Factorisation patterns of division polynomials

By Hugues VERDURE

Institutt for matematikk og statistikk, Universitetet i Tromsø
9037 Tromsø, Norway

(Communicated by Heisuke HIRONAKA, M. J. A., May 12, 2004)

Abstract: The choice of an elliptic curve for the implementation of an elliptic curve cryptosystem requires counting the number of points on such a curve over a finite field. An improvement of Schoof's algorithm for counting the number of rational points on an elliptic curve defined over a finite field takes advantage of some factor of the division polynomials. In this paper, we study the possible factorisations of such division polynomials.

Key words: Elliptic curve; division poynomial; factorisation.

1. Introduction and notation. An improvement of Schoof's algorithm for counting the number of rational points on an elliptic curve defined over a finite field, namely the SEA algorithm (see [1]) takes advantage of some factor of the division polynomials. In this paper, we study the possible factorisations of such division polynomials.

We refer to [2] for a complete overview on the theory of elliptic curves. Let $p > 3$ be a prime number and q a power of p. Let $\mathbf{F}_q$ be the finite field with q elements. We consider an elliptic curve E defined over $\mathbf{F}_q$ by the Weierstrass equation

$$E : y^2 = x^3 + ax + b.$$

If $\mathbf{K}$ is a field extension of $\mathbf{F}_q$, the group of $\mathbf{K}$-rational points of E is denoted by $E(\mathbf{K})$, and the point at infinity $\mathcal{O}$ acts as the neutral element. If n is any positive integer, we denote by $E(\mathbf{K})[n]$ (or simply $E[n]$ if $\mathbf{K}$ is the algebraic closure $\overline{\mathbf{F}_q}$ of $\mathbf{F}_q$) the n-torsion subgroup of $E(\mathbf{K})$. It is known that if n is relatively prime to p, then $E[n] \approx (\mathbf{Z}/n\mathbf{Z})^2$. In this case, we denote by

$$e_n : E[n] \times E[n] \longrightarrow \mu_n$$

the Weil pairing which is a bilinear, antisymmetric, Galois-invariant, non-degenerate map, where μ_n is the set of n-th roots of unity in $\overline{\mathbf{F}_q}$.

Finally, if a and b are integers, then $a \vee b$ denotes the least common multiple of a and b.

1.1. Division polynomials. Define

$$\psi_1 = 1, \qquad \psi_2 = 2y,$$
$$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$
$$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),$$
$$\psi_{2i+1} = \psi_{i+2}\psi_i^3 - \psi_{i-1}\psi_{i+1}^3, \ i > 1,$$
$$2y\psi_{2i} = \psi_i(\psi_{i+2}\psi_{i-1}^2 - \psi_{i-2}\psi_{i+1}^2), \ i > 2.$$

The ψ_i's are polynomials in two variables over $\mathbf{F}_q$, and working modulo the curve equation, ψ_{2i+1} and $(\psi_{2i}/2y)$ are polynomials of one variable of degrees $2i(i+1)$ and $2(i-1)(i+1)$ respectively. These polynomials have the following property:

$$\forall P = (x, y) \in E(\overline{\mathbf{F}_q}) \backslash \{\mathcal{O}\},$$
$$P \in E[n] \Leftrightarrow \psi_n(x, y) = 0.$$

1.2. Frobenius. Define

$$\begin{array}{rccc} \varphi : & E(\overline{\mathbf{F}_q}) & \longrightarrow & E(\overline{\mathbf{F}_q}) \\ & (x, y) & \longmapsto & (x^q, y^q) \\ & \mathcal{O} & \longmapsto & \mathcal{O} \end{array}.$$

This is the Frobenius endomorphism, and it characterizes the $\mathbf{F}_{q^n}$-rational points:

$$\forall P \in E(\overline{\mathbf{F}_q}), \ P \in E(\mathbf{F}_{q^n}) \Leftrightarrow \varphi^n(P) = P.$$

1.3. Twists. Let D be a non-square in $\mathbf{F}_q$. Define

$$\widetilde{E}^D : y^2 = x^3 + D^2ax + D^3b.$$

This is an elliptic curve defined over $\mathbf{F}_q$, which is isomorphic to E over $\mathbf{F}_{q^2}$. If $\delta \in \mathbf{F}_{q^2}$ is such that $\delta^2 = D$, then an isomorphism is given by

$$\begin{array}{rccc} \phi_\delta : & E(\overline{\mathbf{F}_q}) & \longrightarrow & \widetilde{E}^D(\overline{\mathbf{F}_q}) \\ & (x, y) & \longmapsto & (Dx, \delta^3 y) \\ & \mathcal{O} & \longmapsto & \mathcal{O} \end{array}.$$

Twists have the property that

$$\#E(\mathbf{F}_q) + \#\widetilde{E}^D(\mathbf{F}_q) = 2q + 2$$

2000 Mathematics Subject Classification. 14H52, 11T71.

and

$$\#E(\mathbf{F}_q) \cdot \#\widetilde{E}^D(\mathbf{F}_q) = \#E(\mathbf{F}_{q^2}).$$

2. Patterns of l-th division polynomials. We want to find all the possible factorisation patterns of division polynomials of elliptic curves defined over a finite field. In this section, we see which factorisations can occur. We begin with some useful notation: Given a polynomial P defined over a field $\mathbf{K}$, unique factorisation yields P as a product of a constant $k \in \mathbf{K}$ and monic irreducible polynomials which are unique up to order. Let us suppose that we have arranged these polynomials so that

$$P = k \prod_{i=1}^{d} \prod_{j=1}^{n_i} P_{i,j}$$

where $k \in \mathbf{K}$, the $P_{i,j}$ are monic irreducible polynomials, and $\alpha_1, \ldots, \alpha_d$ are positive integers with the following property: for each integer i between 1 and d, the polynomials $P_{i,1}, \ldots, P_{i,n_i}$ are all of degree α_i. Then we will say that P has factorisation pattern (or just pattern for short)

$$\left((\alpha_1, n_1), \ldots, (\alpha_d, n_d)\right).$$

Note that the degrees α_i need not be distinct. If they are, and indeed arrange them in ascending order $\alpha_1 < \cdots < \alpha_d$, then with these extra conditions imposed, the pattern will be unique. However, it will be convenient for us in the sequel not to make such assumptions.

Example 1. Over $\mathbf{R}$, the polynomial

$$P(X) = X^5 + 2X^4 + X^3 - X^2 - 2X - 1$$

factors as

$$P(X) = (X+1)(X+1)(X-1)(X^2+X+1).$$

Thus $P(X)$ has pattern $\left((1,1),(1,1),(1,1),(2,1)\right)$ or, equivalently $\left((1,3),(2,1)\right)$.

The study of division polynomials is related to the study of torsion subgroups, and finding the factorisation pattern is almost equivalent to finding the degrees of the extensions over which a torsion point is defined. Thus, studying the action of the Frobenius on torsion subgroups will give the desired answer. We will distinguish between two major cases: either all the l-torsion points generate the same extension, or they generate different extensions. In the first case, the Frobenius endomorphism is difficult to describe, but the factorisation is quite straightforward, while in the second case, the Frobenius is easy to make explicit.

2.1. The l-torsion generate the same extension. When all the l-torsion points generate the same extension of $\mathbf{F}_q$, then all the irreducible factors of $\psi_l(x)$ have the same degree, namely the degree of this extension, or half of it.

Proposition 1. *Let E be an elliptic curve defined over $\mathbf{F}_q$, and let $l \neq p$ be an odd prime. Let α be the degree of the minimal extension over which a l-torsion point on E is defined. Let $\beta = \alpha$ if α is odd, and $\beta = \alpha/2$ if α is even. Assume finally that $E[l] \subset E(\mathbf{F}_{q^\alpha})$. Then the factorisation pattern of $\psi_l(x)$ is*

$$\left(\left(\beta, \frac{l^2-1}{2\beta}\right)\right).$$

Proof. Let $I(x)$ be an irreducible factor of $\psi_l(x)$, and d its degree. Let $x_0 \in \mathbf{F}_{q^d}$ be a root of I. Let y_0 be a root of $y^2 - x_0^3 - ax_0 - b$. Then the point $P = (x_0, y_0)$ is a point of l-torsion, and is defined over either $\mathbf{F}_{q^d}$ or $\mathbf{F}_{q^{2d}}$, thus $\alpha = 2d$ or $\alpha = d$.

If α is odd, then we must have $d = \alpha$. Assume then that $\alpha = 2\beta$ is even. Let $D \in \mathbf{F}_{q^\beta}$ be a quadratic non-residue, and consider the elliptic curve $\widetilde{E}^D$. We have

(1)
$$\#E(\mathbf{F}_{q^\beta})\#\widetilde{E}^D(\mathbf{F}_{q^\beta}) = \#E(\mathbf{F}_{q^\alpha}) = \#\widetilde{E}^D(\mathbf{F}_{q^\alpha}).$$

Since all the l-torsion points of E are in $E(\mathbf{F}_{q^\alpha})$, then all the l-torsion points of $\widetilde{E}^D$ are in $\widetilde{E}^D(\mathbf{F}_{q^\alpha})$ by isomorphism. But by hypothesis, $l \not| \#E(\mathbf{F}_{q^\beta})$, so that in fact, all the l-torsion points of $\widetilde{E}^D$ are in $\widetilde{E}^D(\mathbf{F}_{q^\beta})$ using (1) modulo l. This means that

$$Dx_0 \in \mathbf{F}_{q^\beta} \Rightarrow x_0 \in \mathbf{F}_{q^\beta},$$

so that $d \leqslant \beta$. With what we have seen before, $d = \beta$.

Thus, all the irreducible factors of $\psi_l(x)$ have the same degree, namely β. Now, since the degree of $\psi_l(x)$ is $(l^2-1)/2$, we get the desired result. □

Example 2. Let E be the elliptic curve defined over $\mathbf{F}_{29}$ by

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

For $l = 11$, we get that $\alpha = 40$, and the pattern of $\psi_{11}(x)$ is $\left((20,3)\right)$.

2.2. The l-torsion points generate different extensions. In this case, we see that the

Frobenius has an eigenvector, and then using the Weil pairing, we can define some invariants that will give us the factorisation of the l-th division polynomial.

Lemma 1. *Let E be an elliptic curve defined over $\mathbf{F}_q$. Let α be the degree of the minimal extension over which a l-torsion point is defined. Assume that $E[l] \not\subset E(\mathbf{F}_{q^\alpha})$. Then there exists $\rho \in \mathbf{F}_l^*$ of order α and a basis (P, Q) of $E[l]$ over $\mathbf{F}_l$ in which the n-th power of the Frobenius endomorphism can be expressed as*:

$$\begin{bmatrix} \rho^n & 0 \\ 0 & \left(\frac{q}{\rho}\right)^n \end{bmatrix} \quad \text{if } \rho^2 \neq q,$$

$$\begin{bmatrix} \rho^n & n\rho^{n-1} \\ 0 & \rho^n \end{bmatrix} \quad \text{otherwise.}$$

The number ρ is uniquely defined by the above properties.

Proof. Let $P \in E(\mathbf{F}_{q^\alpha})[l]$ be non-zero. If $\varphi(P)$ was not a multiplum of P, then together with P, it will be a basis of $E[l]$, which will contradict the assertion $E[l] \not\subset E(\mathbf{F}_{q^\alpha})$. Thus, there exists $\rho \in \mathbf{F}_l^*$ such that $\varphi(P) = \rho P$. Since P is defined over $\mathbf{F}_{q^\alpha}$, we must have that the order of ρ is α.

Let then Q be another l-torsion point such that (P, Q) is a basis of $E[l]$. Write $\varphi(Q) = \lambda Q + \mu P$. Let $\zeta = e_l(P, Q)$. It is a primitive l-th root of unity since (P, Q) is a basis. Then

$$\begin{aligned} \zeta^q &= e_l(P, Q)^\varphi = e_l(\varphi(P), \varphi(Q)) \\ &= e_l(\rho P, \lambda Q + \mu P) = e_l(P, Q)^{\rho\lambda} = \zeta^{\rho\lambda}. \end{aligned}$$

Since ζ is primitive, we must have $\lambda\rho = q$ in $\mathbf{F}_l$, and thus

$$\varphi Q = \frac{q}{\rho} Q + \mu P.$$

Now, if $(q/\rho) \neq \rho$, then Q can be chosen such that $\mu = 0$, while otherwise $\mu \neq 0$. But then, changing P to μP, we still have

$$\varphi(P) = \rho P$$

and

$$\varphi(Q) = \frac{q}{\rho} Q + P = \rho Q + P.$$

A recursion then gives the first part.

The fact that ρ is unique comes from the fact that it is the eigenvalue corresponding to points defined over $\mathbf{F}_{q^\alpha}$, and those are multiples of P. □

Proposition 2. *Let E be an elliptic curve defined over $\mathbf{F}_q$. Let α be the degree of the minimal extension over which E has a non-zero l-torsion point. Assume that $E[l] \not\subset E(\mathbf{F}_{q^\alpha})$. Let $\rho \in \mathbf{F}_l^*$ be as defined in Lemma 1. Let β be the order of (q/ρ) in $\mathbf{F}_l^*$. Then the pattern of $\psi_l(x)$ is*:

$$\left(\left(\alpha, \tfrac{l-1}{2\alpha}\right), \left(\beta, \tfrac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \tfrac{(l-1)^2}{2(\alpha\vee\beta)}\right)\right)$$
if α and β are odd, and $q \neq \rho^2$,

$$\left(\left(\alpha, \tfrac{l-1}{2\alpha}\right), \left(\tfrac{\beta}{2}, \tfrac{l-1}{\beta}\right), \left(\alpha \vee \beta, \tfrac{(l-1)^2}{2(\alpha\vee\beta)}\right)\right)$$
if α is odd, β is even and $q \neq \rho^2$,

$$\left(\left(\tfrac{\alpha}{2}, \tfrac{l-1}{\alpha}\right), \left(\beta, \tfrac{l-1}{2\beta}\right), \left(\alpha \vee \beta, \tfrac{(l-1)^2}{2(\alpha\vee\beta)}\right)\right)$$
if α is even, β is odd and $q \neq \rho^2$,

$$\left(\left(\tfrac{\alpha}{2}, \tfrac{l-1}{\alpha}\right), \left(\tfrac{\beta}{2}, \tfrac{l-1}{\beta}\right), \left(\tfrac{\alpha\vee\beta}{2}, \tfrac{(l-1)^2}{\alpha\vee\beta}\right)\right)$$
if α and β are even and $q \neq \rho^2$,

$$\left(\left(\alpha, \tfrac{l-1}{2\alpha}\right), \left(\alpha l, \tfrac{l-1}{2\alpha}\right)\right) \quad \text{if } \alpha \text{ is odd and } q = \rho^2,$$

$$\left(\left(\tfrac{\alpha}{2}, \tfrac{l-1}{\alpha}\right), \left(\tfrac{\alpha l}{2}, \tfrac{l-1}{\alpha}\right)\right) \quad \text{if } \alpha \text{ is even and } q = \rho^2.$$

Proof. We use the following property: if I is an irreducible factor of $\psi_l(x)$ of degree d, and P a point of l-torsion corresponding to one of its roots, then d is the minimal positive integer n such that $\varphi^n(P) = \pm P$. This comes from the fact that the Frobenius on the points is defined componentwise by the Frobenius on the field, and that two points have the same x-coordinate if and only if they are equal or opposite. Let (P, Q) be a basis as described in Lemma 1. We now distinguish between the two cases $q \neq \rho^2$ and $q = \rho^2$.

In the first case, if R is a l-torsion point which is a non-zero multiplum of P, we have $\varphi^n(R) = \pm R$ with n minimal if and only if $n = \alpha$ or $n = \alpha/2$ depending on the parity of α. If R is a l-torsion point which is a non-zero multiplum of Q, then we have $\varphi^n(R) = \pm R$ with n positive minimal if and only if $n = \beta$ or $n = \beta/2$ depending on the parity of β. Finally, if R is any non-zero l-torsion point not of the two previous forms, then $\varphi^n(R) = \pm R$ with n minimal if and only if $n = \alpha \vee \beta$ or $n = (\alpha \vee \beta)/2$ in the case when both α and β are even. We then count the number of points of each type, namely $l-1$, $l-1$ and $(l-1)^2$, to find the number of factors of each type.

In the second case, a point which is a non-zero

multiplum of P leads to factors of degree α and $\alpha/2$ as before. If R is not a multiplum of P, then in order to have $\varphi^n(R) = \pm R$, we have to have that $\rho^n = \pm 1$ and $n\rho^{n-1} = 0$. Then, depending on the parity of α, we have that $n = \alpha \vee l$ or $n = (\alpha/2) \vee l$. Finally since $\alpha \mid l - 1$, it is relatively prime to l, and these two values are respectively αl and $\alpha l/2$. We find the number of different factors as before. □

Example 3. Consider the elliptic curve

$$E : y^2 = x^3 + x + 5$$

defined over $\mathbf{F}_{17}$ and take $l = 7$. Then $\alpha = 2$, $\rho = 6$ and $\beta = 3$. The pattern of $\psi_7(x)$ is

$$((1,3),(3,1),(6,3)).$$

Example 4. Consider the elliptic curve

$$E : y^2 = x^3 + 3x + 20$$

defined over $\mathbf{F}_{29}$ and take $l = 7$. Then $\alpha = 2$ and $\rho = 6$. The pattern of $\psi_7(x)$ is

$$((1,3),(7,3)).$$

References

[1] Elkies, N. D.: Elliptic and modular curves over finite fields and related computational issues. Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, pp. 21–76 (1998).

[2] Silverman, J. H.: The Arithmetic of Elliptic Curves. Grad. Texts in Math., 106, Springer-Verlag, New York (1986).