PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 37–41

Alina Ostafe

On some extensions of the Ailon-Rudnick Theorem

written by Lorenzo Menici

Let $a, b \in \mathbb{N}_{\geq 2}$ be multiplicatively independent in $\mathbb{Q}^*$. The quantity $\gcd(a^n - 1, b^n - 1)$, $n \in \mathbb{N}$, has been investigated by several authors. An important result was obtained by Bugeaud, Corvaja and Zannier [3], who proved that for any $\epsilon > 0$,

$$\gcd(a^n - 1, b^n - 1) \leq \exp(\epsilon n) ,$$

as n tends to infinity.

The function field analogue, given $f, g \in \mathbb{C}[X]$, corresponds to finding upper bounds for $\deg \gcd(f^n - 1, g^n - 1)$. The following definition is central for the next results.

Definition 1 *The polynomials* $F_1, \dots, F_s \in \mathbb{C}[X_1, \dots, X_\ell]$ *are multiplicatively independent if there exists no nonzero vector* $(\nu_1, \dots, \nu_s)$ *in* $\mathbb{Z}^s$ *such that*

$$F_1^{\nu_1} \cdots F_s^{\nu_s} = 1.$$

Similarly, the polynomials $F_1, \dots, F_s \in \mathbb{C}[X_1, \dots, X_\ell]$ *are multiplicatively independent in the group* $\mathbb{C}(X_1, \dots, X_\ell)^*/\mathbb{C}^*$ *if there exists no nonzero vector* $(\nu_1, \dots, \nu_s) \in \mathbb{Z}^s$ *and* $a \in \mathbb{C}^*$ *such that*

$$F_1^{\nu_1} \cdots F_s^{\nu_s} = a.$$

Ailon and Rudnick [1] showed that for multiplicatively independent polynomials $f, g \in \mathbb{C}[X]$, there exists $h \in \mathbb{C}[X]$ such that

$$\gcd(f^n - 1, g^n - 1) \mid h \tag{1}$$

for all $n \geq 1$. If in addition $\gcd(f - 1, g - 1) = 1$, then there is a finite union of arithmetic progressions $\cup_{d_i}\mathbb{N}$, $d_i \geq 2$, such that, for n outside these progressions, $\gcd(f^n - 1, g^n - 1) = 1$.

Corvaja and Zannier [4] extended the result of Ailon and Rudnick [1] to S-units: let $S \subset \mathbb{C}$ be a finite set and let $u, v \in \mathbb{C}(X)$ be multiplicatively independent rational functions with all their zeroes and poles in S. Then

$$\deg \gcd(u - 1, v - 1) \ll \max(\deg u, \deg v)^{2/3}. \tag{2}$$

As a corollary, if $f, g \in \mathbb{C}[X]$ are multiplicatively independent, then one gets $\deg \gcd(f^n - 1, g^n - 1) \ll n^{2/3}$, which improves the trivial bound $\ll n$.

In [5] several extensions of the Ailon-Rudnick theorem over $\mathbb{C}$ are developed in order to study:

1. $\gcd\left(h_1(f^n), h_2(g^m)\right)$, where $h_1, h_2 \in \mathbb{C}[X]$;
2. $\gcd\left(f_1^{n_1} \cdots f_\ell^{n_\ell} - 1, g_1^{m_1} \cdots g_r^{m_r} - 1\right)$, where $f_1, \ldots, f_\ell$ and g_1, $\ldots, g_r$ belong to $\mathbb{C}[X]$;
3. $\gcd\left(h_1(F^n), h_2(G^m)\right)$, where $h_1, h_2 \in \mathbb{C}[X]$ and both F and G belong to $\mathbb{C}[X_1, \ldots, X_m]$;
4. the set of common zeros of $F_1^{n_1} - 1, \ldots, F_{\ell+1}^{n_{\ell+1}} - 1$ over $\mathbb{C}$, which is denote by $Z\left(F_1^{n_1} - 1, \ldots, F_{\ell+1}^{n_{\ell+1}} - 1\right)$, where $F_1, \ldots, F_{\ell+1} \in \mathbb{C}[X_1, \ldots, X_\ell]$.

The goal is to obtain uniform bounds for the degree of these gcd's in the sense that they do not depend on the powers $n, m, \ldots$.

Using a uniform bound for the number of points on a curve with coordinates roots of unity due to Beukers and Smyth [2], one obtains an upper bound on $\deg\gcd(f^n-1, g^m-1)$ that depends only the degrees of f and g:

Lemma 1 *Let $f, g \in \mathbb{C}[X]$ be non constant polynomials. If f and g are multiplicatively independent, then*

$$\deg\gcd\left(f^n-1, g^m-1\right) \leq \left(11(d_f+d_g)^2\right)^{\min(d_f,d_g)}.$$

for all $n, m \geq 1$.

This result can be generalized to:

Theorem 2 *Let $f, g, h_1, h_2 \in \mathbb{C}[X]$. If f and g are multiplicatively independent in $\mathbb{C}(X)^*/\mathbb{C}^*$, then*

$$\deg\gcd\left(h_1\left(f^n\right), h_2\left(g^m\right)\right) \leq d_{h_1}d_{h_2}\left(11(d_f+d_g)^2\right)^{\min(d_f,d_g)}.$$

for all $n, m \geq 1$.

Another extension of the Ailon-Rudnick theorem obtained in [5] is the following:

Theorem 3 *Let $f_1, \dots, f_\ell, g_1, \dots, g_r \in \mathbb{C}[X]$, $\ell, r \geq 1$, be multiplicatively independent polynomials. Then, for all $n_1, \dots, n_\ell, m_1, \dots, m_r \geq 1$, there exists a polynomial $h \in \mathbb{C}[X]$ such that*

$$\gcd\left(f_1^{n_1}\cdots f_\ell^{n_\ell}-1, g_1^{m_1}\cdots g_r^{m_r}-1\right) \mid h.$$

If in addition

$$\gcd(f_1\cdots f_\ell-1, g_1\cdots g_r-1) = 1,$$

then there exists a finite number of monoids $\mathcal{L}_s$ in $\mathbb{N}^{\ell+r}$ such that $\mathbb{N}^{\ell+r}\setminus\cup_s\mathcal{L}_s$ is infinite and for any vector $(n_1, \dots, n_\ell, m_1, \dots, m_r) \in \mathbb{N}^{\ell+r}\setminus\cup_s\mathcal{L}_s$,

$$\gcd\left(f_1^{n_1}\cdots f_\ell^{n_\ell}-1, g_1^{m_1}\cdots g_r^{m_r}-1\right) = 1.$$

Theorem 3 can also be reformulated in terms of S-units in $\mathbb{C}[X]$ and gives a uniform bound for $\deg\gcd(u-1, v-1)$. Such a uniform bound is not present in (2) which, on the other hand, applies to more general situations.

It might be possible to unify Theorems 2 and 3 to obtain a similar result for

$$\gcd\left(h_1\left(f_1^{n_1}\cdots f_\ell^{n_\ell}\right), h_2\left(g_1^{m_1}\cdots g_r^{m_r}\right)\right),$$

where $h_1, h_2 \in \mathbb{C}[X]$. Similar ideas may work for this case however they require a uniform bound for the number of points on intersections of curves in the torus $\mathbb{G}_m^{\ell+r}$ with algebraic subgroups of dimension $k \leq \ell + r - 2$, which is not available. This will also give a bound for $\deg h$ in Theorem 3.

In the multivariate case, applying Hilbert's Irreducibility Theorem to reduce via specializations to the univariate case, we get:

Theorem 4 *Let $h_1, h_2 \in \mathbb{C}[X]$ and $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$. We denote by*

$$D = \max_{i=1\ldots,\ell}\left(\deg_{X_i} F, \deg_{X_i} G\right).$$

If F, G are multiplicatively independent in $\mathbb{C}(X_1, \ldots, X_\ell)^*/\mathbb{C}^*$, then for all $n, m \geq 1$ we have

$$\deg\gcd\left(h_1\left(F^n\right), h_2\left(G^m\right)\right) \leq d_{h_1} d_{h_2}\left(44(D+1)^{2\ell}\right)^{(D+1)^\ell}.$$

Lastly, for an integer $D \geq 1$, if we denote $\gamma_\ell(D) = \binom{\ell+1+D^\ell}{\ell+1}$, then we have the following result:

Theorem 5 *Let $F_1, \ldots, F_{\ell+1} \in \mathbb{C}[X_1, \ldots, X_\ell]$ be multiplicatively independent polynomials of degree at most D. Then,*

$$\bigcup_{n_1,\ldots,n_{\ell+1}\in\mathbb{N}} Z\left(F_1^{n_1} - 1, \ldots, F_{\ell+1}^{n_{\ell+1}} - 1\right)$$

is contained in at most

$$N \leq \left(0.792\gamma_\ell(D)/\log\left(\gamma_\ell(D)+1\right)\right)^{\gamma_\ell(D)}$$

algebraic varieties, each defined by at most $\ell+1$ polynomials of degree at most

$$(\ell+1)D^{\ell}\prod_{p\le\gamma_\ell(D)} p$$

(the product runs over all primes $p \le \gamma_\ell(D)$).

References

[1] N. Ailon and Z. Rudnick, *Torsion points on curves and common divisors of a^k-1 and b^k-1*, Acta Arith., **113** (2004), no. 1, 31–38.

[2] F. Beukers and C. J. Smyth, *Cyclotomic points on curves*, Number Theory for the Millenium (Urbana, Illinois, 2000), I, A K Peters, 2002, 67–85.

[3] Y. Bugeaud, P. Corvaja and U. Zannier, *An upper bound for the G.C.D. of a^n-1 and b^n-1*, Math. Z., **243** (2003), 79–84.

[4] P. Corvaja and U. Zannier, *Some cases of Vojtas conjecture on integral points over function fields*, J. Alg. Geom., **17** (2008), 295–333.

[5] A. Ostafe, *On some extensions of the Ailon-Rudnick Theorem*, `arXiv:1505.03957` (2015).

Lorenzo Menici,
Dipartimento di Matematica e Fisica
Università Roma Tre
L.go San Leonardo Murialdo 1
00146, Roma Italy.
email: `menici@mat.uniroma3.it`