C11 - Arithmétique

I. Divisibilité

1. Relation de divisibilité

Association

a et b $\in \mathbb{Z}$ sont dit associés ssi $a|b$ et $b|a$

Ils sont associés ssi :

$$|a| = |b| \Leftrightarrow a = \pm\, b \Leftrightarrow \exists \epsilon \in \{\pm 1\}$$

Démonstration
Supposons $a = \epsilon b$ avec $\epsilon \in \{\pm 1\}$
alors $b|a$ et $b = \epsilon a$ Donc $a|b$
a et b sont associés

Supposons que a et b soient associés :

- Si $a = 0$ alors comme $a|b$, $b = 0$
  donc $a = \pm\, b$ donc $|a| = |b|$
- Si $b = 0$ se même $|a| = |b|$
- Si $a \neq 0$ et $b \neq 0$
  Alors comme $a|b$, il existe $|a||k| = |b|$
  Comme $b \neq 0$, $k \neq 0$ donc $|k| \geq 1$ et comme $|a|$ et $|b|$ sont positifs
  $|a| \leq |b|$
  Par symétrie des roles, $|b| \leq |a|$
  Donc $|a| = |b|$

Démonstration de la conséquence

R et T par "restriction"
Antisymétrique :
Soient $a, b \in \mathbb{N}$ tq $a|b$ et $b|a$

Alors par la proposition : $|a| = |b|$ or $a, b \in \mathbb{N}$,
Donc $a = b$
De plus $2 \nmid 3$ et $3 \nmid 2$
Donc l'ordre n'est pas total.

II. Diviseurs et multiples communs

2. Cas des entiers relatifs

Proposition 18

Démonstration

Soient $a, b \in \mathbb{Z}$ et $k \in \mathbb{Z}^*$
On a $a \wedge b \mid a$ donc $k(a \wedge b) \mid ka$
De même $k(a \wedge b) \mid (ka) \wedge (kb)$
De plus il existe $u, v \in \mathbb{Z}$ tq
$a \wedge b = au + bv$
On a alors $k(a \wedge b) = (ka)u + (kb)v$
or

$$\begin{cases} (ka) \wedge (kb) \mid (ka) \\ (ka) \wedge (kb) \mid (kb) \end{cases}$$

donc

$$(ka) \wedge (kb) \mid (ka)u + (kb)v$$

$$(ka) \wedge (kb) \mid k(a \wedge b)$$

Ainsi $k(a \wedge b)$ et $(ka) \wedge (kb)$ sont associés et comme ce sont des entiers naturels, ils sont égaux.

3. Nombre premiers entre eux

Théorème

Soit $a, b \in \mathbb{Z}$ alors

$$a \wedge b = 1 \Leftrightarrow (\exists u, v \in \mathbb{Z}, au + bv = 1)$$

Démonstration:

$\Rightarrow$: Relation de Bézout
$\Leftarrow$: Supposons qu'il existe $u, v \in \mathbb{Z}$ tel que :

$$au + bv = 1$$

Tout diviseur commun d de a et b divise la CLE $au + bv = 1$
or $1 \in \mathbb{N}$ et $1 \mid a$ et $1 \mid b$ donc par la caractérisation des PGCD, $1 = a \wedge b$

Théorème de Gauss

Soient $a, b, c \in \mathbb{Z}$

$$\left.\begin{array}{r} a \mid bc \\ a \wedge b = 1 \end{array}\right\} \Rightarrow a \mid c$$

Supposons que $a \mid bc$ et $a \wedge b = 1$
Par la relation de Bézout, il existe $u, v \in \mathbb{Z}$ tel que :

$$au + bv = 1$$

On a alors

$$a(uc) + (bc)v = c$$

or $a \mid a(uc)$ et $a \mid (bc)v$
Donc a divise la CLE

$$a(uc) + (bc)v = c$$

Théorème : Divisibilité par produit

Soient $a, b, c \in \mathbb{Z}$

$$\left.\begin{array}{r} a \mid b \\ b \mid c \\ a \wedge b = 1 \end{array}\right\} \Rightarrow ab \mid c$$

Démonstration :
Supposons $a \mid b$, $b \mid c$ et $a \wedge b = 1$

Comme $a \mid c$ il existe $k \in \mathbb{Z}$ tq $ak = c$
Or $b \mid c$ i.e. $b \mid ak$
et $b \wedge a = 1$
Donc par le théorème de Gauss

Théorème

Soient $a, b, c \in \mathbb{Z}$

$$\left.\begin{matrix} a \wedge b \\ b \wedge c \end{matrix}\right\} \Rightarrow (ab) \wedge c = 1$$

Théorème

$$\forall r \in \mathbb{Q}, \exists!(p, q) \in \mathbb{Z} \times \mathbb{N}^*, \begin{cases} p \wedge q = 1 \\ \frac{p}{q} = r \end{cases}$$

Démonstration

Unicité

Soient $(p, q), (p', q') \in \mathbb{Z} \times \mathbb{N}^*$, tel que $p \wedge q$ = $p' \wedge q' = 1$
et $\frac{p}{q} = \frac{p'}{q'}$
On a alors $pq' = p'q$ donc $pp'q'$ ou $p \wedge q = 1$ (Gauss) De même $p' \mid p$ donc $q' = \pm q$ or $q, q' \in \mathbb{N}^*$,
Donc $q' = q$ et $p' = p$

Définition

L'écriture $r = \frac{p}{q}$ s'appelle l'écriture irréductible du rationnel r

4. PGCD de plus de 2 entiers

Définition

Soient $a, b, c \in \mathbb{Z}$,
Le PGCD de 3 entiers est :

$$a \wedge b \wedge c$$

Propriété

La loi $\wedge$ est associative te commutative et admet 0 comme élément neutre $(\text{sur } \mathbb{N})$.

Proposition 21

Démonstration
L'assertion de recurrence est la proposition

Initialisation

A_2 est la relation de Bézout déja vue et prouvée

Hérédité

Soit $n \geq 2$ tq A_n
Soient $a_1, \ldots, a_{n+1} \in \mathbb{Z}$
Par H.R. il existe $u_1, \ldots u_n \in \mathbb{Z}$ tq

$$\bigwedge_{i=1}^{n} a_i = \sum_{i=1}^{n} u_i a_i$$

Puis par A_2 :

$$\bigwedge_{i=1}^{n} a_i \ \wedge a_{n+1} = (\bigwedge_{i=1}^{n} a_i)u + a_{n+1}v$$

Cela se réécrit :

$$\bigwedge_{i=1}^{n+1} a_i = \left(\sum_{i=1}^{n} a_i(u_i u) \right) + a_{n+1}v = \sum_{i=1}^{n+1} a_{i\tilde{u_i}}$$

En posant :

$$\begin{cases} \forall i \in [\![1, n]\!], \tilde{u_i} = u_i u \in \mathbb{Z} \\ u_{\tilde{n+1}} = v \in \mathbb{Z} \end{cases}$$

Ainsi A_{n+1} est vérifiée
Cela achève l'hérédité

Définition

Soient $a_1, \ldots, a_n \in \mathbb{Z}$
On dit qu'ils sont

1. Premiers entre eux deux a deux ssi $\forall i, j \in [\![1, n]\!], (i \neq j \Rightarrow a_i \wedge a_j = 1$
2. Premiers entre eux dans leur ensemble

ssi

$$\bigwedge_{i=1}^{n} a_i = 1$$

Démonstration
Si $a = 0$ ou $b = 0$ le seul multiple positif de a et b est 0 et $min_{|\mathbb{N}}(\{0\}) = 0$
Si $a \neq 0$ et $b \neq 0$
On note $d = a \wedge b \neq 0$ (car $a \neq 0$)
On pose $m = \frac{ab}{d}$
Comme $d \mid b$, alors $\frac{b}{d} \in \mathbb{N}$ et $m = a\left(\frac{b}{d}\right)$
est un multiple de a
De même m est un multiple de b, donc m est un multiple commun à a et b
Soit n un multiple commun de a et b Posons $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$
On a $a' \wedge b' = 1$
(On a vu que si $k \mid a$ et $k \mid b$, $\left(\frac{a}{k}\right) \wedge \left(\frac{b}{k}\right) = \frac{a \wedge b}{k}$)
On a $a \mid n$ donc $a' \mid \frac{n}{d}$
Puis de même $b' \mid \frac{n}{d}$
or $a' \wedge b' = 1$ donc $a'b' \mid \frac{n}{d}$
i.e. $\frac{a}{d} \times \frac{b}{d} \mid \frac{n}{d}$
en multipliant par d, $m = \frac{ab}{d} \mid n$
Donc m divise tout multiple commun de a et b

Théorème de Bézout

$$\forall a_1, \ldots, a_n \in \mathbb{Z}, \bigwedge_{i=1}^{n} a_i = 1 \Leftrightarrow \left(\exists u_1, \ldots, u_n, \sum_{i=1}^{n} u_i a_i = 1\right)$$

5. PPCM

Définition dans $\mathbb{Z}$ du PPCM

Pour $a, b \in \mathbb{Z}$, on pose

$$a \vee b = |a| \vee |b|$$

Propriété

Pour $a \neq 0$ et $b \neq 0$, $a \vee b$ est aussi le plus petit des multiples communs positifs de a et b au sens de l'ordre usuel $\leq$

Propriété : Caractérisation du PPCM

Soient $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}$
Alors

$$m = a \vee b \Leftrightarrow \begin{cases} a \mid m \text{ et } b \mid m \\ \forall n \in \mathbb{Z}, (a \mid n \text{ et } b \mid n \Rightarrow m \mid n) \end{cases}$$

Propriété

$$\forall a, b \in \mathbb{Z}, (a \wedge b)(a \vee b) = |ab|$$

Méthode de calcul $a \vee b$

$$42 \wedge 54 = 6$$

Donc

$$42 \vee 54 = \frac{42 \times 54}{6} = 42 \times 9 = 378$$

Propriété

$$\forall a, b, n \in \mathbb{Z}, (na) \vee (nb) = |n|(a \vee b)$$

III. Nombres premiers

1. Définition et premières propriétés

Définition

Un nombre premier est un entier naturel $p \neq 1$ et dont les seuls diviseurs positifs sont 1 et p

Remarque : 1 n'est pas premier

Notation (du prof)

On notera $\mathcal{P}$ l'ensemble des nombres premiers

Exemple

$$2, 3, 5, 7, 11 \in \mathcal{P}$$

Définition

$n \neq 1$ et non premier est dit composé.
Il existe alors $ab \in \mathbb{N} \backslash \{1, n\}$ tel que
$n = ab$. Si $n \neq 0$, on a $a, b \in [\![2, n-1]\!]$ et $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$

Cela justifie la méthode su crible d'Ératosthène pour trouver tous les nombres premiers inférieur ou égaux a une borne fixée.

$$\begin{array}{cccccccccc}
1 & \boxed{2} & \boxed{3} & 4 & \boxed{5} & 6 & \boxed{7} & 8 & 9 & 10 \\
\boxed{11} & 12 & \boxed{13} & 14 & 15 & 16 & \boxed{17} & 18 & \boxed{19} & 20 \\
21 & 22 & \boxed{23} & 24 & 25 & 26 & 27 & 28 & \boxed{29} & 30 \\
\boxed{31} & 32 & 33 & 34 & 35 & 36 & \boxed{37} & 38 & 39 & 40 \\
\boxed{41} & 42 & \boxed{43} & 44 & 45 & 46 & \boxed{47} & 48 & 49 & 50
\end{array}$$

Propriété

Soit $p \in \mathcal{P}$ et $n \in \mathbb{Z}$
Alors

$$n \wedge p \neq 1 \Leftrightarrow p \mid n$$

i.e. on a une alternative

- Soit $p \mid n$ et $p \wedge n = p$
- Soit p et n sont premiers entre eux

Lemme d'Euclide

Soit $p \in \mathcal{P}$ et $e, b \in \mathbb{Z}$ Alors

$$p \mid ab \Rightarrow (p \mid a \text{ ou } p \mid b)$$

Démonstration
Supposons $p \mid ab$
On a deux cas :

- Si $p \mid a$ c'est fini
- Si $p \nmid a$ alors $p \wedge a = 1$
  Donc par le théorème de Gauss
  Comme $p \wedge a = 1$ et $p \mid ab$, alors $p \mid b$

Théorème

$\mathcal{P}$ est fini

2. Décomposition en facteurs premiers

Théorème

$$\forall n \in \mathbb{N}^*, \exists k \in \mathbb{N}, \exists p_1, \ldots, p_k \in \mathcal{P}, \exists \alpha_1, \ldots, \alpha_k \in \mathbb{N}^*, n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$$

De plus cette écriture est unique à l'ordre des facteurs près

Démonstration

Existence par récurrence forte sur $\mathbb{N}$

Pour $n \in \mathbb{N}^*$ on pose
$A_n : \exists k \in \mathbb{N}, \exists p_1, \ldots, p_k \in \mathcal{P}, \exists \alpha_1, \ldots, \alpha_k \in \mathbb{N}^*, n = \prod_{i=1}^{k} p_i^{\alpha_i}$

Initialisation

$1 = \prod_{i=1}^{0} p_i^{\alpha_i}$ Donc A_1 est vérifiée

Hérédité

Soit $n \in \mathbb{N}^*$ tel que $A_1, A_2, \ldots, A_n$
Soient vérifiées
On a deux cas :

- Si $n+1 \in \mathcal{P}$: en prenant $k=1$ $p_1 = n+1$ et $\alpha_1 = 1$ on a

$$n+1 = \prod_{i=1}^{1} p_i^{\alpha_i}$$

- Si $n+1 \in \mathcal{P}$
  Comme $n+1 \geq 2$, alors il est composé i.e. s'écrit $n+1 = ab$ avec $a, b \in [\![2, n]\!]$
  Ainsi par H.R. A_a et A_b sont vérifiées
  Donc a s'écrit comme produits de puissances de premiers et b aussi.
  En regroupant les deux produits et éventuellement les puissances de même premiers, puis en les ordonants on a

$$(n+1) = \prod_{i=1}^{k} p_i^{\alpha_i}$$

  Donc A_{n+1} est vraie

Théorème

Soit $u \in \mathbb{C}^{\mathbb{N}}$, $l \in \mathbb{C}$

$$u_n \to l \Leftrightarrow \begin{cases} Re(u_n) \to Re(l) \\ Im(u_n) \to Im(l) \end{cases}$$

Démonstration :
$\Rightarrow$: Supposons que $u_n \to l$

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, \forall n \geq N, |u_n - l| \leq \epsilon$$

Soir $\epsilon > 0$ et N_ϵ associé
Pour $n \geq N_\epsilon$,

$$\begin{cases} |Re(u_n) - Re(l)| = |Re(u_n - l)| \leq |u_n - l| \leq \epsilon \\ |Im(u_n) - Im(l)| = |Im(u_n - l)| \leq |u_n - l| \leq \epsilon \end{cases}$$

Ainsi

$$\begin{cases} Re(u_n) \to Re(l) \\ Im(u_n) \to Im(l) \end{cases}$$

$\Leftarrow$: Supposons que $\begin{cases} Re(u_n) \to Re(l) \\ Im(u_n) \to Im(l) \end{cases}$

Soit $\epsilon > 0$
Comme $Re(u_n) \to Re(l)$ il existe $N \in \mathbb{N}$ tel que

$$\forall n \geq N, |Re(u_n) - Re(l)| \leq \frac{\epsilon}{\sqrt{2}}$$

Comme $Im(u_n) \to Im(l)$ il existe $N' \in \mathbb{N}$ tel que

$$\forall n \geq N', |Im(u_n) - Im(l)| \leq \frac{\epsilon}{\sqrt{2}}$$

Soit $N'' = max(N, N')$
Pour $n \geq N''$,

$$|u_n - l|^2 = (Re(u_n - l))^2 + (Im(u_n - l))^2 = (Re(u_n) - Re(l))^2 + (Im(u_n) - Im$$

$$|u_n - l|^2 \leq \frac{\epsilon^2}{2} + \frac{\epsilon^2}{2} = \epsilon^2 \leq \epsilon$$

Par positivité de ϵ

Ainsi

$$\forall \epsilon > 0, \exists N \in \mathbb{N}, |u_n - l| \leq \epsilon$$

Idée de la preuve de l'unicité :

Si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_l^{\beta_l}$
avec les hypothèses
Comme $p_1 | n, p_1 | q_1^{\beta_1} \dots q_l^{\beta_l}$
Comme p_1 est premier par le Lemme d'Euclide il divise l'un d'entre eux : $q_j^{\beta_j}$
et encore par le lemme d'Euclide comme $p_1 \mid q_1 \times \dots \times q_j$ et $p_1 \in \mathcal{P}$ alors $p_1 \mid q_j$

Comme q_j est premier $p_j = q_j$
Si $j \neq 1$ on aurait : $p_1 > q_1$
Or par le même raisonnement q_1 est l'un des p_i donc $p_1 \leq p_i = q_1$
Contradiction
Ainsi $j = 1$ i.e. $p_1 = q_1$
quitte a échanger les notations, on peut supposer que $\alpha_1 \leq \beta_1$
En divisant par p^{α_1} on obtiens :

$$p_2^{\alpha_2} \dots p_k^{\alpha_k} = p_1^{\beta_1 - \alpha_1} q_2^{\beta_2} \dots q_l^{\beta_l}$$

Si on avait $\beta_1 - \alpha_1 > 0$, le même raisonnement précédent prouvait que $p_2 = p_1$ ce qui n'est pas le cas.
Ainsi on a prouvé que si

$$p_1^{\alpha_1} \dots p_k^{\alpha_k} = q_1^{\beta_1} \dots q_l^{\beta_l}$$

avec

$$p_1, \dots, p_k, q_1, q_l \in \mathcal{P}$$

alors

$$p_1 = q_1 \text{ et } \alpha_1 = \beta_1$$

En divisant par $p_1^{\alpha_1}$ on obtient

$$p_2^{\alpha_2} \dots p_k^{\alpha_k} = q_2^{\beta_2} \dots q_l^{\alpha_l}$$

et $p_2 = q_2$, $\alpha_2 = \beta_2$ etc.
Par récurrence immédiate, les deux décompositions sont les mêmes

Définition

Soit $p \in \mathcal{P}$,
Pour $n \in \mathbb{N}^*$, on appelle valuation p-adique de n le nombre :

$$v_p(n) = max\{k \in \mathbb{N} \mid (p^k \mid n)\}$$

Lorsque $p \mid n$, c'est aussi la puissance de p dans la décomposition en facteurs premiers de n
Lorsque $p \nmid n$, $v_p(n) = 0$

Définition

Pour $n \in \mathbb{N}^*$, l'ecriture :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

S'appelle la factorisation-première de n

Théorème

Avec la convention qu'on ne prend pas en compte les factorisations
$p^\circ = 1$ par $p \nmid n$

$$\forall p \in \mathcal{P}, v_p(ab) = v_p(a) + v_p(b)$$

$$a \mid b \Leftrightarrow \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$$

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{min(v_p(a), v_p(b))} \text{ et } a \vee b = \prod_{p \in \mathcal{P}} p^{max(v_p(a), v_p(b))}$$

i.e.

$$\forall p \in \mathcal{P}, \begin{cases} v_p(a \wedge b) = min(v_p(a), v_p(b)) \\ v_p(a \vee b) = max(v_p(a), v_p(b)) \end{cases}$$

Cas pratique : On utilise ce produit de manière abstraite : en pratique on écrit que les premiers qui servent.

IV Congruences

Définition

Pour $n \in \mathbb{N}$,
On dit que $a, b \in \mathbb{Z}$ sont congrus modulo n ssi $n \mid a - b$
On note $a \equiv b[n]$
et lorsque on a besoin $\equiv_n a_k$ relation sur $\mathbb{Z}$ appelé congruence modulo n

Propriété

$\equiv_n$ est une relation d'équivalence
Démonstration :

- R : Pour $a \in \mathbb{Z}$ $n \mid 0 = a - a$
  Donc $a \equiv a[n]$
- S : Pour $a, b \in \mathbb{Z}$ tel que $a \equiv b[n]$
  On a $n \mid b - a$ dans $n \mid a - b$
  Donc $b \equiv a[n]$
- T : Pour $a, b, c \in \mathbb{Z}$, tel que
  $a \equiv b[n]$
  $b \equiv c[n]$
  $c - a = (c - b) + (b - a)$
  est divisible par n puisque
  $n \mid b - a$
  $n \mid c - b$
  Donc $a \equiv c[n]$

Pour la suite on suppose $n \geq 2$

Notation

On note, lorsqu'il n'y a pas ambiguïté, $\overline{a}$ la classe d'équivalence par $\equiv_n$ qu'on appelle classe de congruences modulo n de a :

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b[n]\} \subset \mathbb{Z}$$

i.e.

$$\overline{a} \in \mathcal{P}(\mathbb{Z})$$

- Exemple :
  Les classes de congruences modulo 3 sont :

$$\overline{0} = 3\mathbb{Z}, \overline{1} = 3\mathbb{Z} + 1, \overline{2} = 3\mathbb{Z} + 2$$

Reformulation

Soient $a, b \in \mathbb{Z}$,

$$a \equiv b[n] \Leftrightarrow n \mid b - a \Leftrightarrow a \in \overline{b} \Leftrightarrow b \in \overline{a} \Leftrightarrow \overline{a} = \overline{b}$$

Propriété

Les classes de congruences modulo n sont au nombre de n. Ce sont $\overline{0}, \overline{1}, \ldots, \overline{n-1}$

- Démonstration :
  Soit $n \in \mathbb{Z}$,
  On effectue la division euclidienne de a par n $(n \neq 0)$

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

  Comme $n \mid nq = a - r$, $a \equiv r[n]$
  i.e.

$$\overline{a} = \overline{r}$$

  Ainsi toute division est de la forme $\overline{k}$ avec $k \in [\![0, n-1]\!]$
  De plus c'est classes dont deux à deux d... :
  Soient $k, k' \in [\![0, n-1]\!]$ tels que $\overline{k} = \overline{k'}$
  On a alors $n \mid k' - k$ et $|k' - k| < n$ donc $k = k'$

Notation

L'ensemble quotient de $\mathbb{Z}$ par $\equiv_n$ qui est l'ensemble des classes de congruences modulo n est noté :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{k}; k \in [\![0, n-1]\!]\}$$

$('\mathbb{Z} \text{ sur } n\mathbb{Z}')$

- Exemple :

$$\mathbb{Z}/3\mathbb{Z} = \{\overline{9}, \overline{-2}, \overline{11}\}$$

Rappel

Sur les relations d'équivalences les classes forment une partition de l'ensemble sur lequel est définie la relation binaire, ici :

$$\mathbb{Z} = \bigsqcup_{k=0}^{n-1} \overline{k} = \bigsqcup_{c \in \mathbb{Z}/n\mathbb{Z}} c$$

Avec les classes non vides

Propriété

Compatibilité de $\equiv_n$ avec les opérations de $\mathbb{Z}$

$$\forall a, b, a', b' \in \mathbb{Z}, (a \equiv a'[n] \text{ et } b \equiv b'[n]) \Rightarrow a + b \equiv a' + b'[n] \text{ et } ab \equiv a'b'[n]$$

Démonstration Produit :
Soient $a, a', b, b' \in \mathbb{Z}$ tq
$a \equiv a'[n]$ et $b \equiv b'[n]$
Alors

$$a'b' - ab = (a' - a)b' + a(b' - b)$$

Comme $n \mid a' - b$ et $n \mid b' - b$ par hypothèse, n divise alors cette combinaison linéaire i.e.

$$ab \equiv a'b'[n]$$

Propriété

Soit $m \neq 0$ Alors

$$\forall a, b \in \mathbb{Z}, a \equiv b[n] \Leftrightarrow ma \equiv mb[n]$$

Avant première

A l'aide des compatibilités précédentes on peut définir

- L'addition
  Pour $c, d \in \mathbb{Z}/n\mathbb{Z}$
  On définit $c \dot{+} d$
  Comme $a + b$ ou $\overline{a} = c$ et $\overline{b} = d$
  Ce qui fonctionne bien parce qu'avec d'autres représentants a', b' tel que $\overline{a'} = c$ et $\overline{b'} = d$
  On a

$a \equiv a'[n]$ et $b \equiv b'[n]$
Donc $a + b \equiv a' + b'[n]$ i.e.

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

- La multiplication
  On définit $c \dot{\times} d$ qui ne dépends pas des représentants a de c et b de d choisis.
- Exemple :

$$\overline{1} + \overline{2} = \overline{1+2} = \overline{3}$$

(La meme pour la multiplication)

Propriété

$$(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times}) \text{ est un anneau}$$

En pratique, on note $\dot{+}$ et $\dot{\times}$ --> $+$ et $\times$ (abus pratique)

- Exercice :

$$\mathbb{Z}/n\mathbb{Z} \text{ corp} \Leftrightarrow n \in \mathcal{P}$$

- Exemple : Tableau des opérations sur $\mathbb{Z}/n\mathbb{Z}$

$\dot{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

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

$\mathbb{Z}/4\mathbb{Z}$,n'est pas un corp puisque $\overline{2} \neq \overline{0}$ et $\overline{2}$ n'est pas inversible
(Par contre $\overline{3}$ l'est)

Propriété

Soit $a \in \mathbb{Z}$ Alors

$$(\exists u \in \mathbb{Z}, au \equiv 1[n]) \Leftrightarrow a \wedge n = 1$$

- Démonstration :
  Par le théorème de Bézout

$$a \wedge n = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}, au + vn = 1 \Leftrightarrow \exists u \in \mathbb{Z}(\exists v \in \mathbb{Z}, au = 1 - nv)$$
$$\Leftrightarrow \exists u \in \mathbb{Z}(\exists k \in \mathbb{Z}, au = 1 + kn) \Leftrightarrow \exists u \in \mathbb{Z}, au \equiv 1[n]$$

Traduction dans $\mathbb{Z}/n\mathbb{Z}$

$$\overline{a} \text{ est inversible } \Leftrightarrow a \wedge n = 1$$

(au sens de $\dot{\times}$)
(Puisque $au \equiv_1 [n] \Leftrightarrow \overline{au} = \overline{1} \Leftrightarrow \overline{a}.\overline{u} = \overline{1}$)

Par abus, on dira que a est inversible modulo n u est un inverse de a modulo n

Application :
Résolution de (E) : $8x \equiv 7[15]$ d'inconnue $x \in \mathbb{Z}$
Par la propriété,
Comme $8 \wedge 15 = 1$ alors il existe $u \in \mathbb{Z}$ tq $8u \equiv 1[15]$
On a alors pour $x \in \mathbb{Z}$

$$8x \equiv 7[15] \Rightarrow x \equiv 7u[15]$$

et aussi

$$x \equiv 7u[15] \Rightarrow 8x \equiv 7[15]$$

Ainsi

$$(E) \Leftrightarrow x \equiv 7u[15] \Leftrightarrow x \in 7u + 15\mathbb{Z}$$

Maintenant trouver u
On se sert pour cela de la preuve constructive de la proposition:
Pour résoudre (E) on trouve une relation de Bézout pour 8 et 15. Ici il y en a une "apparente" : $8 \times 2 + 15 \times (-1) = 1$
Ainsi 2 est inverse de 8 modulo 15 et pour $x \in \mathbb{Z}$,
$(E) \Leftrightarrow x \equiv 14[15] \Leftrightarrow x \equiv -1[15]$ donc l'ensemble des solutions est:

$$-1 + 15\mathbb{Z}$$

Petit théorème de Fermat :

Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tel que $p \nmid a$
Alors :

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

On démontre d'abord le lemme 1.
Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$ tel que $p \nmid a$.
On note r le reste de la division euclidienne de a par p
On a $r \in \mathbb{N}$ et $a \equiv r[p]$ donc $a^p \equiv r^p[p]$
Par le lemme 1 :

$$r^p \equiv r[p]$$

Donc :

$$a^p \equiv a[p]$$

Comme $p \nmid a$ et $p \in \mathcal{P}$, $a \wedge p = 1$
Donc il existe $u \in \mathbb{Z}$ tel que $au \equiv 1[p]$
On a alors $a^{p-1} \equiv a^{p-1}au \equiv a^p u \equiv au \equiv 1[p]$

Lemme 1

Soit $p \in \mathcal{P}$
Alors :

$$\forall a \in \mathbb{N}, a^p \equiv a[p]$$

Démonstration :
Par récurrence sur a

Pour $a \in \mathbb{N}$ on pose :

$$\mathcal{A}_a :' a^p \equiv a[p]'$$

- Initialisation ez
- Hérédité
  Soit $a \in \mathbb{N}$ tq $\mathcal{A}_n$
  Alors

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k \ \ + a^p$$

  On admet le lemme 2
  et on a alors

$$\sum_{k=1}^{p-1} \binom{p}{k} a^k \equiv \sum_{k=1}^{p-1} 0.a^k \equiv 0[p]$$

  Donc

$$(a+1)^p \equiv 1 + a^p[p] \equiv 1 + a[p]$$

  Ainsi $\mathcal{A}_{a+1}$
- Conclusion
  Cela achève l'hérédité, la récurrence et la preuve du Lemme 1

Lemme 2

$$\forall p \in \mathcal{P}, \forall k \in [\![1, p-1]\!], p \mid \binom{p}{k}$$

Démonstration :
Soit $p \in \mathcal{P}$ et $k \in [\![1, p-1]\!]$
On a

$$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k(k-1)\dots 1}$$

$$p \mid p(p-1)\dots(p-k) = k!\binom{p}{k}$$

Or $k!$ est un produit d'entiers $(1, 2, \ldots, k)$ premiers avec p car p ne les divisent pas (car $r < p$) et p et $p \in \mathcal{P}$, donc $p \wedge (k!) = 1$
Par le lemme de Gauss, $p \mid \binom{p}{k}$ (Ou le lemme d'Euclide)

Méthode de résolution des équations de la forme $ax + by = c$

Inconnues : $(x, y) \in \mathbb{Z}^2$ (a, b, c sont des constantes dans $\mathbb{Z}$)

- Existence des solutions
  Notons $d = a \wedge b$)
  - Si $d \mid c$ alors il existe des solutions par la relation de Bézout :
    On trouve d'abord : $u, v \in \mathbb{Z}$
    tel que $au + bv = d$
    Puis en multipliant par le facteur adéquat e,
    $a(ue) + b(ve) = de = c$
  - Si $d \nmid c$
    il n'y a pas de solutions
    On le démontre par l'absurde.
    Si x, y étaient solutions de (E)
    On aurait $d \mid a$ et $d \mid b$
    Donc $d \mid ax + by = c$
    Contradiction
- Déterminer l'ensemble des solutions
  On se place dans le cas ou les solutions existent
  i.e. $d \mid c$ eou $d = a \wedge b$
  Etape 1 : Simplification
  On pose : $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$, $c' = \frac{c}{d}$
  et alors pour $(x, y) \in \mathbb{Z}$

  $$(E) \Leftrightarrow (E') : a'x - b'y = c'$$

  et on a $a' \wedge b' = 1$
  Quitte a faire cette eatpe avant de mettre des notations en on suppose dès le départ que $a \wedge b = 1$

Etape 2 : Soleutions particulières
On est dans le cadre d'une équation

$$(E) : ax + by = c \text{ avec } a, b, c \in \mathbb{Z}$$

On peut alors déterminer $u, v \in \mathbb{Z}$ tel que $au + bv = 1$ (relation de Bézout)
En posant

$$x_0 = cu \text{ et } y_0 = cv$$

On obtiens une solution particulière (x_0, y_0) de (E)

Etape 3 : Résolution (Rédaction subtile)
Pour $(x, y) \in \mathbb{Z}$

$$(E) \Leftrightarrow ax + by = ax_0 + by_0 \Leftrightarrow a(x - x_0) = b(y_0 - y) : (\star)$$

On résout $(\star)$ par Analyse-Synthèse

Analyse :
Supposons que (x, y) vérifie $(\star)$
Alors $a \mid a(x - x_0) = b(y_0 - y)$
et comme $a \wedge b = 1$ par le théorème de Gauss,
$a \mid y_0 - y$ i.e. il existe $k \in \mathbb{Z}$
tel que : $y = y_0 - ak$
En reportant dans $(\star)$, on a $a(x - x_0) = bak$ (Stabilité)
et comme $a \neq 0$, $x = x_0 + bk$

Synthèse :
Pour $k \in \mathbb{Z}$,
$a((x_0 + bk) - x_0) = abk = b(y_0 - (y_0 - ak))$

Conclusion :
L'ensemble des solutions de (E) est celui de $(\star)$ qui est :

$$\mathcal{S}_E = (x_0, y_0) + \mathbb{Z}(b, -a)$$

Autrement dit :

$$\mathcal{S}_E = \{(x_0, y_0) + k(b, -a); k \in \mathbb{Z}\} = \{(x_0 + kb, y_0 - ka); k \in \mathbb{Z}\}$$

Important :

En pratique il faut tout refaire dans le cas particulier ou vous êtres placés