ACTA ARITHMETICA
159.2 (2013)

On the exponential local-global principle

by

Boris Bartolome (Auréville), Yuri Bilu (Bordeaux)
and Florian Luca (México)

Dedicated to Andrzej Schinzel

1. Introduction. Let $\mathbb{K}$ be a number field, $\alpha_1, \dots, \alpha_m, \lambda_1, \dots, \lambda_m$ non-zero elements in $\mathbb{K}$, and S a finite set of places of $\mathbb{K}$ (containing all the infinite places) such that the ring of S-integers

$$\mathcal{O}_S = \mathcal{O}_{\mathbb{K},S} = \{\alpha \in \mathbb{K} : |\alpha|_v \le 1 \text{ for places } v \notin S\}$$

contains $\lambda_1, \dots, \lambda_m, \alpha_1, \dots, \alpha_m, \alpha_1^{-1}, \dots, \alpha_m^{-1}$. Then, for every $n \in \mathbb{Z}$,

$$A(n) = \lambda_1\alpha_1^n + \cdots + \lambda_m\alpha_m^n \in \mathcal{O}_S.$$

The expression $A(n)$ will be called a *power sum*. The following conjecture was suggested by Skolem [7].

Conjecture 1.1 (Exponential local-global principle). *Assume that for every non-zero ideal $\mathfrak{a}$ of the ring $\mathcal{O}_S$, there exists $n \in \mathbb{Z}$ such that $A(n) \equiv 0 \bmod \mathfrak{a}$. Then there exists $n \in \mathbb{Z}$ such that $A(n) = 0$.*

Some particular cases of this conjecture, all addressing the instance when $m = 2$ and $\{A(n)\}_{n\ge 0} \subseteq \mathbb{Z}$, have been dealt with in [1, 4, 5, 6]. For some results on the analogous Skolem conjecture over function fields, see [9].

In this note, we prove this conjecture in a special case. Let Γ be the multiplicative group generated by $\alpha_1, \dots, \alpha_m$. Then Γ is the product of a finite abelian group and a free abelian group of finite rank, say ρ. In this case we shall call $A(n)$ a *power sum of rank ρ.*

Theorem 1.2. *Conjecture* 1.1 *holds for power sums of rank one.*

Surprisingly enough, our proof makes no use of the Chebotarev theorem, usually an indispensable ingredient in this kind of arguments. Instead, it relies on two "heavy tools" from Diophantine Approximations. One is the

2010 *Mathematics Subject Classification*: Primary 11D61; Secondary 11J86, 11J87.
Key words and phrases: power sums, local-global principles, subspace theorem.

DOI: 10.4064/aa159-2-1

celebrated Subspace Theorem of Schmidt–Schlickewei, which is used through a theorem of Corvaja and Zannier (see Theorem 2.2). The other tool is Baker's inequality (see Theorem 3.5).

2. Heights and logarithmic gcd. In this section we recall and/or introduce the definitions of the height and of the logarithmic gcd, and of some related quantities, to be used throughout the article. We also state one theorem of Corvaja and Zannier and obtain its consequence which will be one of our principal tools.

2.1. Definitions. We normalize the absolute values on number fields so that they extend standard absolute values on $\mathbb{Q}$: if $v \mid p$ then $|p|_v = p^{-1}$ and if $v \mid \infty$ then $|2013|_v = 2013$. We denote by $M_{\mathbb{K}}$ the set of places (normalized absolute values) of the number field $\mathbb{K}$.

The *height* of an algebraic number α is defined as

$$\mathrm{h}(\alpha) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} [\mathbb{K}_v : \mathbb{Q}_v] \log^+ |\alpha|_v,$$

where $\mathbb{K}$ is a number field containing α and $\log^+ = \max\{\log, 0\}$. It is well-known that the height does not depend on the particular choice of $\mathbb{K}$, but only on the number α itself. It is equally well-known that $\mathrm{h}(\alpha) = \mathrm{h}(\alpha^{-1})$, so that

$$\mathrm{h}(\alpha) = \frac{1}{[\mathbb{K} : \mathbb{Q}]} \sum_{v \in M_{\mathbb{K}}} -[\mathbb{K}_v : \mathbb{Q}_v] \log^- |\alpha|_v = \sum_{v \in M_{\mathbb{K}}} \mathrm{h}_v(\alpha),$$

where $\log^- = \min\{\log, 0\}$ and

$$\mathrm{h}_v(\alpha) = -\frac{[\mathbb{K}_v : \mathbb{Q}_v]}{[\mathbb{K} : \mathbb{Q}]} \log^- |\alpha|_v.$$

The quantities $\mathrm{h}_v(\alpha)$ can be viewed as "local heights". Clearly, $\mathrm{h}_v(\alpha) \geq 0$ for any v and α.

We define the *logarithmic gcd* of two algebraic numbers α and β, not both 0, as

$$\mathrm{lgcd}(\alpha, \beta) = \sum_{v \in M_K} \min\{\mathrm{h}_v(\alpha), \mathrm{h}_v(\beta)\},$$

where $\mathbb{K}$ is a number field containing both α and β. Again, lgcd depends only on α and β, not on $\mathbb{K}$. A simple verification shows that for $\alpha, \beta \in \mathbb{Z}$ we have $\mathrm{lgcd}(\alpha, \beta) = \log \gcd(\alpha, \beta)$.

Now let $\mathbb{K}$ be a number field and S be a set of places of $\mathbb{K}$. We define the *S-height* and the *S-free height* by

$$\mathrm{h}_S(\alpha) = \sum_{v \in S} \mathrm{h}_v(\alpha), \qquad \mathrm{h}_{\neg S}(\alpha) = \mathrm{h}_{M_{\mathbb{K}} \setminus S}(\alpha) = \mathrm{h}(\alpha) - \mathrm{h}_S(\alpha).$$

Similarly we define lgcd_S and $\mathrm{lgcd}_{\neg S}$.

The following properties of heights and logarithmic gcd are straightforward and will be used in the text without special notice.

PROPOSITION 2.1.

(i) *For non-zero algebraic numbers* α, β, γ *we have*

$$\operatorname{lgcd}(\alpha\beta, \gamma) \le \operatorname{lgcd}(\alpha, \gamma) + \operatorname{lgcd}(\beta, \gamma),$$

and similarly for lgcd_S.

In the next items, $\mathbb{K}$ *is a number field,* S *is a set of places of* $\mathbb{K}$ *containing the infinite places, and* α, β, γ *belong to the ring* $\mathcal{O}_S$ *of* S*-integers.*

(ii) α *and* β *are co-prime in* $\mathcal{O}_S$ *if and only if* $\operatorname{lgcd}_{\neg S}(\alpha, \beta) = 0$.

(iii) *If* α *and* β *are co-prime in* $\mathcal{O}_S$ *then*

$$\operatorname{lgcd}_{\neg S}(\alpha\beta, \gamma) = \operatorname{lgcd}_{\neg S}(\alpha, \gamma) + \operatorname{lgcd}_{\neg S}(\beta, \gamma).$$

(iv) *We have* $\operatorname{lgcd}_{\neg S}(\alpha, \beta) \le \mathrm{h}_{\neg S}(\alpha)$, *with equality exactly when* α *divides* β *in* $\mathcal{O}_S$.

2.2. A theorem of Corvaja and Zannier. One of our main tools will be the following result of Corvaja and Zannier [2, p. 204, Corollary 1].

THEOREM 2.2. *Let* Γ *be a finitely generated subgroup of* $\bar{\mathbb{Q}}^\times$, *and* $\varepsilon > 0$. *Then for multiplicatively independent* $\alpha, \beta \in \Gamma$ *we have*

$$\operatorname{lgcd}(\alpha - 1, \beta - 1) \le \varepsilon \max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} + O(1),$$

where the constant implied by $O(1)$ *depends on* Γ *and* ε, *but not on* α *or* β.

The proof of this result is based on the Subspace Theorem of Schlickewei and Schmidt.

We shall use Theorem 2.2 through the following statement.

COROLLARY 2.3. *Let* $\mathbb{K}$ *be a number field,* S *a finite subset of* $M_{\mathbb{K}}$ *containing the infinite places,* $\beta, \gamma \in \mathcal{O}_S^\times$ *multiplicatively independent, and* $\varepsilon > 0$. *Then for* $k, n \in \mathbb{Z}$ *we have*

$$\operatorname{lgcd}_{\neg S}(\gamma^k - 1, \gamma^n - \beta) \le \varepsilon |k| + O(1),$$

where the implied constant depends on γ, β, $\mathbb{K}$, S *and* ε, *but not on* k *or* n.

Proof. Replacing, if necessary, γ by γ^{-1}, we may assume that $k > 0$. Also, since $n \equiv n' \bmod k$ implies the congruence $\gamma^n \equiv \gamma^{n'} \bmod (\gamma^k - 1)$ in the ring $\mathcal{O}_S$, we may assume that $0 \le n < k$. Applying Theorem 2.2 with $\Gamma = \langle \gamma, \beta \rangle$, with γ^k as α and with $\gamma^n \beta^{-1}$ as β, we obtain

$$\begin{aligned}\operatorname{lgcd}_{\neg S}(\gamma^k - 1, \gamma^n - \beta) &= \operatorname{lgcd}_{\neg S}(\gamma^k - 1, \gamma^n \beta^{-1} - 1) \le \operatorname{lgcd}(\gamma^k - 1, \gamma^n \beta^{-1} - 1) \\ &\le \varepsilon(k\mathrm{h}(\gamma) + \mathrm{h}(\beta)) + O(1) = \varepsilon \mathrm{h}(\gamma) k + O(1).\end{aligned}$$

Redefining ε, we obtain the result. ∎

3. Cyclotomic polynomials. In this section we establish properties of the cyclotomic polynomials, needed for the proof. We denote by $\Phi_k(T)$ the kth cyclotomic polynomial. Since $T^k - 1 = \prod_{d|k} \Phi_d(T)$, we have

$$\Phi_k(T) = \prod_{d|k} (T^d - 1)^{\mu(k/d)}, \tag{1}$$

where μ is the Möbius function. We shall systematically use this in what follows.

3.1. Divisibility. All the results of this subsection are well-known, but it is easier to supply quick proofs than to find references.

PROPOSITION 3.1. *Let k and l be distinct positive integers. Then the resultant of $\Phi_k(T)$ and $\Phi_l(T)$ divides (in $\mathbb{Z}$) a power of kl.*

Proof. The resultant of these polynomials is a product of factors of the type $\zeta_k - \zeta_l$, where ζ_k (respectively, ζ_l) is a primitive kth (respectively, lth) root of unity. The elementary theory of cyclotomic fields (see, for instance, [10, Chapters 1 and 2]) implies that $\zeta_k - \zeta_l$ divides kl in the ring $\mathbb{Z}[\zeta_{kl}]$. Hence the resultant divides a power of kl in $\mathbb{Z}[\zeta_{kl}]$. Since $\mathbb{Q} \cap \mathbb{Z}[\zeta_{kl}] = \mathbb{Z}$, the resultant divides the same power of kl in $\mathbb{Z}$. ∎

COROLLARY 3.2. *Let $\mathbb{K}, S$ be as in the Introduction, and k, l as in Proposition* 3.1.

(i) *Assume that S contains the places dividing kl. Then for any $\gamma \in \mathcal{O}_S$ we have $\gcd(\Phi_k(\gamma), \Phi_l(\gamma)) = 1$ in the ring $\mathcal{O}_S$; that is, no prime ideal of $\mathcal{O}_S$ divides both $\Phi_k(\gamma)$ and $\Phi_l(\gamma)$.*

(ii) *Assume that S contains the places dividing kl and $k \nmid l$. Then for any $\gamma \in \mathcal{O}_S$ we have $\gcd(\Phi_k(\gamma), \gamma^l - 1) = 1$ in the ring $\mathcal{O}_S$.*

(iii) *Assume that S contains the places dividing k. For $\gamma \in \mathcal{O}_S^\times$ let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_S$ dividing $\Phi_k(\gamma)$. Then γ is of exact order k in $(\mathcal{O}_S/\mathfrak{p})^\times$. In particular, if for some $n \in \mathbb{Z}$ we have $\gamma^n \equiv 1 \bmod \mathfrak{p}$ then $k \mid n$.*

Proof. Part (i) is immediate from Proposition 3.1. For (ii) observe that $\gamma^l - 1$ is a product of factors of the type $\Phi_{l'}(\gamma)$ with $l' \mid l$, and by the assumption none of these l' is equal to k. Hence (ii) follows from (i). Finally, (iii) follows immediately from (ii). ∎

3.2. Heights. We need an asymptotic expression for the height of the algebraic number $\Phi_k(\gamma)$, in terms of $\mathrm{h}(\gamma)$ and k. In general, if $f(x)$ is a polynomial with algebraic coefficients, then, using basic properties of heights, it is not difficult to show that $\mathrm{h}(f(\gamma)) = \deg f \, \mathrm{h}(\gamma) + O(1)$ as f is fixed and γ is varying. We, however, need a result of different type: find the asymptotics of $\mathrm{h}(\Phi_k(\gamma))$ as γ is fixed, but k is growing.

For a positive integer k we denote by $\varphi(k)$ the Euler function and by $\omega(k)$ the number of distinct prime divisors of k.

PROPOSITION 3.3. *Let γ be an algebraic number. Then*

$$|\mathrm{h}(\Phi_k(\gamma)) - \varphi(k)\mathrm{h}(\gamma)| \le 2^{\omega(k)}(\log k + O(1)),$$

where the constant implied by $O(1)$ depends on γ, but not on k.

The proof requires a complex analytic lemma.

LEMMA 3.4. *For a positive integer k we have*

$$\max_{|z|\le 1} \log|\Phi_k(z)| \le 2^{\omega(k)}(\log k + O(1)),$$

the maximum being over the unit disc on the complex plane, and the implied constant being absolute.

Proof. By the maximum principle, it suffices to show that

$$\log|\Phi_k(z)| \le 2^{\omega(k)}(\log k + O(1)) \tag{2}$$

for a complex z with $|z| = 1$. Thus, fix such z. We can write it in a unique way as $z = \zeta e^{2\pi i\theta/k}$, where ζ is a kth root of unity (not necessarily primitive) and $-1/2 < \theta \le 1/2$. Let l be the exact order of ζ; thus, l is a divisor of k and ζ is a primitive lth root of unity. Let d be any other divisor of k. If $l \nmid d$ then $2 \ge |z^d - 1| \ge 2\sin(\pi d/2k)$, which implies that

$$\big|\log|z^d - 1|\big| \le \log k + O(1). \tag{3}$$

And if $l \mid d$ then, we have $|z^d - 1| = 2\sin(\pi\theta d/k)$. Writing $d = d'l$, we get

$$\log|z^{d'l} - 1| = \log d' - \log(k/l\theta) + O(1). \tag{4}$$

Identity (1) implies that

$$\begin{aligned}\log|\Phi_k(z)| &= \sum_{d\mid k} \mu(k/d)\log|z^d - 1| \\ &= \sum_{d\mid k,\, l\nmid d} \mu(k/d)\log|z^d - 1| + \sum_{d'\mid k/l} \mu((k/l)/d')\log|z^{ld'} - 1|.\end{aligned}$$

Notice that the first sum above has at most $2^{\omega(k)} - 1$ non-zero summands. Now substituting here (3) and (4), we obtain

$$\begin{aligned}\log|\Phi_k(z)| &\le (2^{\omega(k)} - 1)(\log k + O(1)) + \sum_{d'\mid k/l} \mu\left(\frac{k/l}{d'}\right)\left(\log d' - \log\left(\frac{k}{l\theta}\right)\right) \\ &= (2^{\omega(k)} - 1)(\log k + O(1)) + \Lambda(k/l) - \delta\log(k/l\theta),\end{aligned}$$

where $\Lambda(\cdot)$ is the von Mangoldt function, $\delta = 0$ if $l < k$ and $\delta = 1$ if $l = k$. In any case we obtain (2), proving the lemma. ∎

Proof of Proposition 3.3. Fix a number field $\mathbb{K}$ containing γ. For a finite place v of $\mathbb{K}$ we obviously have

$$\log^+ |\Phi(\gamma)|_v = \begin{cases} \varphi(k) \log |\gamma|_v, & |\gamma|_v > 1, \\ 1, & |\gamma|_v \le 1. \end{cases} \tag{5}$$

For infinite places we have similar "approximate" statements

$$\log^+ |\Phi(\gamma)|_v \begin{cases} = \varphi(k) \log |\gamma|_v + O(2^{\omega(k)}), & |\gamma|_v > 1, \\ \le 2^{\omega(k)} (\log k + O(1)), & |\gamma|_v \le 1. \end{cases} \tag{6}$$

The second inequality follows from Lemma 3.4. To prove the first one, assume that $|\gamma|_v > 1$. Then for $n \ge 1$ we have $|\gamma^n - 1|_v = n \log |\gamma|_v + O(1)$. Using (1) we find

$$\begin{aligned} \log |\Phi_k(\gamma)|_v &= \sum_{d|k} \mu(k/d) \log |\gamma^d - 1|_v = \log |\gamma|_v \sum_{d|k} d\mu(k/d) + O(2^{\omega(k)}) \\ &= \varphi(k) \log |\gamma|_v + O(2^{\omega(k)}), \end{aligned}$$

as desired.

The (in)equalities (5) and (6) imply that

$$\left| \log^+ |\Phi(\gamma)|_v - \varphi(k) \log^+ |\gamma|_v \right| \begin{cases} = 0, & v \text{ finite}, \\ \le 2^{\omega(k)} (\log k + O(1)), & v \text{ infinite}. \end{cases}$$

Summing this up over $v \in M_{\mathbb{K}}$, we obtain the result. ∎

3.3. Using Baker's inequality. Besides Theorem 2.2 of Corvaja and Zannier, our second principal tool is the celebrated inequality of Baker (see the first two contributions in [11]).

THEOREM 3.5. *Let $\gamma_1, \dots, \gamma_r$ be non-zero algebraic numbers, and v a place of a number field containing them. Then for any $n_1, \dots, n_r \in \mathbb{Z}$ we have either $\gamma_1^{n_1} \cdots \gamma_r^{n_r} = 1$ or*

$$|\gamma_1^{n_1} \cdots \gamma_r^{n_r} - 1|_v \ge e^{-C \log N}, \qquad N = \max\{2, n_1, \dots, n_r\},$$

where C is a positive constant depending on $\gamma_1, \dots, \gamma_r$ and v, but not on $n_1, \dots, n_r$.

We deduce from it the following property of cyclotomic polynomials, inspired by the work of Schinzel [3] and Stewart [8].

PROPOSITION 3.6. *Let $\mathbb{K}$ be a number field, S a finite set of places of $\mathbb{K}$, and $\gamma \in \mathbb{K}$ not a root of unity. Then for any integer $k > 1$ we have*

$$\mathrm{h}_S(\Phi_k(\gamma)) = O(2^{\omega(k)} \log k),$$

where the implied constant depends on $\mathbb{K}$, S and γ, but not on k.

Proof. Since the set S is finite, it suffices to prove that for any $v \in M_{\mathbb{K}}$ we have

$$\mathrm{h}_v(\Phi_k(\gamma)) = O(2^{\omega(k)} \log k);$$

here and below the constants implied by $O(\cdot)$ depend only on γ and v. Equivalently, we have to show that

$$\left|\log^- |\Phi_k(\gamma)|_v\right| = O(2^{\omega(k)} \log k). \tag{7}$$

If $|\gamma|_v > 1$ then $\log |\Phi_k(\gamma)|_v = \varphi(k) \log |\gamma|_v + O(2^{\omega(k)})$ (see the proof of Proposition 3.3). It follows that $\log^- |\Phi_k(\gamma)|_v = O(2^{\omega(k)})$, better than (7).

Now assume that $|\gamma|_v \le 1$. Using Theorem 3.5 with $r = 1$, we deduce that $|\gamma^n - 1|_v \ge e^{-C \log n}$ with $C > 0$ depending on γ and v. Hence

$$\log 2 \ge \log |\gamma^n - 1|_v \ge -C \log n,$$

which implies that $\left|\log |\gamma^n - 1|_v\right| = O(\log n)$. Using (1), we obtain

$$\log |\Phi_k(\gamma)|_v = \sum_{d|k} \mu(k/d) \log |\gamma^d - 1|_v = O(2^{\omega(k)} \log k),$$

which proves (7). ∎

Combining Propositions 3.3 and 3.6, we obtain

COROLLARY 3.7. *In the set-up of Proposition* 3.6 *we have*

$$\mathrm{h}_{\neg S}(\Phi_k(\gamma)) = \varphi(k)\mathrm{h}(\gamma) + O(2^{\omega(k)} \log k).$$

4. Proof of Theorem 1.2. Let $A(n) = \lambda_1 \alpha_1^n + \cdots + \lambda_m \alpha_m^n$ be a power sum of rank 1. Assume that

(L) for every non-zero ideal $\mathfrak{a}$ of the ring $\mathcal{O}_S$ there exists $n \in \mathbb{Z}$ such that $A(n) \equiv 0 \bmod \mathfrak{a}$.

We want to prove that

(G) there exists $n \in \mathbb{Z}$ such that $A(n) = 0$.

4.1. General observations. We start with some general observations, which hold true for any power sum, not just power sums of rank 1.

Extension of the set of places. We may replace the set S by any bigger (finite) set of places. Indeed, condition (G) does not depend on S, and condition (L) becomes weaker when S is replaced by a bigger set. In particular, extending the set S, we may assume that

$$\lambda_1, \ldots, \lambda_m \in \mathcal{O}_S^\times. \tag{8}$$

Extension of the base field. We may replace the field $\mathbb{K}$ by a finite extension $\mathbb{K}'$, the set S being replaced by the set of places S' of $\mathbb{K}'$ extending those from $\mathbb{K}$. Condition (G) is again not concerned, and condition (L) is replaced by an equivalent one (each ideal of $\mathcal{O}_{\mathbb{K}',S'}$ is contained in an ideal coming from $\mathcal{O}_{\mathbb{K},S}$).

The group Γ is torsion-free. We may assume that the group Γ, generated by the "roots" $\alpha_1, \ldots, \alpha_m$, is torsion-free. Indeed, since it is finitely generated, its torsion subgroup is finite; denote its order by μ. Then the group $\Gamma^\mu = \{x^\mu : x \in \Gamma\}$ is torsion-free. Now consider instead of $A(n)$ the power sum

$$\widetilde{A}(n) = A(\mu n)A(\mu n + 1) \cdots A(\mu n + \mu - 1) = \tilde{\lambda}_1 \tilde{\alpha}_1^n + \cdots + \tilde{\lambda}_{\widetilde{m}} \tilde{\alpha}_{\widetilde{m}}^n.$$

Clearly, each of the conditions (L) and (G) holds simultaneously for $A(n)$ and $\widetilde{A}(n)$, and the group generated by $\tilde{\alpha}_1, \ldots, \tilde{\alpha}_m$ is contained in Γ^μ, a torsion-free group. Hence we may replace $A(n)$ by $\widetilde{A}(n)$ and assume that Γ is torsion-free.

4.2. Using the rank 1 assumption. Now we use the assumption that the rank of Γ is 1. Since we may assume that Γ is torsion-free, this means that $\Gamma = \langle\gamma\rangle$, where $\gamma \in \mathbb{K}^\times$ is not a root of unity. Write $\alpha_j = \gamma^{\nu_j}$ with $\nu_j \in \mathbb{Z}$. Assuming that $\nu_1 < \cdots < \nu_m$, we write

$$A(n) = \lambda_m \gamma^{\nu_1 n} P(\gamma^n),$$

where

$$P(T) = T^{\nu_m - \nu_1} + \frac{\lambda_{m-1}}{\lambda_m} T^{\nu_{m-1} - \nu_1} + \cdots + \frac{\lambda_2}{\lambda_m} T^{\nu_2 - \nu_1} + \frac{\lambda_1}{\lambda_m} \in \mathbb{K}[T].$$

Extending the field $\mathbb{K}$, we may assume that it contains all the roots of the polynomial $P(T)$. It follows from (8) that

(9) the roots of $P(T)$ are S-units.

Condition (G) is equivalent to saying that one of the roots of $P(T)$ belongs to Γ. Thus, we assume from now on that

(10) no root of $P(T)$ belongs to Γ,

and we shall find a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_S$ such that $P(\gamma^n) \not\equiv 0 \bmod \mathfrak{a}$ for any $n \in \mathbb{Z}$. This will prove the theorem, since $A(n)$ is equal to $P(\gamma^n)$ times an S-unit.

4.3. The ideal $\mathfrak{a}$. We are going now to define the ideal $\mathfrak{a}$. First of all, we split the polynomial $P(T)$ into two factors: $P(T) = P_{\mathrm{ind}}(T)P_{\mathrm{dep}}(T)$, such that each of the roots of $P_{\mathrm{ind}}(T)$ is multiplicatively independent of γ, and those of $P_{\mathrm{dep}}(T)$ are multiplicatively dependent on γ. Fix a positive integer q such that $\beta^q \in \Gamma$ for every root β of $P_{\mathrm{dep}}(T)$. Then for every such β we have $\beta^q = \gamma^r$, where $r = r(\beta) \in \mathbb{Z}$. Further, fix a prime number p, not dividing q and such that

(11) $$r(\beta) \not\equiv r(\beta') \bmod p$$

for any roots β, β' of $P_{\mathrm{dep}}(T)$ such that $r(\beta) \neq r(\beta')$. Extending the set S we may assume that

(12) all places dividing pq belong to S.

Assumption (12) has one implication that will be crucial in the sequel.

OBSERVATION. *Let ζ_μ be a primitive μth root of unity for some $\mu \mid pq$. Then ζ_μ is of exact order μ modulo $\mathfrak{p}$ for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_S$.*

Indeed, if this is not true, then $\mathfrak{p} \mid \zeta_{\mu'} - 1$ for some $\mu' \mid \mu$, $\mu' > 1$, which implies that $\mathfrak{p} \mid \mu$, contradicting (12).

We let $\mathfrak{a}$ be the principal ideal generated by $a = \Phi_{p^l}(\gamma)\Phi_{p^lq}(\gamma)$, where Φ_k denotes the kth cyclotomic polynomial and the positive integer l will be specified later. We will show that both $P_{\mathrm{ind}}(\gamma^n)$ and $P_{\mathrm{dep}}(\gamma^n)$ have a "small" common divisor with $\mathfrak{a}$. This will imply that, when l is chosen suitably, $P(\gamma^n)$ cannot be divisible by $\mathfrak{a}$ for any n.

Until the end of the proof the constants implied by $O(\cdot)$ may depend on the polynomial $P(T)$, on γ, on p and q, and on the parameter ε introduced below, but they do not depend on l or n.

We claim the following.

CLAIM I. Fix $\varepsilon > 0$. Then for any $n \in \mathbb{Z}$ we have

$$\mathrm{lgcd}_{\neg S}(P_{\mathrm{ind}}(\gamma^n), a) \leq \varepsilon p^l + O(1).$$

CLAIM D. *Let n be a rational integer. Then in the ring $\mathcal{O}_S$ we have either* $\gcd(P_{\mathrm{dep}}(\gamma^n), \Phi_{p^l}(\gamma)) = 1$ *or* $\gcd(P_{\mathrm{dep}}(\gamma^n), \Phi_{p^lq}(\gamma)) = 1$.

We postpone the proof of the claims until later, and now show how they imply the theorem.

4.4. Proof of the theorem (assuming the claims). Assuming the claims, we will now show that when the parameter l is chosen large enough, we have $P(\gamma^n) \not\equiv 0 \bmod \mathfrak{a}$ for any $n \in \mathbb{Z}$.

Thus, assume that for some n we have $P(\gamma^n) \equiv 0 \bmod \mathfrak{a}$. In other words, both $\Phi_{p^l}(\gamma)$ and $\Phi_{p^lq}(\gamma)$ divide $P(\gamma^n)$ in the ring $\mathcal{O}_S$. In addition, Corollary 3.2(i) together with (12) implies that they are co-prime in $\mathcal{O}_S$. It follows that

$$\begin{aligned}(13)\quad \mathrm{lgcd}_{\neg S}(P(\gamma^n), a) &= \mathrm{lgcd}_{\neg S}(P(\gamma^n), \Phi_{p^l}(\gamma)) + \mathrm{lgcd}_{\neg S}(P(\gamma^n), \Phi_{p^lq}(\gamma)) \\ &= \mathrm{h}_{\neg S}(\Phi_{p^l}(\gamma)) + \mathrm{h}_{\neg S}(\Phi_{p^lq}(\gamma)) \\ &= \varphi(p^l)\mathrm{h}(\gamma) + \varphi(p^lq)\mathrm{h}(\gamma) + O(l)\end{aligned}$$

(see Corollary 3.7).

On the other hand, Claim D implies that

$$\mathrm{lgcd}_{\neg S}(P_{\mathrm{dep}}(\gamma^n), a) \leq \max\{\mathrm{h}_{\neg S}(\Phi_{p^l}(\gamma)), \mathrm{h}_{\neg S}(\Phi_{p^lq}(\gamma))\} = \varphi(p^lq)\mathrm{h}(\gamma) + O(l),$$

again by Corollary 3.7. Combining this with Claim I, we obtain

$$\lgcd_{\neg S}(P(\gamma^n), a) \le \varepsilon p^l + \varphi(p^l q)\mathrm{h}(\gamma) + O(l). \tag{14}$$

Now select ε to have $\varepsilon < (1 - p^{-1})\mathrm{h}(\gamma)$. Then (13) and (14) become contradictory for large l. This proves the theorem. ∎

4.5. Proof of Claim I. Clearly, $a \mid \gamma^{p^l q} - 1$. Corollary 2.3 implies that

$$\lgcd_{\neg S}(\gamma^n - \beta, a) \le \lgcd_{\neg S}(\gamma^n - \beta, \gamma^{p^l q} - 1) \le \varepsilon p^l q + O(1).$$

Hence

$$\lgcd_{\neg S}(P_{\mathrm{ind}}(\gamma^n), a) \le \varepsilon p^l q \deg P_{\mathrm{ind}} + O(1).$$

Redefining ε, we obtain the result. ∎

4.6. Proof of Claim D. Let us assume the contrary and let $\mathfrak{p}, \mathfrak{p}'$ be prime ideals of $\mathcal{O}_S$ such that

$$\mathfrak{p} \mid \gcd(P_{\mathrm{dep}}(\gamma^n), \Phi_{p^l}(\gamma)) \quad \text{and} \quad \mathfrak{p}' \mid \gcd(P_{\mathrm{dep}}(\gamma^n), \Phi_{p^l q}(\gamma)).$$

There exist (not necessarily distinct) roots β, β' of $P_{\mathrm{dep}}(T)$ such that

$$\gamma^n \equiv \beta \bmod \mathfrak{p}, \qquad \gamma^n \equiv \beta' \bmod \mathfrak{p}'.$$

Further, let $r \in \mathbb{Z}$ be such that $\beta^q = \gamma^r$ (see the beginning of Subsection 4.3). Then $\gamma^{qn-r} \equiv 1 \bmod \mathfrak{p}$.

On the other hand, Corollary 3.2(iii) implies that for any root β of $P_{\mathrm{ind}}(T)$ we have

$$\gamma \text{ is of exact order } p^l \text{ in } (\mathcal{O}_S/\mathfrak{p})^\times. \tag{15}$$

In particular, $qn \equiv r \bmod p^l$. Similarly, if $r' \in \mathbb{Z}$ is such that $(\beta')^q = \gamma^{r'}$ then Corollary 3.2(iii) implies that $qn \equiv r' \bmod p^l q$. We obtain the congruence $r \equiv r' \bmod p$, which, by our choice of p (see (11)), implies that $r = r'$. Thus, we have $qn \equiv r \bmod p^l q$, which gives $q \mid r$. It follows that $\beta = \zeta\gamma^\nu$ with $\nu \in \mathbb{Z}$ and ζ a qth root of unity, not necessarily primitive.

Now it is time to use our basic assumption (10). We deduce that $\beta \notin \Gamma$, which means that $\zeta \ne 1$. Thus, $\zeta = \zeta_\mu$ is a primitive μth root of unity with $\mu \mid q$ and $\mu > 1$.

Since $\zeta_\mu \equiv \gamma^{n-\nu} \bmod \mathfrak{p}$, the image of ζ_μ in $(\mathcal{O}_S/\mathfrak{p})^\times$ belongs to the subgroup generated by the image of γ. Hence the order of ζ_μ modulo $\mathfrak{p}$ divides the order of γ. But the order of ζ_μ is μ (see the Observation in Subsection 4.3), and the order of γ is p^l (see (15)). Thus, $\mu \mid p^l$, which contradicts co-primarity of p and q. This proves the claim. ∎

Acknowledgments. Boris Bartolome and Florian Luca were supported by the joint Franco-Mexican project CNRS/CONACYT 25224/171999 *Lin-*

ear recurrences, arithmetic functions and additive combinatorics. Yuri Bilu was supported by the *Agence Nationale de la Recherche* project "HAMOT" (ANR 2010 BLAN-0115-01), by the ALGANT scholarship program and by the Hausdorff Research Institute for Mathematics.

References

[1] K. A. Broughan and F. Luca, *On the Fürstenberg closure of a class of binary recurrences*, J. Number Theory 130 (2010), 696–706.

[2] P. Corvaja and U. Zannier, *A lower bound for the height of a rational function at S-unit points*, Monatsh. Math. 144 (2005), 203–224.

[3] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. 268/269 (1974), 27–33.

[4] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. 27 (1975), 397–420.

[5] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. 32 (1977), 245–274; Addendum and corrigendum, ibid. 36 (1980), 101–104.

[6] A. Schinzel, *On the congruence $u_n \equiv c \pmod p$, where u_n is a recurring sequence of the second order*, Acta Acad. Paedagog. Agriensis Sect. Math. 30 (2003), 147–165.

[7] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Avhdl. Norske Vid. Akad. Oslo I, 1937, no. 12, 16 pp.

[8] C. L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, in: A. Baker and D. W. Masser (eds.), Transcendence Theory: Advances and Applications, Academic Press, London, 1977, 79–92.

[9] C. L. Sun, *Solutions of a linear equation in a subgroup of units in a function field*, arXiv:1101.3045.

[10] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

[11] G. Wüstholz (ed.), *A Panorama of Number Theory, or The View from Baker's Garden*, Cambridge Univ. Press, Cambridge, 2002.

Boris Bartolome
Enteleia Tech
La Cour
31320 Auréville, France
E-mail: Boris.Bartolome@enteleia.com

Yuri Bilu
IMB, Université Bordeaux 1
351 cours de la Libération
33405 Talence France
E-mail: yuri@math.u-bordeaux1.fr

Florian Luca
Fundación Marcos Moshinsky
Circuito Exterior, C.U., Apdo. Postal 70-543
Mexico D.F. 04510, México
E-mail: fluca@matmor.unam.mx

Received on 27.2.2012
and in revised form on 20.3.2013 (6988)