Cours Algèbre 2–I: Divisibilité. Le quotient $\mathbb{Z}/n\mathbb{Z}$. Le théorème chinois

Andrei Teleman

Département de Mathématiques, Aix-Marseille Université

19 mars 2021

Table of Contents

Table of Contents

1

Théorème 1.1 (le théorème de division euclidienne)

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ telle que $n = mq + r$ et $0 \leqslant r < |m|$.

1

Théorème 1.1 (le théorème de division euclidienne)

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ telle que $n = mq + r$ et $0 \leqslant r < |m|$.

Les entiers q, r donnés par ce théorème s'appellent le quotient, respectivement le reste de la division euclidienne de n par m.

1

Théorème 1.1 (le théorème de division euclidienne)

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ telle que $n = mq + r$ et $0 \leqslant r < |m|$.

Les entiers q, r donnés par ce théorème s'appellent le quotient, respectivement le reste de la division euclidienne de n par m.

Si $r = 0$, on dit que n est divisible par m (soit que m divise n, m est un diviseur de n, ou n est un multiple de m) et on écrit $m|n$.

1

Théorème 1.1 (le théorème de division euclidienne)

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ telle que $n = mq + r$ et $0 \leqslant r < |m|$.

Les entiers q, r donnés par ce théorème s'appellent le quotient, respectivement le reste de la division euclidienne de n par m.

Si $r = 0$, on dit que n est divisible par m (soit que m divise n, m est un diviseur de n, ou n est un multiple de m) et on écrit $m|n$.

En posant

$$m\mathbb{Z} := \{mk |\ k \in \mathbb{Z}\},$$

on constate que $m|n$ si et seulement si $n \in m\mathbb{Z}$.

2

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Le pgcd et le ppcm du couple (m, n) sont définis par

$$\mathrm{pgcd}(m, n) := \max\left\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\right\},$$

$$\mathrm{ppcm}(m, n) := \min\left\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\right\}.$$

2

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Le pgcd et le ppcm du couple (m, n) sont définis par

$$\mathrm{pgcd}(m, n) := \max\left\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\right\},$$

$$\mathrm{ppcm}(m, n) := \min\left\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\right\}.$$

Important :

2

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Le pgcd et le ppcm du couple (m, n) sont définis par

$$\mathrm{pgcd}(m, n) := \max\left\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\right\},$$

$$\mathrm{ppcm}(m, n) := \min\left\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\right\}.$$

Important :

$\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\} \subset \mathbb{N}^*$ est non-vide et majoré.
$\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\} \subset \mathbb{N}^*$ est non-vide.

2

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Le pgcd et le ppcm du couple (m, n) sont définis par

$$\mathrm{pgcd}(m, n) := \max\left\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\right\},$$

$$\mathrm{ppcm}(m, n) := \min\left\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\right\}.$$

Important :

$\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\} \subset \mathbb{N}^*$ est non-vide et majoré.
$\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\} \subset \mathbb{N}^*$ est non-vide.

Conclusion : le pgcd et le ppcm d'un couple $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$ sont bien définis (existent).

Définition 1.2

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. On dit que m, n sont premiers entre eux si $\mathrm{pgcd}(m, n) = 1$.

Remarque 1.3

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$.

1. *Soit* $\mu \in \mathbb{Z}$ *un multiple commun de* (m, n). *Alors* $\mathrm{ppcm}(m, n)|\mu$.
2. *Soit* $\delta \in \mathbb{Z}^*$ *un diviseur commun de* (m, n). *Alors* $\delta|\mathrm{pgcd}(m, n)$.

Dém: (1) Soient q, r le quotient et le reste de la DE de μ par $\mathrm{ppcm}(m, n)$. On a q, $r \in \mathbb{Z}$ et $0 \leqslant r < \mathrm{ppcm}(m, n)$.

Remarque 1.3

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$.

1. *Soit* $\mu \in \mathbb{Z}$ *un multiple commun de* (m, n). *Alors* $\mathrm{ppcm}(m, n) | \mu$.
2. *Soit* $\delta \in \mathbb{Z}^*$ *un diviseur commun de* (m, n). *Alors* $\delta | \mathrm{pgcd}(m, n)$.

Dém: (1) Soient q, r le quotient et le reste de la DE de μ par $\mathrm{ppcm}(m, n)$. On a q, $r \in \mathbb{Z}$ et $0 \leqslant r < \mathrm{ppcm}(m, n)$.

Supposons par l'absurde que $\mathrm{ppcm}(m, n)$ ne divise pas μ.

Remarque 1.3

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$.

1. *Soit* $\mu \in \mathbb{Z}$ *un multiple commun de* (m, n). *Alors* $\mathrm{ppcm}(m, n) | \mu$.
2. *Soit* $\delta \in \mathbb{Z}^*$ *un diviseur commun de* (m, n). *Alors* $\delta | \mathrm{pgcd}(m, n)$.

Dém: (1) Soient q, r le quotient et le reste de la DE de μ par $\mathrm{ppcm}(m, n)$. On a q, $r \in \mathbb{Z}$ et $0 \leqslant r < \mathrm{ppcm}(m, n)$.

Supposons par l'absurde que $\mathrm{ppcm}(m, n)$ ne divise pas μ.

Alors $r \in \mathbb{N}^*$ et $r = \mu - q\,\mathrm{ppcm}(m, n)$ sera un multiple commun de m et n strictement positif et strictement inférieur à $\mathrm{ppcm}(m, n)$. Ceci contredit la définition de $\mathrm{ppcm}(m, n)$.

(2) m, n sont des multiples communs de $d := \mathrm{pgcd}(m, n)$ et δ d'où, d'après (1), on a $\mathrm{ppcm}(d, \delta)|m$ et $\mathrm{ppcm}(d, \delta)|n$.

(2) m, n sont des multiples communs de $d := \mathrm{pgcd}(m, n)$ et δ d'où, d'après (1), on a $\mathrm{ppcm}(d, \delta)|m$ et $\mathrm{ppcm}(d, \delta)|n$.

Donc $\mathrm{ppcm}(d, \delta)$ est un diviseur commun strictement positif de m et n.

(2) m, n sont des multiples communs de $d := \mathrm{pgcd}(m, n)$ et δ d'où, d'après (1), on a $\mathrm{ppcm}(d, \delta)|m$ et $\mathrm{ppcm}(d, \delta)|n$.

Donc $\mathrm{ppcm}(d, \delta)$ est un diviseur commun strictement positif de m et n.

Mais $\mathrm{ppcm}(d, \delta) \geqslant d$ et $d := \mathrm{pgcd}(m, n)$ est le diviseur commun *maximal* de m et n. Il en résulte $\mathrm{ppcm}(d, \delta) = d$, donc δ divise $d = \mathrm{pgcd}(m, n)$. ■

(2) m, n sont des multiples communs de $d := \mathrm{pgcd}(m, n)$ et δ d'où, d'après (1), on a $\mathrm{ppcm}(d, \delta)|m$ et $\mathrm{ppcm}(d, \delta)|n$.

Donc $\mathrm{ppcm}(d, \delta)$ est un diviseur commun strictement positif de m et n.

Mais $\mathrm{ppcm}(d, \delta) \geqslant d$ et $d := \mathrm{pgcd}(m, n)$ est le diviseur commun *maximal* de m et n. Il en résulte $\mathrm{ppcm}(d, \delta) = d$, donc δ divise $d = \mathrm{pgcd}(m, n)$. ■

Remarque 1.4

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $d = \mathrm{pgcd}(m, n)$. Posons $m' := m/d$, $n' := n/d$. Alors m', n' sont premiers entre eux.

Dém: Exercice. ■

4

Un entier positif $p \in \mathbb{N}^*$ est dit nombre premier si $p \geqslant 2$ et les seuls diviseurs positifs de p sont 1 et p.

4

Un entier positif $p \in \mathbb{N}^*$ est dit nombre premier si $p \geqslant 2$ et les seuls diviseurs positifs de p sont 1 et p.

On va noter par $\mathcal{P} \subset \mathbb{N}^*$ l'ensemble des nombres premiers.

Un entier positif $p \in \mathbb{N}^*$ est dit nombre premier si $p \geqslant 2$ et les seuls diviseurs positifs de p sont 1 et p.

On va noter par $\mathcal{P} \subset \mathbb{N}^*$ l'ensemble des nombres premiers.

Tout nombre naturel $n \in \mathbb{N}^*$ se décompose de manière unique comme produit de nombres premiers.

4

Un entier positif $p \in \mathbb{N}^*$ est dit nombre premier si $p \geqslant 2$ et les seuls diviseurs positifs de p sont 1 et p.

On va noter par $\mathcal{P} \subset \mathbb{N}^*$ l'ensemble des nombres premiers.

Tout nombre naturel $n \in \mathbb{N}^*$ se décompose de manière unique comme produit de nombres premiers.

Plus précisément, pour tout $p \in \mathcal{P}$ nous avons une application $v_p : \mathbb{N}^* \to \mathbb{N}$ telle que pour tout $n \in \mathbb{N}^*$ on a une décomposition

$$n = \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \neq 0}} p^{v_p(n)}.$$

4

Un entier positif $p \in \mathbb{N}^*$ est dit nombre premier si $p \geqslant 2$ et les seuls diviseurs positifs de p sont 1 et p.

On va noter par $\mathcal{P} \subset \mathbb{N}^*$ l'ensemble des nombres premiers.

Tout nombre naturel $n \in \mathbb{N}^*$ se décompose de manière unique comme produit de nombres premiers.

Plus précisément, pour tout $p \in \mathcal{P}$ nous avons une application $v_p : \mathbb{N}^* \to \mathbb{N}$ telle que pour tout $n \in \mathbb{N}^*$ on a une décomposition

$$n = \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \neq 0}} p^{v_p(n)}.$$

Donc $v_p(n) = 0$ si p ne divise pas n et est égale à la puissance de p dans la factorisation de n en nombres premiers, si p divise n. Plus précisément : $v_p(n) = \max\{k \in \mathbb{N} |\ p^k | n\}$.

Remarque 1.5

Soient $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors $m|n$ si et seulement si pour tout $p \in \mathcal{P}$ on a $v_p(m) \leqslant v_p(n)$.

Remarque 1.5

Soient $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors $m|n$ si et seulement si pour tout $p \in \mathcal{P}$ on a $v_p(m) \leqslant v_p(n)$.

Remarque 1.6

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors

1. $$\operatorname{pgcd}(m, n) = \prod_{\substack{p \in \mathcal{P} \\ v_p(m) \neq 0 \text{ et } v_p(n) \neq 0}} p^{\min(v_p(|m|), v_p(|n|))},$$

Remarque 1.5

Soient $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors $m|n$ si et seulement si pour tout $p \in \mathcal{P}$ on a $v_p(m) \leqslant v_p(n)$.

Remarque 1.6

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors

1. $$\operatorname{pgcd}(m, n) = \prod_{\substack{p \in \mathcal{P} \\ v_p(m) \neq 0 \text{ et } v_p(n) \neq 0}} p^{\min(v_p(|m|), v_p(|n|))},$$
$$\operatorname{ppcm}(m, n) = \prod_{\substack{p \in \mathcal{P} \\ v_p(m) \neq 0 \text{ ou } v_p(n) \neq 0}} p^{\max(v_p(|m|), v_p(|n|))}.$$

Remarque 1.5

Soient $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors $m|n$ si et seulement si pour tout $p \in \mathcal{P}$ on a $v_p(m) \leqslant v_p(n)$.

Remarque 1.6

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors

1. $$\operatorname{pgcd}(m, n) = \prod_{\substack{p \in \mathcal{P} \\ v_p(m) \neq 0 \text{ et } v_p(n) \neq 0}} p^{\min(v_p(|m|), v_p(|n|))},$$
$$\operatorname{ppcm}(m, n) = \prod_{\substack{p \in \mathcal{P} \\ v_p(m) \neq 0 \text{ ou } v_p(n) \neq 0}} p^{\max(v_p(|m|), v_p(|n|))}.$$
2. *On a l'identité* $|mn| = \operatorname{pgcd}(m, n) \operatorname{ppcm}(m, n)$.

Dém: Exercice. Pour démontrer (3)(b) remarquer d'abord que

$$\operatorname{pgcd}(m,n) = \prod_{\substack{p\in\mathcal{P} \\ v_p(m)\neq 0 \text{ ou } v_p(n)\neq 0}} p^{\min(v_p(|m|),v_p(|n|))}.$$

Utiliser l'identité $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$. ■

Théorème 1.7 (L'égalité de Bézout)

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors il existe un couple $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que

$$\operatorname{pgcd}(m, n) = um + vn\,.$$

Théorème 1.7 (L'égalité de Bézout)

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors il existe un couple $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que

$$\operatorname{pgcd}(m, n) = um + vn\,.$$

En utilisant la notation $m\mathbb{Z} + n\mathbb{Z} := \{um + vn |\ (u, v) \in \mathbb{Z} \times \mathbb{Z}\}$, le théorème de Bézout dévient

$$\operatorname{pgcd}(m, n) \in m\mathbb{Z} + n\mathbb{Z}\,.$$

Théorème 1.7 (L'égalité de Bézout)

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors il existe un couple $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que

$$\operatorname{pgcd}(m, n) = um + vn\,.$$

En utilisant la notation $m\mathbb{Z} + n\mathbb{Z} := \{um + vn |\ (u, v) \in \mathbb{Z} \times \mathbb{Z}\}$, le théorème de Bézout dévient

$$\operatorname{pgcd}(m, n) \in m\mathbb{Z} + n\mathbb{Z}\,.$$

Dém: (de l'égalité de Bézout) Posons :

$$\mathcal{E} := \{k \in \mathbb{N}^* |\ \exists (u, v) \in \mathbb{Z}\times\mathbb{Z} \text{ tel que } k = um+vn\} = (m\mathbb{Z}+n\mathbb{Z})\cap\mathbb{N}^*\,.$$

Théorème 1.7 (L'égalité de Bézout)

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors il existe un couple $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que

$$\operatorname{pgcd}(m, n) = um + vn\,.$$

En utilisant la notation $m\mathbb{Z} + n\mathbb{Z} := \{um + vn |\ (u, v) \in \mathbb{Z} \times \mathbb{Z}\}$, le théorème de Bézout dévient

$$\operatorname{pgcd}(m, n) \in m\mathbb{Z} + n\mathbb{Z}\,.$$

Dém: (de l'égalité de Bézout) Posons :

$\mathcal{E} := \{k \in \mathbb{N}^* |\ \exists (u, v) \in \mathbb{Z}\times\mathbb{Z}$ tel que $k = um+vn\} = (m\mathbb{Z}+n\mathbb{Z})\cap\mathbb{N}^*$.

$\mathbb{N}^* \supset \mathcal{E}$ est non-vide (pourquoi ?), donc $\delta := \min(\mathcal{E})$ existe.

$$\delta \in \mathcal{E} \Rightarrow \delta = u_\delta m + v_\delta n \text{ avec } (u_\delta, v_\delta) \in \mathbb{Z} \times \mathbb{Z}.$$

$\delta \in \mathcal{E} \Rightarrow \delta = u_\delta m + v_\delta n$ avec $(u_\delta, v_\delta) \in \mathbb{Z} \times \mathbb{Z}$.

Nous allons montrer que $\delta = \mathrm{pgcd}(m, n)$. Il suffit de montrer :

(a) δ est un diviseur commun de m et n.

(b) Tout diviseur commun de m et n est un diviseur de δ.

$\delta \in \mathcal{E} \Rightarrow \delta = u_\delta m + v_\delta n$ avec $(u_\delta, v_\delta) \in \mathbb{Z} \times \mathbb{Z}$.

Nous allons montrer que $\delta = \mathrm{pgcd}(m, n)$. Il suffit de montrer :

(a) δ est un diviseur commun de m et n.

(b) Tout diviseur commun de m et n est un diviseur de δ.

Pour (a) appliquons le TDE aux couples (δ, m) et (δ, n). On obtient

$$m = \delta q + r, \ \ n = \delta q' + r' \ ,$$

où $(q, q') \in \mathbb{Z} \times \mathbb{Z}$, $0 \leqslant r < \delta$, $0 \leqslant r' < \delta$.

$\delta \in \mathcal{E} \Rightarrow \delta = u_\delta m + v_\delta n$ avec $(u_\delta, v_\delta) \in \mathbb{Z} \times \mathbb{Z}$.

Nous allons montrer que $\delta = \operatorname{pgcd}(m, n)$. Il suffit de montrer :

(a) δ est un diviseur commun de m et n.

(b) Tout diviseur commun de m et n est un diviseur de δ.

Pour (a) appliquons le TDE aux couples (δ, m) et (δ, n). On obtient

$$m = \delta q + r, \ \ n = \delta q' + r' \, ,$$

où $(q, q') \in \mathbb{Z} \times \mathbb{Z}$, $0 \leqslant r < \delta$, $0 \leqslant r' < \delta$.

Nous montrons que $r = r' = 0$. Si, par l'absurde, $r > 0$ on aura

$$\mathbb{N}^* \ni r = m - q\delta = m - q(u_\delta m + v_\delta n) = (1 - qu_\delta)m + (-qv_\delta)n \, ,$$

qui, évidemment, est un élément de $\mathcal{E}$.

$\delta \in \mathcal{E} \Rightarrow \delta = u_\delta m + v_\delta n$ avec $(u_\delta, v_\delta) \in \mathbb{Z} \times \mathbb{Z}$.

Nous allons montrer que $\delta = \operatorname{pgcd}(m, n)$. Il suffit de montrer :

(a) δ est un diviseur commun de m et n.

(b) Tout diviseur commun de m et n est un diviseur de δ.

Pour (a) appliquons le TDE aux couples (δ, m) et (δ, n). On obtient

$$m = \delta q + r, \ \ n = \delta q' + r' \, ,$$

où $(q, q') \in \mathbb{Z} \times \mathbb{Z}$, $0 \leqslant r < \delta$, $0 \leqslant r' < \delta$.

Nous montrons que $r = r' = 0$. Si, par l'absurde, $r > 0$ on aura

$$\mathbb{N}^* \ni r = m - q\delta = m - q(u_\delta m + v_\delta n) = (1 - qu_\delta)m + (-qv_\delta)n \, ,$$

qui, évidemment, est un élément de $\mathcal{E}$.

Mais $r < \delta$, ce qui contredit la définition de δ. Il en résulte $r = 0$.

Pareil $r' = 0$. Donc $r = r' = 0 \Rightarrow (\delta | m) \wedge (\delta | n)$.

Pareil $r' = 0$. Donc $r = r' = 0 \Rightarrow (\delta | m) \wedge (\delta | n)$.

Pour (b) soit $d \in \mathbb{Z}^*$ diviseur commun de m et n. Alors $d | u_\delta m$ et $d | v_\delta n$, donc $d | (u_\delta m + v_\delta n) = \delta$. ■

Pareil $r' = 0$. Donc $r = r' = 0 \Rightarrow (\delta | m) \wedge (\delta | n)$.

Pour (b) soit $d \in \mathbb{Z}^*$ diviseur commun de m et n. Alors $d | u_\delta m$ et $d | v_\delta n$, donc $d | (u_\delta m + v_\delta n) = \delta$. ■

Il existe un algorithme simple qui permet de trouver à la fois $\mathrm{pgcd}(m, n)$ et un couple (u, v) tel que $\mathrm{pgcd}(m, n) = um + vn$: l'algorithme d'Euclid.

Pareil $r' = 0$. Donc $r = r' = 0 \Rightarrow (\delta | m) \wedge (\delta | n)$.

Pour (b) soit $d \in \mathbb{Z}^*$ diviseur commun de m et n. Alors $d | u_\delta m$ et $d | v_\delta n$, donc $d | (u_\delta m + v_\delta n) = \delta$. ■

Il existe un algorithme simple qui permet de trouver à la fois $\mathrm{pgcd}(m, n)$ et un couple (u, v) tel que $\mathrm{pgcd}(m, n) = um + vn$: l'algorithme d'Euclid.

1. La DE de n par m nous donne $n = q_1 m + r_1$ avec $q_1 \in \mathbb{Z}$ et $0 \leqslant r_1 < |m|$. On pose la question : est-ce que le reste r_1 est nul ? Si oui, on a $\mathrm{pgcd}(m, n) = |m|$ et on arrête l'algorithme. Sinon, on passe à l'étape suivante.

Pareil $r' = 0$. Donc $r = r' = 0 \Rightarrow (\delta | m) \wedge (\delta | n)$.

Pour (b) soit $d \in \mathbb{Z}^*$ diviseur commun de m et n. Alors $d | u_\delta m$ et $d | v_\delta n$, donc $d | (u_\delta m + v_\delta n) = \delta$. ■

Il existe un algorithme simple qui permet de trouver à la fois $\mathrm{pgcd}(m, n)$ et un couple (u, v) tel que $\mathrm{pgcd}(m, n) = um + vn$: l'algorithme d'Euclid.

1. La DE de n par m nous donne $n = q_1 m + r_1$ avec $q_1 \in \mathbb{Z}$ et $0 \leqslant r_1 < |m|$. On pose la question : est-ce que le reste r_1 est nul ? Si oui, on a $\mathrm{pgcd}(m, n) = |m|$ et on arrête l'algorithme. Sinon, on passe à l'étape suivante.
2. On remarque $r_1 = n - q_1 m \in m\mathbb{Z} + n\mathbb{Z}$, on remplace le couple (m, n) par (r_1, m). La DE de m par r_1 nous donne $m = q_2 r_1 + r_2$ avec $q_2 \in \mathbb{Z}$ et $0 \leqslant r_2 < r_1$ et on repose la question (1) pour le nouveau reste.

Si oui, on a $\mathrm{pgcd}(m, n) = r_1$ et on arrête l'algorithme. Sinon, on passe à l'étape suivante.

Si oui, on a $\operatorname{pgcd}(m, n) = r_1$ et on arrête l'algorithme. Sinon, on passe à l'étape suivante.

3. On remarque que

$$r_2 = m - q_2 r_1 = m - q_2(n - q_1 m) \in m\mathbb{Z} + n\mathbb{Z}\,,$$

on remplace le couple (r_1, m) par (r_2, r_1) et on continue de la même manière.

Si oui, on a $\mathrm{pgcd}(m, n) = r_1$ et on arrête l'algorithme. Sinon, on passe à l'étape suivante.

3. On remarque que

$$r_2 = m - q_2 r_1 = m - q_2(n - q_1 m) \in m\mathbb{Z} + n\mathbb{Z}\,,$$

on remplace le couple (r_1, m) par (r_2, r_1) et on continue de la même manière.

$\mathrm{pgcd}(m, n)$ coïncide soit avec $|m|$ si m divise n, soit avec le dernier reste *non-nul* dans la suite finie de divisions euclidiennes obtenues de cette manière.

Si oui, on a $\mathrm{pgcd}(m, n) = r_1$ et on arrête l'algorithme. Sinon, on passe à l'étape suivante.

3. On remarque que

$$r_2 = m - q_2 r_1 = m - q_2(n - q_1 m) \in m\mathbb{Z} + n\mathbb{Z}\,,$$

on remplace le couple (r_1, m) par (r_2, r_1) et on continue de la même manière.

$\mathrm{pgcd}(m, n)$ coïncide soit avec $|m|$ si m divise n, soit avec le dernier reste *non-nul* dans la suite finie de divisions euclidiennes obtenues de cette manière.

Par récurrence on obtient des relations de la forme $r_k = u_k m + v_k n$, en particulier une décomposition explicite de cette forme pour le dernier reste non-nul, qui coïncide avec $\mathrm{pgcd}(m, n)$.

Exemple 1.1

En appliquant l'algorithme d'Euclid pour le calcul de $\mathrm{pgcd}(8, 135)$, on obtient successivement

$$135 = 16 \cdot 8 + 7\,,\ r_1 = 7 = (-16) \cdot 8 + 135\,,$$

$$8 = 1 \cdot 7 + 1\,,\quad r_2 = 1 = 1 \cdot 8 - 1 \cdot 7 = 1 \cdot 8 - 1 \cdot ((-16) \cdot 8 + 135)$$

$$= 17 \cdot 8 + (-1) \cdot 135\,,$$

et $r_3 = 0$. Donc $\mathrm{pgcd}(8, 135) = r_2 = 1 = 17 \cdot 8 + (-1) \cdot 135$.

Exemple 1.1

En appliquant l'algorithme d'Euclid pour le calcul de $\mathrm{pgcd}(8, 135)$, on obtient successivement

$$135 = 16 \cdot 8 + 7\,,\ r_1 = 7 = (-16) \cdot 8 + 135\,,$$

$$8 = 1 \cdot 7 + 1\,,\quad r_2 = 1 = 1 \cdot 8 - 1 \cdot 7 = 1 \cdot 8 - 1 \cdot ((-16) \cdot 8 + 135)$$

$$= 17 \cdot 8 + (-1) \cdot 135\,,$$

et $r_3 = 0$. Donc $\mathrm{pgcd}(8, 135) = r_2 = 1 = 17 \cdot 8 + (-1) \cdot 135$.

Corollaire 1.8 (Le théorème de Bézout)

Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors m, n sont premiers entre eux si et seulement s'il existe un couple $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $um + vn = 1$.

L'implication

$$\big(\exists (u, v) \in \mathbb{Z} \times \mathbb{Z},\ um + vn = 1\big) \Rightarrow \operatorname{pgcd}(m, n) = 1$$

est évidente, parce que tout diviseur commun de m et n est un diviseur de $um + vn$. L'implication dans le sens contraire est un cas spécial de l'égalité de Bézout.

L'implication

$$\big(\exists (u, v) \in \mathbb{Z} \times \mathbb{Z},\ um + vn = 1\big) \Rightarrow \operatorname{pgcd}(m, n) = 1$$

est évidente, parce que tout diviseur commun de m et n est un diviseur de $um + vn$. L'implication dans le sens contraire est un cas spécial de l'égalité de Bézout.

Corollaire 1.9 (Le théorème de Gauss dans $\mathbb{Z}$)

Soient $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $x \in \mathbb{Z}$. Si n divise le produit mx et m, n sont premiers entre eux, alors n divise x.

L'implication

$$\big(\exists (u, v) \in \mathbb{Z} \times \mathbb{Z},\ um + vn = 1\big) \Rightarrow \operatorname{pgcd}(m, n) = 1$$

est évidente, parce que tout diviseur commun de m et n est un diviseur de $um + vn$. L'implication dans le sens contraire est un cas spécial de l'égalité de Bézout.

Corollaire 1.9 (Le théorème de Gauss dans $\mathbb{Z}$)

Soient $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $x \in \mathbb{Z}$. Si n divise le produit mx et m, n sont premiers entre eux, alors n divise x.

Dém: Soit $k \in \mathbb{Z}$ tel que $mx = kn$ et soit $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $um + vn = 1$.

L'implication

$$\big(\exists (u, v) \in \mathbb{Z} \times \mathbb{Z},\ um + vn = 1\big) \Rightarrow \operatorname{pgcd}(m, n) = 1$$

est évidente, parce que tout diviseur commun de m et n est un diviseur de $um + vn$. L'implication dans le sens contraire est un cas spécial de l'égalité de Bézout.

Corollaire 1.9 (Le théorème de Gauss dans $\mathbb{Z}$)

Soient $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$ et $x \in \mathbb{Z}$. Si n divise le produit mx et m, n sont premiers entre eux, alors n divise x.

Dém: Soit $k \in \mathbb{Z}$ tel que $mx = kn$ et soit $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $um + vn = 1$. On obtient

$$x = 1 \cdot x = (um + vn)x = umx + vnx = ukn + vnx = n(uk + vx)$$

avec $(uk + vx) \in \mathbb{Z}$, donc n divise x. ■

13

Démonstration alternative en utilisant les factorisations en nombres premiers de m, n et x :

13

Démonstration alternative en utilisant les factorisations en nombres premiers de m, n et x :

$n|(mx) \Rightarrow$ tout nombre premier qui intervient dans la factorisation de n doit intervenir dans la factorisation de mx (donc dans la factorisation de x) avec un exposant supérieur.

Démonstration alternative en utilisant les factorisations en nombres premiers de m, n et x :

$n|(mx) \Rightarrow$ tout nombre premier qui intervient dans la factorisation de n doit intervenir dans la factorisation de mx (donc dans la factorisation de x) avec un exposant supérieur.

Corollaire 1.10

Soient m, $n \in \mathbb{Z}^*$ `premiers entre eux`*. Pour un couple $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ les deux conditions suivantes sont équivalentes :*

1. $mx = ny$.
2. *Il existe $k \in \mathbb{Z}$ tel que $x = kn$ et $y = km$.*

Démonstration alternative en utilisant les factorisations en nombres premiers de m, n et x :

$n|(mx) \Rightarrow$ tout nombre premier qui intervient dans la factorisation de n doit intervenir dans la factorisation de mx (donc dans la factorisation de x) avec un exposant supérieur.

Corollaire 1.10

Soient m, $n \in \mathbb{Z}^*$ `premiers entre eux`*. Pour un couple $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ les deux conditions suivantes sont équivalentes :*

1. $mx = ny$.
2. *Il existe $k \in \mathbb{Z}$ tel que $x = kn$ et $y = km$.*

Dém: 2.⇒1. est évidente. Pour 1.⇒2. : L'égalité $mx = ny$ implique $n|(mx)$, donc (Gauss) $n|x$. Soit $k \in \mathbb{Z}$ tel que $x = kn$.

Démonstration alternative en utilisant les factorisations en nombres premiers de m, n et x :

$n|(mx) \Rightarrow$ tout nombre premier qui intervient dans la factorisation de n doit intervenir dans la factorisation de mx (donc dans la factorisation de x) avec un exposant supérieur.

Corollaire 1.10

Soient $m, n \in \mathbb{Z}^*$ `premiers entre eux`*. Pour un couple $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ les deux conditions suivantes sont équivalentes :*

1. $mx = ny$.
2. *Il existe $k \in \mathbb{Z}$ tel que $x = kn$ et $y = km$.*

Dém: 2.⇒1. est évidente. Pour 1.⇒2. : L'égalité $mx = ny$ implique $n|(mx)$, donc (Gauss) $n|x$. Soit $k \in \mathbb{Z}$ tel que $x = kn$. On a $mkn = ny \overset{n\neq 0}{\Longrightarrow} y = km$. ■

Une équation diophantienne est une équation polynomiale à coefficients entiers (à une ou plusieurs inconnues), dont les inconnues sont aussi des entiers.

Une équation diophantienne est une équation polynomiale à coefficients entiers (à une ou plusieurs inconnues), dont les inconnues sont aussi des entiers.

Soit $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$. Nous allons étudier l'équation diophantienne

$$ax + by = c, \tag{1}$$

donc nous allons déterminer l'ensemble des solutions entières

$$S_{a,b,c} := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} |\ ax + by = c\}$$

de cette équation.

Une équation diophantienne est une équation polynomiale à coefficients entiers (à une ou plusieurs inconnues), dont les inconnues sont aussi des entiers.

Soit $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$. Nous allons étudier l'équation diophantienne

$$ax + by = c, \tag{1}$$

donc nous allons déterminer l'ensemble des solutions entières

$$S_{a,b,c} := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} |\ ax + by = c\}$$

de cette équation.
Posons $d := \operatorname{pgcd}(a, b)$ et soit $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $ua + vb = d$.
On peut écrire $a = da'$, $b = db'$ avec a', $b' \in \mathbb{Z}^*$ premiers entres eux. Pourquoi ?

Proposition 1.11

Soit $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$.

1. *Si* d *ne divise pas* c, *alors* $S_{a,b,c} = \emptyset$, *donc l'équation diophantienne (1) n'admet aucune solution.*

Proposition 1.11

Soit $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$.

1. *Si* d *ne divise pas* c, *alors* $S_{a,b,c} = \emptyset$, *donc l'équation diophantienne (1) n'admet aucune solution.*
2. *Supposons* $d|c$ *et soit* $q := \frac{c}{d}$. *Alors*
   1. $(qu, qv) \in S_{a,b,c}$, *c'est à dire* (qu, qv) *est une solution particulière de l'équation diophantienne (1).*

Proposition 1.11

Soit $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$.

1. *Si d ne divise pas c, alors $S_{a,b,c} = \emptyset$, donc l'équation diophantienne (1) n'admet aucune solution.*
2. *Supposons $d|c$ et soit $q := \frac{c}{d}$. Alors*
   1. *$(qu, qv) \in S_{a,b,c}$, c'est à dire (qu, qv) est une solution particulière de l'équation diophantienne (1).*
   2. *L'ensemble $S_{a,b,c}$ des solutions de l'équation diophantienne (1) s'écrit :*

$$S_{a,b,c} = \{(qu + kb', qv - ka') |\ k \in \mathbb{Z}\}.$$

Proposition 1.11

Soit $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$.

1. *Si d ne divise pas c, alors $S_{a,b,c} = \emptyset$, donc l'équation diophantienne (1) n'admet aucune solution.*
2. *Supposons $d|c$ et soit $q := \frac{c}{d}$. Alors*
   1. *$(qu, qv) \in S_{a,b,c}$, c'est à dire (qu, qv) est une solution particulière de l'équation diophantienne (1).*
   2. *L'ensemble $S_{a,b,c}$ des solutions de l'équation diophantienne (1) s'écrit :*

$$S_{a,b,c} = \{(qu + kb', qv - ka') |\ k \in \mathbb{Z}\}.$$

Dém: 1. Si $S_{a,b,c} \neq \emptyset$ alors il existe une solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, donc

$$c = ax + by = d(a'x + b'y) \Rightarrow d|c\,.$$

2. En multipliant l'égalité $ua + vb = d$ par q on obtient $a(uq) + b(vq) = dq = c$, donc $(qu, qv) \in S_{a,b,c}$.

2. En multipliant l'égalité $ua + vb = d$ par q on obtient $a(uq) + b(vq) = dq = c$, donc $(qu, qv) \in S_{a,b,c}$.

Soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Nous avons $(x, y) \in S_{a,b,c}$ si et seulement si

$$ax+by = c \Leftrightarrow ax+by-(aqu+bqv) = 0 \Leftrightarrow a(x-qu)+b(y-qv) = 0$$
$$\Leftrightarrow a'(x - qu) + b'(y - qv) = 0 \Leftrightarrow a'(x - qu) = b'(qv - y).$$

2. En multipliant l'égalité $ua + vb = d$ par q on obtient $a(uq) + b(vq) = dq = c$, donc $(qu, qv) \in S_{a,b,c}$.

Soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Nous avons $(x, y) \in S_{a,b,c}$ si et seulement si

$$ax+by = c \Leftrightarrow ax+by-(aqu+bqv) = 0 \Leftrightarrow a(x-qu)+b(y-qv) = 0$$

$$\Leftrightarrow a'(x - qu) + b'(y - qv) = 0 \Leftrightarrow a'(x - qu) = b'(qv - y).$$

D'après le corollaire 1.10 l'égalité $a'(x - qu) = b'(qv - y)$ est équivalente à la condition

$$\exists k \in \mathbb{Z},\ \left((x - qu = kb') \wedge (qv - y = ka')\right),$$

2. En multipliant l'égalité $ua + vb = d$ par q on obtient $a(uq) + b(vq) = dq = c$, donc $(qu, qv) \in S_{a,b,c}$.

Soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Nous avons $(x, y) \in S_{a,b,c}$ si et seulement si

$$ax+by = c \Leftrightarrow ax+by-(aqu+bqv) = 0 \Leftrightarrow a(x-qu)+b(y-qv) = 0$$

$$\Leftrightarrow a'(x - qu) + b'(y - qv) = 0 \Leftrightarrow a'(x - qu) = b'(qv - y).$$

D'après le corollaire 1.10 l'égalité $a'(x - qu) = b'(qv - y)$ est équivalente à la condition

$$\exists k \in \mathbb{Z},\ \left((x - qu = kb') \wedge (qv - y = ka')\right),$$

donc à la condition

$$\exists k \in \mathbb{Z},\ \left((x = qu + kb') \wedge (y = qv - ka')\right),$$

2. En multipliant l'égalité $ua + vb = d$ par q on obtient $a(uq) + b(vq) = dq = c$, donc $(qu, qv) \in S_{a,b,c}$.

Soit $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Nous avons $(x, y) \in S_{a,b,c}$ si et seulement si

$$ax+by = c \Leftrightarrow ax+by-(aqu+bqv) = 0 \Leftrightarrow a(x-qu)+b(y-qv) = 0$$

$$\Leftrightarrow a'(x - qu) + b'(y - qv) = 0 \Leftrightarrow a'(x - qu) = b'(qv - y).$$

D'après le corollaire 1.10 l'égalité $a'(x - qu) = b'(qv - y)$ est équivalente à la condition

$$\exists k \in \mathbb{Z},\ \left((x - qu = kb') \wedge (qv - y = ka')\right),$$

donc à la condition

$$\exists k \in \mathbb{Z},\ \left((x = qu + kb') \wedge (y = qv - ka')\right),$$

qui est équivalente à $(x, y) \in \{(qu + kb', qv - ka') |\ k \in \mathbb{Z}\}$.

Table of Contents

Définition 2.1

Soit A un ensemble. Une relation sur A est un sous-ensemble $R \subset A \times A$. On convient d'écrire $x\,R\,y$ au lieu de $(x, y) \in R$. Si $x\,R\,y$ on dit que x est en relation R avec y.

Définition 2.1

Soit A un ensemble. Une relation sur A est un sous-ensemble $R \subset A \times A$. On convient d'écrire $x\,R\,y$ au lieu de $(x, y) \in R$. Si $x\,R\,y$ on dit que x est en relation R avec y.
Une relation R sur A est dite relation d'équivalence si

1. *R est réflexive, i.e.*
$$\forall x \in A,\ x\,R\,x.$$

Définition 2.1

Soit A un ensemble. Une relation sur A est un sous-ensemble $R \subset A \times A$. On convient d'écrire $x\,R\,y$ au lieu de $(x, y) \in R$. Si $x\,R\,y$ on dit que x est en relation R avec y.
Une relation R sur A est dite relation d'équivalence si

1. *R est réflexive, i.e.*
$$\forall x \in A,\ x\,R\,x.$$
2. *R est symétrique, i.e.*
$$\forall (x, y) \in A \times A\ (x\,R\,y \Rightarrow y\,R\,x).$$

Définition 2.1

Soit A un ensemble. Une relation sur A est un sous-ensemble $R \subset A \times A$. On convient d'écrire $x\,R\,y$ au lieu de $(x, y) \in R$. Si $x\,R\,y$ on dit que x est en relation R avec y.
Une relation R sur A est dite relation d'équivalence si

1. *R est réflexive, i.e.*
$$\forall x \in A,\ x\,R\,x.$$
2. *R est symétrique, i.e.*
$$\forall (x, y) \in A \times A\ (x\,R\,y \Rightarrow y\,R\,x).$$
3. *R est transitive, i.e.*
$$\forall (x, y, z) \in A \times A \times A\ ((x\,R\,y) \wedge (y\,R\,z) \Rightarrow x\,R\,z).$$

Définition 2.2

Deux ensembles C, D sont dits disjoints si $C \cap D = \emptyset$.

Soit A un ensemble et soit $\mathcal{P}(A)$ l'ensemble des parties de A. Pour un *sous-ensemble* $\mathcal{Q} \subset \mathcal{P}(A)$ (donc pour un ensemble de parties de A) nous définissions

$$\bigcup_{C \in \mathcal{Q}} C := \{x \in A |\ \exists C \in \mathcal{Q},\ x \in C\},$$

Définition 2.2

Deux ensembles C, D sont dits disjoints si $C \cap D = \emptyset$.

Soit A un ensemble et soit $\mathcal{P}(A)$ l'ensemble des parties de A. Pour un *sous-ensemble* $\mathcal{Q} \subset \mathcal{P}(A)$ (donc pour un ensemble de parties de A) nous définissions

$$\bigcup_{C \in \mathcal{Q}} C := \{x \in A |\ \exists C \in \mathcal{Q},\ x \in C\},$$

$$\bigcap_{C \in \mathcal{Q}} C := \{x \in A |\ \forall C \in \mathcal{Q},\ x \in C\}.$$

Définition 2.3

Soit A un ensemble. Une partition (non-indexée) de A est un sous-ensemble $\mathcal{Q} \subset \mathcal{P}(A)$ tel que les conditions suivantes soient vérifiées :

Définition 2.3

Soit A un ensemble. Une partition (non-indexée) de A est un sous-ensemble $\mathcal{Q} \subset \mathcal{P}(A)$ tel que les conditions suivantes soient vérifiées :

1. $$\forall C \in \mathcal{Q},\ C \neq \emptyset.$$

Définition 2.3

Soit A un ensemble. Une partition (non-indexée) de A est un sous-ensemble $\mathcal{Q} \subset \mathcal{P}(A)$ tel que les conditions suivantes soient vérifiées :

1. $$\forall C \in \mathcal{Q},\ C \neq \emptyset.$$
2. $$\bigcup_{C \in \mathcal{Q}} C = A.$$

Définition 2.3

Soit A un ensemble. Une partition (non-indexée) de A est un sous-ensemble $\mathcal{Q} \subset \mathcal{P}(A)$ tel que les conditions suivantes soient vérifiées :

1. $$\forall C \in \mathcal{Q},\ C \neq \emptyset.$$
2. $$\bigcup_{C \in \mathcal{Q}} C = A.$$
3. $$\forall C \in \mathcal{Q}\ \forall C' \in \mathcal{Q}\ \left(C \neq C' \Rightarrow C \cap C' = \emptyset\right).$$

Définition 2.3

Soit A un ensemble. Une partition (non-indexée) de A est un sous-ensemble $\mathcal{Q} \subset \mathcal{P}(A)$ tel que les conditions suivantes soient vérifiées :

1. $$\forall C \in \mathcal{Q},\ C \neq \emptyset.$$
2. $$\bigcup_{C \in \mathcal{Q}} C = A.$$
3. $$\forall C \in \mathcal{Q}\ \forall C' \in \mathcal{Q}\ \left(C \neq C' \Rightarrow C \cap C' = \emptyset\right).$$

Donc une partition de A est une décomposition de A en réunion de sous-ensembles *non-vides et disjoints deux à deux*.

Exemples 2.1

1. Le sous-ensemble $\mathcal{Q} = \{]-\infty, 0],]0, \infty[\} \subset \mathcal{P}(\mathbb{R})$ est une partition de $\mathbb{R}$.

Exemples 2.1

1. Le sous-ensemble $\mathcal{Q} = \{]-\infty, 0],]0, \infty[\} \subset \mathcal{P}(\mathbb{R})$ est une partition de $\mathbb{R}$.
2. Soit A un ensemble et soit $\mathcal{S} := \{\{a\} |\ a \in A\} \subset \mathcal{P}(A)$ l'ensemble des singletons de A. $\mathcal{S}$ est une partition de A.

Exemples 2.1

1. Le sous-ensemble $\mathcal{Q} = \{]-\infty, 0],]0, \infty[\} \subset \mathcal{P}(\mathbb{R})$ est une partition de $\mathbb{R}$.
2. Soit A un ensemble et soit $\mathcal{S} := \{\{a\} |\ a \in A\} \subset \mathcal{P}(A)$ l'ensemble des singletons de A. $\mathcal{S}$ est une partition de A.
3. Soit $B \subset A$ un sous-ensemble de A tel que $B \neq \varnothing$ et $B \neq A$. Alors $\{B, {}^cB\}$ est une partition de A.

Exemples 2.1

1. Le sous-ensemble $\mathcal{Q} = \{]-\infty, 0],]0, \infty[\} \subset \mathcal{P}(\mathbb{R})$ est une partition de $\mathbb{R}$.
2. Soit A un ensemble et soit $\mathcal{S} := \{\{a\} |\ a \in A\} \subset \mathcal{P}(A)$ l'ensemble des singletons de A. $\mathcal{S}$ est une partition de A.
3. Soit $B \subset A$ un sous-ensemble de A tel que $B \neq \emptyset$ et $B \neq A$. Alors $\{B, {}^cB\}$ est une partition de A.
4. Soient

$$2\mathbb{Z} := \{2k |\ k \in \mathbb{Z}\},\ 2\mathbb{Z}+1 := \{2k+1 |\ k \in \mathbb{Z}\}$$

les ensembles des nombres entiers pairs, respectivement impairs. Alors $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$ est une partition de $\mathbb{Z}$.

Définition 2.4

Soit R une relation d'équivalence sur A et soit $x \in A$.

1. *La classe d'équivalence de x par rapport à R est le sous-ensemble de A défini par $[x]_R := \{y \in A | \ x \, R \, y\}$.*

Définition 2.4

Soit R une relation d'équivalence sur A et soit $x \in A$.

1. *La classe d'équivalence de x par rapport à R est le sous-ensemble de A défini par $[x]_R := \{y \in A | \ x \, R \, y\}$. Donc $[x]_R$ est l'ensemble de tous les éléments de A qui sont R-équivalents à x.*

Définition 2.4

Soit R une relation d'équivalence sur A et soit $x \in A$.

1. *La classe d'équivalence de x par rapport à R est le sous-ensemble de A défini par $[x]_R := \{y \in A | \ x \, R \, y\}$. Donc $[x]_R$ est l'ensemble de tous les éléments de A qui sont R-équivalents à x.*
2. *Un sous-ensemble $C \subset A$ est dit classe d'équivalence par rapport à R s'il existe $x \in A$ tel que $C = [x]_R$.*

Définition 2.4

Soit R une relation d'équivalence sur A et soit $x \in A$.

1. *La classe d'équivalence de x par rapport à R est le sous-ensemble de A défini par $[x]_R := \{y \in A |\ x\ R\ y\}$. Donc $[x]_R$ est l'ensemble de tous les éléments de A qui sont R-équivalents à x.*
2. *Un sous-ensemble $C \subset A$ est dit classe d'équivalence par rapport à R s'il existe $x \in A$ tel que $C = [x]_R$.*
3. *L'ensemble quotient de A par R est l'ensemble A/R des classes d'équivalence par rapport à R :*

$$A/R := \{C \in \mathcal{P}(A) |\ \exists x \in A,\ C = [x]_R\}.$$

Définition 2.4

Soit R une relation d'équivalence sur A et soit $x \in A$.

1. *La classe d'équivalence de x par rapport à R est le sous-ensemble de A défini par $[x]_R := \{y \in A |\ x\ R\ y\}$. Donc $[x]_R$ est l'ensemble de tous les éléments de A qui sont R-équivalents à x.*
2. *Un sous-ensemble $C \subset A$ est dit classe d'équivalence par rapport à R s'il existe $x \in A$ tel que $C = [x]_R$.*
3. *L'ensemble quotient de A par R est l'ensemble A/R des classes d'équivalence par rapport à R :*
$$A/R := \{C \in \mathcal{P}(A) |\ \exists x \in A,\ C = [x]_R\}.$$
4. *La surjection canonique $p_R : A \to A/R$ est définie par*
$$p_R(x) := [x]_R,$$
donc p_R associe à $x \in A$ sa classe d'équivalence $[x]_R$.

Proposition 2.5

Soit A un ensemble et soit R une relation d'équivalence sur A. Alors

1. *Pour tout $x \in A$ on a $x \in [x]_R$, en particulier toute classe d'équivalence par rapport à R est non-vide.*

Proposition 2.5

Soit A un ensemble et soit R une relation d'équivalence sur A. Alors

1. *Pour tout $x \in A$ on a $x \in [x]_R$, en particulier toute classe d'équivalence par rapport à R est non-vide.*
2. *Soient x, $x' \in A$ et soient $C = [x]_R$, $C' = [x']_R \in A/R$ leurs classes d'équivalence. Sont équivalentes :*
   1. $C \cap C' \neq \emptyset$.
   2. $x \, R \, x'$.
   3. $C = C'$.

Proposition 2.5

Soit A un ensemble et soit R une relation d'équivalence sur A. Alors

1. *Pour tout $x \in A$ on a $x \in [x]_R$, en particulier toute classe d'équivalence par rapport à R est non-vide.*
2. *Soient x, $x' \in A$ et soient $C = [x]_R$, $C' = [x']_R \in A/R$ leurs classes d'équivalence. Sont équivalentes :*
   1. $C \cap C' \neq \emptyset$.
   2. $x \, R \, x'$.
   3. $C = C'$.

   Donc deux classes d'équivalence $[x]_R$, $[x']_R$ sont soit égales (quand $x \, R \, x'$), soit disjointes (quand $x \not R \, x'$).
3. *On a $\bigcup_{C \in A/R} C = A$.*
4. *A/R est une partition de A.*

Dém: 1. Soit $x \in A$. R est réflexive, donc $x\,R\,x$, donc $x \in [x]_R$.

Dém: 1. Soit $x \in A$. R est réflexive, donc $x\,R\,x$, donc $x \in [x]_R$.

2. On va démontrer $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

Dém: 1. Soit $x \in A$. R est réflexive, donc $x\,R\,x$, donc $x \in [x]_R$.

2. On va démontrer $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

$(a) \Rightarrow (b)$: Soit $y \in C \cap C'$. Donc $y \in [x]_R$ et $y \in [x']_R$, i.e. $x\,R\,y$ et $x'\,R\,y$. Par symétrie et transitivité on obtient $x\,R\,x'$.

Dém: 1. Soit $x \in A$. R est réflexive, donc $x\,R\,x$, donc $x \in [x]_R$.

2. On va démontrer $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

$(a) \Rightarrow (b)$: Soit $y \in C \cap C'$. Donc $y \in [x]_R$ et $y \in [x']_R$, i.e. $x\,R\,y$ et $x'\,R\,y$. Par symétrie et transitivité on obtient $x\,R\,x'$.

$(b) \Rightarrow (c)$: Supposant $x\,R\,x'$, montrons $C = C'$ par double inclusion.

Dém: 1. Soit $x \in A$. R est réflexive, donc $x\,R\,x$, donc $x \in [x]_R$.

2. On va démontrer $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

$(a) \Rightarrow (b)$: Soit $y \in C \cap C'$. Donc $y \in [x]_R$ et $y \in [x']_R$, i.e. $x\,R\,y$ et $x'\,R\,y$. Par symétrie et transitivité on obtient $x\,R\,x'$.

$(b) \Rightarrow (c)$: Supposant $x\,R\,x'$, montrons $C = C'$ par double inclusion.

Soit $y \in C = [x]_R$. On a donc $x\,R\,y$. Puisque $x\,R\,x'$ on obtient (par symétrie et transitivité) $x'\,R\,y$ donc $y \in [x']_R = C'$.
Argument similaire pour l'inclusion inverse.

Dém: 1. Soit $x \in A$. R est réflexive, donc $x\,R\,x$, donc $x \in [x]_R$.

2. On va démontrer $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

$(a) \Rightarrow (b)$: Soit $y \in C \cap C'$. Donc $y \in [x]_R$ et $y \in [x']_R$, i.e. $x\,R\,y$ et $x'\,R\,y$. Par symétrie et transitivité on obtient $x\,R\,x'$.

$(b) \Rightarrow (c)$: Supposant $x\,R\,x'$, montrons $C = C'$ par double inclusion.

Soit $y \in C = [x]_R$. On a donc $x\,R\,y$. Puisque $x\,R\,x'$ on obtient (par symétrie et transitivité) $x'\,R\,y$ donc $y \in [x']_R = C'$.
Argument similaire pour l'inclusion inverse.

$(c) \Rightarrow (a)$: Supposons $C = C'$. On a $C \cap C' = C$, qui est non-vide d'après 1.

3. L'inclusion $\bigcup_{C\in A/R} C \subset A$ est évidente (toute classe C est sous-ensemble de A). Pour l'inclusion inverse, soit $x \in A$.

3. L'inclusion $\bigcup_{C\in A/R} C \subset A$ est évidente (toute classe C est sous-ensemble de A). Pour l'inclusion inverse, soit $x \in A$.

Nous savons $x \in [x]_R$, donc x appartient à sa propre classe d'équiv. (qui "participe" à la réunion), donc $x \in \bigcup_{C\in A/R} C$.

3. L'inclusion $\bigcup_{C\in A/R} C \subset A$ est évidente (toute classe C est sous-ensemble de A). Pour l'inclusion inverse, soit $x \in A$.

Nous savons $x \in [x]_R$, donc x appartient à sa propre classe d'équiv. (qui "participe" à la réunion), donc $x \in \bigcup_{C\in A/R} C$.

4. En tenant compte de la définition 2.3, l'affirmation 4. est une conséquence directe de 1., 2. et 3. ■

3. L'inclusion $\bigcup_{C\in A/R} C \subset A$ est évidente (toute classe C est sous-ensemble de A). Pour l'inclusion inverse, soit $x \in A$.

Nous savons $x \in [x]_R$, donc x appartient à sa propre classe d'équiv. (qui "participe" à la réunion), donc $x \in \bigcup_{C\in A/R} C$.

4. En tenant compte de la définition 2.3, l'affirmation 4. est une conséquence directe de 1., 2. et 3. ■

Définition 2.6

Soit R une relation d'équivalence sur A. Une application $f : A \to B$ est dite compatible avec R si

$$\forall x \in A\ \forall y \in A\ \big(x\,R\,y \Rightarrow f(x) = f(y)\big).$$

Exemple 2.1

Soit R la relation d'équivalence sur $\mathbb{Z}$ définie par : $x\,R\,y$ si $y - x \in 2\mathbb{Z}$. L'application $f : \mathbb{Z} \to \{\pm 1\}$ définie par $f(k) = (-1)^k$ est compatible avec R.

Exemple 2.1

Soit R la relation d'équivalence sur $\mathbb{Z}$ définie par : $x\,R\,y$ si $y - x \in 2\mathbb{Z}$. L'application $f : \mathbb{Z} \to \{\pm 1\}$ définie par $f(k) = (-1)^k$ est compatible avec R.

Remarque 2.7

Soient R une relation d'équivalence sur A et $f : A \to B$ une application compatible avec R. La formule $[x]_R \mapsto f(x)$ définit une application $\bar{f} : A/R \to B$ sur l'ensemble quotient A/R. Cette application a la propriété $\bar{f} \circ p_R = f$.

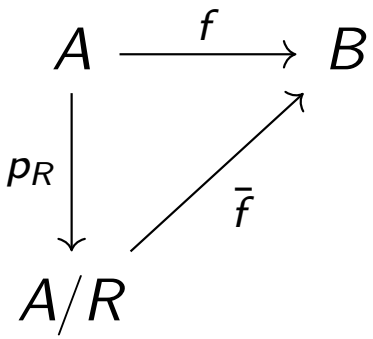
Exemple 2.1

Soit R la relation d'équivalence sur $\mathbb{Z}$ définie par : $x\,R\,y$ si $y - x \in 2\mathbb{Z}$. L'application $f : \mathbb{Z} \to \{\pm 1\}$ définie par $f(k) = (-1)^k$ est compatible avec R.

Remarque 2.7

Soient R une relation d'équivalence sur A et $f : A \to B$ une application compatible avec R. La formule $[x]_R \mapsto f(x)$ définit une application $\bar{f} : A/R \to B$ sur l'ensemble quotient A/R. Cette application a la propriété $\bar{f} \circ p_R = f$.

Dém: Exercice.



On peut reformuler cette remarque de la manière suivante : si f est compatible avec R, alors f "descend" au quotient A/R. On va dire aussi que $\bar{f}$ est *induite* par f.

Soit $n \in \mathbb{N}^*$ et soit

$$n\mathbb{Z} := \{nk | \ k \in \mathbb{Z}\}$$

l'ensemble des multiples entiers de n. Pour $x \in \mathbb{Z}$ posons

$$x + n\mathbb{Z} = \{x + nk | \ k \in \mathbb{Z}\}.$$

Soit $n \in \mathbb{N}^*$ et soit

$$n\mathbb{Z} := \{nk | \ k \in \mathbb{Z}\}$$

l'ensemble des multiples entiers de n. Pour $x \in \mathbb{Z}$ posons

$$x + n\mathbb{Z} = \{x + nk | \ k \in \mathbb{Z}\}.$$

La relation de congruence mod n sur $\mathbb{Z}$ est définie par

$$x \equiv y \, [n] \text{ si } n|(y - x). \tag{2}$$

Soit $n \in \mathbb{N}^*$ et soit

$$n\mathbb{Z} := \{nk |\ k \in \mathbb{Z}\}$$

l'ensemble des multiples entiers de n. Pour $x \in \mathbb{Z}$ posons

$$x + n\mathbb{Z} = \{x + nk |\ k \in \mathbb{Z}\}.$$

La relation de congruence mod n sur $\mathbb{Z}$ est définie par

$$x \equiv y\ [n] \text{ si } n|(y - x). \tag{2}$$

C'est une relation d'équivalence sur $\mathbb{Z}$ (à justifier !), qu'on va aussi désigner par $\underset{n}{\equiv}$.

Soit $n \in \mathbb{N}^*$ et soit

$$n\mathbb{Z} := \{nk |\ k \in \mathbb{Z}\}$$

l'ensemble des multiples entiers de n. Pour $x \in \mathbb{Z}$ posons

$$x + n\mathbb{Z} = \{x + nk |\ k \in \mathbb{Z}\}.$$

La relation de congruence mod n sur $\mathbb{Z}$ est définie par

$$x \equiv y\,[n] \text{ si } n|(y - x). \tag{2}$$

C'est une relation d'équivalence sur $\mathbb{Z}$ (à justifier !), qu'on va aussi désigner par $\underset{n}{\equiv}$. La définition (2) devient :

$$x \underset{n}{\equiv} y \text{ si } y - x \in\ n\mathbb{Z}\,. \tag{3}$$

Soit $n \in \mathbb{N}^*$ et soit

$$n\mathbb{Z} := \{nk |\ k \in \mathbb{Z}\}$$

l'ensemble des multiples entiers de n. Pour $x \in \mathbb{Z}$ posons

$$x + n\mathbb{Z} = \{x + nk |\ k \in \mathbb{Z}\}.$$

La relation de congruence mod n sur $\mathbb{Z}$ est définie par

$$x \equiv y\,[n] \text{ si } n|(y - x). \tag{2}$$

C'est une relation d'équivalence sur $\mathbb{Z}$ (à justifier !), qu'on va aussi désigner par $\underset{n}{\equiv}$. La définition (2) devient :

$$x \underset{n}{\equiv} y \text{ si } y - x \in\ n\mathbb{Z}\,. \tag{3}$$

La classe d'équivalence de $x \in \mathbb{Z}$ par rapport à $\underset{n}{\equiv}$ est

$$[x]_n = \{y \in \mathbb{Z} |\ x \underset{n}{\equiv} y\} = \{y \in \mathbb{Z} |\ \exists k \in \mathbb{Z},\ y = x + nk\} = x + n\mathbb{Z},$$

en particulier la classe de 0 (la classe triviale mod n) est

$$[0]_n = n\mathbb{Z}.$$

en particulier la classe de 0 (la classe triviale mod n) est

$$[0]_n = n\mathbb{Z}.$$

Notre but : comprendre en détail l'ensemble quotient $\mathbb{Z}/\underset{n}{\equiv}$.

en particulier la classe de 0 (la classe triviale mod n) est

$$[0]_n = n\mathbb{Z}.$$

Notre but : comprendre en détail l'ensemble quotient $\mathbb{Z}/\underset{n}{\equiv}$.

La notation standard pour cet ensemble quotient est $\mathbb{Z}/n\mathbb{Z}$. On utilise aussi la notation simplifiée $\mathbb{Z}_n$.

Proposition 2.8

Soit $n \in \mathbb{N}^*$.

1. *L'application $\gamma : \{0, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$ définie par $\gamma(k) := [k]_n$ est bijective.*

Proposition 2.8

Soit $n \in \mathbb{N}^*$.

1. *L'application $\gamma : \{0, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$ définie par $\gamma(k) \coloneqq [k]_n$ est bijective.*
2. *Les classes d'équivalence $[0]_n, \ldots, [n-1]_n$ sont distinctes deux à deux et l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ s'écrit explicitement*

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \ldots, [n-1]_n\}.$$

En particulier $\operatorname{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

Proposition 2.8

Soit $n \in \mathbb{N}^*$.

1. *L'application $\gamma : \{0, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$ définie par $\gamma(k) := [k]_n$ est bijective.*
2. *Les classes d'équivalence $[0]_n, \ldots, [n-1]_n$ sont distinctes deux à deux et l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ s'écrit explicitement*

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \ldots, [n-1]_n\}.$$

En particulier $\mathrm{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

Dém: On va définir une application $\rho : \mathbb{Z}/n\mathbb{Z} \to \{0, \ldots, n-1\}$ telle que $\gamma \circ \rho = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$ et $\rho \circ \gamma = \mathrm{id}_{\{0,\ldots,n-1\}}$.

Expliquer pourquoi l'existence d'une telle application démontre la bijectivité de γ.

Expliquer pourquoi l'existence d'une telle application démontre la bijectivité de γ.

ρ est définie de la manière suivante : pour $\xi = [k]_n \in \mathbb{Z}/n\mathbb{Z}$

$$\rho(\xi) := \text{ le reste de la division euclidienne de } k \text{ par } n \qquad (4)$$

Expliquer pourquoi l'existence d'une telle application démontre la bijectivité de γ.

ρ est définie de la manière suivante : pour $\xi = [k]_n \in \mathbb{Z}/n\mathbb{Z}$

$$\rho(\xi) := \text{ le reste de la division euclidienne de } k \text{ par } n \qquad (4)$$

ρ est bien définie : si on remplace k par un autre "représentant" k' de ξ, on aura $k' - k \in n\mathbb{Z}$, donc le reste de la DE de k' par n coïncide avec le reste de la DE de k par n. Donc le membre droit de (4) dépend seulement de ξ.

Expliquer pourquoi l'existence d'une telle application démontre la bijectivité de γ.

ρ est définie de la manière suivante : pour $\xi = [k]_n \in \mathbb{Z}/n\mathbb{Z}$

$$\rho(\xi) := \text{ le reste de la division euclidienne de } k \text{ par } n \qquad (4)$$

ρ est bien définie : si on remplace k par un autre "représentant" k' de ξ, on aura $k' - k \in n\mathbb{Z}$, donc le reste de la DE de k' par n coïncide avec le reste de la DE de k par n. Donc le membre droit de (4) dépend seulement de ξ.

L'égalité $\rho \circ \gamma = \mathrm{id}_{\{0,\dots,n-1\}}$ est évidente. Démontrons l'égalité $\gamma \circ \rho = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$, i.e. montrons $\gamma(\rho([k]_n) = [k]_n$ pour tout $k \in \mathbb{Z}$.

Expliquer pourquoi l'existence d'une telle application démontre la bijectivité de γ.

ρ est définie de la manière suivante : pour $\xi = [k]_n \in \mathbb{Z}/n\mathbb{Z}$

$$\rho(\xi) := \text{ le reste de la division euclidienne de } k \text{ par } n \qquad (4)$$

ρ est bien définie : si on remplace k par un autre "représentant" k' de ξ, on aura $k' - k \in n\mathbb{Z}$, donc le reste de la DE de k' par n coïncide avec le reste de la DE de k par n. Donc le membre droit de (4) dépend seulement de ξ.

L'égalité $\rho \circ \gamma = \mathrm{id}_{\{0,\dots,n-1\}}$ est évidente. Démontrons l'égalité $\gamma \circ \rho = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$, i.e. montrons $\gamma(\rho([k]_n) = [k]_n$ pour tout $k \in \mathbb{Z}$.

Remarquer : k et le reste de la DE de k par n sont congrus mod n, donc leurs classes mod n coïncident.

2. Est une conséquence directe de 1. Préciser les détails. ■

2. Est une conséquence directe de 1. Préciser les détails. ■

Exemple 2.2

Pour $n = 5$ on obtient $\mathbb{Z}/5\mathbb{Z} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$. Montrer qu'on a aussi

$$\mathbb{Z}/5\mathbb{Z} = \{[33]_5, [56]_5, [27]_5, [15]_5, [29]_5\}.$$

L'addition sur $\mathbb{Z}/n\mathbb{Z}$ est définie par

$$[x]_n + [y]_n := [x + y]_n.$$

Cette définition est cohérente : le membre droit $[x + y]_n$ dépend seulement des classes $[x]_n$, $[y]_n$, pas des représentants x, y de ces classes.

L'addition sur $\mathbb{Z}/n\mathbb{Z}$ est définie par

$$[x]_n + [y]_n := [x + y]_n.$$

Cette définition est cohérente : le membre droit $[x + y]_n$ dépend seulement des classes $[x]_n$, $[y]_n$, pas des représentants x, y de ces classes.

En effet, si on choisit représentants x', y' de ces classes, il existe $k \in \mathbb{Z}$, $l \in \mathbb{Z}$ tels que $x' - x = kn$, $y' - y = ln$, donc $(x' + y') - (x + y) = (k + l)n \in n\mathbb{Z}$, donc $[x' + y']_n = [x + y]_n$.

L'addition sur $\mathbb{Z}/n\mathbb{Z}$ est définie par

$$[x]_n + [y]_n := [x + y]_n.$$

Cette définition est cohérente : le membre droit $[x + y]_n$ dépend seulement des classes $[x]_n$, $[y]_n$, pas des représentants x, y de ces classes.

En effet, si on choisit représentants x', y' de ces classes, il existe $k \in \mathbb{Z}$, $l \in \mathbb{Z}$ tels que $x' - x = kn$, $y' - y = ln$, donc $(x' + y') - (x + y) = (k + l)n \in n\mathbb{Z}$, donc $[x' + y']_n = [x + y]_n$.

La multiplication sur $\mathbb{Z}/n\mathbb{Z}$ est définie par $[x]_n \cdot [y]_n := [xy]_n$.

L'addition sur $\mathbb{Z}/n\mathbb{Z}$ est définie par

$$[x]_n + [y]_n := [x + y]_n.$$

Cette définition est cohérente : le membre droit $[x + y]_n$ dépend seulement des classes $[x]_n$, $[y]_n$, pas des représentants x, y de ces classes.

En effet, si on choisit représentants x', y' de ces classes, il existe $k \in \mathbb{Z}$, $l \in \mathbb{Z}$ tels que $x' - x = kn$, $y' - y = ln$, donc $(x' + y') - (x + y) = (k + l)n \in n\mathbb{Z}$, donc $[x' + y']_n = [x + y]_n$.

La multiplication sur $\mathbb{Z}/n\mathbb{Z}$ est définie par $[x]_n \cdot [y]_n := [xy]_n$.

Exercice 2.1

Montrer que la définition de la multiplication est cohérente. Plus précisément, montrer que si $[x']_n = [x]_n$ et $[y']_n = [y]_n$, alors $[x'y']_n = [xy]_n$.

En utilisant les propriétés élémentaires de l'addition et de la multiplication sur $\mathbb{Z}$ on obtient facilement :

Proposition 2.9

Les opérations $+$ et $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$ satisfont les propriétés :

1. *L'addition est associative :*

$$\forall(\alpha,\beta,\gamma)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ (\alpha+\beta)+\gamma=\alpha+(\beta+\gamma).$$

En utilisant les propriétés élémentaires de l'addition et de la multiplication sur $\mathbb{Z}$ on obtient facilement :

Proposition 2.9

Les opérations $+$ et $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$ satisfont les propriétés :

1. *L'addition est associative :*

$$\forall(\alpha,\beta,\gamma)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ (\alpha+\beta)+\gamma=\alpha+(\beta+\gamma).$$

2. *La classe nulle $[0]_n$ est élément neutre pour l'addition :*

$$\forall\alpha\in\mathbb{Z}/n\mathbb{Z},\ \alpha+[0]_n=[0]_n+\alpha=\alpha.$$

En utilisant les propriétés élémentaires de l'addition et de la multiplication sur $\mathbb{Z}$ on obtient facilement :

Proposition 2.9

Les opérations $+$ et $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$ satisfont les propriétés :

1. *L'addition est associative :*

$$\forall(\alpha,\beta,\gamma)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ (\alpha+\beta)+\gamma=\alpha+(\beta+\gamma).$$

2. *La classe nulle $[0]_n$ est élément neutre pour l'addition :*

$$\forall\alpha\in\mathbb{Z}/n\mathbb{Z},\ \alpha+[0]_n=[0]_n+\alpha=\alpha.$$

3. *Pour toute classe $\alpha=[k]_n\in\mathbb{Z}/n\mathbb{Z}$ la classe $-\alpha:=[-k]_n$ est un élément symétrique de α par rapport à l'addition :*

$$\alpha+(-\alpha)=(-\alpha)+\alpha=[0]_n.$$

4. L'addition est commutative :

$$\forall(\alpha,\beta)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ \alpha+\beta=\beta+\alpha.$$

4. L'addition est commutative :

$$\forall(\alpha,\beta)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ \alpha+\beta=\beta+\alpha.$$

5. La multiplication est associative :

$$\forall(\alpha,\beta,\gamma)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ (\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma).$$

4. L'addition est commutative :

$$\forall(\alpha,\beta)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ \alpha+\beta=\beta+\alpha.$$

5. La multiplication est associative :

$$\forall(\alpha,\beta,\gamma)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ (\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma).$$

6. La classe $[1]_n$ est élément neutre pour la multiplication :

$$\forall\alpha\in\mathbb{Z}/n\mathbb{Z},\ \alpha\cdot[1]_n=[1]_n\cdot\alpha=\alpha.$$

4. L'addition est commutative :

$$\forall(\alpha,\beta)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ \alpha+\beta=\beta+\alpha.$$

5. La multiplication est associative :

$$\forall(\alpha,\beta,\gamma)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ (\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma).$$

6. La classe $[1]_n$ est élément neutre pour la multiplication :

$$\forall\alpha\in\mathbb{Z}/n\mathbb{Z},\ \alpha\cdot[1]_n=[1]_n\cdot\alpha=\alpha.$$

7. La multiplication est distributive par rapport à l'addition :

$$\forall(\alpha,\beta,\gamma)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ \alpha\cdot(\beta+\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma.$$

8. La multiplication est commutative :

$$\forall(\alpha,\beta)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ \alpha\cdot\beta=\beta\cdot\alpha.$$

8. La multiplication est commutative :

$$\forall(\alpha,\beta)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ \alpha\cdot\beta=\beta\cdot\alpha.$$

Ces propriétés nous permettront de conclure que $\mathbb{Z}/n\mathbb{Z}$ (muni de l'addition et la multiplication définies ci-dessus) est un *anneau commutatif*. Il s'appelle l'anneau des entiers mod n.

8. La multiplication est commutative :

$$\forall(\alpha,\beta)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ \alpha\cdot\beta=\beta\cdot\alpha.$$

Ces propriétés nous permettront de conclure que $\mathbb{Z}/n\mathbb{Z}$ (muni de l'addition et la multiplication définies ci-dessus) est un *anneau commutatif*. Il s'appelle l'anneau des entiers mod n.

Remarque 2.10

La multiplication des nombres (dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{C}$) a une propriété très importante : le produit de deux éléments non-nuls est toujours non-nul. Difficulté : si $n\geqslant 2$ n'est pas un nombre premier, cette propriété n'est pas vraie dans $\mathbb{Z}/n\mathbb{Z}$.

8. La multiplication est commutative :

$$\forall(\alpha,\beta)\in(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z}),\ \alpha\cdot\beta=\beta\cdot\alpha.$$

Ces propriétés nous permettront de conclure que $\mathbb{Z}/n\mathbb{Z}$ (muni de l'addition et la multiplication définies ci-dessus) est un *anneau commutatif*. Il s'appelle l'anneau des entiers mod n.

Remarque 2.10

La multiplication des nombres (dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{C}$) a une propriété très importante : le produit de deux éléments non-nuls est toujours non-nul. Difficulté : si $n\geqslant 2$ n'est pas un nombre premier, cette propriété n'est pas vraie dans $\mathbb{Z}/n\mathbb{Z}$.

Exemple : $[2]_6\neq[0]_6$, $[3]_6\neq[0]_6$, mais $[2]_6\cdot[3]_6=[0]_6$.

Définition 2.11

Un élément $\xi \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible, s'il est inversible par rapport à la multiplication, c'est à dire s'il existe $\eta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\xi\eta = [1]_n$. Le sous-ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sera noté $(\mathbb{Z}/n\mathbb{Z})^\times$.

Définition 2.11

Un élément $\xi \in \mathbb{Z}/n\mathbb{Z}$ est dit inversible, s'il est inversible par rapport à la multiplication, c'est à dire s'il existe $\eta \in \mathbb{Z}/n\mathbb{Z}$ tel que $\xi\eta = [1]_n$. Le sous-ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sera noté $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proposition 2.12

Une classe $\xi = [k]_n$ appartient à $(\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $\mathrm{pgcd}(k, n) = 1$. En particulier, si p est un nombre premier on a $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})\backslash\{[0]_p\}$, donc $(\mathbb{Z}/p\mathbb{Z})^\times = \{[1]_p, \ldots, [p-1]_p\}$.

Dém: Nous avons les équivalences :

$$[k]_n \in (\mathbb{Z}/n\mathbb{Z})^\times \Leftrightarrow \exists \lambda \in \mathbb{Z}/n\mathbb{Z},\ [k]_n\lambda = [1]_n \Leftrightarrow$$

$$\Leftrightarrow \exists l \in \mathbb{Z},\ [k]_n[l]_n = [1]_n \Leftrightarrow \exists l \in \mathbb{Z},\ 1 - kl \in n\mathbb{Z} \Leftrightarrow$$

$$\Leftrightarrow \exists (l, q) \in \mathbb{Z} \times \mathbb{Z},\ 1 - kl = nq \Leftrightarrow \exists (l, q) \in \mathbb{Z} \times \mathbb{Z},\ kl + nq = 1 \Leftrightarrow$$

$$\Leftrightarrow \operatorname{pgcd}(k, n) = 1.$$

Pour la dernière équivalence on a utilisé le th. de Bézout. ■

Dém: Nous avons les équivalences :

$$[k]_n \in (\mathbb{Z}/n\mathbb{Z})^\times \Leftrightarrow \exists \lambda \in \mathbb{Z}/n\mathbb{Z},\ [k]_n\lambda = [1]_n \Leftrightarrow$$

$$\Leftrightarrow \exists l \in \mathbb{Z},\ [k]_n[l]_n = [1]_n \Leftrightarrow \exists l \in \mathbb{Z},\ 1 - kl \in n\mathbb{Z} \Leftrightarrow$$

$$\Leftrightarrow \exists (l, q) \in \mathbb{Z} \times \mathbb{Z},\ 1 - kl = nq \Leftrightarrow \exists (l, q) \in \mathbb{Z} \times \mathbb{Z},\ kl + nq = 1 \Leftrightarrow$$

$$\Leftrightarrow \operatorname{pgcd}(k, n) = 1.$$

Pour la dernière équivalence on a utilisé le th. de Bézout. ■

Exemple 2.3

Pour $n = 30$ on obtient :

$$(\mathbb{Z}/30\mathbb{Z})^\times = \left\{[1]_{30}, [7]_{30}, [11]_{30}, [13]_{30}, [17]_{30}, [19]_{30}, [23]_{30}, [29]_{30}\right\}$$

donc $\operatorname{card}((\mathbb{Z}/30\mathbb{Z})^\times) = 8$.

Remarque 2.13

$(\mathbb{Z}/n\mathbb{Z})^\times$ est stable par rapport à la multiplication, c'est à dire

$$(\xi \in (\mathbb{Z}/n\mathbb{Z})^\times) \wedge (\eta \in (\mathbb{Z}/n\mathbb{Z})^\times) \Rightarrow \xi\eta \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Remarque 2.13

$(\mathbb{Z}/n\mathbb{Z})^\times$ *est stable par rapport à la multiplication, c'est à dire*

$$(\xi \in (\mathbb{Z}/n\mathbb{Z})^\times) \wedge (\eta \in (\mathbb{Z}/n\mathbb{Z})^\times) \Rightarrow \xi\eta \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Exercice 2.2

Préciser le sous-ensemble $(\mathbb{Z}/12\mathbb{Z})^\times \subset \mathbb{Z}/12\mathbb{Z}$ et faire la table de la multiplication sur ce sous-ensemble.

Remarque 2.13

$(\mathbb{Z}/n\mathbb{Z})^\times$ est stable par rapport à la multiplication, c'est à dire

$$(\xi \in (\mathbb{Z}/n\mathbb{Z})^\times) \wedge (\eta \in (\mathbb{Z}/n\mathbb{Z})^\times) \Rightarrow \xi\eta \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

Exercice 2.2

Préciser le sous-ensemble $(\mathbb{Z}/12\mathbb{Z})^\times \subset \mathbb{Z}/12\mathbb{Z}$ et faire la table de la multiplication sur ce sous-ensemble.

Notation simplifiée : On utilise souvent la notation $\mathbb{Z}_n$ pour le quotient $\mathbb{Z}/n\mathbb{Z}$ et la notation $\mathbb{Z}_n^\times$ pour le sous-ensemble des éléments inversibles.

Rappel : Soient A un ensemble, $R \subset A \times A$ une relation d'équivalence sur A et $p_R : A \to A/R$ la surjection canonique.

Rappel : Soient A un ensemble, $R \subset A \times A$ une relation d'équivalence sur A et $p_R : A \to A/R$ la surjection canonique.

Une application $F : A \to B$ est dite compatible avec R si

$$x \, R \, y \Rightarrow F(x) = F(y).$$

Rappel : Soient A un ensemble, $R \subset A \times A$ une relation d'équivalence sur A et $p_R : A \to A/R$ la surjection canonique.

Une application $F : A \to B$ est dite compatible avec R si

$$x \, R \, y \Rightarrow F(x) = F(y).$$

Si c'est le cas, alors la formule $[x]_R \mapsto F(x)$ définit une application $f : A/R \to B$.

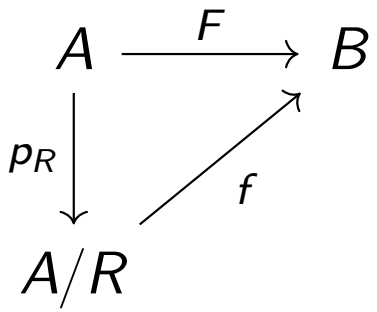
Rappel : Soient A un ensemble, $R \subset A \times A$ une relation d'équivalence sur A et $p_R : A \to A/R$ la surjection canonique.

Une application $F : A \to B$ est dite compatible avec R si

$$x \, R \, y \Rightarrow F(x) = F(y).$$

Si c'est le cas, alors la formule $[x]_R \mapsto F(x)$ définit une application $f : A/R \to B$.

Cette application a la propriété : $f \circ p_R = F$.



Dans ce chapitre on va utiliser la notation $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

Dans ce chapitre on va utiliser la notation $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

Soient $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$, $n := \prod_{i=1}^{k} n_i$ leur produit.

Dans ce chapitre on va utiliser la notation $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

Soient $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$, $n := \prod_{i=1}^k n_i$ leur produit.

Remarque 2.14

L'application

$$F : \mathbb{Z} \to \times_{i=1}^k \mathbb{Z}_{n_i}, \ F(x) := ([x]_{n_1}, \ldots, [x]_{n_k})$$

est compatible avec la relation d'équivalence $\underset{n}{\equiv}$*, donc la formule*

$$f([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k})$$

définit de manière cohérente une application $f : \mathbb{Z}_n \to \times_{i=1}^k \mathbb{Z}_{n_i}$.

Pour $x,\ y \in \mathbb{Z}$ nous avons :

$$F(x) := ([x]_{n_1}, \ldots, [x]_{n_k}),\ F(y) := ([y]_{n_1}, \ldots, [y]_{n_k}).$$

Dém: Nos devons vérifier l'implication

$$x \underset{n}{\equiv} y \Rightarrow F(x) = F(y).$$

Pour $x,\ y \in \mathbb{Z}$ nous avons :

$$F(x) := ([x]_{n_1}, \ldots, [x]_{n_k}),\ F(y) := ([y]_{n_1}, \ldots, [y]_{n_k}).$$

Dém: Nos devons vérifier l'implication

$$x \underset{n}{\equiv} y \Rightarrow F(x) = F(y).$$

Mais $n = \prod_{i=1}^{k} n_i$, donc

$$x \underset{n}{\equiv} y \Rightarrow \Big(\prod_{i=1}^{k} n_i\Big) \mid (y - x) \Rightarrow$$

$$\forall i \in \{1, \ldots, k\},\ n_i | (y-x) \Rightarrow \forall i \in \{1, \ldots, k\},\ [x]_{n_i} = [y]_{n_i} \Rightarrow F(x) = F(y).$$

Remarque 2.15

L'application f ainsi obtenue est compatible avec les deux opérations $+$ et $\cdot$ sur $\mathbb{Z}_n$ et $\times_{i=1}^{k}\mathbb{Z}_{n_i}$.

Remarque 2.15

L'application f ainsi obtenue est compatible avec les deux opérations $+$ et $\cdot$ sur $\mathbb{Z}_n$ et $\times_{i=1}^{k}\mathbb{Z}_{n_i}$.
Plus précisément :

$$f(\xi+\eta)=f(\xi)+f(\eta),\ f(\xi\eta)=f(\xi)f(\eta)$$

où a droite on a utilisé les opérations sur $\times_{i=1}^{k}\mathbb{Z}_{n_i}$ définies par

Remarque 2.15

L'application f ainsi obtenue est compatible avec les deux opérations $+$ et $\cdot$ sur $\mathbb{Z}_n$ et $\times_{i=1}^{k}\mathbb{Z}_{n_i}$.
Plus précisément :

$$f(\xi+\eta)=f(\xi)+f(\eta),\ f(\xi\eta)=f(\xi)f(\eta)$$

où a droite on a utilisé les opérations sur $\times_{i=1}^{k}\mathbb{Z}_{n_i}$ définies par

$$(\xi_1,\ldots,\xi_k)+(\eta_1,\ldots,\eta_k):=(\xi_1+\eta_1,\ldots,\xi_k+\eta_k),$$

$$(\xi_1,\ldots,\xi_k)(\eta_1,\ldots,\eta_k):=(\xi_1\eta_1,\ldots,\xi_k\eta_k).$$

Remarquons aussi que $f([1]_n)=([1]_{n_1},\ldots,[1]_{n_k})$.

En utilisant la terminologie de la théorie des anneaux, ces propriétés montrent que $f : \mathbb{Z}_n \to \times_{i=1}^{k} \mathbb{Z}_{n_i}$ est un homomorphisme (morphisme) d'anneaux.

En utilisant la terminologie de la théorie des anneaux, ces propriétés montrent que $f : \mathbb{Z}_n \to \times_{i=1}^{k} \mathbb{Z}_{n_i}$ est un homomorphisme (morphisme) d'anneaux.

Lemme 2.16

Soient $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et $x \in \mathbb{Z}$. Alors sont équivalentes :

(i) *n_i divise x pour $1 \leqslant i \leqslant k$.*

En utilisant la terminologie de la théorie des anneaux, ces propriétés montrent que $f : \mathbb{Z}_n \to \times_{i=1}^{k} \mathbb{Z}_{n_i}$ est un homomorphisme (morphisme) d'anneaux.

Lemme 2.16

Soient $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et $x \in \mathbb{Z}$. Alors sont équivalentes :

(i) *n_i divise x pour $1 \leqslant i \leqslant k$.*

(ii) *$n = \prod_{i=1}^{k} n_i$ divise x.*

En utilisant la terminologie de la théorie des anneaux, ces propriétés montrent que $f : \mathbb{Z}_n \to \times_{i=1}^{k} \mathbb{Z}_{n_i}$ est un homomorphisme (morphisme) d'anneaux.

Lemme 2.16

Soient $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et $x \in \mathbb{Z}$. Alors sont équivalentes :

(i) *n_i divise x pour $1 \leqslant i \leqslant k$.*

(ii) *$n = \prod_{i=1}^{k} n_i$ divise x.*

Dém: L'implication 2. $\Rightarrow$ 1. toujours vraie, évidente.

En utilisant la terminologie de la théorie des anneaux, ces propriétés montrent que $f : \mathbb{Z}_n \to \times_{i=1}^{k} \mathbb{Z}_{n_i}$ est un homomorphisme (morphisme) d'anneaux.

Lemme 2.16

Soient $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et $x \in \mathbb{Z}$. Alors sont équivalentes :

(i) *n_i divise x pour $1 \leqslant i \leqslant k$.*

(ii) *$n = \prod_{i=1}^{k} n_i$ divise x.*

Dém: L'implication 2. $\Rightarrow$ 1. toujours vraie, évidente.
1. $\Rightarrow$ 2. : Supposons $n_i | x$ pour $1 \leqslant i \leqslant k$. Montrons : $n | x$.

On peut supposer $x \neq 0$.

On peut supposer $x \neq 0$.

On va comparer les décompositions en produit de nombres premiers de n et x.

On peut supposer $x \neq 0$.

On va comparer les décompositions en produit de nombres premiers de n et x.

Soit p^s un facteur qui intervient dans la décomposition de $n = \prod_{j=1}^{k} n_j$.

On peut supposer $x \neq 0$.

On va comparer les décompositions en produit de nombres premiers de n et x.

Soit p^s un facteur qui intervient dans la décomposition de $n = \prod_{j=1}^{k} n_j$.

Il existe un unique $j \in \{1, \ldots, k\}$ tel que le facteur p^s intervient aussi dans la factorisation de n_j. Pourquoi j est unique ?

On peut supposer $x \neq 0$.

On va comparer les décompositions en produit de nombres premiers de n et x.

Soit p^s un facteur qui intervient dans la décomposition de $n = \prod_{j=1}^{k} n_j$.

Il existe un unique $j \in \{1, \ldots, k\}$ tel que le facteur p^s intervient aussi dans la factorisation de n_j. Pourquoi j est unique ?

$n_j | x \Rightarrow p$ intervient aussi dans la factorisation de x avec un exposant $t \geqslant s$.

On peut supposer $x \neq 0$.

On va comparer les décompositions en produit de nombres premiers de n et x.

Soit p^s un facteur qui intervient dans la décomposition de $n = \prod_{j=1}^{k} n_j$.

Il existe un unique $j \in \{1, \ldots, k\}$ tel que le facteur p^s intervient aussi dans la factorisation de n_j. Pourquoi j est unique ?

$n_j | x \Rightarrow p$ intervient aussi dans la factorisation de x avec un exposant $t \geqslant s$. Ceci est vrai pour tous les facteurs p^s de la décomposition de n en facteurs premiers, donc $n | x$.

On peut supposer $x \neq 0$.

On va comparer les décompositions en produit de nombres premiers de n et x.

Soit p^s un facteur qui intervient dans la décomposition de $n = \prod_{j=1}^{k} n_j$.

Il existe un unique $j \in \{1, \ldots, k\}$ tel que le facteur p^s intervient aussi dans la factorisation de n_j. Pourquoi j est unique ?

$n_j | x \Rightarrow p$ intervient aussi dans la factorisation de x avec un exposant $t \geqslant s$. Ceci est vrai pour tous les facteurs p^s de la décomposition de n en facteurs premiers, donc $n | x$.

Argument plus rapide : x est un multiple commun des n_i, donc x est un multiple de $\mathrm{ppcm}(n_1, \ldots, n_k)$. Puisque n_i sont premiers entre eux deux à deux, $\mathrm{ppcm}(n_1, \ldots, n_k) = \prod_{i=1}^{k} n_i = n$.

Théorème 2.17 (théorème des restes chinois)

Soient $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$, $n := \prod_{i=1}^k n_i$ *et soit* $f : \mathbb{Z}_n \to \times_{i=1}^k \mathbb{Z}_{n_i}$ *l'application définie par*

$$f([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k}).$$

Si $n_1, \ldots, n_k$ *sont premiers entre eux deux à deux, alors* f *est bijective.*

Théorème 2.17 (théorème des restes chinois)

Soient $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$, $n := \prod_{i=1}^k n_i$ et soit $f : \mathbb{Z}_n \to \times_{i=1}^k \mathbb{Z}_{n_i}$ l'application définie par

$$f([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k}).$$

Si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, alors f est bijective.

Dém: M. q. f est injective. Soient $[x]_n$, $[y]_n \in \mathbb{Z}_n$.

Théorème 2.17 (théorème des restes chinois)

Soient $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$, $n := \prod_{i=1}^k n_i$ et soit $f : \mathbb{Z}_n \to \times_{i=1}^k \mathbb{Z}_{n_i}$ l'application définie par

$$f([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k}).$$

Si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, alors f est bijective.

Dém: M. q. f est injective. Soient $[x]_n$, $[y]_n \in \mathbb{Z}_n$.

$$f([x]_n) = f([y]_n) \Leftrightarrow ([x]_{n_i} = [y]_{n_i} \text{ pour } 1 \leqslant i \leqslant k) \Leftrightarrow$$

$$\Leftrightarrow n_i | (y - x) \text{ pour } 1 \leqslant i \leqslant k \overset{\text{Lemme}}{\Leftrightarrow} n | (y - x) \Leftrightarrow [x]_n = [y]_n.$$

Donc f est injective.

Pour la bijectivité : remarquer que les ensembles $\mathbb{Z}_n$, $\times_{i=1}^{k}\mathbb{Z}_{n_i}$ sont finis et

$$\mathrm{card}(\mathbb{Z}_n) = \mathrm{card}(\times_{i=1}^{k}\mathbb{Z}_{n_i}) = n.$$ ■

Pour la bijectivité : remarquer que les ensembles $\mathbb{Z}_n$, $\times_{i=1}^{k}\mathbb{Z}_{n_i}$ sont finis et

$$\mathrm{card}(\mathbb{Z}_n) = \mathrm{card}(\times_{i=1}^{k}\mathbb{Z}_{n_i}) = n.$$ ■

Remarque 2.18

On va voir que, en utilisant la terminologie de la théorie des anneaux, la remarque 2.15 et le théorème 2.17 nous permettent de conclure que, si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, alors l'application $f : \mathbb{Z}_n \to \times_{i=1}^{k}\mathbb{Z}_{n_i}$ définie dans la remarque 2.14 est un isomorphisme d'anneaux.

Pour la bijectivité : remarquer que les ensembles $\mathbb{Z}_n$, $\times_{i=1}^{k}\mathbb{Z}_{n_i}$ sont finis et

$$\mathrm{card}(\mathbb{Z}_n) = \mathrm{card}(\times_{i=1}^{k}\mathbb{Z}_{n_i}) = n. \qquad \blacksquare$$

Remarque 2.18

On va voir que, en utilisant la terminologie de la théorie des anneaux, la remarque 2.15 et le théorème 2.17 nous permettent de conclure que, si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, alors l'application $f : \mathbb{Z}_n \to \times_{i=1}^{k}\mathbb{Z}_{n_i}$ définie dans la remarque 2.14 est un isomorphisme d'anneaux.

Soit $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$. En utilisant la remarque 2.15 on déduit facilement que $f(\mathbb{Z}_n^\times) \subset \times_{i=1}^{k}\mathbb{Z}_{n_i}^\times$.

Pour la bijectivité : remarquer que les ensembles $\mathbb{Z}_n$, $\times_{i=1}^{k}\mathbb{Z}_{n_i}$ sont finis et

$$\mathrm{card}(\mathbb{Z}_n) = \mathrm{card}(\times_{i=1}^{k}\mathbb{Z}_{n_i}) = n. \qquad \blacksquare$$

Remarque 2.18

On va voir que, en utilisant la terminologie de la théorie des anneaux, la remarque 2.15 et le théorème 2.17 nous permettent de conclure que, si $n_1, \ldots, n_k$ sont premiers entre eux deux à deux, alors l'application $f : \mathbb{Z}_n \to \times_{i=1}^{k}\mathbb{Z}_{n_i}$ définie dans la remarque 2.14 est un isomorphisme d'anneaux.

Soit $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$. En utilisant la remarque 2.15 on déduit facilement que $f(\mathbb{Z}_n^\times) \subset \times_{i=1}^{k}\mathbb{Z}_{n_i}^\times$.
Si $n_1, \ldots, n_k$ sont premiers entre eux, cette inclusion est une égalité et f induit une bijection $\mathbb{Z}_n^\times \to \times_{i=1}^{k}\mathbb{Z}_{n_i}^\times$.

Proposition 2.19 (la version multiplicative du lemme chinois)

Soit $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et soit $n := \prod_{i=1}^k n_i$ leur produit. Alors la formule

$$h([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k})$$

définit une bijection $h : \mathbb{Z}_n^\times \xrightarrow{\simeq} \times_{i=1}^k \mathbb{Z}_{n_i}^\times$.

Proposition 2.19 (la version multiplicative du lemme chinois)

Soit $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et soit $n := \prod_{i=1}^k n_i$ leur produit. Alors la formule

$$h([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k})$$

définit une bijection $h : \mathbb{Z}_n^\times \xrightarrow{\simeq} \times_{i=1}^k \mathbb{Z}_{n_i}^\times$.

On va voir que cette bijection est un isomorphisme de groupes.

Proposition 2.19 (la version multiplicative du lemme chinois)

Soit $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et soit $n := \prod_{i=1}^k n_i$ leur produit. Alors la formule

$$h([x]_n) := ([x]_{n_1}, \ldots, [x]_{n_k})$$

définit une bijection $h : \mathbb{Z}_n^\times \xrightarrow{\simeq} \times_{i=1}^k \mathbb{Z}_{n_i}^\times$.

On va voir que cette bijection est un isomorphisme de groupes.

On peut reformuler le théorème des restes chinois de la manière suivante :

Corollaire 2.20

Soit $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et soit $n := \prod_{i=1}^{k} n_i$ leur produit. Soit $(y_1, \ldots, y_k) \in \mathbb{Z}^k$ une famille arbitraire de k nombres entiers. Alors

1. *Il existe $x \in \mathbb{Z}$ tel que $[x]_{n_i} = [y_i]_{n_i}$ pour $1 \leqslant i \leqslant k$.*
2. *La classe de congruence $[x]_n$ est déterminée uniquement par $([y_1]_{n_1}, \ldots, [y_k]_{n_k})$.*

Corollaire 2.20

Soit $(n_1, \ldots, n_k) \in (\mathbb{N}^*)^k$ une famille de k nombres premiers entre eux deux à deux et soit $n := \prod_{i=1}^{k} n_i$ leur produit. Soit $(y_1, \ldots, y_k) \in \mathbb{Z}^k$ une famille arbitraire de k nombres entiers. Alors

1. *Il existe $x \in \mathbb{Z}$ tel que $[x]_{n_i} = [y_i]_{n_i}$ pour $1 \leqslant i \leqslant k$.*
2. *La classe de congruence $[x]_n$ est déterminée uniquement par $([y_1]_{n_1}, \ldots, [y_k]_{n_k})$.*

Remarque 2.21

Dans les conditions et avec les notations du corollaire il existe $x \in \mathbb{Z}$ qui résout simultanément les congruences $x \underset{n_i}{\equiv} y_i$ et la classe $[x]_n$ est déterminée uniquement.

Algorithme pour déterminer une solution x des congruences

$$x \underset{n_i}{\equiv} y_i :$$

Algorithme pour déterminer une solution x des congruences

$$x \underset{n_i}{\equiv} y_i :$$

Posons $\hat{n}_j := \prod_{s \neq j} n_s$. Remarquons : $\operatorname{pgcd}(n_j, \hat{n}_j) = 1$.

Algorithme pour déterminer une solution x des congruences

$$x \underset{n_i}{\equiv} y_i :$$

Posons $\hat{n}_j := \prod_{s \neq j} n_s$. Remarquons : $\operatorname{pgcd}(n_j, \hat{n}_j) = 1$.

D'après Bézout : il existe $(u_j, v_j) \in \mathbb{Z} \times \mathbb{Z}$ tels que :

$$u_j n_j + v_j \hat{n}_j = 1 \,.$$

Algorithme pour déterminer une solution x des congruences

$$x \underset{n_i}{\equiv} y_i :$$

Posons $\hat{n}_j := \prod_{s \neq j} n_s$. Remarquons : $\operatorname{pgcd}(n_j, \hat{n}_j) = 1$.

D'après Bézout : il existe $(u_j, v_j) \in \mathbb{Z} \times \mathbb{Z}$ tels que :

$$u_j n_j + v_j \hat{n}_j = 1 \,.$$

On peut trouver explicitement un tel couple (u_j, v_j) avec l'algorithme de Euclid.

Algorithme pour déterminer une solution x des congruences

$$x \underset{n_i}{\equiv} y_i :$$

Posons $\hat{n}_j := \prod_{s \neq j} n_s$. Remarquons : $\operatorname{pgcd}(n_j, \hat{n}_j) = 1$.

D'après Bézout : il existe $(u_j, v_j) \in \mathbb{Z} \times \mathbb{Z}$ tels que :

$$u_j n_j + v_j \hat{n}_j = 1 \, .$$

On peut trouver explicitement un tel couple (u_j, v_j) avec l'algorithme de Euclid.

Posons $x_j := v_j \hat{n}_j$. Remarquons que

$$x_j \equiv 1 \ (\text{mod}) \ n_j \ , \ x_j \equiv 0 \ (\text{mod}) \ n_i \ \text{ pour } i \neq j \, .$$

Soit $x := \sum_{j=1}^{k} y_j x_j$.

Pour $1 \leqslant i \leqslant k$ fixé on obtient

$$[x]_{n_i} = \Big[\sum_{j=1}^{k} y_j x_j\Big]_{n_i} = \sum_{j=1}^{k} [y_j]_{n_i}[x_j]_{n_i} = [y_i]_{n_i} \ ,$$

parce que $[x_j]_{n_i} = 0$ pour $j \neq i$ et $[x_i]_{n_i} = 1$.

Pour $1 \leqslant i \leqslant k$ fixé on obtient

$$[x]_{n_i} = \Big[\sum_{j=1}^{k} y_j x_j\Big]_{n_i} = \sum_{j=1}^{k} [y_j]_{n_i}[x_j]_{n_i} = [y_i]_{n_i} \ ,$$

parce que $[x_j]_{n_i} = 0$ pour $j \neq i$ et $[x_i]_{n_i} = 1$.

Donc x est bien une solution des congruences $x \equiv y_i \mod n_i$.

Pour $1 \leqslant i \leqslant k$ fixé on obtient

$$[x]_{n_i} = \Big[\sum_{j=1}^{k} y_j x_j\Big]_{n_i} = \sum_{j=1}^{k} [y_j]_{n_i}[x_j]_{n_i} = [y_i]_{n_i} \ ,$$

parce que $[x_j]_{n_i} = 0$ pour $j \neq i$ et $[x_i]_{n_i} = 1$.

Donc x est bien une solution des congruences $x \equiv y_i \mod n_i$.

Exercice 2.3

Trouver $[m]$, $[n]$, $[p]$, $[q] \in \mathbb{Z}_{140}$ tels que :

1. $m \equiv 1 \pmod 4$, $m \equiv 0 \mod 5$, $m \equiv 0 \mod 7$.
2. $n \equiv 0 \pmod 4$, $n \equiv 1 \mod 5$, $n \equiv 0 \mod 7$.
3. $p \equiv 0 \pmod 4$, $p \equiv 0 \pmod 5$, $p \equiv 1 \mod 7$.
4. $q \equiv 2 \pmod 4$, $q \equiv 3 \pmod 5$, $q \equiv 3 \mod 7$.