Arch. Math. 97 (2011), 251–257

0003-889X/11/030251-7
published online August 30, 2011
DOI 10.1007/s00013-011-0295-5

Archiv der Mathematik

One half log discriminant and division polynomials

Robin de Jong

Abstract. Szpiro and Tucker recently proved that, under mild conditions, the valuation of the minimal discriminant of an elliptic curve with semistable reduction over a discrete valuation ring can be expressed in terms of intersections between n-torsion and 2-torsion, where n tends to infinity. The argument of Szpiro and Tucker is geometric in nature. We give a proof based on the arithmetic of division polynomials, and generalize the result to the case of hyperelliptic curves.

Mathematics Subject Classification (2010). Primary 11G20, Secondary 11B83.

Keywords. Discriminant, Division polynomial, Hyperelliptic curve.

1. Introduction. Let K be a field of characteristic $p \neq 2$ endowed with a non-trivial discrete valuation, and let O be the ring of integers of K. Let E be an elliptic curve over K given by a minimal equation $y^2 = f(x)$ with $f(x) \in O[x]$ a monic cubic separable polynomial. Let $\mathbb{P}^1_O$ be the projective line over O. Let D be the Zariski closure in $\mathbb{P}^1_O$ of the scheme of zeroes of f on $\mathbb{P}^1_K$, and for each positive integer n with $p \nmid n$ let H_n be the Zariski closure in $\mathbb{P}^1_O$ of the pushforward under $x\colon E \to \mathbb{P}^1_K$ of the n-torsion minus the 2-torsion in E.

In [5] Szpiro and Tucker proved the following theorem.

Theorem 1.1. *Assume that E has semistable reduction over K. Let Δ be the discriminant of f. Then the formula:*

$$\lim_{\substack{n\to\infty \\ p\nmid n}} \frac{1}{n^2}(D, H_n)_\nu = \frac{1}{2}\nu(\Delta)$$

holds, where $\nu\colon K^* \to \mathbb{Z}$ is the normalised valuation of K and where $(,)_\nu$ is the geometric intersection pairing on the arithmetic surface $\mathbb{P}^1_O$.

Birkhäuser

As is known, the underlying reduced scheme of H_n can be conveniently described by a *division polynomial* $\psi_n \in O[x]$ (cf. [4, Exercise 3.7]). The polynomial ψ_n has degree $(n^2-1)/2$ if n is odd, degree $(n^2-4)/2$ if n is even, and has leading coefficient n. An alternative way of writing the conclusion of the theorem is therefore that:

$$\frac{1}{n^2}\sum_{\alpha:f(\alpha)=0}\log|\psi_n^2(\alpha)|_\nu \longrightarrow \frac{1}{2}\log|\Delta|_\nu$$

as $n\to\infty$ with $p\nmid n$, where $|\cdot|_\nu\colon K^*\to\mathbb{R}^+$ is any absolute value determined by ν. The proof in [5] of Theorem 1.1 uses the geometry of the special fiber of the minimal regular model of E over O.

Our purpose in this note is to show that Theorem 1.1 can alternatively be derived from a study of the arithmetic of the division polynomials ψ_n alone. As a consequence we will remove the assumption that E should have semistable reduction over K, as well as the assumption that K should be a discretely valued field. In fact, using the division polynomials introduced by Cantor [1], to be explained below, we can even prove a result in the more general context of hyperelliptic curves.

Let g be a positive integer, and let k be a field of characteristic p where $p=0$ or $p\geq 2g+1$. Let $|\cdot|$ be an absolute value on k. Let (X,o) be an elliptic curve or a pointed hyperelliptic curve of genus $g\geq 2$ over K, given by an equation $y^2=f(x)$ with $f(x)\in k[x]$ monic, separable and of degree $2g+1$, putting o at infinity.

Theorem 1.2. *Let $\psi_n\in k[x]$ be the nth (Cantor's) division polynomial of (X,o) and let $\alpha\in k$ be a root of f. Then:*

$$\frac{1}{n^2}\log|\psi_n^2(\alpha)| \longrightarrow \frac{1}{2}\log|f'(\alpha)|$$

as $n\to\infty$. Here, only integers n are taken with $p\nmid(n-g+1)\cdots(n+g-1)$. In particular, under the same conditions we have:

$$\frac{1}{n^2}\sum_{\alpha:f(\alpha)=0}\log|\psi_n^2(\alpha)| \longrightarrow \frac{1}{2}\log|\Delta|$$

as $n\to\infty$ where $\Delta=\prod_{\alpha:f(\alpha)=0}f'(\alpha)$ is the discriminant of f.

The motivation in [5] to study limits of intersection numbers as in Theorem 1.1 is that, when working over a number field K, these limits are natural local non-archimedean heights associated to the scheme D. As D consists only of torsion points, its global height vanishes; this is used in [5] to show that the total archimedean contribution to the height is equal to $\frac{1}{2}\log|N_{K/\mathbb{Q}}(\Delta)|$ where $N_{K/\mathbb{Q}}(\Delta)$ is the norm of Δ in $\mathbb{Z}$. Our Theorem 1.2 provides local heights at each of the archimedean places too, and allows one to verify a posteriori that the global height is zero, by the product formula.

We note that the condition that $p\nmid(n-g+1)\cdots(n+g-1)$ appears to be rather natural from the theory of Weierstrass points in positive characteristic (see [3] for example, esp. Remark 2.8). It generalizes the natural condition $p\nmid n$ from the case of elliptic curves.

2. Cantor's division polynomials. Our main result is a statement about the asymptotic behavior of certain special values of division polynomials associated to hyperelliptic curves. We briefly recall from [1] the construction of these division polynomials and their main properties.

Let again $g \geq 1$ be an integer. Let $a_1, \ldots, a_{2g+1}$ be indeterminates and write R for the commutative ring $\mathbb{Z}[a_1, \ldots, a_{2g+1}]$. Let $F(x)$ be the polynomial $x^{2g+1} + a_1 x^{2g} + \cdots + a_{2g}x + a_{2g+1}$ in $R[x]$, and let $\Delta \in R$ be the discriminant of F. Let y be a variable satisfying $y^2 = F(x)$, and let $E_1(z)$ be the polynomial $E_1(z) = (F(x-z) - y^2)/z$ in $R[x, z]$. Put

$$S(z) = (-1)^{g+1} y \sqrt{1 + zE_1(z)/y^2},$$

where $\sqrt{1 + zE_1(z)/y^2}$ is the power series in $R[x, y^{-1}][[z]]$ obtained by binomial expansion on $1 + zE_1(z)/y^2$. One has:

$$S(z)^2 = F(x-z), \quad \text{and} \quad S(z) = \sum_{j=0}^{\infty} P_j(x)(2y)^{1-2j} z^j$$

for some $P_j(x) \in R[x]$ of degree $2jg$ and with leading coefficient in $\mathbb{Z}$.

Let $n \geq g$ be an integer. Then Cantor's polynomial ψ_n (in genus g) is defined to be the element of $R[x]$ given by:

$$\psi_n = \begin{cases} \begin{vmatrix} P_{g+1} & P_{g+2} & \cdots & P_{(n+g)/2} \\ P_{g+2} & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & P_{n-2} \\ P_{(n+g)/2} & \cdots & P_{n-2} & P_{n-1} \end{vmatrix} & n \equiv g \bmod 2, \\ \begin{vmatrix} P_{g+2} & P_{g+3} & \cdots & P_{(n+g+1)/2} \\ P_{g+3} & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & P_{n-2} \\ P_{(n+g+1)/2} & \cdots & P_{n-2} & P_{n-1} \end{vmatrix} & n \equiv g+1 \bmod 2. \end{cases}$$

For $n = g$ and $n = g+1$ we understand that ψ_n is the unit element. We have:

$$\deg \psi_n = \begin{cases} g(n^2 - g^2)/2 & n \equiv g \bmod 2, \\ g(n^2 - (g+1)^2)/2 & n \equiv g+1 \bmod 2. \end{cases}$$

Next, denote by $b(n)$ the leading coefficient of ψ_n in R. Then $b(n)$ is an integer, and we have:

$$p \nmid (n-g+1) \cdots (n+g-1) \Rightarrow p \nmid b(n)$$

for each prime integer p. Moreover, the $b(n)$ are the values at the integers $n \geq g$ of a certain numerical polynomial $b \in \mathbb{Q}[x]$ which can be written down explicitly.

The geometric meaning of the ψ_n is as follows. Let k be a field of characteristic p where either $p = 0$ or $p \geq 2g+1$. Note that in particular $p \neq 2$. Let $f(x) \in k[x]$ be a monic and separable polynomial of degree $2g+1$, and let (X, o) be the elliptic or pointed hyperelliptic curve of genus g over k given by the equation $y^2 = f(x)$. The point o is meant to be the unique point at infinity of X. Let $J = \mathrm{Pic}^0 X$ be the jacobian of X. It comes equipped with a natural symmetric theta divisor, represented by the classes $[q_1 + \cdots + q_{g-1} - (g-1)o]$ in J where $q_1, \ldots, q_{g-1}$ are points running through X. Also we have a natural Abel-Jacobi embedding $\iota\colon X \to J$ given by sending $p \mapsto [p - o]$. Let $[n]\colon J \to J$ be the multiplication-by-n map on J. For integers n such that $n \geq g$ and $p \nmid (n-g+1)\cdots(n+g-1)$ we then put

$$X_n = \iota^*[n]^*\Theta.$$

This X_n turns out to be an effective divisor on X of degree gn^2. In fact, X_n is the scheme of Weierstrass points of the line bundle $\mathcal{O}_X(o)^{\otimes n+g-1}$ on X; cf. [3] for a further study of such schemes. Note that X_n is a generalization of the scheme of n-torsion points on an elliptic curve. In analogy to what we did in that case in the Introduction, we subtract from each X_n the part coming from the hyperelliptic ramification points. More precisely we put:

$$X_n^* = \begin{cases} X_n - X_g & n \equiv g \bmod 2, \\ X_n - X_{g+1} & n \equiv g+1 \bmod 2. \end{cases}$$

We have:

$$X_g = \frac{g(g-1)}{2} D + go, \quad X_{g+1} = \frac{g(g+1)}{2} D,$$

where D denotes the reduced divisor of degree $2g+2$ on X consisting of the hyperelliptic ramification points of X. It can be shown (in fact we will see a proof below) that these X_n^* are effective k-divisors on X with support disjoint from the hyperelliptic ramification points. Note that:

$$\deg X_n^* = \begin{cases} g(n^2 - g^2) & n \equiv g \bmod 2, \\ g(n^2 - (g+1)^2) & n \equiv g+1 \bmod 2. \end{cases}$$

We have the following theorem.

Theorem 2.1. (*Cantor* [1]) *Let $n \geq g$ be an integer such that p does not divide $(n-g+1)\cdots(n+g-1)$. Specialize the polynomial ψ_n from equation (2.1) to a polynomial in $k[x]$, by sending $a_1, \ldots, a_{2g+1}$ to the coefficients of f. Then X_n^* is equal to the scheme of zeroes of ψ_n on X.*

We note that if (X, o) is an elliptic curve, the polynomials ψ_n with $n \geq 1$ coincide with the "usual" division polynomials from elliptic function theory (cf. [4, Exercise 3.7]).

3. Proof of Theorem 1.2. We just evaluate the determinants at the right hand side of equation (2.1) at α, where α is a root of $F = x^{2g+1} + a_1 x^{2g} + \cdots + a_{2g}x + a_{2g+1}$ in an algebraic closure $\overline{Q(R)}$ of the fraction field $Q(R)$ of R, and then specialize to k. Let $c_m = \frac{1}{2m+1}\binom{2m+1}{m}$ for $m \geq 0$ be the mth Catalan number. We start with:

Lemma 3.1. *The identity:*

$$P_j(\alpha) = (-1)^g \cdot c_{j-1} \cdot F'(\alpha)^j$$

holds in $R[\alpha]$ for all integers $j \geq 1$.

Proof. We recall the relations:

$$S(z) = \sum_{j=0}^{\infty} P_j(x)(2y)^{1-2j} z^j, \quad S(z)^2 = F(x-z).$$

We claim that:

$$\frac{1}{j!}\frac{d^j S(z)}{dz^j} = \frac{R_j(x,z)}{(2S(z))^{2j-1}} \tag{3.1}$$

for some $R_j(x,z) \in Q(R)[x,z]$ with $R_j(\alpha,0) = -c_{j-1} \cdot F'(\alpha)^j$, for all $j \geq 1$. This gives what we want since $S(0) = (-1)^{g+1}y$ hence $P_j(x) = (-1)^{g+1}R_j(x,0)$.

To prove the claim we argue by induction on j. We have $\frac{dS}{dz} = -\frac{F'(x-z)}{2S(z)}$ which settles the case $j=1$ with $R_1(x,z) = -F'(x-z)$. Now assume that (3.1) holds with $R_j(x,z) \in Q(R)[x,z]$, and with $R_j(\alpha,0) = -c_{j-1} \cdot F'(\alpha)^j$ for a certain $j \geq 1$. Then a small calculation yields:

$$\frac{1}{(j+1)!}\frac{d^{j+1}S}{dz^{j+1}} = \frac{1}{j+1}\frac{d}{dz}\frac{R_j(x,z)}{(2S(z))^{2j-1}} = \frac{R_{j+1}(x,z)}{(2S(z))^{2j+1}}$$

with:

$$R_{j+1}(x,z) = \frac{2}{j+1}\left(2\left(\frac{d}{dz}R_j(x,z)\right)F(x-z) + (2j-1)R_j(x,z)F'(x-z)\right).$$

We find $R_{j+1}(x,z) \in Q(R)[x,z]$ and:

$$\begin{aligned} R_{j+1}(\alpha,0) &= \frac{2(2j-1)}{j+1}R_j(\alpha,0) \cdot F'(\alpha) \\ &= -\frac{2(2j-1)}{j+1}c_{j-1} \cdot F'(\alpha)^{j+1} \\ &= -c_j \cdot F'(\alpha)^{j+1} \end{aligned}$$

by the induction hypothesis. This completes the induction step. □

Now evaluating equation (2.1) at α with the help of the Lemma then yields the equality:

$$\psi_n(\alpha) = c(n) \cdot F'(\alpha)^{d(n)} \tag{3.2}$$

for all $n \geq g$ in $R[\alpha]$, where:

$$c(n) = \begin{cases} \begin{vmatrix} c_g & c_{g+1} & \cdots & c_{(n+g)/2-1} \\ c_{g+1} & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & c_{n-3} \\ c_{(n+g)/2-1} & \cdots & c_{n-3} & c_{n-2} \end{vmatrix} & n \equiv g \bmod 2, \\ \begin{vmatrix} c_{g+1} & c_{g+2} & \cdots & c_{(n+g-1)/2} \\ c_{g+2} & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & c_{n-3} \\ c_{(n+g-1)/2} & \cdots & c_{n-3} & c_{n-2} \end{vmatrix} & n \equiv g+1 \bmod 2, \end{cases}$$

at least up to a sign, and where $d(n) \in \mathbb{Z}$ is given by:

$$d(n) = \begin{cases} (n^2 - g^2)/4 & n \equiv g \bmod 2, \\ (n^2 - (g+1)^2)/4 & n \equiv g+1 \bmod 2. \end{cases}$$

We claim that $p \nmid (n-g+1) \cdots (n+g-1) \Rightarrow p \nmid c(n)$ holds for every prime number p and every integer n and that the $c(n)$'s are the values at the integers $n \geq g$ of a numerical polynomial $c \in \mathbb{Q}[x]$. This follows from a general result on Hankel determinants of Catalan numbers due to Desainte-Catherine and Viennot (see [2, Section 6]): for arbitrary integers $l, m \geq 1$ we have the identity

$$\begin{vmatrix} c_l & c_{l+1} & \cdots & c_{l+m-1} \\ c_{l+1} & \iddots & \iddots & \vdots \\ \vdots & \iddots & \iddots & c_{l+2m-3} \\ c_{l+m-1} & \cdots & c_{l+2m-3} & c_{l+2m-2} \end{vmatrix} = \prod_{1 \leq i \leq j \leq l-1} \frac{i+j+2m}{i+j}.$$

In particular $c(n)$ is non-vanishing in k if the characteristic p of k satisfies $p \nmid (n-g+1) \cdots (n+g-1)$. Also $c(n)$ has only polynomial growth in n.

Let us now place ourselves in the situation of Theorem 1.2. In particular we work over a field k of characteristic p with $p = 0$ or $p \geq 2g+1$, and now α is a given root of $f \in k[x]$ in k. Let $n \geq g$ be an integer such that $p \nmid (n-g+1) \cdots (n+g-1)$. From equation (3.2) we obtain by specializing:

$$\psi_n(\alpha) = c(n) \cdot f'(\alpha)^{d(n)} \tag{3.3}$$

in k. Since $f'(\alpha)$ and $c(n)$ are both non-zero in k we deduce that $\psi_n(\alpha)$ is non-zero in k as well. In particular we find that X_n^* has support disjoint from the hyperelliptic ramification points, a claim that we made earlier. Theorem 1.2 follows from equation (3.3) upon taking absolute values and logarithms (which we can do because of the non-vanishing), and letting n tend to infinity, always under the condition that $p \nmid (n-g+1) \cdots (n+g-1)$.

Acknowledgments. The research done for this paper was supported by VENI grant 639.033.402 from the Netherlands Organisation for Scientific Research (NWO). Part of the research was done at the Max Planck Institute in Bonn, whose hospitality is greatly acknowledged.

References

[1] D. Cantor, On the analogue of the division polynomials for hyperelliptic curves, J. Reine Angew. Math. **447** (1994), 91–145.

[2] M. Desainte-Catherine and G. Viennot, Enumeration of certain Young tableaux with bounded height, in: Combinatoire énumérative (Montreal 1985), Lecture Notes in Math. **1234**, Springer-Verlag Berlin, 1986.

[3] A. Neeman, Weierstrass points in characteristic p, Inv. Math. **75** (1984), 359–376.

[4] J. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics **106**, Springer-Verlag 1986.

[5] L. Szpiro and T. Tucker, One half log discriminant, in: Diophantine Geometry, CRM Series **4**, Ed. Norm., Pisa, 2007.

Robin de Jong
Mathematical Institute,
University of Leiden,
PO Box 9512,
2300 RA Leiden,
The Netherlands
e-mail: rdejong@math.leidenuniv.nl

Received: 1 February 2011