

ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

zadaca 2.29

1. Eliptička krivulja nad \mathbb{Q} zadana je jednađbom

$$E : y^2 = x^3 + 10000x + 46875.$$

Odredite njezinu minimalnu Weierstarssovu jednađbu.

2. Kakvu redukciju (dobru ili lošu; aditivnu ili multiplikativnu; rascjepivu ili nerascjepivu) ima krivulja iz 1. zadatka za $p = 13$?
3. Nađite sve točke konačnog reda, te odredite strukturu torzijske grupe za eliptičku krivulju

$$y^2 = x^3 - 46035x - 3116178.$$