

Arithmetique

Par Lorenzo

23 November 2024

Contents

Arrivé apres le premier CM (cours à venir)

1 Structures algébriques

1.1 Lois de compositions internes

Définition 1.1. Soit E un ensemble. On appelle **loi de composition interne** (l.c.i) sur E une opération binaire.

On parle d'application $E \times E \rightarrow E$

Définition 1.2. Soit $*$ une l.c.i sur E . On dit $*$

- **associative** si $\forall x, y, z \in E, x * (y * z) = (x * y) * z$
- **commutative** si $\forall x, y \in E, x * y = y * x$
- a un **élément neutre** $e \in E$ vérifiant $\forall x \in E, x * e = e * x = x$

1.2 Groupes

Définition 1.3. Soit G un ensemble et $*$ une l.c.i sur G . On dit que $(G, *)$ est un **groupe** lorsque les axiomes suivants sont vérifiés.

- $*$ est associative
- $*$ admet un élément neutre $e \in G$
- $\forall x \in G, \exists x' \in G$ tel que $x * x' = x' * x = e$ (on dit que x' est l'élément inverse ou symétrique de x pour $*$)

Remarques 1.1. Si de plus $*$ est commutative, alors le groupe est dit **abélien** (ou commutatif).

Exemple 1.1. Si X est un ensemble, notons $\text{Bij}(X)$, l'ensemble des application de X dans X admettant une application réciproque

$$\forall f : X \rightarrow X, \exists g : X \rightarrow X, g \circ f = f \circ g = \text{Id}_X : \begin{cases} X & \longrightarrow X \\ x & \longmapsto x \end{cases}$$

Ainsi $(\text{Bij}(X), \circ)$ est un groupe.

Proposition 1.1.

Si $(G, *)$ est un groupe alors

(a) L'élément neutre de G est unique

(b) Chaque $x \in G$ admet un unique élément inverse

(c) Si $x, y, z \in G$ tel que $x * y = z * y$ alors $x = z$ (indépendamment de l'ordre)

Démonstration 1.1.

(a): Soient e, e' des éléments neutres de G par $*$, $e * e' = e' * e = e = e'$

(b): Soient x', x'' des éléments inverse de $x \in G$,
 $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$

(c): Posons $x^{-1} * (x * y) = x^{-1} * (x * z) \implies (x^{-1} * x) * y = (x^{-1} * x) * z \implies e * y = e * z \implies y = z$

□

Remarques 1.2. Lorsqu'il n'y a pas d'ambiguïtés, l'inverse d'un élément x sera noté x^{-1} . Notons que $(x^{-1})^{-1} = x$

Définition 1.4. Soit $(G, *)$ un groupe. Soit $H \subset G$, on dit que H est un **sous-groupe** de G lorsque les conditions suivantes sont vérifiées.

1) $\forall x, y \in H, x * y \in H$. On dit que H est stable par $*$

2) Muni de $*$, H est un groupe

Proposition 1.2.

Soit $(G, *)$ un groupe et $H \subset G$. Les conditions suivantes sont équivalentes.

(a): H est un sous groupe de G

(b): $H \neq \emptyset$, H est stable par $*$ et par passage au symétrique ($\forall x \in H, x^{-1} \in H$)

(c): $H \neq \emptyset$ et $\forall x, y \in H, x * y^{-1} \in H$

Démonstration 1.2.

• Démontrons que (a) \implies (b).

◇ H est un sous groupe donc doit admettre un élément neutre (e_H) donc $H \neq \emptyset$. Montrons que $e_H = e_G$, on a $e_H * e_H = e_H = e_G * e_H = e_G$.

◇ La stabilité par $*$ fait partie de la définition de sous groupe.

◇ Soit $x \in H$, soit s' son symétrique dans H . x' est aussi un symétrique dans G . Dans G par unicité du symétrique $x^{-1} = x' \in H$.

• Démontrons que (b) \implies (c).

◇ Soient $x, y \in H$. Alors $y^{-1} \in H$ et encore par $x * y^{-1} \in H$.

• Démontrons que (c) \implies (a).

◇ l'associativité est montré par $\forall x, y, z \in H, x, y, z \in G, x * (y * z) = (x * y) * z$

◇ l'élément neutre par $\exists x \in H, e = x * x^{-1} \in G$, ainsi $\forall x \in H, x \in G$

◇ l'élément inverse par $x \in H$, prenons $y = e$, ainsi $x^{-1} * e = x^{-1}$, ici x^{-1} est le symétrique de x dans H .

◇ la stabilité par $*$ dans H par $x, y \in H$, posons $z = y^{-1}$, ainsi $x * y = x * z^{-1} \in H$.

Finalemment par implication circulaire nous avons démontré que
 (a) \iff (b) \iff (c)

□

Définition 1.5. Soient $(G, *)$ et (H, \square) deux groupes.

On appelle morphisme de groupes toute application $f : G \rightarrow H$ vérifiant

$$\forall x, y \in G, f(x * y) = f(x) \square f(y)$$

Proposition 1.3.

Si $f : G \rightarrow H$ est un morphisme de groupe, alors $f(e_G) = e_H$

Démonstration 1.3.

$$f(e_G) = f(e_G * e_G) = f(e_G) \square f(e_G)$$

$$f(e_G) = f(e_G) \square e_H$$

$$f(e_G) \square f(e_G) = f(e_G) \square e_H \implies f(e_G) = e_H$$

□

Proposition 1.4.

Si $f : G \rightarrow H$ est un morphisme de groupe, alors $\forall x \in G, f(x^{-1}) = f(x)^{-1}$

Démonstration 1.4.

$$f(x^{-1}) = f(x^{-1}) \square f(x) \square f(x)^{-1} = f(x^{-1} * x) \square f(x)^{-1} = f(x)^{-1}$$

□

2 Anneaux et Corps

Définition 2.1. Un anneau est $(A, +, \times)$ où A est un ensemble, $+$ et \times sont deux l.c.i sur A vérifiant les axiomes suivants

- $(A, +)$ est un groupe abélien (on note 0_A sont élément neutre)
- \times est associative
- \times est distributive sur $+$

Remarques 2.1. On dit que $(A, +, \times)$ est un anneau commutatif si, de plus \times est commutative.

Un élément $x \in A$ est dit inversible dans A lorsqu'il admet un symétrique pour \times .

Proposition 2.1.

Soit $(A, +, \times)$ un anneau alors

$$\forall x \in A, 0_A \times x = 0_A$$

Démonstration 2.1.

$$\begin{aligned} 0_A \times x &= (0_A + 0_A) \times x \\ &= 0_A \times x + 0_A \times x \implies 0_A = 0_A \times x \text{ (par soustraction de } 0_A \times x) \end{aligned}$$

□

Proposition 2.2.

Soient $x, y, z \in A$, Si $x \times z = y \times z$ et z est inversible alors $x = y$

Démonstration 2.2.

$$\begin{aligned} x \times z = y \times z &\implies (x \times z) \times z^{-1} = (y \times z) \times z^{-1} \\ &\implies x \times (z \times z^{-1}) = y \times (z \times z^{-1}) \\ &\implies x \times 1_A = y \times 1_A \\ &\implies x = y \end{aligned}$$

□

Définition 2.2. Un corps est la donnée d'un triplet $(\mathbb{K}, +, \times)$ où \mathbb{K} est un ensemble, $+$ et \times sont deux l.c.i sur \mathbb{K} vérifiant les axiomes suivants:

- $(\mathbb{K}, +, \times)$ est un anneau commutatif
- (\mathbb{K}^*, \times) est un groupe abélien (de neutre noté $1_{\mathbb{K}}$).

Remarques 2.2. De manière équivalente, un corps est un anneau commutatif avec un élément neutre pour \times où tout élément non-nul est inversible.

3 Arithmétique des entiers

3.1 Rappels sur \mathbb{N} et \mathbb{Z}

À vérifier, certains théorèmes manque de consistance

Théorème 3.1. (propriétés de $+$ et \times sur \mathbb{N})

(a) $+$ et \times sont associative et commutative sur \mathbb{N}

(b) 0 est élément neutre pour $+$ tandis que 1 est neutre pour \times

(c) Il y a une distributivité de \times sur $+$

$$(d) \forall x, y, m \in \mathbb{N}, x + m = y + m \implies x = y$$

Théorème 3.2. (propriétés de \leq sur \mathbb{N})

1) (relation d'ordre total) $\forall m, n, p \in \mathbb{N}$

$$(a) n \leq n$$

$$(b) m \leq n \wedge n \leq m \iff m = n$$

$$(c) m \leq n \wedge n \leq p \implies m \leq p$$

$$(d) m \leq n \vee n \leq m$$

2) Les opérations $+$ et \times sont compatibles avec la relation d'ordre

$$\forall n, m, p \in \mathbb{N}, n \leq m \implies (n + p \leq m + p) \wedge (n \times p \leq m \times p)$$

3) $\forall n \in \mathbb{N}, 0 \leq n$

$$4) \forall n, m \in \mathbb{N}, \forall p \in \mathbb{N}^*, n \leq m \implies n \times p \leq m \times p$$

Théorème 3.3.

1. Toute partie finie de \mathbb{N} admet un plus grand élément.

2. Toute partie non vide de \mathbb{N} admet un plus petit élément.

3. Toute partie non vide et majorée de \mathbb{N} admet un plus grand élément.

4. \mathbb{N} n'admet pas de plus grand élément.

Théorème 3.4. (propriétés de $+$ et \times sur \mathbb{Z})

(a) $+$ et \times sont associative et commutative sur \mathbb{Z}

(b) 0 est élément neutre pour $+$ tandis que 1 est neutre pour \times

(c) Il y a une distributivité de \times sur $+$

(d) Tout $m \in \mathbb{Z}$ admet un symétrique (élément inverse), $-m \in \mathbb{Z}$ pour $+$

Théorème 3.5. (propriétés de \leq sur \mathbb{Z})

1) \leq est une relation d'ordre totale sur \mathbb{Z} .

2) Soient $n, m, p \in \mathbb{Z}$

$$(a) n \leq m \iff n + p \leq m + p$$

$$(b) \forall p \in \mathbb{Z}_+^*, n \leq m \iff np \leq mp$$

$$(c) \forall p \in \mathbb{Z}_-^*, n \leq m \iff mp \leq np$$

$$(d) \forall p \in \mathbb{Z}^*, m = n \iff mp = np$$

3.2 Arithmétique élémentaire dans \mathbb{Z}

Définition 3.1. Soient x et y dans \mathbb{Z} . On dit que x divise y s'il existe $k \in \mathbb{Z}$ tel que $y = kx$. La notation associée est $x \mid y$. x est un diviseur de y ou y est un multiple de x

Remarques 3.1. tout entier relatif divise 0.

0 divise uniquement 0.

si x est un diviseur de y alors $(-x)$ est un diviseur de y

1 et -1 sont les diviseurs de tout entier relatifs.

les diviseurs de 1 et -1 sont 1 et -1

$$\forall x, y \in \mathbb{N}^* \implies (x \mid y \implies x \leq y)$$

Définition 3.2. On dit que $p \in \mathbb{N}$, $p \geq 2$ est un nombre premier si les seuls diviseurs positifs de p sont 1 et p .

Remarques 3.2. Une autre définition est tout nombre qui a exactement 2 diviseurs.

Remarques 3.3. Pour vérifier qu'un nombre est premier, on peut regarder pour chaque $\forall k \in \mathbb{N}, k \leq \sqrt{p}$ si k divise p .

Définition 3.3. Soit $n \in \mathbb{Z}^*$, on appelle décomposition en facteurs premiers de n une écriture de la forme

$$n = c \text{multip}_i = c(p_1 \times \dots \times p_k)$$

où $c \in \{+, -\}$, $k \in \mathbb{N}$, p_1, \dots, p_k sont premiers

Proposition 3.1.

Tout $n \in \mathbb{Z}^*$ admet une décomposition en facteurs premier.

Démonstration 3.1.

Il suffit de le démontrer pour $n \in \mathbb{N}^*$ et $c = 1$ et pour les négatifs on se ramène à \mathbb{N}^* en posant $c = -1$

Démonstration par récurrence forte.

Initialisation: $n = 1$, on pose $c = 1, k = 0$, c'est un produit vide.

Initialisation: Soit $n \in \mathbb{N}^*, \forall d \leq n$, on ait une telle décomposition. Si $n + 1$ est premier, on pose $k = 1$ $P_1 = n + 1$. Si $n + 1$ n'est pas premier il admet un diviseur $d \in [2, n]$. Par hypothèse de récurrence $d = c \times p_1 \times \dots \times p_k$. De même $d' = \frac{n+1}{d} \in [2, n]$ $d' = p'_1 \times \dots \times p'_k$.

Donc $n + 1 = d \times d' = p_1 \times \dots \times p_k \times p'_1 \times \dots \times p'_k$

□

Corollaire: Tout entier $n \geq 2$ admet au moins un diviseur premier

Proposition 3.2.

L'ensemble des nombre premiers est infini.

Démonstration 3.2.

Supposons (par l'absurde) qu'il y ait un nombre fini de nombres premiers p_1, \dots, p_m

On pose $N = p_1 \times \dots \times p_m + 1$

Alors N admet un diviseur premier $p_i (i \in [1, m])$ i.e. $N = p_i N' \implies N = \text{multip}_j + 1 \implies p_i N' - p_i \text{multi}_{i \rightarrow j} p_j = 1 \implies p_i (N' - \text{multi}_{j \rightarrow i} p_j) = 1$

□

Théorème 3.6. Soient $a \in \mathbb{Z}, b \in \mathbb{N}^*$.

Alors il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}, a = bq + r$ avec $b > r \geq 0$

Démonstration 3.3.

Existence: Pour $a \in \mathbb{N}$, raisonnement par récurrence.

Initialisation: $a = 0$: On pose $q = 0$ et $r = 0 \implies 0 = b \times 0 + 0$

Hérédité: Si $a = bq + r$ avec $(b > r \geq 0)$

Alors $a + 1 = bq + (r + 1)$, C'est une division euclidienne lorsque $r + 1 < b \implies r < b - 1$

Lorsque $r = b - 1$

$a + 1 = bq + ((b - 1) + 1) = bq + b = b(q + 1) + 0$, C'est une division euclidienne.

Si $a < 0$ alors $(-a) > 0$ Donc $\exists(q, r) \in \mathbb{Z} \times \mathbb{N}$, $-a = bq + r \implies a = b \times (-q) + (-r)$ avec $(b > r \geq 0)$

Si $r = 0$, c'est une division euclidienne.

Sinon $-b < -r < 0 \implies 0 < -r + b < b$

Donc $a = b \times (-q) + (-r + b) - b = b \times (-q - 1) + (-r + b)$ C'est une division euclidienne.

Unicité: Si $a = bq + r$ et $a = bq' + r'$ avec $b > r, r' \geq 0$

Par soustraction: $0 = b(q - q') + r - r' \implies r' - r = b(q - q')$

$b - 1 \geq r' - r \geq -b - 1$ Donc $r' - r = 0 \implies r = r'$

Ainsi $bq + r = bq' + r' \implies bq = bq' \implies q = q'$

□

Définition 3.4. le **pgcd** de deux nombres $a, b \in \mathbb{Z}^*$ est le plus grand diviseur commun à a et b . Il est noté $PGCD(a, b)$ (ou encore $a \wedge b$)

On dit que a et b sont **premiers entre eux** si $PGCD(a, b) = 1$.

Le **ppcm** de deux nombres $a, b \in \mathbb{Z}^*$ est le plus petit multiple strictement positif commun à a et b . Il est noté $PPCM(a, b)$ (ou encore $a \vee b$)

Proposition 3.3.

$$\forall a, b \in \mathbb{Z}^*, PGCD(a, b) \times PPCM(a, b) = |ab|$$

Démonstration 3.4.

Si on remplace a et b par leurs valeurs absolues: $||a||b|| = |ab|$

Les multiples et les diviseurs de $|a|$ et de a sont les mêmes.

Donc $PGCD(a, b) = PGCD(|a|, |b|)$ et $PPCM(a, b) = PPCM(|a|, |b|)$

Ainsi il suffit de montrer le résultat pour $a, b \in \mathbb{N}^*$

On pose $d = PGCD(a, b)$

$\exists a', b' \in \mathbb{N}^*, a = da'$ et $b = db'$

$$\frac{ab}{d} = \frac{da'b}{d} = a'b \quad \frac{ab}{d} = \frac{adb'}{d} = ab'$$

□

Méthode 3.1.

L'algorithme d'Euclide:

Le PGCD peut se calculer avec l'algorithme d'Euclide:

1. (Eventuellement) remplacer a et b par $|a|$ et $|b|$

2. De manière récursive:

2.1 Calculer la division euclidienne de a par b : $a = bq + r$

2.2 Si $r \neq 0$: recommencer en remplaçant (a, b) par (b, r) Sinon sortir de la récursion

3. Le pgcd est le dernier reste non-nul calculé.

Proposition 3.4.

Si d est un diviseur commun à a et b alors $d \mid PGCD(a, b)$

Corollaire:

Le PGCD est aussi le plus grand diviseur commun au sens de la divisibilité.

Proposition 3.5.

Soient $a, b \in \mathbb{Z}^*$. Il existe $u, v \in \mathbb{Z}$ tels que
 $au + bv = \text{PGCD}(a, b)$

Lemme 3.1. Les sous-groupes de \mathbb{Z} sont les $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$ avec $n \in \mathbb{Z}$

Démonstration 3.5.

- 1) $\{nk \mid k \in \mathbb{Z}\}$ sous groupe de $(\mathbb{Z}, +)$ (cf TD1)
- 2) Soit H un sous groupe de $(\mathbb{Z}, +)$ alors $0 \in H$
 si $H = \{0\}$ alors $H = 0\mathbb{Z}$

□

Définition 3.5. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruences.

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ est un ensemble fini à n éléments.

Proposition 3.6.

Soient a, a', b, b' dans \mathbb{Z} tels que $a \equiv a'[n]$ et $b \equiv b'[n]$ Alors $a + b \equiv a' + b'[n]$

Démonstration 3.6.

$$\begin{aligned}(a - a') &= kn \text{ et } (b - b') = k'n \\(a + b) - (a' + b') &= a - a' + b - b' = kn + k'n = (k + k')n \\ \text{Donc } a + b &\equiv a' + b'[n]\end{aligned}$$

□

Définition 3.6. Soient $a, b \in \mathbb{Z}$. On pose dans $\mathbb{Z}/n\mathbb{Z}$: $\bar{a} + \bar{b} = \overline{a + b}$ et $\bar{a} \times \bar{b} = \overline{a \times b}$

Proposition 3.7.

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.
 $\bar{0}$ est l'élément neutre pour l'addition et $\bar{1}$ est l'élément neutre pour la multiplication.

Démonstration 3.7.

□

On peut faire des tables d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$

Exemple 3.1.

Lemme 3.2. Soient a et b dans \mathbb{Z} tels que $a \equiv b[n]$.

Pour tout $p \in \mathbb{N}^*$, $a^p \equiv b^p[n]$

Démonstration 3.8.

Dans $\mathbb{Z}/n\mathbb{Z}$ on veut montrer que $\overline{a^p} = \overline{b^p}$
 Or $\overline{a^p} = \overline{a \times \dots \times a} = \bar{a} \times \dots \times \bar{a} =$

□

Remarques 3.4. En revanche on n'a pas $p \equiv q[n] \implies a^p \equiv a^q[n]$

Théorème 3.7. $\{\mathbb{Z}/n\mathbb{Z}, +, \times\}$ est un corps si et seulement si n est premier.

Démonstration 3.9.

Dire que \bar{a} est inversible dans $\mathbb{Z}/n\mathbb{Z}$ c'est dire qu'il existe \bar{u} tel que $\bar{a}\bar{u} = \bar{1} \iff \exists u \in \mathbb{Z}, \exists k \in \mathbb{Z}, au = 1 + kn \iff \exists u \in \mathbb{Z}, \exists k' \in \mathbb{Z}, au + k'n = 1$ Cette équation a des solutions si n et m sont premier entre eux (bezout)

□

Théorème 3.8. Soient $n_1, n_2, \dots, n_k \in \mathbb{N}^*$, tels que $\forall i, n_i \geq 2$, avec les n_i deux à deux premiers entre eux. Alors pour tous $a_1, \dots, a_k \in \mathbb{Z}$, il existe $x \in \mathbb{Z}$, unique modulo $n := \Pi n_i$, tel que

$$\forall i \in [1, k], x \equiv a_i \text{ mod } n_i$$

Plus formellement, on a une application bijective,

$$\{\mathbb{Z}/n\mathbb{Z} \rightarrow (\mathbb{Z}/n_1\mathbb{Z}) \times \dots \times (\mathbb{Z}/n_k\mathbb{Z})\} \{x \text{ mod } n \mapsto (x \text{ mod } n_1, \dots, x \text{ mod } n_k)$$

Démonstration 3.10.

Montrons déjà que

$$\text{PGCD}(\Pi_{i=1}^{k-1} n_i, n_k) = 1$$

Soit p un facteur premier de $\Pi_{i=1}^{k-1} n_i$ Alors p divise l'un des n_i .

Comme n_i et n_k sont premier entre eux p ne divise pas n_k .

Donc $\Pi_{i=1}^{k-1} n_i$ et n_k n'ont pas de facteur premier en commun : leurs PGCD est 1.

De même pour $i \in [1; k]$ $\text{PGCD}(\Pi_{i \neq j} n_j, n_i) = 1$.

Ainsi on pose une relation de Bezout

$$(\Pi_{i \neq j} n_j) u_i + n_i v_i = 1$$

Soit $x_i := (\Pi_{j \neq i} n_j) u_i$

Alors $x_i \equiv \{0 \text{ mod } n_j \text{ si } j \neq i\} \{1 \text{ mod } n_i$

On pose $x = \sum_{i=1}^k a_i x_i$ alors $x \equiv a_i \text{ mod } n_i$

Si $y = x + qn$ alors $y = x + q \Pi_{j=1}^k n_j = x + q(\Pi_{j=1}^k n_j) n_i \equiv x \text{ mod } n_i \equiv x_i \text{ mod } n_i$

En particulier l'application ϕ est bien définie

D'après la première partie, ϕ est surjective.

Il nous reste à démontrer l'injectivité qui est équivalente à l'unicité modulo n .

Regardons les cardinaux $\text{Card}(\mathbb{Z}/n\mathbb{Z}) = n$

$$\text{Card}(\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}) = n_1 \times \dots \times n_k = n$$

Ainsi ϕ est injective

□

Remarques 3.5. ϕ est un "isomorphisme" d'anneau

Pour $k = 2$

$$\{x \equiv a_1 \text{ mod } n_1\} \{x = a_1 + k_1 n_1\} \{x \equiv a_2 \text{ mod } n_2\} \iff \{x = a_2 + k_2 n_2$$

$$\text{Alors } a_1 + k_1 n_1 = a_2 + k_2 n_2 \iff k_1 n_1 - k_2 n_2 = a_2 - a_1$$

c'est une équation diophotienne qu'on sait résoudre

Ensuite, il suffit de poser $x = a_1 + k_1 n_1$

4 Polynômes et Fractions rationnelles

Définition 4.1. Un *polynôme à coefficient dans \mathbb{k}* : une suite $A = (a_n)_{n \in \mathbb{N}}$ telle que $\exists N \in \mathbb{N}, \forall n > N, a_n = 0$.

On écrira souvent $A = a_0 + a_1X + a_2X^2 + \dots + a_NX^N = \sum_{i=0}^N a_iX^i = \sum_{i \in \mathbb{N}} a_iX^i = \sum a_iX^i$

$\mathbb{k}[X] = \{\text{polynômes à coefficients dans } \mathbb{k}\}$

polynôme nul : tous les coefficients sont nuls.

polynôme constant : $\forall i > 0, a_i = 0$ ($A = cX^0 = c$ où $c \in \mathbb{k}$)

monôme : polynôme de la forme

Symbole de Kronecker $\delta_{i,j} = 1$ si $i = j$ sinon 0

Propriétés 4.1.

Démonstration 4.1.

Soient $A = \sum (a_iX^i)$ et $B = \sum (b_iX^i)$

$C = A + B$ avec $c_i = a_i + b_i$

Si $i > \max(\deg A, \deg B)$ alors

□