Grupuri ciclice, Ordinul unui element – Seminar 10

Definitia 1. Se numeste **grup** o multime G impreuna cu o operatie binara • , o operatie unara **'** , si un element neutru **e,** notat (G, **•**, **'**, **e**), care satisface proprietatile

1. • este asociativa,
2. x • e = e • x = x, e ∈ G este element neutru pentru operatia • (e este unic cu aceasta proprietate, se mai noteaza cu 1_G)
3. pentru orice x ∈ G, exista x**'** ∈ G astfel incat x • x**'** = x**'** • x = e , x**'** este inversul lui x fata de operatia • (x**'** este unic cu aceasta proprietate)

Definitia 2. Un grup G este **ciclic** daca poate fi generat de un element al sau.

Exemple 1. Daca a ∈ G, a genereaza G, unde G este un grup multiplicativ, atunci G este de forma
$G = \{a^n \mid n \in Z\}$
2. Daca a ∈ G genereaza G, unde G este un grup aditiv, atunci G este de forma
$G = \{na \mid n \in Z\}$
3. (Z, +, - ,0) este un grup ciclic (aditiv) infinit, generat de 1.
4. (Z_m, +, - , 0) este un grup ciclic (aditiv) finit, generat de 1, pentru m > 1,
$Z_m = \{0, 1, 2, \ldots, m-1\}$

Observatia 1. Grupul multiplicativ, finit, (Z^*_m, . , ', 1) nu este neaparat ciclic.
$Z^*_m = \{a \in Z_m \mid (a,m) = 1\}$, este format din acele elemente din Z_m care admit un invers.

Observatia 2. Daca Φ este functia lui Euler atunci $\Phi(m) = | Z^*_m |$ (cardinalul multimii Z^*_m)

Observatia 3. Cateva proprietati (de neuitat) ale functiei lui Euler:
$\Phi(1) = 1$, $\Phi(p) = p-1$ pt. orice p numar prim,
$\Phi(ab) = \Phi(a)\Phi(b)$, pt orice a si b prime intre ele, deci aceasta proprietate nu se aplica pentru 2 si 4, sau pt 2 si 6. Atentie! Nu calculati $\Phi(8) = \Phi(2)\Phi(2)\Phi(2) = 1$ (total gresit!)
$\Phi(p^n) = p^n - p^{n-1}$, asadar $\Phi(8) = \Phi(2^3) = 2^3 - 2^2 = 4$ si
$\Phi(12) = \Phi(4.3) = \Phi(4)\Phi(3) = (2^2 - 2)(3 - 1) = 4$
$\Phi(n) = \Phi(p_1^{e1})\, \Phi(p_2^{e2}) \ldots \Phi(p_n^{en})$ unde $n = p_1^{e1}\, p_2^{e2} \ldots p_n^{en}$ este descompunerea unica a lui n in produs de puteri de factori primi (Teorema fundamentala a aritmeticii).

Exemple $Z_5 = \{0, 1, \ldots, 4\}$, $Z^*_5 = \{1, 2, 3, 4\}$, $\Phi(5) = 5-1 = 4 = | Z^*_5 |$
$Z_6 = \{0, 1, \ldots, 5\}$, $Z^*_6 = \{1, 5\}$, $\Phi(6) = \Phi(2)\, \Phi(3) = 2 = | Z^*_6 |$
$Z_{14} = \{0, 1, 2, \ldots, 13\}$, $Z^*_{14} = \{1, 3, 5, 9, 11, 13\}$, $\Phi(14) = \Phi(2)\, \Phi(7) = 6 = | Z^*_{14} |$

Tema Ex. 1 Calculati Φ(24), Φ(29), Φ(38), Φ(210) folosind proprietatile functiei lui Euler.

Observatia 4. Teorema lui Euler: $a^{\Phi(m)} \equiv 1 \bmod m$, pentru orice $m \geq 1$ si $(a,m) = 1$.

Definitia 3. Se numeste **ordinul lui a modulo m**, notat $ord_m(a) = \min\{k \geq 1 | a^k \equiv 1 \bmod m\}$

Observatia 5. $ord_m(a) = ord_{Z^*m}(a)$

Observatia 6. $(Z^*_m, \ . \ , ', 1)$ nu este intotdeauna ciclic, dar atunci cand este ciclic generatorii lui Z^*_m se numesc radacini primitive modulo m.

Teorema 1. $a \in Z^*_m$ este radacina primitiva mod m daca si numai daca $ord_m(a) = \Phi(m)$.

Exemple 1. Calculati $ord_7(3)$

Rezolvare: $3^1 \equiv 3 \bmod 7$, $3^2 \equiv 2 \bmod 7$, $3^3 \equiv 6 \bmod 7$, $3^4 \equiv 4 \bmod 7$, $3^5 \equiv 2 \bmod 7$, $3^6 \equiv 1 \bmod 7$
In concluzie $ord_7(3) = 6 = \Phi(7)$ (6 este valoarea minima pentru care $3^6 \equiv 1 \bmod 7$),
Asadar, **3 este radacina primitiva modulo 7**.

Exemple 2. Calculati $ord_7(2)$

Rezolvare: $2^1 \equiv 2 \bmod 7$, $2^2 \equiv 4 \bmod 7$, $2^3 \equiv 1 \bmod 7$, asadar $ord_7(2) = 3$ (3 este valoarea minima pentru care $2^3 \equiv 1 \bmod 7$) **2 nu este radacina primitiva modulo 7.**

Observatie Daca exista radacini primitive mod m, atunci numarul acestora este $\Phi(\Phi(m))$.

Tema Ex. 2 Demonstrati ca 3 si 5 sunt radacini primitive modulo 14.

Teorema 2. (Gauss) Z^*_m este ciclic daca si numai daca $m \in \{1, 2, 4, p^k, 2p^k\}$ unde $k \geq 1$ si $p \geq 3$ este un numar prim.

Teorema 3. Fie $m \geq 1$, astfel incat Z^*_m este ciclic, atunci ecuatia $x^n \equiv 1 \bmod m$ are $(n, \Phi(m))$ solutii in Z^*_m de forma $\alpha^i \bmod m$, unde α este radacina primitiva modulo m si i este solutie a ecuatiei $in \equiv 0 \bmod \Phi(m)$.

Observatie Rezolvand ecuatia liniara congruentiala $in \equiv 0 \bmod \Phi(m)$, cu necunoscuta i se gasesc solutiile de forma $i \in \{ k\, \Phi(m)/ (n, \Phi(m)) \mid 0 \leq k < (n, \Phi(m)) \}$
(A se vedea rezolvarea ecuatiei congruentiale liniare de forma $ax \equiv b \bmod m$!)

Exemple 1. Rezolvati ecuatia $x^4 \equiv 1 \bmod 50$

Solutiile ec. sunt de forma $\alpha^i \bmod 50$, unde α este radacina primitiva mod 50, si
$i \in \{ k\, \Phi(50)/ (4, \Phi(50)) \mid 0 \leq k < (4, \Phi(50)) \}$, $\Phi(50) = \Phi(2)\, \Phi(25) = 20$

Asadar, $i \in \{ k\, 20/4 \mid 0 \le k < 4 \} = \{ 5k \mid 0 \le k < 4 \} = \{ 0, 5, 10, 15\}$.

Radacinile primitive modulo 50 sunt in numar de $\Phi(\Phi(50)) = \Phi(20) = 8$ si anume
$\{3, 13, 17, 23, 27, 33, 37, 47\}$ deci α poate fi orice valoare din aceasta multime.

Teorema 4. Fie p un numar prim atunci ecuatia $x^n \equiv -1 \bmod p$ are solutii daca si numai daca $(n, p-1)$ divide $(p-1)/2$. In caz afirmativ ecuatia are exact $(n, p-1)$ solutii de forma $\alpha^i \bmod p$, unde α este radacina primitiva modulo p si i este solutie a ecuatiei $in \equiv (p-1)/2 \bmod (p-1)$.

Observatie Rezolvand ecuatia liniara congruentiala $in \equiv (p-1)/2 \bmod (p-1)$, de necunoscuta i, se gasesc solutiile de forma $i \in \{ (p-1)/ 2(n, p-1) + k (p-1)/(n, p-1) \mid 0 \le k < (n, p-1) \}$.

Exemple 2. Rezolvati ecuatia $x^4 \equiv - 1 \bmod 17$.

Solutiile ec. sunt de forma $\alpha^i \bmod 17$, unde α este radacina primitiva mod 17, si
$i \in \{ (17-1)/ 2(4, 17-1) + k (17-1)/(4, 17-1) \mid 0 \le k < (4, 17-1) \} = \{ 16/ 8 + k16/4 \mid 0 \le k < 4\}$

Asadar, $i \in \{ 2 + 4k \mid 0 \le k < 4 \} = \{ 2, 6, 10, 14\}$.
Radacinile primitive modulo 17 sunt in numar de $\Phi(\Phi(17)) = \Phi(16) = 8$ si anume
$\{3, 5, 6, 7, 10, 11, 12, 14\}$ deci α poate fi orice valoare din aceasta multime.

Tema Ex. 3 Rezolvati ecuatiile congruentiale

1. $x^6 \equiv 1 \bmod 38$,
2. $x^5 \equiv 1 \bmod 22$,
3. $x^7 \equiv - 1 \bmod 29$,
4. $x^3 \equiv - 1 \bmod 31$.

Grupuri ciclice, Ordinul unui element

Alte exemple de ecuatii (rezolvate)

Exemplul 3. Rezolvati ecuatia $x^4 \equiv 1 \bmod 17$

Solutiile ec. sunt de forma $\alpha^i \bmod 17$, unde α este radacina primitiva mod 17, si

$i \in \{ k\,\Phi(17)/(4, \Phi(17)) \mid 0 \le k < (4, \Phi(17)) \}$, $\Phi(17) = 16$

Asadar, $i \in \{ 16k/4 \mid 0 \le k < 4 \} = \{ 4k \mid 0 \le k < 4 \} = \{ 0, 4, 8, 12\}$.

Radacinile primitive modulo 17 sunt in numar de $\Phi(\Phi(17)) = \Phi(16) = 8$ si anume
$\{3, 5, 6, 7, 10, 11, 12, 14\}$, α poate fi orice valoare din aceasta multime.

Exemplul 4. Rezolvati ecuatia $x^{11} \equiv -1 \bmod 23$.

Solutiile ec. sunt de forma $\alpha^i \bmod 23$, unde α este radacina primitiva mod 23, si
$i \in \{ (23\text{-}1)/2(11, 23\text{-}1) + k\,(23\text{-}1)/(11, 23\text{-}1) \mid 0 \le k < (11, 22) \} = \{ 22/22 + 22k/11 \mid 0 \le k < 11\}$
$= \{ 1 + 2k \mid 0 \le k < 11\} = \{ 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21\}$

Radacinile primitive mod 23 sunt in numar de $\Phi(\Phi(23)) = \Phi(22) = 10$ si anume
$\{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$, α poate fi orice valoare din aceasta multime.

Observatie Radacini primitive modulo m

Pentru tema data nu va cer sa determinati toate radacinile primitive modulo m, este destul de laborios. Este suficient sa "ghiciti" doar o singura radacina.

Cum se "ghiceste" o radacina primitiva modulo m?

Raspuns

Radacinile primitive modulo m se gasesc printre elementele multimii $Z^*_m = \{a \in Z_m \mid (a,m) = 1\}$. Asadar se incepe cu cel mai mic element al multimii Z^*_m.

1 nu are nici o sansa, decat daca m = 2. Presupunem ca **a** este urmatorul element (dupa 1 in ordine crescatoare). Se calculeaza $ord_m(a)$ asa cum am aratat in Exemplele 1 si 2, pt. $ord_7(3)$ si $ord_7(2)$, sau Exercitiul 2 din Tema (este foarte simplu).

Daca $ord_m(a) = \Phi(m)$ atunci a este radacina primitiva modulo m, daca nu continuati procedeul cu urmatorul element din Z^*_m. Va opriti la primul **a** care este radacina primitiva modulo m.

Daca vreti neaparat sa determinati toate radacinile primitiva modulo m atunci calculati $ord_m(a)$ pentru orice $a \in Z^*_m$. Radacinile primitive vor fi doar acelea pentru care $ord_m(a) = \Phi(m)$ si vor fi in numar de $\Phi(\Phi(m))$ (in cazul in care Z^*_m admite radacini primitive, adica atunci cand Z^*_m este grup ciclic, a se vedea Teorema lui Gauss pt. cazurile in care Z^*_m este grup ciclic).

Grupuri ciclice, Ordinul unui element – Aplicatii

Exercitiul 1. a) Calculati $ord_{17}(5)$

Rezolvare $ord_{17}(5) \mid \Phi(17)$, conform cu Coralarul 2.1.2 (Grupuri ciclice III)

Deoarece $\Phi(17) = 16$ avem $ord_{17}(5) \in \{1, 2, 4, 8, 16\}$ (divizorii lui 16).

Se calculeaza $5^1 = 5 \bmod 17$, $5^2 = 8 \bmod 17$, $5^4 = 13 \bmod 17$, $5^8 = 16 \bmod 17$, $5^{16} = 1 \bmod 17$,

Asadar $ord_{17}(5) = 16$.

b) Calculati $ord_{22}(9)$

Rezolvare $ord_{22}(9) \mid \Phi(22)$, conform cu Coralarul 2.1.2 (Grupuri ciclice III)

Deoarece $\Phi(22) = 10$ avem $ord_{22}(9) \in \{1, 2, 5, 10\}$ (divizorii lui 10).

Se calculeaza $9^1 = 9 \bmod 22$, $9^2 = 15 \bmod 22$, $9^5 = 7\bullet7\bullet9 \bmod 22 = 5\bullet9 \bmod 22 = 1 \bmod 22$

Asadar $ord_{22}(9) = 5$.

Exercitiul 2. Calculati un element de ordinul d in Z^*_m pentru

a) $d = 2, m = 23$ b) $d = 4, m = 17$.

Rezolvare a) Conform cu Teorema 2.1.4 (Grupuri ciclice III) avem

$ord_{23}(\alpha^i) = \Phi(22) / (i, \Phi(23)) = 22 / (i, 22) = 2$ asadar $i = 11$, unde α este oricare din radacinile primitive modulo 23. Daca se considera $\alpha = 5$ atunci un element de ordinul 2 al lui Z^*_{23}

este $a = 5^{11} \bmod 23 = 22$.

Rezolvare b) Conform cu Teorema 2.1.4 (Grupuri ciclice III) avem

$Ord_{17}(\alpha^i) = \Phi(17) / (i, \Phi(17)) = 16 / (i, 16) = 4$ asadar $i = 4$.

unde α este oricare din radacinile primitive modulo 17.

Daca se considera $\alpha = 3$ atunci un element de ordinul 4 al lui Z^*_{17} este $a = 3^4 \bmod 17 = 13$.