Arithmétique des congruences

$\mathbb{Z}/n\mathbb{Z}$

Exemple :
$\mathbb{Z}/6\mathbb{Z}$

-6	-5	-4	-3	-2	-1
0	1	2	3	4	5
6	7	8	9	10	11
12	13	14	15	16	17
18	19	20	21	22	23
24	25	...			

$\mathbb{Z}/6\mathbb{Z}=\{0,1,2,3,4,5 \mathrm{mod}(6)\}$

Attention : dans $\mathbb{Z}/6\mathbb{Z}$ le nombre 1 représente tous les entiers de sa colonne:-11, -5, 1, 7, 13, 19, 25,...

On écrira $13 \equiv 1(6)$ ou $21 \equiv 15 \equiv 3(6)$, ...

ℂongruence :

- **Définition** : 2 nombres entiers **a** et **b** sont *congrus modulo n* (avec n un entier >1) ssi ils ont le même reste dans la division euclidienne par n.

  on note **a≡b(n)**

conséquence : a-b est multiple de **n**

donc **a-b=𝕜n** ou **a=b+𝕜n** avec 𝕜 un entier relatif

- **𝔼xemples :**

28≡0(7) ; 131≡14(13) ; 131≡-12(13)

Définition de $\mathbb{Z}/n\mathbb{Z}$

- Soit **n** un entier **>1** . On regroupe dans une même classe tous les entiers ayant le même reste dans la division euclidienne par **n**.
- Il y a donc **n-1** classes.
- On note **a mod(n)** les entiers de la forme **a+kn** avec **k** un entier relatif.
- **$\mathbb{Z}/n\mathbb{Z}$={0,1,2,...,n-1 mod(n)}**
- **Ex : $\mathbb{Z}/2\mathbb{Z}$={0,1 mod(2)}**

  (1 et 3 sont deux représentants de la même classse de $\mathbb{Z}/2\mathbb{Z}$ car **$1\equiv 3(2)$)**

$\mathbb{Z}/6\mathbb{Z}$: addition et multiplication

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

L'opposé de 2(6) est 4(6) donc -2≡4(6)

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

Eléments **inversibles** pour la multiplication dans $\mathbb{Z}/6\mathbb{Z}$:

$(\mathbb{Z}/6\mathbb{Z})^* = \{1,5 \bmod(6)\}$

Calculs dans $\mathbb{Z}/n\mathbb{Z}$

- Pour effectuer a+b ou a$\times$b dans $\mathbb{Z}/n\mathbb{Z}$ on peut prendre des représentants quelconques de a ou de b.

dans $\mathbb{Z}/6\mathbb{Z}$:

3+5$\equiv$ 8$\equiv$ 2(6) ou 15+17$\equiv$ 32$\equiv$ 2(6)

7$\times$5$\equiv$ 35$\equiv$ 5(6) ou 7$\times$5$\equiv$ 1x5$\equiv$ 5(6)

ou 7$\times$5$\equiv$ 7$\times$(-1)$\equiv$ -7$\equiv$5(6)

Calculs dans $\mathbb{Z}/n\mathbb{Z}$

- Dans $\mathbb{Z}/n\mathbb{Z}$ le résultat de a^p ne dépend pas du choix du représentant de a .

$7^{1234} \equiv 1^{1234} \equiv 1(6)$

- Attention avec la division :

$2a \equiv 2(6)$ n'équivaut pas à $a \equiv 1(6)$

car 2 n'est pas inversible dans $\mathbb{Z}/6\mathbb{Z}$ $(2 \times 3 \equiv 0(6))$

$5a \equiv 2(6)$ équivaut à $a \equiv 10 \equiv 4(6)$ (car l'inverse de 5 est 5 lui-même dans $\mathbb{Z}/6\mathbb{Z}$)

Calculs dans $\mathbb{Z}/n\mathbb{Z}$

- **Propriété :**

  un nombre entier **a** de $\mathbb{Z}/n\mathbb{Z}$ admet un inverse $\mathbf{a^{-1}}$ (tel que $\mathbf{a \times a^{-1} \equiv 1 (n)}$) **ssi a** et **n** sont premiers entre eux (leur seul diviseur commun est 1)

- On note $\mathbf{a \wedge n = 1}$ si **a** et **n** sont premiers entre eux
- Plus généralement $\mathbf{a \wedge b}$ représente le **pgcd** de **a** et **b** (le plus grand commun diviseur)

Algorithme d'Euclide

- **Propriété** : a et b deux entiers,

  $\mathbf{a \wedge b = b \wedge r}$ ou **r** est le reste de la division euclidienne de **a** par **b**

Algorithme Euclide(a,b)

si b==0 retourner a

sinon retourner Euclide(b,r)

- **En Python : r=a %b**
- **Euclide (27,33)=Euclide(33,27)=Euclide(27,6)**

  =Euclide(6,3)=Euclide(3,0)=3 donc $27 \wedge 33 = 3$

Euclide-Etendu

- **Identité de Bézout** :

  Pour tout couple d'entiers (a,b) il existe un couple d'entiers (u,v) tel que :

  $au+bv=a\wedge b$

- **Application :**

  si $a\wedge b=1$ alors u est l'inverse de a dans $\mathbb{Z}/b\mathbb{Z}$

- L'algorithme Euclide-Etendu(a,b) renvoie $a\wedge b$, u et v.

Euclide-Etendu(a,b)

si b==0 retourner (a,1,0)

sinon (d',u',v')=Euclide-Etendu(b,r)

(d,u,v)=(d',v',u'-qv') / q est le quotient de a par b

retourner (d,u,v)

entrées			sorties		
a	b	q	d	u	v
47	25	1	1	8	-15
25	22	1	1	-7	8
22	3	7	1	1	-7
3	1	3	1	0	1
1	0	X	1	1	0

Exponentiation-modulaire(a,b,n)

/ cet algo calcule « rapidement » $a^b \bmod(n)$

$d \leftarrow 1$

/$b_{\beta-1}\ b_{\beta-2}\ \ldots\ldots b_1 b_0$ est l'écriture en base 2 de b

Pour i=β-1 **jusqu'à** 0 **en décrémentant de** -1 :

$d \leftarrow d \times d \bmod(n)$

si b_i==1 **faire** :

$d \leftarrow d \times a \bmod(n)$

fin Si

Fin Pour

Retourner d

Exponentiation-modulaire

- Trace de l'algo pour $7^{28} \bmod (11)$:

i	4	3	2	1	0
bi	1	1	1	0	0
d	7	2	6	3	9

Donc $7^{28} = 9 \bmod (11)$

Fonction d'Euler

- **φ(n)** est le nombre d'éléments inversibles de $\mathbb{Z}/\mathrm{n}\mathbb{Z}$.

- C'est aussi le nombre d'entiers positifs inférieurs à **n** et premiers avec **n**.
- Si p est premier on a donc **φ(p) = p-1**
- On admettra que si **p** et **q** sont premiers on a **φ(p×q)=(p-1)(q-1)**

Théorème d’Euler

- Pour tous les entiers $\mathbf{n \geq 1}$ et a tels que $\mathbf{a \wedge n = 1}$

$$\mathbf{a^{\varphi(n)} \equiv 1 \bmod (n)}$$

Période de x dans $(\mathbb{Z}/n\mathbb{Z})^*$

$(\mathbb{Z}/n\mathbb{Z})^*$ est l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

(il y en a $\varphi(n)$)

$\mathbb{P}$our $x \in (\mathbb{Z}/n\mathbb{Z})^*$ on pose:

$$<x> = \{x^i(n),\ i \in \mathbb{N}\}$$

$\mathbb{L}$a période de x dans $(\mathbb{Z}/n\mathbb{Z})^*$ est notée $\omega(x)$ elle est égale au cardinal de <x> et vérifie

$$x^{\omega(x)} \equiv 1(n)$$

$\omega(x)$ est un diviseur de $\varphi(n)$