ON SOME EXTENSIONS OF THE AILON-RUDNICK THEOREM

ABSTRACT

ALINA OSTAFE
UNIVERSITY OF NEW SOUTH WALES

Let a, b be multiplicatively independent positive integers and $\varepsilon > 0$. Bugeaud, Corvaja and Zannier (2003) proved that

$$\gcd\left(a^n - 1, b^n - 1\right) \le \exp(\varepsilon n)$$

for a sufficiently large n. Moreover, Ailon and Rudnick conjectured that when $\gcd(a-1, b-1) = 1$, then $\gcd(a^n - 1, b^n - 1) = 1$ infinitely often. Using finiteness of the number of torsion points on curves, Ailon and Rudnick (2004) proved the function field analogue of this conjecture, in a stronger version, that is, if $f, g \in \mathbb{C}[X]$ are multiplicatively independent polynomials, then there exists $h \in \mathbb{C}[X]$ such that for all $n \ge 1$ we have

$$\gcd(f^n - 1, g^n - 1) \mid h.$$

In this talk we present some extensions of this result, both in the univariate and multivariate cases.

Using a a uniform bound for the number of points on a curve with coordinates roots of unity due to Beukers and Smyth (2002), combined with Hilbert's Irreducibility Theorem, we give a uniform bound for

$$\deg \gcd\left(h_1\left(F^n\right), h_2\left(G^m\right)\right),$$

where $h_1, h_2 \in \mathbb{C}[X]$ and $F, G \in \mathbb{C}[X_1, \ldots, X_m]$, $m \ge 1$, satisfy the more restrictive condition of being multiplicatively independent polynomials with constants.

Moreover, using a finiteness result of Bombieri, Masser and Zannier (2008) for the number of points on the intersection of curves in $\mathbb{G}_m^n$ with algebraic subgroups, we conclude similar result for

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

where $f_1, \ldots, f_\ell, g_1, \ldots, g_r \in \mathbb{C}[X]$, $\ell, r \ge 1$, are multiplicatively independent.

E-mail address: `alina.ostafe@unsw.edu.au`