$\mathbb{Z}_n^+$ $\mathbb{Z}_n^\times$ rendel $n = 7, 8, 12$

$\mathbb{Z}_7^+$

	rend
0	1
1	7
2	7
.	=
.	
k	7

$0 + 0 = 0$

$1, 1+1, 1+1, \dots, 6, 0$

$2, 2+2=4, 2+2+2=6, \dots$

$\frac{o(1)}{(o(1), 2)} = 7$ $\quad 2 = 1+1$

$(k, 7) = 1 \quad k \neq 0.$

$\mathbb{Z}_8^+, \mathbb{Z}_{12}^+$ ugyanígy pl $\mathbb{Z}_{12}^+$ $o(8) = \frac{o(1)}{(o(1), 8)} = \frac{12}{(12, 8)} = \frac{3}{=}$

ill $8, 8+8=4$

$8+4=0$

$\mathbb{Z}_6^+ \cong \mathbb{Z}_7^\times$ (tömb)

	1	2	3	4	5	6
k	1	2	3	4	5	6
3^k	3	2	6	4	5	1

rend

1
3
6
6
6
2

$o(3) = 6$

$\mathbb{Z}_7^\times$ ciklikus

3 primitív vmod 7

$4 = 3^4$

$2, 2^2 = 4, 2^3 = 1$

$3, 3^2 = 2, 3 \cdot 2 = -1, \dots$

$4, 4^2 = 2, 4 \cdot 2 = 1$

$-1, (-1)^2 = 1$

$o(4) = \frac{o(3)}{(o(3), 4)} = \frac{6}{(6, 4)} = 3$

$\cong 3^4$

$\mathbb{Z}_8^\times$ $\quad 1, 3, 5, 7 \qquad 3^2 = 5^2 = 7^2 = 1$

$o(1) = 1 \qquad o(3) = o(5) = o(7) = 2$

$\mathbb{Z}_{12}^\times$ $\quad 1, 5, 7, 11 \qquad o(5) = o(7) = o(11) = 2.$

$5^2 = 25 \equiv 1 \qquad 7^2 = 49 \equiv 1 \qquad 11^2 = 121 \equiv 1$

$\mathbb{Z}_5^\times$ ciklikus $\quad 1, 2, 4, 4$

4 rendű $\varphi(4) = 2$ db

$\varphi(2) = 1$ db.

$\mathbb{R}^+ \quad o(-1) = \infty$

$\mathbb{R}^\times \quad o(-1) = 2 \qquad (-1)^2 = 1$

$\mathbb{Z}_{11}[x]^+ \qquad o(x+1) = 11$

$x+1,\ (x+1)+(x+1) = 2x+2, \ldots$

$\mathbb{Z}_{11}[x]^\times \quad o(5) = ?$ ugyanaz, mint $\mathbb{Z}_{11}^\times$-ban.

egység: $T[x]$ egységei: T test: $\neq 0$ konst.

A7 2 rendi elem.

↳ perm: (ab)(cd||ef)...

↳ páros perm! ~~(ab)~~ ~~(ab)(cd||ef)~~ pl. (ab)(cd||ef)(gh) nem fér el.

↳ diszjunkt

(ab)(cd) i.c. $\binom{7}{4} \cdot 3$

{a,b,c,d} = {1,2,3,4}

(12)(34)
(13)(24)
(14)(23)
} 3 db $\frac{\binom{4}{2}}{2}$

3 rendi
4 -"- hány?

↳ (abc)

$\binom{7}{3} \cdot 2$ + $\frac{\binom{7}{3}\cdot\binom{4}{3}}{2} \cdot 2 \cdot 2$

(123)
(132)

4 rendű A_7-ben.

$(abcd)(ef)$

$\binom{7}{4} \cdot 3! \cdot \binom{3}{2}$

HF 14. feladat vége.

15, 16, 18, 19, 20

↳ $o(gh) \stackrel{?}{=} o(g)o(h)$ ha $(o(g), o(h)) = 1$.

$o(g) = n$, $o(h) = m$

$gh = hg$

$(gh)^{nm} = g^{nm}h^{nm} = 1 \Rightarrow o(gh) \mid o(g) \cdot o(h)$

↗ $gh = hg$ kihasználva!

$k = o(gh)$ $(gh)^k = 1 \Rightarrow (gh)^{kn} = 1 \Rightarrow h^{kn} = 1$

$g^{kn} \cdot h^{kn}$, $g^{kn} = 1$

$\Rightarrow o(h) \mid kn$, $o(h) = m$

$(m, n) = 1 \Rightarrow m \mid k$

Hasonlóan $n \mid k$.

$(m, n) = 1 \Rightarrow mn \mid k$.

$(o(g), o(h)) = 1$ kell?

$\mathbb{R}^\times = \{1, -1\}$

$o(-1) = 2$ $o(-1) = 2$ $o((-1)(-1)) = o(1) = 1 \neq 4$

$(o(g), o(h)) = 1$ $\quad o(gh) \neq o(g)\, o(h)$

$gh \neq hg$ - za polda

S_3 $\quad g = (12)$ (2) $\quad (12)(123) = (1)(23)$

$h = (123)$ (3) $\quad o(gh) = 2$

16

$x^2 = 1 \ \forall x \Rightarrow$ G Abelova IGEN

$x^4 = 1 \ \forall x \overset{?}{\Rightarrow}$ G Abelova NEM

$\hookrightarrow o(x) = 1, 2, 4$ možni strukturni D_4

$\rightarrow xx = x^2 = 1 \quad yy = y^2 = 1$

$(xy)^2 = 1 \quad xyxy = 1$

$xyxyyy = y$

$xxyx = xy$ ✓

G véges, van prímrendű elem.

S_3 $(1\,2)$ jó

$\mathbb{Z}_5^+$ 1 jó

$\mathbb{Z}_{10}^+$ 1 nem jó $o(1) = 10$

2 jó, $o(2) = 5$ ✓

$$o(2) = \frac{o(1)}{(o(1), 2)} = \frac{10}{2} = 5$$

$g \in G$

$o(g)$ nem jó $o(g) = 15$

$$o(g^3) = \frac{o(g)}{(o(g), 3)} = \frac{15}{3} = 5 \checkmark$$

$o(g) = n$ nem prím $n = pm$ p prím

$$o(g^m) = \frac{o(g)}{(o(g), m)} = \frac{pm}{m} = p \checkmark$$

$|G| = 1$ az egyelemű ilyen.

Ha $|G| \neq 1 \Rightarrow \exists g \neq 1$, $g \in G$ $\Rightarrow o(g) \neq 1$
$\Rightarrow \exists$ prímosztója $o(g)$-nek

$G \quad \exists \quad g \in G \qquad o(g) = 5$

$\exists \cdot e \geq \varphi(5) = 4$ db 5 rendi?

$$o(g^2) = \frac{o(g)}{(o(g), 2)} = \frac{5}{(5, 2)} = 5$$

$o(g^3) = 5 \quad , \; o(g^4) = 5$ ✓

A'et $o(g) = d$

$\varphi(d)$ db d rendi: g^k $1 \leq k \leq d$

$(k, d) = 1$

$\varphi(d)$ db.

Igaz e, hogy $\varphi(d)$-nek

Első nem lehet

$d = 2 \qquad \varphi(2) = 1$ ↗ 1-nél első 2 rendű nem

Rombus szimm.

$\mathbb{Z}_8^\times$, $\mathbb{Z}_{12}^\times$ stb.