Odd Cubics
An arithmetic study of a special set of curves

Cristian Baeza Miranda

December 11, 2020

To my father and my mother.

“Earn this... earn it” J.H. Miller.

Contents

1 Introduction

The so called elliptic curves are objects that appear in different branches of mathematics, possibly the first one to ever propose an arithmetic problem, that later (thousands of years later) would be identified with elliptic curves, was *Diophantus* when he proposed the following problem

Divide a number into two pieces such that their product is equivalent
to the cube of a number diminished by its root

Say for instance that the aforementioned number is 4, so with the convenient algebraic language we have today (that *Diophantus* certainly didn't have) and a proper choice of variables we can put the statement into the algebraic form

$$y(4-y) = x^3 - x$$

Years later, we find elliptic curves in different contexts such as algebraic geometry, number theory and cryptography, where they are known to be curves of genus one having a specified base point, being one the most known forms the so called Weierstrass form. Such curves have a very particular property which is their inherent structure as an abelian group. Briefly, given an elliptic curve E in Weierstrass form over a field $K = \bar{K}$ (it is usually required that char$K \neq 2, 3$), we can produce an abelian group by following the "chord-and-tangent" rule. We look to study the main arithmetic aspects concerning this underlying property for a special type of curve that presents a different kind of symmetry, explicitly the zero-set of

$$f(x, y) = a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 + a_5x + a_6y$$

defined over different fields. We are mainly interested in finite prime fields, and for completeness, we also study such curves over algebraically closed fields.

Chapter 2 includes a general review of some concepts that support most of the work done in this presentation. Chapter 3 introduces the main object of study with some it's elementary properties. Chapter 4 describes the group law, which is the most important aspect of the curve we use in this presentation. Chapter 5 shows specific cases with different particular properties. Chapter 6 shows some relations between well know curves and the model introduced in this work.

It is worth mentioning that this study started with a paper by De Feo ([2]) about isogeny based cryptography. It was this document that got me interested in elliptic curves and their arithmetic relevance. The main resources for this work can be found in the classic *The Arithmetic of Elliptic Curves* ([13]) by J.H. Silverman as well as its brother *Rational Points on Elliptic Curves* ([14]), and *An Introduction to Mathematical Cryptography* by J. Hoffstein, J.C. Piper and J.H. Silverman. ([8])

2 Background

We briefly introduce some previous results and notation that support most of the work in this presentation, following the notation as in Fulton's *Algebraic Curves* [6].

2.1 Bezout's Theorem

In this subsection k is an algebraically closed field. Recall that two projective plane curves F and G defined by the solutions of homogeneous polynomials p and q over k have a *common component* if and only if there exists r non-constant such that $(p, q) = r$. From here on, curves are always to be defined as set of solutions of polynomials (see p.2 [7]), or the *zero* set of a polynomial, thus the following notation in the example

Example 1 *On $\mathbb{C}[x, y]$ consider $F = Z(x^3 - y^3)$ and $G = Z(x - y)$, then $(F, G) = G$.*

Definition 2.1 *Given two plane curves F and G intersecting at P with no common component passing through P, $I(P, F \cap G)$ is the* **intersection number** *of the curves at P (§3.3 [6]).*

It satisfies several algebraic relations, such as

1. $I(P, F \cap G) = I(P, G \cap F)$
2. $I(P, F \cap G) = 0$ iff $P \notin F \cap G$.
3. $I(P, F \cap GH) = I(P, F \cap G) + I(P, F \cap H)$
4. $I((0, 0), X^n \cap Y) = n$
5. $I(P, Y - X^2 \cap Y - X) = 1$ for $P = (1, 1)$

and the following important property

Theorem 2.1 *Given two plane curves F and G and $P \in \mathbb{A}^2(k)$, the intersection number is uniquely determined by the identity*

$$I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{A}^2(k))/(F, G))$$

where $\mathcal{O}_p$ indicates the local ring at P.

Bezout's theorem tell us what happens when we intersect projective curves over an algebraically closed field ([6]). For more examples and a deeper discussion on Bezout's theorem we refer to ([11]), especially section 3.

Theorem 2.2 (Bezout) *Let F and G be projective plane curves of degree m and n respectively. Assume F and G have no common component. Then*

$$\sum_P I(P, F \cap G) = mn$$

Which justifies that whenever we intersect a cubic G $(deg(G) = 3)$ and a line F $(deg(F) = 1)$ with no common component, we obtain three points (not necessarily different). It is a slightly non-trivial exercise to show that the set $F \cap G$ is finite, so by a projective change of coordinates we can assume that no P lies at infinity (see p.54, problem 5.7 [6]).

2.2 About Intersection Cycles

We briefly collect ideas from § 5.5, 8.1 [6], that clarify the main tool used later in § 4 when we prove that the group law produces an abelian group. A *divisor* on $\mathbb{P}^2$ is a formal sum $\sum_{P\in\mathbb{P}^2} n_P P$, where all $n_P \in \mathbb{Z}$ and all but a finite number of them are 0. The set of all divisors on $\mathbb{P}^2$ form an abelian group. The *degree* of a divisor $c_1 = \sum_{P\in\mathbb{P}^2} n_P P$ is defined to be $\deg(c_1) = \sum_{P\in\mathbb{P}^2} n_P$

Definition 2.2 (Intersection cycle) *Let F and G be projective plane curves of degree m and n respectively, with no common components. The expression*

$$F \bullet G = \sum_{P\in\mathbb{P}^2} I(P, F \cap G)P$$

is called the **intersection cycle** *of F and G.*

Several properties of intersection numbers translate nicely into properties of intersection cycles, such as

1. $F \bullet G = G \bullet F$
2. $F \bullet GH = F \bullet G + F \bullet H$
3. $F \bullet (G + AF) = F \bullet G$ if A is homogeneous of degree $\deg(G) - \deg(F)$

2.3 About degree three equation and cubic residues

The main subject of this work are curves of degree three over finite fields, so we expose here some facts concerning cubic residues that will be helpful later on.

Definition 2.3 *Let p be a prime and $a \in \mathbb{F}_p^*$, a is called* cubic residue modulo p *(or just cubic residue) if the equation $x^3 = a \pmod p$ is solvable in $\mathbb{F}_p$.*

Proposition 2.1 *Let p be a prime with $p = 1 \pmod 3$ and $a \in \mathbb{F}_p^*$, then a is cubic residue modulo p if and only if $a^{(p-1)/3} = 1 \pmod p$.*

Proof: ($\Longrightarrow$) If a is cubic residue, there exists $b \in \mathbb{F}_p^*$ such that $b^3 = a \pmod p$, so

$$a^{(p-1)/3} = (b^3)^{(p-1)/3} = b^{p-1} = 1 \pmod p$$

where the last equality holds due to Fermat's Little Theorem (FLT, see p.96 [5]).

($\Longleftarrow$) Recall that $\mathbb{F}_p^*$ is cyclic [1], so there is an element $g \in \mathbb{F}_p^*$ such that every $x \in \mathbb{F}_p^*$ can be expressed as $g^k = x$ for some $1 \leq k \leq p-1$. Hence

$$1 = a^{(p-1)/3} = g^{k(p-1)/3}$$

and given that $ord(g) = p-1$, $(p-1)$ divides $k(p-1)/3$, so $k/3 \in \mathbb{Z}$, i.e., there exists $k' \in \mathbb{Z}$ such that $k = 3k'$. Thus we finally have that

$$a = g^k = g^{3k'} = (g^{k'})^3$$

so a is cubic residue modulo p. ■

Corollary 2.1 *Let p be a prime with $p = 1 \pmod 3$, then the number of cubic residues modulo p is $\frac{p+2}{3}$.*

Proof: As in the previous proof, given a primitive root g for $\mathbb{F}_p^*$ and an element $a \in \mathbb{F}_p^*$ there exists $k = 3k'$ such that $a = g^{3k'}$, so when considering the set $A = \{3, 6, \dots, p-1\}$ we have that g^k is cubic residue for every $k \in A$. Since g is primitive root $k \neq j \Longrightarrow g^k \neq g^j$ and $|A| = \frac{p-1}{3}$, so there are $\frac{p-1}{3}$ non-zero cubic residues, the solutions of the polynomial $x^{(p-1)/3} - 1 = 0 \pmod p$. Finally, we include 0 and find $\frac{p+2}{3}$ cubic residues modulo p. ■

Proposition 2.2 *Let p be a prime with $p = 2 \pmod 3$, then every $a \in \mathbb{F}_p^*$ is cubic residue modulo p.*

Proof: If $p = 2$ then $\mathbb{F}_2^* = \{1\}$ and 1 is clearly a solution of $x^3 = 1 \pmod 2$. For $p \geq 5$, using FLT we see that

$$a^{p-1} = 1 \pmod p \Longrightarrow a^{p-2} = a^{-1} \pmod p \Longrightarrow (a^{(p-2)/3})^3 = a^{-1} \pmod p$$

$$\Longrightarrow ((a^{(p-2)/3})^{-1})^3 = a \pmod p \Longrightarrow a \text{ is cubic residue modulo } p. \quad ■$$

We now recall some well-known results about the cubic equation concerning its irreducibility.

[1] see p.65 th.62 [12]

Proposition 2.3 *Let $f(u) = u^3 + a_1u^2 + a_2u + a_3$ with $a_i \in \mathbb{F}_p$ and $p > 3$, then f(u) is irreducible in $\mathbb{F}_p[x]$ if an only if f(u)=0 has no solutions in $\mathbb{F}_p$.*

There are several methods to find solutions for a cubic, such as the rational roots criteria or the well-known formula for the solution of the cubic. When dealing with a large prime p and large coefficients in the cubic, we might require different techniques. Given $f(x) = x^3 + ax^2 + bx + c$, applying the usual substitution for the cubic $x \mapsto u = x - a/3$ yields

$$f(u) \quad = \quad u^3 + \alpha u + \beta \tag{2.1}$$

where $\alpha = (3b - a^2)/3$ and $\beta = (2a^3 - 9ab + 27c)/27$, so as seen in §14.6 [5] we have

Definition 2.4 *For $f(u)$ as in (2.1), the value*

$$\Delta := -4\alpha^3 - 27\beta^2$$

is called the **discriminant** *of f.*

According to the previous propositions, we distinguish two cases: $p = 1 \pmod 3$ and $p = 2 \pmod 3$, so its *discriminant* is easier to compute.

Proposition 2.4 *For $f(u)$ as in (2.1) in $\mathbb{F}_p[x]$ with $p = 2 \pmod 3$ and discriminant Δ,*

$$\left(\frac{-3\Delta}{p}\right) = 1 \Longrightarrow f \textit{ has a root in } \mathbb{F}_p$$

Proof: Follows directly from the solutions of a cubic in $\mathbb{F}_p$ (§14.7 [5]), which are

$$u_1 = \frac{1}{3}(A + B), \quad u_2 = \frac{1}{3}(A\rho + B\rho^2), \quad u_3 = \frac{1}{3}(A\rho^2 + B\rho)$$

with ρ a cubic root of unity in $\mathbb{F}_p$ and

$$A = \sqrt[3]{\frac{-27\beta + 3\sqrt{-3\Delta}}{2}}, \quad B = \sqrt[3]{\frac{-27\beta - 3\sqrt{-3\Delta}}{2}}$$

since, according to proposition (2.2), the cubic roots are always in $\mathbb{F}_p$, so we only require -3Δ to be quadratic residue for u_1 to be in $\mathbb{F}_p$. ■

(recall the discriminant is invariant under translation). The converse however fails to be true, consider $p = 41$ and

$$f(u) = u^3 + 30u^2 + 3u + 30 \pmod p$$

in this case 2, 20 and 30 are solutions of f, but -3Δ is not quadratic residue. Although the original form of Δ in terms of a, b and c is somewhat bigger than in the reduced case, computationally, this shall no represent a big issue since the operations involved to compute Δ and then raising to the $(p - 1)/2$ power (to check that it is quadratic residue) do not require a big effort.

Now for $p = 1 \pmod 3$, since we require the elements under the cubic root to be a quadratic residues, it's immediate from the previous proposition the following

Proposition 2.5 *Let f as in (2.1) in $\mathbb{F}_p[x]$ with $p = 1 \pmod 3$ and Δ its discriminant, then*

$$\left[\left(\frac{-3\Delta}{p}\right) = 1\right] \wedge \left[\left(\frac{-27\beta \pm 3\sqrt{-3\Delta}}{2}\right)^{(p-1)/3} = 1 \pmod p\right] \Longrightarrow f \text{ has a solution in } \mathbb{F}_p$$

Even though this previous results are good enough to check whether a cubic is reducible or not, for completeness we restate a result from Dickson [3] with necessary and sufficient conditions over a cubic equation for it to be irreducible over $\mathbb{F}_p$.

Theorem 2.3 *Let p be a prime greater than 3 and $f(x) = x^3 + ax + b$ a polynomial over $\mathbb{F}_p$. Then f is irreducible if and only if the following two conditions hold:*

1. *Δ is a quadratic residue in $\mathbb{F}_p^\times$, say $\Delta = (3^2\mu)^2$.*
2. *$\alpha := (-b + \mu\sqrt{-3})/2$ is a cubic non-residue in $\mathbb{F}_p(\sqrt{-3})$.*

where $\Delta = -(4a^3 + 27b^2)$.

2.4 A useful identity

In § 5.2 we will use the following result:

Proposition 2.6 *If $p, q, r, s \in K$ such that $rs \neq 0$ and $p/r = q/s$ then for any $\lambda_1, \lambda_2 \in K^*$,*

$$\frac{p}{r} = \frac{q}{s} = \frac{p\lambda_1 + q\lambda_2}{r\lambda_1 + s\lambda_2}$$

whenever defined.

Proof: Observe that

$$\frac{p}{r} = \frac{q}{s} \quad \Longrightarrow \quad \frac{p}{r} = \frac{q}{s} = \frac{p\lambda_1}{r\lambda_1} = \frac{q\lambda_2}{s\lambda_2}$$

also

$$\begin{aligned}\frac{p}{r} = \frac{q}{s} \quad &\Longrightarrow \quad \frac{p}{q} = \frac{r}{s} \\ &\Longrightarrow \quad \frac{p+q}{q} = \frac{r+s}{s} \\ &\Longrightarrow \quad \frac{p}{r} = \frac{q}{s} = \frac{p+q}{r+s}\end{aligned}$$

so

$$\frac{p}{r} = \frac{q}{s} = \frac{p\lambda_1}{r\lambda_1} = \frac{q\lambda_2}{s\lambda_2} = \frac{p\lambda_1 + q\lambda_2}{r\lambda_1 + s\lambda_2}$$

■

2.5 About the Group Law

We expose succinctly the group law for elliptic curves in Weierstrass from. Let E be a non-singular elliptic curve over $K = \bar{K}$ ($\mathrm{char}(K) \neq 2$) in Weierstrass form of equation

$$E : \quad y^2 = x^3 + ax^2 + bx + c \tag{2.2}$$

and the points $A, B \in E$ (not necessarily distinct). Consider L to be the line between A and B (tangent line if $A = B$), and call C the third point of intersection of $E \cap L$. Consider C' to be the reflection of C with respect to the x-axis and write $A \oplus B = C'$. As a result $(E, \oplus)$ is an abelian group with identity been the point at infinity $\mathcal{O} = [0 : 1 : 0]$ (p.52 [13]).

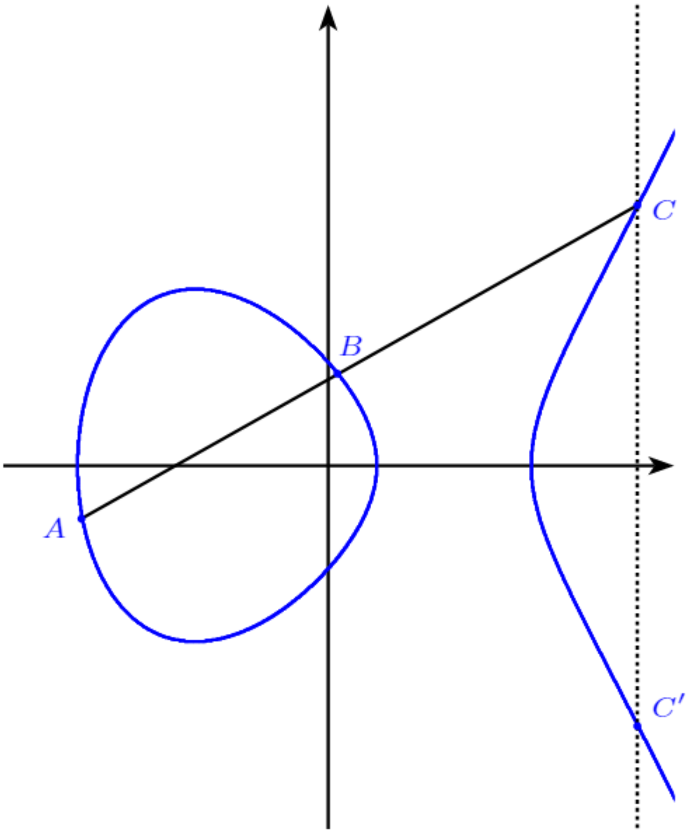


Figure 1: Real representation of the group law

2.6 About Projective Points

Recall that points in $\mathbb{P}^2(k)$, or just $\mathbb{P}^2$ when clear from context, have the usual representation $[x : y : z]$, which is unique up to non-trivial scalar transformation, i.e. in $\mathbb{P}^2$

$$[x : y : z] = [\lambda x : \lambda y : \lambda z] \quad \forall \lambda \in k^*$$

We briefly describe a procedure to identify points in $\mathbb{A}^2$ with points in $\mathbb{P}^2$. Say we have the point $(x_1, y_1) \in \mathbb{A}^2$, to find a projective equivalent, an immediate choice would be $[x_1 : y_1 : 1]$, but we can do better by considering the relations

$$x_1 = \frac{X_1}{Z_1}, \quad y_1 = \frac{Y_1}{Z_1}$$

so

$$[x_1 : y_1 : 1] = \left[\frac{X_1}{Z_1} : \frac{Y_1}{Z_1} : 1\right] = [X_1 : Y_1 : Z_1]$$

Moreover, the same process can be applied for more complex relations, such as $(x_1+x_0, a-x_1x_0)$ so in this case we obtain

$$[x_1 + x_0, a - x_1x_0 : 1] = \left[\frac{X_1}{Z_1} + \frac{X_0}{Z_0}, a - \frac{X_1}{Z_1}\frac{X_0}{Z_0} : 1\right] = [X_1Z_0 + X_0Z_1 : aZ_0Z_1 - X_1X_0 : Z_0Z_1]$$

for a constant. We shall apply this procedure further in § 5.2.1.

3 Odd Cubics, a first insight

For elliptic curves in Weierstrass form there is an algorithm that naturally produces an abelian group, the so called chord-tangent method, which led me to think: "On elliptic curves, when we take two points, find a third one and reflect it with respect to the x-axis, we obtain, an abelian group. What if we reflect such point with respect to the origin instead?". In algebraic terms we want to make sense of taking a point $P = (x, y)$ on a curve E and ensuring that $P' = (-x, -y)$ is also on E. For elliptic curves in Weierstrass form we mostly do not have this kind of property, but we still want such curve to have degree 3 so for any straight line L, $E \cap L$ consists of exactly three points. Explicitly, let K be a field and $a_1, \ldots, a_{10} \in K$, if

$$f(x, y) = a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 + a_5x^2 + a_6xy + a_7y^2 + a_8x + a_9y + a_{10} = 0$$

is the affine equation of odd degree for the kind of curve we are looking for, then we require f to satisfy $f(-x, -y) = 0$, i.e.

$$f(-x, -y) = -a_1x^3 - a_2x^2y - a_3xy^2 - a_4y^3 + a_5x^2 + a_6xy + a_7y^2 - a_8x - a_9y + a_{10} = 0$$

so after adding the relations we find $a_5x^2 + a_6xy + a_7y^2 + a_{10} = 0$ for every (x, y) on the curve and $f(-x, -y) = -f(x, y)$, which means that f has to be an odd function, thus the name "odd cubics", with terms of degree 3 and 1. We state this idea in a more precise definition. Let $K = \bar{K}$ with $\mathrm{char}(K) > 3$

Definition 3.1 (Odd Cubic) *Let E be a curve defined over a field K (=E/K) by the set of solutions of $f \in K[x, y]$ such that*

$$f(x, y) = a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 + a_5x + a_6y \tag{3.1}$$

We say that E is an odd cubic

Since we want to start with a general case, we take as usual the x variable as reference, requiring for instance $a_1 \neq 0$. Think of it as when trying to solve a quadratic polynomial $ax^2 + bx + c = 0$ in $\mathbb{C}$, we set $a \neq 0$, so it does not turn into a polynomial of degree 1 with no interesting properties about quadratic equations. Thus, unless otherwise stated in this subsection we consider odd cubics as in (3.1) with $a_1 = 1$ and say that such curves are in "general form".

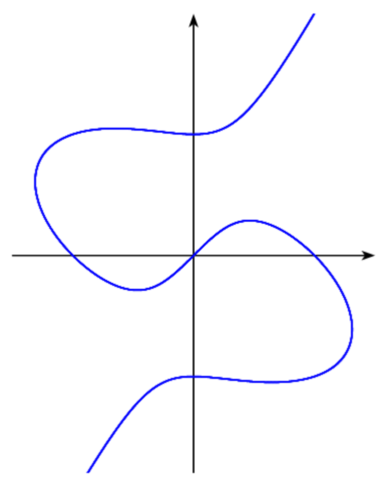
Definition 3.2 (General Form of an Odd Cubic) *Let E/K be a curve defined by the set of solutions of $f \in K[x, y]$ such that*

$$f(x, y) = x^3 + ax^2y + bxy^2 + cy^3 + dx + ey \tag{3.2}$$

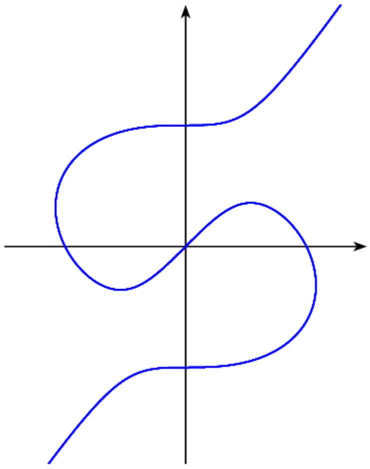
We say that E is an odd cubic in **general form***.*

Remark 3.1 *The expression "odd cubic" is not a standard name for any type of odd degree polynomials in two variables, but it refers to the form and degree of the defining equation (possibly with a linear part).*

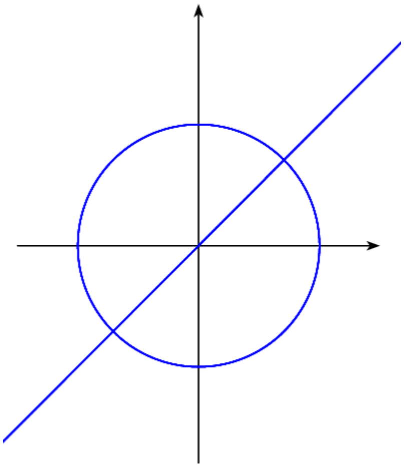
We take a first look at a few examples of odd cubics over $\mathbb{R}$.



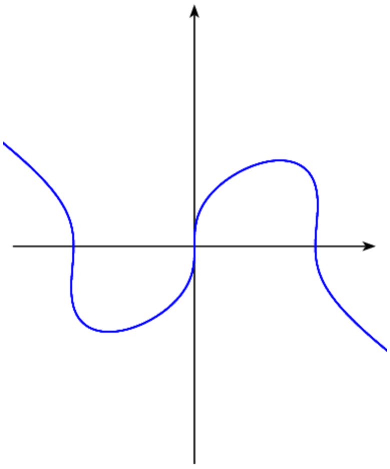
$x^3+x^2y+xy^2-y^3-x+y=0$



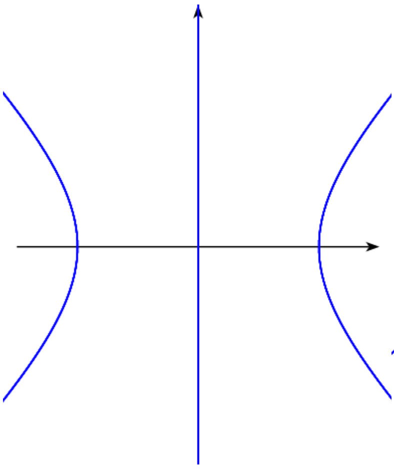
$x^3+xy^2-y^3-x+y=0$



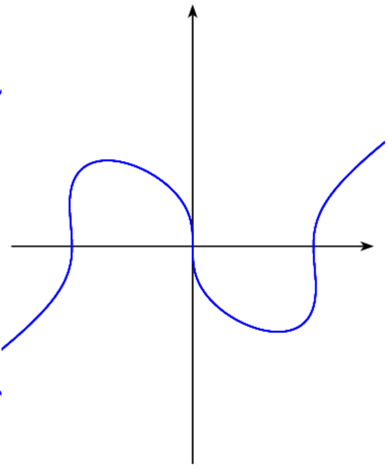
$x^3-x^2y+xy^2-y^3-x+y=0$



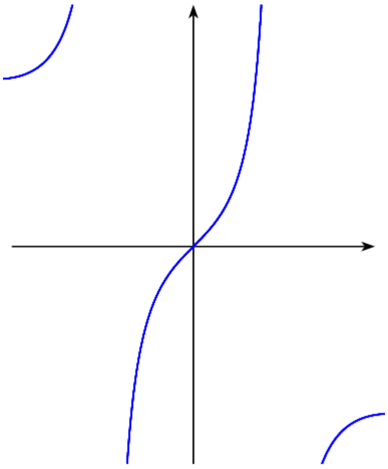
$x^3-xy^2+2y^3-x=0$



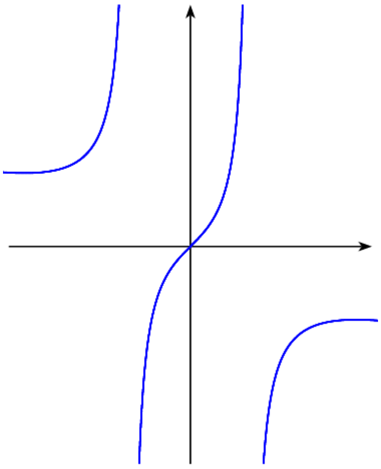
$x^3-xy^2-x=0$



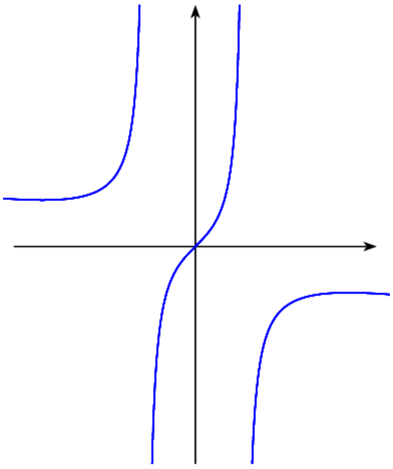
$x^3-xy^2-2y^3-x=0$



$x^3+2x^2y+x-y=0$



$x^3+4x^2y+x-y=0$



$x^3+6x^2y+x-y=0$

A few questions arise just from looking at real representations of odd cubics, such as

1. What is the genus of this curves? Under what conditions do these curves have genus 1?
2. Are there curves non-singular?
3. Are they all unbounded?
4. What are the possible asymptotic behaviours?
5. When is a cubic connected?, irreducible?

The first aspect we want to settle is the irreducibility of E, due to the possibility of E to be factored and lead to problems with the operation we want to produce. After looking at the previous examples, we see that some curves can be decomposed (third example in first row and second example in second row), and of course their equations are reducible, explicitly

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

in the first case, and

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

in the second case.

More generally, we know that a reducible polynomial of degree 3 has at least one factor of degree 1 (a line).

This we want to avoid since when working with two points in this line we could not define uniquely a third point of intersection. Nevertheless, there is a nice criteria to check whether an odd cubic is irreducible or not. We first consider a special polynomial

Definition 3.3 (Discriminant of Reducibility) *Given E/K an odd cubic defined by f in general form (def 3.2), we call the polynomial*

$$D_E(t) = t^3 - at^2 + bt - c$$

the discriminant of reducibility of E.

with this in mind we have the following result

Proposition 3.1 (Irreducibility Criteria) *Let E/K be an odd cubic in general form not divisible by x with $K = \bar{K}$, then*

1. *If $de \neq 0$, then E is irreducible if and only if $D_E(e/d) \neq 0$.*
2. *If only one of d or e is zero, then E is irreducible.*
3. *If $d = e = 0$, then E is reducible over K.*

Proof: Keeping f as above, $y \nmid f$ since f is monic in x^3. Second, $x|f$ if and only if $c = e = 0$, so for E to have a chance of being irreducible we require $c \neq 0$ or $e \neq 0$, which is the same as saying that E is not divisible by x. Third, say $x + ty|f$ for $t \neq 0$, then by the division algorithm, we find that the reminder of f divided by $x + ty$ is $r(y) = y((e - td) - D_E(t)y^2)$, so if $d \neq 0$

$$\begin{aligned} x + ty|f &\iff r(y) \equiv 0 \quad \forall y \in K^* \\ &\iff \exists t \in K : \, (D_E(t) = 0) \wedge (td - e = 0) \\ &\iff D_E(e/d) = 0 \end{aligned}$$

which means that when $de \neq 0$ and $t \neq 0$ as before,

$$E \text{ is irreducible over } K \iff D_E(e/d) \neq 0$$

More generally when E is reducible, since $td = e$, we have that $d = 0$ if and only if $e = 0$, so d and e are both zero or both non-zero, or

$$E \text{ reducible } \implies [d = 0 \wedge e = 0] \vee [d \neq 0 \wedge e \neq 0]$$

whose contrapositive is

$$[d = 0 \wedge e \neq 0] \vee [d \neq 0 \wedge e = 0] \implies E \text{ irreducible}$$

Now, what if $d = e = 0$? Since $K = \bar{K}$, f can be factored as $f(x, y) = (x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y)$ for some $\alpha_1, \alpha_2, \alpha_3 \in K$. This way the case $d = e = 0$ turns out to be uninteresting. ■

From now on we consider odd cubics as irreducible curves as well.

Now we find the points at infinity. To do so we look at the projective version of f, i.e.

$$X^3 + aX^2Y + bXY^2 + cY^3 + dXZ^2 + eYZ^2 = 0 \tag{3.3}$$

after making $Z = 0$ we look for the solution of $X^3 + aX^2Y + bXY^2 + cY^3 = 0$, explicitly

$$X^3 + aX^2Y + bXY^2 + cY^3 = (X - \alpha Y)(X - \beta Y)(X - \gamma Y) \quad \text{for some } \alpha, \beta, \gamma \in K$$

so the points at infinity are $[\alpha : 1 : 0]$, $[\beta : 1 : 0]$ and $[\gamma : 1 : 0]$.

Observe that $[1 : 0 : 0]$ is never a solution of (3.3), this will come in handy later in section 4 when we perform addition of points.[2]

Remark 3.2 *If the coefficients of both x^3 and y^3 in definition (3.1) had been zero, we would have $aX^2Y + bXY^2 = XY(aX + bY) = 0$, whose points at infinity are immediate, namely*

$$[0 : 1 : 0] \quad [1 : 0 : 0] \quad [b : -a : 0]$$

This leads to the Huff's model for elliptic curves, therefore odd cubics as defined in (3.1) enclose this model and lead eventually to new ones. Also, this time we have that $[1 : 0 : 0]$ is one of the points at infinity, which is not in conflict with the previous analysis since curves in Huff's model exclude X^3 from the defining equation.

[2] Heuristically speaking, as we shall see in section 4, the operation consists on considering the line between two points, and reflecting the third point of intersection with respect to the origin.

Interestingly enough, over a finite prime field $\mathbb{F}_p$, the relation $x^3 + ax^2y + bxy^2 + cy^3 = 0$ may not have non-trivial solutions, that is to say for some cubics none of the points at infinity are $\mathbb{F}_p$-rational.

Example 2 *An exhaustive search shows the relation $x^3+2x^2y+xy^2-2y^3 = 0$ has no non-trivial solutions in $K = \mathbb{F}_{11}$.*

3.1 Simplifying the Odd Cubic

Since an odd cubic in general form has five coefficients and given that curves in Weierstrass form have two or three coefficient, our first goal will be, if possible, to reduce the cubic down to three or two parameters.

We look to reduce coefficients as much as possible without loss of generality, so let's assume for instance that the cubic in the usual form has non-zero coefficients.

Let E/K be an odd cubic defined by f in general form. Broadly speaking, the linear map

$$\phi(x, y) = (sx + ty, ux + vy) \qquad s, t, u, v \in K, sv - tu \neq 0$$

produces another odd cubic when composed with f, nevertheless there are some interesting cases of such map we want to point out. The first interesting transformation for an odd cubic we consider comes from preserving their structure as much as possible, in geometric terms rotations and homotheties, namely maps of the form $\phi(x, y) = (sx + ty, -tx + sy)$ for some $s, t \in K$ such that $s^2 + t^2 \neq 0$, (a rotation if $s^2 + t^2 = 1$ and a homothety if $t = 0$). Hence, applying ϕ to the cubic yields

$$f(\phi(x, y)) = a_1(s, t)x^3 + a_2(s, t)x^2y + a_3(s, t)xy^2 + a_4(s, t)y^3 + a_5(s, t)x + a_6(s, t)y \tag{3.4}$$

where

$$\begin{aligned}
a_1(s, t) &= s^3 - ats^2 + bt^2s - ct^3 \\
a_2(s, t) &= as^3 + (3 - 2b)ts^2 + (3c - 2a)t^2s + bt^3 \\
a_3(s, t) &= bs^3 - (3c - 2a)ts^2 + (3 - 2b)t^2s - at^3 \\
a_4(s, t) &= cs^3 + bts^2 + at^2s + t^3 \\
a_5(s, t) &= ds - et \\
a_6(s, t) &= es + dt
\end{aligned} \tag{3.5}$$

so the question is under what conditions there exist $s, t \in K$ such that some $a_i(s, t)$ cancels. Also, it is easily checked that if $t = 0$ or $s = 0$, the substitution yields to one of the maps: $\phi_1(x, y) = (sx, sy)$ or $\phi_2(x, y) = (ty, -tx)$, none of which reduces any coefficient in the resulting equation, thus without loss of generality, we can assume that s and t are both non-zero.

There are two basic cases when dealing with odd cubics: 1) $a_1 = a_4 = 0$, which gives a curve in Huff model, and 2) when at least one of a_1 or a_4 is non-zero. Although the earlier is treated in [9], it is important to note these models are only possible if the group over F_q contains a subgroup isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which means this model is only possible for a subset of all curves, and therefore is less general. Our interest is therefore for the second case, which is more general (and in fact always possible to obtain). For completeness, we state a theorem (§3.1, [9]) where we see that we have a wider requirement for E/K in order to be birationally equivalent to a curve in Huff's form.

Theorem 3.1 *Let E/K be an elliptic curve with K a perfect field of characteristic $\neq 2$ that contains a subgroup $\mathbb{G}$ isomorphic $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then E is birationally equivalent over K to a curve in Huff's form.*

Without loss of generality, we will assume that $a_1 \neq 0$ (otherwise the transformation with $s = 0$, $t = 1$ "interchanges" x and y and gives $a_1 \neq 0$). Furthermore, we will normalize the equation, dividing it by a_1 so the coefficient of x^3 is 1. All further simplifications will start from these conditions.

Since a_4 is the coefficient of y^3 of $f(\phi(x, y))$, we could try to find a pair $(s, t) \in K$ such that $a_4(s, t) = 0$, which is always possible[3] so after normalizing we have an equation of the form

$$f_0(x, y) = x^3 + b_1x^2y + b_2xy^2 + b_3x + b_4y \tag{3.6}$$

We have the following result concerning simpler versions of odd cubics that later will have each one their specific features.

Lemma 3.1 *Let E/K be an odd cubic in general form defined by f with $de \neq 0$, then we can transform f into*

$$f_1(x, y) = x^3 + ax^2y + bxy^2 + cy^3 - y$$

and

$$f_2(x, y) = x^3 + ax^2y + bxy^2 + x - y$$

Proof: For the first case (when $a_4 \neq 0$) we can choose $s, t \in K$ such that $a_5(s, t) = ds - et$ in the system (3.5) is equal to 0, leading to

$$f(x, y) = x^3 + a'x^2y + b'xy^2 + c'y^3 + e'y$$

where a', b', c', e' are the resulting constants in K. Consider now the transformation $y \mapsto -y/e'$, obtaining

$$f_1(x, y) = x^3 + a''x^2y + b''xy^2 + c''y^3 - y$$

For the second case ($a_4 = 0$), we first transform f into f_0 as given in (3.6). Next consider the transformation $y \mapsto -(b_3/b_4)y$, where we obtain

$$f(x, y) = x^3 + a'x^2y + b'xy^2 + b_3x - b_3y$$

[3] Observe that when divided by s^3, a_4 is essentially a degree 3 polynomial in the variable (t/s) over an algebraically closed field.

Now, for $\lambda \in K$ such that $\lambda^2 = b_3$, the map $(x, y) \mapsto (\lambda x, \lambda y)$ yields

$$\begin{aligned} & \lambda^3(x^3 + a'x^2y + b'xy^2) + b_3\lambda(x - y) = 0 \\ \Longrightarrow \quad & x^3 + a'x^2y + b'xy^2 + x - y = 0 \quad \blacksquare \end{aligned}$$

As a result we consider two additional forms of cubics

Definition 3.4 *An odd cubic E/K represented by*

$$f(x, y) = x^3 + ax^2y + bxy^2 + y^3 - y$$

is said to be in **first form***, and if*

$$f(x, y) = x^3 + ax^2y + bxy^2 + x - y$$

than E is said to be in **second form***.*

The first one having the advantage of a nice condition about its singularity and being immediately irreducible, whereas the second one entails a faster computation of the group law.

3.2 Singularities

Last but not least, we determine the singularities of an odd cubic. Since any odd cubic with non trivial linear part can be reduced to an equation in first form, we consider first a cubic with this expression to begin with. We look at the partial derivatives of its projective version

$$\begin{aligned} \frac{\partial F}{\partial X} &= 3X^2 + 2aXY + bY^2 \\ \frac{\partial F}{\partial Y} &= aX^2 + 2bXY + 3Y^2 - Z^2 \\ \frac{\partial F}{\partial Z} &= -2YZ \end{aligned}$$

and check what happens when (if possible) all of them are zero. Hence the following result

Proposition 3.2 *Let E be and odd cubic in first form, then E is non-singular if and only if $4(a^3 + b^3) - a^2b^2 - 18ab + 27 \neq 0$.*

Proof: Observe first that $Y = 0 \Longrightarrow X = Z = 0$ which is not possible, so we make $Y = 1$ and $Z = 0$, that gives the relations

$$3X^2 + 2aX + b = 0 = aX^2 + 2bX + 3$$

which holds if and only if one of $(-a \pm \sqrt{a^2-3b})/3$ is equal to one of $(-b \pm \sqrt{b^2-3a})/a$. Let us explore this briefly

$$\begin{aligned}
& \frac{-a \pm \sqrt{a^2-3b}}{3} = \frac{-b \pm \sqrt{b^2-3a}}{a} \\
\Longleftrightarrow\ & -a^2 \pm a\sqrt{a^2-3b} = -3b \pm 3\sqrt{b^2-3a} \\
\Longleftrightarrow\ & 3b - a^2 = \mp a\sqrt{a^2-3b} \pm 3\sqrt{b^2-3a} \\
\Longleftrightarrow\ & (3b-a^2)^2 = a^2(a^2-3b) + 3^2(b^2-3a) \pm 6a\sqrt{(a^2-3b)(b^2-3a)} \\
\Longleftrightarrow\ & 3^2a - a^2b = \pm 2a\sqrt{(a^2-3b)(b^2-3a)} \\
\Longleftrightarrow\ & (3^2-ab)^2 = 4(a^2b^2 + 3^2ab - 3a^3 - 3b^3) \\
\Longleftrightarrow\ & 81 + a^2b^2 - 18ab = 4a^2b^2 + 36ab - 12a^3 - 12b^3 \\
\Longleftrightarrow\ & 4(a^3+b^3) - a^2b^2 - 16ab + 27 = 0 \quad \blacksquare
\end{aligned}$$

From this relation we find a couple of ways of producing non-singular curves, such as considering $ab = 1$, which simplifies the requirement to $a^3 + b^3 \neq -5/2$, which is certainly easier to compute.

For odd cubics in second form, applying the same ideas we have:

$$\frac{\partial F}{\partial X} = 3X^2 + 2aXY + bY^2 + Z^2 \tag{3.7}$$

$$\frac{\partial F}{\partial Y} = aX^2 + 2bXY - Z^2 \tag{3.8}$$

$$\frac{\partial F}{\partial Z} = 2(X-Y)Z \tag{3.9}$$

this time we have

Proposition 3.3 *Let E be and odd cubic in second form, then E is non-singular if and only if* $(1+a+b)(a^2b-4b^2) \neq 0$.

Proof: Suppose $Z \neq 0$, then from (3.9) $X = Y$, so we have the system

$$X^2(3+2a+b) + Z^2 = 0 \quad \wedge \quad X^2(a+2b) - Z^2 = 0$$

so if either $X = 0$, $3 + 2a + b = 0$ or $a + 2b = 0$, then $Z = 0$, a contradiction. Adding them up we obtain $3X^2(1 + a + b) = 0$, which is true if and only if $1 + a + b = 0$. In which case we have the singular points $[1 : 1 : \pm\sqrt{a+2b}]$

Say now $Z = 0$, then we have the system

$$3X^2 + 2aXY + bY^2 = 0 \quad \wedge \quad aX^2 + 2bXY = 0$$

which holds if and only if one of $(-a \pm \sqrt{a^2-3b})/3$ is equal to $-2b/a$, when developed

$$\begin{aligned}
& \frac{-a \pm \sqrt{a^2-3b}}{3} = \frac{-2b}{a} \\
\Longleftrightarrow\ & -a^2 \pm a\sqrt{a^2-3b} = -6b \\
\Longleftrightarrow\ & a^2(a^2-3b) = (a^2-6b)^2 \\
\Longleftrightarrow\ & -3a^2b = -12a^2b + 36b^2 \\
\Longleftrightarrow\ & a^2b - 4b^2 = 0
\end{aligned}$$

This way we require both $1 + a + b$, and $a^2b - 4b^2$ to be different from 0 in order to have a non-singular cubic. $\blacksquare$

As we see, this conditions is somewhat easier to manipulate than the first one in order to produce non-singular cubics.

4 Group Law

We describe first a general method for the group operation we want to consider with E in general form. As well as in the case for elliptic curves, we want to mimic the action of taking two points and obtaining a third one. At first we follow the convention that if $P = (x, y)$, then $P' = (-x, -y)$.

Definition 4.1 (Group Law) *Let E/K an odd cubic. Given P and Q two points on the cubic E, consider the line L between them. L passes through P, Q and a third point R. Reflect this point with respect to the origin to obtain R' and write $R' = P \oplus Q$.*

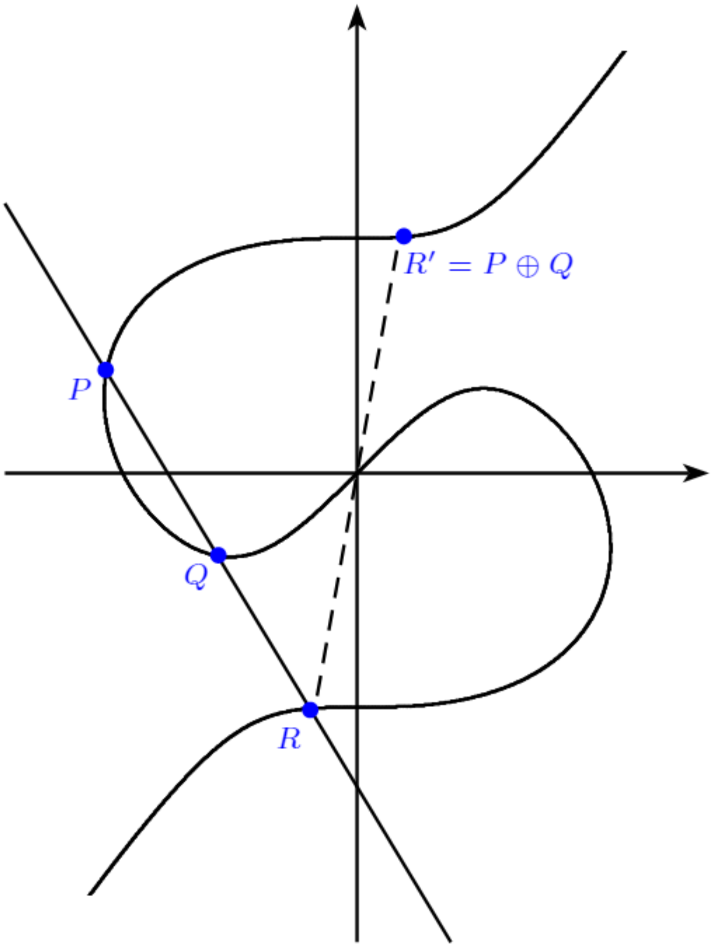


Figure 2: Representation of the group law in $\mathbb{A}^2(\mathbb{R})$

We use $\oplus$ first since this process could be seen as addition of points, and as it turns out, $(E, \oplus)$ is actually an abelian group with (0,0) being the identity element (or just 0).

Proposition 4.1 *Let E/K be a non-singular odd cubic. $(E, \oplus)$ is an abelian group. Namely*

1. *$(E, \oplus)$ is closed.*
2. *$A \oplus B = B \oplus A$ for every $A, B \in E$.*
3. *$A \oplus 0 = A$ for every $A \in E$.*
4. *$A \oplus (A') = 0$ for all $A \in E$.*
5. *$(A \oplus B) \oplus C = A \oplus (B \oplus C)$ for every $A, B, C \in E$.*

Proof:

1. Follows from Bezout's theorem, since an odd cubic has degree 3 and a line has degree 1.
2. Clear from definition (4.1), since the line between two points does not depend on the order the points are taken.
3. Suppose $A = [\alpha : \beta : \gamma]$ not all zero, then the line between A and 0 is $\beta X - \alpha Y = 0$ (projectively) and observe that $A' = [-\alpha : -\beta : \gamma]$ also satisfies this relation, so the line between A and 0, intersects E again at A', whose reflection is A.
4. A similar argument as before shows that the line between A and A', intersects E again at 0, whose reflection is itself.
5. We sketch the proof of this part as a consequence of the Max Noether's fundamental theorem (§ 5.6 of [6]).

   As shown in the diagram bellow, consider A, B, C and the auxiliaries $D, D'F, F'$ such that $A \oplus B = F'$, $C \oplus F' = G'_1$, $B \oplus C = D'$ and $A \oplus D' = G'_2$, from which we obtain $(A \oplus B) \oplus C = G'_1$ and $A \oplus (B \oplus C) = G'_2$, so we only need to show $G_1 = G_2$. Using intersection cycles consider the lines L_1, L_2, L_3 and M_1, M_2, M_3 such that

   $$L_1 \bullet E = A + B + F, \quad M_1 \bullet E = F + O + F' \quad L_2 \bullet E = F' + G_1 + C$$

   $$M_2 \bullet E = B + C + D, \quad L_3 \bullet E = D + O + D' \quad M_3 \bullet E = D' + G_2 + A$$

   Now consider the cubics $C_1 = L_1 L_2 L_3$ and $C_2 = M_1 M_2 M_3$, and let L be a line through G_1 that does not pass through G_2 so $L \bullet E = G_1 + P + Q$ (for some other P and Q), then

   $$\begin{aligned} LC_2 \bullet E &= L \bullet E + C_2 \bullet E \\ &= (G_1 + P + Q) + (A + B + C + D + D' + F + F' + G_2 + O) \\ &= (G_2 + P + Q) + (A + B + C + D + D' + F + F' + G_1 + O) \\ &= (G_2 + P + Q) + C_1 \bullet E \end{aligned}$$

   so there exists a line L_0 such that $L_0 \bullet E = G_2 + P + Q$, which means the points G_2, P, Q belong to E and are collinear, and observe that the same is true for the points G_1, P, Q, therefore since both lines contain P and Q, we have $L = L_0$ and $G_1 = G_2$. ■

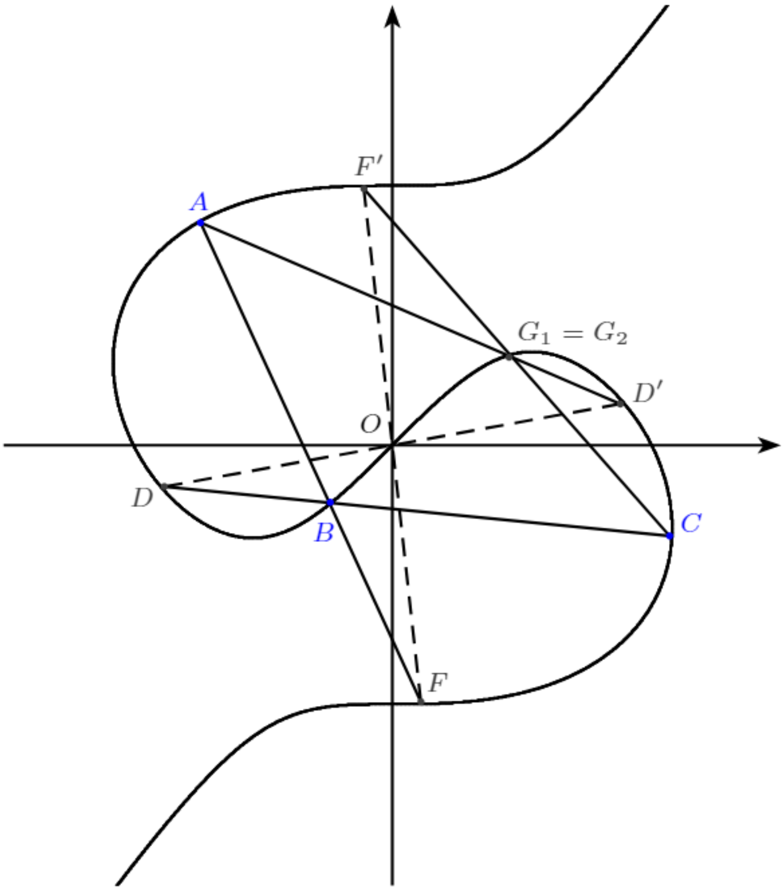


Figure 3: Associativity of composition

Now it is straightforward that for a point A on the cubic A' acts as its inverse, so from now on we write $-A$ instead and because of the proposition we use the $+$ sign for the operation instead.

Remark 4.1 *Observe that if $P = [\alpha : 1 : 0]$, then $[\alpha : 1 : 0] = [-\alpha : -1 : 0] = -P$ so $P = -P$, i.e. the points at infinity are of 2-torsion.*

4.1 Addition formulae

We give now explicit formulae for the addition of points in a very general fashion before digging into particular cases.

1. On E, consider the points $P = (x_0, y_0)$ and $Q = (x_1, y_1)$ for the moment assumed to be affine, so the line L between them is

$$L \quad : \quad y = \lambda x + \mu \tag{4.1}$$

where λ is the slope of the line and $\mu = y_1 - \lambda x_1$ and suppose for instance $x_0 \neq x_1$, so evaluating in the points we have the system

$$\begin{aligned} x_0^3 + ax_0^2y_0 + bx_0y_0^2 + cy_0^3 + dx_0 + ey_0 &= 0 \\ x_1^3 + ax_1^2y_1 + bx_1y_1^2 + cy_1^3 + dx_1 + ey_1 &= 0 \end{aligned}$$

subtracting and factoring

$$\begin{aligned}
0 &= x_1^3 - x_0^3 + a(x_1^2 y_1 - x_0^2 y_0) + b(x_1 y_1^2 - x_0 y_0^2) + c(y_1^3 - y_0^3) + d(x_1 - x_0) + e(y_1 - y_0) \\
&= (x_1 - x_0)(x_1^2 + x_1 x_0 + x_0^2 + a(x_1 + x_0) y_1 + b y_1^2 + d) \\
&\quad +(y_1 - y_0)(c(y_1^2 + y_1 y_0 + y_0^2) + a x_0^2 + b x_0 (y_1 + y_0) + e) \\
\frac{y_1 - y_0}{x_1 - x_0} &= -\frac{x_1^2 + x_1 x_0 + x_0^2 + a(x_1 + x_0) y_1 + b y_1^2 + d}{a x_0^2 + b x_0 (y_1 + y_0) + c(y_1^2 + y_1 y_0 + y_0^2) + e}
\end{aligned}$$

which gives the usual form of the slope. For $P = Q$, we use implicit differentiation to obtain the slope

$$\begin{aligned}
& x^3 + ax^2 y + bxy^2 + cy^3 + dx + ey = 0 \\
\Longrightarrow\ & x'(3x^2 + 2axy_1 + by^2 + d) + y'(ax^2 + 2bxy + 3cy^2 + e) = 0 \\
\Longrightarrow\ & \frac{y'}{x'} = -\frac{3x^2 + 2axy + by^2 + d}{ax^2 + 2bxy + 3cy^2 + e}
\end{aligned}$$

thus we have

$$\lambda = \begin{cases} (y_1 - y_0)/(x_1 - x_0) & \text{if } P \neq Q \\ -\dfrac{3x_1^2 + 2ax_1y_1 + by_1^2 + d}{ax_1^2 + 2bx_1y_1 + 3cy_1^2 + e} & \text{if } P = Q \end{cases} \tag{4.2}$$

Replacing (4.1) in the cubic in general form gives us

$$\alpha(\lambda)x^3 + \beta(\lambda)x^2 + \gamma(\lambda)x + \delta(\lambda) = 0 \tag{4.3}$$

where

$$\begin{aligned}
\alpha(\lambda) &= c\lambda^3 + b\lambda^2 + a\lambda + 1 \\
\beta(\lambda) &= (y_1 - \lambda x_1)(a + 2b\lambda + 3c\lambda^2) = \mu\alpha'(\lambda) \\
\gamma(\lambda) &= (e\lambda + d + b(y_1 - \lambda x_1)^2 + 3c(y_1 - \lambda x_1)^2\lambda) = e\lambda + d + \mu^2\alpha''(\lambda)/2 \\
\delta(\lambda) &= c(y_1 - \lambda x_1)^3 + e(y_1 - \lambda x_1) = c\mu^3 + e\mu
\end{aligned}$$

and we consider α' and α'' as formal derivatives with $\alpha(\lambda) \neq 0$. Let $-R = (x_2, y_2)$ be the third point of intersection between (4.1) and the cubic, so x_2 is the third solution of (4.3). The following relations hold[4]

$$x_0 + x_1 + x_2 = -\frac{\beta(\lambda)}{\alpha(\lambda)}, \quad x_0x_1 + x_1x_2 + x_2x_0 = \frac{\gamma(\lambda)}{\alpha(\lambda)}, \quad x_0x_1x_2 = -\frac{\delta(\lambda)}{\alpha(\lambda)} \tag{4.4}$$

and from the first one we obtain $x_2 = -\dfrac{\mu\alpha'(\lambda)}{\alpha(\lambda)} - x_0 - x_1$, so using (4.1) again we find

$$P + Q = R = (-x_2, -y_2) = \left(\frac{\mu\alpha'(\lambda)}{\alpha(\lambda)} + x_0 + x_1, \lambda\left(\frac{\mu\alpha'(\lambda)}{\alpha(\lambda)} + (x_1 + x_0)\right) - \mu\right)$$

$$R = \left(\frac{\mu\alpha'(\lambda)}{\alpha(\lambda)} + x_0 + x_1, \frac{\mu(\alpha'(\lambda)\lambda - \alpha(\lambda))}{\alpha(\lambda)} + \lambda(x_1 + x_0)\right) \tag{4.5}$$

[4] If $(x-a)(x-b)(x-c) = x^3 + d_1x^2 + d_2x + d_3$, then $d_1 = -(a+b+c)$, $d_2 = ab + bc + ac$ and $d_3 = -abc$

2. With the same conditions as before except with $\alpha(\lambda) = 0$, we have
$$\beta(\lambda)x^2 + \gamma(\lambda)x + \delta(\lambda) = 0$$
which has two solutions, so the third point of intersection occurs at infinity, say $R_\infty = [\lambda^{-1} : 1 : 0]$[5]. Indeed, P and Q satisfy the cubic and for R_∞ we look at its projective form and evaluate
$$\begin{aligned} X^3 + aX^2Y + bXY^2 + cY^3 + dXZ^2 + eYZ^2|_{R_\infty} &= (\lambda^{-1})^3 + a(\lambda^{-1})^2 + b(\lambda^{-1}) + c \\ &= (\lambda^{-3})\underbrace{(1 + a\lambda + b\lambda^2 + c\lambda^3)}_{\alpha(\lambda)} \\ &= 0 \end{aligned}$$
Therefore $P + Q = R_\infty = [\lambda^{-1} : 1 : 0]$ where λ depends on whether $P = Q$ or not (see (4.2)).

Remark 4.2 *We have indirectly shown that whenever we have a point at infinity, say $\tilde{P} = [\lambda^{-1} : 1 : 0]$, then $\alpha(\lambda) = 0$.*

3. Suppose now that $x(P) = x(Q) = x_0$ (i.e. P and Q have the same $x-$coordinate) and the line L between P and Q has unbounded slope. In this case
$$L \;:\; x = x_0$$
so when replaced in the equation of the cubic yields
$$x_0^3 + ax_0^2y + bx_0y^2 + cy^3 + dx_0 + ey = 0$$
where, once we look at the coefficients
$$\begin{aligned} y_0 + y_1 + y_2 = -\frac{bx_0}{c} &\implies y_2 = -\frac{bx_0}{c} - y_0 - y_1 \\ &\implies P + Q = (-x_0, \frac{bx_0}{c} + y_0 + y_1) \end{aligned}$$
Provided that $c \neq 0$. If $c = 0$, we look at the projective form of the cubic, i.e.
$$X^3 + aX^2Y + bXY^2 + dXZ^2 + eYZ^2 = 0$$
whose solutions are $[x_0 : y_0 : 1]$, $[x_0 : y_1 : 1]$ and $[0 : 1 : 0]$, so $P + Q = [0 : 1 : 0]$.

4. Suppose now we add $P = (x_0, y_0) \neq 0$ with a point at infinity, say $Q_\infty = [\lambda_1^{-1} : 1 : 0]$. We consider P in projective form as $P = [x_0 : y_0 : 1]$. According to part 2 we have that $\alpha(\lambda_1) = 0$, so again $\beta(\lambda_1)x^2 + \gamma(\lambda_1)x + \delta(\lambda_1) = 0$ and if $-R = (x_2, y_2)$ is the remaining point of intersection we have
$$x_0 + x_2 = -\frac{\gamma(\lambda_1)}{\beta(\lambda_1)}, \quad x_0x_2 = \frac{\delta(\lambda_1)}{\beta(\lambda_1)} \tag{4.6}$$

[5] As mentioned in section 3, $[0 : 1 : 0]$ is never a solution of the projective form of the cubic, so λ is actually non-zero.

provided $\alpha'(\lambda_1) \neq 0$. This way, with $\mu = y_0 - \lambda_1 x_0$, $P + Q_\infty = R$ where

$$\begin{aligned}
R &= \left(x_0 + \frac{\gamma(\lambda_1)}{\beta(\lambda_1)}, \lambda_1 \left(x_0 + \frac{\gamma(\lambda_1)}{\beta(\lambda_1)}\right) - \mu\right) \\
R &= \left(x_0 + \frac{e\lambda_1 + d + \mu^2(b + 3c\lambda_1)}{\mu(a + 2b\lambda_1 + 3c\lambda_1^2)}, \lambda_1 \left(x_0 + \frac{e\lambda_1 + d + \mu^2(b + 3c\lambda_1)}{\mu(a + 2b\lambda_1 + 3c\lambda_1^2)}\right) - \mu\right) \\
R &= \left(x_0 + \frac{\mu^2(b + 3c\lambda_1) + d + e\lambda_1}{\mu(a + 2b\lambda_1 + 3c\lambda_1^2)}, \lambda_1 x_0 + \frac{\lambda_1(d + e\lambda_1) - \mu^2(b\lambda + a)}{\mu(a + 2b\lambda_1 + 3c\lambda_1^2)}\right)
\end{aligned}$$

5. Now we add two points at infinity, say $P_\infty = [\lambda_0^{-1} : 1 : 0]$ and $Q_\infty = [\lambda_1^{-1} : 1 : 0]$. In this case both points satisfy $X^3 + aX^2Y + bXY^2 + cY^3 = 0$ so if $R_\infty = [\lambda_2^{-1} : 1 : 0]$ is the third point at infinity then

$$X^3 + aX^2Y + bXY^2 + cY^3 = (X - \lambda_0 Y)(X - \lambda_1 Y)(X - \lambda_2 Y)$$

therefore we have that $P_\infty + Q_\infty = R_\infty$ which means that the points at infinity, altogether with the origin form the Klein group V.

Remark 4.3 *Observe that since each of the five cases just listed takes elements in K and produces rational combinations, then $(E, +)$ is actually closed in any subfield $k \subsetneq K$,*

4.1.1 Extra Formulae

As seen at the beginning of the previous part, making $\Delta x := x_1 - x_0$ and $\Delta y := y_1 - y_0$ we obtain

$$\lambda = \frac{\Delta y}{\Delta x} = -\frac{x_1^2 + x_0 x_1 + x_0^2 + a y_1(x_0 + x_1) + b y_1^2 + d}{a x_0^2 + b x_0(y_0 + y_1) + c(y_1^2 + y_0 y_1 + y_0^2) + e}$$

Using the other relations in (4.4) we find different forms for x_2

$$\begin{aligned}
\frac{x_0 + x_1 + x_2}{\beta(\lambda)} = \frac{x_0 x_1 x_2}{\delta(\lambda)} &\implies \beta(\lambda) x_0 x_1 x_2 - \delta(\lambda) x_2 = \delta(\lambda)(x_0 + x_1) \\
&\implies x_2 = \frac{\delta(\lambda)(x_1 + x_0)}{\beta(\lambda) x_1 x_0 - \delta(\lambda)} \\
&\implies x_2 = \frac{(c\mu^2 + e)(x_1 + x_0)}{\alpha'(\lambda) x_1 x_0 - (c\mu^2 + e)} \qquad (4.7)
\end{aligned}$$

which comes in handy when E is in second form, in such case $c = 0$, $d = -e = 1$ so

$$x_2 = \frac{-(x_1 + x_0)}{1 + \alpha'(\lambda) x_1 x_0} \Longrightarrow P + Q = \left(\frac{x_1 + x_0}{(2b\lambda + a)x_1 x_0 + 1}, \frac{\lambda(x_1 + x_0)}{(2b\lambda + a)x_1 x_0 + 1} - \mu\right) \qquad (4.8)$$

One of the benefits of this form is that it lowers the exponents of the λ's so it's easier to compute. But there is a small setback, the formula assumes that $x_0 = -x_1$ implies $P = -Q$ which is no necessarily true.

Another interesting case is $b = c = 0$, where the y coordinate can immediately be isolated from the equation defining the curve, turning the addition (4.7) into

$$R = \left(\frac{e(x_1 + x_0)}{e - ax_1x_0}, \frac{-x_2^3 - dx_2}{ax_2^2 + e} \right)$$

This case we shall develop further in section 5.

Remark 4.4 *Let $K = \mathbb{F}_q$ with $q = p^k$. When f is in general form, finding a non trivial solution to $X^3 + aX^2Y + bXY^2 + cY^3 = 0$ when we calculate the points at infinity, is equivalent to finding a solution of $\alpha(\lambda) = c\lambda^3 + b\lambda^2 + a\lambda + 1$, so if there are no $K-$rational points at infinity, then the addition form (4.5) is well defined in K.*[6] *Hence, since $0 \in (E, +)$ and for any $P \in E$, $P \in (E, +)$ if and only if $-P \in (E, +)$, we find that $|(E, +)|$ is odd, and the addition formulae is reduced simply to that of (4.5).*

Curves without any K-rational points at infinity can be identified using the results in section 2.3.

[6] Observe that this last statement is also true in any extension K' of K provided the points at infinity are not $K'-$rational.

5 Particular Cases

In this section we explore particular cases of odd cubics with conditions on the coefficients, some of which have already been studied in other contexts.

5.1 Huff's Model for Elliptic Curves

Take now as starting point the most general odd cubic

$$f(x,y) = a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 + a_5x + a_6y$$

with $a_i \in K$ (usually $\mathbb{Q}$ or a finite field). Making $a_1 = a_4 = 0$, $a_2 + a_6 = a_3 + a_5 = 0$ yields

$$f(x,y) = a_2x^2y - a_5xy^2 + a_5x - a_2y$$

whose zero set is the Huff's model for an elliptic curve when $a_2a_5(a_2^2 - a_5^2) \neq 0$. We usually find this model in the form

$$ax(y^2-1) = by(x^2-1) \qquad a,b \in K \tag{5.1}$$

with $ab(a^2-b^2) \neq 0$ and K a field of odd characteristic.

As exposed by Joye, Tibouchi and Vergnaud in [9] and by Wu and Feng in [18], Huff's model has several interesting properties. We summarise some of them below, where the field considered is usually $\mathbb{Q}$ or a finite field of odd characteristic, which has its justification in the next problem.

Problem 5.1 (A Diophantine Problem) *Let $a, b \in \mathbb{Q}$ with $a \neq b$, find $x \in \mathbb{Q}$ such that, in $\mathbb{R}^2$ the distance from $(x, 0)$ to the points $(0, \pm a)$ and $(0, \pm b)$ are rational.*

Proposition 5.1 *(1.1, [9]) In the preceding problem, let u and v be solutions of the system*

$$x^2 + a^2 = u^2 \quad x^2 + b^2 = v^2$$

then the set of homogeneous equations $x^2 + a^2z^2 = u^2$, $x^2 + b^2z^2 = v^2$ define a curve of genus 1 in $\mathbb{P}^3$ birationally equivalent to the curve

$$ax(y^2-1) = by(x^2-1) \tag{5.2}$$

for some $a, b \in \mathbb{Q}$. This last curve defines an elliptic curve as long as $ab(a^2-b^2) \neq 0$, and the characteristic of the field is odd.

Proposition 5.2 *(2.1, [9]) Let H be a curve in Huff's model, using $(0,0)$ as the neutral element, the map*

$$\begin{aligned} \oplus : H \times H &\longmapsto H \\ (x_0,y_0) \oplus (x_1,y_1) &= \left(\frac{(x_0+x_1)(1+y_0y_1)}{(1+x_0x_1)(1-y_0y_1)}, \frac{(y_0+y_1)(1+x_0x_1)}{(1-x_0x_1)(1+y_0y_1)} \right) \end{aligned}$$

induces an abelian group whenever $x_0x_1 \neq \pm 1$ and $y_0y_1 \neq \pm 1$.

This map, altogether with specific algebraic relations (that do not quite hold for a more general case), is derived from the same group law we have already described and advantageously, this group law does not depend on parameters of the curve. Moreover, the formulae are *unified*, i.e. it can be used to double a point. Also the last requirement represents no complications since the operation happens to be *complete* for points of odd order, which means that the operation is closed for such points, whereas the points of even order are the points at infinity $[1:0:0], [0:1:0]$ and $[a:b:0]$.

5.2 A Simple Model

The next model comes from both looking for relevant properties on specific odd cubics and an efficient computation of the group law when $K=\mathbb{F}_p$, where some level of independence is reached (see the addition formula (4.8)). This time we consider the cubic as follows

$$E: f(x,y) = x^3 - x^2y + ax - by, \quad ab(a-b) \neq 0, -b \notin K^2$$

Observe first that the gradient of its projective version $F(X,Y,Z) = X^3 - X^2Y + (aX - bY)Z^2$ is

$$\nabla F = (3X^2 - 2XY + aZ^2, -X^2 - bZ^2, 2(aX - bY)Z)$$

which is null over K if and only if $[x:y:z] = [0:1:0]$. There are of course more solutions over $\bar{K}$, but again we are first interested to see what happens over K. Notice that since $-b \notin K^2$, then we can express the relation defining E in the form $y = (x^3+ax)/(x^2+b)$ so we actually have a function in the x variable from K to itself. As a consequence, two different points on E have always different x-coordinate (which is good for the group law). Also, for the slope at any given point $P=(x,y)$ we have the relation

$$\lambda = \frac{3x^2 - 2xy + a}{x^2 + b}$$

therefore, since $-b \notin K^2$, $x^2 + b \neq 0$ and the slope is always well defined.

Let us take a first look at a real example of a curve in this model

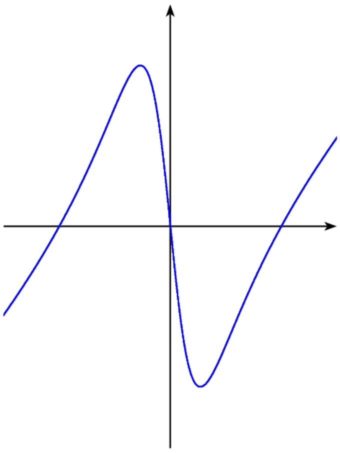


Figure 4: $x^3 - x^2y - x - y/10 = 0$

Regarding the composition of points and as seen in § 4.1.1, if $P = (x_0, y_0)$, $Q = (x_1, y_1)$ and $R = (x_2, y_2)$ such that $P + Q = R$, then

$$R = \left(\frac{b(x_0 + x_1)}{b - x_0 x_1}, \frac{x_2^3 + a x_2}{x_2^2 + b} \right) \tag{5.3}$$

so developing for y_2

$$\begin{aligned} \frac{x_2^3 + a x_2}{x_2^2 + b} &= \frac{b(x_0 + x_1)}{b - x_0 x_1} \frac{\left(\frac{b(x_0 + x_1)}{b - x_0 x_1} \right)^2 + a}{\left(\frac{b(x_0 + x_1)}{b - x_0 x_1} \right)^2 + b} \\ &= \frac{b(x_0 + x_1)}{b - x_0 x_1} \frac{(b^2 (x_0 + x_1)^2 + a(b - x_0 x_1)^2)}{(b^2 (x_0 + x_1)^2 + b(b - x_0 x_1)^2)} \\ &= \frac{(x_0 + x_1)}{b - x_0 x_1} \frac{(b^2 (x_0 + x_1)^2 + a(b - x_0 x_1)^2)}{(b(x_0 + x_1)^2 + (b - x_0 x_1)^2)} \end{aligned}$$

therefore

$$R = \left(\frac{b(x_0 + x_1)}{b - x_0 x_1}, \frac{(x_0 + x_1)}{b - x_0 x_1} \frac{(b^2 (x_0 + x_1)^2 + a(b - x_0 x_1)^2)}{(b(x_0 + x_1)^2 + (b - x_0 x_1)^2)} \right) \tag{5.4}$$

5.2.1 Projective Form and Cost

From the last expression we can easily produce its projective form (as seen in § 2.7)

$$\begin{aligned} X_2 &= b(X_0 Z_1 + X_1 Z_0)(b(X_0 Z_1 + X_1 Z_0)^2 + (b Z_0 Z_1 - X_0 X_1)^2) \\ Y_2 &= (X_0 Z_1 + X_1 Z_0)(b^2 (X_0 Z_1 + X_1 Z_0)^2 + a(b Z_0 Z_1 - X_0 X_1)^2) \\ Z_2 &= (b Z_0 Z_1 - X_0 X_1)(b(X_0 Z_1 + X_1 Z_0)^2 + (b Z_0 Z_1 - X_0 X_1)^2) \end{aligned} \tag{5.5}$$

This formula is however not well defined for the points at infinity $P_\infty = (1, 1, 0)$ and $Q_\infty = (0, 1, 0)$ (this last one with multiplicity 2). Nevertheless, as seen in section 4, we can still make sense of operating with P_∞ and Q_∞. Explicitly for the general case when $x_0 y_0 \neq 0$, $(x_0 : y_0 : 1) + Q_\infty = (-x_0 : -y_0 : 1)$, and $(x_0 : y_0 : 1) + P_\infty = (-b : -b + x_0 y_0 - x_0^2 : x_0)$.

Let **m** and **s** be the cost of multiplication and squaring in $\mathbb{F}_p$ respectively, then the costs for producing the forms in (5.5) is 11**m**+3**s**. Explicitly in more detail the earlier can be evaluated as

$$m_1 = X_0 Z_1, \quad m_2 = X_1 Z_0, \quad m_3 = Z_0 Z_1, \quad m_4 = X_0 X_1, \quad m_5 = b m_3, \quad m_6 = b(m_1 + m_2)$$

$$s_1 = (m_1 + m_2)^2, \quad s_2 = (m_5 - m_4)^2, \quad s_3 = m_6^2, \quad m_7 = (b s_1 + s_2), \quad m_8 = a s_2$$

$$m_9 = m_6 (b s_1 + s_2), \quad m_{10} = (m_1 + m_2)(s_3 + m_8), \quad m_{11} = (m_5 - m_4)(b s_1 + s_2)$$

so $X_2 = m_9$, $Y_2 = m_{10}$ and $Z_2 = m_{11}$.

This way we see a similar cost of calculation compared to that of curves in Huff's model, which is 12**m** (§2.2, [9]).

6 Maps

In this section we explore maps between odd cubics and maps from odd cubics to curves in Weierstrass form and vice versa. We briefly recall some definitions from [13] and [10] stated for elliptic curves over $\mathbb{P}^2(\bar{k})$.

Definition 6.1 (Rational Map) *Given E_1 and E_2 elliptic curves over k. We say that a map $\phi : E_1 \to E_2$ of the form*

$$\phi = [\phi_0, \phi_1, \phi_2]$$

where $\phi_i \in \bar{k}(E_1)$, is a rational map if for every $P \in E_1$ such that the ϕ_i are all defined,

$$\phi(P) = [\phi_0(P), \phi_1(P), \phi_2(P)] \in E_2$$

of course when we say defined we mean not all zero.

Definition 6.2 (Birational Map) *Given E_1 and E_2 elliptic curves over k. If there are rational maps $f : E_1 \to E_2$ and $g : E_2 \to E_1$ such that they are inverse of each other (except possibly at a finite set of points over $\bar{k}$), then we say that E_1 and E_2 are birational or birationally equivalent.*

Definition 6.3 (Regular Map) *Given E_1 and E_2 elliptic curves over k. We say that a rational map $\phi : E_1 \to E_2$ of the form*

$$\phi = [\phi_0, \phi_1, \phi_2]$$

where $\phi_i \in \bar{k}(E_1)$, is regular at $P \in E_1$ if there is a function $g \in \bar{k}(E_1)$ such that

(i) Each $g \circ \phi_i$ is well defined at P.

(ii) There is some i for which $(g \circ \phi_i)(P) \neq 0$

if such a g exists, then we set $\phi(P) = [(g \circ \phi_0)(P), (g \circ \phi_1)(P), (g \circ \phi_2)(P)]$.

Definition 6.4 (Morphism) *A rational map which is everywhere regular, is called morphism.*

Definition 6.5 (Isomorphism) *We say that two elliptic curves E_1 and E_2 are isomorphic if there are morphisms $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_1$ such that $\phi \circ \psi = I_{E_2}$ and $\psi \circ \phi = I_{E_1}$, i.e. the identity map on their respective curves. In such case we write $E_1 \cong E_2$.*

A couple of maps show up immediately as those seen in [16] (lecture 5):

- **Null Map:** Every odd cubic passes through the origin so we can trivially map any point on the curve to 0, therefore we have the map

$$\begin{array}{rccc} [0]: & E & \longrightarrow & E \\ & P & \longmapsto & 0 \end{array}$$

  or more explicitly $[0](x, y) = (0, 0)$ in affine coordinates.

- **Negation Map:** From the very beginning, we wanted the curve to satisfy the relation $f(-P) = -f(P)$, so the first non-trivial map that comes naturally is

$$\begin{array}{rccc} [-1]: & E & \longrightarrow & E \\ & P & \longmapsto & -P \end{array}$$

or more explicitly $[-1](x, y, z) = (-x, -y, z)$ in projective coordinates.

- **The Multiplication-by-m Map:** Since we have a group law that takes P and Q into $P + Q$, we can make sense of taking P to $2P$, and more generally for $m \in \mathbb{N}$, taking P to mP i.e. the map

$$\begin{array}{rccl} [m]: & E & \longrightarrow & E \\ & P & \longmapsto & mP = \underbrace{P + \ldots + P}_{m \text{ times}} \end{array}$$

By composing $[m]$ with $[-1]$ we can extend $[m]$ to any integer value of m, as $[m'] = [-m'] \circ [-1]$, thus we have a multiplication-by-m map for every $m \in \mathbb{Z}$. We show explicit formulae for the doubling map $[2]$ of a cubic in second form. From section 4.1 we see that when $P = Q$

$$\lambda = \frac{3x^2 + 2axy + by^2 + 1}{1 - 2bxy - ax^2} \tag{6.1}$$

so

$$[2](x, y) = \left(\frac{(y - \lambda x)(a + 2b\lambda)}{b\lambda^2 + a\lambda + 1} + 2x, \frac{(y - \lambda x)(b\lambda^2 - 1)}{b\lambda^2 + a\lambda + 1} + 2x\lambda \right) \tag{6.2}$$

or the equivalent form (recall third relation in (4.4))

$$[2](x, y) = \left(\frac{(\lambda x - y)}{(b\lambda^2 + a\lambda + 1)x^2}, \frac{(\lambda x - y)(\lambda + x^2(b\lambda^2 + a\lambda + 1))}{(b\lambda^2 + a\lambda + 1)x^2} \right) \tag{6.3}$$

when $P \neq 0$ (note that from (6.2) we obtain $[2]P = P$ when $P = 0$). To reduce the degree of the λ's we perform the following calculation, applying the same principle shown in § 2.6

$$\begin{aligned}
\frac{(y - \lambda x)(a + 2b\lambda)}{b\lambda^2 + a\lambda + 1} + 2x &= \frac{(\lambda x - y)}{(b\lambda^2 + a\lambda + 1)x^2} \\
\frac{(y - \lambda x)(a + 2b\lambda) + 2x(b\lambda^2 + a\lambda + 1)}{b\lambda^2 + a\lambda + 1} &= \frac{(\lambda x - y)}{(b\lambda^2 + a\lambda + 1)x^2} \\
\frac{(y - \lambda x)(a + 2b\lambda) + 2x(b\lambda^2 + a\lambda + 1)}{b\lambda^2 + a\lambda + 1} &= \frac{-(y - \lambda x)(a + 2b\lambda)}{(b\lambda^2 + a\lambda + 1)x^2(a + 2b\lambda)} \\
\frac{(y - \lambda x)(a + 2b\lambda) + 2x(b\lambda^2 + a\lambda + 1) - (y - \lambda x)(a + 2b\lambda)}{b\lambda^2 + a\lambda + 1 + (b\lambda^2 + a\lambda + 1)x^2(a + 2b\lambda)} &= \frac{(\lambda x - y)(a + 2b\lambda)}{(b\lambda^2 + a\lambda + 1)x^2(a + 2b\lambda)} \\
\frac{2x(b\lambda^2 + a\lambda + 1)}{(b\lambda^2 + a\lambda + 1)(1 + x^2(a + 2b\lambda))} &= \frac{(\lambda x - y)(a + 2b\lambda)}{(b\lambda^2 + a\lambda + 1)x^2(a + 2b\lambda)} \\
\frac{2x}{1 + x^2(a + 2b\lambda)} &= \frac{(\lambda x - y)}{(b\lambda^2 + a\lambda + 1)x^2}
\end{aligned}$$

so $x_2 = \dfrac{2x}{1 + x^2(a + 2b\lambda)}$, and simplifying for λ

$$\begin{aligned}\frac{2x}{1+x^2(a+2b\lambda)} &= \frac{2x(1-2bxy-ax^2)}{(1+ax^2)(1-2bxy-ax^2)+2bx^2(3x^2+2axy+by^2+1)}\\ &= \frac{2x(1-2bxy-ax^2)}{1-a^2x^4+4bx^4},\end{aligned}$$

whereas for y_2

$$\begin{aligned}y_2 &= \frac{2x\lambda(1-2bxy-ax^2)}{1-a^2x^4+4bx^4}-\mu\\ &= \frac{2x(3x^2+2axy+by^2+1)}{1-a^2x^4+4bx^4}-y+\lambda x\\ &= \frac{2x(3x^2+2axy+by^2+1)(1-2bxy-ax^2)-y(1-a^2x^4+4bx^4)(1-2bxy-ax^2)}{(1-a^2x^4+4bx^4)(1-2bxy-ax^2)}\\ &\quad+\frac{x(3x^2+2axy+by^2+1)(1-a^2x^4+4bx^4)}{(1-a^2x^4+4bx^4)(1-2bxy-ax^2)}\\ &= \frac{2x((a^2-4b)x^4+(2a+4b)x^2+1)}{(1-a^2x^4+4bx^4)(1-2bxy-ax^2)}\end{aligned}$$

so finally

$$[2](x,y)=\left(\frac{2x(1-2bxy-ax^2)}{1-a^2x^4+4bx^4},\frac{2x((a^2-4b)x^4+(2a+4b)x^2+1)}{(1-a^2x^4+4bx^4)(1-2bxy-ax^2)}\right)$$

Using that $(1-2bxy-ax^2)^2=(a^2-4b)x^4-(2a+4b)x^2+1$, the projective form of the map is now straightforward

$$\begin{aligned}[2]_x(X,Y,Z) &= 2XZ((a^2-4b)X^4-(2a+4b)X^2Z^2+Z^4)\\ [2]_y(X,Y,Z) &= 2XZ((a^2-4b)X^4+(2a+4b)X^2Z^2+Z^4)\\ [2]_z(X,Y,Z) &= ((a^2-4b)X^4-Z^4)(aX^2+2bXY-Z^2)\end{aligned}$$

Nevertheless, a calculation shows that this form of [2] is not well defined for $(0,1,0)$ and $(x,y,0)$ with $ax+2by=0$, so we need to find an alternative version of the map. In the first case we use that

$$\frac{X^2+aXY+bY^2}{Z^2}=\frac{Y-X}{X}$$

multiplying each coordinate of [2] by $\dfrac{(Y-X)^3}{X^3}$, so after developing we find

$$\begin{aligned}[2]_x(X,Y,Z) &= 2(Y-X)Z((a^2-4b)X^2(Y-X)^2-(2a+4b)(Y-X)^2Z^2+(X^2+aXY+bY^2)^2)\\ [2]_y(X,Y,Z) &= 2(Y-X)Z((a^2-4b)X^2(Y-X)^2+(2a+4b)(Y-X)^2Z^2+(X^2+aXY+bY^2)^2)\\ [2]_z(X,Y,Z) &= ((a^2-4b)X^2(Y-X)^2-(X^2+aXY+bY^2)^2)\\ &\quad\cdot((aX+2bY)(Y-X)-(X^2+aXY+bY^2))\end{aligned}$$

so $[2](0,1,0)=(0,0,-b^3)=(0,0,1)$ when $b\neq 0$. In the second case, after disregarding the trivial solution, when developing the condition $ax+2by=0$ we find that $(x,y,0)\in E$ if and only if $a^2-4b=0$, but we have already imposed the condition for a^2-4b to be a non-zero (end §3), so we no longer need to worry about this case. This representation shows that [2] is everywhere regular, i.e. a morphism.

- **The Frobenius Map:** Let $K = \mathbb{F}_p$. From the usual Frobenius automorphism π over $\bar{K}$ we can make sense of the map $\pi_E : E(\bar{K}) \to E(\bar{K})$ such that $\pi_E(x, y, z) = (x^p, y^p, z^p)$. Observe that for $a, b \in \mathbb{F}_p$

$$\begin{aligned}(x^3 + ax^2y + bxy^2 + (x-y)z^2)^p &= (x^3)^p + (ax^2y)^p + (bxy^2)^p + ((x-y)z^2)^p \\ &= (x^p)^3 + a^p(x^p)^2y^p + b^px^p(y^p)^2 + (x-y)^p(z^2)^p \\ &= (x^p)^3 + a(x^p)^2y^p + bx^p(y^p)^2 + (x^p - y^p)(z^p)^2\end{aligned}$$

so for any point $P = (x, y, z)$, $\pi_E(P) = (x^p, y^p, z^p) \in E(\bar{K})$.

- **The Rotation Map:** This special case of a rational map was already described in section 3.1. Consider in $\mathbb{F}_p$ the matrix

$$M = \begin{pmatrix} s & -t \\ t & s \end{pmatrix}$$

with $s^2 + t^2 = 1$, so (in geometric terms) M rotates the axis counterclockwise with respect to the origin. It inherits the same ideas of rotating objects in $\mathbb{R}^2$. For instance, the matrix

$$M = 108 \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$$

will take the line $y + 2x = 0$ into the line $x = 0$. In parallel, observe that in $\mathbb{R}^2$ the required values of s and t would be

$$s = \frac{2}{\sqrt{5}} \quad t = \frac{1}{\sqrt{5}}$$

so we have to make sense of the inverse of $\sqrt{5}$ in $\mathbb{F}_p$ in order to proceed. One of its possible values being 108.

Now, depending on the form of the cubic we are using, different types of maps between curves arise, such as

- Given E_1 and E_2 as

$$\begin{aligned}E_1 &: x^3 + bxy^2 + cy^3 - y = 0 \\ E_2 &: x^3 + Bxy^2 + Cy^3 - y = 0\end{aligned}$$

the map $\phi : E_1 \to E_2$ such that $\phi(x, y) = (\lambda x, \lambda^3 y)$ is a linear change of coordinates when $B\lambda^4 = b$ and $C\lambda^6 = c$. Let f be the relation defining E_1, observe that if $\phi'(x, y) = (x, \lambda^2 y)$, then $f(\phi(x, y)) \neq \lambda^3 f(\phi'(x, y))$ because f is not homogeneous, so there is not redundant λ in ϕ. Moreover we have

$$f(\phi(x, y)) = \lambda^3(f(\phi'(x, y)) + (1 + \lambda^2)y)$$

6.1 Maps between Odd Cubics and curves in Weierstrass form

Now we map odd cubics into curves in Weierstrass form and vice versa, i.e.

$$x^3 + ax^2y + bxy^2 + cy^3 + dx + ey = 0 \quad \longleftrightarrow \quad y^2 = x^3 + \alpha x^2 + \beta x + \gamma \tag{6.4}$$

Without lost of generality we consider odd cubics in first form. From right to left first, what we do is a simple change of perspective:

1: Making $t = x/y$ and $s = 1/y$ we obtain

$$t^3 + \alpha t^2 s + \beta t s^2 + \gamma s^3 - s = 0$$

this way we map the neutral element $\mathcal{O}$ in the (x, y)-coordinates to the origin and send straight lines to straight lines, explicitly $y = \lambda x + \mu \longleftrightarrow 1 = \lambda t + \mu s$, which means this map is actually an isomorphism. We shall refer to this map as φ_c.

6.1.1 Nagell's Algorithm

In this part we collect ideas from [17] and [15] in order to birationally map odd cubics to curves in Weierstrass form. We briefly describe the general method:

1. Given a non-singular cubic E over a field of characteristic different than 2. Take a point $\mathcal{O}$ that is not an inflection point. The tangent line at $\mathcal{O}$ intersects E again at a different point P.
2. Change the coordinate system so P is at the origin and $\mathcal{O}$ lies on the y-axis, and let $F(x, y) = 0$ be the resulting form of E.
3. Since E has degree 3 and $F(P) = 0$, write F as

   $$F = F_1 + F_2 + F_3$$

   where the F_d are homogeneous polynomials of degree d.
4. Let t be a parameter such that $y = tx$, then we have

   $$F(x, y) = xF_1(1, t) + x^2 F_2(1, t) + x^3 F_3(1, t) = 0 \tag{6.5}$$

5. Discard one x and complete the square to obtain

   $$(2F_3(1, t)x + F_2(1, t))^2 \;=\; F_2(1, t)^2 - 4F_3(1, t)F_1(1, t)$$

   and make $s = 2F_3(1, t)x + F_2(1, t)$ and $G(t) = F_2(1, t)^2 - 4F_3(1, t)F_1(1, t)$.
6. Since $s^2 = G(t)$, the transformation $(x, y) \longmapsto (t, s)$ maps E to a curve in Weierstrass form birationally. Explicitly the maps are

   $$(x, y) \longmapsto (t, s) = \left(\frac{y}{x}, 2F_3\left(1, \frac{y}{x}\right)x + F_2\left(1, \frac{y}{x}\right)\right),\ (t, s) \longmapsto (x, y) = \left(\frac{s - F_2(1, t)}{2F_3(1, t)}, \frac{ts - tF_2(1, t)}{2F_3(1, t)}\right)$$

   we shall refer to this map as φ_n.

The previous algorithm was improved by Tibouchi in [17] for any characteristic as follows:

1. As in part 4 of the preceding algorithm, multiply (6.5) by $F_3(1,t)/x$ to obtain
$$x^2F_3(1,t)^2 + F_3(1,t)F_2(1,t)x = -F_3(1,t)F_1(1,t)$$
2. Making $u = F_3(1,t)x$ yields
$$u^2 + G_1(t)u = G_3(t)$$
where $G_1 = F_2$ and $G_3 = -F_1F_3$.
3. Finally the maps are expressed as follows
$$(x,y) \longmapsto (t,u) = \left(\frac{y}{x}, \frac{F_3(x,y)}{x^2}\right), \quad (t,u) \longmapsto (x,y) = \left(\frac{u}{F_3(1,t)}, \frac{tu}{F_3(1,t)}\right)$$

Example 3 *Consider the cubic $E : f(x,y) = x^3 + xy^2 - y^3 - x + y = 0$ over $\mathbb{F}_{2011}$, the first algorithm maps E to*
$$C : s^2 = 1300t^3 + 711t^2 + 294t + 1789$$
which can be rescaled down to
$$C : s^2 = t^3 + 1998t^2 + 2009t + 389$$

Explicitly, we consider the point $\mathcal{O} = (-1,0) = (2010,0)$ and $P = (773,463)$. We first apply the change
$$(x,y) \longmapsto (x - 773, y - 463)$$
taking P into the origin. Now, as seen in § 2.6, we consider the rotation (in the new coordinates system)
$$(x,y) \longmapsto (108(2x - y), 108(x + 2y))$$
taking $\mathcal{O}$ into the y-axis, and after developing and cleaning constants
$$F(x,y) = 9x^3 + 2000x^2y + 2009xy^2 + 1998y^3 + 1438x^2 + 997xy + 1527y^2 + 1250x + 1064y$$
now for each homogeneous part
$$\begin{aligned} F_1 &= 1250x + 1064y \\ F_2 &= 1438x^2 + 997xy + 1527y^2 \\ F_3 &= 9x^3 + 2000x^2y + 2009xy^2 + 1998y^3 \end{aligned}$$
using the parameter t such that $y = tx$ we obtain
$$\begin{aligned} F(x,y) &= xF_1(1,t) + x^2F_2(1,t) + x^3F_3(1,t) \\ &= x\,(1250 + 1064t) + x^2\left(1438 + 997t + 1527t^2\right) + x^3\left(9 + 2000t + 2009t^2 + 1998t^3\right) \end{aligned}$$

We make $s = 2F_3(1,t)x + F_2(1,t)$ and
$$\begin{aligned} G(t) &= F_2(1,t)^2 - 4F_3(1,t)F_1(1,t) \\ &= 1300t^3 + 711t^2 + 294t + 1789 \\ \Longrightarrow \quad s^2 &= 1300t^3 + 711t^2 + 294t + 1789 \end{aligned}$$

now, since $711 = -1300 \pmod{2011}$

$$\begin{aligned} s^2 &= 1300t^3 - 1300t^2 + 294t + 1789 \\ (13s)^2 &= 100(13t)^3 - 1300(13t)^2 + 1422t + 691 \\ (13s)^2 &= 100(13t)^3 - 1300(13t)^2 + 1422 \times 13^{-1}(13t) + 691 \end{aligned}$$

using that $100^{-1} = 181 \pmod{2011}$ and $13^{-1} = 1547 \pmod{2011}$

$$(602s)^2 \;=\; (13t)^3 - 13(13t)^2 + 2009(13t) + 389$$

and this is how we can rescale to

$$s^2 = t^3 - 13t^2 + 2009t + 389 = t^3 + 1998t^2 + 2009t + 389.$$

At this point it is worth asking ourselves if we really need more than one map to pass from curves in Weierstrass equation to odd cubics back and forth, and we probably don't since φ_c is much easier to compute than φ_n. Nevertheless Nagell's algorithm is more general since it does not require a cubic in any specific form.

7 Final words

About the model we have introduced, I tested the computations with small examples using `RStudio` and I wish I had the opportunity to have them tested with really large numbers, i.e. considerably bigger than a regular computer is able to handle. Other than that I consider that this new approach has its advantages in some cases with a wide path to keep going on the investigation.

From the Simple Model we have explored, with a subtle change in the perspective we see that the relation $R(x, y) = t(x + y)/(t - xy)$ satisfies

$$R(R(x, y), z) = R(x, R(y, z))$$

whenever each valuation is properly defined, so characterising functions with this property may lead to different ways to encode elements with a group law, not necessarily embedded in an elliptic curve (or at least not at first glance), therefore it could be of interest to explore this kind of associativity in functional equations. A first insight into this topic can be found in the works of K. Domnáska ([4]) and J. Brawly, S. Gao and D. Mills ([1])

Finally, there was plenty of reading that didn't make it into this work, such as the study of isogenies and different ways of producing a groups with different composition laws and curves of different degrees, which together with testing computations with large numbers, are at the top of the list of subjects to keep working on in the near future.

8 References

[1] J. V. Brawley, S. Gao, and D. Mills. Associative rational functions in two variables. In *Finite fields and applications (Augsburg, 1999)*, pages 43–56. Springer, Berlin, 2001.

[2] L. De Feo. Mathematics of isogeny based cryptography. *CoRR*, abs/1711.04062, 2017.

[3] L. E. Dickson. Criteria for the irreducibility of functions in a finite field. *Bull. Amer. Math. Soc.*, 13(1):1–8, 1906.

[4] K. Domańska. An analytic description of the class of rational associative functions. *Ann. Univ. Paedagog. Crac. Stud. Math.*, 11:111–122, 2012.

[5] D. S. Dummit and R. M. Foote. *Abstract algebra.* John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[6] W. Fulton. *Algebraic curves.* Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[7] R. Hartshorne. *Algebraic geometry.* Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[8] J. Hoffstein, J. Pipher, and J. H. Silverman. *An introduction to mathematical cryptography.* Undergraduate Texts in Mathematics. Springer, New York, 2008.

[9] M. Joye, M. Tibouchi, and D. Vergnaud. Huff's model for elliptic curves. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 234–250. Springer, Berlin, 2010.

[10] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes.* Princeton University Press, Princeton, NJ, 1992.

[11] D. Menon. Bezout's theorem for curves. *Semantic Scholar, Corpus ID: 50023091*, 2011.

[12] J. Rotman. *Galois theory.* Universitext. Springer-Verlag, New York, second edition, 1998.

[13] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[14] J. H. Silverman and J. Tate. *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[15] R. J. Stroeker and B. M. M. de Weger. Solving elliptic Diophantine equations: the general cubic case. *Acta Arith.*, 87(4):339–365, 1999.

[16] A. V. Sutherland. Isogeny volcanoes. *arXiv e-prints*, page arXiv:1208.5370, Aug. 2012.

[17] M. Tibouchi. A nagell algorithm in any characteristic. In *Cryptography and Security: From Theory to Applications*, pages 474–479. Springer, 2012.

[18] H. Wu and R. Feng. Elliptic curves in Huff's model. *Wuhan Univ. J. Nat. Sci.*, 17(6):473–480, 2012.