University of South-Eastern Norway

Faculty of Technology, Natural Sciences and Maritime Sciences

Master's Thesis

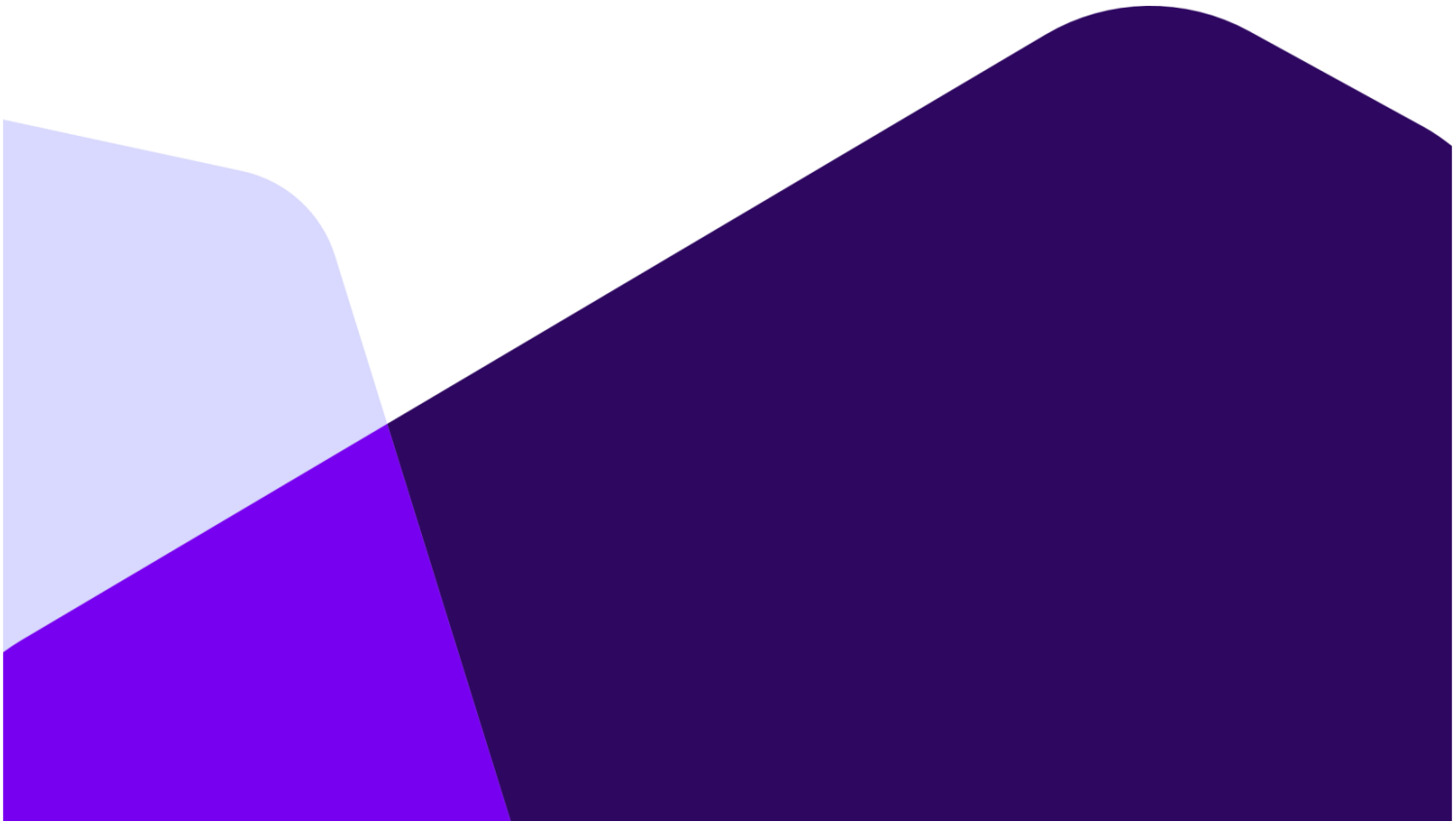
Lektorutdanning i Realfag (LUR)

Master’s level teacher programme in natural sciences and technology

Spring 2024

Håvard Skjæveland

Elliptic Curves and Discrete Dynamical Systems



Contents

Dedication and Acknowledgments

This paper is dedicated to my wife, Jovana, my son, Einar Sergej, and my daughter, Inga Danica. I am especially thankful to my wife for her patience and kind words of encouragement during the (often difficult) writing process.

I would also like to thank my supervisor, Daniel Larsson, for his insights, encouragement, and most of all, for making himself available as much as he has. He is very generous with his time, and that has been a huge help in this process.

Abstract

This paper gives an introduction to elliptic curves and discrete dynamical systems. It lays out the foundations of the theory of elliptic curves, along with important concepts like torsion points and isogenies, and makes heavy use of the John Cremona Database of Elliptic Curves. For dynamical systems, this paper gives an introduction to them, along with concepts like (in)stability, periodicity, and Lattès maps.

Introduction

I wrote this paper as an introduction to the two topics in the title, namely elliptic curves and discrete dynamical systems. It's intended to be read in a straight-forward way, and hints at potential uses in cryptography.

The reader should have some familiarity with abstract algebra (in particular groups and fields) and a general notion of concepts and terminology in mathematics, but beyond that much of what is needed will be explained along the way.

This paper first explores elliptic curves, and gives an overview of the development from general cubic equations in two dimensions, to general elliptic curves, through to elliptic curves in Weierstrass model, which is the type of elliptic curve which is the main focus of this paper.

Secondly, this paper goes into some detail about dynamical systems, in particular the logistic map. It gives a few other examples of dynamical systems, but mainly focuses on giving examples of different variations on the logistic map.

Thirdly, this paper briefly touches on Lattès maps, giving the formal definition of a Lattès map, together with an example. This part also ties together the two threads in the paper (broadly, elliptic curves and dynamical systems) by noting that the definition of Lattès maps involves elliptic curves, and the dynamical evolution over time of points on these curves.

The illustrations are generated with the free graphing tool Desmos for elliptic curves, and WolframAlpha's tool "CobwebPlot" by Paul Abbott for the cobweb plots.

Chapter 1

Cubic Curves, Elliptic Curves, and Weierstrass Model

1.1 Generalizing from Cubics to Weierstrass Model

Note: In this document we will consistently refer to plane curves (i.e. curves in two variables) as simply curves for the sake of brevity. We will not consider curves in space or higher dimensions.

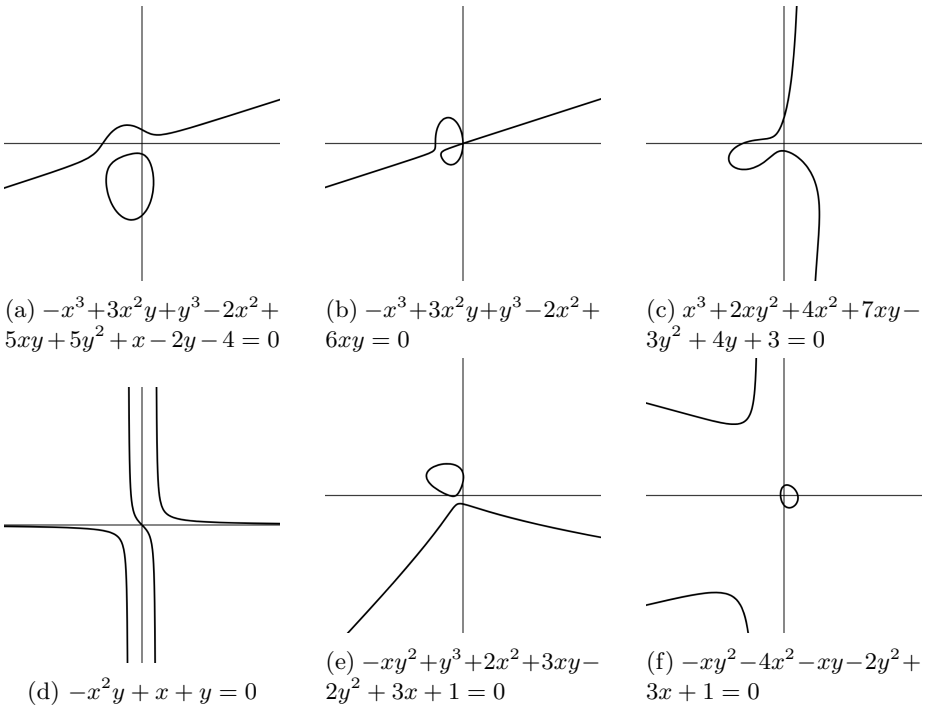
To begin with, we will investigate how to go from a general cubic curve, via general elliptic curves, to the specifics of elliptic curves expressed in Weierstrass form. A general cubic curve is defined as follows.

Definition 1.1.1 (Cubic curve)**.** A *cubic curve* is a polynomial in x and y of order (or degree) 3 with coefficients from a field K, usually expressed in the form $f(x, y) = 0$. Expanding this, we get

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0.$$

To illustrate how cubic curves look and behave, consider the few following examples.

Example 1.1.1 (Some cubic curves)**.** See Figure 1.1 for some examples.



(a) $-x^3+3x^2y+y^3-2x^2+5xy+5y^2+x-2y-4=0$

(b) $-x^3+3x^2y+y^3-2x^2+6xy=0$

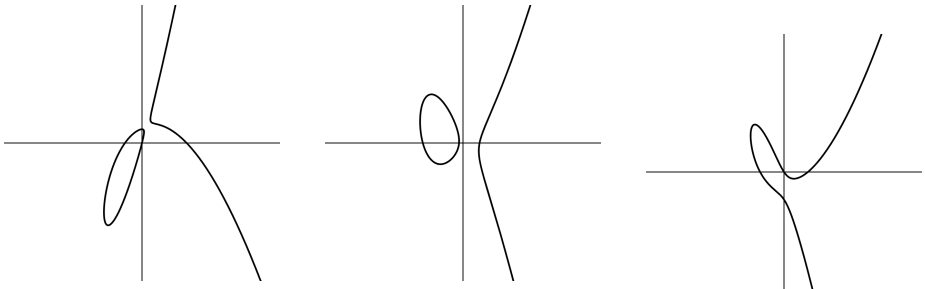
(c) $x^3+2xy^2+4x^2+7xy-3y^2+4y+3=0$

(d) $-x^2y+x+y=0$

(e) $-xy^2+y^3+2x^2+3xy-2y^2+3x+1=0$

(f) $-xy^2-4x^2-xy-2y^2+3x+1=0$

Figure 1.1: Some examples of general cubic curves.



(a) $y^2 - 4xy - y = x^3 - 2x^2 - 4x$ (b) $y^2 + xy + a_3y = x^3 + 2x^2 - 3x - 1$ (c) $y^2+3xy+2y = x^3-3x$

Figure 1.2: Some examples of elliptic curves, varying a_1, a_2, a_3, a_4, and a_6.

The curves are somewhat chaotic, and there are no "nice" symmetries, so we will move on to elliptic curves, which, as we will see, are more specific in nature than general cubics.

Definition 1.1.2 (Elliptic curve and Weierstrass model)**.** An *elliptic curve* is an algebraic curve defined over a field K with points in K^2 (the Cartesian product of K with itself). A general elliptic curve can be described by the equation

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

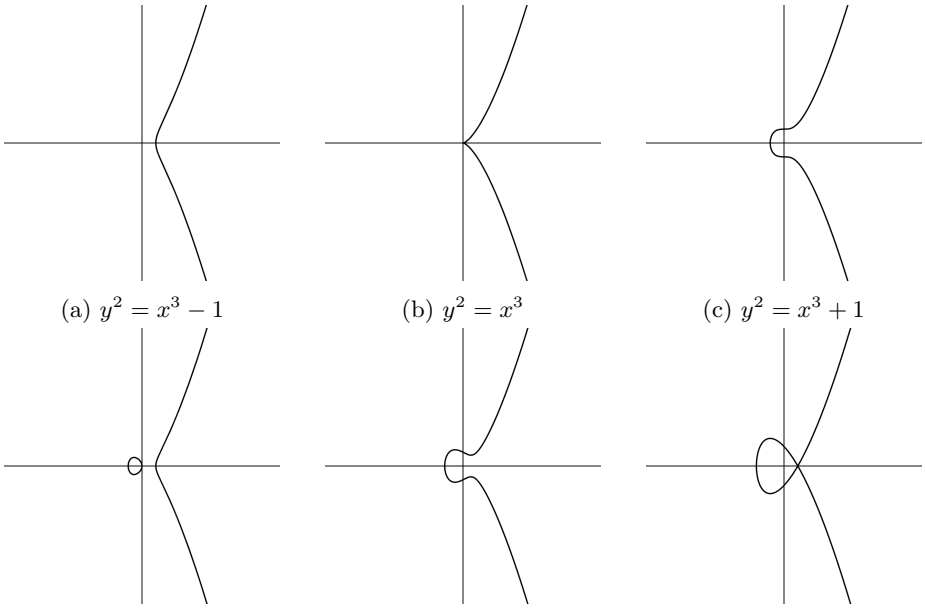
(There is no a_5 purely for historical reasons.) If the characteristic of the field K is different from 2 and 3, the curve can be described by the equation

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

known as *Weierstrass model*, with the coefficients from the field K. Note that in general, $a \neq a_4$ and $b \neq a_6$. In addition to the points in K^2, an elliptic curve also includes a special "point at infinity," denoted by the infinity symbol $\infty \stackrel{\text{def}}{=\!=} \{\infty\}$. It's not a part of K^2 itself, but it's helpful to think of it as infinitely far away from the y-axis.

Example 1.1.2 (Some elliptic curves)**.** See Figure 1.2 for some examples. Notice that these particular curves are not symmetric about the horizontal axis.

Example 1.1.3 (Some elliptic curves in Weierstrass form)**.** See Figure 1.3 for some examples. Notice that (b) has a cusp and (f) has a crossing (called a *crunode* or, in modern language, simply a *node*). These two are examples of *singular* elliptic curves.



(a) $y^2 = x^3 - 1$ (b) $y^2 = x^3$ (c) $y^2 = x^3 + 1$

(d) $y^2 = x^3 - x$ (e) $y^2 = x^3 - x + 1$ (f) $y^2 = x^3 - 3x + 2$

Figure 1.3: Some examples of elliptic curves in Weierstrass form, varying a and b.

Notice also that unlike general elliptic curves, curves in Weierstrass form *are* symmetric about the horizontal axis.

1.2 Addition of Points on Elliptic Curves

There are some operations we can perform on the points of an elliptic curve, most notably addition of two points. Geometrically, adding two points of an elliptic curve can be thought of as drawing a straight line between the two points, and having the negation of the vertical component of the intersection point with the curve itself be the result of this addition. It is a well-known fact about elliptic curves that this line is guaranteed to intersect the curve at a third point.

Note that some sources use the regular addition sign ($+$) whereas other sources use the asterisk ($*$) to denote this operation. We will use the regular addition sign.

Addition of points on elliptic curves is defined in a way such that elliptic curves form an abelian group, namely that addition should be commutative. This paper doesn't show the derivation of the addition algorithm, but merely states it.

A note on notation: Points in the projective plane $\mathbb{P}^2$ are usually given as the triplet

$$P = (a : b : c).$$

If $c \neq 0$ we can homogenize point and get

$$P = \left(\frac{a}{c} : \frac{b}{c} : 1\right) = (a' : b' : 1).$$

Thus, points not at infinity will be of the form $(a' : b' : 1)$ and the point at infinity can be described as $\infty = (0 : 1 : 0)$. We can therefore denote points not at infinity as simply $(x : y)$, and the point at infinity by the usual ∞ symbol.

Definition 1.2.1 (Addition of points on elliptic curves)**.** Let E be an elliptic curve in Weierstrass form,

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

and let $P_1 = (x_1 : y_1)$ and $P_2 = (x_2 : y_2)$ be points on E. First note that if $x_1 = x_2$, then this implies that $y_1 = -y_2$, since elliptic curves in Weierstrass

form are always symmetric about the x-axis. Furthermore, addition of such points always lead to the point at infinity, so $P_1 + P_2 = \infty$. Otherwise, we will define the quantities

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1}, & \nu &= \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}, & &\text{if } x_1 \neq x_2 \\ \lambda &= \frac{3x_1^2 + a}{2y_1}, & \nu &= \frac{-x_1^3 + ax_1 + 2b}{2y_1}, & &\text{if } x_1 = x_2. \end{aligned}$$

By these quantities, $y = \lambda x + \nu$ is the line going through P_1 and P_2, or the line tangential to both P_1 and P_2 if $P_1 = P_2$. The sum of these points can now be given by

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2 : -\lambda^3 + \lambda x_1 + \lambda x_2 - \nu).$$

In the special case that $P_1 = P_2 = P$, we use the notation

$$P + P + \ldots + P = [N]P,$$

where N is the number of times we add the point to itself.

Using this definition of addition of points, we can derive an explicit formula for adding points to itself, the so-called *duplication formula*. Deriving it is outside the scope of this paper, so here we merely state it.

Definition 1.2.2 (Duplication formula)**.** Given an elliptic curve E in Weierstrass form, $E : y^2 = x^3 + ax + b$, and a point $P = (x : y)$, adding this point to itself is known as the *duplication formula*, and is given by

$$[2]P = \left(\frac{x^4 - 2bx^2 + b^2}{4y^2} : \frac{x^6 + 2ax^5 + 5bx^4 - 5b^2x^2 - 2ab^2x - b^3}{8y^3} \right).$$

Next, we cover some special kinds of points, namely *torsion points*. These are points which for some finite number of iterations eventually come to rest at the point at infinity. A more precise definition follows.

1.3 Torsion points and Isogenies

Note: All examples involving elliptic curves taken from Cremona's database of elliptic curves will be labeled by the identifier string of the corresponding elliptic curve. In addition, when used in the examples themselves, the elliptic curve in question will have its Cremona label as a subscript, e.g. E_{11a3}. Its corresponding Weierstrass form will similarly be denoted by W_{11a3}. All calculations in the examples are done using SageMath.

Definition 1.3.1 (Torsion points)**.** A *torsion point* is a point on an elliptic curve such that $[N]p = \infty$ for some natural number $N \geq 2$. The order of the torsion point is N, and we call such points N-torsion points for a given N.

The set of all torsion points for a given elliptic curve E and a given N is denoted

$$E[N] \stackrel{\text{def}}{=\!=} \{P \in E \mid [N]P = \infty\}.$$

The set of *all* torsion points for a given elliptic curve E, regardless of N, is quite naturally the union of all of the N-torsion points of the given elliptic curve E, and is denoted

$$E_{\text{tor}} = \bigcup_{N \geq 2} E[N].$$

Example 1.3.1 (Trivial torsion point)**.** The point at infinity, ∞, is always a torsion point, since $\infty + \infty = \infty$, and is in fact called simply the *trivial torsion point*. It is also an N-torsion point for all $N \in \mathbb{N}$, since

$$\infty + \infty + \ldots + \infty = \infty$$

whenever you add ∞ to itself N times.

Example 1.3.2 (Cremona `80a1`)**.** Consider the elliptic curve

$$E_{\texttt{80a1}} : y^2 = x^3 - 7x + 6.$$

It has the torsion points

$$E_{\texttt{80a1}}[N] = \{(-3:0), (1:0), (2:0)\}.$$

The first point is of order 2 because $(-3:0) + (-3:0) = \infty$. It turns out that all the other torsion points on this particular elliptic curve are also of order 2, and so in fact the above set should be written as

$$E_{\texttt{80a1}}[2] = \{(-3:0), (1:0), (2:0)\}$$

and properly referred to as the curve's 2-torsion points.

Example 1.3.3 (Cremona `20a1`)**.** Consider the elliptic curve

$$E_{\texttt{20a1}} : y^2 = x^3 + x^2 + 4x + 4$$

and its corresponding Weierstrass model

$$W_{\texttt{20a1}} : y^2 = x^3 + 4752x + 127872.$$

It has the torsion points

$$E_{\texttt{20a1}}[N] = \{(-1:0), (0:\pm 2), (4:\pm 10)\}.$$

Of these, one is of order 2, two are of order 3, and two are of order 6, so we have

$$\begin{aligned} E_{\texttt{20a1}}[2] &= \{(-1:0)\} \\ E_{\texttt{20a1}}[3] &= \{(0:\pm 2)\} \\ E_{\texttt{20a1}}[6] &= \{(4:\pm 10)\}. \end{aligned}$$

Looking at the torsion points of its Weierstrass model, we have

$$\begin{aligned} W_{\texttt{20a1}}[2] &= \{(-24:0)\} \\ W_{\texttt{20a1}}[3] &= \{(12:\pm 432)\} \\ W_{\texttt{20a1}}[6] &= \{(156:\pm 2160:1)\}. \end{aligned}$$

This example illustrates that even though the torsion points of an elliptic curve and its corresponding Weierstrass model are different, they are still of corresponding order. Note also that this implies that $E_{\texttt{20a1}} \simeq \mathbb{Z}/6$.

We now come to an aspect of elliptic curves, in particular connections between elliptic curves, that have important applications for cryptography, namely isogenies.

Definition 1.3.2 (Isogeny)**.** An *isogeny* between two elliptic curves E and E' is a morphism $f : E \to E'$ such that

$$f(\alpha \underset{E}{+} \beta) = f(\alpha) \underset{E'}{+} f(\beta) \qquad \text{and} \qquad f(\underset{E}{\infty}) = \underset{E'}{\infty},$$

where $\underset{E}{+}$ and $\underset{E'}{+}$ are the usual addition of points for the elliptic curves E and E', respectively, and $\underset{E}{\infty}$ and $\underset{E'}{\infty}$ are the points at infinity for E and E', respectively.

If an isogeny is also one-to-one, it's called an *isomorphism*.

All calculations related to isogenies in the following examples are calculated using SageMath. An easy way to generate an explicit isogeny is to consider

Example 1.3.4 (Cremona `80a1`, revisited)**.** Consider the elliptic curve

$$E_{\texttt{80a1}} : y^2 = x^3 - 7x + 6.$$

There exist isogenies between `80a1` and several other elliptic curves, enumerated below with its Cremona label.

$E_{\texttt{20a1}} : y^2 = x^3 + x^2 + 4x + 4$ (This is the curve from Example 1.3.3)
$E_{\texttt{20a2}} : y^2 = x^3 + x^2 - x$
$E_{\texttt{20a3}} : y^2 = x^3 + x^2 - 36x - 140$
$E_{\texttt{20a4}} : y^2 = x^3 + x^2 - 41x - 116$

The fact that the letter `a` appears in all of these curves is no coincidence, but a deliberate choice on the part of the authors of the Cremona Database; it describes the isogeny class.

Although it is in general very hard to generate an explicit formula for an isogeny between two elliptic curves, it is nonetheless possible. We can generate a cyclic subgroup of E from one of its torsion points, and choose a point from that list as a basis for an isogeny, and we use the following theorem to justify it. ([Lar24])

Theorem 1.3.1. *Let $f : E \to E'$ be an isogeny. Then f is surjective over the algebraic closure of the ring we are working with, with finite kernel, i.e.,*

$$\#\ker(f) < \infty.$$

Given a finite subgroup $g \subset E$ there exists a unique isogeny $f_g : E \to E_g$ such that $g = \ker(f_g)$. Furthermore, since f is surjective, we have that $E_g \simeq E/g$.

The degree of f is the number of elements in its kernel, and f is an N-isogeny where $N = \#\ker(f)$.

SageMath can help us calculate many isogenies between these curves, but here we present only one of them for illustration purposes.

$$\phi_1 = \frac{x^8 + 2x^7 - 3x^6 + 5x^5 - 5x^4 + 3x^3 - 4x^2 - 3x + 3}{x^7 + 2x^6 + 2x^5 - 4x^4 - 4x^3 + 2x + 3}$$

Note that ϕ is a rational map, and that in general it can become very complicated. This particular isogeny was generated with SageMath in Python in the following way:

```
E = EllipticCurve(GF(11), '80a1'); # Instantiate an elliptic curve with
                                   # Cremona label '80a1' over a finite field
                                   # of size 11.

E.gens();                          # Returns the generators for the curve.

P = E(10, 10);                     # Choose the first point from the list
                                   # above.

phi = E.isogeny(P);                # Define an isogeny based on the point P

phi.rational_maps();               # Outputs the rational maps. The first one
                                   # is the one used in the example above.
```

Chapter 2

Iteration of functions

2.1 Dynamical Systems

We are now ready to look at dynamical systems, and we will begin with a couple of definitions. Firstly, what a dynamical system is, mathematically, and then define orbits, periodicity, and fixed points, and finally Lattès maps. The definitions in this section are essentially verbatim from [Sil07].

Definition 2.1.1 (Dynamical system)**.** A *dynamical system* is composed of a set S and a function $\phi : S \to S$. In other words, it maps S to itself. A common notation for composition of such functions is

$$\phi^n = \underbrace{\phi \circ \phi \circ \cdots \circ \phi}_{n \text{ times}} = n^{th} \text{ iterate of } \phi$$

(By convention, ϕ^0 is the identity map on S.)

Definition 2.1.2 (Orbits, periodicity, and fixed points)**.** The *(forward) orbit* of a point $\alpha \in S$ is defined as the set

$$\mathcal{O}_\phi(\alpha) = \mathcal{O}(\alpha) = \{\phi^n(\alpha) \mid n \geq 0\}$$

A point $\alpha \in S$ is called *periodic* if $\phi^n(\alpha) = \alpha$ for some $n \geq 1$. The smallest such n is called the *exact period* of α. The point α is called *preperiodic* if some

iterate ϕ^m is periodic. We denote the sets of periodic and preperiodic points (respectively) by

$$\begin{aligned}\operatorname{Per}(\phi, S) &= \{\alpha \in S \mid \phi^n(\alpha) = \alpha \text{ for some } n \geq 1\},\\ \operatorname{PrePer}(\phi, S) &= \{\alpha \in S \mid \phi^{m+n}(\alpha) = \phi^m(\alpha) \text{ for some } n \geq 1, m \geq 0\}\\ &= \{\alpha \in S \mid \mathcal{O}_\phi(\alpha) \text{ is finite}\}.\end{aligned}$$

A *fixed point* is a point where the exact period is 1.

To see how these definitions fit in to the underlying mathematics, we'll look at a few examples. First, some "trivial" examples (in the sense that they are compact and easy to follow, yet don't produce much in the way of actual dynamics), and then at the *logistic map*, which is very dynamic.

Example 2.1.1 (Two elements, surjective map)**.** Let $S = \{a, b\}$ and $\phi(a) = \phi(b) = a$. Here a is periodic with an exact period of 1 (which means a is also a fixed point), and b is preperiodic. The orbit of a is $\mathcal{O}_\phi(a) = \{a, a, \ldots\}$ and the orbit of b is $\mathcal{O}_\phi(b) = \{b, a, a, \ldots\}$

Example 2.1.2 (Three elements, injective map)**.** Let $S = \{a, b, c\}$ and $\phi(a) = b$, $\phi(b) = c$, and $\phi(c) = a$ (each element gets mapped to the next one in the set, and the last gets mapped to the first). Here, all points are periodic, and all points have the same exact periodicity, namely 3.

The orbits of all the points are essentially the same, just shifted by one element. We'll take the orbit of a as an example: $\mathcal{O}_\phi(a) = \{a, b, c, a, \ldots\}$.

Example 2.1.3 (Attraction/expulsion from the origin)**.** Let $S = \mathbb{R}$ and $\phi(\alpha) = c\alpha$ where α is an arbitrary point in S and c is a positive real constant. For $c = 1$ this of course reduces ϕ to the identity map, and the point α doesn't go anywhere. For $c > 1$, all points fly away from the origin, and for $0 < c < 1$, all points gradually get closer to (but will never reach) the origin.

The only case where the points in S can be periodic is when $c = 1$, with $|\operatorname{Per}(\phi, S)| = \infty$. For $c \neq 1$, $|\operatorname{Per}(\phi, S)| = \varnothing$.

For the following example (2.1.4) we need a definition of a *cobweb diagram*, sometimes called simply a *web diagram*, for its resemblance to a spider's web.

Definition 2.1.3 (Cobweb diagram)**.** A *cobweb diagram* (sometimes also called a *Lémeray diagram* or *Verhulst diagram*) is a way to visualize the evolution of a single-variable, single-valued function. (For the sake of this definition, let that function be $\phi : \mathbb{R} \to \mathbb{R}$.)

The nth value is plotted along the horizontal axis and the $n+1$st value along the vertical axis. In addition, the function operating on the initial value is plotted on the resulting plane, along with a diagonal line. The algorithm for producing the diagram is as follows:

1. Draw a vertical line from x_0 on the horizontal axis up to where the line meets the graph of ϕ. This is the point $(x_0, \phi(x_0))$.
2. Draw a horizontal line from the point $(x_0, \phi(x_0))$ to the vertical line. This is the point $(\phi(x_0), \phi(x_0))$.
3. Draw a vertical line from the point $(x_0, \phi(x_0))$ up to where the line meets the graph of ϕ. This is the point $(\phi(x_0), \phi(\phi(x_0)))$.
4. Repeat step 2 for as many steps as is needed.

With this definition in hand, we are ready for the logistic map example.

Example 2.1.4 (Logistic map)**.** The *logistic map* is defined by

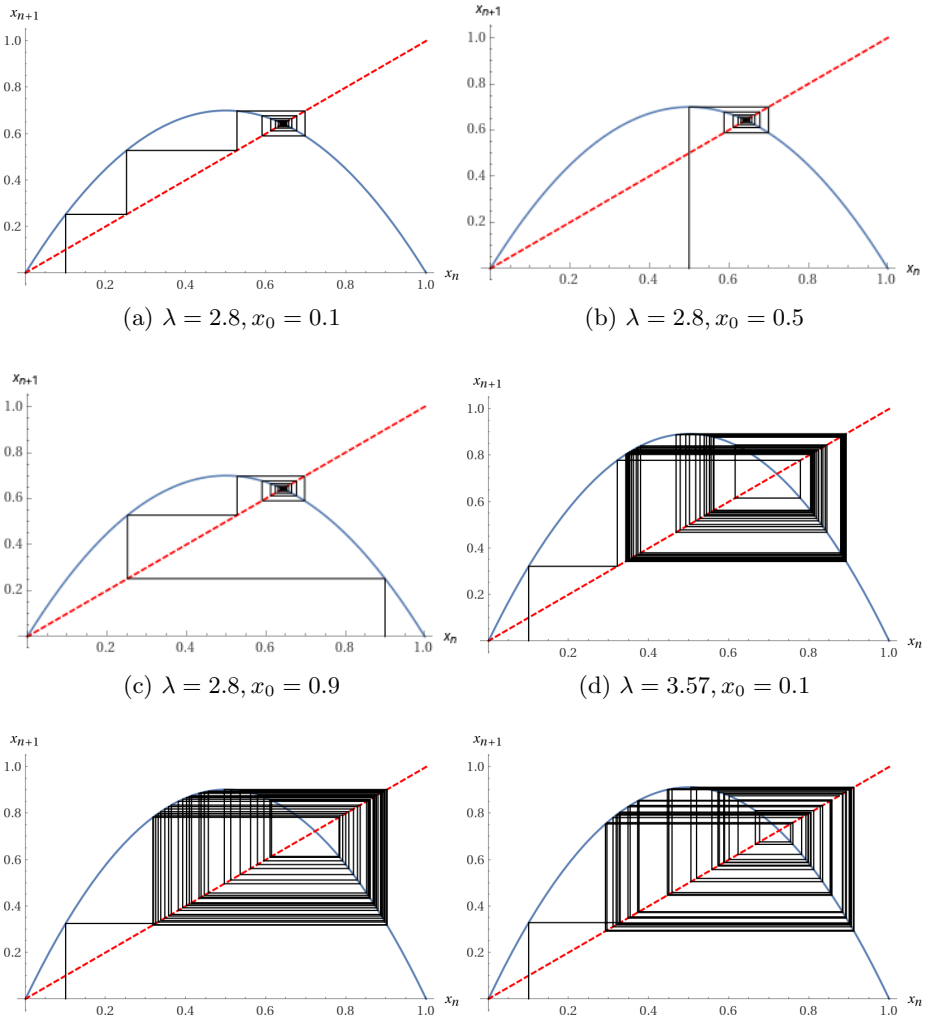
$$x_{n+1} = \lambda x_n(1 - x_n),$$

where λ and the initial condition x_0 can be varied to get some interesting results. (See Figure 2.1 for some examples.)

Interestingly, you can obtain closed-form solutions for some choices of λ and x_0. For instance, if you choose $\lambda = 4$ and $x_0 = 0.1$ you get the closed-form solution

$$x_n = \sin^2\left(2^{n-1}\cos^{-1}\left(1 - 2x_0\right)\right).$$

(As calculated by WolframAlpha.)



(a) $\lambda = 2.8, x_0 = 0.1$

(b) $\lambda = 2.8, x_0 = 0.5$

(c) $\lambda = 2.8, x_0 = 0.9$

(d) $\lambda = 3.57, x_0 = 0.1$

(e) $\lambda = 3.61, x_0 = 0.1$

(f) $\lambda = 3.65, x_0 = 0.1$

Figure 2.1: Some cobweb diagrams of the evolution of the logistic map for various values of λ and x_0. In (a)-(c) the parameter λ is fixed, but the initial condition varies, and the end points converge to around 0.64 despite the rather large variations in x_0 from 0.1 to 0.9. (d)-(f) shows some examples of chaotic behavior, even for very small perturbations of the parameter λ. Inspiration taken from [Cru11a] and [Cru11b].

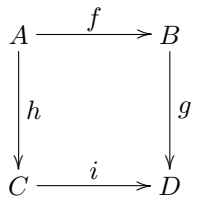
2.2 Diagrams

Next, in order to begin looking at Lattès maps, we first need to define diagrams, and in particular, commutative diagrams.

Definition 2.2.1 ((Commutative) diagram)**.** A *diagram* is a collection of sets $A, B, C, \ldots$ together with maps $f, g, h, \ldots$ between the sets such that composition of the maps is well-defined.

A *commutative diagram* is a diagram where every path from a starting point to an end point yields the same result, i.e. the composition is path-independent. In practice it's common to call these diagram "commutative diagrams," whether or not they actually commute.

Example 2.2.1. Let $f : A \to B$, $g : B \to D$, $h : A \to C$, and $i : C \to D$. If $g \circ f = i \circ h$, then this diagram commutes. If not, then the diagram doesn't commute. We can visualize this as the following diagram:



As a further example, we can construct maps such that these compositions commute. For this example we only consider maps from $\mathbb{R}$ to $\mathbb{R}$. Let

$$\begin{aligned} f(x) &= 2x, \\ g(x) &= 3x, \\ h(x) &= \frac{1}{2}x, \text{ and} \\ i(x) &= 12x. \end{aligned}$$

This diagram now commutes, since $g(f(x)) = 6x = i(h(x))$. Changing just one of the coefficients in any of these functions will make the diagram non-commutative.

2.3 Lattès maps

Definition 2.3.1 (Projective lines, rational maps, and Lattès maps)**.** The *projective line* $\mathbb{P} = \mathbb{P}^1$, looking at it geometrically, is the set of all lines in K^2, where K is a field, that go through the origin, but excluding the origin.

We can define this as the set

$$\mathbb{P}^1 = \frac{\{(a,b) \in K^2 \mid (a,b) \neq (0,0)\}}{\sim},$$

where $\sim$ is the equivalence relation $(a,b) \sim (ka,kb)$ for all $k \in K$. Since all we need to define a line are two points, we require that this set is modulo the equivalence relation $\sim$. Thus all points on a given line that goes through the origin (but importantly doesn't include the origin) are considered the same point by this equivalence relation.

By this construction we only need a single point to describe a given projective line, and it is therefore customary to write $[a,b]$ for a given projective line.

A *rational map* is a map of the form

$$\phi(x) = \frac{F(x)}{G(x)} = \frac{a_0 + a_1 x + \cdots + a_d x^d}{b_0 + b_1 x + \cdots + b_d x^d},$$

in other words a ratio of polynomials. The *degree* of ϕ is

$$\deg \phi = \max\{\deg F, \deg G\}.$$

A map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ is of the form

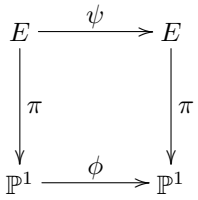
$$[a,b] \mapsto [F(a,b), G(a,b)],$$

and by dividing through by $G(a,b)$ we get

$$[a,b] \mapsto \left[\frac{F(a,b)}{G(a,b)}, 1\right],$$

thus we call it a *rational* map. If $G(a, b) = 0$, then by convention the point at infinity is denoted $[a, 0]$.

A rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree $d \geq 2$ is a *Lattès map* if there is an elliptic curve E, a morphism $\psi : E \to E$, and a finite separable covering $\pi : E \to \mathbb{P}^1$ such that the following diagram is commutative:



Note that the definition of a Lattès map makes reference to elliptic curves.

Example 2.3.1 (Doubling map)**.** (Note: This example is example #6.41 on page 351 of [Sil07].)

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, $\psi(P) = [2]P$ be the duplication map (see 1.2.2) for points on the curve, and $\pi(P) = \pi(x, y) = x$ be a projection map. We can let $x : E/\{\pm 1\} \to \mathbb{P}^1$ be an isomorphism , which yields the Lattès map

$$\phi(x) = x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}.$$

Bibliography

[Cru11a] James P. Crutchfield. "The Topology of Chaos, Chapter 1". In: (2011). URL: https://csc.ucdavis.edu/~chaos/courses/poci/Readings/ch1.pdf (visited on 05/23/2024).

[Cru11b] James P. Crutchfield. "The Topology of Chaos, Chapter 2". In: (2011). URL: https://csc.ucdavis.edu/~chaos/courses/poci/Readings/ch2.pdf (visited on 05/23/2024).

[Gal13] Michael Galperin. "Torsion Points of Elliptic Curves". In: (2013). URL: https://math.uchicago.edu/~may/REU2013/REUPapers/Galperin.pdf (visited on 05/23/2024).

[Lar24] D. Larsson. "Arithmetic of Elliptic Curves". In: (2024). URL: https://www.numberlab.net/_files/ugd/d10f42_4283fd7eaec84667af45260318cffcf4.pdf (visited on 05/23/2024).

[Mil06] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006, pp. 238+viii. ISBN: 1-4196-5257-5.

[Sil07] Joseph H. Silverman. *The Arithmetic of Dynamical Systems*. Graduate Texts in Mathematics. Springer, 2007. ISBN: 9780387699035.

[Sut15] Andrew Sutherland. "18.783 Elliptic Curves, Lecture #5". In: (2015). URL: https://math.mit.edu/classes/18.783/2015/LectureNotes5.pdf (visited on 05/23/2024).