MULTIPLES OF POINTS ON PICARD CURVES

RAHUL RAM (ADVISED BY PROF. PINEIRO BARCELO)

ABSTRACT. Inspired by the formulas on Elliptic curves, we use coordinates defined by Mumford to be able to work on some family of genus three curves.

1. Elliptic curves

An Elliptic Curve is a curve given by an equation of the form

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

where $\Delta = 4A^3 + 27B^2 \neq 0$ and the coefficients A, B are in some field K. Equivalently, the polynomial $P(x) = x^3 + Ax + B$ has three distinct roots in K. This ensures that the curve is nonsingular. To work with a "compact" space, we add a point "at infinity" denoted by: $\mathcal{O} = (0, 1, 0)$. In total

$$E = \{(x, y) \in K^2 \,|\, y^2 = x^3 + Ax + B\} \cup \mathcal{O}.$$

1.1. **Addition of points.** It turns out that we have a way to add two points P, Q on E following the steps:

(1) Join the points P and Q with a secant line L.
(2) Find the third point R where L meet the elliptic curve E.
(2) Draw the vertical line through R. This line intersects E on another point defined as $P + Q$.

We can see an example on $y^2 = x^3 + 7$ in figure 1. For $P = Q$ we will be in the particular case of doubling a point. In the first step in our formula for addition, we take the **tangent line** at the point P intersecting E at only one extra point R and again proceed to draw the vertical line though R (figure 2).

Remark 1.1. *It is worth noticing that any vertical line touches the graph at exactly two points: if one of them is P, the other one will be denoted by $-P$. (figure 3)*

The addition law has the following properties:

(a) $P + \mathcal{O} = P = \mathcal{O} + P$.
(b) $P + (-P) = \mathcal{O}$.
(c) $P + (Q + R) = (P + Q) + R$.
(d) $P + Q = Q + P$

Exercise 1.2. *Find an explicit formula for the duplication of a point on the elliptic curve*

$$E : y^2 = x^3 + Ax + B.$$

Solution. Given a point $P = (x_P, y_P)$, we aim to double it by finding the inverse of the other point at which the line tangent to E at P hits E, denoted by the equation $y = mx + b$ with slope m and y-intercept b. We know the slope of the tangent line $m = \frac{dy}{dx}$, and using implicit differentiation of the equation of E with respect to x, we get that $2y\frac{dy}{dx} = 3x^2 + A$, so $\frac{dy}{dx}|_{x=x_P} = m = \frac{3x_P^2+A}{2y_P}$.

To solve for the line's y-intercept, we take note that $y = mx + b$ means $b = y_P - mx_P$ as we have it at the point P, i.e. $b = y_P - \frac{3x_P^3+Ax_P}{2y_P}$, making the tangent line equation

$$y = \frac{3x_P^2 + A}{2y_P}x + y_P - \frac{3x_P^3 + Ax_P}{2y_P} = m(x - x_P) + y_P.$$

If $y_P \geq 0$, then we consider the non-negative

$$y = \sqrt{x^3 + Ax + B} = m(x - x_P) + y_P = \frac{3x_P^2 + A}{2\sqrt{x_P^3 + Ax_P + B}}(x - x_P) + \sqrt{x_P^3 + Ax_P + B}$$

and similarly for $y_P < 0$, then we consider the negative

$$y = -\sqrt{x^3 + Ax + B} = m(x - x_P) + y_P = \frac{3x_P^2 + A}{2\sqrt{x_P^3 + Ax_P + B}}(x - x_P) + \sqrt{x_P^3 + Ax_P + B}.$$

Therefore, using the cubic formula, $x_{2P} = \frac{x_P^4 - 2Ax_P^2 - 8Bx_P + A^2}{4(x_P^3 + Ax_P + B)}$ and assuming $y_P \neq 0$, we get

$$y_{2P} = -\lambda^3 + \lambda(2x_P) - \nu$$

with $\lambda = \frac{3x_P^2 + A}{2y_P}$ and $\nu = \frac{-x_P^3 + Ax_P + 2B}{2y_P}$. Therefore, for $P = (x, y)$, its double is

$$2P = (x_{2P}, y_{2P}) = (\lambda^2 - 2x_P, -\lambda^3 + 2x_P\lambda - \nu).$$

Exercise 1.3. *Use your formula to determine $2P$ for $P = (1, 2)$ on $E : y^2 = x^3 - 5x + 8$.*

Solution. For the elliptic curves $E : y^2 = x^3 - 5x + 8$, the values of A and B are $A = -5$ and $B = 8$. If we take the point $P = (x_P, y_P) = (1, 2)$, the double point will be

$$2P = (x_{2P}, y_{2P}) = (\lambda^2 - 2x_P, -\lambda^3 + 2x_P\lambda - \nu),$$

for values of

$$\lambda = \frac{3x_P^2 + A}{2y_P} = \frac{3(1)^2 - 5}{2(2)} = -\frac{1}{2} \quad \text{and} \quad \nu = \frac{-x_P^3 + Ax_P + 2B}{2y_P} = \frac{1^3 - 5(1) + 2(8)}{2(2)} = 3.$$

With this results in mind we get

$$2P = (x_{2P}, y_{2P}) = (\lambda^2 - 2x_P, -\lambda^3 + 2x_P\lambda - \nu) = ((-\frac{1}{2})^2 - 2(1), -(-\frac{1}{2})^2 + 2(1)(-\frac{1}{2}) - 3) = (-\frac{7}{4}, -\frac{17}{4}),$$

and

$$2P = (x_{2P}, y_{2P}) = (-\frac{7}{4}, -\frac{27}{8}).$$

Figure 1. Addition of two points on the curve $y^2 = x^3 + 7$

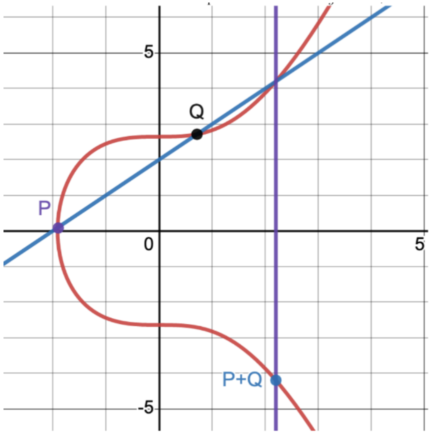


FIGURE 2. Doubling a point P on the curve $y^2 = x^3 + 7$

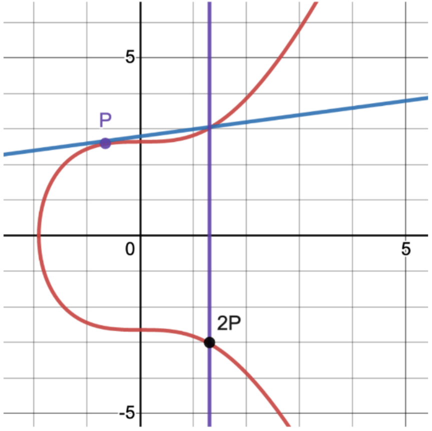
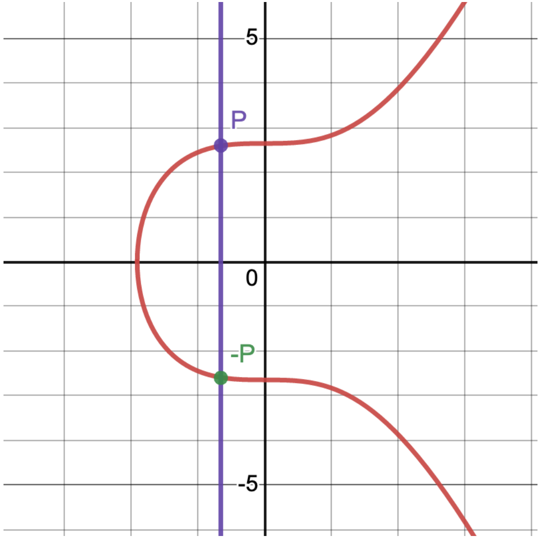


FIGURE 3. Inverse of a point P on $y^2 = x^3 + 7$



2. ALGEBRAIC CURVES OF HIGHER GENUS

The fact that we were able to add points on an elliptic curve E is a consequence of a more general result on curves. For a projective curve C of genus g, we can construct a projective algebraic variety $\mathrm{J}(C)$, called the Jacobian variety of C, which is a complete algebraic algebraic variety as well as an algebraic group. The dimension of $J(C)$ is g and for elliptic curves over algebraically closed fields, $\mathrm{J}(C) \cong C$. The addition of points on E is just a reflection of the group structure on the Abelian variety $\mathrm{J}(C)$. Now, in general, Jacobian variety of a curve C can be described as the quotient of the group of divisors of degree zero by the subgroup of principal divisors:

$$\mathrm{J}(C) = \mathrm{Div}^0(C)/\mathrm{P}(C).$$

Any divisor of degee zero D can then be reduced, using linear equivalence, to a divisor of the sort

$$D_f = P_1 + P_2 + \cdots + P_g - g\infty,$$

where $P_1, P_2, \ldots, P_g$ are points on the curve and ∞ is a fixed point on C.
For curves C of genus $g > 1$, the role of points is played now by divisors of degree zero of the form D_f above. Somehow when we add two elements

$$D_f = P_1 + P_2 + \cdots + P_g - g\infty \quad \text{and} \quad D'_f = P'_1 + P'_2 + \cdots + P'_g - g\infty$$

we should define a procedure that computes the points $Q_1, Q_2, \ldots, Q_g$ on C such that

$$D_f + D'_f = Q_1 + Q_2 + \cdots + Q_g - g\infty,$$

up to linear equivalences.

3. Picard curves

Elliptic curves are curves of genus 1. To work with curves of higher genus we move to Picard curves having genus $g = 3$. A Picard curve admits an affine equation of the form:

$$C\colon y^3 = p_4(x),$$

where p_4 is a polynomial with distinct roots and coefficients on a field K. The point at infinity, ∞, will be the extra point with projective coordinates $(0 : 1 : 0)$. In general points $R_{x_i} = (x_i, 0)$ obtained with the zeroes of the polynomial p_4 will be called ramification points. The curve admit involutions $\sigma, \sigma^2\colon C \to C$, given by keeping x fixed and multiplying the y by the different third roots of unity in $\bar{K}$. Some identities of divisors on C are:

$$(x - a) = P_a + \sigma P_a + \sigma^2 P_a - 3\infty \qquad (y) = R_{x_1} + R_{x_2} + R_{x_3} + R_{x_4} - 4\infty.$$

We want to implement the algorithm 3.9 in [1] to compute the multiples of a divisor D in the Jacobian variety $\mathrm{J}(C)$ of C. For example suppose that we are working with

$$C_1\colon y^3 = x(x-1)(x-2)(x-3)$$

and we are working over $K = \mathbb{F}_p$ for a prime $p = 5$. We have the point $P = (-3, 0) \in C$. We want to use the coordinates $(u(x), v(x))$ (and even $w(x)$) to implement the algorithm and compute mP in the Jacobian $J(C)$
What does this means? We can build the list of multiples:

$$P,\ 2P,\ 3P,\ 4P, \ldots,$$

where already $4P = Q_1 + Q_2 + Q_3$ and the $Q_1, Q_2, Q_3 \in C$ are to be found from the points on the curve, namely among

$$P,\ R_0 = (0,0),\ R_1 = (1,0),\ R_2 = (2,0),\ R_3 = (3,0) \text{ and } R_\infty = \infty.$$

We can also use the curve:

$$C_2\colon y^3 = x(x-1)(x-2)(x+4).$$

Here you have a few points by just looking: $R_0 = (0,0)$, $R_1 = (1,0)$, $R_2 = (2,0)$ and $R_{-4} = (-4,0)$. Those points with y-coordinate zero are called ramification points. The extra point at infinity ∞ is also there. Also, the point $P = (4,4)$. If you want to work it on the homogeneous equation it will be:

$$y^3 z = z^4 p_4(x/z).$$

In here, $P_0 = (0 : 0 : 1)$, etc.
Another Picard curve to use as testing grounds could be the curve on the examples 3.10 and 3.11 of [1]:

$$C_3\colon y^3 = x^4 - 1$$

over the fields F_{13} and F_{23}. Our tasks for now:

(1) Estimate the order of $\mathrm{J}(C)$ for C_1, C_2 and C_3 over small fields F_p.
(2) Determine the reduction $4P = Q_1 + Q_2 + Q_3$ for $P = (-3, 0)$ in C_1.
(3) Determine the reduction $4P = Q_1 + Q_2 + Q_3$ for $P = (4, 4)$ in C_2.
(4) Understand the examples 3.10 and 3.11 to see how coordinates (u, v) are obtained.

We describe C_1 as $y^3 = x(x-1)(x-2)(x-3)$, $C_2 = x(x-1)(x-2)(x+4)$, and C_3 as $y^3 = x^4 - 1 = (x-1)(x+1)(x+i)(x-i)$, minimally factorizable over $\mathbb{F}_7(i)$.

3.1. **Interpolatinon of points on C.** Let $P_1, \dots, P_5$ be points on $C : y^3 = p_4(x) \cup \infty$. To find a quadric

$$q(x,y) = a_{20}x^2 + a_{11}xy + a_{0,2}y^2 + a_{01}y + a_{101}x + a_{00}$$

that passes though the points $P_1, P_2, \dots, P_5$ is equivalent to solve a linear system of equations. If all points P_i are affine and $P_i \neq P_j$ for $i \neq j$, we get:

$$\begin{cases} a_{20}x_1^2 + a_{11}x_1y_1 + a_{02}y_1^2 + a_{01}y_1 + a_{10}x_1 + a_{00} = 0 \\ a_{20}x_2^2 + a_{11}x_2y_2 + a_{02}y_2^2 + a_{01}y_2 + a_{10}x_2 + a_{00} = 0 \\ a_{20}x_3^2 + a_{11}x_3y_3 + a_{02}y_3^2 + a_{01}y_3 + a_{10}x_3 + a_{00} = 0 \\ a_{20}x_4^2 + a_{11}x_4y_4 + a_{02}y_4^2 + a_{01}y_4 + a_{10}x_4 + a_{00} = 0 \\ a_{20}x_5^2 + a_{11}x_5y_5 + a_{02}y_5^2 + a_{01}y_5 + a_{10}x_5 + a_{00} = 0 \end{cases}$$

When some points are repeated, we need to change equations to reflect a contact of higher order at that point, for example, for $P_1 = P_2 \neq R_i, P_3, P_4, P_5$ and $(q) \geq D = 2P_1 + P_3 + P_4 + P_5$ (and no other repeated points among P_i), we get:

$$\begin{cases} a_{20}x_1^2 + a_{11}x_1y_1 + a_{0,2}y_1^2 + a_{01}y_1 + a_{10}x_1 + a_{00} = 0 \\ 2x_1a_{20} + a_{11}(c_1x_1 + y_1) + a_{01}c_1 + 2a_{02}c_1y_1 + a_{10} = 0 \\ a_{20}x_3^2 + a_{11}x_3y_3 + a_{02}y_3^2 + a_{01}y_3 + a_{10}x_3 + a_{00} = 0 \\ a_{20}x_4^2 + a_{11}x_4y_4 + a_{02}y_4^2 + a_{01}y_4 + a_{10}x_4 + a_{00} = 0 \\ a_{20}x_5^2 + a_{11}x_5y_5 + a_{02}y_5^2 + a_{01}y_5 + a_{10}x_5 + a_{00} = 0 \end{cases}$$

The number c_1 is denoting the rate of change at P_1:

$$c_1 = \partial y / \partial x|_{x=x_1}$$

In a similar way, using

$$c_2 = \partial^2 y / \partial x^2|_{x=x_1} \quad c_3 = \partial^3 y / \partial x^3|_{x=x_1}$$

we obtain $(q) \geq 3P_1 + P4 + P_5$ by solving the system:

$$\begin{cases} a_{20}x_1^2 + a_{11}x_1y_1 + a_{0,2}y_1^2 + a_{01}y_1 + a_{10}x_1 + a_{00} = 0 \\ 2x_1a_{20} + a_{11}(c_1x_1 + y_1) + a_{01}c_1 + 2a_{02}c_1y_1 + a_{10} = 0 \\ 2a_{20} + (c_2x_1 + 2c_1)a_{11} + c_2a_{01} + 2(c_2y_1 + c_1^2)a_{02} = 0 \\ a_{20}x_4^2 + a_{11}x_4y_4 + a_{02}y_4^2 + a_{01}y_4 + a_{01}x_4 + a_{00} = 0 \\ a_{20}x_5^2 + a_{11}x_5y_5 + a_{02}y_5^2 + a_{01}y_5 + a_{10}x_5 + a_{00} = 0 \end{cases}$$

and $(q) \geq 4P_1 + P_5$ with the linear system:

$$\begin{cases} a_{20}x_1^2 + a_{11}x_1y_1 + a_{0,2}y_1^2 + a_{01}y_1 + a_{10}x_1 + a_{00} = 0 \\ 2x_1a_{20} + a_{11}(c_1x_1 + y_1) + a_{01}c_1 + 2a_{02}c_1y_1 + a_{10} = 0 \\ 2a_{20} + (c_2x_1 + 2c_1)a_{11} + c_2a_{01} + 2(c_2y_1 + c_1^2)a_{02} = 0 \\ \qquad\quad (c_3x_1 + 3c_2)a_{11} + c_3a_{01} + 2(c_3y_1 + 3c_1c_2)a_{02} = 0 \\ a_{20}x_5^2 + a_{11}x_5y_5 + a_{0,2}y_5^2 + a_{01}y_5 + a_{10}x_5 + a_{00} = 0. \end{cases}$$

For the quadric $q(x,y) = a_{20}x^2 + a_{11}xy + a_{0,2}y^2 + a_{01}y + a_{10}x + a_{00}$ to contain the point ∞ is equivalent to consider some coefficients of higher degree zero, for example

$$(q) \geq \infty \qquad \iff \qquad a_{02} = 0.$$

$$(q) \geq 2\infty \qquad \iff \qquad a_{02} = a_{11} = 0.$$

For example, for $P \neq \infty$ and $P = (x_1, y_1)$ with $y_1 \neq 0$, $q(x,y) \geq 4P + \infty$ is equivalent to find solutions for the system of equations

$$\begin{cases} a_{20}x_1^2 + a_{11}x_1y_1 + y_1a_{01} + x_1a_{10} + a_{00} = 0 \\ 2x_1a_{20} + (c_1x_1 + y_1)a_{11} + c_1a_{01} + a_{10} = 0 \\ 2a_{20} + (c_2x_1 + 2c_1)a_{11} + c_2a_{01} \qquad = 0 \\ \qquad (c_3x_1 + 3c_2)a_{11} + c_3a_{01} \qquad = 0 \end{cases}$$

3.2. **The generic case.** Let $D_0 = D = P_1 + P_2 + P_3 + P_4$, without pairs of conjugates or collinear points. Let us assume that the coordinates $(D) = (u, v, w)$ are given by

$$u = \prod_i (x - x_i) = \sum_l (-1)^l s_l x^l, \quad (v) \geq D \quad \text{and} \quad w = R_y(C, v)/u,$$

where $v = v(x,y) = a_{20}x^2 + a_{11}xy + a_{01}y + a_{10}x + a_{00}$ is a quadric with degree 2 and determinant

$$\Delta = -a_{00}a_{11}^2 + a_{10}a_{01}a_{11} - a_{20}a_{10}^2 \neq 0$$

and $R_y(C, v)$ denotes the resultant of the curve $C : y^3 - p_4(x)$ and $v(x,y)$.
We want to find the coordinate vector of polynomials $(D_1) = (u_1, v_1, w_1)$ from the $(D_0) = (u, v, w)$. The first polynomial is just

$$u_1 = w/\text{leading coeff of } w.$$

For the $v_1(x,y) = b_{20}x^2 + b_{01}y + b_{10}x + b_{00}$ there are two possibilities:
If $a_{11} = 0$ we get

$$\begin{aligned} b_{01} &= \lambda s_2/a_{20} \\ b_{10} &= \lambda(s_1/a_{01} + a_{10}s_2/(a_{20}a_{01})) \\ b_{00} &= \lambda(-s_0/a_{01} + a_{00}s_2/(a_{20}a_{01})) \\ b_{11} &= 0. \end{aligned}$$

For $a_{11} \neq 0$ we get

$$\begin{aligned} b_{20} &= -\lambda/a_{11} \\ b_{10} &= \lambda(-s_1a_{20}a_{01} - a_{20}a_{11}s_0 - a_{11}a_{00}(-s_2 + a_{01}/a_{11}) + a_{01}a_{10}(-s_2 + a_{01}/a_{11}))/\Delta \\ b_{00} &= \lambda(-s_1a_{11}a_{00} + a_{20}a_{01}s_0 - a_{10}a_{11}s_0 + a_{01}a_{00}(-s_2 + a_{01}/a_{11}))/\Delta \\ b_{01} &= \lambda(-s_1a_{11}a_{01} - a_{11}^2s_0 + a_{01}^2(-s_2 + a_{01}/a_{11}))/\Delta. \end{aligned}$$

As always, the w_1 can be obtain from u_1 and v_1 using the result of the curve $C : y^3 = p_4(x)$ and the quartic $v_1(x,y)$:

$$w_1 = R_y(C, v_1)/u_1.$$

The idea is to repeat the process

$$(D_0) \rightarrow (D_1) \rightarrow (D_2).$$

If we started with four generic points, the D_2 should be reduced already, that is $D_2 = Q_1 + Q_2 + Q_3$. If our initial divisor is D of degree > 4, we would need more steps. In general a sequence of coordinate divisors

$$(D_0) \rightarrow (D_1) \rightarrow (D_2) \rightarrow (D_3) \rightarrow \ldots (D_{3n+1}) \rightarrow (D_{3n+2}),$$

where $D_{3n+2} = Q_1 + Q_2 + Q_3$ is a reduced and linearly equivalent to $D = D_0$.

The step from $(D_2) = (P_1 + P_2 + P_3)$ to $(D_3) = (D_3 + E_3)$: Suppose that $(D_2) = (u_2, v_2, w_2)$ and $u_2(x)$ has no repeated roots. In this case $u_2 = \prod_{i=1}^3 (x - x_i)$ for $D_2 = P_1 + P_2 + P_3$ and $P_i = (x_i, y_i)$ and $E_3 = P_4$.

If $v_2(x_4, y_4) = 0$ and $u_2(x_4) \neq 0$, then $(D_3) = (u_3 = u_2(x - x_4), v_3 = v_2, w_3 = R_y(v_3, C)/u_3)$
Else compute:

$$\begin{aligned} a'_{20} &= (a'_{11}(b_{10} + s'_2 b_{20}) + b_{20} a'_{01})/b_{01} \\ a'_{10} &= (a'_{11}(b_{00} - s'_1 b_{20}) + b_{10} a'_{01})/b_{01} \\ a'_{00} &= (a'_{11} s'_0 b_{20} + b_{00} a'_{01})/b_{01}, \end{aligned}$$

where $v_3 = a'_{20}x^2 + a'_{11}xy + a'_{01}y + a'_{1,0}x + a'_{00}$ and we obtain the coefficients $a'_{11} \neq 0$ and a'_{01} from the above formulas and the equation

$$v_3(x_4, y_4) = a'_{20}x_4^2 + a'_{11}x_4y_4 + a'_{01}y_4 + a'_{1,0}x_4 + a'_{00} = 0.$$

The step from $(D_2) = (P_1 + P_2)$ to $(D_3) = (D_3 + E_3)$: Suppose that $(D_2) = (u_2, v_2, w_2)$ and $u_2(x)$ has no repeated roots. In this case $u_2 = \prod_{i=1}^{2}(x - x_i)$ for $D_2 = P_1 + P_2$ and $P_i = (x_i, y_i)$ and $E_3 = P_3 + P_4$. Also assume that P_3 and P_4 are not conjugate.
The coordinates $(D_3) = (D_2 + E_3) = (u_3 = u_2(x - x_3)(x - x_4), v_3, w_3)$, where $v_3(x, y) = a'_{20}x^2 + a'_{11}xy + a'_{01}y + a'_{1,0}x + a'_{00}$ and we can use that

$$R_y(v_2, v_3) = \lambda u_2(x)$$

to obtain:

$$\begin{aligned} a'_{20} &= (b_{10}a'_{11} + \lambda s'_2)/b_{01} \\ a'_{10} &= (b_{10}a'_{01} + a'_{11}b_{00} - \lambda s'_1)/b_{01} \\ a'_{00} &= (b_{00}a'_{01} + \lambda s'_0)/b_{01} \end{aligned}$$

To obtain a'_{11} and a'_{01}, we use the above formulas in the system of equations:

$$\begin{aligned} v_3(x_3, y_3) &= a'_{20}x_3^2 + a'_{11}x_3y_3 + a'_{01}y_3 + a'_{1,0}x_3 + a'_{00} = 0 \\ v_3(x_4, y_4) &= a'_{20}x_4^2 + a'_{11}x_4y_4 + a'_{01}y_4 + a'_{1,0}x_4 + a'_{00} = 0. \end{aligned}$$

References

[1] J. Estrada, E. Reynaldo, J. Pineiro, *On the Jacobian Varieties of Picard Curves: Explicit Addition Law and Algebraic Structure*. Math. Nach. Vol 208, 1999, pp 149-166.

[2] D. Mumford, *Tata Lectures on Theta II*. Jacobian theta functions and differential equations. Progress in Math. 42. Birkhauser Verlag, 1984

[3] G. Filippone, *On the discrete logarithm problem for elliptic curves over local fields.* https://arxiv.org/abs/2304.14150v1, 2023

[4] J. Silverman, *Introduction to Diophantine Geometry*. Springer-Verlag, New York, (2000).

[5] J. Silverman, *The arithmetic of elliptic curve*. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.