ONE HALF LOG DISCRIMINANT

LUCIEN SZPIRO AND THOMAS J. TUCKER

Abstract. We give a geometric proof that one may compute a particular generalized Mahler integral using equidistribution of preperiodic points of a dynamical system on the sphere. The dynamical system is associated to the multiplication by 2 map on an elliptic curve over a number field K with Weierstrass equation $y^2 = P(x)$ (a Lattès dynamical system). At each finite place v, we prove the local equidistribution formula

$$\frac{1}{2}v(\Delta) = \lim_{n\to\infty} \frac{1}{n^2}(D.H_n)_v,$$

where H_n is the Zariski closure in $\mathbb{P}^1_{\mathcal{O}_K}$ of the image in $\mathbb{P}^1_K$ of the n-torsion minus the 2-torsion and Δ is the discriminant of the polynomial $P(x)$. One consequence of this result is the formula

$$\frac{1}{2}\log|\operatorname{Norm}_{K/\mathbb{Q}}(\triangle)| = \sum_{\sigma:K\to\mathbb{C}} \int_{\mathbb{P}^1(\mathbb{C})} \log|P(x)|_\sigma \frac{dx\wedge d\bar{x}}{\Im(\tau)_\sigma |P(x)|^2_\sigma}.$$

In [21], Szpiro, Ullmo, and Zhang proved that for any abelian variety A over $\mathbb{Q}$, any continuous function g on $A(\mathbb{C})$, and any nonrepeating sequence of point $\beta_n \in A(\overline{\mathbb{Q}})$ with Néron-Tate height tending to zero, one has

$$\frac{1}{|\operatorname{Gal}(\beta_n)|}\sum_{\sigma\in\operatorname{Gal}(\beta_n)} g(\sigma(\beta_n)) = \int_{A(\mathbb{C})} g\, d\mu,$$

where $d\mu$ is the normalized Haar measure on A and $\operatorname{Gal}(\beta_n)$ is the Galois group of the Galois closure of $\mathbb{Q}(\beta_n)$ in $\mathbb{C}$. This result says, in effect, that Galois orbits of points with small Néron-Tate height are equidistributed in $A(\mathbb{C})$. Ullmo [22] and Zhang [23] later used this fact to give proofs of the Bogomolov conjecture for abelian varieties.

When the abelian variety A is an elliptic curve, the multiplication by 2 map gives rise to a map on the projective line, called a Lattès map. Thus, in this case, the work of [21] can be viewed as an equidistribution result for a rational map on the projective line. Recently, a variety of authors have proven more general equidistribution results for

The first author was partially supported by NSF Grant 0071921. The second author was partially supported by NSF Grant 0101636.

The authors would like to thank M. Baker and R. Rumely for many helpful discussions.

arbitrary rational maps of degree greater than 1 on the projective line; see Autissier [2], Baker/Rumely [5], Bilu [6], Chambert-Loir [7], and Favre/Rivera-Letelier [12, 11], for example. Many of these results hold for measures at finite places as well as at archimedean places.

In [15], it is shown that for any nonconstant map $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ of degree greater than 1 over a number field K, the canonical height $h_\varphi(\alpha)$ of an algebraic point α with minimal polynomial F can be calculated by integrating $\log |F|$ along the invariant measures for the map φ. This gives a generalization of the notion of a Mahler measure of a polynomial (see [14]). Everest, Ward, and Fhlathuin [10, 9] had previously extended the notion of Mahler measures to elliptic curves.

Additional difficulties arise, however, when one attempts to prove equidistribution results for the functions $\log |F|_v$. Indeed, the exact analog of the main result of [21] is not true when the continuous function g is replaced by a function of the form $\log |F|$ (see [1] or [4]). On the other hand, it is possible to prove an equidistribution result for functions of the form $\log |F|_v$ provided that one averages over all points of period n as n goes to infinity rather than over Galois orbits of families of points of small height (see [19]). In the case of elliptic curves, Baker, Ih, and Rumely [4] were able to refine this to prove that for any algebraic number α and any Lattès map φ one has

$$[K(\alpha) : \mathbb{Q}]\, h_\varphi(\alpha) = \sum_{\text{places } v \text{ of } K} \lim_{n\to\infty} \frac{1}{|\operatorname{Gal}(\beta_n)|} \sum_{\sigma \in \operatorname{Gal}(\beta_n)} \log |F(\beta_n^\sigma)|_v$$

for any nonrepeating sequence of algebraic points β_n such that $h_\varphi(\beta_n) = 0$ for all n. Both [4] and [19] use results from diophantine approximation, specifically Roth's theorem ([16]) and A. Baker's work on linear forms in logarithms ([3]).

When one applies the results of [4] and [15] to the points of period 2 for a Lattès map corresponding to multiplication by 2 on the elliptic curve E with Weierstrass equation $y^2 = P(x)$, one obtains the formula

$$\begin{aligned} \frac{1}{2} \log |\operatorname{Norm}_{K/\mathbb{Q}}(\triangle)| &= \sum_{\sigma : K \hookrightarrow \mathbb{C}} \lim_{n\to\infty} \frac{1}{n^2} \log \prod_{\beta \in \operatorname{Supp} H_n} |P(\beta)|_\sigma \\ &= \sum_{\sigma : K \hookrightarrow \mathbb{C}} \int_{\mathbb{P}^1(\mathbb{C})} \log |P(x)|_\sigma \, \frac{dx \wedge d\bar{x}}{\Im(\tau)_\sigma |P(x)|_\sigma^2}, \end{aligned}$$

where Δ is the discriminant of F over K and τ_σ denotes the element corresponding to the elliptic curve E_σ in the fundamental domain for the action of $\mathrm{SL}(2, \mathbb{Z})$ on the Poincaré upper half space in $\mathbb{C}$. Using the product formula and the fact that $h_\varphi(\alpha) = 0$ for periodic points α, this is equivalent to showing that at each nonarchimedean place v of

K, we have

$$\lim_{n\to\infty}\frac{1}{n^2}\log\prod_{\beta\in\operatorname{Supp}H_n}|P(\beta)|_\sigma = \lim_{n\to\infty}\frac{1}{n^2}\log\mathrm{Norm}_{H_n/\mathcal{O}_K}(P_{|H_n})$$
$$= \lim_{n\to\infty}\frac{1}{n^2}\sum_v (D.H_n)_v\log\mathrm{N}(v),$$

where $N(v)$ is the cardinality of the residue field at v and H_n is the Zariski closure in $\mathbb{P}^1_{\mathcal{O}_K}$ of the image in $\mathbb{P}^1_K$ of the n-torsion minus the 2-torsion

We give here a local proof using blow-ups of closed points and intersection theory on $\mathbb{P}^1_V$. This proof uses resolution of singularities (in fact separation of branches) of one-dimensional schemes by blowing up. It also uses information about the special fiber of an elliptic curve with semistable reduction (see [17]). We do not use diophantine approximation. The proof we give is valid for equicharacteristic V (local geometric case) as well as for unequal characteristic (local arithmetic case). Note that the case of positive characteristic does not follow from the results of [4] and [19], since the relevant approximation theorems are not valid in characteristic p. Relations between the discriminant of an elliptic curve and its n-torsion have been studied in [13] and in [20]. The main theorem of this paper is the following.

Theorem. *Let V be a discrete valuation ring with fraction field K. Let $y^2 = P(x)$ be the minimal Weierstrass equation with coefficients in V of an elliptic curve E. Suppose that E has semi-stable reduction over V, that the roots of $P(x)$ are rational over K, and that the residual characteristic of V is not 2. Let D be the scheme of zeroes of $P(x)$ in $\mathbb{P}^1_V$ and let H_n be the Zariski closure in $\mathbb{P}^1_V$ of the image in $\mathbb{P}^1_K$ of the kernel of the multiplication by n in E_K minus the 2-torsion. Then*

$$\lim_{n\to\infty}\frac{1}{n^2}(D.H_n)_v = \frac{1}{2}v(\triangle),$$

where v is the normalized valuation of V, $\triangle$ is the discriminant of E over V, and $(-.-)_v$ is the geometric intersection pairing on the surface $\mathbb{P}^1_V$.

The conditions on the rationality of the roots of P and on the characteristic of V are not essential for the theorem but they make the proof easier. They imply that the valuation of the discriminant is even; we write $2k = v(\triangle)$. One knows (see for example [17] or [8]) that the closed fiber of the minimal model $\mathcal{E}$ for E over V is a cycle of $2k$ projective lines of self intersection (-2); it is obtained by blowing up the plane model for the elliptic curve k times. Recall that the Néron model in this case is

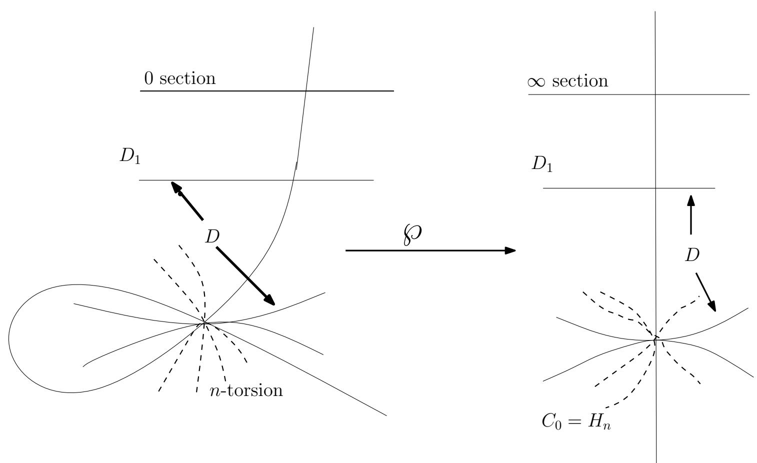
$$\mathcal{E} \setminus \{\text{singular points of the special fiber}\} \text{ (see figure 3).}$$

The strategy of the proof is to compute intersections in the Néron model for E after a suitable base change. The multiplicative structure of the special fiber is simply $\mathbb{G}_m$ crossed with the group of components. One can easily see how the n-torsion distributes itself among the components, and that allows one to calculate intersections without difficulty.

We will use the fact that the Néron model for E has $2k$ components in its special fiber(see [17, page 365]). It is naturally a $2:1$ cover of a model for $\mathbb{P}^1$ with $k+1$ components. The hyperelliptic map induces a map on components that sends a component and its inverse to a single component; there are two components that are their own inverse (the identity and the component of order 2), which gives a total of $2(k-1)/2+2 = k+1$ components on a model of $\mathbb{P}^1$.

We begin with the plane model E for E_K coming from the equation $y^2 = P(x)$. In this case, the special fiber is simply a nodal cubic because we have not begun blowing up yet. Here, and elsewhere in the figures, we depict sections (such as D_1 and the 0 and ∞ sections) as horizontal lines, each of which meets the special fiber in a point.

Figure 1



E – a plane model of the degenrate fibre

x-axis

Definition 1. *Let D_0 denote the divisor D. We define the divisor D_i recursively (for $i \leq k$) as the proper transform of D_{i-1} for the blow-up $\sigma_i : X_i \to X_{i-1}$ centered at the point P_{i-1} of multiplicity 2 on D_{i-1}.*

Note that this is a horizontal divisor of degree 3 which intersects the special fiber F_0 of $\mathbb{P}^1_V = X_0$ in 2 points: one P_0 of multiplicity 2 on D_0, the other one of multiplicity 1 on D_0. We now define the divisors in our models X_i coming from H_n.

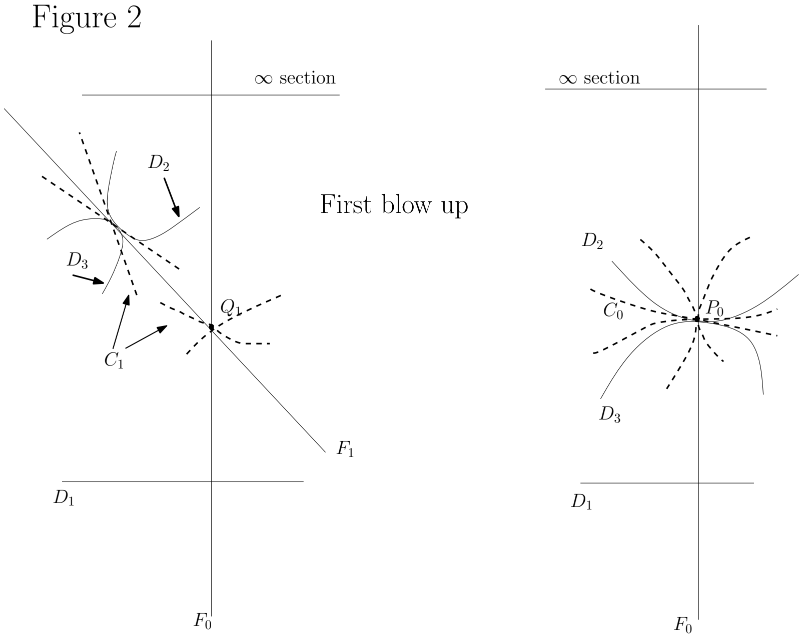
Definition 2. *The horizontal divisor C_0 is defined to be H_n for some fixed odd n. The divisor C_i is the proper transform of C_{i-1} in X_i.*

The degree of C_0 (on the generic fiber) is $(n^2 - 1)/2$ when n is odd and $(n^2/2) - 3$ when n is even. This follows from the fact that the hyperelliptic map sends each point and its inverse to the same point in $\mathbb{P}^1$.

Definition 3. *Define $\wp_K : E_K \to \mathbb{P}^1_K$ to be the projection onto "the x axis" (i.e., $\wp$ is the Weierstrass $\wp$ function). We will, by abuse of language, note $\wp : E_i \to X_i$ to be the the extension of $\wp_K$ to model E_i for E_K over V.*

Figure 2 below illustrates what happens when one first begins to blow-up the model for $\mathbb{P}^1$. Here F_0 denotes the original special fiber on right and its strict tranform on the left, while F_1 is the exceptional divisor.

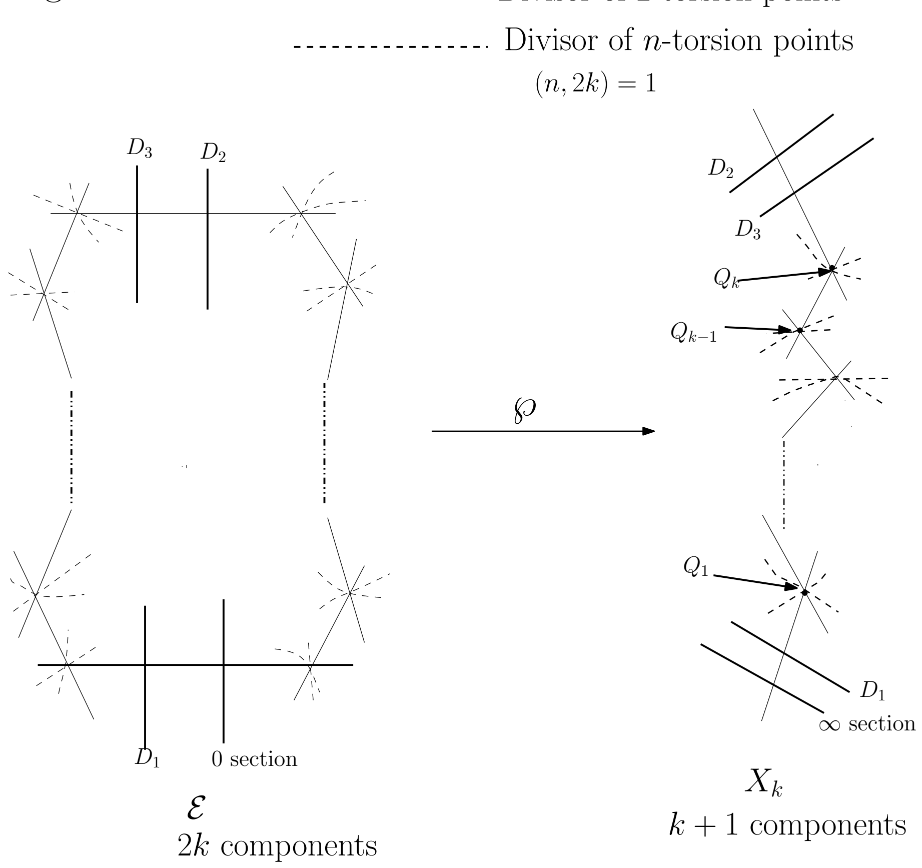
Figure 2



Lemma. *Assume that n is odd or that the residual characteristic is not 2, then after k successive blow-ups of the points P_i of multiplicity 2 on D_i, the proper transform D_k is étale and the proper transforms D_k and C_k do not meet.*

Proof. (*Of Lemma.*) If $\wp^*(C_k)$ and $\wp^*(D_k)$ are both in the Néron model (i.e., if n and $(2k)$ have a common factor m), then H_n and 2-torsion are distinct; hence, when the characteristic is not 2, they do not meet in the Néron model. If n is prime to $2k$ and $\wp^*(H_k)$ is not inside the Néron model, then $\wp^*(H_k) \bigcap \wp^*(D_k) = \emptyset$, since $\wp^*(D_k)$ is in the Néron model (see figure 3 below and recall our earlier explanation about the number of components in the special fibers of the model $\mathcal{E}$ for E and the model X_K for the projective line). $\square$

Figure 3



We are now ready to prove the main theorem.

Proof. We treat first the case when n is prime to $2k$. The exceptional divisor of σ_i will be denoted as F_i. By abuse of language the proper transform of F_i will still be called F_i after $\sigma_{i+1}, \dots, \sigma_k$. We will let Q_i denote the point of intersection of F_i with F_{i-1} in X_i (see figure 2).

We will denote the usual pull-back map for divisors with $*$. We denote the composed map $\sigma_i \cdot \sigma_{i-1} \cdots \sigma_1$ as ρ_i. After i blow-ups, one has integers $m_{j,i}$ such that

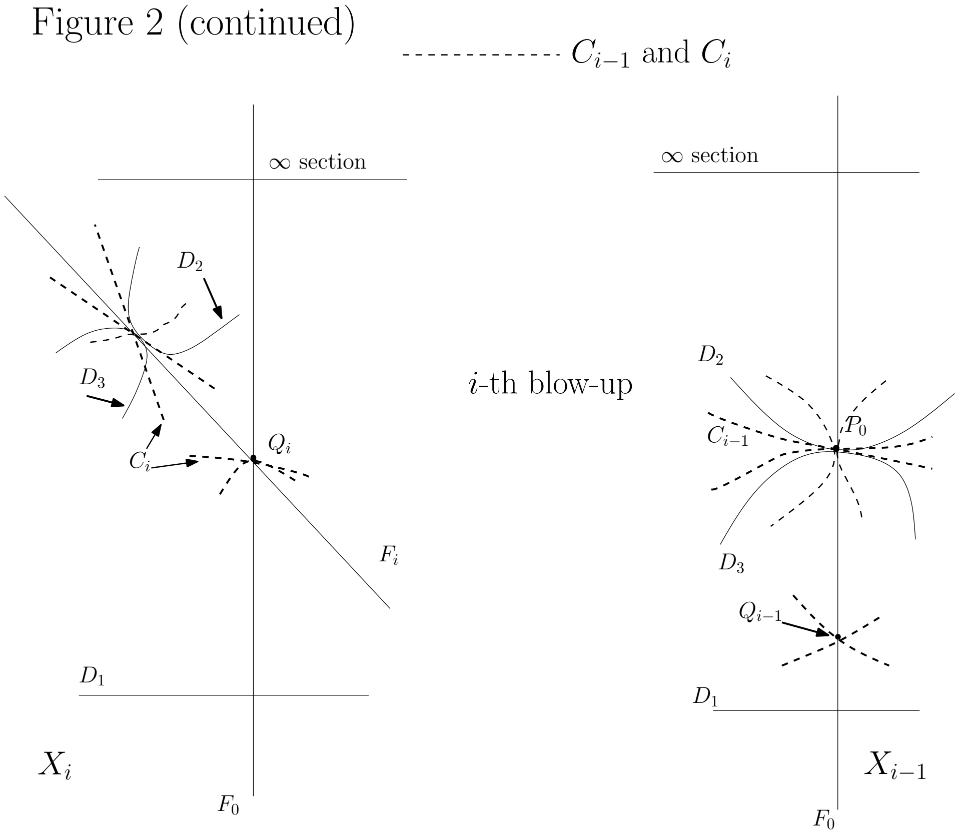
$$\rho_i^* D = D_i + \sum_{j \leq i} m_{j,i} F_j$$

and

$$\pi_{i+1}^* D = \sigma_{i+1}^* D_i + \sum_{j \leq i} m_{j,i} \sigma_{i+1}^* F_j .$$

The figure below illustrates what happens when we take the i-th blow-up. This is quite similar to what happens after the first blow-up: one obtains an additional component in the special fiber coming from the exceptional divisor.

Figure 2 (continued)



As long as i is less than $(k-1)$, one has

$$\sigma_{i+1}^* D_i = D_{i+1} + 2F_{i+1},$$

since the multiplicity of D_i at P_i is still 2. Since $\sigma_{i+1}^* F_i = F_i + F_{i+1}$ we have $m_{j,i} = m_{j,j}$ for any $i \geq j$, so we have

$$m_{j,i} = m_{j,j} = m_{j-1,j-1} + 2$$

for all $i \geq j$. Thus, by induction, we have $m_{j,j} = 2j$ for each j, which means that $m_{j,i} = 2j$ for all $i \geq j$.

The intersection multiplicity we are looking for can be computed as follows

$$(*) (H_n.D) = (C_0.D_0) = (C_k.(D_k + \sum_{j \leq k} m_{j,k} F_j)) = 2 \sum_{j \leq k} j(C_k.F_j).$$

One is left with computing each $(C_k.F_j)$. We will achieve this by looking at the special fiber of various models of E_K over V. By the projection formula for $\wp$ we can compute intersections on the minimal model $\mathcal{E}$ of E_K or on the k-th blow-up X_k of $\mathbb{P}^1$. In fact we will use the projection formula to compute intersections on the minimal model $\mathcal{E}'$ for E after the base change $\operatorname{Spec} V[X]/(X^n - \pi) \to \operatorname{Spec} V$ where π is a uniformizing parameter of V. A description of the resolution of singularities of the base change can be found in [18, Exposé 1, Proposition 2.2].

On the minimal model $\mathcal{E}'$, the special fiber has $2kn$ components. Let Z_0 denote the component of the origin of the elliptic curve, and let us denote the other components as $Z_1, \ldots, Z_{2kn-1}$ in such a way that Z_i meets Z_{i+1} for $0 \leq i \leq (2kn-1)$ and Z_{2k-1} meets Z_0 (figure 4).

The divisor of n-torsion points meets only the components Z_i for which i is a multiple of $2k$; the multiplicity of each intersection is n. The components Z_j for which j is a multiple of n are the only ones not contracted by the morphism to the plane model E. The contribution at Q_j in the intersection number $(C_k.F_j)$ for $j \neq 0, k$ will be

$$n \cdot \left| \{ m \text{ such that } (j-1)n \leq 2km \leq jn \} \right|$$

Write $n = 2kq + r$ with $0 \leq r < 2k$. We have

$$\left| \left| \{ m \text{ such that } (j-1)n \leq 2km \leq jn \} \right| - q \right| \leq 1.$$

Thus, we have

$$(**) \left| (C_k.F_j) - 2n \frac{n-r}{2k} \right| \leq 2n.$$

Since $(C_k.F_k) = n\frac{n-r}{k}$ we obtain

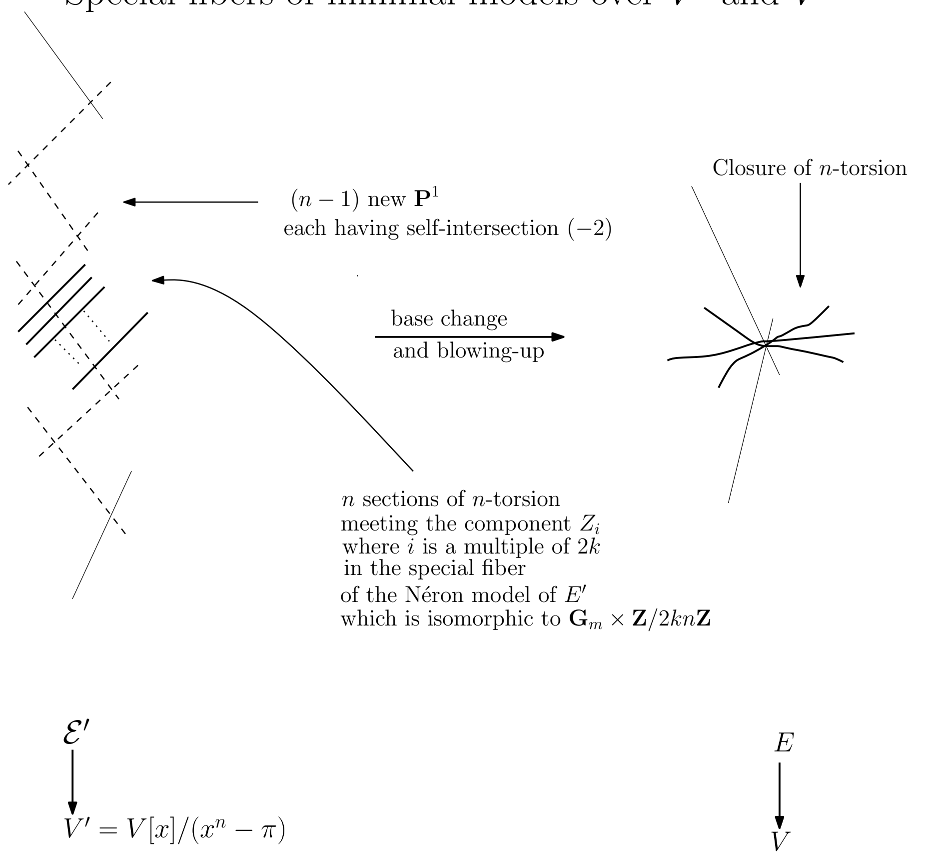
$$\begin{aligned}\left|(H_n.D) - \Big(2\sum_{j\le(k-1)} j2n\frac{n-r}{2k} + 2kn\frac{n-r}{k}\Big)\right| &\le 2\sum_{j\le(k-1)} j(2n)\\ &= 2\frac{k(k-1)}{2}2n.\end{aligned}$$

Hence, we have $|(H_n.D) - (n-r)nk| \le k(k-1)2n$, so

$$\lim_{n\to\infty}\frac{1}{n^2}(H_n.D) = k.$$

Figure 4 below illustrates what happens to the component group when one extends the base to $V' = V[x]/(x^n - \pi)$ from V; simply put, the number of components increases in a way that makes it easier to calculate the relevant intersections.

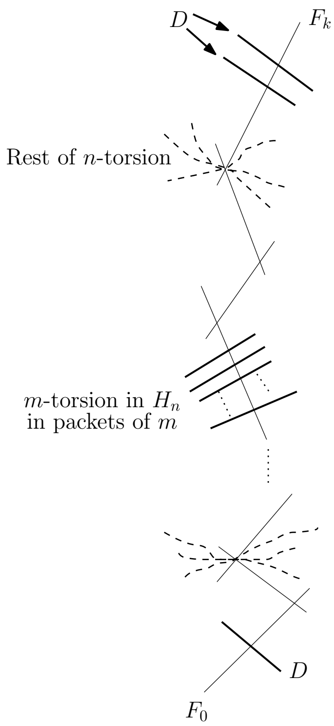
Figure 4
Special fibers of minimal models over V' and V



This finishes the proof in the case when n and $2k$ are relatively prime. For the case where n and $2k$ have a gcd m greater than 1 the formula (*) is still valid. The n-torsion distribute themselves in packets of m in components of the special fiber (as illustrated in figure 5 below). Thus, the estimate (**) for $(C_k.F_i)$ has now an error term of at most m.

Figure 5

$(2k, n) = m$



Adding as before, we now obtain

$$|(H_n.D) - (n-r)nk| \leq \sum_{j \leq (k-1)} 2jm = mk(k-1) \leq k(k-1)(2k).$$

Letting n go to ∞ we see again that

$$\lim_{n\to\infty} \frac{1}{n^2}(H_n.D) = k.$$

$\square$

References

[1] P. Autissier, letter to L. Szpiro, September 2005.

[2] ———, *Points entiers sur les surfaces arithmétiques*, J. reine. angew. Math **531** (2001), 201–235.

[3] A. Baker, *Transcendentaumber theory*, Cambridge University Press, Cambridge, 1975.

[4] M. Baker, S. I. Ih, and R. Rumely, *A finiteness property of torsion points*, 2005, preprint, 30 pages.

[5] M. Baker and R. Rumely, *Equidistribution of small points, rational dynamics, and potential theory*, Ann. Inst. Fourier (2005), to appear. Available at `arxiv:math.NT/0407426`, 50 pages.

[6] Y. Bilu, *Limit distribution of small points on algebraic tori*, Duke Math. J. **89** (1997), 465–476.

[7] A. Chambert-Loir, *Mesures et équidistribution sur les espaces de Berkovich*, preprint. Available at `arxiv:abs/math.NT/0304023`, 20 pages, 2004.

[8] P. Deligne, *Courbes elliptiques: formulaire (d'aprés J.Tate)*, Springer Lecture Notes **476** (1972), 53–74.

[9] G. Everest and Bríd Ní Fhlathúin, *The elliptic Mahler measure*, Math. Proc. Cambridge Philos. Soc. **120** (1996), 13–25.

[10] G. Everest and T. Ward, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Springer-Verlag, New York, 1999.

[11] C. Favre and J. Rivera-Letelier, *Équidistribution des points de petite hauteur*, preprint. Available at `arxiv:abs/math.NT/0407471`, 34 pages, 2004.

[12] ———, *Théorème d'équidistribution de Brolin en dynamique p-adique*, C. R. Math. Acad. Sci. Paris **339** (2004), no. 4, 271–276.

[13] Sur les propriétés numériques du dualisant relatif d'une surface arithmétique, *Grothendiek festshrift*, Dynamical Systems, Valparaiso 1986, Birkh"auser, 1990.

[14] K. Mahler, *An application of Jensen's formula to polynomials*, Mathematica **7** (1960), 98–100.

[15] J. Piñeiro, L. Szpiro, and T. Tucker, *Mahler measure for dynamical systems on $\mathbb{P}^1$ and intersection theory on a singular arithmetic surface*, Geometric methods in algebra and number theory (F. Bogomolov and Y. Tschinkel, eds.), Progress in Mathematics 235, Birkhäuser, 2004, (Available at http://math.gc.cuny.edu/faculty/szpiro/504miami.pdf), pp. 219–250.

[16] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20, corrigendum, ibid. **2** (1955), 168.

[17] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[18] L. Szpiro, *Séminaire sur les pinceaux de courbes de genre au moins deux*, Astérisque **86** (1981), 1–142.

[19] L. Szpiro and T. J. Tucker, *Equidistribution and generalized Mahler measures*, preprint. Available at `arxiv:math.NT/0510404`, 29 pages, 2005.

[20] L. Szpiro and E. Ullmo, *Variations de la hauteur de Faltings dans une classe d'isogénie*, Duke Math. J. **97** (1999), 81–97.

[21] L. Szpiro, E. Ullmo, and S. Zhang, *Equirépartition des petits points*, Invent. Math. **127** (1997), 337–347.

[22] E. Ullmo, *Positivité et discrétion des points algébriques des courbes*, Ann. of Math. (2) **147** (1998), no. 1, 167–179.

[23] S. Zhang, *Equidistribution of small points on abelian varieties*, Ann. of Math. (2) **147** (1998), no. 1, 159–165.