BULLETIN DE LA S. M. F.

D. W. MASSER

Counting points of small height on elliptic curves

Bulletin de la S. M. F., tome 117, n° 2 (1989), p. 247-265

<http://www.numdam.org/item?id=BSMF_1989__117_2_247_0>

Bull. Soc. math. France,
117, 1989, p. 247–265.

COUNTING POINTS OF SMALL HEIGHT ON ELLIPTIC CURVES

BY

D. W. MASSER (*)

RÉSUMÉ. — Soit k un corps de nombres et soit E une courbe elliptique définie sur k. On prouve un résultat d'énumération qui donne, entre autre, l'existence d'une constante positive C, effectivement calculable en fonction de k et de E, avec la propriété suivante. Pour chaque extension K de k de degré relatif au plus D (≥ 2), la hauteur canonique absolue logarithmique de chaque point d'ordre infini de $E(K)$ est au moins $CD^{-3}(\log D)^{-2}$.

ABSTRACT. — Let k be a number field and let E be an elliptic curve defined over k. We prove a counting result which gives, among other things, the existence of a positive constant C, effectively computable in terms of k and E, with the following property. For any extension K of k of relative degree at most D (≥ 2), the absolute logarithmic canonical height of any non-torsion point of $E(K)$ is at least $CD^{-3}(\log D)^{-2}$.

1. Introduction

Let k be a number field, let g_2, g_3 be elements of k with $g_2^3 \neq 27g_3^2$, and let E be the elliptic curve defined by

$$y^2 = 4x^3 - g_2x - g_3.$$

We view E as a complete variety in complex projective space $\mathbb{P}_2(\mathbb{C})$ in the usual way, and for a subfield K of $\mathbb{C}$ containing k we use the standard notation $E(K)$ for the group of points on E defined over K. Let $\bar{k}$ be the algebraic closure of k. For a point P in $E(\bar{k})$ we define the Weil height $h(P)$ as the absolute logarithmic height of the corresponding projective point (see for example [S' p. 215]). We also write $q(P)$ for the associated Néron–Tate height

$$q(P) = \lim_{n\to\infty} \frac{h(2^nP)}{4^n}.$$

(*) Texte reçu le 16 février 1988 , révisé le 10 octobre 1988.
D. W. MASSER, University of Michigan, Department of Mathematics, Ann Arbor, Michigan 48109-1003, U.S.A .

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037-9484/1989/247/$ 5.00

For a positive integer D let K be an extension of k with relative degree $[K:k]$ not exceeding D. The elliptic analogue of a famous question of LEHMER (see for example [AM p. 24]) asks whether there exists a positive constant c, depending only on k, g_2, g_3 but not on D or K, such that

$$q(P) \geq \frac{c}{D} \tag{1.1}$$

for all non-torsion P in $E(K)$. This has not yet been answered (and neither has the original question); however, it is known that inequalities similar to (1.1) are valid. For convenience assume henceforth that $D \geq 3$. Then it was proved in [AM] that

$$q(P) \geq \frac{c}{D^{10}(\log D)^6} \tag{1.2}$$

for all such P; and if E has complex multiplication this was improved to

$$q(P) \geq \frac{c}{D^3(\log D)^2}. \tag{1.3}$$

SILVERMAN [S] further sharpened (1.2) to $q(P) \geq cD^{-2}$, but only in the case that K is an abelian extension of k. Finally LAURENT [L] greatly improved (1.3) (for complex multiplication) to

$$q(P) \geq \frac{c}{D}\Big(\frac{\log\log D}{\log D}\Big)^3; \tag{1.4}$$

this is rather close to (1.1). One may also refer to an interesting conditional result of HINDRY [H p. 90]).

In the present paper we shall extend (1.3) to all elliptic curves, whether there is complex multiplication or not. This will be a consequence of our Theorem below, which gives a reasonable upper bound for the number of P in $E(K)$, torsion as well as non-torsion, that fail to satisfy (1.1) for a suitably small constant c. Another consequence is that we recover the lower bounds of [M] for the degrees of the division fields associated with E.

In addition, all our results will be made explicit in their dependence on g_2 and g_3. After the work [C] of Paula COHEN, this is a fairly straightforward matter. Let $w \geq 1$ (standing for log Weierstrass) be an upper bound for the absolute logarithmic height of the point in projective space with coordinates 1, g_2, g_3; this relatively unsophisticated measure suffices for our purposes. We can now state our main result.

THEOREM. — *There is a positive effective constant C, depending only on the degree of k, such that for any $D \geq 1$ and any extension K of k of relative degree at most D, the number of points P in $E(K)$ with*

$$q(P) < \frac{1}{CD}$$

is at most $C\sqrt{w}D(w + \log D)$.

From this we deduce the following consequences.

COROLLARY 1. — *There is a positive effective constant C_1, depending only on the degree of k, such that*

$$q(P) \geq \frac{1}{C_1 w D^3 (w + \log D)^2}$$

for all non-torsion P in $E(K)$.

This implies (1.3) without any hypothesis of complex multiplication. For fixed D we recover the result of COROLLARY 1 (p. 110) of [M'], at least for elliptic curves.

COROLLARY 2. — *There is a positive effective constant C_2, depending only on the degree of k, such that the torsion subgroup of $E(K)$ has cardinality at most $C_2\sqrt{w}D(w + \log D)$.*

A slightly larger estimate was found by Paula COHEN in [C], but only for the exponent of the torsion subgroup (see also the recent work of DAVID [Da] for abelian varieties). For fixed D the estimates of COROLLARY 2 (p. 111) of [M'] give even better bounds for cardinality.

Finally for a positive integer n let $k(E_n)$ be the field obtained by adjoining to k the coordinates of all torsion points of $E(\overline{k})$ whose order divides n.

COROLLARY 3. — *There is a positive effective constant C_3, depending only on the degree of k, such that, for all n,*

$$[k(E_n) : k] \geq \frac{n^2}{C_3\sqrt{w}(w + \log n)}$$

This is the main theorem of [M] with the dependence on E made explicit.

The proofs of these results will be given in section 6 of this paper. They will be deduced from a Proposition which is proved in section 5. But first we have to record some technical preliminaries. In section 2 we recall the

concept of distance on E which was introduced in [M'], and we refine the Box Principle of [M']. Then in section 3 we prove some new asymptotic growth estimates for certain entire functions. In section 4 we complete the preliminaries and state our Proposition.

Throughout the paper, the various symbols c_1, $c_2, \ldots$ will denote unspecified positive constants that are effectively computable in terms of the appropriate quantities. For convenience we renumber the constants at the start of each section.

The research in this paper was partially supported by the National Science Foundation.

2. Distances

For this section we do not assume that g_2, g_3 are algebraic, and we consider them only as complex numbers. We recall here the distance function $r(P)$ defined in [M'] for all P in $E(\mathbb{C})$. Let T temporarily denote the tangent space of E at its origin O, and let D temporarily denote a symmetric very ample divisor on E. Then there is a Hermitian form H on T associated with D (see for example [I pp. 64-70]). For simplicity we take D as three times the origin of E; this is the polar divisor of the function y. To calculate H we identify T with $\mathbb{C}$ by means of the differential dx/y. The exponential map $\exp_E$ on $E(\mathbb{C})$ is then given in terms of the Weierstrass elliptic function $\wp$ with invariants g_2, g_3; in fact if Ω is the period lattice of $\wp$ in $\mathbb{C}$, then of course for any z not in Ω the point $\exp_E(z)$ has projective coordinates 1, $\wp(z)$, $\wp'(z)$.

If A denotes the area of any fundamental parallelogram for Ω, then we find that $H(z) = c|z|^2/A$ for an absolute constant c (depending on normalization). For us it is especially convenient to define the related quantity

$$r(z) = \frac{\pi|z|^2}{A}. \tag{2.1}$$

Then for P in $E(\mathbb{C})$ we write

$$r(P) = \inf r(z), \tag{2.2}$$

where the infimum is taken over all z with $\exp_E(z) = P$. The double use of the same symbol here should not cause any confusion.

To work with these functions it is helpful to introduce basis elements ω_1, ω_2 of Ω in such a way that $\tau = \omega_2/\omega_1 = \xi + i\eta$ lies in the standard fundamental region for the modular group. In particular $|\xi| \leq \frac{1}{2}$ and

$\eta \geq \frac{1}{2}\sqrt{3}$. This makes τ almost unique; and in fact $\eta = \Im m\, \tau$ is unique. We shall need the following Box Principle for $E(\mathbb{C})$, which generalizes that of paragraph 4 of [M']. The constants in this section will be absolute.

LEMMA 2.1. — *Given integers B, S with $1 \leq S \leq B$, and points $P_0, \ldots, P_B$ of $E(\mathbb{C})$, we can find distinct integers $b_0, \ldots, b_S$, between 0 and B, such that the points $Q_0 = P_{b_0}, \ldots, Q_S = P_{b_S}$ satisfy*

$$r(Q_i - Q_j) \leq c_1 \max\Big(\frac{S}{B}, \eta\Big(\frac{S}{B}\Big)^2\Big) \qquad (0 \leq i\ , j \leq S).$$

Proof. — Let η_0 be a positive absolute constant such that $\eta \geq \eta_0$; for example $\eta_0 = \frac{1}{2}\sqrt{3}$. Define

$$\mu = \max\Big(1, \sqrt{\frac{B}{S}}\sqrt{\frac{\eta_0}{\eta}}\Big)$$

and integers

$$N_1 = [\mu], \quad N_2 = [B/(S\mu)].$$

Clearly N_1 is a positive integer. And if $\mu = 1$ then N_2 is also a positive integer; but otherwise if $\mu \neq 1$ then

$$\frac{B}{S\mu} = \sqrt{\frac{\eta}{\eta_0}}\sqrt{\frac{B}{S}} \geq 1,$$

so N_2 is still a positive integer.

Let F be the set of complex numbers of the form $x_1\omega_1 + x_2\omega_2$ for real x_1, x_2 satisfying $0 \leq x_1, x_2 < 1$. Divide F into N_1N_2 equal subsets each congruent to the subset defined by $0 \leq x_1 < 1/N_1$, $0 \leq x_2 < 1/N_2$. Choose $z_0, \ldots, z_B$ in F with

$$\exp_E(z_b) = P_b \qquad (0 \leq b \leq B).$$

Observe that $N_1N_2 \leq B/S$, so that

$$SN_1N_2 < B + 1.$$

The classical Box Principle now shows that at least one of the subsets of F must contain at least $S + 1$ of the numbers $z_0, \ldots, z_B$; more precisely, we can find distinct integers $b_0, \ldots, b_S$, between 0 and B, such that $z_{b_0}, \ldots, z_{b_S}$ all lie in a single subset. It follows from (2.1) and (2.2) that for the points $Q_0 = P_{b_0}, \ldots, Q_S = P_{b_S}$ we have

$$r(Q_i - Q_j) < \frac{\pi}{A}\Big(\frac{|\omega_1|^2}{N_1^2} + \frac{|\omega_2|^2}{N_2^2}\Big) \qquad (0 \leq i,\ j \leq S).$$

But $A = \eta|\omega_1|^2$, and since $|\xi| \leq \frac{1}{2}$ we deduce $|\omega_2| \leq c_2\eta|\omega_1|$. Therefore

$$r(Q_i - Q_j) \leq c_3\Big(\frac{1}{\mu^2\eta} + \mu^2\eta\Big(\frac{S}{B}\Big)^2\Big) \qquad (0 \leq i,\ j \leq S). \tag{2.3}$$

Finally the definition of μ gives

$$\frac{1}{\mu^2\eta} \leq \frac{c_4}{\eta}\frac{S\eta}{B} = c_4\Big(\frac{S}{B}\Big)$$

and also

$$\mu^2\eta\Big(\frac{S}{B}\Big)^2 \leq c_5 \max\Big(\frac{S}{B}, \eta\Big(\frac{S}{B}\Big)^2\Big).$$

These together with (2.3) complete the proof of the present lemma.

3. Analytic growth

As in the preceding section, we do not assume that g_2, g_3 are algebraic numbers. Write

$$\gamma = \max\Big(\sqrt{\frac{1}{4}|g_2|}, \sqrt[3]{\frac{1}{4}|g_3|}\Big) > 0$$

and

$$\Delta = g_2^3 - 27g_3^2 \neq 0, \quad j = \frac{1728g_2^3}{\Delta}.$$

Let τ and $\eta = \Im m\,\tau$ be as before. The constants of this section will again be absolute. We shall need the inequality

$$\frac{e^{2\pi\eta}}{c_1} \leq \max(1, |j|) \leq c_1 e^{2\pi\eta}, \tag{3.1}$$

which is easily proved using the well-known Fourier series (see for example [FP p. 187]. Let $\wp(z)$ and $r(z)$ also be as before.

LEMMA 3.1. — *There exists $\theta_0(z)$ such that $\theta(z) = \gamma\theta_0(z)$ and $\tilde{\theta}(z) = \wp(z)\theta_0(z)$ are entire functions with no common zeroes and such that*

$$m(z) = \log\max\big(|\theta(z)|, |\tilde{\theta}(z)|\big)$$

satisfies

$$|m(z) - r(z)| \leq c_2\eta$$

for all complex z.

Proof. — In her thesis [C], Paula COHEN constructed $\theta_0'(z)$ such that the corresponding function $m'(z)$ satisfies

$$|m'(z)| \leq c_3 r(z) + C,$$

where C is a certain expression in g_2, g_3 (see also [FP p. 189]. The more precise asymptotic inequality of the present lemma holds only for $\theta_0(z) = e^{\beta z^2}\theta_0'(z)$, where β is in general non-zero. It can be established by modifying the arguments of [C]; compare also PROPOSITION 3.1 (p. 212) of [Da].

However, it turns out that our inequality can be deduced rather quickly from a result of ZIMMER [Z']. Because [C] is relatively inaccessible, we present this deduction here.

We start by defining $\theta_0(z)$. With ω_1, ω_2 as in the previous section write η_1, η_2 for the corresponding quasi-periods, so that $\eta_1\omega_2 - \eta_2\omega_1 = 2\pi i$. Define

$$\alpha = \frac{\eta_1\overline{\omega}_2 - \eta_2\overline{\omega}_1}{\omega_1\overline{\omega}_2 - \omega_2\overline{\omega}_1} = \frac{i}{2A}\left(\eta_1\overline{\omega}_2 - \eta_2\overline{\omega}_1\right), \quad \theta_0(z) = e^{-\alpha z^2}\left(\sigma(z)\right)^2,$$

where $\sigma(z)$ is the Weierstrass sigma function associated with the lattice Ω. Temporarily writing $z = x_1\omega_1 + x_2\omega_2$ for real x_1, x_2, and then temporarily defining z^* as $x_1\eta_1 + x_2\eta_2$, we find that $z^* = \alpha z + \pi A^{-1}\overline{z}$. Thus $\Re e(zz^*) = \Re e(\alpha z^2) + r(z)$, so that if we further write

$$\delta(z) = -\log|\sigma(z)| + \frac{1}{2}\Re e(zz^*) - \frac{1}{12}\log|\Delta|,$$

then we end up with

$$\log|\theta_0(z)| - r(z) = -2\delta(z) - \frac{1}{6}\log|\Delta|,$$

at least if z is not in Ω.

The reason for introducing δ is that, according to Theorem C (p. 243) of [Z'], it is the local Néron function on the elliptic curve E corresponding to the standard infinite valuation. In particular we can write $\delta(z) = \delta(P)$ for $P = \exp_E(z) \neq O$ on $E(\mathbb{C})$. If we also write $\wp(z) = x(P)$, and, following [Z' p. 222],

$$\mu = -\log\gamma, \quad d(P) = \frac{1}{2}\max\left(-\mu, \log|x(P)|\right),$$

then we find that

$$m(z) - r(z) = -2\left(\delta(P) - d(P) + \frac{1}{12}\log|\Delta|\right).$$

The Corollary (p. 224) of [Z'] now gives

$$|m(z) - r(z)| \leq c_4 + \frac{1}{3}|L|, \tag{3.2}$$

where $L = 6\mu + \log|\Delta|$. But $L = -\log M$ where

$$M = \frac{1}{12^6}\max\bigl(27|j|, 4|j - 1728|\bigr),$$

and clearly

$$\frac{1}{c_5}\max(1, |j|) \leq M \leq c_5 \max(1, |j|).$$

This together with (3.1) and (3.2) completes the proof of the present lemma.

We would like to point out that the possibility of having $c_2\eta$ on the right-hand side of (3.2), instead of a more complicated function of g_2 and g_3, was suggested by a remark of G. WÜSTHOLZ.

4. More preliminaries

From here onwards we assume that g_2, g_3 lie in our number field k, and we recall the parameter $w \geq 1$, which is an upper bound for the absolute logarithmic height of the point with projective coordinates ℓ, g_2, g_3. The constants of this section will depend only on the degree of k. Recall the heights h, q defined in section 1.

LEMMA 4.1. — *For all P in $E(\overline{k})$, we have*

$$|h(P) - q(P)| \leq c_1 w.$$

Proof. — This is well-known, and in fact the inequalities of [Z p. 40] show that c_1 can be taken as an absolute constant.

The following "analytic analogue" concerns the functions $m(z)$, $r(z)$ appearing in section 3.

LEMMA 4.2. — *For all complex z, we have*

$$|m(z) - r(z)| \leq c_2 w.$$

Proof. — This is immediate from inequality (3.1), LEMMA 3.1, and easy height estimates for $j = 1728g_2^3/(g_2^3 - 27g_3^2)$.

We shall also need estimates for the quantities A and γ introduced earlier.

LEMMA 4.3. — *We have*

$$A \geq \frac{1}{c_3^w}, \qquad \frac{1}{c_4^w} \leq \gamma \leq c_4^w.$$

Proof. — The inequalities for γ are immediate from height considerations. For A we note first the well-known relation

$$\Delta(\tau) = \left(\frac{\omega_1}{2\pi}\right)^{12} \Delta,$$

where

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}, \quad q = e^{2\pi i \tau}.$$

Now $|q| = e^{-2\pi\eta}$, and so (3.1) gives easily $|q| \geq c_5^{-w}$. Since τ is in the fundamental region we have $|q| \leq e^{-\pi\sqrt{3}} < 1$, and it follows that $|\Delta(\tau)| \geq c_6^{-1}|q| \geq c_7^{-w}$. But $|\Delta| \leq c_8^w$, so we deduce

$$|\omega_1| \geq \frac{1}{c_9^w}.$$

Finally, as claimed,

$$A = \eta|\omega_1|^2 \geq \frac{1}{c_3^w}.$$

Next we record the following lemma, where $h(1, \alpha_1, \ldots, \alpha_n)$ denotes the absolute logarithmic height of the point in $\mathbb{P}_n$ with algebraic projective coordinates $1, \alpha_1, \ldots, \alpha_n$. For $n = 1$ we refer to $h(1, \alpha)$ loosely as the height of α.

LEMMA 4.4. — *For $M \geq 1$, $h \geq 0$ let K be a number field of degree M generated over $\mathbb{Q}$ by algebraic numbers of heights at most h. Then we can find basis elements $\alpha_1, \ldots, \alpha_M$ of K over $\mathbb{Q}$ with*

$$h(1, \alpha_1, \ldots, \alpha_M) \leq (M-1)h.$$

Proof. — We suppose $K = \mathbb{Q}(\beta_1, \ldots, \beta_n)$ for algebraic numbers $\beta_1, \ldots, \beta_n$ of heights at most h. Writing

$$m_i = [\mathbb{Q}(\beta_1, \ldots, \beta_i) : \mathbb{Q}(\beta_1, \cdots, \beta_{i-1})] \qquad (1 \leq i \leq n),$$

we see that $m_1 \ldots m_n = M$, and we can take $\alpha_1, \ldots, \alpha_M$ as the monomials

$$\beta_1^{k_1} \cdots \beta_n^{k_n} \qquad (0 \leq k_i \leq m_i - 1\,;\ 1 \leq i \leq n).$$

Clearly

$$h(1, \alpha_1, \ldots, \alpha_M) \leq h \sum_{i=1}^{n} (m_i - 1).$$

But the inequality

$$\sum_{i=1}^{n} (m_i - 1) \leq \left(\prod_{i=1}^{n} m_i \right) - 1$$

is readily verified to hold for any real numbers $m_1 \geq 1, \ldots, m_n \geq 1$; and the lemma follows.

In the next section we shall prove the following result.

PROPOSITION. — *There is a positive effective constant C_0, depending only on the degree of k, such that for any $D \geq 1$ and any extension K of k of relative degree at most D, the number of points P in $E(K)$ with*

$$\max(Dq(P), r(P)) < \frac{1}{C_0}$$

is at most $2C_0 D(w + \log D)$.

5. Proof of Proposition

It plainly suffices to prove the Proposition under the additional assumption that K is generated over $\mathbb{Q}$ by g_2 and g_3 together with the coordinates of the points P under consideration. For then the general case follows by replacing K and k by appropriate subfields.

In this section the constants will depend only on the degree of k. We write for brevity

$$\mathcal{L} = w + \log D \geq 1.$$

If the constant C_0 of the Proposition is large enough, we shall deduce a contradiction from the existence of more than $2C_0 D\mathcal{L}$ points P satisfying the conditions of the Proposition. We shall actually work with the constant $C = C_0^{1/4}$.

Define

$$N = \left[C^2 \sqrt{wD} \right].$$

Now at most

$$N^2 \leq C^4 wD \leq C^4 D\mathcal{L} = C_0 D\mathcal{L}$$

of these points P satisfy $NP = O$; and after removing them (if any), we can suppose that for

$$S = [C^4 D\mathcal{L}]$$

there are distinct points $P_1, \dots, P_S$ in $E(K)$ such that

$$q(P_s) < \frac{1}{C^4 D}, \quad r(P_s) < \frac{1}{C^4}, \quad NP_s \neq O \qquad (1 \leq s \leq S).$$

In particular we can write

$$P_s = \exp_E(u_s) \qquad (1 \leq s \leq S)$$

with

$$|u_s|^2 < \frac{A}{\pi C^4} \qquad (1 \leq s \leq S). \tag{4.1}$$

Introduce the parameters

$$L = [C^3 wD], \qquad T = \left[\frac{Cw^2 D}{\mathcal{L}}\right],$$

and let $M = [K:\mathbb{Q}]$. Our assumptions on K, together with LEMMA 4.1, imply that it is generated over $\mathbb{Q}$ by algebraic numbers of heights at most $c_1 w$. Thus by LEMMA 4.4 we can find basis elements $\alpha_1, \dots, \alpha_M$ of K over $\mathbb{Q}$ with

$$h(1, \alpha_1, \dots, \alpha_M) \leq c_1 wM \leq c_2 wD. \tag{4.2}$$

LEMMA 5.1. — *There are rational integers $p(m, \ell_1, \ell_2)$, not all zero, of absolute values at most $\exp(c_3 C^3 w^2 D)$, such that the function*

$$f(z) = \sum_{m=1}^{M} \sum_{\ell_1=0}^{L} \sum_{\ell_2=0}^{L} p(m, \ell_1, \ell_2) \alpha_m \big(\wp(z)\big)^{\ell_1} \big(\wp(Nz)\big)^{\ell_2}$$

has a zero of order at least T at $z = u_1, \dots, u_S$.

Proof. — The number of variables $p(m, \ell_1, \ell_2)$ is

$$M(L+1)^2 > C^6 w^2 D^2 M$$

and the number of equations is

$$ST \leq C^5 w^2 D^2.$$

Since the equations are defined over a field of degree M, there is a non-trivial solution in rational integers. The heights are estimated as follows. Notice that d/dz maps the ring $\mathbb{Z}[\frac{1}{2}g_2, \wp(z), \wp'(z)]$ into itself. From this it is a standard deduction that $(d/dz)^t(\wp(z))^\ell$ is a polynomial in $\frac{1}{2}g_2, \wp(z), \wp'(z)$ of total degree at most $c_4(t+\ell)$ whose coefficients are rational integers of absolute values at most $t!\,c_4^{t+\ell}$. Also, for $n = 1$ or N, we have

$$q(nP_s) = n^2 q(P_s) < w \qquad (1 \le s \le S),$$

so that by LEMMA 4.1 the numbers $\wp(u_s)$, $\wp'(u_s)$, $\wp(Nu_s)$, $\wp'(Nu_s)$ $(1 \le s \le S)$ have heights at most $c_5 w$. Hence using for example the Proposition (p. 32) of [AM] and (4.2) we end up with the estimate

$$c_6^{wD}\, T!\, c_6^{w(T+L)}\, N^T \le \exp\bigl(c_3 C^3 w^2 D\bigr)$$

for the coefficients $p(m, \ell_1, \ell_2)$. This proves the present lemma.

For an entire function $F = F(z)$ write $M(F, R)$ for its maximum modulus on the circle defined by $|z| = R$. With $\theta_0(z)$ as in LEMMA 3.1, the function

$$F(z) = \bigl(\theta_0(z)\bigr)^L \bigl(\theta_0(Nz)\bigr)^L f(z)$$

is entire, since we have

$$(4.3) \qquad F(z) = \sum_{m=1}^{M} \sum_{\ell_1=0}^{L} \sum_{\ell_2=0}^{L} p(m, \ell_1, \ell_2) \times \alpha_m \bigl(\tilde{\theta}(z)\bigr)^{\ell_1} \bigl(\gamma^{-1}\theta(z)\bigr)^{L-\ell_1} \bigl(\tilde{\theta}(Nz)\bigr)^{\ell_2} \bigl(\gamma^{-1}\theta(Nz)\bigr)^{L-\ell_2}$$

Define

$$T' = \Bigl[\frac{C^4 w^2 D}{\mathcal{L}}\Bigr].$$

LEMMA 5.2. — *We have*

$$|F^{(t)}(u_s)| \le \frac{1}{3^{ST}} \qquad (1 \le s \le S,\ 0 \le t < T').$$

Proof. — With $U = \pi^{-1/2} C^{-2} A^{1/2}$, the function F has at least ST zeroes z satisfying $|z| \le U$, by (4.1). Hence a standard application of the maximum modulus principle gives

$$(4.4) \qquad M(F, 2U) \le \frac{1}{5^{ST}} M(F, 22U).$$

But using (4.3) together with LEMMAS 4.2, 4.3, 5.1 and the estimates $|\alpha_m| \leq c_7^{wD^2}$ $(1 \leq m \leq M)$ arising from (4.1) we find that

$$M(F, 22U) \leq \exp\bigl(c_3 C^3 w^2 D\bigr)\, c_7^{wD^2}\, c_8^{wL} \exp\left(\frac{484L(N^2+1)}{C^4}\right)$$
$$\leq \exp\bigl(c_9 C^3 w^2 D^2\bigr).$$

However,

$$ST \geq \frac{1}{2} C^5 w^2 D^2,$$

and therefore (4.4) gives

$$M(F, 2U) \leq \frac{1}{4^{ST}}.$$

Finally Cauchy's Integral Formula leads in the standard way to

$$M\bigl(F^{(t)}, U\bigr) \leq \frac{t!\, M(F, 2U)}{U^t},$$

and using LEMMA 4.3 to estimate U from below we find that

$$M\bigl(F^{(t)}, U\bigr) \leq T'! \frac{C^{2T'}\, c_{10}^{wT'}}{4^{ST}} \leq \frac{1}{3^{ST}} \qquad (0 \leq t < T').$$

This implies the present lemma.

LEMMA 5.3. — *There exist s, t with $1 \leq s \leq S$ and $0 \leq t < T'$ such that*

$$f^{(t)}(u_s) \neq 0.$$

Proof. — This is of course a zero estimate. But we cannot use the standard theory, as the points P_s have no additive structure. Neither can we use the resultant arguments of [BM], since T' is not large enough. We are forced to use the simpleminded method of [M]. Note that f is not identically zero because $N^2 \geq \frac{1}{2} C^4 wD$ whereas $L \leq C^3 wD$ (see [M p. 51]). It is an elliptic function with respect to Ω of order

$$Z \leq 2L + 2LN^2 \leq c_{11} C^7 w^2 D^2.$$

Thus it cannot have more than Z zeroes modulo Ω, and since

$$ST' \geq \frac{1}{2} C^8 w^2 D^2 > Z$$

this completes the proof.

From now on we suppose that s is chosen as in the above lemma, and that t is picked minimally for this choice of s.

LEMMA 5.4. — *We have*

$$|f^{(t)}(u_s)| \leq \frac{1}{2^{ST}}.$$

Proof. — The relation

$$f^{(t)}(u_s) = \frac{F^{(t)}(u_s)}{(\theta_0(u_s))^L(\theta_0(Nu_s))^L}$$

follows from the minimality of t. For $n = 1$ or N, LEMMA 4.2 and (4.1) show that

$$|\theta_0(nu_s)| \max\bigl(\gamma, |\wp(nu_s)|\bigr) \geq \frac{1}{c_{12}^w} \exp\left(\frac{n^2}{C^4}\right) \geq \frac{1}{c_{12}^w}.$$

But we have already seen during the proof of LEMMA 5.1 that the numbers $\wp(nu_s)$ have heights at most $c_5 w$. It follows that $|\wp(nu_s)| \leq c_{13}^{wD}$, and, since also $\gamma \leq c_{13}^w$ from LEMMA 4.3, we conclude that

$$|\theta_0(nu_s)| \geq \frac{1}{c_{14}^{wD}}.$$

The present lemma is therefore a consequence of LEMMA 5.2.

LEMMA 5.5. — *We have*

$$|f^{(t)}(u_s)| \geq \exp\bigl(c_{15} C^4 w^2 D^2\bigr).$$

Proof. — We simply estimate the height, as in the proof of LEMMA 5.1, but allowing t to go up to T' instead of T. We obtain the (exponentiated) upper bound

$$\exp\bigl(c_{16} C^3 w^2 D\bigr)\, T'!\, c_{16}^{w(T'+L)}\, N^{T'} \leq \exp\bigl(c_{17} C^4 w^2 D\bigr).$$

Since $f^{(t)}(u_s)$ is a non-zero algebraic number of degree at most $M \leq c_{18} D$, the lower bound of the present lemma is immediate.

Finally since $ST \geq \frac{1}{2} C^5 w^2 D^2$ the preceding two lemmas contradict each other if C is sufficiently large; and this completes the proof of the Proposition.

6. Proof of Theorem

Again the constants will depend only on the degree of k. Let $C_0 \geq 1$ be as in the Proposition, and let $B+1$ be the number of points P in $E(K)$ with $q(P) < \frac{1}{4}(C_0 D)^{-1}$. Call these points $P_0, \ldots, P_B$, and write $S = [2C_0 D\mathcal{L}]$ with $\mathcal{L} = w + \log D$ as before. If $B < S$ then there is nothing more to prove. So henceforth we assume that $B \geq S$.

We may therefore use LEMMA 2.1 to find distinct points $Q_0, \ldots, Q_S$ among $P_0, \ldots, P_B$ such that

$$r(Q_s - Q_0) \leq c_1 \max\Big(\frac{S}{B}, \eta\Big(\frac{S}{B}\Big)^2\Big) \quad (0 \leq s \leq S),$$

with $\eta = \Im m\, \tau$ as before. Since

$$q(Q_s - Q_0) \leq \Big(\sqrt{q(Q_s)} + \sqrt{q(Q_0)}\Big)^2 < \frac{1}{C_0 D} \qquad (0 \leq s \leq S),$$

the Proposition implies that

$$c_1 \max\Big(\frac{S}{B}, \eta\Big(\frac{S}{B}\Big)^2\Big) \geq \frac{1}{C_0}.$$

Thus we have either

$$B \leq c_1 C_0 S \quad \text{or} \quad B \leq \sqrt{c_1 C_0 \eta} S.$$

Because $\eta \leq c_2 w$ by (3.1), each of the above inequalities implies the Theorem.

The Corollaries are deduced in the usual way. Let C denote the constant of the Theorem, and suppose there exists P in $E(K)$ with

$$q(P) < \frac{1}{C^3 w D^3 \mathcal{L}^2}.$$

Let $M = [C\sqrt{w} D\mathcal{L}]$, and let m be any integer with $0 \leq m \leq M$. Then

$$q(mP) = m^2 q(P) < \frac{1}{CD},$$

so that the $M+1$ points $0, P, \ldots, MP$ of $E(K)$ satisfy the conditions of the Theorem. They therefore cannot be all distinct, and so P must be a torsion point. This proves COROLLARY 1, with $C_1 = C^3$.

COROLLARY 2 is obvious with $C_2 = C$. And finally this result applied to $K = k(E_n)$ gives the estimate

$$n^2 \leq C\sqrt{w}D(w + \log D) \tag{6.1}$$

for $D = [K:k]$. If $D > n^2$ there is nothing more to prove; otherwise $D \leq n^2$ and (6.1) yields

$$n^2 \leq 2C\sqrt{w}D(w + \log n).$$

This establishes COROLLARY 3 with $C_3 = \max(1, 2C)$. A similar argument shows that any point P of order n generates a field of degree at least $C_3^{-1}w^{-1/2}n(w + \log n)^{-1}$ over k. We can also obtain analogous lower bounds when P satisfies $nP = Q$ for some fixed non-torsion point Q; but these are of order of magnitude only $(n/\log n)^{2/3}$ as $n \to \infty$.

We conclude this paper with some miscellaneous comments. First we discuss the extent to which our estimates could be improved. For the moment regard E as fixed and D as varying. We have already seen in SECTION 1 that COROLLARY 1 is probably not best possible. However, it was pointed out in [M] that COROLLARY 3 is best possible apart from the factor $\log n$. Therefore COROLLARY 2 and the Theorem are also best possible apart from the factor $\log D$.

Next regard D as fixed and E as varying. In this situation it seems plausible that the number of points in the Theorem should be bounded above independently of w. But the present methods of proof are unlikely to yield such estimates. At best we may be able to replace certain powers of w by powers of $\eta = \operatorname{Im}\tau$; for example the arguments at the beginning of this section immediately give the upper bound $C\sqrt{\eta}D(w + \log D)$ instead of $C\sqrt{w}D(w + \log D)$.

In the case of complex multiplication some of these results can be improved. For example, in the above proof of COROLLARY 1 we could take complex multiples of P. For a fixed elliptic curve this leads to $q(P) \geq cD^{-2}(\log D)^{-1}$; but to calculate the dependence on w we need estimates for the endomorphism ring of E. Such estimates were obtained by FAISANT and PHILIBERT (see [FP p. 187], although there is no proof). They lead to

$$q(P) \geq \frac{1}{C(\sqrt{w})^3 D^2(w + \log D)}$$

for positive effective C depending only on the degree of k. We omit the details of the proof, since it is possible that better bounds could be found by calculating the constants in LAURENT'S result (1.4) (see [L p. 138]).

Finally we mention that our Theorem has an analogue for the multiplicative group $\mathbb{G}_m$. Thus one can show that for any number field K of degree at most $D \geq 3$ there are at most $CD \log D$ elements of K with absolute logarithmic height at most $1/(CD)$. Here C is positive, effective, and absolute.

This result appears to be new, and it implies multiplicative analogues of our Corollaries. By contrast these are not new; the analogue of COROLLARY 1 is much inferior to DOBROWOLSKI'S original analogue [Do] of 1.4, while the analogues of COROLLARIES 2 and 3 are equivalent merely to an estimate of the form

$$\varphi(n) \geq \frac{cn}{\log n}$$

for Euler's totient function. For these reasons there seems to be no point in giving complete proofs. But for someone wishing to construct proofs we should make the following remark. Whereas the group $E(\mathbb{C})$ is compact, the group $\mathbb{G}_m(\mathbb{C}) = \mathbb{C}^*$ is not, and so there is no obvious analogue of the Box Principle (our LEMMA 2.1). However, all the algebraic numbers α under consideration can be assumed to have heights at most $D^{-1} \log 2$, and this implies that they lie in the region defined by $\frac{1}{2} \leq |\alpha| \leq 2$. Since this region is compact, a suitable Box Principle can be established without difficulty.

Addendum

The referee kindly pointed out that our Theorem enables Silverman's estimate $q(P) \geq cD^{-2}$ to be improved to $q(P) \geq cD^{-1}(\log D \log \log D)^{-2}$. Actually we can even prove the following result.

COROLLARY 4. — *There is a positive effective constant C_4, depending only on the degree of k, such that if K is an abelian extension of k of relative degree at most D, we have*

$$q(P) \geq \frac{1}{C_4 w D (w + \log D)^2}$$

for all non-torsion P in $E(K)$.

Proof. — We need the initial remark that if Q_1, Q_2 are conjugates of a non-torsion point P satisfying $r_1 Q_1 = r_2 Q_2$ for positive integers r_1, r_2, then $r_1 = r_2$. This is easily proved; the simple multiplicative argument of DOBROWOLSKI'S paper [Do p. 395]) carries over with no change (compare also p. 142 of [L]).

Next suppose there exists non-torsion P in $E(K)$ with

$$q(P) < \frac{1}{C(C+1)^2 w D \mathcal{L}^2},$$

where $\mathcal{L} = w + \log D$ and C is the constant of the Theorem. Write K_0 for the subfield of K generated over k by the coordinates of P. Let Γ be the torsion subgroup of $E(K_0)$, and let $\mathcal{Q}$ be a maximal set of conjugates of P over k that are mutually incongruent modulo Γ. Further write $M = 1 + [C\sqrt{w}\mathcal{L}]$, and denote by $\mathcal{S}$ the set of points of the form $mQ + T$ for T in Γ, Q in $\mathcal{Q}$, and integers m with $1 \leq m \leq M$. Since K_0 is a Galois extension of k, the elements of $\mathcal{S}$ lie in $E(K_0)$. Moreover they are distinct. To see this, suppose $m_1Q_1 + T_1 = m_2Q_2 + T_2$ for T_1, T_2 in Γ, Q_1, Q_2 in $\mathcal{Q}$, and positive integers m_1, m_2. Multiplying by the cardinality t of Γ, we find that $tm_1Q_1 = tm_2Q_2$; so $m_1 = m_2$ from our initial remark. Hence $m_1(Q_1 - Q_2) = T_2 - T_1$, so that the point $Q_1 - Q_2$ of $E(K_0)$ has finite order, and is consequently in Γ. But the definition of $\mathcal{Q}$ implies now that $Q_1 = Q_2$. Thus finally $T_1 = T_2$ as well, and indeed the points of $\mathcal{S}$ are distinct.

Their cardinality is therefore $s = tqM$, where q is the cardinality of $\mathcal{Q}$. However, P has $D_0 = [K_0 : k] \leq D$ distinct conjugates over k, and since any congruence class modulo Γ has at most t elements, it follows that $D_0 \leq tq$. Thus

$$s \geq D_0 M > C\sqrt{w} D_0 (w + \log D_0).$$

Also since $M \leq (C+1)\sqrt{w}\mathcal{L}$ we have

$$q(mQ + T) = m^2 q(P) \leq M^2 q(P) < \frac{1}{CD} \leq \frac{1}{CD_0}$$

for every point $mQ + T$ of $\mathcal{S}$. These inequalities contradict our Theorem applied to the field K_0, and thereby establish COROLLARY 4 with $C_4 = C(C+1)^2$.

BIBLIOGRAPHIE

[AM] ANDERSON (M.) and MASSER (D.W.). — Lower bounds for heights on elliptic curves, *Math. Z.*, t. **174**, 1980, p. 23–34.

[BM] BROWNAWELL (W.D.) and MASSER (D.W.). — Multiplicity estimates for analytic functions I, *J. Reine Angew. Math.*, t. **314**, 1979, p. 200–216.

[C] COHEN (P.). — Explicit calculation of some effective constants in transcendence proofs, *Ph. D. Thesis, University of Nottingham*, 1985, Chapter 3.

[Da] DAVID (S.). — Fonctions thêta et points de torsion des variétés abéliennes, *C. R. Acad. Sci. Paris*, t. **305**, 1987, p. 211–214.

[Do] DOBROWOLSKI (E.). — On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.*, t. **34**, 1979, p. 391–401.

[FP] FAISANT (A.) and PHILIBERT (G.). — Quelques résultats de transcendance liés à l'invariant modulaire j, *J. Number Theory*, t. **25**, 1987, p. 184–200.

[H] HINDRY (M.). — Géométrie et hauteurs dans les groupes algébriques, *Thèse de Doctorat de l'Université Paris VI*, 1987.

[I] IGUSA (J.). — *Theta functions.* — Berlin-Heidelberg-New York, Springer-Verlag, 1972.

[L] LAURENT (M.). — Minoration de la hauteur de Néron-Tate, [Séminaire de Théorie de Nombres, Paris 1981 – 2], *Boston-Basel-Stuttgart, Birkhäuser*, 1983, pp. 137–152.

[M] MASSER (D.W.). — Division fields of elliptic functions, *Bull. London Math. Soc.*, t. **9**, 1977, p. 49–53.

[M′] MASSER (D.W.). — Small values of heights on families of abelian varieties, [Lecture Notes in Math., vol. **1290**], *New York-Berlin-Heidelberg-Tokyo, Springer-Verlag*, 1987, pp. 109–148.

[S] SILVERMAN (J.H.). — Lower bounds for the canonical height on elliptic curves, *Duke Math. J.*, t. **48**, 1981, p. 633–648.

[S′] SILVERMAN (J.H.). — *The arithmetic of elliptic curves.* — New York-Berlin-Heidelberg-Tokyo, Springer-Verlag, 1986.

[Z] ZIMMER (H.G.). — On the difference of the Weil height and the Néron-Tate height, *Math. Z.*, t. **147**, 1976, p. 35–51.

[Z′] ZIMMER (H.G.). — Quasi-functions on elliptic curves over number fields, *J. Reine Angew. Math.*, t. **307**, 1979, p. 221–246.