Prsten $\mathbb{Z}_{26}$

- Skup $\{0, 1, 2, ...25\}$ označimo sa $\mathbb{Z}_{26}$;
- Na skupu $\mathbb{Z}_{26} = \{0, 1, 2, ...25\}$ definirajmo dvije operacije zbrajanje $(+_{26})$ i množenje $(\cdot_{26})$ na isti način kao u skupu cijelih brojeva, ali tako da se rezultat (ako nije iz $\mathbb{Z}_{26}$) na kraju zamijeni njegovim ostatkom pri dijeljenju s 26. Koristimo oznake:

$$a +_{26} b \quad \text{ili} \quad (a + b) \bmod 26$$
$$a \cdot_{26} b \quad \text{ili} \quad (a \cdot b) \bmod 26$$

  Primjer:

$$\begin{aligned} 11 +_{26} 23 &= (11 + 23) \bmod 26 = 8 \\ 5 \cdot_{26} 9 &= (5 \cdot 9) \bmod 26 = 19 \end{aligned}$$

- Skup $\mathbb{Z}_{26} = \{0, 1, 2, ...25\}$ uz operacije $+_{26}$ i $\cdot_{26}$ zadovoljava aksiome matematičke strukture koja se naziva *prsten* (štoviše, to je *komutativan prsten s jedinicom).* Naime, vrijedi:

  - operacije $+_{26}$ i $\cdot_{26}$ su zatvorene (rezultat je ponovno iz $\mathbb{Z}_{26}$);
  - operacije $+_{26}$ i $\cdot_{26}$ su komutativne, tj. za sve $a, b \in \mathbb{Z}_{26}$ vrijedi

$$\begin{aligned} a +_{26} b &= b +_{26} a, \\ a \cdot_{26} b &= b \cdot_{26} a; \end{aligned}$$

  - asocijativnost ($+_{26}$ i $\cdot_{26}$), tj. za sve $a, b, c \in \mathbb{Z}_{26}$ vrijedi

$$\begin{aligned} (a +_{26} b) +_{26} c &= a \cdot_{26} (b +_{26} c)\,, \\ a \cdot_{26} (b \cdot_{26} c) &= (a \cdot_{26} b) \cdot_{26} c; \end{aligned}$$

  - distributivnost množenja prema zbrajanju, tj. za sve $a, b, c \in \mathbb{Z}_{26}$ vrijedi

$$(a +_{26} b) \cdot_{26} c = (a \cdot_{26} c) +_{26} (b \cdot_{26} c)\,;$$

  - broj (element) 0 je neutralni element za zbrajanje, tj. za sve $a \in \mathbb{Z}_{26}$ vrijedi

$$a +_{26} 0 = 0 +_{26} a = a;$$

  - svaki element $a \in \mathbb{Z}_{26}$ ima suprotni element (aditivni inverz) $-a$. Za $a \neq 0$, to je broj $26 - a$ jer vrijedi

$$a +_{26} (26 - a) = (26 - a) +_{26} a = 0.$$

    (Pomoću ovoga možemo definirati oduzimanje u $\mathbb{Z}_{26}$, kao $a. -_{26} b =: a. +_{26} (-b)$);

    Primjer:

$$a = 7 \Rightarrow -a = 26 - 7 = 19 \;\; \text{jer je } 7 +_{26} 19 = 19 +_{26} 7 = 0;$$

- broj (element) 1 je neutralni element za množenje, tj. za sve $a \in \mathbb{Z}_{26}$ vrijedi
$$a \cdot_{26} 1 = 1 \cdot_{26} a = a;$$

Uočimo: Samo neki elementi $a \in \mathbb{Z}_{26}$ imaju multiplikativni inverz u $\mathbb{Z}_{26}$, tj. element a^{-1} za koji vrijedi

$$a \cdot_{26} a^{-1} = a^{-1} \cdot_{26} a = 1,$$

(a to su oni $a \in \mathbb{Z}_{26}$ koji su relativno prosti s 26.)

Primjer:

$$\begin{aligned} a &= 5 \Rightarrow a^{-1} = 21 \text{ jer je } 5 \cdot_{26} 21 = 21 \cdot_{26} 5 = 1, \\ a &= 13 \text{ nema multiplikativni inverz u } \mathbb{Z}_{26}. \end{aligned}$$

Još jedna oznaka: Ako cijeli brojevi a i b imaju isti ostatak pri dijeljenju s 26, to zapisujemo
$$a \equiv b \bmod 26,$$
i kažemo da su a i b *kongruentni* modulo 26.

Napomena:

- potpuno analogno se definira skup $\mathbb{Z}_m$ i operacije na njemu, za proizvoljan prirodan broj m;
- ako je $m = p$ prost, onda svaki element $a \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ ima multiplikativni inverz, pa $\mathbb{Z}_p$ ima strukturu *polja.*