Rev.R.Acad.Cienc.Exact.Fis.Nat. (Esp)
Vol. 94, N.º 3, pp 377-381, 2000
Monográfico: Contribuciones al estudio algorítmico de problemas de moduli aritméticos

ON THE DIVISION POLYNOMIALS OF ELLIPTIC CURVES[1]

(elliptic curve/isogeny/division polynomial)

J. GONZÁLEZ

Escola Universitària Politècnica de Vilanova i la Geltrú. Departament de Matemàtica Aplicada i Telemàtica. Av. Víctor Balaguer, s/n, 0880 Vilanova i la Geltrú, Spain. E-mail: josepg@mat.upc.es

RESUMEN

Mostramos un procedimiento para calcular los coeficientes de los polinomios de división de una curva elíptica, y calculamos sus seis coeficientes de grado mayor.

ABSTRACT

We show a procedure for computing the coefficients of the division polynomials of an elliptic curve, and compute their six coefficients of greatest degree.

INTRODUCTION

In this paper, our goal is to give a method for computing the coefficients of the division polynomials of an elliptic curve. In the first section, we summarize some known results on isogenies between elliptic curves defined over fields of characteristic 0. Also, to each finite and non-trivial subgroup C of an elliptic curve E we attach a polynomial:

$$\psi_C(x) = x^{d-1} - s_1 x^{d-2} + \text{lower order terms},$$

where $d = |C|$, and study the relationship between this polynomial and the formulas given by Vélu **[Ve 71]**. In the second section, we provide a procedure for computing the coefficients of the division polynomials and compute the six coefficients of greatest degree.

1. ISOGENIES BETWEEN ELLIPTIC CURVES

Let K be an algebraically closed field of characteristic 0. In the sequel, an elliptic curve means an elliptic curve given by an equation of the form $Y^2 = X^3 + AX + B$ with $A, B \in K$. After fixing an elliptic curve E, we use the following notation:

- O is the origin of E.
- $(x(Q), y(Q))$ denote the affine coordinates of the point $Q \in E(K)\backslash\{O\}$.
- ω_E is the regular differential dX/Y.

Let E and E' be elliptic curves. Every isogeny $\mu : E \to E'$ determines an element $\gamma_\mu \in K$, individualized by the condition:

$$\mu^* (\omega_{E'}) = \gamma_\mu \omega_E .$$

It is clear that $\gamma_\mu = 0$ if and only if μ is the constant isogeny. If μ is non-constant, then it is given by an expression of the form:

$$\mu(x, y) = \left(f_\mu(x), \frac{1}{\gamma_\mu} y \frac{d f_\mu(x)}{d x} \right), \quad \text{with } f_\mu(x) \in K(x).$$

The assignment $\mu \mapsto \gamma_\mu$, from the set of all isogenies between elliptic curves in the field K, satisfies the following properties:

(1) *Composition.* If $\mu : E \to E'$ and $\nu : E' \to E''$ are isogenies, then $\gamma_{\nu \circ \mu} = \gamma_\nu \cdot \gamma_\mu$.

(2) *Addition.* If $\mu, \mu' : E \to E'$ are isogenies, then $\gamma_{\mu+\mu'} = \gamma_\mu + \gamma_{\mu'}$. Properties 1 and 2 are a consequence of the fact that the action of the isogenies on the regular differentials satisfies:

$$(\nu \circ \mu)^* = \mu^* \circ \nu^*, \quad (\mu + \mu')^* = \mu^* + \mu'^*.$$

(3) *Product by integers.* If $[m]$ denotes the multiplication by the integer m on E, then $\gamma_{[m]} = m$.

(4) *$\mathbb{Q}$-algebra of endomorphisms.* The map $\mathbb{Q} \otimes \text{End}(E) \to K$, $a \otimes \nu \mapsto a\gamma_\nu$ is a $\mathbb{Q}$-embedding of $\mathbb{Q} \otimes \text{End}(E)$ into K. This property is a conse-

[1] This research has been partially supported by DGES, PB96-0970-C02-02.

quence of the preceding properties and the fact that $v = 0$ if and only if $\gamma_v = 0$.

(5) *Twists.* Given $\delta \in K^*$ and an elliptic curve $E : Y^2 = X^3 + AX + B$, we denote by E_δ the elliptic curve which has the equation $Y^2 = X^3 + A\delta^4 X + B\delta^6$ and by μ_δ the isomorphism of E into E_δ given by $(x, y) \mapsto (x\delta^2, y\delta^3)$. Then, $\gamma_{\mu_\delta} = 1/\delta$.

Normalized Isogenies

We say that an isogeny μ is *normalized* if $\gamma_\mu = 1$. The set of normalized isogenies is stable under the action of the group Gal(K/$\mathbb{Q}$). The following proposition, although elementary, shows the significance of these isogenies.

Proposition 1.1. *Let $\mu_1, \mu_2 : E \to E'$ be normalized isogenies. Then $\mu_1 = \mu_2$.*

Proof. Let $\hat{\mu}_1$ be the dual isogeny of μ_1. We have that $\nu_1 := \mu_1 \circ \hat{\mu}_1$, $\nu_2 := \mu_2 \circ \hat{\mu}_1$ are endomorphisms of E' such that $\gamma_{\nu_1} = \gamma_{\nu_2}$. Then $\nu_1 = \nu_2$ and, thus, $\mu_1 = \mu_2$. □

Note that to every isogeny $\mu : E \to E'$ there corresponds a normalized isogeny μ': E $\to$ E'', where $E'' = E'_{\gamma_\mu}$ and $\mu' = \mu_{\gamma_\mu} \circ \mu$. This normalization $\mu' : E \to E''$ is determined by the conditions:

$$\ker \mu = \ker \mu', \quad \gamma_{\mu'} = 1.$$

With a finite and non-trivial subgroup C of $E(K)$ fixed, we denote by $\mu_C : E \to E_C$ the normalized isogeny such that its kernel is C. If E and E_C are given by the equations

$$E : Y^2 = X^3 + AX + B \quad , \quad E_C : Y^2 = X^3 + A_C X + B_C,$$

then the expressions for μ_C, A_C and B_C have been computed by Vélu **[Ve 71]**. The isogeny μ_C is given by:

$$\begin{cases} \mu_C(x, y) = \left(f_C(x), y \dfrac{\mathrm{d} f_C(x)}{\mathrm{d} x} \right), \\ f_C(x) = x + \sum_{Q \in C\setminus\{O\}} \left(\dfrac{t(Q)}{x - x(Q)} + \dfrac{u(Q)}{(x - x(Q))^2} \right), \end{cases} \tag{1.1}$$

where $t(Q) = 3x(Q)^2 + A$ and $u(Q) = 2(x(Q)^3 + Ax(Q) + B)$. The values that we give for $t(Q)$ and $u(Q)$ are different from the values given in **[Ve 71]**. The reason for this disagreement is that, here, we take summatories extended over the set $Q \in C\setminus\{O\}$ instead of the set $(C\setminus\{O\})/\sim$, where $\sim$ denotes the equivalence relation $Q \sim Q'$ if and only if $Q = \pm Q'$.

The coefficients of E_C are obtained by:

$$\begin{cases} A_C = A - 5t, & \text{with } t = \sum_{Q \in C\setminus\{O\}} t(Q), \\ B_C = B - 7w, & \text{with } w = \sum_{Q \in C\setminus\{O\}} (u(Q) + x(Q)t(Q)). \end{cases} \tag{1.2}$$

We note that the normalized model $\mu_C : E \to E_C$ is compatible with the action of the group Gal $(K/\mathbb{Q})$. That is, for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have that

$$^\sigma(E_C) = (^\sigma E)_{^\sigma C}, \quad ^\sigma(\mu_C) = \mu_{(^\sigma C)}.$$

Polynomial attached to a finite subgroup

As before, let C be a finite and non-trivial subgroup of $E(K)$. We consider the polynomial:

$$\psi_C(X) := \prod_{Q \in C\setminus\{O\}} (X - x(Q)) \in K[X].$$

Let d = $|C|$. Put

$$\psi_C(X) = X^{d-1} + \sum_{i \geq 1} (-1)^i s_i X^{d-1-i},$$

where $s_i = 0$ for $i > d - 1$.

Every root of $\psi_C(X)$ is double or simple. The polynomial $\psi_C(X)$ has simple roots if and only if $C\setminus\{O\}$ contains a 2-torsion point and, in this case, the simple roots are the values $x(Q)$ with $Q \in C \cap E[2]\setminus\{O\}$. We note that if E is defined over a subfield L of K, then

$^\tau C = C$ for all $\tau \in \mathrm{Gal}(K/L)$ if and only if $\psi_C(X) \in L[X]$.

When this happens, that is, if E and C are L-defined, then E_C and μ_C are L-defined.

Proposition 1.2. *The values s_1, s_2, s_3 and the integer $d = |C|$ determine the subgroup C.*

Proof. Indeed, applying to (1.2) the relations:

$$\sum_{Q \in C\setminus\{O\}} x(Q) = s_1, \qquad \sum_{Q \in C\setminus\{O\}} x(Q)^2 = s_1^2 - 2s_2,$$

$$\sum_{Q \in C\setminus\{O\}} x(Q)^3 = s_1^3 - 3s_1 s_2 + 3s_3,$$

we obtain that

$$\begin{cases} A_C = -15s_1^2 + 30s_2 + (6 - 5d)A, \\ B_C = -35s_1^3 + 105s_1 s_2 - 105s_3 - 21As_1 + (15 - 14d)B. \end{cases} \tag{1.3}$$

The curves E and E_C determine a unique normalized isogeny $\mu_C : E \to E_C$ and, thus, its kernel C. □

In fact, by Proposition 1.1 the values t and w determine C, but the statement of Proposition 1.2 is more suitable for our purpose. Next, we will show the procedure for determining f_C and C from the values d, s_1, s_2 and s_3. To simplify certain expressions, we sometimes write t and w instead of their values in the variables s_1, s_2, s_3 and d.

a) Computation of $f_C(X)$ from $d, s_1, \ldots, s_{d-1}$. The formula (1.1) for $f_C(x)$, shows that $f_C(x) = x + P_C(x)/\psi_C(x)$ with $P_C(x) \in K[x]$ and $\deg P_C < \deg \psi_C$. The coefficients of $P_C(x)$ can be computed without the mentioned formula, using the fact that $f_C(x)$ is a solution of the differential equation:

$$f_C^3(x) + A_C f_C(x) + B_C = f_C'(x)^2(x^3 + Ax + B) \qquad (1.4)$$

For instance, we obtain that

$$P_C(x) = tx^{d-2} + (w - ts_1)x^{d-3} + (s_2 t - s_1 w + t(t-A)/3)x^{d-4} + \frac{(-6B + 11As_1 - 33s_3 + 9w - 11s_1 t)t + (-15A + 33s_2)w}{33} x^{d-5} + \cdots \qquad (1.5)$$

Observe that if $x + P_C(x)/\psi_C(x)$ is a solution of (1.4) then $x + x^n P_C(x)/(x^n \psi_C(x))$ is a solution too. Thus, taking into account that $s_i = 0$ for $i > d - 1$, the expression (1.4) is true although $d - 5 < 0$.

b) Computation of $\{s_i\}_{i>3}$ from d, s_1, s_2, s_3. We proceed as follows. We put

$$g_C(x) := \frac{1}{x}\left(f_C(1/x) - 1/x\right) =$$

$$= \sum_{Q \in C\setminus\{O\}} \frac{t(Q)}{1 - x x(Q)} + \sum_{Q \in C\setminus\{O\}} \frac{x u(Q)}{(1 - x x(Q))^2}.$$

We obtain the following relation:

$$\frac{\mathrm{d}^i g_C}{\mathrm{d}x^i}(0) = i! \sum_{Q \in C\setminus\{O\}} x(Q)^{i-1}\left(t(Q)x(Q) + iu(Q)\right) =$$

$$= i!(3 + 2i) \sum_{Q \in C\setminus\{O\}} x(Q)^{i+2} + i!A(1 + 2i) \sum_{Q \in C\setminus\{O\}} x(Q)^i +$$

$$+ 2i!Bi \sum_{Q \in C\setminus\{O\}} x(Q)^{i-1}. \qquad (1.6)$$

Changing x by $1/x$ in (1.3) and replacing $f_C(1/x)$ and $f_C'(1/x)$ by the relations

$$f_C(1/x) = x g_C(x) + 1/x, \quad f_C'(1/x) = 1 - x^2\left(g_C(x) + x g_C'(x)\right),$$

we obtain that $g_C(x)$ is a solution of the differential equation $R(x, y, y') = 0$, where

$$R(x, y, y') = -x^4(1 + Ax^2 + Bx^3)y'^2 +$$
$$+ 2x(1 - yx^2)(1 + Ax^2 + Bx^3)y' + x^4y^3 +$$
$$+ x^2(2 - Ax^2 + Bx^3)y^2 + (5 + 2Ax^2 + A_C x^2 + 2Bx^3)y +$$
$$+ A_C - A + x(B_C - B). \qquad (1.7)$$

For each i-th derivative, we have a differential equation

$$R^{i)}(x, y, y', \ldots, y^{i+1)}) = 0.$$

When $i > 1$, the replacement of the value $x = 0$ in these equations and the values (1.6) yield s_i as a polynomial in $A, B, d, s_1, \ldots, s_{i-1}$. For $i < 2$, the value $x = 0$ and (1.6) yield the formulas of Vélu for the coefficients of E_C:

$$i = 0: \quad g_C(0) = (A - A_C)/5, \quad \text{and } g_C(0) = t.$$
$$i = 1: \quad g_C'(0) = (B - B_C)/7, \quad \text{and } g_C'(0) = w.$$

For $i = 2, 3$ we have the following equalities:

$$i = 2: \quad g_C''(0) = -2g_C(0)\left(2A + A_C + 2g_C(0)\right)/9.$$
$$i = 3: \quad g_C'''(0) = \left(-6g_C'(0)(A_C + 4A + 2g_C(0)) - 12Bg_C(0)\right)/11.$$

Introducing (1.6) in these, we obtain

$$s_4 = \frac{(-2 + 3d - d^2)A^2 + (48A + 12Ad + 6s_2)s_2}{84} + \frac{(2B + 14s_3 - 8s_1s_2 + 4As_1 - Ads_1 + 2s_1^3)s_1}{14}, \qquad (1.8)$$

$$s_5 = \frac{2AB(3 - 4d + d^2) + 12Bs_2(5 - d) + As_3(-117 + 15d) + 75s_2s_3}{165} + s_1P \qquad (1.9)$$

where $P \in \mathbb{Q}[A, B, d, s_1, s_2, s_3, s_4]$.

This procedure yields $g_C^{i)}(0)$ as a polynomial in the variables A, B, t and w with rational coefficients. When the function $g_C(x)$ is known, the relation

$$f_C(x) = x + \frac{g_C(1/x)}{x}$$

provides the function $f_C(x)$.

2. ON DIVISION POLYNOMIALS

Let E be an elliptic curve given by the equation $Y^2 = X^3 + AX + B$. By the theorem of Riemann-Roch, every function on E which has a single pole at O is a polynomial in the functions X and Y, and can be written as a polynomial of the set $K[X] \oplus YK[X]$ in only one way. As in **[Si 86]**, for each integer $m > 0$ the polynomials $\psi_m \in \mathbb{Z}[A, B, X] \oplus Y\mathbb{Z}[A, B, X]$ denote the m-division polynomials for E. These polynomials are viewed as functions on E and satisfy

$$\operatorname{div} \psi_m = \sum_{Q \in E[m]\setminus\{O\}} (Q) - (m^2 - 1)(O).$$

Thus, $\psi_m \in \mathbb{Z}[A, B, X]$ if m is odd and $\psi_m \in Y\mathbb{Z}[A, B, X]$ if m is even. The polynomials ψ_m are determined by the values

$$\psi_m = \begin{cases} 1 & \text{if } m=1, \\ 2Y & \text{if } m=2, \\ 3X^4+6AX^2+12BX-A^2 & \text{if } m=3, \\ 4Y(X^6+5AX^4+20BX^3-5A^2X^2-4ABX-8B^2-A^3 & \text{if } m=4, \end{cases}$$

and by the recursive relations

$$\begin{cases} \psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 & \text{if } m \geq 2, \\ 2Y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) & \text{if } m \geq 3. \end{cases}$$

The polynomials $\psi_m(X, Y)$ can be written as follows:

$$\psi_m(X, Y)/m = \begin{cases} \sum_{i\geq 0}(-1)^i S_{i,m} X^{\frac{m^2-1}{2}-i} & \text{if } m \text{ is odd}, \\ Y\left(\sum_{i\geq 0}(-1)^i S_{i,m} X^{\frac{m^2}{2}-2-i}\right. & \text{if } m \text{ is even}, \end{cases}$$

where $mS_{i,m} \in \mathbb{Z}$ for all $i \geq 0$.

Proposition 2.1. *For all $m \geq 1$ we have $S_{0,m} = 1$. The polynomial $\psi_m^2(X)/m^2$ coincides with the polynomial $\psi_{E[m]}(X)$ attached to the subgroup $E[m]$.*

Proof. We will prove that $S_{0,m} = 1$ by induction on m. The assertion is true for $m \leq 4$. Let us assume that $m > 4$ and $S_{0,k} = 1$ for all $k < m$. Using the recursive relations, we obtain

$$mS_{0,m} = \begin{cases} k\big((k+2)(k-1)^2-(k-2)(k+2)^2\big)/2 = 2k = m & \text{if } m=2k, \\ (k+2)k^3-(k-1)(k+1)^3 = 2k+1 = m & \text{if } m=2k+1. \end{cases}$$

Therefore, $S_{0,m} = 1$ for all m. We recall that the squares of the division polynomials satisfy:

$$\psi_m^2 \in \mathbb{Z}[A, B, X], \quad \deg \psi_m^2 = m^2 - 1.$$

Since the polynomials $\psi_m^2(X)/m^2$ and $\psi_{E[m]}(X)$ are monic and have the same divisor viewed as functions on E, they are equal. □

We put:

$$\psi_m^2(X)/m^2 = \psi_{E[m]}(X) := X^{m^2-1} + \sum_{i>0} (-1)^i s_{i,m} X^{m^2-1-i}.$$

In this case, $s_{i,m} = 0$ for $i > m^2 - 1$. The following proposition provides the values $\{s_{i,m}\}_m$ for $1 \leq i \leq 5$ and shows the procedure for computing $s_{i,m}$ for a fixed i.

Proposition 2.2. *For all $m \geq 1$, we have*

$$s_{i,m} = \begin{cases} 0 & \text{if } i = 1, \\ \frac{(m-1)(m+1)(m^2+6)}{30}A & \text{if } i = 2, \\ -\frac{(m-1)(m+1)(m^4+m^2+15)}{105}B & \text{if } i = 3, \\ \frac{(m-1)(m+1)(m-2)(m+2)(m^4+75m^2+294)}{12\,600}A^2 & \text{if } i = 4, \\ -\frac{(m-1)(m+1)(m-2)(m+2)(m^6+16m^4+54m^2+261)}{6930}AB & \text{if } i = 5. \end{cases}$$

Proof. First, we prove that $S_{1,m} = 0$. We consider the polynomials in X

$$f_m = \begin{cases} \psi_m & \text{if } m \text{ is odd}, \\ \psi_m/Y & \text{if } m \text{ is even}. \end{cases}$$

Let S be a set of polynomials in one variable (with coefficients in any field) having the property that the sum of all its roots is 0. We have that:

i) If $f, g \in S$ then $fg \in S$.

ii) If $f, g \in S$ and $\deg f - \deg g \neq \pm 1$, then $f \pm g \in S$.

In our case, the polynomials $f_m(X)$, $1 \leq m \leq 4$, and $X^3 + AX + B$ satisfy this property. For $m > 4$, it is easy to check that the recursive formulas provide polynomials $f_m(X)$ with this property. Thus, $S_{1,m} = 0$ and $s_{1,m} = 0$. When K is a subfield of $\mathbb{C}$, we can give the following alternative proof. Since the condition $s_{1,m} = 0$ is invariant by twists, we can consider that the elliptic curve E is given by the equation $Y^2 = 4X^3 - AX - B$. By the uniformization theorem for elliptic curves, we can choose τ in the upper half-plane such that $g_2(\tau) = A$ and $g_3(\tau) = B$. Here, g_2 and g_3 denote the usual modular functions of weight 4 and 6 for the group $\Gamma(1) = \mathbf{SL}_2(\mathbb{Z})$. Now, we consider the function

$$h(\tau) = \sum_{\substack{0 \leq i,j \leq m-1, \\ i+j \neq 0}} \wp\left(\frac{i\tau + j}{m}; \tau\right),$$

where $\wp(z; \tau)$ denotes the Weierstrass $\wp$-function for the lattice $\langle 1, \tau \rangle$. It is easy to check that the function h is a modular function of weight 2 for the group $\Gamma(1)$. Since the unique modular function of weight 2 for $\Gamma(1)$ is the constant function zero, it follows that $h = 0$ and $s_{1,m} = 0$.

Now, we consider $C = E[m]$. In this case, $d = |C| = m^2$ and the coefficients of the elliptic curve E_C are $A_C = Am^4$, $B_C = Bm^6$. Applying (1.3) we obtain

$$Am^4 = 30s_{2,m} + (6 - 5\,m^2)A,$$

$$Bm^6 = -105s_{3,m} + (15 - 14m^2)B.$$

Therefore, $s_{2,m} = (m^4 + 5m^2 - 6)A/30$

and

$$s_{3,m} = -(m^6 + 14m^2 - 15)B/105.$$

For $i = 4$ (resp. $i = 5$), the statement is obtained from (1.8) (resp. (1.9)), replacing s_1, s_2, s_3 and d by 0, $s_{2,m}$, $s_{3,m}$ and m^2 respectively. □

Note that in the two preceding propositions we have proved that $S_{0,m} = 1$ and $S_{1,m} = 0$. The computation of $S_{i,m}$, $2 \leq i \leq 5$, can be obtained from the relations

$$s_{2,m} = 2S_{2,m} + \varepsilon_m A, \quad s_{3,m} = 2S_{3,m} - \varepsilon_m B,$$

$$s_{4,m} = 2S_{4,m} + S_{2,m}^2 + 2\varepsilon_m A S_{2,m},$$

$$s_{5,m} = 2S_{5,m} + 2S_{2,m}S_{3,m} + \varepsilon_m(AS_{3,m} - BS_{2,m}),$$

where $\varepsilon_m = (1 + (-1)^m)/2$.

The proposition 2.2 provides a method for computing $s_{k,m}$ for a fixed k. Indeed, it suffices to compute an analogue relation to 1.9. This relation can be obtained computing $R^{i)}(x, y, \ldots, y^{i+1)})$ for $i \leq k - 2$ and using (1.6). Finally, the previous values $s_{1,m}, \ldots, s_{k-1,m}$ provide $s_{k,m}$.

We also observe that from the recursive formulas of the division polynomials, we can deduce that

$$s_{k,m} = \sum_{2r+3j=k} a_{k,r}(m)A^r B^j, \quad \text{with} \quad m^2 a_{k,r}(m) \in \mathbb{Z}.$$

The differential equation (1.7) and the procedure presented here show that $a_{k,r}(m) = P_{k,r}(m^2)$, where $P_{k,r}(x) \in \in \mathbb{Q}[x]$ and $P_{k,r}(i^2) = 0$ for all integers $i \neq 0$ such that $i^2 < k + 1$.

REFERENCES

1. **[Si 86]** Silverman, J. H. (1986), *The Arithmetic of Elliptic Curves,* GTM **106**, Springer-Verlag.
2. **[Ve 71]** Vélu, J. (1971), Isogénies entre courbes elliptiques, *C.R. Acad. Sc. Paris,* 238-241.