Domácí úkol číslo 4

Buď a liché, $e \geq 3$. Dokažte, že potom má kongruence $x^2 \equiv a \pmod{2^e}$ má

1. čtyři řešení, právě když zároveň platí $a \equiv 1 \pmod 4$ a $a^{2^{e-3}} \equiv 1 \pmod{2^e}$,
2. nula řešení jinak.

Na další straně naleznete radu, jak na to.

Použijte fakt, že -1 a 5 generují grupu $\mathbb{Z}_{2^e}^\star$ a řád 5 v této grupě je 2^{e-2}.