Moodularvutus (mooduli rakendamine)

Kui **m** ja **n** on naturaalarvud: $\mathbf{m}, \mathbf{n} \in \mathbf{N}$, siis

$$\mathbf{n} \bmod \mathbf{m} \in \{0, 1, 2, 3, 4, 5 \ldots\ldots m-1\}$$

ehk

$$0 \leq (\mathbf{n} \bmod \mathbf{m}) \leq m-1$$

näide:

1 mod 4 = 1	1 mod 5 = 1	19 mod 8 = 3
2 mod 4 = 2	2 mod 5 = 2	15 mod 6 = 3
3 mod 4 = 3	3 mod 5 = 3	6 mod 3 = 0
4 mod 4 = 0	4 mod 5 = 4	8 mod 2 = 0
5 mod 4 = 1	5 mod 5 = 0	9 mod 2 = 1
6 mod 4 = 2	6 mod 5 = 1	10 mod 2 = 0
7 mod 4 = 3	7 mod 5 = 2	11 mod 2 = 1
8 mod 4 = 0	8 mod 5 = 3	12 mod 2 = 0
9 mod 4 = 1	9 mod 5 = 4	13 mod 2 = 1
10 mod 4 = 2	10 mod 5 = 0	14 mod 2 = 0
11 mod 4 = 3	11 mod 5 = 1	15 mod 2 = 1

Eelnevast loetelust näeme, et
mooduli *m* rakendamise tulemus osutub võrdseks
arvuga *m* (täisarvulise) **jagamise jäägiga**:

jagatav : jagaja = jagatis (! jääk !)

Mooduli rakendamine v ä h e n d a b arvu etteantud vahemikku.
Mooduli *m* rakendamisel osutub selleks vahemikuks **0 . . . . (*m*−1)**

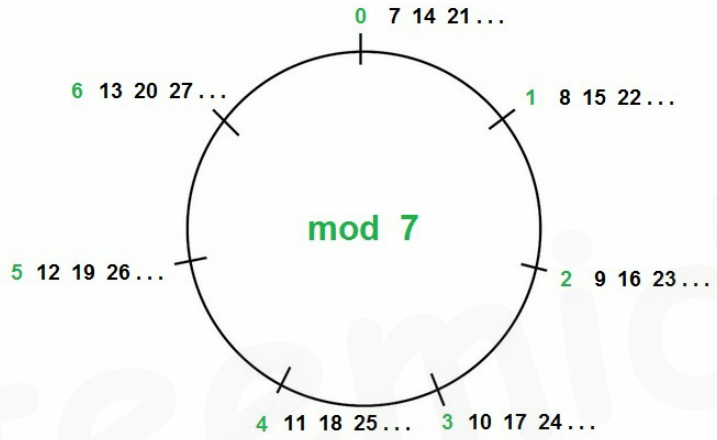
Võtame mingi juhusliku *mooduli* : **mod 7**

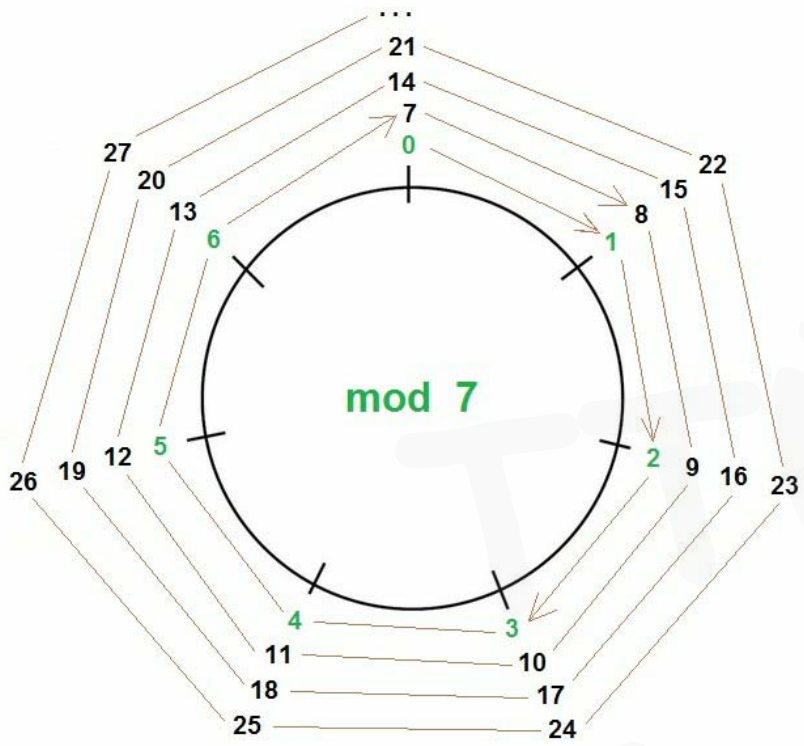
$$\mathbf{n} \bmod 7 \in \{0, 1, 2, 3, 4, 5, 6\}$$

ehk

$$0 \leq (\mathbf{n} \bmod 7) \leq 6$$

mooduli **7** *rakendamise* visuaalne illustratsioon :





"vastavaks osutuvad" arvud **mod 7** rakendamisel

pane tähele :

sekundid ja **minutid** loenduvad (inkrementaalselt) **mooduliga 60** ;

tunnid loenduvad (inkrementaalselt) **mooduliga 24** ;