ANALOGUES OF LEHMER’S PROBLEM IN POSITIVE CHARACTERISTIC

AMÍLCAR PACHECO

Abstract. Let $C$ be a smooth projective irreducible curve defined over a finite field $\mathbb{F}_q$ and $K = \mathbb{F}_q(C)$. We show that every non-torsion element $\alpha \in \overline{K}$ of degree $d$ over $K$ of a Drinfeld $A$-module $\phi$ defined over $K$ has canonical height $\hat{h}_\phi(\alpha)$ at least $1/d$. Similarly, if $E/K$ is a non-constant elliptic curve defined over a function field $K = l(C)$ of a curve $C$ defined over an algebraically closed field $l$ of characteristic 0 or $p > 3$, we show that every point of infinite order $P \in E(\overline{K})$ of degree $d$ over $K$ has canonical height $\hat{h}_E(P)$ at least $c/d$, where $c$ depends only on the degree of the $j$-map associated to $E/K$.

1. Introduction

Let $\alpha$ be an algebraic number of degree $d$ over $\mathbb{Q}$ and suppose it is not a root of unity. Let $h : \mathbb{Q} \to \mathbb{R}$ be the absolute logarithmic height. Lehmer’s conjecture consists in asking for an absolute real constant $c > 0$ such that $h(\alpha) \geq \frac{c}{d}$.

Although this question remains open, analogues of this conjecture have been considered in other contexts. Let $E$ be an elliptic curve defined over a number field $K$, $j_E$ its $j$-invariant, $\overline{K}$ the algebraic closure of $K$, $P \in E(\overline{K})$ a point of infinite order and $\hat{h}_E : E(\overline{K}) \to \mathbb{R}$ its canonical height. Let $K(P)$ be the field generated over $K$ by the coordinates of $P$, $d = [K(P) : K]$ and $D = [K : \mathbb{Q}]$. In [4 Corollary 0.2] it is shown that if $j_E$ is non-integral, then there exists $c > 0$ depending on $E/K$ such that $\hat{h}_E(P) \geq \frac{c}{d(\log d)^2}$. Let $h = \max\{1, h(j_E)\}$. This result was improved in [4 Corollary 1.4], where it was proved that there exist absolute effective computable real constants $c_5, c_6 > 0$ such that $\hat{h}_E(P) \geq c_5 h(dD)^{-3} \left(1 + \frac{\log(dD)}{h}\right)^{-2}$, if $j_E$ is integral, and $\hat{h}_E(P) \geq c_6 D^{-3} d^{-15/8} h^{-2} \left(1 + \frac{\log(dD)}{h}\right)^{-2}$, otherwise. In section 3 we prove an analogue of this result for non-constant elliptic curves over function fields over algebraically closed fields of characteristic 0 or $p > 3$.

Let $C$ be a smooth irreducible projective curve defined over a finite field $\mathbb{F}_q$ of $q$ elements and $K = \mathbb{F}_q(C)$. The direct translation of Lehmer’s conjecture to $K$ is trivial, because the requirement that $\alpha$ is not a root of unity is equivalent to $\alpha \in K - \mathbb{F}_q$, thus there is a discrete valuation $v : K \to \mathbb{Z} \cup \{\infty\}$ of $K$ such that $v(\alpha) < 0$ and therefore $h(\alpha) \geq \frac{1}{d}$.

Another instance of the Lehmer problem is to consider the canonical height $\hat{h}_\phi : \overline{K} \to \mathbb{R}$ of a Drinfeld $A$-module $\phi : A \to K\{\tau\}$ of rank $r$ defined over a $K = \mathbb{F}_q(C)$. We also have a notion of torsion elements in this context and we ask for a constant $c$ depending on $\phi$ such that for every non-torsion element $\alpha \in \overline{K}$

Date: March 1, 2022.

This work was partially supported by CNPq research grant 300896/91-3 and Pronex #41.96.0830.00.
with \([K(\alpha) : K] = d\) we have \(\hat{h}_\phi(\alpha) \geq \frac{1}{d}\). We prove this in section 2 starting with 
the case where \(K = \mathbb{F}_q(T)\) is the rational function field over \(\mathbb{F}_q\) and \(A = \mathbb{F}_q[T]\).

The general result is then deduced from this case. Analogues of this type of result 
were proved in [3].

2. DRINFELD MODULES

Let \(A = \mathbb{F}_q[T]\) be the polynomial ring in one variable over the finite field \(\mathbb{F}_q\) of \(q\) elements, \(k = \mathbb{F}_q(T)\) its field of fractions and \(\phi : A \to \text{End}_k(\mathbb{G}_a) \cong k\{\tau\}\) a Drinfeld 
\(A\)-module of rank \(r\) defined over \(k\) with respect to the inclusion \(A \subset k\). Denote 
\(\phi_T = T + a_1 \tau + \ldots + a_r \tau^r\).

Let \(\overline{k}\) be the algebraic closure of \(k\) and \(h : \overline{k} \to \mathbb{R}\) the absolute logarithmic Weil 
height. The global height of the Drinfeld module \(\phi\) at \(\alpha \in \overline{k}\) is defined by (cf. [2] §2)

\[
\hat{h}_\phi(\alpha) = \lim_{n \to \infty} \frac{h(\phi_T^n(\alpha))}{q^{nr}}.
\]

Analogously to the case of elliptic curves this global height decomposes in a sum of 
local heights which are defined as follows. Let \(L = k(\alpha)\) and \(M_L\) the set of places 
of \(L\) normalized so that they correspond to discrete valuations \(v : L \to \mathbb{Z} \cup \{\infty\}\). Let 
\(d_v\) be the degree of \(v\) and \(d = [L : k]\). The local height of \(\alpha\) at \(v\) with respect 
to \(\phi\) is defined by (cf. [2] §4)

\[
\hat{h}_{\phi,v}(\alpha) = -\frac{d_v}{d} \lim_{n \to \infty} \min \{0, v(\phi_T^n(\alpha))\}/q^{nr}.
\]

It follows from the above definitions that

\[
(2.1) \quad \hat{h}_\phi(\alpha) = \sum_{v \in M_L} \hat{h}_{\phi,v}(\alpha).
\]

An element \(\alpha \in \overline{k}\) is called a torsion element of \(\phi\) if there exists \(f \in A - \{0\}\) such 
that \(\phi_f(\alpha) = 0\).

**Theorem 2.1.** Let \(\alpha \in \overline{k}\) be a non-torsion element of \(\phi\) and \(d = [k(\alpha) : k]\). Then 

\[
\hat{h}_\phi(\alpha) \geq \frac{1}{d}.
\]

**Proof.** Let \(S \subset M_L\) be the set consisting of the poles of \(T = a_0, a_1, \ldots, a_r\) and 
the zeros of \(a_r\). Suppose there exists \(v \notin S\) such that \(v(\alpha) < 0\). Then, for every 
\(0 \leq i < d\),

\[
q^i v(\alpha) + v(a_i) = q^i v(\alpha) < q^i v(\alpha) + v(a_i),
\]

hence \(v(\phi_T(\alpha)) = q^r v(\alpha)\). By induction, for every \(n \geq 1\), we also have \(v(\phi_T^n(\alpha)) = q^{nr} v(\alpha)\), thus \(\hat{h}_{\phi,v}(\alpha) = -\frac{d_v}{d} v(\alpha) \geq \frac{1}{d} = \frac{1}{d}\).

Assume now that all the poles of \(\alpha\) lie in \(S\). Let \(v \in S\) be a pole of \(\alpha\). Let

\[
M_{\phi,v} = \min_{0 \leq i < r} \frac{v(a_i) - v(a_r)}{q^r - q^i}.
\]

Suppose \(v(\alpha) < M_{\phi,v}\) and \(v(a_r) \leq 0\). The first inequality implies \(v(\phi_T(\alpha)) = v(a_r) + q^r v(\alpha)\). The two inequalities imply

\[
q^r (q^r - q^i) v(\alpha) < (q^r - q^i) v(\alpha) < v(a_i) - v(a_r) \leq v(a_i) - v(a_r) - (q^r - q^i) v(a_r),
\]

for every \(0 \leq i < r\), i.e.,

\[
q^r v(\alpha) + (q^r + 1) v(a_r) < q^r v(\alpha) + q^r v(a_r) + v(a_i),
\]
such that

\[ H \leq \frac{q^{2r} - 1}{q^r - 1} v(a_r). \]

Hence,

\[ \psi \]

The general case.

2.1. The general case. The Lehmer problem for Drinfeld modules can be formulated in a more general set-up and its proof is reduced to that of Theorem 2.1.

Let \( C \) be a smooth projective irreducible curve defined over a finite field \( \mathbb{F}_q \) of \( q \) elements. Let \( \infty \) be a fixed place of \( K = \mathbb{F}_q(C) \), the ring of functions in \( K \) which are regular everywhere except at \( \infty \), \( v_\infty : K \to \mathbb{Z} \cup \{ \infty \} \) the normalized discrete valuation associated to \( \infty \) and \( d_\infty \) the degree of \( \infty \). For any \( a \in A \), let \( \deg(a) = -d_\infty v_\infty(a) \). The field \( K \) is an \( A \)-module with respect to the inclusion \( A \subset K \). A Drinfeld \( A \)-module of rank \( r \) defined over \( K \) is a ring homomorphism

i.e.,

\[ v(\phi_T^r(a)) = q^{2r}v(a) + (q^r + 1)v(a_r) = q^{2r}v(a) + \frac{q^{2r} - 1}{q^r - 1} v(a_r). \]

Suppose we have proved that for every integer \( 1 \leq m < n \) we have

\[ v(\phi_T^m(a)) = q^{mr}v(a) + \frac{q^{mr} - 1}{q^r - 1} v(a_r). \]

Then

\[ q^r(q^r - q^i)v(\phi_{T^r - 2}(a)) \]

\[ = q^r(q^r - q^i)(q^{(n-2)r}v(a) + (q^{(n-3)r} + \ldots + q^r + 1)v(a_r)) \]

\[ \leq q^{(n-1)r}(q^r - q^i)v(a) < (q^r - q^i)v(a) < v(a_i) - v(a_r) \]

\[ \leq v(a_i) - v(a_r) - (q^r - q^i)v(a_r). \]

Thus,

\[ v(\phi_{T^r}(a)) = q^{nr}v(a) + (q^{(n-1)r} + \ldots + q^r + 1)v(a_r) \]

\[ < q^{(n-1)r} + v(a) + (q^{(n-2)r} + \ldots + q^r + q^i)v(a_r) + v(a_i), \]

i.e.,

\[ v(\phi_{T^r}(a)) = q^{nr}v(a) + (q^{(n-1)r} + \ldots + q^r + 1)v(a_r) = q^{nr}v(a) + \frac{q^{mr} - 1}{q^r - 1} v(a_r). \]

Hence,

\[ \hat{h}_{\phi,v}(\alpha) = -\frac{d}{d} \left( v(\alpha) + \frac{1}{q^r - 1} v(a_r) \right) \geq \frac{1}{d}. \]

Suppose now that \( v(\alpha) < M_{\phi,v} \), but \( v(a_r) > 0 \). Let \( \xi \) be a sufficiently negative power of a local parameter at \( v \) so that \( v(\xi q^{-1} a_r) \leq 0 \). The Drinfeld module \( \psi = \xi^{-1} \phi \xi \) is isomorphic to \( \phi \) and by [2] Proposition 2 \( \hat{h}_{\psi,v} = \hat{h}_{\psi,v} \). Note that

\[ \psi_T = T + \xi q^{-1} \alpha_1 \tau + \ldots + \xi q^{-1} \alpha_r \tau^r. \]

Then for every \( 0 \leq i < r \) we have

\[ (q^r - q^i)v(a) < v(a_i) - v(a_r) < v(a_i) - v(a_r) - v(\xi)(q^r - q^i) = v(\xi^{-1} a_i) - v(\xi^{-1} a_r), \]

in particular, \( v(\alpha) < M_{\psi,v} \). By the argument of the last paragraph we conclude that \( \hat{h}_{\psi,v}(\alpha) = \hat{h}_{\psi,v}(\alpha) \geq \frac{1}{d} \).

If \( v(\alpha) \geq M_{\phi,v} \), let \( \xi \) be a sufficiently positive power of a local parameter at \( v \) such that

\[ M_{\psi,v} = \min_{0 \leq i < r} \frac{v(a_i \xi^{-1} q^i) - v(a_r \xi^{-1} q^i)}{q^r - q^i} = \min_{0 \leq i < r} \left( \frac{v(a_i) - v(a_r)}{q^r - q^i} + v(\xi) \right) > v(\alpha). \]

Once again we take the Drinfeld module \( \psi = \xi^{-1} \phi \xi \) which is isomorphic to \( \phi \). By the two last cases and [2] Proposition 2 we conclude that \( \hat{h}_{\psi,v}(\alpha) = \hat{h}_{\psi,v}(\alpha) \geq \frac{1}{d} \).

By the non-negativity of the local canonical heights we conclude that \( \hat{h}_{\psi,v}(\alpha) \geq \frac{1}{d} \).
ϕ : A → \text{End}_K(G_a) \cong K}\{τ\} such that for every a ∈ A, deg(ϕ_a) = q^{r \deg(a)} and the constant term of \(\phi_a\) is a itself.

Let a ∈ A − \mathbb{F}_q. The global height of a ∈ K is defined as (cf. [2 §2])

\[
\hat{h}_\phi(α) = \lim_{n \to \infty} \frac{h(\phi_{\alpha^n}(α))}{\deg(\phi_{\alpha^n})}.
\]

Let L = K(α) and d = [L : K]. For every discrete valuation \(v : L \to \mathbb{Z} \cup \{\infty\}\) of degree \(d_v\) the local height is defined as (cf. [9 §4])

\[
\hat{h}_{\phi,v}(α) = \lim_{n \to \infty} -\frac{d_v}{d} \min\{0, v(\phi_{\alpha^n}(α))\}.
\]

As observed in [9 Proposition 3] these heights are independent of the choice of a ∈ A − \mathbb{F}_q.

The Dedekind domain A is a finitely generated \(\mathbb{F}_q\)-algebra. Let \(A\) the the set of generators of A as an \(\mathbb{F}_q\)-algebra, \(T \in A\), \(\deg(T) = d_T\) and \(ϕ_T = T + a_1(T)τ + \cdots + a_rτ^r\). Let α ∈ K be a non-torsion element for φ with \([K(α) : K] = d\). Replacing the \(a_i\)'s in the proof of Theorem 2.1 by the \(a_i(T)\)'s the proof of Theorem 2.1 shows that

\[
(2.2) \quad \hat{h}_\phi(α) \geq \frac{1}{d}.
\]

3. Elliptic curves

Let C be a smooth irreducible projective curve defined over an algebraically closed field l of characteristic 0 or \(p > 3\), let K = l(C) be its function field and \(\overline{K}\) its algebraic closure. Let E/K be a non-constant semistable elliptic curve defined over K, \(ϕ_E : E → C\) its minimal semi-stable regular model, \(j_E : C → \mathbb{P}^1\) the j-map induced by \(ϕ_E\) and \(\hat{h}_E : E(\overline{K}) → \mathbb{R}\) its canonical height.

Let \(P \in E(\overline{K})\) and \(L = K(P)\) the field generated by K and the coordinates of P. Let \(d = [L : K]\), \(M_L\) the set of places v of L which are normalized so that \(v : L → \mathbb{Z} \cup \{∞\}\) is the corresponding discrete valuation. Let \(L_v\) be the completion of L with respect to v and \(λ_v : E(K_v) → \mathbb{R}\) its local Néron function [11 Chapter VI]. Let \(w = v_k, e(v|w)\) the ramification index of v over w, \(w' = e(v|w)w : K → \mathbb{Z} \cup \{∞\}\) the normalization of w, \(K_w\) the completion of K with respect to w and \(n(v|w) = [L_v : K_w]\). Then

\[
(3.1) \quad \hat{h}_E(P) = \frac{1}{d} \sum_{v \in M_L} n(v|w)λ_v(P),
\]

[11] VI, Theorem 2.1].

Let \(D_{E/K}\) be the minimal discriminant of E/K and \(d_{E/K} = \text{deg}(D_{E/K})\). Since E/K is semi-stable, it follows from [10] Chapter VII, Proposition 5.1 that \(w'(D_{E/K}) = -w'(j_E)\) for every pole \(w'\) of \(j_E\), thus \(\text{deg}(j_E) = d_{E/K}\). For every v ∈ \(M_L\), let \(v^+ = \max\{v, 0\}\).

Lemma 3.1. [5 Proposition 1.3] Let A, N ≥ 1 be integers, \(Q_0, \cdots, Q_{6AN} ∈ E(L_v)\) distinct points. Then there exists \(P_0, \cdots, P_N \in \{Q_0, \cdots, Q_{6AN}\}\) such that for each i = l,

\[
λ_v(P_i - P_l) ≥ \frac{1 - A^{-1}}{12} v^+(j_E^{-1}).
\]

Proposition 3.2. \#\{Q \in E(L) | \hat{h}_E(Q) < \frac{d_{E/K}}{96d}\} ≤ 24.
Proof. Denote \( S = \{ Q \in E(L) \mid \hat{h}_E(Q) < \frac{d_{E/K}}{96d} \} \) and suppose \( \# S > 24 \). Let \( A = 2 \) and \( N + 1 = \left\lceil \frac{\# S}{12} \right\rceil > 1 \) the integral part of \( \frac{\# S}{12} \), then \( 1 < N + 1 \leq \frac{\# S}{12} \). So we can choose \( 12N + 1 \) distinct points \( P_0, \cdots, P_{12N+1} \in S \). By Lemma 5.1 there exist \( P_0, \cdots, P_N \in \{ Q_0, \cdots, Q_{12N+1} \} \) such that \( \lambda_v(P_i - P_l) \geq \frac{1}{24} v^{-}(j_E^{-1}) \) for \( i \neq l \). It follows from the triangle inequality that

\[
(3.2) \quad H = \max_{Q \in S} \hat{h}_E(Q) \geq \max_{1 \leq i \leq N} \hat{h}(P_i) \geq \frac{1}{4N(N+1)} \sum_{i \neq l} \hat{h}_E(P_i - P_l).
\]

Hence, by (3.1) and (3.2),

\[
(3.3) \quad H \geq \frac{1}{4N(N+1)d} \sum_{i \neq l} \sum_{v \in M_{K}} n(v|w) \lambda_v(P_i - P_l) \geq \frac{1}{96d} \sum_{v \in M_{K}} n(v|w) v^{+}(j_E^{-1})
\]

\[
= \frac{1}{96d} \sum_{w' \in M_{K}} \sum_{v|w} \frac{n(v|w)}{e(v|w)} w'^{+}(j_E^{-1}) \geq \frac{1}{96d} \sum_{w' \in M_{K}} w'^{+}(j_E^{-1}) = \frac{d_{E/K}}{96d}.
\]

\[ \square \]

Remark 3.3. We used the fact that \( l \) is algebraically closed just to ensure that the poles of \( j_E \) have all degree 1.

As a consequence of Proposition 3.2 we obtain a theorem which simultaneously deals with the Lehmer and the Lang problems for elliptic curves over function fields. Recall that the Lang problem is to find a constant \( c > 0 \) depending on \( E/K \) such that for every non-torsion point \( P \in E(K) \) we have \( \hat{h}_E(P) \geq cd_{E/K} \).

Theorem 3.4. Let \( P \in E(K) \) be a non-torsion point of \( E/K \) and \( d = [K(P) : K] \). Then there exists an absolute real constant \( c > 0 \) such that \( \hat{h}_E(P) \geq c d_{E/K} \).

Proof. Suppose \( \hat{h}_E(P) < \frac{d_{E/K}}{96d} \). Then for every \( 1 \leq n \leq 25 \), \( \hat{h}_E(nP) = n^2 \hat{h}_E(P) < \frac{d_{E/K}}{96d} \), which contradicts Proposition 3.2. So we take \( c = \frac{1}{96000} \).

\[ \square \]

Remark 3.5. The constant for the Lehmer problem is \( \frac{d_{E/K}}{96000} \) so it depends only on \( \deg(j_E) = d_{E/K} \), in the semi-stable case.

Remark 3.6. In [6] Theorem 0.2] Hindry and Silverman proved Lang’s conjecture for function fields over algebraically closed fields of characteristic 0. In the case where \( d_{E/K} \geq 24(g - 1) \), where \( g \) denotes the genus of \( K \), they obtained an absolute constant \( c \). However, our constant is greater than theirs, thus improving the result. In the case where \( d_{E/K} < 24(g - 1) \), their constant depends exponentially on \( g \), whereas ours is absolute and improves the constant part of their bound. Nevertheless, we have just proved Lang’s conjecture in the case of semi-stable elliptic curves. Inspired on [6] Theorem 0.2] we had previously proved Lang’s conjecture for semi-stable elliptic curves over function fields of positive characteristic [7] Theorem 5] using [5] Proposition 1.2]. First, the bounds we obtained there do not have absolute constants, they depended not only on \( g \) but also on the inseparable degree of \( j_E \). Furthermore, the present bound improves their constant parts. The reason for obtaining an absolute constant is that [5] Proposition 1.3] gives a lower bound which depends only on the choice of a positive integer \( A \), however the lower bound of [5] Proposition 1.2] depends on the number \( N + 1 \) of points \( P_0, \cdots, P_N \) chosen in \( E(L_v) \) (cf. [7] proof of Proposition 3)].
Another consequence of Proposition 3.2 is a bound for the order of the torsion group \( E(K)_{\text{tor}} \).

**Corollary 3.7.** \( \#E(K)_{\text{tor}} \leq 24 \).

**Remark 3.8.** Previous bounds for the torsion of elliptic curves over function fields in characteristic 0 were obtained in [6] Theorem 7.2 and in the case of characteristic \( p \), Goldfeld and Szpiro treated the case where \( C \) is defined over a finite field [4] Theorem 13, but the result extends to algebraically closed fields of characteristic \( p > 3 \) and we also obtained a bound (cf. [7] Theorem 7) using [4] Proposition 3. In the case of characteristic 0, the upper bound depended on \( d_{E/K} \). Using Szpiro’s theorem on the minimal discriminant of elliptic curves over function fields [13] Théorème 1, i.e., \( d_{E/K} \leq 6p^e(2g - 2 + f_{E/K}) \), where \( p^e \) is the inseparable degree of \( j_E \) and \( f_{E/K} \) is the degree of the conductor divisor of \( E/K \), it follows an upper bound whose constant part is worse than the bound of Corollary 3.7. The bounds in characteristic \( p \) (in the semi-stable case) were \( \sigma_{E/K}^2 \), respectively \( 2\sigma_{E/K}^2 \), where \( \sigma_{E/K} = \frac{d_{E/K}}{f_{E/K}} \). If \( d_{E/K} \geq 24p^e(g - 1) \), then (using again [13] Théorème 1) \( \sigma_{E/K} \leq 12p^e \) and otherwise \( \sigma_{E/K} \leq d_{E/K} < 24p^e(g - 1) \). Not only is the bound of Corollary 3.7 absolute, but also it is better than the estimates for \( \sigma_{E/K}^2 \).

### 3.1. Integral points

Theorem 3.4 and Corollary 3.7 imply as in [6] §8 an upper bound for the number of integral points of an \( S \)-minimal Weierstrass equation of \( E/K \).

Let \( S \) be a finite set of places of \( K \) and \( R_S \subset K \) the ring of \( S \)-integers. For every \( a \in K \) let \( h_K(a) = [K : l(a)] \). A Weierstrass equation \( y^2 = x^3 + Bx + C \) with discriminant \( \Delta \) is called \( S \)-minimal if \( h_K(\Delta) \) is minimal subject to \( f(x) \in R_S[x] \). Let \( \delta = \min \{ h_E(P) \mid P \in E(K) \cap E(R_S) \} \) and \( \epsilon = \max \{ h_E(P) \mid P \in E(R_S) \} \). In [12] Lemma 1.2 (a) it is shown that \( \#E(R_S) \leq \#E(K)_{\text{tor}}(1 + 2\sqrt{\epsilon})^r_E \), where \( r_E \) denotes the rank of \( E(K) \). It follows from [7] Remark 14 that

\[
\epsilon \leq p^e(12g + 4\#S + 5d_{E/K}).
\]

**Theorem 3.9.** Let \( y^2 = x^3 + Bx + C \) be an \( S \)-minimal Weierstrass equation for \( E/K \). If \( d_{E/K} \geq 24p^e(g - 1) \), then \( \#E(R_S) \leq 24(2299\sqrt{p^e\#S})^r_E \), otherwise \( \#E(R_S) \leq 24(2021\sqrt{p^e\#S})^r_E \).

**Proof.** By Theorem 3.4 \( \delta \geq \frac{d_{E/K}}{60000} \). If \( d_{E/K} \geq 24p^e(g - 1) \), then \( g \leq \frac{d_{E/K}}{24p^e} + 1 \). Thus, since \( \#S \geq 1 \),

\[
\frac{\epsilon}{\delta} \leq 60000 \frac{p^e}{d_{E/K}}(12g + 4\#S + 5d_{E/K})
\]

\[
\leq 60000p^e \left( 12 \left( \frac{1}{24p^e} + 1 \right) + 9\#S \right)
\]

\[
\leq 1320000p^e\#S.
\]

The first statement follows from (3.5) and Corollary 3.7.

Suppose now that \( d_{E/K} < 24p^e(g - 1) \). In this case, since \( \#S \geq 1 \) and \( g \geq 2 \), we have

\[
\frac{\epsilon}{\delta} \leq 60000 \frac{p^e}{d_{E/K}}(12g + 4\#S + 5d_{E/K}) \leq 60000p^e(12g + 9\#S)
\]

\[
\leq 1020000p^e g\#S.
\]
The second statement follows from (3.6) and Corollary 3.7.

Remark 3.10. The bound of Theorem 3.9 improves the bounds of [8, Theorem 8.1] in the case of characteristic 0 when $d_{E/K} \geq 24(g - 1)$. When $d < 24(g - 1)$ we also have an improvement of the constant part (which does not depend on the rank $r_E$ of $E(K)$) if $g \geq 3$. Note that in this latter case, the constant part of their bound depends on $g$, whereas ours does not. In both cases the bound of Theorem 3.9 improves that of [7, Theorem 15].

3.2. Lehmer problem : the general case. If we no longer suppose that $E/K$ is a semi-stable elliptic curve, then $\deg(j_E) < d_{E/K}$ (cf. [10, Chapter VII, Proposition 5.1]). In this case, instead of Proposition 3.2, we need to bound the cardinality of a smaller set

$$\# \left\{ Q \in E(L) ; \hat{h}_E(Q) < \frac{\deg(j_E)}{96d} \right\} \leq 24.$$  

As a consequence, Theorem 3.9 is replaced by: for every non-torsion point $P$ of $E$ of degree $d$ over $K$ we have $\hat{h}_E(P) \geq \frac{c'}{d}$, where $c' = \frac{\deg(j_E)}{6000}$. We cannot obtain Lang’s conjecture as in Theorem 3.4, because Lemma 3.1 involves $v^+(j_E^{-1})$, hence the proof of Proposition 3.2 only gives $\deg(j_E)$ and not $d_{E/K}$.

3.3. Integral points : the general case. The bound of (3.7) also implies that $\#E(K)_{\text{tor}} \leq 24$. Note that in the general case

$$f_{E/K} < 2\#\{\text{poles of } j_E\} \leq 2\deg_s(j_E),$$

where $\deg_s(j_E)$ denotes the separable degree of $j_E$.

Theorem 3.11. Let $y^2 = x^3 + Bx + C$ be an $S$-minimal Weierstrass equation for $E/K$. If $d_{E/K} \geq 24p^e(g - 1)$, then $\#E(R_S) \leq 24(13788\sqrt{gp^eS})^{r_E}$, otherwise $\#E(R_S) \leq 24(12121g\sqrt{gp^eS})^{r_E}$.

Proof. If $d_{E/K} \geq 24p^e(g - 1)$, then

$$\frac{\epsilon}{\delta} \leq 60000 \frac{p^e}{\deg(j_E)} (12g + 4\#S + 5d_{E/K})$$

$$\leq 60000 \frac{p^e}{\deg(j_E)} \left( \frac{d_{E/K}}{2p^e} + 12 + 9d_{E/K} \#S \right)$$

$$\leq 132000 \frac{p^e}{\deg(j_E)} d_{E/K} \#S.$$  

Szpiro’s discriminant theorem [13, Théorème 1] was first proved in the case of semi-stable elliptic curves. However, this result was extended by Pesenti and Szpiro to any elliptic curve [8, Théorème 0.1]. It follows from [8, Théorème 0.1], (3.8) and $f_{E/K} < 2\deg_s(j_E)$ that

$$\frac{\epsilon}{\delta} \leq 7920000 \frac{p^{2e}}{\deg(j_E)} (2g - 2 + f_{E/K}) \#S$$

$$\leq 23760000 \frac{p^{2e}}{\deg(j_E)} f_{E/K} \#S \leq 47520000p^e g \#S.$$  

The result now follows from (3.9) and $\#E(K)_{\text{tor}} \leq 24$. 


Suppose now that \(d_{E/K} < 24p^e(g - 1)\), then
\[
\frac{\epsilon}{\delta} \leq 60000 \frac{p^e}{\deg(j)} (12g + 4\#S + 5d_{E/K}) \leq 1020000 \frac{p^e}{\deg(j)} gd_{E/K} \#S
\]
\[
\leq 6120000 \frac{p^{2e}}{\deg(j)} g(2g - 2 + f_{E/K}) \#S \leq 18360000 \frac{p^{2e}}{\deg(j)} g^2 f_{E/K} \#S
\]
\[
\leq 36720000 p^e g^2 \#S.
\]

The result now follows from (3.10) and \(#E(K)_{\text{tor}} \leq 24\). \(\square\)

**Remark 3.12.** Observe that the bounds of Theorem 3.11 are worse than those of Theorem 3.9.

**References**

[1] S. David, *Points de petite hauteurs sur les courbes elliptiques*, J. Number Th. 64 (1997), 104-129.

[2] L. Denis, *Hauteurs canoniques et modules de Drinfeld*, Math. Ann. 294 (1992), 213-223.

[3] L. Denis, *Problème de Lehmer en caractéristique finie*, Compositio Math. 98 (1995), 167-175.

[4] D. Goldfeld, L. Szpiro, *Bounds for the Tate-Shafarevich group*, Compositio Math. 86 (1995), 71-87.

[5] M. Hindry, J. Silverman, *On Lehmer’s conjecture for elliptic curves*, in Sémin. Th. Nombres Paris, 1988-1989, Prog. Math. 91 (1990), 103-166.

[6] M. Hindry, J. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. 91 (1998), 419-450.

[7] A. Pacheco, *Integral points on elliptic curves over function fields of positive characteristic*, Bull. Aust. Math. Soc. 58 (1998), 353-357.

[8] J. Pesenti, L. Szpiro, *Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques*, Compositio Math. 120 (2000), 83-117.

[9] B. Poonen, *Local height functions and the Mordell-Weil theorem for Drinfeld modules*, Compositio Math. 97 (1995), 349-368.

[10] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[11] J. Silverman, *Advanced Topics on the Arithmetic of Elliptic Curves*, Springer-Verlag, 1994.

[12] J. Silverman, *A quantitative version of Siegel’s theorem: integral points on elliptic curves and Catalan curves*, J. Reine Angew. Math. 378 (1987), 60-100.

[13] L. Szpiro, *Discriminant et conducteur d’une courbe elliptique*, Astérisque 86 (1990), 7-18.