Johann Radon Institute for Computational and Applied Mathematics Austrian Academy of Sciences (ÖAW)

Group Seminar

Applied Discrete Mathematics and Cryptography

On the GCD of shifted polynomial powers, iterations and their relatives

Alina Ostafe, University of New South Wales, Sydney

Tuesday, July 30, 2019, 10:00
SP2 416-2

Abstract

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

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

for a sufficiently large n. Ailon and Rudnick (2004) considered the function field analogue and proved a much stronger result, 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 $n \geq 1$ we have

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

In this talk we present several extensions of the result of Ailon and Rudnick, both in the univariate and multivariate cases. We also look at some gcd problems for compositional iterates of polynomials, or for linear recurrence sequences, and pose some open questions.