D. Division polynomials

Let us fix a field K of characteristic $p \neq 2, 3$, and let $a, b \in K$ be such that $4a^2 + 27b^2 \neq 0$. Use E to denote the smooth Weierstraß curve given by $y^2 = x^3 + ax + b$. Recall that $E[m]$ denotes the group of all $P \in E$ such that $[m]P = \infty$. This group is a subgroup of $E(\bar{K})$.

If $p \nmid m$, then $|E[m]| = m^2$, by Theorem G.1. There are thus $m^2 - 1$ affine points $P = (\alpha, \beta)$ for which $[m]P = \infty$.

Note that $(\alpha, \beta) \in E[m] \Leftrightarrow (\alpha, -\beta) \in E[m]$. This is because $(\alpha, -\beta) = \ominus P$. Hence, if m is odd and $p \nmid m$, then there are exactly $(m^2 - 1)/2$ different values of α that occur within the affine points $(\alpha, \beta) \in E$ that are of order that divides m.

If m is even, then we have to be a bit more cautious since in this case $E[m]$ contains involutions. There are three of them, and they are equal to $(\zeta_i, 0)$, where $x^3 + ax + b = \prod(x - \zeta_i)$, $1 \leq i \leq 3$. Hence in this case, provided $p \nmid m$, the number of α is exactly $((m^2 - 1) - 3)/2 + 3 = (m^2 + 2)/2$.

It is thus not surprising that there exist polynomials $\tilde{\psi}_m \in K[x]$ of respective orders $(m^2 - 1)/2$ and $(m^2 + 2)/2$ such that $(\alpha, \beta) \in E[m] \Leftrightarrow \tilde{\psi}_m(\alpha) = 0$.

Of course, if $m_1 \mid m_2$, then $E[m_1] \leq E[m_2]$ and $\tilde{\psi}_{m_1}$ divides $\tilde{\psi}_{m_2}$.

Therefore $\tilde{\psi}_2$ divides $\tilde{\psi}_m$ if m is even. A point $(\alpha, \beta) \in E$ is an involution if and only if $\alpha^3 + a\alpha + b = 0$. Hence $\tilde{\psi}_2 = x^3 + ax + b$.

Another criterion for (α, β) being an involution is that $\beta = 0$. This criterion is more easy to check. Because of that (and because of compatibility with the theory of Weierstraß equations in characteristics 2 and 3) it is usual to use polynomials ψ_m that are in defined in variables x and y, and not polynomials $\tilde{\psi}_m \in K[x]$ that are defined only in x. The difference is small. In our case of $y^2 = x^3 + ax + b$, $\mathrm{char}(K) \neq 2, 3$, the polynomial ψ_2 is defined as $2y$. Furthermore, $\psi_m = \tilde{\psi}_m$ if m is odd and $\psi_m = 2y\tilde{\psi}_m/(x^3 + ax + b)$ if m is even.

What is extremely important is the fact that the *division polynomials* ψ_m may be defined recursively, e.g. in the following way:

$$
\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \text{ where } m \geq 2, \text{ and}\\
\psi_{2m} &= (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m/2y, \text{ where } m \geq 3.
\end{aligned}
\tag{D.1}
$$

However, the definition of ψ_{2m+1} and ψ_{2m} as given above is <u>not</u> correct without a further adjustment. The formula upon the right always yields a polynomial in x and y. In this polynomial there may be occurences of y^i with $i \geq 2$. If this happens then y^i is replaced by $y^{i-2}(x^3 + ax + b)$ until the polynomial contains y in power at most 1. The final polynomial is equal to some $a(x)$ in the case of $2m + 1$, and to $ya(x)$ in the case of $2m$.

Every $P = (\alpha, \beta) \in E$ satisfies

$$[m]P = \infty \iff \psi_m(\alpha, \beta) = 0. \tag{D.2}$$

This is true for all $m \geq 1$, even for those with $p \mid m$. In addition to that the division polynomials can be used to express $[m]P$ for those $P = (\alpha, \beta) \in E$ that do not belong to $E[m]$. If $P \notin E[m]$, $m \geq 2$ and $P \notin E[2]$, then

$$[m]P = \left(\alpha - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \ \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4\beta\psi_m^3} \right). \tag{D.3}$$

The above formula is written compactly, for the sake of clarity. For example the numerator in the former fraction should be read as $\psi_{m-1}(\alpha,\beta)\psi_{m+1}(\alpha,\beta)$.

None of (D.1) and (D.3) is easy to prove. Below we shall verify (D.1) for $m \in \{3,4,5\}$, and (D.3) for $m = 2$.

Instead of polynomials $\tilde{\psi}_m$ it is usual to work with polynomials $\bar{f}_m \in K[x]$. The meaning is nearly the same. The difference is that polynomials $\bar{f}_m$ ignore the involutions. They are defined so that if $P = (\alpha, \beta) \in E$, then

$$P \in E[m] \setminus E[2] \iff \bar{f}_m(\alpha) = 0. \tag{D.4}$$

The connection between $\bar{f}_m$ and ψ_m is such that

$$\bar{f}_m = \begin{cases} \psi_m & \text{if } m \text{ is odd, and} \\ \psi_m/2y & \text{if } m \text{ is even.} \end{cases} \tag{D.5}$$

Thus $\bar{f}_0 = 0$, $\bar{f}_1 = 1$, $\bar{f}_2 = 1$, $\bar{f}_3 = 3x^4 + 6ax^2 + 12bx - a^2$ and $\bar{f}_4 = 2(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$.

For $m \geq 5$ the polynomials $\bar{f}_m$ may be defined recursively. While the formula is straightforwardly derived from (D.1), it looks slightly more complicated. This is because only the variable x is involved.

$$\begin{aligned} \bar{f}_{2m+1} &= \begin{cases} \bar{f}_{m+2}\bar{f}_m^3 - 16(x^3+ax+b)^2\bar{f}_{m-1}\bar{f}_{m+1}^3 & \text{if } m \geq 3 \text{ is odd,} \\ 16(x^3+ax+b)^2\bar{f}_{m+2}\bar{f}_m^3 - \bar{f}_{m-1}\bar{f}_{m+1}^3 & \text{if } m \geq 2 \text{ is even, and} \end{cases} \\ \bar{f}_{2m} &= \bar{f}_m(\bar{f}_{m+2}\bar{f}_{m-1}^2 - \bar{f}_{m-2}\bar{f}_{m+1}^2) \quad \text{for any } m \geq 3. \end{aligned} \tag{D.6}$$

As may be guessed from the formulas above, division polynomials contain many nonzero coefficients of large values. Hence for large q it is not possible to represent them in computer memory if m is very big. Because of that the division polynomials cannot be used, say, to directly verify the order of $E(\mathbb{F}_q)$. Nevertheless this order can be determined by considering the behaviour of polynomials $\bar{f}_m$ where m runs through a set of not too large primes. This is how Schoof's algorithm works.

Note that polynomials $\bar{f}_m$ are not monic. In fact the leading coefficient of $\bar{f}_m$ is equal to m when m is odd, and to $m/2$ when m is even. This is important since when $m = p$ is the characteristic of the field, then $\deg(\bar{f}_m) < (m^2-1)/2$.

D.1. **The division polynomial for order 3.** Let $P = (\alpha, \beta)$ be a point upon E, $\beta \neq 0$. The tangent of E at P can be expressed by the equation $y = \lambda x + \mu$ in which $\lambda = (3\alpha^2 + a)/2\beta$ and $\mu = \beta - \lambda\alpha$. The chord and tangent process, as described in Section A, considers the intersections of the tangent and the curve E.

The first coordinate of such an intersection is a solution to the equation

$$(\lambda x + \mu)^2 = x^3 + ax + b. \tag{D.7}$$

From the logic of the chord and tangent process it follows that α is always a double root of the polynomial

$$x^3 + ax + b - (\lambda x + \mu)^2 = x^3 - \lambda^2 x^2 + (a - 2\lambda\mu)x + b - \mu^2. \tag{D.8}$$

This may also be seen immediately if we write (D.7) in the form

$$(\lambda x + \mu - \beta)^2 = x^3 + ax + b - 2\beta(\lambda x + \mu) + \beta^2$$

and observe that α is a root not only of the polynomials on both sides of this equation, but also of their derivatives.

The point P is of order 3 if and only if the tangent intersects E in no other point of E. This happens if and only if α is the triple root of the polynomial in (D.8). We already know that the multiplicity of α is at least two. The multiplicity is hence equal to three if and only if $\lambda^2 = 3\alpha$. Substituting $\alpha^3 + a\alpha + b$ for β^2 in the denominator of λ^2 turns the equation $\lambda^2 = 3\alpha$ into

$$\begin{aligned} (3\alpha^2 + a)^2 &= 12\alpha(\alpha^3 + a\alpha + b), \\ 9\alpha^4 + 6a\alpha^2 + a^2 &= 12\alpha^4 + 12a\alpha^2 + 12b\alpha \text{ and} \\ 3\alpha^4 + 6a\alpha^2 + 12b\alpha - a^2 &= 0. \end{aligned} \tag{D.9}$$

We have verified the formula for $\psi_3 = \bar{f}_3$. A point $(\alpha, \beta) \in E$ is of order 3 if and only if α is a root of $3x^4 + 6ax^2 + 12bx - a^2$.

Note that in this way we obtain all elements of $E[3]$. Only some of them are K-rational. To get a K-rational point of $E[3]$ the root α has to be from K and $\alpha^3 + a\alpha + b$ has to be a square in K.

D.2. **The division polynomial for order 4.** Suppose that $P = (\alpha, \beta) \in E$ is not an involution. This means that $\beta \neq 0$. In such a case $[4]P = \infty$ if and only if $[2]P = (\alpha', \beta')$ is an involution. This takes place if and only if $\beta' = 0$.

By (A.6) and (A.7), $\beta' = \lambda(\alpha - \alpha') - \beta$, $\alpha' = \lambda^2 - 2\alpha$ and $\lambda = (3\alpha^2 + a)/2\beta$. This gives the following expression of $\beta' = \lambda(\alpha - \alpha') - \beta$:

$$\lambda(3\alpha - \lambda^2) - \beta = (2\beta)^{-3}\left((3\alpha^2 + a)(12\alpha\beta^2 - (3\alpha^2 + a)^2) - 8\beta^4\right). \tag{D.10}$$

If $\beta \neq 0$, then $\beta' = 0$ if and only if $(2\beta)^3\beta' = 0$. In order to express $(2\beta)^3\beta'$ in terms of α, observe that

$$\begin{aligned} 12x(x^3 + ax + b) - (3x^2 + a)^2 &= 3x^4 + 6ax^2 + 12bx - a^2, \\ (3x^2 + a)(3x^4 + 6ax^2 + 12bx - a^2) &= 9x^6 + 21ax^4 + 36bx^3 + 3a^2x^2 + 12abx - a^3, \\ \text{and } -8(x^3 + ax + b)^2 &= -8x^6 - 16ax^4 - 16bx^3 - 8a^2x^2 - 16abx - 8b^2. \end{aligned}$$

By summing up the latter two rows we obtain that

$$\begin{aligned} &(3x^2 + a)(12x(x^3 + ax + b) - (3x^2 + a)^2) - 8(x^3 + ax + b)^2 \\ &\qquad = x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2 = \bar{f}_4(x)/2. \end{aligned}$$

This verifies that

$$(3\alpha^2 + a)(12\alpha\beta^2 - (3\alpha^2 + a)^2) - 8\beta^4 = \bar{f}_4(\alpha)/2 \text{ for all } (\alpha, \beta) \in E. \tag{D.11}$$

Hence if $(\alpha, \beta) \in E$ and $\beta \neq 0$, then $(2\beta)^3\beta' = 0$ if and only if $\bar{f}_4(\alpha) = 0$.

D.3. **Doubling.** Assume $m = 2$ and suppose that $P = (\alpha, \beta) \in E$ is not an involution. By (D.1), $\psi_{m-1}(\alpha, \beta) = 1$, $\psi_m^2(\alpha, \beta) = 4\beta^2$ and $\psi_{m+1}(\alpha, \beta) = 3\alpha^4 + 6\alpha^2 + 12b\alpha - a^2$.

By (D.9) the latter is equal to $12\alpha\beta^2 - (3\alpha^2 + a)^2$. Set $\lambda = (3\alpha^2 + a)/2\beta$. We have

$$\alpha - \left(\frac{\psi_1\psi_3}{\psi_2^2}\right)(\alpha, \beta) = \alpha - 12\alpha/4 + \lambda^2 = \lambda^2 - 2\alpha.$$

This verifies that if $m = 2$, then the first coordinate of (D.3) corresponds to the doubling formula (A.6) and (A.7).

By these formulas the second coordinate of $[2]P$ is equal to $\lambda(3\alpha - \lambda^2) - \beta$, and that can be expressed, by (D.10) and (D.11), as $(2\beta)^{-3}\bar{f}_4(\alpha)/2$. This agrees with formula (D.3) since for $m = 2$ the second coordinate at the right hand side of (D.3) is equal to

$$\psi_4(\alpha, \beta)/4\beta\psi_2^3(\alpha, \beta) = 2\beta\bar{f}_4(\alpha)/4\beta(2\beta)^3 = \bar{f}_4(\alpha)/16\beta^3.$$

D.4. **Order and characteristic 5.** As already mentioned, verifying formulas (D.1) and (D.3) in their generality is technically demanding. Here it will not be performed. However, we shall illustrate upon the case of $m = 5$ why ψ_m has much smaller number of roots when $\mathrm{char}(K)$ divides m.

What we shall do first is to use (D.6) to get the general formula for $\bar{f}_5$, and then we shall observe how dramatically $\bar{f}_5$ changes when it is considered in characteristic 5. By (D.6),

$$\bar{f}_5 = 16(x^3 + ax + b)^2 \bar{f}_4 \bar{f}_2^3 - \bar{f}_1 \bar{f}_3^3 = 16(x^3 + ax + b)^2 \bar{f}_4 - \bar{f}_3^3.$$

$$\text{Since } (x^3 + ax + b)^2 = x^6 + 2ax^4 + 2bx^3 + a^2x^2 + 2abx + b^2$$
$$\text{and } \bar{f}_4/2 = x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3$$

we may express $(x^3 + ax + b)^2 \bar{f}_4/2$ as

$$x^{12} + 7ax^{10} + 22bx^9 + 6a^2x^8 + 48abx^7 + (33b^2 - 6a^3)x^6 + 12a^2bx^5 + (21ab^2 - 7a^4)x^4$$
$$+ (4b^3 - 16a^3b)x^3 - (21b^2a^2 + a^5)x^2 - (20ab^3 + 2a^4b)x - 8b^4 - a^3b^2,$$

while $\bar{f}_3^3 = (3x^4 + 6ax^2 + 12bx - a^2)^3$ is equal to

$$27x^{12} + 162ax^{10} + 324bx^9 + 297a^2x^8 + 1296abx^7 + (108a^3 + 1296b^2)x^6 + 1080a^2bx^5$$
$$+ (2592ab^2 - 99a^4)x^4 + (1728b^3 - 432a^3b)x^3 - (432a^2b^2 - 18a^5)x^2 + 36a^4bx - a^6.$$

Therefore $\bar{f}_5 = 16(x^3 + ax + b)^2 \bar{f}_4 - \bar{f}_3^3$ is equal to

$$5x^{12} + 62ax^{10} + 380bx^9 - 105a^2x^8 + 240abx^7 - (240b^2 + 300a^3)x^6$$
$$- 696a^2bx^5 - (1920ab^2 + 125a^4)x^4 - (1600b^3 + 80a^3b)x^3 - (240b^2a^2 + 50a^5)x^2$$
$$- (640ab^3 + 100a^4b)x - (256b^4 + 32a^3b^2 - a^6).$$

Modulo 5 this yields $2ax^{10} - a^2bx^5 - b^4 - 2a^3b^2 + a^6$. Let $r, s, t \in \bar{K}$ be such that $r^5 = 2a$, $s^5 = -a^2b$ and $t^5 = -b^4 - 2a^3b^2 + a^6$. If K is assumed, as usual, to be a perfect field, then $r, s, t \in K$.

We see now that if $\mathrm{char}(K) = 5$, then $\bar{f}_5(x) = (rx^2 + sx + t)^5$. This implies $|E[5]| = 5$, provided $a \neq 0$. If $a = 0$, then $E[5]$ is a trivial group.