Algebra : 4

Principiel includere si excludere

An multime limite

1 V Ail + \$\begin{array}{c} A: 1-5 | A: 0 A | + \end{array}

Atance | VAil+ E | Ail- E | Ain Ayl+

+ E | Acar of OAx| + (-1)^n+ | A\_1 \cap A\_2 \cap A\_n|

- exception

Dem

professive n=1  $|A_1|=|A_1|$  everent n=2  $|A_1\cup A_2|=|A_1|+|A_2|-|A_1\cap A_2|$ 

An 1 Az = q an, , and An 1 Az for oylo An 1 Az = for oylo

-unductee dupa n

A. 2 42

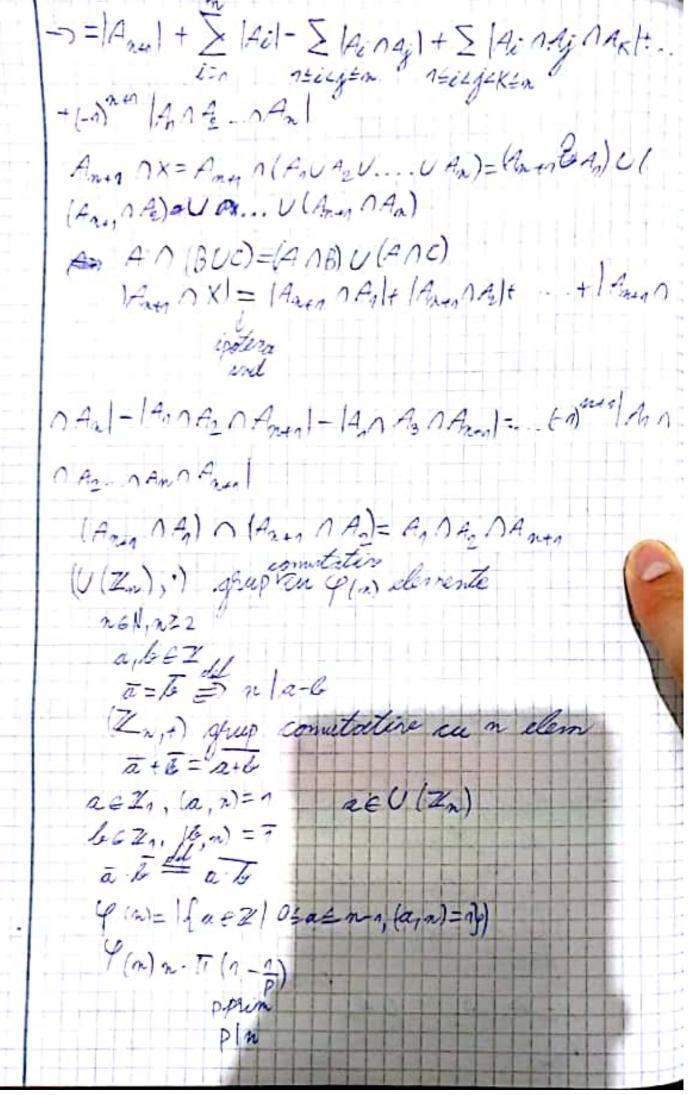
t+hez= |An U Az| |A|+|Az|-|An BAz|=(t+h)+(s+h)-+t+s+h) = # Exseh= |Ap Az| -DA Adere pt n dem st n=1

An Az, An mullime Simile

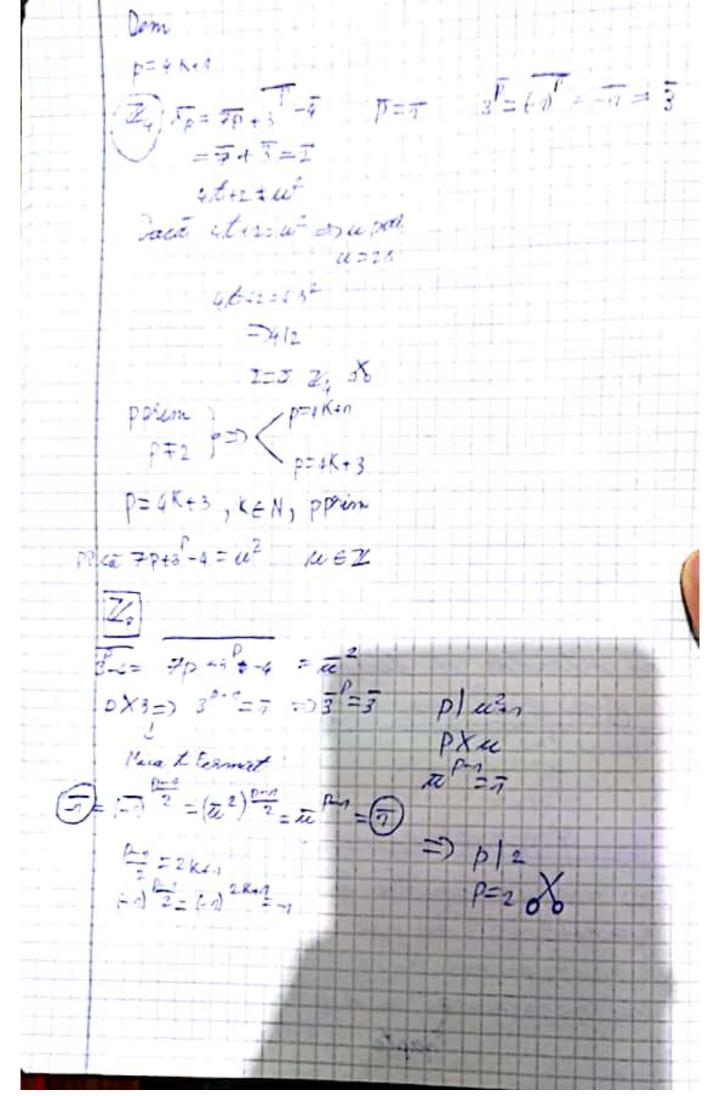
J=n 2 = |x U A ment = |x | + |Ament - |x O Ament= = 2

X= AnUA2 THUAN

de indudice et « caicula |x|



Pacpica. - Epi By Pen, a EN P(1)= (P, a-P, a-1)(P2 = Baz-7 Lorema lui Lagrange: (6, ) grap comutative finet 2 elem & rectre 161 =) 9=B GA Adic Lagrange pentra (6, )= (U(Zn), )
a = Z, (a, n)=1= ) , a U(Zn) = 7 Edema (Euler)  $a \in \mathbb{Z}$  |a, n| = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1n a 9/2)-1 Car particular al tessemei lui Eciler relim 2=1 Edmaz Pla)=P-P= P-1=2-1 Ex: pprim =) 7p+3 4 mu este patrat perfect 1/2=14+9-4=19 mu epp 13721727-4=44 mucpp 7=35+283-4=2764 mul pp sapte



Algoritmul Le dieptare RS+
(Revert, Shanner, Adleman)
4 CESAR
48 CD XYZ
ZARURILE AU FOST ARVNEATE
(2,0) -> publice
n=p-q Pin sime distancte mari
P. 2 secrete (P. 9) = (P-1)(2-1)
1EN (e, 9(m)) = 1
Alfabet" 26 Lnc26 K+2
26-lungimes alfaletuliu
STEAVA ECSB o secrenta de minholida
a transforma interuna de
- Hamourune
aj to m
P= an 26 + Mr 26 + 1 + 0, 26 + 20
metajul criptat este pe = a  Zn 0 = a = 1
a=B, 26 + + B, 26+B
EX
$n = 713$ $e = 89$ $26^2 = 676$
NU->13.26+20=358 263>713
15 26

