MAT2053 2A
Mathématiques et cryptographie

Construction de l'ensemble $\mathbf{Z}/n\mathbf{Z}$

Construction de $\mathbf{Z}/n\mathbf{Z}$

Soit $n \in \mathbf{N}^*$, Pour $(a,b) \in \mathbf{Z}^2$, on note $a \equiv b\,[n] \Leftrightarrow n \,|\, (b-a) \Leftrightarrow \exists k \in \mathbf{Z}, b-a = k\,n$
On sait que la relation binaire définie ci-dessus, appelée relation de congruence modulo n est une relation d'équivalence sur $\mathbf{Z}$, définissons la classe d'équivalence un élément $x \in \mathbf{Z}$

Classe d'équivalence modulo n

Pour $x \in \mathbf{Z}$, on note $cl(x) = \{y \in \mathbf{Z} / x \equiv y\,[n]\}$: appelé la classe de x modulo n
$cl(x)$ est noté aussi $\overline{x} = \{x + k\,n / k \in \mathbf{Z}\}$

Propriétés

Soient $n \in \mathbf{N}^*$ et $x \in \mathbf{Z}$ si $\overline{x}$ désigne la classe de x modulo n on a :
1) $x \in \overline{x}$
2) Si $y \in \mathbf{Z}$, $\overline{x} = \overline{y} \Leftrightarrow y \in \overline{x} \Leftrightarrow x \in \overline{y} \Leftrightarrow x \equiv y\,[n] \Leftrightarrow n \,|\, (y-x)$
3) Si r est le reste dans la division euclidienne de x par n alors $x \equiv r\,[n]$ c'est-à-dire $\overline{x} = \overline{r}$

Définition

$\mathbf{Z}/n\mathbf{Z} = \{\overline{x} / x \in \mathbf{Z}\}$
D'où d'après la division euclidienne et la propriété précédente on a :
$\mathbf{Z}/n\mathbf{Z} = \{\overline{r} / r \in \mathbf{N}, 0 \le r \le n-1\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

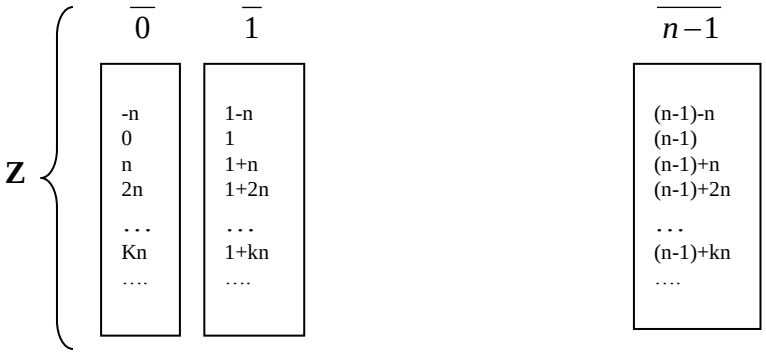
Exemples et remarques

1) Dans $\mathbf{Z}/2\mathbf{Z}$, $\overline{3} = \overline{1}$ car $3 \equiv 1\,[2]$ mais dans $\mathbf{Z}/4\mathbf{Z}$, $\overline{3} \neq \overline{1}$, car 4 ne divise pas $(3-1)$

2) La classe d'équivalence dépend du choix de n

Dans $\mathbf{Z}/2\mathbf{Z}$, $\overline{0} = \{y \in \mathbf{Z} / 0 \equiv y\,[2]\} = \{2k / k \in \mathbf{Z}\}$
mais
Dans $\mathbf{Z}/4\mathbf{Z}$, $\overline{0} = \{y \in \mathbf{Z} / 0 \equiv y\,[4]\} = \{4k / k \in \mathbf{Z}\}$
C'est à dire la classe de 0 dans $\mathbf{Z}/2\mathbf{Z}$ est différente de la classe de 0 dans $\mathbf{Z}/4\mathbf{Z}$
En général, si $(n,m) \in \mathbf{N}^* \times \mathbf{N}^*$ et $n \neq m$ alors la classe de 0 dans $\mathbf{Z}/n\mathbf{Z}$ est différente de la classe de 0 dans $\mathbf{Z}/m\mathbf{Z}$

3) Soit $(n,m)\in \mathbf{N}^*\times\mathbf{N}^*$ si $n\neq m$ alors $(\mathbf{Z}/n\mathbf{Z})\not\subset(\mathbf{Z}/m\mathbf{Z})$ (cf. la propriété précédente)
En particulier $(\mathbf{Z}/2\mathbf{Z})\not\subset(\mathbf{Z}/4\mathbf{Z})$ même si $\mathbf{Z}/2\mathbf{Z}=\{\overline{0},\overline{1}\}$ et $\mathbf{Z}/4\mathbf{Z}=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$
4) $\mathbf{Z}/n\mathbf{Z}=\{\overline{0},\overline{1},\ldots,\overline{n-1}\}$ est une partition de $\mathbf{Z}$:
$\mathbf{Z}=\overline{0}\cup\overline{1}\cup\ldots\cup\overline{n-1}$ et $\overline{a}\cap\overline{b}=\emptyset$ si $(a,b)\in\{0,1,\ldots,n-1\}^2$ et $a\neq b$



Propriétés
Soit $n\in\mathbf{N}^*$, dans $\mathbf{Z}/n\mathbf{Z}$ on a :

1) Pour tout $x\in\mathbf{Z}$ et pour tout $k\in\mathbf{Z}$, $\overline{x}=\overline{x+kn}$
En particulier : pour tout $k\in\mathbf{Z}$, $\overline{kn}=\overline{0}$

- **Opérations dans $\mathbf{Z}/n\mathbf{Z}$**

Pour $x\in\mathbf{Z}$ et $y\in\mathbf{Z}$ on a :
$\overline{x}=\{y\in\mathbf{Z}/x\equiv y[n]\}=\{x+kn/n\in\mathbf{Z}\}$ et $\overline{y}=\{y+kn/n\in\mathbf{Z}\}$
On pose $\overline{x}+\overline{y}=\{a+b/a\in\overline{x},b\in\overline{y}\}$ et $\overline{x}.\overline{y}=\{a.b/a\in\overline{x},b\in\overline{y}\}$
On montre facilement que $\overline{x}+\overline{y}=\{x+y+kn/k\in\mathbf{Z}\}$ et $\overline{x}.\overline{y}=\{x.y+kn/k\in\mathbf{Z}\}$
On définit alors l'addition et la multiplication dans $\mathbf{Z}/n\mathbf{Z}$ par :

$\overline{x}+\overline{y}=\overline{x+y}$ et $\overline{x}.\overline{y}=\overline{x.y}$

Propriétés
Soit $n\in\mathbf{N}^*$, dans $\mathbf{Z}/n\mathbf{Z}$ on a :
1) Pour tout $x\in\mathbf{Z}$ et pour tout $y\in\mathbf{Z}$, $x.\overline{y}=\overline{x.y}=\overline{x}\,y=\overline{x}.\overline{y}$
En particulier : $-\overline{x}=\overline{-x}$, $\overline{x}+\overline{x}=2\overline{x}=\overline{2x}$ et $\overline{x}-\overline{x}=\overline{x-x}=\overline{0}$
2) Pour tout $x\in\mathbf{Z}$ et pour tout $(k,m)\in\mathbf{N}^*\times\mathbf{N}^*$ $\left(\overline{x}\right)^k=\overline{x^k}$ et $\left(\overline{x}\right)^k.\left(\overline{x}\right)^m=\left(\overline{x}\right)^{(k+m)}=\overline{x^{k+m}}$

Exemples

1) Dans $\mathbf{Z}/8\mathbf{Z}$, $\overline{3}+\overline{7}=\overline{3+7}=\overline{10}=\overline{2}$, $\overline{3}.\overline{7}=\overline{3.7}=\overline{21}=\overline{5}$ et $3.\overline{7}=\overline{3.7}=\overline{21}=\overline{5}$

2) Dresser les tables de l'addition et de la multiplication de $\mathbf{Z}/n\mathbf{Z}$ pour $n\in\{2,3,4\}$

- **L'opposé d'un élément de $\mathbf{Z}/n\mathbf{Z}$**

Propriétés et défitinions

1) Pour tout $\bar{x} \in \mathbf{Z}/n\mathbf{Z}$ on a : $\bar{x}+\bar{0}=\bar{0}+\bar{x}=\bar{x}$ d'où $\bar{0}$ est l'élément neutre de $(\mathbf{Z}/n\mathbf{Z},+)$

2) Pour tout $\bar{x} \in \mathbf{Z}/n\mathbf{Z}$, il existe un unique $\bar{y} \in \mathbf{Z}/n\mathbf{Z}$ vérifiant $\bar{x}+\bar{y}=\bar{y}+\bar{x}=\bar{0}$

$\bar{y}$ s'appelle l'opposé de $\bar{x}$ dans $(\mathbf{Z}/n\mathbf{Z},+)$ et on a : $\bar{y}=-\bar{x}$

3) $(\mathbf{Z}/n\mathbf{Z},+)$ est un groupe abélien (à prouver)

Exemple

Dans $(\mathbf{Z}/20\mathbf{Z},+)$, l'opposé de $\overline{17}$ est $\bar{y}=-\overline{17}=\overline{-17}=\bar{3}$

- **L'inverse (s'il existe) d'un élément de $\mathbf{Z}/n\mathbf{Z}$**

Définition

Soit $\bar{x} \in \mathbf{Z}/n\mathbf{Z}$

On dit que $\bar{x}$ est inversible ou admet un inverse s'il existe $\bar{y} \in \mathbf{Z}/n\mathbf{Z}$ vérifiant $\bar{x}.\bar{y}=\bar{y}.\bar{x}=\bar{1}$

$\bar{y}$ s'appelle l'inverse de $\bar{x}$ dans $(\mathbf{Z}/n\mathbf{Z},.)$

Remarques

1) $(\mathbf{Z}/n\mathbf{Z},.)$ n'est pas un groupe

2) D'après la table de multiplication de $\mathbf{Z}/4\mathbf{Z}$, $\bar{2}$ n'est pas inversible mais $\bar{3}$ est inversible et son inverse est $\bar{3}$

Théorème (existence de l'inverse dans $\mathbf{Z}/n\mathbf{Z}$)

Soit $\bar{x} \in \mathbf{Z}/n\mathbf{Z}$

$\bar{x}$ admet un inverse dans $(\mathbf{Z}/n\mathbf{Z},.) \Leftrightarrow p\gcd(x,n)=1$

Preuve.

Utilise le théorème de Bezout : $p\gcd(x,n)=1 \Leftrightarrow \exists (u,v) \in \mathbf{Z}\times\mathbf{Z}, xu+nv=1$

- **Calcul de l'inverse (s'il existe) d'un élément de $\mathbf{Z}/n\mathbf{Z}$**

1ère méthode (Utilisation de l'Algorithme d'Euclide)

Soit $\bar{x}$ un élément inversible de $\mathbf{Z}/n\mathbf{Z}$ on a donc $p\gcd(x,n)=1$ et d'après l'Algorithme on calcul

$(u_0,v_0) \in \mathbf{Z}\times\mathbf{Z}$ tel que $xu_0+nv_0=1$ par suite dans $\mathbf{Z}/n\mathbf{Z}$ on a :

$\overline{xu_0+nv_0}=\bar{1}$ d'où $\bar{x}\,\bar{u_0}+\bar{n}\,\bar{v_0}=\bar{1} \Leftrightarrow \bar{x}\,\bar{u_0}=\bar{1}=\bar{u_0}\,\bar{x}$ car $\overline{nv_0}=\bar{0}$ dans $\mathbf{Z}/n\mathbf{Z}$ et la multiplication est commutative dans $\mathbf{Z}/n\mathbf{Z}$,

D'où l'inverse de $\bar{x}$ dans $\mathbf{Z}/n\mathbf{Z}$ est $\bar{u_0}$

Rappel (important)

si p est premier et $a \in \mathbf{Z}$. alors soit $p \text{gcd}(p,a)=1$ soit p divise a

Exemple

Prouver que $\bar{5}$ est inversible dans $\mathbf{Z}/23\mathbf{Z}$ puis calculer son inverse.

En effet $\bar{5}$ est inversible dans $\mathbf{Z}/23\mathbf{Z}$ car $p \text{gcd}(5,23)=1$ puisque 5 est premier et 5 ne divise pas 23 De plus

$23=5\times 4+3 \rightarrow 3=23-5\times 4$ (1)

$5=3\times 1+2 \rightarrow 2=5-3\times 1$ (2)

$3=2\times 1+1 \rightarrow 1=3-2\times 1$ (3)

Dans (3) on remplace le reste 2 par l'expression donnée par (2) d'où

$1=3-(5-3\times 1)\times 1=2\times 3-5$

puis on remplace le reste 3 par l'expression donnée par (1) donc

$1=2\times(23-5\times 4)-5=2\times 23-9\times 5$

D'où dans $\mathbf{Z}/23\mathbf{Z}$ on a : $\bar{1}=\overline{2\times 23}-\overline{9\times 5}=\overline{-9}\times\overline{5}$

Conclusion : l'inverse de $\bar{5}$ dans $(\mathbf{Z}/23\mathbf{Z},.)$ est $\overline{-9}=\overline{14}$

Autre méthode (plus simple) : on remarque que $\bar{5}\times\bar{9}=\overline{45}=\overline{-1}$ dans $\mathbf{Z}/23\mathbf{Z}$

D'où $\bar{5}\times(\overline{-9})=\bar{1}$ dans $\mathbf{Z}/23\mathbf{Z}$, par suite l'inverse de $\bar{5}$ dans $(\mathbf{Z}/23\mathbf{Z},.)$ est $\overline{-9}=\overline{14}$

2ème méthode (Calcul de puissance)

Soit $\bar{x}\in\mathbf{Z}/n\mathbf{Z}$, s'il existe $k\in\mathbf{N}, k\geq 2$ tel que $\left(\bar{x}\right)^k=\bar{1}$

alors $\bar{x}$ est inversible et son inverse dans $(\mathbf{Z}/n\mathbf{Z},.)$ est $\left(\bar{x}\right)^{(k-1)}$

Preuve

$\left(\bar{x}\right)^k=\bar{1}\Leftrightarrow\left(\bar{x}\right)^{(k-1)}.\bar{x}=\bar{1}\Leftrightarrow\bar{x}.\left(\bar{x}\right)^{(k-1)}=\bar{1}$ donc $\bar{x}$ est inversible est son inverse dans $(\mathbf{Z}/n\mathbf{Z},.)$ est $\left(\bar{x}\right)^{(k-1)}$ car $(k-1)\geq 1$

Exemple

Prouver que $\bar{3}$ est inversible dans $(\mathbf{Z}/14\mathbf{Z},.)$ puis calculer son inverse.

En effet, $p \text{gcd}(3,14)=1$ car 3 est premier et 3 ne divise 14 donc $\bar{3}$ est inversible dans $(\mathbf{Z}/14\mathbf{Z},.)$

De plus dans $\mathbf{Z}/14\mathbf{Z}$ on a : $\left(\bar{3}\right)^6=\bar{1}$ car $3^2\equiv -5[14]$ donc $3^3\equiv -15\equiv -1[14]$

par suite $3^6\equiv 1[14]$

Comme dans $\mathbf{Z}/14\mathbf{Z}$ on a $\left(\bar{3}\right)^6=\bar{1}$ d'où $\left(\bar{3}\right)^5$ est l'inverse de $\bar{3}$

Conclusion. L'inverse de $\bar{3}$ dans $(\mathbf{Z}/14\mathbf{Z},.)$ est $\bar{5}$ car $3^5\equiv 3^2.3^3\equiv(-5).(-1)\equiv 5[14]$