Domácí úkol z 23. března 2017

Řešte úlohu 5.12 uvedenou v knize L. C. Washington: Elliptic Curves (2nd edition) na straně 168.

Poznámky k zadání:

Přestože je v zadání odkaz na cvičení 4.7, ukažte sami, že $\#E(\mathbb{F}_2) = 5$. *Pro tvrzení o supersingulárnosti* E *a pro rovnost* $\phi_2^2 + 2\phi_2 + 2 = 0$ *se odkažte na vhodné věty z knihy. Odtud pak sami odvodíte (a). Rovněž pro část (c) využijte vhodnou větu. V části (b) by bylo možné vypsat všechny body a počítat jejich řády, existuje však mnohem snadnější cesta založená na výsledcích částí (a) a (c).*