Fiche de révision : Arithmétique

Mohamed Kadhem Karray
https://mohamedkadhem.com/baccalaureat/

Les numéros des énoncés (*Définition 16.1*, *Théorème 16.1*, etc.) renvoient aux énoncés numérotés du cours 16 [1], sur l'arithmétique. Le numéro entre crochets renvoie à la bibliographie en fin de document. Ce cours est disponible sur la page `mohamedkadhem.com/baccalaureat`.

Les lettres a, b, c, d, k, m, n, q, r, u, v, x, y désignent des entiers relatifs, sauf mention contraire, et p désigne un nombre premier.

1 Divisibilité

- **Définition 16.1 et Exemple 16.1 (divisibilité) :** a *divise* b, noté $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$; a est un *diviseur* de b, et b un *multiple* de a. Tout entier divise 0, et 0 ne divise que 0 ; 1 et -1 divisent tout entier ; $a \mid b$ équivaut à $-a \mid b$ et à $a \mid -b$.
- **Théorème 16.1 (règles de calcul) :** (i) si $a \mid b$, alors $a \mid mb$ pour tout $m \in \mathbb{Z}$; (ii) si $a \mid b$ et $b \mid c$, alors $a \mid c$ (*transitivité*) ; (iii) si $a \mid b$ et $a \mid c$, alors $a \mid mb + nc$ pour tous $m, n \in \mathbb{Z}$ (*divisibilité d'une combinaison linéaire*) ; (iv) si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$; (v) si $a \mid b$ et $b \mid a$, alors $a = b$ ou $a = -b$.

2 Division euclidienne

- **Propriété 16.1 (bon ordre, admise) :** toute partie non vide de $\mathbb{N}$ a un plus petit élément. Elle sert à montrer qu'un objet existe, ou qu'un procédé s'arrête (Remarque 16.1).
- **Théorème 16.2 et Définition 16.2 (division euclidienne) :** soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que

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

  L'entier q est le *quotient* et r le *reste* de la division euclidienne de a par b. Le diviseur b de la division n'est pas en général un diviseur de a (Remarque 16.2).
- **Théorème 16.3 (reste et divisibilité) :** pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, (i) $b \mid a$ si et seulement si le reste de la division euclidienne de a par b est nul ; (ii)

tout entier a s'écrit sous l'une des formes bq, $bq+1$, …, $bq+(b-1)$, avec $q \in \mathbb{Z}$.

- **Exemple 16.2 (dividende négatif) :** $-17 = 5 \times (-4) + 3$ et $0 \leq 3 < 5$: le quotient de -17 par 5 est -4 et le reste est 3, et non -2.

3 Congruences

- **Définition 16.3 (congruence) :** soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n, et l'on note $a \equiv b\,[n]$, si $n \mid a - b$.
- **Théorème 16.4 (congruence et reste) :** soit $n \in \mathbb{N}^*$. (i) $a \equiv b\,[n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n. (ii) Le reste de la division euclidienne de a par n est l'unique entier $r \in \{0, 1, \ldots, n-1\}$ tel que $a \equiv r\,[n]$. (iii) $a \equiv a\,[n]$; si $a \equiv b\,[n]$, alors $b \equiv a\,[n]$; si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $a \equiv c\,[n]$.
- **Théorème 16.5 (opérations) :** si $n \in \mathbb{N}^*$, $a \equiv b\,[n]$ et $c \equiv d\,[n]$, alors (i) $a + c \equiv b + d\,[n]$; (ii) $ac \equiv bd\,[n]$; (iii) $a^k \equiv b^k\,[n]$ pour tout $k \in \mathbb{N}$.
- **Remarque 16.3 (pas de division) :** on ne peut pas simplifier une congruence : $2 \times 3 \equiv 2 \times 0\,[6]$, mais $3 \not\equiv 0\,[6]$. Le Corollaire 16.3 dit quand c'est permis.
- **Exemple 16.3 (reste d'une puissance) :** $2^3 \equiv 1\,[7]$ et $100 = 3 \times 33 + 1$, donc $2^{100} = \left(2^3\right)^{33} \times 2 \equiv 2\,[7]$ (Théorème 16.5 (iii) et (ii)) ; comme $0 \leq 2 < 7$, le reste de 2^{100} par 7 est 2 (Théorème 16.4 (ii)).

4 PGCD et algorithme d'Euclide

- **Définition 16.4 et Remarque 16.4 (PGCD) :** pour $a, b \in \mathbb{Z}$ *non tous deux nuls*, $\mathrm{PGCD}\,(a, b)$ est le plus grand des entiers qui divisent à la fois a et b ; il existe et vaut au moins 1. (i) $\mathrm{PGCD}\,(a, b) = \mathrm{PGCD}\,(b, a) = \mathrm{PGCD}\,(|a|, |b|)$; (ii) $\mathrm{PGCD}\,(a, 0) = |a|$ si $a \neq 0$, et plus généralement $\mathrm{PGCD}\,(a, b) = |a|$ si $a \neq 0$ et $a \mid b$.
- **Théorème 16.6 et Remarque 16.5 (divisions successives) :** si $a = bq + r$, les diviseurs communs de a et b sont ceux de b et r ; si de plus $b \neq 0$, $\mathrm{PGCD}\,(a, b) = \mathrm{PGCD}\,(b, r)$. On peut donc remplacer a par son reste dans la division euclidienne par $b \in \mathbb{N}^*$.
- **Théorème 16.7 (algorithme d'Euclide) :** soient $a, b \in \mathbb{N}^*$, $r_0 = a$, $r_1 = b$ et, tant que $r_k \neq 0$, r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k. (i) L'algorithme s'arrête : il existe $N \geq 1$ tel que $r_N \neq 0$ et $r_{N+1} = 0$. (ii) Les diviseurs communs de a et b sont exactement les diviseurs de r_N. (iii) $\mathrm{PGCD}\,(a, b) = r_N$, le dernier reste non nul ; si $b \mid a$, c'est b (Exemple 16.5).

- **Exemple 16.5 (PGCD de 252 et 198) :** $252 = 198 \times 1 + 54$, $198 = 54 \times 3 + 36$, $54 = 36 \times 1 + 18$, $36 = 18 \times 2 + 0$, donc $\mathrm{PGCD}\,(252, 198) = 18$.
- **Corollaire 16.1 (diviseurs du PGCD) :** pour $a, b \in \mathbb{Z}$ non tous deux nuls, d divise a et b si et seulement si d divise $\mathrm{PGCD}\,(a, b)$.
- **Théorème 16.8 (PGCD et produit) :** pour $a, b \in \mathbb{Z}$ non tous deux nuls et $k \in \mathbb{N}^*$, $\mathrm{PGCD}\,(ka, kb) = k\,\mathrm{PGCD}\,(a, b)$.
- **Définition 16.5 et Corollaire 16.2 (premiers entre eux) :** a et b, non tous deux nuls, sont *premiers entre eux* si $\mathrm{PGCD}\,(a, b) = 1$. Si $d = \mathrm{PGCD}\,(a, b)$, alors $a = da'$ et $b = db'$, où a' et b' sont premiers entre eux ; par exemple $252 = 18 \times 14$ et $198 = 18 \times 11$ (Exemple 16.6).

5 Bézout et Gauss

- **Théorème 16.9 et Remarque 16.6 (identité de Bézout) :** soient $a, b \in \mathbb{Z}$, non tous deux nuls, et $d = \mathrm{PGCD}\,(a, b)$. Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = d$. Le couple (u, v) n'est pas unique : $(u + b, v - a)$ convient aussi.
- **Exemple 16.7 (remonter l'algorithme) :** avec les divisions de l'Exemple 16.5, $18 = 54 - 36 = 4 \times 54 - 198 = 4 \times 252 - 5 \times 198$. On vérifie : $1008 - 990 = 18$.
- **Théorème 16.10 (théorème de Bézout) :** a et b, non tous deux nuls, sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.
- **Corollaire 16.3 (inverse modulo n) :** soient $n \geq 2$ et $a \in \mathbb{Z}$. Il existe $u \in \mathbb{Z}$ tel que $au \equiv 1\,[n]$ si et seulement si a et n sont premiers entre eux ; un tel u est un *inverse* de a modulo n. On peut alors simplifier par a : si $ax \equiv ay\,[n]$, alors $x \equiv y\,[n]$.
- **Théorème 16.11 (théorème de Gauss) :** soient $a, b, c \in \mathbb{Z}$, avec a et b *premiers entre eux*. Si $a \mid bc$, alors $a \mid c$.
- **Corollaire 16.4 et Remarque 16.7 (produit de deux diviseurs) :** si a et b sont premiers entre eux, $a \mid c$ et $b \mid c$, alors $ab \mid c$. L'hypothèse est utile : $6 \mid 12$ et $4 \mid 12$, mais $24 \nmid 12$.

6 Équation $ax + by = c$

- **Théorème 16.12 (équation $ax + by = c$) :** soient $a, b \in \mathbb{Z}$ *non nuls*, $c \in \mathbb{Z}$, $d = \mathrm{PGCD}\,(a, b)$, $a = da'$ et $b = db'$. (i) L'équation $ax + by = c$ a des solutions $(x, y) \in \mathbb{Z}^2$ si et seulement si $d \mid c$. (ii) Si (x_0, y_0) est une solution, les solutions sont les couples $(x_0 + kb',\ y_0 - ka')$, $k \in \mathbb{Z}$.
- **Exemple 16.8 (méthode, $252x + 198y = 36$) :** *Étape 1 (existence)* : $\mathrm{PGCD}\,(252, 198) = 18$ et $18 \mid 36$. *Étape 2 (solution particulière)* : on

multiplie par 2 l'égalité de Bézout de l'Exemple 16.7, d'où $(x_0, y_0) = (8, -10)$. *Étape 3 (toutes les solutions)* : avec $a' = 14$ et $b' = 11$, les solutions sont les couples $(8 + 11k,\ -10 - 14k)$, $k \in \mathbb{Z}$. *Vérification* : pour $k = -1$, $252 \times (-3) + 198 \times 4 = 36$.

7 Nombres premiers

- **Définition 16.6 et Exemple 16.9 (nombre premier) :** un entier naturel n est *premier* s'il a *exactement deux diviseurs positifs*, 1 et n ; un entier $n \geq 2$ qui n'est pas premier est *composé*. Ni 0 ni 1 ne sont premiers.
- **Théorème 16.13 et Remarque 16.8 (plus petit diviseur, test) :** soient $n \geq 2$ et s le plus petit diviseur de n tel que $s \geq 2$. (i) s est premier : tout entier $n \geq 2$ a un diviseur premier. (ii) Si n est composé, $s^2 \leq n$. Donc $n \geq 2$ est premier si et seulement si aucun nombre premier p tel que $p^2 \leq n$ ne divise n ; ainsi 97 est premier, car il n'est divisible ni par 2, ni par 3, ni par 5, ni par 7, et $11^2 > 97$.
- **Théorème 16.14 (infinité) :** il y a une infinité de nombres premiers.
- **Théorème 16.15 (nombre premier et produit) :** soit p premier. (i) Pour tout $a \in \mathbb{Z}$, ou bien $p \mid a$, ou bien a et p sont premiers entre eux. (ii) Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$. (iii) Si p divise un produit $a_1 a_2 \cdots a_k$ de $k \geq 1$ entiers, p divise l'un des a_i.
- **Théorème 16.16 et Remarque 16.9 (décomposition en facteurs premiers) :** tout entier $n \geq 2$ s'écrit

  $$n = p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j},$$

  où $p_1 < p_2 < \cdots < p_j$ sont des nombres premiers et $k_1, \ldots, k_j \in \mathbb{N}^*$; cette écriture est unique (l'unicité est admise). En pratique, on divise n par son plus petit diviseur premier, puis le quotient par le sien, et ainsi de suite : $252 = 2^2 \times 3^2 \times 7$.
- **Théorème 16.17 et Exemple 16.10 (diviseurs d'un entier) :** si $n = p_1^{k_1} \cdots p_j^{k_j}$ est la décomposition de $n \geq 2$, les diviseurs positifs de n sont les entiers $p_1^{e_1} \cdots p_j^{e_j}$ avec $0 \leq e_i \leq k_i$ pour tout i ; il y en a $(k_1 + 1) \cdots (k_j + 1)$, soit 18 pour 252. Pour $m \geq 2$, $\mathrm{PGCD}\,(n, m)$ est le produit des nombres premiers communs aux deux décompositions, chacun avec le plus petit de ses deux exposants : $198 = 2 \times 3^2 \times 11$, donc $\mathrm{PGCD}\,(252, 198) = 2 \times 3^2 = 18$.
- **Théorème 16.18 (petit théorème de Fermat) :** soient p un nombre premier et $a \in \mathbb{Z}$. (i) Si $p \nmid a$, alors $a^{p-1} \equiv 1\,[p]$. (ii) Pour tout $a \in \mathbb{Z}$, $a^p \equiv a\,[p]$.
- **Exemple 16.11 (reste de 5^{2026} par 7) :** 7 est premier et $7 \nmid 5$, donc $5^6 \equiv 1\,[7]$; $2026 = 6 \times 337 + 4$, donc $5^{2026} \equiv 5^4\,[7]$; $5^2 \equiv 4\,[7]$, donc $5^4 \equiv 16 \equiv 2\,[7]$: le reste est 2.

8 PPCM

- **Définition 16.7 (PPCM) :** pour $a, b \in \mathbb{Z}$ *non nuls*, $\text{PPCM}(a, b)$ est le plus petit entier strictement positif multiple de a et de b.
- **Théorème 16.19 et Exemple 16.12 (PGCD et PPCM) :** soient $a, b \in \mathbb{Z}$ non nuls, $d = \text{PGCD}(a, b)$ et $m = \text{PPCM}(a, b)$. (i) Les multiples communs de a et b sont exactement les multiples de m. (ii) $dm = |ab|$. Par exemple, $\text{PPCM}(252, 198) = \frac{252 \times 198}{18} = 2772$.

Références

[1] Mohamed Kadhem Karray. Cours 16. Arithmétique, niveau baccalauréat. https://mohamedkadhem.com/baccalaureat/.