COUNTING POINTS ON ELLIPTIC CURVES

OLE ANDRE BIRKEDAL

Abstract. hei hei

Contents

1. Algebraic geometry

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.

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 $\lambda \in k$ such that $x_i = \lambda y_i$. The equivalence class $\{(x_0, \ldots, x_n)\}$ is denoted $[x_0, \ldots, x_n]$. Here $\mathbb{A}^n = \{(x_1, \ldots, x_n) : x_i \in \bar{k}\}$ is the affine n-space.

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

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

Similarly we define the set of k-rational points in $\mathbb{P}^n$ to be

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

Definition 2. *A polynomial $f \in \bar{k}[X]$ 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 $I(V) \in \bar{k}[X]$ generated by

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

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

Definition 5. *Let V/k be a projective variety (i.e. V defined over k), 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

$$M_p = \{f \in \bar{k}[V] : f(P) = 0\}$$

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*

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

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

Example 1. *If V is a variety given by a single non-constant polynomial equation*

$$f(x_1, \ldots, x_n) = 0$$

then the dimension of the variety $dim(V)$ is $n-1$. The (projective) varieties we will study are called elliptic curvevs *and are given by polynomial equations*

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

They correspond to polynomials of the form $f(x,y) = x^3+ax+b-y^2$ so $dim(E) = 1$. We say curves are projective varieties of dimension 1*.*

The objects we will be working on are projective varieties, but they are not very interesting unless we define maps between them.

Definition 7. *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 8. *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. $\bar{k}$).*

1.1. **Curves and divisors.** 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.

Definition 9. *Let C be a curve and $P \in C$ a non-singular point on the curve. A valuation on $\bar{k}[C]_P$ is given by*

$$ord_P : \bar{k}[C]_P \to \{0, 1, 2, \ldots\} \cup \{\infty\}$$

$$ord_P(f) = max\{d \in \mathbb{Z} : f \in M_P^d\}$$

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 $ord_P(f) < 0$ f has a pole at P and we write $f(P) = \infty$. If $ord_P(f) \geq 0$ f has a zero and is defined at P, so $f(P)$ can be calculated.

Proposition 1. *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.*

Proof. FIXME. Prop 1.2 AEC. □

Definition 10. *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 almost all 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

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

$$sum(D) = sum(\sum_{P\in C} n_P(P)) = \sum_{P\in C} n_P P \in E(\bar{k})$$

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. 1) 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 valution 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 11. *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 $deg(div(f)) = 0$. [EGET TEOREM?]*

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 addition we can put a partial ordering on $Div(C)$, saying 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 write $D_1 \geq D_2$ to indicate that $D_1 - D_2$ is positive.

Example 2. *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 satisy some inequality. This turns out to make up a finite dimensional $\bar{k}$-vector space.

Definition 12. *Let $D \in Div(C)$ be a divisor, and we define the set of functions*

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

Proposition 2. *$\mathscr{L}(D)$ is a finite dimensional $\bar{k}$-vector space, and we denote its dimension by*

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

Proof. First note that if $D' > D$ then $D' = D + P_1 \dots P_s$, so we get an ascending chain of subspaces

$$\mathscr{L}(D) \subseteq \mathscr{L}(D + P_1) \subseteq \dots \subseteq \mathscr{L}(D + P_1 \dots P_s)$$

□

Definition 13. *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 releations 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

$$\omega = \sum f_i dx_i$$

Divisors in the image of the map $div : \Omega_C \to Pic(C)$ 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. It will also serve as a definition of the genus g.

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.*

Proof. A proof would be outside the scope of this paper + referanser. □

Theorem 2.

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

is a group isomorphism

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 [referanse] 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 [3.3 korrolar til riemann-roch] $P = P'$.

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 [3.3-korrolaret].

We have thus established the group isomorphism which we again will call σ

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

□

2. Weil pairing and Tate module

Proposition 3. *The* multiplication by n *map*

$$[n] : E \to E$$
$$P \mapsto nP$$

has order n^2.

Proof. Dual isogeny. □

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 14. *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 indentity 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 [et teorem] 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. Therefor 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 15. *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 4. *We have the following isomorphism of abelian groups*

$$E[n] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Proof. fund. teorem. osv. □

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

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

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 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 the groups $E[\ell^n]$ has a $\mathbb{Z}/\ell^n\mathbb{Z}$-module structure, $T_\ell(E)$ will have natrual structure as a module over the ring og ℓ-adic integers $\mathbb{Z}_\ell$.

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.*

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

3. Frobnius 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 16. *The* frobenius *endomorphism is the q^{th}-power map*

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

which induces a map on curves as follows

$$\phi : E(k) \to E(k)$$
$$(x_0, \ldots, x_n) \mapsto (x_0^q, \ldots, x_n^q)$$

Proposition 5. *The degree map*

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

is a positive quadratic form.

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

$$End(E_1, E_2) \times End(E_1, E_2) \to \mathbb{Z}$$
$$(\phi, \psi) \mapsto deg(\phi + \psi) - deg(\phi) - deg(\psi)$$

For this proof we will make extentive 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

$$\begin{aligned} FIXLANGLERANGLE[<\phi, \psi>] &= [deg(\phi + \psi)] - [deg(\phi)] - [deg(\psi)] \\ &= (\phi \hat{+} \psi)(\phi + \psi) - \hat{\phi}\phi - \hat{\psi}\psi \\ &= \hat{\phi}\psi + \hat{\psi}\phi \end{aligned}$$

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

$$\begin{aligned} [<\phi_1 + \phi_2, \psi>] &= \hat{\psi}(\phi_1 + \phi_2) + (\phi_1 \hat{+} \phi_2)\psi \\ &= (\hat{\psi}\phi_1 + \hat{\phi_1}\psi) + (\hat{\psi}\phi_2 + \hat{\phi_2}\psi) \\ &= [<\phi_1, \psi>] + [<\phi_2, \psi>] \end{aligned}$$

□

Theorem 3. *Let ϕ be the q^{th} frobenius map. Then the map $1 - \phi$ is seperable, and $\#ker(1 - \phi) = deg(1 - \phi)$.*

Proof. Proofs by the means of galois theory are given in [silverman-referanse], more elementary proofs are available in [lawrence-ref]. □

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. fixme □

4. Schoof's algorithm

4.1. **Division polynomials.** 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.

Definition 17. *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 throrough examination of this method can be found in [serge lang-ref].

Another way which is more elementary by highly computational is to work explicitly with the addition formulas for elliptic curves. + mer forklaring.

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

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

4.2. **Computing the number of points.** 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 section [referanse]. 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.

The argument above is the gist of Schoof's algorithm, we will now look at how to calculate $t\,(mod \ell)$. Let ϕ be the Frobenius endomorphism resticted 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

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

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

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

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

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

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

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

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

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 $\tau^2 \equiv 4q_\ell \,(mod \ell)$

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

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

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

The right hand side is as before given by

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

4.3. **Modular polynomials.** fixme

4.4. **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 $\phi|E[\ell]$ 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 18. *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 [ref til modulrpoly-teorem] 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 7. *$\Phi_\ell(j(E), x) = 0$ 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

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

5. Satoh's algorithm

fixme