Domácí úkol č. 1 - Počítání modulo n

1. V $\mathbb{Z}_{267}$ najděte všechna x, pro která platí $114x = 15$.
2. Spočtěte 51^{-1} v $\mathbb{Z}_{73}$. (Použijte rozšířený Eukleidův algoritmus.)
3. Určete zbytek po dělení třinácti z čísla 270^{149}.
4. Spočtěte 7^{131} v $\mathbb{Z}_{26}$.
5. Spočtěte 5^{-1} a 21^{-1} v $\mathbb{Z}_{27}$. (Použijte Euler-Fermatovu větu.)
6. Určete řády všech prvků v aditivní grupě $(\mathbb{Z}_{12}, +)$. Je tato grupa cyklická? Pokud ano, které prvky jsou jejím generátorem?
7. Je dána multiplikativní grupa $(\mathbb{Z}_{25}^*, \cdot)$.

   Určete řád prvku 6 a použijte jej k výpočtu $x = 6^{57}$ v $\mathbb{Z}_{25}$.

   Najděte nějaký generátor grupy $\mathbb{Z}_{25}^*$, pokud existuje.

   Najděte všechny prvky řádu 4.

   Řešte rovnici $x^5 = 1$ v grupě $\mathbb{Z}_{25}^*$.
8. Která z následujících multiplikativních grup je cyklická: $\mathbb{Z}_{15}^*$, $\mathbb{Z}_{17}^*$, $\mathbb{Z}_{26}^*$? (Nalezněte generátor.)
9. Je dána multiplikativní grupa $(\mathbb{Z}_{31}^*, \cdot)$.

   Najděte nějaký její generátor. Jaká je pravděpodobnost, že při náhodné volbě prvku z této grupy zvolíme právě generátor?

   Najděte všechny prvky řádu 6.

   Určete řád prvku 27 a použijte jej k výpočtu $x = 27^{101112}$ v $\mathbb{Z}_{31}$.

   Řešte rovnici $x^{12} = 1$ v grupě $\mathbb{Z}_{31}^*$.

Výsledky

1. $x_1 = 54$, $x_2 = 143$, $x_3 = 232$.
2. $51^{-1} = 63$ v $\mathbb{Z}_{73}$.
3. Zbytek je 4.
4. $7^{131} = 15$ v $\mathbb{Z}_{26}$.
5. $5^{-1} = 11$ a 21^{-1} neexistuje v $\mathbb{Z}_{27}$.
6. Grupa $\mathbb{Z}_{12}$ je cyklická, jejím generátorem je 1 nebo 5 nebo 7 nebo 11.
7. Prvek 6 má řád 5, odtud $x = 6^2 = 11$ v $\mathbb{Z}_{25}$.

   Grupa $\mathbb{Z}_{25}^*$ je cyklická, jejím generátorem je např. 2.

   Prvky řádu 4 jsou $b \in \{7, 18\}$.

   Řešení rovnice jsou v podgrupě $< 16 >= \{16, 6, 21, 11, 1\}$.
8. Grupa $\mathbb{Z}_{15}^*$ není cyklická, ostatní ano. $\mathbb{Z}_{17}^*$ má generátor např. $a = 3$, $\mathbb{Z}_{26}^*$ má generátor např. $a = 7$.
9. $\mathbb{Z}_{31}^*$ má generátor např. $a = 3$, pravděpodobnost trefy je $p = \frac{8}{30}$.

   Prvky řádu 6 jsou $b \in \{6, 26\}$ v $\mathbb{Z}_{31}^*$.

   Prvek 27 má řád 10, odtud $x = 27^2 = 16$ v $\mathbb{Z}_{31}$.

   Řešení rovnice jsou $\pm 1, \pm 5, \pm 6$.