

LEÇON N° 14 :

Congruences dans \mathbb{Z} . Anneau $\mathbb{Z}/n\mathbb{Z}$.

Pré-requis :

- Relation d'équivalence ;
- Définitions d'un groupe, d'un anneau, d'un corps ;
- Division euclidienne dans \mathbb{Z} , notation d'un cardinal ($|\cdot|$) ;
- Nombres premiers (et notation \wedge), PGCD, théorème de Bézout.

14.1 Congruences dans \mathbb{Z} ($n \in \mathbb{N}, n \geq 2$)

Définition 1 : Soit $(x, y) \in \mathbb{Z}^2$. On dit que x est congru à y modulo n si $x - y \in n\mathbb{Z}$. On note alors $x \equiv y [n]$.

Proposition 1 : La relation de congruence est une relation d'équivalence.

démonstration :

Réflexivité : $x - x = 0 \cdot n \in n\mathbb{Z}$, donc $x \equiv x [n]$.

Symétrie : On suppose que $x \equiv y [n]$, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $x - y = kn$. Alors $y - x = -k \cdot n \in n\mathbb{Z}$, donc $y \equiv x [n]$.

Transitivité : On suppose cette fois que $x \equiv y [n]$ et $y \equiv z [n]$, c'est-à-dire qu'il existe $k, k' \in \mathbb{Z}$ tels que $x - y = kn$ et $y - z = k'n$. Alors $x - z = (x - y) + (y - z) = kn + k'n = (k + k')n \in n\mathbb{Z}$, donc $x \equiv z [n]$.

Les trois points d'une relation d'équivalence sont vérifiées, donc celle de congruence en est une. ■

Proposition 2 : La relation de congruence est compatible avec l'addition et la multiplication de \mathbb{Z} , c'est-à-dire que

$$\begin{cases} x \equiv y [n] \\ x' \equiv y' [n] \end{cases} \Rightarrow \begin{cases} x + x' \equiv y + y' [n] \\ x \cdot x' \equiv y \cdot y' [n]. \end{cases}$$

démonstration : On a les implications suivantes :

$$\begin{aligned} \begin{cases} x = y + kn \\ x' = y' + k'n \end{cases} &\Leftrightarrow \begin{cases} x + x' = y + y' + \overbrace{(k + k')n}^{\in \mathbb{Z}} \\ x \cdot x' = y \cdot y' + \underbrace{(ky' + k'y + nkk')}_{\in \mathbb{Z}} n. \end{cases} \\ &\Leftrightarrow \begin{cases} x + x' \equiv y + y' [n] \\ x \cdot x' \equiv y \cdot y' [n], \end{cases} \end{aligned}$$

ce qui démontre le résultat. ■

Exercice : Soit $p \in \mathbb{N}$. Montrer que $x \equiv y [n]$ implique à la fois $px \equiv py [n]$ et $x^p \equiv y^p [n]$.

Solution : En effet, il existe $k \in \mathbb{Z}$ tel que $x - y = kn$. D'une part, on a ainsi que $p(x - y) = p(kn) \Leftrightarrow px - py = (pk)n \Leftrightarrow px \equiv py [n]$. Attention cependant à la réciproque, parce que la division par p ne garantit que le multiplicateur de n soit entier ! Il faut alors que p divise n pour satisfaire cette condition.

D'autre part, on procède par récurrence pour la seconde congruence. Pour $p = 1$, il n'y a aucun problème. Supposant le résultat vrai au rang $p - 1$, on applique la proposition 2 pour montrer qu'il l'est toujours au rang p , et ainsi achever la récurrence. \diamond

14.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}^*$)

Définition 2 : L'ensemble quotient de \mathbb{Z} sur la relation de congruence est noté $\mathbb{Z}/n\mathbb{Z}$. On note \bar{x} la classe d'équivalence de x dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire $\bar{x} = \{y \in \mathbb{Z} \mid y \equiv x [n]\}$.

Théorème 1 : Pour tout $x \in \mathbb{Z}$, il existe un unique $r \in \bar{x}$ tel que $0 \leq r < n$.

démonstration : On effectue la division euclidienne de x par n : il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $x = qn + r$ et $0 \leq r < n$, donc $r \in \bar{x} \Leftrightarrow r \equiv x [n] \Leftrightarrow r \in \bar{x}$ et $0 \leq r < n$. \blacksquare

Exercice : Montrer qu'en particulier, $x \equiv y [n]$ si et seulement si x et y ont même reste dans la division euclidienne par n .

Solution : Notons $x = qn + r$ et $y = q'n + r'$, avec $0 \leq r, r' < n$. On a alors les équivalences suivantes :

$$\begin{aligned} x \equiv y [n] &\Leftrightarrow x - y = kn \Leftrightarrow qn + r - q'n - r' = kn \Leftrightarrow r - r' = n(k - q + q') \\ &\Leftrightarrow r \equiv r' [n] \stackrel{0 \leq r, r' < n}{\Leftrightarrow} r = r', \end{aligned}$$

et le résultat est ainsi démontré. \diamond

Corollaire 1 : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, et $|\mathbb{Z}/n\mathbb{Z}| = n$.

démonstration : Par le théorème précédent, $r \in \bar{x}$ est unique. Donc, par transitivité, tous les éléments congrus à r modulo n le sont aussi à x modulo n , ce qui nous amène à écrire que $\bar{r} = \bar{x}$. Mais $\bar{r} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, d'où le résultat. \blacksquare

Proposition 3 : On définit une addition $+$ et une multiplication \cdot sur $\mathbb{Z}/n\mathbb{Z}$ de la manière suivante : pour tous $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$, il existe $a, b \in \mathbb{Z}$ tels que $\bar{a} = \alpha$ et $\bar{b} = \beta$, et l'on pose ainsi

$$\alpha + \beta = \bar{a} + \bar{b} = \overline{a + b} \quad \text{et} \quad \alpha \cdot \beta = \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

démonstration : Il faut vérifier que $+$ et \cdot sont bien définies sur $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{cases} \alpha = \bar{a} = \bar{a}' \\ \beta = \bar{b} = \bar{b}' \end{cases} \Rightarrow \begin{cases} a \equiv a' [n] \\ b \equiv b' [n] \end{cases} \xrightarrow{\text{prop 2}} \begin{cases} a + b \equiv a' + b' [n] \\ a \cdot b \equiv a' \cdot b' [n] \end{cases} \Rightarrow \begin{cases} \overline{a + b} = \overline{a' + b'} \\ \overline{a \cdot b} = \overline{a' \cdot b'} \end{cases}$$

donc cette définition est indépendante du choix des représentants, ce qui la rend pertinente. ■

Théorème 2 : $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

démonstration : Découle directement du fait que \mathbb{Z} soit un anneau commutatif. ■

14.3 Eléments inversibles

Théorème 3 : $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si $x \wedge n = 1$.

démonstration : On a les équivalences suivantes :

$$\begin{aligned} \bar{x} \text{ inversible dans } \mathbb{Z}/n\mathbb{Z} &\Leftrightarrow \exists \bar{y} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{x} \cdot \bar{y} = \bar{1} \\ &\Leftrightarrow \exists x, y \in \mathbb{Z} \mid x \cdot y \equiv 1 [n] \\ &\Leftrightarrow \exists x, y, u \in \mathbb{Z} \mid x \cdot y + u \cdot n = 1 \\ &\stackrel{\text{Bézout}}{\Leftrightarrow} x \wedge n = 1. \end{aligned}$$

■

Théorème 4 : Les propositions suivantes sont équivalentes :

- (i) n premier ;**
- (ii) $\mathbb{Z}/n\mathbb{Z}$ est intègre ;**
- (iii) $\mathbb{Z}/n\mathbb{Z}$ est un corps.**

démonstration :

(i) \Rightarrow (iii) : n premier $\Rightarrow \forall a \in \{1, \dots, n - 1\}, a \wedge n = 1 \xrightarrow{\text{thm 3}} \forall \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*, \bar{a}$ est inversible $\Rightarrow \mathbb{Z}/n\mathbb{Z}$ est un corps.

(ii) \Rightarrow (i) : On procède par contraposée : n non premier $\Rightarrow \exists n_1, n_2 \in \mathbb{N} \mid (n_1 n_2 = n \text{ et } 1 < n_1, n_2 < n) \Rightarrow \bar{n}_1 \cdot \bar{n}_2 = \bar{n} = \bar{0}$. Mais $\bar{n}_1 \neq \bar{0}$ et $\bar{n}_2 \neq \bar{0}$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

Enfin, puisque tout corps est intègre, le théorème est démontré. ■

14.4 Applications

14.4.1 Théorème des restes chinois

Théorème 5 (des restes chinois) : Soient $p, q \in \mathbb{N}^*$. Alors

$$p \wedge q = 1 \iff \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}.$$

démonstration :

" \implies " : Soit f l'application définie par

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ x &\longmapsto (\bar{x}, \tilde{x}). \end{aligned}$$

On vérifie aisément grâce à la proposition 3 que f est un morphisme d'anneaux.

Déterminons alors son noyau. Soit $x \in \mathbb{Z}$ tel que $f(x) = (\bar{0}, \tilde{0})$. Alors on a simultanément $\bar{x} = \bar{0}$ et $\tilde{x} = \tilde{0}$, c'est-à-dire p et q divisent x . Or $p \wedge q = 1$ par hypothèse, donc la produit pq divise aussi x , de sorte que $x \in pq\mathbb{Z}$, et le noyau recherché n'est autre que $pq\mathbb{Z}$.

L'application quotient $\bar{f} : \mathbb{Z}/pq\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ est donc injective, et les deux ensembles ont même cardinal, donc \bar{f} est bijective, d'où $\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

" \impliedby " : Soit g l'isomorphisme (d'après le sens direct) d'anneau défini par

$$\begin{aligned} g : \mathbb{Z}/pq\mathbb{Z} &\longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \hat{x} &\longmapsto (\bar{x}, \tilde{x}). \end{aligned}$$

Supposons $p \wedge q = d \neq 1$. Alors il existe p', q' tels que $p = p'd$ et $q = q'd$. Puisque $g(\hat{1}) = (\bar{1}, \tilde{1})$ et $\hat{1}$ est d'ordre pq pour l'addition, il doit en être de même pour $(\bar{1}, \tilde{1})$.

Or $dp'q'(\bar{1}, \tilde{1}) = (q'(p\bar{1}), p'(q\tilde{1})) = (\bar{0}, \tilde{0})$, donc $(\bar{1}, \tilde{1})$ est d'ordre inférieur ou égal à $dp'q' < pq$. On aboutit à une contradiction qui prouve bien que $p \wedge q = 1$. ■

14.4.2 Petit théorème de Fermat

Théorème 6 (de Fermat) : Si p est premier, alors pour tout $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

démonstration : Puisque p est premier, alors pour tout $k \in \{1, \dots, p-1\}$, p divise $\binom{p}{k}$. En effet, $\binom{p}{k} = p(p-1) \cdots (p-k+1)/k! \iff k! \binom{p}{k} = p(p-1) \cdots (p-k+1)$. Comme p est premier, il est premier avec tout entier le précédent, donc $p \wedge k! = 1$, et il vient que p ne divise pas $k!$. Par le théorème de Gauss, il s'ensuit que p divise $\binom{p}{k}$.

Procédons ensuite par récurrence sur l'entier $a \in \mathbb{N}$.

- **Initialisation :** Si $a = 0$, le résultat est évident.
- **Hérédité :** Supposons que $(a-1)^p \equiv a-1 \pmod{p}$.

$$a^p = (a-1+1)^p = \sum_{k=0}^p \binom{p}{k} (a-1)^k \equiv (a-1)^p + 1 \pmod{p} \stackrel{H.R.}{\equiv} a-1+1 \pmod{p} \equiv a \pmod{p}.$$

Si $a \in (-\mathbb{N})^*$, alors $-a \in \mathbb{N} \Rightarrow (-a)^p \equiv -a [p]$. Supposons alors un instant $p \neq 2$ de sorte que la condition p premier soit équivalente à dire que p est impair. La relation de congruence précédente devient alors $-a^p \equiv -a [p] \Leftrightarrow a^p \equiv a [p]$. Enfin, si $p = 2$, alors quelque soit a , l'entier $a^p - a$ est pair, et donc divisible par p . ■

14.4.3 Théorème de Wilson

Théorème 7 (de Wilson) : Soit $p \geq 2$ un entier naturel. Alors p est premier si et seulement si $(p - 1)! \equiv -1 [p]$.

démonstration :

" \Rightarrow " : Supposons p non premier, de sorte qu'il existe d, p' tel que $p = dp'$. d est strictement compris entre 1 et p , et puisque p divise $(p - 1)! + 1$ par hypothèse, d le divise aussi. Or d est l'un des facteurs de $(p - 1)!$ donc d divise $(p - 1)!$, et on arrive ainsi à la contradiction que d divise 1. Finalement, p est premier.

" \Leftarrow " : Puisque p est premier, a ne le divise pas. D'après le petit théorème de Fermat, $a^p \equiv a [p] \Leftrightarrow a(a^{p-1} - 1) \equiv 0 [p] \Rightarrow a^{p-1} \equiv 1 [p] \Leftrightarrow \bar{a}^{p-1} = \bar{1}$. Par suite, le polynôme $X^{p-1} - \bar{1}$ admet pour racines tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ et, le produit des racines valant $-\bar{1}$, il vient que $(p - 1)! + \bar{1} = \bar{0}$, c'est-à-dire $(p - 1)! \equiv -1 [p]$. ■

14.4.4 Critères de divisibilité

En base 10, tout entier naturel N s'écrit sous la forme $N = a_0 + 10a_1 + \dots + 10^n a_n$.

Puisque $10 \equiv 1 [3/9]$, $10^n \equiv 1 [3/9]$ pour tout n , donc $N \equiv a_0 + a_1 + \dots + a_n [3/9]$. On en tire le critère suivant : « **Un nombre est divisible par 3 (ou 9) si la somme de ses chiffres l'est** ».

De même, $10 \equiv -1 [11] \Rightarrow \forall n \in \mathbb{N}, 10^n \equiv (-1)^n [11] \Rightarrow N \equiv a_0 - a_1 + a_2 + \dots + (-1)^n a_n [11]$. D'où le critère suivant : « **Un nombre est divisible par 11 si la différence de la somme de ses chiffres de rang pairs par celle de ses chiffres de rang impairs l'est** ».

Exercice : Dire si les nombres suivants sont multiples de 3, 9 et/ou 11 :

324, 1948617, 18690045, 2310905821257, 1073741824.

Solution : On récapitule ceci selon le tableau suivant (Σ_p désigne la somme des chiffres de rang pairs et Σ_i celle des chiffres de rangs impairs) :

Nombre	324	1948617	18690045	2310905821257	1073741824
Sommes des chiffres	9	36	33	45	37
Divisible par 3 ?	oui	oui	oui	oui	non
Divisible par 9 ?	oui	oui	non	oui	non
Σ_p	2	18	22	17	19
Σ_i	7	18	11	28	18
Différence	5	0	11	11	1
Divisible par 11 ?	non	oui	oui	oui	non



Congruences dans \mathbb{Z} . Anneau $\mathbb{Z}/n\mathbb{Z}$.

Ces critères permettent aussi de commencer la décomposition d'un nombre en produit de facteurs premiers, mais ceci sera l'objet de la leçon n° 13... \diamond

© 2011 par Martial LENZEN.

Aucune reproduction, même partielle, autres que celles prévues à l'article L. 122-5 du code de la propriété intellectuelle, ne peut être faite sans l'autorisation expresse de l'auteur.