

RESULTANTS MODULO p

Carlos D'Andrea

Universitat de Barcelona, Spain

cdandrea@ub.edu

Several problems in elimination theory involving arithmetic over the integers (like resultants, the Nullstellensatz, etc) have as an outcome an integer number which if it is not zero modulo a prime p , often imply that classical results over the complex number (dimension, number of zeroes, etc.) “descend” to the residual field. But what happens when p does divide this number? In this talk, we will show that in the case of multivariate resultants, if the input system has a finite number of zeroes modulo p , then p powered to this cardinality (counted with multiplicities) divides the resultant.

Joint work with Martin Sombra (ICREA & Universitat de Barcelona).