Math & expert

R.Abed Prof Agrégé

Arithmétique
dans $\mathbb{Z}$

Cours complet avec définitions, théorèmes, propriétés, exercices résolus et applications

- Divisibilité dans $\mathbb{Z}$
- Division euclidienne
- Congruences
- PGCD & PPCM
- Théorèmes de Bezout & Gauss
- Nombres premiers
- Décomposition en facteurs
- Anneaux $\mathbb{Z}/n\mathbb{Z}$
- Systèmes de numération
- Exercices d'application

Prof. Abed
Professeur de Mathématiques
Maths Expert — Classe de 1ère Bac SM

À propos de ce cours

Ce polycopié de cours est destiné aux élèves de **2ème Bac Sciences Mathématiques**. Il couvre l'intégralité du chapitre « **Arithmétique dans** $\mathbb{Z}$ » conformément au programme officiel marocain.

Contenu :

- Rappels sur la divisibilité et la division euclidienne.
- Congruences modulo n et leurs propriétés.
- PGCD, PPCM et algorithme d'Euclide.
- Théorèmes de Bézout et de Gauss.
- Équations diophantiennes $ax + by = c$.
- Nombres premiers et décomposition en facteurs premiers.
- L'anneau $\mathbb{Z}/n\mathbb{Z}$ et inversibilité.
- Systèmes de numération et critères de divisibilité.

Organisation : Chaque notion est introduite par une définition rigoureuse, illustrée d'exemples et suivie d'exercices d'application progressifs.

Table des Matières

Table des matières

1 Rappels Divisibilité et Division Euclidienne

1.1 Divisibilité dans $\mathbb{Z}$

Définition 1.1 — Divisibilité

Soient $a, b \in \mathbb{Z}$. On dit que b **divise** a dans $\mathbb{Z}$, s'il existe $k \in \mathbb{Z}$ tel que $a = k \cdot b$. On note alors $b \mid a$.

$$b \mid a \iff \exists k \in \mathbb{Z}, \quad a = k \cdot b$$

Proposition 1.1 — Combinaisons linéaires

Soient $a, b \in \mathbb{Z}$, $u, v \in \mathbb{Z}$ et $d \in \mathbb{Z}$.

1. Si $d \mid a$ et $d \mid b$, alors $d \mid (au + bv)$.
2. Si $d \mid a$ et $d \mid b$, alors d divise $a + b$, $a - b$, ab, a^2, b^2.

Remarque

1. 1 divise tous les éléments de $\mathbb{Z}$.
2. 0 est divisible par tous les éléments de $\mathbb{Z}$.
3. Soit $a \in \mathbb{Z}$. Si $0 \mid a$, alors $a = 0$.
4. Les seuls diviseurs de 1 sont 1 et -1.

Exemple(s)

$D_6 = \{\pm 1, \pm 2, \pm 3, \pm 6\}$ et $3\mathbb{Z} = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

Proposition 1.2 — Propriétés fondamentales

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

1. $a \mid b \iff \pm a \mid \pm b \iff |a| \mid |b|$
2. **Transitivité :** Si $a \mid b$ et $b \mid c$, alors $a \mid c$.

3. Si $a \mid b$ et $b \mid a$, alors $|a| = |b|$.

4. Combinaisons linéaires : Si $a \mid b$ et $a \mid c$, alors pour tout $(\alpha, \beta) \in \mathbb{Z}^2$:

$$a \mid \alpha b + \beta c$$

5. Si $a \mid b$ et $d \mid c$, alors $ad \mid bc$.

6. $a \mid b \iff D_a \subset D_b \iff b\mathbb{Z} \subset a\mathbb{Z}$

Proposition 1.3 — Inégalité des diviseurs

Soit $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}$.

1. Si $b \mid a$, alors $|b| \leq |a|$.

2. Si de plus $b \in \mathbb{Z}^*$: si $a \mid b$ et $b \mid a$, alors $|a| = |b|$.

Exercice 1.1

1. Soient $p, n \in \mathbb{Z}$ tels que $p \mid 13n + 1$ et $p \mid -2n + 3$. Montrer que $p \mid 41$.

2. Déterminer les entiers relatifs a tels que $(a - 5) \mid (a + 7)$.

3. Montrer que pour tout $n \in \mathbb{N}$, $n(n + 1)(n + 2)$ est divisible par 6.

Solution. **1.** On forme la combinaison $2\times(13n+1)+13\times(-2n+3) = 26n+2-26n+39 = 41$. Donc $p \mid 41$.

2. $(a - 5) \mid (a + 7) \iff (a - 5) \mid [(a + 7) - (a - 5)] = 12$. Les diviseurs de 12 sont $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$. Donc $a - 5 \in \{1, 2, 3, 4, 6, 12, -1, -2, -3, -4, -6, -12\}$, soit $a \in \{6, 7, 8, 9, 11, 17, 4, 3, 2, 1, -1, -7\}$.

3. Parmi trois entiers consécutifs, l'un est divisible par 2 et l'un est divisible par 3. Comme $2 \wedge 3 = 1$, on conclut que $6 \mid n(n + 1)(n + 2)$.

1.2 La Division Euclidienne

1.2.1 Dans $\mathbb{N}$

Théorème 1.1 — Division euclidienne dans $\mathbb{N}$

Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un **unique** couple $(q, r) \in \mathbb{N}^2$ tel que :

$$a = bq + r \qquad \text{et} \qquad 0 \leq r < b$$

q est le **quotient** et r est le **reste** de la division euclidienne de a par b.

Exercice 1.2 — Application directe

Donner le quotient et le reste de la division euclidienne de 2017 par 16.

Solution : $2017 = 16 \times 126 + 1$. Donc $q = 126$ et $r = 1$.

1.2.2 Dans $\mathbb{Z}$

Théorème 1.2 — Division euclidienne dans $\mathbb{Z}$

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un **unique** couple $(q, r) \in \mathbb{Z}^2$ tel que :

$$\boxed{a = bq + r \qquad \text{et} \qquad 0 \leq r < |b|}$$

Exercice 1.3 — Applications

Donner le quotient et le reste de la division euclidienne de a par b dans les cas suivants :

1. $a = -2017$ et $b = 16$.
   Solution : On écrit $-2017 = 16 \times (-127) + 15$, donc $q = -127$, $r = 15$.
2. $a = 2017$ et $b = -16$.
   Solution : On a $|b| = 16$, donc $2017 = (-16) \times (-126) + 1$, ainsi $q = -126$, $r = 1$.
3. $a = -2017$ et $b = -16$.
   Solution : $-2017 = (-16) \times 127 + (-1)$. Mais $r = -1 < 0$, on ajuste : $-2017 = (-16) \times 126 + (-1)$... On recalcule : $-2017 = (-16) \times (127) + (-1)$. Comme $r < 0$, on prend $q = 127 - 1 = 126 + 1$ non... En fait $-2017 = (-16) \times 127 + (-2017 + 16 \times 127) = (-16) \times 127 + 15$. Donc $q = 127$, $r = 15$. ✓

Remarque

b divise a si et seulement si le reste dans la division euclidienne de a par b est **nul**.

Exercice 1.4 — Reste paramétré

Soit $n \in \mathbb{N}^*$. Déterminer le reste de la division euclidienne de :

1. $n^2 + 2n$ par $n + 1$.
2. $7n + 15$ par $3n + 2$.

Solution. **1.** On écrit $n^2 + 2n = n(n + 1) + n$. Comme $0 \leq n < n + 1$, le reste est $\boxed{n}$.

2. $7n + 15 = 2(3n + 2) + (n + 11)$. Pour $n \geq 5$, $n + 11 < 3n + 2$ donc le reste est $n + 11$. Pour $n \in \{2, 3, 4\}$: $7n + 15 = 3(3n + 2) + (-2n + 9)$, le reste est $-2n + 9$. Pour $n = 1$: $7n + 15 = 4(3n + 2) + (-5n + 7)$, le reste est 2.

Congruences Modulo n 2

2.1 Définition et propriétés fondamentales

Définition 2.1 — Congruence

Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. On dit que a est **congru** à b modulo n si n divise $a - b$. On écrit :

$$a \equiv b \pmod{n} \iff n \mid (a - b)$$

Exemple(s)

1. $3 \equiv -7 \pmod{5}$ car $5 \mid (3 - (-7)) = 10$. ✓
2. $-39 \equiv -5 \pmod{17}$ car $17 \mid (-39 + 5) = -34$. ✓

Proposition 2.1 — La congruence est une relation d'équivalence

Soient $a, b, c \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

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 $a \equiv c \pmod{n}$.

Proposition 2.2 — Compatibilité avec les opérations

Soient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$.

1. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a + c \equiv b + d \pmod{n}$.
2. Si $a \equiv b \pmod{n}$, alors $ac \equiv bc \pmod{n}$.
3. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $ac \equiv bd \pmod{n}$.
4. Si $a \equiv b \pmod{n}$, alors $\forall m \in \mathbb{N}$, $a^m \equiv b^m \pmod{n}$.

Proposition 2.3 — Lien avec la division euclidienne

Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ et $r \in \mathbb{Z}$. r est le reste dans la division euclidienne de a par b si et seulement si :

$$a \equiv r \pmod{b} \quad \text{et} \quad 0 \leq r < |b|$$

2.2 Exercices sur les congruences

Exercice 2.1

1. Soit $n \in \mathbb{N}$. Déterminer le reste de la division euclidienne de 2^n par 7.
2. En déduire les restes de la division euclidienne de 37^{26} et 37^{250} par 7.
3. Déterminer le reste de la division euclidienne de $N = 37^{21212^5}$ par 11.

Exercice 2.2

Soit $n \in \mathbb{N}$. Déterminer le reste de la division euclidienne de

$$a = 851^{3n} + 851^{2n} + 851^n + 2$$

par 7.

Exercice 2.3

Déterminer les valeurs de l'entier naturel n pour que le nombre $n^2 - 3n + 6$ soit divisible par 5.

Exercice 2.4

Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $212 \equiv x \pmod{11}$ avec $0 < x < 11$.
2. $1111 \equiv x \pmod{23}$ avec $-23 < x < 0$.

Exercice 2.5

Soit $n \in \mathbb{N}$ avec $n \geq 2$. Déterminer n dans les cas suivants :

1. $13 \equiv 2 \pmod{n}$.
2. $131 \equiv 7 \pmod{n}$.

Proposition 2.4

oient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$.

1. **Addition :** Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors :

$$a + c \equiv b + d \pmod{n}$$

2. **Soustraction :** Si $a \equiv b \pmod{n}$, alors $a + c \equiv b + c \pmod{n}$.
3. **Multiplication :** Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors :

$$ac \equiv bd \pmod{n}$$

4. **Puissances :** Si $a \equiv b \pmod{n}$, alors pour tout $m \in \mathbb{N}$:

$$a^m \equiv b^m \pmod{n}$$

Démonstration

Pour les puissances. Par récurrence sur $m \in \mathbb{N}$:

- *Initialisation* : $a^1 \equiv b^1 \pmod{n}$ par hypothèse.
- *Hérédité* : Si $a^m \equiv b^m \pmod{n}$ et $a \equiv b \pmod{n}$, alors par compatibilité de la multiplication : $a^{m+1} = a \cdot a^m \equiv b \cdot b^m = b^{m+1} \pmod{n}$.

...

Remarque

Attention : Pièges classiques .

1) $a \times b \equiv 0 \pmod{6}$ **n'implique pas** $a \equiv 0$ ou $b \equiv 0 \pmod{6}$.
2) Si $2x \equiv 4 \pmod{12}$ alors $x \equiv 2 \pmod{6}$ (et **non** modulo 12 !)
3) $a \equiv b \pmod{n}$ **n'implique pas** $p^a \equiv p^b \pmod{n}$ en général.

Proposition 2.5 — Simplification

Soient $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}^*$ et $d = c \wedge n$.

1. Si $ac \equiv bc \pmod{n}$ et $c \wedge n = 1$, alors $a \equiv b \pmod{n}$.
2. Si $ac \equiv bc \pmod{n}$, alors $a \equiv b \pmod{n/d}$.

Exemple(s)

[Chiffre des unités] **Quel est le chiffre des unités de 7^{98} ?**
On note que $7^4 = 2401 \equiv 1 \pmod{10}$. Or $98 = 4 \times 24 + 2$, donc $7^{98} = (7^4)^{24} \cdot 7^2 \equiv 1^{24} \cdot 49 \equiv 49 \equiv 9 \pmod{10}$.
Le chiffre des unités de 7^{98} est $\boxed{9}$.

Exemple(s)

On calcule les puissances de 3 modulo 10 : $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 7$, $3^4 \equiv 1 \pmod{10}$.
La suite est périodique de période 4. Or $2015 = 4 \times 503 + 3$, donc $3^{2015} \equiv 3^3 = 27 \equiv 7 \pmod{10}$.
Le chiffre des unités de 3^{2015} est $\boxed{7}$.

Exemple(s)

Quel est le reste de la division euclidienne de $451 \times 6^{43} - 912$ par 7 ?
On calcule : $6 \equiv -1 \pmod 7$, donc $6^{43} \equiv (-1)^{43} = -1 \equiv 6 \pmod 7$.
$451 = 7 \times 64 + 3$, donc $451 \equiv 3 \pmod 7$.
$912 = 7 \times 130 + 2$, donc $912 \equiv 2 \pmod 7$.
Ainsi : $451 \times 6^{43} - 912 \equiv 3 \times 6 - 2 = 18 - 2 = 16 \equiv 2 \pmod 7$.
Le reste est $\boxed{2}$.

Exercice 2.6 — Résoudre une équation par congruences

On considère l'équation $(E) : x^2 - 7y^2 = 3$ où x et y sont deux entiers relatifs.

1. Montrer que si (x, y) est solution alors $x^2 \equiv 3 \pmod 7$.

2. Déterminer les restes possibles de x^2 modulo 7.

3. En déduire que (E) n'a pas de solution.

Solution. **1.** Si (x, y) est solution : $x^2 = 3 + 7y^2 \equiv 3 \pmod 7$.

2. Les restes de x mod 7 sont $0, 1, 2, 3, 4, 5, 6$. On calcule :

$x \pmod 7$	0	1	2	3	4	5	6
$x^2 \pmod 7$	0	1	4	2	2	4	1

Les restes possibles de x^2 modulo 7 sont $\{0, 1, 2, 4\}$.

3. Le reste 3 n'apparaît pas dans ce tableau, donc $x^2 \equiv 3 \pmod 7$ est impossible. L'équation (E) n'admet **aucune solution**.

Exercice 2.7 — Divisibilité par 5

Démontrer que $2^{4n+1} + 3^{4n+1}$ est divisible par 5 pour tout $n \in \mathbb{N}$.

Solution. $2^4 = 16 \equiv 1 \pmod 5$, donc $2^{4n+1} = 2^{4n} \cdot 2 \equiv 1^n \cdot 2 = 2 \pmod 5$.
$3^4 = 81 \equiv 1 \pmod 5$, donc $3^{4n+1} = 3^{4n} \cdot 3 \equiv 1^n \cdot 3 = 3 \pmod 5$.
Ainsi $2^{4n+1} + 3^{4n+1} \equiv 2 + 3 = 5 \equiv 0 \pmod 5$. □

Exercice 2.8 — Disjonction de cas

Démontrer que pour tout $n \in \mathbb{N}$, $n(n^2 + 5)$ est divisible par 3.

Solution. Tout entier est congru à 0, 1 ou 2 modulo 3. On traite chaque cas :

- $n \equiv 0 \pmod 3$: $n(n^2+5) \equiv 0 \pmod 3$.
- $n \equiv 1 \pmod 3$: $n^2+5 \equiv 1+5 = 6 \equiv 0 \pmod 3$.
- $n \equiv 2 \pmod 3$: $n^2+5 \equiv 4+5 = 9 \equiv 0 \pmod 3$.

Dans tous les cas, $3 \mid n(n^2+5)$. □

Exercice 2.9 — Résoudre $4x \equiv 5 \pmod 9$

1. Compléter la table des restes modulo 9 :

$x \pmod 9$	0	1	2	3	4	5	6	7	8
$4x \pmod 9$	0	4	8	3	7	2	6	1	5

2. En déduire la solution de $4x \equiv 5 \pmod 9$.

3. Sachant que $4 \times 7 \equiv 1 \pmod 9$, résoudre $7x \equiv 8 \pmod 9$.

Solution. **2.** D'après la table, $4x \equiv 5 \pmod 9 \iff x \equiv 8 \pmod 9$.

3. $4 \times 7 \equiv 1 \pmod 9$, donc 7 est l'inverse de 4 modulo 9. $7x \equiv 8 \pmod 9 \implies 4 \times 7x \equiv 4 \times 8 \pmod 9 \implies x \equiv 32 \equiv 5 \pmod 9$.

PGCD et PPCM 3

3.1 Définitions

Définition 3.1 — PGCD et PPCM

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

1. Le **plus grand commun diviseur** (PGCD) de a et b est le plus grand diviseur positif commun à a et b. On le note $a \wedge b$.
2. Le **plus petit multiple commun** (PPCM) de a et b est le plus petit multiple positif commun à a et b. On le note $a \vee b$.

Remarque

En posant $D_a = \{x \in \mathbb{Z} \mid x \mid a\}$ et $M_a = \{x \in \mathbb{Z} \mid a \mid x\}$, on a :

$$a \wedge b = \max(D_a \cap \mathbb{N}^*,\ D_b \cap \mathbb{N}^*) \qquad a \vee b = \min(M_a \cap \mathbb{N}^*,\ M_b \cap \mathbb{N}^*)$$

3.2 Caractérisations

Caractérisation du PGCD

$d = a \wedge b$ si et seulement si :

(i) $d > 0$

(ii) $d \mid a$ et $d \mid b$

(iii) Pour tout $x \in \mathbb{Z}$, si $x \mid a$ et $x \mid b$, alors $x \leq d$

Caractérisation du PPCM

$m = a \vee b$ si et seulement si :

(i) $m > 0$

(ii) $a \mid m$ et $b \mid m$

(iii) Pour tout $x \in \mathbb{Z}$, si $a \mid x$ et $b \mid x$, alors $m \leq x$

Proposition 3.1 — Propriétés algébriques

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

1. $a \wedge b = b \wedge a$ et $a \vee b = b \vee a$ (commutativité)
2. $a \mid b \iff a \wedge b = |a|$ et $b \mid a \iff a \vee b = |a|$
3. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ et $(a \vee b) \vee c = a \vee (b \vee c)$ (associativité)
4. $(ca) \wedge (cb) = |c|(a \wedge b)$ et $(ca) \vee (cb) = |c|(a \vee b)$

3.3 Algorithme d'Euclide

Proposition 3.2 — Lemme d'Euclide

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Si r est le reste dans la division euclidienne de a par b, alors :

$$a \wedge b = b \wedge r$$

Théorème 3.1 — Algorithme d'Euclide

Soient $a, b \in \mathbb{Z}^*$. On effectue les divisions successives :

$$\begin{aligned}
a &= q_0 \cdot b + r_0, \quad 0 \leq r_0 < |b| \\
b &= q_1 \cdot r_0 + r_1, \quad 0 \leq r_1 < r_0 \\
&\vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} \cdot r_n + 0
\end{aligned}$$

Alors :

$$\boxed{a \wedge b = b \wedge r_0 = r_0 \wedge r_1 = \cdots = r_n}$$

Le PGCD est le dernier reste non nul.

Exercice 3.1 — Application : Algorithme d'Euclide

Déterminer $2016 \wedge 54$.

Solution :

$$\begin{aligned}
2016 &= 54 \times 37 + 18 \\
54 &= 18 \times 3 + 0
\end{aligned}$$

Donc $\mathbf{2016 \wedge 54 = 18}$.

Exercice 3.2

Soit $x, y \in \mathbb{N}^*$. On pose $a = 9x + 4y$ et $b = 2x + y$. Montrer que $a \wedge b = x \wedge y$.

Solution. **1.** $a - 4b = (9x + 4y) - 4(2x + y) = x$ et $5b - a = 5(2x + y) - (9x + 4y) = y$. Donc $a \wedge b = b \wedge (a - 4b) = b \wedge x$. De même $a \wedge b$ divise y. Par combinaisons linéaires, $x \wedge y \mid a \wedge b$ et $a \wedge b \mid x \wedge y$, donc $a \wedge b = x \wedge y$.

2. $(x \wedge y)(x \vee y) = xy \Rightarrow xy = 60 \times 3600 = 216000$. Avec $x+y$ à trouver : $x = 60a'$, $y = 60b'$ avec $a' \wedge b' = 1$ et $a'b' = 60$. Les couples (a', b') sont : $(1, 60), (3, 20), (4, 15), (5, 12)$, d'où $(x, y) \in \{(60, 3600), (180, 1200), (240, 900), (300, 720)\}$.

Exercice 3.3

Soit $a, b, c \in \mathbb{N}^*$. Montrer que $a \wedge (a^2bc + ac + b) = a \wedge b$.

Nombres Premiers Entre Eux 4

4.1 Définition et exemples

Définition 4.1 — Nombres premiers entre eux

Soient $a, b \in \mathbb{Z}^*$. On dit que a et b sont **premiers entre eux** si $a \wedge b = 1$.

Exemple(s)

1. 16 et 9 sont premiers entre eux ($16 \wedge 9 = 1$).
2. 25 et -12 sont premiers entre eux ($25 \wedge 12 = 1$).

Exercice 4.1

Montrer que $\forall n \in \mathbb{Z}$, les nombres n et $n+1$ sont premiers entre eux.

4.2 Caractérisation et corollaire

Proposition 4.1 — Caractérisation du PGCD via la décomposition

Soient $a, b \in \mathbb{Z}^*$ et $d \in \mathbb{N}^*$. On a :

$$d = a \wedge b \iff \exists\, a', b' \in \mathbb{Z} : a = da',\ b = db',\ a' \wedge b' = 1$$

Corollaire 4.1 — Relation PGCD-PPCM

Soient $a, b \in \mathbb{Z}^*$. On a :

$$\boxed{(a \wedge b) \cdot (a \vee b) = |ab|}$$

Théorème 4.1 — Identité de Bézout (forme générale)

Soient $a, b \in \mathbb{Z}^*$ et $d = a \wedge b$. Il existe $(u, v) \in \mathbb{Z}^2$ tel que :

$$au + bv = d$$

Exercice 4.2

Résoudre dans $\mathbb{N}^2$ le système : $\begin{cases} x \wedge y = 60 \\ x \vee y = 3600 \end{cases}$

Exercice 4.3

Soit $a, b \in \mathbb{N}$. Montrer que $a \wedge b = 1 \iff (a+b) \wedge (ab) = 1$. En déduire que pour tout $(x, y) \in (\mathbb{Z}^*)^2$: $(x+y) \wedge (x \vee y) = x \wedge y$. Résoudre dans $(\mathbb{N}^*)^2$ le système : $\begin{cases} x + y = 276 \\ x \vee y = 1440 \end{cases}$

Théorèmes de Bézout et de Gauss 5

5.1 Théorème de Bézout

Théorème 5.1 — Bézout

Soient $a, b \in \mathbb{Z}^*$. On a l'équivalence :

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

Méthode : Déterminer les coefficients de Bézout

Exemple : Trouver u, v tels que $99u + 56v = 1$.

Étape 1 Algorithme d'Euclide (descente) :

$$\begin{aligned} 99 &= 56 \times 1 + 43 \\ 56 &= 43 \times 1 + 13 \\ 43 &= 13 \times 3 + 4 \\ 13 &= 4 \times 3 + 1 \\ 4 &= 1 \times 4 + 0 \end{aligned}$$

Donc $99 \wedge 56 = 1$.

Étape 2 Remontée (substitutions successives) :

$$\begin{aligned} 1 &= 13 - 4 \times 3 \\ &= 13 - (43 - 13 \times 3) \times 3 = 10 \times 13 - 3 \times 43 \\ &= 10(56 - 43) - 3 \times 43 = 10 \times 56 - 13 \times 43 \\ &= 10 \times 56 - 13(99 - 56) = 23 \times 56 - 13 \times 99 \end{aligned}$$

Donc $u = \mathbf{-13}$ et $v = \mathbf{23}$.

Exercice 5.1

Montrer que $\forall n \in \mathbb{N}$:

1. $5n + 3$ et $2n + 1$ sont premiers entre eux.

2. $2n-1$ et $3-7n$ sont premiers entre eux.

5.2 Théorème de Gauss

Théorème 5.2 — Gauss

Soient $a, b, c \in \mathbb{Z}^*$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Remarque

Remarque. La condition $a \wedge b = 1$ est **indispensable**. Par exemple : $6 \mid 18$ et $9 \mid 18$, mais $54 \nmid 18$.

Proposition 5.1

Soient $a, b, c \in \mathbb{Z}^*$. Si $a \mid c$, $b \mid c$ et $a \wedge b = 1$, alors $ab \mid c$.

Proposition 5.2

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

1. Si $a \wedge c = 1$ et $b \wedge c = 1$, alors $ab \wedge c = 1$.
2. Si $a \wedge b = 1$, alors $\forall n \in \mathbb{N} : a \wedge b^n = 1$.
3. Si $a \wedge b = 1$, alors $\forall n, m \in \mathbb{N} : a^n \wedge b^m = 1$.

5.3 Congruences et simplification

Proposition 5.3

Soient $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}^*$. Si $ac \equiv bc \pmod{n}$ et $c \wedge n = 1$, alors $a \equiv b \pmod{n}$.

Proposition 5.4

Soient $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}^*$ et $d = c \wedge n$. Si $ac \equiv bc \pmod{n}$, alors $a \equiv b \pmod{n/d}$.

5.4 Équations diophantiennes $ax + by = c$

Théorème 5.3 — Équation diophantienne

Soient $a, b, c \in \mathbb{Z}$ et $d = a \wedge b$. On considère l'équation dans $\mathbb{Z}^2$:

$$ax + by = c \quad (E)$$

1. Si $d \nmid c$, l'équation (E) n'admet **aucune solution**.

2. Si $d \mid c$, on pose $a = da'$, $b = db'$, $c = dc'$ avec $a' \wedge b' = 1$. Soit (x_0, y_0) une solution particulière de $a'x + b'y = c'$. L'ensemble des solutions est :

$$\mathcal{S} = \{(x_0 + kb',\ y_0 - ka') \mid k \in \mathbb{Z}\}$$

Exercice 5.2 — Application

Résoudre dans $\mathbb{Z}^2$ l'équation $9x - 15y = 24$.

Solution : $d = 9 \wedge 15 = 3$. Comme $3 \mid 24$, on divise par 3 : $3x - 5y = 8$.

On cherche une solution particulière de $3x - 5y = 1$ par l'algorithme d'Euclide : $5 = 3 \times 1 + 2$, $3 = 2 \times 1 + 1$, d'où $1 = 3 - 2 = 3 - (5 - 3) = 2 \times 3 - 5$. Donc $u_0 = 2$, $v_0 = -1$.

Solution particulière de $3x - 5y = 8$: $x_0 = 2 \times 8 = 16$, $y_0 = (-1) \times 8 = -8$.

Ensemble des solutions : $\mathcal{S} = \{(16 + 5k,\ -8 - 3k) \mid k \in \mathbb{Z}\}$.

Exercice 5.3

1. Résoudre dans $\mathbb{Z}^2$: $212x + 37y = 1$.

2. Déterminer le plus petit entier naturel dont les restes sont 5, 13, 17 lors des divisions par 15, 23, 27 respectivement.

Solution. **2.** Soit N cet entier. $N + 10 = 15(q_1 + 1) = 23(q_2 + 1) = 27(q_3 + 1)$. Donc $N + 10$ est multiple commun de 15, 23 et 27. $\text{ppcm}(15, 23, 27) = 27 \times 23 \times 5 = 3105$ (car $15 \wedge 23 = 15 \wedge 27 = 23 \wedge 27 = 1$). Donc $N + 10 = 3105$, soit $N = 3095$.

PGCD de Plusieurs Entiers 6

Définition 6.1 — PGCD de n entiers

Soient $a_1, a_2, \ldots, a_n$ des entiers relatifs non nuls. Le plus grand entier naturel positif non nul qui divise tous les a_i s'appelle leur **PGCD**. On le note $a_1 \wedge a_2 \wedge \cdots \wedge a_n$.

Remarque

$d = a_1 \wedge a_2 \wedge \cdots \wedge a_n$ si et seulement si :

$$d > 0, \quad d \mid a_i \ \forall i, \quad \text{et} \quad \forall c \in \mathbb{Z} : (c \mid a_i \ \forall i) \Rightarrow c \leq d$$

Proposition 6.1 — Calcul récursif

$a_1 \wedge a_2 \wedge \cdots \wedge a_n \wedge a_{n+1} = (a_1 \wedge a_2 \wedge \cdots \wedge a_n) \wedge a_{n+1}$

Définition 6.2 — Premiers entre eux dans leur ensemble

On dit que $a_1, a_2, \ldots, a_n$ sont **premiers entre eux dans leur ensemble** si $a_1 \wedge a_2 \wedge \cdots \wedge a_n = 1$.

Exemple(s)

6, 8 et 15 sont premiers entre eux dans leur ensemble car :

$$6 \wedge 8 \wedge 15 = (6 \wedge 8) \wedge 15 = 2 \wedge 15 = 1$$

Nombres Premiers 7

7.1 Définition et premières propriétés

Définition 7.1 — Nombre premier

Soit $a \in \mathbb{Z}$. On dit que a est un **nombre premier** si $|a| \geq 2$ et si ses seuls diviseurs sont ± 1 et $\pm a$.

Exemple(s)

$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ sont des nombres premiers positifs.

Proposition 7.1

Soit $a \in \mathbb{N}^*$ avec $a \geq 2$. Si a n'est pas premier, alors le plus petit entier > 1 qui divise a est un **nombre premier**.

Proposition 7.2

Soit $a \in \mathbb{N}^*$ avec $a \geq 2$. Si a n'est pas premier, alors a admet un diviseur premier p tel que $p^2 \leq a$.

Critère de primalité

Proposition : Soit $a \in \mathbb{N}^*$, $a \geq 2$. Si aucun nombre premier $p \leq \sqrt{a}$ ne divise a, alors a est **premier**.

Application : Pour tester si 541 est premier : $\sqrt{541} \approx 23{,}3$. Les nombres premiers ≤ 23 sont : $2, 3, 5, 7, 11, 13, 17, 19, 23$. Aucun ne divise 541. Donc **541 est premier**.

Exercice 7.1

1979 et 2003 sont-ils des nombres premiers ?

Théorème 7.1

L'ensemble des nombres premiers est **infini**.

Démonstration d'Euclide

Supposons par l'absurde qu'il n'existe qu'un nombre fini de premiers $p_1, p_2, \ldots, p_n$. Posons $N = p_1 p_2 \cdots p_n + 1$. Alors $N > 1$, donc N admet un diviseur premier p. Mais p ne peut être aucun des p_i (car N laisse un reste de 1 dans la division par chaque p_i). Contradiction. □

7.2 Propriétés des nombres premiers

Proposition 7.3

Soient $p, q \in \mathbb{N}^*$.

1. Si p et q sont premiers et $p \neq q$, alors $p \wedge q = 1$.
2. Soit $a \in \mathbb{Z}$ et p un nombre premier. Alors : $p \mid a$ ou $p \wedge a = 1$.

Proposition 7.4

Soient $p, a, b \in \mathbb{N}^*$.

1. Si p est premier, $p \mid ab$ et $p \nmid a$, alors $p \mid b$.
2. Si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.
3. Si p est premier et $p \mid a_1 a_2 \cdots a_n$, alors $\exists\, i$ tel que $p \mid a_i$.
4. Si p est premier et $p \mid p_1 p_2 \cdots p_n$ (tous premiers), alors $\exists\, i$ tel que $p = p_i$.

Proposition 7.5

Soit p un nombre premier. Pour tout $k \in [\![2, p-1]\!]$:

$$p \mid C_p^k$$

7.3 Petit théorème de Fermat

Théorème 7.2 — Fermat

Soit p un nombre premier.

1. $\forall a \in \mathbb{Z} : a^p \equiv a \pmod{p}$.
2. Si $p \nmid a : a^{p-1} \equiv 1 \pmod{p}$.

Exercice 7.2 — Applications de Fermat

1. Montrer que $\forall n \in \mathbb{N} : n^5 \equiv n \pmod{30}$.
2. Montrer que $\forall n \in \mathbb{N} : 12^{12n+1} + 1 \equiv 0 \pmod{13}$.
3. Montrer que $\forall n \in \mathbb{N} : 10^{6n+4} + 3 \equiv 0 \pmod{7}$.
4. Déterminer le reste de la division euclidienne de 5^{2017} par 11.

Solution. **1.** Par Fermat, $n^5 \equiv n$ modulo 2, 3 et 5. Comme $2 \wedge 3 \wedge 5 = 1$ et $2 \times 3 \times 5 = 30$, par le théorème des restes chinois, $n^5 \equiv n \pmod{30}$.

2. Par Fermat : $5^{10} \equiv 1 \pmod{11}$. Or $2017 = 10 \times 201 + 7$, donc $5^{2017} \equiv 5^7 \pmod{11}$. $5^2 = 25 \equiv 3$, $5^4 \equiv 9$, $5^7 = 5^4 \times 5^2 \times 5 \equiv 9 \times 3 \times 5 = 135 \equiv 3 \pmod{11}$. Le reste est $\boxed{3}$.

3. $11 \equiv 4 \pmod{7}$, $11^2 \equiv 16 \equiv 2$, $11^3 \equiv 8 \equiv 1 \pmod{7}$. Donc l'ordre de 11 mod 7 est 3, et $11^6 \equiv (11^3)^2 \equiv 1 \pmod{7}$. $2018 = 6 \times 336 + 2$, donc $11^{2018} \equiv 11^2 \equiv 121 \equiv 2 \pmod{7}$.

8 Décomposition en Facteurs Premiers

Théorème 8.1 — Décomposition unique

Soit $n \in \mathbb{Z}^*$, $n \neq \pm 1$. Il existe des nombres premiers **uniques** $p_1 < p_2 < \cdots < p_m$ et des entiers naturels non nuls **uniques** $\alpha_1, \alpha_2, \ldots, \alpha_m$ tels que :

$$\boxed{n = \varepsilon \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}, \quad \varepsilon \in \{-1, 1\}}$$

Exemple(s)

$-2520 = -1 \times 2^3 \times 3^2 \times 5 \times 7$.

Proposition 8.1 — PGCD et PPCM par décomposition

Soient $a = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ et $b = p_1^{\beta_1} \cdots p_m^{\beta_m}$ (avec $\alpha_i, \beta_i \in \mathbb{N}$). Alors :

$$a \wedge b = p_1^{\min(\alpha_1, \beta_1)} \cdots p_m^{\min(\alpha_m, \beta_m)}$$

$$a \vee b = p_1^{\max(\alpha_1, \beta_1)} \cdots p_m^{\max(\alpha_m, \beta_m)}$$

Exemple(s)

$a = 120 = 2^3 \times 3 \times 5$ et $b = 588 = 2^2 \times 3 \times 7^2$.
$a \wedge b = 2^2 \times 3 = 12$ et $a \vee b = 2^3 \times 3 \times 5 \times 7^2 = 5880$.

Proposition 8.2 — Nombre de diviseurs

Soit $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m} \in \mathbb{N}$ avec $\alpha_i \in \mathbb{N}^*$. Le nombre de diviseurs positifs de a est :

$$\mathcal{D}(a) = (1 + \alpha_1)(1 + \alpha_2) \cdots (1 + \alpha_m)$$

Exemple(s)

$a = 2520 = 2^3 \times 3^2 \times 5 \times 7$.
Nombre de diviseurs : $D(2520) = (3+1)(2+1)(1+1)(1+1) = 4 \times 3 \times 2 \times 2 = 48$.

Exercice 8.1

Soit $a = p_1^{\alpha_1} \cdots p_m^{\alpha_m} \in \mathbb{N}^* \setminus \{1\}$ et $\mathcal{D}(a)$ son nombre de diviseurs.

1. Montrer que $\mathcal{D}(a) = (1+\alpha_1) \cdots (1+\alpha_m)$.
2. Montrer que si $a \wedge b = 1$, alors $\mathcal{D}(ab) = \mathcal{D}(a) \cdot \mathcal{D}(b)$.
3. Déterminer le plus petit entier naturel a tel que $\mathcal{D}(a) = 29$.
4. Montrer que a est un carré parfait si et seulement si $\mathcal{D}(a)$ est impair.

Solution. **2.** 29 est premier. $D(a) = 29 \Rightarrow a = p^{28}$. Le plus petit est $a = 2^{28}$.

3. $D(a) = \prod(1+\alpha_i)$ est impair $\iff$ tous les $(1+\alpha_i)$ sont impairs $\iff$ tous les α_i sont pairs $\iff$ a est un carré parfait.

L'Anneau $\mathbb{Z}/n\mathbb{Z}$ 9

9.1 Classes de congruence

Définition 9.1 — Classe de congruence

Soit $n \in \mathbb{N}^*$. Pour tout $x \in \mathbb{Z}$, on pose :

$$\bar{x} = \{y \in \mathbb{Z} \mid y \equiv x \pmod{n}\}$$

Exemple(s)

Pour $n = 3$:

$$\bar{0} = \{3k \mid k \in \mathbb{Z}\}, \quad \bar{1} = \{1 + 3k \mid k \in \mathbb{Z}\}, \quad \bar{2} = \{2 + 3k \mid k \in \mathbb{Z}\}$$

Ces trois ensembles forment une partition de $\mathbb{Z}$.

Définition 9.2 — L'ensemble $\mathbb{Z}/n\mathbb{Z}$

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

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$$

Définition 9.3 — Opérations dans $\mathbb{Z}/n\mathbb{Z}$

Soient $\bar{x}, \bar{y} \in \mathbb{Z}/n\mathbb{Z}$ et $k \in \mathbb{Z}$. On définit :

1. $\bar{x} + \bar{y} = \overline{x + y}$
2. $\bar{x} \times \bar{y} = \overline{x \times y}$
3. $k \cdot \bar{x} = \overline{kx}$

Exercice 9.1

Donner le tableau de l'addition et de la multiplication de $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

9.2 Inversibilité

Définition 9.4 — Élément inversible

Soit $n \in \mathbb{N}^*$ et $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$. On dit que $\bar{x}$ est **inversible** dans $\mathbb{Z}/n\mathbb{Z}$ pour $\times$, s'il existe $\bar{y} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{x} \times \bar{y} = \bar{1}$.

Proposition 9.1 — Critère d'inversibilité

Soit $n \in \mathbb{N}^*$ et $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$. $\bar{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ pour $\times$ si et seulement si :

$$x \wedge n = 1$$

Théorème 9.1 — Corps $\mathbb{Z}/p\mathbb{Z}$

Soit $p \in \mathbb{N}^*$. Si p est premier, alors tous les éléments de $\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ sont inversibles dans $(\mathbb{Z}/p\mathbb{Z}, \times)$.

Tables de $\mathbb{Z}/5\mathbb{Z}$

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

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

Dans $\mathbb{Z}/5\mathbb{Z}$: $\bar{2}^{-1} = \bar{3}$, $\bar{3}^{-1} = \bar{2}$, $\bar{4}^{-1} = \bar{4}$.

Systèmes de Numération 10

10.1 Écriture en base b

Théorème 10.1 — Représentation en base b

Soit $b \in \mathbb{N}^*$, $b \geq 2$. Pour tout entier naturel non nul n, il existe des entiers naturels $a_0, a_1, \ldots, a_m$ **uniques** tels que :

$$n = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0, \quad a_m \neq 0, \quad 0 \leq a_i < b$$

On note : $n = \overline{a_m a_{m-1} \cdots a_1 a_0}_{(b)}$.

Exemple(s)

- $37 = 32 + 4 + 1 = 2^5 + 2^2 + 2^0$, donc $37 = \overline{100101}_{(2)}$.
- $37 = 27 + 9 + 1 = 3^3 + 3^2 + 3^0$, donc $37 = \overline{1101}_{(3)}$.

Exercice 10.1

Comparer les nombres suivants :

1. $\overline{2051}_{(6)}$ et $\overline{2051}_{(7)}$.
2. $\overline{2051}_{(6)}$ et $\overline{20510}_{(6)}$.

Exercice 10.2

Calculer et comparer :

1. $\overline{2343}_{(5)} + \overline{341}_{(5)}$ et $\overline{2343}_{(5)} \times \overline{341}_{(5)}$.
2. $\overline{697}_{(12)} + \overline{458}_{(12)}$ et $\overline{697}_{(12)} \times \overline{458}_{(12)}$.

10.2 Critères de divisibilité

Proposition 10.1 — Critères en base 10

Soit $x = \overline{a_m a_{m-1} \cdots a_1 a_0}_{(10)}$. On a :

1. $x \equiv 0 \pmod 5 \iff a_0 = 0$ ou $a_0 = 5$.
2. $x \equiv 0 \pmod 3 \iff \sum_{k=0}^{m} a_k \equiv 0 \pmod 3$.
3. $x \equiv 0 \pmod 9 \iff \sum_{k=0}^{m} a_k \equiv 0 \pmod 9$.
4. $x \equiv 0 \pmod{11} \iff \sum_{k=0}^{m} (-1)^k a_k \equiv 0 \pmod{11}$.
5. $x \equiv 0 \pmod 4 \iff \overline{a_1 a_0}_{(10)} \equiv 0 \pmod 4$.

Exercice 10.3

Déterminer $x, y \in \mathbb{N}$ pour que le nombre $\overline{26x95y}_{(10)}$ soit divisible par 3 et par 11.

Exercice 10.4

Soit $b \in \mathbb{N}$ avec $b \geq 6$, et $N = \overline{1540}_{(b)}$.

1. Montrer que N est divisible par b, par $b+1$ et par $b+4$.
2. Déterminer les valeurs de b (si elles existent) telles que N soit divisible par $b-1$.

Critère de divisibilté par 9

On a $10 \equiv 1 \pmod 9$, donc $10^k \equiv 1^k = 1 \pmod 9$ pour tout $k \geq 0$.
Ainsi $x = \sum_{k=0}^{m} a_k \times 10^k \equiv \sum_{k=0}^{m} a_k \times 1 = \sum_{k=0}^{m} a_k \pmod 9$. D'où $9 \mid x \iff 9 \mid \sum a_k$.

Critère de divisibilté par 11

$10 \equiv -1 \pmod{11}$, donc $10^k \equiv (-1)^k \pmod{11}$.
Ainsi $x \equiv \sum_{k=0}^{m} (-1)^k a_k \pmod{11}$.

Exemple(s)

L'entier $N = 8\,176\,312\,459\,102\,535\,214\,621$ est-il divisible par 3 ? Par 9 ?
Somme des chiffres : $8+1+7+6+3+1+2+4+5+9+1+0+2+5+3+5+2+1+4+6+2+1 = 78$.
$78 = 3 \times 26$ donc $3 \mid N$. Mais $78 = 9 \times 8 + 6$, donc $9 \nmid N$.

Exemple(s)

$619\,852\,805$: somme alternée $= 5-0+8-2+5-8+9-1+6 = 22 \equiv 0 \pmod{11}$.
Donc $11 \mid 619\,852\,805$.

Exemple(s)

Critère : Pour savoir si n est divisible par 7, on sépare le chiffre des unités u des autres chiffres q, et on forme $q - 2u$. Alors $7 \mid n \iff 7 \mid (q - 2u)$.

Exercice 10.5 — Critère de divisibilité par 7

1. Vérifier que 4361 est divisible par 7.

2. Démontrer ce critère pour un nombre à trois chiffres $n = \overline{abc}_{(10)}$.

Solution. **1.** $436 - 2 \times 1 = 434$. $43 - 2 \times 4 = 35 = 7 \times 5$. Donc $7 \mid 4361$.

2. $n = 100a + 10b + c$. On a $100 \equiv 2 \pmod 7$, $10 \equiv 3 \pmod 7$. Donc $n \equiv 2a + 3b + c \pmod 7$. $m = \overline{ab} - 2c = 10a + b - 2c$. $10 \equiv 3 \pmod 7$, donc $m \equiv 3a + b - 2c \pmod 7$. On calcule $n - 3m = (2a + 3b + c) - 3(3a + b - 2c) = -7a + 7c \equiv 0 \pmod 7$. Donc $7 \mid (n - 3m)$, et $7 \mid n \iff 7 \mid 3m \iff 7 \mid m$. □

Exercices Récapitulatifs 11

11.1 Divisibilité

Exercice 11.1

Déterminer les entiers n qui, divisés par 23, donnent un quotient égal au reste.

Exercice 11.2

Quel est le reste de la division euclidienne de $2018^{2^{1017}}$ par 7 ?

Exercice 11.3

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

1. Quels sont les entiers n pour lesquels le reste de la division euclidienne de $(n+2)^3$ par n^2 est $12n+8$?
2. Quels sont les entiers n pour lesquels le reste de la division euclidienne de $(n+1)^3$ par n^2 est $3n+1$?
3. Déterminer le reste et le quotient de $2n^2+n$ par $n+1$.

Exercice 11.4

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

1. Montrer que n^2 est pair $\iff$ n est pair.
2. Montrer que n^2 est impair $\iff$ n est impair.

Exercice 11.5

1. Soient $a, b \in \mathbb{N}$ tels que $a^2 - 2b^2 = 1$. Prouver que a est impair et b est pair.
2. Montrer que si $n \in \mathbb{N}$ n'est pas divisible par 3, alors $2n^2+1$ est divisible par 3.
3. Démontrer que pour tout $n \in \mathbb{N}$, $A = n(n+1)(n+2)$ est divisible par 6.

11.2 Congruences

Exercice 11.6

Montrer que $11^6 \equiv 1 \pmod 7$. En déduire le reste de la division euclidienne de 11^{2018} par 7.

Exercice 11.7

On considère l'équation dans $\mathbb{Z}^2$: $11x^2 - 7y^2 = 5 \quad (E)$.

1. Montrer que si (x, y) est solution de (E), alors $x^2 \equiv 2y^2 \pmod 5$.
2. Quels sont les restes possibles de x^2 et de $2y^2$ modulo 5 ?
3. En déduire que si (x, y) est solution de (E), alors x et y sont multiples de 5.
4. Résoudre l'équation (E).

Exercice 11.8 — Défi — Cube se terminant par 2009

Le but est de montrer qu'il existe $n \in \mathbb{N}$ tel que $n^3 \equiv 2009 \pmod{10000}$.
On considère la suite (u_n) définie par $u_0 = 2009$ et $u_{n+1} = u_n^3$.

1. Déterminer le reste de 2009^2 divisé par 16.
2. En déduire que $2009^{8001} \equiv 2009 \pmod{16}$.
3. Montrer que $\forall n \in \mathbb{N}$: u_n est divisible par 5^{n+1}.
4. Vérifier que $u_3 = 2009^{250} - 1$. En déduire que $2009^{250} \equiv 1 \pmod{625}$.
5. Démontrer que $2009^{8001} \equiv 2009 \pmod{625}$.
6. Montrer que $2009^{8001} \equiv 2009 \pmod{10000}$.
7. Conclure.

11.3 Exercices de synthèse sur les congruences

Exercice 11.9

11.4 Équation diophantienne et congruences On considère l'équation (E) : $11x^2 - 7y^2 = 5$ dans $\mathbb{Z}^2$.

1. Montrer que si (x, y) est solution, alors $x^2 \equiv 2y^2 \pmod 5$.
2. Quels sont les restes possibles de x^2 et $2y^2$ modulo 5 ?
3. Montrer que si (x, y) est solution, alors $5 \mid x$ et $5 \mid y$.
4. Conclure que (E) n'admet pas de solution.

Solution. **1.** $11x^2 - 7y^2 = 5 \Rightarrow x^2 \equiv 2y^2 \pmod 5$.
2. $x^2 \pmod 5 \in \{0, 1, 4\}$. $2y^2 \pmod 5 \in \{0, 2, 3\}$.

3. $x^2 \equiv 2y^2 \pmod 5$ avec $\{0,1,4\} \cap \{0,2,3\} = \{0\}$. Donc $x^2 \equiv 0$ et $2y^2 \equiv 0 \pmod 5$, soit $5 \mid x$ et $5 \mid y$.

4. Posons $x = 5x'$, $y = 5y'$. En substituant : $11 \times 25x'^2 - 7 \times 25y'^2 = 5$, soit $25(11x'^2 - 7y'^2) = 5$, impossible car $5 \nmid 25$. Donc (E) n'a pas de solution.

Exercice 11.10

11.5 Nombres de Fermat On appelle **nombres de Fermat** les entiers $F_n = 2^{2^n} + 1$.

1. Calculer F_0, F_1, F_2, F_3, F_4.

2. Montrer que $F_{n+1} = (F_n - 1)^2 + 1$.

3. Montrer que pour $n \geq 2$, F_n se termine par le chiffre 7.

Solution. **1.** $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$.

2. $(F_n - 1)^2 + 1 = (2^{2^n})^2 + 1 = 2^{2^{n+1}} + 1 = F_{n+1}$. ✓

3. Par récurrence. $F_2 = 17 \equiv 7 \pmod{10}$. Si $F_n \equiv 7 \pmod{10}$, alors $F_n - 1 \equiv 6 \pmod{10}$, donc $(F_n - 1)^2 \equiv 36 \equiv 6 \pmod{10}$, et $F_{n+1} = (F_n - 1)^2 + 1 \equiv 7 \pmod{10}$.

Exercice 11.11

11.6 Répunits carrés parfaits Un **répunit** est un entier dont l'écriture ne comprend que le chiffre 1 (ex : 11, 111, 1111). Trouver tous les répunits qui sont des carrés parfaits.

Solution. Soit n^2 un répunit. Son chiffre des unités est 1, donc $n \equiv 1$ ou $n \equiv 9 \pmod{10}$, i.e. $n = 10k \pm 1$. $n^2 = (10k)^2 \pm 20k + 1 = 100k^2 \pm 20k + 1 \equiv \pm 20k + 1 \equiv 1 \pmod{20}$. Un répunit à m chiffres vaut $R_m = \frac{10^m - 1}{9}$. $R_m \equiv 1 \pmod{20} \Rightarrow 20 \mid R_m - 1 = \frac{10^m - 10}{9}$. On vérifie que $R_1 = 1 = 1^2$ est le seul répunit carré parfait.

Appendice : Formulaire récapitulatif

Résumé des résultats essentiels

Divisibilité : $b \mid a \iff \exists k \in \mathbb{Z}, a = kb$
Division euclidienne : $\forall a \in \mathbb{Z}, b \in \mathbb{Z}^*, \exists!(q,r) : a = bq + r, 0 \leq r < |b|$
Congruence : $a \equiv b \pmod{n} \iff n \mid (a-b)$
Propriétés clés : Si $a \equiv b$ et $c \equiv d \pmod{n}$, alors :

- $a + c \equiv b + d \pmod{n}$
- $ac \equiv bd \pmod{n}$
- $a^m \equiv b^m \pmod{n}$ $(m \in \mathbb{N})$

Algorithme d'Euclide : $a \wedge b =$ dernier reste non nul des divisions successives.
Bézout : $a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2 : au + bv = 1$
Gauss : $a \mid bc$ et $a \wedge b = 1 \Rightarrow a \mid c$
Diophantienne : $ax + by = c$ a des solutions $\iff (a \wedge b) \mid c$.
Fermat : p premier $\Rightarrow a^p \equiv a \pmod{p}$
PGCD par décomposition : $a \wedge b = \prod p_i^{\min(\alpha_i, \beta_i)}$
Nombre de diviseurs : $a = \prod p_i^{\alpha_i} \Rightarrow D(a) = \prod(1 + \alpha_i)$
Inversibilité dans $\mathbb{Z}/n\mathbb{Z}$: $\bar{x}$ inversible $\iff x \wedge n = 1$
$\mathbb{Z}/p\mathbb{Z}$ **est un corps** si p est premier.
Critères de divisibilité (base 10) :

- Par 3 ou 9 : somme des chiffres divisible par 3 ou 9.
- Par 11 : somme alternée des chiffres divisible par 11.

ń Les mathématiques sont la reine des sciences, et la théorie des nombres est la reine des mathématiques. ż
Carl Friedrich Gauss

Arithmétique dans $\mathbb{Z}$

Un cours rigoureux et complet
pour la réussite en $1^{\text{ère}}$ Bac Sciences Mathématiques

Prof. Abed • Année 2025/2026