První domácí úloha

Příklad. *Pomocí vlastností dělitelnosti ukažte, že diofantická rovnice* $x^3 + y^3 + z^3 = 31$ *nemá řešení v celých číslech.*

Poznámka. Možný postup: nejprve rozhodněte jaké zbytky může mít třetí mocnina mod 9 a pak ukažte, že součet tří takových nemůže dát zbytek 4 ($31 = 4 \pmod 9$)

Příklad. *V protokolu RSA použijte* $p = 23$ *a* $q = 29$. *Zvolte si vlastní (vhodné)* e*, zašifrujte zprávu* $m = 25$ *a pak ji dešifrujte. Ukažte, jak by útočník, vaši zprávu dešifroval (tj. prolomil šifru při znalosti* $n = pq$ *a* e*).*

Poznámka. Volte e tak, aby šifra nebyla triviální.