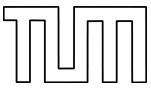


TECHNISCHE UNIVERSITÄT MÜNCHEN
FAKULTÄT FÜR MATHEMATIK

Bachelor's Thesis in Mathematics

Schoof's algorithm for elliptic curves

Lorenz Panny

Advisor: Prof. Dr. Gregor Kemper
Date: July 15, 2015

I assure the single-handed composition of this thesis only supported by declared resources.

Garching, July 15, 2015

Contents

1 Introduction

Elliptic curves, a certain class of algebraic varieties, have a long-standing history of great importance in algebraic geometry, culminating in Andrew Wiles' 1993 proof of Fermat's last theorem (for all integers $n > 2$, there are no positive integers a, b, c such that $a^n + b^n = c^n$). In recent decades, elliptic curves have received increased attention in algorithmic number theory and cryptography, thereby yielding factorization algorithms as well as asymmetric encryption and signature schemes, to name only a few of countless applications (see Section 4 for introductory examples).

In simple terms, an elliptic curve is the set of zeroes of a special form of polynomial over a finite field which can be equipped with an abelian group structure. In the cryptographic context, it typically serves as a replacement for the (traditionally wide-spread) multiplicative groups of finite fields. For most cryptosystems that can be built from elliptic curves, or finite abelian groups in general, precise knowledge of the group order is crucial for evaluating the security of the system; for (a small subset of) potential attacks see Section 4.

This document's main topic is *Schoof's algorithm*, a polynomial-time algorithm for computing the number of points on an elliptic curve over a finite field. It was discovered in 1985 by René Schoof (hence the name). The algorithm works by computing the number of points (or strictly speaking, the very closely related trace of the Frobenius endomorphism) modulo a set of small primes and then lifting the result to the integers using the Chinese remainder theorem. Doing so requires a priori knowledge of a bound on the number of points; this is provided by Hasse's theorem (Section 5.4), which is interesting in its own right.

Despite being outperformed in practice by more recent developments such as, most prominently, the SEA algorithm [4, Section VII.2], the ideas underlying Schoof's algorithm still remain the basis of those improvements, which definitely makes it worth studying.

2 Algebraic varieties

In order to define elliptic curves and show some of their properties required for Schoof's algorithm, we first need to establish some general theory of algebraic varieties.

The definitions in this section follow Silverman [19] unless noted otherwise; for brevity we refrain from adding references individually.

Let K denote a field with algebraic closure $\bar{K}$.

2.1 Affine varieties

Definition 1. Any set $V \subseteq \bar{K}^n$ that admits a description of the form

$$V = \{\, P \in \bar{K}^n \mid \forall f \in \mathcal{I}.\ f(P) = 0 \,\},$$

where $\mathcal{I}$ is an ideal of the polynomial ring $\bar{K}[X_1, \ldots, X_n]$, is called *affine algebraic set*. The affine algebraic set obtained from a given ideal $\mathcal{I}$ is denoted by $V(\mathcal{I})$.
Conversely, a given affine algebraic set V's *ideal* $\mathcal{I}(V)$ is defined by

$$\mathcal{I}(V) = \{\, f \in \bar{K}[X_1, \ldots, X_n] \mid \forall P \in V.\ f(P) = 0 \,\},$$

and its *ideal over* K is $\mathcal{I}(V/K) = \mathcal{I}(V) \cap K[X_1, \ldots, X_n]$.

We say that V is *defined over* K, symbolically V/K, if the ideal $\mathcal{I}(V)$ is generated by polynomials in $K[X_1, \ldots, X_n]$. If this is the case, the set of *K-rational points* of V is defined as

$$V(K) = V \cap K^n = \{\, P \in K^n \mid \forall f \in \mathcal{I}(V).\ f(P) = 0 \,\}.$$

Definition 2. An *affine variety* is an affine algebraic set whose ideal is prime over $\bar{K}$.

Definition 3. Let $V \subseteq \bar{K}^n$ be an affine variety defined over K. The *coordinate ring* of V over K is

$$K[V] = K[X_1, \ldots, X_n]/\mathcal{I}(V/K).$$

Intuitively, this ring consists of n-variate polynomials over K, two of which are identified if their difference vanishes on the whole variety V; thus one may rewrite subterms using the relations given by $\mathcal{I}(V/K)$ without changing the considered function in any way.

The ring $K[V]$'s quotient field, denoted $K(V) = \mathrm{Quot}(K[V])$, is called *function field* of V over K and its elements are called *rational functions* on V.

Definition 4. The *dimension* $\dim V$ of an affine variety V is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

Definition 5. Let V be an affine variety whose ideal is generated by $f_1, \ldots, f_n \in \bar{K}[X_1, \ldots, X_m]$. Then V is said to be *nonsingular* or *smooth* at P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{i,j}$$

has rank $n - \dim V$ and *singular* otherwise. As usual, V is called *smooth* if it has no singular points.

2.2 Projective varieties

Definition 6. A polynomial $f \in \bar{K}[X_0, \ldots, X_n]$ is called *homogenous* if all of its monomials are of the same degree. A *homogenous* ideal is one that is generated by a finite set of homogenous polynomials.

Definition 7. *Projective n-space* over $\bar{K}$ is defined as

$$\mathbb{P}^n = \mathbb{P}^n\bar{K} = (\bar{K}^{n+1} \setminus \{0\})/\sim,$$

where the equivalence relation $\sim$ is given by

$$v \sim w \quad :\Longleftrightarrow \quad \exists \lambda \in \bar{K}^*.\ v = \lambda w.$$

We denote by $[x_0 : \cdots : x_n]$ the equivalence class of $(x_0, \ldots, x_n)$ under $\sim$ and refer to the individual x_i as *homogenous coordinates* of the represented point. The set of *K-rational points* in $\mathbb{P}^n$, denoted $\mathbb{P}^n K$, is the set of those points in $\mathbb{P}^n$ which can be represented by coordinates in K.

Definition 8. Any set $V \subseteq \mathbb{P}^n$ that admits a description of the form

$$V = \{\, P \in \mathbb{P}^n \mid \forall f \in \mathcal{I}.\ f(P) = 0 \,\},$$

where $\mathcal{I}$ is a homogenous ideal of the polynomial ring $\bar{K}[X_0, \ldots, X_n]$, is called *projective algebraic set*. The algebraic set obtained from a given homogenous ideal $\mathcal{I}$ is denoted by $V(\mathcal{I})$.
Conversely, a given projective algebraic set V's *ideal* $\mathcal{I}(V)$ is the ideal generated by the homogenous polynomials vanishing on V, that is

$$\mathcal{I}(V) = (\{\, f \in \bar{K}[X_0, \ldots, X_n] \text{ homogenous} \mid \forall P \in V.\ f(P) = 0 \,\}),$$

and its *ideal over* K is $\mathcal{I}(V/K) = \mathcal{I}(V) \cap K[X_0, \ldots, X_n]$.

Just like in the affine case, we say that a projective variety V is *defined over* K if $\mathcal{I}(V)$ is generated by homogenous polynomials over K. In this case, the set of K*-rational points* of V is defined as

$$V(K) = V \cap \mathbb{P}^n K = \{\, P \in \mathbb{P}^n K \mid \forall f \in \mathcal{I}(V).\ f(P) = 0 \,\}.$$

Remark. An ideal $\mathcal{I}$ being generated by homogenous polynomials implies that the corresponding projective algebraic set is well-defined: For $f \in \mathcal{I}$ of degree d and $\lambda \in \bar{K} \setminus \{0\}$, we have $f(\lambda P) = \lambda^d f(P) = 0$ if and only if $f(P) = 0$, hence the predicate $f(P) \stackrel{?}{=} 0$ is independent of the choice of homogenous coordinates for P.

Definition 9. A *projective (algebraic) variety* is a projective algebraic set whose ideal is prime over $\bar{K}$.

Definition 10. By intersecting a projective algebraic set V with

$$U_i := \{\, [x_0 : \cdots : x_n] \in \mathbb{P}^n \mid x_i \neq 0 \,\}$$

and mapping each equivalence class to the unique representant which satisfies $x_i = 1$, we can obtain an affine algebraic set A: Its ideal is given by

$$\mathcal{I}(A) = \{\, f(X_1, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n) \mid f \in \mathcal{I}(V) \,\},$$

and the process of obtaining A from V is known as *dehomogenization* with respect to X_i.

Definition 11. On the other hand, there is a unique (up to permutation of variables) projective algebraic set associated with each affine algebraic set: From a polynomial $f \in \bar{K}[X_1, \ldots, X_n]$, we obtain the *homogenization* of f, denoted $\bar{f}$, by multiplying each monomial in f by an appropriate power of a fresh variable Y such that the resulting polynomial is homogenous of minimum degree. Now the *projective closure* of an affine algebraic set V, denoted $\bar{V}$, is defined by the homogenous ideal

$$\mathcal{I}(\bar{V}) = (\{\, \bar{f} \mid f \in \mathcal{I}(V) \,\}) \subseteq \bar{K}[X_1, \ldots, X_n, Y],$$

where again $\mathcal{I}(\bar{V})$ is the ideal *generated by* $\{\, \bar{f} \mid f \in \mathcal{I}(V) \,\}$.

Example. For the cubic polynomial $f = Y^2 - X^3 - aX - b \in \bar{K}[X, Y]$, we have the homogenization $\bar{f} = Y^2Z - X^3 - aXZ^2 - bZ^3 \in \bar{K}[X, Y, Z]$.

Definition 12. We shall refer to the points that are only present in the projective "version" of a variety, that is, those with the additional coordinate being zero, as *points at infinity*, while all the other points are called *finite*.

Lemma 13 (Silverman [19, Proposition I.2.6])**.** If V is an affine variety, then $\bar{V}$ is a projective variety and V is the dehomogenization of $\bar{V}$ with respect to the additional coordinate.

If V is a projective variety, then each of its dehomogenizations is an affine variety which is either empty or has V as its projective closure.

It is easy to see from the definitions that dehomogenization and projective closure preserve the property of being defined over K.

Remark. The preceding lemma legitimates that one may use affine and projective varieties somewhat interchangeably, depending on the context: For instance, it is customary to define a projective variety by giving inhomogenous equations and understanding that one really meant the projective closure.

Definition 14. The *function field* over K of a projective variety V is taken to be the set $K(V)$ of rational functions $f/g \in \mathrm{Quot}(K[V])$ such that f and g have representants in $K[X_0, \ldots, X_n]$ which are homogenous of the same degree.

Lemma 15. If A is a non-empty dehomogenization of a projective variety V, then

$$K(A) \cong K(V).$$

Definition 16. We call a projective variety *smooth* if one of its non-empty dehomogenizations is smooth.

2.3 Rational maps and morphisms

Definition 17. Let V be a variety and $P \in V$ a point. A rational function $f/g \in K(V)$ is called *regular* or *defined* at P if there is some $\alpha \in K(V)^*$ such that it makes sense to evaluate $(\alpha f)/(\alpha g)$ at P, that is, if αg is non-zero at P.

Definition 18. Let $V_1 \subseteq \mathbb{P}^m$ and $V_2 \subseteq \mathbb{P}^n$ be projective varieties. A *rational map* from V_1 to V_2 is a tuple

$$\varphi = [\varphi_0, \ldots, \varphi_n]$$

of homogenous polynomials $\varphi_i \in \bar{K}[X_0, \ldots, X_m]$ of the same degree such that for all $f \in \mathcal{I}(V_2)$, we have $f(\varphi_0, \ldots, \varphi_n) \in \mathcal{I}(V_1)$.

Clearly we can evaluate φ at some point P by setting

$$\varphi(P) := [\varphi_0(P) : \cdots : \varphi_n(P)]$$

whenever one of the φ_i is non-zero at P. However, even if all φ_i vanish at P, one can potentially rewrite φ to make sense of it: We shall call φ *regular* or *defined* at a point $P \in V_1$ if there are homogenous polynomials $\phi_0, \ldots, \phi_n \in \bar{K}[X_0, \ldots, X_m]$ of the same degree such that $\forall i, j.\ \varphi_i\phi_j \equiv \varphi_j\phi_i \pmod{\mathcal{I}(V_1)}$ and some $\phi_i(P) \neq 0$. In that case, we define

$$\varphi(P) := [\phi_0(P) : \cdots : \phi_n(P)].$$

A rational map that is defined on the whole variety V_1 is called *morphism*.

Definition 19. Let $\varphi\colon V_1 \to V_2$ be a rational map. Precomposition with φ constitutes a homomorphism

$$\varphi^*\colon K(V_2) \to K(V_1),\ f \mapsto f \circ \varphi$$

of function fields, called the *pullback* of $K(V_2)$ along φ, so there is a field extension

$$K(V_1)/\varphi^*K(V_2).$$

We define the *degree* of φ to be

$$\deg \varphi = \begin{cases} [K(V_1) : \varphi^*K(V_2)] & \text{if } K(V_1)/\varphi^*K(V_2) \text{ is finite;} \\ 0 & \text{else.} \end{cases}$$

and similarly call φ *(in)separable* whenever $K(V_1)/\varphi^*K(V_2)$ has that property.

3 Elliptic curves

The usual abstract definition of elliptic curves requires the notion of a variety's *genus*, which is quite tedious to define and shall therefore be omitted.

Definition 20 (Silverman [19, Section III.3])**.** An *elliptic curve* is a smooth projective variety of genus one.

Instead, we will use a more accessible, equivalent characterization: One can show that each such variety can be made into a curve of comparably simple form by a linear change of coordinates:

Definition 21 (Blake, Seroussi, and Smart [4, Section III.1])**.** An *elliptic curve* is a smooth projective variety defined by a single equation of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

where a_1, a_3, a_2, a_4, a_6 are constants. This equation is known as the (long) *Weierstraß form* of the represented elliptic curve.
To a Weierstraß equation, one associates the quantities

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6, \quad b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Note that with these definitions, the smoothness requirement is equivalent to the *discriminant*

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

being distinct from zero.
For convenience and readability, we will usually define an elliptic curve by dehomogenizing the equation given above with respect to z, that is,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and understanding that this should denote the projective closure.

Lemma 22 (Washington [22, Section 2.1])**.** In the common case that $\operatorname{char} K \notin \{2, 3\}$, there is an even simpler normal form: Then each elliptic curve defined over K is isomorphic to a curve given by a *short Weierstraß equation*, that is

$$y^2 = x^3 + ax + b,$$

and its discriminant simplifies to

$$\Delta = -16(4a^3 + 27b^2).$$

Lemma 23. An elliptic curve has exactly one point at infinity.

Proof. Let E be an elliptic curve and assume $P = [x : y : 0] \in E$. This simplifies the Weierstraß equation to $0 = x^3$, hence $x = 0$; but at least one coordinate of P must be non-zero, therefore $P = [0 : 1 : 0]$. □

We will use the symbol ∞ to denote the point $[0 : 1 : 0]$.

Lemma 24 (Silverman [19, Proposition II.2.1])**.** Any rational map $\varphi\colon E \to V$ from a (smooth) elliptic curve E to a projective variety V is a morphism.

Lemma 25 (Silverman [19, Theorem II.2.3])**.** A morphism $\varphi\colon E_1 \to E_2$ of elliptic curves is either constant or surjective. The first case occurs if and only if $\deg \varphi = 0$.

Definition 26 (Silverman [19, Section III.4])**.** A morphism $\varphi\colon E_1 \to E_2$ of elliptic curves is called *isogeny* if it takes E_1's point at infinity to E_2's.

Lemma 27 (Silverman [19, Theorem III.4.10(c)])**.** Let $\varphi\colon E_1 \to E_2$ be a non-constant separable isogeny of elliptic curves. Then

$$\#\,\varphi^{-1}(\{\infty\}) = \deg \varphi.$$

3.1 The elliptic curve group

Of great interest in the study and applications of elliptic curves is the abelian group that can be constructed on its rational points, with the point at infinity as the neutral element. Using the standard Weierstraß representation $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$, the formulas describing the addition of two points on the curve are unfortunately a bit involved. It is convenient to give the formulas for affine coordinates using special cases for ∞, with the obvious homogenization for projective coordinates.

Algorithm 28 (Elliptic curve point addition)**.**
Input. Two points $P, Q \in E$.
Output. The sum $P + Q$.

1. **if** either $P = \infty$ or $Q = \infty$, **then return** the other.
2. $[x_1 : y_1 : 1] := P; \qquad [x_2 : x_2 : 1] := Q.$
3. **if** $x_1 \neq x_2$ **then**
   $$\lambda := \frac{y_2 - y_1}{x_2 - x_1}; \qquad \nu := \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$
   else if $-y_1 = y_2 + a_1x_2 + a_3$ or $2y_1 + a_1x_1 + a_3 = 0$ **then return** ∞.
   else
   $$\lambda := \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}; \qquad \nu := \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$
4. $x_3 := \lambda^2 - a_1\lambda - a_2 - x_1 - x_2; \qquad y_3 := -(\lambda + a_1)x_3 - \nu - a_3.$
5. **return** $[x_3 : y_3 : 1]$.

In the case $K = \mathbb{R}$, this computation has a nice geometric intuition: It corresponds to taking two points P and Q on the curve and drawing a straight line through them to give a third point of intersection (which may be the point at infinity). The result of mirroring this point along the x-axis is then defined to be the sum of the points P and Q. In other words: The sum of the three points of intersection of a straight line with the curve is always the point at infinity.

Lemma 29. The addition $+\colon E \times E \to E$ defined by Algorithm 28 makes $(E, +, \infty)$ an abelian group. For each subfield $K \subseteq \bar{K}$ over which E is defined, its set of K-rational points $E(K)$ forms a subgroup of E.

Proof. The first claim can be shown using either the formulas from Algorithm 28 in a geometric argument (which makes it quite tedious to prove associativity, see for instance Washington [22, Section 2.4]), or the fact that $+$ is induced from the degree-0 part of E's divisor class group via a natural bijection (more about which can be read in Silverman [19, Proposition III.3.4]).

The second claim is easily seen by observing that Algorithm 28 performs only operations in the field its inputs belong to; hence its output coordinates are also contained in that field. □

Lemma 30. The inversion map $i\colon E \to E,\ P \mapsto -P$ is an isogeny given by $i = [x, -y - a_1x - a_3, z]$.

Lemma 31. For any $Q \in E$, the *translation-by-Q map*

$$E \to E,\ P \to P + Q$$

is a morphism.

Definition 32. Let $m \in \mathbb{Z}$. We write $[m]\colon E \to E$ for the function sending each point of an elliptic curve E to its mth power (with respect to point addition).

Lemma 33. $[m]\colon E \to E$ is a non-constant separable isogeny.

Definition 34. Define the *subgroup of m-torsion points on E* as

$$E[m] := \ker[m] = \{\, P \in E \mid [m]P = \infty \,\}.$$

Lemma 35. Every isogeny $\varphi\colon E_1 \to E_2$ of elliptic curves is a group homomorphism.

Definition 36. Let E be an elliptic curve. The *endomorphism ring* of E is the set

$$\mathrm{End}(E) = \{\, \varphi\colon E \to E \mid \varphi \text{ isogeny} \,\}$$

with addition induced by the point addition on E and multiplication being the composition of endomorphisms.

4 Elliptic curve cryptography

One of the most fundamental cryptographic breakthroughs is the discovery of *asymmetric cryptosystems* in the 1970s; the first of which to become publicly known having been the *Diffie-Hellman key agreement* which enables two communicating parties to establish a shared secret over a public channel [5]. "Asymmetric" means in this context that the keys needed for encryption and decryption of messages are different and the decryption key cannot feasibly be determined from the encryption key. This makes it possible to distribute the encryption key to the whole world such that everyone can *en*crypt messages, while nobody but the intended recipient can *de*crypt them. Similar schemes have been conceived for digital signature, allowing an individual to sign a message using their private key in such a way that anyone in possession of the corresponding public key can reliably verify that the message has indeed originated at that user.

Typically, asymmetric cryptosystems are not used alone for encryption, but in combination with symmetric-key (that is: the keys necessary for encryption and decryption are the same) algorithms — this is known as *hybrid encryption*. This approach is the reason that the Diffie-Hellman key agreement in its pure form is useful: the shared secret allows two previously unacquainted parties to communicate using generally more performant symmetric-key methods instead of pure public-key protocols.

Alongside the RSA cryptosystem based on the assumed difficulty of computing roots in groups of hidden order [14], the Diffie-Hellman system's variants (in particular, increasingly: the elliptic-curve analogues) continue to be the most important pillars of modern cryptography, including but not limited to applications in core internet protocols like Transport Layer Security (TLS; in particular HTTPS), Secure Shell (SSH), Pretty Good Privacy (PGP), and many more.

4.1 The discrete logarithm problem

The security of the exemplary algorithms presented in this section crucially depends on the hardness of the following problem:

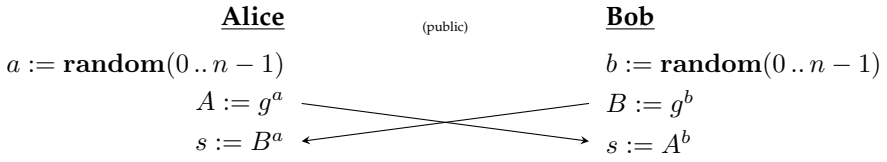
Definition 37. Let G be a cyclic group generated by $g \in G$. The *discrete logarithm problem in G to the base g* is the task of, given some $y \in G$, obtaining an exponent $x \in \mathbb{Z}$ such that $g^x = y$.

For our purposes, G will be an elliptic curve group as described in Section 3.1. There is the following result on the *generic* hardness of the discrete logarithm problem:

Theorem 38 (Shoup [18])**.** Let G be a cyclic group whose order has p as its largest prime divisor. Any generic — that is, independent of a specific representation of G — algorithm that solves the discrete logarithm problem in G with non-negligible probability takes $\Omega(\sqrt{p})$ operations in G.

4.1.1 The Diffie-Hellman key agreement

Definition 39. Let $G = \langle g \rangle$ be a publicly known cyclic group of order n. To agree upon a shared secret, two parties Alice and Bob proceed according to the following diagram:



That is, Alice generates a secret random exponent a (her private key) and shares the corresponding power $A := g^a$ of g (her public key) with Bob, who proceeds analogously. She then takes the ath power of the element B she received from Bob (his public key) to compute a group element $s = B^a = (g^a)^b = g^{ab}$ (the shared secret). Clearly, they both obtain the same value of s since $(g^a)^b = g^{ab} = (g^b)^a$.

Traditionally, the only groups practically used for this key agreement mechanism were multiplicative groups of prime fields; however elliptic curve groups have recently been becoming increasingly attractive due to the impact of continuously improving subexponential algorithms for the discrete logarithm problem in finite fields [8, 1, 9, 2]. A practical consequence of these developments is that the key

lengths required in finite-field instantiations of Diffie-Hellman need to be much larger than is the case for elliptic curve groups (recommendations vary, but the order of magnitude is about 4096 vs. 256 bits), inducing performance and usability disadvantages.

Formally, the hardness assumption on which the Diffie-Hellman protocol is based is the difficulty of the following problem:

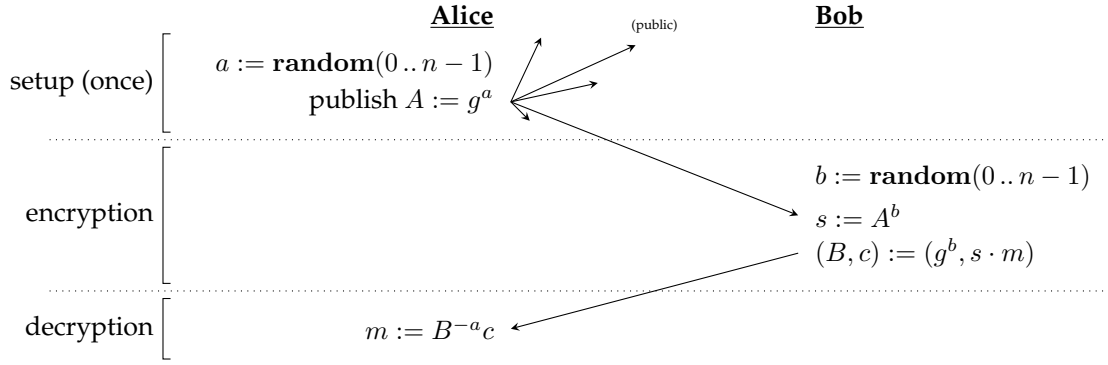
Definition 40. Let g be a generator of a cyclic group G. The *Diffie-Hellman problem in G to the base g* is the task of, given some $g^x, g^y \in G$, obtaining the element g^{xy}.

Obviously, the Diffie-Hellman problem is at most as hard as the discrete logarithm problem: Being able to recover one of the exponents, for instance y, allows simply computing $(g^x)^y = g^{xy}$ by exponentiation. A well-known paper by Ueli M. Maurer concerns the other direction: He proved that under certain assumptions, both problems are equivalent [12]. Hence, it is just natural that a lot of cryptographic research revolving around Diffie-Hellman variants focuses on the discrete logarithm problem: In fact, all of the attacks and countermeasures described in this thesis try to break or harden the discrete logarithm problem in elliptic curve groups.

4.1.2 The Elgamal encryption scheme

A straight-forward application of the Diffie-Hellman agreement to obtain a non-interactive public-key encryption scheme was published by Taher Elgamal in 1985.

Definition 41 (Elgamal encryption)**.** Suppose Bob wants to send a message m to Alice using the Elgamal encryption scheme over a cyclic group G of order n with generator g. To achieve this, they perform the following operations:



A careful inspection of the diagram above shows that Elgamal encryption is nothing more than the Diffie-Hellman key agreement (with one fixed and one ephemeral public key) followed by encryption of the message consisting of multiplication with the shared secret.

Lemma 42. Decrypting an Elgamal ciphertext given only the corresponding public key (but not the private counterpart) is equivalent to solving the Diffie-Hellman problem.

Proof. Clearly, solving the Diffie-Hellman problem is sufficient to decrypt the message. On the other hand, suppose there is an algorithm that breaks Elgamal (in the mentioned sense). Then we can run that algorithm on the input $(A, (B, e))$, where e denotes G's neutral element, to obtain the element $B^{-a}e = g^{-ab}$ from which one can trivially derive g^{ab}, thus solving the Diffie-Hellman problem. □

4.2 Generic algorithms for logarithms

There is a wide range of attacks on badly chosen elliptic-curve instantiations of discrete-logarithm-based cryptosystems. They fall into one of three categories: Generic algorithms, which are not specific to elliptic curves and could in fact be applied to any kind of group representation; elliptic curve transfer attacks, which reduce logarithms in some badly chosen elliptic curves to logarithms in a finite field; and

fault attacks, which exploit failure of implementations to perform required sanity checks on the input data, exposing an augmented surface for mathematical attacks. More about the latter kinds of attacks can be found in Bernstein and Lange [3].

In this section, we will present the generic algorithms applicable to any discrete logarithm instantiation. In particular, these are the most prominent reason why it is very important to know the exact number of rational points on an elliptic curve, since this count lacking a large prime divisor results in potentially severe security breaches.

Algorithm 43 (Baby-step giant-step algorithm)**.**
Input. A cyclic group G of order n, a generator g of G and an element $y \in G$.
Output. Some $x \in \mathbb{N}$ with $g^x = y$.
Runtime. $\mathcal{O}(\sqrt{n})$ operations in G.

1. $m := \lceil \sqrt{n} \rceil$.
2. Initialize a lookup table $T\colon G \to \{0, \ldots, m-1\}$.
3. $t := e$. (neutral element of G)
4. **for all** $j \in \{0, \ldots, m-1\}$:
   $T[t] := j$; $t := gt$.
5. $t := y$; $h := g^{-m}$.
6. **for all** $i \in \{0, \ldots, m-1\}$:
   if t is in T **then return** $im + T[t]$.
   $t := ht$.

Correctness. First note that at the beginning of the loop bodies, we have the invariants $t = g^j$ for the first loop and $t = yg^{-im}$ for the second.

Let x denote y's logarithm to the base g. Since $x < n \leq m^2$, it has a two-digit base-m representation $x = im + j$. In step 6, the algorithm terminates at precisely that i: When it is reached, we have $yg^{-im} = g^{x-im} = g^j$ which is contained in T since $0 \leq j < m$; and then $im + T[yg^{-im}] = im + T[g^j] = im + j = x$ is returned. □

Runtime. Clearly, the loops perform one operation in G during each iteration, and there is a maximum of $2m$ iterations in total. The computation of h in step 5 can be done in $1 + 2\lceil \log_2 m \rceil$ operations using exponentiation by squaring, therefore the total number of group operations is bounded by

$$2m + 1 + 2\lceil \log_2 m \rceil \in \mathcal{O}(m + \log m) = \mathcal{O}(m) = \mathcal{O}(\sqrt{n}).$$

□

Algorithm 44 (Pohlig and Hellman [13])**.**
Input. A cyclic group G of prime-power order $n = p^r$, a generator g of G and an element $y \in G$.
Output. Some $x \in \mathbb{N}$ with $g^x = y$.
Runtime. $\mathcal{O}(r(\log n + \sqrt{p}))$ operations in G.

1. $h := g^{p^{r-1}}$; $x_0 := 0$.
2. **for all** $k \in \{0, \ldots, r-1\}$:
   $n_k := p^{r-1-k}$; $y_k := (g^{-x_k} y)^{n_k}$.
   compute $\delta_k := \log_h y_k$ in $\langle h \rangle \subseteq G$ using algorithm 43.
   $x_{k+1} := x_k + p^k \delta_k$.
3. **return** x_r.

Correctness. Let x denote y's logarithm to the base g. We show by induction on k that $x_k \equiv x \pmod{p^k}$ holds for all $k \in \{0, \dots, r\}$: the base case $k = 0$ is obvious. Suppose that $x_k \equiv x \pmod{p^k}$. Then

$$\begin{aligned}(g^{n_k})^{x_{k+1}} &= (g^{n_k})^{x_k + p^k \delta_k} = g^{n_k x_k} g^{n_k p^k \delta_k} = g^{n_k x_k} g^{p^{r-1} \delta_k} = g^{n_k x_k} h^{\delta_k} \\ &= g^{n_k x_k} y_k = g^{n_k x_k} (g^{-x_k} y)^{n_k} = g^{n_k x_k} g^{n_k (x - x_k)} = (g^{n_k})^x,\end{aligned}$$

hence $x_{k+1} \equiv x \pmod{k+1}$ since $\operatorname{ord} g^{n_k} = \operatorname{ord} g / n_k = p^r / p^{r-1-k} = k + 1$.

In particular, we have shown $x_r \equiv x \pmod{n}$, which yields the claim. □

Runtime. Using exponentiation by squaring, computing h requires $\mathcal{O}(\log p^{r-1}) \subseteq \mathcal{O}(\log n)$ group operations.

The main loop performs r iterations, in each of which two powers in G with exponents bounded by n are computed, taking $\mathcal{O}(\log n)$, as well as a logarithm in a group of size $\operatorname{ord} h = p^r / p^{r-1} = p$, thereby performing $\mathcal{O}(\sqrt{p})$ operations in $\langle h \rangle \subseteq G$. Hence the total number of group operations is bounded by $\mathcal{O}(r(\log n + \sqrt{p}))$. □

Algorithm 45 (Pohlig and Hellman [13])**.**

Input. A cyclic group G of order $n = p_1^{e_1} \dots p_r^{e_r}$, a generator g of G and an element $y \in G$.
Output. Some $x \in \mathbb{N}$ with $g^x = y$.
Runtime. $\mathcal{O}(\sum_{k=1}^{r} e_k(\log n + \sqrt{p_k}))$ operations in G.

1. **for all** $k \in \{1, \dots, r\}$:
   $n_k := n / p_k^{e_k}$; $\quad g_k := g^{n_k}$; $\quad y_k := y^{n_k}$.
   compute $x_k := \log_{g_k} y_k$ in $\langle g_k \rangle \subseteq G$ using Algorithm 44.
2. Solve the simultaneous congruence
   $$\forall k \in \{1, \dots, r\}. \quad x \equiv x_k \pmod{p_k^{e_k}}$$
   and **return** the result.

Correctness. Let x denote y's logarithm to the base g. From the algorithm,

$$g_k^x = (g^{n/p_k^{e_k}})^x = (g^x)^{n/p_k^{e_k}} = y^{n/p_k^{e_k}} = y_k = g_k^{\log_{g_k} y_k} = g_k^{x_k}$$

holds for all $k \in \{1, \dots, r\}$, hence $x \equiv x_k \pmod{p_k^{e_k}}$ since $\operatorname{ord} g_k = \operatorname{ord} g / n_k = n / (n / p_k^{e_k}) = p_k^{e_k}$. The claim follows with the Chinese remainder theorem. □

Runtime. In the kth iteration, the algorithm computes two powers in G with exponents bounded by n, taking $\mathcal{O}(\log n)$ group operations, as well as a logarithm in the group $\langle g_k \rangle \subseteq G$ of size $p_k^{e_k}$, requiring $\mathcal{O}(e_k(\log p_k^{e_k} + \sqrt{p_k}))$ operations. In sum, the number of group operations is bounded by

$$\sum_{k=1}^{r} (\mathcal{O}(\log n) + \mathcal{O}(e_k(\log p_k^{e_k} + \sqrt{p_k}))) \subseteq \mathcal{O}\Big(\sum_{k=1}^{r} e_k(\log n + \sqrt{p_k}) \Big).$$

□

5 Schoof's algorithm

In these sections, we shall collect the various ingredients required for Schoof's algorithm and eventually describe the algorithm itself.

5.1 The Frobenius endomorphism

Definition 46. Let $E/\mathbb{F}_q$ be an elliptic curve. The *Frobenius endomorphism* of E over $\mathbb{F}_q$ is defined by

$$\varphi\colon E \to E,\ [x:y:z] \mapsto [x^q : y^q : z^q].$$

Note that since E is assumed to be defined over $\mathbb{F}_q$, the homomorphism $a \mapsto a^q$ leaves the equation defining E invariant, hence $\varphi(E) \subseteq E$.

Lemma 47. The Frobenius endomorphism is an isogeny.

Lemma 48 (van Tuyl [21, Theorem 2.5])**.** Let E be an elliptic curve defined over $\mathbb{F}_q$ and with Frobenius endomorphism φ. Then

$$\deg \varphi = q.$$

Proof. Since the function fields of E and the dehomogenization of E with respect to z are isomorphic, we may instead treat E as an affine variety given by a Weierstraß equation

$$0 = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \quad =: f(x,y).$$

Let K denote the image of $\mathbb{F}_q$ under the natural map

$$\mathbb{F}_q \to \mathbb{F}_q[x,y] \to \mathbb{F}_q(E).$$

Clearly, we have

$$[K(x) : K(x^q)] = q$$

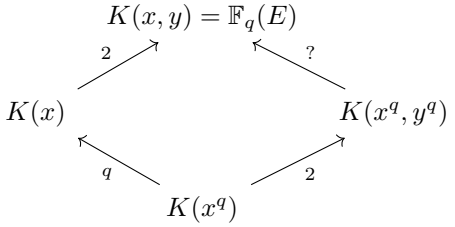
since x is a zero of $T^q - x^q \in K(x^q)[T]$ and x^q is transcendental over K, hence $T^q - x^q$ is irreducible. Also, the polynomial

$$f(\xi, T) = T^2 + (a_1\xi + a_3)T - (\xi^3 + a_2\xi^2 + a_4\xi + a_6) \quad \in K(\xi)[T]$$

is irreducible over $K(\xi)$ for any element ξ which is transcendental over K: According to Gauß's lemma, it is sufficient to show that f is irreducible over $K[\xi]$. Suppose for the purpose of contradiction that there is a nontrivial factorization $f(\xi,T) = (T-\gamma_1)(T-\gamma_2)$ with polynomials $\gamma_1, \gamma_2 \in K[\xi]$ which must therefore satisfy $-(\gamma_1+\gamma_2) = a_1\xi + a_3$ and $-\gamma_1\gamma_2 = \xi^3 + a_2\xi^2 + a_4\xi + a_6$. Since K is a field, the latter implies $\deg(\gamma_1\gamma_2) = \deg\gamma_1 + \deg\gamma_2 = 3$. But the first relation $-(\gamma_1+\gamma_2) = a_1\xi + a_3$ forces that all non-linear coefficients cancel when adding γ_1 and γ_2, hence we have either $\deg\gamma_1 = \deg\gamma_2 \geq 2$ or $\max\{\deg\gamma_1, \deg\gamma_2\} \leq 1$, both of which contradict $\deg(\gamma_1\gamma_2) = 3$. Therefore, $f(x,T)$ is y's minimal polynomial over $K(x)$; and similarly $f(x^q,T)$ is y^q's minimal polynomial over $K(x^q)$, yielding

$$[K(x,y) : K(x)] = [K(x^q,y^q) : K(x^q)] = \deg f(\xi,T) = 2.$$

We have established the following diagram of field extensions, with the degrees annotated at the edges:



With the degree multiplication theorem, the conclusion

$$[K(x,y) : K(x^q,y^q)] = \frac{[K(x,y) : K(x^q)]}{[K(x^q,y^q) : K(x^q)]} = \frac{[K(x,y) : K(x)][K(x) : K(x^q)]}{[K(x^q,y^q) : K(x^q)]} = \frac{2q}{2} = q$$

follows. □

Lemma 49. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and let $\varphi\colon E \to E$ denote E's Frobenius endomorphism. Then a point $P \in E$ is $\mathbb{F}_q$-rational if and only if it is fixed by φ. In particular,

$$E(\mathbb{F}_q) = \ker(1 - \varphi).$$

Proof. As $\mathbb{F}_q$ is fixed by φ according to Fermat's little theorem, any point in $E(\mathbb{F}_q)$ is invariant under φ.

On the other hand, suppose that $\varphi(P) = P$. There is some intermediate field $\mathbb{F}_{q^d}$ of $\bar{\mathbb{F}}_q/\mathbb{F}_q$ such that $P \in E(\mathbb{F}_{q^d})$. We may assume that P is a finite point since the claim is trivial otherwise, so it has affine coordinates $P = (x, y)$. Each coordinate is invariant under φ, hence either zero or contained in a subgroup of $\mathbb{F}_{q^d}^*$ of order dividing $q - 1$. But $\mathbb{F}_{q^d}^*$ is cyclic, so this subgroup is unique and must therefore be the embedding of a subgroup of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^d}^*$. □

Lemma 50 (Silverman [19, Corollary III.5.5])**.** Let E be an elliptic curve defined over $\mathbb{F}_q$ with Frobenius endomorphism φ. Then the endomorphism $1 - \varphi$ is separable.

Corollary 51.

$$\#E(\mathbb{F}_q) = \deg(1 - \varphi).$$

Proof. This follows from Lemmas 49 and 27 using Lemma 50. □

5.2 Division polynomials

Our main goal in this section is to derive explicit closed formulas for the multiplication-by-m map on an elliptic curve. We show that such expressions, in terms of so-called *division polynomials*, exist and prove some of their properties later needed for Schoof's algorithm (Section 5.5). It is quite evident that such formulas exist: By repeatedly evaluating the addition formulas from Algorithm 28 at symbolic points (x, y, z), one obtains fractional expressions for all coordinates of the resulting points.

The definitions in this section are taken from Blake, Seroussi, and Smart [4, Section III.4]. For the scope of this section, let E/K be an elliptic curve given by a Weierstraß equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Definition 52. Let x and y denote indeterminates over K. The *division polynomials* $\hat{\psi}_m \in K[x, y]$ are defined as

$$\begin{aligned}
\hat{\psi}_1 &= 1;\\
\hat{\psi}_2 &= 2y + a_1x + a_3;\\
\hat{\psi}_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8;\\
\hat{\psi}_4 &= \hat{\psi}_2 \cdot \left(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2\right),
\end{aligned}$$

where

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \qquad b_4 = a_1a_3 + 2a_4 \qquad b_6 = a_3^2 + 4a_6\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,
\end{aligned}$$

and for $m \geq 5$ recursively via

$$\begin{aligned}
\hat{\psi}_{2k+1} &= \hat{\psi}_{k+2}\hat{\psi}_k^3 - \hat{\psi}_{k-1}\hat{\psi}_{k+1}^3 && \text{for odd } m = 2k + 1 \geq 5;\\
\hat{\psi}_{2k} &= (\hat{\psi}_{k-1}^2\hat{\psi}_k\hat{\psi}_{k+2} - \hat{\psi}_{k-2}\hat{\psi}_k\hat{\psi}_{k+1}^2)/\hat{\psi}_2 && \text{for even } m = 2k \geq 6.
\end{aligned}$$

Note that the one needs to show that the division by $\hat{\psi}_2$ in the equation for $\hat{\psi}_{2k}$ is always possible; this is a corollary to the following lemma.

Lemma 53.

$$\hat{\psi}_m \in \begin{cases} K[x, \hat{\psi}_2^2] & \text{if } m \text{ is odd;}\\ \hat{\psi}_2K[x, \hat{\psi}_2^2] & \text{if } m \text{ is even.}\end{cases}$$

Proof. Let $R = K[x, \hat{\psi}_2^2]$. The proof is done by induction: Clearly, the statement holds for $m \leq 4$.

Let $m = 2k+1 \geq 5$ be odd. Then the parities of $k+2$ and k match, and so do $k-1$ and $k+1$'s. Hence the polynomials $\hat{\psi}_{k+2}\hat{\psi}_k^3$ and $\hat{\psi}_{k-1}\hat{\psi}_{k+1}^3$ are in R since $\hat{\psi}_2 R \cdot \hat{\psi}_2 R \subseteq \hat{\psi}_2^2 R \subseteq R$.

If $m = 2k \geq 6$ is even, an analogous argument shows that exactly two of the factors in each of the products $\hat{\psi}_{k-1}^2\hat{\psi}_k\hat{\psi}_{k+2}$ and $\hat{\psi}_{k-2}\hat{\psi}_k\hat{\psi}_{k+1}^2$ are in $\hat{\psi}_2 R$ with the other two being in R, thus division by $\hat{\psi}_2$ shows the claim. □

Lemma 54. Consider the map

$$s\colon K[x, \hat{\psi}_2] \to K[x, \hat{\psi}_2] \subseteq K[x, y]$$

defined as the $K[x]$-linear extension of the monomial map

$$\hat{\psi}_2^{2i+j} \mapsto \hat{\psi}_2^j \cdot (4x^3 + b_2x^2 + 2b_4x + b_6)^i \qquad \text{(for } i \in \mathbb{N},\, j \in \{0,1\}\text{)}$$

and let $\iota\colon K[x,y] \to K(E)$ be the embedding into E's function field. Then

$$\iota \circ s = \iota|_{K[x,\hat{\psi}_2]}.$$

Proof. This is shown by a simple calculation using the Weierstraß equation for E, essentially consisting of validating the congruence $\iota(\hat{\psi}_2^2) = \iota(4x^3 + b_2x^2 + 2b_4x + b_6)$. □

Definition 55. If $\operatorname{char} K \neq 2$, we define the polynomials

$$\hat{\phi}_m = x\hat{\psi}_m^2 - \hat{\psi}_{m+1}\hat{\psi}_{m-1};$$
$$\hat{\omega}_m = (\hat{\psi}_{m-1}^2\hat{\psi}_{m+2}/\hat{\psi}_2 - \hat{\psi}_{m-2}\hat{\psi}_{m+1}^2/\hat{\psi}_2 - a_1\hat{\phi}_m\hat{\psi}_m - a_3\hat{\psi}_m^3)/2.$$

Remark. In the case of $\operatorname{char} K = 2$, it is possible to proceed completely analogously — in particular, the division polynomials' applications in the following sections work independently of the characteristic. However, due to the division by 2 in the definition of $\hat{\omega}_m$, it must be defined a bit different in that case: For a thorough treatment of this topic, see Koblitz [10] or, for non-supersingular curves, Blake, Seroussi, and Smart [4, Section III.4.2].

Lemma 56.

$$\psi_m = \begin{cases} \psi_2(mx^{m^2/2-2} + \text{lower-order terms})/2 & \text{if } m \text{ is even;} \\ mx^{(m^2-1)/2} + \text{lower-order terms} & \text{if } m \text{ is odd.} \end{cases}$$

In particular, if m is odd, then $\deg \psi_m = (m^2-1)/2$.

Proof. Clearly, the statement is true for $m \leq 4$. Let $m > 4$ and suppose the claim holds for all smaller indices. We perform a case distinction on $m \bmod 4$.

- Note that $(k-1)^2(k+2) - (k-2)(k+1)^2 = 4$ and assume $m = 2k$ is even.
  - If k is even, then

$$\begin{aligned}
\psi_m &= \psi_k(\psi_{k-1}^2\psi_{k+2} - \psi_{k-2}\psi_{k+1}^2)/\psi_2 \\
&= \psi_k(\psi_2(k-1)^2(k+2)x^{3k^2/2}/2 - \psi_2(k-2)(k+1)^2x^{3k^2/2}/2 + \dots)/\psi_2 \\
&= \psi_k((k-1)^2(k+2) - (k-2)(k+1)^2)(x^{3k^2/2} + \dots)/2 \\
&= 4\psi_k(x^{3k^2/2} + \dots)/2 \\
&= \psi_2(2kx^{k^2/2-2} + \dots)(x^{3k^2/2} + \dots)/2 \\
&= \psi_2(mx^{m^2/2-2} + \dots)/2.
\end{aligned}$$

– If k is odd, then

$$\begin{aligned}\psi_m &= \psi_k(\psi_{k-1}^2\psi_{k+2} - \psi_{k-2}\psi_{k+1}^2)/\psi_2 \\ &= \psi_k\psi_2((k-1)^2(k+2)x^{3(k^2-1)/2} - (k-2)(k+1)^2x^{3(k^2-1)/2} + \dots)/4 \\ &= \psi_k((k-1)^2(k+2) - (k-2)(k+1)^2)(x^{3(k^2-1)/2} + \dots)/4 \\ &= 4\psi_k(x^{3(k^2-1)/2} + \dots)/4 \\ &= \psi_2(2kx^{(k^2-1)/2} + \dots)(x^{3(k^2-1)/2} + \dots)/2 \\ &= \psi_2(mx^{m^2/2-2} + \dots)/2.\end{aligned}$$

- Note that $\psi_2^4 = 16x^6 + \dots$ and $(k+2)k^3 - (k-1)(k+1)^3 = 2k+1$. If $m = 2k+1$ is odd, then

$$\begin{aligned}\psi_m &= \psi_{k+2}\psi_k^3 - \psi_{k-1}\psi_{k+1}^3 \\ &= \begin{Bmatrix}\psi_2^4((k+2)k^3x^{2k^2+2k-6} + \dots)/16 - ((k-1)(k+1)^3x^{2k^2+2k} + \dots) & \text{if } k \text{ is even;} \\ ((k+2)k^3x^{2k^2+2k} + \dots) - \psi_2^4((k-1)(k+1)^3x^{2k^2+2k-6} + \dots)/16 & \text{if } k \text{ is odd.}\end{Bmatrix} \\ &= ((k+2)k^3 - (k-1)(k+1)^3)(x^{2k^2+2k} + \dots) \\ &= (2k+1)(x^{2k^2+2} + \dots) \\ &= mx^{(m^2-1)/2} + \dots.\end{aligned}$$

□

Remark. Since we are only interested in the $\hat{\psi}_m$s' images under ι, this lemma legitimates us to identify $\hat{\psi}_m$ and $s(\hat{\psi}_m)$ for our purposes, hence yielding polynomials in $K[x]$ or $\hat{\psi}_2K[x]$. Thus, we shall from now on use the "reduced" division polynomial $\psi_m := s(\hat{\psi}_m)$ instead of $\hat{\psi}_m$; and deal with $\hat{\phi}_m$ and $\hat{\omega}_m$ in a similar fashion. Hence, as an immediate consequence to Lemma 53:

$$\psi_m \in \begin{cases}K[x] & \text{if } m \text{ is odd;} \\ \psi_2K[x] & \text{if } m \text{ is even.}\end{cases}$$

Lemma 57 (Blake, Seroussi, and Smart [4, Lemma III.5])**.** For all $m \in \mathbb{N}_{\geq 1}$ and $P = [x : y : 1] \in E \setminus \{\infty\}$,

$$[m]P = [\phi_m(x,y)\psi_m(x,y) : \omega_m(x,y) : \psi_m^3(x,y)].$$

Moreover, the zeroes of ψ_m are precisely the finite m-torsion points of E.

Proof. One way to prove this is by induction using the addition formulas (Algorithm 28); this approach is highly computational and laborious [4, Section III.4].
A more pleasant analytic proof can be found in Lang [11, Chapter II]. □

Lemma 58. Let E be an elliptic curve defined over K and suppose $\operatorname{char} K$ does not divide $m \in \mathbb{Z}$. Then

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

Proof. This can be proven using the division polynomials, see Washington [22, Section 3.2], or more abstractly using the *dual isogeny*, see Silverman [19, Corollary III.6.4]. □

5.3 The Tate module

In this section, we will introduce the *Tate module* of an abelian group, which is of great aid in the study of elliptic curves. In particular, there is a highly useful correspondence between isogenies of elliptic curves and endomorphisms of the Tate module.

Definition 59 (Silverman [19, Section III.7])**.** Consider an abelian group G and let $\ell \in \mathbb{Z}$ be a prime. The *(ℓ-adic) Tate module of G* is the group

$$T_\ell(G) = \varprojlim_n G[\ell^n],$$

where the inverse limit is taken with respect to the natural maps

$$G[\ell^{n+1}] \xrightarrow{[\ell]} G[\ell^n].$$

In other words: Each element of $T_\ell(G)$ is defined to be a sequence $(g_n)_{n\in\mathbb{N}_{\geq 1}}$ of elements of G such that $g_n = g_{n+1}^\ell$ for all indices $n \in \mathbb{N}_{\geq 1}$.

We will mostly work with the Tate module of an elliptic curve E, which thus consists of sequences $(P_n)_{n\in\mathbb{N}_{\geq 1}}$ of points on E such that for all $n \in \mathbb{N}_{\geq 1}$,

$$P_n = [\ell]P_{n+1}.$$

With this definition, $T_\ell(E)$ becomes a $\mathbb{Z}_\ell$-module in a natural way — addition and scalar multiplication of curve points carry over to the Tate module via component-wise application:

$$+\colon T_\ell(E) \times T_\ell(E) \to T_\ell(E),\ (P_n)_n + (Q_n)_n := (P_n + Q_n)_n;$$

$$\cdot\colon \mathbb{Z}_\ell \times T_\ell(E) \to T_\ell(E),\ z \cdot (P_n)_n := ([z \bmod \ell^n]P_n)_n.$$

Definition 60. Let $\varphi\colon E_1 \to E_2$ be an isogeny of elliptic curves. Then by component-wise application, φ induces the map

$$\varphi_\ell\colon T_\ell(E_1) \to T_\ell(E_2),\ \varphi_\ell((P_n)_n) := (\varphi(P_n))_n.$$

Clearly, this map is $\mathbb{Z}_\ell$-linear, hence a morphism of $\mathbb{Z}_\ell$-modules.

For the rest of this section, assume that ℓ be a prime other than the characteristic of K or $\mathbb{F}_q$, depending on the context.

Lemma 61 (Silverman [19, Proposition III.8.3])**.** There is a bilinear, alternating, non-degenerate map

$$\mathbf{e}\colon T_\ell(E) \times T_\ell(E) \to T_\ell(\bar{\mathbb{F}}_q^*),$$

known as *Weil pairing*. Formally, its properties are

$$\begin{aligned}
\text{linear:}\quad & \forall v_1, v_2, w \in T_\ell(E).\ \mathbf{e}(v_1 + v_2, w) = \mathbf{e}(v_1, w) \cdot \mathbf{e}(v_2, w);\\
& \forall v, w_1, w_2 \in T_\ell(E).\ \mathbf{e}(v, w_1 + w_2) = \mathbf{e}(v, w_1) \cdot \mathbf{e}(v, w_2);\\
\text{alternating:}\quad & \forall v, w \in T_\ell(E).\ \mathbf{e}(v, w) = \mathbf{e}(w, v)^{-1};\\
\text{non-degenerate:}\quad & \forall v \in T_\ell(E).\ [\mathbf{e}(v, T_\ell(E)) = \{1\} \implies v = 0].
\end{aligned}$$

Furthermore, for all endomorphisms $\varphi \in \mathrm{End}(E)$ and all $v, w \in T_\ell(E)$, we have

$$\mathbf{e}(\varphi_\ell v, \varphi_\ell w) = \mathbf{e}([\deg \varphi]_\ell v, w).$$

Lemma 62. The ℓ-adic Tate module $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2.

Proof. Since each ℓ^n-torsion subgroup $E[\ell^n]$ of E is isomorphic to $\mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n$ by Lemma 58,

$$T_\ell(E) \cong \varprojlim_n (\mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n) \cong \varprojlim_n (\mathbb{Z}/\ell^n) \times \varprojlim_n (\mathbb{Z}/\ell^n) = \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

□

Lemma 63. Let $\varphi\colon E \to E$ be an isogeny of elliptic curves defined over some field K. Then

$$\det \varphi_\ell = \deg \varphi.$$

Proof. From Lemma 62, the ℓ-adic Tate module $T_\ell(E)$ has a two-element $\mathbb{Z}_\ell$-basis $\{v, w\} \subseteq T_\ell(E)$ and there are $a, b, c, d \in \mathbb{Z}_\ell$ such that

$$\varphi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \text{that is} \qquad \begin{cases} \varphi_\ell v = av + cw; \\ \varphi_\ell w = bv + dw. \end{cases}$$

We now use the Weil pairing $\mathbf{e}$ from Lemma 61 to compute

$$\begin{aligned} \mathbf{e}(v,w)^{\deg\varphi} &= \mathbf{e}([\deg\varphi]_\ell v, w) \\ &= \mathbf{e}(\varphi_\ell v, \varphi_\ell w) \\ &= \mathbf{e}(av + cw, bv + dw) \\ &= \mathbf{e}(av, bv) \cdot \mathbf{e}(av, dw) \cdot \mathbf{e}(cw, bv) \cdot \mathbf{e}(cw, dw) \\ &= \mathbf{e}(av, dw) \cdot \mathbf{e}(cw, bv) \\ &= \mathbf{e}(v,w)^{ad} \cdot \mathbf{e}(w,v)^{cb} \\ &= \mathbf{e}(v,w)^{ad-bc} \\ &= \mathbf{e}(v,w)^{\det\varphi_\ell}, \end{aligned}$$

and since $\mathbf{e}$ is nondegenerate, this shows the conclusion. □

Corollary 64. If $E/\mathbb{F}_q$ is an elliptic curve with Frobenius endomorphism φ, then

$$\#E(\mathbb{F}_q) = q + 1 - \operatorname{tr}\varphi_\ell.$$

Proof. Writing φ_ℓ as a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ like in the proof of Lemma 63, we have

$$1 + \det\varphi_\ell - \det(1 - \varphi_\ell) = 1 + ac - bd - 1 + a + c - ac + bd = a + c = \operatorname{tr}\varphi_\ell.$$

Applying Lemmas 63 and 48 and Corollary 51 yields

$$\operatorname{tr}\varphi_\ell = 1 + \deg\varphi - \deg(1 - \varphi) = 1 + q - \#E(\mathbb{F}_q).$$

□

Corollary 65. The Frobenius endomorphism φ of an elliptic curve $E/\mathbb{F}_q$ satisfies

$$\varphi^2 - [\operatorname{tr}\varphi_\ell]\varphi + [q] = 0.$$

Proof. Since $\varphi_\ell = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is an endomorphism of a two-dimensional $\mathbb{Z}_\ell$-module, we have the characteristic polynomial

$$\chi_{\varphi_\ell} = (X - a)(X - d) - bc = X^2 - aX - dX + ad - bc = X^2 - (\operatorname{tr}\varphi_\ell)X + \det\varphi_\ell.$$

Let $\tau := \operatorname{tr}\varphi_\ell$. With the Cayley-Hamilton theorem, Corollary 64 and Lemma 48, one obtains

$$\varphi_\ell^2 - [\tau]\varphi_\ell + [q] = 0$$

and hence

$$\deg(\varphi^2 - [\tau]\varphi + [q]) = \det(\varphi_\ell^2 - [\tau]\varphi_\ell + [q]) = \det 0 = 0,$$

therefore $\varphi^2 - [\tau]\varphi + [q]$ is constant. □

5.4 A bound on the number of points: Hasse's theorem

Since the (short) Weierstraß equation

$$E\colon y^2 = x^3 + ax + b$$

over $\mathbb{F}_q$ has at most two solutions y for each value of x, it is clear that

$$\#E(\mathbb{F}_q) \leq 2q + 1.$$

However, it may intuitively be expected that the actual number of points is much smaller: If one (not too implausibly) assumed the right-hand side $x^3 + ax + b$ to be a square for approximately half of the $x \in \mathbb{F}_q$, then the number of points could be estimated to be about $q + 1$. Theorem 68, first proven by Helmut Hasse [7, §4.2] in 1936, clarifies and formalizes this intuition by giving a rigorous bound. To be able to establish this bound, we first need some auxiliary results.

Lemma 66 (Washington [22, Proposition 3.16])**.** Let α, β denote endomorphisms of an elliptic curve E/K and let $r, s \in \mathbb{Z}$. Then

$$\deg([r]\alpha - [s]\beta) = r^2 \deg\alpha + rs(\deg(\alpha - \beta) - \deg\alpha - \deg\beta) + s^2 \deg\beta.$$

Proof. Let ℓ be a prime different from $\operatorname{char} K$. Write $\alpha_\ell = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\beta_\ell = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)$. Using Lemma 63,

$$\begin{aligned}
\deg([r]\alpha - [s]\beta) &= \det(r\alpha_\ell - s\beta_\ell) \\
&= \det\begin{pmatrix} ra - se & rb - sf \\ rc - sg & rd - sh \end{pmatrix} \\
&= r^2(ad - bc) + rs(-ah - de + bg + cf) + s^2(eh - fg) \\
&= r^2 \det\alpha_\ell + rs(\det(\alpha_\ell - \beta_\ell) - \det\alpha_\ell - \det\beta_\ell) + s^2 \det\beta_\ell \\
&= r^2 \deg\alpha + rs(\deg(\alpha - \beta) - \deg\alpha - \deg\beta) + s^2 \deg\beta.
\end{aligned}$$

□

Lemma 67 (Silverman [19, Lemma V.1.2])**.** Let E be an elliptic curve and let $\alpha, \beta \in \operatorname{End}(E)$. Then

$$|\deg(\alpha - \beta) - \deg\alpha - \deg\beta| \leq 2\sqrt{\deg\alpha \deg\beta}.$$

Proof. Set $L := \deg(\alpha - \beta) - \deg\alpha - \deg\beta$. From Lemma 66 and since degrees are non-negative,

$$\begin{aligned}
0 &\leq \deg([-L]\alpha - [2\deg\alpha]\beta) \\
&= (-L)^2 \deg\alpha + (-L) \cdot 2\deg\alpha \cdot L + (2\deg\alpha)^2 \deg\beta \\
&= \deg\alpha \cdot (-L^2 + 4\deg\alpha\deg\beta)
\end{aligned}$$

Since the claim is trivial when $\alpha = 0$, we may assume that $\deg\alpha \neq 0$ and divide by $\deg\alpha$, yielding

$$0 \leq 4\deg\alpha\deg\beta - L^2,$$

which is easily shown equivalent to the conclusion by adding L^2 and taking the square root of both sides of the inequality. □

Theorem 68 (Hasse [7])**.** Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Then

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Proof. Let φ denote E's Frobenius endomorphism over $\mathbb{F}_q$. By applying Lemma 67 to $\deg(1 - \varphi)$, we obtain the inequality

$$|\deg(1 - \varphi) - \deg 1 - \deg\varphi| \leq 2\sqrt{\deg 1 \deg\varphi},$$

and substituting according to Corollary 51 and Lemma 48 yields

$$|\#E(\mathbb{F}_q) - 1 - q| \leq 2\sqrt{q}.$$

□

5.5 Schoof's point counting algorithm

The exposition in this section is based on Blake, Seroussi, and Smart [4, Section VII.1].

Consider an elliptic curve E defined over a finite field $\mathbb{F}_q$ and an odd prime ℓ different from the characteristic of $\mathbb{F}_q$, and let $E[\ell]^*$ denote the set

$$E[\ell]^* := E[\ell] \setminus \{\infty\} = \{\, P \in E \mid \operatorname{ord} P = \ell \,\}.$$

To compute the number $\#E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on E, Corollary 51 shows that it is sufficient to determine the trace $\tau := \operatorname{tr} \varphi_\ell$ of the Frobenius endomorphism φ. Knowing from Corollary 65 that φ satisfies the functional equation

$$\varphi^2 + [q] = [\operatorname{tr} \varphi_\ell]\varphi$$

in the endomorphism ring $\operatorname{End}(E)$, one could compute the trace τ modulo ℓ by somehow choosing a point $[\xi : \eta : 1] \in E[\ell]^*$ of order ℓ on the curve and checking which $k \in \{0, \dots, \ell - 1\}$ makes the equation

$$[\xi^{q^2} : \eta^{q^2} : 1] + [q][\xi : \eta : 1] = [k][\xi^q : \eta^q : 1]$$

become true. It is clear that there is exactly one such k since since φ is a group homomorphism, hence $\varphi([\xi : \eta : 1]) = [\xi^q : \eta^q : 1] \neq \infty$ has order distinct from one, but dividing ℓ, which is a prime. Note that this implies:

Lemma 69. If $\varphi^2(P) + [q]P = [k]\varphi(P)$ for one $P \in E[\ell]^*$, then $k \equiv \tau \pmod{\ell}$ and hence $\varphi^2 + [q] = [k]\varphi$ holds on the whole of $E[\ell]^*$.

Determining τ modulo different primes ℓ in this way such that the product of all the moduli is sufficiently large (by Hasse's Theorem 68), the trace τ could be recovered using the Chinese remainder theorem, and with it the number of $\mathbb{F}_q$-rational points on E.

However, obtaining a point of order ℓ is neither entirely trivial, nor can the resulting algorithm be expected to exhibit a particularly desirable running time, compared to the following modification: The concrete evaluation at a point is substituted by *symbolically* checking whether the morphisms $\varphi^2 + [q]$ and $[k]\varphi$ agree on a ℓ-torsion point. This is realized using the division polynomial ψ_ℓ, which is a polynomial in one variable x only since we assumed ℓ to be odd (cf. Lemma 53): A univariate polynomial $f \in \mathbb{F}_q[x]$ vanishes on the x-coordinates of all the finite ℓ-torsion points of E if and only if it is a multiple of ψ_ℓ. Similarly, there *exists* a point in $E[\ell]^*$ on which f vanishes if and only if $\gcd(f, \psi_\ell) \neq 1$ in $\mathbb{F}_q[x]$.

Using these properties, we will now describe a procedure for deciding which $k \in \{0, \dots, \ell - 1\}$ fulfills the relation $\varphi^2 + [q] = [k]\varphi$ on the ℓ-torsion points. Since it is easier to work with affine varieties (and we are now only interested in the finite points of E anyway), we will treat the elliptic curve E as an affine variety and deal with the point at infinity in case distinctions. In this spirit, assume E to be given by an affine Weierstraß equation $0 = w \in \mathbb{F}_q[x, y]$ and let R_ℓ denote the quotient ring

$$R_\ell := \mathbb{F}_q[x, y]/(w, \psi_\ell).$$

Unless noted otherwise, all computations are now understood to take place in the ring R_ℓ. For this purpose, we shall use the polynomials $f \in \mathbb{F}_q[x, y]$ which are of the form $f = f_1 y + f_0$ with $f_0, f_1 \in \mathbb{F}_q[x]$ of degree less than $\deg \psi_\ell$ as the representants for elements of the ring R_ℓ, and reduce all intermediate results to this representation as soon as possible to avoid dealing with polynomials of large degree. These representants can easily be computed by reducing a given polynomial modulo the Weierstraß polynomial $w = y^2 + \dots$ for all the terms which are nonlinear in y and modulo the division polynomial $\psi_\ell = x^{(\ell^2-1)/2} + \dots \in \mathbb{F}_q[x]$, cf. Lemma 56, for subterms of sufficiently large degree in x.

Note that we are no longer in need of the facts about φ and point addition being morphisms; in fact we can limit ourselves to using the explicit formulas from the definition of the Frobenius endomorphism φ, Lemma 57, and Algorithm 28.

From the preceding discussion, one can derive the following algorithm:

Algorithm 70.
Input. Rational functions $\alpha, \beta \in \operatorname{Quot} R_\ell$.
Output. Whether there exists a point $P \in E$ of order ℓ with $\alpha(P) = \beta(P)$.
Runtime. $\mathcal{O}(\ell^4 \log^2 q)$.

1. Multiply $\alpha - \beta \in \operatorname{Quot} R_\ell$ by the least common denominator to obtain a function $f \in R_\ell$.
2. $f_1 y + f_0 := f$.
3. **if** $f_1 = 0$ in R_ℓ **then return** ("true" if $\gcd(f_0, \psi_\ell) \neq 1$, else "false").
4. **return** ("true" if $\gcd(f_1^2 w(x, -f_0/f_1), \psi_\ell) \neq 1$, else "false").

Correctness. Note that the greatest common divisors are computed in the polynomial ring $\mathbb{F}_q[x]$.

Lemma 57 states that the zeroes of ψ_ℓ are precisely the (x-coordinates of the) points of order ℓ on E. If, in the first case, $f = f_0$ and ψ_ℓ have a common zero, there is a point in $E[\ell]^*$ which vanishes on f (and hence has equal image under α and β). In the second case, a point $[\xi : \eta : 1]$ of order ℓ makes $[\xi : -(f_0/f_1)(\xi) : 1]$ lie on E if and only if ξ is a zero of f. □

Runtime. If implemented correctly, the algorithm deals only with polynomials of degree bounded by $\mathcal{O}(\ell^2)$. Each multiplication of such polynomials and subsequent reduction modulo w and ψ_ℓ takes $\mathcal{O}(\ell^4)$ operations in $\mathbb{F}_q$, which require $\mathcal{O}(\log^2 q)$ arithmetic operations each. Therefore, the total running time is in $\mathcal{O}(\ell^4 \log^2 q)$. □

Algorithm 71 (Finding the trace of Frobenius modulo ℓ)**.**
Input. An elliptic curve $E/\mathbb{F}_q$ given by a Weierstraß equation and an odd prime ℓ.
Output. The unique $k \in \{0, \ldots, \ell - 1\}$ such that $\varphi^2 + [q]$ and $[k]\varphi$ coincide on $E[\ell]$.
Runtime. $\mathcal{O}(\ell^5 \log^2 q)$.

In the following, for an isogeny $\alpha \in \operatorname{End}(E)$, we write $\mathbf{x}(\alpha) \in \operatorname{Quot} R_\ell$ and $\mathbf{y}(\alpha) \in \operatorname{Quot} R_\ell$ for the dehomogenizations of the x- and y-coordinate functions of α with respect to z.

As the left-hand side morphism $\varphi^2 + [q]$ contains an addition, the quest of determining which $[k]\varphi$ it coincides with on $E[\ell]^*$ involves a case distinction:

- We will first determine whether some finite ℓ-torsion point $P \in E[\ell]^*$ satisfies $\varphi^2(P) \in \{\pm[q]P\}$, which is the condition for Algorithm 28 to take one of the exceptional paths when adding $\varphi^2(P)$ and $[q]P$. To do so, represent the multiplication-by-q map by division polynomials in the equation $\mathbf{x}(\varphi^2) \stackrel{?}{=} \mathbf{x}([q])$, hence yielding $x^{q^2} \stackrel{?}{=} \phi_q/\psi_q^2$, and pass it to Algorithm 70. If the algorithm fails, **go to** the next bullet. Otherwise, there is a point $P \in E[\ell]^*$ such that the x-coordinates of φ^2 and $[q]$ match on P, hence the two possibilities are $\varphi^2(P) = [q]P$ and $\varphi^2(P) = -[q]P$.

  To obtain the correct sign, we proceed accordingly with $\mathbf{y}(\varphi^2) \stackrel{?}{=} \mathbf{y}([q])$, that is, $y^{q^2} \stackrel{?}{=} \omega_q/\psi_q^3$.

  - If $\varphi^2(P) = -[q](P)$, then $\varphi^2(P) + [q](P) = \infty = [0]\varphi(P)$, so by Lemma 69 the trace τ satisfies $\tau \bmod \ell = 0$. Hence, **return** 0.
  - If $\varphi^2(P) = [q]P$, then $\varphi^2(P) + [q](P) = [2q](P)$, so the trace τ of φ_ℓ satisfies $[2q](P) = [\tau]\varphi(P)$. If we are in this case, then τ is invertible modulo ℓ since $2q$ is, hence $\varphi(P) = [2q \cdot \tau^{-1} \bmod \ell](P)$. Therefore $q \equiv (2q)^2\tau^{-2} \pmod{\ell}$, that is $\tau^2 \equiv 4q \pmod{\ell}$, so q has a square root w modulo ℓ (which we can simply compute by trying all possible values) and we know that $\varphi(P) \in \{\pm[w](P)\}$.

    To determine the correct sign $s \in \{\pm 1\}$ with $\varphi(P) = s[w](P)$, apply Algorithm 70 to the equation $\mathbf{y}(\varphi) \stackrel{?}{=} \mathbf{y}([w])$, that is, $y^q \stackrel{?}{=} \omega_w/\psi_w^3$.

    Now the identity $\varphi^2 + [q] = [\tau]\varphi$ simplifies to $[2q] = [(sw)^2] + [q] = [\tau][sw]$, hence we can compute $k \in \{0, \ldots, \ell - 1\}$ with $k \equiv \tau \equiv 2q(sw)^{-1} \pmod{\ell}$ and **return** it.

  These implications also show that we cannot have $\varphi^2(P) = [q]P$ for some points $P \in E[\ell]^*$ and $\varphi^2(P) = -[q]P$ for others (which would make the procedure ambiguous): They would yield contradicting congruences for τ, hence only one case can occur at a time.

- Now suppose that for all $P \in E[\ell]^*$, we have $\varphi^2(P) \notin \{\pm[q]P\}$, so the addition Algorithm 28 takes the generic path in which the two input x-coordinates differ.

  For all $k \in \{0, \ldots, \ell - 1\}$, we perform the following steps:

By this case's assumption, the x-coordinate functions of the involved maps satisfy

$$\mathbf{x}(\varphi^2 + [q]) = \lambda^2 - a_1\lambda - a_2 - x^{q^2} - \frac{\phi_q}{\psi_q^2};$$
$$\mathbf{x}([k]\varphi) = \phi_k(x^q)/\psi_k^2(x^q),$$

where $\lambda = (\omega_q/\psi_q^3 - y^{q^2})/(\phi_q/\psi_q^2 - x^{q^2})$.

We can, again, pass the equation $\mathbf{x}(\varphi^2 + [q]) \stackrel{?}{=} \mathbf{x}([k]\varphi)$ to Algorithm 70 to determine whether the x-coordinates of $\varphi^2 + [q]$ and $[k]\varphi$ coincide on some point $P \in E[\ell]^*$ of order ℓ. If they don't, **continue** with the next k.

If they do, we have $\varphi^2(P) + [q]P \in \{\pm[k]\varphi(P)\}$ and hence, from Lemma 69, either $\varphi^2 + [q] = [k]\varphi$ or $\varphi^2 + [q] = -[k]\varphi$ on the set $E[\ell]^*$.

Now we can use the formulas for the y-coordinates

$$\mathbf{y}(\varphi^2 + [q]) = (-\lambda + a_1) \cdot \mathbf{x}(\varphi^2 + [q]) - \nu - a_3;$$
$$\mathbf{y}([k]\varphi) = \omega_k(x^q)/\psi_k^3(x^q),$$

where $\nu = (y^{q^2}\phi_q/\psi_q^2 - x^{q^2}\omega_q/\psi_q^3)/(\phi_q/\psi_q^2 - x^{q^2})$, to determine the correct sign $s \in \{\pm 1\}$ such that $\varphi^2 + [q] = s[k]\varphi$ on $E[\ell]^*$, and subsequently **return** sk.

Runtime. This procedure performs $\mathcal{O}(\ell)$ subroutine calls to Algorithm 70, which take $\mathcal{O}(\ell^4 \log^2 q)$ elementary arithmetic operations each. □

Algorithm 72 (Schoof [16, 17])**.**
Input. An elliptic curve E defined over a finite field $\mathbb{F}_q$ given by a Weierstraß equation.
Output. The number of $\mathbb{F}_q$-rational points $\#E(\mathbb{F}_q)$ on E.
Runtime. $\mathcal{O}(\log^8 q)$.

1. $A := 1$; $\ell := 3$; $C := \emptyset$.
2. **while** $A < 4\sqrt{q}$:
   find $k \in \{0, \ldots, \ell - 1\}$ with $(\varphi^2 + [q])|_{E[\ell]} = [k]\varphi|_{E[\ell]}$ using Algorithm 71.
   $A := \ell A$; $C := C \cup \{(k, \ell)\}$; $\ell := \texttt{next\_prime}(\ell + 1)$.
3. Compute $a \in \{-\frac{A-1}{2}, \ldots, \frac{A-1}{2}\}$ with
   $$\forall (x, n) \in C.\ a \equiv x \pmod{n}$$
   using the Chinese remainder theorem.
4. **return** $q + 1 - a$.

Correctness. Clear from the preceding discussion. □

Runtime. One can show [15] that there is a constant C such that

$$\prod_{\ell \le \log q \text{ prime}} \ell \ge Cq,$$

hence the largest prime ℓ used by the algorithm is bounded by $\mathcal{O}(\log q)$. The subroutine call for each ℓ requires $\mathcal{O}(\ell^5 \log^2 q) \subseteq \mathcal{O}(\log^7 q)$ operations; so in total the algorithm amounts to $\mathcal{O}(\log^8 q)$ operations. □

References

[1] Leonard M. Adleman. "The function field sieve". *Algorithmic Number Theory*. Springer, 1994, pp. 108–121.

[2] Razvan Barbulescu et al. "A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic". *Advances in Cryptology — Eurocrypt 2014*. Springer, 2014, pp. 1–16.

[3] Daniel J. Bernstein and Tanja Lange. *SafeCurves: choosing safe curves for elliptic-curve cryptography*. URL: http://safecurves.cr.yp.to.

[4] Ian Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic curves in cryptography*. London Mathematical Society Lecture Note Series 265. Cambridge University Press, 1999. ISBN: 0-521-65374-6.

[5] Whitfield Diffie and Martin E. Hellman. "New directions in cryptography". *IEEE Transactions on Information Theory* 22.6 (Nov. 1976), pp. 644–654.

[6] Taher Elgamal. "A public key cryptosystem and a signature scheme based on discrete logarithms". *IEEE Transactions on Information Theory* 31.4 (July 1985), pp. 469–472.

[7] Helmut Hasse. "Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung." *Journal für die reine und angewandte Mathematik* 175 (1936), pp. 193–208.

[8] Martin E. Hellman and Justin M. Reyneri. "Fast computation of logarithms in $\mathrm{GF}(q)$". *Advances in Cryptology: Proceedings of Crypto '82*. Springer, 1983, pp. 3–13.

[9] Antoine Joux and Reynald Lercier. "The function field sieve in the medium prime case". *Advances in Cryptology — Eurocrypt 2006*. Springer, 2006, pp. 254–270.

[10] Neal Koblitz. "Constructing elliptic curve cryptosystems in characteristic 2". *Advances in Cryptology — CRYPTO '90*. Lecture Notes in Computer Science. Springer, 1991, pp. 156–167.

[11] Serge Lang. *Elliptic curves: Diophantine analysis*. Grundlehren der mathematischen Wissenschaften 231. Springer, 1978. ISBN: 978-3-642-05717-5 / 978-3-662-07010-9.

[12] Ueli M. Maurer. "Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms". *Advances in Cryptology — Crypto '94*. Lecture Notes in Computer Science. Springer, Aug. 1994, pp. 271–281.

[13] Stephen C. Pohlig and Martin E. Hellman. "An improved algorithm for computing logarithms over $\mathrm{GF}(p)$ and its cryptographic significance". *IEEE Transactions on Information Theory* 24.1 (Jan. 1978), pp. 106–110.

[14] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". *Communications of the ACM* 21.2 (Feb. 1978), pp. 120–126.

[15] J. Barkley Rosser and Lowell Schoenfeld. "Approximate formulas for some functions of prime numbers". *Illinois Journal of Mathematics* 6 (1962), pp. 64–94.

[16] René Schoof. "Elliptic curves over finite fields and the computation of square roots $\bmod p$". *Mathematics of Computation* 44.170 (Apr. 1985), pp. 483–494.

[17] René Schoof. "Counting points on elliptic curves over finite fields". *Journal de Théorie des Nombres de Bordeaux* 7 (1995), pp. 219–254.

[18] Victor Shoup. "Lower bounds for discrete logarithms and related problems". *Advances in Cryptology — Eurocrypt '97*. Springer, 1997, pp. 256–266.

[19] Joseph H. Silverman. *The arithmetic of elliptic curves*. 2nd ed. Graduate Texts in Mathematics 106. Errata: Silverman [20]. Springer, 2009. ISBN: 978-0-387-09493-9.

[20] Joseph H. Silverman. *Errata and Corrections to The Arithmetic of Elliptic Curves, 2nd Edition*. Apr. 2015. URL: http://math.brown.edu/~jhs/AEC/AECErrata.pdf.

[21] Adam Leonhard van Tuyl. "The field of n-torsion points of an elliptic curve over a finite field". Master's thesis. Queen's University, Sept. 1997. URL: http://flash.lakeheadu.ca/~avantuyl/papers/masterthesis.pdf.

[22] Lawrence C. Washington. *Elliptic curves: Number theory and cryptography*. 2nd ed. Discrete Mathematics and its Applications. Chapman & Hall/CRC, 2008. ISBN: 978-1-4200-7146-7.