Domácí úkol z 16. listopadu 2017

Rovnicí

$$Y^2 = X^3 + X - 4$$

je zadána eliptická křivka E nad jedenáctiprvkovým tělesem $\mathbb{Z}_{11}$.

1. Ukažte, že body $A = (1, 3)$ a $B = (-1, 4)$ leží na E a že bod A zde má řád 5.

2. Na eliptické křivce E spočítejte hodnotu Tateova-Lichtenbaumova párování $\langle A, B \rangle_5$.

[Návod: užijte definici párování, která je ve Washingtonově knize popsána na stranách 355-356.]