Pedro Berrizbeita
Simon Bolivar University, Venezuela.

"AKS with Gaussian Sums"

The so called practical version of the AKS primality test makes use of modular congruences in Kummer Extensions rather than in cyclotomic extensions, that were used in the original version of AKS. In both versions a group G is associated to certain congruences modulo n, the number to be tested for primality. The primality of such n follows from estimates on the size of this group.

We will show here how to make use of Gaussian Sums, which generate a Kummer Extension, so that with aditional but neglectable computational effort one can increase the lower bound of the size of the group, obtaining in this way an improvement in the running time of the algorithm.