
ADELA GHERGA, The University of British Columbia
Implementing Algorithms to Compute Elliptic Curves Over \mathbb{Q}

Let $S = \{p_1, \dots, p_k\}$ be a set of rational primes and consider the set of all elliptic curves over \mathbb{Q} having good reduction outside S and bounded conductor N . Currently, using modular forms, all such curves have been determined for $N \leq 390000$, the bulk of this work being attributed to Cremona.

Early attempts to tabulate all such curves often relied on reducing the problem to one of solving a number of certain integral binary forms called Thue-Mahler equations. These are Diophantine equations of the form

$$F(x, y) = u,$$

where

$$F(x, y) = f_0x^n + f_1x^{n-1}y + \dots + f_{n-1}xy^{n-1} + f_ny^n$$

is a given binary form of degree at least 3 and u is an S -unit. A theorem of Bennett-Rechnitzer show that the problem of computing all elliptic curves over \mathbb{Q} of conductor N reduces to solving a number of Thue-Mahler equations. To compute all such equations, there exists a practical method of Tzanakis-de Weger using bounds for linear forms in p -adic logarithms and various reduction techniques. In this talk, we describe our implementation of this method and discuss the key steps in used in our algorithm.