COUNTING POINTS ON ELLIPTIC CURVES

OLE ANDRÉ BIRKEDAL

Abstract. Elliptic curve cryptography is an approach to public-key cryptography. The elliptic curve chosen should be such that its number of points is divisible by a large prime factor. Ideally there should be a prime number of points on the curve.

In this paper we present the first efficient point counting algorithm due to Schoof, before giving a significant improvement due to Elkies. In the final section I give Satoh's algorithm which is even faster for fields of small characteristic, and has paved the way for the field of p-adic point counting.

Preface

At the start of my final year at the university I was fairly uncertain as to what my thesis would be about. After having consulted several potential advisors, all with very interesting topics, I finally talked to Kristian Gjøsteen who presented me with suggestion for a thesis concerning elliptic curves. I had for a long time been interested in number theory which is why I finally settled on this topic.

I would like to thank my high school teacher Thuy Skjæveland for being the first to spark my interest in mathematics. In addition I would like to thank Erlend Hamberg for all the much needed coffee and backgammon breaks through the semester.

A special thanks goes out to my thesis advisor Kristian Gjøsteen who always explained things in such a way that even I could grasp them. This guy has an answer to everything.

Contents

1. Algebraic curves

In this section we define the fundamental objects in algebraic geometry and state some facts about their structure. We will then move on to the theory of curves and Weil divisors. We will closely be following [Silverman, 1992] with some aid from [Fulton, 1969].

Given a field k we write $\mathbb{A}^n = \left\{(x_1, \ldots, x_n) : x_i \in \bar{k}\right\}$ for the affine n-space, where $\bar{k}$ denotes the algebraic closure of the field k.

Definition 1. Projective n-space *over a field k denoted $\mathbb{P}^n$ is the set of all $(n+1)$-tuples*

$$(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}$$

modulo the equivalence relation given by $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ if there exists $\lambda \in \bar{k}$ such that $x_i = \lambda y_i$. The equivalence class containing $(x_0, \ldots, x_n)$ is denoted $[x_0, \ldots, x_n]$.

Elements of the real projective 1-space can be identified with lines through the origin, that is the 1-dimensional subspaces of k^2.

Let $Gal(\bar{k}/k)$ be the Galois group of $\bar{k}/k$. This group acts on $\mathbb{A}^n$ in the following way: given $\sigma \in Gal(\bar{k}/k)$ and $P \in \mathbb{A}^n$ we define $\sigma(P) = (\sigma(x_1), \ldots, \sigma(x_n))$. Now we can define the set of k-rational points in $\mathbb{A}^n$ to be those fixed under action by the Galois group

$$\mathbb{A}^n(k) = \left\{P \in \mathbb{A}^n : \sigma(P) = P \quad \forall\, \sigma \in Gal(\bar{k}/k)\right\}.$$

Similarly it can be shown that the set of k-rational points in $\mathbb{P}^n$ are

$$\mathbb{P}^n(k) = \left\{P \in \mathbb{P}^n : \sigma(P) = P \quad \forall\, \sigma \in Gal(\bar{k}/k)\right\}.$$

Definition 2. *A polynomial $f \in \bar{k}[x_0, \ldots, x_n]$ is said to be* homogeneous of degree *d if for all $\lambda \in \bar{k}$ we have.*

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n).$$

Furthermore an ideal $I \subseteq \bar{k}[X]$ is said to be homogeneous *if it is generated by homogeneous polynomials.*

Definition 3. *A* projective algebraic set *is of the form*

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0\, \forall \textit{homogeneous}\, f \in I\}.$$

Given such a set V we associate to it an ideal $I(V) \in \bar{k}[x_0, \ldots, x_n]$ generated by

$$\left\{f \in \bar{k} : f\, \textit{homogeneous and}\, f(P) = 0\, \forall P \in V\right\}.$$

Definition 4. *A projective algebraic set V is called a* projective variety *if the homogeneous ideal defined above is a prime ideal in $\bar{k}[x_0, \ldots, x_n]$.*

We say that the variety V is *defined over k*, denoted V/k, if its associated ideal $I(V)$ can be generated by polynomials in $k[x_0, \ldots, x_n]$.

Definition 5. *Let V/k be a projective variety, then the projective coordinate ring of V/k is defined by*

$$k[V] = \frac{k[x]}{I(V/k)}.$$

Note that since $I(V/k)$ is a prime ideal, the coordinate ring is an integral domain. This enables us to form the quotient field of $k[V]$ which we denote $k(V)$, and it is called the function field *of V.*

A rather interesting ideal to keep in mind is given by

$$M_P = \left\{ f \in \bar{k}[V] : f(P) = 0 \right\}.$$

This is a maximal ideal because the map $\phi : \bar{k}[V] \to \bar{k}$ given by $f \mapsto f(P)$ has kernel exactly M_P. It is clearly onto, so it induces an isomorphism

$$\tilde{\phi} : \bar{k}[V]/M_P \to \bar{k}.$$

Definition 6. *The* localization of $\bar{k}[V]$ at M_P *is given by*

$$\bar{k}[V]_P = \left\{ h \in \bar{k}[V] : h = f/g \, f, g \in \bar{k}[V] \, and \, g(P) = 0 \right\}.$$

The functions in $\bar{k}[V]_P$ are all defined at P.

For more information about localization in commutative rings I refer to [Matsumura, 1986].

Definition 7. *Let V be a variety, then the* dimension *of V is the transcendence degree of $\bar{k}(V)$ over $\bar{k}$. We denote this value by $dim(V)$.*

Given the above definition we have in particular that the transcendence degree of $\bar{k}(x, y)$ over $\bar{k}$ is 2, because x and y are two (independent) transcendental variables.

Example 1. *Let V be the variety given as*

$$V : y^2 = x^3 + ax + b.$$

This corresponds to a polynomial $f(x, y) = x^3 + ax + b - y^2 \in \bar{k}[x, y]$. Since there is imposed a relation between x and y we have that the transcendence degree is 1 and $dim(V) = 1$. The varieties of dimension 1 are called curves*, and is what we'll be working with.*

We now have the objects, the next logical step is to define maps between the varieties.

Definition 8. *Let V_1 and V_2 be projective varieties, a* rational map *$\phi : V_1 \to V_2$ is a set of maps $\{\phi_0, \ldots, \phi_n\}$ with $\phi_i \in \bar{k}(V_1)$ such that for every $P \in V_1$ we define*

$$\phi(P) = [\phi_0(P), \ldots, \phi_n(P)] \in V_2.$$

Such a rational map is called a morphism *if it is defined at every point P.*

The varieties and the morphisms between them make up a category, so our next definition of an isomorphism will be the general one found in category theory.

Definition 9. *Two varieties V and W are* isomorphic *denoted $V \simeq W$ if there exist morphisms $\phi : V \to W$ and $\psi : W \to V$ such that $\phi\psi = 1_W$ and $\psi\phi = 1_V$. If the rational functions ψ and ϕ are defined over k we say that V and W are isomorphic over k. If not, they are isomorphic over some field extension of k (i.e. $\bar{k}$).*

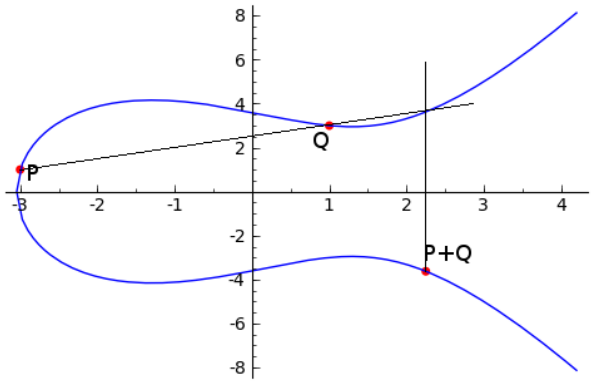


FIGURE 1. The elliptic curve $y^2 = x^3 - 5x + 13$

Recall that curves are projective varieties of dimension one. Even more special are elliptic curves, which are curves with *genus* equal to 1. This will be introduced later on. These are in practise the only curves we will be working with.

Composition of points on an elliptic curve can be done in the following way: let $P, Q \in E$ and l the line connecting them. We let R be the third point that l intersects, then composition denoted $P + Q$ is the mirror point of R (i.e. $-R$). See Figure 1.

Proposition 1. *An elliptic curve E is an abelian group with the group operation as described above. The identity element is denoted O.*

For a proof of the above proposition i refer to [Silverman, 1992].

Out fields k shall never be of characteristic 2 or 3, this enables us to assume that every elliptic cure is given by a Weierstrass equation of the form

$$E : y^2 = x^3 + ax + b$$

with $a, b \in k$ [Silverman, 1992].

Example 2. *As an example of point addition we consider*

$$E : y^2 = x^3 - 5x + 13$$

as in Figure 1. We have that $P = (-3, 1)$ and $Q = (1, 3)$. By the composition law as described above we have that $P + Q = (\frac{9}{4}, \frac{-29}{8})$.

Definition 10. *Let C be a curve defined by the polynomial equation*

$$f(x, y) = 0$$

and $P = (x_0, y_0) \in C$ a point on the curve. Then P is singular *if and only if all partial derivatives vanish at P*

$$\frac{\partial}{\partial x} f(P) = \frac{\partial}{\partial y} f(P) = 0.$$

This is in fact the implicit function theorem at work, saying that there is no way to represent the curve as the graph of a function of one variable near P. In addition we say that a curve C is *smooth* if it has no singular points.

Definition 11. *Let C be a curve and $P \in C$ a non-singular point on the curve. The* valuation *on $\bar{k}[C]_P$ is given by*

$$ord_P : \bar{k}[C]_P \to \{0, 1, 2, \ldots\} \cup \{\infty\}$$
$$ord_P(f) = max\left\{d \in \mathbb{Z} : f \in M_P^d\right\}$$

This is called the order of f at P. *Letting $ord_P(f/g) = ord_P(f) - ord_P(g)$ we can extend the definition to the entire quotient ring $\bar{k}(C)$*

$$ord_P : \bar{k}(C) \to \mathbb{Z} \cup \{\infty\}.$$

The definition of order agrees with the one found in complex analysis. If $ord_P(f) < 0$ then f has a pole at P, similarly if $ord_P(f) \geq 0$ then f has a zero and is defined at P.

Proposition 2. *Let C be a smooth curve. If $f \in \bar{k}(C)$ is not the constant function, then f has finitely many poles and zeros.*

Definition 12. *The* divisor group *of a curve C is the free abelian group generated by points of C, denoted $Div(C)$. A divisor $D \in Div(C)$ is of the form*

$$D = \sum_{P \in C} n_P(P)$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many P.

With this in mind we can define the degree of a divisor as the sum of its coefficients. We also define the sum of a divisor as the sum in the group $E(\bar{k})$, so

$$\deg(D) = \deg\left(\sum_{P \in C} n_P(P)\right) = \sum_{P \in C} n_P \in \mathbb{Z}$$
$$sum(D) = sum\left(\sum_{P \in C} n_P(P)\right) = \sum_{P \in C} n_P P \in E(\bar{k}).$$

These functions enable us to define the subgroup of divisors of degree zero, $Div^0(C) \subset Div(C)$, so $Div^0(C) = \{D \in Div(C) : \deg D = 0\}$.

Now let C be a smooth curve and $f \in \bar{k}(C)$ a non-zero function. Since f has finitely many poles and zeros (Prop. 2) we can define the divisor of a function as

$$div(f) = \sum_{P \in C} ord_P(f)(P)$$

Note that ord_P is a valuation we have $ord_P(fg) = ord_P(f) + ord_P(g)$ for non-zero $f, g \in \bar{k}(C)$. Thus we get a group homomorphism

$$div : \bar{k}(C)^* \to Div(C).$$

Definition 13. *The* principal divisors *of C are the divisors of the form $D = div(f)$ for some non-zero $f \in \bar{k}(C)$. This is exactly the image of the function div and we denote this set by $Prin(C)$.*

Note that since divisors of rational functions have the same number of poles and zeros (when counted correctly), we have $\deg(div(f)) = 0$.

Two divisors are said to be *equivalent* denoted $D_1 \sim D_2$ if their difference is a principal divisor, $D_1 - D_2 = div(f)$ for some $f \in \bar{k}(C)$. We say that

a divisor D is *positive* $\sum n_P(P) = D \geq 0$ if $n_P \geq 0$ for every $P \in C$. Furthermore we can put a partial ordering on on $Div(C)$ writing $D_1 \geq D_2$ to indicate that $D_1 - D_2$ is positive.

Definition 14. *Let C be a curve. The* Picard group of C *is the quotient $Div(C)/Prin(C)$ and is denoted $Pic(C)$. Note that since $Prin(C) \subseteq Div^0(C)$ we define $Pic^0(C) = Div^0(C)/Prin(C)$ which is the* degree 0 part *of the Picard group.*

Example 3. *Inequalities can easily summarize some key properties of a function. So instead of saying $f \in \bar{k}(C)$ is regular everywhere except at P and Q, where it has a pole and a root of order m and n respectively, we could write*

$$div(f) \geq -m(P) + n(Q).$$

The last example motivates our next definition, where we collect all functions which satisfy some inequality. This turns out to make up a finite dimensional $\bar{k}$-vector space.

Definition 15. *Let $D \in Div(C)$ be a divisor, and we define the set of functions*

$$\mathscr{L}(D) = \left\{ f \in \bar{k}(C) : div(f) \geq -D \right\} \cup \{0\}.$$

This vector space can be seen to be finite by the next proposition, a proof of which can be found in [Fulton, 1969].

Proposition 3. *$\mathscr{L}(D)$ is a finite dimensional $\bar{k}$-vector space, and we denote its dimension by*

$$\ell(D) = dim_{\bar{k}} \mathscr{L}(D).$$

Next we introduce differential forms on our curves, these will be useful for different purposes as described below. In addition they will help us state the Riemann-Roch theorem and a definition of the genus g.

Definition 16. *The space of differential forms on a curve C is a $\bar{k}(C)$-vector space denoted Ω_C generated by symbols subject to the relations known from analysis. For $x, y \in \bar{k}(C)$ and $a \in \bar{k}$*

1. $d(x + y) = dx + dy$
2. $d(xy) = xdy + ydx$
3. $da = 0$

Let $f_i \in \bar{k}(C)$ and dx_i be the symbols as defined above, a general element $\omega \in \Omega_C$ is of the form

$$\omega = \sum f_i dx_i.$$

It can be shown that if $t \in \bar{k}(C)$ is the uniformizer [Fulton, 1969] then $\omega = fdt$ for some $f \in \bar{k}(C)$ and we define

$$ord_P(\omega) = ord_P(f).$$

The divisor of a differential is given by

$$div(\omega) = \sum_{P \in C} ord_P(\omega)(P) \in Div(C).$$

Divisors in the image of the map $div : \Omega_C \to Div(C)$ are called *canonical divisors*. They will play a role in the next theorem which will serve as an important tool for calculating the dimension of the vector space $\mathscr{L}(D)$, which will be crucial in establishing an important isomorphism.

Theorem 1. ***(Riemann-Roch)*** *Let C be a smooth curve and K_C a canonical divisor on C. Then for any $D \in Div(C)$ we have*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1$$

where $g \geq 0$ is called the genus *of the curve C.*

A proof would be well outside the scope of this paper, but a classical proof based on Noether's reduction lemma can be found in [Fulton, 1969]. Almost directly from the above theorem follows a nice corollary, its short proof can be found in [Silverman, 1992].

Corollary 1. *Let K_C be a canonical divisor, then*

a) $\ell(K_C) = g$
b) $\deg K_C = 2g - 2$
c) $\deg D > 2g - 2 \implies \ell(D) = \deg D - g + 1$

Given a non-constant map of curves $\phi : C_1 \to C_2$, we have an induced map on function fields

$$\phi^* : K(C_2) \to K(C_1)$$
$$f \mapsto f\phi.$$

From this again we get an induced map on differential forms

$$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$$
$$\phi^*\left(\sum f_i dx_i\right) = \sum (\phi^* f_i) d(\phi^* x_i).$$

Definition 17. *Let $\phi : C_1 \to C_2$ be a map of curves and ϕ^* its induced map on function fields. We then say that ϕ is a* separable map *if $K(C_1)/\phi^* K(C_2)$ is a separable extension.*

Similarly, the degree of ϕ (as above) is the degree of the associated field extension. Recall that a field extension is separable if and only if the derivative of the minimal polynomial for each element is non-zero. This fact is the motivation for our next result, which gives a useful criterion for determining when a map is separable.

Proposition 4. *Let $\phi : C_1 \to C_2$ be a map of curves, then ϕ is separable if and only if the induced map $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is non-zero.*

The next result gives us the key property that we need in separable maps, important for point counting.

Theorem 2. *If ϕ is a separable map then*

$$\#\ker \phi = \deg \phi.$$

Before leaving the realm of differentials for a while we introduce a special differential.

Definition 18. *The* invariant differential *on* $E : y^2 = x^3 + ax + b$ *is given by*

$$\omega = \frac{dx}{\frac{d}{dy}(y^2 - x^3 - ax - b)} = \frac{dx}{2y}.$$

This is a *holomorphic* differential, having no poles or zeros [Silverman, 1992]. The name comes from it being invariant under the translation isomorphism

$$t_Q : E \to E$$
$$P \mapsto P + Q$$

as shown in [Silverman, 1992]. We note that since $t_Q^*(\omega) = \omega$ we have that $t_Q^*(k\omega) = kt_Q^*(\omega) = k\omega$ for any integer k. Especially we have that $2\omega = \frac{dx}{y}$ is also invariant under translation, this differential will be used in Section 7 .

Proposition 5. *Let* C *be a curve of genus* 1 *(think elliptic curve), and let* $P, Q \in C$ *be points on the curve and* $(P), (Q)$ *their corresponding divisors. Then we have that*

$$\text{Âă}(P) \sim (Q) \iff P = Q.$$

Proof. We prove from left to right, the other implication is trivial. Let $f \in \bar{k}(C)$ be such that

$$div(f) = (P) - (Q)$$

so if $div(f) = 0$ then we are done. We have the vector space

$$\mathscr{L}(Q) = \left\{ f \in \bar{k}(C) : div(f) \geq -(Q) \right\} \cup \{0\}$$

which has dimension $\ell(Q) = dim_{\bar{k}}\mathscr{L}(Q)$. Since $\deg Q = 1$ and $g = 1$ we can use Corollary 1c

$$\ell(Q) = \deg Q - g + 1 = 1.$$

But since the constant functions are always in $\mathscr{L}(Q)$ we have by the dimension restriction that they are the only ones, and $f \in \bar{k}$. This means that $div(f) = 0$ and we are done. □

Theorem 3. *Let* E *be an elliptic curve and* $Pic^0(E) = Div^0(E)/Prin(E)$ *be the Picard group, then*

$$sum : Pic^0(E) \to E(\bar{k})$$

is an isomorphism of abelian groups.

Proof. We begin by showing that there is a unique point $P \in E(\bar{k})$ associated to each $D \in Div^0(E)$ as follows

$$D \sim (P) - (O).$$

This will be given by a map

$$\sigma : Div^0(E) \to E(\bar{k}).$$

From Corollary 1 we have that $\ell(D + (O)) = \deg(D + (O)) = 1$ since $\deg D = 0$. Let then $f \in \bar{k}(E)$ be a generator for $\mathscr{L}(D + (O))$, so by definition

$$div(f) \geq -D - (O).$$

But since $\deg(div(f)) = 0$ and $\deg(-D - (O)) = -1$ we have for some $P \in E(\bar{k})$ that

$$div(f) = -D - (O) + (P)$$

which is exactly the definition of

$$D \sim (P) - (O).$$

This point P is unique, because if we assume that P' is another point with the same property, then

$$(P) \sim D + (O) \sim (P')$$

so by Proposition 5 we have that $P = P'$.

The map σ is easily seen to be a surjection, because for any $P \in E(\bar{k})$ we have

$$\sigma((P) - (O)) = P.$$

Now if we can show that the kernel of σ is exactly the principal divisors we are done. Let us assume that $\sigma(D) = O$ so from definition we have that $D \sim (O) - (O) \sim (O)$ meaning $D - (O) = div(f)$ for some $f \in \bar{k}(E)$, so $D = div(f)$ is principal. For the other implication we assume that $D = div(f)$ is principal. Using the definition and letting P be any point and $f, f' \in \bar{k}(E)$ a calculation yields

$$\sigma(D) = \sigma(div(f)) = (P) - (O)$$

$$div(f) \sim (P) - (O)$$

$$div(f) - (P) - (O) = div(f')$$

$$(O) - (P) = div(f') - div(f) = div(f'f)$$

So $(P) \sim (O)$ which implies $P = O$ from Proposition 5.

For a proof that the group law on E described earlier is the same as the group law on $Pic^0(C)$ I refer to [Silverman, 1992].

We have thus established the group isomorphism which we again will denote by

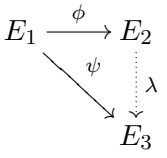
$$\sigma : Div^0(E)/Prin(E) = Pic^0(E) \to E(\bar{k}).$$

□

Definition 19. *An* isogeny *between two elliptic curves E_1 and E_2 is a morphism $\phi : E_1 \to E_2$ which satisfies $\phi(O) = O$. In addition, two curves are said to be* isogenous *(of degree n) if there exists a non-zero isogeny (of degree n) between them.*

The following is a nice result about isogenies using separability, see [Silverman, 1992] for a proof.

Proposition 6. *Let ϕ be a separable isogeny as below and $\ker\phi \subseteq \ker\psi$, then there exists a unique $\lambda : E_2 \to E_3$ such that the diagram commutes*



Now note that $\phi : E_1 \to E_2$ induces a map on Picard groups

$$\phi^* : Pic^0(E_2) \to Pic^0(E_1).$$

In addition we have isomorphisms $E_1 \overset{\sigma_1}{\simeq} Pic^0(E_1)$ and $E_2 \overset{\sigma_2}{\simeq} Pic^0(E_2)$ from Theorem 3, combining this gives a composition

$$E_2 \overset{\sigma_2^{-1}}{\to} Pic^0(E_2) \overset{\phi^*}{\to} Pic^0(E_1) \overset{\sigma_1^{-1}}{\to} E_1.$$

Proposition 7. *The composition above is the* dual isogeny *of ϕ, denoted $\widehat{\phi} : E_2 \to E_1$. It has the following properties*

(1) $\widehat{\phi}\phi = [\deg \phi]$ *on* E_1 *and* $\phi\widehat{\phi} = [\deg \phi]$ *on* E_2.
(2) *If* $\psi : E_2 \to E_3$ *is another isogeny then* $\widehat{\psi\phi} = \widehat{\phi}\widehat{\psi}$.
(3) *If* $\lambda : E_1 \to E_2$ *is another isogeny then* $\widehat{\phi + \phi} = \widehat{\phi} + \widehat{\psi}$.
(4) $\deg \widehat{\phi} = \deg \phi$.
(5) $\widehat{\widehat{\phi}} = \phi$.

We end this section by a short comment on the dual isogeny. If ϕ is a separable map then the first property follows by the following argument: letting $\deg \phi = m$ we have that $\# \ker \phi = m$ which is clearly a subgroup of elements of order m

$$\ker \phi \subseteq \ker[m].$$

Using Proposition 6 we have that there exists a unique $\lambda : E_2 \to E_1$ such that $\lambda\phi = [m]$ which by setting $\lambda = \widehat{\phi}$ is exactly what we want. The case where ϕ is assumed inseparable can be found in [Silverman, 1992].

2. p-ADIC NUMBERS

There are several definitions of p-adic integers, we will start with the easiest. Later we will see an algebraic construction using inverse limits as found in [Rot, 1979]. For this chapter we will closely be following [Rob, 2000].

Definition 20. *A p-adic integer is a formal power series with coefficients $a_i \in \mathbb{Z}/p\mathbb{Z}$*

$$\sum_{i=0}^{\infty} a_i p^i.$$

We denote the set of p-adic integers by $\mathbb{Z}_p$.

With this in mind you can identify a p-adic integer with a sequence of coefficients $(a_i)_{i>0}$. This is in fact a Cauchy sequence with the p-adic metric in $\mathbb{Q}$ given as follows: let x be a rational number then we can write $x = p^n \frac{a}{b}$ where p does not divide a or b. If they do not contain p as a factor we set $n = 0$. We then let the p-adic metric be given as $|x|_p = p^{-n}$. This is similar to how the real numbers are constructed using equivalence classes of Cauchy sequences from analysis.

Already we can see that the ring of p-adic integers is not countable. We do this by taking a countable sequence of p-adic integers

$$a = \sum a_i p^i \quad b = \sum b_i p^i \quad c = \sum c_i p^i \quad \dots$$

then we construct a new p-adic integer

$$x = \sum x_i p^i$$

where we choose $x_0 \neq a_0$, $x_1 \neq b_1$, $x_2 \neq c_2$, ... This new p-adic integer is different from those already in the set, thus they do not exhaust the whole set of p-adic integers. This shows that a mapping from $\mathbb{N}$ into the p-adic integers is never a surjection.

Addition of two p-adic integers is done component-wise, using a system of carries if the new coefficient exceeds $p-1$. This is best illustrated by an example.

Example 4. *Let $p > 3$ with $a = 3 + 0p + 0p^2 + 0p^3 + \dots$ and $b = (p-2) + (p-2)p + (p-2)p^2 + (p-2)p^3 + \dots$ two p-adic integers. Adding them together component-wise yields*

$$a + b = (p+1) + (p-2)p + (p-2)p^2 + (p-2)p^3 + \dots.$$

Since the first component exceeds $p-1$ by 2 we reduce is modulo p and carry 2 over to the next component, giving us

$$a + b = 1 + (p-2+2)p + (p-2)p^2 + (p-2)p^3 + \dots.$$

The second component now exceeds $p-1$ by 1, so reducing it modulo p and carrying the 1 gives

$$a + b = 1 + 0p + (p-1)p^2 + (p-2)p^3 + \dots.$$

There are nothing more to carry and the addition is finished. In theory you could be carrying forever, because recall that these are infinite formal sums.

It is clear that every p-adic integer has an additive inverse thus making $\mathbb{Z}_p$ an abelian group under the addition we just defined. Multiplication can be done similarly using a system of carries to keep components in the range $0 < a_i < p$. Not all elements have an inverse under multiplication, for example the element $p = 0 + p + 0p^2 + \ldots$ has no inverse because

$$p \sum_{i=0}^{\infty} a_i p^i = a_0 p + a_1 p^2 + \ldots \neq 1.$$

We thus have that $\mathbb{Z}_p$ is a commutative ring. The next result enables us to construct a field of p-adic numbers.

Proposition 8. *$\mathbb{Z}_p$ has no zero divisors (i.e. it is an integral domain).*

Proof. Let $a = \sum a_i p^i$ and $b = \sum b_i p^i \in \mathbb{Z}_p$ be non-zero. We denote by a_v the first non-zero coefficient of a and similarly b_w the first non-zero coefficient of b. Note that $a_v, b_w \in \{0, 1, \ldots, p-1\}$, so p divides neither of them. As a consequence p does not divide their product $a_v b_w$ either. By multiplying a and b we see that the first non-zero coefficient of the product ab is c_{v+w}, the coefficient of p^{v+w}. This coefficient is defined by

$$c_{v+w} \equiv a_v b_w \pmod{p}$$

But since p does not divide $a_v b_w$ we have that $c_{v+w} \neq 0$ and thus the product ab can never be zero. □

Before moving on I want to view this from an entirely algebraic perspective. Again letting $x = \sum a_i p^i \in \mathbb{Z}_p$ we can reduce it modulo p, so $x \equiv a_0 \pmod{p}$. Reducing it modulo p^2 gives $x \equiv a_0 + a_1 p \pmod{p}$, and so on. In general we can define reduction modulo p^n as follows

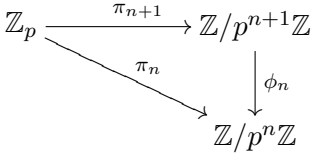
$$\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$$

$$\pi_n(x) = \sum_{i=0}^{n-1} a_i p^i \pmod{p^n}.$$

In a sense we have that $\pi_n(x) = x$ when $n \to \infty$, thus we want to say that the ring $\mathbb{Z}/p^n\mathbb{Z}$ converges to $\mathbb{Z}_p$. This is exactly the inverse limit construction from homological algebra [Rot, 1979], with respect to the homomorphisms

$$\phi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$$

given by reduction modulo p^n. This gives us a commutative diagram



which we can interpret by saying that $\mathbb{Z}_p$ is closer to $\mathbb{Z}/p^{n+1}\mathbb{Z}$ than it is to $\mathbb{Z}/p^n\mathbb{Z}$. We have that

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} \subseteq \prod \mathbb{Z}/p^n\mathbb{Z}$$

so a p-adic integer corresponds to a sequence $(a_n)_{n \leq 0}$. Given $x = (x_0, x_1, \ldots) \in \mathbb{Z}_p$ we have that

$$\pi_n(x) = \phi_n \pi_{n+1}(x) \implies x_n \equiv x_{n+1} \pmod{p^{n+1}}$$

The n^{th} elements of this sequence is the partial sum $x_n = \sum_{i=0}^{n-1} x_i p^i$.

Now since $\mathbb{Z}_p$ is an integral domain we can form its quotient field, $Quot(\mathbb{Z}_p)$ which we denote by

$$\mathbb{Q}_p = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}_p, b \neq 0 \right\}.$$

Letting $q = p^r$ we can construct the ring $\mathbb{Z}_q$, this is similar to the construction of $\mathbb{F}_q$ from $\mathbb{F}_p$. It is convenient to introduce the notation $\pi = \pi_1$, which is viewed as the projection down to $\mathbb{Z}/p\mathbb{Z}$. We then let $f \in \mathbb{Z}_p[x]$ be a polynomial of degree r such that $\pi(f) \in \mathbb{Z}/p\mathbb{Z}[x]$ is irreducible. Our new ring of q-adic integers is then given by the quotient

$$\mathbb{Z}_q = \mathbb{Z}_p[x]/(f).$$

This is again an integral domain and we can form its quotient field $Quot(\mathbb{Z}_q) = \mathbb{Q}_q$, which we call *the field of q-adic numbers*. It is this field that we will be lifting to in Satoh's algorithm.

In practice one only computes a p-adic integer up to some precision N.

Definition 21. *Given a p-adic integer $x \in \mathbb{Z}_p$ we say that*

$$\pi_N(x) \in \mathbb{Z}/p^N\mathbb{Z}$$

is an approximation of x with precision N.

3. Weil pairing and Tate module

Proposition 9. *The* multiplication by n *map*

$$[n] : E \to E$$

$$P \mapsto nP$$

has order n^2.

Proof. The shortest proof relies heavily on the dual isogeny, so letting $d = \deg[n]$ and using the properties of the dual isogeny we calculate

$$[d] = \widehat{[n]}[n] = [n][n] = [n^2]$$

and since $End(E)$ is torsion free [Silverman, 1992] we get that $d = n^2$. □

A subgroup of $E(k)$ that will be of special interest to us is the group of points P with finite order n, this is by definition the kernel of the multiplication by n map.

Definition 22. *The* n*-torsion subgroup denoted* $E[n]$ *is the group of points of order* n *in* E.

$$E[n] = \{P \in E : nP = O\}.$$

We are now ready to construct a bilinear pairing between the n-torsion subgroups of an elliptic curve and the roots of unity μ_n. This will prove useful to us in coming proofs. In addition it has well established applications within number theory, cryptography and identity based encryption.

The pairing we want to construct is of the form

$$e_n : E[n] \times E[n] \to \mu_n.$$

Let $T \in E[n]$ be an n-torsion point. From [Washington, 2008] we know that there exists $f \in \bar{k}(E)$ such that $div(f) = n(T) - n(O)$. Now letting $T' \in E[n^2]$ be such that $nT' = T$, we have a function $g \in \bar{k}(E)$ such that

$$div(g) = \sum_{R \in E[n]} (T' + R) - (R).$$

This follows from the fact that there are n^2 points in $E[n]$, the points (R) in the sum cancel, so we are left with $n^2T' = nT = O$. Clearly $\deg(div(g)) = 0$.

If we now form the composition $f \circ [n]$, we notice that the points $P = T' + R$ with $R \in E[n]$ are those with the property $nP = T$. Now since f has a root at T from construction, we see that $f \circ [n]$ has a root at P. Using the fact that ord_P is a valuation so that $div(g^n) = n\ div(g)$, and writing out the divisors of our functions we see that

$$div(f \circ [n]) = n \sum_{R \in E[n]} (T' + R) - n \sum_{R \in E[n]} (R) = div(g^n).$$

Since our two rational functions $f \circ [n]$ and g^n have the same divisors, they have the same poles and zeros. Therefore they differ by multiplication of a constant, so $f \circ [n] = \lambda g^n$ with $\lambda \in \bar{k}$. With a suitable choice of λ we can assume that

$$f \circ [n] = g^n.$$

Letting $S \in E[n]$ be another n-torsion point and $X \in E(\bar{k})$ a point on the curve we calculate that

$$g(X+S)^n = (f \circ [n])(X+S) = f([n]X + [n]S) = f([n]X) = g(X)^n.$$

Definition 23. *Given the above calculation the* Weil pairing *is defined as*

$$e_n : E[n] \times E[n] \to \mu_n$$
$$(S,T) \mapsto \frac{g(X+S)}{g(X)}.$$

Proposition 10. *The Weil pairing e_n satisfies the following properties*

1. *Bilinear in both variables: $e_n(P_1+P_2,Q) = e_n(P_1,Q)e_n(P_2,Q)$ and similarly for the other variable.*
2. *Alternating: $e_n(P,Q) = e_n(Q,P)^{-1}$.*
3. *Non-degenerate: If $e_n(P,Q) = 1$ for all $P \in E[n]$ then $Q = O$.*
4. *Galois invariant: For all $\sigma \in Gal(\bar{k}/k)$ we have $e_n(P,Q)^\sigma = e_n(\sigma(P),\sigma(Q))$.*

Proof. See [Silverman, 1992]. □

Proposition 11. *Letting ℓ be a prime not dividing $char(k)$ we have the following isomorphism of abelian groups*

$$E[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

The last proposition enables us to view automorphism of $E[\ell]$ as 2×2 invertible matrices, so we obtain a mod ℓ Galois representation

$$Gal(\bar{k}/k) \xrightarrow{\rho} Aut(E[\ell]) \simeq GL_2(\mathbb{Z}/\ell\mathbb{Z}).$$

To avoid working with congruences and instead work with equalities, we can construct and work with a field of characteristic 0. This is done by taking the inverse limit as introduced in Chapter 2 of the sequence

$$\ldots \xrightarrow{[l]} E[\ell^{n+1}] \xrightarrow{[l]} E[\ell^n] \xrightarrow{[l]} E[\ell^{n-1}] \to \ldots$$
$$T_\ell(E) = \varprojlim E[\ell^n].$$

This is called the *ℓ-adic Tate module* of E. Notice that since each of the groups $E[\ell^n]$ has a $\mathbb{Z}/\ell^n\mathbb{Z}$-module structure, $T_\ell(E)$ will have natural structure as a module over the ring of ℓ-adic integers $\mathbb{Z}_\ell$ as follows: $r \in \mathbb{Z}_\ell$ and $x = (x_n)_n \in T_\ell(E)$ then

$$r(x_n)_n = ((r \mod p^n)x_n)_n.$$

Similarly we can in a sense "glue" together the Weil pairings

$$e_{\ell^n} : E[\ell^n] \times E[\ell^n] \to \mu_{\ell^n}$$

by constructing the ℓ-adic roots of unity, and we obtain what is called the *ℓ-adic Weil pairing*

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu).$$

We end this section by stating a result which enables us to view endomorphisms on E as 2×2 matrices by choosing a $\mathbb{Z}_\ell$ basis.

Proposition 12. *The map $\phi : End(E) \to End(T_\ell(E))$ is an injective ring homomorphism. In addition we have that $End(T_\ell(E)) \simeq M_2(\mathbb{Z}_\ell)$ where M_2 is the ring of 2×2 matrices with $\mathbb{Z}_\ell$ coefficients.*

This will prove useful later on when establishing relations between determinants, trace and degrees of maps.

4. Frobenius and finite fields

Throughout this section our fields k will be finite, so let $char(k) = p$ for a prime p. This means that $k = \mathbb{F}_q$ for some $q = p^r$.

Definition 24. *The* Frobenius *endomorphism is the p^{th}-power map*

$$\phi : k \to k$$
$$x \mapsto x^p$$

which induces a map on curves as follows

$$\phi : E(k) \to E^{\phi}(k)$$
$$(x_0, \ldots, x_n) \mapsto (x_0^p, \ldots, x_n^p)$$

where E^{ϕ} is the curve E with ϕ applied to its coefficients.

$$E : y^2 = x^3 + ax + b \quad E^{\phi} : y^2 = x^3 + \phi(a)x + \phi(b).$$

We can apply the Frobenius endomorphism r times

$$\phi^r(x) = x^{p^r} = x^q$$

And since every finite field of q elements is the splitting field of $x^q - x$, it is in other words the fixed points of the q^{th} Frobenius endomorphism

$$\phi^r(x) = x \iff x \in \mathbb{F}_q.$$

The same is true for all intermediate fields of size p^k with $0 < k \leq r$, so in general we have that the ϕ^k fixes the elements of the field $\mathbb{F}_{p^k}$.

Proposition 13. *Let $\sigma : E \to E^{\sigma}$ be the p^{th} Frobenius on an elliptic curves*

$$E : y^2 = x^3 + ax + b.$$

Then we have that $j(E^{\sigma}) = \sigma(j(E))$ where j is the j-invariant of E.

Proof. This follows directly from the fact that the Frobenius map is an endomorphism and that the j-invariant is given by an algebraic expression [Silverman, 1992]

$$j(E) = \frac{6912a^3}{4a^3 + 27b^2}.$$

Applying σ gives us

$$\sigma(j(E)) = \frac{6912\sigma(a)^3}{4\sigma(a)^3 + 27\sigma(b)^2} = j(E^{\sigma}).$$

□

Definition 25. *Given an abelian group A and let $\mathbb{R}$ be the set of real numbers, then*

$$d : A \to \mathbb{R}$$

is called a positive definite quadratic form if

1. *$d(a) = d(-a)$ for all $a \in A$.*
2. *The pairing*
$$A \times A \to \mathbb{R}$$
$$(a, b) \mapsto d(a + b) - d(a) - d(b)$$
for all $a, b \in A$.
3. *$d(a) \geq 0$ for all $a \in A$.*

(4) $d(a) = 0 \iff a = 0$.

The next result is one of the important ingredients of the proof of the Hasse bound.

Proposition 14. *The degree map*

$$\deg : Hom(E_1, E_2) \to \mathbb{Z}$$

is a positive definite quadratic form.

Proof. Clearly $\deg f = \deg(-f)$. The only thing that takes a proof is the bilinearity of the pairing

$$Hom(E_1, E_2) \times Hom(E_1, E_2) \to \mathbb{Z}$$

$$\langle \phi, \psi \rangle \mapsto \deg(\phi + \psi) - \deg \phi - \deg \psi.$$

For this proof we will make extensive use of the dual isogeny, but first notice that we have an injection of multiplication by n maps

$$[\quad] : \mathbb{Z} \to End(E_1).$$

A calculation then yields

$$\begin{aligned} [\langle \phi, \psi \rangle] &= [\deg(\phi + \psi)] - [\deg \phi] - [\deg \psi] \\ &= \widehat{(\phi + \psi)}(\phi + \psi) - \widehat{\phi}\phi - \widehat{\psi}\psi \\ &= \widehat{\phi}\psi + \widehat{\psi}\phi \end{aligned}$$

The pairing is then shown to be linear in the first variable, the second variable is similar.

$$\begin{aligned} [\langle \phi_1 + \phi_2, \psi \rangle] &= \widehat{\psi}(\phi_1 + \phi_2) + \widehat{(\phi_1 + \phi_2)}\psi \\ &= (\widehat{\psi}\phi_1 + \widehat{\phi_1}\psi) + (\widehat{\psi}\phi_2 + \widehat{\phi_2}\psi) \\ &= [\langle \phi_1, \psi \rangle] + [\langle \phi_2, \psi \rangle] \end{aligned}$$

□

For a complete proof of the next theorem we refer to [Silverman, 1992], it is essentially the fact that enables us to do point counting.

Theorem 4. *Let ϕ be the q^{th} Frobenius map on $E/\mathbb{F}_q$. Then the map $1 - \phi$ is separable, and $\#\ker(1 - \phi) = \deg(1 - \phi)$.*

Proof. Recall from Chapter 4 that a map ψ is separable if and only if $\psi^*(\omega) \neq 0$, where ω is the invariant differential. Using that the Frobenius ϕ is inseparable [Silverman, 1992] we compute

$$\begin{aligned} (1 - \phi)^*(\omega) &= [1]^*\omega - \phi^*(\omega) \\ &= \omega - 0 \\ &= \omega \end{aligned}$$

thus $(1 - \phi)^*(\omega) = 0$ if and only if $\omega = 0$, but the invariant differential is non-zero so $(1 - \phi)^*(\omega) \neq 0$ which means $1 - \phi$ is separable. The last fact follows from Theorem 2. □

With the theory we developed so far we get the Hasse bound as a special case of the next lemma.

Lemma 1. ***(Cauchy-Schwartz inequality)***. *Let A be an abelian group and*

$$d : A \to \mathbb{Z}$$

a positive definite quadratic form. Then for all $\psi, \phi \in A$ the following holds

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}.$$

Proof. Let $\psi, \phi \in A$. From the definition of a quadratic form there is a bilinear pairing

$$L(\psi, \phi) = d(\psi - \phi) - d(\psi) - d(\phi).$$

Using this definition, the fact that d is positive definite and letting $m, n \in \mathbb{Z}$ where $m = -L(\psi, \phi)$ and $n = 2d(\psi)$ we calculate

$$\begin{aligned} 0 \leq d(m\psi - n\phi) &= d(m\psi) + L(m\psi, n\phi) + d(n\phi) \\ &= m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi) \\ &= d(\psi)\left(4d(\psi)d(\phi) - L(\psi, \phi)^2\right) \end{aligned}$$

where on the last line we make the substitution. If $d(\psi) = 0$ the inequality is trivial, if $d(\psi) \neq 0$ we divide it out and obtain our result

$$L(\psi, \phi)^2 \leq 4d(\psi)d(\phi).$$

□

Theorem 5. ***(Hasse's theorem)***. *Let E be an elliptic curve over a finite field k with q elements, then*

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

Proof. We let $\phi_q : E \to E$ be the q^{th} Frobenius endomorphism on E given by $(x, y) \mapsto (x^q, y^q)$. Recall that ϕ_q fixes our field of q elements, thus

$$P \in E(k) \quad \iff \quad \phi_q(P) = P.$$

Writing out the right hand side of the implication we see that

$$0 = P - \phi_q(P) = (1 - \phi_q)(P)$$

which enables us to count the number of points in $E(k)$ by counting the number of points in the kernel of the separable map $1 - \phi_q$. Recall from before that the number of points in the kernel is equal to the degree of the separable map

$$\#E(k) = \#\ker(1 - \phi_q) = \deg(1 - \phi_q).$$

We have shown in that the degree map on $End(E)$ is a positive definite quadratic form, so by using the inequality from the previous theorem we calculate

$$|\deg(1 - \phi_q) - \deg \phi_q - \deg 1| = |\#E(k) - q - 1| \leq 2\sqrt{\deg \phi_q} = 2\sqrt{q}.$$

□

The Hasse bound is used in all our coming algorithms. For Schoof-Elkies it tells us how many small primes we have to calculate the Frobenius trace for. In the case of Satoh it supplies us with the sufficient precision needed to recover the Frobenius trace.

Proposition 15. *If $\psi \in End(E)$ then $\det \psi_\ell = \deg \psi$, where ψ_ℓ is a 2×2 matrix acting on the Tate module $T_\ell(E)$.*

Proof. We fix a basis $v_1, v_2 \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ for $T_\ell(E)$ and denote the matrix associated to this basis by

$$\psi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

We now calculate by relying heavily on the ℓ-adic Weil pairing, $e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$.

$$\begin{aligned} e(v_1, v_2)^{\deg \psi} &= e([\deg \psi]v_1, v_2) \\ &= e(\psi_\ell \widehat{\psi_\ell} v_1, v_2) \\ &= e(\psi_\ell v_1, \psi_\ell v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(av_1, dv_2)e(cv_2, bv_1) \\ &= e(av_1, dv_2)e(bv_1, cv_2)^{-1} \\ &= e(v_1, v_2)^{ad} e(v_1, v_2)^{-bc} \\ &= e(v_1, v_2)^{ad-bc} \\ &= e(v_1, v_2)^{\det \psi_\ell} \end{aligned}$$

Since the pairing is non-degenerate we obtain $\deg \psi = \det \psi_\ell$. □

Writing out the determinant of $1 - A$ for any matrix A we get

$$\begin{vmatrix} 1-a & -b \\ -c & 1-d \end{vmatrix} = 1 - (a+d) + ad - bc = 1 - tr(A) + \det A$$

and we see that $tr(\psi_\ell) = 1 + \det \psi_\ell - \det(1 - \psi_\ell)$. Using the previous theorem we get

$$tr(\psi_\ell) = 1 + \deg \psi_\ell - \deg(1 - \psi_\ell).$$

By substituting with the q^{th} Frobenius endomorphism on $T_\ell(E)$ and setting $\tau = tr(\phi_q)$ we get

$$\#E(k) = 1 + q - \tau$$

where we know from Hasse's theorem that $|\tau| \leq 2\sqrt{q}$.

The next proposition will be used in Chapter 7, it is easy to prove and gives a nice expression of the Frobenius trace in terms of the dual isogeny.

Proposition 16. *Let $\phi : E \to E$ be the q^{th} Frobenius endomorphism and $\widehat{\phi}$ its dual, then the following holds*

$$t = tr(\phi) = \phi + \widehat{\phi}.$$

Proof. Recall that $1 - \phi$ is separable, so

$$(1 - \phi)(\widehat{1 - \phi}) = \deg(1 - \phi) = \#\ker(1 - \phi) = \#E(k).$$

Expanding the product on the left we get

$$\begin{aligned} (1 - \phi)(\widehat{1 - \phi}) &= (1 - \phi)(1 - \widehat{\phi}) \\ &= 1 - (\phi + \widehat{\phi}) + \phi\widehat{\phi} \\ &= 1 - (\phi + \widehat{\phi}) + q \end{aligned}$$

From before we had that $\#E(k) = q + 1 - t$ and we just calculated that $\#E(k) = q + 1 - (\phi + \widehat{\phi})$ so the result follows. □

A very useful property of the q^{th} Frobenius endomorphism ϕ is its characteristic polynomial. Letting $\phi_\ell \in M_2(\mathbb{Z})$ a trivial calculation using $\det \phi_\ell = \deg \phi = q$ Âăgives

$$\begin{aligned} \det(Ix - \phi_\ell) &= x^2 - (a+d)x + ad - bc \\ &= x^2 - tr(\phi_\ell) + \det \phi_\ell \\ &= x^2 - \tau x + q \end{aligned}$$

In other words we have that the Frobenius ϕ satisfies

$$\text{Âă}\phi^2 - \tau\phi + q = 0.$$

5. Modular polynomials

This section will serve as an introduction to modular polynomials. I will be following [Lan, 1987] and [Adv, 1994], and I refer to those for a more thorough examination with proofs.

These polynomials get their name from the theory of modular functions. That is a topic which is well beyond the scope of this article, but they are functions invariant under some fractional linear transform.

Given a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

we can define an action of γ on some $\tau \in \mathbb{C}$ as

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d}.$$

Recall that an elliptic curve over $\mathbb{C}$ is isomorphic to a lattice

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

in $\mathbb{C}$. Letting $\tau = \frac{\omega_1}{\omega_2}$ we consider the j-invariant as a function on the upper half-plane. $j(\tau)$ is the j-invariant of the curve given by such a lattice.

It can be shown that j is a modular function of weight 0 satisfying

$$j(\tau) = j(\tau + 1) \quad \text{and} \quad j(\tau) = j(-\frac{1}{\tau}).$$

These are exactly the transformations given by the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

It can be shown that these matrices generate the modular group $SL_2(\mathbb{Z})$, so we have that

$$j(\tau) = j(\alpha\tau) \quad \alpha \in SL_2(\mathbb{Z}).$$

We are not so much interested in how j stays invariant under the modular group, but rather how it is acted upon by matrices of the bigger group $GL_2(\mathbb{Z})$. We thus define

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

to be the j-invariant of the curve given by the lattice $\mathbb{Z} + \mathbb{Z}\tau'$ with

$$\tau' = \frac{a\tau + b}{c\tau + d}.$$

Letting n be a positive integer we define a subgroup

$$S_n^* = \left\{ \alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid \det(\alpha) = n,\ \gcd(a, b, d) = 1,\ 0 \leq b < d \right\} \subset GL_2(\mathbb{Z}).$$

It can be shown that if $n = \ell$ a prime number we have that $\#S_n^* = \ell + 1$.

Definition 26. *The* modular polynomial of degree ℓ *is given by*

$$\Phi_\ell(x, j) = \Phi_\ell(j, x) = \prod_{\alpha \in S_\ell^*} (x - j\alpha)$$

and is of degree $\ell - 1$.

Notice that the roots of the above polynomials is by definition some j' which is one of transformations of j under the subgroup S_ℓ^*. The next theorem gives us a connection between the roots of the modular polynomial and isogenies between elliptic curves, a proof can be found in [Lan, 1987].

Theorem 6. *Let E_1 and E_2 be two elliptic curves with j-invariants $j(E_1)$ and $j(E_2)$ respectively. Then there exits an isogeny $f : E_1 \to E_2$ with* $\ker(f)$ *cyclic of size ℓ if and only if*

$$\Phi_\ell(j(E_1), j(E_2)) = 0.$$

This theorem holds in any field of characteristic 0 and for a finite field of characteristic p where $\ell \neq p$.

Example 5. *The following are the two modular polynomials $\Phi_2(x, y)$ and $\Phi_3(x, y)$. They were calculated using the mathematics software* Sage.

$$\begin{aligned}\Phi_2(x,y) &= -x^2y^2 + x^3 + 1488x^2y + 1488xy^2 + y^3 - \\ &\quad 162000x^2 + 40773375xy - 162000y^2 + 8748000000x + \\ &\quad 8748000000y - 157464000000000\end{aligned}$$

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

This clearly serves as a demonstration of how large the coefficients are. In fact the largest coefficient of the polynomial $\Phi_{41}(x, y)$ has length about 10^{607}. With coefficients growing this rapidly it is makes these polynomials very inefficient in practice. Other variants of these polynomials do exist, an example is the Atkins modular polynomials. *The same coefficient for the 41^{th} Atkins polynomial is* 64000000 *which is a huge improvement over the classical modular polynomials.*

More information about such improvements can be found in [Han, 2005] *and* [Blake et al., 1999].

We end this section with a theorem of Kronecker which gives us explicitly the modular polynomials modulo p.

Theorem 7. *Let $\Phi_p(x, y)$ be the modular polynomial, then we have that*

$$\hat{A}\check{a}\Phi_p(x,y) \equiv (x^p - y)(x - y^p) \,(mod\, p).$$

6. Schoof's algorithm and improvements

The idea of Schoof's algorithm is to calculate the Frobenius trace modulo small primes, then assemble this information using the Chinese remainder theorem. Choosing the set of small primes such that their product $N > 4\sqrt{q}$ (with q the size of our field) gives us the trace t modulo N, which by the Hasse bound is exactly the Frobenius trace.

Recall for this section that an elliptic curve corresponds to a lattice Λ so we have an isomorphism

$$\bar{k}/\Lambda \simeq E(\bar{k})$$
$$z \mapsto (\wp(z), \wp'(z))$$

where $\wp(z)$ is the elliptic Weierstrass function

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} c_k z^{2k}.$$

Definition 27. *The* division polynomials *are polynomials* $\Psi_n(x, y) \in \mathbb{Z}[x, y, A, B]$ *defined by the recurrence relations*

$$\begin{aligned}
\Psi_0 &= 0 \\
\Psi_1 &= 1 \\
\Psi_2 &= 2y \\
\Psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\Psi_{2n+1} &= \Psi_{n+2}\Psi_n^3 - \Psi_{n+1}^3\Psi_{n-1} \\
\Psi_{2n} &= (2y)^{-1}\Psi_n(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2)
\end{aligned}$$

where $\Psi_n(x, y) = 0$ *is and only if* $(x, y) \in E[n]$.

The construction of these polynomials can be done in at least two ways and I will discuss both of them briefly.

One way of doing this is to construct a function having poles at the n-torsion points of our elliptic curve as follows

$$f_n(z) = n^2 \prod(\wp(z) - \wp(u))$$

where the product is taken over all n-torsion points of $\bar{k}/\Lambda$, denoted $\bar{k}/\Lambda[n]$. This function has roots at exactly the n-torsion points by definition, which is at least what we want. A more thorough examination of this method can be found in [Lang, 1979]. Another way which is more elementary but highly computational is to work explicitly with the addition formulas for elliptic curves.

Replacing the terms y^2 in Ψ_n by $x^3 + Ax + B$ we obtain polynomials Ψ'_n in $\mathbb{F}_q[x]$ if is n is odd or $y\mathbb{F}_q[x]$ if n is even. To avoid this distinction we define

$$f_n(x) = \begin{cases} \Psi'_n(x, y) & \text{if n is odd.} \\ \Psi'_n(x, y)/y & \text{if n is even.} \end{cases}$$

Proposition 17. *Let* $n \geq 2$ *and* Ψ_n *the division polynomial as defined above, then*

$$nP = (x - \frac{\Psi_{n-1}\Psi_{n+1}}{\Psi_n^2}, \frac{\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2}{4y\Psi_n^3}).$$

6.1. **Schoof's algorithm.** For an elliptic curve over $\mathbb{F}_q$ given by

$$E : y^2 = x^3 + Ax + B$$

we want to compute the size of $\#E(\mathbb{F}_q)$, we know from before that

$$\#E(\mathbb{F}_q) = q + 1 - t$$

where t is the trace of the Frobenius as seen in chapter 4. We know that t satisfies the Hasse bound namely

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

Let $S = \{3, 5, 7, 11, \dots L\}$ be the set of odd primes $\leq L$ such that the product is bigger than the Hasse interval

$$N = \prod_{\ell \in S} \ell > 4\sqrt{q}.$$

If we can then calculate $t \,(mod\, \ell)$ for all $\ell \in S$ we can uniquely determine $t \,(mod\, N)$ by invoking the Chinese remainder theorem, which then by the Hasse bound is our Frobenius trace t.

We will now look at how to calculate $t \,(mod\, \ell)$. Let ϕ be the Frobenius endomorphism restricted to $E[\ell]$ and let q_ℓ, τ be q and t reduced modulo ℓ respectively. The computation of τ can then be done by checking if

$$\phi^2(P) + q_\ell P = \tau\phi(P)$$

holds for $P \in E[\ell]$. To perform the addition on the left hand side of the equality we need to distinguish the cases where the points are on a vertical line or not. In other words we have to verify if for $P = (x, y) \in E[\ell]$ the following holds

$$\phi^2(P) = \pm q_\ell P.$$

Noting that $-P = (x, -y)$ we write out the equality for the x-coordinates in terms of division polynomials

$$x^{q^2} = x - \frac{\Psi_{q_\ell - 1}\Psi_{q_\ell + 1}}{\Psi^2_{q_\ell}}(x, y).$$

Writing this out in terms of $f_n(x)$ and noting that for n even we have $\Psi_n(x, y) = y f_n(x)$, a calculation for q_ℓ even yields

$$\begin{aligned} x^{q^2} &= \frac{f_{q_\ell - 1}(x) f_{q_\ell + 1}(x)}{(f_{q_\ell}(x) y)^2} \\ &= \frac{f_{q_\ell - 1}(x) f_{q_\ell + 1}(x)}{f^2_{q_\ell}(x)(x^3 + Ax + B)} \end{aligned}$$

The calculation for q_ℓ odd is similar and we get the equality

$$x^{q^2} = \begin{cases} x - \frac{f_{q_\ell - 1}(x) f_{q_\ell + 1}(x)}{f^2_{q_\ell}(x)(x^3 + Ax + B)} & \text{if } q_\ell \text{ is even} \\ x - \frac{f_{q_\ell - 1}(x) f_{q_\ell + 1}(x)(x^3 + Ax + B)}{f^2_{q_\ell}(x)} & \text{if } q_\ell \text{ is odd} \end{cases}$$

We thus get two equations and we want to verify they have any solutions $P \in E[\ell]$. For doing this we compute the following greatest common divisors

$$\gcd((x^{q^2} - x) f^2_{q_\ell}(x)(x^3 + Ax + B) + f_{q_\ell - 1}(x) f_{q_\ell + 1}(x), f_\ell(x)) \quad (q_\ell \text{ even})$$

$$\gcd((x^{q^2}-x)f_{q_\ell}^2(x)+f_{q_\ell-1}(x)f_{q_\ell+1}(x)(x^3+Ax+B),f_\ell(x)) \quad (q_\ell \text{ odd})$$

We are now going to treat the rest in two cases, depending on the value from the above gcds.

Case 1: gcd $\neq 1$ meaning there exist a non-zero ℓ-torsion point P such that $\phi^2(P)=\pm q_\ell P$. If $\phi^2(P)=-q_\ell P$ we have that $\tau\phi(P)=0$ but since $\phi(P)\neq 0$ we know that $\tau=0$. If $\phi^2(P)=q_\ell P$ we have that

$$2q_\ell P=\tau\phi(P)\Leftrightarrow\phi(P)=\frac{2q_\ell}{\tau}.$$

Substituting the last equality into $\phi^2(P)=q_\ell P$ we obtain

$$\frac{4q_\ell^2}{\tau^2}=q_\ell P\Leftrightarrow 4q_\ell P=\tau^2 P.$$

We thus obtain the congruence $\tau^2\equiv 4q_\ell \pmod{\ell}$

Case 2: gcd $=1$ so $\phi^2(P)\neq\pm q_\ell P$ meaning the two points are not equal nor are they on the same vertical line for any ℓ-torsion point P. This enables us to do the addition $\phi^2(P)+q_\ell P$ using the appropriate addition formulas. Recall that if $P=(x_1,y_1)$ and $Q=(x_2,y_2)$ are two points on E with $P\neq Q$ we have that their sum is given by $P+Q=(x_3,y_3)$ where

$$\lambda=\frac{y_2-y_1}{x_2-x_1}$$

$$x_3=-x_1-x_2+\lambda^2$$

$$y_3=-y_1-\lambda(x_3-x_1).$$

We can now write out the addition explicitly in terms of polynomials as follows

$$\lambda=\frac{\Psi_{q_\ell+2}\Psi_{q_\ell-1}^2-\Psi_{q_\ell-2}\Psi_{q_\ell+1}^2-4y^{q^2+1}\Psi_{q_\ell}^3}{4\Psi_{q_\ell}y((x-x^{q^2})\Psi_{q_\ell}^2-\Psi_{q_\ell-1}\Psi_{q_\ell+1}}$$

with the left hand side given by

$$\phi^2(P)+q_\ell P=\left(-x^{q^2}-x+\frac{\Psi_{q_\ell-1}\Psi_{q_\ell+1}}{\Psi_{q_\ell}^2}+\lambda^2,-y^{q^2}-\lambda\left(-2x^{q^2}-x+\frac{\Psi_{q_\ell-1}\Psi_{q_\ell+1}}{\Psi_{q_\ell}^2}\right)\right).$$

The right hand side is as before given by

$$\tau\phi(P)=\left(x^q-\left(\frac{\Psi_{\tau+1}\Psi_{\tau-1}}{\Psi_\tau^2}\right)^q,\left(\frac{\Psi_{\tau+2}\Psi_{\tau-1}^2-\Psi_{\tau-2}\Psi_{\tau+1}^2}{4y\Psi_\tau^3}\right)^q\right)$$

So figuring out if

$$\phi^2(P)+q_\ell P=\tau\phi(P)$$

amounts to checking if the difference of the two expressions are zero modulo the division polynomials for some $0\leq\tau<\ell$. More explicit formulas can be found in [Schoof, 1985].

6.2. **Schoof-Elkies algorithm.** When doing the calculations in Schoof's algorithm we were working modulo the division polynomials $\Psi(x, y)$ of degree $\ell^2 - 1$. Instead we can exploit some special primes called *Elkies primes* that enables us to work in a cyclic subgroup C of $E[\ell]$. Here C will correspond to a 1-dimensional eigenspace.

The Frobenius endomorphism restricted to $E[\ell]$ satisfies the characteristic equation

$$\phi^2 - \tau\phi + q_\ell = 0$$

where τ and q_ℓ is as before. The roots of this equations are the eigenvalues of ϕ restricted to $E[\ell]$ and they are given by

$$\lambda_{1,2} = \frac{\tau \pm \sqrt{\tau^2 - 4q_\ell}}{2}.$$

If the discriminant $\tau^2 - 4q_\ell$ is a square modulo ℓ we have that $\lambda_{1,2} \in \mathbb{F}_q$.

Definition 28. *A prime ℓ such that $\tau^2 - 4q_\ell$ is a square modulo ℓ is called an* Elkies prime*.*

For primes of this type we obtain a factorization

$$(\phi - \lambda_1)(\phi - \lambda_2) = 0$$

so for an eigenvalue λ we have that $\phi(P) = \lambda P$ for a point P. Thus P is the generator for a cyclic eigenspace $C \subset E[\ell]$ of order ℓ corresponding to λ. Notice that we have an exact sequence of groups

$$0 \to C \to E \to E/C \to 0$$

where the map $E \to E/C$ has cyclic kernel C of order ℓ. Determining which primes are Elkies primes can be done by working with the modular polynomials. From Theorem 6 we have that $\Phi_\ell(j(E), j(E/C)) = 0$, so letting the isogeny $f : E \to E'$ have cyclic kernel C we get an exact sequence

$$0 \to C \to E \to E' \to 0$$

which by a diagram chase yields $E' \simeq E/C$. This argument gives us the following result

Proposition 18. *$\Phi_\ell(j(E), x) = 0$ for $x \in \mathbb{F}_q$ if and only if ℓ is an Elkies prime.*

Figuring out if ℓ is an Elkies prime can thus be done fast by calculating

$$\gcd(\Phi_\ell(j(E), x), x^q - x).$$

Now since we are working only with primes of this type we restrict ourself to working in the subspace C of order ℓ. There is thus a factor $G_\ell(x)$ of the division polynomial which has the x-coordinates of points in C as roots. Since similar points in C of different sign are on the same vertical line we only include unique points up to sign. In this way we get that the degree of $G_\ell(x)$ is $\frac{\ell-1}{2}$.

From the theory of eigenvalues we know that if λ_1, λ_2 are eigenvalues of ϕ then

$$tr(\phi) = \lambda_1 + \lambda_2$$

We also know using Proposition 15 that

$$\lambda_1\lambda_2 = \det\phi = q$$

Using this we can recover the trace of ϕ by calculating one of the eigenvalues

$$\tau \equiv \lambda + \frac{q}{\lambda} \quad (mod\, \ell).$$

To compute the eigenvalue λ we can thus check which of the relations

$$\phi(P) = (x^q, y^q) = \lambda P$$

holds on the eigenspace C, this mean we can work modulo $G_\ell(x)$. This enables us to work in the much smaller ring

$$\mathbb{F}_q[x,y]/(G(x), y^2 - x^3 - Ax - B)$$

and thus greatly improves Schoof's original approach.

The obstacle that remains is how we can possible calculate the factor

$$G_\ell(x) = \prod_{(x',y')\in C} (x - x')$$

of the division polynomial where the product is taken over all unique points $P = (x', y')$ up to sign. When calculating the gcd $\gcd(\Phi_\ell(j(E), x), x^q - x)$ we obtain a polynomial whose roots (at most two) are the j-invariants of the ℓ-isogenous curves $\tilde{E} = E/C$ where C is the eigenspace corresponding to λ. The next theorem enables us to calculate an explicit formula for the Weierstrass equation of $\tilde{E}$.

Theorem 8. *Let E be given by the equation*

$$E : y^2 = x^3 + Ax + B$$

with $j = j(E)$. Then the equation for the ℓ-isogenous curve $\tilde{E}$ with $\tilde{j} = j(\tilde{E})$ is given by

$$\tilde{E} : y^2 = x^3 + \bar{A}x + \bar{B}$$

$$\bar{A} = -\frac{\tilde{j}'^2}{48\tilde{j}(\tilde{j} - 1728)} \quad \bar{B} = -\frac{\tilde{j}'^3}{864\tilde{j}^2(\tilde{j} - 1728)}.$$

And letting

$$\Phi_{\ell,x} = \frac{\partial\Phi_\ell}{\partial x} \quad \Phi_{\ell,y} = \frac{\partial\Phi_\ell}{\partial y}$$

be the partial derivatives with respect to x and y respectively we have that

$$\bar{j}' = -\frac{18B\Phi_{\ell,x}(j,\bar{j})}{\ell A\Phi_{\ell,y}(j,\bar{j})}j.$$

The next theorem will enable us to compute the sum of the x-coordinates of the points in our subspace C. This value will be used to calculate every coefficient of $G_\ell(x)$, notice that if we formally multiply out the product of $G_\ell(x)$ we get

$$G_\ell(x) = x^{\frac{\ell-1}{2}} - \frac{p_1}{2}x^{\frac{\ell-3}{2}} + \dots.$$

Here p_1 is the sum of the x-coordinates of C, the division by two is because they appear twice as a result of the symmetry around the x-axis.

Theorem 9. *Given our two curves* $E : y^2 = x^3 + Ax + B$ *and* $\tilde{E} : y^2 = x^3 + \bar{A}x + \bar{B}$ *we let* $E_4 = -48A$, $E_6 = 864B$ *and similarly for our* ℓ*-isogenous curve* $\bar{E}_4 = -48\bar{A}$, $\bar{E}_6 = 864\bar{B}$. *Then we obtain an explicit formula for*

$$p_1 = \sum_{(x,y)\in C} x$$

$$p_1 = \frac{\ell}{2}J + \frac{\ell}{4}\left(\frac{E_4^2}{E_6} - \ell\frac{\bar{E}_4^2}{\bar{E}_6}\right)$$

where by using the usual partial derivative notation $\Psi_{\ell,xx} = \frac{\partial^2\Psi_\ell}{\partial x^2}$ *etc. we write* J *as*

$$J = -\frac{j'^2\Psi_{\ell,xx}(j,\tilde{j}) + 2\ell j'\tilde{j}'\Psi_{\ell,xy}(j,\tilde{j}) + \ell^2\tilde{j}'^2\Psi_{\ell,yy}(j,j')}{j'\Psi_{\ell,x}(j,j')}.$$

Here $j' = -j\frac{E_6}{E_4}$ *and similarly* $\tilde{j}' = -\tilde{j}\frac{\bar{E}_6}{\bar{E}_4}$.

Given the value of p_1 we can calculate the rest of the coefficients using a theorem from [Schoof, 1995].

Theorem 10. *Let* $\ell \neq char(k)$ *be a prime, and* $\phi : E \to \widetilde{E}$ *be an isogeny with* $\ker(\phi)$ *cyclic of size* ℓ*, then the polynomial* $G_\ell(x)$ *which vanishes on the* x*-coordinates of elements of* $\ker(\phi)$ *satisfies*

$$z^{\ell-1}G_\ell(\wp(z)) = exp(-\frac{1}{2}p_1z^2 - \sum_{k=1}^{\infty}\frac{\widetilde{c}_k - \ell c_k}{(2k+1)(2k+2)}z^{2k+2}).$$

Proof. The proof of Schoof uses analytic theory heavily, he introduces the Weierstrass ζ-function which is defined by

$$\zeta(z) = \frac{1}{z} - \sum_{k=1}^{\infty}\frac{c_k}{2k+1}z^{2k+1}.$$

Differentiating we see that $\zeta'(z) = -\wp(z)$. Let $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ be the lattice corresponding to E and then we have that $\widetilde{\Lambda} = \frac{\omega_1}{\ell}\mathbb{Z} + \omega_2\mathbb{Z}$ is the lattice corresponding to $\widetilde{E}$. Setting ζ and $\widetilde{\zeta}$ to be the Weierstrass ζ-functions for E and $\widetilde{E}$ respectively, Schoof eventually arrives at the equality

$$-\ell\zeta(z) + \widetilde{\zeta}(z) - p_1z = \sum_{i=1}^{(\ell-1)/2}\frac{\wp'(z)}{\wp(z) - \wp(\frac{i}{\ell}\omega_1)}.$$

Notice that $\frac{d}{dz}\wp(z) - \wp(\frac{i}{\ell}\omega_1) = \wp'(z)$ so we can invert the process of logarithmic differentiation

$$\frac{df}{dz} = \frac{f'}{f}$$

on both sides of the equality, setting

$$f(z) = \prod_{i=1}^{(\ell-1)/2}(\wp(z) - \wp(\frac{i}{\ell}\omega_1).$$

A thorough proof can be found in [Schoof, 1995]. □

The coefficients of $G_\ell(x)$ can thus be obtained by expanding both sides of the equality from the previous theorem and comparing the coefficients of like powers of z. Setting $w = z^2$ and letting $A(w)$ be the function on the right-hand side of the equality expanded as a power series in w. Also let $C(w) = \wp(z) - \frac{1}{w} = \sum_{k=1}^{\infty} c_k w^k$, the Weierstrass $\wp$-function with the first term removed. For notational convenience we write $[B(w)]_j$ for the coefficient of w^j in the power series $B(w)$. Letting g_i be the coefficient of x^i in $G_\ell(x) = x^d + \sum_{i=0}^{d-1} g_i x^i$ with $d = \frac{\ell-1}{2}$ we get the recursion

$$g_{d-i} = [A(w)]_i - \sum_{k=1}^{i} \left(\sum_{j=0}^{k} \binom{d-i+k}{k-j} [C(w)^{k-j}]_j \right) g_{d-i+k}$$

as seen in [Blake et al., 1999].

We end this section by given a short summary of the Schoof-Elkies algorithm: choose S to be the set of small odd primes such that the product is bigger than the Hasse interval. For each such prime $\ell \in S$ we check if the following holds

$$\phi^2(P) + q_\ell P = \tau\phi(P) \tag{1}$$

for all $P \in E[\ell]$. Here the addition is done using the appropriate addition law on E, treated in special cases depending on whether the two points are on the same vertical line or not. The points $q_\ell P$ and $\tau\phi(P)$ can be calculated by using properties of the division polynomials. We then proceed by checking if (1) holds for $P \in E[\ell]$ and $0 \leq \tau < \ell$, all calculations done modulo the division polynomials $\Psi_\ell(x)$ and the curve equation for E. This gives an algorithm of complexity $O(\log^8 q)$ [Schoof, 1995].

The improvement due to Elkies is the restriction of the setÂăof small primes S. Choosing only the small primes ℓ such that $\tau^2 - 4q_\ell$ is a square modulo ℓ (Elkies primes), we obtain a factorization of the characteristic equation of the Frobenius. This thus gives you a cyclic eigenspace $C \subset E[\ell]$ of dimension 1 corresponding to an eigenvalue λ. Computing one of the eigenvalues λ will give us the trace modulo ℓ. We thus have to check if

$$\hat{\mathrm{A}}\check{\mathrm{a}}\phi(P) = \lambda P$$

holds on C. This enables us to use a factor of the division polynomial $G_\ell(x)$ of degree $\frac{\ell-1}{2}$. The improvement is thus to do the calculations of x^q, y^q etc. modulo $G_\ell(x)$ of much smaller degree, instead of working with the full division polynomial $\Psi_\ell(x)$. Schoof-Elkies can thus be shown [Schoof, 1995] to have complexity $O(\log^5 q)$.

7. Satoh's algorithm

This algorithm is divided into two parts. First we do what is called a *lifting* to desired precision, then we recover the trace of the Frobenius from the lifted data.

7.1. **Lifting the j-invariants.** We begin by establishing some notation, so let $\mathbb{F}_q$ be our finite field with $q = p^n$ as before, $\mathbb{Z}_p$ the p-adic integers and $\mathbb{Q}_q$ the q-adic rationals as defined in Section 2. For this section we let σ be the p^{th} Frobenius, and ϕ_q be the q^{th} Frobenius. As for previous sections we denote the curves over our finite fields as $E/\mathbb{F}_q$, for the lifted curves we write $\mathscr{E}/\mathbb{Q}_q$.

Definition 29. *The* canonical lift $\mathscr{E}$ *of an elliptic curve E over $\mathbb{F}_q$ is an elliptic curve over $\mathbb{Q}_q$ such that $End(\mathscr{E}) \simeq End(E)$.*

The existence of such a canonical lift is vital because of the isomorphic endomorphism rings. This enables us to lift the endomorphisms, especially the Frobenius which we are interested in.

Theorem 11. ***(Lubin-Serre-Tate)*** *Let $E/\mathbb{F}_q$ be an elliptic curve with j-invariant $j(E)$ and σ the p^{th} Frobenius on $\mathbb{Q}_q$ then the system of equations*

$$\Phi_p(x, \sigma(x)) = 0 \quad x \equiv j(E)\,(mod\, p)$$

where Φ_p is the p-th modular polynomial has a unique solution $J \in \mathbb{Z}_q$ which is the j-invariant of the canonical lift $\mathscr{E}$ of E.

The latter theorem gives an efficient way of calculating the j-invariants, in addition it has been shown [Deuring, 1941] that the canonical lift always exists and is unique (up to isomorphism).

Knowing $j(\mathscr{E})$ we can explicitly write out the Weierstrass equation for $\mathscr{E}$, but instead of lifting E to $\mathscr{E}$ directly we can consider all its conjugates

$$E, E^{\sigma}, E^{\sigma^2}, \ldots, E^{\sigma^{n-2}}, E^{\sigma^{n-1}}.$$

Letting $E^{\sigma^i} = E^i$ we get a sequence of maps

$$E \xrightarrow{\sigma} E^1 \xrightarrow{\sigma} E^2 \xrightarrow{\sigma} \ldots \xrightarrow{\sigma} E^{n-1}.$$

Where the composition is the q^{th} Frobenius $\phi_q = \sigma\sigma\ldots\sigma : E \to E$. Recall that the $\deg \sigma = p$.

Since the endomorphism rings are isomorphic we can lift every Frobenius on E to a Frobenius on $\mathscr{E}$. We thus obtain a commutative diagram

$$\begin{array}{ccccccccc}
\mathscr{E} & \xrightarrow{\sigma} & \mathscr{E}^1 & \xrightarrow{\sigma} & \cdots & \xrightarrow{\sigma} & \mathscr{E}^{n-1} & \xrightarrow{\sigma} & \mathscr{E} \\
\downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} & & & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\
E & \xrightarrow{\sigma} & E^1 & \xrightarrow{\sigma} & \cdots & \xrightarrow{\sigma} & E^{n-1} & \xrightarrow{\sigma} & E
\end{array}$$

Since the lifted Frobenius also has degree p we have that

$$\Phi_p(j(\mathscr{E}^{i+1}), j(\mathscr{E}^i)) = 0 \quad j(\mathscr{E}^i) \equiv j(E^i)\,(mod\, p).$$

We thus define a function $\Theta : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ by

$$\Theta(x_0, x_1, \ldots, x_{n-1}) = (\Phi_p(x_0, x_1), \Phi_p(x_1, x_2), \ldots, \Phi_p(x_{n-1}, x_0)).$$

Note that the roots of Θ are the j-invariants of our lifted curves

$$\Theta(j(\mathscr{E}^{n-1}), j(\mathscr{E}^{n-2}), \ldots, j(\mathscr{E}^{0})) = (0, 0, \ldots, 0)$$

so by solving $\Theta(\bar{x}) = 0$ using a multivariate Newton-Raphson iteration, we can recover the j-invariants to desired precision. Setting up the Jacobian matrix J_Θ of Θ, the iteration is given by

$$\bar{x}_{n+1} = \bar{x}_n - J_\Theta^{-1}\Theta(\bar{x}_n)$$

where the matrix $J_\Theta(x_0, x_1, \ldots, x_{n-1})$ is given as

$$\begin{pmatrix} \frac{\partial}{\partial x_0}\Phi_p(x_0,x_1) & \frac{\partial}{\partial x_1}\Phi_p(x_0,x_1) & 0 & \ldots & 0 & 0 \\ 0 & \frac{\partial}{\partial x_1}\Phi_p(x_1,x_2) & \frac{\partial}{\partial x_2}\Phi_p(x_1,x_2) & 0 & \ldots & 0 \\ 0 & & & & & \\ \vdots & & \ddots & & & \vdots \\ 0 & & & & & \\ \frac{\partial}{\partial x_0}\Phi_p(x_{n-1},x_0) & 0 & \ldots & 0 & 0 & \frac{\partial}{\partial x_{n-1}}\Phi_p(x_{n-1},x_0) \end{pmatrix}$$

The elements on the diagonal of this matrix are given by

$$\text{Âă}\frac{\partial}{\partial x_i}\Phi_p(x_i, x_{i+1}) \quad i = 0, 1, \ldots, n-1$$

recalling the congruence relation from Theorem 7 we calculate

$$\begin{aligned} \frac{\partial}{\partial x_i}\Phi_p(x_i, x_{i+1}) &= \frac{\partial}{\partial x_i}(x_i^p - x_{i+1})(x_i - x_{i+1}^p) \\ &= px_i^{p-1}(x_i - x_{i+1}^p) + (x_i^p - x_{i+1}) \\ &\equiv x_i^p - x_{i+1}\,(mod\,p) \end{aligned}$$

A similar calculation for the elements on the semi-diagonal shows that

$$\text{Âă}\frac{\partial}{\partial x_{i+1}}\Phi_p(x_i, x_{i+1}) \equiv x_{i+1}^p - x_i\,(mod\,p).$$

The Jacobian matrix modulo p thus has non-zero diagonal elements

$$\begin{aligned} \frac{\partial}{\partial x_i}\Phi_p(j(\mathscr{E}^{i+1}), j(\mathscr{E}^{i})) &\equiv j(\mathscr{E}^{i+1})^p - j(\mathscr{E}^{i}) \\ &\equiv j(\mathscr{E}^{i})^{p^2} - j(\mathscr{E}^{i}) \\ &\not\equiv 0 \quad (mod\,p) \end{aligned}$$

while the elements on the semi-diagonal are all zero

$$\begin{aligned} \frac{\partial}{\partial x_{i+1}}\Phi_p(j(\mathscr{E}^{i+1}), j(\mathscr{E}^{i})) &\equiv j(\mathscr{E}^{i})^p - j(\mathscr{E}^{i+1}) \\ &\equiv j(\mathscr{E}^{i})^p - j(\mathscr{E}^{i})^p \\ &\equiv 0 \quad (mod\,p) \end{aligned}$$

By similar means we can show that the bottom left element is also 0 modulo p, so in fact the Jacobian matrix J_Θ is a diagonal matrix modulo p. It is therefore certainly invertible and the Newton-Raphson iteration can be performed.

Because of the Hasse bound we only need to calculate the lifting to a desired precision. Letting τ be the Frobenius trace

$$\mid \tau \mid \leq 2\sqrt{q} = 2p^{\frac{n}{2}} \leq p^{\frac{n}{2}+1}$$

we have that the j-invariant must be lifted with precision $\frac{n}{2}+1$ in order to accurately recover the Frobenius trace.

7.2. **Recovering the trace.** Let ϕ be the q^{th} Frobenius and ϕ^* be the induced Frobenius on differentials, we have that $c = tr(\phi) = \phi + \widehat{\phi}$ so investigating the action of the Frobenius on the invariant differential ω we see that

$$\begin{aligned} [tr(\phi)]^*(\omega) &= [tr(\phi)](\omega) \\ &= (\phi + \widehat{\phi})^*(\omega) \\ &= \phi^*(\omega) + \widehat{\phi}^*(\omega) \\ &= \widehat{\phi}^*(\omega) \end{aligned}$$

Where the last equality is using the fact that $\phi^* = 0$ since ϕ is inseparable, we thus get that $\widehat{\phi}^*(\omega) = c\omega$. Recall from Chapter 1 that $\frac{dx}{y}$ is also holomorphic and invariant under translation, so for the rest of this section we define our invariant differential as such

$$\omega = \frac{dx}{y}.$$

Instead of working with ϕ we work with its dual $\widehat{\phi}$ and the dual of the p^{th} Frobenius $\widehat{\sigma}$. This is because we will later be lifting the kernel of σ which is trivial. But the dual of the Frobenius is separable and its kernel can be lifted. In addition the trace of $\widehat{\sigma}$ is equal to the trace of σ. Our diagrams will be turned around so we get commutative squares

$$\begin{array}{ccc} \mathscr{E}^{i+1} & \xrightarrow{\widehat{\sigma}_{i+1}} & \mathscr{E}^{i} \\ \downarrow \pi & & \downarrow \pi \\ E^{i+1} & \xrightarrow{\widehat{\sigma}_{i+1}} & E^{i} \end{array}$$

Letting $\widehat{\mathscr{F}_q}$ be the lifted of the dual q^{th} Frobenius we have that $\widehat{\mathscr{F}_q} = \widehat{\sigma}\widehat{\sigma}\ldots\widehat{\sigma}$. So if $\omega_i = \omega^{\sigma^i}$ we have that $\widehat{\sigma}_i^*(\omega_i) = c_i\omega_{i+1}$. A calculation then yields, using that $\sigma_i^* = c_i$

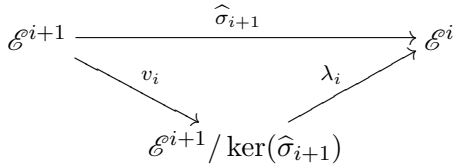
$$\begin{aligned} \widehat{\mathscr{F}_q}(\omega) &= (\widehat{\sigma}_1 \circ \widehat{\sigma}_2 \circ \ldots \circ \widehat{\sigma}_{n-1})(\omega) \\ &= ([c_1] \circ \ldots \circ [c_{n-1}](\omega) \\ &= [c_1 \ldots c_{n-1}](\omega) \end{aligned}$$

Since $\widehat{\mathscr{F}_q}(\omega) = c\omega$ we have that

$$c = \prod_{i=1}^{n-1} c_i \pmod q.$$

It then remains for us to calculate each c_i for every lifted p^{th} Frobenius endomorphism $\widehat{\sigma}_i$.

From [Silverman, 1992] we have that there exists a commutative triangle



From formulas due to Vélu (see [Vélu, 1971] or [Sato, 2003]) we can calculate the map v_i and the Weierstrass equation for the curve $\mathscr{E}^{i+1}/\ker(\widehat{\sigma}_{i+1})$. This means that in order to investigate the action of $\widehat{\sigma}_{i+1}$ on the invariant differential for all i amount to investigating how the composition $\lambda_i v_i$ acts. In addition, if we let v_i^* be the map induced on differentials then by the formulas of Vélu it has trivial action on the invariant differential ω. It is then enough to calculate how the isomorphism λ_i acts on the invariant differential. Given the Weierstrass equations for our curves

$$\mathscr{E}^{i+1}/\ker(\widehat{\sigma}_{i+1}) : y^2 = x^3 + \alpha_{i+1}x + \beta_{i+1}$$
$$\mathscr{E}^{i} : y^2 = x^3 + a_i x + b_i$$
$$\lambda_i : \mathscr{E}^{i+1}/\ker(\widehat{\sigma}_{i+1}) \to \mathscr{E}_i.$$

Here the coefficients α_{i+1} and β_{i+1} are given by

$$\alpha_{i+1} = (6-5p)a_{i+1} - 30(h_{i,1}^2 - 2h_{i,2})$$
$$\beta_{i+1} = (15-14p)b_{i+1} - 70(3h_{i,1}h_{i,2} - h_{i,1}^3 - 3h_{i,3}) + 42a_{i+1}h_{i,1}$$

where $h_{i,k}$ is the coefficient of x^{d-k} in the polynomial $H_i(x)$ from 7.3.

The function which preserves the coefficients of the curves is given by

$$(x, y) \mapsto (u_i^2 x, u_i^3 y).$$

Calculating how this acts on the curve we get the curve

$$y^2 = x^3 + u_i^{-4}a_i x + u_i^{-6}b_i$$

comparing coefficients we get the two equalities

$$u_i^{-4}a_i = \alpha_{i+1} \text{ and } u_i^{-6}b_i = \beta_{i+1}.$$

Solving for u_i^2 we get

$$u_i^2 = \frac{\alpha_{i+1}b_i}{\beta_{i+1}a_i}$$

and we have our isomorphism. Now for calculating how λ_i acts on the holomorphic differential $\omega = \frac{dx}{y}$ we recall from Chapter 1 and calculate

$$\begin{aligned}
\lambda_i^*(\frac{1}{y}dx) &= \lambda_i^*(\frac{1}{y})d(\lambda_i^*(x)) \\
&= \frac{1}{u_i^3 y}d(u_i^2 x) \\
&= \frac{u_i^2 dx}{u_i^3 y} \\
&= u_i^{-1}\omega
\end{aligned}$$

From our commutative triangle we thus have that

$$\widehat{\sigma}_i{}^*(\omega_i) = c_i = (\lambda_i v_i)^*(\omega_i) = \lambda_i^*(\omega_i) = u_i^{-1}\omega_{i+1}$$

so we have found c_i for all i, its square is given by

$$c_i^2 = \frac{\beta_{i+1}a_i}{\alpha_{i+1}b_i}.$$

By our product formula for c we have the square of c given as

$$c^2 = \prod_{i=1}^{n-1} c_i = \prod_{i=1}^{n-1} \frac{\beta_{i+1}a_i}{\alpha_{i+1}b_i}.$$

Taking the square root we obtain the trace c up to sign.

7.3. **Factor of the division polynomial.** Recall that in order to calculate the curve equation for $\mathscr{E}_{i+1}/\ker(\widehat{\sigma}_{n+1})$ we needed coefficients of the factor

$$H_i(x) = \prod_{(x',y')\in\ker(\widehat{\sigma}_{i+1})} (x - x')$$

of the p^{th} division polynomial Ψ_{i+1}. Here the product is taken over all points in the kernel excluding the identity O and up to sign. Since $\#\ker(\widehat{\sigma}_{i+1}) = p$ we have that $\deg(H_i(x)) = \frac{p-1}{2}$.

The following result is due to Satoh and serves as a modified Hensel lifting [Rob, 2000], it can be found in [Satoh, 2002] and [Han, 2005].

Proposition 19. *Let $p \geq 3$ be a prime and $\Psi(x) \in \mathbb{Z}_p[x]$ such that $\Psi'(x) \equiv 0\,(mod\,p)$ and $\Psi'(x) \not\equiv 0\,(mod\,p^2)$. Let $h(x) \in \mathbb{Z}_p[x]$ be a monic polynomial such that*

(1) *$h(x)\,(mod\,p)$ is square-free and relative prime to $\frac{\Psi'(x)}{p}\,(mod\,p)$.*
(2) *$\Psi(x) \equiv f(x)h(x)\,(mod\,p^{n+1})$*

Then the polynomial

$$H(x) = h(x) + \left(\left(\frac{\Psi(x)}{\Psi'(x)}h'(x)\right)\,(mod\,h(x))\right)$$

satisfies $H(x) \equiv h(x)(mod\,p^n)$ and $\Psi(x) \equiv F(x)H(x)(mod\,p^{2n+1})$ for some $F(x)$.

This gives us the following algorithm, as seen in [Han, 2005]. So let the function $liftkernel(\Psi_p, N)$ be given as

Require: p-division polynomial $\Psi_p(x)$ of $\mathscr{E}$ and precision N
  if $N = 1$ **then**
    $H(x) \leftarrow h(x)$ such that $\Psi_p(x) \equiv \delta h(x)^p (mod\,p)$
  else
    $N' \leftarrow \lceil \frac{N-1}{2} \rceil$
    $H(x) \leftarrow liftkernel(\Psi_p(x), N')$
    $H(x) \leftarrow H(x) + \left(\frac{H'(x)\Psi_p(x)}{\Psi_p'(x)}\,mod\,H(x)\right)\,mod\,p^N$
  end if
  return $H(x)$

This ends the algorithm of Satoh and we give a short summary: starting out with an elliptic curve E of the form

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

we calculate the j-invariants of all its conjugates E^i. We then calculate the j-invariants of all the canonical lift $\mathscr{E}^i$, this is the q-adic integer obtained from

the Newton-Raphson iteration. By properties of the invariant differential ω it is sufficient to calculate how the isomorphism λ_i acts on ω

$$\lambda_i^*(\omega) = c\omega.$$

Then c is given by a product of the curve coefficients of $\mathscr{E}^{i+1}/\ker(\widehat{\sigma}_{i+1})$ and $\mathscr{E}^i$. The time complexity of this algorithm is $O(n^5)$ where n is such that $q = p^n$.

References

[Rot, 1979] (1979). *An Introduction to Homological Algebra*. Academic Press.

[Lan, 1987] (1987). *Elliptic Functions*. Springer-Verlag.

[Adv, 1994] (1994). *Advanced Topics in the Arithemtic of Elliptic Curves*. Springer-Verlag.

[Rob, 2000] (2000). *A Course in p-adic Analysis*. Springer.

[Han, 2005] (2005). *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC.

[Blake et al., 1999] Blake, I. F., Seroussi, G., and Smart, N. P. (1999). *Elliptic Curves in Cryptography*. Cambridge University Press.

[Deuring, 1941] Deuring, M. (1941). Die typen der multiplikatorenringe elliptischer funktionenkÃűrper. *Abh. Math. Sem. der Univ. Hamburg.*, 14(1).

[Fulton, 1969] Fulton, W. (1969). *Algebraic Curves*. W.A. Benjamin, Inc.

[Lang, 1979] Lang, S. (1979). *Elliptic Curves: Diophantine Analysis*. Springer.

[Matsumura, 1986] Matsumura, H. (1986). *Commutative ring theory*. Cambridge University Press.

[Sato, 2003] Sato, A. (2003). On the reduction of certain isogenies of elliptic curves via the formulas by vélu.

[Satoh, 2002] Satoh, T. (2002). On p-adic point counting algorithms for elliptic curves over finite fields. In *Lecture Notes in Computer Science*, volume 2369/2002. Springer.

[Schoof, 1985] Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computations*, 44.

[Schoof, 1995] Schoof, R. (1995). Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7.

[Silverman, 1992] Silverman, J. H. (1992). *The Arithmetic of Elliptic Curves*. Springer.

[Vélu, 1971] Vélu, J. (1971). Isogénies entre courbes elliptiques. *C. R. Acad. Sc. Paris*, 26.

[Washington, 2008] Washington, L. C. (2008). *Elliptic Curves: Number Theory and Cryptography*. Chapman and Hall/CRC.