On prime-order elliptic curves with embedding degrees $k = 3, 4$ and 6

Koray Karabina and Edlyn Teske

Dept. of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1,
kkarabina@uwaterloo.ca, eteske@uwaterloo.ca

Abstract. We further analyze the solutions to the Diophantine equations from which prime-order elliptic curves of embedding degrees $k = 3, 4$ or 6 (MNT curves) may be obtained. We give an explicit algorithm to generate such curves. We derive a heuristic lower bound for the number $E(z)$ of MNT curves with $k = 6$ and discriminant $D \leq z$, and compare this lower bound with experimental data.

Keywords: Elliptic curves, pairing-based cryptosystems, embedding degree, MNT curves.