Ag7 : Congruences ; Z/nZ

I Congruences

I.1 Relations d'équivalence

a. Définition

Soit E un ensemble, $\mathscr{R}$ une relation binaire sur E. On dit que $\mathscr{R}$ est une **relation d'équivalence** sur E lorsqu'elle est

1. **réflexive** : $\forall x \in E \quad x \mathscr{R} x$
2. **symétrique** : $\forall (x,y) \in E^2 \quad \Big(x \mathscr{R} y\Big) \Longrightarrow \Big(y \mathscr{R} x\Big)$
3. **transitive** : $\forall (x,y,z) \in E^3 \quad \Big(x \mathscr{R} y \text{ et } y \mathscr{R} z\Big) \Longrightarrow \Big(x \mathscr{R} z\Big)$

La relation d'équivalence la plus simple est la relation =.

I.2 Relation de congruence modulo n

a. Définition

Soit n un entier naturel non nul. Soit a, b deux entiers. On dit que a est congru à b modulo n lorsque n divise $b-a$, et on note $a \equiv b\ [n]$ ou $a \equiv b \mod n$.

$$a \equiv b\ [n] \iff n | b-a$$

b. Premières propriétés

La relation de congruence modulo n est une relation d'équivalence sur **Z**.

I.3 Compatibilité avec les lois

a. Compatibilité avec +

On peut ajouter des congruences « de même module ».

Proposition Si $n \in \mathbf{N}_*$, si a, b, c sont trois entiers, alors

$$\left.\begin{array}{l} a \equiv b\ [n] \\ c \equiv d\ [n] \end{array}\right\} \Longrightarrow a + c \equiv b + d\ [n]$$

b. Compatibilité avec ×

On peut mutliplier des congruences « de même module ».

Proposition Si $n \in \mathbf{N}_*$, si a, b, c sont trois entiers, alors

$$\left.\begin{array}{l} a \equiv b\ [n] \\ c \equiv d\ [n] \end{array}\right\} \Longrightarrow ac \equiv bd\ [n]$$

En particulier, $a \equiv b\ [n] \implies ka \equiv kb\ [n]$ (k entier quelconque).

Corollaire $a \equiv b\ [n] \implies \forall k \in \mathbf{N}\ a^k \equiv b^k\ [n]$

I.4 Exemple d'application : les caractères de divisibilité

On écrit ici les entiers en base 10 : la notation $\overline{a_p a_{p-1} \dots a_0}$ désigne le nombre $a_0 + 10a_1 + \dots + 10^p a_p$, les a_k étant des entiers entre 0 et 9.

Proposition Le nombre $\overline{a_p a_{p-1} \dots a_0}$ est congru modulo 9 et modulo 3 à la somme de ses chiffres. En particulier, un nombre écrit en base 10 est divisible par 9 (ou par 3) si et seulement si la somme de ses chiffres l'est.

Proposition On peut énoncer une proposition similaire concernant la divisibilité par 11.

I.5 Le petit théorème de Fermat (« version congruences »)

Théorème Soit p un nombre premier, a un entier non multiple de p. Alors

$$a^{p-1} \equiv 1\ [p]$$

Lemme Si $(x, y) \in \mathbf{Z}^2$, si p est un nombre premier,

$$(x+y)^p \equiv x^p + y^p \ [p]$$

⚠En fait, c'est ici le lemme en lui-même qui est intéressant. Pour le petit théorème de Fermat, voir plus loin « la » bonne démonstration utilisant l'ordre d'un élément du groupe $\left(\left(\mathbf{Z}/p\mathbf{Z}\right)^*, \times\right)$.

II Z/nZ

II.1 Ensemble quotient

Définition Soit $\mathscr{R}$ une relation d'équivalence sur un ensemble X. Si $x \in X$, la classe d'équivalence de x pour la relation $\mathscr{R}$ est l'ensemble des éléments de X qui sont en relation avec x par $\mathscr{R}$. Si on note $\overline{x}$ cette classe,

$$y \in \overline{x} \iff y \mathscr{R} x$$

Si $y \in \overline{x}$, alors $\overline{y} = \overline{x}$; on dit que y est un représentant de $\overline{x}$.

Proposition Les classes d'équivalence pour la relation $\mathscr{R}$ forment une partition de X : elles sont non vides, deux à deux disjointes, et leur réunion est X.

Définition Soit $\mathscr{R}$ une relation d'équivalence sur un ensemble X. L'ensemble quotient de X par $\mathscr{R}$, noté parfois $X/\mathscr{R}$, est l'ensemble des classes d'équivalence dans X pour la relation $\mathscr{R}$.

II.2 L'ensemble $\mathbf{Z}/n\mathbf{Z}$

Définition Soit $n \geq 2$. $\mathbf{Z}/n\mathbf{Z}$ est l'ensemble quotient de $\mathbf{Z}$ par la relation de congruence modulo n.

Exemple Pour $n = 2$,

$$\mathbf{Z}/2\mathbf{Z} = \{I, P\} = \{\overline{0}, \overline{1}\}$$

Proposition (description) Soit $n \geq 2$. $\mathbf{Z}/n\mathbf{Z}$ est un ensemble à n éléments. De plus,

$$\mathbf{Z}/n\mathbf{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

Remarque La description donnée ci-dessus n'est pas la seule possible. Si on veut par exemple avoir la liste des carrés dans $\mathbf{Z}/7\mathbf{Z}$, on écrira plutôt

$$\mathbf{Z}/7\mathbf{Z} = \{\overline{-3}, \overline{-2}, \overline{-1}, \overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

II.3 Addition sur $\mathbf{Z}/n\mathbf{Z}$

Si on retient

$$\overline{a} + \overline{b} = \overline{a+b}$$

on aura une connaissance « opérationnelle » de l'addition. Mais pour savoir écrire des raisonnements corrects dans le cadre d'un ensemble quotient, il importe de comprendre pourquoi
« soit $\overline{a}, \overline{b} \in \mathbf{Z}/n\mathbf{Z}$. Définissons $\overline{a} + \overline{b} = \overline{a+b}$ »
est à la fois mal rédigé et mal justifié.

II.4 Multiplication sur $\mathbf{Z}/n\mathbf{Z}$

Table de multiplication de $\mathbf{Z}/5\mathbf{Z}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$					
$\overline{1}$					
$\overline{2}$					
$\overline{3}$					
$\overline{4}$					

Table de multiplication de $\mathbf{Z}/6\mathbf{Z}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$						
$\overline{1}$						
$\overline{2}$						
$\overline{3}$						
$\overline{4}$						
$\overline{5}$						

II.5 Structure d'anneau sur $\mathbf{Z}/n\mathbf{Z}$; morphisme « canonique »

Proposition Les deux opérations précédentes confèrent à $\mathbf{Z}/n\mathbf{Z}$ une structure d'anneau commutatif. L'application

$$k \longmapsto \overline{k}$$

est un morphisme surjectif de l'anneau $(\mathbf{Z}, +, \times)$ sur l'anneau $(\mathbf{Z}/n\mathbf{Z}, +, \times)$.

II.6 Eléments inversibles de $\mathbf{Z}/n\mathbf{Z}$; indicatrice d'Euler

Voyons voir, étant donné un entier x, si $\overline{x}$ est inversible dans $\mathbf{Z}/n\mathbf{Z}$. Pour l'instant, comme on n'est pas encore très instruit en calcul dans $\mathbf{Z}/n\mathbf{Z}$, on descend au niveau des congruences et divisibilités. Mais ce n'est pas en général une bonne tactique quand on commence à connaître un peu mieux cette structure.

$$\begin{aligned}
\overline{x} \in (\mathbf{Z}/n\mathbf{Z})^* &\iff \exists y \in \mathbf{Z} \quad \overline{x} \times \overline{y} = \overline{1} \\
&\iff \exists y \in \mathbf{Z} \quad xy \equiv 1\ [n] \\
&\iff \exists (y,k) \in \mathbf{Z}^2 \quad xy - 1 = nk
\end{aligned}$$

Théorème et définition Soit $n \geq 2$. Si x est un entier,

$$\overline{x} \in (\mathbf{Z}/n\mathbf{Z})^* \iff x \wedge n = 1$$

On définit, sur $\mathbf{N}^*$, l'indicatrice d'Euler ϕ par, si $n \geq 2$,

$$\phi(n) = \sharp\left((\mathbf{Z}/n\mathbf{Z})^*\right) = \sharp\left(\{x \in \{1, 2, \ldots, n\}\ ;\ x \wedge n = 1\}\right)$$

On définit aussi $\phi(1) = 1$.

Théorème d'Euler Soit $n \geq 2$; si $a \wedge n = 1$, alors $a^{\phi(n)} \equiv 1\ [n]$.

Dans le cas où n est premier, le théorème d'Euler se nomme…

II.7 Théorème

Les trois propriétés suivantes sont équivalentes :
(i) $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ est un corps
(ii) $(\mathbf{Z}/n\mathbf{Z}, +, \times)$ est un anneau intègre
(iii) n est premier
Notation : On note, si p est premier, $\mathrm{F}_p = \mathbf{Z}/p\mathbf{Z}$.

II.8 Un exercice

Démontrer que, si A est un ensemble fini, si $(A, +, \times)$ est un anneau commutatif, alors A est intègre si et seulement si A est un corps. On pourra s'intéresser, si $a \in A \setminus \{0_A\}$, à l'application

$$\begin{array}{rccc} f_a : & A & \longrightarrow & A \\ & x & \longmapsto & a \times x \end{array}$$

Technique intéressante : entre ensembles finis de même cardinal, la surjectivité et l'injectivité sont équivalentes. On sait que pour les applications linéaires entre espaces vectoriels de même dimension, c'est encore vrai. Et on peut utiliser la même technique dans les algèbres de dimension finie, par exemple pour montrer que l'inverse d'une matrice triangulaire supérieure inversible est une matrice triangulaire supérieure...

II.9 Calcul dans $\mathbf{Z}/n\mathbf{Z}$

a. $k\overline{a}$, $\overline{ka}$ et $\overline{k}\,\overline{a}$

On a, si $k \in \mathbf{N}^*$, par définition :

$$k\,\overline{a} = \underbrace{\overline{a} + \overline{a} + \cdots + \overline{a}}_{k \text{ fois}}$$

et donc

$$k\,\overline{a} = \underbrace{\overline{a + a + \cdots + a}}_{k \text{ fois}} = \overline{ka} = \overline{k}\,\overline{a}$$

En multipliant tout par $\overline{-1}$, on étend ce résultat à $k \in \mathbf{Z}$.

Pour insister : quand dans un énoncé, on parle de $4x$ où $x \in \mathbf{Z}/n\mathbf{Z}$, cela revient au même d'écrire $\overline{4}x$. C'est agréable…et embarrassant, car cela peut inciter à confondre les classes et les entiers, ce qui est parfois ennuyeux.

b. Classe d'un quotient

Soit p un nombre premier, a et b deux entiers. Même si b divise a, parler de $\overline{\left(\frac{a}{b}\right)}$ n'est pas très judicieux. Si b ne divise pas a, c'est interdit. Mais remarquons que, si $a = bq$, on a $\overline{a} = \overline{b}\overline{q}$. En supposant $\overline{b}$ inversible (si p est premier, cela équivaut tout simplement à supposer $\overline{b} \neq \overline{0}$), on obtient

$$\underbrace{\overline{\left(\frac{a}{b}\right)}}_{\text{déconseillé}} = \overline{q} = \left(\overline{b}\right)^{-1}\overline{a} = \overline{a}\left(\overline{b}\right)^{-1}$$

Par exemple, dans $\mathbf{Z}/29\mathbf{Z}$,

$$\underbrace{\overline{\left(\frac{22}{2}\right)}}_{\text{déconseillé}} = \overline{22}\left(\overline{2}\right)^{-1} = \overline{22} \times \overline{15}$$

Exercice : Vérifier de même, dans $\mathbf{Z}/17\mathbf{Z}$, que

$$\overline{15} \times (\overline{3})^{-1} = \overline{5}$$

c. Notations

Il vaut mieux éviter de dire « soit $\overline{a}$ un élément de $\mathbf{Z}/n\mathbf{Z}$ ». En effet, le statut de a dans cette phrase est un peu incertain. Il vaut beaucoup mieux dire, comme quand on considère n'importe quel ensemble : « soit x un élément de $\mathbf{Z}/n\mathbf{Z}$ ». Ensuite, on a le droit de vouloir un représentant, on dira alors « …et soit a un entier tel que $x = \overline{a}$ »

d. Problèmes de définition

Une des choses les plus délicates, lorsqu'on travaille dans $\mathbf{Z}/n\mathbf{Z}$, est de justifier une définition d'application du type

$$\overline{a} \longmapsto f(a)$$

Il faut commencer par montrer que, si $\overline{a} = \overline{b}$, $f(a) = f(b)$.

II.10 Un exemple d'utilisation de $\mathbf{Z}/p\mathbf{Z}$

1. Ecrire, sous forme de fraction réduite, $1+1/2$, puis $1+1/2+1/3+1/4$, puis$1+1/2+1/3+1/4+1/5+1/6$.

   Dans toute la suite, p désigne un nombre premier impair.

2. Montrer que l'application $x \mapsto x^{-1}$ est une bijection de $\left(\mathbf{Z}/p\mathbf{Z}\right)^*$ sur lui-même.

3. Montrer que $\displaystyle\sum_{x\in\left(\mathbf{Z}/p\mathbf{Z}\right)^*} x^{-1} = \overline{0}$.

4. (Posé à l'oral des Mines) On écrit $1+\dfrac{1}{2}+\cdots+\dfrac{1}{p-1}=\dfrac{a}{b}$. Montrer que p divise a (on pourra commencer par tout multiplier par $(p-1)!$).

5. On rappelle (petit théorème de Fermat) que les éléments de $\left(\mathbf{Z}/p\mathbf{Z}\right)*$ sont les racines dans $\mathbf{Z}/p\mathbf{Z}$ du polynôme $X^{p-1}-\overline{1}$. En déduire la valeur de $\displaystyle\sum_{k=1}^{p-1}\left(\prod_{\substack{j=1\\ j\neq k}}^{p-1}\overline{j}\right)$, puis retrouver le résultat de la question précédente.

III Annexe : équations du second degré

Le programme ne demande pas de savoir résoudre des équations du second degré sur $\mathbf{Z}/p\mathbf{Z}$*. C'est néanmoins un moyen agréable de se familiariser avec les calculs sur cet ensemble. Et on révise la mise sous forme canonique d'un polynôme de degré 2, c'est important.*

III.1 Une première équation

Résoudre, sur $\mathbf{Z}/11\mathbf{Z}$, l'équation

$$x^2 - \overline{6}\,x + \overline{5} = \overline{0}$$

III.2 Une deuxième équation

Résoudre, sur $\mathbf{Z}/31\mathbf{Z}$, l'équation

$$x^2 - \overline{11}\,x - \overline{1} = \overline{0}$$

III.3 Où se situe le problème

Si p est un nombre premier, si $y \in \left(\mathbf{Z}/p\mathbf{Z}\right)^*$, résoudre l'équation d'inconnue x :

$$x^2 = y^2$$

Calculer $|A|$ où

$$A = \{x^2\ ;\ x \in \left(\mathbf{Z}/p\mathbf{Z}\right)^*\}$$

III.4 Une troisième équation

Discuter, suivant les valeurs de $a \in \mathbf{Z}/13\mathbf{Z}$, le nombre de solutions de l'équation

$$x^2 + x + a = \overline{0}$$

III.5 Cas très particulier

Expliquer pourquoi le concept d'« équation du second degré » sur $\mathbf{Z}/2\mathbf{Z}$ n'est pas très intéressant.

III.6 Un exercice d'oral

Il peut être utile de regarder d'abord le théorème chinois, section suivante, pour la deuxième question de l'exercice
Résoudre, dans $\mathbf{Z} \times \mathbf{Z}$, le système $x + y \equiv 4[11]$ et $xy \equiv 10[11]$. Même question en remplaçant 11 par 341.

Parmi les multiples intérêts de cet énoncé, on retiendra ceci : une congruence peut s'exprimer à l'aide d'une divisibilité (on « descend ») ou à l'aide d'une égalité dans $\mathbf{Z}/n\mathbf{Z}$ (on « monte »). Les examinateurs cherchent plutôt à voir, en général, si le candidat sait prendre l'ascenseur vers le haut.

IV Produit fini d'anneaux ; théorème chinois

IV.1 Un système de congruences

Résoudre le système (à inconnue $x \in \mathbf{Z}$) :

$$\begin{cases} x \equiv 2 \quad [14] \\ x \equiv 3 \quad [25] \end{cases}$$

On pourra par exemple commencer par résoudre les systèmes

$$\begin{cases} x \equiv 1 \quad [14] \\ x \equiv 0 \quad [25] \end{cases}$$

et

$$\begin{cases} x \equiv 0 \quad [14] \\ x \equiv 1 \quad [25] \end{cases}$$

en utilisant une relation de Bezout entre 14 et 25.

Dire pourquoi le système (à inconnue $x \in \mathbf{Z}$) :

$$\begin{cases} x \equiv 2 \quad [26] \\ x \equiv 3 \quad [38] \end{cases}$$

n'a pas de solution.

IV.2 Structure d'anneau produit

On considère deux anneaux $(A, +, \times)$ et $(B, +, *)$ (la loi $+$ n'est pas la même sur A et sur B en général, mais elle n'est jamais notée autrement que $+$) ; les écritures

$$(a, b) + (a', b') = (a + a', b + b')$$

$$(a, b) \star (a', b') = (a \times a', b * b')$$

définissent deux lois internes $+$ (encore un autre $+\ldots$) et $\star$ sur $A \times B$. Et $(A \times B, +, \star)$ est un anneau, dit anneau produit de $(A, +, \times)$ et $(B, +, *)$.

On peut étendre cette définition à un nombre fini d'anneaux : si les $(A_i, +, *_i)$ $(1 \leq i \leq p)$ sont des anneaux, sur $A = A_1 \times A_2 \cdots \times A_p$ on définit une structure d'anneau, dite « anneau produit » des $(A_i, +, *_i)$ $(1 \leq i \leq p)$ par

$$(a_1, \ldots, a_p) + (a'_1, \ldots, a'_p) = (a_1 + a'_1, \ldots, a_p + a'_p)$$
$$(a_1, \ldots, a_p) * (a'_1, \ldots, a'_p) = (a_1 *_1 a'_1, \ldots, a_p *_p a'_p)$$

IV.3 Problème de notation

Lorsque, a étant entier, on note $\overline{a}$ la classe de a dans $\mathbf{Z}/n\mathbf{Z}$, la notation ne comporte aucune référence explicite à n. Quand on se situe toujours dans le même $\mathbf{Z}/n\mathbf{Z}$, ce n'est pas un problème. Mais si on travaille alternativement dans $\mathbf{Z}/n\mathbf{Z}$ et dans $\mathbf{Z}/m\mathbf{Z}$, c'est plus problématique. On notera donc $a \bmod m$ (lire « classe de a modulo m » ou plus brièvement« a modulo m ») la classe de a dans $\mathbf{Z}/m\mathbf{Z}$.
Par exemple, le système de la première question s'écrit

$$(x \bmod 14\ ,\ x \bmod 25) = (2 \bmod 14\ ,\ 3 \bmod 25)$$

Pour étudier l'existence d'une solution à ce système, il n'est pas absurde de s'intéresser à l'application

$$\phi\ :\ a \longmapsto (a \bmod 14\ ,\ a \bmod 25)$$

définie sur $\mathbf{Z}$, à valeurs dans $\mathbf{Z}/14\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z}$. Et on applique un schéma assez usuel, donc intéressant.
On remarque que ϕ est un morphisme d'anneaux. Et son noyau est assez facile à déterminer. C'est

Cela permet à la fois de définir

$$\begin{array}{rccc} \psi\ : & \mathbf{Z}/350\mathbf{Z} & \longrightarrow & \mathbf{Z}/14\mathbf{Z} \times \mathbf{Z}/25\mathbf{Z} \\ & a \bmod 350 & \longmapsto & (a \bmod 14, a \bmod 25) \end{array}$$

et d'avoir son injectivité. On obtient donc la surjectivité par un moyen détourné : une application injective d'un ensemble fini dans un ensemble fini de même cardinal est surjective.
On utilisera plus souvent, en algèbre linéaire, le résultat : une application linéaire injective d'un espace vectoriel de dimension finie dans un espace vectoriel de même dimension finie est surjective.

IV.4 Le théorème chinois

Théorème Si m et n sont deux entiers naturels ≥ 2 premiers entre eux, on peut définir

$$\begin{array}{rccc} \psi : & \mathbf{Z}/mn\mathbf{Z} & \longrightarrow & \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \\ & a \bmod mn & \longmapsto & (a \bmod m, a \bmod n) \end{array}$$

et ψ est un isomorphisme d'anneaux.

IV.5 Extension

Théorème Si $m_1, \ldots, m_p$ sont des entiers naturels ≥ 2 deux à deux premiers entre eux, si l'on note $M = m_1 \ldots m_p$ on peut définir

$$\begin{array}{rccc} \psi : & \mathbf{Z}/M\mathbf{Z} & \longrightarrow & \mathbf{Z}/m_1\mathbf{Z} \times \cdots \times \mathbf{Z}/m_p\mathbf{Z} \\ & a \bmod M & \longmapsto & (a \bmod m_1, \ldots, a \bmod m_p) \end{array}$$

et ψ est un isomorphisme d'anneaux.

IV.6 Corollaire : un calcul de $\phi(n)$

Lemme 1 Soit $u : A \to B$ un isomorphisme d'anneaux. Alors $u(A^*) = B^*$ (en plus clair : les éléments inversibles de B sont les images par u des éléments inversibles de A). D'ailleurs u induit un isomorphisme du groupe $(A^*, \times)$ sur le groupe $(B^*, \times)$.

Lemme 2 Les éléments inversibles de l'anneau produit $A \times B$ sont les éléments de $A^* \times B^*$.

Théorème Si $m \wedge n = 1$, alors $\phi(mn) = \phi(m)\,\phi(n)$.

Lemme 3 Si p est un nombre premier, si $\alpha \in \mathbf{N}^*$,

$$\phi(p^\alpha) =$$

Corollaire Si $n = \prod_{i=1}^{d} p_i^{\alpha_i}$ est la décomposition de n en facteur premiers (les p_i sont premiers, les α_i sont des naturels non nuls), alors

$$\phi(n) = n \prod_{i=1}^{d} \left(1 - \frac{1}{p_i}\right)$$

Exemple Calculer $\phi(36)$; vérifier.

Remarque Ce résultat peut se montrer à l'aide de probabilités !

IV.7 Utilisation du théorème chinois

Un essai : Essayons de résoudre l'équation du second degré :

$$x^2 - \overline{4}x - \overline{5} = \overline{0}$$

dans $\mathbf{Z}/253\mathbf{Z}$.

Un autre... Résoudre l'équation :

$$x^2 + \overline{3}x + \overline{4} = \overline{0}$$

dans $\mathbf{Z}/77\mathbf{Z}$.

Table des matières