Domácí úkol z 3. listopadu 2016

Řešte úlohu 3.6 uvedenou v knize L. C. Washington: Elliptic Curves (2nd edition) na straně 93.

Poznámka k zadání: Úvahy vedoucí k řešení úlohy Vám může jednodušit, pokud daný bod P doplníte dalším bodem do báze $E[n]$ a v této bázi si vyjádříte bod Q. Při tomto postupu je ovšem zapotřebí dokázat, že je toto doplnění vždy možné (to lze odvodit z toho, že $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$ a že řád bodu P je podle zadání roven právě n).