Cvičení 11: Aplikace teorie čísel

Příklad 1. *Popište test Millera a Rabina na složenost a s využitím algoritmu modulárního umocňování demonstrujte, jak tento test odhalí složenost čísla* 1105 *s využitím svědka složenosti* $a = 2$. *Výpočet proveďte bez využití výpočetní techniky.*

Příklad 2. *Bohuslav s Andrejem si posílají zprávy zašifrované pomocí Rabinova kryptosystému s veřejným klíčem 437. Bohuslav poslal Andrejovi číslo 101. Najděte všechny možnosti původní (nezašifrované) zprávy.*

Příklad 3. *Bob s Alicí si posílají zprávy zašifrované pomocí šifry ElGamal s parametry* $p = 29$ *a primitivním kořenem* $g = 2$. *Bob zveřejnil* $(29, 2, 18)$ *a obdržel od Alice dvojici* $(12, 26)$. *Jakou zprávu poslala Alice Bobovi?*

Příklad 4. *(Bonusový, doporučený zejména příznivcům geocachingu)*

GC12NFZ *S využitím vhodného softwaru rozložte na prvočísla číslo*

$$164147978573005557898426507320901206480422691305326428639125085909563268362 3.$$

GC197GF *S využitím vhodného softwaru nalezněte diskrétní logaritmus čísla*

$$6361196924231058595008858273263807320$$

o základu 5 modulo

$$158605840895317983583081182943282025 87.$$