COMPOSITIO MATHEMATICA

DORIAN GOLDFELD
LUCIEN SZPIRO

Bounds for the order of the Tate-Shafarevich group

Compositio Mathematica, tome 97, n° 1-2 (1995), p. 71-87
<http://www.numdam.org/item?id=CM_1995__97_1-2_71_0>

Compositio Mathematica **97**: 71–87, 1995.

Bounds for the order of the Tate–Shafarevich group

Dedicated to Frans Oort on the occasion of his 60th birthday

DORIAN GOLDFELD*
Department of Mathematics, Columbia University, NY NY 10027

and

LUCIEN SZPIRO
Department of Mathematics, Columbia University, NY NY 10027 &CNRS, Department of Mathematics, Batiment 425, Université d'Orsay, 91405 France

Received 7 March 1995; accepted in final form 3 April 1995

Abstract. In this paper we show, *over* $\mathbb{Q}$, with classical conjectures like Birch and Swinnerton-Dyer, the equivalence for modular elliptic curves between the following two conjectures:

(1) $|Ш| = \mathrm{O}\left(N^{1/2+\epsilon}\right)$

(2) $D = \mathrm{O}\left(N^{6+\epsilon'}\right)$

relating the order $|Ш|$ of the Tate–Shafarevich group, the conductor N and the discriminant D of an elliptic curve.

We also show for *function fields* that (1) stands because (2) has been proved earlier by one of us.

1. Introduction

In this paper we study bounds for the order of the Tate–Shafarevich group Ш for elliptic curves over a global field k. In the tradition of A. Weil's, Basic number theory [23], we treat both the case where k is a number field, of finite dimension over $\mathbb{Q}$, and the case where k is a function field of one variable over a finite field. The primary objective is to relate bounds for Ш and bounds for the discriminant of the elliptic curve (in both cases in terms of the conductor). Our principal results are given in Theorems 1, 2, 3, and 15.

Let E be an elliptic curve over a fixed number field k of discriminant D and conductor $N \to \infty$. Let Ш denote the Tate–Shafarevich group of E. We conjecture that a bound for the cardinality of Ш of type

$$|Ш| = \mathrm{O}(N^{1/2+\epsilon}) \tag{1.1}$$

* Supported in part by NSF grant No. DMS-9003907.

(for some fixed $\epsilon > 0$) is equivalent to a bound for the discriminant of type

$$D = O(N^{6+\epsilon'}) \tag{1.2}$$

for some other fixed $\epsilon' > 0$. In (1.1) and (1.2), the constant in the big O-symbol depends at most on k, ϵ, and ϵ', while in (1.1) it also depends on the Mordell–Weil rank of E over k. The latter bound was conjectured by the second author [17] and is known to imply the ABC-conjecture. The conjectured equivalence of the two bounds points out the inherent difficulty in proving the ABC-conjecture by this approach since Ш has only very recently been proved finite by Rubin [14] for certain CM-curves over $\mathbb{Q}$, and more generally by Kolyvagin for certain modular elliptic curves defined over $\mathbb{Q}$ (see [8, 6]). It has recently been announced by Andrew Wiles that all semi-stable elliptic curves defined over $\mathbb{Q}$ are modular [24, 20].

In this paper we show that

$$(1.2) \Longrightarrow (1.1)$$

for modular elliptic curves (of fixed rank defined over $\mathbb{Q}$) satisfying the Birch–Swinnerton-Dyer conjecture. We also show that

$$(1.1) \Longrightarrow (1.2)$$

for modular elliptic curves defined over $\mathbb{Q}$. The Birch–Swinnerton-Dyer conjecture is not needed in this direction since we may pass to the case of rank zero (where the Birch–Swinnerton-Dyer conjectured is proved by Kolyvagin (see [6])) by quadratic base change.

Now (1.2) is known for function fields over finite fields (see [17]), while the finiteness of Ш is still open in the case of function fields. We, therefore, thought it worthwhile to see if our methods applied to this case. We prove that (1.1) holds for elliptic curves E defined over function fields provided the Tate–Shafarevich group for the function field is finite. It is known [12] that the finiteness of Ш in the case of function fields is equivalent to the fact that the ℓ-primary part of Ш (all elements of Ш annihilated by any power of ℓ) is finite for any prime ℓ. This is in fact equivalent to Tate's conjecture for $H^2_{\text{etale}}(X; \mathbb{Z}_\ell)$. When combined with our results this implies that Ш is finite if and only if

$$|Ш_\ell| = 1$$

(where $Ш_\ell$ denotes the ℓ-torsion in Ш) for any prime ℓ greater than the upper bound for Ш obtained in Section 4. This provides an effective algorithm for determining if Ш is finite in the case of function fields. As is well known, such an algorithm is not presently available for elliptic curves over number fields. It is interesting to remark, however, that even in the case of an elliptic curve over $\mathbb{Q}$ of conductor $N \to \infty$, if

$$|Ш_\ell| \neq 1$$

for some prime $\ell \gg N^{1/2+\epsilon}$ then either (1.1) is false or the Birch–Swinnerton-Dyer conjecture is false or the Shimura–Taniyama–Weil conjecture is false (highly unlikely [24]). This is a consequence of the results of Section 4.

2. Dictionary

Consider an elliptic curve E: $y^2 = 4x^3 - ax - b$ given in Weierstrass normal form. Assume E is defined over a global field K which is either an algebraic number field or a function field of one variable defined over a finite field of $q = p^m$ elements for some prime number p. Set $f(x, y) = y^2 - 4x^3 - ax - b$, with $a, b \in \mathrm{O}_K$ where O_K denotes the ring of integers of K. Then $\mathrm{O}_K[x, y]/f$ has Krull dimension two, so that E may be viewed as a surface over $\mathrm{Spec}(\mathrm{O}_K)$. The following dictionary defines the invariants of E in the case of a number field or function field. For clarity, the definitions may only be approximately correct in some cases. For example, when needed, we assume E has semi-stable reduction.

	Number Field	Function Field
Discriminant	$D = a^3 - 27b^2$	$D = \sum_{\substack{P=\text{zero of } a^3-27b^2 \\ n_P=\text{multiplicity of } P}} n_P[P]$
Conductor	$N = \prod_{p \mid D} p$	$N = q^{\#\{P,\ n_P \neq 0\}}$
Period	$\Omega = 2\int_{E(\mathbb{R})} \frac{dx}{y}$	$q^{-\alpha}$, $\alpha =$ Euler–Poincaré char.
One Cycles	Mordell–Weil group	Néron–Severi group
Two Cycles	Tate–Shafarevich group	Brauer group
Intersections	Néron–Tate height and Arakelov intersection	Intersection Theory on the Surface
Model	Minimal Model over O_K	Relative Minimal Elliptic Surface over a Curve C

We explain certain cohomological notation attached to projective morphisms of algebraic varieties at the beginning of Section 4.

3. Modular Elliptic Curves over $\mathbb{Q}$

We now consider a modular elliptic curve E defined over $\mathbb{Q}$ of conductor N. Let $L_E(s)$ denote the L-function of E which satisfies the functional equation see [1]

$$\left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L_E(s) = \pm \left(\frac{\sqrt{N}}{2\pi}\right)^{2-s} \Gamma(2-s) L_E(2-s). \tag{3.1}$$

If $L_E(s)$ has a zero of order $r \geqslant 0$ at $s = 1$, then the Birch–Swinnerton-Dyer conjecture predicts that for s near 1

$$L_E(s) = \left(\frac{c_E \Omega_E \cdot |Ш_E| \cdot \mathrm{vol}(E(\mathbb{Q}))}{|E(\mathbb{Q})_{\mathrm{tor}}|^2} \right) \cdot (s-1)^r + \mathrm{O}(s-1)^{r+1}, \qquad (3.2)$$

where r is the rank of the Mordell–Weil group of $E/\mathbb{Q}$, Ω_E is either the real period or twice the real period of E (depending on whether or not $E(\mathbb{R})$ is connected), $|Ш_E|$ is the order of the Tate–Shafarevich group of $E/\mathbb{Q}$, $\mathrm{vol}(E(\mathbb{Q}))$ is the volume of the Mordell–Weil group for the Néron–Tate bilinear pairing, $|E(\mathbb{Q})_{\mathrm{tors}}|$ is the order of the torsion subgroup of $E/\mathbb{Q}$, and $c_E = \prod_p c_p$ where $c_p = 1$ unless E has bad reduction at E in which case c_p is the order $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$. Here $E_0(\mathbb{Q}_p)$ is the set of points reducing to non-singular points of $E(\mathbb{Z}/p\mathbb{Z})$ (see [15]).

THEOREM 1. *Let E be a modular elliptic curve over $\mathbb{Q}$ which satisfies the Birch–Swinnerton-Dyer conjecture* (3.1). *Then the bound* (1.2) *implies* (1.1) *with $\epsilon = c'\epsilon' + c''$ for certain fixed constants $c', c'' \geqslant 0$. If we assume Lang's conjecture* [10] *then we we may take $c'' = 0$.*

Proof. The function

$$\left(\sqrt{\frac{N}{2\pi}} \right)^s \Gamma(s) L_E(s) \cdot (s-1)^{-r}$$

is holomorphic and satisfies a functional equation for the transformation $s \longrightarrow 1 - s$ induced from the functional equation (3.1). It is absolutely bounded when $\mathrm{Re}(s) > 3/2 + \epsilon$ and bounded by $N^{1/2+\epsilon}$ when $\mathrm{Re}(s) = 1/2$, by the functional equation. The usual convexity argument as in the Phragmén–Lindelöf theorem (see [21]) implies that

$$L_E^r(1) = \mathrm{O}(N^{c_1+\epsilon}),$$

with $c_1 = 1/4$ and $\epsilon > 0$ is fixed. The assumption of the Riemann hypothesis for $\mathrm{L}_E(s)$, however, would yield the much better constant $c_1 = 0$. It follows from (3.2) that

$$\frac{c_E\, \Omega_E \cdot |Ш_E| \cdot \mathrm{vol}(E(\mathbb{Q}))}{|E(\mathbb{Q})_{\mathrm{tor}}|^2} \ll N^{c_1+\epsilon}. \qquad (3.3)$$

Now $c_E \geqslant 1$ and $|E(\mathbb{Q})_{\mathrm{tor}}|^{-2} \geqslant 1/256$, by Mazur's result [11]. Assuming (1.2), we also have a lower bound for the volume (see [7])

$$\mathrm{vol}(E(\mathbb{Q})) \gg N^{-c_2} \qquad (3.4)$$

for some constant $c_2 > 0$. If (P, Q) denotes the bilinear symmetric form associated with the Néron–Tate height, then the volume of $E(\mathbb{Q})$ may be expressed as a determinant of the height pairing

$$\mathrm{vol}(E(\mathbb{Q})) = |\det(P_i, P_j)|,$$

where $\{P_1, \ldots, P_r\}$ is any basis of $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$. The lower bound (3.4) is a consequence of the lower bound for $|\det(P_i, P_j)|$ which was conjectured by Lang [10] and proved by Hindry and Silverman [7] under the assumption of (1.2). The full strength of Lang's conjectures [10] imply that $c_2 = \epsilon$.

Furthermore, the assumption of (1.2) implies (see [5]) that

$$\Omega_E \gg N^{-c_3},$$

for some other constant $c_3 > 0$. We expect $c_3 > 1/2$. Putting these bounds into (3.3) yields

$$|\text{Ш}_E| \ll N^{c_1+c_2+c_3+\epsilon},$$

which proves the theorem. This type of argument can be found in Lang [10] who was the first to conjecture upper bounds for

$$|\text{Ш}_E| \cdot \mathrm{vol}(E(\mathbb{Q})),$$

in analogy with the bounds given in the Brauer–Siegel theorem for the class number times the regulator of a number field.

We now go in the other direction and show that (1.1) implies (1.2) for modular elliptic curves over $\mathbb{Q}$.

THEOREM 2. *Assume the bound* (1.1) *holds for modular elliptic curves defined over* $\mathbb{Q}$ *with* $\epsilon > 0$. *Then* (1.2) *also holds with* $\epsilon' = 12(\epsilon + 1)$. *Moreover, if we assume the Riemann hypothesis for Rankin–Selberg zeta functions associated to modular forms of weight* $3/2$ *then we may take* $\epsilon' = 13\epsilon$.

Proof. Let E be a modular elliptic curve defined over $\mathbb{Q}$ of conductor N and discriminant D. Let Ω_1, Ω_2 denote the periods of E. We may assume (without loss of generality) that Ω_1 is real and Ω_2 is pure imaginary. If

$$\Delta(z) = e^{2\pi i z} \prod_{n=1}^{\infty} \left(1 - e^{2\pi i n z}\right)^{24}$$

is the Ramanujan cusp form of weight 12 for the full modular group which satisfies the transformation formula

$$\Delta\left(-\frac{1}{z}\right) = z^{12}\Delta(z),$$

then we have

$$D = C \cdot \frac{\Delta\left(\frac{(-1)^j\Omega_j}{\Omega_k}\right)}{\Omega_k^{12}}$$

where $\{j, k\} = \{1, 2\}$ or $\{2, 1\}$ and $C > 0$ is a constant.

Clearly, we can choose (j,k) appropriately so that $\left|\frac{\Omega_j}{\Omega_k}\right| > 1$. In this case $\Delta\left(\frac{(-1)^j\Omega_j}{\Omega_k}\right)$ is absolutely bounded from above by a fixed constant $c_4 > 0$ and it immediately follows that

$$D < \frac{c_4}{\Omega_k^{12}}.$$

To prove the theorem it is enough to show that the bound (1.1)

$$|\text{Ш}| = O(N^{1/2+\epsilon})$$

(which is assumed to hold for all modular elliptic curves defined over $\mathbb{Q}$) implies that

$$\Omega_k \gg \frac{1}{N^{1/2+\epsilon}}.$$

To demonstrate this last assertion, we consider quadratic twists (mod q) of our elliptic curve E. If E is defined by a Weierstrass equation

$$E\colon\ y^2 = 4x^3 - ax - b$$

then the twisted elliptic curve E_χ is defined to be

$$E_\chi\colon\ y^2 = 4x^3 - aq^2x - bq^3,$$

which is also an elliptic curve defined over $\mathbb{Q}$. Let $\mathrm{L}_E(s,\chi)$ be the L-function associated to E_χ. Then the nth coefficient of $\mathrm{L}_E(s,\chi)$ is just the nth coefficient of $\mathrm{L}_E(s)$ multiplied by $\chi(n)$. We would like to choose quadratic Dirichlet characters χ where E_χ has Mordell–Weil rank 0 and χ satisfies $\chi(-1) = (-1)^j$. In this case

$$\frac{\mathrm{L}_E(1,\chi)}{\Omega_k} = c_\chi \text{Ш}_\chi$$

where Ш_χ is the Shafarevich–Tate group of E_χ and $c_\chi \ll \sqrt{q}$ depends at most on q.

Applying the Rankin–Selberg method as in [9, 5] one obtains

$$\sum_{\substack{q\leqslant N^2\\ \chi(-1)=(-1)^j}} \mathrm{L}_E(1,\chi) \sim c_5 N^2,$$

for some constant $c_5 > 0$. It follows that for some twist χ with $q \leqslant N^2$, we must have $L_E(1,\chi) \gg 1$. The nonvanishing of the L-function at $s = 1$ implies that the Mordell–Weil rank of E_χ must be zero. Therefore, the assumption (1.1) for all elliptic curves defined over $\mathbb{Q}$ implies that

$$\frac{1}{\Omega_E} \ll \frac{L_E(1,\chi)}{\Omega_E} \ll c_\chi N^{1/2+\epsilon} \tag{3.5}$$

which implies that $\Omega_E \gg c_\chi N^{-1/2-\epsilon}$. This establishes the first part of the theorem. If one assumes the Riemann hypothesis for the Rankin–Selberg zeta function associated to the weight 3/2 modular form associated to E by the Shintani–Shimura lift, then the asymptotics will hold in a much shorter range

$$\sum_{\substack{q\leqslant N^\epsilon \\ \chi(-1)=(-1)^j}} L_E(1,\chi) \sim c_6 N^\epsilon.$$

In this case, there will exist a character χ of conductor $q < N^\epsilon$ where $L_E(1,\chi) \gg 1$. Inequality (3.5) again holds, but this time $c_\chi < N^\epsilon$. The theorem follows.

4. The Function Field Case

The vocabulary and notation of Grothendieck's algebraic geometry is used when needed in the treatment of the function field case. We thought that it would be worthwhile for the reader (more oriented towards number theory) to recall some basic notation. If $f\colon X \to Y$ is a morphism of schemes (or algebraic varieties) and F is a sheaf on X, one can consider, for every U open in Y, the groups $H^0(f^{-1}(U), F)$. The sheaf associated to this presheaf is denoted f_*F (direct image). In the same mode, the sheaf associated to the presheaf $U \to H^i(f^{-1}(U), F)$ is denoted $R^i f_*(F)$. Here $R^i f_*$ is the ith derived functor of f_*.

For example, if f is a proper map and F is a coherent sheaf on X, it is a classical theorem that the $R^i f_* F$ are coherent. Moreover, if $f\colon X \to C$ is a projective morphism from a smooth surface X to a smooth complete curve C (over a field k) and if f is flat and the generic fiber of f is geometrically connected then f_*O_X and $R^1 f_* O_X$ commute with base change. In particular,

$$\dim_{k(P)} H^1(X_P, O_{X_P}) = \dim_{k(P)} \left(R^1 f_* O_X\right) \otimes k(P) < \infty$$

for every point P in C with residual field $k(P)$ (This number is independent of P and is equal to the genus of the generic fiber).

In this section, X will denote a smooth geometrically connected projective surface over a finite field $\mathbb{F}_q$ with $q = p^n$ elements (p a prime). We suppose, moreover, that X is an *elliptic pencil*, i.e., that there exists a projective, smooth, geometrically connected curve C over $\mathbb{F}_q$ with a projective morphism $f\colon X \to C$ whose generic fiber is a smooth elliptic curve. By the results of Weil and Deligne [3] one knows that the zeta function of X has the form:

$$\zeta(X,t) = \frac{P_1(X,t)P_3(X,t)}{(1-t)P_2(X,t)(1-q^2t)}$$

where $P_i(X,t)$ is a polynomial with integer coefficients whose reciprocal roots have absolute value $q^{i/2}$.

Let K denote the function field of C. By [19], Theorem 3.1, the Brauer group of X is equal to the Tate–Shafarevich group $Ш(X_K)$ and the Artin–Tate analogue of the Birch–Swinnerton-Dyer conjecture for function fields takes the form:

$$P_2(X, q^{-s}) \sim \frac{(-1)^{r(X)-1}\,|Ш(X_K)|\,\mathrm{vol}(NS(X))}{q^{\alpha(X)}|NS(X)_{\mathrm{tor}}|^2} \cdot (1 - q^{1-s})^{r(X)} \qquad (4.1)$$

for $s \to 1$ where $r(X) = r$ is the rank of the Néron–Severi group of X and

(1) The volume of $NS(X)$ is computed by the intersection matrix, i.e., if $D_1, \ldots, D_\rho$ denotes a basis of $NS(X)/\mathrm{torsion}$ then

$$\mathrm{vol}(NS(X)) = |\det(D_i \cdot D_j)|,$$

(2) $\alpha(X) = \chi(X, O_X) - 1+$ the dimension of the Picard variety of X.

Many cases of this conjecture have been proved (see Milne [12]). An important line bundle associated to $f\colon\ X \to C$ is

$$\omega = \epsilon^* \Omega^1_{X/C},$$

where ϵ is the zero section. One knows that $f^*\omega = \omega_{X/C}$, the relative dualizing sheaf of X over C, and that the discriminant divisor (Δ) corresponds to a section of $\omega^{\otimes 12}$. We have

$$(\Delta) = \sum_{P \in S} n_P[P],$$

where S is the set of points of C with singular fiber, and n_P is an integer. In the case that $f\colon\ X \to C$ is semi-stable (i.e. with multiplicative reduction only) then n_P is the number of components of the fiber of P. The following theorem is proved in [16] or [17].

THEOREM 3. *Let $f\colon\ X \to C$ be a nonconstant family of elliptic curves (i.e. j-map is nonconstant) of conductor of degree m. With the notation introduced above, we have*

$$\deg(\Delta) \leqslant 6p^e(2g - 2 + m)$$

where p^e is the inseparability degree of the j-map: $C \to \mathbb{P}^1$ associated to f.

In characteristic zero, the j map is always separable, so its derivative (the Kodaira–Spencer map of f) is also non-zero. In characteristic $p > 0$ (which is our current situation), the nonvanishing of the Kodaira–Spencer map is *after seperable base change* equivalent to saying that $f\colon\ X \to C$ is not a pull back by the Frobenius morphism of C.

The theorem is detailed in [17] only for a semi-stable family. The fact that it is valid even in the non semi-stable case is in [13]. It follows from staring at the table of different bad reductions in Tate [18] and doing easy computations. This works perfectly in char $\neq 2$ or 3. For char 2 and char 3, a bigger effort is made in [13].

LEMMA 4. *Let X be as above. If the family is not constant then the dimension of* $\mathrm{Pic}(X)$ *is* g.

Proof. Since $\mathrm{Pic}(X)$ contains $\mathrm{Pic}(C)$ its dimension must be at least g. On the other hand, the tangent space to $\mathrm{Pic}(X)$ is $H^1(X, \mathcal{O}_X)$ so the dimension of $\mathrm{Pic}(X)$ is less than $\dim(H^1(f_*\mathcal{O}_*)) + \dim(H^0(R^1f_*\mathcal{O}_X))$. But $f_*\mathcal{O}_X = \mathcal{O}_C$, so we will have proven the lemma if we know that $H^0(R^1f_*\mathcal{O}_X) = 0$. By duality, we have $R^1f_*\mathcal{O}_X = \omega^{\otimes -1}$. Since $\omega^{\otimes 12}$ has a section it follows that $H^0(C, \omega^{\otimes -1}) = 0$ except when $\omega = \mathcal{O}_C$ This last case does not occur if the family is not constant as there is no nonconstant family with good reduction everywhere over a complete curve.

LEMMA 5. *With X as above we have* $\chi(X, \mathcal{O}_X) = \deg(\omega)$.

Proof. We have

$$\begin{aligned}\chi(X, \mathcal{O}_X) &= \chi(f_*\mathcal{O}_X) - \chi(R^1f_*\mathcal{O}_X)\\ &= 1 - g - (-\deg(\omega) - g + 1).\end{aligned}$$

COROLLARY 6. *If $f\colon X \to C$ is a nonconstant fibration then we have* $\alpha(X) = \deg(\omega) - 1 + g \leqslant (p^e + 1)(g - 1) + \frac{m}{2}p^e$.

We now want to find a lower bound for $\det(D_i \cdot D_j)$ for a basis of the Néron–Severi group. For this we need to prove in *any characteristic* the following statement which was proved by Hindry and Silverman [7] only for function fields in characteristic zero.

THEOREM 7. *Let X_K be an elliptic curve over a function field of one variable over a field in any characteristic. Let $\hat{h}$ denote the Néron–Tate height on X_K. Then for every point $P \in X_K(K)$ which is not a torsion point:*

$$\hat{h}(P) \geqslant 10^{-13}\deg(\Delta) \quad \textit{if} \quad \deg(\Delta) \geqslant 24(g-1),$$

and

$$\hat{h}(P) \geqslant 10^{-13-23g}\deg(\Delta) \quad \textit{if} \quad \deg(\Delta) < 24(g-1).$$

In fact, the beautiful proof of Hindry–Silverman carries through in characteristic $p > 0$ once one has a good expression in local terms for the Néron–Tate height. We give such a formula in Proposition 11 below. To compute the volume of $NS(X)$ we must decompose it into an orthogonal sum:

$$(\mathbb{Z} \cdot E_O + V) \oplus X_K(K)$$

where V = *vertical divisors*. (One should remember that if D is a divisor such that D_K is of degree $m > 0$, then $D_K - (m-1)O$ must be linearly equivalent to a point P by the Riemann–Roch theorem.)

The intersection matrix on $X_K(K)$ is by our choice $(\langle x_i \cdot x_j \rangle)$ where (x_i) is a base of $X_K(K)$/torsion, and $\langle , \rangle$ is the Néron–Tate pairing.

On $\mathbb{Z} \cdot E_O + V$ one may analyze the intersection matrix as follows: For every $v \in S$, the components of $f^{-1}(v)$ not meeting E_O are $n_v - 1$ in number, where $n_v =$ valuation of Δ at v (X is semi-stable). It follows that if F is one full fiber, its intersection matrix can be computed as

$$\begin{pmatrix} 0 & 1 & \\ 1 & -\deg(\omega) & 0 \\ & 0 & A_v \end{pmatrix}$$

where A_v is the intersection matrix of the set of components of $f^{-1}(v)$ not meeting 0. In geometric notation, one has

$$A_v = \begin{pmatrix} -2 & 1 & & \\ 1 & -2 & & 0 \\ & 0 & \ddots & 1 \\ & & 1 & -2 \end{pmatrix}.$$

An easy computation gives $\det(A_v) = (-1)^n n$.

DEFINITION. Let $f\colon X \to C$ be a projective morphism from a regular surface X to a regular curve C with generic fiber a smooth connected curve. A divisor D on X is said to be of degree absolutely zero if for every divisor V contained in the fibers of C one has $(V \cdot D) = 0$.

Recall the following classical lemma.

LEMMA 8. *If V is a divisor contained in the fibers of f then $(V \cdot V) \leqslant 0$, and if $(V \cdot V) = 0$, then V is a sum of full fibers.*

COROLLARY 9. *If D_1 and D_2 are divisors on X of degree absolutely zero, and if D_1 and D_2 coincide at the generic fiber of f then $D_1 = D_2 + V$ where V is a sum of full fibers.*

Proof. The divisor $D_1 - D_2$ is contained in fibers because it is zero on the generic fiber. It is of degree absolutely zero so $((D_1 - D_2) \cdot (D_1 - D_2)) = 0$ which proves the corollary by the previous lemma.

Suppose that $X \xrightarrow{f} C$ is an elliptic fibration, i.e. the generic fiber X_K is a smooth connected elliptic curve with origin denoted O. (Recall that K is the function field of C.) We let E_P denote the section of F corresponding to a rational point $P \in X(K)$. (E_P is a divisor on X, the restriction of F to $E_P \to C$ is an isomorphism, and generically E_P is P.)

DEFINITION. Let $X \xrightarrow{f} C$ be an elliptic fibration and let P be a rational point of the generic fiber X_K. We let ϕ_P denote a $\mathbb{Q}$-divisor with support in the fibers of f such that $(E_P - E_O + \phi_P)$ is of degree absolutely zero.

LEMMA 10. *For every rational point P of X_K a $\mathbb{Q}$-divisor ϕ_P exists. It is unique up to the addition of full fibers (so $-\phi_P^2$ is well defined). Moreover, if K' is a finite extension of K and P' is a rational point of $X_K(K')$ then there exists a constant A, independent of P', K' (depending only on $f\colon X \to C$), such that $-\phi_{P'}^2 \leqslant [K'\colon K]A$.*

We will establish this lemma for every point ν of C with a nonsmooth fiber, and find a $\phi_{P,\nu}$ with support in the fiber $f^{-1}(-\nu)$. Then ϕ_P is equal to $\sum \phi_{P,\nu}$; this sum is finite and $\phi_P^2 = \sum \phi_{P,\nu}^2$ because $(\phi_{P,\nu} \cdot \phi_{P,\nu'}) = 0$ if $\nu \neq \nu'$.

Let F_i be the irreducible components of $f^{-1}(\nu)$. ($f^{-1}(\nu) = \sum m_i F_i$, with $m_i \in \mathbb{N}$). We solve the equations

$$\left(\left(E_P - E_O + \sum x_i F_i\right) \cdot F_j\right) = 0$$

for all j. Suppose $E_P \cdot F_{i_1} = 1$ (hence $m_{i_1} = 1$) and $E_P \cdot F_j = 0$ for all $j \neq i_1$. Also, define i_0 to be the index such that $E_O \cdot F_{i_0} = 1$. The equations look like:

$$\begin{aligned}
\sum_i x_i(F_i \cdot F_j) &= 0 \quad \text{if } j \neq i_1, i_0\\
\sum_i x_i(F_i \cdot F_{i_0}) &= 1 \quad \text{if } i_0 \neq i_1\\
\sum_i x_i(F_i \cdot F_{i_1}) &= -1 \quad \text{if } i_0 \neq i_1\\
\sum_i x_i(F_i \cdot F_{i_1}) &= 0 \quad \text{if } i_0 = i_1 \text{ (in which case } x_i = 0 \text{ for all } i).
\end{aligned}$$

So one sees that $-\phi_P^2$ depends only on the coefficients of the intersection matrix of the components of the fibers. Then an easy computation in the semi-stable case (which is sufficient) concludes the proof of the lemma.

PROPOSITION 11. *Let $f\colon X \to C$ be an elliptic fibration over a smooth connected projective curve over a field k of any characteristic. The Néron–Tate height $\hat{h}(P)$ of a point $P \in X_K(K')$ (where K' is a finite extension of K, the function field of C) is given by the expression*

$$2[K'\colon K]\hat{h}(P) = -(E_P - E_O + \phi_P)^2.$$

Proof. To prove this proposition (due to Manin), we will use the axiomatic characterization of $\hat{h}(P)$ given by Tate:

(1) $\hat{h}(nP) = n^2 \hat{h}(P)$

(2) $|\hat{h}(P) - h(P)|$ is bounded on $\overline{K}$.

Here $\overline{K}$ is the algebraic closure of K.

We first prove (2). Note that $h(P)$ is the *naive height* of P associated to the theta divisor E_O. (One has, $[K' : K]h(P) = (E_O \cdot E_P)$.)

Define $\rho(P)$ by:

$$\begin{aligned} 2[K' : K]\rho(P) &= -(E_P - E_O + \phi_P)^2 \\ &= -(E_P^2 + E_O^2 - 2(E_P \cdot E_O) - \phi_P^2). \end{aligned}$$

One has

$$\begin{aligned} |\rho(P) - h(P)| &= \left|\rho(P) - \frac{(E_P \cdot E_O)}{[K' : K]}\right| \\ &= \frac{\deg(f_*\omega_{X'/C'})}{[K' : K]} - \frac{\phi_P^2}{2[K' : K]} \end{aligned}$$

because by adjunction

$$E_P^2 = E_O^2 = -\omega_{X'/C'} \cdot E_P = -\deg(f_*\omega_{X'/C'}).$$

So we get (2) because

a) $\deg(f_*\omega_{X'/C'}) \leqslant [K' : K]\deg(\omega_{X/C})$ because 12 $\deg(f_*\omega_{X'/C'})$ is the minimal discriminant which is smaller than the discriminant of the base change $12[K' : K]\deg(f_*\omega_{X/C})$

b) $-\phi_P^2 \leqslant A[K' : K]$ (by Lemma 10).

To obtain (1) note that at the generic fiber one has

$$[nP] = n(P - O) + O$$

where nD is the divisor D multiplied by n and $[nP]$ is the point n times P in the group $X_K(\overline{K})$. Thus $E_{[nP]} - E_O + \phi_{[nP]}$ and $n(E_P - E_O + \phi_P)$ are two divisors of degree absolutely zero that are the same on the generic fiber. Corollary 12 now follows from Corollary 9. Theorem 7 then follows from the original proof in [7].

COROLLARY 12. *We have*

$$\mathrm{vol}(NS(X)) \geqslant 2^m 2^{-r} \frac{\pi^{r/2}}{\Gamma\left(\frac{r+2}{2}\right)} 10^{-13r-23gr}(2m)^r$$

if $\deg(\Delta) < 24(g-1)$.

Proof. Note that each $n_v \geqslant 2$ for $v \in S$. Hence 2^m is a lower bound for $\prod n_v$. Also, $2m$ is a lower bound for $\deg(\Delta)$. One recognizes

$$\frac{\pi^{r/2}}{\Gamma\left(\frac{r+2}{2}\right)}$$

as the volume of the unit ball B in $\mathbb{R}^r$. Minkowski's famous theorem on points of a lattice $X_K(K)$ in a bounded symmetric convex domain B gives

For $\lambda^r \operatorname{vol}(B) = 2^r \operatorname{vol}(X_K(K))$
there is a non-zero point in $B \cap X_K(K)$.

Formula (4.1) contains a torsion term. We require an upper bound for this torsion term. It is given in the following theorem. (Note that for constant elliptic curves the torsion is bounded by $1 + 2q^{1/2} + q$ as one easily checks that torsion sections are constant.)

THEOREM 13. *Let $X \xrightarrow{f} C$ be a nonconstant pencil of elliptic curves over a curve C of genus g defined over a finite field k (with q elements) of characteristic $p > 0$. Then if K is the function field of C and p^e is the inseparability degree of the j map $C \to \mathbb{P}^1$ associated to f, one has*

$$|X(K)_{\mathrm{tor}}| \leqslant \operatorname{Sup}\left(\left(6p^e\left(\frac{2g-2}{s}+1\right)\right)^2,\ 16(q-1)^2\right)$$

where s is the degree of the conductor of $X \xrightarrow{f} C$.

Proof. Note that if f is not semi-stable, the order of a torsion point divides $4(q-1)$ (see [18]), so we are reduced to the semi-stable case. To prove this theorem we use a local argument of G. Frey as reported in [4]. This says that in the semi-stable local case, the valuation of the discriminant of the elliptic curve divided by the subgroup generated by a torsion point P of order a prime number ρ is the discriminant of the original elliptic curve multiplied or divided by ρ. Then one applies Theorem 3 to the two elliptic curves to get the result. The only trouble is that the inseperability degree of the j-map may change. We now show that this cannot happen.

(a) First suppose that the inseparability degree of the j-map is zero, i.e. the Kodaira–Spencer class is not zero. If we let S denote the set of points of C where the fiber of $f\colon X \to C$ is not smooth, one has the commutative diagram:

$$\begin{array}{ccc} X & \xrightarrow{\pi} & X' = X/\langle P\rangle \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f'} \\ C - S & = & C - S \end{array}$$

where by abuse of notation $f^{-1}(C-S))$ is again denoted S. On the level of tangent spaces one has a commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_{X/(C-S)} & \longrightarrow & T_{X/k} & \longrightarrow & f^*T_{C-S} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \| & & \\ 0 & \longrightarrow & \pi^*T_{X'/(C-S)} & \longrightarrow & \pi^*T_{X/k} & \longrightarrow & \pi^*f'^*T_{C-S} & \longrightarrow & 0 \end{array}$$

The vertical maps are not zero because the morphism π is separable (even when the order of P is divisible by the characteristic, the morphism π has general fiber finite of cardinal the order of P!) The Kodaira–Spencer map of f is:

$$\begin{array}{ccc}
T_{(C-S)} & \longrightarrow & R^1 f_* T_{X/(C-S)} \\
\Big\Vert & & \Big\downarrow \alpha \qquad R^1 f_*(\pi^* T_{X'/(C-S)}) \\
\Big\downarrow & & \qquad\qquad \Big\Vert \\
T_{(C-S)} = f'_*(\pi_* O_X \otimes f'^* T_{C-S}) & \longrightarrow & R^1 f'_* \left(\pi_* O_X \otimes T_{X'/(C-S)}\right)
\end{array}$$

The first horizontal arrow is the Kodaira–Spencer map of f, so it is non-zero by hypothesis. Because T_{C-S} is a line bundle, the map must be injective.

On the open set $C - S'$, $S \subset S'$ (of C) where the map π is etale, the vertical map X is an isomorphism, so the map

$$T_{C-S} \longrightarrow R^1 f'_*(\pi_* O_{X'} \otimes T_{X'/(C-S)})$$

is not zero. (Note that S' is closed and not equal to C because $S' - S$ is the locus where $\ker(X' \to X) \to C - S$ is etale.)

Now we can deduce what we want:

$$T_{C-S} \longrightarrow R^1 f'_*(T_{X'/(C-S)})$$

is not zero because its composition with the natural map

$$R^1 f'_*(T_{X'/(C-S)}) \longrightarrow R^1 f'_*(\pi_* O_{X'} \otimes T_{X'/(C-S)})$$

is not zero.

(b) If the Kodaira–Spencer map associated to $f\colon X \to C$ is zero, and the family is not constant, there exists a finite separable morphism

$$\pi\colon C_1 \to C$$

from a smooth curve C_1 such that X_1 (the regular minimal model of $X \underset{C}{\times} C_1$) is a pull back by $F^e_{C_1}$ where F_{C_1} is the Frobenius morphism of C_1. Here π is the map that makes points of order 5 rational. (If char $= 5$, π is the map which makes points of order 7 rational.) It follows that we will be reduced to (a) if we can prove the following lemma.

LEMMA 14. *Let X be a nonconstant elliptic curve over a function field of one variable K over a finite field k, and let P be a torsion point in $X(K)$ of prime order ℓ. Then the inseparability degree of the j-map associated to $X/\langle P\rangle$ is:*

(i) *equal to the inseparability of the j-map associated to X if $\ell \neq p$;*

(ii) *equal to $1/p$ times the inseparability of the j-map associated to X.*

Proof. Part (i) follows from the fact that the injection

prime to p-torsion in $X(K) \to$ prime to p-torsion in $X(K^{1/p})$

is a bijection (making a point of $(\ell \neq p)$-torsion rational requires a seperable field extension). For part (ii), we first note that since X and $X/\langle P\rangle$ are nonconstant, they must be ordinary. The map $X \to X/\langle P\rangle$ factors through the multiplication by p-map in X, so one gets a dual map

$$X/\langle P\rangle \xrightarrow{\alpha} X.$$

Because $X/\langle P\rangle$ is ordinary, α is purely inseparable of degree p. The relative Frobenius

$$F_X\colon X/\langle P\rangle \to (X/\langle P\rangle) \underset{K}{\otimes} K^{1/p}$$

is also purely inseparable of degree p and its kernel is a simple p-group. Hence, the intersection with ker(α) is zero or all ker(α). But, if it was zero, $X/\langle P\rangle$ would be supersingular for the kernel of multiplication by p in $X/\langle P\rangle$ would be filled up by ker(α) and ker(F). Hence, X is the pull-back of $X/\langle P\rangle$ by the Frobenius of K. This proves (ii).

Remark. The argument of (ii) proves that *the order of the p-torsion in X is bounded by p^e, the inseparability degree of the j-map*. This result is contained in the article [22] of F. Voloch.

THEOREM 15. *Let $f\colon X \to C$ denote a pencil of elliptic curves over a complete nonsingular curve of genus g defined over a finite field with q elements. Let m denote the degree of the conductor of X over C. Suppose that* Br(X) *is finite. Then one has the following bound for the Tate–Shafarevich group*:

$$|\mathrm{Br}(X)| \leqslant C(g,r) \cdot (2^{12}q)^{p^e m/2}$$

where $C(g,r)$ depends only on g and the rank r of $X(K)$.

Proof. We have already bounded all the necessary terms on the right-hand side of (4.1). It only remains to bound $P_2(X, q^{-s})$ as $s \to 1$.

First, we bound $h^2 = \dim_{\mathbb{Q}_\ell}(H^2(\overline{X}, \mathbb{Q}_\ell))$. Since the Euler–Poincaré characteristic c_2 is equal to deg(Δ), i.e., 12deg(ω), it is enough to bound

$$h^1 = h^3 = \dim_{\mathbb{Q}_\ell}(H^1(\overline{X}, \mathbb{Q}_\ell)).$$

By Lemma 4, Pic(X) = Pic(C), so that

$$\dim_{\mathbb{F}_\ell}(H^1(\overline{X}, \mu)) = \dim_{\mathbb{F}_\ell}(H^1(\mathrm{Pic}(\overline{X}), \mu_\ell)),$$

i.e., $h^1 = 2g$. Using Theorem 3 we get

$$h^2 \leqslant c_2 + 2h^1 - 2h^0 \leqslant 6p^e(2g - 2 + m) + 4g - 2.$$

By (4.1), and what we have done so far, it only remains to prove that

$$\lim_{s\to 1}\left|\frac{P_2(X,q^{-s})}{1-q^{1-s}}\right| \leqslant 2^{h_2-r}.$$

This bound follows from Deligne [3], Tate's conjecture (the number of roots of P_2 equal to q is exactly r) and the observations:

$$P_2(X,t)=\prod_{i=1}^{h_2}(1-\alpha_i t),$$

where $|\alpha_i| = q$, so that

$$|1-\alpha_i q^{-s}| \leqslant 2^{1+\epsilon}.$$

Remark. The rank r is bounded also in terms of the genus of C and the conductor (see [2]).

Acknowledgements

The authors wish to thank E. Fouvry, J. Silverman, and F. Voloch for helpful discussions.

References

1. Birch, B. J. and Swinnerton-Dyer, H. P. F.: Elliptic curves and modular functions, in *Modular Functions of One Variable IV*, Lecture Notes in Math. 476, Springer-Verlag, 1975, pp. 2–32.
2. Brumer, A.: The average rank of elliptic curves I, *Invent. Math.* **109** (1992), 445–472.
3. Deligne, P.: La conjecture de Weil 1, *Publ. Math. IHES* **43** (1974), 273–307.
4. Flexor, H. and Oesterle, J.: Points de torsion des courbes elliptiques, in L. Szpiro (ed.), *Pinceaux de Courbes Elliptiques*, Asterisque 183 (1990), 25–36.
5. Goldfeld, D.: Modular elliptic curves and diophantine problems, in *Number Theory*, Proc. Conf. of the Canad. Number Theory Assoc., Banff, C Alberta, Canada, 1988, pp. 157–176.
6. Gross, B. H.: Kolyvagin's work on elliptic curves, in *L-functions and Arithmetic*, Proc. of the Durham Symp., 1989, pp. 235–256.
7. Hindry, M. and Silverman, J. H.: The canonical height and integral points on elliptic curves, *Invent. Math.* **93** (1988), 419–450.
8. Kolyvagin, V.A.: Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a class of Weil curves, *Izv. Akad. Nauk SSSR* **52** (1988).
9. Kohnen, W. and Zagier, D. B.: Values of L-series of modular forms at the centre of the critical strip, *Invent. Math.* **64** (1981), 175–198.
10. Lang, S.: Conjectured diophantine estimates on elliptic curves, in *Arithmetic and Geometry*, Papers dedicated to I.R. Shafarevich on the occasion of his sixtieth birthday, Vol. I, Arithmetic, Birkhäuser, 1983, pp. 155–172.
11. Mazur, B.: Modular curves and the Eisenstein ideal, *IHES Publ. Math.* **47** (1977), 33–186.
12. Milne, J. S.: On a conjecture of Artin and Tate, *Annals of Math.* **102** (1975), 517–533.
13. Pesenti, J. and Szpiro, L.: Discriminant et conducteur des courbes elliptiques non semi-stable, à paraitre.
14. Rubin, K.: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, *Invent. Math.* **64** (1981), 455–470.

15. Silverman, J.: *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106, Springer-Verlag, 1986.
16. Szpiro, L.: Propriétés numériques du faisceau dualisant relatif, in *Pinceaux de Courbes de Genre au Moins Deux*, Asterisque 86 (1981), 44–78.
17. Szpiro, L.: Discriminant et conducteur, in *Seminaire sur les Pinceaux de Courbes Elliptiques*, Asterisque 183 (1990), 7–17.
18. Tate, J.: An algorithm for determining the type of a singular fiber in an elliptic pencil, in *Modular Functions of One Variable IV*, Lecture Notes in Math. 476, Springer-Verlag, 1975, pp. 33–52.
19. Tate, J.: On a conjecture of Birch and Swinnerton-Dyer and a geometric analogue, *Seminaire N. Bourbaki*, Exposé 306, 1966.
20. Taylor, R. and Wiles, A.: Ring theoretic properties of certain Hecke algebras, to appear.
21. Titchmarsh, E. C.: *The Theory of Functions*, 2nd edn., Oxford University Press, Oxford, 1939.
22. Voloch, F.: On the conjectures of Mordell and Lang in positive characteristic, *Inventiones Math.* **104** (1991), 643–646.
23. Weil, A.: *Basic Number Theory*, Springer-Verlag, 1967.
24. Wiles, A.: Modular elliptic curves and Fermat's last theorem, to appear.