JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Francesco AMOROSO

Small points on a multiplicative group and class number problem

Tome 19, n° 1 (2007), p. 27-39.

<http://jtnb.cedram.org/item?id=JTNB_2007__19_1_27_0>

Journal de Théorie des Nombres
de Bordeaux **19** (2007), 27-39

Small points on a multiplicative group and class number problem

par Francesco AMOROSO

Résumé. Soit V une sous-variété algébrique du tore $\mathbb{G}_m^n \hookrightarrow \mathbb{P}^n$ et notons V^* le complémentaire dans V de l'adhérence de Zariski de l'ensemble des points de torsion de V. Par un théorème de Zhang, V^* est discrète pour la métrique induite par la hauteur normalisée $\hat{h}$. Nous décrirons certaines versions quantitatives de ce résultat, proche des conjectures les plus précises que l'on puisse formuler, et ses applications à l'étude du groupe de classes d'idéaux de certains corps de nombres.

Abstract. Let V be an algebraic subvariety of a torus $\mathbb{G}_m^n \hookrightarrow \mathbb{P}^n$ and denote by V^* the complement in V of the Zariski closure of the set of torsion points of V. By a theorem of Zhang, V^* is discrete for the metric induced by the normalized height $\hat{h}$. We describe some quantitative versions of this result, close to the conjectural bounds, and we discuss some applications to study of the class group of some number fields.

1. Lehmer's problem

Let $\alpha \in \overline{\mathbb{Q}}$ and let K be a number field containing α. We denote by $\mathcal{M}_K$ the set of places of K. For $v \in K$, let K_v be the completion of K at v and let $|\cdot|_v$ be the (normalized) absolute value of the place v. Hence, if v is an archimedean place associated with the embedding $\sigma\colon K \hookrightarrow \overline{\mathbb{Q}}$

$$|\alpha|_v = |\sigma\alpha|,$$

and, if v is a non archimedean place associated with the prime ideal P over the rational prime p,

$$|\alpha|_v = p^{-\lambda/e},$$

where e is the ramification index of P over p and λ is the exponent of P in the factorization of the ideal (α) in the ring of integers of K. This normalization agrees with the product formula

$$\prod_{v \in \mathcal{M}_K} |\alpha|_v^{[K_v:\mathbb{Q}_v]} = 1$$

Manuscrit reçu le 31 décembre 2005.

which holds for $\alpha \in K^*$. We define the Weil height of α by

$$h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} [K_v : \mathbb{Q}_v] \log \max\{|\alpha|_v, 1\}.$$

More generally, if $\boldsymbol{\alpha} = (\alpha_0 : \cdots : \alpha_n) \in \mathbb{P}^n(K)$, we define the Weil height of $\boldsymbol{\alpha}$ as

$$h(\boldsymbol{\alpha}) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \mathcal{M}_K} [K_v : \mathbb{Q}_v] \log \max\{|\alpha_0|_v, \cdots, |\alpha_n|_v\}.$$

It is easy to see that these definitions do not depend on the field K containing the coordinates of $\boldsymbol{\alpha}$. The height of an algebraic number satisfies:

i) $h(\alpha) = 0$ if and only if $\alpha = 0$ or α is a root of unity.
ii) $h(\alpha^n) = |n| h(\alpha)$ for any integer n.

It is therefore natural to ask for a lower bound $h(\alpha) \geq f(d)$ for non torsion $\alpha \in \overline{\mathbb{Q}}^*$ of degree d, where f is a positive function. Looking at $2^{1/d}$ we see that the best possible lower bound for such an α is

$$h(\alpha) \geq \frac{c}{d}, \tag{1}$$

where $c > 0$ is an absolute constant.

This problem was considered for the first time by Lehmer in [18]. More precisely, Lehmer considers the polynomial

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

which has precisely one root α on $(1, \infty)$. Since α is a Salem number (*i.e.,* all the conjugates of α, except α itself and α^{-1}, lie on the unit circle), its height is

$$h(\alpha) = \frac{\log \alpha}{10}\ .$$

Notice that $\alpha \approx 1.176$. In the quoted paper, Lehmer asks for the following problem:

If ε is a positive quantity, to find a polynomial of the form $f(x) = x^r + a_1 x^{r-1} + ... + a_r$ where the a's are integers, such that the absolute value of the product of those roots of f which lie outside the unit circle, lies between 1 and 1+ε. (...) Whether or not the problem has a solution for $\varepsilon < 0.176$ we do not know.

The best known result in the direction of (1) is Dobrowolski's theorem (*cf.* [15]), which implies

Theorem 1.1 (Dobwolski, 1979)**.**
For any $\varepsilon > 0$ there exists $c(\varepsilon) > 0$ such that, for all non torsion points $\alpha \in \overline{\mathbb{Q}}^*$ of degree d,

$$h(\alpha) \geq \frac{c(\varepsilon)}{d^{1+\varepsilon}}\ .$$

More generally, we can look for lower bounds for the height for special families of numbers. Let S be a set of algebraic numbers and let $\boldsymbol{\mu}$ be the set of roots of unity. Let's define, for $d \in \mathbb{N}$,

$$f_S(d) = \inf\{h(\alpha) \text{ such that } \alpha \in S\backslash\boldsymbol{\mu},\ \alpha \neq 0,\ [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq d\}\ .$$

For instance we have (see [29]),

Theorem 1.2 (Smyth, 1971)**.**
If $\alpha \in \overline{\mathbb{Q}}^*$ is not a reciprocal number (i.e., if α^{-1} is not an algebraic conjugate of α), then

$$h(\alpha) \geq \frac{\log \theta_0}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}\ ,$$

where $\theta_0 > 1$ is the only real root of the equation $x^3 - x - 1 = 0$.

Also, Mignotte (see [20]) gives a positive answer to Lehmer's problem for any α of degree d such that there exists a prime $p \leq d \log d$ which splits completely in $\mathbb{Q}(\alpha)$. More recently, Lehmer's problem was solved by Borwein, Dobrowolski and Mossinghoff (see [12]) for algebraic integers whose minimal polynomial has coefficients all congruent to 1 modulo a fixed $m \geq 2$.

Hence, if S is the set of non reciprocal numbers, or the set of algebraic α such that there exists a prime $p \leq [\mathbb{Q}(\alpha) : \mathbb{Q}] \log([\mathbb{Q}(\alpha) : \mathbb{Q}])$ which splits completely in $\mathbb{Q}(\alpha)$, or the set of algebraic integers whose minimal polynomial has coefficients all congruent to 1 modulo a fixed $m \geq 2$, then

$$f_S(d) \geq \frac{c}{d}$$

for some absolute constant $c > 0$.

For other set S we know even more than Lehmer:

$$f_S(d) \geq c \tag{2}$$

for an absolute constant c. For instance, if $\mathbb{Q}(\alpha)$ is a totally real field and $\alpha \neq \pm 1$, then, by a special case of a result of Schinzel (see [25]),

$$h(\alpha) \geq \frac{1}{2} \log \varphi$$

where φ is the golden ratio $\frac{1+\sqrt{5}}{2}$. This also holds if $\mathbb{Q}(\alpha)$ is a CM field, provided that[1] $|\alpha| \neq 1$ (op. cit.). This last condition can be very restrictive for some applications; it was removed for abelian extensions[2] in [8]:

[1] In a CM field $|\alpha|_v = 1$ for an archimedean place if and only if $|\alpha|_v = 1$ for any archimedean place.

[2] We remark that there exist algebraic numbers α (necessarly of absolute value 1 by Schinzel's result) with positive and arbitrarily small height such that $\mathbb{Q}(\alpha)$ is a CM field (see [9]).

Theorem 1.3 (A. – Dvornicich, 2000)**.**
Let $\alpha \in \overline{\mathbb{Q}}^*$ not a root of unity, and assume that $\mathbb{Q}(\alpha)/\mathbb{Q}$ is an abelian extension. Then

$$h(\alpha) \geq \frac{\log 5}{12} .$$

As remarked before, given an arbitrary algebraic number α, we cannot hope for nothing more than Lehmer's conjecture. Nevertheless, if we look at several multiplicatively independent numbers, we have a bound which is close to (2).

Theorem 1.4 (A. – David, 1999)**.**
Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^*$ multiplicatively independent. Then, for any $\varepsilon > 0$

$$\max\{h(\alpha_1), \ldots, h(\alpha_n)\} \geq \frac{c(n,\varepsilon)}{d^{1/n+\varepsilon}}$$

where $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$ and $c(n,\varepsilon) > 0$.

This result is better understood in the more general setting of the next section.

2. Lower bounds for the height in $\mathbb{G}_m^n$

2.1. Normalized height and essential minimum. Let h be a height on subvarieties of $\mathbb{P}^n(\overline{\mathbb{Q}})$, for instance the height defined by Philippon in [22] or an other equivalent: for our purposes two projective heights h_1 and h_2 are equivalent if for any subvariety[3] V we have

$$|h_1(V) - h_2(V)| \leq c \deg(V)$$

for some $c > 0$ independent of V. We consider the n power of the multiplicative group $\mathbb{G}_m^n$ which is naturally embedded in $\mathbb{P}^n$. We denote by $[l]$ the "multiplication" by $l \in \mathbb{Z}$ in $\mathbb{G}_m^n(\overline{\mathbb{Q}})$. Let, as in the rest of this paper, V be a subvariety[4] of $\mathbb{G}_m^n(\overline{\mathbb{Q}})$; by degree $\deg(V)$ and height $h(V)$ we mean the degree and the height of the Zariski closure of V in $\mathbb{P}_n$. Following David and Philippon (see [14]), we define the normalized height $\hat{h}(V)$ of V by a limit process:

$$\hat{h}(V) = \lim_{l \to +\infty} \frac{h([l]V) \deg(V)}{l \deg([l]V)}$$

The same height can be defined using Arakelov theory. It satisfies:

i) $\hat{h}(\cdot)$ is non-negative;
ii) for every $l \in \mathbb{N}$ we have

$$\hat{h}([l]^{-1}V) = l^{\operatorname{codim}(V)-1} \hat{h}(V)$$

[3] By a subvariety of $\mathbb{P}^n(\overline{\mathbb{Q}})$ we mean an algebraic and geometrically irreducible subvariety defined over $\overline{\mathbb{Q}}$.

[4] V is a subvariety of $\mathbb{G}_m^n(\overline{\mathbb{Q}})$ if $V = \tilde{V} \cap \mathbb{G}_m^n(\overline{\mathbb{Q}})$, where $\tilde{V}$ is a subvariety of $\mathbb{P}^n(\overline{\mathbb{Q}})$.

iii) for every torsion point $\boldsymbol{\zeta}$ we have $\hat{h}(\boldsymbol{\zeta}V) = \hat{h}(V)$.

For $\theta \geq 0$ let

$$V(\theta) = \{\boldsymbol{\alpha} \in V(\overline{\mathbb{Q}}) \text{ such that } \hat{h}(\boldsymbol{\alpha}) \leq \theta\},$$

where $\hat{h}(\boldsymbol{\alpha}) = h((1 : \alpha_1 : \cdots, \alpha_n))$. Hence $V(0)$ is the set of torsion points on V. It is now important to recall the former Manin-Mumford conjecture for $\mathbb{G}_m^n$ (see [17]):

Theorem 2.1 (Laurent, 1984)**.**
The Zariski closure of $V(0)$ is a finite union of translates of subtori by torsion points (= torsion varieties).

Let define the *essential minimum* $\hat{\mu}^{\mathsf{ess}}(V)$ of V as the infimum of the set of $\theta \geq 0$ such that $V(\theta)$ is Zariski dense in V. Then (see [30]),

Theorem 2.2 (Zhang, 1995)**.**
The following assertions are equivalent:

i) *V is torsion;*
ii) *$\hat{\mu}^{\mathsf{ess}}(V) = 0$;*
iii) *$\hat{h}(V) = 0$.*

More precisely, the equivalence between *ii)* and *iii)* follows by a special case of Zhang's inequality (see again [30]), which shows that the normalized height and the essential minimum are closely related:

$$\hat{\mu}^{\mathsf{ess}}(V) \leq \frac{\hat{h}(V)}{\deg(V)} \leq (\dim(V) + 1)\hat{\mu}^{\mathsf{ess}}(V).$$

2.2. Lower bounds. Let V be a subvariety of $\mathbb{G}_m^n(\overline{\mathbb{Q}})$ and let K be a subfield of $\overline{\mathbb{Q}}$. We denote by $\overline{V}^K$ the union of the orbit of V under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$; therefore

$$\deg\left(\overline{V}^K\right) = [LK : K] \deg(V),$$

where L is the field of definition of V.

Let us also define the "obstruction index" of V over K as the minimum $\omega_K(V)$ of $\deg\left(\overline{Z}^K\right)$ where Z is an hypersurface containing V. For instance, if $V = \{\boldsymbol{\alpha}\} \subseteq \mathbb{G}_m^n(\overline{\mathbb{Q}})$,

$$\omega_K(V) \leq n[K(\boldsymbol{\alpha}) : K]^{1/n} \tag{3}$$

by a linear algebra argument.

We propose two conjectural lower bounds for the essential minimum:

Conjecture 2.3 (A. – David, 1999–2003)**.**
There exists $c(n) > 0$ having the following properties.

- **Arithmetic case.** *Let us assume that V is not contained in any proper torsion subvariety. Then,*

$$\hat{\mu}^{\mathsf{ess}}(V) \geq \frac{c(n)}{\omega_{\mathbb{Q}}(V)}.$$

- **Geometric case.** *Assume further that V is not contained in any translate of a proper subgroup. Then,*

$$\hat{\mu}^{\mathsf{ess}}(V) \geq \frac{c(n)}{\omega_{\overline{\mathbb{Q}}}(V)}.$$

As for Lehmer's conjecture, the previous statement is best possible, since

$$\hat{\mu}^{\mathsf{ess}}([l]^{-1}V) = l\hat{\mu}^{\mathsf{ess}}(V) \quad \text{and} \quad \omega_K([l]^{-1}V) \leq l\omega_K(V).$$

In [2], [3] and [4] we prove that conjecture 2.3 holds up to an $\varepsilon > 0$.

Theorem 2.4 (A. – David, 1999–2003)**.**
For any $\varepsilon > 0$ there exists $c(n, \varepsilon) > 0$ having the following properties.

- **Arithmetic case.** *Let us assume that V is not contained in any proper torsion subvariety. Then,*

$$\hat{\mu}^{\mathsf{ess}}(V) \geq \frac{c(n, \varepsilon)}{\omega_{\mathbb{Q}}(V)^{1+\varepsilon}}.$$

- **Geometric case.** *Assume further that V is not contained in any translate of a proper subgroup. Then,*

$$\hat{\mu}^{\mathsf{ess}}(V) \geq \frac{c(n, \varepsilon)}{\omega_{\overline{\mathbb{Q}}}(V)^{1+\varepsilon}}.$$

We remark that a 0-dimensional variety $V = \{\boldsymbol{\alpha}\}$ is contained in a proper torsion subvariety if and only if $\alpha_1, \ldots, \alpha_n$ are multiplicatively dependent. Moreover

$$\hat{\mu}^{\mathsf{ess}}(V) = h(\boldsymbol{\alpha}) \leq \max\{h(\alpha_1), \ldots, h(\alpha_n)\} \quad \text{and} \quad \omega_{\mathbb{Q}}(V) \leq nd^{1/n}.$$

by (3), where $d = [\mathbb{Q}(\boldsymbol{\alpha}) : \mathbb{Q}]$. Therefore the lower bound

$$\max\{h(\alpha_1), \ldots, h(\alpha_n)\} \geq \frac{c(n, \varepsilon)}{d^{1/n+\varepsilon}}$$

of theorem 1.4 for multiplicatively independent $\alpha_1, \ldots, \alpha_n$ is a corollary of theorem 2.4.

2.3. Small points. Let V be a non-torsion subvariety of $\mathbb{G}_m^n(\overline{\mathbb{Q}})$ and define V^* as the complement in V of the union of torsion subvarieties *contained* in V. Then, theorem 2.2 implies that the height on $V^*(\overline{\mathbb{Q}})$ is bounded from below by a positive quantity.

Similarly, if V is not a union of translates of subgroups we define, following [11], V^0 as the complement in V of the union of translate of subgroups B of positive dimension with $B \subseteq V$. Bombieri and Zannier (see [11]) and Schmidt (see [26]) prove that, outside a finite set, the height on $V^0(\overline{\mathbb{Q}})$ is bounded from below by a positive quantity depending only on the ideal of definition of V and not on its field of definition. Later, their lower bound was strongly improved by David and Philippon (see [14]).

Let K be any subfield of $\overline{\mathbb{Q}}$ and define $\delta_K(V)$ as the minimum integer δ such that V is the intersection of hypersurfaces $Z_1, \ldots, Z_r$ with $\deg \overline{Z_j}^K \leq \delta$. Then

$$\left(\deg \overline{V}^K\right)^{1/\operatorname{codim}(V)} \leq \delta_K(V) \leq \deg \overline{V}^K.$$

and both lower and upper bounds can be attained.

We propose the following conjectural lower bounds for the distribution of small points:

Conjecture 2.5 (A. – David, 2004–2005)**.**
There exists $c(n) > 0$ having the following properties.

- **Arithmetic case.** *For any $\alpha \in V^*(\overline{\mathbb{Q}})$ we have*

$$h(\alpha) \geq \frac{c(n)}{\delta_{\mathbb{Q}}(V)}.$$

- **Geometric case.** *For all but finitely many $\alpha \in V^0(\overline{\mathbb{Q}})$ we have*

$$h(\alpha) \geq \frac{c(n)}{\delta_{\overline{\mathbb{Q}}}(V)}.$$

In [5] and [6] we prove that conjecture 2.5 holds up to an $\varepsilon > 0$.

Theorem 2.6 (A. – David, 2004–2005)**.**
For any $\varepsilon > 0$ there exists $c(n, \varepsilon) > 0$ having the following properties.

- **Arithmetic case.** *For any $\alpha \in V^*(\overline{\mathbb{Q}})$ we have*

$$h(\alpha) \geq \frac{c(n, \varepsilon)}{\delta_{\mathbb{Q}}(V)^{1+\varepsilon}}.$$

- **Geometric case.** *For all but finitely many $\alpha \in V^0(\overline{\mathbb{Q}})$ we have*

$$h(\alpha) \geq \frac{c(n, \varepsilon)}{\delta_{\overline{\mathbb{Q}}}(V)^{1+\varepsilon}}.$$

2.4. More conjectures and results.

• The proofs in the quoted papers [2], [4], [5] and [6] follow the usual steps of a transcendence proof: interpolation (construction of an auxiliary function), extrapolation, zero estimates and conclusion. Unfortunately, for subvarieties of codimension > 1, we need a rather technical extra step (descent argument). It will be very interesting to find an alternative proof removing this extra step. Recently C. Pontreau succeeds in this task for subvarieties of $\mathbb{G}_m^2(\overline{\mathbb{Q}})$ in the arithmetic case (see [23]) and for subvarieties of $\mathbb{G}_m^3(\overline{\mathbb{Q}})$ in the geometric case.

• In the geometric case of conjecture 2.5 we could ask for an upper bound for the exceptional points:

Conjecture 2.7 (A. – David, 2005)**.**
There exist translates of subgroups $B_1, \dots, B_m \subseteq V$ with

$$\deg(B_1) + \cdots + \deg(B_m) \leq c(n)^{-1} \delta_{\overline{\mathbb{Q}}}(V)^n.$$

such that

$$h(\alpha) \geq \frac{c(n)}{\delta_{\overline{\mathbb{Q}}}(V)}.$$

for any $\alpha \in V(\overline{\mathbb{Q}})$ outside $B_1 \cup \cdots \cup B_m$.

Recently, Pontreau gives some partial results in this direction for curves in $\mathbb{G}_m^2$ and for surfaces in $\mathbb{G}_m^3$ (see [24])

• The arithmetic part of conjectures 2.3 and 2.5 can be generalized by replacing $\mathbb{Q}$ with $\mathbb{Q}^{\mathrm{ab}}$. For instance, for the essential minimum we can formulate:

Conjecture 2.8 (A. – David, 2005)**.**
Let V be a subvariety of $\mathbb{G}_m^n(\overline{\mathbb{Q}})$ which is not contained in any torsion subvariety. Then,

$$\hat{\mu}^{\mathsf{ess}}(V) \geq \frac{c(n)}{\omega_{\mathbb{Q}^{\mathrm{ab}}}(V)}.$$

For $n = 1$ ("relative Lehmer Problem") this conjecture was proved up to an ε (see [10]).

Theorem 2.9 (A. – Zannier, 2000)**.**
Let $\alpha \in \overline{\mathbb{Q}}^*$ not a root of unity and let $\varepsilon > 0$. Then

$$h(\alpha) \geq \frac{c(\varepsilon)}{d^{1+\varepsilon}}.$$

where $c(\varepsilon) > 0$ and $d = [\mathbb{Q}^{\mathrm{ab}}(\alpha) : \mathbb{Q}^{\mathrm{ab}}]$.

3. Size of the class group of some fields

Lower bounds for the height can be used to obtain informations on the size of the ideal class group of a field K, following a general construction which we summarize as follows :

I) Let assume that the ideal class group of K is "small" and construct algebraic integers of small norm by analytic methods.
II) Construct algebraic numbers of small height from algebraic integers of small norm.
III) Use lower bounds for the height to get a contradiction.

In the next three subsections we describe how this construction works for cyclotomic fields, for CM fields and for other more general fields. To simplify the notations, we only state the results concerning the exponent of the class group, *i.e.,* the smallest positive integer e such that I^e is principal for any ideal I of K, although the method can give more general informations on the size of the class group and on its Galois structure. As we see in the next subsections, this construction produces a good lower bound for the exponent for families of fields for which it is known, by classical methods, that the class number goes to infinity.

3.1. Cyclotomic fields. Let's start by the simpler case of a cyclotomic field $K_m = \mathbb{Q}(\zeta_m)$ where ζ_m is a m-th primitive root of unity. Let e_m be the exponent of the class group of K_m.

I) By Linnik's theorem, there exists an absolute constant L and a prime $p \leq m^L$ which splits completely in K_m. Let P be a prime ideal of K_m over p; by definition $P^{e_m} = (\gamma)$ for some integer $\gamma \in K_m$. We have

$$|\mathrm{N}_{\mathbb{Q}}^{K_m}\gamma| = p^{e_m} \leq m^{Le_m}.$$

II) Let $\alpha = \gamma/\overline{\gamma}$. Then, $|\alpha|_v = 1$ for every archimedean place $v \in \mathcal{M}_{K_m}$ and, if $v \in \mathcal{M}_{K_m}$ is non archimedean

$$|\alpha|_v = \begin{cases} p^{-e_m}, & \text{if } v \text{ is associated to } P; \\ p^{e_m}, & \text{if } v \text{ is associated to } \overline{P}; \\ 1, & \text{otherwise.} \end{cases}$$

Therefore

$$h(\alpha) = \frac{e_m \log p}{[K_m : \mathbb{Q}]} \leq \frac{e_m L \log m}{\varphi(m)} \ ,$$

where $\varphi(\cdot)$ is the Euler function.

III) Since $K_m/\mathbb{Q}$ is abelian, we can use theorem 1.3:

$$\frac{\log 5}{12} \leq h(\alpha) \leq \frac{e_m L \log m}{\varphi(m)} \ .$$

We obtain (see [7]):

Theorem 3.1 (A. – Dvornicich, 2003)**.**
The exponent e_m of the class group of the m-th cyclotomic field satisfies

$$e_m \geq \frac{\log 5}{12L} \times \frac{\varphi(m)}{\log m} .$$

3.2. CM fields. If we want to obtain similar results for a CM field K, then we must take into account two main problems: first, there are no sharp unconditional results as Linnik's theorem, second as $K/\mathbb{Q}$ need not to be abelian, we cannot use theorem 1.3.

The construction of subsection 3.1 can be modified as follows. Let Δ be the discriminant of K, $d = [K : \mathbb{Q}]$ and let e_K be the exponent of the class group of K.

I) Assume the Generalized Riemann Hypothesis for the Dedekind zeta function of K. Then, the effective Chebotarev's theorem of Lagarias and Odlyzko (see [16]) gives primes ideals $P_1, \ldots, P_n$ of K of degree 1, non-ramified over $\mathbb{Q}$, and such that

$$\log |N_{\mathbb{Q}}^K P_j| \leq 3 \log\log |\Delta| + c(n)$$

where $c(n)$ depends only on n. As before $P_j^{e_K} = (\gamma_j)$ for some integers $\gamma_j \in K$.

II) As for cyclotomic fields, let $\alpha_j = \gamma_j/\overline{\gamma_j}$; then

$$h(\alpha_j) \leq \frac{e_K(3 \log\log |\Delta| + c(n))}{d} .$$

III) Since $\alpha_1, \ldots, \alpha_n$ are easily seen to be multiplicatively independent, we can apply theorem 1.4, which gives:

$$e_K \geq \frac{c(n,\varepsilon) d^{1-1/n-\varepsilon}}{3 \log\log |\Delta| + c(n)}$$

for any $\varepsilon > 0$. This inequality is good, except if $|\Delta|$ is very big with respect to d. In this last situation it is better to use the lower bound

$$h(\alpha_1) \geq \frac{\log |\Delta| - d \log d}{2d(d-1)}$$

which easily follows by Hadamard's inequality since α_1 is a generator of K and so $\mathrm{disc}(\alpha_1) \mid \Delta$ (see [27] or [28] for details). This gives:

$$e_k \geq \frac{\log |\Delta| - d \log d}{2(d-1)(3 \log\log |\Delta| + c(1))}$$

Putting together these two lower bounds we get (see again [7]):

Theorem 3.2 (A. – Dvornicich, 2003)**.**
Let K be a CM field of discriminant Δ and degree d. Then, assuming the Generalized Riemann Hypothesis for the Dedekind zeta function of K, for any $\varepsilon > 0$ the exponent e_K of the class group of K satisfies:

$$e_K \geq \max\left\{\frac{C\log|\Delta|}{d\log\log|\Delta|}, C(\varepsilon)d^{1-\varepsilon}\right\},$$

where C and $C(\varepsilon)$ are positive constants.

We recall that, under suitable assumptions, the class number of a CM field goes to infinity with $|\Delta|$ (see [21]). Theorem 3.2 proves, under GRH, the corresponding result for the exponent, giving a positive answer to a conjecture of Louboutin and Okazaki [19].

3.3. Some other fields. The main problem in extending the method of section 3.2 to other fields is the construction of algebraic numbers of small height from integers of small norm. A first attempt to attack this problem is the following. Let K be a number field of discriminant Δ and degree d and let $\gamma_1, \ldots, \gamma_t \in \mathcal{O}_K$ of norm $\leq x$. Let also r be the rank of the unit group E_K, δ be a bound for the sum of the height of a system of generators of $E_K/(E_K)_{\mathrm{tors}}$ and let m and N be two positive integers satisfying $mN^r < t$. The box principle gives m units $u_1, \ldots, u_m$ and $m+1$ distinct indexes $i_0, i_1, \ldots, i_m \in \{1, \ldots, t\}$ such that

$$h(u_j\gamma_{i_j}\gamma_{i_0}^{-1}) \leq \frac{\log x}{d} + \frac{\delta}{N}$$

for $j = 1, \ldots, m$. Unfortunately, r is at least $d/2$ and so the parameter t must be exponential in the degree, excluding in most cases reasonable applications.

Let Γ be the group of $\mathbb{Q}$-automorphisms of K; to avoid this undesired growth, we assume that there exists a "small" ϕ in the group ring $\mathbb{Z}[\Gamma]$ such that the rank of E_K^{ϕ} is also small. More precisely, let $\|\phi\|_1$ be the sum of the absolute values of the coefficients of ϕ, let $r_\phi = \mathrm{rank}(E_K^{\phi})$ and let δ_ϕ be a bound for the sum of the height of a system of generators of $(E_K)^{\phi}/(E_K)_{\mathrm{tors}}$. Then, if $mN^{r_\phi} < t$ we can find as before m units $u_1, \ldots, u_m$ and $m+1$ distinct indexes $i_0, i_1, \ldots, i_m \in \{1, \ldots, t\}$ such that

$$h(u_j\gamma_{i_j}\gamma_{i_0}^{-1}) \leq \frac{\|\phi\|\log x}{d} + \frac{\delta_\phi}{N}$$

for $j = 1, \ldots, m$. This construction could give a good lower bound for the exponent (using effective Chebotarev's theorem and lower bounds for the height as in subsection 3.2), if

$$\|\phi\|_1 r_\phi \log\left(d\delta_\phi/(r_\phi+1)+2\right)$$

is small. For instance, let α be a Salem number and let $\tau \in \Gamma$ defined by $\alpha^\tau = \alpha^{-1}$. Put $\phi = 1 - \tau$. Then $\|\phi\|_1 = 2$, $r_\phi = 1$ and $d\delta_\phi \leq 2 \log \alpha$. We obtain (see [1]):

Theorem 3.3 (A., 2005)**.**
Let α be a Salem number and let $K = \mathbb{Q}(\alpha)$. Then, assuming the Generalized Riemann Hypothesis for the Dedekind zeta function of K, for any $\varepsilon > 0$ the exponent of the class group of K satisfies:

$$e_K \geq \frac{\max(Cd^{-1} \log |\Delta|, C_\varepsilon d^{1-\varepsilon})}{\log \log |\Delta| + \log(\log \alpha + 2)} .$$

We mention that an analogous result for the class number of the field generated by a Salem number was proved in [13] using a relation between Salem numbers and the derivative at 0 of an Artin L-function.

References

[1] F. Amoroso, *Une minoration pour l'exposant du groupe des classes d'un corps engendré par un nombre de Salem*. International Journal of Number Theory **3**, no. 2 (2007), 1–13.

[2] F. Amoroso, S. David, *Le problème de Lehmer en dimension supérieure*. J. Reine Angew. Math. **513** (1999), 145–179.

[3] F. Amoroso, S. David, *Densité des points à cordonnées multiplicativement indépendantes*. Ramanujan J. **5** (2001), 237–246.

[4] F. Amoroso, S. David, *Minoration de la hauteur normalisée dans un tore*. Journal de l'Institut de Mathématiques de Jussieu **2**, no. 3 (2003), 335–381.

[5] F. Amoroso, S. David, *Distribution des points de petite hauteur dans les groupes multiplicatifs*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5) **3**, no. 2 (2004), 325–348.

[6] F. Amoroso, S. David, *Points de petite hauteur sur une sous-variété d'un tore (2005)*. Compos. Math. (to appear).

[7] F. Amoroso, R. Dvornicich, *Lower bounds for the height and size of the ideal class group in CM fields*. Monatsh. Math. **138**, no.2 (2003), 85–94.

[8] F. Amoroso, R. Dvornicich, *A Lower Bound for the Height in Abelian Extensions*. J. Number Theory **80**, no. 2 (2000), 260–272.

[9] F. Amoroso, F. Nuccio, *Algebraic Numbers of Small Weil's height in CM-fields: on a Theorem of Schinzel (2005)*. J. Number Theory (to appear).

[10] F. Amoroso, U. Zannier, *A relative Dobrowolski's lower bound over abelian extensions*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **29**, no 3 (2000), 711–727.

[11] E. Bombieri, U. Zannier, *Algebraic points on subvarieties of $\mathbb{G}_m^n$*. Internat. Math. Res. Notices, **7** (1995), 333–347.

[12] P. Borwein, E. Dobrowolski, M. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*. Bull. London Math. Soc., **36** (2004), 332–338.

[13] T. Chinburg, *On the arithmetic of two constructions of Salem numbers*. J. Reine Angew. Math. **348** (1984), 166-179.

[14] S. David, P. Philippon, *Minorations des hauteurs normalisées des sous-variétés des tores*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4), **28**, no. 3 (1999), 489-543; Errata, ibidem **29**, no 3 (2000), 729-731.

[15] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*. Acta Arith. **34** (1979), 391–401.

[16] J. C. Lagarias, A. M. Odlyzko, *Effective versions of the Čebotarev density theorem*. Algebraic Number Fields, Durham Symposium, Academic Press, 1977.

[17] M. Laurent, *Equations diophantiennes exponentielles*. Invent. Math. **78** (1984), 299–327.

[18] D. H. Lehmer, *Factorization of certain cyclotomic functions*. Ann. of Math. **34** (1933), 461–479.

[19] S. Louboutin, R. Okazaki, *Exponents of the ideal class groups of CM number fields*. Math. Z. **243**, no.1 (2003), 155–159.
[20] M. Mignotte, *Estimations élémentaires effectives sur les nombres algébriques*. Publications I. R. M. A., Strasbourg, 1979.
[21] A. M. Odlyzko, *Some analytic estimates of class numbers and discriminants*. Invent. Math. **29** (1975), 275–286.
[22] P. Philippon, *Critères pour l'indépendance algébrique*. Inst. Hautes Etudes Sci. Publ. Math. **64** (1986), 5–52.
[23] C. Pontreau, *Minoration effective de la hauteur des points d'une courbe de* $\mathbb{G}_m^2$. Acta Arith. **120**, no. 1 (2005), 1–26.
[24] C. Pontreau, *Points de petite hauteur d'une surface*. Canadian Journal of Mathematics. À paraître.
[25] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*. Acta Arith. **24** (1973), 385–399. Addendum; ibid. **26** (1973), 329–361.
[26] W. M. Schmidt, *Heights of points on subvarieties of* $\mathbb{G}_m^n$. In Number Theory 93–94. S. David editor, London Math. Soc. Ser., volume **235**, Cambridge University Press, 1996.
[27] J. H. Silverman, *Lower bounds for height functions*. Duke Math. J. **51** (1984), 395–403.
[28] D. Simon, *The index of nonmonic polynomials*. Indag. Math. New Ser. **12**, no.4 (2001), 505–517.
[29] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic number*. Bull. London Math. Soc. **3** (1971), 169–175.
[30] S. Zhang, *Positive line bundles on arithmetic varieties*. J. Amer. Math. Soc. **8**, no. 1 (1995), 187–221.

Francesco Amoroso
Université de Caen
Laboratoire de Mathématiques
Nicolas Oresme, U.M.R. 6139 (C.N.R.S.)
Campus II, BP 5186
F–14032 Caen Cedex
E-mail: `francesco.amoroso@math.unicaen.fr`