Posudek vedoucího bakalářské práce
Složitost některých faktorizačních algoritmů
Viléma Štěpánka

Algoritmus ECM je velice efektivní metoda pro odhalování 'malých' (10 - 40 -ti ciferných) prvočíselných dělitelů složeného čísla. Tuto metodu mohou využívat i asymptoticky rychlejší faktorizační algoritmy, např. číselné síto.

Metodu ECM publikoval v roce 1987 H. W. Lenstra v Annals of Mathematics. Její hrubý popis je celkem jednoduchý - máme složené číslo N, $\mathrm{NSD}(N, 6) = 1$, N dělitelné alespoň dvěma různými prvočísly. Zvolíme $a, b, x, y \in \mathbb{Z}_N$ vhodné, tak aby $y^2 \equiv x^3 + ax + b \bmod N$. Pak (x, y) je bodem na každé eliptické křivce $Y^2 \equiv X^3 + aX + b \bmod p$, kde p je prvočíselný dělitel N. Pro vhodné k zkusíme na této křivce spočítat $k(x, y)$, protože ale neznáme p, počítáme dle stejných vzorců v $\mathbb{Z}_N$ místo v $\mathbb{Z}_p$. Pokud se v průběhu výpočtu dostaneme do situace, že potřebujeme spočíst z^{-1} v $\mathbb{Z}_N$ a $0 \neq z$ je soudělné s N, získali jsme vlastní dělitel N.

Cílem práce bylo prostudovat heuristický odhad složitosti z Lenstrova článku, což samo o sobě není snadné. Jednak prezentace v článku vynechává některé detailnější úvahy, druhak pracuje s látkou přesahující možnosti standardní bakalářské práce (modulární křivky a práce s L-funkcemi). Proto jsou zde Tvrzení 14, 15(b) a 17 uvedena bez důkazu. Pokud chceme analyzovat složitost algoritmu ECM, je třeba studovat náhodně volenou křivku a náhodně volený bod na křivce. Lenstrův článek nedává návod, jak konkrétně naložit s pojmem eliptické křivky nad $\mathbb{Z}_N$. Definice obvyklá v literatuře je trochu komplikovaná, zde jsme to zkusili obejít v Definici 14 a sčítacím algoritmu 1.3.1, snad to nebylo na úkor korektnosti.

Druhá kapitola práce obsahuje některé poznámky k implementaci, zejména jsou diskutovány různé reprezentace bodů eliptické křivky. Autor nakonec implementoval pouze ECM s klasickou afinní reprezentací. Ve třetí kapitole jsou uvedeny výsledky měření výkonu této implementace, dále pak výstup z testování hypotézy ze strany 20.

S předloženou prací jsem jako vedoucí spokojen, autor zpracoval obtížnější téma a v průběhu práce se snažil o hlubší pochopení různých souvislostí, samostatně si dohledával další literaturu k tématu. Vlastnímu zpracování by se dala vytknout určitá kostrbatost některých formulací (úvaha nad Důsledkem 13, důkaz Věty 22). Dále asi nebylo vhodné pouštět měření implementace ECM na nepředpokládaných vstupech (soudělných s šesti).

Co se týče výstupu z testování hypotézy na str. 20, je trochu nešt'astné, že jsou zde hypotézy dvě, výrazně označená je jen jedna z nich. Součástí práce mohlo být nějaké přesnější vymezení funkce $o(1)$ na straně 20 nahoře, přesněji formulace hypotézy odhadující toto $o(1)$ pomocí nějaké jednoduché funkce. Pokud autor na základě naměřených dat k nějaké takové hypotéze nakonec dospěl, mohl by ji zmínit u obhajoby.

Předloženou práci doporučuji uznat jako práci bakalářskou.

V Praze, 18. 6. 2016

Pavel Příhoda