27 Mai 2014

N = Ensemble des entiers naturels

Z = Ensemble des entiers relatifs

(Z, +, x) est un anneau commutatif et unitaire. On sous-entend parfois l’existence de l’addition et de la multiplication dans Z en écrivant que Z est un anneau.

N\* désigne l’ensemble des entiers non nuls.

1°) Définitions :

Soit a ε Z et n ε Z

A multiple de n lorsqu’il existe q εZ tel que a=nq

Lorsque a ε Z\* et n ε Z\* et a multiple de n, on dit que n divise a  n|a

Donc n|a a ε nZ

1.2) Divisibilité dans N\*≡≡

Voir relation d’ordre partiel. Il a y des nombres plus petits et des nombres plus grands.

1.3) Division Euclidienne

a = n\*q+r avec 0<= r <n

a, n, q, r sont appelé dividende, diviseurs (ou modulo), quotient et reste.

Congruence modulo

Gauss défini que la théorie des congruences rotation ≡ symbole de la congruence. Voir le théorème chinois.

Arithmétique modulaire = technologie des horloges.

2.1.1) Relation de congruence

A et b sont congrus quand ils ont le même reste dans la division euclidienne.

Donc, a ≡ b (mod n) ou a ≡ b (n)

Exemple : 34≡18≡2 (16) = 18 est congru a 2 modulo 16 OU 64≡0(16)

Si n est un diviseur de a, alors reste r = 0 (n)

Connaitre les critères de divisibilité par 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 16, 25.

* Un nombre est divisible par 2 si il est pair {0,2,4,6,8} exemples: 13 574 ; 279 836
* Un nombre est divisible par 3 si la somme des chiffres est divisible par 3. exemples: 741 (7+4+1 = 12) ; 8 433 (8+4+3+3 = 18)
* Un nombre est divisible par 4 lorsque les deux chiffres de droite forment un nombre multiple de 4: {00, 04, 08, 12,............80, 84, 88, 92, 96}. exemples: 148 ; 57 376
* Un nombre est divisible par 5 lorsque le chiffre des unités est: 0 ou 5. exemples: 3 570 ; 14 235
* Un nombre est divisible par 6 : divisible par 2 et par 3 Donc ce nombre doit être pair et la somme des chiffres qui le composent doit être 3. Par exemple 4 506 est divisible par 6 puisqu’il est pair et la somme 4+5+0+6 = 15 un nombre divisible par 3.
* Un nombre est divisible par 7
* Un nombre est divisible par 8 lorsque les 3 chiffres de droite forment un nombre. Multiple de 8: 008, 016, 024,......072, 080, 088,.....520, 528,.....984, 992. exemples: 69 776(776=8x97) ; 98 024
* Un nombre est divisible par 9 lorsque la somme de ses chiffres est un nombre multiple de 9. exemple : 12 345 678 (1+2+3+4+5+6+7+8 = 36)
* Un nombre est divisible par 10 lorsque le chiffre des unités est: 0. exemples: 120 ; 13 000
* Un nombre est divisible par 11 lorsque la différence entre la somme des chiffres de rang pair et la somme des chiffres de rang impair est un multiple de 11. exemple : 919 380 (9+9+8 = 26 ; 1+3+0 = 4; 26 - 4 = 22 = 2x11)
* Un nombre est divisible par 16
* Un nombre est divisible par 25 lorsque les deux chiffres de droite sont : {00, 25, 50 ou 75}. exemples: 3 325 ; 723 775

Proposition 2 :

a ≡ b (n)  n | a -b  a – b ε n – Z

15 ≡ 33 ≡ 6 (9)

33 – 15 = 18 donc 9|18

Proposition 3 :

La congruence module n est une relation équivalente dans Z.

Proposition 4 :

Congruence compatible avec l’addition et la multiplication dans Z

Donc, si a ≡ b (n)

∀ signifie Pour tout ensemble de

1°) ∀ c ε Z, a + c ≡ b + c (n) et ac = bc (n)

pour tout ensemble appartenant à Z

2°) –a ≡ -b (n)

3°) ∀ k ε N, ak ≡ bk (n)

Exercice : Montré que :

A1°) ∀ k ε N, 10k ≡ 1(9). En déduire une règle sur les entiers de divisibilité par 9.

A2°) a) ∀ k ε N, 102k ≡ 1(11).et 102k+1 ≡ -1(11). En déduire une règle sur les entiers de divisibilité par 11.

B°) Calculer l’entier naturel x tel que O <= x <= 10 et 48139670543215 ≡ x(11)

A1°) 10 ≡ 1(9)

10k ≡ 1k(9)

≡ 1

abcd ≡ 1000\*a + 100\*b + 10\*c + d

≡ 103 a + 102 b + 10 c + 101 d

≡ 1 a + 1 b + 1 c + 1 d

≡ a+b+c+d

 Voir 2°) de la proposition 4.

A2°) 100 ≡ 1

102 ≡ 100 ≡ 1

104 ≡ 102 \* 102 ≡ 1\*1 ≡ 1

102k ≡ 1(11)

102 ≡ 100 ≡ -1(11)

103 ≡ 102 \* 101 ≡ 1\*10 ≡ -1

106 ≡ 102 \* 103 ≡ 1\*(-1) ≡ -1

102K-1 ≡ -1(11)

Règle de divisibilité par 11 :

abcdef = 105 a + 104 b + 103 c + 102 d + 101 e + 100 f

= -a + b + (-c) + d + (-e) + f

= (b+d+f) – (a+c+e) (11)

Voir 1°) de la proposition 4

143198

soit a = 8+1+4 = 13

soit b = 9 + 3 +1 = 13

a - b = 13-13 = 0  143198 est divisible par 11

si a ≡ b (n) alors ak ≡ bk (n)

4 813 …… ≡ 3 (11)

315 ≡ ? (11)

31 ≡ 3 (11)

32 ≡ 9 (11)

33 ≡ 27

34 ≡ 33 x 31 ≡ 5 x13 ≡ 15 ≡ 4 (11)

35 ≡ 34 x 31 ≡ 4 x 3 ≡ 12 ≡ 1 (11)

36 ≡

71 ≡ 07 (100)

72 ≡ 49 (100)

73 ≡ 43 (100)

74 ≡ 73 x 71 ≡ 01 (100)

74k ≡ 01

79 ≡ 07 ((79)9)9 ≡ 79 ≡ 07

(79)9 ≡ (7)9 ≡ 07

Définition d’un inverse = Deux nombres relatifs a et b sont inverses si leur produit est égal à 1 ;

a X b = 1

L'inverse du nombre relatif a non nul est http://www.mathematiquesfaciles.com/cgi-bin/mimetex.cgi?%5Cfrac%7B1%7D%7Ba%7D

Si a et b sont non nuls, l'inverse de la fraction http://www.mathematiquesfaciles.com/cgi-bin/mimetex.cgi?%5Cfrac%7Ba%7D%7Bb%7D est http://www.mathematiquesfaciles.com/cgi-bin/mimetex.cgi?%5Cfrac%7Bb%7D%7Ba%7D

Table de multiplication dans Z6

Exemple 3 x 5 = 15 diviser par 6, il reste 3

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| x | 0 | 1 | 2 | 3 | 4 | 5 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | **0** | 2 | 4 |
| 3 | 0 | 3 | **0** | 3 | **0** | 3 |
| 4 | 0 | 4 | 2 | **0** | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

Z6\* = {1,5}

Table de multiplication dans Z7

Exemple 4 x 6 = 24 diviser par 7, il reste 3

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| x | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | **1** | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | **1** | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | **1** | 4 |
| 4 | 4 | **1** | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | **1** | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | **1** |

Z7\* = {1,2,3,4,5,6}

Table de multiplication dans Z9

Exemple 4 x 6 = 24 diviser par 9, il reste 6

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 | **1** | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 2 | 4 | 6 | 8 | **1** | 3 | 5 | 7 |
| 3 | 3 | 6 | **0** | 3 | 6 | **0** | 3 | 6 |
| 4 | 4 | 8 | 3 | 7 | 2 | 6 | **1** | 5 |
| 5 | 5 | **1** | 6 | 2 | 7 | 3 | 8 | 4 |
| 6 | 6 | 3 | **0** | 6 | 3 | **0** | 6 | 3 |
| 7 | 7 | 5 | 3 | **1** | 8 | 6 | 4 | 2 |
| 8 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | **1** |

Z9\* = {1,2,4,5,7,8}

Zn  si n est premier pas de problème, tous les éléments sont inversible et univers inversible

Zn  si n n’est pas premier, on décompose en facteur premier et on élimine tous les multiples des facteurs premiers

Table de multiplication dans Z10

Exemple

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1 |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |

Z10\* = {1,3,7,9}

247349 dans Z7

247349 ≡  . (7)

247 ≡ 2 (7)

247349 ≡  2349 (7)

Calculatrice :

Factor (1517) = 37 x 41

Factor (2309) = 2309 donc premier

2 nombre sont premier entre eux sur leur pgcd = 0

Bachet bezout :

1. Algorithme d’Euclide pgcd
2. Algorithme d’Euclide étendu
3. Ensuite méthode

1800 ^1296 = 72

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1800 | 1296 | 504 | 288 | 216 | 72 |
| 1296 | 504 | 288 | 216 | **72** | 0 |

1800/1296 (1800= 1 x 1296 + 504)

504 = 1800 – 1 x 1296

1296/504 288 = 1296 – 2 x 504

504/288 216 = 504 – 1 x 288

288/216 72 = 288 – 1 x 216

1800 u + 1296 v = 72

a u + b v = a ^ b

72 = 288 – 1 x 216

= 288 – 1 x (504 – 1 x 288)

= 288 – 1 x 504 + 1 x 288

= 2 x 288 – 1 x 504

= 2 x (1296 – 2 x 504) – 1 x 504

= 2 x 1296 – 4 x 504 – 1 x 504

= 2 x 1296 – 5 x 504

= 2 x 1296 – 5 x (1800- 1 x 1296)

= 2 x 1296 – 5 x 1800 + 5 x 1296

= 7 x 1296 – 5 x 1800

72 = 1800 x (-5) + 1296 x (7)

72 =1800 u + 1296 v

u représente -5 et v représente 7

1 = 25 x (-5) + 18 x (7)

25 x (-5) + 18 x 7 = 1

Je me place dans Z25 :

0 + 18 x 7 ≡ 1 (25)

L’inverse de 18 est 7 (225)

Je me place dans Z18 :

25 x -5 ≡ 1

7 x (-5) = 1

-5 + 18 = 13  7 x 13 ≡ 1

Z4 = {1,2,3}

Z4\* = {1,3}

Z6 = {1,2,3,4,5}

Z6\* = {1,5}

Z12 12 : 1

2

3

4

6

12

12= ᵠ(1) + ᵠ(2) + ᵠ(3) + ᵠ (4) + ᵠ (6) + ᵠ (12)

**ᵠ(n) = n π (1 – 1/pi)**

ᵠ(12) = 12 x (1 – ½)(1 – 1/3)

ᵠ(12) = 12 x ½ x 2/3

= 4

ᵠ(26) = 26 x (1 – ½)(1 – 1/13)

= 26 x ½ x 12/13

= 2 x 6

= 12

2112 ≡ 1 (26)

Tous les nombre premier à 26 boucles à 1 puissance 12.

247349 ≡  (7)

2349 ≡  ? (7)

aᵠ(n) ≡  1 (n)

aᵠ(7) ≡  1 (7)

26 ≡  1 (7)

Dans un univers premier, la puissance de boucle est simplement celle de l’univers – 1.

Exemple Dans un univers Z23 il sera bouclé par 22.