

This thesis focuses on the Coppersmith method for finding roots of modular polynomials. The method is based on the base reduction of a lattice. Firstly, we define a lattice and show a simplified form of the LLL algorithm. Then we describe the Coppersmith method and related theorems. Furthermore, we introduce a solved example from the article written by D. Boneh and G. Durfee. The general form of the method from the article written by E. Jochemsz and A. May and we add some proofs. In the last chapter we solve examples using the method in general form.