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

Pré-requis:
- Définition d'une relation d'équivalence.
- Notions de $PGCD$ (noté $(,)$), de nombre premier et de nombres premiers entre eux (avec en particulier les théorèmes de Bezout et d'Euclide).
- Définitions d'anneaux et de corps.
- Division euclidienne.

0.1 Congruence dans $\mathbb{Z}$.

Proposition 0.1.1.
Soit $n \in \mathbb{Z} \setminus \{0\}$. La relation définie sur $\mathbb{Z}$ par:

$$\forall (a,b) \in \mathbb{Z}^2, \qquad a\,\mathcal{R}\,b \Leftrightarrow n|(a-b)$$

est une relation d'équivalence.

Démonstration. $\forall a \in \mathbb{Z}$, $a\,\mathcal{R}\,a \Leftrightarrow n|0$ ce qui est toujours vrai.
$\forall (a,b) \in \mathbb{Z}^2$, $a\,\mathcal{R}\,b \Leftrightarrow n|(a-b) \Leftrightarrow n|(b-a) \Leftrightarrow b\,\mathcal{R}\,a$.
$\forall (a,b,c) \in \mathbb{Z}^3$,

$$\left\{\begin{array}{l} a\,\mathcal{R}\,b \\ b\,\mathcal{R}\,c \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} n|(a-b) \\ n|(b-c) \end{array}\right. \Rightarrow n|(a-b+b-c)$$

donc $a\,\mathcal{R}\,c$. ∎

Notation: On note cette relation $a \equiv b[n]$ et on dit que a est congru à b modulo n.
Exemples:
- $5 \equiv 0[10]$
- $3 \equiv 1[2]$ mais aussi $3 \equiv -2[2]$
- $17 \equiv -2[19]$

Proposition 0.1.2.
La relation de congruence est compatible avec l'addition et la multiplication dans $\mathbb{Z}$, c'est-à-dire:
Soient $n \in_I N^*$, $(a,b,a',b') \in \mathbb{Z}^4$,

$$\text{si } \left\{\begin{array}{l} a \equiv a'[n] \\ b \equiv b'[n] \end{array}\right. \quad \text{alors, } \left\{\begin{array}{l} a+b \equiv a'+b'[n] \\ ab \equiv a'b'[n] \end{array}\right.$$

Démonstration. $a \equiv a'[n]$ alors il existe $k \in \mathbb{Z}$ tel que $a = a' + kn$ et $b \equiv b'[n]$ donc il existe $l \in \mathbb{Z}$ tel que $b = b' + ln$ ainsi $a + b = a' + b' + (k+l)n$ d'où $a + b \equiv a' + b'[n]$.

$$\begin{aligned} ab &= (a'+kn)(b'+ln) \\ &= a'b' + (a'l + kb' + kln)n \end{aligned}$$

donc $ab \equiv a'b'[n]$. ∎

Exercices: Soit $n \in \mathbb{N}$,
- Si n est pair alors $n^2 \equiv 0[2n]$.
  Si n est impair alors $n^2 \equiv n[2n]$.
- Si $n \equiv 0[3]$ alors $n^2 \equiv 0[3n]$.
  Si $n \equiv 1[3]$ alors $n^2 \equiv n[3n]$.
  Si $n \equiv 2[3]$ alors $n^2 \equiv 2n[3n]$.

0.2 L'anneau $\mathbb{Z}/n\mathbb{Z}$.

Définition 0.2.1.

- Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. Soit x un élément de E. On appelle classe d'équivalence de x et on note $\overline{x}$ le sous-ensemble de E définit par:

$$\overline{x} = \{y \in E | y \,\mathcal{R}\, x\}$$

  x est alors appelé un représentant de $\overline{x}$.
- On appelle ensemble quotient de E par $\mathcal{R}$ et on note $E/\mathcal{R}$ l'ensemble:

$$E/\mathcal{R} = \{\overline{x} | x \in E\}\,.$$

- On appelle système de représentants de $E/\mathcal{R}$ toute famille $(x_i)_{i\in I}$ d'éléments de E telle que:

$$\forall x \in E,\ \exists ! i \in I \text{ tel que } x \in \overline{x_i}.$$

Remarques: La famille $(x_i)_{i\in I}$ forme une partition de E et $E/\mathcal{R} = \{\overline{x_i} | i \in I\}$, d'où $|E/\mathcal{R}| = |I|$.
Notation: On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation $\mathcal{R}$.

Proposition 0.2.2.
Soient a et b dans $\mathbb{Z}$. Alors $a \equiv b[n]$ si, et seulement si a et b ont le même reste dans la division euclidienne par n.

Démonstration. $\boxed{\Rightarrow}$ Si $a \equiv b[n]$, effectuons la division euclidienne de a et b par n:

$$a = nq + r \qquad \text{où } 0 \leq r \leq n-1$$

et

$$b = nq' + r' \qquad \text{où } 0 \leq r' \leq n-1.$$

Par hypothèse, il existe $k \in \mathbb{Z}$ tel que $a - b = kn$ or

$$a - b = (q - q')n + r - r'.$$

Comme $n|(a-b)$, alors $n|(r-r')$, mais $1 - n \leq r - r' \leq n - 1$ et le seul multiple de n dans $[1-n, n-1]$ est 0 donc $r - r' = 0$.
$\boxed{\Leftarrow}$ Si $r = r'$, alors $a - b = (q - q')n$ et donc $a \equiv b[n]$.

■

Proposition 0.2.3.
L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$, admet pour système de représentants $(0, 1, \dots, n-1)$. Ainsi,

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\} \quad \text{et} \quad |\mathbb{Z}/n\mathbb{Z}| = n.$$

Démonstration. Soit $a \in \mathbb{Z}$, la division euclidienne par n nous donne un unique r dans $[\![0, n-1]\!]$ tel que $a \equiv r[n]$, c'est-à-dire $a \in \overline{r}$. Donc $(0, 1, \dots, n-1)$ est un système de représentant. ■

Proposition 0.2.4.
Soit $n \in \mathbb{N}^*$. On peut définir sur $\mathbb{Z}/n\mathbb{Z}$ une addition et une multiplication de la façon suivante:

$$\forall \alpha, \beta \in \mathbb{Z}/n\mathbb{Z}, \exists a, b \in \mathbb{Z} \text{ tels que } \alpha = \overline{a} \ \text{ et } \ \beta = \overline{b},$$

on pose

$$\alpha + \beta = \overline{a} + \overline{b} := \overline{a+b}$$

et

$$\alpha\beta = \overline{a} \cdot \overline{b} := \overline{ab}.$$

Démonstration. Ces deux opérations sont bien définies: Prenons a' et b' deux autres représentants: $\alpha = \overline{a} = \overline{a'}$ et $\beta = \overline{b} = \overline{b'}$ alors

$$\begin{cases} a \equiv a'[n] \\ b \equiv b'[n] \end{cases} \text{alors, } \begin{cases} a + b \equiv a' + b'[n] \\ ab \equiv a'b'[n] \end{cases}$$

ainsi

$$\begin{cases} \overline{a+b} = \overline{a'+b'} \\ \overline{ab} = \overline{a'b'} \end{cases}$$

Ainsi on trouve le même résultat pour $\alpha+\beta$ et $\alpha\beta$, quels que soient les représentants choisis. ■

Théorème 0.2.5.
Soit $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

Démonstration.
- ⋄ $+$ est commutative, associative sur $\mathbb{Z}/n\mathbb{Z}$ car elle l'est dans $\mathbb{Z}$.
- ⋄ $\overline{0}$ est l'élément neutre pour $+$.
- ⋄ L'opposé de $\overline{a}$ est $\overline{-a}$.
- ⋄ $\cdot$ est commutative, associative et distributive par rapport à $+$ sur $\mathbb{Z}/n\mathbb{Z}$ car elle l'est dans $\mathbb{Z}$.
- ⋄ $\overline{1}$ est l'élément neutre pour $\cdot$.

■

Proposition 0.2.6.
Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z} \setminus \{0\}$. Alors $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si $(a, n) = 1$.

Démonstration. Si $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, alors il existe b dans $\mathbb{Z}$ tel que $\overline{a}\cdot\overline{b}=\overline{1}$, donc il existe k dans $\mathbb{Z}$ tel que $ab=1+kn$ c'est-à-dire $ab-kn=1$ donc d'après le théorème de Bezout, $(a,n)=1$.

Si $(a,n)=1$ alors d'après le théorème de Bezout, il existe $(u,v)\in\mathbb{Z}^2$ tel que $au+nv=1$ ainsi

$$\overline{au+nv}=\overline{1}\Rightarrow\overline{au}+\overline{nv}=\overline{1}\Rightarrow\overline{a}\cdot\overline{u}+\underbrace{\overline{n}\cdot\overline{v}}_{=\overline{0}}=\overline{1},$$

donc $\overline{a}\cdot\overline{u}=\overline{1}$. ∎

Théorème 0.2.7.
Soit $p\in\mathbb{Z}\setminus\{0\}$. Les trois propositions suivantes sont équivalentes:
(i) p est un nombre premier.
(ii) $\mathbb{Z}/p\mathbb{Z}$ est intègre.
(iii) $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Démonstration. $\boxed{\text{(iii)}\Rightarrow\text{(ii) :}}$ Si $\overline{x}\cdot\overline{y}=\overline{0}$ et $\overline{x}\neq\overline{0}$, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, $\overline{x}$ possède un inverse $(\overline{x})^{-1}$ or $(\overline{x})^{-1}(\overline{x}\cdot\overline{y})=\left((\overline{x})^{-1}\overline{x}\right)\overline{y}=\overline{y}$ et $(\overline{x})^{-1}(\overline{x}\cdot\overline{y})=(\overline{x})^{-1}\cdot\overline{0}=\overline{0}$ donc $\overline{y}=\overline{0}$.

$\boxed{\text{(ii)}\Rightarrow\text{(i) :}}$ Soit a un diviseur non nul de p: il existe b dans $\mathbb{Z}$ tel que $ab=p$, dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}\cdot\overline{b}=\overline{p}=\overline{0}$, or par hypothèse, $\mathbb{Z}/p\mathbb{Z}$ est intègre donc $\overline{a}=\overline{0}$ ou $\overline{b}=\overline{0}$.
Si $\overline{a}=\overline{0}$, alors il existe u dans $\mathbb{Z}$ tel que $a=up=uab$ or $a\neq 0$ donc $ub=1$ et par conséquent, $b=\pm1$ et $a=\pm p$. De même, si $\overline{b}=\overline{0}$ alors $a=\pm1$ et $b=\pm p$ donc p est premier.

$\boxed{\text{(i)}\Rightarrow\text{(iii) :}}$ Soit $\overline{a}\in\mathbb{Z}/p\mathbb{Z}\setminus\{\overline{0}\}$, $\overline{a}\neq\overline{0}$ donc p ne divise pas a or p étant premier, $(p,a)=1$ et la proposition précédente nous permet de dire que $\overline{a}$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$.

∎

0.3 Applications.

0.3.1 Le petit théorème de Fermat.

Lemme 0.3.1.
Soient a, b dans $\mathbb{Z}\setminus\{0\}$ tels que $(a,b)=1$ alors

$$\mathbb{Z}/b\mathbb{Z}\setminus\{0\}=\left\{\overline{a},\overline{2a},\ldots,\overline{(b-1)a}\right\}.$$

Démonstration. $\mathbb{Z}/b\mathbb{Z}\setminus\{\overline{0}\}$ possède $b-1$ éléments, il suffit donc de montrer que $\overline{a}$, $\overline{2a}$, ..., $\overline{(b-1)a}$ sont distincts deux à deux et différents de $\overline{0}$.

Montrons tout d'abord qu'ils sont différents de $\overline{0}$: Si il existe k dans $\mathbb{Z}$ tel que $\overline{ka}=\overline{0}$ alors $b|ka$ or $(a,b)=1$ donc par le lemme d'Euclide $b|k$ ainsi $k\geq b$ or $k\in\{1,2,\ldots,b-1\}$.

Montrons maintenant qu'ils sont deux à deux distincts: Si il existe k et l dans $\{1,2,\ldots,b-1\}$ tels que $\overline{ka}=\overline{la}$ alors $b|(k-l)a$ or $(a,b)=1$ donc, toujours d'après le lemme d'Euclide, $b|(k-l)$ or $2-b\leq k-l\leq b-2$ et le seul multiple de b dans $[2-b,b-2]$ est 0 donc $k-l=0$. ∎

Théorème 0.3.2.

Soit p un nombre premier et $a \in \mathbb{Z}$ tel que p ne divise pas a, alors

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

Remarque: Si $p|a$, alors $a \equiv 0[p]$ et $a^{p-1} \equiv 0[p]$.

Démonstration. $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\} = \{\overline{1}, \overline{2}, \dots, \overline{p-1}\}$ or p est premier et ne divise pas a donc $(a,p) = 1$ et d'après le lemme, $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\} = \left\{\overline{a}, \overline{2a}, \dots, \overline{(p-1)a}\right\}$. Ainsi

$$\overline{1} \cdot \overline{2} \cdot \dots \cdot \overline{p-1} = \overline{a} \cdot \overline{2a} \cdot \dots \cdot \overline{(p-1)a}$$

donc

$$\overline{(p-1)!} = \overline{(p-1)!}\,(\overline{a})^{p-1} \Rightarrow \overline{(p-1)!}\left((\overline{a})^{p-1} - \overline{1}\right) = \overline{0}.$$

De plus, p ne divise pas $(p-1)!$ donc $\overline{(p-1)!} \neq \overline{0}$ et $\mathbb{Z}/p\mathbb{Z}$ est intègre donc $(\overline{a}) = \overline{1}$ c'est-à-dire $a^{p-1} \equiv 1[p]$. ∎

0.3.2 Le théorème des restes Chinois.

Théorème 0.3.3.

Soit m et n dans $\mathbb{Z} \setminus \{0\}$ tels que $(m,n) = 1$. Pour tous a et b dans $\mathbb{Z}$, le système d'équations:

$$\begin{cases} x \equiv a[n] \\ x \equiv b[m] \end{cases} \qquad \text{(E)}$$

possède des solutions dans $\mathbb{Z}$ qui sont de la forme $x_0 + kmn$ où x_0 est une solution particulière et k décrit $\mathbb{Z}$.
Réciproquement, si (E) possède au moins une solution dans $\mathbb{Z}$, alors $(m,n) = 1$.

Démonstration. $\boxed{\Rightarrow}$ Si $(m,n) = 1$, (E) est équivalent à l'existence d'un couple (k,l) de $\mathbb{Z}$ tel que $x = a + kn = b + lm$ ainsi, $b - a = kn - lm$. $(m,n) = 1$ alors d'après le théorème de Bezout il existe $(u,v) \in \mathbb{Z}^2$ tel que $un + vm = 1$ ainsi $u(b-a)n + v(b-a)m = b - a$. Posons $k = u(b-a)n$ et $l = -v(b-a)m$ ainsi $a + k = b + l := x_0$ qui est solution particulière de (E). Alors

$$\begin{cases} x \equiv a \equiv x_0[n] \\ x \equiv b \equiv x_0[m] \end{cases}$$

donc $n|(x - x_0)$ et $m|(x - x_0)$. Or $(m,n) = 1$ donc $mn|(x - x_0)$, par conséquent il existe r dans $\mathbb{Z}$ tel que $x = x_0 + rmn$ et $\forall r \in \mathbb{Z}$, $x = x_0 + rmn$ est solution de (E).

$\boxed{\Leftarrow}$ Réciproquement, prenons $a = 1$ et $b = 0$ alors par hypothèse il existe x dans $\mathbb{Z}$ tel que $\begin{cases} x \equiv 1[n] \\ x \equiv 0[m] \end{cases}$, donc il existe un couple (k,l) de $\mathbb{Z}$ tel que $x = 1 + kn = lm$ d'où $lm - kn = 1$ et d'après le théorème de Bezout $(m,n) = 1$.

∎