الكلية متعددة التخصصات الناظور
ⵜⴰⵖⵉⵡⴰⵏⵜ ⵜⴰⵎⵜⵉⵏⴻⵜ ⵏ ⵏⴰⴹⵓⵔ
Faculté Pluridisciplinaire de Nador

Cours d'algèbre 1 (M.I.P)

Chapitre 4 : Arithmétique dans $\mathbb{Z}$

(Ce document ne peut en aucun cas remplacer les séances de cours en présentiel)

Pr. EL MEHDI BOUBA

Année universitaire :2023–2024

4. **Arithmétique dans $\mathbb{Z}$**

4.1. **L'ensemble $\mathbb{Z}$ des entiers relatifs.**

On désigne par $\mathbb{Z}$ l'ensemble des entiers relatifs, soit

$$\mathbb{Z} = \{\dots, -n, \dots, -3, -2, -1, 0, 1, 2, 3, \dots, n, \dots\}.$$

On rappelle que l'ensemble $(\mathbb{Z}, +, \cdot)$ des entiers relatifs est un anneau unitaire, commutatif et intègre.

L'ensemble $\mathbb{Z}$ est muni d'une relation d'ordre total, à savoir la relation d'ordre usuel $\leq$.

L'ensemble $\mathbb{Z}$ est bien ordonné, c'est-à-dire que :

- toute partie non vide et minorée de Z admet un plus petit élément,
- toute partie non vide et majorée de Z admet un plus grand élément.

4.2. **Division dans $\mathbb{Z}$.**

4.2.1. **Relation de divisibilité.**

Définition 4.1. Soient a et b deux entiers relatifs. On dit que a divise b ou b est un multiple de a, s'il existe $k \in \mathbb{Z}$ tel que $b = ak$. On note alors $a|b$.

Définition 4.2. Soit n un entier de $\mathbb{Z}$.

1. L'ensemble des multiples de n est noté $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$.
2. L'ensemble des diviseurs de n dans $\mathbb{Z}$ est noté D_n.
3. L'ensemble $D_n \cap \mathbb{N}$ est l'ensemble des diviseurs positifs de n.
4. Pour tous a, b dans $\mathbb{Z}$, on a les équivalences : $a|b \Leftrightarrow b \in a\mathbb{Z} \Leftrightarrow a \in D_b$.

Exemples 21.

- L'ensemble des multiples de 2 est $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}$.
- L'ensemble des multiples de 3 est $3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\} = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$.
- $D_{12} = D_{-12} = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$.

Lemme 4.1. *Si $a|b$ alors ($b = 0$ ou $|a| \leq |b|$).*

Preuve. Si $a|b$, alors il existe $k \in \mathbb{Z}$ tel que $b = ak$. Si $k = 0$, alors $b = 0$. Si $k \neq 0$, alors $|k| \geq 1$, ceci implique que $|b| = |ak| = |a||k| \geq |a|$. □

Remarque 4.3. Soient a et b deux éléments de $\mathbb{Z}$. En écrivant $a|b$, on définit une relation binaire sur l'ensemble $\mathbb{Z}$. Cette relation est :

1. réflexive, car $a|a$.
2. transitive, car si $a|b$ et $b|c$, alors $a|c$.
3. mais elle n'est ni symétrique ni antisymétrique. Donc ce n'est ni relation d'équivalence ni relation d'ordre.

En outre on a l'équivalence :

$$(a|b \text{ et } b|a) \Leftrightarrow a = \pm b \Leftrightarrow |a| = |b|.$$

En revanche, la restriction de la relation de divisibilité à $\mathbb{N}$ est une relation d'ordre (partiel).

On dit de deux entiers relatifs qui se divisent mutuellement (c'est-à-dire : qui sont égaux ou opposés, ou encore : qui ont la même valeur absolue) qu'ils sont associés. On retiendra que deux entiers associés ont exactement les mêmes propriétés par rapport à la relation de divisibilité.

Propriétés 1. *Nous avons les propriétés suivantes.*

1. *Pour tous entiers relatifs a et b, on a les équivalences :* $a|b \Leftrightarrow b\mathbb{Z} \subset a\mathbb{Z} \Leftrightarrow D_a \subset D_b$. *On en déduit que :* $a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow |a| = |b| \Leftrightarrow D_a = D_b$.
2. *Les égalités* $(-n)\mathbb{Z} = n\mathbb{Z}$ *et* $D_{-n} = D_n$ *font qu'on se limite souvent à* $n \geq 0$.
3. *Si a, b sont dans $n\mathbb{Z}$, et si u, v sont dans $\mathbb{Z}$, alors $au + bv$ est dans $n\mathbb{Z}$. Une telle propriété est fausse pour D_n : par exemple 2 et 3 sont dans D_6 mais $2 + 3 = 5$ n'y est pas.*
4. *Si $d|a$ et $d|b$, alors $d|au + bv$ pour tout $(u, v) \in \mathbb{Z}^2$.*
5. *Si $a|b$ et $c|d$, alors $ac|bd$. En particulier, si $a|b$ alors $a^n|b^n$ pour tout $n \in \mathbb{N}$.*
6. *Si $d \neq 0$, alors $a|b \Longleftrightarrow ad|bd$.*

4.2.2. **Division euclidienne.**

Théorème 4.2 (division euclidienne dans $\mathbb{Z}$)**.** *Soit (a, b) dans $\mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique couple (q, r) de $\mathbb{Z} \times \mathbb{N}$ tel que*

$$a = qb + r \qquad \text{et} \qquad 0 \leq r \leq |b| - 1. \tag{4}$$

Preuve. On suppose que $b > 0$ et on pose :

$$A = \{k \in \mathbb{Z} \mid bk \leq a\}.$$

Donc l'ensemble A est non vide, car :
- pour $a \geq 0$, 0 est dans A, puisque $0b = 0 \leq a$, et
- pour $a < 0$, a est dans A, puisque $a - ab = a(1 - b) \geq 0$.

De plus A est majoré :
- pour $a \geq 0$, a majore A, car pour tout $k \in A$ on a : si $k \leq 0$ le résultat est evident ; et si $k \geq 0$, alors forcement $k \leq a$, car sinon on aura

$$k \geq a \Longleftrightarrow kb \geq ab > a \text{ ce qui est absurde, et}$$

- pour $a < 0$, 0 majore A, puisque $bk \leq a < 0$ implique $k \leq 0$.

D'où A admet un plus grand élément q qui vérifie :

$$qb \leq a < b(q + 1).$$

Il suffit alors de poser : $r = a - bq$.

Pour $b < 0$ on travaille avec $-b$ et on a l'existence de (q', r') vérifiant :

$$\begin{cases} a = -bq' + r', \\ 0 \leq r' < b. \end{cases}$$

Et il suffit de poser $q = -q'$ et $r = r'$.

Supposons qu'il existe deux couples d'entiers (q, r) et (q', r') vérifiant (4) avec $q \neq q'$. On a alors :

$$|r - r'| = |b(q - q')| \geq |b| \text{ puisque } q - q' \neq 0,$$

avec r et r' dans $]-|b|, |b|[$. D'autre part, on a : $-b < r - r' < b$, d'où $|r - r'| < |b|$; ce qui est impossible. On a donc $q = q'$ et $r = r'$, Le couple (q, r) vérifiant (4) est donc unique. $\square$

Définition 4.4. (division euclidienne dans $\mathbb{Z}$).
Soit (a, b) dans $\mathbb{Z} \times \mathbb{Z}^*$. Il existe un unique couple (q, r) de $\mathbb{Z} \times \mathbb{N}$ tel que

$$a = qb + r \qquad \text{et} \qquad 0 \leq r \leq |b| - 1.$$

Le passage du couple (a, b) au couple (q, r) s'appelle la division euclidienne de a par b. Dans cette division, a est le dividende, b le diviseur, q le quotient et r le reste.

Remarques 4.5.

1. Soient $b \in \mathbb{Z}^*$ et $a \in \mathbb{Z}$. Alors b divise a si et seulement si le reste de la division euclidienne de a par b est nul.
2. **Division euclidienne de a ou de $-a$ par b.**
   Soit $a = qb + r$ la division euclidienne de a par b.
   Si a est multiple de b (c'est-à-dire $r = 0$), la division euclidienne de $-a$ par b s'écrit : $-a = (-q)b$.
   Sinon (donc si $1 \leq r \leq b - 1$), alors
   $$-a = -qb - r = -qb - b + b - r = b(-q - 1) + (b - r).$$

4.3. **Plus grand commun diviseur (PGCD).**

Définition 4.6. Soit $(a, b) \in \mathbb{Z}^2 - \{(0,0)\}$. Le plus grand commun diviseur de a et b est le plus grand entier (strictement positif) de l'ensemble des diviseurs communs de a et b, i.e. $D_a \cap D_b$. On le note $\mathrm{pgcd}(a, b)$ ou $a \wedge b$.

Proposition 4.3. *Soit $(a, b) \in \mathbb{Z}^2 - \{(0,0)\}$. Alors $a \wedge b = |a| \wedge |b|$.*

Preuve. Par définition. □

Exemples 22.

1. Cherchons $12 \wedge 28$. Pour cela il suffit de chercher les diviseurs positifs de 12 et 28. On a $D_{12}^+ = \{1, 2, 3, 4, 6, 12\}$ et $D_{28}^+ = \{1, 2, 4, 7, 14, 28\}$, donc $12 \wedge 28 = 4$.
2. Cherchons $15 \wedge 35$. On a $D_{15}^+ = \{1, 3, 5, 15\}$ et $D_{35}^+ = \{1, 5, 7, 35\}$, donc $15 \wedge 35 = 5$.

Propriétés 2. *Soit $(a,b) \in \mathbb{N}^2 - \{(0,0)\}$.*

1. *Il est clair que $a \wedge b = b \wedge a$.*
2. *Pour tout $a \in \mathbb{N}$, $a \wedge 1 = 1$.*
3. *Pour tout $a \in \mathbb{N}^*$, $a \wedge 0 = a$.*
4. *Les diviseurs de $a \wedge b$ sont également des diviseurs communs à a et b. On verra que la réciproque est vraie : les diviseurs communs à a et b sont aussi des diviseurs de $a \wedge b$.*
5. *On a l'égalité $a \wedge b = a$ si et seulement si a est un diviseur de b.*
6. $a \wedge b = \delta \Leftrightarrow \begin{cases} \exists a' \in \mathbb{N}, a = a'\delta, \\ \exists b' \in \mathbb{N}, b = b'\delta, \\ a' \wedge b' = 1. \end{cases}$

Lemme 4.4. *Soient a, $b \in \mathbb{N}^*$. Soient q et r le quotient et le reste de la division euclidienne de a par b.*

1. *Un entier c divise a et b si et seulement s'il divise b et r. Autrement dit, les diviseurs communs de a et b sont exactement ceux de b et r.*

2. $a \wedge b = b \wedge r$.

Preuve. 1. Comme c divise a et b, alors il divise $a - bq = r$; donc c divise b et r. Et si c divise b et r, alors il divisera $bq + r = a$; d'où le résultat.
2. Immédiat. □

Une application répétée de ce principe conduit au célèbre algorithme d'Euclide.
Un **algorithme** est une suite finie et non ambiguë d'opérations ou d'instructions permettant de résoudre un problème ou d'obtenir un résultat. Le mot algorithme vient du nom arabe du mathématicien Al-Khawarizmi. La science qui étudie les algorithmes est appelé **l'algorithmique**. Cette science est utilisé actuellement dans de plusieurs domaines.

Théorème 4.5 (Algorithme d'Euclide)**.** *Soient a, $b \in \mathbb{N}^*$. On veut calculer $a \wedge b$.*
On forme une suite finie d'entiers r_k, à commencer par $r_0 = a$ et $r_1 = b$.
Soit $k \geq 1$. On suppose que r_{k-1} et r_k sont connus.
Si $r_k > 0$, on note $r_{k-1} = q_k r_k + r_{k+1}$ la division euclidienne de r_{k-1} par r_k. Sous l'hypothèse $r_k > 0$, on a donc défini r_{k+1}, avec $0 \leq r_{k+1} < r_k$. La suite d'entiers naturels $(r_k)_{k\geq 1}$ est finie car elle est strictement décroissante. Il existe donc un entier naturel n tel que $r_n > 0$ et $r_{n+1} = 0$. Avec ces notations, on a : $a \wedge b = r_n$. Ainsi $a \wedge b$ est le dernier reste non nul dans cette succession de divisions.

Preuve. Soient a et b deux entiers naturels non nuls, notons $r_0 = a$ et $r_1 = b$.
Par la division euclidienne de a par b on a : $r_0 = r_1 q_1 + r_2$, avec $0 \leq r_2 < b = r_1$.
→ Si $r_2 = 0$, alors $b = r_1$ divise $r_0 = a$ et $a \wedge b = b$.
→ Si $r_2 \neq 0$, alors $a \wedge b = b \wedge r_2$; et $b = r_2 q_2 + r_3$, avec $0 \leq r_3 < r_2$.
  → Si $r_3 = 0$, alors r_2 divise b et $a \wedge b = b \wedge r_2 = r_2$.
  → Si $r_3 \neq 0$, alors $b \wedge r_2 = r_2 \wedge r_3$; $r_2 = r_3 q_3 + r_4$, et $0 \leq r_4 < r_3$.
On construit ainsi une suite (r_k) d'entiers naturels tels que :

$$a = r_0 > r_1 = b > r_2 > r_3 > ... > r_{n-1} > r_n \geq 0.$$

Cette suite est strictement décroissante, et son nombre de termes non nuls est fini. Notons n le plus petit entier tel que $r_n = 0$. D'où r_{n-1} est le dernier reste non nul. Par suite $a \wedge b = r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge r_n = r_{n-1} \wedge 0 = r_{n-1}$. □

Remarque 4.7. Soient a, $b \in \mathbb{N}^*$. Soit (q, r) le quotient et le reste de la division euclidienne de a par b. Pour calculer $a \wedge b$, on suggère l'algorithme suivant.
1. Réaliser la division euclidienne de a par b. Ceci produit des entiers q et r.
2. Si $r = 0$, alors rendre comme résultat b.
3. Sinon, remplacer a par b et b par r.
4. Retourner en 1.

Exemples 23.

1. Cherchons $256 \wedge 74$. Les divisions successives qui donnent ce pgcd sont :

$$\begin{aligned}
256 &= 74 \times 3 + 34\\
74 &= 34 \times 2 + 6\\
34 &= 6 \times 5 + 4\\
6 &= 4 \times 1 + 2\\
4 &= 2 \times 2 + 0.
\end{aligned}$$

Le dernier reste non nul est 2. Donc $256 \wedge 74 = 2$

2. Cherchons $3675 \wedge 456$. Les divisions successives qui donnent ce pgdc sont :

$$\begin{aligned}
3675 &= 456 \times 8 + 27\\
456 &= 27 \times 16 + 24\\
27 &= 24 \times 1 + 3\\
24 &= 3 \times 8 + 0.
\end{aligned}$$

Le dernier reste non nul est 3. Donc $3675 \wedge 456 = 3$.

Théorème 4.6 (identité de Bezout). *Soient $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$ et $\delta = a \wedge b$. Alors il existe $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = \delta$. Le couple (u,v) s'appelle un couple de coefficients de Bezout.*

Remarques 4.8.

1. Les coefficients de Bezout ne sont pas uniques. Si (u_0, v_0) est un couple de coefficients de Bezout, tous les couples de la forme $(u_0 + kb, v_0 - ka)$ avec $k \in \mathbb{Z}$ le sont aussi. En effet,

$$a(u_0 + kb) + b(v_0 - ka) = au_0 + akb + bv_0 - bka = au_0 + bv_0 + k(ab - ba) = au_0 + bv_0 = \delta.$$

2. La réciproque de ce théorème est fausse. Ainsi $6 = 6 \times 6 - 2 \times 15$ mais $6 \wedge 15 \neq 6$.

Preuve du théorème. Soit l'ensemble

$$A = \{n \in \mathbb{N}^* \mid n = au + bv, u \in \mathbb{Z}, v \in \mathbb{Z}\}.$$

On a $A \neq \varnothing$, car $a^2 + b^2 = a.a + b.b$, ($u = a$ et $b = v$), donc $a^2 + b^2 \in A$. Par suite A est une partie non vide de $\mathbb{N}$, d'où A admet un plus petit élément, i.e.

$$\exists p \in A \text{ tel que } \forall x \in A, p \leq x.$$

Donc il existe $(u_0, v_0) \in \mathbb{Z}^2$ tel que $p = au_0 + bv_0$. Montrons que $p = \delta$.

Puisque $\delta | a$ et $\delta | b$, alors $a = \delta k_1$ et $b = \delta k_2$, $k_i \in \mathbb{Z}$. D'où

$$p = au_0 + bv_0 = \delta(k_1 u_0 + k_2 v_0),$$

alors $\delta | p$ et par suite $\delta \leq p$.

Par la division euclidienne de a par p, il existe $(q,r) \in \mathbb{Z}^2$ tel que $a = pq + r$ et $0 \leq r < p$, d'où $r = a - q(au_0 + bv_0) = (1 - qu_0)a - bv_0$. (1)
Donc si $r > 0$, alors l'équation (1) implique que $r \in A$, et comme $r < p$ alors ceci contredit le fait que p est le plus petit élément de A. Donc $r = 0$, et par suite $p | a$. On démontre de la même façon que $p | b$. Ceci implique que p est un diviseur commun de a et b, d'où $p \leq \delta$. Donc $p = \delta$. □

De cette démonstration, on déduit le lemme suivant.

Lemme 4.7. *Soit* $(a,b) \in \mathbb{Z}^{*2}$. $\delta = a \wedge b$ *est le plus petit élément strictement positif de l'ensemble* $A = \{x \in \mathbb{Z} \mid x = au + bv, (u,v) \in \mathbb{Z}^2\}$.

Exemple 4.9 (L'algorithme d'Euclide et les coefficients de Bezout). Considérons le nombre $3675 \wedge 456$ de l'exemple 23. Réécrivons les divisions euclidiennes de l'algorithme d'Euclide sous une autre forme :

$$\begin{aligned} 27 &= 3675 - 456 \times 8 \\ 24 &= 456 - 27 \times 16 \\ 3 &= 27 - 24 \times 1. \end{aligned}$$

On part ensuite du pgcd (c'est-à-dire 3) et on remonte les lignes de la manière suivante :

$$\begin{aligned} 3 &= 27 - 24 \times 1. \\ &= 27 - (456 - 27 \times 16) \times 1 = 27 - 456 + 27 \times 1 \times 16 = 27 \times 17 - 456 \times 1 \\ &= (3675 - 456 \times 8) \times 17 - 456 \times 1 = 3675 \times 17 - 456 \times 8 \times 17 - 456 \times 1 \\ &= 3675 \times 17 - 456 \times 135. \end{aligned}$$

Ceci donne l'identité de Bezout : $3 = 3675 \times 17 - 456 \times 135$.

Proposition 4.8. *Soit* $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. *L'entier strictement positif* $\delta = a \wedge b$ *est caractérisé par l'égalité*

$$D_\delta = D_a \cap D_b.$$

Preuve. Soit $c \in D_\delta$, c-à-d, c est un diviseur de δ. Comme δ divise a et b, alors c divise a et b, par suite $c \in D_a \cap D_b$. D'où $D_\delta \subset D_a \cap D_b$.

Réciproquement, soit $c \in D_a \cap D_b$, donc c est un diviseur commun de a et b, par suite $a = ck_1$ et $b = ck_2$. Or il existe $(u,v) \in \mathbb{Z}^2$ tel que $\delta = au + bv$; d'où $\delta = au + bv = c(uk_1 + vk_2)$, ce qui donne que c divise δ. □

Proposition 4.9. *Soit* $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$.

1. *Pour tout entier strictement positif* c, *on a :* $(ca) \wedge (cb) = c(a \wedge b)$.
2. *Si* k *est un diviseur commun de* a *et* b, *alors* $\frac{a}{k} \wedge \frac{b}{k} = \frac{a \wedge b}{|k|}$.

Preuve. 1. Posons $\delta = a \wedge b$, alors $a = \delta k_1$ et $b = \delta k_2$, d'où $ca = c\delta k_1$ et $cb = c\delta k_2$. Par suite $c\delta$ est un diviseur commun de ca et cb, d'où $c\delta \leq \delta'$, où $\delta' = ca \wedge cb$.

D'autre part, il existe u, v dans $\mathbb{Z}$ tels que $\delta = au+bv$, ce qui donne que $c\delta = cau+cbv$; d'où $c\delta \in A = \{u(ca) + v(cb) \mid u, v \in \mathbb{Z}\}$. Par suite $\delta' \leq c\delta$, puisque δ' est le plus petit élément de A, et donc $\delta' = c\delta$.

2. Si k est un diviseur commun de a et b, alors il existe $(a', b') \in \mathbb{Z}^2$ tel que $a = ka'$ et $b = kb'$; d'après le point (1) on a : $a \wedge b = (ka') \wedge (kb') = |k|(a' \wedge b')$, donc

$$\frac{a \wedge b}{|k|} = a' \wedge b' = \frac{a}{k} \wedge \frac{b}{k}.$$

□

4.4. **Nombres premiers entre eux.**

4.4.1. **Définition et propriétés.**

Définition 4.10. Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On dit que a et b sont premiers entre eux si $a \wedge b = 1$.

Exemple 4.11.
- 3 et 13 sont premiers entre eux.
- 15 et 32 sont premiers entre eux.

Théorème 4.10 (Théorème de Bezout)**.** *Soit $(a,b) \in \mathbb{Z}^2 - \{(0,0)\}$. On a alors l'équivalence :*

$$a \wedge b = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2,\ au + bv = 1.$$

Preuve. Le sens direct est trivial par le Théorème 4.6

Réciproquement, soient a et b dans $\mathbb{Z}$ tels que $au + bv = 1$, où u et v sont dans $\mathbb{Z}$, alors nous avons déjà montré que tout diviseur commun de a et b divise 1, donc $D_a \cap D_b = \{-1, 1\}$. Par suite $\mathrm{pgcd}(a,b) = 1$. □

Théorème 4.11 (Lemme de Gauss)**.** *Soit $(a,b,c) \in \mathbb{Z}^3$ tel que $c|ab$ et $a \wedge c = 1$. Alors $c|b$.*

Preuve. Si c divise ab et $a \wedge c = 1$, alors ils existent u, v et k dans $\mathbb{Z}$ tels que $ab = kc$ et $au + cv = 1$; donc $b = b(au + cv) = abu + bcv = kcu + bcv = c(ku + bv)$, ce qui implique c divise b. □

Théorème 4.12. *Soient a, b et c dans $\mathbb{Z}$ tels que $a \wedge b = 1$, $a \mid c$ et $b \mid c$. Alors $ab \mid c$.*

Preuve. Comme a divise c, alors il existe $k \in \mathbb{Z}$ tel que $c = ak$. Or $b|c$, donc $b|ak$, et comme $a \wedge b = 1$, alors par le Lemme de Gauss on a $b|k$, il existe donc $k' \in \mathbb{Z}$ tel que $abk' = c$. D'où $ab|c$. □

Proposition 4.13. *Soient $a_1, a_2, \cdots, a_r$ des entiers dans $\mathbb{Z}$ et $n \in \mathbb{Z}$.*

1. *Si $a_1, a_2, \cdots, a_r$ sont tous premiers avec n, alors le produit $a_1 a_2 \cdots a_r$ est également premier avec n.*
2. *Si $a_1, a_2, \cdots, a_r$ sont premiers entre eux deux à deux. Alors le produit $a_1 a_2 \cdots a_r$ divise n si et seulement pour tout i, a_i divise n.*

Preuve. Par récurrence sur r. □

4.4.2. **Équation diophantienne du premier degré.**
On se donne trois entiers relatifs a, b et c tels que $(a,b) \neq (0,0)$. On veut résoudre dans $\mathbb{Z}^2$ l'équation

$$ax + by = c$$

d'inconnues x et y.

Lemme 4.14. *L'équation $ax + by = c$ admet au moins une solution dans $\mathbb{Z}^2$ si, et seulement si, $\delta = a \wedge b$ divise c.*

Preuve. Supposons que l'équation admette une solution (x_0, y_0). Comme δ divise a et b, $\delta \mid ax_0 + by_0 = c$ d'où le résultat.
Si $c = \delta c'$ est un multiple de δ, en écrivant que $\delta = au_0 + bv_0$ avec u_0, v_0 dans $\mathbb{Z}$

(Théorème4.6), alors $c = \delta c' = au_0c' + bv_0c'$. On déduit donc que $(x_0, y_0) = (u_0c', v_0c')$ est une solution de $ax + by = c$. $\square$

Théorème 4.15. *L'équation $ax + by = c$ possède une solution, si et seulement si $a \wedge b | c$. Lorsque cette condition est satisfaite, et si (x_0, y_0) est une solution particulière de l'équation, alors tout autre solution (x,y) est de la forme $x = x_0 + kb'$ et $y = y_0 - ka'$, $k \in \mathbb{Z}$, où $a' = \frac{a}{a \wedge b}$ et $b' = \frac{b}{a \wedge b}$.*

Pour déterminer une solution particulière, on utilise l'algorithme d'Euclide pour déterminer des coéffcients de Bézout (u,v) du couple (a,b). On a alors $au + bv = d = a \wedge b$. On pose $h = \frac{c}{d}$, alors $(x_0, y_0) = (uh,vh)$ est une solution particulière de l'équation.

Exemple 4.12. Soit à résoudre l'équation $224x + 175y = 21$. On a $224 \wedge 175 = 7 | 21$, donc l'équation possède des solutions. On a $(-7 \times 224) + (9 \times 175) = 7$. Donc, $(-21 \times 224) + (27 \times 175) = 21$. Une solution particulière est donc $(-21,27)$. $a' = \frac{224}{7} = 32$, $b' = \frac{175}{7} = 25$. La solution générale de l'équation est $(x,y) = (-21 + 25k, 27 - 32k)$, $k \in \mathbb{Z}$.

4.5. **Plus petit commun multiple (PPCM).**

Définition 4.13. Soient a et b deux entiers relatifs non nuls. Un multiple commun de a et b est un entier relatif divisible à la fois par a et b. L'ensemble des multiples communs de a et b est noté $a\mathbb{Z} \cap b\mathbb{Z}$.

Définition 4.14. Soient a et b deux entiers relatifs non nuls. **Le plus petit commun multiple** de a et b est le plus petit entier strictement positif de l'ensemble des multiples communs de a et b, i.e. $a\mathbb{Z} \cap b\mathbb{Z}$. On le note $\text{ppcm}(a, b)$ ou $a \vee b$.

Remarque 4.15. Le $\text{ppcm}(a, b)$ est défini aussi comme étant l'entier naturel m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Propriétés 3. *Soient a, b et c dans $\mathbb{Z}^*$.*

1. *Il est clair que $a \vee b = b \vee a$.*
2. *Il est clair aussi que $(a \vee b) \vee c = a \vee (b \vee c)$.*
3. *Pour tout $a \in \mathbb{Z}^*$, on a : $a \vee 1 = |a|$.*
4. *Pour tout $a \in \mathbb{Z}^*$, $a \vee a = |a|$.*
5. $a|b \Longleftrightarrow a \vee b = |b|$.
6. *Tout multiple commun de a et b est un multiple de $m = ppmc(a, b)$.*

Preuve. Montrons la dernière propriété.
Soit M un multiple commun de a et b. La division euclidienne de M par $m = a \vee b$ nous donne $M = mq + r$, où $0 \leq r < m$. Comme m et M sont des multiples de a et b, alors ils existent k_1 et k_2 dans $\mathbb{Z}$ tels que $M = ak_1$ et $m = ak_2$, d'où

$$r = M - mq = ak_1 - ak_2q = a(k_1 - k_2q).$$

Ceci implique que r est un multiple de a. De la même façon on montre que r est un multiple de b. Donc r est un multiple commun de a et b, or $0 \leq r < m$ et $m = a \vee b$, alors $r = 0$; d'où $M = mq$. $\square$

Théorème 4.16. *Soient a et b dans $\mathbb{Z}^*$. Posons $\delta = a \wedge b$ et $m = a \vee b$, alors*

$$m\delta = |ab|.$$

Preuve. Posons $\delta = a \wedge b$ et $m = a \vee b$, donc il existent α, β, c et d tels que

$$\begin{cases} a = \delta\alpha,\ b = \delta\beta, \\ \alpha \wedge \beta = 1, \\ m = ac = bd. \end{cases}$$

Donc en multipliant a par c, et b par d on a :

$$ac = bd \Longrightarrow \delta\alpha c = \delta\beta d \Longrightarrow \alpha c = \beta d,$$

d'où $\alpha|\beta d$, et comme $\alpha \wedge \beta = 1$, alors $\alpha|d$. Par suite il existe $k \in \mathbb{Z}$ tel que $d = \alpha k$, donc

$$\alpha c = \beta d \Longrightarrow \alpha c = \beta\alpha k \Longrightarrow c = \beta k.$$

Par suite $m = ac = a\beta k = \delta\alpha\beta k$, c'est-à-dire que $|\delta\alpha\beta|$ est un diviseur de m ; d'autre part $|\delta\alpha\beta|$ est un multiple commun de a et b (car $\beta a = \alpha\delta\beta$ et $\alpha b = \alpha\beta\delta$), donc forcement on doit avoir $m = |\alpha\beta\delta|$, ceci implique que $m\delta = |\alpha\delta\beta\delta| = |ab|$. □

Le résultat suivant est une simple déduction du théorème précédent.

Corollaire 4.17. *Soient a et b deux entiers relatifs premiers entre eux. Alors*

$$a \vee b = |ab|.$$

Preuve. Du fait que $|ab|$ est un multiple de a et b on déduit que $\mu = a \vee b$ divise $|ab|$.

D'autre part, il existe deux entiers k, k' tels que $\mu = ka = k'b$. Donc a divise $k'b$, et comme a est premier avec b, alors a divise k' (Lemme de Gauss). Ce qui donne $\mu = k''ab$. D'où $|ab|$ divise μ, par suite l'égalité $\mu = |ab|$. □

Proposition 4.18. *Soient a et b deux éléments de $\mathbb{Z}$.*
1. *Pour tout $c \in \mathbb{Z}$, on a : $ac \vee bc = |c|(a \vee b)$.*
2. *Pour tout diviseur commun $d \neq 0$ de a et b, on a : $\dfrac{a}{d} \vee \dfrac{b}{d} = \dfrac{a \vee b}{d}$.*

4.6. **Nombres premiers et factorisation.**

Définition 4.16. Soit $p \geq 2$ un entier. On dit que p est **premier** si les seuls diviseurs positifs de p sont 1 et p. Un entier ≥ 2 qui n'est pas premier est dit **composé**.

Exemple 4.17. 2, 3, 5, 7, 11 sont premiers, $4 = 2 \times 2$, $6 = 2 \times 3$, $8 = 2 \times 4$ ne sont pas premiers.

Théorème 4.19. *Tout entier $n \geq 2$ admet au moins un diviseur qui est un nombre premier.*

Preuve. Soit $\mathfrak{D}$ l'ensemble des diviseurs de n qui sont ≥ 2 :

$$\mathfrak{D} = \{k \geq 2|\ k|n\}$$

$\mathfrak{D}$ est une partie non vide de $\mathbb{N}$ (car $n \in \mathfrak{D}$), donc $\mathfrak{D}$ possède un plus petit élément p. Montrons que p est premier. Soit $d > 1$ un diviseur de p. On a $d \leq p$. Or $d|n$. D'où, par minimalité de p, $d = p$. □

Théorème 4.20 (Théorème d'Euclide sur les nombres premiers)**.** *Il existe une infinité de nombres premiers.*

Preuve. Par l'absurde, supposons qu'il n'y ait qu'un nombre fini de nombres premiers que l'on note $p_1 = 2$, $p_2 = 3$, p_3,..., p_n. Considérons l'entier $N = p_1 \times p_2 \times \cdots \times p_n + 1$. Soit p un diviseur premier de N (un tel p existe par le Théorème précédent), alors d'une part p est l'un des entiers p_i donc $p|p_1 \times p_2 \times \cdots \times p_n$, d'autre part $p|N$ donc p divise la différence $N - p_1 \times p_2 \times \cdots \times p_n = 1$. Cela implique que $p = 1$, ce qui contredit que p soit un nombre premier. □

Remarque 4.18. Les nombres premiers forment une suite d'entiers. A l'heure actuelle, on connait très peu de choses sur cette suite.

Proposition 4.21. *Soient $n \in \mathbb{Z}$ et p un nombre premier, alors ou bien $p|n$ ou bien $p \wedge n = 1$.*

Preuve. Supposons que $p \nmid n$ et soit $d = p \wedge n$. Comme $d|p$, on a $d = 1$ ou $d = p$. Supposons que $d = p$, alors $p|n$. Absurde. Donc $d = 1$. □

Théorème 4.22 (Lemme d'Euclide)**.** *Soient a, $b \in \mathbb{Z}$ et p un nombre premier. Si $p|ab$, alors $p|a$ ou $p|b$.*

Preuve. Si p ne divise pas a alors $p \wedge a = 1$ (d'après la proposition précédente). Ainsi par le lemme de Gauss $p|b$. □

Corollaire 4.23. *Soit p un nombre premier.*
1. *Si p divise un produit, alors il divise l'un de ses facteurs.*
2. *Si p divise un produit de nombres premiers, alors il est égal à l'un d'eux.*

Théorème 4.24. *Pour tout entier naturel $n \geq 2$, il existe des nombres premiers $p_1 < p_2 < \ldots < p_k$, des entiers naturels non nuls $m_1, m_2, \ldots, m_k$ tels que n s'écrit de manière unique sous la forme $n = p_1^{m_1} \times p_2^{m_2} \times \cdots p_k^{m_k}$.*

Exemple 4.19.

$$504 = 2^3 \times 3^2 \times 7 \qquad\qquad 300 = 2^2 \times 3 \times 5^2$$

Pour calculer le pgcd on réécrit ces décompositions

$$504 = 2^3 \times 3^2 \times 5^0 \times 7^1 \qquad\qquad 300 = 2^2 \times 3^1 \times 5^2 \times 7^0$$

Le pgcd s'obtient en prenant le plus petit exposant de chaque facteur premier

$$504 \wedge 300 = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12$$

Pour le ppcm on prend le plus grand exposant de chaque facteur premier

$$504 \vee 300 = 2^3 \times 3^2 \times 5^2 \times 7^1 = 12600$$

4.7. **Congruences dans $\mathbb{Z}$.**

Définition 4.20. Soit n un entier naturel, et soient a, b deux entiers relatifs quelconques. On dit que a et b sont congrus modulo n, et on écrit $a \equiv b\ [n]$, si $b-a$ est dans $n\mathbb{Z}$, c'est-à-dire $b-a$ est un multiple de n.

$$a \equiv b\ [n] \Longleftrightarrow \exists k \in \mathbb{Z},\, b-a = kn.$$

On définit ainsi une relation sur $\mathbb{Z}$, appelée relation de congruence modulo n.

Remarque 4.21.

- On a l'équivalence : $a \equiv b \quad [n] \Leftrightarrow (\exists k \in \mathbb{Z}, a = b + kn)$.
- $a \equiv b\ [n]$ équivaut à «a et b ont le même reste dans la division euclidienne par n».
- Pour $n = 0$, on a $0\mathbb{Z} = 0$ et $a \equiv b\ [0]$ revient à dire que $a = b$.
- Pour $n = 1$, on a $1\mathbb{Z} = \mathbb{Z}$, et la relation $a \equiv b\ [1]$ est toujours vérifiée.
- **On suppose donc, dans ce qui suit que $n \geq 2$.**

Proposition 4.25. *Soit n un entier naturel. La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.*

Preuve. Voir le chapitre 3. □

Proposition 4.26. *Soit n un entier strictement positif.*

1. *Pour tous entiers relatifs a, b, c, d on a les implications*

$$\begin{cases} a \equiv b\ [n] \\ c \equiv d\ [n] \end{cases} \Longrightarrow a + c \equiv b + d\ [n] \text{ et } ac \equiv bd\ [n]$$

On dit que la congruence est compatible avec l'addition et la multiplication.

2. *Pour tout entier naturel k, on a l'implication : $a \equiv b\ [kn] \Rightarrow a \equiv b\ [n]$.*
3. *Pour tout entier naturel k, on a l'implication : $a \equiv b\ [n] \Rightarrow a^k \equiv b^k\ [n]$.*
4. *Si q est un entier strictement positif, on a l'équivalence :*
   $a \equiv b\ [n] \Leftrightarrow qa \equiv qb\ [qn]$.
5. *Si les entiers q et n sont premiers entre eux, alors : $qa \equiv qb\ [n] \Rightarrow a \equiv b[n]$.*

Classes d'équivalences Soit n un entier strictement positif fixé. On note souvent $\overline{a}$ la classe d'équivalence de a pour la relation de congruence modulo n, c'est-à-dire l'ensemble des b de $\mathbb{Z}$ tels que $b \equiv a\ [n]$,

$$\overline{a} = \{b \in \mathbb{Z} |\ b \equiv a[n]\} = \{b \in \mathbb{Z} |\ b = a + kn, k \in \mathbb{Z}\} = \{a + kn |\ k \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

Tout élément x de $\overline{a}$ est un représentant de $\overline{a}$.
Avec ces notations, $\overline{0} = \overline{n}$ est l'ensemble de tous les multiples de n dans $\mathbb{Z}$.

Proposition 4.27. *Si a est un entier relative et n est un entier naturel, alors le reste de la division euclidienne de a par n est l'unique entier b tel que*

$$a \equiv b \pmod{n} \text{ et } 0 \leq b < n.$$

Preuve. Notons par q et r le quotient et le reste la division euclidienne de a par n, alors

$$a = nq + r \text{ et } 0 \leq r < n.$$

Donc $a-r=nq$, d'où $a \equiv r \pmod{n}$.

Supposons b est un entier tel que $a \equiv b \pmod{n}$ et $0 \leq b < n$. Comme $a \equiv r \pmod{n}$, alors $b \equiv r \pmod{n}$. D'où $b-r$ est un multiple de n. Or $-n < b-r < n$, donc $b-r=0$, c-à-d, $b=r$. □

De cette proposition découle que tout entier relatif a est congru, modulo n, à un unique entier r de $\{0, ..., n-1\}$ qui est le reste dans la division de a par n.
Il y a donc exactement n classes d'équivalences modulo n, et on note souvent l'ensemble des classes d'équivalence par :

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$
$$\mathbb{Z}_0 = \mathbb{Z}/0\mathbb{Z} = \{\{a\} |\ a \in \mathbb{Z}\}.$$
$$\mathbb{Z}_1 = \mathbb{Z}/1\mathbb{Z} = \{\mathbb{Z}\} = \{\overline{0}\}.$$

Théorème 4.28. *Pour tout entier naturel non nul n, on a : $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$. Cet ensemble est de cardinal égal à n et il est en bijection avec l'ensemble de tous les restes dans la division euclidienne par n.*

Théorème 4.29 (Petit Théorème de Fermat). *Soit p un nombre premier, alors pour tout $a \in \mathbb{Z}$ on a :*

$$a^p \equiv a \pmod{p}.$$

De plus, si $a \wedge p = 1$, alors $a^{p-1} \equiv 1 \pmod{p}$.

Lemme 4.30. *p divise $\binom{p}{k}$ pour $1 \leq k \leq p-1$, c'est-à-dire $\binom{p}{k} \equiv 0 \pmod{p}$.*

Preuve. $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ donc $p! = k!(p-k)!\binom{p}{k}$. Ainsi $p | k!(p-k)!\binom{p}{k}$. Or comme $1 \leq k \leq p-1$ alors p ne divise pas $k!$ (sinon p divise l'un des facteurs de $k!$ mais il sont tous $< p$). De même p ne divise pas $(p-k)!$, donc par le lemme d'Euclide p divise $\binom{p}{k}$. □

Preuve du théorème. Nous le montrons par récurrence pour les $a \geq 0$.

- Si $a = 0$ alors $0 \equiv 0 \pmod{p}$.
- Fixons $a \geq 0$ et supposons que $a^p \equiv a \pmod{p}$. Calculons $(a+1)^p$ à l'aide de la formule du binôme de Newton :
$$(a+1)^p = a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \cdots + \binom{p}{1} + 1$$
Réduisons maintenant modulo p :
$$\begin{aligned}(a+1)^p &\equiv a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \cdots + \binom{p}{1} + 1 \pmod{p} \\ &\equiv a^p + 1 \pmod{p} \quad \text{grâce au lemme 4.30} \\ &\equiv a + 1 \pmod{p} \quad \text{à cause de l'hypothèse de récurrence}\end{aligned}$$
- Par le principe de récurrence nous avons démontré le petit théorème de Fermat pour tout $a \geq 0$. Il n'est pas dur d'en déduire le cas des $a \leq 0$.

□

Exemple 4.22. Calculons $14^{3141} \pmod{17}$. Le nombre 17 étant premier on sait par le petit théorème de Fermat que $14^{16} \equiv 1 \pmod{17}$. Écrivons la division euclidienne de 3141 par 16 :

$$3141 = 16 \times 196 + 5.$$

Alors

$$\begin{aligned} 14^{3141} &\equiv 14^{16\times196+5} \equiv 14^{16\times196} \times 14^5 \\ &\equiv \left(14^{16}\right)^{196} \times 14^5 \equiv 1^{196} \times 14^5 \\ &\equiv 14^5 \pmod{17} \end{aligned}$$

Il ne reste plus qu'à calculer 14^5 modulo 17. Cela peut se faire rapidement : $14 \equiv -3 \pmod{17}$ donc $14^2 \equiv (-3)^2 \equiv 9 \pmod{17}$, $14^3 \equiv 14^2 \times 14 \equiv 9 \times (-3) \equiv -27 \equiv 7 \pmod{17}$, $14^5 \equiv 14^2 \times 14^3 \equiv 9 \times 7 \equiv 63 \equiv 12 \pmod{17}$. Conclusion : $14^{3141} \equiv 14^5 \equiv 12 \pmod{17}$.