Miloslav Sobotka:

Faktorizace polynomů a problém batohu

posudek oponenta

V práci je popsána jedna z verzí van Hoeijova rychlého algoritmu na faktorizaci celočíselných polynomů. Jde o poměrně obtížný materiál: k pochopení algoritmu je třeba znát základy teorie p-adických čísel a princip LLL-redukce mřížek, informace nejsou uceleně uvedeny v žádné učebnici, bylo třeba prostudovat původní články a řadu doplňujících materiálů.

Teorie, která není pokryta v základních kurzech, je shrnuta v první části práce. Druhá část je věnována vysvětlení algoritmu a v příloze najdeme implementaci algoritmu v systému Mathematica a ukázky běhu na konkrétních příkladech.

Úroveň textu je velmi dobrá, po stylistické i obsahové stránce. První část je čtivá, čtenář se stručně a poměrně jasně dozví, co potřebuje. Popis algoritmu je však dosti technický, neškodilo by větší množství motivačních a vysvětlujících poznámek, chybí mi popis „vyššího smyslu" jednotlivých kroků. Dobré je uvedení dvou verzí algoritmu, základní a optimalizované. Možná stálo zato si rozmyslet ještě jednodušší verzi, kde by nebyly odhady úplně přesně specifikované, a byly by doplněny později na základě odhadů, jimiž nyní kapitola začíná.

Implementace je funkční a předložené příklady ilustrativní.

Závěr: Navrhuji uznat předloženou práci jako bakalářskou a ohodnotit stupněm **výborně**.

V Praze, 6.9.2010

David Stanovský