \leq \lfloor \frac{m_1}{2} \rfloor$*, then* $|r_2| \leq m_2$*.*

Proof. We can rewrite Equation (29) to have $r_2 = \frac{t - t_E - m_E m_2 r_1}{m_E m_1}$. Then, recalling that by assumption $m_E m_1 m_2 > 4\sqrt{p}$ and $|t| \leq 2\sqrt{p}$,

$$\begin{aligned} |r_2| &\leq \frac{|t| + |t_E| + m_E m_2 |r_1|}{m_E m_1} \leq \frac{2\sqrt{p}}{m_E m_1} + \frac{1}{m_1} + \frac{m_2}{2} \\ &\leq \frac{m_2}{2} + \frac{1}{m_1} + \frac{m_2}{2} = m_2 + \frac{1}{m_1}\,. \end{aligned}$$

Since m_1, m_2, and r_2 are all integers, it follows that $|r_2| \leq m_2$, as needed. □

Recall that the order of group $E(\mathbb{F}_p)$ is $p + 1 - t$. Thus, for any $\mathbb{F}_p$-rational point P of E, we have $[p+1]P = [t]P = [t_E + m_E(m_1 r_2 + m_2 r_1)]P$. Therefore, we can write $[p + 1 - t_E]P - [r_1 m_2 m_E]P = [r_2 m_1 m_E]P$. We shall consider the expression on the left-hand side as the one defining the baby steps. The expression on the right is the one defining the giant steps.

Specifically, we first pick a random point P on $E/\mathbb{F}_p$. Then we go over the possible values of t_1. For each such value, we use Equation (30) to choose r_1 such that $|r_1| \leq \lfloor \frac{m_1}{2} \rfloor$. The next step is to compute $Q_{r_1} = [p + 1 - t_E]P - [r_1 m_2 m_E]P$ and store the tuple (Q_{r_1}, r_1) in a table. It is important to keep the table sorted to speed up the procedure. Up to here is the analogue of the baby step part.

Next, we iterate over the possible values of t_2. From Lemma 4 we only that the value of r_2 we seek satisfies $|r_2| \leq m_2$. We also know that r_2 satisfies Equation (30). This allows us to construct a set $R_2^{t_2}$ of possible r_2 values corresponding to t_2. For each such possible value, we compute $Q'_{r_2} = [r_2 m_1 m_E]P$ and compare it to the values we stored in the table. We continue until a match is found.

Once a match is found, we can recover the value t from Equation (29). Then, the order of the group of $\mathbb{F}_p$-rational points is determined from Hesse's equation (13). Blake, Seroussi, and Smart [6] note that in practice there are still some tests to be made to make sure we indeed have the correct group order and that the group suffices for cryptographic purposes.

4.7 Complete SEA algorithm

The running time of the SEA algorithm is in the order of $O(\log^{2+2\mu} p)$ and the storage requirement is in the order of $O(\log^2 p)$, as discussed in [13].

We provide here the full SEA algorithm in pseudo-code, adapted from and expanded on the one in [6]. The algorithm we provide is not efficient, in the sense that some of the computations are done multiple times and the use of method parameters is redundant and space-consuming. This was done to keep the important parts of the algorithm free of unnecessary clutter.

The main SEA algorithm is as given in Figure 5, where the first step of the Elkies procedure (*i.e.*, finding a factor of the division polynomial) is the algorithm given in Figure 4. We assumed that we have functions with the following signatures:

1. `NextPrime`(p)
   Input: A prime p.
   Output: The smallest prime number larger than p.

2. `FindNonSquareInFiniteField`(l)
   Input: A prime l.
   Output: An integer $0 < d < l$ with $\left(\frac{d}{l}\right) = -1$.

3. `GeneratorOfMultiplicativeGroup`(l, d)
   Input: A prime l and an integer d with $\left(\frac{d}{l}\right) = -1$.
   Output: A generator g of $\mathbb{F}_l[\sqrt{d}]^*$.

```
GetFactorOfDivisionPolynomial$(l, E, p)$
Input: An Elkies prime $l$ and an elliptic curve $E$ over a prime field $\mathbb{F}_p$.
Output: A factor $F_l(x)$ of degree $d = (l-1)/2$ of $f_l(x)$.

determine $j$ from Equation (5)
determine $E_4(q), E_6(q) \mod \mathfrak{B}$ from Equation (8)
determine $j'$ from Equation (22)
$\tilde{\jmath} \leftarrow$ a root of $\Phi_l(x, j)$ in $\mathbb{F}_p$
determine $\tilde{\jmath}'$ from Equation (23)
determine $j''/j' - l\tilde{\jmath}''/\tilde{\jmath}'$ from Equation (24)
determine $E_4(q^l), E_6(q^l) \mod \mathfrak{B}$ from Equation (25)
determine $p_1$ from Equation (26)
determine $c_k$ and $\tilde{c_k}$ for $k \leq d$ from Equation (27)
determine $F_l$ from Equation (28)
return $F_l(x)$
```

Figure 4: Factor of division polynomial

```
SchoofElkiesAtkinAlgorithm($E, p$)
Input: An elliptic curve $E$ over a prime field $\mathbb{F}_p$.
Output: The order of $E(\mathbb{F}_p)$.
```

```
$M \leftarrow 1$, $l \leftarrow 2$, $A_p \leftarrow \{\}$, $E_p \leftarrow \{\}$
determine $j$ from Equation (5)
while $M < 4\sqrt{p}$ do
    if $\deg(\gcd(\Phi_l(x, j), x^p - x)) = 0$ then                    // Atkin prime
        $T \leftarrow \{\}$
        determine $r$ from Theorem 9
        $d \leftarrow$ FindNonSquareInFiniteField($l$)
        $g \leftarrow$ GeneratorOfMultiplicativeGroup($l, d$)
        $S \leftarrow \{g^{i(l^2-1)/r} \mid \gcd(i, r) = 1\}$
        for each $\gamma_i \in S$ do
            write $\gamma_i = g_{i_1} + \sqrt{d} g_{i_2}$
            $z \leftarrow p(g_{i_1} + 1)/2 \pmod{l}$
            if $\left(\frac{z}{l}\right) = 1$ then
                $x \leftarrow \sqrt{z} \pmod{l}$
                $T \leftarrow T \cup \{2x, -2x\}$
        $A_p \leftarrow A_p \cup (T, l)$
    else                                                               // Elkies prime
        $F_l(x) \leftarrow$ GetFactorOfDivisionPolynomialFactor($l, E, p$)
        find $\lambda$ such that $\gcd(\psi_\lambda^2(x^p - x) + \psi_{\lambda-1}\psi_{\lambda+1}, F_l(x)) \neq 1$
        $t \leftarrow \lambda + \lambda/p \pmod{l}$
        $E_p \leftarrow E_p \cup \{(t, l)\}$
    $M \leftarrow M \times l$
    $l \leftarrow$ NextPrime($l$)
recover $t$ using the sets $A_p$ and $E_p$, as explained in Section 4.6
return $p + 1 - t$
```

Figure 5: SEA algorithm

A Appendix

We present in the appendix SAGE code that was applied in Examples 1, 2, and 5.

```
sage: #== General Definitions ==#
sage: R = IntegerModRing(17)
sage: x = PolynomialRing(GF(17), 'x').gen()
sage: E1 = EllipticCurve([GF(17)(0),0,0,1,2]); E1
  Elliptic Curve defined by y^2  = x^3 + x + 2 over Finite Field of size 17}

sage: j = E1.j_invariant(); j
  1

sage: P1 = PolynomialRing(GF(17), 'x'); x = P1.gen()
sage: f5 = 5*x^12 - 6*x^10 - 5*x^9 - 3*x^8 + 4*x^7 - 2*x^6 + 2*x^5 - 2*x^4 - 6*x^3 - 7*x^2 + x - 7
sage: # F_{17}[a]/(f_5) is the univariate ring we work over.
sage: # It is not taken modulo the curve equation, so we have to carry the y's manually.
sage: F17f5 = P1.quotient(f5, 'a'); a = F17f5.gen(); F17f5
  Univariate Quotient Polynomial Ring in a over Finite Field of size 17 with modulus 5*x^12
  + 11*x^10 + 12*x^9 + 14*x^8 + 4*x^7 + 15*x^6 + 2*x^5 + 15*x^4 + 11*x^3 + 10*x^2 + x + 10

sage: #== Computing lambda ==#
sage: # numeratorOfLambda is the numerator of lambda, divided by y
sage: numeratorOfLambda = 32*(a^3 + a + 2)^((17^2+3)/2) - 4*(a^6 + 5*a^4 + 40*a^3 - 5*a^2 - 8*a - 33)
sage: denominatorOfLambda = 32*(a^3 + a + 2)^2*(a^(17^2) - a) + 8*(a^3 + a + 2)*(3*a^4 + 6*a^2 + 24*a - 1)
sage: # lambda5 is lambda, divided by y
sage: lambda5 = numeratorOfLambda/denominatorOfLambda; lambda5
  9*a^11 + 14*a^10 + 14*a^9 + 14*a^8 + 15*a^7 + 12*a^6 + a^5 + 15*a^4 + 10*a^3 + 9*a^2 + 4*a + 6

sage: #== Computing the expression for y_5 ==#
sage: # y5 is y_5, divided by y
sage: y5 = lambda5*(2*a^(17^2) - lambda5^2*(a^3 + a + 2) + a - (3*a^4 + 6*a^2 + 24*a - 1)
/(4*(a^3 + a + 2))) - (a^3 + a + 2)^((17^2-1)/2); y5
  14*a^11 + 11*a^10 + 11*a^9 + 6*a^8 + 3*a^7 + 7*a^6 + 12*a^5 + 6*a^4 + 15*a^3 + 11*a^2 + 15*a + 13

sage: #== Comparing y_5 with y^{17} ==#
sage: (a^3 + a + 2)^8 + y5
  0
```

Figure 6: Example 1 (SAGE code)

```
sage: # Phi_3(x,j=1):
sage: c1 = R(2232)
sage: c2 = R(-1069956)
sage: c3 = R(3686400)
sage: c4 = R(2587918086)
sage: c5 = R(8900222976000)
sage: c6 = R(452984832000000)
sage: c7 = R(-770845966336000000)
sage: c8 = R(1855425871872000000000)
sage: a4 = 1              # Coefficient of x^4
sage: a3 = R(-1+c1+c2+c3) # Coefficient of x^3
sage: a2 = R(c1+c4+c5+c6) # Coefficient of x^2
sage: a1 = R(c2+c5+c7+c8) # Coefficient of x
sage: a0 = R(1+c3+c6+c8)  # Scalar
sage: Phi3 = a4*x^4 + a3*x^3 + a2*x^2 + a1*x + a0; Phi3
  x^4 + 12*x^3 + 4*x^2 + 16*x + 5

sage: # This shows that Phi_3 is an Elkies prime for E_1.
sage: # The root of the linear factor is the j-invariant of an isogenous curve.
sage: Phi3.factor()
  (x + 5) * (x^3 + 7*x^2 + 3*x + 1)

sage: # Phi_5(x,j=1):
sage: d1 = R(3720)
sage: d2 = R(-4550940)
sage: d3 = R(2028551200)
sage: d4 = R(-246683410950)
sage: d5 = R(1963211489280)
sage: d6 = R(1665999364600)
sage: d7 = R(107878928185336800)
sage: d8 = R(383083609779811215375)
sage: d9 = R(128541798906828816384000)
sage: d10 = R(1284733132841424456253440)
sage: d11 = R(-441206965512914835246100)
sage: d12 = R(26898488858380731577417728000)
sage: d13 = R(-192457934618928299655108231168000)
sage: d14 = R(280244777828439527804321565297868800)
sage: d15 = R(5110941777552418083110765199360000)
sage: d16 = R(36554736583949629295706472332656640000)
sage: d17 = R(6692500042627997708487149415015068467200)
sage: d18 = R(-264073457076620596259715790247978782949376)
sage: d19 = R(53274330803424425450420160273356509151232000)
sage: d20 = R(141359947154721358697753474691071362751004672000)
sage: b6 = 1                           # Coefficient of x^6
sage: b5 = R(-1+d1+d2+d3+d4+d5)        # Coefficient of x^5
sage: b4 = R(d1+d6+d7+d8+d9+d10)       # Coefficient of x^4
sage: b3 = R(d2+d7+d11+d12+d13+d14)    # Coefficient of x^3
sage: b2 = R(d3+d8+d12+d15+d16+d17)    # Coefficient of x^2
sage: b1 = R(d4+d9+d13+d16+d18+d19)    # Coefficient of x
sage: b0 = R(1+d5+d10+d14+d17+d19+d20) # Scalar
sage: Phi5 = b6*x^6 + b5*x^5 + b4*x^4 + b3*x^3 + b2*x^2 + b1*x + b0; Phi5
  x^6 + 6*x^5 + 15*x^4 + 3*x^3 + 10*x^2 + 11*x + 9

sage: # This shows that 5 is an Atkin prime for E_1.
sage: gcd(Phi5, x^17 - x)
  1
```

Figure 7: Example 2 (SAGE code)

```
sage: #== Finding the partial derivatives of Phi_3, evaluated at j = 1 and \tilde{j} = -5 ==#
sage: tj = R(-5)
sage: Phi3x = R(4*j^3 - 3*j^2*tj^3 + 3*c1*j^2*tj^2 + 2*c1*j*tj^3 + 3*c2*j^2*tj + c2*tj^3
+ 3*c3*j^2 + 2*c4*j*tj^2 + 2*c5*j*tj + c5*tj^2 + 2*c6*j + c7*tj + c8); Phi3x
  16

sage: Phi3y = R(4*tj^3 - 3*tj^2*j^3 + 3*c1*tj^2*j^2 + 2*c1*tj*j^3 + 3*c2*tj^2*j + c2*j^3
+ 3*c3*tj^2 + 2*c4*tj*j^2 + 2*c5*tj*j + c5*j^2 + 2*c6*tj + c7*j + c8); Phi3y
  2

sage: Phi3xx = R(12*j^2 - 6*j*tj^3 + 6*c1*j*tj^2 + 2*c1*tj^3 + 6*c2*j*tj + 6*c3*j + 2*c4*tj^2
+ 2*c5*tj + 2*c6); Phi3xx
  6

sage: Phi3yy = R(12*tj^2 - 6*tj*j^3 + 6*c1*tj*j^2 + 2*c1*j^3 + 6*c2*tj*j + 6*c3*tj + 2*c4*j^2
+ 2*c5*j + 2*c6); Phi3yy
  16

sage: Phi3xy = R(-9*j^2*tj^2 + 6*c1*j^2*tj + 6*c1*j*tj^2 + 3*c2*j^2 + 3*c2*tj^2 + 4*c4*j*tj
+ 2*c5*j + 2*c5*tj + c7); Phi3xy
  15
```

Figure 8: Example 5 (SAGE code)

References

[1] ANSI, *Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA)*, Tech. Report ANSI X9.62, American National Standards Institute, 2005.

[2] Roberto M. Avanzi, *Generic algorithms for computing discrete logarithms*, Handbook of Elliptic and Hyperelliptic Curve Cryptography (Henri Cohen and Gerhard Frey, eds.), Chapman & Hall/CRC, 2006, pp. 477–494.

[3] Roberto M. Avanzi and Tanja Lange, *Introduction to public-key cryptography*, Handbook of Elliptic and Hyperelliptic Curve Cryptography (Henri Cohen and Gerhard Frey, eds.), Chapman & Hall/CRC, 2006, pp. 1–15.

[4] Roberto M. Avanzi and Nicolas Thériault, *Index calculus*, Handbook of Elliptic and Hyperelliptic Curve Cryptography (Henri Cohen and Gerhard Frey, eds.), Chapman & Hall/CRC, 2006, pp. 495–509.

[5] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid, *Recommendation for key management—part 1: General (revised)*, Tech. Report NIST Special Publication 800-57, National Institute of Standards and Technology, May 2006.

[6] Ian Blake, Gadiel Seroussi, and Nigel Smart, *Elliptic curves in cryptography*, Undergradute Texts in Mathematics, Springer-Verlag, 2006.

[7] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, Journal of London Mathematical Society **41** (1966), 193–291.

[8] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory **IT-22** (1976), no. 6, 644–654.

[9] Christophe Douce and Tanja Lange, *Arithmetic of elliptic curves*, Handbook of Elliptic and Hyperelliptic Curve Cryptography (Henri Cohen and Gerhard Frey, eds.), Chapman & Hall/CRC, 2006, pp. 267–302.

[10] Gerhard Frey and Tanja Lange, *Transfer of discrete logarithms*, Handbook of Elliptic and Hyperelliptic Curve Cryptography (Henri Cohen and Gerhard Frey, eds.), Chapman & Hall/CRC, 2006, pp. 529–543.

[11] Serge Lang, *Elliptic curves: Diophantine analysis*, A Series of Comprehensive Studies in Mathematics 231, Springer-Verlag, 1978.

[12] ______, *Elliptic functions*, 2nd ed., Gradute Texts in Mathematics, Springer-Verlag, 1987.

[13] Reynald Lercier, David Lubicz, and Frederik Vercauteren, *Point counting on elliptic and hyperelliptic curves*, Handbook of Elliptic and Hyperelliptic Curve Cryptography (Henri Cohen and Gerhard Frey, eds.), Chapman & Hall/CRC, 2006, pp. 407–453.

[14] Reynald Lercier and François Morain, *Counting points on elliptic curves over f_{p^n} using couveignes's algorithm*, 1996, ⟨`http://citeseer.ist.psu.edu/article/lercier96counting.html`⟩.

[15] Julio López and Ricardo Dahab, *An overview of elliptic curve cryptography*, Institute of Computing, State University of Campinas, May 2000.

[16] Alfred J. Menzes, Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of applied cryptography*, CRC Press, 1996.

[17] Volker Müller, *Ein algorithmus zur bestimmung der punktanzahl elliptischer kurven über endlichen körpern der charakteristik größer drei*, Ph.D. thesis, Saarlandes University, Saarbrücken, 1995.

[18] René Schoof, *Elliptic curve over finite fields and the computation of square roots mod p*, Mathematics of Computation **44** (1985), no. 170, 483–495.

[19] ______, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres **7** (1995), 219–254.

[20] Joseph H. Silverman, *The arithmetic of elliptic curves*, Gradute Texts in Mathematics, Springer-Verlag, 1986.

[21] ______, *Advanced topics in the arithmetic of elliptic curves*, Gradute Texts in Mathematics, Springer-Verlag, 1994.

[22] William Stein, David Kohel, and Iftikhar Burhanuddin, *Module of supersingular points*, 2006, ⟨`http://sage.math.washington.edu/home/burhanud/SSMod/ssmod.py.txt`⟩.

[23] Frederik Vercauteren, *The SEA algorithm in characteristic 2*, ⟨`http://citeseer.ist.psu.edu/663372.html`⟩.