CH 2 : CONGRUENCES DANS Z

Objectif : un nouvel outil pour résoudre des problèmes de divisibilité

I. DÉFINITIONS

Dans ces définitions : n désigne un entier , n□2 ; a et b sont des entiers relatifs.

1. rappel cercle trigo

rappel cercle trigo Ÿ pls mesures : pi = 3 pi, -pi/2 = 3pi/2 .. Ÿ est-ce que 1492 = 2010 mod 6 ? Ÿ deux méthodes Ÿ deux définitions

def 1 **a et b sont congrus modulo n lorsqu'il existe k ∈ Z tel que a = b + k*n**

exemple : 28 = 22 mod3 ; 28 = -2 mod3

exercices : ex 42 ; simplifier n! modulo 30

2. traduction en termes de division euclidienne par n

def 2 **a et b ont même reste dans div par n** [sert à relier à mesure principale]

dem

* def 1 Ÿ def 2 soit la div eucl de a par n : a=nq+r

si def1:a = b + k*n alors b+kn =nq+r donc b = nq+r-kn = n(q-k) + r qui est l'écriture de la div eucl de b par n, dont le reste est bien r.

def2 Ÿ def 1:a=nq+r et b =nq'+r donc a = b+n(q-q') Ÿ def1 avec k=q-q'

3. traduction en termes de multiple de n

def3 **a-b multiple de n** [sert à relier à divisibilité]

dem : : a = b + k*n ssi a- b =kn

II. PROPRIÉTÉS

1. congruence est une relation d'équivalence

De par sa définition. la relation de congruence est une « relation d'équivalence », elle vérifie les propriétés suivantes , analogues a celle de l'égalité :

* réflexivité : a = a (mod n)
* symétrie : si a= b (mod n) alors b = a (mod n)
* transitivité : si a = b (mod n) et b =c (mod n) alors a =c (mod n). Cette dernière propriéte nous autorise a écrire des « congruences à la chaine ». telle que: l7 = 13 = 5 = -7 (mod 4).

2- congruences et opérations

Théoreme: a. b. c et d désignent des entiers relatifs et n un entier naturel n□2.

*** somme : Si a = b (mod n) et c = d (mod n). alors: a+c=b+d (modn)**
*** produit: Si a = b (mod n) et c = d (mod n).alors ac = bd (modn)**
*** puissance : Si a = b (mod n) alors pour tout entier naturel k: $a^k = b^k$ (mod n).**

Démonstrations:

a = b (mod n) et c = d (mod n) signifient quõil existe des entiers relatifs k et k' tels que a = b +k.n et c = d + kôn.

* En additionnant membre à membre. on obtient:

a+c = b+d +(k+k')*n

CQFD
* En multipliant membre à membre. on obtient:
ac = (b+kn)(d +k'n) = bd+(kd+k'c+kk'n)*n
CQFD
* On atteint la puissance k de proche en proche en appliquant la prop ci-dessus.

On peut résumer ces propriétés par la phrase suivante: la relation de congruence est compatible avec l'addition et la multiplication dans Z.

Attention : Réciproques fausse:
* multiplication : **Si a = b (mod n) alors ac = bc (modn)** mais la récip est fausse **;** La division n'est pas compatible avec la relation de congruence. (on ne peut pas diviser membre à membre deux congruences)
* puissance : Si a = b (mod n) alors $a^k = b^k$ (mod n) mais la rcip est fausse : a =2 , b = 4, n =3 , k= 2: on a $a^k = b^k$ (4=16 mod3) mais a ≠ b (2 ≠4 mod3)

III. UTILISATION DES CONGRUENCES

1. démontrer une divisibilité

PROP1 N multiple de n ssi N=0 (mod n)
exercice :
** mq 6^2010-1 est div par 7*
** mq 1^2003+2^2003+3^2003+4^2003 est divisible par 5*

2. déterminer un reste par une div eucl

Prop2 : **si r=reste div a par n alors a=r(mod n)** ;
exemples : 28=1 mod 3 ; 28=??? mod 5 ; 28=??? mod 10 ; 10^91+1=??? mod 2
P2bis(récip) **si a=r(mod n) avec 0<r<n alors r=reste div a par b**

dem en exercice
exercices : reste div eucl de 32^45 par 7 ?

3. résoudre une équation

exercices :
** mq l'eq $x^2=3(mod7)$ n'a pas de solution ; mq si 7 divise a^2+b^2 alors 7 divise a et 7 divise b.*