On a conjecture of G. Rémond

Francesco Amoroso

On a conjecture of G. Rémond

Francesco Amoroso[(1)]

[(1)] *Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 6139*
Université de Caen, Campus II, BP 5186
14032 Caen Cedex, France

Abstract. We provide an example which gives some new evidence to a recent conjecture of G. Rémond on lower bounds for the height.

Mathematics Subject Classification: 11G50 (Primary), 12E30 (Secondary).

This research was partially supported by ANR 2010 BLAN-0115-01

1 Introduction

Recently Rémond suggests a very general conjecture ([6], conjecture 3.4) on lower bounds for the height in A where A is either an abelian variety of dimension n or a power $\mathbb{G}_{\mathrm{m}}^n$ of the multiplicative group.

Let $h(\cdot)$ be the (absolute, logarithmic) Weil's height on $\overline{\mathbb{Q}}$. Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a subgroup of *finite* rank $k = \dim_{\mathbb{Q}}(\Gamma \otimes_{\mathbb{Z}} \mathbb{Q})$. As usual we define the division group of Γ as

$$\Gamma_{\mathrm{div}} = \{g \in \overline{\mathbb{Q}}^* \text{ such that } \exists n \in \mathbb{Z}_{\geq 1},\ g^n \in \Gamma\}\ .$$

Let $K_\Gamma = \mathbb{Q}(\Gamma)$ be the field of rationality of Γ. In this special setting ($A = \mathbb{G}_{\mathrm{m}}$), Rémond's conjecture reads as follows.

Conjecture 1.1 (Rémond 2011)**.** *Let $\alpha \in \overline{\mathbb{Q}}^* \backslash \Gamma_{\mathrm{div}}$ and put $d = [K_\Gamma(\alpha) : K_\Gamma]$. Then:*

- *(strong form) There exists a positive constant c_Γ such that $h(\alpha) \geq c_\Gamma/d$.*
- *(weak form) For any $\varepsilon > 0$ there exists a positive constant $c_\Gamma(\varepsilon)$ such that $h(\alpha) \geq c_\Gamma(\varepsilon)/d^{1+\varepsilon}$.*

Two cases of conjecture 1.1 were intensively studied. Let first $\Gamma = \{1\}$. Thus $K_\Gamma = \mathbb{Q}$ and Γ_{div} is the subgroup $\overline{\mathbb{Q}}^*_{\mathrm{tors}}$ of torsion points (= roots of unity). The strong form reduces to the celebrated Lehmer's problem, while the weak form is a well-known theorem of Dobrowolski [3]. Remark that the case $d = 1$ is trivial.

Let now $\Gamma = \{1\}_{\mathrm{div}} = \overline{\mathbb{Q}}^*_{\mathrm{tors}}$. Then, by Kronecker-Weber theorem, $K_\Gamma = \mathbb{Q}^{\mathrm{ab}}$ and obviously $\Gamma_{\mathrm{div}} = \Gamma$. The strong form reduces to the so-called "relative Lehmer's problem", while the weak form is the main theorem of [2]. In this situation, even the case $d = 1$ is not trivial. It reduces to the main result of [1]:

$$\forall \alpha \in (\mathbb{Q}^{\mathrm{ab}})^* \backslash \overline{\mathbb{Q}}^*_{\mathrm{tors}}, \quad h(\alpha) \geq \frac{\log 5}{12} .$$

To our knowledge, there are no non-trivial results for subgroup of positive rank, even if $d = 1$. Let us restate conjecture 1.1 in this special case.

Conjecture 1.2. *Let $\Gamma \subset \overline{\mathbb{Q}}^*$ be a subgroup of finite rank. Then there exists a constant $c_\Gamma > 0$ such that for any $\alpha \in \mathbb{Q}(\Gamma)^* \backslash \Gamma_{\mathrm{div}}$ we have $h(\alpha) \geq c_\Gamma$.*

The main purpose of this paper is to give some new evidence to conjecture 1.2.

Let us consider a simple example: $\Gamma = \langle 2 \rangle_{\mathrm{div}}$. Given a positive integer n we denote by ζ_n a primitive n-th root of unity. Then conjecture 1.2 states in this case that for any non-zero $\alpha \in \mathbb{Q}(\zeta_2, 2^{1/2}, \zeta_3, 2^{1/3}, \zeta_4, 2^{1/4}, \ldots)$ either there exists a positive integer N such that $\alpha^N \in \langle 2 \rangle$ or $h(\alpha) \geq c$ for some absolute constant $c > 0$. We are not able to give a positive answer to conjecture 1.2 for $\Gamma = \langle 2 \rangle_{\mathrm{div}}$. However, we can prove it for the rank 1 subgroup $\langle \zeta_{3^t}, 2^{1/3^t} \rangle_{t \geq 1}$ of $\langle 2 \rangle_{\mathrm{div}}$.

Theorem 1.3. *Conjecture 1.2 holds for the subgroup*

$$\Gamma = \langle \zeta_{3^t}, 2^{1/3^t} \rangle_{t \geq 1} .$$

More precisely, let α be a non-zero algebraic number in the infinite extension

$$\mathbb{Q}(\zeta_3, 2^{1/3}, \zeta_{3^2}, 2^{1/3^2}, \zeta_{3^3}, 2^{1/3^3}, \ldots) .$$

Then either there exists a positive integer N such that $\alpha^N \in \langle 2 \rangle$ or

$$h(\alpha) \geq \log(3/2)/18 .$$

Let us briefly explain why we are not able to prove conjecture 1.2 for $\Gamma = \langle 2 \rangle_{\mathrm{div}}$ but we can prove it for $\Gamma = \langle \zeta_{3^t}, 2^{1/3^t} \rangle_{t \geq 1}$. All the known proofs of the weak form of conjecture 1.1 for $\Gamma = \{1\}_{\mathrm{div}}$ (even in dimension > 1, or in other settings, for instance for abelian varieties or in a recent result by Habegger [5]) rest on a dichotomy already present in [1]. Roughly speaking, the core of the diophantine proof (the extrapolation step) consists of two metric properties. The first one, which comes from the standard Frobenius (or, if we prefer, Fermat's Small Theorem) argument, works if there is no ramification. The second one is useful if instead we have ramification. In the present situation we do not succeed to generalize the first metric property and thus we cannot solve conjecture 1.2 even in the said special case. However, we are able to generalize the second metric property in some extensions which are totally ramified at some fixed primes p, as $\mathbb{Q}(\zeta_{3^r}, 2^{1/3^s})$ $(r \geq s \geq 1)$ for $p = 3$. We hope that in the future someone

will also be able to extend the full method of [1] to solve the height problem for the extension $\mathbb{Q}(\zeta_n, 2^{1/n})_{n\geq 1}$. This would probably allow to solve conjecture 1.2 and even the weak form of conjecture 1.1 for an arbitrary subgroup Γ of finite rank.

There is nothing special in the numbers 2 and 3 which appear in theorem 1.3, and indeed we shall prove (theorem 3.3) a lower bound for the height in the infinite extension $\mathbb{Q}(\zeta_p, b^{1/p}, \zeta_{p^2}, b^{1/p^2}, \zeta_{p^3}, b^{1/p^3}, \ldots)$, where p is a prime number and $b \geq 2$ is an integer such that $p \nmid b$ and $p^2 \nmid (b^{p-1} - 1)$. While the first condition is important for our method, the second one can be probably relaxed. More generally, our method could be generalized, at the price of a deeper analysis on the ramification in radical extensions, to get some partial results in the case of an arbitrary subgroup of finite rank (see remark 3.4). Since we are not able to solve conjecture 1.2 even in the special case $\Gamma = \langle 2 \rangle_{\mathrm{div}}$, we have preferred to avoid such technical generalizations.

The plan of this paper is as follows. In section 2 we recall some results on higher ramification groups of the radical extension $\mathbb{Q}(\zeta_{p^r}, b^{1/p^s})$ for $r \geq s \geq 1$ which have been completely and explicitly described in Viviani's Master Thesis [8], written under the supervision of Dvornicich. In section 3 we prove our main result and we discuss some possible generalizations of our method.

Acknowledgement We would like to thank Sinnou David who first draw our attention to Conjecture 1.1. We are indebted to Gaël Rémond for thorough reading of a preliminary version of this paper and for the reference [7]. We also thank Sara Checcoli, Ilaria Del Corso and Roberto Dvornicich for a number of interesting and helpful remarks.

2 Ramifications

We are concerned with lower bounds for the height in the infinite extension

$$\mathbb{Q}(\zeta_p, b^{1/p}, \zeta_{p^2}, b^{1/p^2}, \zeta_{p^3}, b^{1/p^3}, \ldots)$$

where $b \geq 2$ is an integer and $p \geq 3$ is a prime which will remain both fixed for the rest of the paper. For technical reasons, we assume $p \nmid b$ and $p^2 \nmid (b^{p-1} - 1)$. We remark that, under the first assumption, the second hypothesis is equivalent to $b \notin \mathbb{Q}_p^p$.

Let r, s be integers with $r \geq s \geq 0$. We need some facts about the radical extension

$$L_{r,s} := \mathbb{Q}(\zeta_{p^r}, b^{1/p^s}) \, .$$

We easily see that $L_{r,s}/\mathbb{Q}$ is Galois (since $r \geq s$) of degree $\phi(p^r)p^s$. The last assertion is proved in [8], Corollary 2.7 if $r = s$. The same proof works if $r > s$.

Indeed, since $b \notin \mathbb{Q}_p^p$, we have $b \notin \mathbb{Q}^p$ which in turns implies $b \notin \mathbb{Q}(\zeta_{p^r})^p$ by a theorem of Schinzel ([8], Proposition 2.5) and thus $x^{p^s} - b$ is irreducible over $\mathbb{Q}(\zeta_{p^r})$ by a theorem of Capelli ([8], Theorem 2.1). By standard Galois Theory

$$\mathrm{Gal}(L_{r,s}/Q) \cong C(p^s) \rtimes G(p^r) \tag{2.1}$$

where $C(p^s) = \mathbb{Z}/p^s\mathbb{Z}$ and $G(p^r) = (\mathbb{Z}/p^r\mathbb{Z})^*$. The isomorphism is given by $\sigma \mapsto (i,k)$ where i and k are uniquely determined by $\sigma(b^{1/p^s}) = \zeta_{p^s}^i b^{1/p^s}$ and $\sigma(\zeta_{p^r}) = \zeta_{p^r}^k$. For later reference we recall that $G(p^r)$ has a filtration given by the subgroups $G(p^r)^j := \{k \in G(p^r) \text{ such that } k \equiv 1 \bmod p^j\}$ $(j = 0, \ldots, r)$. Remark that $G(p^r)^j$ is cyclic of order p^{r-j} for $j = 1, \ldots, r$, while $G(p^r)^0 = G(p^r)$.

We now recall some facts on the ramifications in the extension $L_{r,s}/\mathbb{Q}$.

Proposition 2.1. *Let r, s be integers with $r \geq s \geq 0$ and $r \geq 1$. Then:*

1) p is totally ramified in $L_{r,s}$. Thus $p\mathcal{O}_{L_{r,s}} = \mathfrak{Q}^e$ with

$$e := [L_{r,s} : \mathbb{Q}] = p^{r-1+s}(p-1)\ .$$

2) Let G_l be the last non trivial ramification group. Then

$$l = \begin{cases} \frac{2p^{2s-1}-p+1}{p+1}, & \text{if } r = s; \\ \frac{(p-1)(p^{2s}-1)}{p+1} + p^{2s}(p^{r-1-s}-1), & \text{if } r > s. \end{cases}$$

3) The fixed field of G_l is

$$L_{r,s}^{G_l} = \begin{cases} L_{r,s-1}, & \text{if } r = s; \\ L_{r-1,s}, & \text{if } r > s. \end{cases}$$

Proof. Let for short $L = L_{r,s}$.

There is only one prime $\mathfrak{Q}$ above p in the extension $L/\mathbb{Q}$ and the completion of L with respect to $\mathfrak{Q}$ is $\mathbb{Q}_p(\zeta_{p^r}, b^{1/p^s})$. If $r = s$, this is proved in [8], Corollary 2.7. The same proof works if $r > s$, as we briefly show. The minimal polynomial $X^{p^s} - b$ of b^{1/p^s} over $\mathbb{Q}(\zeta_{p^r})$ is still irreducible over $\mathbb{Q}_p(\zeta_{p^r})$ by a theorem of Schinzel ([8], Proposition 2.5), since $b \notin \mathbb{Q}_p^p$. A result of Kummer ([8], Lemma 5.1) shows now the desired assertion.

By Theorem 5.5 of [8], the local extension $\mathbb{Q}_p(\zeta_{p^r}, b^{1/p^s})/\mathbb{Q}_p$ is totally ramified. This concludes the proof of 1).

For the proof of 2), see [8], Theorem 5.8. This theorem also gives

$$G_l \cong \begin{cases} C(p), & \text{if } r = s; \\ G(p^r)^{r-1}, & \text{if } r > s \end{cases}$$

where the two groups on the right are naturally identified with subgroups of $C(p^s) \rtimes G(p^r)$ and where the isomorphism is the restriction of (2.1). Assertion 3) easily follows.

□

We also need the following elementary computation:

Lemma 2.2. *Let r, s, e and l be as in Lemma 2.1. Then $p^2(l+1) \geq e$ (and moreover $p(l+1) \geq e$ if $s = 0$ or $r \geq s+2$).*

Proof. Let us assume first $r = s$. Then, according to Proposition 2.1, $e = p^{2s-1}(p-1)$ and

$$l + 1 = \frac{2p^{2s-1} - p + 1}{p+1} + 1 = \frac{2(p^{2s-1}+1)}{p+1} .$$

Thus

$$p^2(l+1) - e = \frac{2p^2(p^{2s-1}+1) - p^{2s-1}(p^2-1)}{p+1} = \frac{p^{2s+1} + 2p^2 + p^{2s-1}}{p+1} > 0 .$$

Let now $r > s$. Proposition 2.1 gives $e = p^{r-1+s}(p-1)$ and

$$l + 1 = \frac{(p-1)(p^{2s}-1)}{p+1} + p^{2s}(p^{r-1-s} - 1) + 1 = p^{r-1+s} - \frac{2(p^{2s}-1)}{p+1} .$$

Thus, if $s = 0$ we have $p(l+1) = p^r > p^{r-1}(p-1) = e$. Similarly, if $r \geq s+2$,

$$p(l+1) - e = p^{r-1+s} - \frac{2p(p^{2s}-1)}{p+1} \geq p^{2s+1} - 2p^{2s} > 0 .$$

If instead $s \geq 1$ and $r = s+1$ we still have

$$p^2(l+1) - e = (p^2 - p + 1)p^{2s} - \frac{2p^2(p^{2s}-1)}{p+1} \geq (p^2 - 3p + 1)p^{2s} > 0 .$$

□

3 Metric properties and proof theorem 1.3.

Let $r \geq s \geq 0$ with $r \geq 1$. Put for short $L = \mathbb{Q}(\zeta_{p^r}, b^{1/p^s})$ and

$$\begin{aligned} &L_0 = \mathbb{Q}(\zeta_{p^r}, b^{1/p^{s-1}}), \quad g = b^{1/p^s}, \quad \text{if } r = s; \\ &L_0 = \mathbb{Q}(\zeta_{p^{r-1}}, b^{1/p^s}), \quad g = \zeta_{p^r}, \qquad \text{if } r > s. \end{aligned} \tag{3.1}$$

Thus $L = L_0(g)$ and L/L_0 is a cyclic extension of degree $p-1$ or p, depending on whether $(r,s) = (1,0)$ or not, with Galois group G_l (see proposition 2.1 point 3). We choose one of its generators σ. In both cases $\sigma g/g$ is a non trivial p-th root of unity.

The following lemma is the key ingredient of our proof. It generalizes the metric property of the ramified case of the lower bound for the height in abelian extensions ([1], lemma 2 and proposition 1). In the proof we use a simplification due to Habegger (see [5], lemma 4.2), which allow us to avoid the use of the Strong Approximation Theorem made in [1] (cf. lemma 1 therein).

Given a place v, we denote by $|\cdot|_v$ the corresponding absolute value normalized to induce on $\mathbb{Q}$ the underlying standard absolute value.

Lemma 3.1. *Let α, $\tilde{g} \in \overline{\mathbb{Q}}^*$ such that $\alpha/\tilde{g} \in L$. We assume:*

1) There exists an integer n such that $\tilde{g}^n \in L_0$;

2) For any place $v \,|\, p$ we have $|\tilde{g}|_v = 1$.

Then either there exists an integer j such that $\alpha/\tilde{g}g^j \in L_0$ or

$$h(\alpha) \geq \frac{\log(p/2)}{2p^2} \ .$$

Proof. We put for short $\beta = \alpha/\tilde{g} \in L$. Let E be the Galois closure of $L(\alpha) = L(\tilde{g})$ over L_0. We still denote by the same letter σ an arbitrary extension of σ to E. We make some elementary remarks.

Remark.

i) By 1) we have $\sigma\tilde{g} = \zeta\tilde{g}$ for some root of unity $\zeta \in E$. Thus $\sigma\beta = \sigma\alpha/\zeta\tilde{g}$ and

$$\sigma\beta^{p^2} - \beta^{p^2} = \big(\sigma\alpha^{p^2} - (\zeta\alpha)^{p^2}\big)/(\zeta\tilde{g})^{p^2} \ .$$

ii) Let v be a place of E dividing p. By 2) we have $|\tilde{g}|_v = 1$. Thus $|\beta|_v = |\alpha|_v$ and, by the previous remark, $|\sigma\beta|_v = |\sigma\alpha|_v$ and

$$|\sigma\beta^{p^2} - \beta^{p^2}|_v = |\sigma\alpha^{p^2} - (\zeta\alpha)^{p^2}|_v \ .$$

Let us now go on with the proof. Assume first $\sigma\beta^{p^2} = \beta^{p^2}$. Let $\omega := \sigma\beta/\beta \in L$. Then ω is a p^2-th root of unity. Since L_0 contains the p-th roots of unity, $\sigma\omega^p = \omega^p$ and thus $\sigma\omega = \eta\omega$ for some p-th root of unity $\eta \in L_0$. From $\sigma\beta = \omega\beta$ and $\sigma\omega = \eta\omega$ we deduce that $\sigma^j\beta = \eta^{1+\cdots+(j-1)}\omega^j\beta$ and thus $\beta = \sigma^p\beta = \omega^p\beta$ which tells us that ω is indeed a p-th root of unity. Since $\sigma g/g$ is a non trivial p-th root of unity, there exists j such that $\omega = \sigma g^j/g^j$. But then $\sigma\beta/\beta = \sigma g^j/g^j$ which shows that $\alpha/\tilde{g}g^j = \beta/g^j$ is in the subfield L_0 fixed by σ, as required.

Assume now $\sigma\beta^{p^2} \neq \beta^{p^2}$. By remark i) $\sigma\alpha^{p^2} \neq (\zeta\alpha)^{p^2}$. We want to apply the product formula to $\sigma\alpha^{p^2} - (\zeta\alpha)^{p^2}$.

Let v be a place of E dividing p and let w be the the restriction of v at L. Assume for the moment $\beta \in \mathcal{O}_w$ the ring of integers of the completion of L at w. By Proposition 2.1 points 1) and 2) we have $p\mathcal{O}_L = \mathfrak{Q}^e$ and $\sigma\beta - \beta \in \mathfrak{Q}^{l+1}$. By Lemma 2.2, we have $p^2(l+1) \geq e$. Thus

$$\sigma\beta^{p^2} - \beta^{p^2} \equiv (\sigma\beta - \beta)^{p^2} \equiv 0 \bmod p\mathcal{O}_w$$

and

$$|\sigma\beta^{p^2} - \beta^{p^2}|_v \leq p^{-1} .$$

If $\beta \notin \mathcal{O}_w$ we have $\beta^{-1} \in \mathcal{O}_w$ and the argument before gives $|\sigma\beta^{-p^2} - \beta^{-p^2}|_v \leq p^{-1}$ from which we easily deduce that

$$|\sigma\beta^{p^2} - \beta^{p^2}|_v \leq p^{-1} \max(1, |\sigma\beta|_v)^{p^2} \max(1, |\beta|_v)^{p^2}$$

Hence this inequality holds in both cases $\beta \in \mathcal{O}_w$ and $\beta^{-1} \in \mathcal{O}_w$. By remark ii)

$$|\sigma\alpha^{p^2} - (\zeta\alpha)^{p^2}|_v \leq p^{-1} \max(1, |\sigma\alpha|_v)^{p^2} \max(1, |\alpha|_v)^{p^2} .$$

For the other places v of E we use the trivial inequality

$$|\sigma\alpha^{p^2} - (\zeta\alpha)^{p^2}|_v \leq C(v) \max(1, |\sigma\alpha|_v)^{p^2} \max(1, |\alpha|_v)^{p^2}$$

with $C(v) = 1$ if $v \nmid \infty$ and $C(v) = 2$ otherwise. Collecting these inequalities in the product formula we get

$$0 \leq -\log p + \log 2 + p^2 h(\sigma\alpha) + p^2 h(\alpha) = 2p^2 h(\alpha) - \log(p/2) .$$

Hence

$$h(\alpha) \geq \frac{\log(p/2)}{2p^2}$$

as required.

□

Let Γ be a subgroup of $\overline{\mathbb{Q}}^*$ and let α be a non-zero algebraic number. Following Silverman (as quoted in [4]), we define the Γ-height of α as

$$h_\Gamma(\alpha) = \inf\{h(g\alpha) \text{ such that } g \in \Gamma\} .$$

For $\Gamma = \{1\}_{\text{div}}$ this is the usual Weil height of α. Obviously, $h_\Gamma(\alpha) = 0$ if $\alpha \in \Gamma$. On the other hand we cannot hope to reverse this statement for an arbitrary subgroup. However, for saturated (*i.e.* $\Gamma_{\text{div}} = \Gamma$) subgroups of finite rank, Rémond [7] proves an explicit lower bound of the shape $h_\Gamma(\alpha) \geq c(\Gamma, [\mathbb{Q}(\alpha) : \mathbb{Q}]) > 0$ for $\alpha \notin \Gamma$. We state a special case (which is enough for our purposes) of his result in the following lemma.

Lemma 3.2. *Let r, $b \in \mathbb{Q}^*$ and n, $x \in \mathbb{Z}$ with $b \neq \pm 1$ and $n \geq 1$. Let us assume that $r^N \notin \langle b \rangle$ for all positive integers N. Put $\alpha = rb^{x/n}$. Then*

$$h(\alpha) \geq \frac{1}{3h(b)} .$$

Proof. For l a rational prime we denote by v_l the l-adic valuation. Since $b \neq \pm 1$, the vector $\mathbf{v} = (v_l(b))_l$ is not zero. Since $r^N \notin \langle b \rangle$ for all positive integers N, the vector $\mathbf{v}' = (v_l(r))_l$ is not a rational multiple of v. Hence, $\mathbf{v}$ and $\mathbf{v}'$ are $\mathbb{Q}$-linearly independent, *i.e.* there exist two (distinct) primes l_1, l_2 such that

$$v_{l_1}(r)v_{l_2}(b) - v_{l_2}(r)v_{l_1}(b) \neq 0 .$$

Since $\alpha^n = r^n b^x \in \mathbb{Q}$, we have $v_l(\alpha^n) = nv_l(r) + xv_l(b)$. Therefore

$$|v_{l_1}(\alpha^n)v_{l_2}(b) - v_{l_2}(\alpha^n)v_{l_1}(b)| = n|v_{l_1}(r)v_{l_2}(b) - v_{l_2}(r)v_{l_1}(b)| \geq n .$$

For $a \in \mathbb{Q}$ we have $|v_l(a)| \leq h(a)/\log l$. Thus

$$n \leq |v_{l_1}(\alpha^n)| \cdot |v_{l_2}(b)| + |v_{l_2}(\alpha^n)| \cdot |v_{l_1}(b)| \leq \frac{2h(b)h(\alpha^n)}{\log l_1 \log l_2} \leq 3nh(b)h(\alpha) ,$$

since $2/(\log l_1 \log l_2) \leq 2/(\log 2 \log 3) \leq 3$.

□

We can now state and prove a lower bound for the height in the infinite extension $\mathbb{Q}(\zeta_p, b^{1/p}, \zeta_{p^2}, b^{1/p^2}, \zeta_{p^3}, b^{1/p^3}, \ldots)$.

Theorem 3.3. *Let $b \geq 2$ be an integer and let $p \geq 3$ be a prime number. We assume that $p \nmid b$ and $p^2 \nmid (b^{p-1} - 1)$. Then conjecture 1.2 holds for the subgroup*

$$\Gamma = \langle \zeta_{p^t}, b^{1/p^t} \rangle_{t \geq 1} .$$

More precisely, let

$$\alpha \in \mathbb{Q}(\zeta_p, b^{1/p}, \zeta_{p^2}, b^{1/p^2}, \zeta_{p^3}, b^{1/p^3}, \ldots)$$

be a non-zero algebraic number. Then either there exists a positive integer N such that $\alpha^N \in \langle b \rangle$ or

$$h(\alpha) \geq \min\left\{ \frac{1}{3h(b)}, \frac{\log(p/2)}{2p^2} \right\} .$$

Proof. Let α be as in the statement of the theorem. Thus there exists $t \geq 0$ such that $\alpha \in \mathbb{Q}(\zeta_{p^t}, b^{1/p^t})$. Let Λ be the set of couple (r, s) of integers with $t \geq r \geq s \geq 0$ and such that there exists $\tilde{g} \in \langle \zeta_{p^t}, b^{1/p^t} \rangle$ for which $\alpha/\tilde{g} \in \mathbb{Q}(\zeta_{p^r}, b^{1/p^s})$. We

remark that Λ is not empty, since $(t,t) \in \Lambda$. We select a minimal element (r,s) of Λ for the standard partial order[1] and we choose $\tilde{g} \in \langle \zeta_{p^t}, b^{1/p^t} \rangle$ such that

$$\alpha/\tilde{g} \in L := \mathbb{Q}(\zeta_{p^r}, b^{1/p^s}) \ .$$

If $r = s = 0$, then $\alpha/\tilde{g} \in \mathbb{Q}$ and, by lemma 3.2, either there exists a positive integer N such that $\alpha^N \in \langle b \rangle$ or

$$h(\alpha) \geq \frac{1}{3h(b)} \ .$$

Thus we may assume that $r \geq 1$. Let L_0 and g as in (3.1):

$$L_0 = \mathbb{Q}(\zeta_{p^r}, b^{1/p^{s-1}}), \qquad g = b^{1/p^s}, \qquad \text{if } r = s;$$

$$L_0 = \mathbb{Q}(\zeta_{p^{r-1}}, b^{1/p^s}), \qquad g = \zeta^{p^r}, \qquad \text{if } r > s.$$

We apply lemma 3.1. Assertions 1) and 2) of that lemma are clearly verified (the first one since $\tilde{g}^{p^t} \in \mathbb{Q}$; the second one by the assumption $p \nmid b$). By lemma 3.1, either there exists an integer j such that $\alpha/\tilde{g}g^j \in L_0$ or

$$h(\alpha) \geq \frac{\log(p/2)}{2p^2}$$

The first conclusion cannot hold. Indeed $\tilde{g}g^j \in \langle \zeta_{p^t}, b^{1/p^t} \rangle$ and, by minimality assumption on (r,s) we deduce that $\alpha/\tilde{g}g^j \notin L_0$. Thus the second conclusion of lemma 3.1 must hold.

□

In the special case $b = 2$, $p = 3$ we have

$$\min\left\{\frac{1}{3h(b)}, \frac{\log(p/2)}{2p^2}\right\} = \frac{\log(3/2)}{18} \ .$$

This proves theorem 1.3.

Remark 3.4. As already remarked in the introduction, our method could in principle be generalized to prove lower bounds for the height in some more general situation. Let K be a number field, G be a finitely generated subgroup of K^*, and S be a set of rational primes. We define the S-division group of G as the subgroup $G_{\mathrm{div},S}$ consisting of those $g \in \overline{\mathbb{Q}}^*$ such that there exists a positive integer n *whose prime factors are in* S for which $g^n \in G$. The standard definition of division group agrees with this one taking for S the set of all primes. We also remark that, for $G = \langle 2 \rangle$ and $S = \{3\}$ we have $G_{\mathrm{div},S} = \langle \zeta_{3^t}, 2^{1/3^t} \rangle_{t \in \mathbb{N}}$. Let us assume that S is finite and that $|g|_v = 1$ for all $g \in G$ and for all place v of K dividing a prime of S. The method of this paper could potentially be extended, at the price of a deeper analysis on the ramification in radical extensions, to prove conjecture 1.2 for $\Gamma = G_{\mathrm{div},S}$.

[1] *i.e.* $(r,s) \leq (r',s')$ if and only if $r \leq r'$ and $s \leq s'$.

References

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

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

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

[4] A. C. de la Maza and E. Friedman. "Heights of algebraic numbers modulo multiplicative group actions". *J. Number Theory* **128** (2008), 2199–2213.

[5] P. Habegger, "Small Height and Infinite Non-Abelian Extensions". *Duke Math. J.* **162** (2013), no. 11, 2027–2076.

[6] G. Rémond, "Généralisations du problème de Lehmer et applications à la conjecture de Zilber-Pink". Preprint 2011. To appear in *Séminaires et congrès.*

[7] G. Rémond, Private communication. 2013.

[8] F. Viviani, "Ramifications groups and Artin conductors of radical extensions of $\mathbb{Q}$". *J. Théor. Nombres Bordeaux* **16** (2004), 779–816.