

This thesis is devoted to estimate complexity of algorithms running time for factorization of integer using ECM. Firstly, basic characteristics of elliptic curves over finite fields are sketched and two theorems on which this problematic is based are presented. Consequently, there are given necessary estimates by some constants and ECM algorithms behavior is sketched. After that there is shown estimated complexity of algorithm ECM and finally there is specified implementation of factoring algorithm ECM.