Z= {1,2,3,4,5,6} ordinal grupular = # de el din grup = | Zm | = p(m) ordinal unuiel. din grup = # de el .. distincte pe care le gen. (dir Im) Φ(7)= 2-1-6 3'=3) | 5' = 5' | 5' = 5' 2 mod 1 = 2) 6 = 67 (1)= f born 1 42 = 2 (52) =4 3=(9)2=2 62 = 1 $3^3 = (27)_4 = 6$ 63 = 6 $(5^3)_{7} = 6$ 3⁴ = 4 6 = 1 $(5')_{2} = 2$ $=(16)_{a}=2$ 35 = 5 45 = 2 ((55)2 = 3 65 =76 25 = (64)2 = 4 4 = 1 (56) ==1 16 mod 7 = 1 36 = 1 66 = 1 phd=(1)=1 $and_{7}(2) = 3$ $\operatorname{grd}_{2}(3)=6$ $\operatorname{grd}_{2}(4)=3$ $\operatorname{grd}_{2}(5)=6$ $\operatorname{grd}_{2}(6)=2$ * $\forall \alpha \in \mathbb{Z}_m$, $\alpha = 1$ $1, 2, 3, 6 | 6 = \text{ord. graphlen'} = \phi(m) = \phi(7)$ 3 Ni 5 au generat toate el grupului Z7 => "generator" = "tradaani primitive" m = 1,2,4,px, 2px, p prum =3 * ord. unui el din of.], nom revisica daca x divisarii ard. of. = m1; ordinal = c.m. mica putor $\phi(12) = \phi(2^2) \cdot \phi(3) = (2^2 - 2^1)(3-1) = 2 \cdot 2 = 4$ Z12 = {1,5,7,11} 1=1 (5') 12 = 5 } +1 7'=7 11'=11 ord. grupului-4; dir. \$\phi(R): 1,2,4 \quad 4

1-4 (5')_R = 5 + 1
$$\frac{1}{4}$$
 = $\frac{1}{4}$ | 11-11 ord apurului - 1; div. $\phi(R)$: 1,2,4 | 4

 $\phi(R)$: (5²)_R = 1 ($\frac{1}{4}$)_R = 1 | 11-11 ord apurului - 1; div. $\phi(R)$: 1,2,4 | 4

 $\phi(R)$: (5²)_R = 1 ($\frac{1}{4}$)_R = 1 | 11-11 ord apurului - 1; div. $\phi(R)$: 1,2,4 | 4

 $\phi(R)$: (5²)_R = 1 ($\frac{1}{4}$)_R = 1 | 11-11 ord apurului - 1; div. $\phi(R)$: 1,2,4 | 4

 $\phi(R)$: (1)-11-12-12

 $\phi(R)$: (1)-12-12 ord $\phi(R)$: (1)-12-12

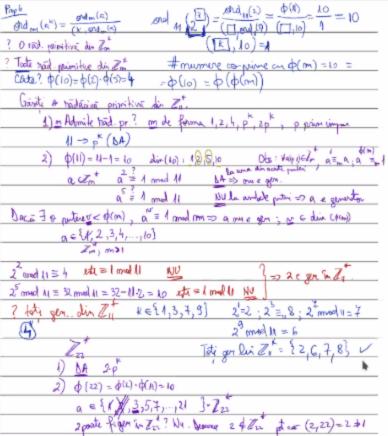
 $\phi(R)$: (1)-12-12 ord $\phi(R)$: (1)-12-12

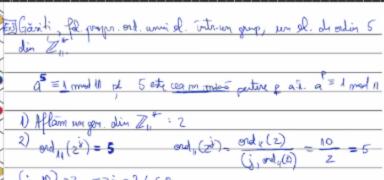
 $\phi(R)$: (1)-12-12

- Functia lui Euler Φ(m) = Zm - câte numere 2 m sunt coprime cu m - $\Phi(m)$ reprezintă ordinul grupului Z_m (1)=1 2) $\phi(p) = p-1$ ρ prim

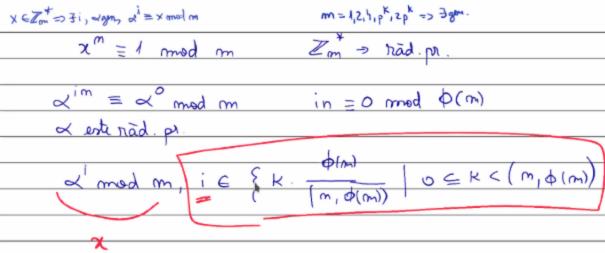
3) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ (a,b) = 14) $\phi(p^e) = p^e - p^{e-1}$ ρ prim

5) $\phi(m) = (p^{e_1} - p^{e_1-1}) \cdot \dots \cdot (p^{e_k} - p^{e_k-1})$ umde $n = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$ Paca ord (a) = t atunci ord (a) = t ddaca (k,t)=1 * Ordinal unui element divide ordinal grapului · Rădăcini primitire Dacă ord m(a) = O(m), atunci a este rad primitiva mod m Câte răd primitive există în Zm? O(O(m))





(j, 10) = 2 => 0 = 2,4,6,8 2 mod 4, 2 mod 4, 2 mod 4, 2 mod 4)



$$a \equiv a \mod m \iff h \equiv h \mod and_{an}(a)$$