Arithmétique sur l'anneau $\mathbb{Z}/n\mathbb{Z}$.

On rappelle que $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence de la congruence modulo n (a est en relation avec b s'ils ont le même reste dans la division euclidienne par n ou a≡b mod(n)). Les classes d'équivalence sont $\mathbb{Z}/n\mathbb{Z}=\{\ \bar{0}\ ,\ \bar{1}\ ,\ \ldots,\overline{n-1}\ \}$.

Définition des opérations sur $\mathbb{Z}/n\mathbb{Z}$: $\bar{a}+\bar{b}=\overline{a+b}$ **et** $\bar{a}\bar{b}=\overline{ab}$

Groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Ce groupe est noté $(\mathbb{Z}/n\mathbb{Z})^\times$

- **$\bar{a}$ n'est inversible que si a et n sont premiers entre eux.**
- **$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.**
- **Les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ sont les générateurs du groupe additif $(\mathbb{Z}/n\mathbb{Z},+)$**

Anneau produit $\mathbb{Z}/m\mathbb{Z}$ X $\mathbb{Z}/n\mathbb{Z}$

$\mathbb{Z}/m\mathbb{Z}$ X$\mathbb{Z}/n\mathbb{Z}$ est un anneau.

- **Chinois et résultats dérivés:**

Si m et n premiers entre eux, a∈$\mathbb{Z}$, f(a)= ($\bar{a}$ dans $\mathbb{Z}/m\mathbb{Z}$, $\bar{a}$ dans $\mathbb{Z}/n\mathbb{Z}$) est un homomorphisme surjectif de noyau mn$\mathbb{Z}$ puisque f(mnp) = ($\bar{0}$,$\bar{0}$).

Par exemple dans $\mathbb{Z}/3\mathbb{Z}$ X $\mathbb{Z}/5\mathbb{Z}$, f(0)=($\bar{0},\bar{0}$), f(1)=($\bar{1},\bar{1}$), f(3)=($\bar{0},\bar{3}$), f(4)=($\bar{1},\bar{4}$), f(5)=($\bar{2},\bar{0}$), f(6)=($\bar{0},\bar{1}$), etc…

- **Surjectif implique tout ($\bar{a},\bar{b}$) ∈ $\mathbb{Z}/m\mathbb{Z}$ X$\mathbb{Z}/n\mathbb{Z}$, il existe c∈$\mathbb{Z}$ tel que c ≡ a mod(m) et c ≡ b mod(n)**
- **Si $\bar{x}$ ∈ $\mathbb{Z}/mn\mathbb{Z}$ g($\bar{x}$) = ($\bar{x}$ dans $\mathbb{Z}/m\mathbb{Z}$, $\bar{x}$ dans $\mathbb{Z}/n\mathbb{Z}$) est un isomorphisme.**
- **Dans le cas où m et n non premiers entre eux** de PPCM p et de PGCD d le théorème chinois reste valable mais l'homomorphisme a pour noyau p$\mathbb{Z}$.

Un élément de l'ensemble image (a+m$\mathbb{Z}$,a+n$\mathbb{Z}$)= (x,y) est tel que x – y est divisible par d=PGCD(m,n)

- **Si m divise n** et a inversible dans $\mathbb{Z}/n\mathbb{Z}$ si f($\bar{a}$)= $\bar{a}$ dans $\mathbb{Z}/m\mathbb{Z}$. f est une surjection de $(\mathbb{Z}/n\mathbb{Z})^\times$ sur $(\mathbb{Z}/m\mathbb{Z})^\times$.

Exemple m=10, n=60 , trouver un antécédent de 9+10$\mathbb{Z}$.
9 inversible dans $\mathbb{Z}/10\mathbb{Z}$ mais pas dans $\mathbb{Z}/60\mathbb{Z}$. 19 inversible dans $\mathbb{Z}/60\mathbb{Z}$ et $\overline{19}$ = 9 dans $\mathbb{Z}/10\mathbb{Z}$

Fonction indicatrice d'Euler

- **φ(n) = nombre d'entiers entre 1(inclus) et n qui sont premiers avec n**

1,3,5,7 sont les seuls entiers premiers avec 8 et inférieurs à 8 donc φ(8)=4

- **Si m et n premiers entre eux φ(mn)=φ(m)φ(n)**

φ(8)=4 , φ(5)=4 , φ(40)=16

- **Pour tout nombre premier p et r > 1 $\varphi(p^r) = p^r - p^{r-1} = p^r\left(1-\frac{1}{p}\right)$**

Parmi les entiers ≤ p^r, il y en a p^{r-1} qui sont divisibles par p (démonstration par récurrence). Les autres sont premiers avec p^r

- **Si D est l'ensemble des diviseurs de n ∈ $\mathbb{N}$ $n=\sum_{d\in D}\varphi(d)$**

15 = φ(3)+ φ(5)+ φ(15) = 3 + 4 + 8

- **Si P est l'ensemble des diviseurs premiers de n $\varphi(n)= n\prod_{p\in P}\left(1-\frac{1}{p}\right)$**

Déduit de la décomposition en facteurs premiers de n= $p_1^r.p_2^sp_3^t$ … où les pi sont premiers et de $pi^r=pi^r(1-\frac{1}{pi})$

- **Pour tout entier n ≥ 3 le nombre φ(n) est pair.**

Si n est pair ≥ 4. $\varphi(n)=\frac{n}{2\prod p}\prod(p-1)$ où les p sont tous premiers et impairs $\frac{n}{2\prod p}$ est un entier et $\prod(p-1)$ produit de pairs est pair.

Si n est impair $\varphi(n)=\frac{n}{\prod p}\prod(p-1)$ où tous les p sont impairs et les p–1 pairs $\frac{n}{\prod p}$ est un entier et donc φ(p) est pair

- **Si m divise n alors φ(m) divise φ(n)**

Si les p sont les diviseurs premiers de n qui ne divisent pas m, φ(n)/φ(m)= $\frac{n/m}{\prod p}\prod(p-1)$. La fraction est un entier $\frac{\varphi(n)}{\varphi(m)}$ aussi.

- **L'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$ est k= φ(n) .**

Le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ est le nombre d'entiers <n premiers avec n =φ $(\mathbb{Z}/6\mathbb{Z})^\times=\{\bar{1},\bar{5}\}$ et φ(6) = 2

- **Si p est premier l'ordre de $(\mathbb{Z}/p\mathbb{Z})^\times$ est p-1 et comme seul le $\bar{0}$ n'est pas inversible l'ordre de $\mathbb{Z}/p\mathbb{Z}$ = p**
- **Euler: Si a premier avec n et k = φ(n) alors $a^k \equiv 1$ mod (n)**

Dans $\mathbb{Z}/6\mathbb{Z}$, k=φ(6)=2 , 5 premier avec 6 , $5^2 \equiv 1$ mod(6)

- **Fermat: Si p premier et a non divisible par p alors $a^{p-1} \equiv 1$ mod(p) et donc $a^p \equiv a$ mod(p)**

Si p premier tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ sauf le 0 sont inversibles. Donc générateurs de $\mathbb{Z}/p\mathbb{Z}$ -{$\bar{0}$} d'où le résultat.