2010:1
Självständigt arbete i matematik
Matematiska institutionen
Stockholms universitet

Gabriel Netterdag: Arbitrary-precision arithmetic in various algebraic structures

Handledare: Torsten Ekedahl

Sammanfattning

This report will present some of the more commonly used methods for performing arbitrary-precision arithmetic. The ability to do arithmetic efficiently with numbers containing hundreds or thousands of digits and in some cases even more, is vital in many computational fields. Cryptography is a major real-world example which takes advantage of these methods. It will introduce, as a reference, the Diffie-Hellman key exchange protocol. Furthermore, it will discuss the methods of classic arithmetic, modular arithmetic and Karatsuba arithmetic. The report will also introduce arithmetic methods based on the Fourier transform and its generalization as well as special representations in finite fields. Finally some concrete computer implementations are given with comparisons between the different algorithms.