Chapitre
Arithmétique.

I Division euclidienne

Théorème (Division euclidienne)

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un $\boxed{\text{unique}}$ couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

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

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

Exercice. Soit $a \in \mathbb{Z}$. Montrer que le reste de la division euclidienne de a^2 par 8 est $0, 1$ ou 4.

Définition (La relation de divisibilité)

Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. On dit que b **divise** a ou que a est **multiple** de b, que l'on note $b|a$ s'il existe $k \in \mathbb{Z}$ tel que : $a = kb$.
On note $b\mathbb{Z}$ l'ensemble des multiples de b et $D(b)$ l'ensemble des diviseurs de b.

Remarques (Caractérisation de la divisibilité par le reste nul)

Lorsque $b > 0$, $b|a$ si et seulement si le reste de la division euclidienne de a par b est nul.

✎ Méthode pratique ✎ (Montrer que b divise a)

- On peut cherche à écrire $a = kb$.
- On peut effectuer la division euclidienne de a par b et on montre que le reste est nul.
- On peut effectuer un calcul de congruence (cf. ci-dessous).
- On peut utiliser le théorème de Gauss (cf. plus loin).

Exercice. Montrer que pour tout $n \in \mathbb{N}$, $11|2^{6n+3} + 3^{2n+1}$

Propriétés (de la divisibilité)

Soit $(a, b, c, d, \lambda, \mu) \in \mathbb{Z}^6$.

1) **Relation d'ordre**. La relation $|$ est une relation d'ordre partielle $\boxed{\text{sur } \mathbb{N}}$ mais pas sur $\mathbb{Z}$ (seule l'antisymétrie est mise en défaut).
2) **Pseudo-antisymétrie**. Si $a|b$ et $b|a$ alors $a = \pm b$.
3) **Produit**. Si $a|b$ et $c|d$ alors $ac|bd$.
4) **Produit-Somme**. Si $a|b$ et $a|c$ alors $a|(\lambda b + \mu c)$.

Exercice.

1) Déterminer les entiers $x \in \mathbb{Z}$ tels que $x - 1|x + 4$.
2) Résoudre dans $\mathbb{Z}$ l'équation $xy = x + 3y$.

II Congruences

Définition (Congruence)

Soient $(a,b,n) \in \mathbb{Z}^3$. On dit que "a **est congru à** b **modulo** n", que l'on note $a \equiv b \ [n]$ ou $a = b \ [n]$ s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.
Cas particulier : si r est le reste de la division euclidienne de a par n, alors $a = r \ [n]$.

Théorème (Opérations sur les congruences)

Les variables qui apparaissent appartiennent à $\mathbb{Z}$.

1) La relation de congruence est une relation d'équivalence sur $\mathbb{Z}$.

2) **On peut multiplier, sommer, multiplier par un scalaire les congruences :**
si $\begin{cases} a_1 \equiv b_1 \ [n] \\ a_2 \equiv b_2 \ [n] \end{cases}$ alors $a_1 a_2 \equiv b_1 b_2 \ [n]$ et $\lambda a_1 + \mu a_2 \equiv \lambda b_1 + \mu b_2 \ [n]$.

3) **Conséquences :**
si $a \equiv b \ [n]$ alors si $p \in \mathbb{N}$, $a^p \equiv b^p \ [n]$ et $a + k \equiv b + k \ [n]$

4) **Multiplication par un entier :**
si $a \equiv b \ [n]$ alors $ka \equiv kb \ [n]$ et $ka \equiv kb \ [kn]$

✎ Méthode pratique ✎ (Application congruences)

- On peut utiliser les congruences pour montrer que a divise b, pour cela on montre que $a \equiv 0 \ [b]$.
- Pour déterminer le reste de la division euclidienne de a par b, on effectue un calcul "modulo b" jusqu'à obtenir un résultat compris entre 0 et $b-1$.

Exercice.

1) Soit $a \in \mathbb{Z}$. Montrer que le reste de la division euclidienne de a^2 par 8 est $0, 1$ ou 4.
2) Montrer que pour tout $n \in \mathbb{N}$, $11 | 2^{6n+3} + 3^{2n+1}$
3) Déterminer le reste de la division euclienne de 3^n par 4.

III PGCD-PPCM

III.1 Définitions et premières propriétés

Définition (PPCM-PGCD)

Soit $(a,b) \in (\mathbb{N})^2$ avec a ou b non nul.

- L'ensemble des diviseurs de $\mathbb{N}^*$ communs à a et b (comme ensemble non vide majoré de $\mathbb{N}$) admet un plus grand élément appelé **plus grand commun diviseur** (PGCD) de a et b noté $a \wedge b$.
- L'ensemble des multiples de $\mathbb{N}^*$ communs à a et b (comme ensemble non vide minoré de $\mathbb{N}$) admet un plus petit élément appelé **plus petit commun multiple** (PPCM) de a et b noté ou $a \vee b$.

Remarques

- Le PPCM est utilisé pour déterminer le "meilleur dénominateur commun" lorsque l'on somme de deux fractions
- On peut étendre les notions de PGCD et PPCM à deux entiers relatifs dont l'un au moins est non nul:
$$a \wedge b = |a| \wedge |b| \qquad a \vee b = |a| \vee |b|.$$

✎ Méthode pratique ✎ (Montrer l'égalité de deux PGCD)

Pour montrer que $a \wedge b = \alpha \wedge \beta$, on prouve que LES diviseurs communs de a et b sont LES diviseurs communs de α et β.

Propriétés (du PGCD)

Soient $(a, b, c) \in (\mathbb{Z}^*)^3$, $k \in \mathbb{N}^*$

1) **Commutativité.** $a \wedge b = b \wedge a$ et $a \vee b = b \vee a$.
2) **Associativité.** $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ et $(a \vee b) \vee c = a \vee (b \vee c)$.
   Cela autorise à écrire sans parenthèses : $a \wedge b \wedge c$ et $a \vee b \vee c$
3) **Factorisation par un diviseur commun.** $(ak) \wedge (bk) = k(a \wedge b)$.

Remarques

On peut définir le PPCM et le PGCD de n entiers : $x_1 \wedge \cdots \wedge x_n$ et $x_1 \vee \cdots \vee x_n$.

Propriétés (Une formule)

Soit $(a, b) \in \mathbb{N}^2$ avec a ou b non nul. Alors: $(a \wedge b) \times (a \vee b) = ab$.

Exercice. Résoudre dans $\mathbb{N}^2$ le système $\begin{cases} x \wedge y = 5 \\ x \vee y = 60 \end{cases}$

III.2 Algorithme d'Euclide

Théorème (Propriété d'Euclide)

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.
Si $a = bq + r$ est la division euclidienne de a par b alors : $a \wedge b = b \wedge r$.

✎ Méthode pratique ✎ (Algorithme d'Euclide : calcul du PGCD)

On souhaite déterminer le PGCD de deux entiers $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$.
L'algorithme repose sur la propriété d'Euclide, il consiste à définir les entiers naturel r_0, r_1,... de la manière suivante:

- au départ $r_0 = a$ et $r_1 = b$
- ensuite si $r_1 \neq 0$, on définit r_2 le reste de la division euclidienne de r_0 par r_1 $(0 \leqslant r_2 < r_1)$
- ...
- on répète le procédé, tant que $r_{k+1} \neq 0$, on note r_{k+2} le reste de la division euclidienne de r_k par r_{k+1} $(0 \leqslant r_{k+2} < r_{k+1})$

La suite (r_k) est strictement décroissante, d'entiers naturels, donc il existe $N \in \mathbb{N}^*$ tel que $r_{N+1} = 0$ et $r_N \neq 0$.
D'après le principe d'Euclide :

$$a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 = \cdots = r_N \wedge r_{N+1} = r_N \wedge 0 = r_N.$$

Autrement dit, $\boxed{a \wedge b \text{ est le dernier reste non nul dans la liste des restes successifs}}$.

Exercice. Déterminer le PGCD de 420 et 108.

Corollaire (Caractérisation des diviseurs et multiples communs à a et b)

Soient $(a,b)\mathbb{Z}^2$.

1) $\boxed{d \text{ est un diviseur commun à } a \text{ et } b \text{ si et seulement si } d \text{ divise } a \wedge b.}$
Autrement dit : sur $\mathbb{N}$, $a \wedge b$ est le plus grand des diviseurs communs à a et b pour la relation d'ordre $|$.

2) $\boxed{m \text{ est un multiple commun à } a \text{ et } b \text{ si et seulement si } m \text{ est multiple de } a \vee b.}$
Autrement dit : sur $\mathbb{N}$, $a \vee b$ est le plus petit des multiples communs à a et b pour la relation d'ordre $|$.

Corollaire (Caractérisation du PGCD)

Soient $(a,b) \in \mathbb{Z}^2$ avec a et b non nuls.

Posons $(a',b',\delta) \in \mathbb{Z}^2$ tels que $\begin{cases} a = a'\delta \\ b = b'\delta \end{cases}$. Alors : $\delta = a \wedge b \Leftrightarrow a' \wedge b' = 1.$

✎ Méthode pratique ✎ (Comment déterminer un PGCD)

- On peut utiliser l'algorithme d'Euclide.
- On peut utiliser la caractérisation précédente. C'est-à-dire que l'on montre qu'il existe deux entiers a', b' tels que $a' \wedge b' = 1$ et $\begin{cases} a = a'\delta \\ b = b'\delta \end{cases}$.
- On peut raisonner par analyse-synthèse. Soit d un diviseur commun à a et b, alors... Puis on utilise les opérations (produit-somme).

Exercice.

1) Soit $(a,b,c) \in (\mathbb{N}^*)^3$. Montrer que: $(ca) \wedge (cb) = c(a \wedge b)$ et $(ca) \vee (cb) = c(a \vee b)$

2) Soit $(a,b,c) \in (\mathbb{N}^*)^3$. Montrer que si $a \wedge b \wedge c = 1$ alors $a \wedge b \wedge c = 1$.

III.3 Relation de Bezout

Théorème (Relation de Bezout)

1) Soient a et b deux entiers relatifs non nuls.
Alors il existe $(u,v) \in \mathbb{Z}^2$ tel que: $au + bv = a \wedge b.$
On dit que (u,v) est **un couple de Bezout** associé à a et b.

2) **Généralisation**. Soient $a_1, \ldots, a_n$, des entiers relatifs non nuls.
Alors, il existe $(u_1,\ldots,u_n) \in \mathbb{Z}^n$ tel que: $a_1u_1 + \cdots + a_nu_n = a_1 \wedge \cdots \wedge a_n.$

Exercice. Déterminer un couple de Bezout lorsque $(a,b) = (2,3)$, $(a,b) = (5,9)$, $(a,b) = (6,8)$.

Remarques (Algorithme d'Euclide étendu : trouver un couple de Bezout)

Soient $(a, b) \in (\mathbb{Z}^*)^2$.

1) On applique l'algorithme d'Euclide à a et b on construit alors une suite de restes (r_n) et une suite de quotients (q_n) qui vérifient donc :

$$r_n = q_{n+1}r_{n+1} + r_{n+2} \qquad r_0 = a \qquad r_1 = b \qquad\qquad 0 < r_{n+1} < r_n.$$

   Le PGCD de a et b est le dernier reste non nul noté r_N.

2) On détermine des suites (u_n) et (v_n) telles que $r_n = u_n a + v_n b$ pour $0 \leqslant n \leqslant N$.

   Les suites (u_n) et (v_n) définies par $\begin{cases}(u_0, v_0) = (1, 0)\\(u_1, v_1) = (0, 1)\end{cases}$ et $\begin{cases}u_{n+2} = u_n - q_{n+1}u_{n+1}\\v_{n+2} = v_n - q_{n+1}v_{n+1}\end{cases}$ conviennent (ce que l'on prouve par récurrence).

3) On déduit alors: $a \wedge b = r_N = u_N a + v_N b$ et donc (u_N, v_N) est un couple de Bezout de a et b.

4) On peut présente les calculs dans un tableau :

	$r_0 = a$	$r_1 = b$	r_2	$\ldots$	r_n	$\ldots$	$a \wedge b$
q_k		q_1	q_2	$\ldots$	q_n	$\ldots$	
u_k	1	0	u_2	$\ldots$	u_n	$\ldots$	u_N
v_k	0	1	v_2	$\ldots$	v_n	$\ldots$	v_N

Exercice.

1) Déterminer un couple de Bezout pour 420 et 108.

2) Déterminer un couple de Bezout pour 17 et 12.

IV Entiers premiers entre eux

Définition (Nombres premiers entre eux)

Soit $(a, b) \in (\mathbb{Z}^*)^2$.
On dit que a et b sont **premiers entre eux** si $a \wedge b = 1$.
Autrement dit, a et b sont premiers entre eux si a et b n'ont pas d'autres diviseurs communs que 1 et -1.

Exercice.

1) Démontrer que deux entiers naturels consécutifs sont premiers entre eux.

2) Montrer que la fraction $\dfrac{21n + 4}{14n + 3}$ est irreductible pour tout $n \in \mathbb{N}$.

Théorème (Théorème de Bezout)

Soit $(a, b) \in (\mathbb{Z}^*)^2$. Alors :

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

✎ Méthode pratique ✎ (Comment prouver que deux entiers sont premiers entre eux)

- On peut montrer que le PCGD vaut 1, par exemple avec l'algorithme d'Euclide.
- On peut montrer qu'un diviseur commun divise nécessairement 1.
- On peut utiliser le théorème de Bezout.

Exercice. Soit $(a, b, c) \in (\mathbb{Z}^*)^3$.

1) Montrer que si a et b sont premiers entre eux, alors les diviseurs de a sont premiers avec b.

2) On suppose $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases}$. Montrer que $a \wedge bc = 1$.
En déduire que pour tout $(p, q) \in (\mathbb{N}^*)^2$, $a^p \wedge b^q = 1$.

Théorème (Théorème de Gauss)

Soit $(a, b, c) \in (\mathbb{Z}^*)^3$.

Si $\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases}$ alors $a \mid c$.

Exercice.

1) Déterminer le plus petit entier naturel $N \geqslant 3$ vérifiant $\begin{cases} N \equiv 2 \ [7] \\ N \equiv 2 \ [3] \end{cases}$.

2) **Equation diophantienne**. Résoudre dans Z les équations :

$$(E_1)\ \ 12x + 8y = 7 \qquad (E_2)\ \ 13x + 5y = 4 \qquad (E_3)\ \ 24x + 20y = 36.$$

Corollaire (Produit d'entiers)

Soit $(a, b, c) \in (\mathbb{Z}^*)^3$.

- Si $\begin{cases} a \mid c \text{ et } b \mid c \\ a \wedge b = 1 \end{cases}$ alors $ab \mid c$.

⚠ **Attention** ⚠ En général : $a \mid c$ et $b \mid c \not\Rightarrow ab|c$.

- Si $\begin{cases} a \wedge c = 1 \\ b \wedge c = 1 \end{cases}$ alors $(ab) \wedge c = 1$.

Définition (n nombres premiers entre eux)

Soient $(a_1, \ldots, a_n) \in (\mathbb{N}^*)^n$.

1) On dit que $a_1, \ldots, a_n$ sont **premiers entre eux dans leur ensemble** si $a_1 \wedge \cdots a_n = 1$.
2) On dit que $a_1, \ldots, a_n$ sont **premiers entre eux 2 à 2** si pour tout $(i, j) \in [\![1, n]\!]^2$, $a_i \wedge a_j = 1$.

Exemples Les entiers $2, 5, 8$ sont premiers entre eux dans leur ensemble. Mais ne sont pas premiers entre eux 2 à 2. Les entiers $2, 5, 7$ sont premiers entre eux dans leur ensemble et 2 à 2.

Remarques (Lien entre ces deux notions?)

"premiers entre eux dans leur ensemble" "premiers entre eux 2 à 2".

V Nombres premiers

V.1 Définitions

Définition (Nombre premier)

Un entier $p \in \mathbb{N}$ est **premier** si $p \geqslant 2$ et si ses seuls diviseurs positifs sont 1 et lui-même.

Exercice. Soit $p > 3$ un nombre premier. Montrer que $24|p^2 - 1$.

✎ **Méthode pratique** ✎ **(Montrer qu'un entier n'est pas premier)**

Pour montrer que n n'est pas premier, on peut montrer que n est **composé** c'est-à-dire qu'il s'écrit $n = ab$ avec a et b deux entiers tels que $a \geqslant 2$ et $b \geqslant 2$.

Exercice. Montrer que pour tout $n \in \mathbb{N}$, $n^4 - n^2 + 16$ n'est pas premier.

V.2 Propriétés

Propriétés (Lien avec "premiers entre eux")

1) Soit $p \in \mathbb{N}$ et $n \in \mathbb{Z}$.
   Si p est premier alors : **soit** $p \,|\, n$, **soit** $p \wedge n = 1$.

2) Deux nombres premiers distincts sont premiers entre eux.

3) Si un nombre premier divise un produit d'entiers alors il divise l'un d'entre eux.
   Conséquence, si p premier divise m^k alors p divise m.

Exercice. Montrer que la racine carrée d'un nombre premier est irrationnel.

Théorème (Le petit théorème de Fermat)

Soit p un nombre premier et $n \in \mathbb{Z}$. Alors

- $n^p \equiv n \ [p]$
- si p ne divise pas n alors $n^{p-1} - 1 \equiv 0 \ [p]$.

Théorème

Tout entier naturel $n \geqslant 2$ admet un diviseur premier

Théorème (Infinité des nombres premiers)

Il existe une infinité de nombres premiers.

V.3 Décomposition d'un entier en produit de facteurs premiers

Théorème (fondamental de l'arithmétique)

Tout entier $n \in \mathbb{N}^*$ se décompose de manière unique comme produit de facteurs premiers

$$n = \prod_{p \in \mathcal{P}} p^{\alpha_p}$$

où

- $\mathcal{P}$ est l'ensemble des nombres premiers
- les α_p sont des entiers naturels tous nuls sauf un nombre fini
- α_p que l'on note aussi $\nu_p(n)$ est appelée la valuation p-adique de n.

Exercice.

1) Prouver que $\log(2)$ est irrationnel.

2) Calculer $\nu_2(100!)$.

3) Montrer que 3528 est divisible par 252

Théorème (Caractérisation de la divisivilité)

Soit $(a, b) \in (\mathbb{N}^*)^2$ donné par les décompositions :

$$a = \prod_{p \in \mathcal{P}} p^{\nu_p(a)} \qquad\qquad b = \prod_{p \in \mathcal{P}} p^{\nu_p(b)}.$$

On a alors :

$$a \,|\, b \Leftrightarrow \forall p \in \mathcal{P},\ \ \nu_p(a) \leqslant \nu_p(b).$$

Exercice. Déterminer l'ensemble des diviseurs de 2020.

Corollaire (Expression du PGCD-PPCM)

Soit $(a, b) \in (\mathbb{N}^*)^2$ donné par les décompositions :

$$a = \prod_{p \in \mathcal{P}} p^{\nu_p(a)} \qquad\qquad b = \prod_{p \in \mathcal{P}} p^{\nu_p(b)}.$$

On a alors :

$$a \wedge b = \prod_{p \in \mathcal{P}} p^{\min(\nu_p(a), \nu_p(b))} \qquad\qquad a \vee b = \prod_{p \in \mathcal{P}} p^{\max(\nu_p(a), \nu_p(b))}$$

Exercice.

1) Déterminer le PGCD et le PPCM des entiers 2520 et 8316.

2) Soient a, b, c deux entiers relatifs non nuls.

   -a- Montrer que si $b^2 | a^2$ alors $b|a$.

   -b- Montrer que si $a \wedge b = 1$ alors $a^p \wedge b^p = 1$.

   -c- Montrer que $(ca) \wedge (cb) = c(a \wedge b)$ et $(ca) \vee (cb) = c(a \vee b)$.