MICHAEL MONAGAN, University of Western Ontario
Solving Linear Systems over Cyclotomic Fields

We present three algorithms for solving a linear system $Ax = b$ over a cyclotomic field. If $m(z)$ is the minimal polynomial for the field, a cyclotomic polynomial, then what makes this problem of special interest is that it is relatively easy to find primes which split $m(z)$ into linear factors. This means we can solve $Ax = b$ modulo a prime at each root of $m(z)$, potentially in parallel.

Our first algorithm uses Chinese remaindering and rational reconstruction. Our second algorithm uses linear p-adic lifting and rational reconstruction. A third approach is to express the solutions as ratios of determinants. This can be a factor of $d = \deg m(z)$ more compact.

In the talk we will present the algorithms and improvements made to improve the complexity of the reconstruction, and, for the p-adic lifting approach, computation of the error.

We have implemented the three algorithms in Maple. We present timings comparing the three algorithms on two sets of benchmarks, firstly, a set of real problems arising from computational group theory. These problems have the property that the size of the rationals in the solution vector x is much smaller than they can be in general. The second set is for problems where the integers in the input are generated at uniformly at random.

This is joint work with Liang Chen at SFU.