Sommaire

Compétences en arithmétique

A la fin de cours vous devriez maîtrisez les techniques suivants :

1. Utiliser l'algorithme d'Euclide pour :
   - déterminer le plus grand diviseur commun de deux entiers
   - déterminer les coefficients de Bézout dans l'écriture :

$$a \wedge b = au + bv$$

2. Écrire un entier naturel dans un système de numération de base donnée
3. Additionner, multiplier et comparer deux entiers dans un système de numération de base donnée
4. Utiliser les écritures dans des systèmes de numération dans des situations d'arithmétique
5. Utiliser la décomposition en produit de facteurs premiers dans :
   - la détermination du plus petit multiple commun (PPCM)
   - la détermination du plus grand diviseur commun (PGCD) de deux ou plusieurs entiers
   - la détermination des diviseurs d'un entier
6. Utiliser :
   - la congruence modulo n
   - les propriétés des opérations dans $\mathbb{Z}/n\mathbb{Z}$
   - la structure de $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ dans des situations d'arithmétique
7. Utiliser :
   - la divisibilité
   - la division euclidienne
   - les théorèmes de Gauss, de Bézout et de Fermat
   - le théorème fondamental de l'arithmétique
   - les propriétés des nombres premiers et des nombres premiers entre eux dans des situations d'arithmétique
8. Résoudre l'équation $ax + by = c$ dans $\mathbb{Z} \times \mathbb{Z}$

I Rappels et compléments

I.1 Propriété fondamentale de $\mathbb{N}$

L'ensemble $\mathbb{N}$ est caractérisé par la propriété suivante que l'on admet:

Théorème I.1 (Admis)**.** Toute partie non vide de $\mathbb{N}$ est minorée et admet un plus petit élément.

De ce théorème on peut conlcure que:

Théorème I.2. Toute partie non vide de $\mathbb{N}$ majorée admet un plus grand élément.

Démonstration. Soit $A \subseteq \mathbb{N}$ une partie non vide et majorée, M un majorant de A, et $S = \{s \in \mathbb{N} \mid \forall n \in A, n \leq s\}$ l'ensemble des majorants de A.
Puisque $M \in S$, l'ensemble S est non vide.
Par le théorème fondamental de $\mathbb{N}$, S admet un minimum, noté $m = \min(S)$.
Prouvons par l'absurde que $m = \max(A)$.
Supposons que $m \neq \max(A)$, c'est-à-dire que $\forall n \in A, n < m$.
Alors, $\forall n \in A, n \leq m-1$, ce qui implique que $m - 1 \in S$.
Cependant, comme $m = \min(S)$, on doit avoir $m \leq m-1$, ce qui est absurde.
Ainsi, $m = \max(A)$.

□

I.2 Propriété fondamentale de $\mathbb{Z}$

Théorème I.3. L'ensemble $\mathbb{Z}$ est caractérisé par la propriété suivante:

- Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.
- Toute partie non vide et minorée de $\mathbb{Z}$ admet un plus petit élément.

Démonstration. 1. Soit $A \subseteq \mathbb{Z}$ une partie non vide et majorée, M un majorant de A.

Soit $B^+ = A \cap \mathbb{N}$, B^+ est une partie de $\mathbb{N}$, on distingue deux cas:

- Si B^+ est non vide alors M est un majorant de B^+.
  Par le deuxième théorème fondamentale de $\mathbb{N}$, B^+ admet un plus grand élément noté M.

  Donc M est aussi maximum de A.

- Si B^+ est vide, alors $A \subset \mathbb{Z}^-$
  On définit $B'^+ = -A \cap \mathbb{Z}^-$, alors $B'^+ \subset \mathbb{N}$.
  Comme B'^+ est non vide, et $B'^+ \subset \mathbb{N}$ alors par le théorème fondamentale de $\mathbb{N}$ admet un minimum note m'.
  On a alors

$$\begin{aligned} m' = \min(B'^-) &\iff \forall n \in B'^- \quad m' \leq n \text{ et } m' \in B'^- \\ &\iff \forall n \in A; \quad m' \leq -n \text{ et } m' \in -A \\ &\iff \forall n \in A; \quad n \leq -m' \text{ et } -m' \in A \\ &\iff -m' = \max(A) \end{aligned}$$

  Dans les deux cas l'ensemble A admet un plus grand élément.

2. Soit B une partie non vide de $\mathbb{Z}$, minorée.
   L'ensemble $A' = -B$ est non vide majorée. donc par la premier point, A' admet un plus grand élément, noté M':

$$\begin{aligned} M' = \max(A') &\iff \forall n \in A'; \quad n \leq M' \text{ et } M' \in A' \\ &\iff \forall n \in B; \quad -n \leq M' \text{ et } M' \in -B \\ &\iff \forall n \in B; \quad -M' \leq n \text{ et } -M' \in B \\ &\iff -M' = \min(B) \end{aligned}$$

   Donc B admet un plus petit élément.

□

Exemple I.4. L'ensemble $A = \{n \in \mathbb{Z}, (n+2)^2 \leq 6\}$ est borné.
Son plus grand élément est 0 et son plus petit élément est -4.

Théorème I.5. Soit a et b deux entiers relatifs tels que $b \neq 0$.
Il existe un entier relatif n tel que : $nb \geq a$.
On dit que $\mathbb{Z}$ est archimédien.

Démonstration. • 1^{er} cas : $b \geq 1$

– si $a \geq 0$, il suffit de prendre : $n = a$;

– si $a < 0$, il suffit de prendre : $n = 0$.

- 2^{em} cas : $b \leq -1$
  On a : $-b \geq 1$; donc il existe un entier relatif m, tel que : $m(-b) \geq a$.
  Il suffit donc de prendre : $n = -m$.

□

II Division euclidienne dans $\mathbb{Z}$

Théorème II.1. La division Euclidienne
Soit a et b deux entiers relatifs tels que : $b \neq 0$.
Il existe un unique couple $(q; r)$ de $\mathbb{Z} \times \mathbb{N}$ tel que : $a = bq + r$ et $0 \leq r < |b|$.

Les nombres q et r s'appellent respectivement le quotient et le reste de la division euclidienne de a par b. Effectuer une division euclidienne c'est déterminer son quotient et son reste.

Démonstration.

- Existence:
  Soit $A = \{n \in \mathbb{N} \quad / \exists q \in \mathbb{Z} : \quad n = a - bq\}$.
  On a $a + |ba| \in A$,
  Donc A est une partie non vide de $\mathbb{N}$,
  Par le théorème fondamentale de $\mathbb{N}$, A admet un plus petit élément $r = \min(A)$.
  Comme $r = \min(A)$; donc $r \geq 0$ et $\exists q \in \mathbb{Z} : \quad r = a - bq$ $(q \in \mathbb{Z})$.
  Montrons par l'absurde que : $r < |b|$
  Supposons que $r \geq |b|$.
  On a : $r - |b| = a - bq - |b| = a - bq'$;
  Donc, $r - |b| \in A$, plus petit que r ; Ce qui est absurde.
  On en déduit qu'il existe un couple $(q; r)$ de $\mathbb{Z} \times \mathbb{N}$ tel que : $a = bq + r$ et $0 \leq r < |b|$.
- Unicité:
  Soit $(q; r)$ et $(q'; r')$ deux couples de $\mathbb{Z} \times \mathbb{N}$ tels que :
  $a = bq + r$, $a = bq' + r'$, $0 \leq r < |b|$ et $0 \leq r' < |b|$.
  On a : $0 = b(q' - q) + (r' - r)$; donc : $|b| \cdot |q' - q| = |r' - r|$.
  Or : $-|b| < r' - r < |b|$; donc : $|r' - r| < |b|$.
  On en déduit que : $|q' - q| = 0$ (si $|q' - q| \geq 1$, on aurait : $|b| \cdot |q' - q| \geq |b|$).
  De plus : $|r' - r| = |b| \cdot |q' - q|$;
  Donc : $q' = q$ et $r' = r$.

□

Exemple II.2. Effectuer la division euclidienne de a par b dans chacun des cas suivants :
$a = 63$ et $b = 13$; $a = -63$ et $b = 13$; $a = 63$ et $b = -13$; $a = -63$ et $b = -13$.

- On a : $63 = 13 \times 4 + 11$ et $0 \leq 11 < 13$.
  Donc : 4 et 11 sont respectivement le quotient et le reste de la division euclidienne de 63 par 13.
- On a : $-63 = 13 \times (-5) - 8 = 13 \times (-6) + 5$ et $0 \leq 5 < 13$.
  Donc : -6 et 5 sont respectivement le quotient et le reste de la division euclidienne de -63 par 13.
- On a : $63 = (-13) \times (-4) + 11$ et $0 \leq 11 < 13$.
  Donc : -4 et 11 sont respectivement le quotient et le reste de la division euclidienne de 63 par -13.
- On a : $-63 = (-13) \times 6 + 5$ et $0 \leq 5 < 13$.
  Donc : 6 et 5 sont respectivement le quotient et le reste de la division euclidienne de -63 par -13.

***Exercice* II.1.** Effectuer la division euclidienne de a par b dans chacun des cas suivants :
$a = 108$ et $b = 7$; $a = -108$ et $b = 7$; $a = 108$ et $b = -7$; $a = -108$ et $b = -7$.

***Exercice* II.2.** On divise 524 par un entier non nul inconnu, d. Le quotient vaut $q = 26$ et le reste r.
Trouver d et r.

III Divisibilité dans $\mathbb{Z}$

III.1 Multiples et diviseurs d'un entier relatif

III.1.1 Définition et propriétés

Définition III.1. Soit a et b deux entiers relatifs. On dit que a est un **multiple** de b s'il existe un entier relatif k tel que :

$$a = k \times b$$

Si de plus $b \neq 0$, on dit que b est un **diviseur** de a ou que b divise a, noté $b \mid a$.

Exemple III.2.
- Puisque $143 = 11 \times 13$:
  - 143 est multiple de 11 et de 13.
  - 11 et 13 divisent 143.
- Puisque $12 = (-4) \times (-3)$:
  - 12 est multiple de -4.
  - -4 divise 12.

Remarque III.3.
- Tout entier relatif est multiple de 1 et -1.
- 1 et -1 divisent tout entier relatif.
- 0 est multiple de tout entier relatif.
- Tout entier relatif non nul divise 0, mais 0 ne divise aucun entier relatif.
- Si $b \neq 0$, alors a est multiple de b (ou b divise a) si et seulement si le reste de la division euclidienne de a par b est nul.

Théorème III.4 (Diviseurs et valeur absolue)**.** Soit a et b deux entiers relatifs non nuls. Si b divise a, alors :

$$|b| \leq |a|$$

Démonstration. Si b divise a, il existe un entier relatif non nul q tel que $a = bq$. Puisque $1 \leq |q|$, on a :

$$|b| \leq |b||q| = |bq| = |a|$$

□

III.2 Propriétés de la divisibilité

Propriété 1. Soit a, b, c trois entiers relatifs $(a \neq 0, b \neq 0)$. Alors :

1. a divise a (*réflexivité*).
2. Si a divise b et b divise a, alors $a = b$ ou $a = -b$ (*antisymétrie*).
3. Si a divise b et b divise c, alors a divise c (*transitivité*).

Démonstration.
1. *Réflexivité* : $a = a \times 1$, donc a divise a.
2. *Antisymétrie* : Si a divise b, alors $|a| \leq |b|$. Si b divise a, alors $|b| \leq |a|$. Ainsi, $|a| = |b|$, d'où $a = b$ ou $a = -b$.
3. *Transitivité* : Si a divise b, alors $b = ak$ pour un entier k. Si b divise c, alors $c = bl$ pour un entier l. Ainsi, $c = a(kl)$, donc a divise c.

□

Propriété 2. Soit a, b, c trois entiers relatifs $(a \neq 0)$. Si a divise b et c, alors pour tous entiers relatifs p et q :

$$a \text{ divise } pb + qc$$

Démonstration. Si a divise b, alors $b = ak$ pour un entier k. Si a divise c, alors $c = al$ pour un entier l. Ainsi, $pb + qc = p(ak) + q(al) = a(pk + ql)$, donc a divise $pb + qc$. □

Exemple III.5.
- La somme ou la différence de deux entiers relatifs pairs est un entier relatif pair.
- Le produit d'un entier relatif par un entier relatif pair est un entier relatif pair.

III.3 Ensemble des multiples

Soit b un entier relatif. Les multiples de b sont les nombres de la forme bk, où $k \in \mathbb{Z}$. On note l'ensemble des multiples de b par $b\mathbb{Z}$.

Exemple III.6.
- $3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$
- $-2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$
- $1\mathbb{Z} = \mathbb{Z}$
- $0\mathbb{Z} = \{0\}$

Remarque III.7. Pour tout entier relatif b, $(b\mathbb{Z}, +)$ est un groupe commutatif.

III.4 Ensemble des diviseurs

Soit a un entier relatif. On note $\mathcal{D}(a)$ l'ensemble des diviseurs de a.

Exemple III.8.
- $\mathcal{D}(4) = \{-4, -2, -1, 1, 2, 4\}$
- $\mathcal{D}(-6) = \{-6, -3, -2, -1, 1, 2, 3, 6\}$
- $\mathcal{D}(1) = \{-1, 1\}$
- $\mathcal{D}(0) = \mathbb{Z}^\star$ (ensemble des entiers relatifs non nuls)

Remarque III.9. Pour tout entier relatif a non nul, $\mathcal{D}(a)$ est :

- Un ensemble fini non vide.
- Symétrique par rapport à 0.
- De cardinal pair (sauf pour $a = 0$).

***Exercice* III.1.**

1. (a) Démontrer que si les entiers naturels non nuls a, b et n vérifient la relation :

$$ab = (a+b)n \quad \text{on a :} \quad a > n \quad \text{et} \quad b > n.$$

   (b) Que devient la relation précédente quand on pose $a = n + X$ et $b = n + Y$?

   (c) Déterminer tous les couples d'entiers (a, b) tels que $ab = 6(a + b)$.

2. (a) Démontrer que si les entiers naturels non nuls x, y, m et p vérifient la relation :

$$xy = px + my \quad \text{on a :} \quad x > m \quad \text{et} \quad y > p.$$

   Transformer cette relation en posant :

$$x = m + X, \quad y = p + Y.$$

   (b) Déterminer les couples d'entiers (x, y) tels que $xy = 3x + 5y$.

3. (a) Transformer la relation $xy = px + my + 9$ en posant $x = m + X$ et $y = p + Y$.

   (b) Résoudre en $\mathbb{N}^2$ l'équation :

$$xy = 4x + 2y + 7.$$

IV Relations binaires

Définition IV.1. Soit E un ensemble non vide. Une *relation binaire* $\mathcal{R}$ sur E est une partie A de $E \times E$. Pour tout $(x, y) \in E \times E$, on note :

$$x\mathcal{R}y \iff (x, y) \in A$$

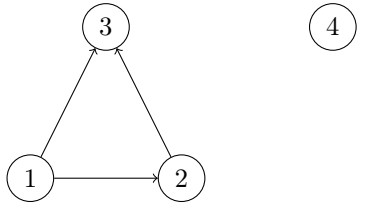
On dit que x est en relation avec y lorsque $x\mathcal{R}y$.

Une relation binaire peut être vue comme une règle qui détermine si deux éléments d'un ensemble sont connectés d'une certaine manière. Par exemple, imaginons un ensemble E représentant des personnes dans un réseau social. Une relation $\mathcal{R}$ pourrait être définie par « $x\mathcal{R}y$ si x est ami avec y ». Dans ce cas, $(x, y) \in \mathcal{R}$ signifie que x et y sont amis. Cette idée s'étend à d'autres contextes, comme des nombres liés par une inégalité (par exemple, $x \leq y$) ou des objets partageant une propriété commune.

IV.1 Représentation graphique

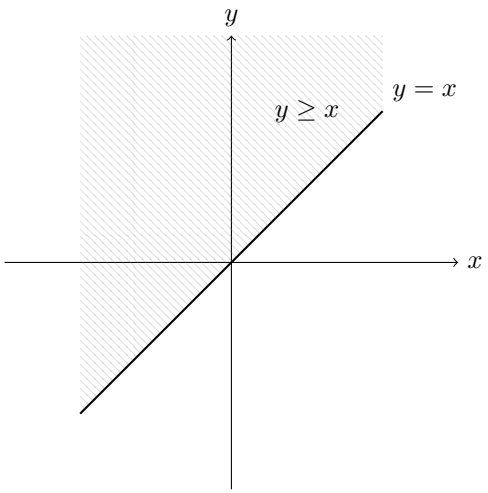
Une relation binaire sur un ensemble E peut être visualisée de deux manières principales :

- **Graphe orienté (pour un ensemble fini)** : Si E est fini, on représente les éléments de E comme des points (sommets) et la relation $\mathcal{R}$ par des flèches (arcs). Une flèche de x à y existe si $x\mathcal{R}y$. Par exemple, pour $E = \{1, 2, 3\}$ et $\mathcal{R} = \{(1, 2), (2, 3), (1, 3)\}$, le graphe est :



$(2, 1)$ n'appartient pas à $\mathcal{R}$ donc ne sont pas en relation(dans cet ordre) : $2\ \mathcal{R}1$.
$(2, 4)$ n'appartient pas à $\mathcal{R}$ donc ne sont pas en relation(dans cet ordre) : $2\ \mathcal{R}4$.

- **Sous-ensemble du plan cartésien (pour $E = \mathbb{R}$)** : Si $E = \mathbb{R}$, la relation $\mathcal{R}$ est un sous-ensemble de $\mathbb{R} \times \mathbb{R}$, visualisé dans le plan cartésien. Par exemple, la relation $x\mathcal{R}y \iff y = x$ correspond à la droite $y = x$. La relation $x\mathcal{R}y \iff x \leq y$ (ou de manière équivalente, $y - x \geq 0$) correspond à la région au-dessus de la droite $y = x$, y compris la droite elle-même. Cette région est illustrée ci-dessous :



Représentation de la relation $x\mathcal{R}y \iff y - x \geq 0$ (ou $y \geq x$) dans le plan cartésien.

Définition IV.2 (Propriétés des relations binaires)**.** Soit $\mathcal{R}$ une relation binaire sur un ensemble E. On dit que $\mathcal{R}$ est :

1. **Réflexive** : si pour tout $x \in E$, $x\mathcal{R}x$.
2. **Symétrique** : si pour tout $x, y \in E$, $x\mathcal{R}y \implies y\mathcal{R}x$.
3. **Antisymétrique** : si pour tout $x, y \in E$, $x\mathcal{R}y$ et $y\mathcal{R}x \implies x = y$.
4. **Transitive** : si pour tout $x, y, z \in E$, $x\mathcal{R}y$ et $y\mathcal{R}z \implies x\mathcal{R}z$.

Définition IV.3 (Relation d'équivalence)**.** Une relation binaire $\mathcal{R}$ sur un ensemble E est une *relation d'équivalence* si elle est :

- Réflexive : $\forall x \in E, x\mathcal{R}x$.
- Symétrique : $\forall x, y \in E, x\mathcal{R}y \implies y\mathcal{R}x$.
- Transitive : $\forall x, y, z \in E, x\mathcal{R}y$ et $y\mathcal{R}z \implies x\mathcal{R}z$.

Définition IV.4 (Relation d'ordre)**.** Une relation binaire $\mathcal{R}$ sur un ensemble E est une *relation d'ordre* si elle est :

- Réflexive : $\forall x \in E, x\mathcal{R}x$.
- Antisymétrique : $\forall x, y \in E, x\mathcal{R}y$ et $y\mathcal{R}x \implies x = y$.
- Transitive : $\forall x, y, z \in E, x\mathcal{R}y$ et $y\mathcal{R}z \implies x\mathcal{R}z$.

Si de plus, pour tout $x, y \in E$, $x\mathcal{R}y$ ou $y\mathcal{R}x$, alors $\mathcal{R}$ est une *relation d'ordre total*. Sinon, elle est une *relation d'ordre partiel*.

Définition IV.5 (Ensemble quotient)**.** Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Pour tout $x \in E$, la *classe d'équivalence* de x est l'ensemble :

$$[x]_{\mathcal{R}} = \{y \in E \mid y\mathcal{R}x\}$$

L'*ensemble quotient* de E par $\mathcal{R}$, noté $E/\mathcal{R}$, est l'ensemble des classes d'équivalence :

$$E/\mathcal{R} = \{[x]_{\mathcal{R}} \mid x \in E\}$$

Remarque IV.6. Soit $(x, y) \in E^2$:

1. $$[x]_{\mathcal{R}} = [y]_{\mathcal{R}} \iff x\mathcal{R}y \text{ et } y\mathcal{R}x \implies x = y$$
2. On suppose $x \neq y$, soit $a \in E$:

   $$a \in [x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} \iff x\mathcal{R}a \text{ et } a\mathcal{R}y \implies x = y$$

   Absurde,
   Donc $[x]_{\mathcal{R}} \cap [y]_{\mathcal{R}} = \emptyset$
3. On dit que deux classes d'équivalence sont soit disjoints soit confondus.

Exemple IV.7. 1. Sur $\mathbb{R}$, on définit la relation $\mathcal{R}$ par :

$$x\mathcal{R}y \iff y - x \in \mathbb{R}_{\geq 0}$$

C'est la relation d'ordre usuelle $\leq$. Cette relation est réflexive, antisymétrique, transitive et totale.

2. Sur $\mathbb{R}$, on définit la relation $\mathcal{R}$ par :

$$x\mathcal{R}y \iff y - x \in \mathbb{R}_{\leq 0}$$

C'est la relation d'ordre usuelle $\geq$. Cette relation est réflexive, antisymétrique, transitive et totale.

3. Soit E un ensemble et $f : E \to E$ une application. On définit sur E la relation $\mathcal{R}$ par :

$$x\mathcal{R}y \iff f(x) = f(y)$$

Cette relation est une relation d'équivalence (réflexive, symétrique et transitive).

4. Sur $\mathbb{N}^*$, la relation de divisibilité est définie par :

$$x\mathcal{R}y \iff \exists k \in \mathbb{N}^*, x = ky$$

Cette relation est réflexive, antisymétrique et transitive, donc c'est une relation d'ordre partiel, mais pas totale.

V Congruence modulo n

V.1 Définition et propriétés

Définition V.1. Soit $n \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$. On dit que a est **congru à** b modulo n, noté $a \equiv b \pmod{n}$, si $a - b$ est un multiple de n.

Exemple V.2.
- $54 \equiv 4 \pmod{10}$
- $-81 \equiv 0 \pmod{9}$
- $9 \equiv -1 \pmod{10}$
- $-5 \equiv 2 \pmod{7}$

Remarque V.3.
- $a \equiv 0 \pmod{n}$ si et seulement si a est multiple de n.
- $a \equiv b \pmod{n}$ si et seulement si $a - b$ est multiple de n.
- Si r est le reste de la division euclidienne de a par n, alors $a \equiv r \pmod{n}$.

Propriété 3. Soit $n \in \mathbb{N}^*$, $a, b, c \in \mathbb{Z}$. La congruence modulo n satisfait :

1. **Réflexivité** : $a \equiv a \pmod{n}$.
2. **Symétrie** : Si $a \equiv b \pmod{n}$, alors $b \equiv a \pmod{n}$.
3. **Transitivité** : Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$.

Donc la congruence est une relation d'équivalence.

Démonstration.
1. $a - a = 0$ est multiple de n, donc $a \equiv a \pmod{n}$.
2. Si $a - b = kn$, alors $b - a = (-k)n$, donc $b \equiv a \pmod{n}$.
3. Si $a - b = kn$ et $b - c = ln$, alors $a - c = (a - b) + (b - c) = (k + l)n$, donc $a \equiv c \pmod{n}$.

□

Propriété 4 (Propriétés opératoires). Soit $n \in \mathbb{N}^*$, $a, b, c, d \in \mathbb{Z}$. Alors :

- Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors :

$$\begin{aligned} a + c &\equiv b + d \pmod{n} \\ a - c &\equiv b - d \pmod{n} \\ ac &\equiv bd \pmod{n} \end{aligned}$$

- Pour tout $k \in \mathbb{Z}$, $ka \equiv kb \pmod{n}$.
- Si $a \equiv b \pmod{n}$ et m divise n, alors $a \equiv b \pmod{m}$.

V.2 Congruence et restes

Théorème V.4. Soit $n \in \mathbb{N}^*$, $a, a' \in \mathbb{Z}$, et r, r' les restes respectifs des divisions euclidiennes de a et a' par n. Alors :

$$a \equiv a' \pmod{n} \iff r = r'$$

Démonstration. Soit $a = nq + r$ et $a' = nq' + r'$ avec $0 \leq r, r' < n$. Alors :

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

Si $a \equiv a' \pmod{n}$, alors n divise $a - a'$, donc n divise $r - r'$. Puisque $|r - r'| < n$, on a $r - r' = 0$, soit $r = r'$. Réciproquement, si $r = r'$, alors $a - a' = n(q - q')$, donc $a \equiv a' \pmod{n}$. □

V.3 Compatibilité des congruences

Théorème V.5. Soit $n \in \mathbb{N}^*$, $a, a', b, b' \in \mathbb{Z}$. Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors :

1. $a + b \equiv a' + b' \pmod{n}$
2. $a \times b \equiv a' \times b' \pmod{n}$

On dit que l'addition et la multiplication sont compatibles avec la relation d'équivalence de congruence.

Cela signifie qu'on peut définit sur l'ensemble quotient $Z/\mathcal{R}$ deux opérations à partir de l'addition et la multiplication.

Démonstration. 1. Si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors $a - a' = kn$ et $b - b' = ln$. Ainsi :

$$(a + b) - (a' + b') = (a - a') + (b - b') = kn + ln = (k + l)n$$

Donc $a + b \equiv a' + b' \pmod{n}$.

2. De même :

$$ab - a'b' = ab - a'b + a'b - a'b' = a(b - b') + (a - a')b' = a(ln) + (kn)b' = n(al + kb')$$

Donc $ab \equiv a'b' \pmod{n}$.

□

V.3.1 La classe d'équivalence d'un entier a

Puisque $\mathcal{R}$ la une relation de congruence est une relation d'équivalence , elle partitionne $\mathbb{Z}$ en *classes d'équivalence* disjointes. La *classe d'équivalence* d'un entier $a \in \mathbb{Z}$ modulo n, notée $[a]$ ou $\overline{a}$, est l'ensemble de tous les entiers $b \in \mathbb{Z}$ congrus à a modulo n :

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Par exemple, pour $n = 5$ et $a = 3$, la classe d'équivalence est :

$$[3] = \{\ldots, -7, -2, 3, 8, 13, \ldots\},$$

car ces entiers diffèrent de 3 par des multiples de 5.

Deux classes $[a]$ et $[b]$ sont égales si et seulement si $a \equiv b \pmod{n}$. Par exemple, pour $n = 5$, $[3] = [8] = [-2]$, car $3 \equiv 8 \pmod{5}$ et $3 \equiv -2 \pmod{5}$.

Pour déterminer la classe d'équivalence d'un entier a, on utilise la division euclidienne : si $a = qn + r$ avec $0 \leq r < n$, alors $[a] = [r]$. Ainsi, les classes d'équivalence sont souvent représentées par les restes possibles $\{0, 1, 2, \ldots, n - 1\}$.

V.3.2 L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$

L'ensemble quotient $\mathbb{Z}/\mathcal{R}$, noté $\mathbb{Z}/n\mathbb{Z}$, est l'ensemble de toutes les classes d'équivalence modulo n :

$$\mathbb{Z}/n\mathbb{Z} = \{[a] \mid a \in \mathbb{Z}\} = \{[0], [1], [2], \ldots, [n - 1]\}.$$

Cet ensemble est fini et contient exactement n éléments, car chaque classe correspond à un reste distinct de la division par n. Par exemple, pour $n = 5$:

$$\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}.$$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est souvent appelé l'*anneau des entiers modulo* n, car il est muni de deux opérations bien définies : l'addition et la multiplication, que nous définirons dans le paragraphe suivant.

V.3.3 Addition sur $\mathbb{Z}/n\mathbb{Z}$

Grâce à la compatibilité des congruences, nous pouvons définir des opérations d'addition et de multiplication sur $\mathbb{Z}/n\mathbb{Z}$ qui ne dépendent pas du choix des représentants des classes.

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

$$[a] + [b] = [a + b],$$

pour tous $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$.

Cette opération est *bien définie*, car si $[a] = [a']$ et $[b] = [b']$, alors $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, et par le théorème, $a + b \equiv a' + b' \pmod{n}$, donc $[a + b] = [a' + b']$.

Propriétés de l'addition :

- **Élément neutre** : La classe $[0]$ est l'élément neutre, car $[a] + [0] = [a + 0] = [a]$.

- **Inverse** : L'inverse additif de $[a]$ est $[-a]$, car $[a]+[-a]=[a+(-a)]=[0]$. Notez que si $a \equiv r \pmod{n}$ avec $r \neq 0$, alors $[-a]=[n-r]$.
- **Associativité et commutativité** : Ces propriétés sont héritées de $\mathbb{Z}$.

Exemple : Pour $n=5$, calculons $[3]+[4]$:

$$[3]+[4]=[3+4]=[7]=[2],$$

car $7 \equiv 2 \pmod{5}$.

V.3.4 Multiplication sur $\mathbb{Z}/n\mathbb{Z}$

La multiplication sur $\mathbb{Z}/n\mathbb{Z}$ est définie par :

$$[a] \times [b] = [a \times b],$$

pour tous $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$.

Cette opération est bien définie, car si $[a]=[a']$ et $[b]=[b']$, alors $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, et par le théorème, $a \times b \equiv a' \times b' \pmod{n}$, donc $[a \times b]=[a' \times b']$.

Propriétés de la multiplication :

- **Élément neutre** : La classe $[1]$ est l'élément neutre, car $[a] \times [1] = [a \times 1] = [a]$.
- **Élément absorbant** : La classe $[0]$ est absorbante, car $[a] \times [0] = [a \times 0] = [0]$.
- **Associativité, commutativité, distributivité** : Ces propriétés sont héritées de $\mathbb{Z}$.

Exemple : Pour $n=5$, calculons $[3] \times [4]$:

$$[3] \times [4] = [3 \times 4] = [12] = [2],$$

car $12 \equiv 2 \pmod{5}$.

Tables d'opérations dans $\mathbb{Z}/n\mathbb{Z}$

Corps $\mathbb{Z}/2\mathbb{Z}$

Table d'addition

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

Table de multiplication

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Corps $\mathbb{Z}/5\mathbb{Z}$

Table d'addition

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Table de multiplication

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

V.4 Applications des congruences

V.4.1 Calculs de restes

Exemple V.6. Considérons $a=137$, $b=73$ avec $a \equiv 12 \pmod{25}$ et $b \equiv -2 \pmod{25}$. Calculons les restes :

- **Somme** :

$$\begin{aligned} a+b &\equiv 12+(-2) \pmod{25} \\ &\equiv 10 \pmod{25} \end{aligned}$$

Le reste est $\boxed{10}$.

- **Produit** :

$$\begin{aligned} ab &\equiv 12\times(-2) \pmod{25} \\ &\equiv -24 \pmod{25} \\ &\equiv 1 \pmod{25} \end{aligned}$$

Le reste est $\boxed{1}$.

- **Combinaison linéaire** :

$$\begin{aligned} 3a-2b &\equiv 3\times 12-2\times(-2) \pmod{25} \\ &\equiv 36+4 \pmod{25} \\ &\equiv 40 \pmod{25} \\ &\equiv 15 \pmod{25} \end{aligned}$$

Le reste est $\boxed{15}$.

- **Expression polynomiale** :

$$\begin{aligned} a^2+3b^3 &\equiv 12^2+3\times(-2)^3 \pmod{25} \\ &\equiv 144-24 \pmod{25} \\ &\equiv 120 \pmod{25} \\ &\equiv 20 \pmod{25} \end{aligned}$$

Le reste est $\boxed{20}$.

V.4.2 Calcul de puissances

Exemple V.7. Calculer le reste de 7^{2002} divisé par 9.

- Calcul des puissances modulo 9 :

$$\begin{aligned} 7^0 &\equiv 1 \pmod{9} \\ 7^1 &\equiv 7 \pmod{9} \\ 7^2 &\equiv 4 \pmod{9} \\ 7^3 &\equiv 1 \pmod{9} \end{aligned}$$

Le cycle est de longueur 3.

- Décomposition de l'exposant : $2002 = 3\times 667+1$.
- Calcul final :

$$\begin{aligned} 7^{2002} &= (7^3)^{667}\times 7 \\ &\equiv 1^{667}\times 7 \pmod{9} \\ &\equiv 7 \pmod{9} \end{aligned}$$

Le reste est $\boxed{7}$.

Exemple V.8. Calculer le reste de $A = 1234^{4321}+4321^{1234}$ divisé par 11.

- Décomposition de 1234 et 4321 :

$$1234 = 11\times 112+3 \text{ et} 4321 = 11\times 392+9$$

V.4.3 Propriétés des congruences

Exemple V.9. Déterminer, suivant les valeurs de $n\in\mathbb{N}$, le reste de 5^n divisé par 3.

- On a : $5^0\equiv 1 \pmod 3$, $5^1\equiv 2 \pmod 3$, $5^2\equiv 1 \pmod 3$.
- Si $n=2k$, alors $(5^2)^k\equiv 1^k \pmod 3$, donc $5^n\equiv 1 \pmod 3$.
- Si $n=2k+1$, alors $(5^2)^k\times 5\equiv 1^k\times 2 \pmod 3$, donc $5^n\equiv 2 \pmod 3$.

V.4.4 Multiplicité par 5

Théorème V.10. Pour tout $n\in\mathbb{N}$, $n(n^4-1)$ est multiple de 5.

Démonstration. On distingue cinq cas selon $n \pmod 5$:

n	0	1	2	3	4
n^4-1	4	0	0	0	0
$n(n^4-1)$	0	0	0	0	0

Dans tous les cas, $n(n^4-1) \equiv 0 \pmod 5$. □

V.4.5 Restes de n^2 modulo 8

Théorème V.11. Pour tout $n \in \mathbb{N}$, le reste de n^2 divisé par 8 est 0, 1 ou 4.

Démonstration. On distingue huit cas selon $n \pmod 8$:

n	0	1	2	3	4	5	6	7
n^2	0	1	4	1	0	1	4	1

Les restes possibles sont 0, 1 ou 4. □

Corollaire V.12. Les nombres de la forme $8k+7$ ($k \in \mathbb{Z}$) ne sont pas la somme de trois carrés parfaits.

Démonstration. Les restes possibles de la somme de trois carrés parfaits modulo 8 sont :

(a,b,c)	Reste
(0,0,0)	0
(0,0,1)	1
(0,0,4)	4
(0,1,1)	2
(0,1,4)	5
(0,4,4)	0
(1,1,1)	3
(1,1,4)	6
(1,4,4)	1
(4,4,4)	4

Le reste 7 est absent, donc $8k+7$ n'est pas la somme de trois carrés parfaits. □

V.4.6 Congruences modulo 9 et 3

Théorème V.13. Pour tout entier $x = \sum_{k=0}^{p} a_k 10^k$, on a :

$$x \equiv \sum_{k=0}^{p} a_k \pmod 9$$

$$x \equiv \sum_{k=0}^{p} a_k \pmod 3$$

Démonstration. Puisque $10 \equiv 1 \pmod 9$ et $10 \equiv 1 \pmod 3$, on a $10^k \equiv 1 \pmod 9$ et $10^k \equiv 1 \pmod 3$. Ainsi :

$$x = \sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p} a_k \cdot 1 \equiv \sum_{k=0}^{p} a_k \pmod 9$$

De même pour modulo 3. □

Exemple V.14. Calcul des restes pour :

1. 1 826 :

$$1+8+2+6 = 17$$
$$17 \equiv 8 \pmod 9$$
$$17 \equiv 2 \pmod 3$$

   Restes : $\boxed{8} \pmod 9$, $\boxed{2} \pmod 3$.

2. 3 252 :

$$3+2+5+2 = 12$$
$$12 \equiv 3 \pmod 9$$
$$12 \equiv 0 \pmod 3$$

   Restes : $\boxed{3} \pmod 9$, $\boxed{0} \pmod 3$.

3. 27 325 :

$$2+7+3+2+5 = 19$$
$$19 \equiv 1 \pmod 9$$
$$19 \equiv 1 \pmod 3$$

   Restes : $\boxed{1} \pmod 9$, $\boxed{1} \pmod 3$.

V.4.7 Congruences modulo 11

Théorème V.15. Pour tout entier $x = \sum_{k=0}^{p} a_k 10^k$, on a :

$$x \equiv \sum_{k=0}^{p} (-1)^k a_k \pmod{11}$$

Démonstration. Puisque $10 \equiv -1 \pmod{11}$, on a $10^k \equiv (-1)^k \pmod{11}$. Ainsi :

$$x = \sum_{k=0}^{p} a_k 10^k \equiv \sum_{k=0}^{p} a_k (-1)^k \pmod{11}$$

□

Exemple V.16. Calcul des restes pour :

1. 1 826 :

$$-1 + 8 - 2 + 6 = 11$$
$$11 \equiv 0 \pmod{11}$$

   Reste : $\boxed{0}$.

2. 3 252 :

$$-3 + 2 - 5 + 2 = -4$$
$$-4 \equiv 7 \pmod{11}$$

   Reste : $\boxed{7}$.

3. 27 325 :

$$2 - 7 + 3 - 2 + 5 = 1$$
$$1 \equiv 1 \pmod{11}$$

   Reste : $\boxed{1}$.

V.4.8 Congruences modulo 5

Théorème V.17. Pour tout entier $x = \sum_{k=0}^{p} a_k 10^k$, on a :

$$x \equiv a_0 \pmod{5}$$

Démonstration. Puisque $10 \equiv 0 \pmod{5}$, on a $10^k \equiv 0 \pmod{5}$ pour $k \geq 1$. Ainsi :

$$x = a_0 + \sum_{k=1}^{p} a_k 10^k \equiv a_0 \pmod{5}$$

□

Exemple V.18. Les restes des divisions par 5 de 1 826, 3 252 et 27 325 sont respectivement 1, 2 et 0.

V.4.9 Congruences modulo 4 et 25

Théorème V.19. Pour tout entier $x = \sum_{k=0}^{p} a_k 10^k$, on a :

$$x \equiv a_1 \cdot 10 + a_0 \pmod{4} \quad \text{et} \quad x \equiv a_1 \cdot 10 + a_0 \pmod{25}$$

Démonstration. Puisque $10^2 \equiv 0 \pmod{4}$ et $10^2 \equiv 0 \pmod{25}$, on a $10^k \equiv 0 \pmod{4}$ et $10^k \equiv 0 \pmod{25}$ pour $k \geq 2$. Ainsi :

$$x \equiv a_1 \cdot 10 + a_0 \pmod{4} \quad \text{et} \quad x \equiv a_1 \cdot 10 + a_0 \pmod{25}$$

□

Exemple V.20. Les restes des divisions par 4 de 1 826, 3 252 et 27 325 sont respectivement 2, 0 et 1.
Les restes des divisions par 25 sont respectivement 1, 2 et 0.

***Exercice* V.1.**

1. Combien y a-t-il de multiples de 11 compris entre -1000 et 1000 ?
2. Déterminer l'ensemble des diviseurs de 60.
3. Déterminer les entiers naturels n et p tels que $n^2 - p^2 = 28$.
4. Démontrer que $2^{32} \equiv 1 \pmod{5}$.
5. Soit n et d deux entiers relatifs non nuls tels que d divise n. Démontrer que pour tous $a, b \in \mathbb{Z}$, si $a \equiv b \pmod{n}$, alors $a \equiv b \pmod{d}$.

6. Sans effectuer la division euclidienne, vérifier que 23 157 est divisible par 9.
7. Déterminer les couples (x, y) de chiffres tels que $724xy$ soit multiple de 9.
8. Soit a, b, c trois entiers relatifs non nuls.
   (a) Démontrer que si bc divise a, alors b divise a et c divise a.
   (b) La réciproque est-elle vraie ?

VI PPCM et PGCD

VI.1 PPCM de deux entiers relatifs

Définition VI.1. Soit $a, b \in \mathbb{Z}^*$. Le **plus petit commun multiple** (PPCM) de a et b, noté $\text{PPCM}(a, b)$, est le plus petit élément strictement positif de $|a|\mathbb{Z} \cap |b|\mathbb{Z}$.

Exemple VI.2.
- Pour $a = 12$, $b = 16$:

$$12\mathbb{Z} = \{\ldots, -24, -12, 0, 12, 24, 36, 48, 60, 72, 84, 96, \ldots\}$$
$$16\mathbb{Z} = \{\ldots, -32, -16, 0, 16, 32, 48, 64, 80, 96, \ldots\}$$
$$12\mathbb{Z} \cap 16\mathbb{Z} = \{\ldots, -48, 0, 48, 96, \ldots\}$$

  Ainsi, $\text{PPCM}(12, 16) = 48$.
- Pour $a = 5$, $b = 7$, le plus petit multiple commun positif est 35, donc $\text{PPCM}(5, 7) = 35$.

Remarque VI.3.
- $\text{PPCM}(a, b) = \text{PPCM}(|a|, |b|)$.
- Pour $a, b \in \mathbb{N}^*$, $\max(a, b) \leq \text{PPCM}(a, b) \leq ab$.
- $\text{PPCM}(a, b) = a$ si et seulement si $a \in b\mathbb{Z}$.

Théorème VI.4. Soit $a, b \in \mathbb{N}^*$, $\mu = \text{PPCM}(a, b)$. Alors :

$$a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$$

Démonstration.
- Si $k \in \mu\mathbb{Z}$, alors k est multiple de μ, donc de a et b, d'où $k \in a\mathbb{Z} \cap b\mathbb{Z}$.
- Si $k \in a\mathbb{Z} \cap b\mathbb{Z}$, la division euclidienne de k par μ donne $k = \mu q + r$, $0 \leq r < \mu$. Puisque k et μ sont multiples de a et b, r l'est aussi. Comme μ est le plus petit multiple commun positif, $r = 0$, donc $k \in \mu\mathbb{Z}$.

□

Théorème VI.5. Soit $a, b, k \in \mathbb{N}^*$. Alors :

$$\text{PPCM}(ka, kb) = k \cdot \text{PPCM}(a, b)$$

Démonstration. Posons $\mu = \text{PPCM}(a, b)$, $\mu_1 = \text{PPCM}(ka, kb)$. Alors :

- $k\mu$ est multiple de ka et kb, donc $\mu_1 \leq k\mu$.
- $\mu_1 = kaa'' = kbb''$, donc $aa'' = bb''$ est multiple commun de a et b, d'où $\mu \leq aa''$. Ainsi, $k\mu \leq kaa'' = \mu_1$.

Donc, $\mu_1 = k\mu$. □

VI.2 PGCD de deux entiers relatifs

Définition VI.6. Soit $a, b \in \mathbb{Z}^*$. Le **plus grand commun diviseur** (PGCD) de a et b, noté $\text{PGCD}(a, b)$, est le plus grand élément de $\mathfrak{D}(a, b)$, l'ensemble des diviseurs communs à a et b.

Exemple VI.7.
- $\mathfrak{D}(24) = \{\ldots, -24, -12, -8, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 8, 12, 24\}$,
  $\mathfrak{D}(30) = \{\ldots, -30, -15, -10, -6, -5, -3, -2, -1, 1, 2, 3, 5, 6, 10, 15, 30\}$,
  $\mathfrak{D}(24, 30) = \{-6, -3, -2, -1, 1, 2, 3, 6\}$. Ainsi, $\text{PGCD}(24, 30) = 6$.
- $\text{PGCD}(5, 12) = 1$ car 5 ne divise pas 12.

Remarque VI.8.
- $\text{PGCD}(a, b) = \text{PGCD}(|a|, |b|)$.
- Pour $a, b \in \mathbb{N}^*$, $1 \leq \text{PGCD}(a, b) \leq \min(a, b)$.
- $\text{PGCD}(a, b) = b$ si et seulement si $b \in \mathfrak{D}(a)$.

Théorème VI.9. Soit $a, b \in \mathbb{N}^*$, $\delta = \text{PGCD}(a, b)$. Alors :

$$\mathfrak{D}(a, b) = \mathfrak{D}(\delta)$$

Démonstration.
- Si d divise δ, alors d divise a et b, donc $\mathfrak{D}(\delta) \subseteq \mathfrak{D}(a, b)$.

- Si $d \in \mathfrak{D}(a,b)$, alors $\text{PPCM}(d,\delta) = \delta$ car d divise δ. Ainsi, $\mathfrak{D}(a,b) \subseteq \mathfrak{D}(\delta)$.

□

Théorème VI.10. Soit $a,b,k \in \mathbb{N}^*$. Alors :

$$\text{PGCD}(ka,kb) = k \cdot \text{PGCD}(a,b)$$

Démonstration. Posons $\delta = \text{PGCD}(a,b)$, $\delta_k = \text{PGCD}(ka,kb)$. Alors :

- $k\delta$ divise ka et kb, donc $k\delta \leq \delta_k$.
- δ_k divise ka et kb, donc δ_k/k divise a et b, d'où $\delta_k/k \leq \delta$. Ainsi, $\delta_k \leq k\delta$.

Donc, $\delta_k = k\delta$. □

Théorème VI.11. Théorème de Bézout: forme générale
Soit $a,b \in \mathbb{N}^*$, $\delta = \text{PGCD}(a,b)$. Un entier m est multiple de δ si et seulement si $m = au + bv$ pour certains $u,v \in \mathbb{Z}$.

Démonstration.
- Si $m = au + bv$, alors m est multiple de δ car δ divise a et b.
- Soit $A = \{au + bv \mid u,v \in \mathbb{Z}\} \cap \mathbb{N}^*$. A est non vide ($a \in A$). Soit p le plus petit élément de A. Alors p divise a et b, donc $p \leq \delta$. Comme p est multiple de δ, on a $p = \delta$.

□

VI.3 Algorithme d'Euclide

Théorème VI.12. Soit $a,b \in \mathbb{N}$, $a > b > 0$, et r le reste de la division euclidienne de a par b. Alors :

- Si $r = 0$, $\text{PGCD}(a,b) = b$.
- Si $r \neq 0$, $\text{PGCD}(a,b) = \text{PGCD}(b,r)$.

Démonstration.
- Si $r = 0$, alors $a = bq$, donc $\mathfrak{D}(a,b) = \mathfrak{D}(b)$, et $\text{PGCD}(a,b) = b$.
- Si $r \neq 0$, alors $a = bq+r$. Tout diviseur de b et r divise a, et tout diviseur de a et b divise r. Ainsi, $\mathfrak{D}(a,b) = \mathfrak{D}(b,r)$, et $\text{PGCD}(a,b) = \text{PGCD}(b,r)$.

□

Exemple VI.13. Pour $\text{PGCD}(304\,939, 151\,097)$:

Dividende	304 939	151 097	2 745	122
Diviseur	151 097	2 745	122	61
Reste	2 745	122	61	0

Ainsi, $\text{PGCD}(304\,939, 151\,097) = 61$.

VII Nombres premiers entre eux

Définition VII.1. Soit $a,b \in \mathbb{Z}^*$. On dit que a et b sont **premiers entre eux** si $\text{PGCD}(a,b) = 1$.

Exemple VII.2.
- $\text{PGCD}(4,17) = 1$, donc 4 et 17 sont premiers entre eux.
- $\text{PGCD}(60,135) = 15$, donc 60 et 135 ne sont pas premiers entre eux.

Théorème VII.3 (Théorème de Bézout)**.** Soit $a,b \in \mathbb{Z}^*$. Alors a et b sont premiers entre eux si et seulement si il existe $u,v \in \mathbb{Z}$ tels que $au + bv = 1$.

Exemple VII.4.
- $49 \times 54 + 115 \times (-23) = 1$, donc $\text{PGCD}(49,115) = 1$.
- Pour n et $n+1$, on a $n \times (-1) + (n+1) \times 1 = 1$, donc ils sont premiers entre eux.

Théorème VII.5 (Théorème de Gauss)**.** Soit $a,b,c \in \mathbb{Z}^*$. Si a divise bc et $\text{PGCD}(a,b) = 1$, alors a divise c.

Démonstration. Puisque $\text{PGCD}(a,b) = 1$, il existe $u,v \in \mathbb{Z}$ tels que $au+bv = 1$. Si a divise bc, alors $bc = ka$. Ainsi, $c = auc + bvc = a(uc + kv)$, donc a divise c. □

Propriété 5. Soit $a,b \in \mathbb{N}^*$, $\delta = \text{PGCD}(a,b)$, $\mu = \text{PPCM}(a,b)$. Alors :

$$\delta\mu = ab$$

Démonstration. Soit $a = \delta a'$, $b = \delta b'$, avec $\text{PGCD}(a',b') = 1$. Alors $\text{PPCM}(a,b) = \delta\text{PPCM}(a',b') = \delta a'b'$, d'où $\delta\mu = ab$. □

Théorème VII.6. Soient a, b, c et $b_1, b_2, \ldots, b_n$ des entiers. Les propriétés suivantes s'appliquent :

1. Si a est premier avec b et avec c, alors a est premier avec bc.

2. Si a est premier avec n nombres $b_1, b_2, \ldots, b_n$ (où $n \geq 2$), alors a est premier avec leur produit.
3. Si a et b sont premiers entre eux, alors pour tous entiers naturels m et p, a^m et b^p sont premiers entre eux.
4. Si b et c sont premiers entre eux et divisent a, alors bc divise a.
5. Si a est divisible par $b_1, b_2, \ldots, b_n$ et si les b_i sont premiers entre eux deux à deux, alors a est divisible par le produit des b_i.

***Exercice* VII.1.**

1. (a) Soient a et b deux entiers relatifs n'admettant pas de diviseurs communs autres que $+1$ et -1. Montrer que si $bx = ay$, les entiers relatifs x et y sont de la forme $x = ak$, $y = bk$ où k désigne un entier relatif quelconque.

   (b) Trouver deux entiers $x = \alpha$ et $y = \beta$ vérifiant : $3x - 4y = 7$ (1) On pose $x = \alpha + X$, $y = \beta + Y$. En déduire la forme générale des entiers relatifs x et y vérifiant la relation (1).

2. Résoudre de même les équations en entiers relatifs :

   (a) $5x + 3y = 9$.

   (b) $12x - 5y = 11$.

   (c) $3x - 5y = 7$.

   (d) $15x + 11y = 12$.

   (e) $7x + 4y = -3$.

   (f) $24x - 13y = 7$.

***Exercice* VII.2.**

1. Trouver tous les couples d'entiers relatifs (x, y) vérifiant : $xy = -15$.
2. Montrer que la relation (1) : $xy + 2x - 3y - 11 = 0$ peut s'écrire sous la forme : $(x-3)(y+2) = 5$. En déduire tous les couples d'entiers relatifs (x, y) vérifiant la relation (1).
3. Résoudre de la même façon les equations suivantes :

   (a) $xy + 3x - 2y - 13 = 0$

   (b) $xy + 2x - y + 4 = 0$

   (c) $xy - x - 3y - 7 = 0$

   (d) $xy - x - 2y + 18 = 0$

   (e) $xy - 3x + 4y + 8 = 0$

   (f) $xy + 7x - 5y - 47 = 0$.

4. (a) Montrer que si x et y sont des entiers relatifs, $x + y$ et $x - y$ sont toujours de même parité.

   (b) En déduire les entiers relatifs, éléments de $\mathbb{Z}^2$ tels que :

   a) $x^2 - y^2 = 45$

   b) $x^2 - y^2 = 60$

   c) $x^2 - y^2 = 120$.

5. (a) Rechercher les entiers positifs x et y tels que : $x^2 + y^2 = k$ pour $k = 2, 5, 13, 17$ et 29 (nombres premiers de la forme $4m + 1$).

   (b) Montrer que :

   $$(\alpha^2+\beta^2)(a^2+b^2) = (a\alpha+b\beta)^2+(a\beta-b\alpha)^2 = (a\alpha-b\beta)^2+(a\beta+b\alpha)^2,$$

   (Indication : on pourra utiliser les nombres complexes.)

   (c) Montrer qu'à une solution de l'équation $x^2 + y^2 = k$ et une solution de l'équation $x^2 + y^2 = l$, on peut, en général associer deux solutions de l'équation $x^2 + y^2 = kl$.
   Étudier le cas où $k = l$, le cas où $k = 2, l \neq 2$, et le cas où $k = l = 2$.

   (d) En déduire le plus grand nombre possible de solutions de l'équation : $x^2 + y^2 = k$ pour $k = 65, 85, 221, 1105, 2210$ et 5525.

   (e) Dans $\mathbb{N}$ on suppose : $\alpha^2 + \beta^2 = mk$ et $a^2 + b^2 = m$ avec m premier.

   i. Montrer que $a^2\alpha^2 - b^2\beta^2$ et $a^2\beta^2 - b^2\alpha^2$ sont divisibles par m.

   ii. En utilisant l'identité de l'exercice précédent, montrer que l'un des couples $(a\alpha + b\beta, a\beta - b\alpha)$ ou $(a\alpha - b\beta, a\beta + b\alpha)$ a ses deux

éléments multiples de m et permet de trouver une solution de l'équation : $x^2 + y^2 = k$.

iii. Sachant que : $36^2 + 37^2 = 2665$ et que $2^2 + 1^2 = 5$, trouver une solution de l'équation $x^2 + y^2 = 533$.
Puis sachant que $533 = 13 \times 41$, trouver trois autres solutions de l'équation $x^2 + y^2 = 2665$ et montrer qu'il ne peut y en avoir d'autres.

***Exercice* VII.3.** Fractions continues

Soit x un nombre rationnel positif donné. On définit la fraction continue de x par le processus suivant :

$$x = a_0 + \frac{1}{x_1}, \quad x_1 = a_1 + \frac{1}{x_2}, \quad x_2 = a_2 + \frac{1}{x_3}, \quad \dots$$

où $a_0, a_1, a_2, a_3, \dots$ désignent respectivement les parties entières de $x, x_1, x_2, x_3, \dots$.

On définit les réduites de la fraction continue par :

$$\begin{aligned}
\frac{P_0}{Q_0} &= \frac{a_0}{1} = (a_0) \\
\frac{P_1}{Q_1} &= a_0 + \frac{1}{a_1} = (a_0, a_1) \\
\frac{P_2}{Q_2} &= a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = (a_0, a_1, a_2) \\
\frac{P_3}{Q_3} &= a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}} = (a_0, a_1, a_2, a_3) \\
&\vdots
\end{aligned}$$

La fraction $\frac{P_k}{Q_k}$, représentée par le symbole $(a_0, a_1, a_2, \dots, a_k)$, est appelée la k-ième réduite r_k du nombre x. On peut écrire :

$$x = (a_0, a_1, \dots, a_{k-1}, a_k).$$

1. Pour $x = \frac{2341}{1045}$:

   a) Calculer les entiers $a_0, a_1, a_2, a_3, \dots$ et montrer que le nombre n de ces coefficients est fini.

   b) Calculer les différentes réduites de x.

2. Pour $a \in \mathbb{Z}$ posons la matrice

$$M(a) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}.$$

   Pour tout $k \geq 2$ montrer que

$$M(a_0)M(a_1)\cdots M(a_k) = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix},$$

   En déduire les relations de récurrence :

$$P_k = a_k P_{k-1} + P_{k-2} \quad \text{et} \quad Q_k = a_k Q_{k-1} + Q_{k-2}$$

   pour $k \geq 2$, avec les conditions initiales :

$$P_0 = a_0, \quad P_1 = a_0 a_1 + 1, \quad Q_0 = 1, \quad Q_1 = a_1.$$

   b) De cette question on peut déduire la procédé rapide pour calculer les réduites à l'aide du tableau suivant :

	a_0	a_1	a_2	a_3	a_4
1	$P_0 = a_0$	$P_1 = a_0a_1 + 1$	$P_2 = a_2P_1 + P_0$	$P_3 = a_3P_2 + P_1$	$P_4 = a_4P_3 + P_2$
0	$Q_0 = 1$	$Q_1 = a_1$	$Q_2 = a_2Q_1 + Q_0$	$Q_3 = a_3Q_2 + Q_1$	$Q_4 = a_4Q_3 + Q_2$

3. (a) Établir la relation :

$$P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k.$$

   (b) En déduire que chaque réduite $\frac{P_k}{Q_k}$ est irréductible.

   (c) Montrer que chaque réduite est comprise entre les deux réduites précédentes.

4. (a) Développer $\frac{157}{68}$ en fraction continue : $(a_0, a_1, \dots, a_{n-1}, a_n)$ et montrer que les termes de la réduite $\frac{P_{n-1}}{Q_{n-1}} = (a_0, a_1, \dots, a_{n-1})$ permettent d'obtenir, dans $\mathbb{Z}$, une solution en entiers de l'équation :

$$68x - 157y + 1 = 0.$$

(b) En déduire, dans $\mathbb{Z}$, une solution de l'équation $68x-157y+37=0$, puis la solution la plus simple de cette équation et sa solution générale.

5. On reprend l'équation précédente : $68x-157y+37=0$ que l'on peut écrire successivement puisque :

$$157 = 68\times 2+21 \quad \text{et} \quad 37 = 21+16 :$$

$$68(x-2y)-21y+37=0 \implies 68(x-2y)-21(y-1)+16=0.$$

(a) Appliquer à nouveau le même procédé jusqu'à obtenir une équation de la forme :

$$(ax+by+c)+m(a'x+b'y+c')=0.$$

(b) Constater que le système :

$$ax+by+c=0; \quad a'x+b'y+c'=0$$

admet une solution dans $\mathbb{Z}$, solution de l'équation proposée (ceci peut s'établir en comparant les coefficients des groupes intermédiaires aux termes P_k et Q_k des diverses réduites de la fraction continue égale à $\frac{157}{68}$).

(c) En déduire la solution générale, dans $\mathbb{Z}$, de l'équation proposée.

6. En utilisant un des procédés des questions précédentes, résoudre dans $\mathbb{Z}$ les équations suivantes :

- $32x-27y=23$
- $41x-67y=49$

Solution:

1. Pour $x=\frac{2341}{1045}$:

(a) calculons les coefficients $a_0, a_1, a_2, \ldots$ en appliquant l'algorithme de la fraction continue :

- $x=\frac{2341}{1045}$. La partie entière est $a_0=\left\lfloor\frac{2341}{1045}\right\rfloor=2$.
- On calcule le reste : $\frac{2341}{1045}-2=\frac{2341-2\cdot1045}{1045}=\frac{2341-2090}{1045}=\frac{251}{1045}$.
- On prend l'inverse : $x_1=\frac{1045}{251}$. La partie entière est $a_1=\left\lfloor\frac{1045}{251}\right\rfloor=4$.
- Reste : $\frac{1045}{251}-4=\frac{1045-4\cdot251}{251}=\frac{1045-1004}{251}=\frac{41}{251}$.
- Inverse : $x_2=\frac{251}{41}$. Partie entière : $a_2=\left\lfloor\frac{251}{41}\right\rfloor=6$.
- Reste : $\frac{251}{41}-6=\frac{251-6\cdot41}{41}=\frac{251-246}{41}=\frac{5}{41}$.
- Inverse : $x_3=\frac{41}{5}$. Partie entière : $a_3=\left\lfloor\frac{41}{5}\right\rfloor=8$.
- Reste : $\frac{41}{5}-8=\frac{41-8\cdot5}{5}=\frac{41-40}{5}=\frac{1}{5}$.
- Inverse : $x_4=\frac{5}{1}=5$. Partie entière : $a_4=\lfloor5\rfloor=5$.
- Reste : $5-5=0$. Le processus s'arrête.

Ainsi, les coefficients sont $a_0=2$, $a_1=4$, $a_2=6$, $a_3=8$, $a_4=5$. Le nombre de coefficients est fini ($n=4$) car x est rationnel, et l'algorithme s'arrête lorsque le reste devient 0. La fraction continue est donc : $[2;4,6,8,5]$

(b) Calcul des réduites :

$$r_0=\frac{P_0}{Q_0}=\frac{2}{1}=2$$
$$r_1=2+\frac{1}{4}=\frac{9}{4}=2.25$$
$$r_2=2+\frac{1}{4+\frac{1}{6}}=\frac{56}{25}=2.24$$
$$r_3=2+\frac{1}{4+\frac{1}{6+\frac{1}{8}}}=\frac{457}{204}\approx 2.2402$$
$$r_4=2+\frac{1}{4+\frac{1}{6+\frac{1}{8+\frac{1}{5}}}}=\frac{2341}{1045}=2.240$$

2. (a) Démonstration par récurrence : Pour $k=0$ on a

$$M(a_0)=\begin{pmatrix}a_0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}P_0 & P_{-1}\\ Q_0 & Q_{-1}\end{pmatrix},$$

puisque $P_0=a_0,\ P_{-1}=1,\ Q_0=1,\ Q_{-1}=0$.

Soit k un entier, Supposons la formule vraie pour $k-1 \geq 0$, c.-à-d.

$$M(a_0)\cdots M(a_{k-1}) = \begin{pmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{pmatrix}.$$

En multipliant à droite par $M(a_k)$ on obtient

$$\begin{aligned} M(a_0)\cdots M(a_k) &= \begin{pmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{pmatrix} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} a_kP_{k-1}+P_{k-2} & P_{k-1} \\ a_kQ_{k-1}+Q_{k-2} & Q_{k-1} \end{pmatrix}. \end{aligned}$$

En posant donc

$$P_k := a_kP_{k-1}+P_{k-2}, \qquad Q_k := a_kQ_{k-1}+Q_{k-2},$$

on reconnaît la forme annoncée pour l'indice k. La propriété est ainsi établie pour tout k par récurrence.

3. (a) Relation fondamentale :

$$P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k$$

Posons $\Delta_k := P_{k-1}Q_k - P_kQ_{k-1}$. Utilisons les relations de récurrence :

$$\begin{aligned} \Delta_k &= P_{k-1}(a_kQ_{k-1}+Q_{k-2}) - (a_kP_{k-1}+P_{k-2})Q_{k-1} \\ &= P_{k-1}Q_{k-2} - P_{k-2}Q_{k-1} \\ &= -\Delta_{k-1}. \end{aligned}$$

Comme $\Delta_1 = P_0Q_1 - P_1Q_0 = a_0a_1 + 1 - a_0a_1 = 1$, on obtient par récurrence $\Delta_k = (-1)^k$ pour tout $k \geq 1$.

(b) Si d divise P_k et Q_k, alors d divise $P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k$, donc $d = \pm 1$. Ainsi $pgcd(P_k, Q_k) = 1$ et chaque réduite est irréductible.

(c) Alternance : Les réduites alternent autour de la valeur limite :

$$r_0 < r_2 < r_4 < \cdots < x < \cdots < r_5 < r_3 < r_1$$

4. (a) Développement et solution de $68x - 157y + 1 = 0$ Algorithme d'Euclide :

$$\begin{aligned} 157 &= 2\cdot 68 + 21, \\ 68 &= 3\cdot 21 + 5, \\ 21 &= 4\cdot 5 + 1, \\ 5 &= 5\cdot 1 + 0. \end{aligned}$$

Donc

$$\frac{157}{68} = [2;3,4,5].$$

(b) On calcule les réduites (mêmes formules que dans §1) :

$$\begin{aligned} &P_0 = 2,\ Q_0 = 1, \\ &P_1 = 3\cdot 2 + 1 = 7,\ Q_1 = 3, \\ &P_2 = 4\cdot 7 + 2 = 30,\ Q_2 = 4\cdot 3 + 1 = 13, \\ &P_3 = 5\cdot 30 + 7 = 157,\ Q_3 = 5\cdot 13 + 3 = 68. \end{aligned}$$

L'identité de §3 avec $k = 3$ donne

$$P_2Q_3 - P_3Q_2 = (-1)^3 = -1.$$

Ceci s'écrit numériquement :

$$30\cdot 68 - 157\cdot 13 = -1.$$

Donc $(x, y) = (30, 13)$ est une solution entière de

$$68x - 157y + 1 = 0 \quad (\text{puisque } 68\cdot 30 - 157\cdot 13 + 1 = 0).$$

(c) On cherche (x, y) tels que $68x - 157y = -37$. En multipliant l'identité précédente par 37 on obtient

$$68\cdot(30\cdot 37) - 157\cdot(13\cdot 37) = -37.$$

Donc une solution particulière est

$$(x_0, y_0) = (30\cdot 37,\ 13\cdot 37) = (1110, 481).$$

Pour obtenir une solution plus simple (valeurs plus petites), on utilise le fait que si (x_0, y_0) est solution alors pour tout $t \in \mathbb{Z}$:

$$x = x_0 + 157t, \qquad y = y_0 + 68t$$

est encore solution car

$$\begin{aligned} 68(x_0 + 157t) - 157(y_0 + 68t) &= 68x_0 - 157y_0 + t(68 \cdot 157 - 157 \cdot 68) \\ &= -37 + t \cdot 0 = -37. \end{aligned}$$

Choisissons $t = -7$ pour réduire x_0 et y_0 :

$$x = 1110 - 7 \cdot 157 = 1110 - 1099 = 11, \qquad y = 481 - 7 \cdot 68 = 481 - 476 = 5.$$

Ainsi $(x, y) = (11, 5)$ est une solution petite et simple. La solution générale est donc

$$\boxed{x = 11 + 157t, \qquad y = 5 + 68t, \quad t \in \mathbb{Z}}.$$

(On vérifie directement : $68 \cdot 11 - 157 \cdot 5 = 748 - 785 = -37$.)

5. (a) Procédé successif (décomposition) — démonstration constructive On reprend l'écriture utilisée dans l'énoncé et on effectue des substitutions successives en suivant les divisions euclidiennes. À titre d'illustration on part de

$$68x - 157y + 37 = 0.$$

Comme $157 = 2 \cdot 68 + 21$ on remplace 157 et on regroupe :

$$68(x - 2y) - 21y + 37 = 0.$$

Comme $37 = 21 + 16$ on écrit

$$68(x - 2y) - 21(y - 1) + 16 = 0.$$

Puis $68 = 3 \cdot 21 + 5$ et $16 = 3 \cdot 5 + 1$ donnent après développements et regroupements successifs une écriture de la forme

$$(ax + by + c) + m(a'x + b'y + c') = 0$$

avec m un entier (ici on trouve $m = 5$ et

$$ax + by + c = 13x - 30y + 7, \qquad a'x + b'y + c' = 3x - 7y + 2.$$

Le système linéaire

$$\begin{cases} 13x - 30y + 7 = 0, \\ 3x - 7y + 2 = 0 \end{cases}$$

admet une solution entière $(11, 5)$ (on résout par élimination ou substitution). Cette solution annule les deux combinaisons et donc annule la combinaison entière qui donne l'équation initiale ; on retrouve la même solution que précédemment. Ce procédé est la traduction algébrique des étapes de l'algorithme d'Euclide et est lié aux P_k, Q_k des réduites.

6. Résolution des équations :

(a) Résolution de : $41x - 67y = 49$ (méthode des fractions continues) Nous résolvons

$$41x - 67y = 49$$

en utilisant le développement en fraction continue de $\frac{67}{41}$ et l'identité

$$P_{k-1}Q_k - P_kQ_{k-1} = (-1)^k$$

qui fournit des combinaisons linéaires entre 67 et 41.

1. Fraction continue de $\frac{67}{41}$. Effectuons les divisions euclidiennes :

$$\begin{aligned} 67 &= 1 \cdot 41 + 26, \\ 41 &= 1 \cdot 26 + 15, \\ 26 &= 1 \cdot 15 + 11, \\ 15 &= 1 \cdot 11 + 4, \\ 11 &= 2 \cdot 4 + 3, \\ 4 &= 1 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Donc

$$\frac{67}{41} = [1; 1, 1, 1, 2, 1, 3].$$

2. Calcul des réduites P_k/Q_k. En appliquant les récurrences $P_k = a_k P_{k-1} + P_{k-2}$, $Q_k = a_k Q_{k-1} + Q_{k-2}$, on obtient

$$\begin{aligned} P_0 &= 1, & Q_0 &= 1,\\ P_1 &= 2, & Q_1 &= 1,\\ P_2 &= 3, & Q_2 &= 2,\\ P_3 &= 5, & Q_3 &= 3,\\ P_4 &= 13, & Q_4 &= 8,\\ P_5 &= 18, & Q_5 &= 11,\\ P_6 &= 67, & Q_6 &= 41. \end{aligned}$$

3. Construction d'une solution. L'identité (question 3) pour $k = 6$ (ou $k = 5$) donne

$$P_5 Q_6 - P_6 Q_5 = (-1)^6 = 1,$$

c'est-à-dire numériquement

$$18 \cdot 41 - 67 \cdot 11 = 1.$$

En multipliant cette identité par 49 on obtient

$$18 \cdot 41 \cdot 49 - 67 \cdot 11 \cdot 49 = 49,$$

donc une solution particulière de $41x - 67y = 49$ est

$$(x_0, y_0) = (18 \cdot 49,\ 11 \cdot 49) = (882, 539).$$

4. Solution générale et solution minimale. La solution générale est

$$x = 882 + 67t, \qquad y = 539 + 41t, \quad t \in \mathbb{Z}.$$

En prenant $t = -13$ on obtient la solution petite

$$x = 882 - 13 \cdot 67 = 11, \qquad y = 539 - 13 \cdot 41 = 6,$$

d'où la forme finale

$$\boxed{x = 11 + 67t, \qquad y = 6 + 41t, \quad t \in \mathbb{Z}}.$$

(b) Résolution de $32x - 27y = 23$ (procédé de la question 5) Nous résolvons l'équation

$$32x - 27y = 23$$

en appliquant le procédé successif présenté en question 5 : on suit l'algorithme d'Euclide mais on conserve à chaque étape les combinaisons linéaires qui permettent d'exprimer 1 (ou la constante recherchée) comme combinaison de 32 et 27.

1. Divisions successives (idéee générale).

$$\begin{aligned} 32 &= 1 \cdot 27 + 5,\\ 27 &= 5 \cdot 5 + 2,\\ 5 &= 2 \cdot 2 + 1,\\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

On retrace maintenant ces égalités en gardant les combinaisons linéaires pour exprimer 1 comme combinaison de 32 et 27.

2. Remontée pour obtenir l'identité combinaison.

$$\begin{aligned} 5 &= 32 - 1 \cdot 27,\\ 2 &= 27 - 5 \cdot 5 = 27 - 5(32 - 27) = 6 \cdot 27 - 5 \cdot 32,\\ 1 &= 5 - 2 \cdot 2\\ &= (32 - 27) - 2(6 \cdot 27 - 5 \cdot 32)\\ &= 11 \cdot 32 - 13 \cdot 27. \end{aligned}$$

Ainsi on a l'identité fondamentale

$$11 \cdot 32 - 13 \cdot 27 = 1.$$

3. Construire une solution de $32x - 27y = 23$. En multipliant l'identité ci-dessus par 23 on obtient

$$(11 \cdot 23) \cdot 32 - (13 \cdot 23) \cdot 27 = 23,$$

donc une solution particulière est

$$x_0 = 11 \cdot 23 = 253, \qquad y_0 = 13 \cdot 23 = 299.$$

4. Procédé de réduction (obtenir la solution minimale comme dans la question 5). Le procédé successif peut aussi conduire à un système de deux équations linéaires de la forme

$$(ax + by + c) + m(a'x + b'y + c') = 0,$$

dont la résolution donne souvent une solution plus petite. En poursuivant les regroupements/interprétations on obtient la solution simple

$$x = 10, \qquad y = 11,$$

puisque $32 \cdot 10 - 27 \cdot 11 = 320 - 297 = 23$.

5. Solution générale. La solution générale de $32x - 27y = 23$ s'obtient en ajoutant les multiples du vecteur $(27, 32)$ (puisque $pgcd(32, 27) = 1$):

$$\boxed{x = 10 + 27t, \qquad y = 11 + 32t, \quad t \in \mathbb{Z}}.$$

VIII Nombres premiers

Définition VIII.1. Un entier naturel $p \geq 2$ est **premier** s'il a exactement deux diviseurs positifs : 1 et p.

Exemple VIII.2. $2, 3, 5, 7, 11, 13$ sont premiers. 12 et 49 ne le sont pas.

Théorème VIII.3. Il existe une infinité de nombres premiers.

Démonstration. Supposons un nombre fini de nombres premiers $p_1, p_2, \ldots, p_s$. Soit $n = p_1 p_2 \cdots p_s + 1$. Alors n admet un diviseur premier p, qui doit être l'un des p_i. Mais p divise n et $p_1 p_2 \cdots p_s$, donc p divise 1, ce qui est impossible. D'où une contradiction. □

VIII.1 Algorithme d'Ératosthène pour le test de primalité

L'algorithme d'Ératosthène permet de déterminer tous les nombres premiers jusqu'à un entier donné n.

1. Écrire tous les entiers de 2 à n.
2. Barrer 1, qui n'est pas premier.
3. Prendre le plus petit nombre non barré (commencer par 2), le déclarer premier, et barrer tous ses multiples à partir de 2^2.
4. Répéter l'étape précédente avec le plus petit nombre non barré suivant, jusqu'à ce que le carré du nombre considéré dépasse n.
5. Les nombres non barrés sont les nombres premiers.

Exemple VIII.4. Pour $n = 30$:

- Liste initiale : 2, 3, 4, 5, 6, ..., 30.
- Barrez les multiples de 2 (sauf 2) : 4, 6, 8, ..., 30.
- Barrez les multiples de 3 (sauf 3) : 6, 9, 12, ..., 30.
- Barrez les multiples de 5 (sauf 5) : 10, 15, 20, 25, 30.
- Le carré de 7 est $49 > 30$, on s'arrête.

Les nombres non barrés sont : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

Pour tester si un entier m est premier, il suffit de vérifier si m est dans la liste des nombres premiers générée jusqu'à m. Cet algorithme est efficace pour des nombres modérément grands.

Théorème VIII.5. Soit $n \in \mathbb{N}$, $n \neq 0, 1$, non premier. Il existe un diviseur premier d tel que $1 < d^2 \leq n$.

Démonstration. Soit d le plus petit diviseur de n tel que $1 < d \leq n$. Alors $n = d \cdot d'$, avec $d \leq d'$, donc $d^2 \leq n$. Si d n'était pas premier, il aurait un diviseur e, $1 < e < d$, qui diviserait n, contredisant la minimalité de d. □

Théorème VIII.6 (Théorème fondamental de l'arithmétique)**.** Tout $n \in \mathbb{N}$, $n \geq 2$, s'écrit de manière unique comme $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, où $p_1 < p_2 < \cdots < p_k$ sont premiers et $\alpha_i \in \mathbb{N}^*$.

Exemple VIII.7. Pour 4 872 :

4 872	2
2 436	2
1 218	2
609	3
203	7
29	29
1	

Ainsi, $4\,872 = 2^3 \times 3 \times 7 \times 29$.

VIII.2 Formules pour PGCD et PPCM à partir des décompositions en facteurs premiers

Soient deux entiers n et m avec leurs décompositions en facteurs premiers :

$$n = \prod_{p \in \mathbb{P}} p^{\alpha_p} \quad \text{et} \quad m = \prod_{p \in \mathbb{P}} p^{\beta_p}$$

où $\mathbb{P}$ désigne l'ensemble des nombres premiers, et $\alpha_p, \beta_p \geq 0$.

Propriété 6. Plus Grand Commun Diviseur (PGCD)

$$\text{PGCD}(n, m) = \prod_{p \in \mathbb{P}} p^{\min(\alpha_p, \beta_p)}$$

Démonstration. Soit $d = \prod_{p \in \mathbb{P}} p^{\min(\alpha_p, \beta_p)}$. Montrons que d est bien le PGCD de n et m.

1. d **divise** n **et** m : Pour tout premier p, l'exposant de p dans d est $\min(\alpha_p, \beta_p) \leq \alpha_p$ et $\min(\alpha_p, \beta_p) \leq \beta_p$, donc $d \mid n$ et $d \mid m$.
2. d **est le plus grand** : Soit d' un diviseur commun de n et m. Alors $d' = \prod_{p\in\mathbb{P}} p^{\gamma_p}$ avec $\gamma_p \leq \alpha_p$ et $\gamma_p \leq \beta_p$ pour tout p, donc $\gamma_p \leq \min(\alpha_p, \beta_p)$. Ainsi, $d' \mid d$.

Donc d est bien le plus grand commun diviseur de n et m. □

Propriété 7. Plus Petit Commun Multiple (PPCM)

$$\text{PPCM}(n, m) = \prod_{p\in\mathbb{P}} p^{\max(\alpha_p, \beta_p)}$$

Démonstration. Soit $m = \prod_{p\in\mathbb{P}} p^{\max(\alpha_p, \beta_p)}$. Montrons que m est bien le PPCM de n et m.

1. n **et** m **divisent** m : Pour tout premier p, l'exposant de p dans m est $\max(\alpha_p, \beta_p) \geq \alpha_p$ et $\max(\alpha_p, \beta_p) \geq \beta_p$, donc $n \mid m$ et $m \mid m$.
2. m **est le plus petit** : Soit m' un multiple commun de n et m. Alors $m' = \prod_{p\in\mathbb{P}} p^{\gamma_p}$ avec $\gamma_p \geq \alpha_p$ et $\gamma_p \geq \beta_p$ pour tout p, donc $\gamma_p \geq \max(\alpha_p, \beta_p)$. Ainsi, $m \mid m'$.

Donc m est bien le plus petit commun multiple de n et m. □

Propriété 8. Relation entre PGCD et PPCM

$$n \times m = \text{PGCD}(n, m) \times \text{PPCM}(n, m)$$

Démonstration. En utilisant les décompositions en facteurs premiers :

$$\begin{aligned} n \times m &= \prod_{p\in\mathbb{P}} p^{\alpha_p+\beta_p} \\ \text{PGCD}(n, m) \times \text{PPCM}(n, m) &= \prod_{p\in\mathbb{P}} p^{\min(\alpha_p, \beta_p)+\max(\alpha_p, \beta_p)} \\ &= \prod_{p\in\mathbb{P}} p^{\alpha_p+\beta_p} \quad \text{car } \min(a, b) + \max(a, b) = a + b \end{aligned}$$

Donc les deux produits sont égaux. □

Exemple

Soient $n = 12 = 2^2 \cdot 3^1$ et $m = 18 = 2^1 \cdot 3^2$. Alors :

$$\begin{aligned} \text{PGCD}(12, 18) &= 2^{\min(2,1)} \cdot 3^{\min(1,2)} = 2^1 \cdot 3^1 = 6 \\ \text{PPCM}(12, 18) &= 2^{\max(2,1)} \cdot 3^{\max(1,2)} = 2^2 \cdot 3^2 = 36 \\ n \times m &= 12 \times 18 = 216 \\ \text{PGCD} \times \text{PPCM} &= 6 \times 36 = 216 \end{aligned}$$

La relation $n \times m = \text{PGCD}(n, m) \times \text{PPCM}(n, m)$ est bien vérifiée.

***Exercice* VIII.1.**

1. Vérifier si $103, 119, 137, 211$ sont premiers.
2. Pour tout $n \in \mathbb{N}$:
   (a) Si n n'est pas multiple de 5, $6n + 5$ est-il premier ?
   (b) $n^2 - n + 41$ est-il premier ?
3. Décomposer en facteurs premiers : $120, 126, 336, 735$.
4. Mettre sous forme irréductible : $\frac{495}{313}$, $\frac{780}{204}$, $\frac{918}{1242}$.
5. Lister les diviseurs de $90, 120, 245$.
6. Pour $a = 4\,312$, $b = 6\,776$ et $a = 28\,665$, $b = 412\,375$, déterminer PGCD et PPCM.
7. Calculer $\frac{51}{1\,925} + \frac{3}{6\,860}$ après décomposition en facteurs premiers.
8. Montrer que : $\forall n \in \mathbb{N}^*; \quad \exists!(p, m) \in \mathbb{N}^2 : n = 2^p(2m + 1)$.

IX Théorème des restes chinois

Théorème IX.1 (Théorème des restes chinois)**.** Soient m et n deux entiers naturels non nuls premiers entre eux (c'est-à-dire $\text{PGCD}(m, n) = 1$).
Soient a et b deux entiers relatifs. Alors le système de congruences suivant admet une solution unique modulo mn :

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

La solution est donnée par :

$$x_0 = anv + bmu$$

Où le couple (u, v) est le couple de Bézout de couple (m, n) c'est-à-dire (u, v) vérifie : $mu + nv = 1$

Démonstration.

- **Existence d'une solution :** Puisque $\text{PGCD}(m, n) = 1$, d'après le théorème de Bézout, il existe deux entiers relatifs u et v tels que $mu + nv = 1$. Posons :

$$x = anv + bmu$$

Alors :

$$\begin{aligned} x \equiv anv \pmod m &\equiv a(nv) \pmod m \\ &\equiv a(1 - mu) \pmod m \equiv a \pmod m \end{aligned}$$

car $mu \equiv 0 \pmod m$. De même :

$$x \equiv b \pmod n$$

Donc x est une solution du système.

- **Unicité modulo mn :** Supposons que x' soit une autre solution. Alors :

$$x \equiv x' \pmod m \quad \text{et} \quad x \equiv x' \pmod n$$

ce qui implique que m et n divisent $x - x'$. Puisque m et n sont premiers entre eux, mn divise $x - x'$, donc :

$$x \equiv x' \pmod{mn}$$

□

Applications

Application 1 : Résolution d'un système simple

Résoudre le système :

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \end{cases}$$

Puisque $\text{PGCD}(3, 5) = 1$, le théorème s'applique. Trouvons u, v tels que $3u+5v = 1$. Une solution est $u = -3$, $v = 2$ (car $3(-3)+5(2) = -9+10 = 1$). Ainsi :

$$x = 2 \cdot 5 \cdot 2 + 4 \cdot 3 \cdot (-3) = 20 - 36 = -16$$

Modulo 15 : $-16 \equiv -16 + 15 \times 2 = 14 \pmod{15}$. Vérification :

$$14 \equiv 2 \pmod 3, \quad 14 \equiv 4 \pmod 5$$

La solution est $x \equiv 14 \pmod{15}$.

Application 2 : Système avec trois congruences

Résoudre :

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

Puisque $2, 3, 5$ sont premiers entre eux deux à deux, on applique le théorème itérativement. D'abord pour les deux premiers :

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \end{cases}$$

Solution : $x \equiv 5 \pmod 6$ (vérification : $5 \equiv 1 \pmod 2$, $5 \equiv 2 \pmod 3$). Maintenant avec la troisième :

$$\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 3 \pmod 5 \end{cases}$$

Puisque $\text{PGCD}(6, 5) = 1$. Trouvons u, v : $6u + 5v = 1$, par exemple $u = 1$, $v = -1$ (6 - 5 = 1). Ainsi :

$$x = 5 \cdot 5 \cdot (-1) + 3 \cdot 6 \cdot 1 = -25 + 18 = -7$$

Modulo 30 : $-7 + 30 = 23$. Vérification :

$$23 \equiv 1 \pmod 2, \quad 23 \equiv 2 \pmod 3, \quad 23 \equiv 3 \pmod 5$$

La solution est $x \equiv 23 \pmod{30}$.

Application 3 : En cryptographie (exemple simplifié)

Le théorème des restes chinois est utilisé en cryptographie, par exemple dans le protocole RSA pour accélérer les calculs. Supposons que nous ayons $n = pq$ avec p, q premiers distincts, et que nous voulions calculer $x^d \pmod{n}$ où d est grand. On peut calculer :

$$x^d \pmod{p} \quad \text{et} \quad x^d \pmod{q}$$

puis recombiner via le théorème des restes chinois pour obtenir $x^d \pmod{n}$, car p et q sont premiers entre eux. Cela réduit la complexité computationnelle.

X Le petit théorème de Fermat

Théorème X.1 (Petit théorème de Fermat)**.** Soit p un nombre premier et a un entier relatif non divisible par p (i.e., $p \nmid a$). Alors :

$$a^{p-1} \equiv 1 \pmod{p}$$

De plus, pour tout entier relatif a, on a :

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

Démonstration. Nous démontrons les deux assertions du théorème.

- **Première assertion : $a^{p-1} \equiv 1 \pmod{p}$ si $p \nmid a$.** Considérons l'ensemble des multiples non nuls de a modulo p : $\{a, 2a, 3a, \ldots, (p-1)a\}$. Nous montrons que ces $p-1$ éléments sont distincts modulo p et forment une permutation des entiers $\{1, 2, \ldots, p-1\}$.
  - **Distinctivité :** Supposons que $ka \equiv la \pmod{p}$ pour $1 \leq k, l \leq p-1$, $k \neq l$. Alors p divise $(k-l)a$. Puisque p est premier et $p \nmid a$, d'après le théorème de Gauss, p divise $k-l$. Mais $|k-l| < p$, donc $k - l = 0$, ce qui est impossible car $k \neq l$. Ainsi, les ka sont distincts modulo p.
  - **Permutation :** Aucun $ka \equiv 0 \pmod{p}$, car $p \nmid a$ et $p \nmid k$ pour $k < p$. Donc, les $p-1$ éléments $\{a, 2a, \ldots, (p-1)a\}$ sont des multiples non nuls modulo p, et comme il y a exactement $p-1$ résidus non nuls modulo p, ils forment une permutation de $\{1, 2, \ldots, p-1\}$.

  Prenons le produit de ces éléments :

  $$a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p}$$

  Cela donne :

  $$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$$

  Puisque $p \nmid (p-1)!$ (car p est premier), on peut simplifier par $(p-1)!$ modulo p, ce qui donne :

  $$a^{p-1} \equiv 1 \pmod{p}$$

- **Deuxième assertion : $a^p \equiv a \pmod{p}$ pour tout a.**
  - Si $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$, et en multipliant par a, on obtient $a^p \equiv a \pmod{p}$.
  - Si $p \mid a$, alors $a \equiv 0 \pmod{p}$ et donc $a^p \equiv 0 \pmod{p}$. De plus, $a \equiv 0 \pmod{p}$, donc $a^p \equiv a \pmod{p}$.

  Ainsi, le théorème est démontré dans les deux cas.

□

Applications

Application 1 : Calcul de puissances modulo un nombre premier

Calculer le reste de 3^{100} divisé par 7.

Puisque 7 est premier et $7 \nmid 3$, le petit théorème de Fermat donne $3^6 \equiv 1 \pmod{7}$. On décompose l'exposant : $100 = 6 \cdot 16 + 4$, donc :

$$3^{100} = (3^6)^{16} \cdot 3^4 \equiv 1^{16} \cdot 3^4 \equiv 3^4 \pmod{7}$$

Calculons $3^4 = 81$, et $81 \div 7 = 11$ reste 4, donc :

$$3^{100} \equiv 4 \pmod{7}$$

Le reste est $\boxed{4}$.

Application 2 : Vérification de primalité

Vérifier si 29 est premier en testant $2^{28} \pmod{29}$.

Si 29 est premier, alors pour $a = 2$, $2^{28} \equiv 1 \pmod{29}$. Calculons :

$$2^{10} = 1024 \equiv 8 \pmod{29} \quad (1024 - 35 \cdot 29 = 8)$$

$$2^{20} = (2^{10})^2 \equiv 8^2 = 64 \equiv 6 \pmod{29} \quad (64 - 2 \cdot 29 = 6)$$

$$2^{28} = 2^{20} \cdot 2^8 = 2^{20} \cdot 256 \equiv 6 \cdot 256 = 1536 \equiv 1 \pmod{29} \quad (1536 - 53 \cdot 29 = 1)$$

Puisque $2^{28} \equiv 1 \pmod{29}$, cela suggère que 29 est premier (bien que d'autres tests soient nécessaires pour une preuve complète).

Application 3 : Résolution d'équations modulaires

Résoudre $x^3 \equiv 2 \pmod{7}$.

Puisque 7 est premier, le petit théorème donne $x^6 \equiv 1 \pmod{7}$ si $7 \nmid x$. Élevons les deux côtés au carré :

$$(x^3)^2 \equiv 2^2 \pmod{7} \implies x^6 \equiv 4 \pmod{7}$$

Puisque $x^6 \equiv 1 \pmod{7}$, on a $1 \equiv 4 \pmod{7}$, ce qui est faux. Donc, il n'existe pas de x tel que $x^3 \equiv 2 \pmod{7}$.

Application 4 : Cryptographie (RSA)

Dans RSA, soit $p = 5$, $q = 11$, $n = p \cdot q = 55$, et $e = 3$ (exposant de chiffrement). Le message $m = 7$ est chiffré en $c = m^e \equiv 7^3 \equiv 13 \pmod{55}$. Pour déchiffrer, on utilise d tel que $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$, soit $3d \equiv 1 \pmod{40}$. On trouve $d = 27$. Le petit théorème aide à vérifier que $c^d \equiv 13^{27} \equiv 7 \pmod{55}$, récupérant le message original.

Application 5 : Somme de puissances

Démontrer que pour tout $a, b \in \mathbb{Z}$, $(a+b)^7 \equiv a^7 + b^7 \pmod{7}$.

Par le petit théorème, pour tout a, $a^7 \equiv a \pmod{7}$. Par le binôme de Newton :

$$(a+b)^7 = \sum_{k=0}^{7} \binom{7}{k} a^k b^{7-k}$$

Les termes pour $1 \leq k \leq 6$ contiennent $\binom{7}{k}$, qui est divisible par 7, donc :

$$(a+b)^7 \equiv a^7 b^0 + a^0 b^7 \equiv a^7 + b^7 \pmod{7}$$

Ceci est cohérent avec $a^7 \equiv a \pmod{7}$, $b^7 \equiv b \pmod{7}$.

XI Numération

XI.1 Bases de numération

Tout au long de l'histoire, de grandes civilisations anciennes, telles que celles de Chine, de Mésopotamie, d'Égypte et d'Amérique du Sud, ont conçu des systèmes de numération variés.
Cependant, ces systèmes présentaient souvent des limites, rendant les opérations arithmétiques complexes et laborieuses.
L'avènement du système décimal (base dix) a marqué un tournant en simplifiant les calculs, grâce à l'introduction du zéro par les arabes et à la notion innovante de valeur positionnelle des chiffres.
De même, le système binaire (base deux) joue un rôle clé en informatique, où il est fréquemment associé au système hexadécimal (base seize) pour **optimiser** la représentation des nombres, notamment dans le code ASCII.

Théorème XI.1. Soit b un entier naturel supérieur ou égal à 2.
Tout entier naturel N non nul peut l'écrire de façon unique :

$$N = a_n b^n + \cdots + a_1 b^1 + a_0 b^0 = \sum_{k=0}^{p} a_{n-k} b^{n-k} = \sum_{k=0}^{p} a_k b^k$$

Où les a_k sont des entiers naturels tels que : $0 \leq a_k < b$ et $a_p \neq 0$.

On écrit : $N = \overline{a_p a_{p-1} \dots a_2 a_1 a_0}^b$. Cette écriture est appelée écriture de N en base b.
Par convention, les écritures sans "barre" sont en base 10.

Remarque Soit $N = \overline{a_p a_{p-1} \dots a_2 a_1 a_0}^b = a_p b^p + a_{p-1} b^{p-1} + \dots + a_2 b^2 + a_1 b + a_0$.

- On a : $N = b(a_p b^{p-1} + a_{p-1} b^{p-2} + \dots + a_2 b + a_1) + a_0$, avec $0 \leq a_0 < b$ donc $q_0 = \overline{a_p a_{p-1} \dots a_2 a_1}^b$ et a_0 sont respectivement le quotient et le reste de la division euclidienne de N par b.
- On a : $q_0 = b(a_p b^{p-2} + a_{p-1} b^{p-3} + \dots + a_2) + a_1$, avec $0 \leq a_1 < b$; donc $q_1 = \overline{a_p a_{p-1} \dots a_2}^b$ et a_1 sont respectivement le quotient et le reste de la division euclidienne de q_0 par b. On peut ainsi déterminer de proche en proche l'écriture de N en base b.
- La suite des restes $(r_k)_{k \geq 0}$ dans la division euclidienne de N par b est définie par :

$$\begin{cases} N = q_0 b + r_0 & \text{avec } 0 \leq r_0 < b, \\ q_0 = q_1 b + r_1 & \text{avec } 0 \leq r_1 < b, \\ q_1 = q_2 b + r_2 & \text{avec } 0 \leq r_2 < b, \\ \vdots & \\ q_{k-1} = q_k b + r_k & \text{avec } 0 \leq r_k < b, \\ \vdots & \end{cases}$$

jusqu'à obtenir un quotient $q_k = 0$. La suite des restes (r_k) est finie et correspond aux chiffres de N en base b, lus de droite à gauche.

On écrit alors $N = \overline{r_k r_{k-1} r_{k-2} \cdots r_2 r_1 r_0}^b$

Exemple XI.2. **Conversion en base sept :**
Pour écrire 127 en base sept :

- $127 = 7 \times 18 + 1$ $(r_0 = 1)$
- $18 = 7 \times 2 + 4$ $(a_1 = 4)$
- $2 = 7 \times 0 + 2$ reste $(a_2 = 2)$

On en déduit que : $127 = \overline{241}^7$.

Exemple XI.3. **Conversion en base décimale :**

$$\begin{aligned} \overline{423}^5 &= 4 \times 5^2 + 2 \times 5^1 + 3 \times 5^0 \\ &= 4 \times 25 + 2 \times 5 + 3 \\ &= 113 \end{aligned}$$

XI.2 Système binaire

Pour écrire un nombre en base deux, l'ensemble des chiffres utilisés est : $[0; 1]$.

Exemples

- Écrire dans le système décimal le nombre : $\overline{10100111001}^2$. On a :

  $\overline{10100111001}^2 = 2^{10}+2^8+2^5+2^4+2^3+2^0 = 1024+256+32+16+8+1 = 1337.$

- Écrire le nombre 87 en base deux. On effectue les divisions successives par 2, Puis on en déduit que : $87 = \overline{1010111}^2$.

$$\begin{aligned} 87 &= 43 \times 2 + 1 \\ 43 &= 21 \times 2 + 1 \\ 21 &= 10 \times 2 + 1 \\ 10 &= 5 \times 2 + 0 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 1 \times 2 + 0 \\ 1 &= 0 \times 2 + 1 \end{aligned}$$

XI.3 Système hexadécimal

Pour écrire un nombre en base seize, l'ensemble des chiffres utilisés est : $[0; 1; 2; 3; 4; 5; 6; 7; 8; 9; A; B; C; D; E; F]$. (A, B, C, D, E et F représentent respectivement 10, 11, 12, 13, 14 et 15.)

Exemples

- Écrire dans le système décimal le nombre : $\overline{FOA5}^{16}$. On a :

$$\begin{aligned}\overline{F0A5}^{16} &= 15\times16^3+0\times16^2+10\times16^1+5\times16^0\\ &= 61440+160+5\\ &= 61605.\end{aligned}$$

- Écrire le nombre 64 206 en base seize. On effectue les divisions successives par 16,Puis on en déduit que : $64\,206=\overline{FACE}^{16}$.

$$\begin{aligned}64\,206 &= 4\,012\times16+\boxed{14\ (E)}\\ 4\,012 &= 250\times16+\boxed{12\ (C)}\\ 250 &= 15\times16+\boxed{10\ (A)}\\ 15 &= 0\times16+\boxed{15\ (F)}\end{aligned}$$

XI.4 Méthodes de conversion entre bases 2, 8 et 16

1. Conversion binaire → octal/hexadécimal

- **Binaire → Octal (base 8)**
  1. Grouper les bits par **3** (de droite à gauche)
  2. Convertir chaque groupe en chiffre octal

  Exemple binaire → octal
  $\overline{101110010}_2=\overline{101}\,\overline{110}\,\overline{010}_2=\overline{562}_8$
- **Binaire → Hexadécimal (base 16)**
  1. Grouper les bits par **4** (de droite à gauche)
  2. Convertir chaque groupe en chiffre hexadécimal

  Exemple binaire → hexadécimal :
  $\overline{11010111100}_2=\overline{0110}\,\overline{1011}\,\overline{1100}_2=\overline{6BC}_{16}$

2. Conversion octal/hexadécimal → binaire

- **Octal → Binaire**
  1. Convertir chaque chiffre octal en **3 bits**
  2. Conserver l'ordre

  Exemple octal → binaire :
  $\overline{347}_8=\overline{347}_8=\overline{011}\,\overline{100}\,\overline{111}_2$
- **Hexadécimal → Binaire**
  1. Convertir chaque chiffre hexa en **4 bits**
  2. Conserver l'ordre

  Exemple hexadécimal → binaire :
  $\overline{A2F}_{16}=\overline{A2F}_{16}=\overline{1010}\,\overline{0010}\,\overline{1111}_2$

3. Conversion directe hexadécimal ↔ octal

Passer par la base 2 comme intermédiaire :

Exemple hex → oct :

$$\begin{aligned}\overline{B4}_{16} &\to \overline{1011}\,\overline{0100}_2\\ &\to \overline{010}\,\overline{110}\,\overline{100}_2 \quad \text{(regroupement par 3)}\\ &\to \overline{264}_8\end{aligned}$$

Exemple oct → hex :

$$\begin{aligned}\overline{632}_8 &\to \overline{110}\,\overline{011}\,\overline{010}_2\\ &\to \overline{0001}\,\overline{1001}\,\overline{1010}_2 \quad \text{(regroupement par 4)}\\ &\to \overline{19A}_{16}\end{aligned}$$

Table de conversion

Décimal	Binaire	Octal	Hexadécimal
0	$\overline{0}$	$\overline{0}$	$\overline{0}$
1	$\overline{1}$	$\overline{1}$	$\overline{1}$
2	$\overline{10}$	$\overline{2}$	$\overline{2}$
3	$\overline{11}$	$\overline{3}$	$\overline{3}$
4	$\overline{100}$	$\overline{4}$	$\overline{4}$
7	$\overline{111}$	$\overline{7}$	$\overline{7}$
8	$\overline{1000}$	$\overline{10}$	$\overline{8}$
15	$\overline{1111}$	$\overline{17}$	$\overline{F}$

***Exercice* XI.1.**

1. **Conversions décimal → binaire/hexadécimal** :
   - Convertir 315 en base 2 (binaire)
   - Convertir 1 024 en base 16 (hexadécimal)
2. **Conversions binaire/hexadécimal → décimal** :
   - Convertir $\overline{11010110}^2$ en base 10
   - Convertir $\overline{\text{A7F}}^{16}$ en base 10
3. **Conversion croisée** :
   - Convertir $\overline{1010\,1111\,1100}^2$ en hexadécimal (en utilisant la méthode des groupes de 4 bits)
   - Convertir $\overline{\text{B2E}}^{16}$ en binaire

XI.5 Comparaison de Nombres

Pour comparer deux nombres dans une même base :

1. Aligner les chiffres de même poids
2. Comparer de gauche à droite jusqu'à trouver une différence
3. Le nombre avec le chiffre le plus élevé à la première position différente est le plus grand

Exemple en base 8 :
Comparons $\overline{356}_8$ et $\overline{427}_8$:

- Centaines : $3 < 4$ donc $\overline{356}_8 < \overline{427}_8$

Exemple en base 16 :
Comparons $\overline{A3F}_{16}$ et $\overline{B2E}_{16}$:

- Milliers : $A(10) < B(11)$ donc $\overline{A3F}_{16} < \overline{B2E}_{16}$

XI.6 Addition dans une Base

L'addition suit les mêmes règles qu'en base 10, avec report lorsque la somme atteint la base.

Algorithme :

1. Additionner chiffre à chiffre de droite à gauche
2. Reporter l'excédent à la colonne suivante si la somme $\geq$ base

Exemple en base 2 :

$$\begin{array}{r} \overline{1011}^2 \\ +\ \overline{1101}^2 \\ \hline \overline{11000}^2 \end{array}$$

Détail : $1 + 1 = 10_2$ (on écrit 0, on retient 1)

Exemple en base 16 :

$$\begin{array}{r} \overline{7A3}^{16} \\ +\ \overline{B5}^{16} \\ \hline \overline{858}^{16} \end{array}$$

Détail : $3 + 5 = 8$, $A(10) + B(11) = 21 = \overline{E5}^{16}$ avec retenue de 1

XI.7 Soustraction dans une Base

La soustraction utilise le principe d'emprunt lorsque le chiffre du *Nombre du haut* est inférieur à celui du *nombre à soustraire*.

Algorithme :

1. Soustraire chiffre à chiffre de droite à gauche
2. Emprunter 1 à la colonne de gauche si nécessaire (vaut la base en valeur)

Exemple en base 8 :

$$\begin{array}{r} \overline{745}_8 \\ -\ \overline{367}_8 \\ \hline \overline{356}_8 \end{array}$$

Détail : Emprunt nécessaire pour $5-7$ (on prend 8+5=13, 13-7=6)

Exemple en base 2 :

$$\begin{array}{r} \overline{10100}_2 \\ -\ \overline{1101}_2 \\ \hline \overline{111}_2 \end{array}$$

Détail : Emprunts successifs pour $0-1$ opérations

Cas Particuliers

- En base 2 : L'addition de 1+1 produit 0 avec retenue de 1
- En base 16 : Les lettres A-F valent 10-15 en calcul
- Toujours vérifier en convertissant en décimal

Vérification des exemples :

$\overline{1011}_2 + \overline{1101}_2 = 11 + 13 = 24_{10} = \overline{11000}_2$

$\overline{7A3}_{16} + \overline{B5}_{16} = 1955 + 181 = 2136_{10} = \overline{858}_{16}$

XI.8 Multiplication en Base b

Algorithme :

1. Multiplier chaque chiffre du multiplicateur par le multiplicande
2. Convertir les produits partiels en base b
3. Additionner avec décalages et retenues

Exemple en base 8 :

$$\begin{array}{r} \overline{53}^8 \\ \times\ \overline{6}^8 \\ \hline \overline{412}^8 \end{array}$$

Détail : $\overline{3}^8 \times \overline{6}^8 = \overline{22}^8$ (2 avec retenue 2)

$\overline{5}^8 \times \overline{6}^8 + \overline{2}^8 = \overline{40}^8$

Exemple en base 16 :

$$\begin{array}{r} \overline{A7}^{16} \\ \times\ \overline{3}^{16} \\ \hline \overline{1F5}^{16} \end{array}$$

Détail : $\overline{7}^{16} \times \overline{3}^{16} = \overline{15}^{16}$ (5 avec retenue 1)

$\overline{A}^{16} \times \overline{3}^{16} + \overline{1}^{16} = \overline{1F}^{16}$

***Exercice* XI.2.**

1. **Multiplication**

   $\overline{1011}^2 \times \overline{11}^2 = ?$; $\overline{B4}^{16} \times \overline{5}^{16} = ?$; $\overline{45}^8 \times \overline{7}^8 = ?$;

2. **Additions/Soustractions**

   $\overline{110101}^2 + \overline{10111}^2 = ?$; $\overline{FF}^{16} + \overline{A3}^{16} = ?$; $\overline{732}^8 - \overline{465}^8 = ?$;

3. Comparer (avec $<$, $>$ ou $=$) :

   - $\overline{101101}^2$? $\overline{110010}^2$
   - $\overline{347}^8$? $\overline{365}^8$
   - $\overline{E4}^{16}$? $\overline{DB}^{16}$

XI.9 Algorithme d'Exponentiation Rapide

L'exponentiation rapide est un algorithme efficace pour calculer a^n en minimisant le nombre de multiplications. Il utilise la représentation binaire de l'exposant n. L'idée est de décomposer n en puissances de 2 et de calculer a^n en combinant les résultats intermédiaires.

Soit $n = \sum_{i=0}^{k} b_i 2^i$ où $b_i \in \{0,1\}$ (représentation binaire de n). Alors :

$$a^n = \prod_{i=0}^{k} (a^{2^i})^{b_i}.$$

Algorithme :

Data: a (base), n (exposant), b (base numérique)
Result: a^n dans la base b
$r \leftarrow 1$
while $n > 0$ **do**
  if n *est impair* **then**
    $r \leftarrow r \times a$
    $n \leftarrow n - 1$
  else
    $a \leftarrow a \times a$
    $n \leftarrow n/2$
return r

En d'autres mots, on procède ainsi:

1. Initialiser résultat = 1, base = a.
2. Pour chaque bit b_i de n (de droite à gauche) :
   - Si $b_i = 1$, multiplier résultat par base.
   - Mettre à jour base = base^2.
3. Répéter jusqu'à ce que tous les bits soient traités.

Application pour 7^{15}

Décomposition binaire de 15 : $\overline{1111}^2$

Étape	n (binaire)	Opération	Résultat partiel
1	1111 (15)	n impair : $r = 1 \times 7 = 7$	$r = 7, x = 7$
2	1110 (14)	n pair : $x = 7^2 = 49$	$r = 7$, $x = 49$
3	111 (7)	n impair : $r = 7 \times 49 = 343$	$r = 343$
4	110 (6)	n pair : $x = 49^2 = 2401$	$r = 343$, $x = 2401$
5	11 (3)	n impair : $r = 343 \times 2401 = 823543$	$r = 823543$
6	10 (2)	n pair : $x = 2401^2 = 5764801$	$r = 823543$, $x = 5764801$
7	1 (1)	n impair : $r = 823543 \times 5764801$	$r = 4\,747\,561\,509\,943$
8	0 (0)	Fin	

Remarque XI.4. Pour effectuer la multiplication de grands nombres, on peut travailler en base hexadécimale afin de simplifier les calculs.

1. **Conversion** des nombres décimaux en hexadécimal :

$$823543_{10} = \overline{C8F7B}^{16}$$
$$5764801_{10} = \overline{57F6C1}^{16}$$

2. **Multiplication hexadécimale** :
   - C8F7B × 1 = C8F7B
   - C8F7B × 6 = 4A5D26 (décalé d'une position)
   - C8F7B × C = 94B1AC (décalé de deux positions)
   - C8F7B × F = B68725 (décalé de trois positions)
   - C8F7B × 7 = 53C6D5 (décalé de quatre positions)
   - C8F7B × 5 = 3C2D4B (décalé de cinq positions)
3. **Addition** des résultats intermédiaires :

$$\begin{aligned} &\text{C8F7B} \\ &+ \text{4A5D260} \\ &+ \text{94B1AC00} \\ &+ \text{B68725000} \\ &+ \text{53C6D50000} \\ &+ \text{3C2D4B00000} \\ \hline &= 41D9242F5C7_{16} \end{aligned}$$

4. **Conversion finale** :

$$41D9242F5C7_{16} = 4\,747\,561\,509\,943_{10}$$

5. **Vérification** :

$$823543 \times 5\,764\,801 = 4\,747\,561\,509\,943$$

$$\boxed{823543_{10} \times 5764801_{10} = 4\,747\,561\,509\,943_{10} = 41D9242F5C7_{16}}$$

Calcul de 5^{13} :

Étape	n (binaire)	Calcul
1	$\overline{1101}^2$	$r = 1$, $x = 5$
2	$\overline{110}^2$	$r = 5$, $x = 25$
3	$\overline{11}^2$	$r = 5$, $x = 625$
4	$\overline{10}^2$	$r = 3125$, $x = 390625$
5	$\overline{1}^2$	$r = 3125$, $x = 1.5259 \times 10^{11}$
6	$\overline{0}^2$	$r = 1.2207 \times 10^9$

Résultat : $\boxed{5^{13} = 1\,220\,703\,125}$

Calcul de $\overline{101}^{2^{\overline{101}^2}}$:

$$\begin{aligned}
\overline{101}^{2^{\overline{101}^2}} &= \overline{101}^{2^{5_{10}}} \\
&= \overline{101}^2 \times (\overline{101}^2 \times \overline{101}^2)^2 \\
&= \overline{101}^2 \times (\overline{11001}^2)^2 \\
&= \overline{101}^2 \times \overline{1001110001}^2 \\
&= \overline{110000110101}^2 \quad (3125_{10})
\end{aligned}$$

Calcul de $\overline{2}^{16^{\overline{A}^{16}}}$:

$$\begin{aligned}
\overline{A}^{16} &= 10_{10} \\
\overline{2}^{16^{10}} &= \overline{2}^{16} \times (\overline{2}^{16} \times \overline{2}^{16})^{\overline{5}^{16}} \\
&= \overline{100}^{16} \quad (256_{10})
\end{aligned}$$

***Exercice* XI.3.**

1. Calculer 3^{20} par exponentiation rapide,
2. Calculer $\overline{11}^{2^{\overline{100}^2}}$ par exponentiation rapide,
3. Déterminer $\overline{3}^{8^{\overline{4}^8}}$,
4. Évaluer $\overline{2}^{16^{\overline{3}^{16}}}$.

XII Exercices et méthodes

Partie I Divisibilité et congruences

***Exercice* XII.1.** 1. Montrer que 11 divise $2^{123}+3^{121}$.

2. Déterminer le reste dans la division euclidienne de 11^{2021} par 25.
3. Déterminer le reste dans la division euclidienne de 16^{21000} par 7.
4. Déterminer les deux derniers chiffres de 7^{2023}.
5. Déterminer le reste dans la division euclidienne de $2^{10n-7}+3^{5n-2}$ par 11 pour tout $n \in \mathbb{N}^*$.
6. Soit $n \in \mathbb{N}^*$. Déterminer le reste dans la division euclidienne par n de la somme des n premiers entiers.
7. Montrer que 11 divise $10^{6n+2}+10^{3n+1}+1$ pour tout $n \in \mathbb{N}$.
8. Montrer que 30 divise n^5-n pour tout $n \in \mathbb{N}$.
9. Montrer qu'un nombre palindrome ayant un nombre pair de chiffres est divisible par 11. Exemple : 12344321

***Exercice* XII.2.** 1. Montrer pour tout $n \in \mathbb{N}$ que $40^n n!/\ (5n)!$.

2. Montrer que pour tout entier $n \geq 2$, on a $10 \mid 2^n-6$.
3. Montrer que pour tout $n \in \mathbb{N}^*$, on a $10 \mid 10^n \equiv 4[7]$.
4. Montrer que pour tout $n \in \mathbb{Z}$, on a $n^7 \equiv n[42]$.
5. Nombres de Fermat : Pour tout $n \in \mathbb{N}$, on note $F_n = 2^{2^n}+1$.
   (a) Montrer que $F_{n+1} = F_0 \cdots F_n + 2$ pour tout $n \in \mathbb{N}$.
   (b) Montrer que $2^{F_n-1} = 1[F_n]$ pour tout $n \in \mathbb{N}$.
6. Soient $n \in \mathbb{N}$ avec $n \geq 3$ et $a \in \mathbb{N}$ impair. Montrer que $a^{2^{n-2}} \equiv 1[2^n]$.
7. Déterminer un multiple de 1996 dont l'écriture décimale ne comporte que le chiffre 4.
8. Montrer pour tout $n \in \mathbb{N}$ que la plus grande puissance de 2 divisant l'entier $5^{2n}-1$ est 2^{n+2}.
9. Soit $k \in \mathbb{N}^*$. Montrer que le produit de k entiers relatifs consécutifs est divisible par $k!$.

Partie II: Numérotation

***Exercice* XII.3.** 1. (a) Résoudre l'équation (en système décimal) définie par : $\overline{abcde} \times 3 = \overline{abcde1}$
   (b) Résoudre l'équation (en système décimal) définie par : $\overline{xy} = (2 \times \overline{xy}) + 1$
2. Dans le système duodécimal (de base douze), un nombre s'écrit $\overline{abc}$. Dans le système de base cinq, le même nombre s'écrit $\overline{abc0}$. Quel est ce nombre ?
3. Un nombre n s'écrit $\overline{abc}$ dans le système de base treize (les nombres dix, onze et douze sont représentés respectivement par les chiffres α, β, γ).
   (a) À quelle condition n est-il divisible par treize ? par le carré de treize ?
   (b) Soient le nombre 1001 du système décimal dans le système de base treize.
4. (a) Déterminer la base du système dans le quel on a : $\overline{46}+\overline{53}=\overline{132}$.
   (b) Effectuer dans ce système l'opération : $\overline{46} \times \overline{53} = \overline{3524}$.
   (c) Même question pour : $\overline{52} \times \overline{25} = \overline{1693}$.
5. Résoudre l'équation (en système décimal) définie par : $\overline{xy} = (2 \times \overline{xy}) + 1$
6. Résoudre l'équation (en système décimal) définie par : $\overline{abcde} \times 3 = \overline{abcde1}$.

***Exercice* XII.4.** 1. Résoudre dans $\mathbb{N}^2$ les systèmes suivants.

a) $\begin{cases} \text{PGCD}(x;y) = 354 \\ x+y = 5\,664 \end{cases}$

b) $\begin{cases} \text{PPCM}(x;y) = 168 \\ x \times y = 1\,008 \end{cases}$

2. Pour tout couple $(a;b)$ d'entiers naturels, on désigne par μ leur PPCM et par δ leur PGCD.

(a) Déterminer les couples $(a;b)$ d'entiers naturels tels que :

$$2\mu + 3\delta = 11$$

.

(b) Dresser la liste des diviseurs de 108.

(c) Déterminer les couples $(a;b)$ d'entiers naturels tels que : $\mu - 3\delta = 108$ et $10 < \delta < 15$.

3. Résoudre les systèmes suivant :

(a) $\begin{cases} \text{PGCD}(x;y) = 72 \\ 2x + 3y = 1\,440 \end{cases}$

(b) $\begin{cases} \text{PPCM}(x;y) = 210 \\ x \times y = 2\,100 \end{cases}$

(c) $\begin{cases} \text{PGCD}(x;y) = 45 \\ x - y = 90 \end{cases}$

(d) $\begin{cases} \text{PPCM}(x;y) = 84 \\ x + y = 336 \end{cases}$

(e) $\begin{cases} \text{PGCD}(x;y;z) = 36 \\ \text{PPCM}(x;y;z) = 1\,800 \\ x + y + z = 540 \end{cases}$

Solution : méthode à connaître

1. Pour résoudre ce genre de système : $\begin{cases} \text{PGCD}(x;y) = 354 \\ x + y = 5\,664 \end{cases}$
On commence toujours par réduire le système en utilisant les nombres premiers ou nombres premiers entre eux. À cet effet, on pose $d = \text{PGCD}(x;y)$.
Ainsi, $\exists a, b$ tels que : $\text{PGCD}(a;b) = 1$ et $x = 354a$ et $y = 354b$.
Notre système devient :
$\begin{cases} \text{PGCD}(x;y) = 354 \\ x = 354a \\ y = 354b \\ \text{PGCD}(a;b) = 1 \\ 354a + 354b = 5\,664 \end{cases}$
Or $5\,664 = 354 \times 16$.
Donc le système devient :
$\begin{cases} \text{PGCD}(x;y) = 354 \\ x = 354a \\ y = 354b \\ \text{PGCD}(a;b) = 1 \\ a + b = 16 \end{cases}$
Maintenant, on va résoudre le sous-système réduit :
$\begin{cases} \text{PGCD}(a;b) = 1 \\ a + b = 16 \end{cases}$
Puisque a et b sont des entiers naturels, les cas possibles sont $(1;15)$, $(15;1)$, $(3;13)$, $(13;3)$, $(5;11)$, $(11;5)$, $(7;9)$, $(9;7)$.
Remarquez que si (a,b) est une solution, alors (b,a) l'est aussi.
Pour trouver x et y, on multiplie a et b par le $\text{PGCD}(x;y) = 354$.
Ainsi, les solutions sont :
- $(x,y) = (354 \times 1, 354 \times 15) = (354, 5310)$,
- $(x,y) = (354 \times 15, 354 \times 1) = (5310, 354)$,
- $(x,y) = (354 \times 3, 354 \times 13) = (1062, 4602)$,
- $(x,y) = (354 \times 13, 354 \times 3) = (4602, 1062)$,
- $(x,y) = (354 \times 5, 354 \times 11) = (1770, 3894)$,
- $(x,y) = (354 \times 11, 354 \times 5) = (3894, 1770)$,
- $(x,y) = (354 \times 7, 354 \times 9) = (2478, 3186)$,
- $(x,y) = (354 \times 9, 354 \times 7) = (3186, 2478)$.

2. Pour résoudre ce genre de système : $\begin{cases} \text{PPCM}(x;y) = 168 \\ x \times y = 1\,008 \end{cases}$
On commence toujours par réduire le système en utilisant les nombres premiers ou nombres premiers entre eux. À cet effet, on pose $m = \text{PPCM}(x;y)$.
Ainsi, $\exists a, b$ tels que : $x = \frac{m}{\text{PGCD}(a;b)} \cdot a$ et $y = \frac{m}{\text{PGCD}(a;b)} \cdot b$, avec $\text{PPCM}(a;b) = \text{PGCD}(a;b) \cdot m$.
Puisque $\text{PPCM}(x;y) = 168$, on a $m = 168$. De plus, $x \times y = 1\,008$, donc :
$\left(\frac{168}{\text{PGCD}(a;b)} \cdot a\right) \times \left(\frac{168}{\text{PGCD}(a;b)} \cdot b\right) = 1\,008$.
Soit $\text{PGCD}(a;b) = d$, alors $x = \frac{168}{d} \cdot a$ et $y = \frac{168}{d} \cdot b$, et :
$\frac{168^2}{d^2} \cdot a \cdot b = 1\,008$.
Ainsi, $d^2 \cdot a \cdot b = \frac{168^2}{1\,008}$. Calculons : $168^2 = 28\,224$ et $\frac{28\,224}{1\,008} = 28$, donc :

$d^2 \cdot a \cdot b = 28$.
Puisque $d = \text{PGCD}(a;b)$, on peut poser $a = d \cdot u$ et $b = d \cdot v$ avec $\text{PGCD}(u;v) = 1$, et le système devient :

$$\begin{cases} \text{PPCM}(x;y) = 168 \\ x = \frac{168}{d} \cdot d \cdot u = 168u \\ y = \frac{168}{d} \cdot d \cdot v = 168v \\ \text{PGCD}(u;v) = 1 \\ d^2 \cdot (d \cdot u) \cdot (d \cdot v) = 28 \end{cases}$$

Or $d^2 \cdot d \cdot u \cdot v = d^3 \cdot u \cdot v = 28$, donc $d^3 \cdot u \cdot v = 28$.
Les diviseurs de 28 sont 1, 2, 4, 7, 14, 28. Puisque d est un PGCD, $d \geq 1$, et u, v sont des entiers naturels premiers entre eux. Testons les valeurs de d :
- Si $d = 1$, alors $1^3 \cdot u \cdot v = 28$, donc $u \cdot v = 28$. Les couples (u, v) avec $\text{PGCD}(u;v) = 1$ sont : $(1, 28)$, $(28, 1)$, $(4, 7)$, $(7, 4)$.
- Si $d = 2$, alors $2^3 \cdot u \cdot v = 8 \cdot u \cdot v = 28$, donc $u \cdot v = 3.5$ (non entier).
- Si $d = 4$, alors $4^3 \cdot u \cdot v = 64 \cdot u \cdot v = 28$, donc $u \cdot v = 0.4375$ (non entier).
- Pour $d \geq 7$, d^3 devient trop grand par rapport à 28.
Ainsi, seul $d = 1$ est valide. Les couples (u, v) sont : $(1, 28)$, $(28, 1)$, $(4, 7)$, $(7, 4)$.
Donc, les solutions sont :
- $(x, y) = (168 \times 1, 168 \times 28) = (168, 4704)$,
- $(x, y) = (168 \times 28, 168 \times 1) = (4704, 168)$,
- $(x, y) = (168 \times 4, 168 \times 7) = (672, 1176)$,
- $(x, y) = (168 \times 7, 168 \times 4) = (1176, 672)$.

Partie III: Révision de cours

Exercice XII.5. Partie théorique

1. (a) Déterminer la division euclidienne de $2^m - 1$ par $2^n - 1$.
   (b) En déduire $\text{pgcd}(2^m - 1, 2^n - 1)$.
2. (a) Soit $x \in \mathbb{N} \setminus \{0, 1\}$, p, q des entiers naturels non nuls et $d = p \wedge q$.
   (b) Montrer que $(x^p - 1) \wedge (x^q - 1) = x^d - 1$.
3. Soit $(a, b) \in \mathbb{N}^2$ avec $a \geq 2$, $b \geq 2$ et $a \wedge b = 1$. Montrer que $\exists (u, v) \in [0, b-1] \times [0, a-1]$, $au - bv = 1$.
   Le couple (u, v) s'appelle **le couple de Bézout**
4. Soit $(a, b) \in (\mathbb{N}^*)^2$ avec $a \wedge b = 1$. Montrer que $\forall x \in \mathbb{N}$ avec $x \geq ab$, $\exists (u, v) \in \mathbb{N}^2$, $au + bv = x$.
5. (a) Montrer que $a^n \wedge b^n = (a \wedge b)^n$.
   (b) Montrer que $(a + b) \wedge (a \vee b) = a \wedge b$.
   (c) Montrer que $(a^2 + ab + b^2) \wedge ab = a^2 \wedge b^2$.
6. Soit $(a, b, c) \in (\mathbb{N}^*)^3$ tel que $\text{pgcd}(a, b) = 3$, $\text{pgcd}(b, c) = 4$ et $abc = 12\,096$.
   Calculer $\text{ppcm}(a, b, c)$.
7. Montrer que pour tout $(a, b, c) \in (\mathbb{N}^*)^3$, on a

$$\text{ppcm}(a, b, c) = \frac{abc \times \text{pgcd}(a, b, c)}{\text{pgcd}(a, b) \times \text{pgcd}(b, c) \times \text{pgcd}(c, a)}$$

   .
8. Soit $(a, b, c) \in (\mathbb{N}^*)^3$. Déterminer une condition nécessaire et suffisante sur (a, b, c) que l'on ait la relation $\text{pgcd}(a, b, c) \times \text{ppcm}(a, b, c) = abc$.

Méthode: Pour trouver un couple de Bézout (u, v) tel que $au + bv = \text{pgcd}(a, b)$:

1. Appliquer l'algorithme d'Euclide pour trouver $\text{pgcd}(a, b)$.
2. Remonter les étapes en exprimant chaque reste comme combinaison linéaire de a et b.
3. Identifier u et v à partir de la dernière équation où le pgcd apparaît.

Exemple:

- Exemple pour $(a, b) = (48, 18)$:

- pgcd$(48, 18)$: $48 = 2 \times 18 + 12$, $18 = 1 \times 12 + 6$, $12 = 2 \times 6 + 0$, donc pgcd $= 6$.
- Remontée : $6 = 18 - 1 \times 12$, $12 = 48 - 2 \times 18$, donc $6 = 18 - 1 \times (48 - 2 \times 18) = 3 \times 18 - 1 \times 48$.
- Couple de Bézout : $(u, v) = (-1, 3)$, car $-1 \times 48 + 3 \times 18 = 6$.

- Exemple pour $(a, b) = (126, 45)$:
  - pgcd$(126, 45)$:
    - $126 = 2 \times 45 + 36$,
    - $45 = 1 \times 36 + 9$,
    - $36 = 4 \times 9 + 0$,

    donc pgcd $= 9$.
  - Remontée :
    - $9 = 45 - 1 \times 36$,
    - $36 = 126 - 2 \times 45$, donc $9 = 45 - 1 \times (126 - 2 \times 45) = 45 - 126 + 2 \times 45 = 3 \times 45 - 1 \times 126$,

    donc $9 = -1 \times 126 + 3 \times 45$.
  - Couple de Bézout : $(u, v) = (-1, 3)$, car $-1 \times 126 + 3 \times 45 = -126 + 135 = 9$.

- Exemple pour $(a, b) = (35, 48)$
  - pgcd$(35, 48)$:
    - $48 = 1 \times 35 + 13$,
    - $35 = 2 \times 13 + 9$,
    - $13 = 1 \times 9 + 4$,
    - $9 = 2 \times 4 + 1$,
    - $4 = 4 \times 1 + 0$,

    donc pgcd $= 1$.
  - Remontée :
    - $1 = 9 - 2 \times 4$,
    - $4 = 13 - 1 \times 9$, donc $1 = 9 - 2 \times (13 - 1 \times 9) = 9 - 2 \times 13 + 2 \times 9 = 3 \times 9 - 2 \times 13$,
    - $9 = 35 - 2 \times 13$, donc $1 = 3 \times (35 - 2 \times 13) - 2 \times 13 = 3 \times 35 - 6 \times 13 - 2 \times 13 = 3 \times 35 - 8 \times 13$,
    - $13 = 48 - 1 \times 35$, donc $1 = 3 \times 35 - 8 \times (48 - 1 \times 35) = 3 \times 35 - 8 \times 48 + 8 \times 35 = 11 \times 35 - 8 \times 48$,

    donc $1 = 11 \times 35 - 8 \times 48$.
  - Couple de Bézout : $(u, v) = (11, -8)$, car $11 \times 35 + (-8) \times 48 = 385 - 384 = 1$.

Méthode: Méthode de résolution des équations diophantiennes linéaires $ax + by = c$:

1. Condition d'existence : Les solutions entières existent si et seulement si $d = pgcd(a, b) \mid c$.
2. Trouver une solution particulière : Calculer $d = pgcd(a, b)$ via l'algorithme d'Euclide, puis utiliser la remontée pour trouver (u_0, v_0) tel que $au_0 + bv_0 = d$. Une solution particulière est $(x_0, y_0) = \left(u_0 \cdot \frac{c}{d}, v_0 \cdot \frac{c}{d}\right)$.
3. On trouve que $a(x - x_0) + b(y - y_0) = 0$
   D'où : $a(x - x_0) = -b(y - y_0)$
   Reste à appliquer théorème de Gauss pour trouver la solution générale:

$$x = x_0 + k \cdot \frac{b}{d}, \quad y = y_0 - k \cdot \frac{a}{d}, \quad \forall k \in \mathbb{Z}$$

.

Exemple:

1. Exemple : Résolution de $17x - 27y = 5$:
   - Calcul de $d = pgcd(17, 27)$:
     $27 = 1 \times 17 + 10$,
     $17 = 1 \times 10 + 7$,
     $10 = 1 \times 7 + 3$,
     $7 = 2 \times 3 + 1$,
     $3 = 3 \times 1 + 0$, donc $d = 1$, et $1 \mid 5$.

- Remontée pour $17u + 27v = 1$:
  $1 = 7 - 2 \times 3$,
  $3 = 10 - 1 \times 7 \Rightarrow 1 = 7 - 2 \times (10 - 1 \times 7) = 3 \times 7 - 2 \times 10$,
  $7 = 17 - 1 \times 10 \Rightarrow 1 = 3 \times (17 - 1 \times 10) - 2 \times 10 = 3 \times 17 - 5 \times 10$,
  $10 = 27 - 1 \times 17 \Rightarrow 1 = 3 \times 17 - 5 \times (27 - 1 \times 17) = 8 \times 17 - 5 \times 27$.
  Couple de Bézout : $(u, v) = (8, -5)$.
- Solution particulière : $(x_0, y_0) = (8 \times 5, -(-5) \times 5) = (40, 25)$, vérification : $17 \times 40 - 27 \times 25 = 680 - 675 = 5$.
- Solution générale : $x = 40 + 27k, \quad y = 25 - 17k, \quad \forall k \in \mathbb{Z}$.

Exercice XII.6. Partie Pratique

1. Trouver le couple de Bézout de :
   (a) $(15, 25)$
   (b) $(18, -12)$
   (c) $(7, 13)$ (premiers entre eux)
   (d) $(-20, 8)$
   (e) $(33, -9)$
2. Résoudre en $\mathbb{Z}^2$, les équations:
   (a) $15x + 25y = 10$
   (b) $18x - 12y = -6$
   (c) $7x + 13y = 5$
   (d) $-20x + 8y = 4$
   (e) $33x - 9y = 12$

Exercice XII.7. Recherche de triples Pythagoriciens

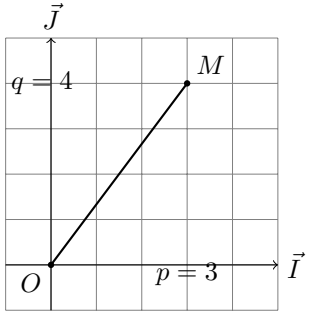
1. Soit $n \in \mathbb{N}^*$ et $(u, v) \in (\mathbb{N}^*)^2$ tels que $u \wedge v = 1$ et $u \cdot v = a^n$. Montrer qu'il existe $(\alpha, \beta) \in \mathbb{N}^2$ tels que $u = \alpha^n$ et $v = \beta^n$.
2. Résoudre l'équation définie sur $\mathbb{Z}/4\mathbb{Z}$ par $x^2 = k$, où k est un entier donné.
3. Considérer le système défini sur $\mathbb{Z}$ par : $\begin{cases} x^2 + y^2 = z^2 \\ x \wedge y \wedge z = 1 \end{cases}$
   (a) Démontrer que z est impair, ainsi que l'un des deux entiers x et y, l'autre étant pair.
   (b) Supposer que y est pair. Calculer $(y + z) \wedge (y - z)$.
4. Démontrer qu'on peut écrire alors $y + z = u^2$, $z - y = v^2$, où u et v sont deux entiers impairs.
5. Déterminer toutes les solutions du problème en fonction de deux paramètres arbitraires u et v, u et v étant des entiers impairs.
6. Déterminer effectivement toutes les solutions telles que $0 < x < 20$, $0 < y < 20$, $0 < z < 20$.
7. Résoudre l'équation définie sur $\mathbb{Z}$ par $x^2 + y^2 = z^2$.

Exercice XII.8. Énigme des palmiers

Un homme décède en laissant en héritage un champ contenant N palmiers à ses 7 enfants. Initialement, seuls deux enfants sont présents et décident de diviser N par 2. La division laisse un reste de 1 palmier.
Lorsqu'un troisième enfant arrive, ils divisent N par 3, et il reste encore 1 palmier.
Ce processus se répète avec 4, 5 et 6 enfants : à chaque fois, la division de N par le nombre d'enfants présents laisse un reste de 1.
Enfin, lorsque les 7 enfants sont réunis, ils divisent N par 7, et le partage est exact, sans reste.

Question :
Quel est le plus petit nombre N de palmiers dans le champ qui satisfait ces conditions ? *Indication*: utilisez le théorème des restes de Chinois.

***Exercice* XII.9.** Le plan est muni du repère $(O, \vec{I}, \vec{J})$. Soit p et q deux entiers naturels non nuls et M le point de coordonnées $(p; q)$. Déterminer, en fonction de p et q, le nombre de points du segment $[OM]$ dont les coordonnées sont des entiers naturels.



***Exercice* XII.10.** 1. Soit (x_n) et (y_n) les suites définies par :

$$\begin{cases} x_0 = 3,\ y_0 = 1 \\ \forall n \in \mathbb{N},\ x_{n+1} = \frac{6}{5}x_n + \frac{2}{5}y_n + 1 \\ \forall n \in \mathbb{N},\ y_{n+1} = \frac{2}{5}x_n + \frac{9}{5}y_n + 2 \end{cases}$$

(a) Démontrer par récurrence que les points M_n de coordonnées (x_n, y_n) sont sur la droite $(\mathfrak{D})$ d'équation $2x - y - 5 = 0$.

(b) En déduire l'expression de x_{n+1} en fonction de x_n.

(c) Démontrer que (x_n) et (y_n) sont des suites d'entiers relatifs.

2. Soit n un entier naturel.

(a) Démontrer que x_n est divisible par 5 si et seulement si y_n est divisible par 5.

(b) Démontrer que si x_n et y_n ne sont pas divisibles par 5, alors ils sont premiers entre eux.

3. Complément :

(a) Démontrer par récurrence que $\forall n \in \mathbb{N},\ x_n = 2^{n+1} + 1$.

(b) Démontrer que x_n est divisible par 5 si et seulement si x_{n+4} est divisible par 5.

(c) En déduire les valeurs de n pour lesquels x_n et y_n sont divisible par 5.

***Exercice* XII.11.** 1. Résoudre dans $\mathbb{Z}^2$ l'équation : $661x - 991y = 1$.

2. Soit (u_n) et (v_n) les suites arithmétiques définies par :

$$\begin{cases} u_0 = 3,\ v_0 = 2 \\ \forall n \in \mathbb{N},\ u_{n+1} = u_n + 991 \\ \forall n \in \mathbb{N},\ v_{n+1} = v_n + 661 \end{cases}$$

Déterminer tous les couples $(p; q)$ d'entiers naturels inférieurs à 2 000, tels que $u_p = v_q$.

***Exercice* XII.12.** Soit à résoudre dans $\mathbb{N}^2$ l'équation : $(E) : 15x^2 - 7y^2 = 1$.

1. Démontrer que dans le système décimal, le dernier chiffre d'un carré est 1, 4, 5, 6 ou 9.
2. En déduire que $7y^2 + 9$ n'est pas divisible par 5.
3. Résoudre l'équation (E).

***Exercice* XII.13.** Soit à résoudre dans $\mathbb{Z}$ l'équation : $(E) : 3x^2 + 3x + 7 = y^3$.

1. Vérifier que (E) est équivalente à :
   $3(x^2+x+2) = y^3 - 1$.
2. Résoudre l'équation (E).
   (On pourra distinguer 3 cas : $y \equiv 0[3]$, $y \equiv 1[3]$, $y \equiv 2[3]$.)

***Exercice* XII.14.** On désigne par $\mathbb{P}$ l'ensemble des entiers naturels premiers. On se propose de résoudre dans $\mathbb{P}^2$ l'équation :
$(E) : x^2 - y^2 = pq$, où p et q sont deux entiers naturels premiers.

1. Étudier le cas où $p = q = 2$.
2. Étudier le cas où $q = 2$ et $p \neq 2$.
3. On suppose que $2 < q \leq p$.
   (a) Démontrer que y est nécessairement égal à 2.
   (b) En déduire que si $p - q = 4$, (E) n'a pas de solution.
4. On suppose que $p - q = 4$.
   (a) Démontrer que si $(x; 2)$ est solution de (E), alors les nombres q, x et p forment une suite arithmétique de raison 2.
   (b) En déduire que (E) n'a de solution que si $q = 3$ et $p = 7$.
   (On pourra démontrer que pour tout entier n, l'un des trois nombres n, $n+2$, $n+4$ est divisible par 3.)
   (c) Quelle est la solution de (E) dans ce cas ?

***Exercice* XII.15.** On se propose de résoudre dans $\mathbb{N}^2$ l'équation

$$(E) : 5^x - 4^x = y^2. \qquad (1)$$

1. Vérification Vérifier que $(1; 1)$ est solution de (E).
   Dans la suite du problème, on suppose que x est différent de 1.
2. L'objet de cette question est de démontrer que x est pair.
   (a) Quels sont les entiers naturels n tels que : $n^2 \equiv 5 \pmod 8$?
   (b) Démontrer que si x est impair, alors $5^x - 4^x \equiv 5 \pmod 8$.
   (c) Conclure.
3. On pose : $x = 2m$ $(m \in \mathbb{N})$.
   Montrer que (E) est équivalente à :
   (a) $(5^m - y)(5^m + y) = 2^{4m}$.
   (b) En déduire qu'il existe deux entiers p et q tels que :
   $$5^m - y = 2p,$$
   $$5^m + y = 2q, \quad \text{avec} \quad p + q = 4m.$$
   (c) Déduire que :
   $$p = 1,$$
   $$q = 4m - 1,$$
   $$5^m = 1 + 4^{2m-1}.$$
   (d) En déduire que : $m \leq 1$. (On pourra faire un raisonnement par l'absurde.)
4. Déterminer les solutions de (E).

***Exercice* XII.16.** 1. Soit p et q deux entiers relatifs premiers entre eux, n un entier naturel non nul.
Démontrer que p et q^n sont premiers entre eux.

2. Soit $P(X) = a_n X^n + \cdots + a_1 X + a_0$ un polynôme à coefficients entiers relatifs admettant une racine rationnelle $\frac{p}{q}$ (p et q sont des entiers relatifs premiers entre eux).
   Démontrer que p divise a_0 et q divise a_n.
3. Factoriser le polynôme : $3X^3 + 7X^2 + 7X + 4$.
4. Résoudre dans $\mathbb{Q}$ l'équation : $x^5 + 127x^4 - 12x^3 + x^2 + 7x - 1 = 0$.

***Exercice* XII.17.** Soit x un entier naturel vérifiant :

$$10^x \equiv 2 \quad [19]$$

1. (a) Vérifier que :
   $$10^{x+1} \equiv 1 \quad [19]$$
   (b) Montrer que :
   $$10^{18} \equiv 1 \quad [19]$$
2. Soit d le plus grand commun diviseur des entiers $x+1$ et 18.
   (a) Montrer que :
   $$10^d \equiv 1 \quad [19]$$
   (b) Montrer que :
   $$d = 18$$
   (c) En déduire que :
   $$x \equiv 17 \quad [18]$$

***Exercice* XII.18.** Soit p un nombre premier et a un entier tel que

$$p \wedge a = 1.$$

On pose

$$F_p(a) = \frac{a^{p-1} - 1}{p}.$$

1. Vérifier que :
   $$F_p(a) \in \mathbb{N}.$$
2. Soit b un entier tel que :
   $$b \wedge p = 1.$$
3. Montrer que
   $$F_p(ab) \equiv F_p(a) + F_p(b) \pmod{p}.$$

***Exercice* XII.19.** **Question préliminaire:** Énonce et démontrer le théorème de Wilson.

Partie 1 : Propriété de la suite modulo un nombre premier

Soit p un nombre premier et soit (u_n) la suite définie par :

$$u_n = n^p + (p-1)! \cdot n$$

Montrer que pour tout entier n, on a :

$$u_n \equiv 0 \pmod{p}$$

Partie 2 : Vérification de primalité

En utilisant le critère d'Ératosthène, vérifier que :

1. 2027 est un nombre premier
2. 2029 est un nombre premier

Partie 3 : Applications

En déduire que :

1. 2027 divise $2028^{2027} + 2026! \times 2028$
2. 2029 divise $2028^{2029} + 2028! \times 2028$

***Exercice* XII.20.** Soient p un nombre premier impair et a un entier premier avec p.

1. Propriété de a
Montrer que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ou $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

2. Équation dans $\mathbb{Z}$
On considère dans $\mathbb{Z}$ l'équation : $ax \equiv 1 \pmod{p}$. Soit x_0 une solution de cette équation.

(a) Montrer que : $x_0^{p-1} \equiv 1 \pmod{p}$.

(b) En déduire que : $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

3. Équation avec n
Soit n un entier naturel non nul.

(a) Montrer que si p divise $2^{2n+1} - 1$ alors $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(b) En déduire que l'équation $(E) : 11x + (2^{2n+1} - 1)y = 1$ admet au moins une solution dans $\mathbb{Z}^2$.

4. Équation dans $\mathbb{Z}$
On considère dans $\mathbb{Z}$ l'équation $(F) : x^2 + 5x + 2 \equiv 0 \pmod{11}$.

(a) Montrer que : $(F) \iff 2(2x+5)^2 \equiv 1 \pmod{11}$.

(b) En déduire que l'équation (F) n'admet pas de solution dans $\mathbb{Z}$.

***Exercice* XII.21.** Soient p et q deux nombres premiers distincts et r un entier naturel premier avec p et avec q.

1. Propriétés de divisibilité

(a) Montrer que p divise $r^{p-1} - 1$ et que q divise $r^{q-1} - 1$.

(b) En déduire que p et q divisent $r^{(p-1)(q-1)} - 1$.

(c) Montrer que pq divise $r^{(p-1)(q-1)} - 1$.

2. Résolution d'équation dans $\mathbb{Z}$
Résoudre dans $\mathbb{Z}$ l'équation : $2024^{192}x \equiv 3 \pmod{221}$ (On donne : $221 = 13 \times 17$).

***Exercice* XII.22.** Soit p un nombre premier impair. On considère dans $\mathbb{Z}$ l'équation $(E) : x^2 \equiv 2 \pmod{p}$.

1. **Propriétés de 2^p**

(a) Montrer que $2^{p-1} \equiv 1 \pmod{p}$.

(b) En déduire que $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ou $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
(On remarque que $(2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1) = 2^{p-1} - 1$.)

2. **Condition nécessaire pour l'existence d'une solution**
Soit x une solution de (E).

(a) Montrer que p et x sont premiers entre eux.

(b) En déduire que $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
(On pourra utiliser le théorème de Fermat.)

3. **Contradiction et étude des coefficients binomiaux**

(a) Montrer que pour tout $k \in \{1, 2, \ldots, p-1\}$, p divise C_p^k.
(Rappel : $C_p^k = \frac{p!}{k!(p-k)!}$ et $kC_p^k = pC_{p-1}^{k-1}$.)

(b) En utilisant la formule de Moivre, montrer que :
$(1+i)^p = 2^{\frac{p}{2}} \cos\left(\frac{p\pi}{4}\right) + i2^{\frac{p}{2}} \sin\left(\frac{p\pi}{4}\right)$,
où i est le nombre complexe tel que $i^2 = -1$.

(c) Montrer que :
$(1+i)^p = \sum_{k=0}^{\frac{p-1}{2}} (-1)^k C_p^{2k} + i \sum_{k=0}^{\frac{p-1}{2}} (-1)^k C_p^{2k+1}$.

(d) En déduire que $2^{\frac{p}{2}} \cos\left(\frac{p\pi}{4}\right) \in \mathbb{Z}$ et
$2^{\frac{p}{2}} \cos\left(\frac{p\pi}{4}\right) \equiv 1 \pmod{p}$.
(On pourra utiliser la question 3-a.)

4. **Cas particulier** on suppose que si $p \equiv 5 \pmod 8$:

   En utilisant les questions 2 et 3 montrer que l'équation (E) n'admet pas de solution dans $\mathbb{Z}$.

***Exercice* XII.23.** On admet que 2969 (l'année Amazighe actuelle?) est un nombre premier. Soient n et m deux entiers naturels vérifiant : $n^8 + m^8 \equiv 0 \pmod{2969}$.

1. Cas où 2969 ne divise pas n
   On suppose dans cette question que 2969 ne divise pas n.

   (a) En utilisant le théorème de BÉZOUT, montrer que : $(\exists u \in \mathbb{Z})$; $u \times n \equiv 1 \pmod{2969}$.

   (b) En déduire que : $(u \times m)^8 \equiv -1 \pmod{2969}$ et que $(u \times m)^{2968} \equiv -1 \pmod{2969}$.
   (On remarque que : $2968 = 8 \times 371$)

   (c) Montrer que 2969 ne divise pas $u \times m$.

   (d) En déduire qu'on a aussi $(u \times m)^{2968} \equiv 1 \pmod{2969}$.

2. Conclusion
   En utilisant les résultats précédents, montrer que 2969 divise n.

   (a) Montrer que : $n^8 + m^8 \equiv 0 \pmod{2969} \implies n \equiv 0 \pmod{2969}$ et $m \equiv 0 \pmod{2969}$.

***Exercice* XII.24.** On considère dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $(D) : 7x^3 - 13y = 5$.

1. Analyse d'une solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ une solution de l'équation (D)

   (a) Montrer que x et 13 sont premiers entre eux.

   (b) En déduire que : $x^{12} \equiv 1 \pmod{13}$.

   (c) Montrer que : $x^3 \equiv 10 \pmod{13}$.

   (d) En déduire que : $x^{12} \equiv 3 \pmod{13}$.

2. Conclusion Déduire des questions précédentes, que l'équation (D) n'admet pas de solution dans $\mathbb{Z} \times \mathbb{Z}$.

***Exercice* XII.25.** **Partie I : Équation (E)**

On considère dans $\mathbb{Z} \times \mathbb{Z}$ l'équation $(E) : 47x - 43y = 1$.

1. Vérification
Vérifier que le couple $(11, 12)$ est une solution particulière de l'équation (E).

2. Résolution
Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation (E).

Partie II : Équation (F)

On considère dans $\mathbb{Z}$ l'équation $(F) : x^{41} \equiv 4 \pmod{43}$.

1. Analyse d'une solution $x \in \mathbb{Z}$
Soit $x \in \mathbb{Z}$ une solution de l'équation (F).

(a) Montrer que x et 43 sont premiers entre eux, en déduire que : $x^{42} \equiv 1 \pmod{43}$.

(b) Montrer que : $4x \equiv 1 \pmod{43}$, en déduire que : $x \equiv 11 \pmod{43}$.

2. Ensemble des solutions
Donner l'ensemble des solutions dans $\mathbb{Z}$ de l'équation (F).

Partie III : Système (S)

On considère dans $\mathbb{Z}$ le système à deux équations suivant (S) :

$$\begin{cases} x^{41} \equiv 4 \pmod{43} \\ x^{47} \equiv 10 \pmod{47} \end{cases}$$

1. Analyse d'une solution x
Soit x une solution du système (S).

(a) Montrer que x est solution du système (S') :

$$\begin{cases} x \equiv 11 \pmod{43} \\ x \equiv 10 \pmod{47} \end{cases}$$

(b) En déduire que : $x \equiv 527 \pmod{2021}$ (On pourra utiliser la partie I).

2. Ensemble des solutions
Donner l'ensemble des solutions dans $\mathbb{Z}$ du système (S).

***Exercice* XII.26.** Soit n un entier naturel strictement supérieur à 1. On considère dans $\mathbb{N}^2$ l'équation $(E_n) : (x+1)^n - x^n = ny$. Soit (x, y) une solution de l'équation (E_n) dans $\mathbb{N}^2$ et soit p le plus petit diviseur premier de n.

1. Propriétés modulo p

a) Montrer que : $(x+1)^n \equiv x^n \pmod{p}$.

b) Montrer que p est premier avec x et avec $(x+1)$.

c) En déduire que : $(x+1)^{p-1} \equiv x^{p-1} \pmod{p}$.

2. Cas où n est pair
Montrer que si n est pair, alors l'équation (E_n) n'admet pas de solution dans $\mathbb{N}^2$.

3. Cas où n est impair
On suppose que n est impair.

a) Montrer qu'il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que : $nu+(p-1)v = 1$. (On rappelle que p est le plus petit diviseur premier de n)

b) Soient q et r respectivement le quotient et le reste dans la division euclidienne de u par $(p-1)$. Vérifier que : $nr = 1-(p-1)(v+nq)$.

***Exercice* XII.27.** Soit n un entier naturel strictement supérieur à 1. On considère dans $\mathbb{N}^2$ l'équation $(E_n) : (x+1)^n - x^n = ny$. Soit (x, y) une solution de l'équation (E_n) dans $\mathbb{N}^2$ et soit p le plus petit diviseur premier de n.

1. Propriétés modulo p

a) Montrer que : $(x+1)^n \equiv x^n \pmod{p}$.

b) Montrer que p est premier avec x et avec $(x+1)$.

c) En déduire que : $(x+1)^{p-1} \equiv x^{p-1} \pmod{p}$.

2. Cas où n est pair
Montrer que si n est pair, alors l'équation (E_n) n'admet pas de solution dans $\mathbb{N}^2$.

3. Cas où n est impair
On suppose que n est impair.

a) Montrer qu'il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que : $nu+(p-1)v = 1$. (On rappelle que p est le plus petit diviseur premier de n)

b) Soient q et r respectivement le quotient et le reste dans la division euclidienne de u par $(p-1)$. Vérifier que : $nr = 1-(p-1)(v+nq)$.

c) On pose : $v' = -(v + nq)$. Montrer que : $v' \geq 0$.

d) Montrer que l'équation (E_n) n'admet pas de solution dans $\mathbb{N}^2$.

***Exercice* XII.28.** 1. Soit p un nombre premier tel que $p = 3 + 4k$ $(k \in \mathbb{N}^*)$.

(a) Montrer que pour tout entier relatif x, si $x^2 \equiv 1 \pmod{p}$ alors $x^{p-5} \equiv 1 \pmod{p}$.

2. Soit x un entier relatif vérifiant : $x^{p-5} \equiv 1 \pmod{p}$.

a) Montrer que x et p sont premiers entre eux.

b) Montrer que : $x^{p-1} \equiv 1 \pmod{p}$.

c) Vérifier que : $2 + (k-1)(p-1) = k(p-5)$.

d) En déduire que : $x^2 \equiv 1 \pmod{p}$.

3. Résoudre dans $\mathbb{Z}$ l'équation : $x^{62} \equiv 1 \pmod{67}$.

***Exercice* XII.29.** Soit : $(E) : 195x - 232y = 1$; $(x, y) \in \mathbb{Z}^2$.

1. Déterminer le plus grand commun diviseur de 232 et 195.
2. Montrer que l'ensemble des solutions de (E) est donné par :
$$S = \{(163 + 232k; 137 + 195k) \in \mathbb{Z}^2; k \in \mathbb{Z}\}$$
3. Déterminer l'entier naturel d qui vérifie les conditions suivantes :
$$195d \equiv 1 \pmod{232}; \quad 0 \leq d \leq 232$$
4. Prouver que l'entier naturel 233 est un nombre premier.
5. Soit : $A = \{n \in \mathbb{N}; 0 \leq n \leq 232\} = [|0; 232|]$.
6. Soit l'application définie ainsi : $f : A \to A$
$$a \mapsto f(a)$$
Avec $f(a)$ est le reste de la division euclidienne de a^{195} par 233.
   (a) Montrer que l'application f est injective.
   (b) Montrer que l'application f est surjective.
   (c) En déduire que l'application f est une bijection puis donner f^{-1}.
7. Soit n un entier naturel strictement supérieur à 1, et soit p un nombre premier. Considérons l'ensemble $A = \{m \in \mathbb{N}; 0 \leq m \leq p-1\}$. Définissons l'application $f : A \to A$ par :
$$f(a) = a^k \mod p,$$
où k est un entier positif donné, avec k et $p-1$ copremiers (c'est-à-dire que $pgcd(k, p-1) = 1$).

Questions généralisées :

(a) Montrer que l'application f est bien définie, c'est-à-dire que $f(a) \in A$ pour tout $a \in A$.

(b) Montrer que l'application f est injective.

(c) Montrer que l'application f est surjective.

(d) En déduire que l'application f est une bijection, puis déterminer f^{-1}.

***Exercice* XII.30.** (Formule d'inversion de Möbius)
On définit la fonction de Möbius par :

$$\forall n \in \mathbb{N}^*,\ \mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par un carré non égal à 1} \\ (-1)^k & \text{si } n = p_1 \dots p_k \text{ où les } p_i \text{ sont premiers 2 à 2 distincts.} \end{cases}$$

On rappelle que l'**indicatrice d'Euler** $\varphi(n)$ est définie comme le nombre d'entiers compris entre 1 et n qui sont premiers avec n.

1. Pour un nombre premier p, Montrer que $\varphi(p) = p - 1$. et $\varphi(p^k) = p^k - p^{k-1}$.
2. En déduire que, si $n = p_1^{k_1} \dots p_r^{k_r}$ est la décomposition en facteurs premiers de n, alors :
$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$
3. Montrer que pour tout $(m, n) \in (\mathbb{N}^*)^2$, si $m \wedge n = 1$, alors $\mu(mn) = \mu(m)\mu(n)$ et $\varphi(mn) = \varphi(m)\varphi(n)$.
(*On dit que μ et φ sont multiplicatives*).
4. Montrer que pour tout $n \in \mathbb{N}^*$, $\sum_{d|n} \mu(d) = \delta_{1,n}$, où $\delta_{i,j}$ est le symbole de Kronecker, égal à 1 si $i = j$ et 0 sinon.
5. Montrer que réciproquement, si ν est une fonction vérifiant l'identité de la question précédente, alors $\nu = \mu$.
6. Soit f et g deux fonctions telles que pour tout $n \in \mathbb{N}^*$,
$$g(n) = \sum_{d|n} f(d).$$
Montrer (formule d'inversion de Möbius) :
$$\forall n \in \mathbb{N}^*,\ f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$
7. Application basique : Soit $f(n) = n$ et $g(n) = \sigma(n) = \sum_{d|n} d$. Utiliser la formule d'inversion de Möbius pour exprimer f en fonction de g.
8. Soit φ l'indicatrice d'Euler. En effectuant un tri des éléments de $\mathbb{Z}/n\mathbb{Z}$, montrer que pour tout $n \in \mathbb{N}^*$,
$$\frac{\varphi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

XIII Problèmes de synthèse

Problème 1

1. **Relations entre racines carrées et nombres parfaits.**
   Soient $a, b, c \in \mathbb{N}$ tels que $\sqrt{a} + \sqrt{b} = \sqrt{c}$,

   (a) Montrer que les produits ab, bc, ca sont des carrés parfaits.

   (b) Montrer qu'il existe des entiers $\alpha, \beta, k \in \mathbb{N}$ tels que :

   $$a = k\alpha^2, \quad b = k\beta^2, \quad c = k(\alpha + \beta)^2.$$

   (c) La relation $\sqrt{a} + \sqrt{b} = c$ est-elle possible si a et b ne sont pas des carrés parfaits ?

2. **Formes spécifiques et parité.**
   Soient $a, b, c \in \mathbb{N}$ tels que :

   $$\sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}} = c.$$

   (a) Montrer que l'on peut écrire :

   $$a = 2k^2 - m, \quad b = 4k^2(k^2 - m), \quad c = 2k, \quad (k, m \in \mathbb{N}).$$

   (b) Déterminer de même la forme de a, b, c lorsque :

   $$\sqrt{a + \sqrt{b}} - \sqrt{a - \sqrt{b}} = c.$$

3. **Résolution d'équations et parité.**
   On considère l'équation en entiers :

   $$x^2 = y^2 + z^2, \quad z = \sqrt{(x + y)(x - y)}.$$

   (a) Montrer que $x + y$ et $x - y$ ont la même parité.

   (b) Si ces deux entiers sont impairs, montrer que x et z sont impairs et que y est pair. Dans ce cas, on échange y et z.

   (c) On peut donc supposer $x + y$ et $x - y$ pairs.
   En posant $2k = pgcd(x + y, x - y)$, en déduire :

   $$x + y = 2k\alpha^2, \quad x - y = 2k\beta^2, \quad (\alpha, \beta \in \mathbb{N}),$$

   puis :

   $$x = k(\alpha^2 + \beta^2), \quad y = k(\alpha^2 - \beta^2), \quad z = 2k\alpha\beta.$$

   (d) Déterminer dans $\mathbb{N}$ les cinq solutions primitives (où x, y, z sont premiers entre eux).

4. **Structure d'un ensemble et multiplication.**
   Soit $m \in \mathbb{N}$ non carré parfait, et soit :

   $$P_m = \{\, x = a + b\sqrt{m} \mid a \in \mathbb{N},\, b \in \mathbb{Z},\, a^2 - mb^2 = 1 \,\}.$$

   (a) Montrer que la multiplication dans P_m définit une loi de groupe abélien.

   (b) Pour $x = a + b\sqrt{m}$ et $x' = a' + b'\sqrt{m}$, calculer :

   $$xx' \quad \text{et} \quad \frac{x}{x'}.$$

   (c) Montrer que $x > 0$, que $x - 1$ est du signe de b, et que :

   $$a > a' \iff |b| > |b'| \iff \left|\tfrac{b}{a}\right| > \left|\tfrac{b'}{a'}\right|.$$

5. **Équation de Pell et groupe monogène.**
   Soit $u = x + \beta\sqrt{m}$ le plus petit élément de P_m strictement supérieur à 1.

   (a) Montrer que $x > u$ équivaut à $\frac{x}{u} \geq u$.

   (b) En déduire que tout élément de P_m est de la forme u^n avec $n \in \mathbb{Z}$ (donc P_m est un groupe monogène).

   (c) Calculer u^2, u^3, u^4 et leurs inverses.

   (d) En déduire que si l'on connaît la solution la plus simple (autre que $(1, 0)$) de l'équation de Pell $x^2 - my^2 = 1$, on peut obtenir toutes les autres.

   (e) **Identités et solutions.**

(f) Établir, pour $n, k \in \mathbb{N}$, les identités :

$$k^2 - (k^2-1)\cdot 1^2 = 1;$$

$$(k^2 \pm 1)^2 - (k^2 \pm 2)\, k^2 = 1;$$

$$(2k+1)^2 - (k^2+k)\, 2^2 = 1;$$

$$(2k^2 \pm 1)^2 - (k^2 \pm 1)\, 2^2 k^2 = 1.$$

(g) En déduire une solution de l'équation de Pell :

$$x^2 - my^2 = 1$$

pour :

$m = k^2 \pm 1$, $m = k^2 \pm 2$, $m = 4(k^2 \pm 1)$ et $m = k(k+1)$ ou $4k(k+1)$.

(h) Trouver ainsi la première solution après $(1,0)$ de l'équation

$$x^2 - my^2 = 1$$

pour

$$m = 2, 3, 5, 6, 7, 8, 10, 11, 12, 14, 15, 17, 18, 20, 23, 24, 26, 27 \text{ et } 30.$$

Y a-t-il des solutions autres que $(1,0)$ pour

$$m = k^2 = 1, 4, 9, 16, 25, 36, \ldots ?$$

6. **Développement en fraction continue.**
On développe $\sqrt{28}$ en fraction continue :

$$\sqrt{28} = 5 + \frac{1}{x_1}, \quad x_1 = \frac{\sqrt{28}+5}{3} = 3 + \frac{1}{x_2}, \quad x_2 = \frac{\sqrt{28}+4}{4} = 2 + \frac{1}{x_3}, \ldots$$

(a) Montrer que $x_{n+4p} = x_n$ et que l'on obtient une fraction continue périodique :

$$(5, 3, 2, 3, 10, 3, 2, 3, 10, \ldots).$$

(b) Établir que ses réduites $r_n = \frac{P_n}{Q_n}$ vérifient :

$$r_{2n} < \sqrt{28} < r_{2n+1}, \quad Q_{2n} > q_1 q_2 \cdots q_{2n} > 10^{2n}.$$

(c) En déduire que les suites $\{r_{2n}\}$ et $\{r_{2n+1}\}$ encadrent $\sqrt{28}$.

7. **Équation de Pell et réduites: un premier exemple**

(a) **Calcul des réduites et solutions.**
Calculer les réduites de $(5, 3, 2, 3, 5)$. Montrer que :

$$\sqrt{28} = (5, 3, 2, 3, 5 + \sqrt{28}) = \frac{\alpha_4 + \alpha_3\sqrt{28}}{\beta_4 + \beta_3\sqrt{28}},$$

(b) En déduire la solution la plus simple de $x^2 - 28y^2 = 1$.

8. **Équation de Pell et réduites: un cas plus générale**
Vérifier sur des exemples que si m est un entier positif, $\sqrt{m}$ se développe en fraction continue périodique :

$$(a, \overline{a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n})$$

où :

- $a_n = 2a$
- $a_{n-p} = a_p$ pour $p = 1, 2, \ldots, n-1$

et que :

(a) Les deux termes de la réduite $r_{n-1} = \frac{\alpha}{\beta}$ constituent une solution (α, β) de l'équation :

$$x^2 - my^2 = (-1)^n$$

(b) r_{2n-1} égal à $\frac{\alpha^2 + m\beta^2}{2\alpha\beta}$ donne :

- Une solution $(\alpha^2 + m\beta^2, 2\alpha\beta)$ de l'équation :

$$x^2 - my^2 = 1$$

- Une solution $(\alpha^2 + m\beta^2, \alpha\beta)$ de l'équation :

$$x^2 - 4my^2 = 1$$

9. **Applications et entraînement.**
Résoudre ainsi l'équation $x^2 - my^2 = 1$ pour l'une des valeurs de m suivantes :

   (a) Première série :

   $$m = 13,\ 19,\ 21,\ 22,\ 29,\ 31,\ 33,\ 39,\ 41,\ 43 \text{ ou } 46$$

   (b) Deuxième série :

   $$m = 12,\ 20,\ 28,\ 40,\ 44,\ 52, \text{ et } 56$$

Problème 2

Préambule

***Définition* XIII.1** (Symbole de Legendre)**.** Soit p un nombre premier impair et a un entier premier avec p. On définit le *symbole de Legendre* par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un résidu quadratique modulo } p, \\ -1 & \text{si } a \text{ n'est pas un résidu quadratique modulo } p. \end{cases}$$

Autrement dit, $\left(\frac{a}{p}\right) = 1$ s'il existe x tel que $x^2 \equiv a \pmod p$, et -1 sinon.

***Définition* XIII.2** (Plus petit reste signé)**.** Pour un entier $m > 0$, on appelle *plus petit reste signé modulo* m de x l'unique entier r tel que :

$$x \equiv r \pmod m, \qquad -\frac{m}{2} < r \leq \frac{m}{2}.$$

L'objectif de ce problème est de démontrer la loi de réciprocité quadratique en trois étapes :

- Partie A: démonstration du lemme de Gauss,
- Parie B: cas particulier $a = 2$,
- Partie C: cas général.

Partie A — Lemme de Gauss.

Soit p un nombre premier impair et a un entier premier avec p.
On considère l'ensemble

$$R_a^p = \{a,\, 2a,\, 3a,\, \ldots,\, \frac{p-1}{2}a\}$$

réduite modulo p sous forme de plus petits restes signés.

1. Montrez que deux entiers distincts de l'ensemble R_a^p donnent des restes signés distincts modulo p.
2. Soit $N_p(a)$ le nombre de termes négatifs dans cette liste réduite.

   Donner le produit des termes *avant* réduction puis le produit des termes *après* réduction.
3. En déduire la congruence :

$$\prod_{n \in R_a^p} n = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}!\right) \equiv (-1)^{N_p(a)} \left(\frac{p-1}{2}!\right) \pmod p.$$

4. Justifiez que l'on peut simplifier par $\left(\frac{p-1}{2}!\right)$ modulo p et conclure que:

$$\left(\frac{a}{p}\right) = (-1)^{N_p(a)}.$$

C'est le lemme de Gauss

Partie B — Cas particulier $a = 2$.

1. Appliquez le lemme de Gauss à $a = 2$ et montrer que $N_p(2)$ est le nombre d'entiers k avec $1 \leq k \leq \frac{p-1}{2}$ vérifiant $2k > \frac{p}{2}$.
2. Montrer que $N_p(2) = \frac{p^2-1}{8}$ et déduire que:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \text{ ou } 7 \pmod 8, \\ -1 & \text{si } p \equiv 3 \text{ ou } 5 \pmod 8. \end{cases}$$

cela signifie que l'équation $x^2 \equiv 2 \pmod p \iff p \equiv 1$ *ou* $7 \pmod 8$

Partie B — Cas général p, q premiers impairs.

1. Soient p et q deux nombres premiers impairs distincts. Appliquez le lemme de Gauss à $\left(\frac{q}{p}\right)$ puis à $\left(\frac{p}{q}\right)$. Introduisez $N_p(q)$ et $N_q(p)$.
2. Considérons les couples (i, j) avec $1 \leq i \leq \frac{p-1}{2}$ et $1 \leq j \leq \frac{q-1}{2}$. Montrez que :

$$N_p(q) + N_q(p) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

   Indication : comparez iq et jp.
3. Concluez que :

$$\boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}}$$

C'est la loi de réciprocité quadratique de Gauss.

XIV Annexes

Les annexes qui suivent pourraient intéresser les élèves de MPSI/MP2I et ceux de bac qui préparent le concours CGM.

A Nombres de Fermat et suite de Fibonacci

A.1 Nombres de Fermat

Définition A.1. Les nombres de Fermat sont définis pour $n \in \mathbb{N}$ par :

$$F_n = 2^{2^n} + 1$$

Exemple A.2. Les premiers nombres de Fermat sont :

- $F_0 = 2^{2^0} + 1 = 3$ (premier)
- $F_1 = 2^{2^1} + 1 = 5$ (premier)
- $F_2 = 2^{2^2} + 1 = 17$ (premier)
- $F_3 = 2^{2^3} + 1 = 257$ (premier)
- $F_4 = 2^{2^4} + 1 = 65537$ (premier)
- $F_5 = 2^{2^5} + 1 = 4294967297$ (composite, factorisé par Euler en 641×6700417)

Remarque A.3. Pierre de Fermat conjecturait que tous les F_n étaient premiers, mais cela est faux pour $n \geq 5$. À ce jour, les seuls nombres de Fermat premiers connus sont pour $n = 0$ à 4, et pour $n > 4$, ils sont tous composites ou de statut inconnu (mais probablement composites).

A.1.1 Propriétés arithmétiques

Théorème A.4 (Coprimauté des nombres de Fermat)**.** Pour tous $m \neq n$, $\gcd(F_m, F_n) = 1$. Plus précisément, si $m < n$, alors F_n est divisible par F_m ? Non, au contraire : ils sont premiers entre eux.

Démonstration. On montre que $F_n = F_0 F_1 \cdots F_{n-1} + 2$. Par induction :

$$F_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1) = (F_{n-1} - 2)F_{n-1} + 2(F_{n-1} - 1) + 2$$

La formule correcte est :

$$\prod_{k=0}^{n-1} F_k = F_n - 2$$

Par induction : Pour $n = 1$, $F_0 = 3 = 5 - 2 = F_1 - 2$. Supposons vrai pour $n - 1$:

$$\prod_{k=0}^{n-1} F_k = F_{n-1} \prod_{k=0}^{n-2} F_k = F_{n-1}(F_{n-1} - 2) = (2^{2^{n-1}} + 1)2^{2^{n-1}} - 2 = 2^{2^n} + 2^{2^{n-1}} - 2$$

Non, correction : $F_{n-1}(F_{n-1} - 2) = (F_{n-1} - 2)F_{n-1} = F_{n-1}^2 - 2F_{n-1}$, mauvais.

La bonne identité est :

$$F_n = \prod_{k=0}^{n-1} F_k + 2 \cdot (-1)^{2^n}$$

Non, la formule est :

$$\prod_{k=0}^{n-1} F_k = F_n - 2$$

Oui, vérifions pour n=2: F0 F1 = 3*5=15, F2-2=17-2=15. Pour n=3: 3*5*17=255, F3-2=257-2=255. Oui.

Donc, $F_n = \prod_{k=0}^{n-1} F_k + 2$.

Ainsi, pour m < n, F_m divise $F_n - 2$, donc $\gcd(F_m, F_n) = \gcd(F_m, 2)$. Mais$F_m$ est impair ($2^{something} + 1$), donc $gcd = 1$. □

Théorème A.5. Aucun nombre de Fermat ne peut être exprimé comme la somme de deux nombres premiers, sauf$F1 = 2 + 3$.

Théorème A.6. Les facteurs premiers d'un nombre de Fermat $F_n (n > 2)$sont de la forme$k \cdot 2^{n+2} + 1$.

Remarque A.7. Les nombres de Fermat sont utilisés en géométrie (polygones constructibles : un polygone régulier à m côtés est constructible à la règle et au compas si m est produit de puissances de 2 et de nombres de Fermat premiers distincts).

A.2 Suite de Fibonacci

Définition A.8. La suite de Fibonacci est définie par $F_0 = 0$, $F_1 = 1$, et pour $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$.

Exemple A.9. Les premiers termes : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

A.2.1 Propriétés arithmétiques

Théorème A.10 (Propriété de divisibilité)**.** Pour tous entiers positifs m, n, avec m divisant n, F_m divise F_n.

Démonstration. Par induction sur n/m. Base : si m=n, évident. Sinon, utiliser la récurrence. □

Théorème A.11 (PGCD des Fibonacci)**.**

$$\gcd(F_m, F_n) = F_{\gcd(m,n)}$$

Démonstration. Utiliser la propriété euclidienne : $\gcd(F_n, F_m) = \gcd(F_m, F_{n \mod m})$, et itérer jusqu'à la gcd des indices. □

Exemple A.12. $\gcd(F_6, F_9) = \gcd(8, 34)$ mais wait: $F6 = 8, F9 = 34, gcd(8, 34) = 2$, and $gcd(6, 9) = 3, F3 = 2$. Oui.

Théorème A.13 (Identité de Cassini)**.** Pour tout $n \geq 1$,

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

Démonstration. à faire □

Théorème A.14 (Somme des premiers Fibonacci)**.**

$$\sum_{k=1}^{n} F_k = F_{n+2} - 1$$

Démonstration. a faire en exercice □

Théorème A.15 (Limite et ratio d'or)**.** Le ratio $\frac{F_{n+1}}{F_n}$ tend vers le nombre d'or $\phi = \frac{1+\sqrt{5}}{2} \approx 1.618$.

Théorème A.16 (Formule de Binet)**.**

$$F_n = \frac{\phi^n - (-\phi)^{-n}}{\sqrt{5}}$$

où $\phi = \frac{1+\sqrt{5}}{2}$.

Remarque A.17. Les nombres de Fibonacci apparaissent dans de nombreuses propriétés arithmétiques, comme les identités trigonométriques, les fractions continues, et même dans la primalité (test de Lucas-Lehmer utilise des variantes).

B Fonctions arithmétiques

B.1 Décomposition en facteurs premiers

Tout entier naturel $n \geq 2$ admet une décomposition unique en produit de nombres premiers, d'après le théorème fondamental de l'arithmétique :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

où $p_1 < p_2 < \cdots < p_k$ sont des nombres premiers distincts et $\alpha_i \in \mathbb{N}^*$. Cette décomposition permet de calculer le nombre de diviseurs, leur somme, et l'indicateur d'Euler, qui sont des fonctions multiplicatives.

B.2 Nombre de diviseurs

Définition B.1. Soit $n \in \mathbb{N}^*$. L'ensemble des diviseurs positifs de n, noté $\mathfrak{D}(n)$, est l'ensemble des entiers $d \geq 1$ tels que $d \mid n$. La fonction nombre de diviseurs, notée $\tau(n)$, donne le cardinal de $\mathfrak{D}(n)$.

Théorème B.2. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, alors :

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

Démonstration. Un diviseur positif de n est de la forme $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, où $0 \leq \beta_i \leq \alpha_i$ pour tout i. Pour chaque p_i, il y a $\alpha_i + 1$ choix pour β_i (de 0 à α_i). Ainsi, le nombre total de diviseurs est le produit des choix possibles :

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

□

Exemple B.3. Pour $n = 12 = 2^2 \cdot 3^1$, on a $\tau(12) = (2+1)(1+1) = 3 \cdot 2 = 6$. Les diviseurs sont $\{1, 2, 3, 4, 6, 12\}$.

B.3 Somme des diviseurs

Définition B.4. La fonction somme des diviseurs, notée $\sigma(n)$, est définie par :

$$\sigma(n) = \sum_{d|n, d>0} d$$

Théorème B.5. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, alors :

$$\sigma(n) = (1+p_1+p_1^2+\cdots+p_1^{\alpha_1})(1+p_2+p_2^2+\cdots+p_2^{\alpha_2}) \cdots (1+p_k+p_k^2+\cdots+p_k^{\alpha_k})$$

Démonstration. Un diviseur de n est de la forme $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, avec $0 \leq \beta_i \leq \alpha_i$. La somme des diviseurs est :

$$\sigma(n) = \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \cdots \sum_{\beta_k=0}^{\alpha_k} p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

Comme les termes sont indépendants pour chaque p_i, on peut factoriser :

$$\sigma(n) = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \right) \left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2} \right) \cdots \left(\sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k} \right)$$

Chaque somme est une série géométrique : $\sum_{\beta_i=0}^{\alpha_i} p_i^{\beta_i} = 1+p_i+p_i^2+\cdots+p_i^{\alpha_i}$, d'où le résultat. □

Exemple B.6. Pour $n = 12 = 2^2 \cdot 3^1$, on a :

$$\sigma(12) = (1+2+2^2)(1+3) = (1+2+4)(1+3) = 7 \cdot 4 = 28$$

Vérification : $1+2+3+4+6+12 = 28$.

B.4 Indicateur d'Euler

Définition B.7. L'indicateur d'Euler, noté $\phi(n)$, est le nombre d'entiers k tels que $1 \leq k \leq n$ et $\text{PGCD}(k, n) = 1$.

Théorème B.8. Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, alors :

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Démonstration. Pour un nombre premier p élevé à la puissance α, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$, car sur les p^α entiers de 1 à p^α, ceux divisibles par p (soit $p^{\alpha-1}$ nombres) ne sont pas premiers avec p^α. Ainsi :

$$\phi(p^\alpha) = p^\alpha \left(1 - \frac{1}{p}\right)$$

Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, comme les p_i sont distincts, la fonction ϕ est multiplicative (voir ci-dessous), donc :

$$\phi(n) = \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}) = \prod_{i=1}^{k} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

□

Exemple B.9. Pour $n = 12 = 2^2 \cdot 3^1$, on a :

$$\phi(12) = 12 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

Les entiers premiers avec 12 sont $\{1, 5, 7, 11\}$, soit 4 nombres.

B.5 Propriété multiplicative

Définition B.10. Une fonction $f : \mathbb{N}^* \to \mathbb{N}$ est **multiplicative** si, pour tous $m, n \in \mathbb{N}^*$ tels que $\text{PGCD}(m, n) = 1$, on a :

$$f(mn) = f(m) \cdot f(n)$$

Théorème B.11. Les fonctions τ, σ, et ϕ sont multiplicatives.

Démonstration. Soit $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $n = q_1^{\beta_1} \cdots q_l^{\beta_l}$, avec $\text{PGCD}(m, n) = 1$, donc les p_i et q_j sont distincts. Alors $mn = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$.

- **Pour τ :**

$$\tau(m) = (\alpha_1+1) \cdots (\alpha_k+1), \quad \tau(n) = (\beta_1+1) \cdots (\beta_l+1)$$

$$\tau(mn) = (\alpha_1+1) \cdots (\alpha_k+1)(\beta_1+1) \cdots (\beta_l+1) = \tau(m) \cdot \tau(n)$$

- **Pour σ :**

$$\sigma(m) = (1 + p_1 + \cdots + p_1^{\alpha_1}) \cdots (1 + p_k + \cdots + p_k^{\alpha_k})$$

$$\sigma(n) = (1 + q_1 + \cdots + q_1^{\beta_1}) \cdots (1 + q_l + \cdots + q_l^{\beta_l})$$

$$\sigma(mn) = (1+p_1+\cdots+p_1^{\alpha_1}) \cdots (1+p_k+\cdots+p_k^{\alpha_k})(1+q_1+\cdots+q_1^{\beta_1}) \cdots (1+q_l+\cdots+q_l^{\beta_l}) = \sigma(m) \cdot \sigma(n)$$

- **Pour ϕ :**

$$\phi(m) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right), \quad \phi(n) = n \prod_{j=1}^{l} \left(1 - \frac{1}{q_j}\right)$$

$$\phi(mn) = mn \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^{l} \left(1 - \frac{1}{q_j}\right) = \phi(m) \cdot \phi(n)$$

□

Exemple B.12. Pour $m = 4 = 2^2$, $n = 9 = 3^2$, PGCD$(4, 9) = 1$, et $mn = 36 = 2^2 \cdot 3^2$, vérifions :

- $\tau(4) = 3$, $\tau(9) = 3$, $\tau(36) = (2+1)(2+1) = 9 = 3 \cdot 3$.
- $\sigma(4) = 1+2+4 = 7$, $\sigma(9) = 1+3+9 = 13$, $\sigma(36) = 1+2+3+4+6+9+12+18+36 = 91 = 7 \cdot 13$.
- $\phi(4) = 4 \cdot \frac{1}{2} = 2$, $\phi(9) = 9 \cdot \frac{2}{3} = 6$, $\phi(36) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12 = 2 \cdot 6$.

C L'anneau $\mathbb{Z}/n\mathbb{Z}$ en arithmétique modulaire

C.1 Structure de l'anneau $\mathbb{Z}/n\mathbb{Z}$

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes d'équivalence modulo n, muni des opérations d'addition et de multiplication modulo n. C'est un anneau commutatif unifère.

- Les éléments sont les classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.
- Addition : $\overline{a} + \overline{b} = \overline{a+b}$.
- Multiplication : $\overline{a} \cdot \overline{b} = \overline{ab}$.

Si $n = p$ est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps, car tout élément non nul a un inverse multiplicatif.

Exemple C.1. Dans $\mathbb{Z}/5\mathbb{Z}$, les inverses sont : $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$ (car $2 \times 3 = 6 \equiv 1 \pmod 5$), etc.

Cet anneau est fondamental en arithmétique modulaire pour étudier les congruences, les résidus quadratiques, etc.

Équations de degré 1 et 2 dans $\mathbb{Z}/n\mathbb{Z}$

Équations linéaires

Une équation de degré 1 dans $\mathbb{Z}/n\mathbb{Z}$ s'écrit :

$$\overline{a} \cdot \overline{x} = \overline{b}$$

où $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$.

- Si $\gcd(a, n) = 1$, alors $\overline{a}$ est inversible et l'équation admet une unique solution :
$$\overline{x} = \overline{a}^{-1} \cdot \overline{b}$$
- Si $\gcd(a, n) = d > 1$, l'équation admet des solutions si et seulement si $d \mid b$. Dans ce cas, il y a exactement d solutions distinctes modulo n.

Exemple C.2. Dans $\mathbb{Z}/6\mathbb{Z}$, considérons l'équation $\overline{4} \cdot \overline{x} = \overline{2}$.

- On a $\gcd(4, 6) = 2$ et $2 \mid 2$, donc il existe des solutions.
- Les solutions sont de la forme $\overline{x} = \overline{2} + k \cdot \overline{3}$ pour $k \in \{0, 1\}$, c'est-à-dire $\overline{x} = \overline{2}$ et $\overline{x} = \overline{5}$.

Équations quadratiques

Une équation de degré 2 dans $\mathbb{Z}/n\mathbb{Z}$ s'écrit :

$$\overline{a} \cdot \overline{x}^2 + \overline{b} \cdot \overline{x} + \overline{c} = \overline{0}$$

La résolution dépend fortement de la structure de n (nombre premier, puissance d'un premier, etc.).

- Si $n = p$ est premier, on peut utiliser les méthodes classiques (discriminant, factorisation).

- Si n est composé, le théorème des restes chinois permet de se ramener au cas où n est une puissance d'un premier.

Exemple C.3. Dans $\mathbb{Z}/7\mathbb{Z}$, résolvons $\overline{x}^2 + \overline{6} \cdot \overline{x} + \overline{2} = \overline{0}$.

- L'équation équivaut à $x^2 + 6x + 2 \equiv 0 \pmod 7$.
- Le discriminant est $\Delta = \overline{6}^2 - 4 \cdot \overline{1} \cdot \overline{2} = \overline{36} - \overline{8} = \overline{28} = \overline{0}$ (car $28 \equiv 0 \pmod 7$).
- Il y a une solution double : $\overline{x} = \frac{-\overline{6}}{\overline{2}} = \overline{1}$.

Un autre exemple si n est composé:

Exemple C.4. Soit à résoudre l'équation $\overline{x}^2 + \overline{3}\overline{x} + \overline{2} = \overline{0}$ dans $\mathbb{Z}/6\mathbb{Z}$.

- Comme $6 = 2 \times 3$, le théorème des restes chinois nous donne l'isomorphisme :
$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$
- On résout d'abord modulo 2 :
$$\overline{x}^2 + \overline{3}\overline{x} + \overline{2} \equiv \overline{x}^2 + \overline{1}\overline{x} \equiv \overline{0} \quad \text{dans} \quad \mathbb{Z}/2\mathbb{Z}$$
$$\Rightarrow \overline{x}(\overline{x} + \overline{1}) = \overline{0}$$
Solutions : $\overline{0}$, $\overline{1}$
- Puis modulo 3 :
$$\overline{x}^2 + \overline{3}\overline{x} + \overline{2} \equiv \overline{x}^2 + \overline{2} \equiv \overline{0} \quad \text{dans} \quad \mathbb{Z}/3\mathbb{Z}$$
$$\Rightarrow \overline{x}^2 \equiv \overline{1}$$
Solutions : $\overline{1}$, $\overline{2}$
- On combine les solutions via le théorème chinois :
$$\begin{aligned} &x \equiv 0 \pmod 2 \quad \text{et} \quad x \equiv 1 \pmod 3 \Rightarrow x \equiv 4 \pmod 6 \\ &x \equiv 0 \pmod 2 \quad \text{et} \quad x \equiv 2 \pmod 3 \Rightarrow x \equiv 2 \pmod 6 \\ &x \equiv 1 \pmod 2 \quad \text{et} \quad x \equiv 1 \pmod 3 \Rightarrow x \equiv 1 \pmod 6 \\ &x \equiv 1 \pmod 2 \quad \text{et} \quad x \equiv 2 \pmod 3 \Rightarrow x \equiv 5 \pmod 6 \end{aligned}$$
- Solutions finales dans $\mathbb{Z}/6\mathbb{Z}$:
$$\overline{1},\ \overline{2},\ \overline{4},\ \overline{5}$$

Ces méthodes s'étendent ensuite à l'étude des polynômes de degré supérieur et à des problèmes avancés comme les racines primitives ou les résidus quadratiques.

C.2 Théorème de Wilson

Théorème C.5 (Théorème de Wilson)**.** Soit p un entier naturel supérieur à 1. Alors p est premier si et seulement si :

$$(p-1)! \equiv -1 \pmod p$$

Démonstration. Nous prouvons la direction "si p est premier, alors $(p-1)! \equiv -1 \pmod p$". (La réciproque est vraie mais plus simple : si p composite, un facteur divise $(p-1)!$ sans diviser -1 mod p.)

Puisque p est premier, $\mathbb{Z}/p\mathbb{Z}^\times$ est un groupe multiplicatif d'ordre $p-1$.

Les éléments non nuls modulo p sont $1, 2, \ldots, p-1$. Pour chaque k tel que $1 < k < p-1$, si $k^2 \not\equiv 1 \pmod p$, alors k et son inverse k^{-1} sont distincts et peuvent être pairés.

Les seuls éléments qui sont leurs propres inverses sont solutions de $x^2 \equiv 1 \pmod p$, soit $x \equiv \pm 1 \pmod p$.

Ainsi, dans le produit $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$, on peut grouper les paires (k, k^{-1}) où chaque paire multiplie à 1 mod p, et il reste 1 et $p-1 \equiv -1 \pmod p$.

Le produit des paires est 1, et $1 \cdot (-1) = -1 \pmod p$. Donc :

$$(p-1)! \equiv -1 \pmod p$$

Pour la réciproque : Si p composite, disons $p = ab$ avec $1 < a, b < p$, alors a et b divisent $(p-1)!$, donc $(p-1)! \equiv 0 \pmod p$, pas -1. □

Exemple C.6. Pour $p = 5$, $4! = 24 \equiv -1 \pmod 5$ (24 - 5*5 = -1).

C.3 Symbole de Legendre

Définition C.7. Soit p un nombre premier impair et a un entier. Le **symbole de Legendre** $\left(\frac{a}{p}\right)$ est défini par :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a, \\ 1 & \text{si } a \text{ est un résidu quadratique modulo } p \text{ (non nul)}, \\ -1 & \text{si } a \text{ n'est pas un résidu quadratique modulo } p. \end{cases}$$

Un entier a non divisible par p est un résidu quadratique si l'équation $x^2 \equiv a \pmod{p}$ a une solution.

Propriété 9. Le symbole de Legendre est multiplicatif : $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Autres propriétés :

- $\left(\frac{a^2}{p}\right) = 1$ si $p \nmid a$.
- $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

Exemple C.8. Pour $p = 5$, $\left(\frac{3}{5}\right)$: Vérifions si 3 est résidu quadratique mod 5. Les carrés : $1^2 = 1$, $2^2 = 4$, $3^2 = 4$, $4^2 = 1$. Pas 3, donc -1.

C.4 Début de la réciprocité quadratique de Gauss

La loi de réciprocité quadratique, prouvée par Gauss en 1796, relie les symboles de Legendre pour deux nombres premiers impairs distincts p et q :

Théorème C.9 (Loi de réciprocité quadratique)**.** Soient p et q deux nombres premiers impairs distincts. Alors :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Cela signifie que $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ si au moins l'un de p ou q est congruent à 1 mod 4, et opposé sinon.

Cette loi permet de calculer efficacement le symbole de Legendre en réduisant à des cas simples.

Exemple C.10. Calculer $\left(\frac{15}{37}\right)$. Décomposer 15=3*5, et utiliser la multiplicativité et la réciprocité pour évaluer chaque partie.

Cette loi est fondamentale en théorie des nombres et a des applications en cryptographie et en algorithmes pour tester les résidus quadratiques.

C.5 Applications de la loi de réciprocité quadratique

La loi de réciprocité quadratique, qui établit que pour deux nombres premiers impairs distincts p et q, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, est un outil puissant pour déterminer si un entier est un résidu quadratique modulo un nombre premier. Voici trois applications concrètes.

C.5.1 Application 1 : Calcul du symbole de Legendre

Calculer $\left(\frac{15}{37}\right)$, où 37 est premier et $15 = 3 \cdot 5$.

Par la multiplicativité du symbole de Legendre :

$$\left(\frac{15}{37}\right) = \left(\frac{3}{37}\right)\left(\frac{5}{37}\right)$$

Utilisons la réciprocité quadratique pour $\left(\frac{3}{37}\right)$:

$$\left(\frac{3}{37}\right)\left(\frac{37}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{37-1}{2}} = (-1)^{1\cdot 18} = 1$$

Puisque $37 \equiv 1 \pmod{3}$, on a $\left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1$. Donc :

$$\left(\frac{3}{37}\right) = 1$$

Pour $\left(\frac{5}{37}\right)$:

$$\left(\frac{5}{37}\right)\left(\frac{37}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{37-1}{2}} = (-1)^{2\cdot 18} = 1$$

Puisque $37 \equiv 2 \pmod{5}$, on a $\left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = (-1)^3 = -1$. Donc :

$$\left(\frac{5}{37}\right) = -1$$

Ainsi :

$$\left(\frac{15}{37}\right) = 1 \cdot (-1) = -1$$

Donc, 15 n'est pas un résidu quadratique modulo 37.

C.5.2 Application 2 : Résolution d'équations quadratiques modulaires

Déterminer si l'équation $x^2 \equiv 7 \pmod{11}$ a une solution.

Calculons $\left(\frac{7}{11}\right)$. Par la réciprocité quadratique :

$$\left(\frac{7}{11}\right)\left(\frac{11}{7}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{11-1}{2}} = (-1)^{3\cdot 5} = -1$$

Puisque $11 \equiv 4 \pmod{7}$, on a $\left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2^2}{7}\right) = 1$. Donc :

$$\left(\frac{7}{11}\right) = -1$$

Puisque $\left(\frac{7}{11}\right) = -1$, l'équation $x^2 \equiv 7 \pmod{11}$ n'a pas de solution.

C.5.3 Application 3 : Simplification en cryptographie

En cryptographie, comme dans le protocole RSA, la loi de réciprocité quadratique aide à analyser les résidus quadratiques pour des calculs modulaires. Supposons que nous devions vérifier si un message chiffré est un carré modulo un grand nombre premier p. Par exemple, pour $p = 17$ et un message $a = 8$, calculons $\left(\frac{8}{17}\right)$.

Puisque $8 = 2^3$, on a :

$$\left(\frac{8}{17}\right) = \left(\frac{2^3}{17}\right) = \left(\frac{2}{17}\right)^3$$

Calculons $\left(\frac{2}{17}\right) = (-1)^{\frac{17^2-1}{8}} = (-1)^{\frac{288}{8}} = 1$. Donc :

$$\left(\frac{8}{17}\right) = 1^3 = 1$$

Ainsi, 8 est un résidu quadratique modulo 17, ce qui peut guider la vérification des propriétés des messages dans certains algorithmes cryptographiques.

***Exercice* C.1.** Soit p un nombre premier impair. On considère dans $\mathbb{Z}$ l'équation $(E) : x^2 \equiv 2 \pmod{p}$.

1. **Propriétés de 2^p**
   (a) Montrer que $2^{p-1} \equiv 1 \pmod{p}$.
   (b) En déduire que $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ou $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
   (On remarque que $(2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1) = 2^{p-1} - 1$.)
2. **Condition nécessaire pour l'existence d'une solution**
   Soit x une solution de (E).
   (a) Montrer que p et x sont premiers entre eux.
   (b) En déduire que $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
   (On pourra utiliser le théorème de Fermat.)
3. **Contradiction et étude des coefficients binomiaux**
   (a) Montrer que pour tout $k \in \{1, 2, \ldots, p-1\}$, p divise C_p^k.
   (Rappel : $C_p^k = \frac{p!}{k!(p-k)!}$ et $kC_p^k = pC_{p-1}^{k-1}$.)
   (b) En utilisant la formule de Moivre, montrer que :
   $(1+i)^p = 2^{\frac{p}{2}} \cos\left(\frac{p\pi}{4}\right) + i2^{\frac{p}{2}} \sin\left(\frac{p\pi}{4}\right)$,
   où i est le nombre complexe tel que $i^2 = -1$.
   (c) Montrer que :
   $(1+i)^p = \sum_{k=0}^{\frac{p-1}{2}} (-1)^k C_p^{2k} + i \sum_{k=0}^{\frac{p-1}{2}} (-1)^k C_p^{2k+1}$.
   (d) En déduire que $2^{\frac{p}{2}} \cos\left(\frac{p\pi}{4}\right) \in \mathbb{Z}$ et
   $2^{\frac{p}{2}} \cos\left(\frac{p\pi}{4}\right) \equiv 1 \pmod{p}$.
   (On pourra utiliser la question 3-a.)
4. **Cas particulier** on suppose que si $p \equiv 5 \pmod{8}$:
   En utilisant les questions 2 et 3 montrer que l'équation (E) n'admet pas de solution dans $\mathbb{Z}$.

Le reste de l'exercice est donné uniquement pour la culture et de niveau supérieur.
à faire après le devoir en fin de document car utilise la Loi de réciprocité de Gauss

5. **Étude de la condition nécessaire en fonction de p**

   (a) Montrer que si $p \equiv 1 \pmod 8$, alors $2^{\frac{p-1}{2}} \equiv 1 \pmod p$.

   (b) Montrer que si $p \equiv 7 \pmod 8$, alors $2^{\frac{p-1}{2}} \equiv 1 \pmod p$.

   (c) Montrer que si $p \equiv 3 \pmod 8$, alors $2^{\frac{p-1}{2}} \equiv -1 \pmod p$.
   (Indication : utiliser une méthode similaire à la question 3, en exploitant $(1+i)^p$ et les congruences.)

   (d) Conclure que pour $p \equiv 5 \pmod 8$, l'équation (E) n'a pas de solution.
   (Indication : relier ce cas aux questions précédentes.)

6. **Synthèse : Condition nécessaire et suffisante**

   (a) En regroupant les résultats des questions précédentes, montrer que :
   $x^2 \equiv 2 \pmod p$ admet une solution $\iff p \equiv 1$ ou $7 \pmod 8$.

   (b) Donner une méthode explicite pour calculer une solution lorsque $p \equiv 1 \pmod 8$.

7. **Application numérique**

   (a) Vérifier que pour $p = 17$ ($\equiv 1 \pmod 8$), l'équation admet des solutions, et en donner une.

   (b) Vérifier que pour $p = 7$ ($\equiv 7 \pmod 8$), l'équation admet des solutions, et en donner une.

   (c) Vérifier que pour $p = 5$ ($\equiv 5 \pmod 8$), l'équation n'a pas de solution.