

## Domácí úkol z 22. září 2016

Řešte úlohu 2.13 uvedenou v knize L. C. Washington: *Elliptic Curves* (2nd edition) na straně 73.

Poznámky k zadání:

Předpokládáme, že pracujeme nad tělesem  $K$ , jehož charakteristika není ani 2 ani 3 a uvažujeme jen  $\lambda \in K$  různá od 0 a 1.

Část (a) je z hlediska počítání s polynomy poměrně náročná, možná bude vhodné si numerické výpočty kontrolovat pomocí nějakého vhodného softwaru (PARI-GP, Maple apod.). Nejprve je třeba substitucí  $x \mapsto x + c$  pro vhodné  $c \in K$  docílit toho, aby na pravé straně byl kubický polynom mající nulový koeficient ve druhé mocnině, abychom pro výpočet  $j$ -invariantu mohli použít definici na straně 46 a po úpravě získat uvedený vzorec.

V části (c), kterou je možná lepší provést dříve než (b), abychom věděli, co předpoklad  $j \neq 0$ ,  $j \neq 1728$  vlastně znamená pro  $\lambda$ , je vhodné si vzpomenout, jak jsme vzorec v (a) odvodili.

V části (b) je třeba si rozmyslet pro dané  $j$ , jaký polynom šestého stupně má  $\lambda$  za kořen a ukázat, že tento polynom nemá násobné kořeny a navíc s každým svým kořenem  $\lambda$  má i kořen  $1 - \lambda$  a  $1/\lambda$ .