ERIC SCHOST, The University of Western Ontario, London, ON

Some applications of multivariate modular composition

In 2008, Kedlaya and Umans introduced the first quasi-linear time algorithm to compute the modular composition of univariate polynomials, namely, $f(g)$ modulo h.

I will describe an extension of this idea to a multivariate setting, and its application to computations with modular polynomials, as seen for instance in the SEA algorithm for elliptic curve point counting.