

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 $\mathcal{I}_G: E \rightarrow E'$ 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.

2000 *Mathematics Subject Classification*. 11G05.

Key words. Elliptic curve, isogeny, rational subgroup.