ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

zadaća 2.30

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

$$E : y^2 = x^3 + 6250x + 375000.$$

   Odredite njezinu minimalnu Weierstarssovu jednadžbu.

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

$$y^2 = x^3 - 19440x + 1026432.$$