Cours 16

Arithmétique

Mathématiques, niveau baccalauréat

Mohamed Kadhem Karray

mohamedkadhem.com/baccalaureat

14 novembre 2026

Plan

Introduction

16.1 Divisibilité

16.2 Division Euclidienne

16.3 Congruences

16.4 PGCD

16.5 Bézout et Gauss

16.6 Équation $ax + by = c$

16.7 Nombres Premiers

16.8 PPCM

À retenir

Introduction

L'arithmétique étudie les entiers : qui divise qui, ce qui reste après une division, les diviseurs communs, les nombres premiers. Tout repose sur une seule propriété de $\mathbb{N}$.

Où se place cette leçon

- **Prérequis :** le raisonnement par récurrence (cours 1 [1]) ; le raisonnement par l'absurde et les quantificateurs (cours 19 [2]) ; le calcul dans $\mathbb{Z}$ (collège).
- **Les objets :** la divisibilité, la division euclidienne, les congruences, le PGCD et le PPCM, les entiers premiers entre eux, les nombres premiers.
- **Ce qu'on saura faire :** calculer un quotient et un reste, un reste de puissance ; calculer un PGCD par l'algorithme d'Euclide et en tirer une égalité de Bézout ; résoudre une équation $ax + by = c$ en entiers ; décomposer un entier en facteurs premiers ; utiliser le petit théorème de Fermat.

Dans toute la leçon, 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 (Définition 16.6). La valeur absolue de a est notée $|a|$.

16.1 Divisibilité

Un entier en divise un autre si le second est un multiple du premier. Les règles de calcul qui suivent servent dans toute la leçon.

Définition 16.1 (Divisibilité). Soient $a, b \in \mathbb{Z}$. On dit que a *divise* b, et l'on note $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. On dit aussi que a est un *diviseur* de b, et que b est un *multiple* de a. On note $a \nmid b$ si a ne divise pas b.

Exemple 16.1 (Premiers Cas).

(i) $5 \mid 15$ car $15 = 3 \times 5$; 14 est un multiple de 7 ; $-3 \mid 12$ car $12 = (-4) \times (-3)$.

(ii) Tout entier a divise 0, car $0 = 0 \times a$. En revanche, 0 ne divise que 0, car $ka = 0$ pour $a = 0$.

(iii) 1 et -1 divisent tout entier b, car $b = b \times 1 = (-b) \times (-1)$.

(iv) $a \mid b$ équivaut à $-a \mid b$ et à $a \mid -b$: il suffit de changer k en $-k$. Si $b \neq 0$, les diviseurs de b sont donc les diviseurs positifs de $|b|$ et leurs opposés.

Théorème 16.1 (Propriétés de la Divisibilité). Soient $a, b, c \in \mathbb{Z}$.

(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 $a = -b$.

Preuve. (i) Si $b = ka$, alors $mb = (mk)\,a$. (ii) Si $b = ka$ et $c = lb$, alors $c = (lk)\,a$. (iii) Si $b = ka$ et $c = k'a$, alors $mb + nc = (mk + nk')\,a$. (iv) Si $b = ka$ et $b \neq 0$, alors $k \neq 0$, donc $|k| \geq 1$ et $|b| = |k|\,|a| \geq |a|$. (v) Si $b = 0$, alors $a = 0$, car $b \mid a$ (Exemple 16.1 (ii)) ; de même, si $a = 0$, alors $b = 0$. Sinon, (iv) donne $|a| \leq |b|$ et $|b| \leq |a|$, donc $|a| = |b|$.

16.2 Division Euclidienne

On divise un entier par un entier strictement positif : il reste un entier plus petit que le diviseur. L'existence de ce reste vient du bon ordre de $\mathbb{N}$.

Le Bon Ordre de $\mathbb{N}$

Propriété 16.1 (Bon Ordre). Toute partie non vide de $\mathbb{N}$ a un plus petit élément. Cette propriété est admise.

Remarque 16.1 (Bon Ordre et Récurrence). La Propriété 16.1 et le principe de récurrence (Théorème 1.13 du cours 1 [1]) se démontrent l'un à partir de l'autre : ce sont deux façons d'exprimer la même propriété de $\mathbb{N}$. La Propriété 16.1 sert à montrer qu'un objet existe (le plus petit élément d'un ensemble), ou qu'un procédé s'arrête : une suite strictement décroissante d'entiers naturels ne peut pas être infinie, car l'ensemble de ses termes aurait un plus petit élément, suivi d'un terme encore plus petit.

Le Théorème de la Division Euclidienne

Théorème 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

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

Définition 16.2 (Quotient et Reste). Dans le Théorème 16.2, q est le *quotient* et r le *reste* de la *division euclidienne* de a par b ; a est le *dividende*.

Remarque 16.2 (Vocabulaire). On appelle parfois b le diviseur de la division ; ce n'est pas en général un diviseur de a au sens de la Définition 16.1 : 5 ne divise pas 17.

Preuve du Théorème 16.2

Existence, si $a \geq 0$. L'ensemble R des entiers $a - bk \geq 0$, où $k \in \mathbb{Z}$, est une partie de $\mathbb{N}$; il contient a ($k = 0$). Il a donc un plus petit élément $r = a - bq$ (Propriété 16.1). Si l'on avait $r \geq b$, alors $r - b = a - b(q + 1)$ serait un élément de R plus petit que r : c'est impossible. Donc $0 \leq r < b$.

Existence, si $a < 0$. On écrit $-a = bq_0 + r_0$ avec $0 \leq r_0 < b$, par le cas précédent. Si $r_0 = 0$, alors $a = b(-q_0) + 0$. Si $r_0 \neq 0$, alors

$$a = -bq_0 - r_0 = b(-q_0 - 1) + (b - r_0), \quad \text{où } 0 < b - r_0 < b.$$

Unicité. Si $a = bq + r = bq' + r'$ avec $0 \leq r < b$ et $0 \leq r' < b$, alors $b(q - q') = r' - r$, donc $b \mid r' - r$, avec $|r' - r| < b$. Si l'on avait $r' \neq r$, le Théorème 16.1 (iv) donnerait $b \leq |r' - r|$. Donc $r' = r$, puis $q = q'$ car $b \neq 0$.

Conséquences

Théorème 16.3 (Reste et Divisibilité). Soient $a \in \mathbb{Z}$ 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 $q \in \mathbb{Z}$.

Preuve. (i) Si $r = 0$, alors $a = bq$. Réciproquement, si $a = bk$, alors $a = bk + 0$ avec $0 \leq 0 < b$, et l'unicité (Théorème 16.2) donne $r = 0$. (ii) Le reste r est l'un des entiers $0, 1, \ldots, b-1$.

Exemple 16.2 (Divisions Euclidiennes).

(i) $17 = 5 \times 3 + 2$ et $0 \leq 2 < 5$: le quotient de 17 par 5 est 3 et le reste est 2.

(ii) $-17 = 5 \times (-4) + 3$ et $0 \leq 3 < 5$: le quotient de -17 par 5 est -4 et le reste est 3 (et non -2).

(iii) Pour $b = 2$, tout entier s'écrit $2q$ (il est pair) ou $2q+1$ (il est impair) ; pour $b = 3$, il s'écrit $3q$, $3q+1$ ou $3q+2$.

16.3 Congruences

Deux entiers sont congrus modulo n s'ils ont le même reste dans la division par n. On calcule avec les congruences comme avec des égalités, sauf pour diviser.

Définition

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 $n \mid a - b$. Par exemple, $17 \equiv 2\,[5]$ et $23 \equiv 3\,[4]$; un entier pair $2k$ est congru à 0 modulo 2, un entier impair $2k + 1$ est congru à 1 modulo 2.

Théorème 16.4 (Congruence et Reste). Soient $n \in \mathbb{N}^*$ et $a, b, c \in \mathbb{Z}$.

(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 r 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 $a \equiv c\,[n]$.

Preuve. (i) Écrivons $a = nq + r$ et $b = nq' + r'$ (Théorème 16.2). Alors $a - b = n(q - q') + (r - r')$, avec $|r - r'| < n$. Si $r = r'$, alors $n \mid a - b$. Si $n \mid a - b$, alors $n \mid r - r'$ (Théorème 16.1 (iii)), donc $r = r'$, car sinon le Théorème 16.1 (iv) donnerait $n \leq |r - r'|$. (ii) Pour $r \in \{0, \ldots, n-1\}$, le reste de r est r ; on applique (i). (iii) $n \mid 0$; $n \mid a - b$ donne $n \mid b - a$; $n \mid a - b$ et $n \mid b - c$ donnent $n \mid a - c$ (Théorème 16.1 (iii)).

Théorème 16.5 (Congruences et Opérations). Soient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$, avec $a \equiv b\,[n]$ 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 $k \in \mathbb{N}$.

Preuve. (i) $(a + c) - (b + d) = (a - b) + (c - d)$. (ii) $ac - bd = (a - b)\,c + b\,(c - d)$. Dans les deux cas, on conclut par le Théorème 16.1 (iii). (iii) Par récurrence sur k (Théorème 1.13 du cours 1 [1]) : $a^0 = b^0 = 1$, et si $a^k \equiv b^k\,[n]$, alors $a^{k+1} \equiv b^{k+1}\,[n]$ par (ii).

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 dira quand c'est permis.

Exemple : Reste d'une Puissance

Exemple 16.3 (Reste de 2^{100} par 7). Étape 1. On cherche une puissance de 2 congrue à 1 : $2^3 = 8 = 7 + 1$, donc $2^3 \equiv 1\,[7]$.

Étape 2. On divise l'exposant par 3 : $100 = 3 \times 33 + 1$, donc $2^{100} = \left(2^3\right)^{33} \times 2$.

Étape 3. Par le Théorème 16.5 (iii) puis (ii), $\left(2^3\right)^{33} \equiv 1^{33} = 1\,[7]$, et $2^{100} \equiv 1 \times 2 = 2\,[7]$.

Conclusion. Comme $0 \leq 2 < 7$, le reste de 2^{100} par 7 est 2 (Théorème 16.4 (ii)).

16.4 PGCD et Algorithme d'Euclide

Le PGCD de deux entiers est leur plus grand diviseur commun. L'algorithme d'Euclide le calcule par divisions successives, et montre que les diviseurs communs sont exactement les diviseurs du PGCD.

Définition

Définition 16.4 (PGCD). Soient $a, b \in \mathbb{Z}$, non tous deux nuls. Le *plus grand commun diviseur* de a et b, noté $\mathrm{PGCD}(a, b)$, est le plus grand des entiers qui divisent à la fois a et b.

Remarque 16.4 (Existence et Premières Valeurs). Si par exemple $a \neq 0$, tout diviseur commun d vérifie $|d| \leq |a|$ (Théorème 16.1 (iv)) : les diviseurs communs sont en nombre fini ; 1 est un diviseur commun, donc le plus grand existe, et $\mathrm{PGCD}(a, b) \geq 1$. Par l'Exemple 16.1 (ii) et (iv) :

(i) $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, a) = \mathrm{PGCD}(|a|, |b|)$;

(ii) $\mathrm{PGCD}(a, 0) = |a|$ si $a \neq 0$; plus généralement, si $a \neq 0$ et $a \mid b$, alors $\mathrm{PGCD}(a, b) = |a|$; en particulier, $\mathrm{PGCD}(a, 1) = 1$ et $\mathrm{PGCD}(a, a) = |a|$ pour $a \neq 0$.

Exemple 16.4 (PGCD de 12 et 18). Les diviseurs positifs de 12 sont $1, 2, 3, 4, 6, 12$; ceux de 18 sont $1, 2, 3, 6, 9, 18$. Les diviseurs communs positifs sont $1, 2, 3, 6$, donc $\mathrm{PGCD}(12, 18) = 6$.

Théorème 16.6 (Diviseurs Communs et Division). Soient $a, b, q, r \in \mathbb{Z}$ tels que $a = bq + r$. Les diviseurs communs de a et b sont les diviseurs communs de b et r. En particulier, si $b \neq 0$, alors $\mathrm{PGCD}(a, b) = \mathrm{PGCD}(b, r)$.

Preuve. Si $d \mid a$ et $d \mid b$, alors $d \mid a - qb = r$; si $d \mid b$ et $d \mid r$, alors $d \mid bq + r = a$ (Théorème 16.1 (iii)). Les deux couples ont les mêmes diviseurs communs, donc le même plus grand.

Remarque 16.5 (Usage). Pour calculer $\mathrm{PGCD}(a, b)$ avec $b \in \mathbb{N}^*$, on peut remplacer a par son reste dans la division euclidienne par b. Par exemple, $18 = 12 \times 1 + 6$, donc $\mathrm{PGCD}(18, 12) = \mathrm{PGCD}(12, 6) = 6$. C'est le principe de l'algorithme d'Euclide.

Théorème 16.7 (Algorithme d'Euclide). Soient $a, b \in \mathbb{N}^*$. On pose $r_0 = a$ et $r_1 = b$; tant que $r_k \neq 0$, on note r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k :

$$r_{k-1} = r_k q_k + r_{k+1}, \quad 0 \leq r_{k+1} < r_k.$$

(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 PGCD est le dernier reste non nul.

Preuve du Théorème 16.7

Preuve. (i) Les restes $r_1 > r_2 > \cdots$ forment une suite strictement décroissante d'entiers naturels, qui ne peut pas être infinie (Remarque 16.1) : un reste finit par être nul. (ii) Par le Théorème 16.6, les couples (r_0, r_1), (r_1, r_2), …, $(r_N, r_{N+1}) = (r_N, 0)$ ont, de proche en proche, les mêmes diviseurs communs ; ceux de $(r_N, 0)$ sont les diviseurs de r_N. (iii) Le plus grand diviseur de $r_N > 0$ est r_N.

Exemple : PGCD de 252 et 198

Exemple 16.5 (Algorithme d'Euclide).

$$\begin{aligned} 252 &= 198 \times 1 + 54, \\ 198 &= 54 \times 3 + 36, \\ 54 &= 36 \times 1 + 18, \\ 36 &= 18 \times 2 + 0. \end{aligned}$$

Le dernier reste non nul est 18, donc $\mathrm{PGCD}\,(252, 198) = 18$ (Théorème 16.7 (iii)). Si $b \mid a$, l'algorithme s'arrête dès la première division ($N = 1$) et donne $\mathrm{PGCD}\,(a, b) = b$. Si $a < b$, la première division est $a = b \times 0 + a$: elle échange a et b. Comme $\mathrm{PGCD}\,(a, b) = \mathrm{PGCD}\,(b, a)$ (Remarque 16.4 (i)), on peut commencer directement par le plus grand des deux.

Conséquences

Corollaire 16.1 (Diviseurs du PGCD). Soient $a, b \in \mathbb{Z}$, non tous deux nuls, et $d \in \mathbb{Z}$. Alors d divise a et b si et seulement si d divise $\mathrm{PGCD}(a, b)$.

Preuve. Les diviseurs de a et de b sont ceux de $|a|$ et de $|b|$ (Exemple 16.1 (iv)). Si a et b sont non nuls, on applique le Théorème 16.7 (ii) et (iii) à $|a|$ et $|b|$. Si $b = 0$, les diviseurs communs sont ceux de a, et $\mathrm{PGCD}(a, 0) = |a|$; de même si $a = 0$.

Théorème 16.8 (PGCD et Produit). Soient $a, b \in \mathbb{Z}$, non tous deux nuls, et $k \in \mathbb{N}^*$. Alors $\mathrm{PGCD}(ka, kb) = k\,\mathrm{PGCD}(a, b)$.

Preuve. Par la Remarque 16.4 (i), on peut supposer $a, b \geq 0$. Si $b = 0$, alors $a > 0$ et les deux membres valent ka (Remarque 16.4 (ii)) ; de même si $a = 0$. Sinon, $a, b \in \mathbb{N}^*$; multiplions par k chaque division de l'algorithme d'Euclide pour a et b : $kr_{j-1} = (kr_j)\,q_j + kr_{j+1}$ avec $0 \leq kr_{j+1} < kr_j$; c'est la division euclidienne de kr_{j-1} par kr_j (unicité, Théorème 16.2). L'algorithme pour ka et kb a donc pour restes kr_j, et son dernier reste non nul est kr_N.

Entiers Premiers entre Eux

Définition 16.5 (Premiers entre Eux). Deux entiers a et b, non tous deux nuls, sont *premiers entre eux* si $\mathrm{PGCD}(a, b) = 1$, c'est-à-dire si leur seul diviseur commun positif est 1.

Corollaire 16.2 (Simplification par le PGCD). Soient $a, b \in \mathbb{Z}$, non tous deux nuls, et $d = \mathrm{PGCD}(a, b)$. Alors $a = da'$ et $b = db'$, où a' et b' sont des entiers premiers entre eux.

Preuve. d divise a et b, d'où a' et b', non tous deux nuls. Par le Théorème 16.8, $d = \mathrm{PGCD}(da', db') = d\,\mathrm{PGCD}(a', b')$, donc $\mathrm{PGCD}(a', b') = 1$ car $d \neq 0$.

Exemple 16.6 (Premiers entre Eux). 12 et 25 sont premiers entre eux ; 12 et 18 ne le sont pas. Avec $d = \mathrm{PGCD}(252, 198) = 18$: $252 = 18 \times 14$ et $198 = 18 \times 11$, et 14 et 11 sont premiers entre eux.

16.5 Bézout et Gauss

En remontant l'algorithme d'Euclide, on écrit le PGCD comme une combinaison des deux entiers. On en déduit le théorème de Gauss, outil de base de toute la suite.

Identité de Bézout

Théorème 16.9 (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 $au + bv = d$.

Preuve. Si $b = 0$, $d = |a|$ et l'on prend $u = \pm 1$, $v = 0$; de même si $a = 0$. Si a et b sont non nuls, changer a en $-a$ (resp. b en $-b$) revient à changer u en $-u$ (resp. v en $-v$), sans changer d (Remarque 16.4 (i)) : on peut supposer $a, b \in \mathbb{N}^*$. On reprend l'algorithme d'Euclide (Théorème 16.7) et l'on montre par récurrence sur $k \geq 1$ (Théorème 1.13 et Remarque 1.5 du cours 1 [1]) la propriété $\mathcal{P}(k)$: si $k \leq N$, alors r_{k-1} et r_k s'écrivent $au + bv$ avec $u, v \in \mathbb{Z}$. Pour $k = 1$: $r_0 = a \times 1 + b \times 0$ et $r_1 = a \times 0 + b \times 1$. Supposons $\mathcal{P}(k)$ vraie et $k + 1 \leq N$; alors $k \leq N$, et $r_{k+1} = r_{k-1} - q_k r_k$ s'écrit aussi $au + bv$: $\mathcal{P}(k+1)$ est vraie. Par $\mathcal{P}(N)$, $r_N = d$ s'écrit $au + bv$. Ce calcul s'appelle l'*algorithme d'Euclide étendu* ; l'Exemple 16.7 le mène en remontant les divisions.

Remarque 16.6 (Pas d'Unicité). Le couple (u, v) n'est pas unique : si $au + bv = d$, alors $a(u + b) + b(v - a) = d$. Par exemple, $\mathrm{PGCD}(12, 18) = 6$ et $12 \times (-1) + 18 \times 1 = 6$, mais aussi $12 \times 17 + 18 \times (-11) = 6$.

Exemple : Remonter l'Algorithme

Exemple 16.7 (Une Égalité de Bézout pour 252 et 198). On reprend les divisions de l'Exemple 16.5 et l'on exprime chaque reste à partir des deux précédents, en partant du dernier reste non nul :

$$\begin{aligned} 18 &= 54 - 36 \\ &= 54 - (198 - 3 \times 54) = 4 \times 54 - 198 \\ &= 4 \times (252 - 198) - 198 = 4 \times 252 - 5 \times 198. \end{aligned}$$

Vérification : $4 \times 252 - 5 \times 198 = 1008 - 990 = 18$. Donc $(u, v) = (4, -5)$ convient, et aussi $(4 + 198, -5 - 252) = (202, -257)$ (Remarque 16.6).

Théorème de Bézout et Inverse Modulo n

Théorème 16.10 (Théorème de Bézout). Deux entiers a et b, non tous deux nuls, sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Preuve. Si $\mathrm{PGCD}(a, b) = 1$, le Théorème 16.9 donne u et v. Réciproquement, si $au + bv = 1$, tout diviseur commun positif d de a et b divise 1 (Théorème 16.1 (iii)), donc $d = 1$ (Théorème 16.1 (iv)).

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 $x \equiv y\,[n]$.

Preuve. $au \equiv 1\,[n]$ signifie qu'il existe $v \in \mathbb{Z}$ tel que $au + nv = 1$; on applique le Théorème 16.10. Si $ax \equiv ay\,[n]$, on multiplie par u : $x \equiv (au)\,x \equiv (au)\,y \equiv y\,[n]$ (Théorème 16.5 (ii), Théorème 16.4 (iii)).

Théorème de Gauss

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 $a \mid c$.

Preuve. Par le Théorème 16.10, $au + bv = 1$, donc $c = a(cu) + (bc)v$. Or a divise $a(cu)$ et bc : il divise c (Théorème 16.1 (iii)).

Corollaire 16.4 (Produit de Deux Diviseurs). Soient $a, b, c \in \mathbb{Z}$, avec a et b premiers entre eux. Si $a \mid c$ et $b \mid c$, alors $ab \mid c$.

Preuve. Écrivons $c = ak$. Alors $b \mid ak$, et b et a sont premiers entre eux, donc $b \mid k$ (Théorème 16.11) : $k = bl$ et $c = abl$.

Remarque 16.7 (L'Hypothèse est Utile). $6 \mid 12$ et $4 \mid 12$, mais $24 \nmid 12$: 6 et 4 ne sont pas premiers entre eux.

16.6 Équation $ax + by = c$

On cherche les couples d'entiers (x, y) tels que $ax + by = c$. Bézout dit quand il y en a, Gauss les donne tous.

Théorème 16.12 (Équation $ax + by = c$). Soient $a, b \in \mathbb{Z}$ non nuls, $c \in \mathbb{Z}$, et $d = \mathrm{PGCD}(a, b)$; on écrit $a = da'$ et $b = db'$ (Corollaire 16.2).

(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 $(x_0 + kb',\ y_0 - ka')$, $k \in \mathbb{Z}$.

Preuve. (i) Si $ax + by = c$, alors $d \mid c$ (Théorème 16.1 (iii)). Si $c = dc'$, le Théorème 16.9 donne $au + bv = d$, et (uc', vc') est une solution. (ii) Si (x, y) est une solution, alors $a(x - x_0) = b(y_0 - y)$, puis, en divisant par $d \neq 0$, $a'(x - x_0) = b'(y_0 - y)$. Donc $b' \mid a'(x - x_0)$, et b' est premier avec a' (Corollaire 16.2, Remarque 16.4 (i)) : $b' \mid x - x_0$ (Théorème 16.11). Écrivons $x = x_0 + kb'$; alors $a'kb' = b'(y_0 - y)$, et $b' \neq 0$ donne $y = y_0 - ka'$. Réciproquement, $a(x_0 + kb') + b(y_0 - ka') = c + k(ab' - ba') = c$, car $ab' = da'b' = ba'$.

Exemple : $252x + 198y = 36$

Exemple 16.8 (Une Équation $ax + by = c$). Étape 1 (existence). $\mathrm{PGCD}\,(252, 198) = 18$ (Exemple 16.5) et $18 \mid 36$: il y a des solutions (Théorème 16.12 (i)).
Étape 2 (solution particulière). Par l'Exemple 16.7, $4 \times 252 - 5 \times 198 = 18$; en multipliant par 2, $252 \times 8 + 198 \times (-10) = 36$: $(x_0, y_0) = (8, -10)$.
Étape 3 (toutes les solutions). Ici $a' = 14$ et $b' = 11$ (Exemple 16.6). Par le Théorème 16.12 (ii), les solutions sont les couples $(8 + 11k,\ -10 - 14k)$, $k \in \mathbb{Z}$.
Vérification. Pour $k = -1$: $(-3, 4)$, et $252 \times (-3) + 198 \times 4 = -756 + 792 = 36$.

16.7 Nombres Premiers

Les nombres premiers sont les briques des entiers : il y en a une infinité, et tout entier au moins égal à 2 en est un produit. Le petit théorème de Fermat calcule les puissances modulo un nombre premier.

Définition et Premier Diviseur

Définition 16.6 (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 dit *composé*.

Exemple 16.9 (Premiers Cas). 2, 3, 5, 7 sont premiers. 6 ne l'est pas : il a quatre diviseurs positifs, $1, 2, 3, 6$. 1 ne l'est pas : il n'a qu'un diviseur positif. 0 ne l'est pas : il a une infinité de diviseurs positifs.

Le Plus Petit Diviseur

Théorème 16.13 (Plus Petit Diviseur). Soit $n \geq 2$, et soit 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, alors $s^2 \leq n$.

Preuve. L'ensemble des diviseurs ≥ 2 de n contient n : il a un plus petit élément s (Propriété 16.1). (i) Les diviseurs positifs de s sont 1, s, et éventuellement des entiers e avec $2 \leq e < s$ (Théorème 16.1 (iv)) ; un tel e diviserait n (Théorème 16.1 (ii)), ce qui contredirait le choix de s. (ii) Écrivons $n = sm$. Si $m = 1$, alors $n = s$ est premier. Sinon $m \geq 2$ divise n, donc $m \geq s$ et $n = sm \geq s^2$.

Remarque 16.8 (Test de Primalité). Un entier $n \geq 2$ est premier si et seulement si aucun nombre premier p tel que $p^2 \leq n$ ne divise n. En effet, si n est composé, le Théorème 16.13 donne un tel p ; si n est premier, son seul diviseur premier est n, et $n^2 > n$. Exemple : 97 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7, et $11^2 = 121 > 97$: 97 est premier.

Théorème 16.14 (Infinité des Nombres Premiers). Il y a une infinité de nombres premiers.

Preuve. Par l'absurde (cours 19 [2]) : supposons qu'il n'y en ait qu'un nombre fini, $p_1, \ldots, p_k$, avec $k \geq 1$ car 2 est premier. L'entier $M = p_1 p_2 \cdots p_k + 1 \geq 2$ a un diviseur premier (Théorème 16.13 (i)), qui est l'un des p_i. Alors p_i divise M et $p_1 \cdots p_k$, donc il divise $M - p_1 \cdots p_k = 1$ (Théorème 16.1 (iii)) : c'est impossible, car $p_i \geq 2$.

Théorème 16.15 (Nombre Premier et Produit). Soit p un nombre 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, alors p divise l'un des a_i.

Preuve. (i) PGCD (a, p) est un diviseur positif de p, donc vaut 1 ou p ; s'il vaut p, alors $p \mid a$. (ii) Si $p \nmid a$, alors a et p sont premiers entre eux par (i), et $p \mid b$ (Théorème 16.11). (iii) Par récurrence sur k (Théorème 1.13 et Remarque 1.5 du cours 1 [1]) : c'est clair pour $k = 1$; si c'est vrai pour k et si $p \mid (a_1 \cdots a_k)\, a_{k+1}$, alors par (ii) $p \mid a_{k+1}$ ou $p \mid a_1 \cdots a_k$, et dans ce second cas p divise l'un des $a_1, \ldots, a_k$.

Théorème 16.16 (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 ; on l'appelle la *décomposition en facteurs premiers* de n. L'unicité est admise.

Preuve de l'existence. Par l'absurde : si l'ensemble des entiers $n \geq 2$ sans décomposition n'était pas vide, il aurait un plus petit élément m (Propriété 16.1). Un nombre premier est sa propre décomposition, donc m est composé. Écrivons $m = pm'$, avec p premier (Théorème 16.13 (i)) ; alors $m' \neq 1$ car m n'est pas premier, et $m' < m$ car $p \geq 2$, donc $2 \leq m' < m$; ainsi m' a une décomposition, et en y ajoutant le facteur p on obtient une décomposition de m : c'est une contradiction.

Remarque 16.9 (En Pratique). On divise n par son plus petit diviseur premier, puis le quotient par le sien, et ainsi de suite : $252 = 2 \times 126 = 2^2 \times 63 = 2^2 \times 3 \times 21 = 2^2 \times 3^2 \times 7$. De même, $8 = 2^3$, $12 = 2^2 \times 3$ et $100 = 2^2 \times 5^2$.

Théorème 16.17 (Diviseurs d'un Entier). Soit $n = p_1^{k_1} \cdots p_j^{k_j}$ 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 ; ils sont deux à deux distincts, donc n a $(k_1 + 1) \cdots (k_j + 1)$ diviseurs positifs. En conséquence, si $m \geq 2$ est un autre entier, $\mathrm{PGCD}(n, m)$ est le produit des nombres premiers communs aux deux décompositions, chacun avec le plus petit de ses deux exposants.

Exemple 16.10 (Par les Décompositions). $252 = 2^2 \times 3^2 \times 7$ et $198 = 2 \times 3^2 \times 11$, donc $\mathrm{PGCD}(252, 198) = 2 \times 3^2 = 18$, comme dans l'Exemple 16.5. Le nombre de diviseurs positifs de 252 est $(2 + 1)(2 + 1)(1 + 1) = 18$.

Preuve du Théorème 16.17

Preuve. Un tel produit divise n : le quotient est $p_1^{k_1-e_1}\cdots p_j^{k_j-e_j}$. Réciproquement, si $n = ef$ avec $e, f \geq 1$, on décompose e et f (Théorème 16.16 ; un facteur égal à 1 a une décomposition vide) ; le produit des deux décompositions est une décomposition de n, donc, par l'unicité, e n'a pour facteurs premiers que des p_i, avec des exposants $e_i \leq k_i$. Deux tels produits d'exposants différents sont distincts : c'est clair si l'un d'eux vaut 1, et sinon c'est encore l'unicité. Enfin, un diviseur commun positif de n et m n'a pour facteurs premiers que des nombres premiers communs aux deux décompositions, chacun avec un exposant au plus égal à ses deux exposants : il divise donc le produit D de ces nombres premiers pris avec le plus petit des deux exposants. Or D est un diviseur commun ; c'est donc le plus grand (Théorème 16.1 (iv)).

Petit Théorème de Fermat

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 $a \in \mathbb{Z}$, $a^p \equiv a\,[p]$.

Preuve du Théorème 16.18

Preuve. (i) Pour $k = 1, \dots, p-1$, notons r_k le reste de ka dans la division par p. Comme $0 < k < p$, $p \nmid k$ (Théorème 16.1 (iv)) ; comme de plus $p \nmid a$, $p \nmid ka$ (Théorème 16.15 (ii)), donc $r_k \neq 0$ (Théorème 16.3 (i)) ; et $ka \equiv r_k\,[p]$ (Théorème 16.4 (ii)). Si $r_k = r_l$ avec $1 \leq k < l \leq p-1$, alors $p \mid (l-k)\,a$ (Théorème 16.4 (i)), donc $p \mid l-k$ (Théorème 16.15 (ii)), ce qui est impossible car $0 < l-k < p$. Les $p-1$ restes $r_1, \dots, r_{p-1}$ sont donc distincts et compris entre 1 et $p-1$: ce sont les entiers $1, 2, \dots, p-1$, dans un autre ordre. Par le Théorème 16.5 (ii),

$$(1 \cdot a)\,(2 \cdot a) \cdots ((p-1)\,a) \equiv r_1 r_2 \cdots r_{p-1}\,[p], \quad \text{soit} \quad (p-1)!\,a^{p-1} \equiv (p-1)!\,[p],$$

où $(p-1)! = 1 \times 2 \times \cdots \times (p-1)$. Ainsi $p \mid (p-1)!\left(a^{p-1}-1\right)$. Or p ne divise aucun des facteurs $1, \dots, p-1$, donc pas leur produit (Théorème 16.15 (iii)) : $p \mid a^{p-1}-1$ (Théorème 16.15 (ii)). (ii) Si $p \mid a$, les deux membres sont congrus à 0 ; sinon, on multiplie (i) par a.

Exemple : Reste de 5^{2026} par 7

Exemple 16.11 (Avec le Petit Théorème de Fermat). Étape 1. 7 est premier et $7 \nmid 5$, donc $5^6 \equiv 1\,[7]$ (Théorème 16.18 (i)).
Étape 2. $2026 = 6 \times 337 + 4$, donc $5^{2026} = \left(5^6\right)^{337} \times 5^4 \equiv 5^4\,[7]$ (Théorème 16.5).
Étape 3. $5^2 = 25 \equiv 4\,[7]$, donc $5^4 \equiv 4^2 = 16 \equiv 2\,[7]$.
Conclusion. Le reste de 5^{2026} par 7 est 2 (Théorème 16.4 (ii)).

16.8 PPCM

Le PPCM de deux entiers est leur plus petit multiple commun strictement positif. Son produit par le PGCD est le produit des deux entiers.

PPCM

Définition 16.7 (PPCM). Soient $a, b \in \mathbb{Z}$ non nuls. Le *plus petit commun multiple* de a et b, noté $\mathrm{PPCM}(a, b)$, est le plus petit entier strictement positif multiple de a et de b. Il existe par la Propriété 16.1, car $|ab|$ est un tel multiple.

Théorème 16.19 (PGCD et PPCM). Soient $a, b \in \mathbb{Z}$ non nuls, $d = \mathrm{PGCD}(a, b)$ et $m = \mathrm{PPCM}(a, b)$.

(i) Les multiples communs de a et b sont exactement les multiples de m.

(ii) $dm = |ab|$.

Exemple 16.12 (PPCM de 252 et 198). $\mathrm{PPCM}(252, 198) = \frac{252 \times 198}{18} = 14 \times 198 = 2772$.

Preuve du Théorème 16.19

Preuve. Les multiples de a sont ceux de $|a|$: on peut supposer $a, b > 0$. Écrivons $a = da'$, $b = db'$ (Corollaire 16.2) et $M = da'b'$. $M = ab' = ba'$ est un multiple commun. Si c est un multiple commun, $c = ak = da'k$, et $db' \mid da'k$ donne $b' \mid a'k$, donc $b' \mid k$ (Théorème 16.11) : $k = b'l$ et $c = Ml$. Les multiples communs sont donc les multiples de M ; le plus petit qui est strictement positif est M, donc $m = M$, et $dm = d^2a'b' = ab$.

À retenir

On retient la division euclidienne et les congruences, le PGCD et l'algorithme d'Euclide, Bézout et Gauss, la résolution de $ax + by = c$, les nombres premiers et le petit théorème de Fermat.

À retenir

Ce que cette leçon a établi.

- Pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple (q, r) tel que $a = bq + r$ et $0 \leq r < b$; $b \mid a$ si et seulement si $r = 0$ (Théorèmes 16.2 et 16.3).
- $a \equiv b\,[n]$ si et seulement si a et b ont le même reste par n ; on additionne, multiplie et élève à une puissance, mais on ne simplifie pas sans inverse (Théorèmes 16.4, 16.5, Corollaire 16.3).
- Le PGCD est le dernier reste non nul de l'algorithme d'Euclide ; les diviseurs communs sont les diviseurs du PGCD (Théorème 16.7, Corollaire 16.1).
- Bézout : $au + bv = \mathrm{PGCD}\,(a, b)$; a et b premiers entre eux si et seulement si $au + bv = 1$. Gauss : si $a \mid bc$ et $\mathrm{PGCD}\,(a, b) = 1$, alors $a \mid c$ (Théorèmes 16.9 à 16.11).
- $ax + by = c$ a des solutions si et seulement si $\mathrm{PGCD}\,(a, b) \mid c$; elles sont $(x_0 + kb', y_0 - ka')$ (Théorème 16.12).
- Tout $n \geq 2$ a un diviseur premier, et un diviseur premier p tel que $p^2 \leq n$ s'il est composé ; il y a une infinité de nombres premiers ; décomposition en facteurs premiers ; si $p \nmid a$, alors $a^{p-1} \equiv 1\,[p]$ (Théorèmes 16.13 à 16.18).
- $\mathrm{PGCD}\,(a, b) \times \mathrm{PPCM}\,(a, b) = |ab|$ (Théorème 16.19).

Merci pour votre attention.

Références

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

[2] Mohamed Kadhem Karray.
Cours 19. Logique et ensembles, niveau baccalauréat.
https://mohamedkadhem.com/baccalaureat/.