SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Counting points on elliptic curves - A study of Schoof's algorithm

av

Oskar Eklund

2018 - No K6

Counting points on elliptic curves - A study of Schoof's algorithm

Oskar Eklund

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Jonas Bergström

2018

Abstract

An elliptic curve over a field is a set of points with an addition operation defined, making it a group. The points are determined by a so called "Weierstrass equation". In this paper we will consider these elliptic curves over finite fields, this will make the sets of points finite, and study ways of counting the number of points on a given elliptic curve. The main algorithm for counting points on elliptic curve that we will study is Shoof's algorithm, but we will also consider some other less efficient algorithms and methods of counting points on elliptic curves over finite fields.

A special thanks to my mentor Jonas Bergström for all the help and guidance he has given me during my work with this essay.

Contents

1 Introduction

An elliptic curve is a curve expressed usually as the solutions to the equation $y^2 = x^3 + Ax + B$ known as the Weierstrass equation, where A, B, x, y are elements of a field and A, B are constants. We do not allow the Weierstrass equation to have multiple roots, namely we do not allow the discriminant to be zero, $\Delta = 4A^3 + 27B^2 \neq 0$.
Over the field of real numbers $\mathbb{R}$ this becomes an iconic curve where we can have a clear picture of the curve going through the coordinate system as shown below.

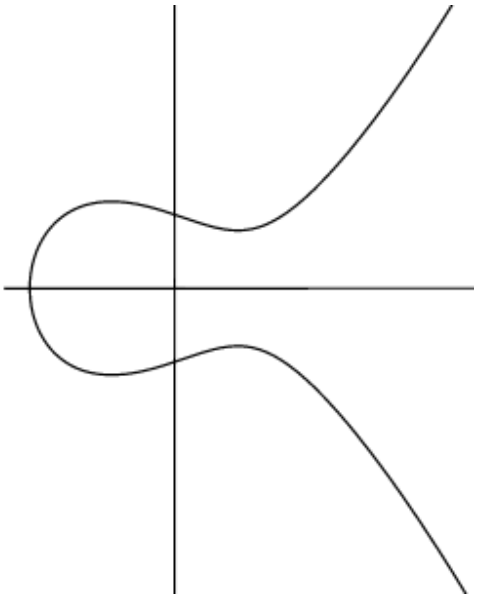

Figure 1: Elliptic curve $y^2 = x^3 - x + 1$ over $\mathbb{R}$

However if we take the curve over an finite field K then the graph of the curve would only consist of a finite number of point spread out over the area K^2, as seen in the example below.

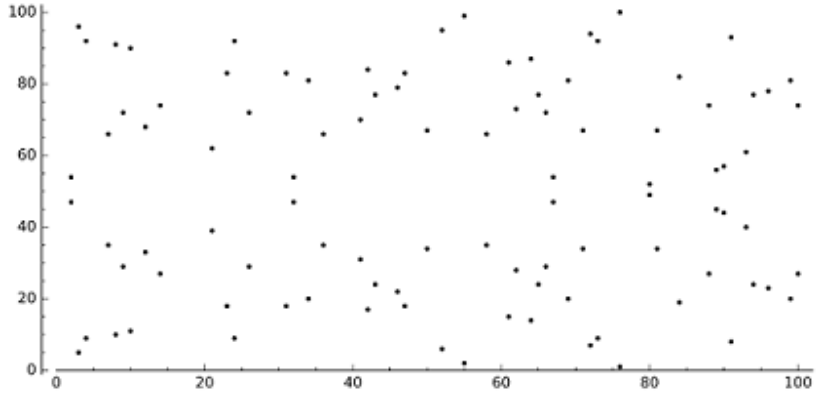

Figure 2: Elliptic curve $y^2 = x^3 + 19x + 42$ over $\mathbf{F}_{101}$

For the rest of this paper this field K will be considered a finite field which we will denote with $\mathbf{F}_q$, where q is the number of elements in the field. For the points on the elliptic curve we can define an additive operation. If we, to our set of points on the elliptic curve, add an point "the point at infinity"$= \infty$, (the name will make sense when we have defined the additive operation on the points) then we can define a way of adding two points together to get a new point within the set. This will make the set of points a group under the additive operation and the point ∞ will be the identity element of the group.

A fundamental property of an elliptic curve over a finite field is the number of points it has. Elliptic curves over finite fields have a very useful application in cryptography, where the number of points on an elliptic curve will be an essential factor to how hard a message will be to decipher. Schoof's algorithm is an algorithm for determining the number of points on an elliptic curve over a finite field.The algorithm works by manipulating finite polynomials of different degrees and the time complexity of the algorithm is $\mathcal{O}(log^8(q))$. This means that when we calculate the number of points on a elliptic curve over a field $\mathbf{F}_q$, the time we can expect it to take depends on how big q is (or rather how big $log^8(q)$ is). As we see from the expression $log^8(q)$ the time grows relatively slow compared to when q grows, which makes the algorithm relatively effective for calculating the number of points on elliptic curves when we consider them over very large finite fields.

There are however improvements done on Schoof's algorithm by both A.O.L Atkin and N.D. Elkies. Atkins improvement regards restricting the possible values of the number of points further and the improvements of Elkies regard working with polynomials of smaller degree when applying the algorithm.
Reference [3], p.241-242
The improvements of Schoof's algorithm is however beyond the scope of this paper and will not be discussed further.

2 General theory about elliptic curves

2.1 Definition of an elliptic curve

2.1.1 The group of an elliptic curve

A fantastic property of the elliptic curves over a field K is that we can define an addition operation on the points. We just have to add

$$\textit{"the point at infinity"} = \infty$$

as the identity to our set of points. If we consider the points defined by the equation $y^2 = x^3 + Ax + B$ over the field of real numbers $\mathbb{R}$ then we can describe the addition of points on an elliptic curve geometrically, but first we have to define what the negative of a point is.

Definition 2.1.
For a point $P = (x, y)$ the negative $-P$ is defined as

$$-P = -(x, y) = (x, -y)$$

Thus we obtain the negative of a point by simply switching the sign on the y-coordinate. Since the points are defined by the Weierstrass equation where y is squared, an elliptic curve's graph is symmetric with respect to the x-axis. We then know in fact that if $P = (x, y)$ lies on the curve then so does $-P = (x, -y)$.

The way we add two points P_1, P_2 to get the new point P_3 can now be described in short that we draw a line through our two points P_1, P_2. This line will then intersect the curve in another point $-P_3$. What we then do is reflect this point through the x-axis (i.e switch the sign of the y-coordinate). This will give us our point P_3. The points $P = (x, y)$ and $-P = (x, -y)$ are in fact the inverses to each other and the vertical line that describes the slope between the points will intersect the curve at *"the point at infinity"* $= \infty$. The proof of the associativity of this operation is rather lengthy and will not be included in this paper. For those who are skeptical I will refer you to the section *2.4 Proof of Associativity* in Washington (2008). Otherwise we now have our group.

We can now define the elliptic curve over any field as the set of points on the curve joined with *the point at infinity*. We will in this paper avoid the case when the characteristic of the field K considered is 2 or 3, thus from this point and forward every field mentioned will have characteristic neither 2 nor 3.

Definition 2.2.
The elliptic curve E over a field K is defined as follows

$$E(K) = \{\infty\} \cup \{(x, y) \in K \times K : y^2 = x^3 + Ax + B\}$$

We can consider points of E defined over a field K with coordinates in a field L such that $L \supseteq K$, we then write instead $E(L)$ and its defined as

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L : y^2 = x^3 + Ax + B\}$$

The more formal description of the group addition, that still works whichever field your elliptic curve is defined over as long as the characteristic is not 2 or 3, is as follows.

For an elliptic curve E: $y^2 = x^3 + Ax + B$,
let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P_1 + P_2 = P_3 = (x_3, y_3)$ then:

1. If $x_1 \neq x_2$, then,

   $$x_3 = m^2 - x_1 - x_2, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}$$

2. If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$.

3. If $P_1 = P_2$, and $y_2 \neq 0$, then

   $$x_3 = m^2 - 2x_1, \qquad y_3 = m(x_1 - x_3) - y_1, \qquad \text{where } m = \frac{3x_1^2 + A}{x_2 - x_1}$$

4. If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.

   And as per usual the identity ∞ does nothing when added to a point, that is $P + \infty = P$

From now on we will consider elliptic curves over finite fields, but first we will state some useful definitions and theorems about finite fields in general.

2.2 Finite fields

For a prime number p there exist a field with p number of elements, namely the congruence classes $\mathbb{Z}/p\mathbb{Z} = \{0, 1, ..., (p-1)\}$. We will denote this finite field with $\mathbf{F}_p$.

2.2.1 The structure and existence of finite fields

We know from just above that there are finite fields with a prime number as cardinality. We may now wonder if there are fields with cardinality that are not prime? And yes there are, these will be denoted by $\mathbf{F}_q$ accordingly. However, it is not the case that for every integer q there exist a field with cardinality q. There are a restriction on q for which there exists a field $\mathbf{F}_q$ with q elements. Before we state the restriction we need to define what the *characteristic* of a field is.

Definition 2.3.
The characteristic of an field is the smallest positive integer n such that

$$n \cdot 1 = 0$$

Reference [1], p.248

Now for finite fields we have that:

Proposition 2.0.1.
If $\mathbf{F}_q$ is a finite field, then the characteristic of $\mathbf{F}_q$ is

$$char(K) = p$$

for some prime p.
Furthermore the cardinality of $\mathbf{F}_q$ is

$$|\mathbf{F}_q| = q = p^n$$

for some positive integer n.

Proof. See [1], p.295 □

Thus the restriction on q is that it has to be a power of the characteristic p,where p is prime. There is a uniqueness to the a finite field described in the next theorem.

Theorem 2.1.
If two finite fields K and L have the same number of elements q, then they are isomorphic. Thus every finite field $\mathbf{F}_q$ is unique up to isomorphism.

Proof. See [1], p.296 □

Thus we can talk about *the* finite field $\mathbf{F}_q$ instead of *a* finite field $\mathbf{F}_q$. The field $\mathbf{F}_p$, which we first introduced, is called the prime field of characteristic p.

Now we will state some important information about the structure and existence of finite fields. The next proposition will tell us the structure of subfields for any given finite field and the following theorem will then tell us the existence of finite fields in general. But first we need a definition of what a subfield is and what an extension field is.

Definition 2.4.
If two fields $\mathbf{K}$ and $\mathbf{L}$ have the relation $\mathbf{K} \subset \mathbf{L}$, then the field $\mathbf{K}$ is called a subfield of $\mathbf{L}$ and the field $\mathbf{L}$ is called an extension field of $\mathbf{K}$.

Reference [1], p.203

Proposition 2.1.1.
For a finite field $\mathbf{K}$*, with* p^n *elements, each subfield will have* p^m *elements for some divisior* m *of* n*. Conversely, for each positive divisor* m *to* n *there exists a unique subfield of* $\mathbf{K}$ *with* p^m *number of elements.*

Proof. See [1], p.296 □

Theorem 2.2.
For each prime p *and each positive integer* n*, there exists a field with* p^n *number of elements.*

Proof. See [1], p.297 □

But how do we get these fields with $q = p^n$ elements then? We will answer this question next and show some small explicit examples of extensions of finite fields.

2.2.2 The construction of finite fields

From definition 2.4 and proposition 2.1.1 we get that the field $\mathbf{F}_{p^n}$ will be an extension field of $\mathbf{F}_p$. The way this extension field is constructed is similar to how the congruence classes $\mathbb{Z}/p\mathbb{Z}$ is constructed, but instead of working only with integers we work with polynomials, note here that integers are included since they are constant polynomials.
We will hence define what it means for a polynomial to be over a field, and we will define it in general over the field $\mathbf{F}_q$.

Definition 2.5.
The polynomials over $\mathbf{F}_q$ *is defined as all the polynomials* $p(x)$ *with coefficients in* $\mathbf{F}_q$*, and is denoted* $\mathbf{F}_q[x]$*.*

Now we can look at the congruence classes of polynomials in $\mathbf{F}_q[x] \mod p(x)$ for a given polynomial $p(x)$ in the same way we looked at the congruence classes of integers in $\mathbb{Z}/n\mathbb{Z}$ for some given integer n. Here in $\mathbf{F}_q[x] \mod p(x)$ we have that the elements is the set of remainder that is produced when the polynomials in $\mathbf{F}_q[x]$ are divided by an polynomial $p(x)$. We denote this set of congruence classes by $\mathbf{F}_q[x]/p(x)$.

Definition 2.6.
A nonconstant polynomial is called irreducible over the field $\mathbf{F}_q$ *if it cannot be factored in* $\mathbf{F}_q[x]$ *into a product of polynomials with smaller degree (if it can, then it is called reducible).*

Reference [1], p.198

Theorem 2.3.
For a field $\mathbf{F}_q$ *and a nonconstant polynomial* $p(x)$ *over* $\mathbf{F}_q$ *we have that* $\mathbf{F}_q[x]/p(x)$ *is a field if and only if* $p(x)$ *is irreducible over* $\mathbf{F}_q$*.*

Proof. See [1], p.206 □

This field $\mathbf{F}_q[x]/p(x)$ will be an extension of the field $\mathbf{F}_q$. Suppose that we find an polynomial $p(x)$ of degree 2 which is irreducible over the finite field $\mathbf{F}_q$. The elements of the field extension $\mathbf{F}_q[x]/p(x)$ will be the remainders in $\mathbf{F}_q[x]$ divided by $p(x)$, which will be on the form $a_1x + a_0$ for $a_1, a_0 \in \mathbf{F}_q$. The number of different possible combinations of coefficients for these element are q for a_1 and q for a_0 resulting in an total of q^2 different elements. With the same reasoning, concerning the degree of the remainder, we get that an extension with a polynomial of degree k will result in a total of q^k number of elements.

This combined with theorem (2.1) says that we can think of the field $\mathbf{F}_{q^n}$ as the field $\mathbf{F}_q[x]/p(x)$ where $p(x)$ has degree n.

For some clarification, here are two simple examples of extensions from $\mathbf{F}_3$ to $\mathbf{F}_{3^2} = \mathbf{F}_9$ as well as $\mathbf{F}_2$ to $\mathbf{F}_{2^3} = \mathbf{F}_8$:

Example 2.1. (*From* $\mathbf{F}_3$ *to* $\mathbf{F}_9$)
First of we have to find a irreducible polynomial p: We find $p(x) = x^2 + 2x + 2$, *since* $p(0) = 2, p(1) = 2$ *and* $p(2) = 1$. *Now since the remainder when polynomials in* $\mathbf{F}_3[x]$ *is divided by* $p(x)$ *is on the form* $a_1x + a_0$ *where* a_1 *and* a_0 *can be 0,1 or 2 respectively, we get the extension field with nine elements*

$$\mathbf{F}_9 = \mathbf{F}_3[x]/(x^2 + 2x + 2) = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}.$$

We can here see that $\mathbf{F}_3 \subset \mathbf{F}_9$ since 0,1 and 2 are elements of both fields and in $\mathbf{F}_9$ they are also closed under both addition and multiplication to the subfield of $\mathbf{F}_3 = \{0,1,2\}$ as well.

Example 2.2. (*From* $\mathbf{F}_2$ *to* $\mathbf{F}_8$)
We find the irreducible polynomial $p(x) = x^3 + x + 1$, *since* $p(0) = 1, p(1) = 1$. *Now since the degree of* $p(x)$ *is 3, we have the elements on the form* $a_2x^2 + a_1x + a_0$ *where* a_2, a_1 *and* a_0 *can each be either 0 or 1. This give us the extension field with eight elements*

$$\mathbf{F}_8 = \mathbf{F}_2[x]/(x^3 + x + 1) = \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}.$$

2.2.3 Algebraic closure of a finite field

To define what algebraic closure is we first we must define what it means for an element to be algebraic over a field.

Definition 2.7.
If an element e is algebraic over a field $\mathbf{K}$, *then there exists a nonzero polynomial* $f(x) \in \mathbf{K}[x]$ *such that* $f(e) = 0$. *Hence e is a root of this polynomial* $f(x)$.

Reference [1], p.271

Definition 2.8.
An algebraic closure of a finite field $\mathbf{F}_q$ *is denoted* $\overline{\mathbf{F}}_q$ *and means that every element* $e \in \overline{\mathbf{F}}_q$ *is algebraic over* $\mathbf{F}_q$.

Reference [6], p.231

Theorem 2.4.
For each field exist a unique (up to isomorphism) algebraic closure.

Proof. See [6], p.234 □

Since the algebraic closure is unique we can consider the algebraic closure $\overline{\mathbf{F}}_q$ of the finite field $\mathbf{F}_q$, then we have that

Lemma 2.1.
The roots to the equation $x^{q^n} - x$ *in* $\overline{\mathbf{F}}_q$ *is a finite field with* q^n *elements.*

Proof. See [1], p.295 □

We will now describe how the algebraic closure $\overline{\mathbf{F}}_q$ is constructed.
From proposition 2.1.1 we have that for every n there exists a unique field with q^n elements within $\overline{\mathbf{F}}_q$, so we can define the union of these fields as

$$\mathbf{L} = \bigcup_{n=1}^{\infty} \mathbf{F}_{q^n}$$

which will also lie within $\overline{\mathbf{F}}_q$.

Now for a element $z \in \overline{\mathbf{F}}_q$ there will be a polynomial $f(x)$ for which z is a root, by the definition of $\overline{\mathbf{F}}_q$. For this polynomial $f(x)$ there will be a subfield $\mathbf{F}_q[x]/p(x)$, with $q^{deg(f(x))}$ number of elements, to $\overline{\mathbf{F}}_q$ in which z is a element. This subfield will, by the construction of $\mathbf{L}$, also lie in $\mathbf{L}$. Since this hold for every element $z \in \overline{\mathbf{F}}_q$ we have that $\mathbf{L}$ is the whole field $\overline{\mathbf{F}}_q$.

So the construction of an *algebraic closure* of an finite field is an infinite process of finite extensions where the algebraic closure $\overline{\mathbf{F}}_q$ is then defined as the union of all these extensions.
Since all finite extensions of $\mathbf{F}_q$ are on the form $\mathbf{F}_{q^n}$ we get that

Lemma 2.2.

$$\overline{\mathbf{F}}_q := \bigcup_{n=1}^{\infty} \mathbf{F}_{q^n}$$

Lemma 2.3. *For any* $a \in \overline{\mathbf{F}}_q$ *we have that*

$$a^q = a \Leftrightarrow a \in \mathbf{F}_q$$

Proof. See [2], p.482 □

Now when we have defined what an *algebraic closure of a field* is we can go back and continue with elliptic curves, next we will define what an torsion point is.

2.3 Torsion points

Definition 2.9. *Torsion points*
On an elliptic curve E over $\mathbf{F}_q$, an $n-$torsion point P is a point with coordinates in $\overline{\mathbf{F}}_q$ which if added to it self n times would end up to be ∞. So it fulfills:

$$\underbrace{P + P + \cdots + P}_{n \text{ times}} = nP = \infty$$

and this set of points on the curve E is denoted by

$$E[n] = \{\forall P \in E(\overline{\mathbf{F}}_q) \mid nP = \infty\}$$

Remark 2.1. *Note that this set is all the points fulfilling $nP = \infty$ over the extension field $\overline{\mathbf{F}}_q$ and not only those who fulfill it over $\mathbf{F}_q$.*

For 2-torsion points you have to see if $2P = \infty \Leftrightarrow P = -P$. If $P = (x, y)$ we get that $-P = -(x, y) = (x, -y)$ and since $P = -P$ we must have that $x = x$ and $y = -y \Leftrightarrow 2y = 0$. This means that $y = 0$ (if we have $E(K)$ where the characteristic of $K \neq 2$). So to find a 2-torsion point we only need to see if there is any point of the form $(x, 0)$ defined on the elliptic curve which is the same as solving the equation $x^3 + Ax + B = 0$. For 3-torsion points the question becomes when $3P = \infty$ which can equivalently be asked as when $2P = -P$, since ∞ is the additive identity. Now with the addition rules from section 3.1 we can figure out that the x-coordinate of $2P$ and $-P$ must be the same and with some manipulations that the equation for this x is $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$. The y-coordinates we can obtain from the Weierstrass equation. We will in the next section continue with expressing the x-coordinate for $nP = \infty$ for different n.

2.4 Division polynomials

We saw in the previous section that we could, in some cases (namely n =2 and 3) with the help of the rules of addition for elliptic curves, deduce polynomials whose roots are the x-coordinates of the regarded torsion points. We will now generalize this idea to be able to express the x-coordinates for any n-torsion with so called "division polynomials". These division polynomials will be denoted by ψ_n where n stands for the number of torsions of the points with x-coordinates

equal to the roots of ψ_n. In other words if the point $P = (x, y)$ is a n-torsion point then the polynomial $\psi_n(x)$ will vanish precisely at this x-coordinate.

$$(x, y) \in E[n] \Rightarrow \psi_n(x) = 0$$

For example we had in the previous section that $\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$ is the division polynomial for the 3-torsion points of some elliptic curve with coefficients A, B.
We will in this section merely define these so called "division polynomials" in general. The A and B are as usual the coefficients of the elliptic curve we study and the n is the number of torsions.

The division polynomials ψ_n can be defined recursively as follows:
$\psi_0 = 0$
$\psi_1 = 1$
$\psi_2 = 2y$
$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$
$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$
$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ for $m \geq 2$
$\psi_{2m} = \frac{\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)}{2y}$ for $m \geq 3$.
Reference : [2], p.81

Now since we will be working in the polynomial ring $\mathbb{Z}[x, A, B]$ and not in the polynomial ring $\mathbb{Z}[x, y, A, B]$ which this definition was intended for, we have to divide the ψ_m in different cases based on whether m is even or odd. This is because whenever n is even, ψ_n can be expressed as $y \cdot \widetilde{\psi}_n(x)$, for some function $\widetilde{\psi}_n(x)$, and when n is odd ψ_n is instead only expressed as a function $\widetilde{\psi}_n(x)$

Remark 2.2.
Note that the function $\widetilde{\psi}_n(x)$ depends on n which makes it different if n is odd or even.

Here are some examples of expressions:

Example 2.3.
Let $E : y^2 = x^3 + 2x + 1$ over $\mathbf{F}_7$

Then we have:

$$\begin{aligned}
\psi_0 &= \widetilde{\psi}_0 = 0 \\
\psi_1 &= \widetilde{\psi}_1 = 1 \\
\psi_2 &= y \cdot \widetilde{\psi}_2 = y \cdot 2 \\
\psi_3 &= \widetilde{\psi}_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \\
&= 3x^4 + 12x^2 + 12x - 4 \\
&= 3x^4 + 5x^2 + 5x + 3 \\
\psi_4 &= y \cdot \widetilde{\psi}_4 = y \cdot 4(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
&= 4y(x^6 + 10x^4 + 20x^3 - 20x^2 - 8x - 8 - 8) \\
&= y \cdot (4x^6 + 5x^4 + 3x^3 + 4x^2 + 3x + 6)
\end{aligned}$$

Here we see that $\psi_i = \widetilde{\psi}_i$ *for* $i = 0, 1, 3$ *but for* $i = 2, 4$ *we instead get that* $\widetilde{\psi}_2 = 2$ *and* $\widetilde{\psi}_4 = 4x^6 + 5x^4 + 3x^3 + 4x^2 + 3x + 6$.

We are using the fact that $y^2 = x^3 + Ax + B$, here in short we will just denote $x^3 + Ax + B$ by Ec "Elliptic curve" and continuously format our expressions accordingly. To clarify the effect of working in the polynomial ring $\mathbb{Z}[x, A, B]$ brings, we will deduce the expressions for ψ_5 and ψ_6 for the same elliptic curve over the same field as in the example above.

Example 2.4.
We have again: $E : y^2 = x^3 + 2x + 1$ *over* $\mathbf{F}_7$, *and we start with* ψ_5.
So we have $n = 5$ *and* $m = 2$ *so the expression becomes:*

$$\begin{aligned}
\psi_5 &= \psi_{2\cdot 2+1} \\
&= \psi_4\psi_2^3 - \psi_1\psi_3^3 \\
&= (y \cdot \widetilde{\psi}_4)(y^3 \cdot \widetilde{\psi}_2^3) - 1 \cdot \psi_3^3 \\
&= y^4 \cdot \widetilde{\psi}_4 \cdot \widetilde{\psi}_2^3 - \psi_3^3 \\
&= Ec^2 \cdot \widetilde{\psi}_4 \cdot \widetilde{\psi}_2^3 - \psi_3^3 \\
&= (x^3 + 2x + 1)^2 \cdot (4x^6 + 5x^4 + 3x^3 + 4x^2 + 3x + 6) \cdot (2)^3 - (3x^4 + 5x^2 + 5x + 3)^3 \\
&= 5x^{12} + 5x^{10} + 2x^9 + 4x^7 + 6x^6 + 2x^5 + 5x^4 + 2x^2 + 4x
\end{aligned}$$

Thus we see that the general formula for ψ_5 *is* $\widetilde{\psi}_5 = Ec^2 \cdot \widetilde{\psi}_4 \cdot \widetilde{\psi}_2^3 - \psi_3^3$
and we got the final expression for our example to

$$\psi_5 = 5x^{12} + 5x^{10} + 2x^9 + 4x^7 + 6x^6 + 2x^5 + 5x^4 + 2x^2 + 4x.$$

We continue with ψ_6.
Here we have $n = 6$ *so* $m = 3$ *and the expression becomes:*

$$
\begin{aligned}
\psi_6 = \psi_{2\cdot 3} &= \\
&= \frac{\psi_3(\psi_5\psi_2^2 - \psi_1\psi_4^2)}{2y} \\
&= \frac{\psi_3(\psi_5(y^2\cdot\widetilde{\psi}_2 y^2) - 1\cdot(y^2\cdot\widetilde{\psi}_4^2))}{2y} \\
&= \frac{y^2\psi_3(\psi_5\widetilde{\psi}_2^2 - \widetilde{\psi}_4^2)}{2y} \\
&= y\cdot\frac{\psi_3(\psi_5\widetilde{\psi}_2^2 - \widetilde{\psi}_4^2)}{2}
\end{aligned}
$$

Here we use that $2\cdot 4 \equiv 8 \equiv 1 \pmod 7 \Leftrightarrow \frac{1}{2} \equiv 4 \pmod 7$

$$
\begin{aligned}
&= y\cdot 4\psi_3(\psi_5\widetilde{\psi}_2^2 - \widetilde{\psi}_4^2) \\
&= y\cdot(4\psi_3\psi_5\widetilde{\psi}_2^2 - 4\psi_3\widetilde{\psi}_4^2)
\end{aligned}
$$

and now we exchange the expressions from earlier results

$$
\begin{aligned}
&= y\cdot(4(3x^4+5x^2+5x+3)(\psi_5)(2)^2 \\
&- 4(3x^4+5x^2+5x+3)(4x^6+5x^4+3x^3+4x^2+3x+6)^2) \\
&= y\cdot(4(3x^4+5x^2+5x+3)(5x^{12}+5x^{10}+2x^9+4x^7+6x^6+2x^5+5x^4+2x^2+4x)(2)^2 \\
&- 4(3x^4+5x^2+5x+3)(4x^6+5x^4+3x^3+4x^2+3x+6)^2) \\
&= y\cdot(6x^{16}+x^{14}+2x^9+2x^8+6x+2)
\end{aligned}
$$

Thus we see here that the general formula for ψ_6 *is* $y\cdot\widetilde{\psi}_6 = y\cdot\frac{\psi_3(\psi_5\widetilde{\psi}_2^2-\widetilde{\psi}_4^2)}{2}$
and the we got the final expression for our example to

$$\psi_6 = y\cdot\widetilde{\psi}_6 = y\cdot(6x^{16}+x^{14}+2x^9+2x^8+6x+2)$$

We can from this in fact conclude four general expressions for ψ_n depending both on whether n is even or odd as well as if m is even or odd. We saw in the case of $n=5$ and $m=2$ that both ψ_{m+2} and ψ_m^3 in $\psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ were even, which thus gave a y^4 contribution in total. In the case that m is odd it will instead be ψ_{m-1} and ψ_{m+1} that gives us a y^4 contribution.
When n is even we saw that for the case of $n=6$ and $m=3$ both ψ_{m-1} and ψ_{m+1}^2 in $\frac{\psi_m(\psi_{m+2}\psi_{m-1}^2-\psi_{m-2}\psi_{m+1}^2)}{2y}$ where even and gave a factor of y^2 to both terms inside the parenthesis, hence we could factorize it and take out the y^2 and divide it with the y from the denominator resulting in only a factor of y.
In the case m is even we instead only have a factor of y from the terms with the

factor ψ_{m+2} and the term with the factor ψ_{m-2} inside the parenthesis but here we also have a y contribution from ψ_m outside of the parenthesis which results in a similar expression as for odd m.

So in general we have:

$$\psi_{2m+1} = \left\{ \begin{array}{ll} \psi_{m+2}\psi_m^3 - (Ec)^2\widetilde{\psi}_{m-1}\widetilde{\psi}_{m+1}^3, & \text{for odd } m \\ (Ec)^2\widetilde{\psi}_{m+2}\widetilde{\psi}_m^3 - \psi_{m-1}\psi_{m+1}^3, & \text{for even } m \end{array} \right\}, \text{for } m \geq 2$$

$$\psi_{2m} = \left\{ \begin{array}{ll} y \cdot \frac{\psi_m(\psi_{m+2}\widetilde{\psi}_{m-1}^2 - \psi_{m-2}\widetilde{\psi}_{m+1}^2)}{2}, & \text{for odd } m \\ y \cdot \frac{\widetilde{\psi}_m(\widetilde{\psi}_{m+2}\psi_{m-1}^2 - \widetilde{\psi}_{m-2}\psi_{m+1}^2)}{2}, & \text{for even } m \end{array} \right\}, \text{ for } m \geq 3$$

It turns out that division polynomials will be very useful in the process of counting points over elliptic curves, for example we can define n times a point (x, y) using them.

2.5 An integer times a point

We start by defining two polynomials.

Definition 2.10.
For any $m \geq 2$

$$\begin{aligned} \phi_m &:= x\psi_m - \psi_{m-1}\psi_{m+1} \\ \omega_m &:= \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y}, \end{aligned}$$

Theorem 2.5.
For a point $P = (x, y)$ on an elliptic curve E over a field K (over a field K with characteristic $\neq 2$) and for a positive integer $n \geq 2$ we have:

$$nP = (x_n, y_n) = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)} \right)$$

For proof see: [2], p.299

Remark 2.3.
The reason for $n \geq 2$ in the theorem is that the case for $n = 0$ or $n = 1$ are trivial and for $n \leq 0$ we can use that $-nP = -(nP) = -(x_n, y_n) = (x_n, -y_n)$. We could define nP for $n \geq 1$ by just defining $\psi_{-1} = -1$ first.

Now again since we are working in the polynomial ring $\mathbb{Z}[x, A, B]$ and not in the polynomial ring $\mathbb{Z}[x, y, A, B]$. We have to divide the formula into different cases based on if n is even or odd. Note that we keep the expressions in fraction form as this will be preferable later.

We start with the x-coordinate and as before $y^2 = x^3 + Ax + B = Ec$.
For odd n we get

$$\begin{aligned}\frac{\phi_n}{\psi_n^2} &= \frac{x\psi_n^2 - \psi_{n-1}\psi_{n+1}}{\psi_n^2} \\ &= \frac{x\psi_n^2 - y^2 \cdot \widetilde{\psi}_{n-1}\widetilde{\psi}_{n+1}}{\psi_n^2} \\ &= \frac{x\psi_n^2 - Ec \cdot \widetilde{\psi}_{n-1}\widetilde{\psi}_{n+1}}{\psi_n^2}\end{aligned}$$

and

$$\begin{aligned}\frac{\omega_n}{\psi_n^3} &= \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y \cdot \psi_n^3} \\ &= \frac{\psi_{n+2}(\widetilde{\psi}_{n-1}^2 \cdot y^2) - \psi_{n-2}(\widetilde{\psi}_{n+1}^2 \cdot y^2)}{4y \cdot \psi_n^3} \\ &= y \cdot \frac{\psi_{n+2}\widetilde{\psi}_{n-1}^2 - \psi_{n-2}\widetilde{\psi}_{n+1}^2}{4 \cdot \psi_n^3}\end{aligned}$$

for even n we get

$$\begin{aligned}\frac{\phi_n}{\psi_n^2} &= \frac{x\psi_n^2 - \psi_{n-1}\psi_{n+1}}{\psi_n^2} \\ &= \frac{x(\widetilde{\psi}_n^2 \cdot y^2) - \psi_{n-1}\psi_{n+1}}{y^2 \cdot \widetilde{\psi}_n^2} \\ &= \frac{x\widetilde{\psi}_n^2 \cdot Ec - \psi_{n-1}\psi_{n+1}}{Ec \cdot \psi_n^2}\end{aligned}$$

and

$$\begin{aligned}\frac{\omega_n}{\psi_n^3} &= \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y \cdot \psi_n^3} \\ &= \frac{(y \cdot \widetilde{\psi}_{n+2})\psi_{n-1}^2 - (y \cdot \widetilde{\psi}_{n-2})\psi_{n+1}^2}{4y \cdot (y^3 \cdot \widetilde{\psi}_n^3)} \\ &= y \cdot \frac{\widetilde{\psi}_{n+2}\psi_{n-1}^2 - \widetilde{\psi}_{n-2}\psi_{n+1}^2}{y^4 \cdot 4 \cdot \widetilde{\psi}_n^3} \\ &= y \cdot \frac{\widetilde{\psi}_{n+2}\psi_{n-1}^2 - \widetilde{\psi}_{n-2}\psi_{n+1}^2}{Ec^2 \cdot 4 \cdot \widetilde{\psi}_n^3}\end{aligned}$$

In summary we have,
if n is odd,

$$nP = (x_n, y_n) = \left(\frac{x\psi_n^2 - Ec \cdot \widetilde{\psi}_{n-1}\widetilde{\psi}_{n+1}}{\psi_n^2}, y \cdot \frac{\psi_{n+2}\widetilde{\psi}_{n-1}^2 - \psi_{n-2}\widetilde{\psi}_{n+1}^2}{4 \cdot \psi_n^3} \right)$$

and; if n is even

$$nP = (x_n, y_n) = \left(\frac{x\widetilde{\psi}_n^2 \cdot Ec - \psi_{n-1}\psi_{n+1}}{Ec \cdot \widetilde{\psi}_n^2}, y \cdot \frac{\widetilde{\psi}_{n+2}\psi_{n-1}^2 - \widetilde{\psi}_{n-2}\psi_{n+1}^2}{Ec^2 \cdot 4 \cdot \widetilde{\psi}_n^3} \right).$$

2.6 Endomorphisms

We will consider endomorphisms of elliptic curves since they will give us a criteria for the points on a elliptic curve, which will be very useful when determining the cardinality of an elliptic curve over a certain field. The goal of this section will be to prepare and give tools so that we later in section *Two fundamental thorems for elliptic curves over finite fields* can state and prove theorem 2.7. We start by defining what an endomorphism is for an elliptic curve

Definition 2.11.
An endomorphism $\alpha : E(\overline{\mathbf{F}}_q) \to E(\overline{\mathbf{F}}_q)$ of an elliptic curve $E(\mathbf{F}_q)$ is a map that fulfills $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$, and can be given by rational functions $R_1(x), R_2(x)$, i.e quotients of polynomials $R_i(x) = \frac{p_i(x)}{q_i(x)}$ with coefficients in $\mathbf{F}_q$, in the following way:

$$\alpha(x, y) = (R_1(x), y \cdot R_2(x)).$$

Furthermore we have that

- $\alpha(\infty) = \infty$
- $deg(\alpha) = max\{deg(p(x)), deg(q(x)\}$
- *with $\alpha \neq 0$ and $R_1'(x) \neq 0$, the endomorphism α is called separable*

Since the endomorphisms are expressed as rational functions, both addition of endomorphisms as well as an integer times an endomorphism is well defined.

Lemma 2.4.
Let α and β be endomorphisms as of definition 2.4,
then they can be added together.

$$(\alpha + \beta)(x, y) := \alpha(x, y) + \beta(x, y)$$

as well as multiplied with an integer n

$$(n \cdot \alpha)(x, y) := n(\alpha(x, y))$$

Proposition 2.5.1.
If $\alpha \neq 0$ is a separable endomorphism of the elliptic curve E, then

$$deg(\alpha) = \#Ker(\alpha)$$

Proof. See [2], p.54 □

Next we will define a very special endomorphism that will play a major roll in the theory of counting points on elliptic curves.

Definition 2.12.
The Frobenius endomorphism is defined as:

$$\Phi_q(x, y) = (x^q, y^q)$$

where

$$\Phi_q(\infty) = \infty.$$

Note that we will in this paper distinguish between Φ_q meaning the Frobenius endomorphism over the field $\mathbf{F}_q$ and ϕ_q meaning the numerator polynomial describing x_q for $qP = q(x, y) = (x_q, y_q)$

Reference [2], s.98

Proposition 2.5.2.
Assume that E is an elliptic curve defined over $\mathbf{F}_q$ where q is a power of a prime p. If $r, s \in \mathbb{N}, r \neq 0$ or $s \neq 0$ then

$$(r\Phi_q + s)(x, y) \text{ is separable } \Leftrightarrow p \nmid s$$

Proof. See [2], p.58 □

Lemma 2.5.
Assume that E is an elliptic curve defined over $\mathbf{F}_q$, and $(x, y) \in E(\overline{\mathbf{F}}_q)$, then

(1.) $\Phi_q(x, y) \in E(\overline{\mathbf{F}}_q)$

(2.) $(x, y) \in E(\mathbf{F}_q) \Leftrightarrow \Phi(x, y) = (x, y)$

Proof. (1.) We look at the Weierstrass equation

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

and raise both sides to the qth power to get

$$(y^2)^q = (x^3 + Ax + B)^q$$

here we have $(a + b)^q = a^q + b^q$ when ever q is a power of the characteristic of the field,

$$(y^2)^q = (x^3)^q + A^q x^q + B^q$$

we have by lemma 2.3 that since q is an power of the characteristic of $\mathbf{F}_q$ that $a^q = a$ for every element a in the field $\mathbf{F}_q$,

$$(y^q)^2 = (x^q)^3 + A(x^q) + B$$

And this means that (x^q, y^q) lies on the curve $E(\overline{\mathbf{F}}_q)$.
(2.) For the implication $(x,y) \in E(\mathbf{F}_q) \Rightarrow \Phi(x,y) = (x,y)$ we have that if $(x,y) \in E(\mathbf{F}_q)$ then $x, y \in \mathbf{F}_q$ and we use lemma 2.3 again and get $x^q = x$ as well as $y^q = q$, thus $\Phi(x,y) = (x^q, y^q) = (x,y)$. For the implication the other way we have that if $\Phi(x,y) = (x^q, y^q) = (x,y)$ then $x, y \in \mathbf{F}_q$ and so $(x,y) \in E(\mathbf{F}_q)$. □

Proposition 2.5.3. *For E defined over $\mathbf{F}_q$ and $n \geq 1$:*
(1.) Ker$(\Phi_q^n - 1) = E(\mathbf{F}_{q^n})$.
(2.) $\Phi_q^n - 1$ is a separable endomorphism, so $\#E(\mathbf{F}_{q^n}) = deg(\Phi_q^n - 1)$.

Proof. (1.)
We first can note that

$$\Phi_q^n(x,y) = \underbrace{\Phi_q(\Phi_q(\cdots(\Phi_q}_{\text{n times}}(x,y)\cdots)) = (x^{q^n}, y^{q^n}) = \Phi_{q^n}(x,y).$$

Then since $\mathrm{Ker}(\Phi_q^n - 1)$ will be the points that is taken to the identity by $\Phi_q^n - 1$, we get $\Phi_{q^n}(x,y) - (x,y) = \infty \Leftrightarrow \Phi_{q^n}(x,y) = (x,y)$, these points are by lemma 2.3 exactly those $(x,y) \in E(\mathbf{F}_{q^n})$.
(2.) By proposition 2.1.2 we have that $\Phi_q - 1$ is separable $\Leftrightarrow p \nmid -1$. Which is true since the only number that can divide its predecessor is 1, since $0/1 = 0$ but here we have p prime so $p \neq 1$. The result then follows from proposition 2.1.1 and we are done. □

2.7 The group of $E[n]$

For finite fields we have a finite number of points and the points form a group. say $\#E(\mathbf{F}_q) = N$. As we saw in the section *Torsion points*, the set of points of order n is denoted $E[n]$. In the case of elliptic curves over finite fields all points on the elliptic curve will be an torsion point since by Lagrange theorem, at least the order of the group N will take every point to the identity.

Proposition 2.5.4.
Every set of torsion points $E[n]$ is a subgroup of the group of points on the elliptic curve.

Proof. For $E[n]$ to be a subgroup it has to fulfill the three conditions from the proposition above.
(i): Here we make use of the associativity of the group action on elliptic curves points. Say we have $P \in E[n], Q \in E[n]$ and $P + Q = R$ then we want to prove

that also $R \in E[n]$. Since $P \in E[n] \Leftrightarrow nP = \infty$ and $\infty + P_i = P_i$ for any P_i on the curve (in particular $P_i = \infty$), we have

$$\begin{aligned}\infty &= \infty + \infty = nP + nQ \\ &= \underbrace{P + P + \cdots + P}_{\text{n times}} + \underbrace{Q + Q + \cdots + Q}_{\text{n times}} \\ &= \underbrace{(P+Q) + (P+Q) + \cdots + (P+Q)}_{\text{n times}} \\ &= n(P+Q) = nR = \infty\end{aligned}$$

Thus we have that $R \in E[n]$ as well.
(ii) The identity ∞ is a member of every torsion group, since for every integer n we have $n \cdot \infty = \infty + \infty + \cdots + \infty = \infty$.
(iii) If $P \in E[n] \Leftrightarrow nP = \infty$ then $n(-P) = -(nP) = -\infty = \infty$, so we have $-P \in E[n]$ as well and the proof is done. □

We can find a basis β_1, β_2 for the elements of $E[n]$. This means that every element of $E[n]$ will be able to be expressed as $m_1\beta_1 + m_2\beta_2$ for some integers m_1, m_2 which is uniquely determined $\pmod n$. Since a endomorphism $\alpha : E(\overline{K}) \to E(\overline{K})$ keep the structure of the group we have that α maps $E[n]$ to $E[n]$, therefore there exist integers a, b, c, d (unique $\pmod n$) such that

$$\alpha(\beta_1) = a\beta_1 + b\beta_2,\ \alpha(\beta_2) = c\beta_1 + d\beta_2.$$

This means that the action of an endomorphism on $E[n]$ can be described with a matrix

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

Reference: [2], p.79 - 80

Proposition 2.5.5.
Let α be an endomorphism defined over an elliptic curve E over a field K with characteristic p, and let n be an positive integer such that $p \nmid n$. Then we can find a matrix $\alpha_n = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$ with entries $s, t, u, v \in \mathbb{Z}$, that describes the action of α on a basis $\{b_1, b_2\}$ of $E[n]$.
We also have that

$$det(\alpha_n) \equiv deg(\alpha) \pmod n$$

Proof. See [2], p.89 □

The last proposition above will be very important in the proof of the second theorem of the next section, the criteria which we spoke of in the beginning of the endomorphism section.

2.8 Two fundamental theorems for elliptic curves over finite fields

First if we look at elliptic curves over finite fields we know that there is a finite number of points on the curve since there is a finite number of values for the x-coordinates. These x-values always gives zero, one or two y-values, resulting in zero, one or two points per x-value.
For a given x-value x_i we get,
(i) zero points if $x_i^3 + Ax_i + B$ is not a square in $\mathbf{F}_q$,
(ii) one point if $x_i^3 + Ax_i + B = 0$ and it is $(x_i, 0)$
(iii) else we get the two points (x_i, y_i) and $(x_i, -y_i)$.

Now since the elliptic curve has a finite number of x-values, when we work over $\mathbf{F}_q$ there are q numbers of potentially x-points that are different, next we will see that the number of points on the curve $E(\mathbf{F}_q)$ has a restriction on the total number of points on the curve.

For an elliptic curve E over a finite field $\mathbf{F}_q$ the number of points on $E(\mathbf{F}_q)$ is close to $q + 1$, namely it differs with a number a such that $|a| \leq 2\sqrt{q}$.

Theorem 2.6. *(Hasse's Theorem)*
We have that

$$\#E(\mathbf{F}_q) = q + 1 - a$$

with $|a| \leq 2\sqrt{q}$

Proof. See [2], p.100 □

Theorem 2.7.
Let E be defined over the field $\mathbf{F}_q$ and let $a = q + 1 - \#E(\mathbf{F}_q)$, then

$$\Phi_q{}^2(x, y) - a\Phi_q(x, y) + q(x, y) = \infty \tag{1}$$

or symbolical

$$\Phi_q^2 + a\Phi_q + q = 0.$$

a is the unique integer such that (1) *holds* $\forall\ (x, y) \in E(\overline{\mathbf{F}}_q)$ *and*

$$a \equiv \mathit{Trace}((\Phi_q)_m) \pmod{m}$$

for all m with $gcd(m, q) = 1$.

Proof.
We acknowledge that if a seperable endomorphism $\alpha \neq 0$, then its kernel would

be finite since by proposition 2.4.1 $\deg(\alpha) = \#\mathrm{Ker}(\alpha)$.
Then we let

$$(\Phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$$

for some m with $\gcd(m, q) = 1$. Since by proposition 2.4.2 we have that

$$(\Phi_q - 1) \text{ is separable,}$$

and we get from proposition 2.4.1 that

$$\#\mathrm{Ker}(\Phi_q - 1) = \deg(\Phi_q - 1).$$

We also have from proposition 2.4.5 that

$$\begin{aligned} \deg(\Phi_q - 1) &\equiv \det((\Phi_q)_m - I) \\ &\equiv \begin{vmatrix} s-1 & t \\ u & v-1 \end{vmatrix} \equiv (s-1)(v-1) - tu \\ &\equiv sv - tu + 1 - (s+v) \pmod{m} \end{aligned}$$

Here we notice that $q \equiv \deg(\Phi_q)_m) \equiv \det(\Phi_q)_m \equiv sv - tu \pmod{m}$
and $\mathrm{Trace}((\Phi_q)_m) = s + v$

We use proposition 2.4.3 and from theorem 2.5 get that $\#E(F_q) = q + 1 - \mathrm{Trace}((\Phi_q)_m)$
Thus we have that $\#\mathrm{Ker}(\Phi_q - 1) \equiv q + 1 - a \pmod{m}$.
So now we have that $\mathrm{Trace}((\Phi_q)_m) \equiv a \pmod{m}$
This was one of the statements from the theorem.

Since the characteristic polynomial of $(\Phi_q)_m$ is $X^2 - aX + q$, we can use the Cayley - Hamilton theorem of linear algebra which says that if we put the matrix $(\Phi_q)_m$ into its characteristic polynomial we have

$$(\Phi_q)_m^2 - a(\Phi_q)_m + qI \equiv 0 \pmod{m},$$

This means that the endomorphism $\Phi_q^2 + a\Phi_q + q$ is zero on $E[m]$. Now m can be chosen from infinitely many integers and $\Phi_q^2 + a\Phi_q + q$ is zero for all of them. Therefore we have that $\mathrm{Ker}(\Phi_q^2 + a\Phi_q + q)$ is infinite, thus we have that the endomorphism $\Phi_q^2 + a\Phi_q + q$ is equal to zero. □

Reference: [4], p.218

3 Algorithms for finding the number of points on an elliptic curve over a finite field

3.1 The Naive method

One way of counting the points on an elliptic curve E over a finite field $\mathbf{F}_q$ is by listing all the elements of the field as x-values, list what $x^3 + Ax + B$ is for respective x-value and then check if there exist square roots of $x^3 + Ax + B$ in the field.
We consider an example

Example 3.1.
Let E be the curve $y^2 = x^3+2x+4$ over $\mathbf{F}_7$, we list the values and points in a table

x	$x^3 + 2x + 4$	y	*points*
0	*4*	± 2	*(0,2),(0,5)*
1	*0*	*0*	*(1,0)*
2	*2*	± 3	*(2,3),(2,4)*
3	*2*	± 3	*(3,3),(3,4)*
4	*6*	-	-
5	*6*	-	-
6	*1*	± 1	*(6,1),(6,6)*
∞		∞	∞

Here we have 10 points, so $E(\mathbf{F}_7) = 10$.

This way of determine the cardinality, by just brute force listing all the points, is however only efficient for small q since the time complexity is $\mathcal{O}(q^2(log(q))^4)$ at worst.
Reference: [5], p.2

3.2 The Baby step, Giant step algorithm

The baby step, giant step algorithm for computing the order of an elliptic curve is based on finding the order of points on the curve and then find the least common multiple of the orders of the points within the gap from Hasse's theorem.

3.2.1 Method

Recall that:

Corollary 3.1.
For a finite group G of order n
For any element $a \in G$:
(1.) *the order of the element $o(a) \mid n$*
(2.) $a^n = e$
Here a^n denotes the n-times repeated group operation on a and e is G:s identity.

Reference: [1], p.111

Lemma 3.1.
For $a \in \mathbb{Z}$ and for some $m \in \mathbb{Z}$ such that $|a| \leq 2m^2$
there exists $a_0, a_1 \in \mathbb{Z}$ where $-m < a_0 \leq m$ and $-m \leq a_1 \leq m$
such that

$$a = a_0 + 2ma_1$$

Proof.
Remember that we have $|a| \leq 2m^2$.
We let $a_0 \equiv a \pmod{2m}$, with $-m < a_0 \leq m$ and $a_1 = \frac{(a-a_0)}{2m}$.
Then we have

$$|a_1| = \Big|\frac{(a-a_0)}{2m}\Big| \leq \frac{|a| + |a_0|)}{|2m|} \leq \frac{|2m^2| + |m|)}{|2m|} = m + \frac{1}{2} < m + 1$$

thus $|a_1| < m + 1 \Rightarrow |a_1| \leq m \Leftrightarrow -m \leq a_1 \leq m$ □

Reference: [1], p.113
In words this lemma means that: with our integer a we can choose an integer m such that a is contained in the interval $[-m^2, m^2]$ and then for an integer $a_1 \in [-m, m]$ another integer $a_0 \in [-m, m]$ will be determined such that $a_0 \equiv a \pmod{2m} \Rightarrow a = a_0 + 2ma_1$

The way we find the order of one randomly picked point on the elliptic curve is that we want to find an integer M such that $MP = \infty$ and for every factor p_i of M we have that $(M/p_i)P \neq \infty$.
We know that the order of the whole group is $N = q + 1 - a$ for some a, and also from the corollary 3.1 that $NP = \infty$ for every P on the curve. Therefore we can deduce that

$$\begin{aligned} \infty &= NP \\ &= (q + 1 - a)P \\ &= (q + 1)P - aP \end{aligned}$$

Here we let the point $(q + 1)P = Q$ and according to lemma 3.1 we can write $a = a_0 + 2ma_1$ for some $m \geq q^{(1/4)}$

$$\begin{aligned} &= Q - (a_0 + 2ma_1)P \\ &= Q - (2ma_1)P - a_0P \end{aligned}$$

Thus we get that $\infty = Q - (2ma_1)P - a_0P \Leftrightarrow Q - (2ma_1)P = a_0P$. Which in the algorithm is denoted by $Q + k(2m)P = \pm jP$.
Since $|a| \leq 2\sqrt{q}$, the task is then to first choose an integer m such that $2\sqrt{q} < 2m^2 \Leftrightarrow q^{1/2} < m^2 \Leftrightarrow q^{(1/4)} < m$.
Then to compute the point $Q = (q+1)P$, the points jP for $j = 0, 1, 2..., m$ (the negative ones are just with switched sign on the y-coordinate) and $Q + k(2m)P$

for $k = -m, -m+1, ..., m$. Now according to the lemma 3.1, there exist a match such that for some k and some j we have $Q + k(2m)P = \pm jP$.

We can then confirm that $Q + k(2m)P \mp jP = (q + 1 + 2mk \mp j)P = \infty$, and set our first guess on that $M_0 = q+1+2mk \mp j$. Then we want to se if M_0 is the smallest number such that $M_0P = \infty$, we check this by prime factorizing our guess $M_0 = p_1 \cdot p_2 \cdots p_g$ and check if for some prime factor $p_i : i \in [1, g]$ we get that $(M_0/p_i)P = \infty$. If that happens for some p_i we set our next guess on $M_1 = (M_0/p_i)$ and repeat until we find a M_k such that for every prime factor $p_i \in [p_1, p_g]$ we have $(M_k/p_i)P \neq \infty$ and then we know that M_k is the order of P.
We can then do the same procedure for more points until we have enough orders to find the least common multiple within the gap from hasses theorem.
Here we go through an example

Example 3.2.
$E : y^2 = x^3 + 2x + 6$ *over* $\mathbf{F}_{121}$
$P = (5x + 2, 7)$
1 :
Compute $Q = (q + 1)P = 122P$*:*
Which gave $Q = (2x + 3, 4x + 1)$
2 :
Choose an integer m *with* $m > q^{(1/4)}$*,*
$q = 121 = 11^2 \Rightarrow q^{(1/4)} = 11^{(1/2)} \approx 3.3$.
We choose m *to* 5.
Compute and store the points jP *for* $j = 0, 1, 2, ..., m$*:*
The list of points we get is:
$\infty, (5x + 2, 7), (4x + 8, 8x + 3), (2x + 10, 9x + 2), (9x + 8, 6x + 4), (5x + 7, 9x + 2)$
3 :
Compute the points: $Q + k(2mP)$ *for* $k = -m, -(m - 1), ..., 0, ..., m$ *until there is a match with a point(or its negative) on the stored list.* $Q + k(2mP) = \pm jP$
Found the match when $k = -m = -5$ *and* $j = 2$ *which both gave us the same point* $(4x + 8, 8x + 3)$.
4 :
Conclude that $(q + 1 + 2mk \mp j)P = \infty$*. Let* $M = q + 1 + 2mk \mp j$.
Now we have found M *such that* $MP = \infty$ *which turned out to be* $M = 70$
We now know (by Lagrange's theorem) that the order of a point divides the order of the group of points
$70 \mid \#E(\mathbf{F}_q)$
Further more we know from Hasse's theorem that the order of the group fulfills $q+1-2\sqrt{q} \leq \#E(\mathbf{F}_q) \leq q+1+2\sqrt{q} \Rightarrow 100 \leq \#E(\mathbf{F}_{121}) \leq 140$*, were we easily see that only multiple of* 70 *within the gap is* 140*.*
Thus the order is: $\#E(\mathbf{F}_{121}) = 140$

The reason the algorithm is called "baby step, giant step" is because we take the baby steps of j first and then take the giant steps of $2m$ to find the match.

This way of finding the cardinality of an elliptic curve takes less time for bigger q then the naive method. This is since we only have to calculate some points and their order, instead of listing all points, to determine the order of the whole group. The time complexity for the baby step, giant step algorithm is $\mathcal{O}(q^{1/4})$. Reference: [3], p.223

3.3 Schoof's algorithm

We have now reached our main topic.
In Schoof's algorithm of finding the cardinality of the group of points, the key lies in computing $a \pmod{\ell}$ for "enough" primes ℓ. According to Hasse's theorem we have that $\#E(\mathbf{F}_q) = q + 1 - a$ where $a \leq 2\sqrt{q}$, with "enough" primes we mean a set $S = \{2, 3, 5, \cdots, L\}$ such that $\prod_i \ell_i > 4\sqrt{q}$. So if we calculate $a \pmod{\ell}$ $\forall \ell \in S$ we can with the help of the Chinese theorem calculate $a \pmod{\prod_i \ell_i}$ and thus decide a uniquely within the potential gap. Then when we have our a we get the number of points through the equation $\#E(\mathbf{F}_q) = q + 1 - a$ and we are done.
We will only describe this algorithm for odd $q > 3$ and for simplicity we let $\ell \neq q$. This ($q = \ell$) never happens in practice when q is a big prime because the small primes ℓ are so much smaller relative to q, what does happen if you take $q = p^n$ (a field extension of the prime subfield $\mathbf{F}_p$) is that you skip that prime p in your set S and continue with the next prime to make the gap $\prod_i \ell_i > 4\sqrt{q}$.

3.3.1 Method

The way you compute a modulo the different ℓ is:

For $\ell = 2$:
For $\ell = 2$ we use the fact that when $(x, y) \in E[2]$ then the point is on the form $(x, 0)$, so if $x^3 + Ax + B$ has a root in $\mathbf{F}_q$ then there exists a point $(x, 0) \in E[2]$ and $(x, 0) \in E(\mathbf{F}_q)$ so $E(\mathbf{F}_q)$ has an even order. To determine if $x^3 + Ax + B$ has a root in $E(\mathbf{F}_q)$ we can use that the roots of $x^q - x$ is precisely the elements of $\mathbf{F}_q$. We can therefore check existence of 2-torsion points namely by computing $\gcd(x^3 + Ax + B, x^q - x)$. If the gcd is 1 then there is no 2-torsion point and the cardinality is odd. If else, there exist a 2-torsion point and the cardinality is even.

$$E(\mathbf{F}_q) = q + 1 - a \equiv \left\{ \begin{array}{llll} 1 & (\text{mod } \ell) \Rightarrow a \equiv 1 & (\text{mod } 2), & \text{if } gcd = 1 \\ 0 & (\text{mod } \ell) \Rightarrow a \equiv 0 & (\text{mod } 2), & \text{if } gcd \neq 1 \end{array} \right\}$$

When q gets large the polynomial x^q will have a large degree. This will effect the computing time for the gcd. However by first reducing $x^q \pmod{x^3 + Ax + B}$ this will go faster. We can do this by succesive squaring, which we will describe below.

We start by converting q to a binary string and then we make a list of the exponents needed for q, this will be very natural for the computer and therefore

go fast.Then we can go through the list of exponents by: successively square x whilst continuously reducing $\pmod{x^3 + Ax + B}$ until we have the required exponent, save the answer and proceed doing the same with the next exponent and multiply the answer for the next exponent with the previous answer and reducing $\pmod{x^3 + Ax + B}$. Repeat until every exponent have been included. This will be called "double and add" and we will go through a example for clarification.

Example 3.3.
$q = 37, y^2 = x^3 + 3x + 2$
$bin(q) = 100101 \Rightarrow 37 = 32 + 4 + 1 = 2^5 + 2^2 + 2^0$
So we have the list of exponents $[5, 2, 0]$
$x^2 \equiv x^2 \pmod{x^3 + 3x + 2}$
$x^4 \equiv (x^2)^2 \equiv 34x^2 + 35x \pmod{x^3 + 3x + 2}$
$x^8 \equiv (34x^2 + 35x)^2 \equiv 14x^2 + 20x + 13 \pmod{x^3 + 3x + 2}$
$x^{16} \equiv (14x^2 + 20x + 13)^2 \equiv 28x^2 + 2x + 11 \pmod{x^3 + 3x + 2}$
$x^{32} \equiv (28x^2 + 2x + 11)^2 \equiv 7x^2 + 27x + 8 \pmod{x^3 + 3x + 2}$

$x^{37} = x^{32} \cdot x^4 \cdot x$
$x^{32} \cdot x^4 \equiv (7x^2 + 27x + 8) \cdot (34x^2 + 35x) \equiv 22x^2 + 15x + 5 \pmod{x^3 + 3x + 2}$
$x^{37} \equiv (22x^2 + 15x + 5) \cdot x \equiv 15x^2 + 13x + 30 \pmod{x^3 + 3x + 2}$

Hence $gcd(x^3 + 3x + 2, x^{37} - x) = gcd(x^3 + 3x + 2, 15x^2 + 13x + 30 - x) = x + 4$

For $\ell > 2$:
Now we continue with the next prime $\ell > 2$, and here we will use theorem 3.3, that on an elliptic curve the equation

$$\Phi_q{}^2(x, y) - a\Phi_q(x, y) + q(x, y) = \infty \tag{2}$$

or symbolically

$$\Phi_q{}^2 - a\Phi_q + q = 0 \tag{3}$$

which equivalently is

$$\Phi_q{}^2 + q = a\Phi_q \tag{4}$$

is fulfilled, $\forall (x, y) \in E(\overline{\mathbf{F}}_q)$.
For proof see [2], p.101

Moreover for a point $(x, y) \in E[\ell]$ and with $q \equiv q_\ell \pmod{\ell}$, we have that (x, y) fulfills equation (1) above and $q(x, y) = q_\ell(x, y)$. So $\forall\ (x, y) \in E[\ell]$ we also have

$$(x^{q^2}, y^{q^2}) + q_\ell(x, y) = a(x^q, y^q) \tag{5}$$

So our goal here is to compute the components of this equation to see what a is for each torsion group $E[\ell]$ which in effect will be what a is congruent to for each prime number $\ell \in S$.

We can be in one of three cases here, either we have that:

$$\textbf{(i)} : {\Phi_q}^2(x,y) \neq \pm q_\ell(x,y),\ \forall (x,y) \in E[\ell]$$
$$\textbf{(ii)} : {\Phi_q}^2(x,y) = \pm q_\ell(x,y)\ \forall (x,y) \in E[\ell]$$

or

$$\textbf{(iii)} : {\Phi_q}^2(x,y) = \pm q_\ell(x,y) \text{ for some } (x,y) \in E[\ell]$$

We want to determine in which case we are in, by looking if the x-coordinates are the same or not. Note that from now on if we do not specify that $(x,y) \in E[\ell]$ then we will consider x as an formal variable.
We determine in which case we are in by computing $\gcd(x^{q^2} - x_{q_\ell}, \psi_{q_\ell})$ with the help of the double-and-add algorithm. Here x_{q_ℓ} is the x-coordinate of $q_\ell(x,y)$ and remember that ψ_{q_ℓ} is the division polynomial were the roots are precisely the x-coordinates for the points in $E[\ell]$.
If the gcd $= \psi_{q_\ell}$ then all roots to $x^{q^2} - x_{q_\ell}$ are in ψ_{q_ℓ} and thus for all points in $E[\ell]$: $x^{q^2} = x_{q_\ell}$ and we are in case (**i**).
If the gcd $= 1$ then they have no roots in common so $x^{q^2} \neq x_{q_\ell}$ for all points in $E[\ell]$ and we are in case (**ii**).
Now if the gcd $= h$ such that $1 \neq h \neq \psi_{q_\ell}$ then for some of the points (namely the roots of h) $x^{q^2} = x_{q_\ell}$. So we will be in case (**iii**).

We begin with the case when the points have different x-coordinates for all points in $E[\ell]$.

Case (**i**) : ${\Phi_q}^2(x,y) \neq \pm q_\ell(x,y)$
So we remember that we have the relation

$$(x^{q^2}, y^{q^2}) + q_\ell(x,y) = a(x^q, y^q)\ \forall\ (x,y) \in E[\ell]$$

Here we have that $x^{q^2} \neq x_{q_\ell}$ which means that we can use the formula for addition of different points to compute $(x',y') = (x^{q^2}, y^{q^2}) + q_\ell(x,y)$ where $(x,y) \in E[\ell]$. We compute an expression for x'.

$$x' = \left(\frac{y^{q^2} - y_{q_\ell}}{x^{q^2} - x_{q_\ell}}\right)^2 - (x^{q^2} + x_{q_\ell})$$

Now since we have two different expression for x_{q_ℓ}, one if q_ℓ is odd and one if q_ℓ is even, we get two different expressions for x' as well.

(**1**.) For q_ℓ odd we have,

$$q_\ell(x,y) = (x_{q_\ell}, y_{q_\ell}) = \left(\frac{x\psi_{q_\ell}^2 - Ec \cdot \widetilde{\psi}_{q_\ell - 1}\widetilde{\psi}_{q_\ell+1}}{\psi_{q_\ell}^2}, y \cdot \frac{\psi_{q_\ell+2}\widetilde{\psi}_{q_\ell-1}^2 - \psi_{q_\ell-2}\widetilde{\psi}_{q_\ell+1}^2}{4 \cdot \psi_{q_\ell}^3}\right)$$

But we will write it short as

$$x_{q_\ell} = \frac{\phi_{q_\ell,odd}}{\psi_{q_\ell}^2},\ y_{q_\ell} = y \cdot \frac{\omega_{q_\ell,odd}}{\psi_{q_\ell}^3}$$

and we change the x_{q_ℓ} and y_{q_ℓ} with the expressions from the formula

$$= \left(\frac{y^{q^2} - y \cdot \frac{\omega_{q_\ell,odd}}{\psi_{q_\ell}^3}}{x^{q^2} - \frac{\phi_{q_\ell,odd}}{\psi_{q_\ell}^2}} \right)^2 - \left(x^{q^2} + \frac{\phi_{q_\ell,odd}}{\psi_{q_\ell}^2} \right),$$

factor out y from the square

$$= y^2 \left(\frac{y^{q^2} - \frac{\omega_{q_\ell,odd}}{\psi_{q_\ell}^3}}{x^{q^2} - \frac{\phi_{q_\ell,odd}}{\psi_{q_\ell}^2}} \right)^2 - \left(x^{q^2} + \frac{\phi_{q_\ell,odd}}{\psi_{q_\ell}^2} \right),$$

write the expressions with common denominators

$$= y^2 \left(\frac{\frac{y^{q^2-1} \cdot \psi_{q_\ell}^3 - \omega_{q_\ell,odd}}{\psi_{q_\ell}^3}}{\frac{x^{q^2}\psi_{q_\ell}^2 - \phi_{q_\ell,odd}}{\psi_{q_\ell}^2}} \right)^2 - \left(\frac{x^{q^2}\psi_{q_\ell}^2 + \phi_{q_\ell,odd}}{\psi_{q_\ell}^2} \right),$$

factor out both the denominators from the m-expression

$$= \frac{y^2\psi_{q_\ell}^4}{\cdot\psi_{q_\ell}^6} \cdot \left(\frac{y^{q^2-1} \cdot \psi_{q_\ell}^3 - \omega_{q_\ell,odd}}{x^{q^2}\psi_{q_\ell}^2 - \phi_{q_\ell,odd}} \right)^2 - \left(\frac{x^{q^2}\psi_{q_\ell}^2 + \phi_{q_\ell,odd}}{\psi_{q_\ell}^2} \right),$$

then simplify, break up the fractions and reduce y^2 to Ec

$$= \frac{Ec}{\psi_{q_\ell}^2} \cdot \frac{(Ec^{\frac{q^2-1}{2}} \cdot \psi_{q_\ell}^3 - \omega_{q_\ell,odd})^2}{(x^{q^2}\psi_{q_\ell}^2 - \phi_{q_\ell,odd})^2} - \frac{(x^{q^2}\psi_{q_\ell}^2 + \phi_{q_\ell,odd})}{\psi_{q_\ell}^2}$$

and finally, we expand the second term to be able to write the whole expression with common denominator

$$= \frac{Ec(Ec^{\frac{q^2-1}{2}} \cdot \psi_{q_\ell}^3 - \omega_{q_\ell,odd})^2}{\psi_{q_\ell}^2(x^{q^2}\psi_{q_\ell}^2 - \phi_{q_\ell,odd})^2} - \frac{(x^{q^2}\psi_{q_\ell}^2 + \phi_{q_\ell,odd})(x^{q^2}\psi_{q_\ell}^2 - \phi_{q_\ell,odd})^2}{\psi_{q_\ell}^2(x^{q^2}\psi_{q_\ell}^2 - \phi_{q_\ell,odd})^2}$$

Now we have an expression for $x' = \frac{x'_{num_{odd}}}{x'_{den_{odd}}}$ were the denominator $x'_{den_{odd}}$ is

$$x'_{den_{odd}} = \psi_{q_\ell}^2(x^{q^2}\psi_{q_\ell}^2 - \phi_{q_\ell,odd})^2$$

and the numerator $x'_{num_{odd}}$ which we are mostly interested in is

$$x'_{num_{odd}} = (Ec(Ec^{\frac{q^2-1}{2}}\psi_{q_\ell}^3 - \omega_{q_\ell,odd})^2 - (x^{q^2}\psi_{q_\ell}^2 + \phi_{q_\ell,odd})(x^{q^2}\psi_{q_\ell}^2 - \phi_{q_\ell,odd})^2.$$

(**2**.) For q_ℓ even we instead have

$$q_\ell(x,y) = (x_{q_\ell}, y_{q_\ell}) = \left(\frac{xpsi_{q_\ell}^2 \cdot Ec - \psi_{q_\ell-1}\psi_{q_\ell+1}}{Ec \cdot psi_{q_\ell}^2}, y.\frac{psi_{q_\ell+2}\psi_{q_\ell-1}^2 - psi_{q_\ell-2}\psi_{q_\ell+1}^2}{Ec^2 \cdot 4 \cdot psi_{q_\ell}^3}\right)$$

which we write in short as

$$x_{q_\ell} = \frac{\phi_{q_\ell,even}}{Ec \cdot \widetilde{\psi}_{q_\ell}^2},\ y_{q_\ell} = y \cdot \frac{\omega_{q_\ell,even}}{Ec^2 \cdot \widetilde{\psi}_{q_\ell}^3}$$

We have again

$$x' = \left(\frac{y^{q^2} - y_{q_\ell}}{x^{q^2} - x_{q_\ell}}\right)^2 - (x^{q^2} + x_{q_\ell})$$

and substitute x_{q_ℓ} and y_{q_ℓ} to their respective expression

$$= \left(\frac{y^{q^2} - y \cdot \frac{\omega_{q_\ell,even}}{Ec^2 \cdot \widetilde{\psi}_{q_\ell}^3}}{x^{q^2} - \frac{\phi_{q_\ell,even}}{Ec \cdot \widetilde{\psi}_{q_\ell}^2}}\right)^2 - \left(x^{q^2} + \frac{\phi_{q_\ell,even}}{Ec \cdot \widetilde{\psi}_{q_\ell}^2}\right),$$

factor out y and write the expressions with common denominators

$$= y^2\left(\frac{\frac{y^{q^2-1} \cdot Ec^2 \cdot \widetilde{\psi}_{q_\ell}^3 - \omega_{q_\ell,even}}{Ec^2 \cdot \widetilde{\psi}_{q_\ell}^3}}{\frac{x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 - \phi_{q_\ell,even}}{Ec \cdot \widetilde{\psi}_{q_\ell}^2}}\right)^2 - \left(\frac{x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 + \phi_{q_\ell,even}}{Ec \cdot \widetilde{\psi}_{q_\ell}^2}\right),$$

factor out both the denominators from the m-expression and break up the fractions

$$= \frac{Ec^3 \cdot \widetilde{\psi}_{q_\ell}^4}{Ec^4 \cdot \widetilde{\psi}_{q_\ell}^6} \cdot \frac{(y^{q^2-1} \cdot Ec^2 \cdot \widetilde{\psi}_{q_\ell}^3 - \omega_{q_\ell,even})^2}{(x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 - \phi_{q_\ell,even})^2} - \frac{(x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 + \phi_{q_\ell,even})}{Ec \cdot psi_{q_\ell}^2},$$

simplify the first fraction and reduce y^2 to Ec (here we have $y^{q^2-1} \cdot Ec^2 = Ec^{\frac{q^2-1}{2}} \cdot Ec^2 = Ec^{\frac{q^2-1}{2}+\frac{4}{2}} = Ec^{\frac{q^2+3}{2}}$)

$$= \frac{1}{Ec \cdot \widetilde{\psi}_{q_\ell}^2} \cdot \frac{(Ec^{\frac{q^2+3}{2}} \cdot \widetilde{\psi}_{q_\ell}^3 - \omega_{q_\ell,even})^2}{(x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 - \phi_{q_\ell,even})^2} - \frac{(x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 + \phi_{q_\ell,even})}{Ec \cdot \widetilde{\psi}_{q_\ell}^2},$$

and finally, expand the last term to be able to write the whole expression with common denominator

$$= \frac{1}{Ec \cdot \widetilde{\psi}_{q_\ell}^2} \cdot$$
$$\frac{(Ec^{\frac{q^2+3}{2}} \cdot \widetilde{\psi}_{q_\ell}^3 - \omega_{q_\ell,even})^2}{(x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 - \phi_{q_\ell,even})^2} - \frac{(x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 + \phi_{q_\ell,even})(x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 - \phi_{q_\ell,even})^2}{Ec \cdot \widetilde{\psi}_{q_\ell}^2 (x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 - \phi_{q_\ell,even})^2}.$$

thus we get the denominator to

$$x'_{den_{even}} = \cdot \widetilde{\psi}_{q_\ell}^2 (x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 - \phi_{q_\ell,even})^2$$

and the numerator to

$$x'_{num_{even}} = (Ec^{\frac{q^2+3}{2}} \cdot \widetilde{\psi}_{q_\ell}^3 - \omega_{q_\ell,even})^2 - (x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 + \phi_{q_\ell,even})(x^{q^2} Ec \cdot \widetilde{\psi}_{q_\ell}^2 - \phi_{q_\ell,even})^2$$

So now we have our x' expressed and we get back to the relation

$$(x^{q^2}, y^{q^2}) + q_\ell(x, y) = a(x^q, y^q)$$

Here our task is to find j such that

$$(x', y') = j(x^q, y^q) = (x_j^q, y_j^q)$$

With $(x, y) \in E[\ell]$ and $(x', y) \neq \infty$ we know that $j \in [1, \ell - 1]$ or since the x-coordinate for $j(x, y) = (x_j, y_j)$ and $-j(x, y) = (x_j, -y_j)$ are the same, we only need to check $j \in [1, \frac{\ell+1}{2}]$ to find a match for the x-coordinates.
So we search for j such that

$$x' - x_j^q \equiv 0 \pmod{\psi_\ell} \tag{6}$$

Note that both x' and x_j^q can be expressed as rational functions of x which reduces the problem of finding j to computing gcd of the numerator of $x' - x_j^q$ and ψ_ℓ
We express x_j with the formula for nP but once again we have to take into account whether j is odd or even. We also have to take into account whether q_ℓ is odd or even for x'. So we get in total four different expressions for the combinations of j and q_ℓ.

q_ℓ odd and j odd:

$x' = \frac{x'_{num_{odd}}}{x'_{den_{odd}}} \quad x_j^q = \left(\frac{\phi_j}{\psi_j^2}\right)^q$

$$\begin{aligned} x' - x_j^q &= \frac{x'_{num_{odd}}}{x'_{den_{odd}}} - \left(\frac{\phi_{j,odd}}{\psi_j^2}\right)^q \\ &= \frac{x'_{num_{odd}}}{x'_{den_{odd}}} - \frac{\phi_{j,odd}^q}{\psi_j^{2q}} \\ &= \frac{x'_{num_{odd}} \cdot \psi_j^{2q} - \phi_{j,odd}^q \cdot x'_{den_{odd}}}{x'_{den_{odd}} \cdot \psi_j^{2q}} \end{aligned}$$

q_ℓ odd and j even:

$x' = \frac{x'_{num_{odd}}}{x'_{den_{odd}}} \quad x_j^q = \left(\frac{\phi_{j,even}}{\widetilde{\psi}_j^2 \cdot Ec}\right)^q$

$$\begin{aligned} x' - x_j^q &= \frac{x'_{num_{odd}}}{x'_{den_{even}}} - \left(\frac{\phi_{j,even}}{\widetilde{\psi}_j^2 \cdot Ec}\right)^q \\ &= \frac{x'_{num_{odd}} \cdot \widetilde{\psi}_j^{2q} \cdot Ec^q - \phi_{j,even}^q \cdot x'_{den_{odd}}}{x'_{den_{odd}} \cdot \widetilde{\psi}_j^{2q} \cdot Ec^q} \end{aligned}$$

q_ℓ even and j odd:

$x' = \frac{x'_{num_{even}}}{x'_{den_{even}}} \quad x_j^q = \left(\frac{\phi_{j,odd}}{\psi_j^2}\right)^q$

$$\begin{aligned} x' - x_j^q &= \frac{x'_{num_{even}}}{x'_{den_{even}}} - \left(\frac{\phi_{j,odd}}{\psi_j^2}\right)^q \\ &= \frac{x'_{num_{even}} \cdot \psi_j^{2q} - \phi_{j,odd}^q \cdot x'_{den_{even}}}{x'_{den_{odd}} \cdot \psi_j^{2q}} \end{aligned}$$

q_ℓ even and j even:

$x' = \frac{x'_{num_{even}}}{x'_{den_{even}}} \quad x_j^q = \left(\frac{\phi_{j,even}}{\widetilde{\psi}_j^2 \cdot Ec}\right)^q$

$$\begin{aligned} x' - x_j^q &= \frac{x'_{num_{even}}}{x'_{den_{even}}} - \left(\frac{\phi_{j,even}}{\widetilde{\psi}_j^2 \cdot Ec}\right)^q \\ &= \frac{x'_{num_{even}} \cdot \widetilde{\psi}_j^{2q} \cdot Ec^q - \phi_{j,even}^q \cdot x'_{den_{even}}}{x'_{den_{even}} \cdot \widetilde{\psi}_j^{2q} \cdot Ec^q} \end{aligned}$$

We check for which j by $\gcd(\text{numerator}(x' - x_j^q), \psi_\ell)$, if the gcd $\neq 1$ then we have our j, if not we try the next j.
Suppose we have found our j, we then proceed to determine the sign since we for now only know the x-coordinate of $j(x, y)$. So to find the right j we have to check if $y' = y_j^q$. We can do this similarly as we checked $x' - x_j^q$, since we can express both y'/y and y_j^q/y as rational functions in x and then we can expand the expression to a numerator and a denomenator. We check $\gcd(\text{numerator}((y' - y_j^q)/y), \psi_\ell)$. If the gcd $\neq 1$ then we know that $a \equiv j \pmod{\ell}$, if not its the negative and we have instead $a \equiv -j \pmod{\ell}$.

Case (ii) : ${\Phi_q}^2(x, y) = \pm q_\ell(x, y)$
If we have

$$ {\Phi_q}^2(x, y) = -q_\ell(x, y) $$

then $\forall (x, y) \in E[\ell]$

$$ {\Phi_q}^2(x, y) + q_\ell(x, y) = \infty = a\Phi_q(x, y) $$

so $a \equiv 0 \pmod{\ell}$ and we are done.

Else we have

$$ {\Phi_q}^2(x, y) = q_\ell(x, y) $$

and here we notice that

$$ a\Phi_q(x, y) = {\Phi_q}^2(x, y) + q_\ell(x, y) = 2q_\ell(x, y) $$

and if we now square both sides we get on the left hand side

$$ a^2\Phi_q^2(x, y) = a^2 q_\ell(x, y) $$

and on the right hand side

$$ (2q_\ell)^2(x, y) = 4q_\ell^2(x, y) $$

Therefore

$$ a^2 q_\ell(x, y) = 4q_\ell^2(x, y) $$

Which for $(x, y) \in E[\ell]$ results in the congruence

$$ \begin{aligned} a^2 q &\equiv 4q^2 \pmod{\ell} \\ &\Leftrightarrow \\ a^2 &\equiv 2^2 q \pmod{\ell} \end{aligned} $$

Here q itself must be a square (mod ℓ) to fulfill the congruence, say

$$q = w^2$$

We can from that conclude that

$$\begin{aligned}
{\Phi_q}^2(x,y) - q(x,y) &= ({\Phi_q}^2 - q)(x,y) \\
&= ({\Phi_q}^2 - w^2)(x,y) \\
&= (\Phi_q + w)(\Phi_q - w)(x,y) \\
&= \infty
\end{aligned}$$

Here for a point $P = (x, y)$ either

$$(\Phi_q + w)P = \infty \Leftrightarrow \Phi_q P = -wP$$

or

$$(\Phi_q - w)P = \infty \Leftrightarrow \Phi_q P = wP$$

If we have $\Phi_q P = -wP$ we get

$$\begin{aligned}
{\Phi_q}^2 - a\Phi_q + q &= q + aw + q \\
&= 2q + aw \\
&= 0
\end{aligned}$$

thus $2q \equiv 2w^2 \equiv -aw \Leftrightarrow -2w \equiv a \pmod{\ell}$
If we instead have $\Phi_q P = wP$ we get in a similar way $2w = a \pmod{\ell}$

We decide computational wise what a is congruent to, by simply looking for $w \in [1, \frac{\ell+1}{2}]$ such that $w^2 = q \pmod{\ell}$, we only need to check half of the w since $w^2 = (-w)^2$. If we don't find w then we have that ${\Phi_q}^2(x,y) = -q_\ell(x,y)$ and thus $a \equiv 0 \pmod{\ell}$, but if we find a w we have to check if

$$x^q - x_w \equiv 0 \pmod{\psi_\ell}$$

We do this by gcd(numerator$(x^q - x_w), \psi_\ell)$. Here we reduce x^q with double-and-add $\pmod{\psi_\ell}$ as usual and we compute x_w with the appropriate version (if w is odd or even) of the derived formulas for $nP = (x_n, y_n)$. If gcd $= 1$ then we are in the case of ${\Phi_q}^2(x,y) = -q_\ell(x,y)$ and we have $a \equiv 0 \pmod{\ell}$ once again, if we instead have $gcd \neq 1$ then we can proceed to decide whether

$$(\Phi_q + w)(x,y) = \infty \Leftrightarrow (x^q, y^q) + (x_w, y_w) = \infty$$

or

$$(\Phi_q - w)(x,y) = \infty \Leftrightarrow (x^q, y^q) - (x_w, y_w) = \infty$$

by checking gcd(numerator$(y^q/y - y_w/y), \psi_\ell)$ If we have this gcd $= 1$ we have that $(x^q, y^q) = -(x_w, y_w)$ and we found earlier that $a \equiv -2w$, but if we have gcd $\neq 1$ then $(x^q, y^q) = (x_w, y_w)$ and $a \equiv 2w$.

Case (iii) : ${\Phi_q}^2(x, y) = \pm q_\ell(x, y)$ for some $(x, y) \in E[\ell]$
In this special case we have that only for some of the points $(x, y) \in E[\ell]$ the equation holds, and the points that fulfills the equation is precisely those with x-coordinates equal to the roots of $\gcd(x^{q^2} - x_{q_\ell}, \psi_\ell) = h(x)$ so in other words $\gcd(x^{q^2} - x_{q_\ell}, h(x)) = h(x)$ which means that we can use the same method as in case (ii) but substitute ψ_ℓ for $h(x)$.

Summing up:
We go through this tests for all remaining primes $\ell \in S$ and determine $a \pmod{\ell} \in S$ thus make a equation system of congruences.

$$\begin{aligned} a &\equiv a_2 \pmod 2 \\ a &\equiv a_3 \pmod 3 \\ &\vdots \\ a &\equiv a_L \pmod L \end{aligned}$$

Then we solve for $a \pmod{\prod_i \ell_i}$ with help of the Chinese remainder theorem. We lastly check if $\frac{1}{2}\prod_i \ell_i < a$ then we just reduce a with $\prod_i \ell_i$ to give our solution in the gap $[-\frac{1}{2}\prod_i \ell_i, \frac{1}{2}\prod_i \ell_i]$ This will in turn determine a uniquely within the gap $[-2\sqrt{q}, 2\sqrt{q}]$.
Now we can calculate the cardinality of the curve with $\#E(\mathbf{F}_q) = q + 1 - a$ and we are done.

Example 3.4.
$y^2 = x^3 + 19x + 42$ *over* $\mathbf{F}_{101}$
We will start by finding our set of small primes, $2 \cdot 3 \cdot 5 \cdot 7 = 210 > 4\sqrt{101} \approx 40.2$. *So* $S = \{2, 3, 5, 7\}$. *Now we check for our first prime if there are any 2-torsion points.*
$\ell = 2$:
We do this with gcd$(x^3 + 5x + 12, x^{101} - x)$. *We reduce* $x^{101} \pmod{\psi_3}$ *with daa (double-and-add) and get that:*
gcd$(x^3 + 5x + 12, x^{101} - x) = 1$ *and we have our first congruence equation*

$$a \equiv 1 \pmod 2.$$

We continue with
$\ell = 3$:
Our q_ℓ *is* $101 \equiv 2 \pmod 3$, *so we have from equation* (4) *the relation*

$$({x^{101}}^2, {y^{101}}^2) + 2(x, y) = a(x^{101}, y^{101}),\ \forall (x, y) \in E[3]$$

We want to see if ${x^{101}}^2 = x_2 \pmod{\psi_3}$ *which we check with gcd*$({x^{101}}^2 - x_2, \psi_3)$. *From the formula for an integer times a point we get* x_2 *and* ${x^{101}}^2$ *we reduce*

with daa. This leads to that $gcd(x^{101^2} - x_2, \psi_3) = \psi_3$ *and* x^{101^2} *and* x_2 *are the same for every* $(x, y) \in E[3]$. *We proceed to see if* q *is a square* $\pmod 3$ *and thus find an* w *such that* $w^2 = q \pmod 3$. *However* $101 \equiv 2 \pmod 3$ *and* $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 1 \pmod 3$ *So* 101 *is not a square and thus* $a \equiv 0 \pmod 3$ *and we have our second congruence equation*

$$a \equiv 0 \pmod 3.$$

$\ell = 5$:
We have now q_ℓ *is* $101 \equiv 1 \pmod 5$, *and the equation* (4) *becomes*

$$(x^{101^2}, y^{101^2}) + (x, y) = a(x^{101}, y^{101}),\ \forall (x, y) \in E[5]$$

We check if we have $x^{101^2} = x \pmod{\psi_5}$ *with* $gcd(x^{101^2} - x, \psi_5)$. *We use daa again but with* $\pmod{\psi_5}$ *and get that* $gcd(x^{101^2} - x, \psi_5) = h(x) = x^2 + 17x + 92$. *So here we have that the* x*-coordinates of* $h(x)$ *are the points for which* $\Psi_q^2(x, y) = (x, y)$ *and we search if there exist a* w *again this time* $\pmod 5$. *We see directly that since* $101 \equiv 1 \pmod 5$ *and* $1^1 = 1$ *is a square, we have that* $w = 1$. *We proceed to check whether we have that* $x^q - x \equiv 0 \pmod{h(x)}$ *by* $gcd(x^q - x, h(x)) = h(x)$ *and so for every point with* x*-coordinate as the root of* $h(x) = x^2 + 17x + 92$ *we have that* $(x^q, y^q) = \pm(x, y)$. *We decide the sign by* $gcd(numerator((y^q - y)/y) = gcd(y^{q-1} - 1) = gcd(Ec^{50} - 1) = 1$, *so* $(x^q, y^q) = -(x, y)$ *and we get that* $a \equiv -2w \equiv -2 \equiv 3 \pmod 5$ *and we have our third congruence equation*

$$a \equiv 3 \pmod 5.$$

And finally for our last small prime,
$\ell = 7$:
This time we get q_ℓ *to* $101 \equiv 3 \pmod 7$ *and the equation* (4) *becomes*

$$(x^{101^2}, y^{101^2}) + 3(x, y) = a(x^{101}, y^{101}),\ \forall (x, y) \in E[7]$$

We check here if we have $x^{101^2} = x_3 \pmod{\psi_7}$ *with* $gcd(x^{101^2} - x_3, \psi_7)$. *As usual we do this with daa and receive that* $gcd(x^{101^2} - x_3, \psi_7) = 1$, *so we have that the points are different for all* $(x, y) \in E[7]$. *We can then use the formula for addition and compute an expression for* $x' = \frac{x'_{num}}{x'_{den}}$ *since we have that* $q_\ell = 3$ *we use the formula for odd* q_ℓ. *Now our task will be to find an* j *such that the* x*-coordinates* x' *and* x_j^q *are the same for points* $(x, y) \in E[7]$, *and this we will do by checking* $gcd(x' - x_j^q, \psi 7)$. *We format our expression for* $(x' - x_j^q)$ *according to if* j *is odd or even and then systematically check for which* j *the* $gcd(x' - x_j^q, \psi 7) \neq 1$. *We find that* $j = 3$ *gives us just that and we now just have to determine the sign of* j *which we will do by comparing the* y*-coordinates. Since* $j = 3$ *we take* $gcd((y^{q^2} - y_3)/y, \psi_7) \neq 1$, *thus we have that the* j*-coordinates are the same and thus we have our fourth and last congruence equation*

$$a \equiv 3 \pmod 7.$$

To decide what a is now we simply solve the equation system of congruences with the Chinese remainder theorem

$$\begin{aligned} a &\equiv 1 \pmod 2 \\ a &\equiv 0 \pmod 3 \\ a &\equiv 3 \pmod 5 \\ a &\equiv 3 \pmod 7 \end{aligned}$$

This gives us that $a \equiv 3 \pmod{210}$ *and we have then determined a uniquely within* $[-2\sqrt{101}, 2\sqrt{101}]$. *So the number of points on* $y^2 = x^3 + 19x + 42$ *over* $\mathbf{F}_{101}$ *is*

$$\#E(\mathbf{F}_{101}) = 101 + 1 - 3 = 99$$

4 References

[1] J.A.Beachy & W.D.Blair: *Abstract Algebra* (2006), Waveland Pr Inc, Illinois.
[2] L.W.Washington: *Elliptic Curves, number theory and cryptography* (2008), Chapman Hall/CRC.
[3] R.Schoof: *Counting points on elliptic curves over finite fields* (1995), Journal de Théorie des Nombres, de Bordeaux 7.
[4] A.Holst & V.Ufnarovski:*Matrix Theory* (2014), Studentlitteratur AB, Lund.
[5] A.Alvarado: *An exposition of Schoof's algorithm* (2005), Arizona state university, Arizona.
[6] S.Lang: *Algebra* (2002), Springer-Verlag, New York.

A Appendix

```
def Schoofs_Algorithm():

    def odd(k):
        return gcd(k,2)==1

    def PrimeList(q):
        primelist = []
        PI = 1
        i = 0
        while PI < 4*int(sqrt(q)):
            p = Primes().unrank(i)
            if gcd(p,q) == 1:
                PI = PI*(p)
                primelist.append(p)
            i += 1
        return primelist

    def psi(i):
        def psi_odd(m):
            if odd(m):
                return psi(m+2)*(psi(m))^3 - (psi(m-1)*(psi(m+1))^3)*(Ec)^2
            else:
                return (Ec)^2*psi(m+2)*(psi(m))^3 - psi(m-1)*(psi(m+1))^3
        def psi_even(m):
            return (psi(m)*(psi(m+2)*(psi(m-1))^2 - psi(m-2)*(psi(m+1))^2))/(2)
        def calculator_of_psi(i):
            if i == -1 or i == 0 or i == 1 or i == 2:
                return i
            elif i == 3:
                return (3*x^4 + 6*A*x^2 + 12*B*x - A^2)
            elif i == 4:
                return 4*(x^6 + 5*A*x^4 + 20*B*x^3 - 5*A^2*x^2 - 4*A*B*x - 8*B^2 - A^3)
            else:
                if odd(i):
                    m = int((i-1)/2)
                    return psi_odd(m)
                else:
                    m = int(i/2)
                    return psi_even(m)
        return calculator_of_psi(i)

    def theta(m):
        term1 = x*psi(m)^2
        term2 = psi(m+1)*psi(m-1)
```

```
    if odd(m):
        return (term1 - term2*(Ec))
    else:
        return (term1*(Ec) - term2)

def omega(m):
    return ((psi(m+2)*psi(m-1)^2 - psi(m-2)*psi(m+1)^2)/4)

def P(n):
    if odd(n):
        the_x = ((theta(n)) * (Ec))/(psi(n))^2
        the_y = omega(n)/psi(n)^3
    else:
        the_x = (theta(n))/((psi(n))^2 * (Ec))
        the_y = omega(n)/(psi(n)^3 * (Ec)^2)
    return (the_x,the_y)

def modpsi(function,psi):
    answer = (function).quo_rem(psi)[1]
    return answer

def daa(expression,q,PSI):
    #binaryexponent: q -> list of exponets of q represented in binary
    def binaryexponent(q):
        d = len(bin(q)[2:])-1
        lst = []
        for i in bin(q)[2:]:
            if int(i) == 1:
                lst.append(d)
            d -= 1
        return lst

    #help: expression,exponentlist,PSI - > x^q (mod PSI)
    def daahelp(expression,explist,PSI):
        totalanswer = 1
        for i in explist:
            answer = expression
            n = 0
            while n < i:
                answer = ((answer)^2).quo_rem(PSI)[1]
                n += 1
            totalanswer = (totalanswer * answer).quo_rem(PSI)[1]
        return totalanswer
    exponentlistan = binaryexponent(q)
    xqmodpsi = daahelp(expression,exponentlistan,PSI)
    return xqmodpsi
```

```
# X_tilde: q,L -> xtilde = numerator(x^(q^2) - x_qL)
def X_tilde(q,L):
    qL = (q).quo_rem(L)[1]
    PSI = psi(L)
    if odd(qL):
        x_tilde = (daa(x,(q^2),PSI)*(psi(qL))^2 - theta(qL))
    else:
        x_tilde = (daa(x,(q^2),PSI)*(psi(qL))^2*(Ec) - theta(qL))
    return modpsi(x_tilde,PSI)

# Xprime: q,L -> x' = x^(q^2) - x_qL (mod PSI)
def Xprime(q,L,PSI):
    qL = (q).quo_rem(L)[1]
    xq2 = daa(x,(q^2),PSI)
    if odd(qL):
        q_minus = int((q^2 - 1)/2)
        # Ec_minus = (Ec)^((q^2 - 1)/2)  (mod PSI)
        Ec_minus = daa(Ec,q_minus,PSI)
        Poly = Ec*((psi(qL))^3 *(Ec_minus) - omega(qL))^2
             - (X_tilde(q,L))^2 *(xq2* (psi(qL))^2 + theta(qL)) # nr 1
    else:
        q_plus = int((q^2 + 3)/2)
        # Ec_plus = (Ec)^((q^2 - 1)/2)  (mod PSI)
        Ec_plus = daa(Ec,q_plus,PSI)
        Poly = ((Ec_plus) *(psi(qL))^3 - omega(qL))^2
             - (X_tilde(q,L))^2 *(xq2 * (psi(qL))^2 * Ec + theta(qL)) # nr 2
    return modpsi(Poly,PSI)

# Xj_tilde: j,L -> Numerator = numerator(x' - (x_j)^q)
def Xj_tilde(j,L,PSI):
    qL = (q).quo_rem(L)[1]
    psi_j2q = daa(psi(j),2*q,PSI)
    theta_jq = daa(theta(j),q,PSI)
    xq2 = daa(x,q^2,PSI)

    if odd(qL):
        Ec_q2_1 = daa(Ec,(q^2 - 1)/2, PSI)

        if odd(j):
            xprimnumerator = (Ec*(Ec_q2_1*psi(qL)^3 - omega(qL))^2 - (xq2 * psi(qL)^2
                           - theta(qL))^2 *(xq2 * psi(qL)^2 + theta(qL)))
            xprimdenomenator = psi(qL)^2 *(x^(q^2) *psi(qL)^2 - theta(qL))^2

            Numerator = xprimnumerator *psi_j2q - theta_jq *xprimdenomenator
        else:
```

```
            Ec_q = daa(Ec,q,PSI)

            xprimnumerator = (Ec*(Ec_q2_1*psi(qL)^3 - omega(qL))^2 - (xq2 * psi(qL)^2
                           - theta(qL))^2 *(xq2 * psi(qL)^2 + theta(qL)))
            xprimdenomenator = psi(qL)^2 *(xq2 *psi(qL)^2 - theta(qL))^2

            Numerator = xprimnumerator *psi_j2q *Ec_q - theta_jq *xprimdenomenator
        else:
            Ec_q2_3 = daa(Ec,(q^2 + 3)/2, PSI)
            if odd(j):
                xprimnumerator = (Ec_q2_3 *psi(qL)^3 -omega(qL))^2 - (xq2 *psi(qL)^2 *Ec
                           - theta(qL))^2 *(xq2 *psi(qL)^2  *Ec + theta(qL))
                xprimdenomenator = (psi(qL)^2 *Ec *(xq2 *psi(qL)^2 *Ec -theta(qL))^2)

                Numerator = xprimnumerator *psi_j2q - theta_jq *xprimdenomenator
            else:
                Ec_q = daa(Ec,q,PSI)
                xprimnumerator = (Ec_q2_3 *psi(qL)^3 -omega(qL))^2 -(xq2 *psi(qL)^2 *Ec
                           - theta(qL))^2 *(xq2 *psi(qL)^2  *Ec + theta(qL))
                xprimdenomenator = (psi(qL)^2 *Ec *(xq2 *psi(qL)^2 *Ec -theta(qL))^2)

                Numerator = xprimnumerator *psi_j2q *Ec_q - theta_jq *xprimdenomenator
        return modpsi(Numerator,PSI)

    # Yprime: L -> y' = y^(q^2) - y_qL (mod PSI)
    def Yprime(L,PSI):
        qL = (q).quo_rem(L)[1]
        psi_ql3 = psi(qL)^3
        omega_ql = omega(qL)
        theta_ql = theta(qL)
        x_tilde2 = (X_tilde(q,L))^2
        x_tilde3 = (X_tilde(q,L))^3
        poly = Xprime(q,L,PSI)
        if odd(qL):
            Ec_q1 = daa(Ec,((q^2 - 1)/2),PSI)
            yprime = ((Ec_q1*psi_ql3 -omega_ql)*(theta_ql*x_tilde2 -poly)
                   -(omega_ql*x_tilde3))
        else:
            Ec_q3 = daa(Ec,((q^2 + 3)/2),PSI)
            yprime =((Ec_q3*psi_ql3 -omega_ql)*(theta_ql*x_tilde2 -poly)
                   -(omega_ql*x_tilde3))
        return modpsi(yprime,PSI)

    # Yj_tilde: j,L -> Numerator = numerator(y' - (y_j)^q)
    def Yj_tilde(j,L,PSI):
        qL = modpsi(q,L)
```

```
    x_tilde3 = (X_tilde(q,L))^3
    psi_j3q = daa(psi(j),3*q,PSI)
    omega_jq = daa(omega(j),q,PSI)
    psi_ql3 = (psi(qL))^3
    Y_tildeprime = Yprime(L,PSI)
    if odd(j):
        if odd(qL):
            Ec_q1 = daa(Ec,(q - 1)/2,PSI)
            Numerator = Y_tildeprime* psi_j3q - omega_jq*x_tilde3*psi_ql3*Ec_q1
        else:
            Ec_q3 = daa(Ec,(q + 3)/2,PSI)
            Numerator = Y_tildeprime* psi_j3q - omega_jq*x_tilde3*psi_ql3*Ec_q3
    else:
        if odd(qL):
            Ec_3q1 = daa(Ec,(3*q + 1)/2,PSI)
            Numerator = Y_tildeprime* psi_j3q*Ec_3q1 - omega_jq*x_tilde3*psi_ql3
        else:
            Ec_3q3 = daa(Ec,(3*q - 3)/2,PSI)
            Numerator = Y_tildeprime* psi_j3q*Ec_3q3 - omega_jq*x_tilde3*psi_ql3
    return modpsi(Numerator,PSI)

#L2: () -> a_2 = a (mod 2)
def L2(Ec,x,q):
    if gcd(Ec, x^q - x) == 1:
        a_2 = 1
    else:
        a_2 = 0
    return a_2

#Find_j: L -> j, such that x'= (x_j)^q with help of Xj_tilde.
def Find_j(L,PSI):
    for j in range(1,(L+1)/2):
        xj_tilde = Xj_tilde(j,L,PSI)
        if gcd(xj_tilde,PSI) != 1:
            return j
        else:
            pass

# w_function: L -> a_L , in the case that q = w^2
def w_function(L,PSI):
    qL = modpsi(q,L)
    w = 0
    for i in range(1,L):
        if IntegerModRing(L)(i^2) == qL:
            w = i
            break
```

```
    if w == 0:
        a_3 = 0
        return a_3
    else:
        xq = daa(x,q,PSI)
        if odd(w):
            #Xw = psi(w)^2 * (x^q - x) + psi(w+1)*psi(w-1)*(Ec)
            Xw = ((psi(w))^2 *xq - theta(w))
        else:
            #Xw = psi(w)^2 * (x^q - x)*(Ec) + psi(w+1)*psi(w-1)
            Xw = ((psi(w))^2 *xq *(Ec) - theta(w))
        if gcd(Xw,PSI) == 1:
            a_L = 0
            return a_L
        else:
            if odd(w):
                Yw = (Ec^((q - 1)/2)*(psi(w))^3 - omega(w))
            else:
                Yw = (Ec^((q + 3)/2)*(psi(w))^3 - omega(w))
            if gcd(Yw,PSI) == 1:
                a_L = modpsi((-2*w),L)
            else:
                a_L = modpsi((2*w),L)
            return a_L

# for_loop: primelist -> a_list , gives us the list of what a is mod each prime.
# (for example the first element in a_list is
# what a is mod the first element in primelist, and so on)
def for_loop(primelist,Ec,x,q):
    a_list = []
    for L in primelist:
        if L == 2:
            a_2 = L2(Ec,x,q)
            a_list.append(a_2)
        else:
            a_L = L_function(L,Ec)
            a_list.append(a_L)
    return a_list

# L_function: L,A,B -> a (mod L) , gives us what 'a' is congruent to
# modulo the input prime L.
# This function is the main function for a choosen prime
# and works according to Schoof's algorithm
# to determine a (mod L) with the help of the equation
# (Q_q)^2 - a* Q_q + q = 0 (where Q_q is the frobenius endomorphism)
def L_function(L,Ec):
```

```
        PSI = psi(L)
        qL = modpsi(q,L)
        gcd_xt_psi = gcd(X_tilde(q,L),PSI)
        if gcd_xt_psi == 1:
            #continue with them different
            j = Find_j(L,PSI)
            if gcd(Yj_tilde(j,L,PSI),PSI) != 1:
                return j
            else:
                return modpsi(L-j,L)
        else:
            #evaluate the w-function
            return w_function(L,gcd_xt_psi)

    def Chi_Rem_Thm(a_list,primelist):
        small_a = CRT_list(a_list,primelist)
        PI = 1
        for i in primelist:
            PI *= i
        if small_a > int(PI/2):
            small_a = small_a - PI
        N = q + 1 - small_a
        return N

    def makeglobal():
        global q
        global A
        global B

#-------The main program----------------------------------------------------------------------

    def mainprogram():
        makeglobal()
        discriminant = (4*A^3 + 27*B^2)
        if gcd(discriminant,q) == 1:
            primelist = PrimeList(q)
            a_list = for_loop(primelist,Ec,x,q)
            Number_of_points = Chi_Rem_Thm(a_list,primelist)
            print("Elliptic curve: y^2 = x^3 + ({})x + ({}) over F_{}".format(A,B,q))
            print("#E(Fq) =",Number_of_points)
            print("a",(q+1-Number_of_points))
            for i in range(len(primelist)):
                print("a =",a_list[i],"(mod {})".format(primelist[i]))
        else:
            print("x^3 + {}x + {}: define a singular curve".format(A,B))
```

```
######## End of functions ####################################################

#== Choose values for q (the field size) and A,B (the coefficients for the elliptic curve)==
    q = 49                    #<---------- Choose q
    Fq = GF(q,'z')
    R = PolynomialRing(Fq,'x')
    x = R.gen()
    A = Fq('2*z+1')            #<---------- Choose A
    B = Fq('4*z')              #<---------- Choose B
    Ec = x^3 + A*x + B
    mainprogram()
#======= End of program ============================================================

Schoofs_Algorithm()

-------------------------------------------------------
Examples of outputs from the program with given q,A,B:

For q = 49, A = 2*z + 1 and B = 4*z:

Elliptic curve: y^2 = x^3 + (2*z + 1)x + (4*z) over F_49
('#E(Fq) =', 52)
('a', -2)
('a =', 0, '(mod 2)')
('a =', 1, '(mod 3)')
('a =', 3, '(mod 5)')


For q = 101, A = 19 and B = 42:

Elliptic curve: y^2 = x^3 + (19)x + (42) over F_101
('#E(Fq) =', 99)
('a', 3)
('a =', 1, '(mod 2)')
('a =', 0, '(mod 3)')
('a =', 3, '(mod 5)')
('a =', 3, '(mod 7)')


For q = 121, A = 2 and B = 6:

Elliptic curve: y^2 = x^3 + (2)x + (6) over F_121
('#E(Fq) =', 140)
('a', -18)
('a =', 0, '(mod 2)')
('a =', 0, '(mod 3)')
```

```
('a =', 2, '(mod 5)')
('a =', 3, '(mod 7)')


For q = 169, A = 2*z and B = 6*z + 4:

Elliptic curve: y^2 = x^3 + (2*z)x + (6*z + 4) over F_169
('#E(Fq) =', 187)
('a', -17)
('a =', 1, '(mod 2)')
('a =', 1, '(mod 3)')
('a =', 3, '(mod 5)')
('a =', 4, '(mod 7)')
```