ADELA GHERGA, The University of British Columbia
Implementing algorithms to compute elliptic curves over Q

Let $S = \{p_1, \ldots, p_v\}$ be a set of rational primes. A theorem of Bennett-Rechnitzer shows that the problem of computing all elliptic curves over $\mathbb{Q}$ having good reduction outside S and bounded conductor N reduces to solving a number of Thue-Mahler equations. These are Diophantine equations of the form

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

where

$$F(x, y) = c_0 x^n + c_1 x^{n-1} y + \cdots + c_{n-1} x y^{n-1} + c_n y^n$$

is a given binary form of degree at least 3 and u is an S-unit. To solve such equations, there exists a practical method of Tzanakis-de Weger using 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 used in our algorithm, as well as the implications to computing elliptic curves.