Continued Fractions and Euclidean Algorithm in Unique Factorization Domains

Kondratyonok, Nikita

The purpose of this project consists in constructing of finite continued fractions theory in arbitrary unique factorization domains and applying this theory to optimization of the Euclidean algorithm. We developed a special reconstruction method for continued fractions and used some ideas from geometry of numbers to obtain the existence criterion of the representation of a fixed element from the field of fractions of a unique factorization domain in the form of a continued fraction with a fixed length. This existence criterion enabled to prove the Kronecker theorem on the minimality of the Euclidean algorithm length for a wide class of unique factorization domains. Our theorems extended and generalized the published results of D. Lazard (1977), H. Rolletschek (1986, 1990), M. Vaskouski and N. Kondratyonok (2013) concerning the minimality of the Euclidean algorithm length. With the help of the results R. Eggleton, C. Lacampagne, J. Selfridge on the characterization of Euclidean domains (1992) we obtained the necessary and sufficient conditions providing the logarithmic complexity of the Euclidean algorithm in unique factorization domains. Our results are important for theories of continued fractions and approximations, theory of algorithms and abstract algebra. The obtained theorems are perspective for optimization of computations based on the Euclidean algorithm including finding of secret keys in cryptanalysis.