Digital Expansions in Imaginary Quadratic Number Fields with Applications in Cryptography

Clemens Heuberger[1] <clemens.heuberger@tugraz.at>
Roberto Avanzi[2]<roberto.avanzi@ruhr-uni-bochum.de>
Helmut Prodinger[3]<hproding@sun.ac.za>

Elliptic curve cryptography relies on the fact that multiples nP of a point P can be computed easily, whereas the inverse problem (discrete logarithm on elliptic curves) seems to be hard. Since subtraction on elliptic curves is as cheap as addition, scalar multiplication can be done using a double, add and subtract algorithm using a binary expansion with digits 0, ± 1. On special Koblitz curves, the doublings can be avoided by using the Frobenius endomorphism. In that case, the digit expansions have to be made with respect to a quadratic algebraic integer base. Optimal expansions as well as their analysis will be discussed.

[1]TU Graz
[2]Ruhr University Bochum
[3]Stellenbosch University