Division Polynomials of Elliptic Curves Over Finite Fields

By J. CHEON and S. HAHN

Department of Mathematics, Korea Advanced Institute of Science and Technology, Republic of Korea

(Communicated by Shokichi IYANAGA, M. J. A., Dec. 12, 1996)

Abstract: We consider an ellipic curve E over the finite field $\boldsymbol{F}_p$ for a prime $p \neq 2,3$. We get the complete description of the p^k-th division polynomials for any positive integer k when E is supersingular. Also, we get a property of the division polynomials when E is ordinary.

Key words: Elliptic curves; supersingular; division polynomials.

Let p be a prime number $\neq 2, 3$ and $q = p^k$ for some positive integer k. Consider an elliptic curve E over the finite field $\boldsymbol{F}_p$ given by a Weierstrass equation:

$$y^2 = x^3 + Ax + B\,; \quad A, B \in \boldsymbol{F}_p.$$

For any $M = (x, y) \in E(\boldsymbol{F}_p)$ and an integer m, the point mM is given by

$$mM = \left(\frac{\phi_m(M)}{\psi_m(M)^2}, \frac{\omega_m(M)}{\psi_m(M)^3}\right),$$

where $\phi_m(M)$ and $\psi_m(M)^2$ are relatively prime polynomials in $\boldsymbol{F}_p[x]$ [3]. Moreover, we have the formula [1]:

$$\begin{aligned} \psi_{mn}(M) &= \psi_m(M)^{n^2}\psi_n(mM) \\ \phi_{mn}(M) &= \psi_m(M)^{2n^2}\phi_n(mM) \qquad (1) \\ \omega_{mn}(M) &= \psi_m(M)^{3n^2}\omega_n(mM) \end{aligned}$$

for any positive integers m, n.

We say that E is supersingular over $\boldsymbol{F}_p$ if E has no nontrivial p-torsion point in the algebraic closure $\bar{\boldsymbol{F}}_p$ of $\boldsymbol{F}_p$. In this case, $\psi_p(M)$ is a non-zero constant because $\psi_p(M)$ has no solution in $\bar{\boldsymbol{F}}_p$. Otherwise, we say that E is ordinary over $\boldsymbol{F}_p$. From now on, every polynomial is considered as an element of $\bar{\boldsymbol{F}}_p[x]$.

Lemma 1. *Suppose that E is supersingular over $\boldsymbol{F}_p$. Let $M = (x, y) \in E(\bar{\boldsymbol{F}}_p)$. Then*

$$\omega_p(M) = y^{p^2}.$$

Proof. From Eq. (1) and the definition of $\omega_p(M)$, it follows that

$$\psi_{2p}(M) = \psi_2(M)^{p^2}\psi_p(2M),$$
$$\psi_{2p}(M) = 2\psi_p(M)\omega_p(M).$$

Note that $\psi_p(M) = \psi_p(2M)$ because $\psi_2(M)$ is a constant. Since $\psi_2(M) = 2y$, we get

$$\omega_p(M) = \frac{1}{2}\,\psi_2(M)^{p^2} = y^{p^2}. \qquad \square$$

Theorem 1. *Suppose that E is supersingular over $\boldsymbol{F}_p$. Let $M = (x, y) \in E(\bar{\boldsymbol{F}}_p)$. Then*

$$\psi_p(M) = -1,\ \omega_p(M) = y^{p^2},\ \phi_p(M) = x^{p^2}.$$

Proof. Since E is supersingular over $\boldsymbol{F}_p$, $|E(\boldsymbol{F}_p)| = p + 1$, i.e. $M_0 \in E(\boldsymbol{F}_p)$ implies $pM_0 = -M_0$. Let $M_0 = (x_0, y_0)$ be a nontrivial element of $E(\boldsymbol{F}_p)$. Then

$$\left(\frac{\phi_p(M_0)}{\psi_p(M_0)^2}, \frac{\omega_p(M_0)}{\psi_p(M_0)^3}\right) = -M_0 = (x_0, -y_0). \qquad (2)$$

Since $\omega_p(M) = y^{p^2}$, we see $\psi_p(M_0)^3 = -1$. But $\psi_p(M)$ is a constant, so that $\psi_p(M)^3 = -1$.

Since $mM = \left(\frac{\phi_m(M)}{\psi_m(M)^2}, \frac{\omega_m(M)}{\psi_m(M)^3}\right)$ is a point of E, we get

$$\left(\frac{\phi_p(M)}{\psi_p(M)^2}\right)^3 + A\frac{\phi_p(M)}{\psi_p(M)^2} + B = \left(\frac{\omega_p(M)}{\psi_p(M)^3}\right)^2,$$

or

$$\phi_p(M)^3 - A\psi_p(M)\phi_p(M) + B - y^{2p^2} = 0.$$

Using $y^2 = x^3 + Ax + B$, it can be factored as follows:

$$(\phi_p(M) - \psi_p(M)^2x^{p^2})(\phi_p(M)^2 + \psi_p(M)^2x^{p^2}\phi_p(M) - \psi_p(M)x^{2p^2} - A\psi_p(M)) = 0. \qquad (3)$$

If $A \neq 0$, the second factor of Eq. (3) is irreducible in $\bar{\boldsymbol{F}}_p[x]$ since its discriminant equals to $\psi_p(M)(3x^{2p^2} + 4A)$, which is not a square in $\bar{\boldsymbol{F}}_p[x]$. If $A = 0$, Eq. (3) is factored as follows:

$$(\phi_p(M) - \psi_p(M)^2x^{p^2})(\phi_p(M) - \alpha x^{p^2})\cdot(\phi_p(M) - \beta x^{p^2}) = 0,$$

if we let α, β be two roots of the equation $t^2 + \psi_p(M)^2t - \psi_p(M) = 0$. In both the cases, $\phi_p(M) = x^{p^2}$ because the leading coefficient of $\phi_p(M)$

1991 Mathematics Subject Classification. 11G20, 14H52.

is 1. Hence we see $\psi_p(M_0)^2 = 1$ from Eq. (2), which implies $\psi_p(M) = -1$ since $\psi_p(M)^3 = -1$. □

Corollary. *Suppose that E is supersingular over $\boldsymbol{F}_p$. Let $M = (x, y) \in E(\bar{\boldsymbol{F}}_p)$. Then*

$$\psi_q(M) = (-1)^k,\ \omega_q(M) = y^{q^2},\ \phi_q(M) = x^{q^2}.$$

Proof. Consider the following equalities: For any positive integer a,

$$\begin{aligned}
\psi_{p^{a+1}}(M) &= \psi_{p^a}(M)^{p^2}\psi_p(p^aM) \\
&= \psi_{p^a}(M)^{p^2}(-1) = -\psi_{p^a}(M)^{p^2} \\
\omega_{p^{a+1}}(M) &= \psi_{p^a}(M)^{3p^2}\omega_p(p^aM) \\
&= \psi_{p^a}(M)^{3p^2}y[p^aM]^{p^2} = \omega_{p^a}(M)^{p^2} \\
\phi_{p^{a+1}}(M) &= \psi_{p^a}(M)^{2p^2}\phi_p(p^aM) \\
&= \psi_{p^a}(M)^{2p^2}x[p^aM]^{p^2} = \phi_{p^a}(M)^{p2}.
\end{aligned}$$

Using these and induction on a, we get the corollary. □

Lemma 2. *Suppose that $q \mid n$. Let $M = (x, y) \in E(\bar{\boldsymbol{F}}_p)$. Then $\phi_n(M)$, $\psi_n(M)$ and $y^q\omega_n(M)$ are polynomials of x^q.*

Proof. Consider the k-th power Frobenius-map

$$\phi_k : E \to E\ ;\ (x, y) \mapsto (x^q, y^q).$$

Since deg $\phi_k = q$, the multiplication-by-q map $[q] : E \to E$ factors through $[q] = \hat{\phi}_k \circ \phi_k$, so that $[n] = [n/q] \circ \hat{\phi}_k \circ \phi_k$. Hence $\dfrac{\phi_n(M)}{\psi_n(M)^2}$ and $\dfrac{\omega_n(M)}{\psi_n(M)^3}$ are rational functions of x^q and y^q. Since $\phi_n(M)$ and $\psi_n(M)^2$ are relatively prime polynomials of x, $\phi_n(M)$, $\psi_n(M)^2$ and so $\psi_n(M)$ are polynomials of x^q. Since $y^q\omega_n(M)$ is a polynomial of x, it is also a polynomial of x^q. □

Theorem 2. *Suppose that E is ordinary over $\boldsymbol{F}_p$. Let $M = (x, y) \in E(\bar{\boldsymbol{F}}_p)$. Then $\psi_q(M) = g(x)^q$ for some seperable polynomial $g(x) \in \boldsymbol{F}_p[x]$ of degree $\dfrac{q-1}{2}$.*

Proof. By Lemma 2, we know $\psi_q(M) = q(x)^q$ for some polynomial $g(x) \in \boldsymbol{F}_p[x]$. Since $E[q] = \boldsymbol{Z}/q\boldsymbol{Z}$, $\psi_q(M)$ has at least $\dfrac{q-1}{2}$ distinct roots. Since $\deg \psi_q(M) < \dfrac{q^2-1}{2}$, $\dfrac{q(q-1)}{2} \leq q \deg g(x) < \dfrac{q^2-1}{2}$. Therefore $\deg g(x) = \dfrac{q-1}{2}$. We are done. □

References

[1] M. Ayad: Points S-entiers des elliptiques. Manuscrtipta Math., **76**, 305–324 (1992).

[2] D. Husemöller: Elliptic Curves. Springer-Verlag, New York (1987).

[3] J. H. Silvermann: The Arithmetic of Elliptic Curves. Springer-Verlag, New York (1986).