

Tato práce se zabývá Coppersmithovou metodou na hledání kořenů celočíselných polynomů modulo N , která je založena na redukci báze mřížky. Nejprve zdefinujeme pojem mřížka a ukážeme si LLL algoritmus ve zjednodušené podobě. Dále popíšeme Coppersmithovu metodu a tvrzení, která se k ní vztahují. Následně ukážeme řešený příklad z článku od D. Boneh a G. Durfee a obecný postup z článku od E. Jochemsz a A. May, který doplníme o několik důkazů navíc. V poslední kapitole vyřešíme příklady pomocí obecného postupu.