Seminar on Elliptic Curves

Cubic Curves

Silvio Barandun* & Florian Held†

3rd November 2020

Abstract

In this first seminar paper we introduce the main ideas and objects of study of this seminar on Elliptic Curves. In the first section we introduce the reader to cubic curves in general and define (geometrically) a group structure on each such curve. The second section is dedicated to the derivation of the *Weierstrass normal form* and a few immediate consequences. Finally, in the last section – using the Weierstrass normal form – we derive explicit formulas for the given group law and formalise so this construction.

Contents

*e-mail: silvioba@student.ethz.ch
†e-mail: heldf@student.ethz.ch

1 Introduction

We are going to study elliptic curves, which are non-singular cubic plane curves. The goal of this section is to give precise definitions of these objects.

1.1 Cubic curves

Definition 1.1 (Algebraic Curves)**.** An *algebraic curve*, or simply curve, $C \subseteq \mathbb{C}^2$ is the zero locus of a polynomial in two variables.

Definition 1.2 (Rational Point)**.** A *rational point* on an algebraic curve C is a point $P = (P_1, P_2) \in C$ such that all the coordinates of P are rational: $P_i \in \mathbb{Q}$.

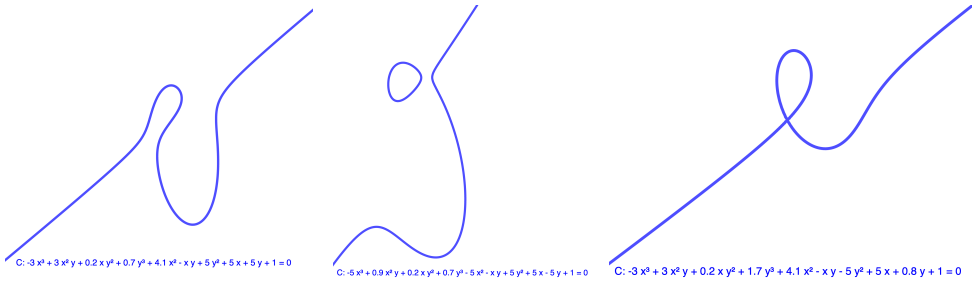
An algebraic curve whose defining polynomial is of degree 3 is called a cubic (algebraic) curve. Cubic curves are the object of study of this paper, so we will concentrate on these form now on. A cubic plane curve is therefore the set of solutions $(x, y) \in \mathbb{C}^2$ of a polynomial of degree 3. We will use the notation

$$C : aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + iY + j = 0.$$

As we will see later in Section 1.4, it's also handy to consider the homogenisation of this curve

$$C : aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3 = 0$$

and it's set of solution $[x : y : z]$ in the projective plane $\mathbb{P}^2 = \mathbb{P}^2_{\mathbb{C}}$.



(a) (b) (c)

Figure 1: Some examples of cubic curves

1.2 Notation

Let's first introduce some notation.

We define by

$$\ell(P, Q) = \{S \in \mathbb{P}^2 : S \text{ lies on the line joining } P \text{ to } Q\} \tag{1.1}$$

the line joining P and Q. Therefore $\ell(P, Q) \cap C$ are the intersection points of C and the line joining P and Q.

If C is the zero locus of $f(X, Y)$ we use the algebraic geometry notation $C = \mathbb{V}(f)$ to denote the curve.

Working in projective geometry, it's easy to show that given two, not necessarily distinct, points $P, Q \in C$ there exists a third, not necessarily distinct, point $R \in C$ such that

$$\ell(P, Q) \cap C = \{P, Q, R\} \tag{1.2}$$

where we do allow duplicates in the left hand side.

Definition 1.3. Let C be a cubic curve. We define the binary operation

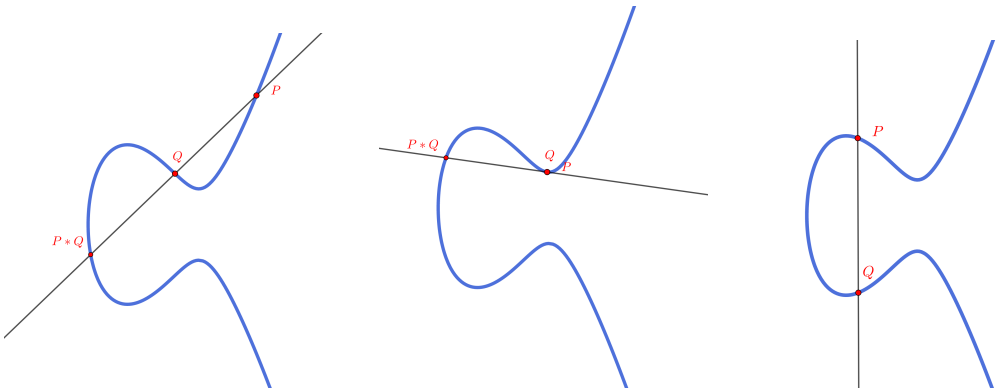
$$\begin{aligned} * : C \times C &\to C \\ (P, Q) &\mapsto P * Q = \ell(P, Q) \cap C - \{P, Q\} \end{aligned}$$

which returns the third point on $\ell(P, Q) \cap C$. We use the convention that

$$\{A, B, B\} - \{A, B\} = \{B\}.$$

In order to make Definition 1.3 precise, we have to clarify what we mean with $\ell(P, P)$. In this case, we simply consider $\ell(P, P)$ to be the tangent line through P. Explicitly, the tangent to $C = \mathbb{V}(f(X, Y, Z))$ through $P \in \mathbb{P}^2$ is given by the zero locus of

$$\left.\frac{\partial f}{\partial X}\right|_P X + \left.\frac{\partial f}{\partial Y}\right|_P Y + \left.\frac{\partial f}{\partial Z}\right|_P Z \in \mathbb{C}[X, Y, Z]. \tag{1.3}$$



(a) General (b) Tangent (c) Need of $\mathbb{P}^2$

Figure 2: Some examples of $P * Q$

1.3 First properties

On our fourth talk we're going to proof Mordell's Theorem which is a statement about rational points on rational cubic curves (i.e. cubic curves with rational coefficients).

We introduce here a first key observation about rational points. Let $P, Q \in C$ be rational point on a cubic curve C whose defining polynomial has rational coefficients. Then the intersection of the line through P and Q and the curve is again rational, i.e. $P * Q \in \mathbb{Q}^2$. This fact is easy to check, indeed the line through two rational point is given by an equation in rational coefficients. The intersection points of this line with a cubic curve are solutions of a cubic equation in rational coefficients with two roots given by rational points. Thus the third one must also be rational.

We now introduce two results that we will need in the next section.

Lemma 1.4 (Bezout)**.** *Let C_1, C_2 be two cubics (in $\mathbb{P}^2$) having no irreducible components in common. Then C_1 and C_2 intersect in nine points counting multiplicity.*

Proposition 1.5 (Intersection points of cubics)**.** *Let C, C_1, C_2 be three cubics (in $\mathbb{P}^2$). If C goes through eight of the nine intersection points of C_1 and C_2 then C goes through the ninth intersection point as well.*

The proof of these results goes beyond the scope of this paper, we thus invite the interested reader to check them in the literature: Lemma 1.4 may be found in [1, p. I.7.8] and Proposition 1.5 in [2, p. 1.2].

1.4 Group structure - Geometrically

Let C be a cubic curve and $e \in C$ a point on it. We define the binary operation

$$\begin{aligned} + : C \times C &\to C \\ (P, Q) &\mapsto e * (P * Q) \end{aligned} \tag{1.4}$$

where $*$ denotes the operation introduced in Definition 1.3.

Lemma 1.6. *Let C be a cubic curve and $e \in C$ a point on it. Then $(C, e, +)$ forms an abelian group.*

The nicest way to consider this construction is to consider the curve in projective space and then choose e as $\mathcal{O} = [0 : 1 : 0]$, a point at infinity. This works for any curve and is the standard choice in the field.

Proof. We prove the lemma for $e = \mathcal{O} = [0 : 1 : 0]$ as, by change of variables, this is not a loss of generality.

We show well-definiteness of the binary operation in Section 3 by giving an explicit formula for it.

It's clear, form a geometrical consideration, that $+$ is commutative. Indeed $\ell(P, Q) = \ell(Q, P)$ trivially, thus $P * Q = Q * P$. Analogously, given one point P the three points of the intersection of C with the line trough P and $\mathcal{O}$ are $\ell(P, \mathcal{O}) = \{P, \mathcal{O}, P * \mathcal{O}\}$. Thus taking the third point on the intersection of C with the line trough $\mathcal{O}$ and $P * \mathcal{O}$ must be P, i.e. $\mathcal{O} + P = P + \mathcal{O} = P$ by commutativity.

We claim that $-P = P * (\mathcal{O} * \mathcal{O})$. Indeed let $\{\mathcal{O}, \mathcal{O}, S\}$ be the points where the tangent to $\mathcal{O}$ intersects C (we count the points with multiplicity, thus $\mathcal{O}$ twice). Let further Q, P, S be the points on the intersection of C and the line through P and S

such that $Q = P * S = P * (\mathcal{O} * \mathcal{O})$. Then $P * Q = S$ and finally $\mathcal{O} * S = \mathcal{O}$. Given this we conclude

$$P + (-P) = P + P * (\mathcal{O} * \mathcal{O}) = \mathcal{O} * (P * (P * (S))) = \mathcal{O} * (P * Q) = \mathcal{O} * S = \mathcal{O}.$$

Associativity is quite technical. It actually follows easily form the Riemann-Roch Theorem (which we do not cover in this seminar) so we allow our self to be a little hand wavy and just provide a sketch of this part. To show

$$P + (Q + R) = (P + Q) + R = \mathcal{O} * (P * (Q + R)) = \mathcal{O} * ((P + Q) * R) \tag{1.5}$$

it is enough to show that

$$P * (Q + R) = (P + Q) * R, \tag{1.6}$$

since if this holds then the third intersection point of C and the line trough $P*(Q+R)$ $= (P + Q) * R$ and $\mathcal{O}$ is unique. We can simplify (1.6) even further by noticing that this holds if and only if $\ell(P, Q + R) \cap \ell(P + Q, R) \in C$.

Consider now the following six lines

$$\ell(\mathcal{O}, P + Q)\ , \ell(P, R)\ , \ell(Q, P + R)\ , \ell(\mathcal{O}, P + R)\ , \ell(P, Q)\ , \ell(R, P + Q).$$

These give us six linear equations and consequently, multiplying the first three equations and the last three equations, we obtain two cubics C_1 and C_2. By Proposition 1.5 we obtain that since C goes through the eight intersection points of C_1 and C_2 listed above, $C_1 \cap C_2 \subset C$. But the ninth point in $C_1 \cap C_2$ must be the point $\ell(P, Q + R) \cap \ell(P + Q, R)$ as these two line are part of the definition of C_1 and C_2. ■

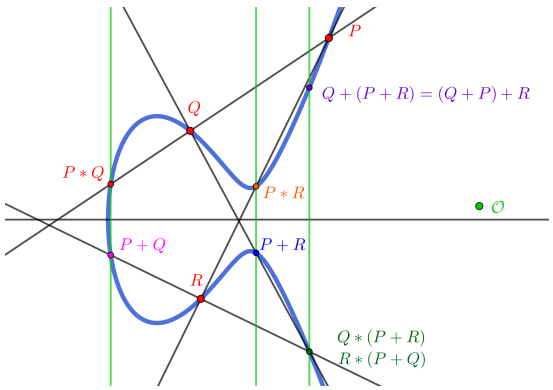


Figure 3: Associativity

In Lemma 1.6 we showed that any element $e \in C$ can be the neural element of the addition on C. But does the choice of e matter? The next lemma shows that this is not the case.

Lemma 1.7. *Let C be a cubic curve and $e, e' \in C$ then $(C, e, +) \cong (C, e', +')$, where $+, +'$ represent the group law (1.4) with respect to e and e' respectively.*

Proof. We explicitly provide an isomorphism

$$\begin{aligned}(C, e, +) &\to (C, e', +')\\ P &\mapsto P + e'\end{aligned}$$

and notice that $P +' Q = P + Q - e'$. ■

2 The Weierstrass normal form and singularity

One topic that we are interested in are rational points on general cubics. The transformation into Weierstrass normal form allows us to reduce this question to the question of rational points on cubics in Weierstrass normal form. This normal form also allows us to state relatively simple formulas for the group law.

2.1 Weierstrass normal form

Definition 2.1 (Weierstrass normal form)**.** A cubic $f(X, Y)$ is in Weierstrass normal form if it is of the form

$$f(X, Y) = X^3 + aX^2 + bX + c - Y^2.$$

We want to find a transformation that brings a general cubic into Weierstrass normal form while keeping track of the rational points on the curve. This allows us to just study curves in this normal form.

We give a sketch of the way the transformation works. We work in the projective plane and assume that we are given a rational point $\mathcal{O}$ on a non-singular curve C. Then we move the coordinates such that $\mathcal{O}$ lies at $[1, 0, 0]$. Next we calculate the tangent T_1 of C at $\mathcal{O}$. We then change the coordinates such that the tangent is the line $Z = 0$. Next we take the third intersection point Q of T_1 and C. Assume that Q and $\mathcal{O}$ are distinct points. Then find the tangent T_2 of C at Q and change the coordinates such that T_2 is the $X = 0$ axis. Now take any line T_3 through $\mathcal{O}$ that is not equal to T_1 and change the coordinates such that T_3 is the $Y = 0$ axis. In Figure 4 you can find a drawing to illustrate the procedure.

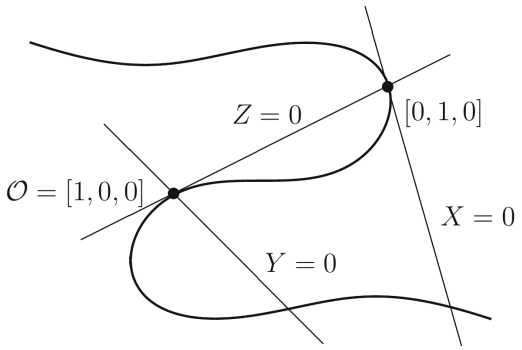


Figure 4: A sketch of the projective transformation from [2]

In the case that Q and $\mathcal{O}$ are identical also choose the tangent at $\mathcal{O}$ as the $Z = 0$ axis. For the $X = 0$ axis we can choose any line not going through $\mathcal{O}$ and the $Y = 0$ axis is again chosen as a line through $\mathcal{O}$ different from the tangent at $\mathcal{O}$.

After these transformations we go back to in-homogeneous coordinates by setting $Z = 1$. Now the equation is of the form

$$XY^2 + (aX + b)Y = cX^2 + dX + e.$$

Multiplying by X gives

$$(XY)^2 + (aX + b)XY = cX^3 + dX^2 + eX$$

by renaming XY as Y we get

$$(Y)^2 + (aX + b)Y = cX^3 + dX^2 + eX.$$

Now we complete the square by replacing Y by $Y - \frac{1}{2}(aX + b)$ and get

$$Y^2 = cX^3 + (d - \frac{1}{4}a^2)X^2 + (2ab + e)X + b^2.$$

To make the coefficient of the X^3-term 1 we replace Y by c^2Y and X by cX and divide the equation by c^4. Note that the X^2-term can be further eliminated by substituting X by $X - \frac{a'}{3}$, where a' is the coefficient of the X^2-term. To sum it up we have a sketch of how to transform a general cubic equation into Weierstrass normal form. As the coordinate transformation and its inverse are rational functions we can keep track of the rational points. The transformation is bijective up to possibly a few points which arise as roots of the denominator of the coordinate transformation. We also mention that the group structure of a curve and its transform are not the same but are connected by the transformation as the transformation is a group homomorphism. A good example of a transformation of a cubic is found in Appendix B of [2] (but be aware of a missing sing in the last formula on page 311). Appendix A of said book also develops the necessary projective geometry to further justify the transformation.

Definition 2.2 (Elliptic curve)**.** A cubic curve of the form $Y^2 = f(X) = X^3 + aX^2 + bX + c$ is called elliptic curve if f has distinct roots. A general cubic curve is called elliptic if it's transform into the Weierstrass normal form is an elliptic curve.

We note that for a curve with the equation $Y^2 = f(X) = X^3 + aX^2 + bX + c$, f having distinct roots is equivalent to being non-singular. To give an idea of what elliptic curves in the Weierstrass normal from look like there are sixteen cubics plotted in figure 5. They are all of the form $Y^2 = X^3 + aX + b$ for $a, b \in \{-1, 0, 1, 2\}$ and they are all elliptic up to the case where $a = b = 0$.

2.2 Singular cubics

Our definition of elliptic curves excludes singular cubics. This comes from the fact that studying the rational points on a singular cubic is completely different from

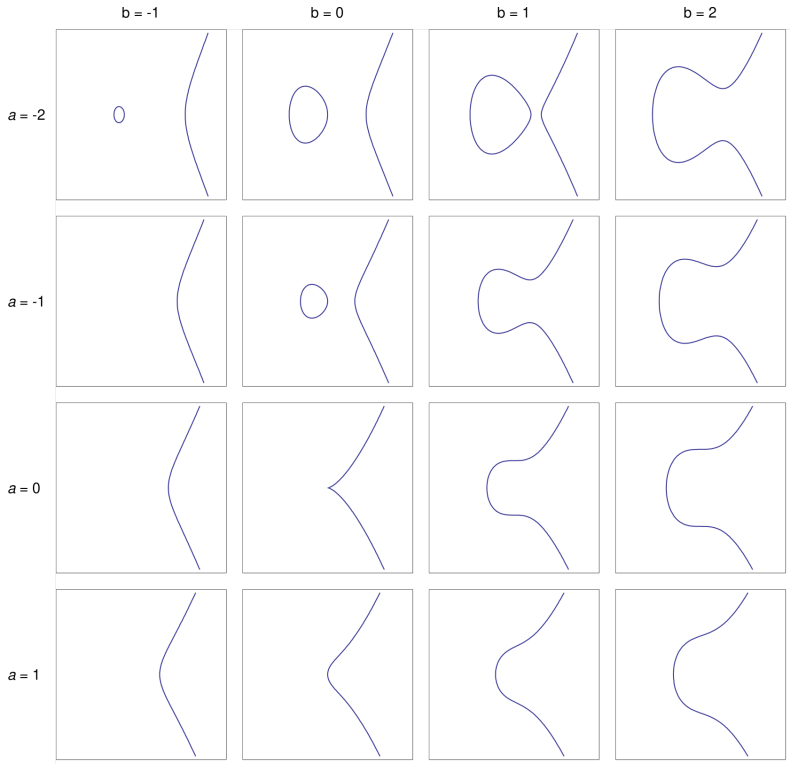


Figure 5: An overview of cubic curves from [3]

studying the rational points on a non-singular cubic. The geometric idea is to take a singular point P on the curve and project a point Q to a line l by taking the intersection of l and $\ell(P,Q)$. We find the rational points of two singular cubics. Suppose $Y^2 = f(X) = (X-d)^3$ for some $d \in \mathbb{Q}$. After a change of coordinates we just look at $Y^2 = X^3$ and note that the rational solutions are exactly of the form (t^2, t^3) for $t \in \mathbb{Q}$. For a second example we have the curve $Y^2 = X^2(X+1)$. By setting $r = \frac{X}{Y}$ we find $X = r^2 - 1$ and $y = rX = r^3 - r$. Now for any rational number r the point (r^2-1, r^3-r) is on the curve and conversely every rational point (x_0, y_0) can be brought into this form with $r = \frac{x_0}{y_0}$.

3 Explicit formulas for the group law

Now we have shown in Section 2 that any elliptic curve can be reduced to Weierstrass normal form, hence we will concentrate only on the curves in this format. We will formalise here the geometrical intuition of Section 1.4 and give explicit formulas for the group law.

3.1 Preliminary results

For the last time we will consider now the homogeneous version of an elliptic curve in Weierstrass normal form

$$C' : Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3 \tag{3.1}$$

for some $a, b, c \in \mathbb{C}$. Remark now that points at infinity, i.e. $P = [x : y : z] \in \mathbb{P}^2 \setminus \mathbb{C}^2$, must satisfy $z = 0$. Plugging this into (3.1), we get $0 = X^3$ and can conclude that the only point on C which is not in $\mathbb{C}$ is $\mathcal{O}$. Therefore from now on we will only consider the standard version of Weierstrass normal form equation

$$C : Y^2 = f(X) = X^3 + aX^2 + bX + c \tag{3.2}$$

and its complex solution, keeping in mind that there is one extra point we need to keep track of.

As a consequence of us working in projective space, we have that every line meets C in exactly three points. Furthermore one clearly sees that C is symmetric with respect to the x-Axis and in particular, as lines through $\mathcal{O}$ are vertical lines in $\mathbb{C}^2$, $-(x, y) = (x, -y)$.

3.2 The addition formula

Goal of this section is to give for any $P_1, P_2 \in C$ an explicit formula for $P_1 + P_2$. As already mentioned, lines through $\mathcal{O}$ are vertical lines in $\mathbb{C}^2$, so it will be enough to compute $P_1 * P_2 = (x_3, y_3)$ as then $P_1 + P_2 = (x_3, -y_3)$.

3.2.1 Addition of two distinct points

We assume now that $P_1 \neq P_2$ and will consider $P_1 + P_1$ separately later. Furthermore we assume that $x_1 \neq x_2$. The case $x_1 = x_2$ is easy to handle since then $P_2 = -P_1$, as already noticed above, and thus $P_1 + P_2 = \mathcal{O}$.

We first remark that the line $\ell(P_1, P_2)$ is given by the point slope equation

$$\ell(P_1, P_2) = \left\{ (x, y) \in \mathbb{C}^2 : y = \lambda x + \nu \text{ for } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \nu = y_1 - \lambda x_1 \right\}. \tag{3.3}$$

We remark that λ is well-defined as $x_1 \neq x_2$. The intersection points of C and this line are therefore given by substituting the condition of (3.3) into (3.2), i.e.

$$\begin{aligned} Y^2 = (\lambda X + \nu)^2 &= X^3 + aX^2 + bX + c \\ \iff 0 &= X^3 + (a - \lambda^2)X^2 + (b - 2\lambda\nu)X + (c - \nu^2). \end{aligned} \tag{3.4}$$

As we pointed out above $|\ell(P_1, P_2) \cap C| = 3$ and more precisely $\ell(P_1, P_2) \cap C = \{P_1, P_2, P_1 * P_2\}$ by definition of $P_1 * P_2$. Therefore the three solutions of (3.4) are exactly x_1, x_2 and x_3. This allows us to conclude

$$X^3 + (a - \lambda^2)X^2 + (b - 2\lambda\nu)X + (c - \nu^2) = (X - x_1)(X - x_2)(X - x_3) = \sum_{i=0}^{3} (-1)^{i+1} X^i e_{3-i}$$

where e_i are the elementary symmetric polynomial evaluated at (x_1, x_2, x_3). Considering now the quadratic term we get

$$(a - \lambda^2) = -e_1 = -x_1 - x_2 - x_3$$

and so

$$x_3 = \lambda^2 - a - x_1 - x_2.$$

It's now easy to get also the y_3 coordinate by inserting x_3 into (3.3).

Summing up, we have shown that if $x_2 \neq x_1$

$$(x_1, y_1) + (x_2, y_2) = (\lambda^2 - a - x_1 - x_2, -\lambda(\lambda^2 - a - x_1 - x_2) - \nu).$$

3.2.2 Addition of a point to itself

We now consider $P_1 + P_2$ for $P_1 = P_2$ and write $2P_1 := P_1 + P_1$. Calculating the line $\ell(P_1, P_1)$ as before isn't well-defined. Instead we choose the tangent to the curve at $P_1 = (x_0, y_0)$. By implicit differentiation of $Y^2 = f(X)$ we get $\lambda = \frac{dx}{dy}|_{P_1} = \frac{f'(x_0)}{2y_0}$. The same calculation as in 3.2.1 leads to

$$2(x_0, y_0) = (x_0, y_0) + (x_0, y_0) = (\lambda^2 - a - 2x_0, -\lambda(\lambda^2 - a - 2x_0) - \nu).$$

By plugging in the terms for λ and ν and using the relation $y_0^2 = f(x_0)$ we find

$$x\text{-coordinate of } 2(x_0, y_0) = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}$$

Doing the same for the y-coordinate we get for $y' = y$-coordinate of $2(x_0, y_0)$

$$\begin{aligned}
y' &= -\lambda(\lambda^2 - a - 2x_0) - \nu \\
&= -\frac{(3x_0^2 + 2ax_0 + b)}{2y_0}\left(\frac{(3x_0^2 + 2ax_0 + b)^2}{4y_0^2} - a - 2x_0\right) - y_0 + \frac{(3x_0^3 + 2ax_0^2 + bx_0)}{2y_0} \\
&= -\frac{(3x_0^2 + 2ax_0 + b)^3 + (3x_0^2 + 2ax_0 + b)(-a - 2x_0)4y_0^2 - (3x_0^3 + 2ax_0^2 + bx_0)4y_0^2 + 8y_0^4}{8y_0^3} \\
&= \frac{x_0^6 + 2ax_0^5 + 5bx_0^4 + 20cx_0^3 + (20ac - 5b^2)x_0^2 + (8a^2c - 2ab^2 - 4bc)x_0 + 4abc - b^3 - 8c^2}{8y_0^3}
\end{aligned}$$

We will use these formulas in a theoretical and computational setting, notably in the proof of Mordell's theorem.

References

[1] Hartshorne Robin, *Algebraic geometry*, eng, Softcover of hardcover 1st ed. 1997, vol. 52, softcover 2010, Graduate texts in mathematics, New York: Springer-Verlag, 2010, ISBN: 978-1-4419-2807-8 (cit. on p. 4).

[2] Silverman Joseph H and Tate John Torrence, *Rational points on elliptic curves*, vol. 9, Springer, 2015 (cit. on pp. 4, 6, 7).

[3] Tos Wikipedia user, *Elliptic curve catalog*, URL: `https://upload.wikimedia.org/wikipedia/commons/thumb/d/db/EllipticCurveCatalog.svg/2000px-EllipticCurveCatalog.svg.png` (cit. on p. 8).