Seminar V. Cornaciu | 03/05/2022

Seminar 11

Inelul claselor de resturi modulo n

$(\mathbb{Z}_n, +, \cdot)$

$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

$U(\mathbb{Z}_n)$ = unitatile lui $\mathbb{Z}_n = \mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$

Ex $\mathbb{Z}_7$

$U(\mathbb{Z}_7) = \{1, 2, 3, 4, 5, 6\}$

$\mathbb{Z}_8$

$U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$

$\mathbb{Z}_{15}$

$U(\mathbb{Z}_{15}) = \{1, 2, 4, 7, 8, 11, 13, 14\}$

$\mathbb{Z}_8$

·	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	(1)	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	(1)	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	(1)	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	(1)

$U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$

$1^{-1} = 1$

$3^{-1} = 3$

$5^{-1} = 5$

$7^{-1} = 7$

Exercitiu: Să se afle inversele claselor nenule din $\mathbb{Z}_{13}$

$\mathbb{Z}_{13} = \{0, 1, \dots, 12\}$

$U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ $\quad 1^{-1} = 1$

$(2,13)=1$

$13 = 2\cdot 6 + 1$

$2 = 1\cdot 2$

$1 = 13 - 2\cdot 6$ | · modulo 13

$1 \overset{13}{\equiv} 0 - 2\cdot 6$

$1 \overset{13}{\equiv} 2\cdot -6$

$1 \overset{13}{\equiv} 2\cdot 7$ $\quad 2^{-1} = 7 \Leftrightarrow 7^{-1} = 2$

$(3,13)=1$

$13 = 3\cdot 4 + 1$ $\rightarrow$ $1 = 13 - 3\cdot 4$

$3 = 1\cdot 3$ $\quad 1 \overset{13}{\equiv} 0 + 3\cdot(-4)$

$1 \overset{13}{\equiv} 3\cdot 9$ $\quad 3^{-1} = 9 \quad 9^{-1} = 3$

$(4,13)=1$

$13 = 4\cdot 3 + 1$ $\rightarrow$ $1 = 13 - 4\cdot 3$

$4 = 1\cdot 4$ $\quad 1 \overset{13}{\equiv} 4\cdot(-3)$

$1 \overset{13}{\equiv} 4\cdot 10 \Rightarrow 4^{-1} = 10$ | $4 = 2^2$

$10^{-1} = 4$ | $4^{-1} = 2^{-1}\cdot 2^{-1} = 7\cdot 7$

$= 49 \overset{13}{\equiv} 10$

$(5,13)=1$

$13 = 5\cdot 2 + 3$ $\rightarrow$ $1 = 3 - 2\cdot 1 = 3 - (5 - 3\cdot 1)\cdot 1 =$

$5 = 3\cdot 1 + 2$ $\quad = 3\cdot 2 - 5\cdot 1 = (13 - 5\cdot 2)\cdot 2 - 5\cdot 1 =$

$3 = 2\cdot 1 + 1$ $\quad = 13\cdot 2 - 5\cdot 5$

$2 = 1\cdot 2$ $\quad 1 \overset{13}{\equiv} 5\cdot(-5) = 5\cdot 8$

$\Rightarrow 5^{-1} = 8 \quad 8^{-1} = 5$

$6^{-1} = (2\cdot 3)^{-1} = 2^{-1}\cdot 3^{-1} = 7\cdot 9 = 63 \overset{13}{\equiv} 11$

$6^{-1} = 11 \quad 11^{-1} = 6$

$12^{-1} = 3^{-1}\cdot 4^{-1} = 9\cdot 10 = 90 \overset{13}{\equiv} 12 \qquad 12^{-1} = 12$

Ex. Să se afle inversele elorelor nenule din $U(\mathbb{Z}_{12})$

$U(\mathbb{Z}_{12}) = \{1, 5, 7, 11\} \quad 1^{-1} = 1$

$(5,12) = 1 \rightarrow 12 = 2\cdot 5 + 2 \rightarrow 1 = 5 - 2\cdot 2 = 5 - (12 - 2\cdot 5)\cdot 2$

$5 = 2\cdot 2 + 1 \qquad = 5 - 12\cdot 2 + 4\cdot 5 =$

$2 = 1\cdot 2 \qquad = 5\cdot 5 - 12\cdot 2$

$\overset{12}{=} 5\cdot 5 \rightarrow 5^{-1}$

$(7,12) = 1 \rightarrow 12 = 1\cdot 7 + 5 \rightarrow 1 = 5 - 2\cdot 2 = 5 - (7 - 5\cdot 1)\cdot 2 =$

$7 = 5\cdot 1 + 2 \qquad = 5 - 7\cdot 2 + 5\cdot 2 =$

$5 = 2\cdot 2 + 1 \qquad = 5\cdot 3 - 7\cdot 2 =$

$2 = 2\cdot 1 \qquad = 5\cdot(12 - 7\cdot 1)\cdot 3 - 7\cdot 2 =$

$= 12\cdot 3 - 7\cdot 3 - 7\cdot 2 =$

$= 12\cdot 3 - 7\cdot 5 \overset{12}{=} 7\cdot -5 \rightarrow 7\cdot 7 \rightarrow 7^{-1}$

$(11,12) = 1 \rightarrow 12 = 1\cdot 11 + 1 \qquad 1 = 12 - 1\cdot 11 \overset{12}{\equiv} 11\cdot -1 = 11\cdot 11 = 11^{-1}$

$11 = 1\cdot 11 \rightarrow$

Def Se numește caracteristica lui Euler, numărul notat cu $\varphi(n)$ al elorelor modulo n reprezentate de numere prime cu n $\quad \varphi(n) = |U(\mathbb{Z}_n)|$

$\mathbb{Z}_{12}$

$(a,12) = 1 \Rightarrow a \in \{1, 5, 7, 11\} \qquad \varphi(12) = 4$

$\mathbb{Z}_{11}$

$(a,11) = 1 \rightarrow a \in \{1, \ldots, 10\} \qquad \varphi(11) = 10$

- $n = p$, p prim $\Rightarrow \varphi(n) = n - 1$
- $n = p^k \Rightarrow \varphi(n) = p^k\left(1 - \frac{1}{p}\right)$
- $n = p_1^{\alpha_1}\cdot \ldots \cdot p_k^{\alpha_k} \Rightarrow \varphi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots(1-$

$\varphi(12) = \varphi(2^2 \cdot 3) \Rightarrow \varphi(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$

Subgrupuri, Grupuri Ciclice, Teorema lui Lagrange

- Se numește subgrup al grupului $(G, \circ)$ o submulțime $H \subset G$, $H \neq \emptyset$ cu proprietățile:
  1) $\forall x, y \in H \Rightarrow x \circ y \in H$
  2) $\forall x \in H \Rightarrow x^{-1} \in H$

Teorema Lagrange

Dacă H este un subgrup al lui G, $m = |H|$, $n = |G|$, atunci $m \mid n$ $\left\{\frac{n}{m}\right\}$

Fie $a \in G$

$[a] = \{a, \underbrace{a^2}_{a \cdot a}, a^3, \dots, \}$

Numărul $m = \min\{k \in \mathbb{N}^*, a^k = e\}$ se numește ordinul lui a.

$[a] = \{a, a^2, a^3, \dots, a^{m-1}, a^m = e\}$

↳ Subgrup generat de elementul a

- Se numește grup ciclic un grup G în care există un element g așa $[g] = G$

  g = generatorul lui G

1. $\mathbb{Z}_p^*$ grup ciclic, p este prim,
2. $\mathbb{Z}_n^*$ grup ciclic $\Leftrightarrow n = 2, 4, p^2, 2 \cdot p^2$ $\quad p$ = prim

Exemple

$\mathbb{Z}_2^*$ grup ciclic

$\mathbb{Z}_7^*$ grup ciclic

$\mathbb{Z}_9^*$ grup ciclic $\quad 9 = 3^2 \to p^2$

$\mathbb{Z}_{34}^*$ grup ciclic $\quad 34 = 2 \cdot 17^1 \to 2 \cdot p^2$

Generatorul grupului ciclic $\mathbb{Z}_n^*$, $n = 2, 4, p^2, 2 \cdot p^2$

Algoritm

1. Se alege un element oarecare din $\mathbb{Z}_n^*$. Fie acesta g
2. Daca $\varphi(n) = m$, se calculează g^{d_i}, unde d_i sunt divizorii naturali ai lui m
3. $d_i = \frac{m}{p_i}$ $\forall i$
4. Dacă $g^{d_i} \not\equiv 1 \pmod n$, trag concluzia că g este generator al lui $\mathbb{Z}_n^*$
5. Se pot găsi ușor alți generatori de forma g^k, $(k, m) = 1$ (k prim cu m)

Ex. Să se determine grupul unităților și un sistem minimal de generatori pentru $\mathbb{Z}_{27}^*$.

$\mathbb{Z}_{27}^* = U(\mathbb{Z}_{27}^*) = \{a \in \mathbb{Z}_{27}^*, (a, 27) = 1\} = \{1, 4, 4, 5, 7, 8, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$

- $n = 27 = 3^3 \Rightarrow \mathbb{Z}_{27}^*$ grup ciclic

Fie $g = 2$

- $m = \varphi(27) = 27\left(1 - \frac{1}{3}\right) = 27 \cdot \frac{2}{3} = 18$

$18 = 2 \cdot 3^2$

- $d_1 = \frac{18}{2} = 9$, $d_2 = \frac{18}{3} = 6$

$d_2 = 6 \rightarrow 2^3 = 8$, $2^6 = 8^2 = 64 \overset{27}{\equiv} 10 \neq 1 \pmod{27}$

$d_1 = 9 \rightarrow 2^9 = 2^6 \cdot 2^3 = 10 \cdot 8 = 80 \overset{27}{\equiv} 26 \neq 1 \pmod{27}$

$\rightarrow g = 2$ generator al lui $\mathbb{Z}_{27}^*$

Alți generatori sunt de forma

2^k, $(k, 18) = 1 \rightarrow k \in \{1, 5, 7, 11, 13, 17\}$

$\hookrightarrow 2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$

$= 2, 5, 20, 23, 11, 14$

$[2] = \{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}, 2^{13}\}$

$= 2, 4, 8, 16, 5, 10, 20, 13, 26, 25, 23, 19, 11$

$$\left\{ \begin{matrix} 2^{14} \\ 22 \end{matrix}, \begin{matrix} 2^{15} \\ 17 \end{matrix}, \begin{matrix} 2^{16} \\ 7 \end{matrix}, \begin{matrix} 2^{17} \\ 14 \end{matrix}, \begin{matrix} 2^{18} \\ 1 \end{matrix}, \right\}$$