version of September 9, 2007

NOTES ON CM DIVISION POLYNOMIALS

MARCO STRENG

Abstract. It was suggested by Chudnovsky and Chudnovsky ([CC86]) to define elliptic divisibility sequences indexed by the endomorphism ring of an elliptic curve using generalized division polynomials. The special cases where the curve has complex multiplication by $\sqrt{-1}$ or a primitive third root of unity had already been studied by Ward ([War50]) and Durst ([Dur52]) respectively. Takakazu Satoh ([Sat04]) has shown that the Chudnovskys' division polynomials have algebraic integers as coefficients. Recently, the author ([Str06], [Str07]) has defined elliptic divisibility sequences using the denominators of multiples of a point and shown that they have primitive divisors. In these notes, we show how CM-indexed division polynomials relate to denominators of multiples of a point.

1. Division Polynomials

Let E be an elliptic curve over a field L of characteristic 0 and denote the point at infinity by O. Let f be an L-isogeny from E to an elliptic curve E'. Consider the divisor

$$D_f = \sum_{P \in \ker(f)} (P - O).$$

This is a divisor of degree $\deg(f) - 1$ since one term is 0. If D_f is principal, then we let ψ_f be a function such that $\operatorname{div}(\psi_f) = D_f$. We normalize ψ_f later in some cases. Notice that $2D_f$ is always principal, since it is the divisor of

$$\prod_{\substack{P \in \ker(f) \\ P \neq O}} (x - x(P)) \quad \in L[x] \subset L(E),$$

where (x, y) are Weierstrass coordinates of E. If f has degree 2, then D_f cannot be principal, since it has only one pole and one zero.

Now suppose that we have chosen Weierstrass models for both E and E'. Then we have a preferred invariant differential on E, given by

$$\omega = \frac{dx}{2y + a_1 x + a_3}.$$

This gives us the constant

$$f^*\omega'/\omega$$

that we will use for the normalization. We define the polynomials ϕ_f and ψ_f^2 by

$$\begin{aligned} \phi_f(x) &= \prod_{\substack{P \in E(\overline{L}) \\ fP = Q}} (x - x(P)) \quad \in L[x] \subset L(E) \quad \text{and} \\ \psi_f^2 &= \left(\frac{f^*\omega'}{\omega}\right)^2 \prod_{\substack{P \in \ker(f) \\ P \neq O}} (x - x(P)) \quad \in L[x] \subset L(E), \end{aligned}$$

Lemma 1.1. *We have the following identity of elliptic functions:*

$$f^*x = \frac{\phi_f}{\psi_f^2}. \tag{1.2}$$

Moreover, there is no cancellation of zeroes on the right hand side.

Proof. It is easily checked that the divisors are the same. Therefore, we have equality up to a multiplicative constant c. Next, we expand both sides of (1.2) as formal Laurent series in a local parameter around the point O. In the notation of [Str07, §2], the left hand side becomes $F_f(T)/w(F_f(T))$, which has $1/(f^*\omega'/\omega)^2$ as its first non-zero coefficient. The first non-zero coefficient of the right hand side is the same, hence $c = 1$. □

2. Endomorphisms

Now suppose $E = E'$, i.e. $f = \alpha \in \mathrm{End}_L(E)$ is an endomorphism. Lemma 1.1 implies in particular that for $\alpha \in \mathbb{Z}$, our definition of the division polynomials ϕ_α and ψ_α coincides with the usual definitions as found for example in [Sil86], [Aya92] and [Was03].

We can also use Lemma 1.1 to compute how the division polynomials behave under composition of endomorphisms:

$$\phi_{\alpha\beta}(x) = \psi_\alpha^{2N(\beta)}(x)\phi_\beta\left(\frac{\phi_\alpha(x)}{\psi_\alpha^2(x)}\right) \in L[x] \quad \text{and} \tag{2.1}$$

$$\psi^2_{\alpha\beta}(x) = \psi_\alpha^{2N(\beta)}(x)\psi^2_\beta\left(\frac{\phi_\alpha(x)}{\psi_\alpha^2(x)}\right) \in L[x]. \tag{2.2}$$

If α is coprime to 2, then we define ψ_α by

$$\psi_\alpha = \alpha \prod_{\substack{P \in E[\alpha]/\pm 1 \\ P \neq O}} (x - x(P)) \quad \in L[x] \subset L(E).$$

If α is divisible by 2, then we set

$$\psi_\alpha = \alpha \ \left(y + \frac{1}{2}(a_1 x + a_3)\right) \prod_{\substack{P \in E[\alpha]/\pm 1 \\ P \notin E[2]}} (x - x(P)) \quad \in L[x, y] \subset L(E).$$

If α is neither divisible by 2, nor coprime to 2, then we leave ψ_α undefined for now. We will define it as a meromorphic function on $\mathbb{C}$ below.

3. The complex case and recurrence

Suppose now on that L is contained in $\mathbb{C}$. There is also a complex analytic definition of the division polynomials ψ_α for arbitrary endomorphisms α. If $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ complex-analytically, then [CC86] gives a meromorphic function ψ_α on $\mathbb{C}$ which is almost Λ-periodic: for all $\alpha \in \mathbb{C}$ and $\lambda \in \Lambda$, we have that $\psi_\alpha(z + \lambda) = \pm\psi_\alpha(z)$, where the sign is -1 if and only if the following three conditions are satisfied:

$$2|N(\alpha), \quad 2 \nmid \alpha \quad \text{and} \quad \frac{\alpha\lambda}{2} \notin \Lambda.$$

In particular, ψ_α^2 is a meromorphic function on $\mathbb{C}/\Lambda$ and if $2|\alpha$ or $2 \nmid N(\alpha)$, then so is ψ_α. Under the isomorphism $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, the function ψ_α^2 corresponds to our division polynomial ψ_α^2 (as can be checked by counting the zeroes) and if $2|\alpha$ or $2 \nmid N(\alpha)$, then the same holds for ψ_α. Moreover, the functions ψ_α of [CC86] satisfy the recurrence relation

$$\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2 \quad m, n \in \mathbb{Z}. \tag{3.1}$$

4. Integers

Suppose that the coefficients of E are in the ring of integers of the number field L.

Lemma 4.1. *The polynomials ϕ_α and ψ_α^2 have coefficients in the ring of integers of L. The same holds for ψ_α if α is coprime to or divisible by 2.*

Proof. If α is coprime to or divisible by 2 and E is in short Weierstrass form $y^2 = x^3 + ax + b$, then [Sat04, Corollary 4.3] says that the coefficients of ψ_α are algebraic integers. We give a proof of the general case below.

We already know that the coefficients are in L, so we only have to show that they are algebraic integers. First, we show this for $\phi_\alpha(x)$.

Extend L such that it contains the roots of ϕ_α and the y-coordinate of a point $Q \in E(\overline{\mathbb{Q}})$ such that $x(Q) = 0$. Let v be any discrete valuation of L. Recall that the set $E_1(L_v)$ of L_v-valued points that are not v-integral is an $\mathcal{O}$-module ([Str07]) and notice that Q is not in that set. Therefore every $P \in \alpha^* Q$ is v-integral, hence so is every zero of ϕ_α, hence every coefficient.

For ψ_α, we will use the power series of [Str07, §2], so let R_v be the ring of v integers of a non-archimedean completion L_v of L. Notice first that $\mathcal{P}^*(1/x) = w(T)/T = T^2 + \cdots$, hence both $p(T) := \mathcal{P}^*(1/x)$ and $\mathcal{P}^*(x)$ are in $R_v((T))$. We know from [Str07] that $F_\alpha(T)$ has coefficients in R_v, hence so does $p(F_\alpha(T)) = \mathcal{P}^*((\alpha^* x)^{-1})$. At the same time, $\mathcal{P}^*(\phi_\alpha(x)) = \phi_\alpha(\mathcal{P}^*(x))$ has integral coefficients and $\alpha^* x = \phi_\alpha \psi_\alpha^{-2}$, hence $\mathcal{P}^*(\psi_\alpha^2) = \mathcal{P}^*(\phi_\alpha(\alpha^* x)^{-1})$ also has integral coefficients.

Write $\psi_\alpha^2(T) = b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$. We prove by induction on k that b_{n-k} is an algebraic integer. So suppose that b_{n-k} is an algebraic integer for all $k < l$. The $-2(n-k)$-th coefficient of $\mathcal{P}^*(\psi_\alpha)$ is $b_{n-l} + \cdots$, where $\cdots$ is a polynomial in b_{n-k} for $k < l$ and the coefficients of $w(T)$, hence b_{n-l} is v-integral.

The final statement follows from the fact that $\mathcal{O}_L[x]$ is integrally closed in $L[x]$. □

Applying Lemma 4.1 to (2.1) and (2.2), we find

Corollary 4.2. *As polynomials with coefficients in $\mathcal{O}_L$, we have $\psi_\alpha^2 | \psi_{\alpha\beta}^2$ and $\phi_{\alpha\beta} \equiv \phi_\alpha^{N(\beta)} (\mathrm{mod}\ \psi_\alpha^2)$.* □

5. Elliptic divisibility sequences

We will now define elliptic divisibility sequences of division polynomial type. For a fixed non-torsion point $P \in E(L)$, let

$$\widehat{\psi}_\alpha^2 = B_1^{2(N(\alpha)-1)} \psi_\alpha^2(P) \quad \text{and} \quad \widehat{\phi}_\alpha = B_1^{2N(\alpha)} \phi_\alpha(P).$$

The L-ideals $\widehat{\psi}_\alpha^2$ and $\widehat{\phi}_\alpha$ are integral since ψ_α^2 is a polynomial in x of degree $N(\alpha)-1$ and ϕ_α is a polynomial of degree $N(\alpha)$. If B_1^2 is principal, then we fix a generator of B_1^2 and view $\widehat{\psi}_\alpha^2$ and $\widehat{\phi}_\alpha$ as elements of $\mathcal{O}_L$.

We call the sequence $(\widehat{\psi}_\alpha^2)_\alpha$ an *elliptic divisibility sequence of division polynomial type*. Notice that Corollary 4.2 implies that such a sequence satisfies the divisibility property $\widehat{\psi}_\alpha^2 | \widehat{\psi}_{\alpha\beta}^2$ $(\alpha, \beta \in \mathcal{O})$. Moreover,

$$\frac{\widehat{\phi}_\alpha}{B_1^2 \widehat{\psi}_\alpha^2} = x(\alpha P)\mathcal{O}_L = A_\alpha B_\alpha^{-2}. \tag{5.1}$$

Since A_α and B_α are coprime by definition, it follows that

$$B_\alpha^2 \mid B_1^2\ \widehat{\psi}_\alpha^2, \tag{5.2}$$

but even more is true:

Proposition 5.3. *The point P reduces to a singular point modulo v if and only if there is an $\alpha \in \mathcal{O}$ such that both*

$$v(\phi_\alpha(P)) > 0 \quad \textit{and} \quad v(\psi_\alpha^2(P)) > 0. \tag{5.4}$$

Proof. [Aya92] proves this statement with $\mathcal{O}$ replaced by $\mathbb{Z}$, so we only have to prove the "if" part. Suppose that (5.4) holds for some $\alpha \in \mathcal{O}$. Then Corollary 4.2 shows that (5.4) also holds with α replaced by $N(\alpha)$. But then Ayad's result shows that P is singular modulo v. □

Corollary 5.5. *If P is non-singular modulo v, then $v(B_\alpha^2) = v(B_1^2\widehat{\psi}_\alpha^2)$ for every α.*

Proof. If $v(B_\alpha^2) \neq v(B_1^2\widehat{\psi}_\alpha^2)$, then by (5.1), we have $v(B_1^2\widehat{\psi}_\alpha^2) > 0$ and $v(\widehat{\phi}_\alpha) > 0$. In the case $v(B_1) > 0$, the valuation of $v(\widehat{\phi}_\alpha) > 0$ is made exactly 0 by the factor $B_1^{2N(\alpha)}$ in $\widehat{\phi}_\alpha$. Therefore, we only have to consider the case $v(B_1) = 0$. But then Proposition 5.3 says that P is singular modulo v. □

This result allows us to transfer results from one kind of sequence to the other. For example, it follows that almost every term in an elliptic divisibility sequence of division polynomial type has a primitive divisor. On the other hand, if 2 does not split in $\mathcal{O}$ and E is non-singular modulo every prime of L, then $B_\alpha = B_1^{N(\alpha)}\psi_\alpha(P)$ for every α, hence the ideal class of B_α is $N(\alpha)$ times the ideal class of B_1. If in addition B_1 is principal and we pick a generator γ, then $B_\alpha = \gamma^{N(\alpha)}\psi_\alpha(P)\mathcal{O}_L$, where $\gamma^{N(\alpha)}\psi_\alpha(P)$ satisfies the recurrence relation (3.1).

References

[Aya92] Mohamed Ayad, *Points S-entiers des courbes elliptiques*, manuscripta mathematica **76** (1992), 305–324.

[CC86] D.V. Chudnovsky and G.V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Advances in Applied Mathematics **7** (1986), 385–434.

[Dur52] L.K. Durst, *The apparition problem for equianharmonic divisibility sequences*, Prod. Natl. Acad. Sci. U.S.A. **38** (1952), 330–333.

[Sat04] Takakazu Satoh, *Generalized division polynomials*, Mathematica Scandinavica **94** (2004), 161–184.

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 1986.

[Str06] Marco Streng, *Elliptic divisibility sequences with complex multiplication*, Master's thesis, http://www.math.leidenuniv.nl/∼streng, 2006.

[Str07] ———, *Divisibility sequences for elliptic curves with complex multiplication*, preprint, http://www.math.leidenuniv.nl/∼streng, 2007.

[War48] Morgan Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **7** (1948), 31–74.

[War50] ———, *Arithmetical properties of the elliptic polynomials associated with the lemniscate elliptic functions*, Proc. Natl. Acad. Sci. U.S.A. **36** (1950), 359–362.

[Was03] Lawrence C. Washington, *Elliptic curves: Number theory and cryptography*, Chapmann & Hall / CRC, 2003.

Universiteit Leiden, P.O. box 9512, 2300 RA Leiden, The Netherlands
E-mail address: streng@math.leidenuniv.nl