ELLIPTIC CURVES AND ALGORITHMS

PREDA MIHĂILESCU

The main goal of the lecture series is to provide theoretical background and algorithmic knowledge of some famous algorithms in symbolic computation, connected to elliptic curves. These may include algorithms like

(1) Schoof Algorithm and the Atkin-Elkies improvements, for counting number of points on a curve,
(2) Atkin-Morain ECPP primality proving,
(3) Elliptic curve factoring,

and the background on Deuring lifts, complex multiplicaiton and function fields.

The accents will be set dynamically, according to the knowledge and motivation of the audience. None is too much – and none is too little.

Orientative books:

[1] D. A. Cox, *Primes of the form $p = x^2 + ny^2$*, Wiley & Sons, 2013.
[2] J. H. Silverman and J. T. Tate, *Rational Points on Elliptic Curves*, Springer, 1994.
[3] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Taylor & Francis Ltd, 2 ed., 2008.

and some journal papers, which can be spread on site.

Mathematisches Institut, Georg-August-University, Göttingen, Germany
Email address: preda@uni-math.gwdg.de
URL: http://www.uni-math.gwdg.de/preda/