Title:
Computational problems of elementary number theory

Author:
Mgr. Jiří Widž

Department:
Department of Mathematics Education

Supervisor:
Prof. RNDr. Štefan Porubský, DrSc.
Institute of Computer Science of the Academy of Sciences of the Czech Republic

Abstract:
The central notion of this presented thesis is the concept of continued fractions. The origin of this concept as one of the oldest mathematical methods is shown here in its historical connections. The technique of continued fractions belongs to classical parts of mathematics. Although the general theory of continued fractions is manifold and layered considerably, in textbooks it is usually treated according to the intended purpose of its use. In the present text we have summarized the foundations of the general theory of convergence of continued fractions with an emphasis on the theory of simple continued fractions and their most common applications. We show several possibilities how the concept of continued fractions can be generalized to other structures such as the Gaussian integers or polynomial continued fractions. In the chapter devoted to matrix continued fractions we shall demonstrate the possibility how to extend it to non-commutative algebraic structures. We also show how the apparatus of continued fractions can be used to solve Diophantine or algebraic equations, to reduce fractions, factorize integers, specify the type of calendar, as well as a simple tool to attack the RSA cryptographic system, etc. Worked examples accompany the exposition. The last part of the thesis contains examples of texts demonstrating the use of the concept of continued fractions in Czech secondary school mathematics textbooks in the past.

Keywords:
general continued fraction, simple continued fraction, Euclid's algorithm, Euclidean rings, convergence of continued fractions, application of continued fractions