# SEMINAR 1

Introducere

https://www.youtube.com/watch?v=i9CBKGLVCME

https://youtu.be/NzyFhSDrrrM?si=49LZiReHoWQxmYnD&t=1380

De citit

https://sherlock-holm.es/stories/pdf/a4/1-sided/danc.pdf

Google sheet
https://docs.google.com/spreadsheets/d/1dmztp1bBcNZFg8jgCk0Giq5kA4eMm47i8c5px8BvegI/edit?usp=sharing

## Cel mai mare divizor comun și inversul unui număr

### Definiție

Fie $a, b \in \mathbb{Z}$ astfel încât $(a \neq 0) \vee (b \neq 0)$. Un număr $d \in N^*$ se numește **cel mai mare divizor comun** al numerelor $a$ și $b$, notat $d = (a, b)$, dacă:

- $d|a \wedge d|b$
- $d'|a \wedge d'|b \Rightarrow d'|d.$

Prin convenție $(0,0) = 0.$

*Exemple:*

- $(3,5) = 1$
- $(12,18) = 6$
- $(a, 0) = a, \forall\, a \in \mathbb{Z}^*.$

> "[The Euclidean algorithm] is the granddaddy of all algorithms, because it is the oldest nontrivial algorithm that has survived to the present day."
>
> Donald Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 2nd edition (1981), p. 318.

- Determinați, prin două metode, cmmdc al numerelor $360$ și $294$.

$$360 = 2^3 \times 3^2 \times 5$$

$$294 = 2 \times 3 \times 7^2$$

$$(360,294) = 2 \times 3 = 6$$

### Algoritmul lui Euclid (versiunea lui Lamé)

Algoritmul lui Euclid determină $d = (a, b)$.

- Dacă $a = 0$ sau $b = 0$, atunci $d = b$, respectiv $d = a$.
- Presupunem $a \neq 0 \wedge b \neq 0$.

  Conform Teoremei împărțirii cu rest, există $q_0, r_0 \in \mathbb{N}$ astfel încât

$$a = bq_0 + r_0 ; 0 \leq r_0 < b.$$

Dacă $r_0 = 0$ atunci $a = bq_0$ și $d = (a, b) = b$.

Dacă $r_0 \neq 0$ aplicăm din nou Teorema împărțirii cu rest pentru b și $r_0$:

$$b = r_0 q_1 + r_1 ; 0 \leq r_1 < r_0.$$

Continuăm procedeul până obținem un rest nul:

$$\ldots r_n = r_{n-1} q_n + r_n ; 0 \leq r_n < r_{n-1}.$$

$$r_{n-1} = r_n q_{n+1} .$$

Mulțimea $\{b, r_0, \ldots, r_n\} \cap \mathbb{N}^*$ este mărginită, deci este finită.

Deoarece șirul de numere naturale $b > r_0 > \ldots > r_n$ este strict descrescător, ajungem la restul egal cu 0 după un număr finit de împărțiri, deci algoritmul prezentat are un număr finit de pași.

$$r_n = (a, b).$$

*Exemplu*

$$(360{,}294)$$
$$360 = 294 \times 1 + 66$$
$$294 = 66 \times 4 + 30$$
$$66 = 30 \times 2 + 6$$
$$30 = 6 \times 5 + 0$$
$$\Longrightarrow (360{,}294) = 6$$

## Identitatea lui Bézout/Algoritmul lui Euclid extins

Fie $a, b \in \mathbb{Z}$ și $d = (a, b)$. Atunci $\exists u, v \in \mathbb{Z}$ cu proprietatea că

$$d = ua + vb.$$

Determinarea numerelor $u$ și $v$ se face cu ajutorul algoritmului lui Euclid.

Considerăm următorul vector:

$$\boldsymbol{x_d} = (\boldsymbol{u}, \boldsymbol{v})$$

pe care îl calculăm pas cu pas urmărind algoritmul lui Euclid.

Îi inițializăm astfel:

$$\boldsymbol{x_a} = (\mathbf{1}, \mathbf{0}), \boldsymbol{x_b} = (\mathbf{0}, \mathbf{1}).$$

| | |
|---|---|
| $a = bq_0 + r_0 \Longrightarrow r_0 = a - q_0 b$ | $\boldsymbol{x}_{r_0} = (1{,}0) - q_0(0{,}1) = (1, -q_0)$ |
| $b = r_0 q_1 + r_1 \Longrightarrow r_1 = b - q_1 r_0$ | $(u, v) = (0{,}1) - q_1(1, -q_0) = (-q_1, 1 - q_0)$ |
| ... | |

### *Exemplu*

| | |
|---|---|
| $360 = 294 \times 1 + 66$ | $\boldsymbol{x_{66} = (1,0) - 1(0,1) = (1,-1)}$ |
| $294 = 66 \times 4 + 30$ | $\boldsymbol{x_{30} = (0,1) - 4(1,-1) = (-4,5)}$ |
| $66 = 30 \times 2 + 6$ | $\boldsymbol{x_{6} = (1,-1) - 2(-4,5) = (9,-11)}$ |
| $30 = 6 \times 5 + 0$ | |

$$\Longrightarrow 6 = 9 \times 360 + (-11) \times 294.$$

## Inelul $\mathbb{Z}_n$

$\mathbb{Z}_n$ are structură de inel comutativ, unitar. Mulțimea elementelor inversabile din $\mathbb{Z}_n$ are structură de grup, iar numărul de elemente este dat de funcția indicatoare a lui Euler.

Funcția indicatoare a lui Euler $\varphi$: $\mathbb{N}^* \to \mathbb{N}$ numără numărul numerelor prime cu numărul mai mici decât numărul.

### *Proprietăți:*

$\varphi(p) = p - 1, \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, dacă $p$ este prim.

$\varphi(ab) = \varphi(a)\varphi(b)$, dacă $(a,b) = 1$

Dacă $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ (descompunerea lui $n$ în factori primi), atunci $\varphi(n) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i})$

## Inversul unui număr în $\mathbb{Z}_n$/Rezolvarea ecuațiilor de tip $ax \equiv b\ (mod\ n)$

Fie $a \in \mathbb{Z}_n$. Dacă $(a,n) = 1$, atunci $\exists a^{-1} \in \mathbb{Z}_n$.

Dacă $(a,n) = 1$, atunci $\exists u, v$ astfel încât

$$1 = ua + vn.$$

Trecând egalitatea în $\mathbb{Z}_n$, obținem

$$1 \equiv ua\ (mod\ n),$$

deci $\exists a^{-1} = u$

Considerând mai general ecuația

$$ax \equiv b\ (mod\ n)$$

ea are soluții dacă $(a,n)|b$. În caz afirmativ, fie $d = (a,n)$

$$a = dA, b = dB, n = dN.$$

$$AX \equiv B\ (mod\ N)$$

În acest caz $(A,N) = 1$, deci $x \equiv A^{-1}B(mod\ N)$. Așadar

$$x \equiv A^{-1}B + kN\ (mod\ n), \text{ unde } k \in \{0,\dots,d-1\}. \quad (1)$$

## Exerciții

1. Pentru fiecare din perechile următoare, determinați c.m.m.d.c. folosind algoritmul lui Euclid și exprimați rezultatul ca o combinație liniară cu coeficienți întregi a numerelor inițiale.
   (a) 26; 19 (b) 187; 34 (c) 841; 160 (d) 1547; 560 (e) 2613; 2171 (f) 4577; 7843.
2. Calculați:
   (a) $\varphi(30)$ (b)$\varphi(40)$ (c) $\varphi(800)$ (d) $\varphi(1024)$ (e) $\varphi(1763)$
3. Rezolvați ecuațiile:
   (a) $122x \equiv 1 \pmod{343}$; (b) $34x \equiv 2 \pmod{187}$; $2171x \equiv 1 \pmod{2613}$
4. Pentru perechile următoare, verificați dacă elementul $\hat{b}$ este inversabil în inelul $\mathbb{Z}_a$ și, în caz afirmativ, determinați $\hat{b}^{-1}$
   (a) a = 97; b = 13 (b) a = 973; b = 347 (c) a = 767; b = 987(d) a = 768; b = 987 (e) a = 419; b = 39.
5. Demonstrași rezutatul (1)

## Implementări

1. CMMDC
2. Inversul

```
int modulo(int k, int n){//extindem operatorul modulo (%) si pentru numere
negative
     if (k < 0)k = n - (-k) % n;
     if (k >= n) return k%n;
     return k;
}

int invers(int a, int n){
     int q, r, x0 = 1, x1 = 0, copy_n = n;
     a = modulo(a, n);
     while (n != 0)
     {
             r = n;
             q = a / n;
             n = a%n;
             a = r;

             r = x1;
             x1 = x0 - q*x1;
             x0 = r;
     }
     if (a == 1)//daca numarul este inversabil
             return modulo(x0, copy_n);
     return -1;//daca numarul nu este inversabil, vom intoarce -1, pentru a
putea afisa mesajul corespunzator
```

# TEME PORTOFOLIU

1. Găsiți numărul minim și maxim de pași pentru algoritmul lui Euclid.

Din fiecare din pachetele de mai jos, abordati exercitiul aferent numarului vostru din fisierul EXCEL

## 2. CMMDC

1. Găsiți cel mai mare divizor comun al lui 12345 și 54321 folosind algoritmul lui Euclid extins pentru a determina coeficienții Bezout.

2. Determinați cel mai mare divizor comun al lui 23456 și 65432 cu ajutorul algoritmului lui Euclid extins pentru a găsi coeficienții Bezout.

3. Folosind algoritmul lui Euclid extins, calculați CMMDC al lui 34567 și 76543 și determinați coeficienții Bezout.

4. Găsiți cel mai mare divizor comun pentru 45678 și 87654 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

5. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 56789 și 98765 și determinați coeficienții Bezout.

6. Determinați cel mai mare divizor comun dintre 67890 și 9876 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

7. Calculați CMMDC al lui 78901 și 10987 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

8. Găsiți cel mai mare divizor comun al lui 89012 și 21098 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

9. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 90123 și 32109 și găsiți coeficienții Bezout.

10. Determinați cel mai mare divizor comun al lui 11223 și 33211 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

11. Calculați CMMDC al lui 22334 și 44332 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

12. Găsiți cel mai mare divizor comun dintre 33445 și 55443 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

13. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 44556 și 66554 și găsiți coeficienții Bezout.

14. Determinați cel mai mare divizor comun al lui 55667 și 77665 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

15. Calculați CMMDC al lui 66778 și 88776 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

16. Găsiți cel mai mare divizor comun al lui 77889 și 99887 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

17. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 88901 și 10987 și găsiți coeficienții Bezout.

18. Determinați cel mai mare divizor comun dintre 99012 și 10098 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

19. Calculați CMMDC al lui 11223 și 21100 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

20. Găsiți cel mai mare divizor comun al lui 12345 și 33221 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

21. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 22334 și 44332 și găsiți coeficienții Bezout.

22. Determinați cel mai mare divizor comun al lui 33445 și 55443 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

23. Calculați CMMDC al lui 44556 și 66554 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

24. Găsiți cel mai mare divizor comun al lui 55667 și 77665 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

25. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 66778 și 88776 și găsiți coeficienții Bezout.

26. Determinați cel mai mare divizor comun al lui 77889 și 99887 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

27. Calculați CMMDC al lui 88901 și 10987 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

28. Găsiți cel mai mare divizor comun dintre 99012 și 10098 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

29. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 12345 și 21100 și găsiți coeficienții Bezout.

30. Determinați cel mai mare divizor comun al lui 11223 și 33221 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

31. Calculați CMMDC al lui 22334 și 44332 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

32. Găsiți cel mai mare divizor comun al lui 33445 și 55443 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

33. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 44556 și 66554 și găsiți coeficienții Bezout.

34. Determinați cel mai mare divizor comun al lui 55667 și 77665 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

35. Calculați CMMDC al lui 66778 și 88776 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

36. Găsiți cel mai mare divizor comun al lui 77889 și 99887 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

37. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 88901 și 10987 și găsiți coeficienții Bezout.

38. Determinați cel mai mare divizor comun dintre 99012 și 10098 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

39. Calculați CMMDC al lui 12345 și 21100 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

40. Găsiți cel mai mare divizor comun al lui 11223 și 33221 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

41. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 22334 și 44332 și găsiți coeficienții Bezout.

42. Determinați cel mai mare divizor comun al lui 33445 și 55443 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

43. Calculați CMMDC al lui 44556 și 66554 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

44. Găsiți cel mai mare divizor comun al lui 55667 și 77665 folosind algoritmul lui Euclid extins și determinați coeficienții Bezout.

45. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 66778 și 88776 și găsiți coeficienții Bezout.

46. Determinați cel mai mare divizor comun al lui 77889 și 99887 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

47. Calculați CMMDC al lui 88901 și 10987 cu ajutorul algoritmului lui Euclid extins și determinați coeficienții Bezout.

48. Găsiți cel mai mare divizor comun dintre 99012 și 10098 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

49. Utilizați algoritmul lui Euclid extins pentru a calcula CMMDC pentru 12345 și 21100 și găsiți coeficienții Bezout.

50. Determinați cel mai mare divizor comun al lui 11223 și 33221 folosind algoritmul lui Euclid extins și găsiți coeficienții Bezout.

## 3. Inversul unui număr în $\mathbb{Z}_n$

1. Găsiți inversul modular al lui 7 modulo 11.

2. Calculați inversul modular al lui 15 modulo 26.

3. Determinați inversul modular al lui 21 modulo 37.

4. Găsiți inversul modular al lui 35 modulo 43.

5. Calculați inversul modular al lui 10 modulo 17.

6. Determinați inversul modular al lui 29 modulo 31.

7. Găsiți inversul modular al lui 12 modulo 19.

8. Calculați inversul modular al lui 25 modulo 47.

9. Determinați inversul modular al lui 18 modulo 29.

10. Găsiți inversul modular al lui 40 modulo 53.

11. Calculați inversul modular al lui 23 modulo 41.

12. Determinați inversul modular al lui 33 modulo 59.

13. Găsiți inversul modular al lui 16 modulo 27.

14. Calculați inversul modular al lui 28 modulo 37.

15. Determinați inversul modular al lui 42 modulo 61.

16. Găsiți inversul modular al lui 19 modulo 31.

17. Calculați inversul modular al lui 36 modulo 67.

18. Determinați inversul modular al lui 44 modulo 73.
19. Găsiți inversul modular al lui 13 modulo 23.
20. Calculați inversul modular al lui 30 modulo 47.
21. Determinați inversul modular al lui 50 modulo 79.
22. Găsiți inversul modular al lui 17 modulo 37.
23. Calculați inversul modular al lui 38 modulo 83.
24. Determinați inversul modular al lui 55 modulo 89.
25. Găsiți inversul modular al lui 20 modulo 43.
26. Calculați inversul modular al lui 27 modulo 59.
27. Determinați inversul modular al lui 48 modulo 97.
28. Găsiți inversul modular al lui 24 modulo 53.
29. Calculați inversul modular al lui 39 modulo 67.
30. Determinați inversul modular al lui 45 modulo 101.
31. Găsiți inversul modular al lui 22 modulo 41.
32. Calculați inversul modular al lui 35 modulo 73.
33. Determinați inversul modular al lui 49 modulo 103.
34. Găsiți inversul modular al lui 26 modulo 47.
35. Calculați inversul modular al lui 51 modulo 107.
36. Determinați inversul modular al lui 60 modulo 109.
37. Găsiți inversul modular al lui 29 modulo 61.
38. Calculați inversul modular al lui 46 modulo 113.
39. Determinați inversul modular al lui 65 modulo 127.
40. Găsiți inversul modular al lui 32 modulo 67.
41. Calculați inversul modular al lui 53 modulo 131.
42. Determinați inversul modular al lui 70 modulo 137.
43. Găsiți inversul modular al lui 18 modulo 37.
44. Calculați inversul modular al lui 56 modulo 139.
45. Determinați inversul modular al lui 75 modulo 149.
46. Găsiți inversul modular al lui 37 modulo 73.

47. Calculați inversul modular al lui 58 modulo 151.

48. Determinați inversul modular al lui 80 modulo 157.

49. Găsiți inversul modular al lui 28 modulo 59.

50. Calculați inversul modular al lui 61 modulo 163.