

POSUDEK VEDOUcíHO NA BAKALÁŘSKOU PRÁCI MICHALA
FEROVA *IRREDUCIBLE POLYNOMIALS MODULO P*

Práce prezentuje probabilistický algoritmus pro nalezení ireducibilního polynomu nad $GF(p)$. Algoritmus má povahu pokus-test. Student tedy nejprve představuje podmínky ireducibility polynomu, poté odhaduje pravděpodobnost náhodného vygenerování ireducibilního polynomu a nakonec formuluje samotný test.

Práce je psána kvalitní angličtinou (na str. 18, ř. 4 má být zřejmě „a few“ namísto „few“), student také doplnil některé drobnosti vynechané v použité literatuře.

Je škoda, že se nepodařilo popsany algoritmus naprogramovat a otestovat.

I tak text považuji za kvalitní; splňuje požadavky na bakalářskou práci.

Praha 31. srpna 2008

Štěpán Holub

navrhují „výborně“