$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ ordinul grupului = # de el. din grup = $|\mathbb{Z}_m^*| = \phi(m)$

$\phi(7) = 7-1 = 6$ ordinul unui el. din grup = # de el. distincte pe care le gen. (din $\mathbb{Z}_m^*$)

$1^1 \bmod 7 = 1$	$2^1 \bmod 7 = 2$	$3^1 = 3$	$4^1 = 4$	$5^1 = 5$	$6^1 = 6$
1^2 " $= 1$	2^2 " $= 4$	$3^2 = (9)_7 = 2$	$4^2 \equiv_7 2$	$(5^2)_7 = 4$	$6^2 \equiv_7 1$
⋮	$(2^3)_7 = (8)_7 = 1$	$3^3 = (27)_7 = 6$	$4^3 \equiv_7 1$	$(5^3)_7 = 6$	$6^3 \equiv_7 6$
⋮	$2^4 = (16)_7 = 2$	$3^4 \equiv_7 4$	$4^4 \equiv_7 4$	$(5^4)_7 = 2$	$6^4 \equiv_7 1$
⋮	$2^5 = (64)_7 = 4$	$3^5 \equiv_7 5$	$4^5 \equiv_7 2$	$(5^5)_7 = 3$	$6^5 \equiv_7 6$
$1^6 \bmod 7 = 1$	$2^6 \equiv_7 1$	$3^6 \equiv_7 1$	$4^6 \equiv_7 1$	$(5^6)_7 = 1$	$6^6 \equiv_7 1$
$ord_7(1) = 1$	$ord_7(2) = 3$	$ord_7(3) = 6$	$ord_7(4) = 3$	$ord_7(5) = 6$	$ord_7(6) = 2$

$\boxed{* \ \forall a \in \mathbb{Z}_m, \ a^{\phi(m)} \equiv_m 1}$ $1, 2, 3, 6 \mid 6$ = ord. grupului = $\phi(m) = \phi(7)$

3 și 5 au generat toate el. grupului $\mathbb{Z}_7^*$ $\Rightarrow$ „generator" = „rădăcini primitive"

$m = 1, 2, 4, p^k, 2p^k$, p prim ≥ 3

$\boxed{\text{* ord. unui el. din gr.}}$; vom verifica dacă $x^{\text{divizorii ord. gr.}} \equiv_m 1$; ordinul = c.m. mică putere

$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ $\phi(12) = \phi(2^2) \cdot \phi(3) = (2^2 - 2^1)(3-1) = 2 \cdot 2 = 4$

$1^1 = 1$ $(5^1)_{12} = 5 \} \neq 1$ $7^1 = 7$ $11^1 = 11$ ord. grupului = 4 ; div. $\phi(12)$: $1, 2, 4 \mid 4$

$1^1 = 1$ $\quad (5^1)_{12} = 5 \; \} \neq 1$ $\quad 7^1 = 7$ $\quad 11^1 = 11$ $\quad$ ord. grupului = 4 ; div. $\phi(12)$: $1, 2, 4 \mid 4$

$ord_{12}(1) = 1$ $\quad (5^2)_{12} = 1$ $\quad (7^2)_{12} = 1$ $\quad 11^2 \equiv_{12} 1$

$(5^4)_{12}$ $\quad ord_{12}(5) = 2$ $\quad ord_{12}(7) = 2$ $\quad ord_{12}(11) = 2$

$\mathbb{Z}_6^* = \{1, 5\}$ $\qquad$ ord. gr. $= \phi(6) = \phi(2) \cdot \phi(3) = (2-1)(3-1) = 1 \cdot 2 = 2$

$\boxed{* \ \# \text{ generatori dintr-un grup}}$

$\phi(\phi(6)) = \phi(2) = 2 - 1 = 1$

$\phi(\phi(7)) = \phi(6) = 2$

Calc. toate r.p. din $\mathbb{Z}_{22}^*$ $\quad$ (?) $\exists$ r.p.? $\quad 2 \cdot p^k \Rightarrow$ DA $\qquad$ avem în total 4 gen. în $\mathbb{Z}_{22}^*$

$\mathbb{Z}_{22}^* = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$ (?) câte $\qquad \phi(\phi(22)) = \phi(\phi(2) \cdot \phi(11)) = \phi(10) = \phi(2) \cdot \phi(5) = \boxed{4}$

ord. gr: $\underline{\underline{10}} = \phi(22)$ $\qquad$ divizorii lui $\phi(m) = 10$: $\underline{1, 2, 5, 10 \mid 10}$

(?) să găsesc o rădăcină primitivă $\alpha \rightarrow ord_m(\alpha) = \phi(m)$

$\Updownarrow$

$\nexists$ o putere $< \phi(m)$ la care ridicat α să dea 1!

gen $\mathbb{Z}_{22}^*$ $\begin{cases} 7^1 \\ ? \; 7^3 \bmod 22 \\ ? \; 7^7 \bmod 22 \\ ? \; 7^9 \bmod 22 \end{cases}$

$3^2 \equiv 9 \bmod 22 \neq 1$ $\quad | \quad 5^2 \equiv_{22} 3 \neq 1$ $\quad | \quad (7^2)_{22} = 5 \neq 1$

$3^5 \equiv_{22} 1 \Rightarrow 3$ nu e gen. $\quad | \quad 5^5 \equiv_{22} 1 \Rightarrow$ nu e gen. $\quad | \quad (7^5)_{22} = 21 \neq 1 \Rightarrow 7$ e gen.

$ord_{22}(3) = 5 \neq \phi(m)$ $\qquad ord_{22}(5) = 5$ $\qquad ord_{22}(7) = 10 = \phi(22)$ $\qquad \dfrac{k \in \{1, 3, 7, 9\}}{(k, \phi(m)) = 1}$

$\boxed{* \ ord_m(a^k) = \dfrac{ord_m(a)}{(k, ord_m(a))}}$ $\qquad ord_{22}(7^k) = \dfrac{\phi(22)}{(k, \phi(22))} = \dfrac{10}{1} = 10$

- Funcția lui Euler $\phi(m) = |\mathbb{Z}_m^*|$

- câte numere $< m$ sunt coprime cu m
- $\phi(m)$ reprezintă ordinul grupului $\mathbb{Z}_m^*$

1) $\phi(1)=1$
2) $\phi(p)=p-1$, p prim
3) $\phi(a\cdot b)=\phi(a)\cdot\phi(b)$, $(a,b)=1$
4) $\phi(p^e)=p^e-p^{e-1}$, p prim
5) $\phi(n)=(p_1^{e_1}-p_1^{e_1-1})\cdot \ldots \cdot(p_k^{e_k}-p_k^{e_k-1})$, unde $n=p_1^{e_1}\cdot \ldots \cdot p_k^{e_k}$

Dacă $ord_m(a)=t$, atunci $ord_m(a^k)=t$ ddacă $(k,t)=1$

Prop. 6 $ord_m(a^k)=\dfrac{ord_m(a)}{(k, ord_m(a))}$

* Ordinul unui element divide ordinul grupului

- Rădăcini primitive

Dacă $ord_m(a)=\phi(m)$, atunci a este răd. primitivă mod m

Câte răd. primitive există în $\mathbb{Z}_m^*$? $\phi(\phi(m))$

Prop 6
$ord_m(a^k) = \frac{ord_m(a)}{(k, ord_m(a))}$ $\quad$ $ord_{11}\left(2^{\boxed{k}}\right) = \frac{ord_{11}(2)}{(\square, ord_{11}(2))} = \frac{\phi(11)}{(\square, 10)} = \frac{10}{1} = 10$

$(\boxed{k}, 10) = 1$

? O răd. primitivă din $\mathbb{Z}_m^*$

? Toate răd. primitive din $\mathbb{Z}_m^*$ $\quad$ # numere coprime cu $\phi(m) = 10$ =

Câte? $\phi(10) = \phi(2)\cdot\phi(5) = 4$ $\quad$ $= \phi(10) = \phi(\phi(m))$

Găsiți o rădăcină primitivă din $\mathbb{Z}_{11}^*$.

1) $\underline{m}$ Admite răd. pr.? $\underline{m}$ de forma $1, 2, 4, p^k, 2p^k$, p prim impar

$11 \to p^k$ (DA)

2) $\phi(11) = 11 - 1 = 10$ $\quad$ div(10): 1, 2, 5, 10 $\quad$ Obs: $\forall a \in \mathbb{Z}_m^*$, $a^1 \equiv_m a$; $a^{\phi(m)} \equiv_m 1$

$a \in \mathbb{Z}_m^*$ $\quad$ $a^2 \overset{?}{\equiv} 1 \bmod 11$ $\quad$ $\underline{DA}$ la una din aceste puteri $\Rightarrow$ nu e gen.

$a^5 \overset{?}{\equiv} 1 \bmod 11$ $\quad$ $\underline{NU}$ la ambele puteri $\Rightarrow$ a e generator

Dacă $\exists$ o putere $\underline{v} < \phi(m)$, $a^v \equiv 1 \bmod m \Rightarrow$ a nu e gen; $\underline{v}$ e din $\phi(m)$

$a \in \{\cancel{1}, 2, 3, 4, \dots, 10\}$

$\mathbb{Z}_m^*$, $m \geq 1$

$2^2 \bmod 11 \equiv 4$ $\quad$ este $\equiv 1 \bmod 11$ $\quad$ $\underline{NU}$

$2^5 \bmod 11 \equiv 32 \bmod 11 = 32 - 11\cdot 2 = 10$ $\quad$ este $\equiv 1 \bmod 11$ $\quad$ $\underline{NU}$ $\quad$ $\Big\}\Rightarrow$ 2 e gen în $\mathbb{Z}_{11}^*$.

? toți gen. din $\mathbb{Z}_{11}^*$ $\quad$ $k \in \{1, 3, 7, 9\}$ $\quad$ $2^1 = 2$; $2^3 \equiv_{11} 8$; $2^7 \bmod 11 = 7$

4 $\quad$ $2^9 \bmod 11 = 6$

$\mathbb{Z}_{22}^*$ $\quad$ Toți gen lui $\mathbb{Z}_{11}^* = \{2, 6, 7, 8\}$ ✓

1) $\underline{DA}$ $\quad$ $2p^k$

2) $\phi(22) = \phi(2)\cdot\phi(11) = 10$

$a \in \{\cancel{1}, \cancel{2}, \underline{3}, 5, 7, \dots, 21\} - \mathbb{Z}_{22}^*$

2 poate fi gen în $\mathbb{Z}_{22}^*$? Nu. Deoarece $2 \notin \mathbb{Z}_{22}^*$ pt. că $(2, 22) = 2 \neq 1$

Ex3 Găsiți, fol. propr. ord. unui el. într-un grup, un el. de ordin 5 din $\mathbb{Z}_{11}^*$.

$a^5 \equiv \underline{1} \bmod 11$ și 5 este $\underline{\text{cea mai mică}}$ putere p a.î. $a^p \equiv 1 \bmod 11$

1) Aflăm un gen. din $\mathbb{Z}_{11}^*$: 2

2) $ord_{11}(2^j) = 5$ $\qquad ord_{11}(2^j) = \dfrac{ord_{11}(2)}{(j, ord_{11}(2))} = \dfrac{10}{2} = 5$

$(j, 10) = 2 \Rightarrow j = 2, 4, 6, 8$

$\{2^2 \bmod 11,\ 2^4 \bmod 11,\ 2^6 \bmod 11,\ 2^8 \bmod 11\}$

$x \in \mathbb{Z}_m^* \Rightarrow \exists i$, a.î., $\alpha^i \equiv x \bmod m$ $\qquad$ $m = 1, 2, 4, p^k, 2p^k \Rightarrow \exists$ gen.

$x^m \equiv 1 \bmod m$ $\qquad$ $\mathbb{Z}_m^* \to$ răd. pr.

$\alpha^{im} \equiv \alpha^0 \bmod m$ $\qquad$ $in \equiv 0 \bmod \phi(m)$

α este răd. pr.

$$\underbrace{\alpha^i \bmod m}_{x}, \quad \boxed{i \in \left\{ k \cdot \frac{\phi(m)}{(m, \phi(m))} \;\middle|\; 0 \leq k < (m, \phi(m)) \right\}}$$

$$\boxed{a^{r} \equiv a^{s} \mod m \iff r \equiv s \mod \operatorname{ord}_{m}(a)}$$