Isogenies between elliptic curves*†

Jacques Vélu

26 July 1971

Given the equation of an elliptic curve E over a field k and the coordinates of the points of a finite subgroup F of E, we give the equations of the isogenous curve E/F and of the isogeny $f\colon E \to E/F$.

1 Background

Let E be an elliptic curve over an algebraically closed field k. To each point P of E we associate a valuation ν_P on the field $k(E)$ of functions defined over k, and for each function $t \in k(E)$ we write $t(P)$ for the value of t at the point P. If $\mathcal{O}$ is a point of E, there exist x and y in $k(E)$ satisfying the conditions

$$\begin{aligned} &\nu_{\mathcal{O}}(x) = -2; \qquad \nu_{\mathcal{O}}(y) = -3; \qquad \frac{y^2}{x^3}(\mathcal{O}) = 1; \\ &\nu_P(x) \geq 0 \qquad \text{and} \qquad \nu_P(y) \geq 0 \text{ for } P \neq \mathcal{O}. \end{aligned} \tag{1}$$

These conditions imply that $k(E) = k(x, y)$ and that x and y are related by a nonsingular cubic equation that we can establish in the following manner: let $z = -x/y$ so that $\nu_{\mathcal{O}}(z) = 1$; write x and y as

$$\begin{aligned} x &= z^{-2} - \alpha_1 z^{-1} - \alpha_2 - \alpha_3 z - \alpha_4 z^2 - \alpha_5 z^3 - \alpha_6 z^4 - \dots, \\ y &= -\frac{x}{z} = -z^{-3} + \alpha_1 z^{-2} + \alpha_2 z^{-1} + \alpha_3 + \alpha_4 z + \alpha_5 z^2 + \alpha_6 z^3 + \dots; \end{aligned} \tag{2}$$

then x and y satisfy

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \tag{3}$$

where

$$\begin{aligned} \alpha_1 &= a_1, & \alpha_4 &= a_1 a_3 + a_4, \\ \alpha_2 &= a_2, & \alpha_5 &= a_2 a_3 + a_1^2 a_3 + a_1 a_4, \\ \alpha_3 &= a_3, & \alpha_6 &= a_1^2 a_4 + a_1^3 a_3 + a_2 a_4 + 2a_1 a_2 a_3 + a_3^2 + a_6. \end{aligned} \tag{4}$$

*This note appeared in the *Comptes rendus de l'Académie des Sciences de Paris, Série A, t. 273.*
†Translated from the original French by Alexandru Ghitza <aghitza@alum.mit.edu>.

It is customary to set

$$
\begin{aligned}
&b_2 = a_1^2 + 4a_2, \qquad b_4 = a_1a_3 + 2a_4, \qquad b_6 = a_3^2 + 4a_6,\\
&b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \qquad \text{whence} \quad 4b_8 = b_2b_6 - b_4^2,\\
&\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.
\end{aligned} \tag{5}
$$

The nonsingularity of equation (3) amounts to $\Delta \neq 0$. Conversely, given five elements $a_1, a_2, a_3, a_4, a_6 \in k$ with $\Delta \neq 0$, equation (3) (once homogenized) defines an elliptic curve in $\mathbb{P}^2$, and, if we let $\mathcal{O}$ be the point at infinity, the functions x and y satisfy conditions (1).

Let G be the polynomial

$$G(\xi, \eta) = \xi^3 + a_2\xi^2 + a_4\xi + a_6 - \eta^2 - a_1\xi\eta - a_3\eta;$$

then the differential of the first kind

$$\omega(x,y) = \frac{dx}{2y + a_1x + a_3} = \frac{dx}{\frac{\partial G}{\partial \xi}(x,y)} = \frac{-dy}{\frac{\partial G}{\partial \eta}(x,y)} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},$$

can be written as

$$
\begin{aligned}
\omega(x,y) = dz\,[1 + a_1z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1a_2 + a_3)z^3&\\
+ (a_1^4 + 3a_1^2a_2 + 6a_1a_3 + a_2^2 + 2a_4)z^4 + \ldots].&
\end{aligned} \tag{6}
$$

2 Isogenies

Let F be a finite subgroup of E and let f be the isogeny with kernel F from E to the elliptic curve $E' = E/F$. For any point P of E we set $P' = f(P)$. The function field $k(E')$ is identified with a subfield of $k(E)$. Consider the functions X and Y defined by

$$
\begin{aligned}
X(P) &= x(P) + \sum_{Q \in F - \{\mathcal{O}\}} (x(P+Q) - x(Q));\\
Y(P) &= y(P) + \sum_{Q \in F - \{\mathcal{O}\}} (y(P+Q) - y(Q));
\end{aligned} \tag{7}
$$

It is clear that $X, Y \in k(E')$ and satisfy $\nu_{\mathcal{O}'}(X) = -2$; $\nu_{\mathcal{O}'}(Y) = -3$; $Y^2/X^3(\mathcal{O}') = 1$; $\nu_{P'}(X) \geq 0$ and $\nu_{P'}(Y) \geq 0$ for all $P' \neq \mathcal{O}'$. Hence $k(E')$ is isomorphic to $k(X,Y)$ and the isogeny f is identified with the map $(x,y) \mapsto (X,Y)$. We can write X and Y as rational functions of x and y; these will be the “equations” of the isogeny f, and the relation between X and Y will be the equation of E'.

3 Results

Let F_2 be the subset of points of order 2 of $F-\{\mathcal{O}\}$ and let R be a subset of $F-\{\mathcal{O}\}-F_2$ such that

$$F-\{\mathcal{O}\}-F_2 = R\cup(-R) \quad \text{and} \quad R\cap(-R)=\emptyset;$$

let $S=F_2\cup R$. The isogeny f has equations

$$\begin{aligned} X &= x+\sum_{Q\in S}\left(\frac{t_Q}{x-x_Q}+\frac{u_Q}{(x-x_Q)^2}\right), \\ Y &= y-\sum_{Q\in S}\left(u_Q\frac{2y+a_1x+a_3}{(x-x_Q)^3}+t_Q\frac{a_1(x-x_Q)+y-y_Q}{(x-x_Q)^2}+\frac{a_1u_Q-g_Q^xg_Q^y}{(x-x_Q)^2}\right), \end{aligned} \tag{8}$$

where

$$\begin{aligned} Q &= (x_Q,y_Q), \\ g_Q^x &= \frac{\partial G}{\partial \xi}(x_Q,y_Q) = 3x_Q^2+2a_2x_Q+a_4-a_1y_Q, \\ g_Q^y &= \frac{\partial G}{\partial \eta}(x_Q,y_Q) = -2y_Q-a_1x_Q-a_3, \\ t_Q &= \begin{cases} g_Q^x & \text{if } Q\in F_2, \\ 2g_Q^x-a_1g_Q^y = 6x_Q^2+b_2x_Q+b_4 & \text{if } Q\notin F_2, \end{cases} \\ u_Q &= (g_Q^y)^2 = 4x_Q^3+b_2x_Q^2+2b_4x_Q+b_6. \end{aligned} \tag{9}$$

We obtain these formulas via the addition formulas on E. Indeed, if $Q\in F_2$, we have

$$\begin{aligned} x(P+Q)-x(Q) &= \frac{t_Q}{x-x_Q}; \\ y(P+Q)-y(Q) &= -\frac{a_1(x-x_Q)+y-y_Q}{(x-x_Q)^2}\,t_Q \qquad \text{and} \qquad u_Q=0, \end{aligned}$$

and if $Q\notin F_2$, we have

$$\begin{aligned} x(P+Q)-x(Q)+x(P-Q)-x(-Q) &= \frac{t_Q}{(x-x_Q)^2}+\frac{u_Q}{(x-x_Q)^3}, \\ y(P+Q)-y(Q)+y(P-Q)-y(-Q) & \\ = -u_Q\,\frac{2y+a_1x+a_3}{(x-x_Q)^3} &- t_Q\,\frac{a_1(x-x_Q)+y-y_Q}{(x-x_Q)^2}-\frac{a_1u_Q-g_Q^xg_Q^y}{(x-x_Q)^2}. \end{aligned}$$

We now consider the relation between X and Y. We set

$$t=\sum_{Q\in S}t_Q, \qquad w=\sum_{Q\in S}(u_Q+x_Qt_Q). \tag{10}$$

We get

$$
\begin{aligned}
&Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6,\\
&\text{where } A_1 = a_1, \qquad A_2 = a_2, \qquad A_3 = a_3,\\
&A_4 = a_4 - 5t, \qquad A_6 = a_6 - b_2t - 7w.
\end{aligned} \tag{11}
$$

To obtain this relation, we plug (2) into (8), which gives

$$
\begin{aligned}
X =&z^{-2} - a_1z - a_2 - a_3z\\
&-(\alpha_4 - t)z^2 - (\alpha_5 - a_1t)z^3 - (\alpha_6 - a_1^2t - a_2t - w)z^4 - \dots,\\
Y =&-z^{-3} + a_1z^{-2} + a_2z^{-1} + a_3 + (\alpha_4 + t)z + \alpha_5z^2 + (\alpha_6 + a_1^2t + 2w)z^3 + \dots.
\end{aligned} \tag{12}
$$

We set $Z = -X/Y$ and conclude from (12) that

$$
\begin{aligned}
Z &= z + 2tz^5 + 3a_1tz^6 + (4a_1^2t + 4a_2t + 3w)z^7 + \dots,\\
z &= Z - 2tZ^5 - 3a_1tZ^6 - (4a_1^2t + 4a_2t + 3w)Z^7 + \dots.
\end{aligned} \tag{13}
$$

We plug z into (12) again and find

$$
\begin{aligned}
X =&Z^{-2} - a_1Z^{-1} - a_2 - a_3Z\\
&-(\alpha_4 - 5t)Z^2 - (\alpha_5 - 5a_1t)Z^3 - (\alpha_6 - 9a_2t - 6a_1^2t - 7w)Z^4 - \dots,
\end{aligned}
$$

which give the formulas (11).

Remarks. 1. We can choose other functions for X and Y. The ones chosen in this paper are such that the uniformizers Z and z coincide to order 5, which is the largest possible order.

2. If we set $\omega(X,Y) = dX/(2Y + a_1X + a_3)$, we have $\omega(x,y) = \omega(X,Y)$.

3. If E is defined over a subfield k_0 of k, and F is separable over k_0 and stable under conjugation over k_0, then the elliptic curve E/F as well as the isogeny f are naturally defined over k_0, and the above formulas are valid over k_0.

4 Application

Consider the elliptic curve over $\mathbb{Q}$ defined by the equation

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

It has a subgroup F of order 7 consisting of the points $\mathcal{O}$, $Q = (1,0)$, $2Q = (-1,-2)$,

$3Q = (3,-6)$, $4Q = (3,2)$, $5Q = (-1,2)$, $6Q = (1,-2)$. We have[1]

$$
\begin{array}{lllll}
x_Q = 1, & t_Q = -2, & u_Q = 4, & g^x_Q = -2, & g^y_Q = -2, \\
x_{2Q} = -1, & t_{2Q} = 4, & u_{2Q} = 16, & g^x_{2Q} = 4, & g^y_{2Q} = 4, \\
x_{3Q} = 3, & t_{3Q} = 40, & u_{3Q} = 64, & g^x_{3Q} = 24, & g^y_{3Q} = 8, \\
b_2 = -3, & b_4 = -5, & b_6 = 13, & t = 42, & w = 198,
\end{array}
\tag{14}
$$

the curve $E' = E/F$ has equation $y^2 + xy + y = x^3 - x^2 - 213x - 1257$, and the isogeny $f\colon E \to E'$ is obtained by plugging the values (14) into (8).

[1]The French original lists the incorrect value $g^x_Q = -4$; we have listed the correct value $g^x_Q = -2$ in the table of results.