**Povzetek**

Diplomsko delo govori o razcepu velikih števil in natančneje opisuje tri metode za razcep, Pollardovo $\rho$ metodo, metodo verižnih ulomkov in metodo kvadratnega sita.

V uvodu je predstavljena najpreprostejša metoda za razcep števil, metoda poskusnega deljenja, pri kateri s poizkušanjem preverjamo, ali je dano število $N$ deljivo s katerim od praštevil, ki so manjša od neke izbrane meje. Ta metoda je uporabna le za iskanje majhnih praštevilskih faktorjev, večje prafaktorje poiščemo z eno od v delu opisanih metod.

Drugo poglavje vsebuje več pripomočkov iz teorije števil, ki so nepogrešljivi za razumevanje metode verižnih ulomkov in metode kvadratnega sita. Seznanimo se z verižnimi ulomki in kvadratnimi kongruencami. V tretjem poglavju je opisana Pollardova $\rho$ metoda za razcep števil oziroma Brentova izboljšava le-te. Četrto poglavje govori o skupnih lastnostih metode verižnih ulomkov in metode kvadratnega sita. Pri obeh metodah moramo poiskati taki števili $x$ in $y$, da velja kongruenca $x^2 \equiv y^2 \pmod{N}$, hkrati pa $x \not\equiv y \pmod{N}$. Z njuno pomočjo potem poiščemo faktor števila $N$. V resnici pri obeh metodah generiramo kongruence oblike $x_k^2 \equiv (-1)^{e_{0k}} p_1^{e_{1k}} \cdots p_n^{e_{nk}} \pmod{N}$, kjer so $p_i$ praštevila. Iz teh kongruenc potem z Gaussovo eliminacijo dobimo kongruenco $x^2 \equiv y^2 \pmod{N}$. Način generiranja kongruenc je pri obeh metodah drugačen. Pri metodi verižnih ulomkov, opisani v petem poglavju, generiramo kongruence s pomočjo razvoja števila $\sqrt{N}$ v verižni ulomek, pri metodi kvadratnega sita, opisani v šestem poglavju, pa oblikujemo tabele vrednosti $x_k = \lfloor\sqrt{N}\rfloor + k$, $y_k = x_k^2 - N$ in $\log y_k$ in poskusno deljenje vrednosti $y_k$ s praštevili iz faktorske baze prevedemo na odštevanje logaritmov. Pri tem za vsako praštevilo vemo, kateri $y_k$ so deljivi z njim, zato sejemo preko tabele vrednosti $\log y_k$.

Dodatek vsebuje primer implementacije vseh treh algoritmov v programu *Mathematica*.

**Math. Sub. Class. (1991):** 11A07, 11A51, 11A55.
**Key words:** factorization, continued fraction, congruences.

## Literatura


[1] R.P. Brent, Parallel algorithms for integer factorisation, v: *Number Theory and Criptography*, ur. J.H. Loxton, London Mathematical Society Lecture Note Series, vol. 154, Cambridge University Press, 1990.

[2] D.M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag New York Inc., 1989.

[3] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg, 1993.

[4] J. Grasselli, Osnove teorije števil, DMFA RS in Državna založba Slovenije, 1975.

[5] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1979.

[6] A. Hurwiz, N. Ktitikos, *Lectures on Number Theory* Springer-Verlag New York, 1986.

[7] D.E. Knuth, *The Art of the Computer Programming*, vol. 2: Seminumerical Algorithms, Addison-Wesley Publishing Company, 1981.

[8] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag New York Inc., 1987.

[9] A. Menezes, S. Vanstone, Solving Large Sparse Linear Systems over Finite Fields, v: *Advances in Cryptology*, vol. 90, Lecture Notes in Computer Science, Springer-Verlag, 1991.

[10] R.D. Silverman, The multiple polynomial quadratic sieve, *Mathematics of Computation*, 48 (1987), 329-339.