Publ. Mat. (2007), 147–163
Proceedings of the *Primeras Jornadas de Teoría de Números*.

GENERALIZATION OF VÉLU'S FORMULAE FOR ISOGENIES BETWEEN ELLIPTIC CURVES

Josep M. Miret, Ramiro Moreno and Anna Rio

Abstract

Given an elliptic curve E and a finite subgroup G, Vélu's formulae concern to a separable isogeny $\mathcal{I}_G\colon E \to E'$ with kernel G. In particular, for a point $P \in E$ these formulae express the first elementary symmetric polynomial on the abscissas of the points in the set $P+G$ as the difference between the abscissa of $\mathcal{I}_G(P)$ and the first elementary symmetric polynomial on the abscissas of the nontrivial points of the kernel G. On the other hand, they express Weierstraß coefficients of E' as polynomials in the coefficients of E and two additional parameters: $w_0 = t$ and $w_1 = w$. We generalize this by defining parameters w_n for all $n \geq 0$ and giving analogous formulae for all the elementary symmetric polynomials and the power sums on the abscissas of the points in $P+G$. Simultaneously, we obtain an efficient way of performing computations concerning the isogeny when G is a rational group.

1. Vélu's formulae

An elliptic curve E over a field K is a smooth projective curve over K of genus one with a distinguished K-rational point. If E/K is an elliptic curve then it has a plane model given by an affine Weierstraß equation

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

such that the coefficients $a_i \in K$ and the distinguished point is the point at infinity $\mathcal{O} = (0 : 1 : 0) \in E(K)$.

2000 *Mathematics Subject Classification.* 11G05.
Key words. Elliptic curve, isogeny, rational subgroup.
The first and second authors were supported in part by grant TIC2003-09188. The third author was supported in part by grants BFM2003-06768-C02-01 and 2005SGR 00443.

As usual (see [**3**]), we define the following quantities associated with the above equation

$$b_2 = a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6, \quad b_8 = (b_2b_6 - b_4^2)/4,$$

$$\Delta = 9b_2b_4b_6 - b_2^2b_8 - 8b_4^3 - 27b_6^2, \quad j = (b_2^2 - 24b_4)^3/\Delta.$$

The equation defines an elliptic curve if and only if Δ is nonzero. And such equations define elliptic curves which are isomorphic over $\bar{K}$ if and only if they give the same quantity j.

An elliptic curve E/K has a natural structure of a commutative algebraic group with the distinguished K-rational point as the identity element. Using the above Weierstraß model, the addition law is as follows. Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$. If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 + P_2 = \mathcal{O}$. Otherwise, let

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\[2ex] \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{otherwise} \end{cases}$$

$$\nu = \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\[2ex] \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{otherwise.} \end{cases}$$

Then, $P + Q = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3)$.

An isogeny between elliptic curves E_1 and E_2 over K is a morphism $\mathcal{I}\colon E_1 \to E_2$ such that $\mathcal{I}(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. Its equations are of the form

$$\mathcal{I}(x, y) = (R(x), S(x, y))$$

where $R(x)$, $S(x, y)$ are rational functions, $R(x) \in \bar{K}(x)$ and $S(x, y) \in \bar{K}(x, y)$.

An isogeny is a group morphism, and if it is non constant, namely $\mathcal{I} \neq \mathcal{O}_{E_2}$, then it is surjective (finite morphism). It induces a field immersion $\mathcal{I}^*\colon \bar{K}(E_2) \to \bar{K}(E_1)$ between the corresponding function fields. The degree of the isogeny is the degree of the field extension and if this extension is separable then it is Galois with Galois group isomorphic to $\ker \mathcal{I}$.

Given an elliptic curve E and a finite subgroup G there exists a unique, up to $\bar{K}$-isomorphism, elliptic curve E' and a separable isogeny $\mathcal{I}_G\colon E \to E'$ (defined up to $\mathrm{Aut}(E')$) such that $\ker \mathcal{I}_G = G$ (see [**3**, III.4.12]). This elliptic curve is denoted by the quotient E/G. If E is defined over K

and G is $\mathrm{Gal}(\bar{K}/K)$ invariant, then the curve E/G and the isogeny $\mathcal{I}_G$ are defined over K. For example, if $Q \in E(K)$ is a point of order m and $G = \langle Q \rangle$ then

$$\mathcal{I}\colon E \to E/\langle Q \rangle$$

is a degree m isogeny defined over K.

If E is an elliptic curve over K, when we look at the local ring $K[E]_{\mathcal{O}}$ and take the completion at its maximal ideal, we get a power series ring in one variable, say $K[[z]]$, for some uniformizer z at $\mathcal{O}$. We can take $z = x/y$ and then the expression of the Weierstraß coordinate x as formal Laurent power series in z is

$$x(z) = \frac{1}{z^2} - \alpha_1 \frac{1}{z} - \alpha_2 - \alpha_3 z - \alpha_4 z^2 - \alpha_5 z^3 - \alpha_6 z^4 - \cdots ,$$

where $\alpha_1 = a_1$, $\alpha_2 = a_2$, $\alpha_3 = a_3$, $\alpha_4 = a_1a_3 + a_4$, $\alpha_5 = a_2a_3 + a_1^2a_3 + a_1a_4$ and $\alpha_6 = a_1^2a_4 + \cdots + a_6$. We have $y = -x/z = -z^{-3} + \alpha_1 z^{-2} + \alpha_2 z^{-1} + \alpha_3 + \alpha_4 z + \cdots$, and the function field $K(E)$ is isomorphic to $K(x, y)$.

For a finite subgroup G of E, Vélu defines

$$\begin{aligned} X(P) &= x(P) + \sum_{Q \in G - \{\mathcal{O}\}} \bigl(x(P+Q) - x(Q)\bigr) \\ &= x + \sum_{T \in PG - \{\mathcal{O}\}} \frac{t(T)}{x - x(T)} + \frac{u(T)}{(x - x(T))^2} \end{aligned}$$

where PG is a system of representatives of the orbits of G under the action of $\{\pm 1\}$, $u(T) = 4x(T)^3 + b_2x(T)^2 + 2b_4x(T) + b_6$, $t(T) = 6x(T)^2 + b_2x(T) + b_4$ if $2T \neq \mathcal{O}$ and $t(T) = 3x(T)^2 + 2a_2x(T) + a_4 - a_1y(T)$ if $2T = \mathcal{O}$. A function $Y(P)$ is defined analogously:

$$Y(P) = y(P) + \sum_{Q \in G - \{\mathcal{O}\}} \bigl(y(P+Q) - y(Q)\bigr).$$

The functions $X, Y \in K(E)$ are invariant under the action of G (by translation), the function field $K(E/G)$ is isomorphic to $K(X, Y)$ and the isogeny $\mathcal{I}_G$ is identified with the transformation $(x, y) \to (X, Y)$ (see [**4**, §2]).

From the second equality for $X(P)$ we get on one hand the expression of X as rational function of x, which gives the equation of the isogeny

$$\mathcal{I}_G\colon (x, y) \mapsto (X = R(x), Y)$$

and on the other hand the expression of X as formal Laurent power series in z

$$\begin{aligned} X(z) = \frac{1}{z^2} - \frac{\alpha_1}{z} - \alpha_2 - \alpha_3 z - (\alpha_4 - w_0)z^2 - (\alpha_5 - w_0\alpha_1)z^3 \\ - \left(\alpha_6 - w_0(\alpha_1^2 + \alpha_2) - w_1\right) z^4 \\ - \left(\alpha_7 - w_0(\alpha_1^3 + 2\alpha_1\alpha_2 + \alpha_3) - 2w_1\alpha_1\right) z^5 - \cdots , \end{aligned}$$

which determines Weierstrass coefficients for E/G

$$a_1' = a_1, \quad a_2' = a_2, \quad a_3' = a_3, \quad a_4' = a_4 - 5w_0, \quad a_6' = a_6 - b_2 w_0 - 7w_1,$$

where $w_0 = \sum_{T\in PG} t(T)$ and $w_1 = \sum_{T\in PG}(u(T) + x(T)t(T))$.

Looking over all these formulae, we see that in order to make explicit computations concerning the isogeny, we have to operate with the abscissas of the points in the kernel G. As we mentioned above, if this group is $\mathrm{Gal}(\bar{K}/K)$ invariant, then the curve E/G and the isogeny $\mathcal{I}_G$ are defined over K. But the computations to obtain equations, for the curve or the isogeny, may involve non K-rational abscissas.

The Galois invariance of the subgroup G is equivalent to the fact that the polynomial

$$\psi_G(x) = \prod_{Q\in G-\{\mathcal{O}\}} (x - x(Q))$$

has coefficients in K (see [**2**]), namely that the elementary symmetric polynomials in the abscissas of $G - \{\mathcal{O}\}$ lie in K. The efficiency of computations would then be improved if we can perform them in terms of these symmetric polynomials.

2. Generalization

The above equality

$$X(P) = \sum_{Q\in G} x(P+Q) - \sum_{Q\in G-\{\mathcal{O}\}} x(Q)$$

can be rewritten in the form

$$\mathbf{S_1} = X + S_1,$$

showing that the first elementary symmetric polynomial in the abscissas of $P + G$ is expressed as the sum of the abscissa of $\mathcal{I}_G(P)$ and the first elementary symmetrical polynomial in the abscissas of the points in $G - \{\mathcal{O}\}$.

Our goal is to obtain analogous formulas for $\mathbf{S_r}$, the r-th elementary symmetric polynomial in the abscissas of $P+G$ and for $\mathbf{S^{(r)}}$, the r-th power sum of these abscissas, for all r such that $1 \leq r \leq \deg \mathcal{I}_G = |G|$.

2.1. Symmetric polynomials.

The first goal is achieved if we are able to determine the coefficients of the polynomial

$$\prod_{Q \in G} (x - x(P+Q)) = x^{|G|} - (X + S_1)x^{|G|-1} + \cdots$$

attached to the preimage of the point $\mathcal{I}_G(P) \in E'$. But this polynomial is obtained from the equality

$$X = R(x) = x(P) + \sum_{T \in PG - \{\mathcal{O}\}} \frac{t(T)}{x - x(T)} + \frac{u(T)}{(x - x(T))^2},$$

and becomes of the form $R_1(x) + (x - X)\psi_G(x)$ when we express the rational function $R(x)$ as $x + R_1(x)/\psi_G(x)$.

Theorem 1. *Let E be an elliptic curve and G a nontrivial finite subgroup of E. If P is a point of E, then*

$$\prod_{Q \in G}(x - x(P+Q)) = x^{|G|} - (X + S_1)x^{|G|-1} + \sum_{r=2}^{|G|}(-1)^r\left(S_{r-1}X + S_r + \sum_{i=0}^{r-2}(-1)^i w_i S_{r-i-2}\right)x^{|G|-r}$$

where X is the abscissa of the isogenous point $\mathcal{I}_G(P)$, S_j is the j-th elementary symmetric polynomial in the abscissas of the points in $G - \{\mathcal{O}\}$ (with $S_{|G|} = 0$) and

$$w_i = \sum_{T \in PG - \{\mathcal{O}\}} \left(t(T)x(T)^i + u(T)\, i\, x(T)^{i-1}\right),$$

with PG a system of representatives of the orbits of G under the action of $\{\pm 1\}$ and

$$t(T) = \begin{cases} 6x(T)^2 + b_2x(T) + b_4, & \text{if } T \in G \setminus E[2], \\ \dfrac{6x(T)^2 + b_2x(T) + b_4}{2}, & \text{if } T \in G \cap E[2], \end{cases}$$

$$u(T) = 4x(T)^3 + b_2x(T)^2 + 2b_4x(T) + b_6, \text{ for all } T \in G - \{\mathcal{O}\},$$

where $E[2]$ denotes the 2-torsion subgroup of E.

Therefore, if $1 \leq r \leq |G|$, *for the* r*-th elementary symmetric polynomial in the abscissas of the points in* $P+G$ *we have*

$$\mathbf{S_r} = S_{r-1}\, X + S_r + \sum_{i=0}^{r-2} (-1)^i\, w_i\, S_{r-i-2}.$$

Proof: As we said above, we begin with the expression of the abscissa of $\mathcal{I}_G(P)$ as rational function of the abscissa of P:

$$X = x + \sum_{T\in PG-\{\mathcal{O}\}} \frac{t(T)}{x-x(T)} + \frac{u(T)}{(x-x(T))^2} = R(x) = x + \frac{R_1(x)}{\psi_G(x)}.$$

Note that the formulae for $t(T)$ given in the theorem agree with the definition previously given.

Taking into account that $x(Q) = x(-Q)$ for all $Q \in G \setminus E[2]$ and $u(T) = 0$ for all $T \in E[2]$, we have

$$\prod_{T\in PG\cap E[2]\setminus\{\mathcal{O}\}} (x - x(T)) \prod_{T\in PG\setminus E[2]} (x-x(T))^2 = \prod_{Q\in G-\{\mathcal{O}\}} (x - x(Q))$$

and this is the polynomial $\psi_G(x) = \sum\limits_{r=0}^{|G|-1} (-1)^r S_r\, x^{|G|-r-1}$.

As for the numerator,

$$\begin{aligned} R_1(x) &= \sum_{T\in PG-\{\mathcal{O}\}} \left(t(T)\frac{\psi_G(x)}{x-x(T)} + u(T)\frac{\psi_G(x)}{(x-x(T))^2}\right) \\ &= \sum_{T\in PG-\{\mathcal{O}\}} t(T) \sum_{r=0}^{|G|-2} (-1)^r S_r(T,t) x^{|G|-r-2} \\ &\quad + \sum_{T\in PG-\{\mathcal{O}\}} u(T) \sum_{r=0}^{|G|-3} (-1)^r S_r(T,u) x^{|G|-r-3} \end{aligned}$$

where we have denoted $S_r(T,t)$ the r-th elementary symmetric polynomial in the abscissas of the points in $G - \{\mathcal{O}, T\}$ and $S_r(T,u)$ the r-th elementary symmetric polynomial in the abscissas of the points in $G - \{\mathcal{O}, \pm T\}$. These polynomials can be expressed in terms of the S_r using the following recurrences

$$\begin{aligned} S_r(T,t) &= S_r - x(T) S_{r-1}(T,t) \\ S_r(T,u) &= S_r - 2x(T) S_{r-1}(T,u) - x(T)^2 S_{r-2}(T,u), \end{aligned}$$

with $S_0(T,*) = 1$ and $S_{-1}(t,*) = 0$. We have

$$S_r(T,t) = \sum_{i=0}^{r} (-1)^i S_{r-i} x(T)^i,$$

$$S_r(T,u) = \sum_{i=0}^{r} (-1)^i (i+1) S_{r-i} x(T)^i$$

and

$$\begin{aligned} R_1(x) = & \sum_{r=0}^{|G|-2} (-1)^r \left(\sum_T t(T) S_r(T,t) \right) x^{|G|-r-2} \\ & + \sum_{r=0}^{|G|-3} (-1)^r \left(\sum_T u(T) S_r(T,u) \right) x^{|G|-r-3} \\ = & \sum_{r=0}^{|G|-2} (-1)^r \left(\sum_T t(T) S_r(T,t) - u(T) S_{r-1}(T,u) \right) x^{|G|-r-2} \\ = & \sum_{r=0}^{|G|-2} (-1)^r \left(\sum_{i=0}^{r} (-1)^i S_{r-i} \right. \\ & \left. \times \left(\sum_T t(T) x(T)^i + u(T) i x(T)^{i-1} \right) \right) x^{|G|-r-2}. \end{aligned}$$

On the other hand, for $0 \leq r \leq |G|$ the coefficient of $x^{|G|-r}$ in $(x - X)\psi_G(x)$ is $(-1)^r (S_r + X S_{r-1})$. Now we have computed the coefficients of the polynomial $R_1(x) + (x - X)\psi_G(x)$ and the result follows. □

We call the

$$w_i = \sum_T t(T) x(T)^i + u(T) i x(T)^{i-1}$$

generalized Vélu parameters. They appear when we consider further terms of X as formal Laurent power series in z:

$$\begin{aligned}X(P) = \frac{1}{z^2} - \frac{\alpha_1}{z} &- \alpha_2 - \alpha_3 z - (\alpha_4 - w_0)z^2 - (\alpha_5 - w_0\alpha_1)z^3\\ &- (\alpha_6 - w_0(\alpha_1^2 + \alpha_2) - w_1)\, z^4\\ &- (\alpha_7 - w_0(\alpha_1^3 + 2\alpha_1\alpha_2 + \alpha_3) - 2w_1\alpha_1)\, z^5\\ &- (\alpha_8 - w_0(\alpha_1^4 + 3\alpha_1^2\alpha_2^2 + 2\alpha_1\alpha_3 + \alpha_4)\\ &\qquad - w_1(3\alpha_1^2 + 2\alpha_2) - w_2)\, z^6 - \cdots\\ &- (\alpha_9 - w_0(\alpha_1^5 + 4\alpha_1^3\alpha_2 + 3\alpha_1^2\alpha_3 + 2\alpha_2\alpha_3 + 3\alpha_1\alpha_2^2 + 2\alpha_1\alpha_4 + \alpha_5)\\ &\qquad - 2w_1(2\alpha_1^3 + 3\alpha_1\alpha_2 + \alpha_3) - 3\alpha_1 w_2)\, z^7 - \cdots\end{aligned}$$

More precisely, the power series $X(P) - x(P) = \sum_{j\geq 2} A_j\, z^j$ has coefficients

$$A_j = \sum_{\substack{n_1<\cdots<n_s\\ h_1n_1+\cdots+h_sn_s+2i=j-2}} \frac{(h_1+\cdots+h_s+i)!}{h_1!\ldots h_s!\ i!}\,\alpha_{n_1}^{h_1}\ldots\alpha_{n_s}^{h_s}\, w_i.$$

Remark 1. The theorem gives the first equation of the isogeny in terms of the elementary symmetric polynomials in the abscissas of the points in $G - \{\mathcal{O}\}$ and the generalized Vélu parameters.

$$\begin{aligned}X &= x + \frac{R_1(x)}{\psi_G(x)}\\ &= \frac{x^{|G|} - S_1x^{|G|-1} + \sum_{r=2}^{|G|}(-1)^r\left(S_r + \sum_{i=0}^{r-2}(-1)^i w_i S_{r-i-2}\right)x^{|G|-r}}{\psi_G(x)}.\end{aligned}$$

For the efficiency of computations we would like to obtain these parameters w_i without computing the abscissas of the points in G. We seek an expression for them which is directly computable from the symmetric polynomials S_j. Plugging the formulae for $t(T)$ and $u(T)$ in the formula giving the w_i we get an alternative expression

$$w_i = (2i+3)S^{(i+2)} + \frac{(i+1)b_2}{2}S^{(i+1)} + \frac{(2i+1)b_4}{2}S^{(i)} + \frac{ib_6}{2}S^{(i-1)}$$

where $S^{(j)}$ indicates the j-th power sum of the abscissas of the points in $G - \{\mathcal{O}\}$. Now, the Newton formulae allow us to obtain these power sums, and the w_i, from the symmetric polynomials S_j.

2.2. Power sums.

The formula $\mathbf{S_1} = X + S_1$ admits yet another generalization, since $\mathbf{S_1}$ is also the first power sum in the abscissas of the points in $P + G$. We denote $\mathbf{S^{(r)}}$ the r-th power sum of these abscissas, for all r such that $1 \leq r \leq |G|$, and $S^{(r)}$ the r-th power sum of the abscissas of the points in $G - \{\mathcal{O}\}$.

Proposition 1. *Let E/K be an elliptic curve and G a nontrivial finite subgroup of E. If x, X denote Weierstraß coordinates of points $P, \mathcal{I}_G(P)$, respectively, and z is a uniformizer at $\mathcal{O}$, then for all r such that $2 \leq r \leq |G|$ there exist elements $\beta_{0,r}, \beta_{1,r}, \dots, \beta_{r-2,r} \in K$ such that*

$$f_r(z) = x(z)^r - X(z)^r - \sum_{i=2}^{r} \beta_{i-2,r} X(z)^{r-i}$$

belongs to the maximal ideal of $K[[z]]$. Namely, as an element of the function field of E, the function f_r vanishes at the infinite point $\mathcal{O}$.

Proof: We denote v the valuation of $K((z))^*$. Since $v(x) = -2$, all nonzero rational functions in x have valuations in the ideal $2\mathbb{Z}$. Therefore, all nonzero polynomial expressions in x and X have valuation in this ideal. Since

$$\begin{aligned} x(z)^r = {} & \frac{1}{z^{2r}} - \frac{r\alpha_1}{z^{2r-1}} - \frac{r\alpha_2 - \binom{r}{2}\alpha_1^2}{z^{2r-2}} - \frac{r\alpha_3 - 2\binom{r}{2}\alpha_1\alpha_2 + \binom{r}{3}\alpha_1^3}{z^{2r-3}} \\ & - \frac{r\alpha_4 - \binom{r}{2}(\alpha_2^2 + 2\alpha_1\alpha_3) + 3\binom{r}{3}\alpha_1^2\alpha_2 - \binom{r}{4}\alpha_1^4}{z^{2r-4}} \\ & + \mathrm{O}(z^{-(2r-5)}), \end{aligned}$$

$$\begin{aligned} X(z)^r = {} & \frac{1}{z^{2r}} - \frac{r\alpha_1}{z^{2r-1}} - \frac{r\alpha_2 - \binom{r}{2}\alpha_1^2}{z^{2r-2}} - \frac{r\alpha_3 - 2\binom{r}{2}\alpha_1\alpha_2 + \binom{r}{3}\alpha_1^3}{z^{2r-3}} \\ & - \frac{r(\alpha_4 - w_0) - \binom{r}{2}(\alpha_2^2 + 2\alpha_1\alpha_3) + 3\binom{r}{3}\alpha_1^2\alpha_2 - \binom{r}{4}\alpha_1^4}{z^{2r-4}} \\ & + \mathrm{O}(z^{-(2r-5)}), \end{aligned}$$

we have that $v(x^r - X^r) \geq -(2r-4)$ (with equality if $w_0 \neq 0$). Since X^{r-2} has valuation $-(2r-4)$, there exists $\beta_{0,r} \in K$ (concretely, $\beta_{0,r} = -rw_0$) such that $v(x^r - X^r - \beta_{0,r}X^{r-2}) \geq -(2r-5)$. If $x^r - X^r - \beta_{0,r}X^{r-2} = 0$, we take all the remaining β's equal to zero and we have finished. If not, $v(x^r - X^r - \beta_{0,r}X^{r-2})$ is even and $\geq -(2r-6)$. We continue with X^{r-3} and iterate the process until we get $v(f_r(z)) > 0$. $\square$

For r fixed, the computation of $\beta_{0,r}, \beta_{1,r}, \ldots, \beta_{r-2,r}$ amounts to solving an homogenous linear system. In this way, we obtain

$$\begin{aligned}
\beta_{0,r} &= -rw_0,\\
\beta_{1,r} &= -rw_1,\\
\beta_{2,r} &= r\left(-w_2 + \frac{r-3}{2!}w_0^2\right),\\
\beta_{3,r} &= r\left(-w_3 + (r-4)w_0w_1\right),\\
\beta_{4,r} &= r\left(-w_4 + \frac{r-5}{2!}w_1^2 + (r-5)w_0w_2 - \frac{(r-4)(r-5)}{3!}w_0^3\right),\\
\beta_{5,r} &= r\left(-w_5 + (r-6)w_0w_3 + (r-6)w_1w_2 - \frac{(r-5)(r-6)}{2!}w_0^2w_1\right)\\
&\vdots
\end{aligned}$$

Proposition 2. *With the hypothesis and notations of the previous proposition, for all r such that $2 \leq r \leq |G|$, let $S^{(r)}$ be the r-th power sum of the abscissas of the points in $G - \{\mathcal{O}\}$ and $\mathbf{S^{(r)}}$ the r-th power sum of the abscissas of the points in $P + G$. Then,*

$$\mathbf{S^{(r)}} - S^{(r)} = X^r + \sum_{i=2}^{r} \beta_{i-2,r}X^{r-i}.$$

Proof: Let us denote

$$\varphi_1 = x(P)^r + \sum_{Q\in G-\{\mathcal{O}\}} \big(x(P+Q)^r - x(Q)^r\big) = \mathbf{S^{(r)}} - S^{(r)}$$

$$\varphi_2 = X(P)^r + \sum \beta_{i-2,r}\, X(P)^{r-i}.$$

Both functions belong to the function field of the isogenous curve $E' = E/G$. In $\bar{K}(E')$ lies also its difference, which can be written in the following way:

$$\varphi_1 - \varphi_2 = f_r + \sum_{Q\in G-\{\mathcal{O}\}} \big(x(P+Q)^r - x(Q)^r\big).$$

It is a function without poles, therefore constant, which vanishes at the infinite point. We conclude that $\varphi_1 - \varphi_2 = 0$ as we claimed. $\square$

2.3. Newton formulae.

At this point we have obtained formulae for symmetric polynomials involving the w_i and formulae for the power sums involving the $\beta_{k,r}$. The classical link between them are the Newton formulae (for $r \leq |G|$)

$$\mathbf{S_r} = \frac{1}{r}\sum_{i=0}^{r-1}(-1)^{r+i-1}\,\mathbf{S^{(r-i)}}\,\mathbf{S_i},$$

which will provide some kind of link between w's and β's, and hopefully an efficient way to compute the β's.

Direct computations that we have already shown give the initial values $\beta_{0,r} = -rw_0$ and $\beta_{1,r} = -rw_1$. This is all we need if $|G|$ is 2 or 3. For $|G| \geq 4$ we would have to compute $\beta_{k,r}$ for $4 \leq r \leq |G|$ and $2 \leq k \leq r-2$.

Proposition 3. *With the hypothesis and notations of the previous propositions, assume that $|G| \geq 4$. For $4 \leq r \leq |G|$ and $2 \leq k < r-2$ we have*

$$\beta_{k,r} = \beta_{k,r-1} - w_k - \sum_{i=0}^{k-2} w_i\beta_{k-i-2,r-i-2}.$$

For the last one, we have

$$\beta_{r-2,r} = -rw_{r-2} - \sum_{j=0}^{r-4} w_j\beta_{r-j-4,r-j-2}.$$

Example 1. If $|G|=5$, we have $\beta_{0,2}=-2w_0$, $\beta_{0,3}=-3w_0$, $\beta_{1,3} = -3w_1$, $\beta_{0,4} = -4w_0$ and $\beta_{1,4} = -4w_1$. Now, using the second formula,

$$\beta_{2,4} = -4w_2 - w_0\beta_{0,2} = -4w_2 + 2w_0^2.$$

We also know $\beta_{0,5} = -5w_0$, $\beta_{1,5} = -5w_1$, and from the first formula we compute

$$\beta_{2,5} = \beta_{2,4} - w_2 - w_0\beta_{0,3} = -5w_2 + 5w_0^2.$$

Finally, $\beta_{3,5} = -5w_3 - (w_0\beta_{1,3} + w_1\beta_{0,2}) = -5w_3 + 5w_0w_1$ and we have the whole family of β's.

Proof of Proposition 3: We plug the above formulae for symmetric polynomials and power sums into the Newton formula to obtain an equality $F_r(X) = 0$ which is polynomial in X. Since X is transcendental over $\bar{K}$, the coefficients must be zero. The degree of F_r is a priori r, but we see that the coefficient of X^r is $S_0 - S_0$ and the coefficient of X^{r-1} is $-S_1 + S_1$. On the other hand, the coefficients of X^{r-2} and X^{r-3} are $\beta_{0,r} - \beta_{0,r-1} + w_0 = 0$ and $\beta_{1,r} - \beta_{1,r-1} + w_1 = 0$, respectively.

We have then $F_r(X)=\sum_{k=2}^{r-2} F_{k,r}X^{r-2-k}$, with

$$F_{k,r}=\sum_{j=0}^{k-2}(-1)^j S_j\gamma_{k-j,r-j}, \quad \text{for} \quad 2\le k\le r-4,$$

$$F_{r-3,r}=\sum_{j=0}^{k-2}(-1)^j S_j\gamma_{k-j,r-j}-\sum_{j=0}^{r-1}(-1)^j S^{(r-j-1)}S_j,$$

$$F_{r-2,r}=\sum_{j=4}^{r}(-1)^{r-j}S_{r-j}\delta_j+\sum_{j=0}^{r}(-1)^j S^{(r-j)}S_j$$
$$+\sum_{j=0}^{r-2}\left(w_{r-j-2}\sum_{i=0}^{j}(-1)^i S^{(j-i)}S_i\right),$$

where

$$\gamma_{k,r}=\beta_{k,r}-\beta_{k,r-1}+w_k+\sum_{i=0}^{k-2}w_i\beta_{k-i-2,r-i-2}, \quad \text{for } 2\le k\le r-1,$$

$$\delta_j=\beta_{j-2,j}+jw_{j-2}+\sum_{i=0}^{j-4}w_i\beta_{j-i-4,j-i-2}, \qquad \text{for } 4\le j\le r.$$

Using the Newton formulae, now considering that the variables are the abscissas of the points in $G-\{\mathcal{O}\}$, we see that all the summations containing power sums vanish and

$$F_{k,r}=\sum_{j=0}^{k-2}k(-1)^j S_j\gamma_{k-j,r-j}, \quad \text{for } 2\le k\le r-3,$$

$$F_{r-2,r}=\sum_{j=4}^{r}(-1)^{r-j}S_{r-j}\delta_j.$$

Let us begin with $F_{r-2,r}=0$. If $r=4$, it gives that $\delta_4=0$ (namely, that $\beta_{2,4}=-4w_2-w_0\beta_{0,2}$). Let us assume that $r>4$ and $\delta_j=0$ for all j between 4 and $r-1$. Then,

$$0=F_{r-2,r}=\sum_{j=4}^{r-1}(-1)^{r-j}S_{r-j}\delta_j+\delta_r$$

and we get $\delta_r = 0$, that is,

$$\beta_{r-2,r} + rw_{r-2} + \sum_{j=0}^{r-4} w_j \beta_{r-j-4,r-j-2} = 0.$$

Now we proceed with $F_{k,r} = 0$ and use induction on k. If $k = 2$, it gives $0 = F_{2,r} = \gamma_{2,r} = \beta_{2,r} - \beta_{2,r-1} + w_2 + w_0\beta_{0,r-2}$ for all $r \geq 5$. Let us assume $k > 2$ and $\gamma_{h,s} = 0$ for all h between 2 and $k-1$ and all $s \geq h+3$. If $r-3 \geq k$, then

$$0 = F_{k,r} = \gamma_{k,r} + \sum_{j=1}^{k-2} (-1)^j S_j \gamma_{k-j,r-j}$$

and the induction hypothesis gives $\gamma_{k,r} = 0$, namely

$$\beta_{k,r} = \beta_{k,r-1} - w_k - \sum_{i=0}^{k-2} w_i \beta_{k-i-2,r-i-2}$$

and we are done. □

The recurrences given in the above proposition show that $\beta_{k,r} \in \mathbb{Q}[w_0, w_1, \ldots, w_k]$ and provide an efficient way to compute them. For the sake of completeness we give also their explicit expression as polynomials in the generalized Vélu parameters:

$$\beta_{k,r} = r \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^{j+1} \binom{r-k+j-2}{j} B_{j\,k},$$

where

$$B_{j\,k} = \sum_{\substack{n_1 < \cdots < n_s \\ h_1 + \cdots + h_s = j+1 \\ h_1 n_1 + \cdots + h_s n_s = k-2j}} \frac{j!}{h_1! \ldots h_s!} w_{n_1}^{h_1} \ldots w_{n_s}^{h_s}.$$

3. Example

We take the example from Vélu's paper, namely the elliptic curve $E/\mathbb{Q}$ defined by the equation

$$E/\mathbf{Q} : y^2 + xy + y = x^3 - x^2 - 3x + 3,$$

and the subgroup G of order 7 generated by the point $Q = (1,0)$. Its elements are the infinite point $\mathcal{O}$ and the points

$$Q = (1,0), \quad 2Q = (-1,-2), \quad 3Q = (3,-6),$$
$$4Q = (3,2), \quad 5Q = (-1,2), \quad 6Q = (1,-2).$$

First of all we compute the symmetric polynomials in the abscissas of these points and the generalized Vélu parameters. Since in this case all the points in G are rational, these parameters can be easily computed from the defining formula.

i	0	1	2	3	4	5	6
S_i	1	6	7	-12	-17	6	9
w_i	42	198	722	2862	10106	35734	

Using the formula of Theorem 1, we compute the symmetric polynomials in the abscissas of the points in $P+G$:

i	$\mathbf{S_i}$
1	$X+6$
2	$6X+49$
3	$7X+42$
4	$-12X-189$
5	$-17X-414$
6	$6X-341$
7	$9X-178$

where X is the abscissa of the isogenous point $\mathcal{I}_G(P)$.

In order to compute the power sums, we need the elements $\beta_{k,r}$, that we obtain from the recurrences of the last proposition:

$r\backslash k$	0	1	2	3	4	5
2	-84					
3	-126	-594				
4	-168	-792	640			
5	-210	-990	5210	27270		
6	-252	-1188	11544	82620	90744	
7	-294	-1386	19642	154602	109606	-852922

Finally, using the formula of Proposition 2 we can get the power sums of the abscissas of the points in $P+G$:

i	$\mathbf{S^{(i)}}$
1	$X+6$
2	X^2-62
3	$X^3-126X-540$
4	$X^4-168X^2-792X+806$
5	$X^5-210X^3-990X^2+5210X+27756$
6	$X^6-252X^4-1198X^3-11544X^2+82620X+92206$
7	$X^7-294X^5-1386X^4+19642X^3+154602X^2+109606X-848548$

The elliptic curve of this example is the curve 26b1 in Cremona's tables (see [**1**]). The isogenous curve, given by Vélu, is

$$E'/\mathbf{Q} : y^2+xy+y = x^3-x^2-213x-1257. \tag{1}$$

Its 7-division polynomial has irreducible factor $x^3+15x^2-94x-\frac{7237}{7}$. The polynomial

$$\begin{aligned}\psi_{G'}(x) &= \left(x^3+15x^2-94x-\frac{7237}{7}\right)^2\\ &= x^6+30x^5+37x^4\\ &\quad -\frac{34214}{7}x^3-\frac{155258}{7}x^2+\frac{1360556}{7}x+\frac{52374169}{49}\end{aligned}$$

has roots the abscissas of the nontrivial points of an order 7 subgroup G' of E'. Its coefficients provide the new S_i, the elementary symmetric polynomials in these six abscissas. Now that we deal with non rational points, to compute the generalized Vélu's parameters we make use of the formula in terms of power sums.

In the following table we provide the values of S_i, $S^{(i)}$ and w_i which we need to compute the equation of the isogeny $\mathcal{I}_{G'}$.

i	S_i	$S^{(i)}$	w_i
0	1	6	1248
1	−30	−30	−304278/7
2	37	826	4100837/7
3	34214/7	−63048/7	−128722659/7
4	−155258/7	1272118/7	14574593267/49
5	−1360556/7	−19030520/7	−328941344849/49
6	52374169/49	2378979868/49	
7		−5571494602/7	

The isogenous curve, obtained from w_0 and w_1, is

$$E''/\mathbf{Q} : y^2 + xy + y = x^3 - x^2 - 6453x + 306765$$

and the abscissa of $\mathcal{I}_{G'}(x, y)$, computed with the formula in the remark above, is

$$\frac{49x^7+1470x^6+62965x^5-534884x^4-34016703x^3-408060457x^2-2288440567x-6221341698}{49x^6+1470x^5+1813x^4-239498x^3-1086806x^2+9523892x+52374169}.$$

The isomorphism $\sigma = (u, r, s, t) = (7, -12, 3, 177)$ (see [**3**]) transforms E'' into the original elliptic curve E and $\sigma \circ \mathcal{I}_{G'}$ is the dual isogeny $\hat{\mathcal{I}}_G$.

Acknowledgement. We are grateful to the referee for her/his helpful comments to the manuscript.

References

[1] J. E. Cremona, Elliptic Curve Data, Available at `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

[2] J. González, On the division polynomials of elliptic curves, Contributions to the algorithmic study of problems of arithmetic moduli, (Spanish), *Rev. R. Acad. Cienc. Exactas Fís. Nat. (Esp.)* **94(3)** (2000), 377–381.

[3] J. H. Silverman, *"The arithmetic of elliptic curves"*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[4] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), A238–A241.

Josep M. Miret and Ramiro Moreno:
Departament de Matemàtica
Universitat de Lleida
25001 Lleida
Spain
E-mail address: miret@matematica.udl.es
E-mail address: ramiro@matematica.udl.es

Anna Rio:
Departament de Matemàtica Aplicada II
Universitat Politècnica de Catalunya
08034 Barcelona
Spain
E-mail address: ana.rio@upc.edu