FAI

Kaliseu

June 1, 2022

1 Rangul unei matrice

rang A = numarul necunoscutelor principale
n - rang A = numarul necunoscutelor secundare sau ordinul de nedeterminare

Definitie: Sn rang A numarul natural r cu proprietatile:

$$0 \leq r \leq min(m, n) \tag{1}$$

$$Exista\ un\ minor\ nenul\ r\ in\ A \tag{2}$$

$$Oricare\ ar\ fi\ x\ minor\ de\ ordin\ \geq\ ordinul\ lui\ r\ este\ nul \tag{3}$$

Particularitatiale metodei de aflare a rangului unei matrice folosind Gauss:

1. Pivotul diferit de 0 si devine 1
2. Linia pivotului se completeaza cu 0
3. Coloana pivotului, sub pivot, se completeaza cu 0
4. Se aplica regula dreptunghiului pentru restul elementelor

2 Rezolvarea sistemelor de ecuatii cu Gauss

Fie un sistem de 3 ecuatii cu 3 necunoscute:

$$\begin{cases} x_1 + x_2 - x_3 = 0 \\ 3x_1 - 2x_2 + 2x_3 = 5 \\ 2x_1 + 3x_2 - 2x_3 = 2 \end{cases} \tag{4}$$

Se construieste matricea A punand pe coloane indicii fiecarui x si se extinde cu coloana rezultatelor:

$$\left(\begin{array}{ccc|c} 1 & 1 & -1 & 0 \\ 3 & -2 & 2 & 5 \\ 2 & 3 & -2 & 2 \end{array}\right) \tag{5}$$

$$unde\ coloana\ 1\ corespunde\ lui\ x_1,\ coloana\ 2\ lui\ x_2\ si\ coloana\ 3\ lui\ x_3$$

Particularitatiale metodei de rezolvare a sistemelor de ecuatii liniare folosind Gauss:

1. Pivotul diferit de 0 si se pastreaza
2. Linia pivotului se pastreaza
3. Coloana pivotului se completeaza cu 0
4. Se aplica regula dreptunghiului pentru restul elementelor

3 Gasirea inversei unei matrice folosind metoda Gauss

Definitie inversa unei matrice:

$$A \cdot A^{-1} = A^{-1} \cdot A = I_n$$

Se extinde matricea A cu matricea unitate, I_n:

$$\left(\begin{array}{c|c} A & I_n \end{array}\right) \tag{6}$$

si se rezolva folosind metoda Gauss pana se ajunge la:

$$\left(\begin{array}{c|c} I_n & A^{-1} \end{array}\right) \tag{7}$$

Particularitatiale metodei de gasite a inversei unei matrice cu Gauss:

1. Pivotul diferit de 0 si se pastreaza
2. Linia pivotului se pastreaza
3. Coloana pivotului se completeaza cu 0
4. Se aplica regula dreptunghiului pentru restul elementelor

4 Spatii vectoriale

Fie u si v doi vectori din R^n peste un corp K:

$$u = (a_1, a_2, ..., a_n)$$
$$v = (b_1, b_2, ..., b_n)$$

Proprietati ale vectorilor:
1. Suma pe coordonate:

$$u + v = (a_1 + b_1, a_2 + b_2, ..., a_n + b_n)$$

2. Element neutru fata de suma pe coordonate:

$$e = (0, 0, ..., 0) \;\; a.i. \;\; u + e = u = (a_1, a_2, ..., a_n)$$

3. Element opus:

$$u' = -u = (-a_1, -a_2, ..., -a_n)$$

4. Inmultirea cu scalar din K:

$$\alpha \cdot u = (\alpha \cdot a_1, \alpha \cdot x_2, ..., \alpha \cdot x_n)$$

Vectorii particulari
Se numesc vectorii particulari ai lui R^n:

$$\begin{aligned} &e_1 = (1, 0, ..., 0) \\ &e_2 = (0, 1, ..., 0) \\ &... \\ &e_n = (0, 0, ..., 1) \end{aligned}$$

si formeaza Baza Canonica in R^n

5 Combinatii liniare

Fie $v_1, v_2, ..., v_n$ vectori in V. Se numeste combinatie liniara:

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = O_V$$

unde:

$$\begin{aligned} &\alpha_1, \alpha_2, ..., \alpha_n \; sunt \; scalari \; din \; K \\ &v_1, v_2, ..., v_n \; sunt \; vectori \; din \; R^n \\ &O_V = (0, 0, ..., 0) \end{aligned}$$

Vectorii $v_1, v_2, ..., v_n$ se numesc linear independenti daca:

$$\alpha_1 = \alpha_2 = ... = \alpha_n = 0$$

Observatie: Vectorii proprii sunt intotdeauna liniar independenti, deoarece formeaza o baza in R^n.

6 Sisteme de generatori

Numim V' un subspatiu vectorial al unui spatiu vectorial V daca toate combinatiile liniare ale vectorilor din V' se afla tot in V.

Se numeste sistem de vectori o multime de vectori si se noteaza prin:

$$\{v_1, v_2, ..., v_r\}$$

Multimea tuturor combinatiilor liniare ale unei multimi de vectori constituie un subspatiu vectorial al lui V, cu $V' \subset V$ si se noteaza prin:

$$[v_1, v_2, ..., v_r]$$

Daca $V' \equiv V$, atunci spunem ca $\{v_1, v_2, ..., v_r\}$ se numeste sistem de generatori ai spatiului V, iar V se numeste spatiu vectorial finit generat.

Proprietati ale sistemelor de generatori

1. Orice vector din V se poate exprima ca o combinatie liniara cu coeficienti din K si vectori din V'
2. In general, aceasta combinatie liniara nu este unica
3. Daca aceasta combinatie liniara este unica, atunci spunem ca $\{v_1, v_2, ..., v_r\}$ formeaza o baza in V

7 Baze ale spatiilor vectoriale

Se numeste baza a lui V, un sistem de vectori $\{v_1, v_2, ..., v_r\}$ daca indeplineste 2 conditii:

1. Vectorii sistemului sunt liniar independenti in V
2. Sistemul constituie un sistem de generatori al lui V

Conform definitiei: Orice vector u din V se poate scrie in mod unic in functie de α din K si $\{v_1, v_2, ..., v_n\}$ prin urmatoarea relatie:

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = u$$

iar coordonatele $\alpha_1, \alpha_2, ..., \alpha_n$ sunt coordonatele lui u in aceasta baza.

Teorema dimensiunii: Oricare 2 baze ale unui spatiu vectorial finit generat V au acelasi numar de elemente. Numarul de elemente ale unei baze se numeste dimensiunea spatiului respectiv.

Proprietati ale bazelor

1. Orice sistem liniar independent $\{v_1, v_2, ..., v_r\}$ din V poate fi completat pana la o baza a lui V.

De aici deducem ca daca dimensiunea unui sistem linear independent = dimensiunea spatiului V, atunci acel sistem formeaza o baza in V

2. Din orice sistem de generaotri ai lui V se poate extrage o baza.

De aici deducem ca daca dimensiunea unui sistem de generatori = dimensiunea spatiului V, atunci acel sistem formeaza o baza in V

Tehnica demonstrare ca un sistem de vectori constituie o baza in V:

1. Se construieste combinatia liniara:

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = O_V$$

Exemplu:

$$\alpha_1(1, -1, 2) + \alpha_2(-2, 3, 5) + \alpha_3(2, -2, 1) = (0, 0, 0)$$

2. Se construieste matricea A care are coordonatele vectorilor pe coloane si se extinde cu coloana rezultatelor (coloana de 0):

$$\left(\begin{array}{cccc|c} v_1 & v_2 & ... & v_n & 0 \end{array}\right)$$

Exemplu:

$$\left(\begin{array}{ccc|c} 1 & -2 & 2 & 0 \\ -1 & 3 & -2 & 0 \\ 2 & 5 & 1 & 0 \end{array}\right)$$

3. Se rezolva sistemul folosind metoda lui Gauss pentru rezolvarea sistemelor de ecuatii, cu exact aceleasi particularitati.

4. Daca la final $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$ si rangul matricei formate este egal cu dimensiunea spatiului V, atunci vectorii respectivi formeaza o baza in spatiul V.

8 Subspatiul generat de un sistem de vectori si o baza a sa

Fie V un spatiu vectorial in R^n, V' un subspatiu vectorial al lui V si A o matrice care are pe coloane coordonatele vectorilor subspatiului V'.

Dimensiunea subspatiului V' = rang A.

O baza a lui V' este formata din vectorii coloanelor ce stabilesc rangul lui A

9 Schimbarea coordonatelor unui vector din Baza Canonica in Baza Oarecare

Fie V un spatiu vectorial in R^n, u un vector din V si $\{v_1, v_2, ..., v_n\}$ o baza oarecare in V. Coordonatele initiale ale lui u sunt date in Baza Canonica. Pentru a afla coordonatele lui u in Baza Oarecare data, se construieste combinatia liniara urmatoare:

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = u$$

Exemplu pentru R^2, u = (1, -1) si $\{v_1 = (2, 3), v_2 = (1, 2)\}$:

$$\alpha_1(2, 3) + \alpha_2(1, 2) = (1, -1)$$

Se construieste matricea A care are pe coloane coordonatele vectorilor din Baza Oarecare si se extinde cu coloana coordonatelor lui u in Baza Canonica.

$$\left(\begin{array}{cccc|c} v_1 & v_2 & ... & v_n & u \end{array}\right)$$

Exemplu pentru R^2, u = (1, -1) si $\{v_1 = (2, 3), v_2 = (1, 2)\}$:

$$\left(\begin{array}{cc|c} 2 & 1 & 1 \\ 3 & 2 & -1 \end{array}\right)$$

Se rezolva folosind regula lui Gauss pentru rezolvarea sistemelor de ecuatii, cu aceleasi particularitati.

Solutiile sistemului, acestea fiind $\alpha_1, \alpha_2, ..., \alpha_n$, reprezinta coordonatele vectorului u in Baza Oarecare data:

$$u = (\alpha_1, \alpha_2, ..., \alpha_n)$$

10 Schimbarea coordonatelor unui vector dintr-o Baza Oarecare in alta Baza Oarecare

Fie V un spatiu vectorial in R^n, w un vector din V.
Fie $B_1 = \{u_1, u_2, ..., u_n\}$ si $B_2 = \{v_1, v_2, ..., v_n\}$ doua baze oarecare ale lui V.

Trecerea de la B_1 la B_2:

1. Se construieste sistemlor de ecuatii pentru trecerea de la B_1 la B_2:

$$\begin{cases} \alpha_{11}u_1 + \alpha_{21}u_2 + \ldots + \alpha_{n1}u_n = v_1 \\ \alpha_{12}u_1 + \alpha_{22}u_2 + \ldots + \alpha_{n2}u_n = v_2 \\ \vdots \\ \alpha_{1n}u_1 + \alpha_{2n}u_2 + \ldots + \alpha_{nn}u_n = v_n \end{cases}$$

Exemplu pentru R^3:

$$\begin{cases} \alpha_{11}u_1 + \alpha_{21}u_2 + \alpha_{31}u_3 = v_1 \\ \alpha_{12}u_1 + \alpha_{22}u_2 + \alpha_{32}u_3 = v_2 \\ \alpha_{13}u_1 + \alpha_{23}u_2 + \alpha_{33}u_3 = v_3 \end{cases}$$

2. Se creeaza matricea A care are pe coloane coordonatele vectorilor $\{u_1, u_2, ..., u_n\}$ si se extinde cu coloane pe care se afla coordonatele vectorilor $\{v_1, v_2, ..., v_n\}$:

$$\left(\begin{array}{cccc|cccc} u_1 & u_2 & \ldots & u_n & v_1 & v_2 & \ldots & v_n \end{array}\right)$$

Exemplu pentru R^3, unde
$u_1 = (a_1, a_2, a_3), u_2 = (b_1, b_2, b_3), u_3 = (c_1, c_2, c_3)$ si
$v_1 = (d_1, d_2, d_3), v_2 = (e_1, e_2, e_3), v_3 = (f_1, f_2, f_3)$:

$$\left(\begin{array}{ccc|ccc} a_1 & b_1 & c_1 & d_1 & e_1 & f_1 \\ a_2 & b_2 & c_2 & d_2 & e_2 & f_2 \\ a_3 & b_3 & c_3 & d_3 & e_3 & f_3 \end{array}\right)$$

3. Se rezolva folosind metoda lui Gauss pentru rezolvarea sistemelor de ecuatii cu aceleasi particularitati pana se ajunge la forma:

$$\left(\begin{array}{c|c} I_n & T \end{array}\right)$$

4. Se calculeaza S $= T^{-1}$ folosind metoda lui Gauss pentru calcularea inversei unei matrice.

5. Daca nu sunt deja date, se calculeaza coordonatele in B_1 ale vectorului caruia vrem sa ii schimbam baza, folosind metoda de **Schimbare a coordonatelor unui vector din Baza Canonica in Baza Oarecare**.

6. Fie $w = (x_1, x_2, ..., x_n)$ in B_1 si $w = (y_1, y_2, ..., y_n)$ in B_2.
Cunoastem coordonatele lui w in B_1 pentru ca ne-au fost date de problema, sau au fost calculate de noi la punctul 5. Formula dupa care putem afla coordonatele lui w in B_2, trecand de la B_1 la B_2 este:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = T^{-1} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

11 Operatii cu subspatii vectoriale

Fie V un spatiu vectorial finit generat in R^n, $B = \{u_1, u_2, ..., u_n\}$ o baza in V si $V' = [v_1, v_2, ..., v_m]$ un subspatiu vectorial al lui V.

Se poate creea sistemul:

$$\begin{cases} \alpha_{11}u_1 + \alpha_{21}u_2 + \ldots + \alpha_{n1}u_n = v_1 \\ \alpha_{12}u_1 + \alpha_{22}u_2 + \ldots + \alpha_{n2}u_n = v_2 \\ \vdots \\ \alpha_{1m}u_1 + \alpha_{2m}u_2 + \ldots + \alpha_{nm}u_n = v_m \end{cases}$$

Rezolvarea sistemului se face exact ca rezolvarea sistemului de la **Schimbarea coordonatelor unui vector dintr-o Baza Oarecare in alta Baza Oarecare** si ne da ca solutii coordonatele vectorilor $\{v_1, v_2, ..., v_m\}$ in baza B, sub forma alpha-urilor din sistem.

De exemplu, coordonatele lui v_1 dupa rezolvarea sistemlui de ecuatii vor fi:

$$v_1 = (\alpha_{11}, \alpha_{21}, ..., \alpha_{n1})$$

Cu aceste coordonate, se poate construi matricea A care are pe coloane coordonatele vectorilor $\{v_1, v_2, ..., v_m\}$ in baza B:

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1m} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2m} \\ \vdots & & & \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nm} \end{pmatrix}$$

Intre V' si A exista urmatoarea legatura:

Teorema: dimensiunea lui V' = rang A

Consecinta: Daca rang A = nr. vectorilor din V', atunci vectorii din V' sunt liniar independenti.

Operatii cu subspatii vectoriale:

Fie V un spatiu vectorial finit generat in R^n si V_1 si V_2 doua subspatii ale lui V.

1. Suma subspatiilor

$$V_1 + V_2 = \{u \in V \;\; \big| \;\; u = u_1 + u_2,\; u_1 \in V_1, u_2 \in V_2\}$$

Proprietatile noile submultimi:

1. Este subspatiu al lui V
2. Este cel mai mic subspatiu care contine si pe V_1 si pe V_2

2. Intersectia subspatiilor

$$V_1 \cap V_2 = \{x \in V \;\; \Big| \;\; x \in V_1 \; si \; x \in V_2\}$$

Proprietatile noile submultimi:

1. Este subspatiu al lui V
2. Este cel mai mare subspatiu comun intre V_1 si V_2

Teorema dimensiunii: Pentru orice pereche de subspatii V_1 si V_2 din V, are loc relatia:

$$dim(V_1 + V_2) = dimV_1 + dimV_2 - dim(V_1 \cap V_2)$$

12 Aplicatii Liniare

Fie V_1 si V_2 doua spatii vectoriale peste un corp comutativ K.
Se numeste aplicatie liniara, o functie $f : V_1 -> V_2$ daca si numai daca:

1. $f(x + y) = f(x) + f(y)$ (aditivitate)
2. $f(\alpha \cdot x) = \alpha \cdot f(x)$ (omogenitate)

Nucleul si Imaginea unei aplicatii liniare

$$Ker(f) = \{x \in V_1 \;\; \Big| \;\; f(x) = O_{V_2}\}$$

Cu proprietateile ca:

1. Ker(f) $\subseteq V_1$
2. Ker(f) este subspatiu al lui V_1

$$Im(f) = \{y \in V_2 \;\; \Big| \;\; f(x) = y, \; x \in V_1\}$$

Cu proprietateile ca:

1. Im(f) $\subseteq V_2$
2. Im(f) este subspatiu al lui V_2

Teorema Rang-Defect:

$$dim(V_1) = dim(Ker(f)) + dim(Im(f))$$

unde:

$$dim(Ker(f)) = defectf$$

$$dim(Im(f)) = rangf$$

13 Matricea asociata unei aplicatii liniare in baza canonica si intr-o baza oarecare

Fie $f : V_1 - > V_2$ o aplicatie liniara, $dim(V_1) = n$, $dim(V_2) = m$, $B_1 = \{e_1, e_2, ..., e_n\}$ baza in V_1 si $B_2 = \{f_1, f_2, ..., f_n\}$ baza a lui V_2.

Matricea A care are pe coloane coordonatele vectorilor $f(e_1)$, $f(e_2)$, ..., $f(e_n)$ in baza B_2, se numeste matrice asociata lui f in bazele B_1 si B_2.

Exemplu pentru $T : R^2 - > R^2; T(x) = (x_1 - x_2, -4x_1 - 2x_2)$ si baza canonica a lui R^2:
$B_1 = \{e_1 = (1, 0), e_2 = (0, 1)\}$ si $B_2 = \{f_1 = (1, 0), f_2 = (0, 1)\}$

$T(e_1) = T(1, 0) = (1 - 0, -4 \cdot 1 - 2 \cdot 0) = (1, -4) = 1 \cdot (1, 0) - 4 \cdot (0, 1)$
$T(e_2) = T(0, 1) = (0 - 1, -4 \cdot 0 - 2 \cdot 1) = (-1, -2) = -1 \cdot (1, 0) - 2 \cdot (0, 1)$

$$A_T^{B_c} = \begin{pmatrix} 1 & -1 \\ -4 & -2 \end{pmatrix}$$

Daca $f : V - > V$ aplicatie liniara,
$B_1 = \{e_1 = (1, 0), e_2 = (0, 1)\}$ si $B_2 = \{f_1 = (1, 0), f_2 = (0, 1)\}$ ale lui V si C matricea de trecere de la baza B_1 la baza B_2

$$A_f^{B_2} = C^{-1} \cdot A_f^{B_1} \cdot C$$

$A_f^{B_1}$ este matricea asociata lui f in baza B_1
$A_f^{B_2}$ este matricea asociata lui f in baza B_2

14 Vectori si valori proprii ale unui operator liniar

Metoda de rezolvare:

1. Se gaseste matricea asociata lui f in Baza Canonica dupa metoda prezentata mai sus, sau construind-o cu coeficientii componentelor pe linii.

Exemplu pentru: $f(x_1, x_2) = (2x_1 - x_2, x_1 + 3x_2)$

$$A = \begin{pmatrix} 2 & -1 \\ 1 & 3 \end{pmatrix}$$

2. Se calculeaza polinomul $P_A(\lambda) = det(A - \lambda \cdot I_n)$

3. Se calculeaza valorile proprii λ egaland $P_A(\lambda) = 0$

4. Vectorii proprii se calculeaza rezolvand sistemul $(A - \lambda \cdot I_n) \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ pentru fiecare λ gasit la punctul 3.

5. Pentru a calcula A^n, mai intai se afla $T = \begin{pmatrix} v_1 & v_2 & \dots & v_n \end{pmatrix}$, unde v_1, v_2, ..., v_n sunt vectorii proprii aflati la punctul 4.

6. Se calculeaza T^{-1} folosind metoda lui Gauss pentru calcularea inversei unei matrice.

7. Se calculeaza matricea coloana $B = T^{-1} \cdot A \cdot T$

8. Se calculeaza $A^n = T \cdot B^n \cdot T^{-1}$

15 Teorema impartirii cu rest. Divizibilitate. Numere prime

Fie $m, n \in Z, n \neq 0$. Atunci exista si este unic $q, r \in Z$ a.i. :

$$m = n \cdot q + r, \ \ 0 \leq r \leq |n| - 1$$

Spunem ca $n \in Z$ divide $m \in Z$, m/n daca exista $q \in Z$ a.i. :

$$m = n \cdot q$$

Proprietati:

1. n/n
2. n/m si m/p atunci n/p
3. n/m si m/n atunci m = +- n
4. n/m atunci $|n| \leq |m|$

Un numar intreg p se numeste prim daca $p \neq 0, 1, -1$ si nu are divizori proprii

Se numeste cel mai mare divizor comun al numerelor naturale a,b, numarul pozitiv d, cmmmdc(a,b), (a,b) cu proprietatile:
1. d/a, d/b
2. c/a, c/b, atunci c/d

Numerele a si b se numesc prime intre ele daca (a,b) = 1

Se numeste cel mai mic multiplu comun al numerelor naturale a si b, numarul natural m, cmmmc(a,b), [a, b] a.i.:
1. a/m si b/m
2. daca a/n, b/n, atunci m/n

$a \cdot b = (a, b) \cdot [a, b]$

Algoritmul lui Euclid pentru gasirea celui mai mare divizor comun:
Oricare ar fi $a, b \in Z$ atunci exista si este unic d = (a, b) si exista $u, v \in Z$ a.i $(a, b) = a \cdot u + b \cdot v$

$$a = b \cdot q_1 + r_1$$
$$b = r_1 \cdot q_2 + r_2$$
$$\vdots$$
$$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}$$
$$r_{n-2} = r_{n-1} \cdot q_n$$

Atunci r_{n-1} este cmmmdc.

16 Grupuri si inele

Teorema lui Lagrange: Daca H este un subgrup al lui G, $m = |H|$, $n = |G|$, atunci m/n.

Fie $a \in G$: [a] = $\{a, a^2, a^3, ...\}$
Numarul m = min $\{k \in N^{\neq 0}, a^k = e\}$ se numeste ordinul lui a si se noteaza cu ord(a)
[a] = $\{a, a^2, a^3, ..., a^{m-1}, a^m = e\}$ se numeste subgrupul generat de a
Se numeste grup ciclic, un grup G in care exista un element g a.i. G = [g]
g se numeste generator al lui G

17 Generatori ai unui grup ciclic

$Z_n^* = U(Z_n) = \{a \in Z_n \ |(a, n) = 1\}$

Teorema: Z_p^* grup ciclic daca p este prim
Teorema: Z_n^* grup ciclic daca n = 2, 4, p^r, $2p^r$, cu p prim

Algoritmul de determinare al unui generator intr-un grup ciclic

1. Se alege un element oarecare din Z_n^* ciclic. Fie acesta g.

2. $\rho(n) = m$. Se calculeaza g^{di}, unde di sunt divizorii maximali ai lui m.

di = m/pi, unde m = $p_1^{\alpha_1)} \cdot p_2^{\alpha_2)} \cdot ... \cdot p_k^{\alpha_k)}$

3. Daca $g^{di} \neq 1$ (mod m), atunci g este un generator al lui Z_n^*

4. Se pot gasi alti generatori de forma g^k, unde (k, m) = 1

Problema logaritmilor discreti

Fie p un numar prim si g un generator al lui Z_p^*. Problema logaritmilor discreti in rezolvarea ecuatiei de forma $g^x = a, a \in Z_p^*$

$$x = log_g\, a$$

Metoda de rezolvare

1. Se descompune n in factori primi

2. Se calculeaza $m = \rho(n) = n(1-1/factor prim)(1-1/al doilea factor prim)...$

3. Se calculeaza d_i = m/fiecare factor prim al sau pe rand, fiecare generand un alt d_i, exemplu d_1, d_2

4. Se aleg pe rand valori pentru g si se verifica daca $g^{d_i} \neq 1$ (mod n). Daca g la toate puterile este diferit de 1 (mod n), atunci acea valoare de g este generator.
5. Se calculeaza $g^x = a$ pentru valoarea de a ceruta, sau pentru toate valorile, dupa caz. Acest lucru se face aplicand $x = log_g a$ si folosind proprietatile claselor de resturi si ale logaritmilor.