Elliptic Curves

Andreas Mars

April 18, 2006

Contents

0 Why study elliptic curves?

The history of elliptic curves goes back to ancient Greece and beyond. They appeared when studying so-called *Diophantine Equations*, where one is looking for integer and rational solutions to polynomial equations. But there are two different approaches to them, one is algebraic number theory, the other is the analysis of algebraic varieties. The algebraic number thoery uses properties of the rings and fields the solutions lie in, whereas algebraic varieties are geometric objects that can be studied.

Now, as we mentioned, there are different kinds of polynomial equations. For example, a linear equation in two variables x and y, such as $ax + by = c$, where at least one of a, b is different from zero, obviously has rational solutions. As it can easily be shown, it has solutions in $\mathbb{Z}$ if and only if the greatest common divisor of a and b divides c. So there is not much more to say about linear equations.

It becomes slightly more difficult when considering quadratic equations, but these have also proven to be fairly easy to analyse. The main tools here are the *Hasse-Minkowski-Theorem*[1], *Hensel's Lemma*[2] and the *law of quadratic reciprocity*, which give us a fairly good understanding of polynomial equations of degree 1 or 2.

However, raising the degree of the polynomial to 3 makes elliptic curves come into play. The focus of present research is on this topic. They have applications in different areas of mathematics, we are going to outline a few of them right now.

0.1 Number theory

As we will see in this paper, the set of points on elliptic curves define an abelian group. Of course, if an elliptic curve is defined over a finite field, the number of points on it is also finite. While in general, the number of points that lie on an elliptic curve is rather difficult to compute, there is an upper bound.

Theorem 0.1 (Hasse's Theorem). [3] *Let $\mathbb{F}_q$ be a finite field and Γ be an elliptic curve. Then the number of points on Γ satisfies*

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

Here $\#\Gamma(\mathbb{F}_q)$ denotes the number of points on the curve. But there are some algorithms used to compute the exact number of points on a curve. For example, one of them is Satoh's algorithm.

Furthermore, as mentioned above and to be shown below, we can endow $\Gamma(\mathbb{F})$ in a natural fashion with the structure of an abelian group. If viewed over a number field (a

[1] for the theorem and a proof see e.g. E. Selmer, A Course in Arithmetic, Springer Verlag, 1973, Chapter IV, Theorem 8.

[2] for the statement and a proof see e.g. J. H. Silverman, The Arithmetic of Elliptic Curves, Springer Verlag, 1986, Chapter IV, Lemma 1.2, p.112f.

[3] for a proof see e.g. J. H. Silverman, The Arithmetic of Elliptic Curves, Springer Verlag, 1986, Chapter V, Theorem 1.1, p131.

field which is an algebraic extension of $\mathbb{Q}$, the set of rational numbers), then its structure is simply the direct sum of two subgroups:

Theorem 0.2 (Mordell-Weil-Theorem). [4] *Let $\mathbb{F}$ be a number field. Then the group $\Gamma(\mathbb{F})$ is finitely generated. In particular,*

$$\Gamma(\mathbb{F}) \cong \Gamma_{tor}(\mathbb{F}) \times A,$$

where A is a free abelian group and $\Gamma_{tor}(\mathbb{F})$ is the maximal finite torsion subgroup.

In practise, the torsion subgroup is relatively easy to compute, but in general the rank of A or the group itself cannot be computed by a fixed algorithm.

0.2 Cryptography

The use of elliptic curves in cryptography goes back to *Neal Koblitz* and *Victor Miller*, who suggested their use independently of each other in 1985. In comparison to *RSA*-encryption, one may use smaller keys when encryption with elliptic curves is used in order to gain the same security level. This relies on the wide belief that the *elliptic curve discrete logarithm problem* is much harder to solve than the factorization of a composite number, which occurs when trying to decrypt a *RSA*-encrypted message without knowing the private key. We will explain the logarithm problem in section 1.3 about point addition.

As the US *National Institute for Standards and Technology* suggests that *RSA* with 1024-bit encryption is sufficient to use until 2010, the question arises, what to do when 2009 has passed. One possibility would be to enlarge the key sizes to be safe for another decade, but the cryptography with elliptic curves provides a serious alternative to that.

0.3 Fermat's Last Theorem

Devised by *Pierre de Fermat* in 1637, his last theorem (often also called his last conjecture) would become one of the most famous theorems in the history of mathematics. It states:

Theorem 0.3 (Fermat's Last Theorem). *Let n be an integer greater than 2, then the equation*

$$x^n + y^n = z^n$$

has no non-trivial integer solutions.

The number of erroneous proofs of Fermat's Last Theorem was tremendous. Even many famous mathematicians spent a lot of time (if not their whole life) working on it, but at the end the theorem remained a conjecture.

[4] for a proof see e.g. J. H. Silverman, The Arithmetic of Elliptic Curves, Springer Verlag, 1986, Chapter VIII, p189ff.

While extremely easy to state, this theorem remained unproved until 1995, when *Andrew Wiles* presented a proof[5]. In fact, Wiles did not prove Fermat's Last Theorem, but a part of the *Taniyama-Shimura-conjecture*, according to which every elliptic curve over $\mathbb{Q}$ is modular. In 1986, *Ken Ribet* showed that a solution to the equation $x^n + y^n = z^n$, for $n \geq 3$, would provide a counterexample to the Taniyama-Shimura-conjecture, thus would define a non-modular elliptic curve. This curve would be of the form

$$y^2 = x(x - a^n)(x + b^n).$$

As said above, Wiles did not prove the whole conjecture, but the part he proved already implies Fermat's Last Theorem. Finally, more than 350 years after Fermat claimed to have a proof, this theorem was proved.

Note that in the beginning, even Wiles's proof seemed to be erroneous. He spent seven years developing it secretly, sharing his thoughts only with one other Professor from Princeton. Working together for another year, they were able to fix the gap and establish the theorem.

1 Introduction

1.1 Basic definitions

Definition 1.1. A *cubic curve* Γ over a field $\mathbb{F}$ is defined by a polynomial of degree 3 in two variables.

We say that a point $P = (x, y) \in \mathbb{F} \times \mathbb{F}$ is an *element of this curve*, denoted by $\Gamma(\mathbb{F})$, if and only if it satisfies

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

where f is the polynomial defining the cubic curve.

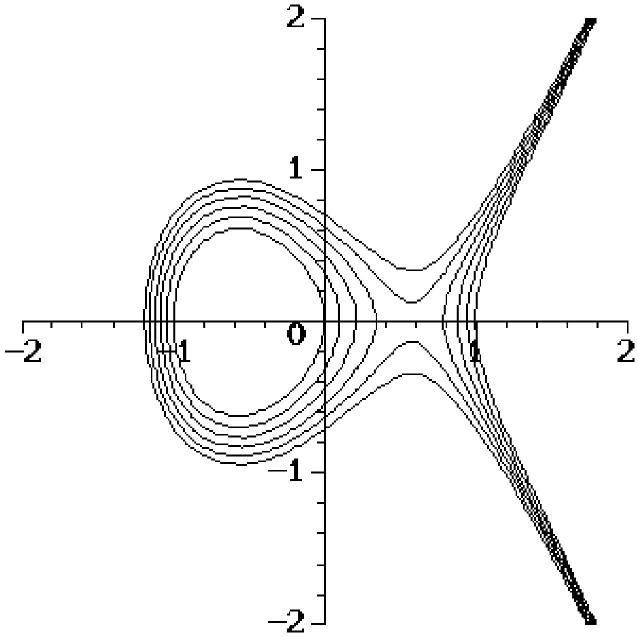
Definition 1.2. Let Γ be a cubic curve and let $\Gamma(\mathbb{F})$ be the set of points on it. Then a point $P \in \Gamma(\mathbb{F})$ where the fraction

$$\frac{\partial f / \partial x_P}{\partial f / \partial y_P}$$

is undefined, is called a *singular point*. A cubic curve without singular points is called an *elliptic curve*.

Therefore, a non-singular cubic curve has no self-intersections or cusps (Those would give two different tangents at those points, which we do not allow). Therefore elliptic curves are called *curves of genus* 1. We will see that non-singularity is a necessary condition for satisfying the group axioms. Here is a picture of a few examples of elliptic curves (over $\mathbb{R}$):

[5]Wiles, Andrew (1995). Modular elliptic curves and Fermat's last theorem, Annals of Mathematics (141) (1995)(3), 443-551



1.2 A binary operation

We shall see that the set of points on an elliptic curve can be endowed with a binary operation of point addition, which is associative and admits inverses such that the set of points together with this operation is a group.

Proposition 1.3. *Let Γ be an elliptic curve. Assume that $P, Q \in \Gamma(\mathbb{F})$ where P and Q are not necessarily distinct. Then there exists a unique point $R \in \Gamma(\mathbb{F})$, which lies on the line passing through both P and Q.*

Note that R is possibly the "line at infinity", see sections 2.2 and 2.3 for details.

Proof. Note that the "line" $\lambda : y = mx + b$ is well-defined by setting

$$m = \frac{\partial f/\partial y_P}{\partial f/\partial x_P}, \text{ if } P = Q.$$

If it happens that $P = (x, y)$ and $Q = (x, -y)$, with $x, y \in \mathbb{F}$, the line λ will be parallel to the y-axis. Therefore we define the third intersection of λ with Γ to be the point at infinity, compare Remark 1.4 and section 2.2.

On the other hand, if the y-coordinates of P and Q do not have the same absolute value, then $m = \frac{y_2 - y_1}{x_2 - x_1}$. But nominator and denominator are elements of the field, and so is m. Hence $d = y - mx$ is also an element of the field $\mathbb{F}$. Now by the definition of the line

λ, it meets the curve where $f(x, mx+b) = 0$. But $f(x, mx+b)$ is a polynomial of degree 3 in x, so we may write

$$f(x, mx+b) = a_0 + a_1 x + a_2 x^2 + a_3 x^3,$$

with $a_i \in \mathbb{F}$ for $i = 0, 1, 2, 3$. But then the sum of the three roots x_1, x_2 and x_3 equals $-\frac{a_2}{a_3}$ (provided that $a_3 \neq 0$), which again is an element of the field. Hence $x_3 = -x_1 - x_2 - \frac{a_2}{a_3} \in \mathbb{F}$. So $R := (x_3, mx_3 + b)$ is the (unique) third point on the line λ, as claimed. □

Remark 1.4. In the case that the leading coefficient in $f(x, mx+b)$ equals 0, we define the third point R to be the "line at infinity", which we will see to be a proper definition when viewing the elliptic curve in the projective space (see section 2.2).

Note that in the proof it was important to have the curve restricted to a non-singular curve. For example, if P is a self-intersection of a cubic curve, then $P * P$ could not be defined, since we would have two different tangents at P, both intersecting the curve in a third point, but they were different. Thus the binary operation would not be well-defined.

Definition 1.5. Let Γ be an elliptic curve. We define a binary operation on $\Gamma(\mathbb{F})$ by setting

$$\begin{aligned} * : \Gamma(\mathbb{F}) \times \Gamma(\mathbb{F}) &\rightarrow \Gamma(\mathbb{F}) \\ (P, Q) &\mapsto P * Q := R, \end{aligned}$$

where R is the third point on the line through P and Q.

Observation 1.6. Since there is a unique third on a line defined by two points on an elliptic curve, this operation is commutative by definition, since $P * Q = Q * P$ for all points $P, Q \in \Gamma(\mathbb{F})$.

Also, every set of three point on a line is uniquely determined, hence for all points $P, Q, R \in \Gamma(\mathbb{F})$:

$$P = Q * R \Leftrightarrow Q = R * P \Leftrightarrow R = P * Q.$$

So the operation $*$ is symmetric.

1.3 Addition in $\Gamma(\mathbb{F})$

In fact, the operation $*$ fails to be associative (this is easily verified), so we cannot use it as our group operation on the set of points on an elliptic curve. But we may use it to define an addition that turns $\Gamma(\mathbb{F})$ into a group.

Definition 1.7. Let $\Gamma(\mathbb{F})$ be the set of points on an elliptic curve Γ and fix a point $O \in \Gamma(\mathbb{F})$. Then we define another binary relation by putting

$$\begin{aligned} + : \Gamma(\mathbb{F}) \times \Gamma(\mathbb{F}) &\rightarrow \Gamma(\mathbb{F}) \\ (P, Q) &\mapsto P + Q := O * (P * Q). \end{aligned}$$

Our next aim is to verify, given the addition $+$ with respect to some point O, that O is the neutral element for $+$ and that all points have additive inverses.

Proposition 1.8. *Let $\Gamma(\mathbb{F})$ be the set of points on an elliptic curve Γ. Assume that the addition $+$ is defined in the above matter by a fixed point $O \in \Gamma(\mathbb{F})$. Then O is the neutral element of $+$, that is:*

$$(\forall P \in \Gamma(\mathbb{F})) : P + O = O + P = P.$$

Further, each point has an inverse with respect to $+$:

$$(\forall P \in \Gamma(\mathbb{F}))(\exists Q \in \Gamma(\mathbb{F})) : P + Q = O$$

Proof. Let $P \in \Gamma(\mathbb{F})$. Then

$$P + O = O * (P * O) = P,$$

since $+$ is commutative (Observation 1.6).

For the existence of inverses, again let $P \in \Gamma(\mathbb{F})$. Defining the point $Q := (O * O) * P$ gives us the additive inverse of P, since

$$Q + P = O * (Q * P) = O * (O * O) = O.$$

So $-P = Q$ exists. □

The only axiom left to verify for $(\Gamma(\mathbb{F}), +)$ to become an abelian group is the associativity of $+$.

Proposition 1.9. *The binary operation $+$ is associative, that is for all $P, Q, R \in \Gamma(\mathbb{F})$:*

$$P + (Q + R) = (P + Q) + R$$

Proof. In fact, this is not obvious, and the proof is rather lengthy. We invite the reader to verify this geometrically using algorithm 2.5 (for a proof see e.g. J. H. Silverman, The Arithmetic of Elliptic Curves, Springer Verlag, 1986, Chapter III, Proposition 2.2, p55.). □

Summarizing the results, we can state the following

Theorem 1.10. *Let Γ be an elliptic curve over a field $\mathbb{F}$. Further, let $\Gamma(\mathbb{F})$ be the set of points on Γ. Then $(\Gamma(\mathbb{F}), +, O)$ is an abelian group.*

Actually, as we have seen, the choice of $O \in \Gamma(\mathbb{F})$ is arbitrary, so after a first glance, one might say that a different choice of O defines a different operation. However, they are not completely different. For, if we fix another point $A \in \Gamma(\mathbb{F})$, then the map

$$P +_2 Q := P + Q - A$$

again defines an associative and commutative operation on the same set. So the affine transformation $X \mapsto X + A$, for $X \in \Gamma(\mathbb{F})$, does nothing than moving the origin, or the neutral element O onto $O + A$.

Going back to the section on cryptography, we see that if we fix a point $P \in \Gamma(\mathbb{F})$, then we can define kP for $k \in \mathbb{N}$ (and similarly for $k \in \mathbb{Z}$) by putting

$$k \cdot P := \underbrace{P + \cdots + P}_{k \text{ times}}, \quad (-k) \cdot P := -(\underbrace{P + \cdots + P}_{k \text{ times}}).$$

Now the logarithm problem mentioned in section 0.2 is to find the integer k given the points P and $Q = kP$. This is an *NP*-Problem, so the task is unsolvable in polynomial time. This fact is also used when using *RSA*-encryption, but the logarithm problem is believed to be even harder to solve than the factorization of a large natural number.

The aim of the next section is to establish a link between elliptic curves and Weierstrass equations, and we introduce the projective space $\mathbb{P}^n$ in which we can choose O such that the addition becomes easy to calculate.

2 Classification of elliptic curves

2.1 Weierstrass equations

Recall that an elliptic curve Γ over a field $\mathbb{F}$ is defined to be a polynomial in two variables of degree 3. However, it can be shown that every elliptic curve Γ can be described by another equation.

Definition 2.1. The polynomial

$$\Gamma : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

defines a curve in the projective space $\mathbb{P}^2$. This equation is said to be a *Weierstrass equation.*

Using non-homogeneous coordinates $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, we get the following equation:

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

If we further assume that $char(\mathbb{F}) \neq 2$, then we can simplify this equation by sending $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ into

$$\Gamma : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where $b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$.

Definition 2.2. Given a curve with the above representation, we define

$$\begin{aligned}
b_8 :=&\quad a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 :=&\quad b_2^2 - 24b_4,\\
\Delta :=&\quad -b_2^2b_8, -8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j :=&\quad \frac{c_4^3}{\Delta}.
\end{aligned}$$

The quantity Δ is called the *discriminant*, and j is called the *j-invariant* of the curve Γ.

The j-invariant gives rise to another property of elliptic curves, that we mention for completeness. The proposition states that two elliptic curves are equivalent (over the algebraic closure of the field) if and only if they have the same j-invariant.

If it also happens that $char(\mathbb{F}) \neq 3$, then the Weierstrass equation of Γ can be transformed into something even simpler. Hence, if $char(\mathbb{F}) \notin \{2, 3\}$, then we may assume Γ to be given by an equation of the form

$$\Gamma : y^2 = x^3 + Ax + B,$$

where A and B are results of the appropiate transformation. In this case, the discriminant and the j-invariant of Γ can be calculated by

$$\Delta = -16(4A^3 + 27B^2),\ j = \frac{1728(4A^3)}{\Delta}.$$

We shall see now that a non-singular curve Γ always has discriminant different from 0 and vice versa.

Proposition 2.3. *Let Γ be a curve defined by a Weierstrass equation. Then che curve Γ is an elliptic curve (i.e. a non-singular curve) if and only if the discriminant Δ is different from* 0*.*

Proof. We omit the proof here (for the proof see J. H. Silverman, The Arithmetic of Elliptic Curves, Springer Verlag, 1986, Chapter III, Proposition 1.4 (a) (i), p50). □

2.2 The projective space

We are now going to view elliptic curves in the projective space $\mathbb{P}^2$. First, we need to define what we mean by a projective space.

Definition 2.4. The projective n-dimensional space $\mathbb{P}^n$ over a field $\mathbb{F}$ is defined as the set of $(n+1)$-tuples $(x_0, \ldots, x_n) \in \mathbb{F}^{n+1}$, where at least one $x_i \neq 0$ and we identify two elements if they are a scalar multiple of each other. The equivalence class of $\{\lambda(x_0, \ldots, x_n), \lambda \in \mathbb{F}\}$ is denoted by $[x_0, \ldots, x_n]$, where these $x_0, \ldots, x_n$ are called the *homogeneous coordinates* of that point.

For example, if we work in $\mathbb{R}^3$, then every non-zero point $a \in \mathbb{R}^3$ defines a 1-dimensional linear subspace. The intersection of this line with the plane $\{(x, y, z) \in \mathbb{R}^3 : z = 1\}$, gives us a well-defined map from $\mathbb{R}^3$ to $\mathbb{P}^2$, where a line parallel to the plane is identified with the point $[0, 1, 0] \in \mathbb{P}^2$, the "point at infinity" which has already been mentioned above. We thus see that a point in $\mathbb{P}^2$ can be uniquely identified with a line in $\mathbb{R}^3$, and vice versa.

More general, an n-dimensional linear subspace of $\mathbb{P}^m$ (assuming that $n \leq m$) uniquely defines an $(n+1)$-dimensional linear subspace in $\mathbb{F}^{m+1}$. This also holds in the reverse direction.

2.3 The neutral element

Now, that we have established a connection between elliptic curves and Weierstrass equations and we introduced the projective space, let us review the results from section 1.3.

Recall that the main result of section 1.3 was that the set of points on an elliptic curve Γ has the algebraic structure of an abelian group, denoted $(\Gamma(\mathbb{F}), +, O)$. The most surprising result was that we may choose the neutral element O as an arbitrary point in $\Gamma(\mathbb{F})$.

However, a good choice of O can make life easier. That is, the operation $+$ gives a fairly easy geometric algorithm to compute the sum of two point P and Q if $O := [0, 1, 0] \in \mathbb{P}^2$, that is if O is the point at infinity. Then adding two points is done by the following algorithm.

Algorithm 2.5 (adding points on elliptic curves)**.** Let Γ be an elliptic curve, and $\Gamma(\mathbb{F})$ be the set of points on it. Choose O to be the point at infinity, and let $P, Q \in \Gamma(\mathbb{F})$. Then the sum $P + Q$ can be computed geometrically as follows:

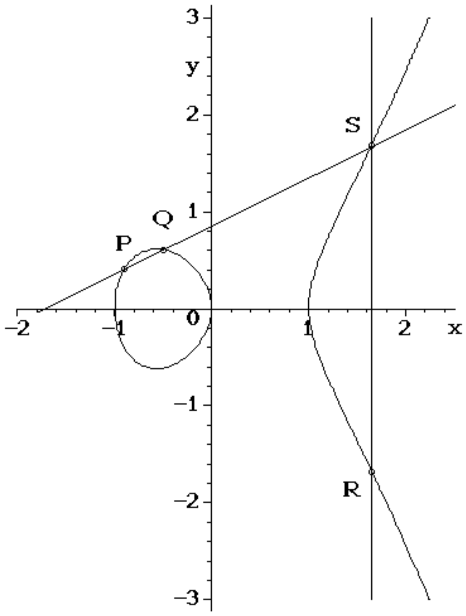
1. Draw the (unique) line λ that intersects Γ at the points P and Q.

2. Find the (unique) third point S where λ intersects Γ. Note that $S = P * Q$.

3. Draw another line μ, intersecting Γ at R and which is parallel to the y-axis (i.e. its intersections are S and O, the point at infinity).

4. The sum $R = P + Q$ is now the third intersection of μ with Γ.

Here is an example of that algorithm:



3 Isogenies

3.1 Definition

As one could have suspected, the operations of addition and inversion of the abelian group $\Gamma(\mathbb{F})$ are in fact more than just group operations, the next theorem will give us a further property of them.

Theorem 3.1. *Let Γ be an elliptic curves and $P_1, P_2, P \in \Gamma(\mathbb{F})$. Then the group law operations*

$$(P_1, P_2) \mapsto P_1 + P_2, \;\; P \mapsto -P$$

define morphisms.

Having noticed this fact, we can turn to isogenies.

Definition 3.2. Let Γ_1 and Γ_2 be elliptic curves. A homomorphism $\varphi : \Gamma_1 \to \Gamma_2$ is called an *isogeny* if and only if $\varphi(O_1) = O_2$, where O_1 and O_2 are the neutral elements of the curves Γ_1 and Γ_2, respectively.

It can be shown that for any isogeny either $\varphi(\Gamma_1) = \{O\}$ or $\varphi(\Gamma_1) = \Gamma_2$ holds. Thus any non-trivial isogeny is an epimorphism onto Γ_2.

3.2 Another group and a ring

Recalling Theorem 1.10, we note that isogenies are homomorphisms between (abelian) groups, thus the isogenies itself carry an algebraic structure.

Definition 3.3. Let Γ_1 and Γ_2 be elliptic curves. Then $\mathrm{Hom}(\Gamma_1, \Gamma_2)$ is defined to be the set of all isogenies from Γ_1 to Γ_2.

For two isogenies $\varphi, \psi \in \mathrm{Hom}(\Gamma_1, \Gamma_2)$ we define

$$(\varphi + \psi)(P) := \varphi(P) + \psi(P).$$

Lemma 3.4. *Under this addition law,* $\mathrm{Hom}(\Gamma_1, \Gamma_2)$ *is a group. Further, if* $\Gamma = \Gamma_1 = \Gamma_2$, *then* $\mathrm{End}(\Gamma) := \mathrm{Hom}(\Gamma, \Gamma)$ *which, together with the mutiplication law*

$$(\varphi\psi)(P) = \varphi(\psi(P)),$$

forms a ring.

Proof. This is geometrically obvious, we invite the reader to check the group and ring axioms. □

Further, the automorphism group $\mathrm{Aut}(\Gamma) \subseteq \mathrm{End}(\Gamma)$ consists of the invertible isogenies.

Example 3.5. For each $k \in \mathbb{Z}$ we can define the isogeny $\varphi_m : \Gamma \to \Gamma$ by defining $\varphi_m(P) = mP$ for all $P \in \Gamma(\mathbb{F})$ (we set $\varphi_0(P) = O$ for all P). Hence we also can regard $\mathrm{Hom}(\Gamma_1, \Gamma_2)$ as a $\mathbb{Z}$-module.

Proposition 3.6. *The map* φ_m *is non-constant provided that* $m \neq 0$.

Proof. First, one shows that if $char(\mathbb{F}) \neq 2$ and $\varphi_2 \equiv \varphi_0$ implies that $\Delta = 0$, so Γ was not an elliptic curve, which is a contradiction. Secondly, using the fact that $\varphi_{mn} = \varphi_m \circ \varphi_n$, one shows that there is a point P of order 2, that is $\varphi_2(P) = O$. But then for m odd, obviously $\varphi_m(P) = P \neq O$.

For $char(\mathbb{F}) = 2$, one finds a point of order 3. □

Theorem 3.7. *Let* Γ, Γ_1 *and* Γ_2 *be elliptic curves.*

1. *The group of isogenies* $\mathrm{Hom}(\Gamma_1, \Gamma_2)$ *is a torsion-free* $\mathbb{Z}$*-module.*
2. *The endomorphism ring* $\mathrm{End}(\Gamma)$ *is an integral domain.*

Proof. We assume that for $\varphi \in \mathrm{Hom}(\Gamma_1, \Gamma_2)$ and for $k \in \mathbb{Z}$

$$\varphi_k \circ \varphi \equiv \varphi_0.$$

Now by Propostion 3.6, we see that either $k = 0$ or $\varphi \equiv \varphi_0$, so $\mathrm{Hom}(\Gamma_1, \Gamma_2)$ is torsion-free.

This result shows that $\mathrm{End}(\Gamma)$ has characteristic 0. But now, if $\varphi, \psi \in \mathrm{End}(\Gamma)$ and $\varphi \circ \psi \equiv \varphi_0$, then either one must be the constant map. Hence $\mathrm{End}(\Gamma)$ is an integral domain. □

As we see from these results, elliptic curves contain even more structure than announced in the introduction. The isogenies of two different groups also form a group, and the isogenies from one curve to itself even carry a ring structure which can be investigated.

Finally, we now have a glance into further analysis of elliptic curves using isogenies. In fact, one uses the maps φ_m as discussed above to study the *torsion subgroup* of $\Gamma(\mathbb{F})$. These are all points such that $\varphi_m(P) = O$. Note that in general the torsion groups are different for different integers m.

Further, by some properties that will not be discussed in this paper, one can deduce the structure of the (finite) torsion group for a fixed n.

Another main result is that any homomorphism between two elliptic curves can be decomposed into an isogeny and a translation.

But this is beyond the scope of this paper.