

ALGEBRA

Cvičenie 5

1. Nech pre prvočíslo p je množina $\mathbb{Z}_p^\#$ daná $\mathbb{Z}_p^\# = \{1, 2, \dots, p - 1\}$. S operáciou násobenia modulo p tvorí množina $\mathbb{Z}_p^\#$ abelovskú grupu. Vypočítajte inverzné prvky k daným prvkom (pomocou Euklidovho algoritmu).

a) $4, 10 \in \mathbb{Z}_{17}^\#$.

b) $9, 13 \in \mathbb{Z}_{19}^\#$.

c) $103, 140 \in \mathbb{Z}_{307}^\#$.

2. Vypíšte všetky párne permutácie štvorprvkovej množiny $\{1, 2, 3, 4\}$. Koľko ich je?

3. Nasledujúce permutácie rozložte na súčin disjunktných cyklov a určte ich paritu.

a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$

b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 1 & 2 & 6 & 3 \end{pmatrix}$

c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 7 & 2 & 8 & 5 & 4 & 6 \end{pmatrix}$

d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 1 & 3 & 5 & 7 & 2 & 6 \end{pmatrix}$