

## Domácí úkol číslo 4

Bud'  $a$  liché,  $e \geq 3$ . Dokažte, že potom rovnice

$$x^2 \equiv a \pmod{2^e}$$

má v množině  $\{1, 2, \dots, 2^e\}$

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