Cours Arithmétique et Polynômes du premier semestre de L1

(écrit par Mireille Fouquet [(*)], version de 2025 avec table des matières)

Table des matières

Sources :

• Liret et Martinais, *Mathématiques pour le DEUG. Algèbre 1ère année.* Éd. Dunod. [512 LIR]

• E. Ramis, C. Deschamps, J. Odoux, Cours de mathématiques [51 L RAM] :
[512 RAM], [514 RAM], [515 RAM], [517 RAM], [517 RAM], niveau L1 seul dans [51 L1 RAM]

• Marc Hindry, *Cours de Mathématiques, Première Année.* Université Paris 7.
(`http://www.imj-prg.fr/~marc.hindry/Cours-L1.pdf`)

Précisions :

Le fichier source contient :
– *des démonstrations* qu'on fait apparaître en vert en remplaçant
`\long\def\invisible#1{}` par `%\long\def\invisible#1{}`
– des compléments, pour s'adapter à d'éventuels nouveaux programmes plus complets, qu'on fait apparaître en rouge en remplaçant
`\long\def\horsprogramme#1{}` par `%\long\def\horsprogramme#1{}`

(*) Pour me contacter : Mireille Fouquet<`fouquet@math.univ-paris-diderot.fr`>

Ch. 1. Arithmétique dans $\mathbb{Z}$

Plan
I. Divisibilité et congruences
II. Nombres premiers entre eux
III. Nombres premiers
IV. Résolution d'équations

I. Divisibilité et congruences

1. Généralités

On appelle entier (ou entier relatif, c'est-à-dire positif ou négatif) tout élément de $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Le sous-ensemble des entiers positifs est noté $\mathbb{N}$ et il est courant de dire que tout élément de $\mathbb{N}$ est un entier naturel.

Définition

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

On dit qu'un entier a est un *multiple* d'un entier b, ou que b est un *diviseur* de a lorsqu'il existe un entier k tel que $a = kb$. On dit aussi que b divise a et on le note $b \mid a$.

Exemples

8 est un multiple de 2 et 2 est un diviseur de 8, puisque $8 = 4 \times 2$.
-6 est un multiple de 3 puisque $-6 = (-2) \times 3$ et -3 est un diviseur de 6 puisque $6 = (-2) \times (-3)$

Propriétés

- Les seuls diviseurs de 1 sont 1 et -1.
- Tout entier divise 0, i.e. 0 est multiple de tout entier.
- Le seul multiple de 0 est 0, i.e. 0 est le seul entier divisible par 0/
- Tout entier est divisible par 1 et -1.
- Tout entier est divisible par lui-même et son opposé.

Proposition

Soit a un entier non nul. Soit b un diviseur de a. Alors il existe un unique entier q tel que $a = bq$.

Démonstration

Soit $a \in \mathbb{Z}^*$. Comme $a \neq 0$, on sait que 0 ne divise pas a donc b diviseur de a est non nul. Supposons qu'il existe q_1 et q_2 entiers tels que $a = bq_1 = bq_2$. Donc $bq_1 - bq_2 = 0 = b(q_1 - q_2)$. Comme $b \neq 0$, on a donc $q_1 - q_2 = 0$ soit $q_1 = q_2$. □

Proposition

Soient a, b et c trois entiers.

1. Si a divise b et b divise c, alors a divise c.
2. Si a divise b et b divise a, alors $a = \pm b$.
3. Si a divise b et a divise c, alors a divise $b + c$.
4. Si a divise b, alors a divise bc.

5. Si a divise b, alors ac divise bc.

Démonstration

Soient a, b et c trois entiers.

1. Supposons que a divise b et que b divise c, donc il existe q_1 et q_2 deux entiers tels que $b = aq_1$ et $c = bq_2$. Donc $c = aq_1q_2 = a(q_1q_2)$ donc a divise c.
2. Supposons que a divise b et que b divise a, donc il existe q_1 et q_2 deux entiers tels que $b = aq_1$ et $a = bq_2$. Donc $a = aq_1q_2$ donc $a - a(q_1q_2) = 0 = a(1 - q_1q_2)$.
   Supposons que $a = 0$ alors $b = aq_1 = 0 = a$.
   Supposons que $a \neq 0$ alors $1 - q_1q_2 = 0$, i.e. $q_1q_2 = 1$ donc $q_1 = q_2 = \pm 1$ et donc $a = \pm b$.
3. Supposons que a divise b et que a divise c, donc il existe q_1 et q_2 deux entiers tels que $b = aq_1$ et $c = aq_2$. Donc $b + c = aq_1 + aq_2 = a(q_1 + q_2)$, donc a divise $b + c$.
4. Supposons que a divise b, donc il existe un entier q tel que $b = aq$. Donc $bc = aqc = a(qc)$ i.e. a divise bc.
5. Supposons que a divise b, donc il existe un entier q tel que $b = aq$. Donc $bc = aqc = (ac)q$, i.e. ac divise bc.

Lemme

Soit a un entier naturel non nul. Soit d est un diviseur de a. On a alors $-a \leq d \leq a$.

Démonstration

Soit a un entier naturel non nul. Soit d est un diviseur de a. Donc il existe un entier q tel que $a = dq$.
Supposons $d > 0$. Supposons $d > a$, alors, comme $a > 0$ et $d > 0$, $q > 0$ donc $q \geq 1$. Donc $a = d \times q > a \times 1 = a$, ce qui est impossible. Donc $d \leq a$.
Supposons $d < 0$. Alors $-d$ est un diviseur de a et $-d > 0$ donc $-d \leq a$, i.e. $d \geq -a$. □

2. Division euclidienne

Pour tous entiers a et b, $b \neq 0$, on peut établir une relation via la division euclidienne.

Théorème

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :
$a = bq + r$ et $0 \leq r < |b|$ « division euclidienne de a par b ».

Dans ce cas, r s'appelle *le reste* et q s'appelle *le quotient*, de la division de a par b.

Exemples

Division euclidienne de 64 par 7 : $64 = 9 \times 7 + 1$. 9 est le quotient de cette division et 1 est son reste.
Division euclidienne de 37 par -5 : $37 = (-7) \times (-5) + 2$. -7 est le quotient de cette division et 2 est son reste.
Division euclidienne de -21 par -4 : $-21 = 6 \times (-4) + 3$. 6 est le quotient de cette division et 3 est son reste.

Démonstration

• On montre tout d'abord l'existence dans le cas où $a \geq 0$.
Récurrence sur $n \in \mathbb{N}$: (H_n) existence de $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ quand $0 \leq a \leq n$ et $b \in \mathbb{Z} \setminus \{0\}$.

(i) On suppose que $n = 0$. On a : $a = 0 = b\,0 + 0$.
Cela montre que (H_0) est vraie.

(ii) On suppose que (H_n) est vraie et $0 \leq a \leq n + 1$:
– soit $0 \leq a < |b|$ puis l'égalité $a = b\,0 + a$ fournit un couple (q, r) ;

– soit $0 < |b| \leq a \leq n+1$ donc $0 \leq a - |b| \leq n$ puis grâce à (H_n) il existe $(q_0, r_0) \in \mathbb{Z} \times \mathbb{Z}$ tel que $a - |b| = bq_0 + r_0$ et $0 \leq r_0 < |b|$, donc $a = b(q_0 + \text{sg}(b)) + r_0$ ce qui donne un couple (q, r).

On en déduit que (H_{n+1}) est vraie.

(iii) Ainsi l'existence est obtenue quand $a \geq 0$.

• On montre maintenant l'existence dans le cas où $a < 0$.

D'après le cas précédent, il existe $(q_1, r_1) \in \mathbb{Z} \times \mathbb{Z}$ tel que $-a = bq_1 + r_1$ et $0 \leq r_1 < |b|$:
– soit $r_1 = 0$ et on utilise l'égalité $a = b(-q_1)$;
– soit $r_1 \neq 0$ et on utilise l'égalité $a = b(-q_1 - \text{sg}(b)) + |b| - r_1$ avec $0 \leq |b| - r_1 < |b|$.

• On montre maintenant l'unicité (dans tous les cas).

On se donne $(q, r), (q', r') \in \mathbb{Z} \times \mathbb{Z}$ tels que :

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

On a : $0 - (|b| - 1) \leq r' - r \leq (|b| - 1) - 0$ et $|b|\,|q - q'| = |r' - r|$ donc $|b|\,|q - q'| \leq |b| - 1$.
D'où : $q = q'$ (par l'absurde), puis $r = r'$ (car $bq + r = bq' + r'$). □

Propriété

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$.
a est divisible par b si et seulement si le reste de la division euclidienne de a par b est nul.

Démonstration

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$.
Supposons que a est divisible par b. Alors il existe un entier q tel que $a = bq$. Donc $a = bq + 0$ et $0 \leq 0 < |b|$. Par unicité du quotient et du reste de la division euclidienne, q est le quotient de la division euclidienne de a par b et 0 son reste.
Inversement, si la division euclidienne de a par b est égal à 0, alors si on note q son quotient, $a = bq + 0 = bq$ et donc a est divisible par b. □

3. Congruences

Définition

Soient a et b deux entiers relatifs et soit n un entier naturel.
On dit que a est congru à b modulo n si et seulement si n divise $a - b$.
On le note $a \equiv b \mod n$ ou $a \equiv b[n]$.

Exemples

- $24 \equiv 10 \mod 7$ puisque 7 divise $24 - 10 = 14$.
- $-13 \equiv 9 \mod 11$ puisque 11 divise $-13 - 9 = -22$.
- $-8 \equiv -13 \mod 5$ puisque 5 divise $-13 - (-8) = -5$.

Remarques

Soient a et b deux entiers.
Si $a \equiv b \mod 0$ alors $0 \mid (a - b)$, donc $a - b = 0$ i.e. $a = b$. La congruence modulo 0 est équivalente à l'égalité classique.
La congruence modulo 1 est triviale pour sa bort, puisque quelque soient a et b, $1 \mid (a - b)$, i.e. quelque soient a et b entiers, $a \equiv b \mod 1$.

Propriétés

Soient a, b, c et d quatre entiers et soient m et n deux entiers naturels non nuls.

1. Si $a \equiv b[n]$ alors $b \equiv a[n]$.
2. Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$.
3. Si $a \equiv c[n]$ et $b \equiv d[n]$, alors $a + b \equiv c + d[n]$ et $ab \equiv cd[n]$.

4. Si $a \equiv b[n]$ alors $ma \equiv mb[mn]$.

Démonstration

Soient a, b, c et d quatre entiers et soient m et n deux entiers naturels non nuls.

1. Supposons $a \equiv b[n]$, alors il existe $q \in \mathbb{Z}$ tel que $a - b = qn$. Donc $b - a = -qn$ donc $b \equiv a[n]$.
2. Supposons $a \equiv b[n]$ et $b \equiv c[n]$, alors il existe $q_1, q_2 \in \mathbb{Z}$ tels que $a - b = q_1 n$ et $b - c = q_2 n$. Donc $a - c = (a - b) + (b - c) = q_1 n + q_2 n = (q_1 + q_2)n$. Donc $a \equiv c[n]$.
3. Supposons $a \equiv c[n]$ et $b \equiv d[n]$, alors il existe $q_1, q_2 \in \mathbb{Z}$ tels que $a-c = q_1 n$ et $b-d = q_2 n$. Donc $(a+b)-(c+d) = (a-c)+(b-d) = q_1 n + q_2 n = (q_1 + q_2)n$. Donc $a+b \equiv c+d[n]$. On a aussi : $ab-cd = (a-c)b+bc-cd = (a-c)b+(b-d)c = q_1 nb + q_2 nc = (q_1 b + q_2 c)n$. Donc $ab \equiv cd[n]$.
4. Supposons $a \equiv b[n]$, alors il existe $q \in \mathbb{Z}$ tel que $a-b = qn$. Donc $ma - mb = m(a-b) = mqn$ donc $ma \equiv mb[mn]$.

Proposition

Soit a un entier relatif et soit n un entier naturel non nul.
On pose r le reste de la division euclidienne de a par n. Alors $a \equiv r \mod n$.

Démonstration

Soit a un entier relatif et soit n un entier naturel non nul. On pose q et r le quotient et le reste de la division euclidienne de a par n, i.e. $a = qn + r$ et $0 \leq r < |a|$. Donc $a - r = qn$ et donc $a \equiv r \mod n$.

II. Nombres premiers entre eux

1. PGCD - Algorithme d'Euclide

Définition-Proposition

Soient $a,\ b \in \mathbb{Z}$ tels que au moins l'un des deux est différent de 0. Il existe un unique $d \in \mathbb{N}$ qui divise a et b et tel que tout diviseur d' dans $\mathbb{Z}$ de a et b est tel que $d' \leq d$. On l'appelle *plus grand commun diviseur* de a et de b.

On le note : $d = \text{pgcd}(a, b)$ ou $d = a \wedge b$.

On posera $\text{pgcd}(0, 0) = 0$.

Démonstration

Soient $a,\ b \in \mathbb{Z}$ tels que au moins l'un des deux est différent de 0.
Supposons que $a \neq 0$.

On considère l'ensemble $\mathcal{D}$ des diviseurs communs positifs ou nuls de a et de b. Cet ensemble est une partie de $\mathbb{N}$ non vide puisque $1 \in \mathcal{D}$ et majorée par $|a|$. Il admet donc un unique plus grand élément. Notons d cet élément. Par définition, tout diviseur naturel d' de a et de b appartient à $\mathcal{D}$ et donc, par définition de d, $d' \leq d$. □

Exemple

$\text{pgcd}(15, 27) = 3$.

Propriétés

- Pour tout $a,\ b \in \mathbb{Z}$, $\text{pgcd}(a, b) = \text{pgcd}(b, a)$.
- Pour tout $a,\ b \in \mathbb{Z}$, $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$.
- Pour tout $a \in \mathbb{Z}$, $\text{pgcd}(0, a) = |a|$.

- Pour tout $a \in \mathbb{Z}$, $\text{pgcd}(1, a) = 1$.

Proposition

Soient $a,\ b \in \mathbb{Z}$ avec $b \neq 0$. On note r le reste de la division euclidienne de a par b. Alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Démonstration

On note q le quotient de la division euclidienne de a par b. On a donc $a = bq + r$ soit $r = a - bq$. On pose $\mathcal{D}$ l'ensemble des diviseurs communs positifs ou nuls de a et de b et $\mathcal{D}'$ l'ensemble des diviseurs communs positifs ou nuls de b et de r. Soit $d \in \mathcal{D}$ donc il existe $k_1,\ k_2 \in \mathbb{Z}$ tel que $a = dk_1$ et $b = dk_2$. Donc $r = a - bq = dk_1 - dk_2q = d(k_1 - k_2q)$ et donc $d \mid r$. Ainsi on a $d \mid b$ et $d \mid r$ et donc $d \in \mathcal{D}'$. Donc $\mathcal{D} \subseteq \mathcal{D}'$. Soit $d' \in \mathcal{D}'$ donc il existe $\ell_1,\ \ell_2 \in \mathbb{Z}$ tel que $b = d'\ell_1$ et $r = d'\ell_2$. Donc $a = bq + r = d'\ell_1 q + d'\ell_2 = d'(\ell_1 q + \ell_2)$ et donc $d' \mid a$. Ainsi on a $d' \mid b$ et $d' \mid a$ et donc $d' \in \mathcal{D}$. Donc $\mathcal{D}' \subseteq \mathcal{D}$. Donc $\mathcal{D} = \mathcal{D}'$ et donc leur plus grand élément est le même.

Algorithme Algorithme d'Euclide

Entrées : $a,\ b \in \mathbb{Z}$ tel que $b \neq 0$. Sortie : $\text{pgcd}(a, b)$ Initialisation : $(r,\ r') \leftarrow (a,\ b)$

Tant que $r' \neq 0$, faire :

- $q \leftarrow$ quotient de la division euclidienne de r par r' ;
- $(r,\ r') \leftarrow (r',\ r - qr')$

Fin Tant que Retourner r.

Remarque

Dans l'algorithme d'Euclide, $r - qr'$ est égal au reste de la division euclidienne de r par r'.

Exemples

Calcul du pgcd de 87 et 35 :

$87 = 35 \times 2 + 17$
$35 = 17 \times 2 + 1$
$17 = 1 \times 17 + 0$
Donc $\text{pgcd}(87,\ 35) = 1$ Calcul du pgcd de 147 et 24 :
$147 = 24 \times 6 + 3$
$24 = 3 \times 8 + 0$
Donc $\text{pgcd}(147,\ 24) = 3$

Proposition

Soient $a,\ b \in \mathbb{Z}$ avec $b \neq 0$. Le résultat de l'algorithme d'Euclide est le pgcd de a et de b.

Démonstration

Soient $a,\ b \in \mathbb{Z}$ avec $b \neq 0$. On pose $r_0 = a$ et $r_1 = b$. On construit la suite (r_i) telle que pour tout $i \geq 0$, r_{i+2} est le reste de la division euclidienne de r_i par r_{i+1}. Soit k le rang du dernier reste non nul, i.e. $r_k \neq 0$ et $r_{k+1} = 0$. Montrons par récurrence la propriété P_i : $\text{pgcd}(a, b) = \text{pgcd}(r_i, r_{i+1})$. Au rang 0, on a bien $\text{pgcd}(a, b) = \text{pgcd}(r_0, r_1)$ par définition de r_0 et de r_1. Soit $i \in \mathbb{N}$. Supposons P_i, i.e. $\text{pgcd}(a, b) = \text{pgcd}(r_i, r_{i+1})$.

Si $r_{i+1} \neq 0$, r_{i+2} est défini et $\text{pgcd}(r_i, r_{i+1}) = \text{pgcd}(r_{i+1}, r_{i+2})$ et donc par hypothèse de récurrence, $\text{pgcd}(a, b) = \text{pgcd}(r_{i+1}, r_{i+2})$.
Si $r_{i+1} = 0$, par hypothèse de récurrence, $\text{pgcd}(a, b) = \text{pgcd}(r_i, 0) = r_i$ et r_{i+2} est non défini.
De plus, par définition du reste, on a $0 \leq r_{i+1} < |r_i|$ (et donc pour tout $i > 1$, $r_i \geq 0$). Donc à partir du rang 2, la suite (r_i) est strictement décroissante et bornée par 0, donc cette suite d'entiers naturels atteint 0. Ainsi l'algorithme d'Euclide se termine et $\text{pgcd}(a, b) = r_k$.

2. Nombres premiers entre eux

Définition

On dit que $a, b \in \mathbb{Z}$ sont *premiers entre eux* si : $\text{pgcd}(a, b) = 1$.

Exemple

6 et 35 sont premiers entre eux.

Proposition

Soient a et b deux entiers non nuls alors $\frac{a}{\text{pgcd}(a,b)}$ et $\frac{b}{\text{pgcd}(a,b)}$ sont premiers entre eux.

Démonstration

On pose $d = \text{pgcd}(a, b)$, $q = \frac{a}{d}$ et $q' = \frac{b}{d}$.
On note $k = \text{pgcd}(q, q')$.
Par définition, $k \mid q$ et $k \mid q'$. Donc $dk \mid dq = a$ et $dk \mid dq' = b$. Par définition de d, $dk \leq d$. Or $d \geq 1$ puisque $a \neq 0$ et $b \neq 0$, donc $k \leq 1$.
De plus comme $a \neq 0$ et $b \neq 0$, $q \neq 0$ et $q' \neq 0$ donc $k \geq 1$. Donc $k = 1$. □

Algorithme Algorithme d'Euclide étendu

Entrées : $a,\ b \in \mathbb{Z}$ tel que $b \neq 0$. Sortie : $r = \text{pgcd}(a, b)$ et $u,\ v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$ Initialisation : $(r,\ u,\ v,\ r',\ u',\ v') \leftarrow (a,\ 1,\ 0,\ b,\ 0,\ 1)$

Tant que $r' \neq 0$, faire :

- $q \leftarrow$ quotient de la division euclidienne de r par r' ;
- $(r,\ u,\ v,\ r',\ u',\ v') \leftarrow (r',\ u',\ v',\ r - qr',\ u - qu',\ v - qv')$

Fin Tant que Retourner $(r,\ u,\ v)$.

Proposition

Soient $a,\ b \in \mathbb{Z}$ tel que $b \neq 0$.
L'algorithme d'Euclide étendu retourne le $\text{pgcd}(a, b)$ et $u,\ v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$.

Démonstration

Soient $a,\ b \in \mathbb{Z}$ avec $b \neq 0$.
Dans l'algorithme d'Euclide étendu, les variables r et r' correspondent respectivement aux variables r et r' de l'algorithme d'Euclide. Donc l'algorithme d'Euclide étendu se termine et retourne $r = pgcd(a, b)$.
On pose $r_0 = a$, $r_1 = b$, $u_0 = 1$, $u_1 = 0$, $v_0 = 0$ et $v_1 = 1$. On construit les suites (r_i), (q_i), (u_i) et (v_i) telles que pour tout $i \geq 0$, r_{i+2} est le reste de la division euclidienne de r_i par r_{i+1}, q_i est le quotient de la division euclidienne de r_i par r_{i+1}, u_{i+2} est égal à $u_i - q_i u_{i+1}$ et v_{i+2} est égal à $v_i - q_i v_{i+1}$. Soit k le rang du dernier reste non nul, i.e. $r_k \neq 0$ et $r_{k+1} = 0$. Soit $i \geq 0$. Montrons la propriété Q_i : "$r_i = au_i + bv_i$ et $r_{i+1} = au_{i+1} + bv_{i+1}$".
Par définition, $r_0 = a$ donc $r_0 = a \times 1 + b \times 0 = au_0 + bv_1$. De même, $r_1 = b = a \times 0 + b \times 1 = au_1 + bv_1$. Donc Q_0 est vraie.
Soit $i \geq 0$. Supposons Q_i.
Si $r_{i+1} = 0$, alors on sort de la boucle tant que de l'algorithme et on a bien, d'après Q_i, $r_i = au_i + bv_i$.
Si $r_{i+1} \neq 0$, $r_{i+2} = r_i - q_i r_{i+1} = au_i + bv_i - q_i(au_{i+1} + bv_{i+1})$, par hypothèse de récurrence.
Donc $r_{i+2} = a(u_i - q_i u_{i+1}) + b(v_i - q_i v_{i+1}) = au_{i+2} + bv_{i+2}$ par définition des suites (u_i) et (v_i). Ainsi, en supposant Q_i, Q_{i+1} vraie. □

L'algorithme d'Euclide étendu nous permet de démontrer le théorème suivant.

Théorème Théorème de Bézout

Soient a et b deux entiers. Il existe $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $au + bv = \text{pgcd}(a, b)$.

Proposition

Soient a et b deux entiers. a et b sont premiers entre eux si et seulement si il existe deux entiers u et v tels que $au + bv = 1$.

Attention ! ce résultat n'est valable que pour $\text{pgcd}(a, b) = 1$. En effet, pour $a = 2$ et $b = 3$, $a \times 4 + b \times (-2) = 2$ et pourtant $\text{pgcd}(a, b) = 1$.

Démonstration

Soient a et b deux entiers.
Supposons que $\text{pgcd}(a, b) = 1$. Alors d'après le théorème de Bezout, il existe deux entiers u et v tels que $au + bv = 1$.
Supposons qu'il existe deux entiers u et v tels que $au + bv = 1$. Soit d un diviseur positif de a et de b, alors d divise au et d divise bv, donc d divise $au + bv = 1$. Comme d est positif, $d = 1$ et donc $\text{pgcd}(a, b) = 1$.

Proposition

Soient a et b deux entiers.

(*i*) Soit d un diviseur commun à a et à b. Alors $d = pgcd(a, b)$ si et seulement si tout diviseur commun à a et à b divise d.

(*ii*) Pour tout entier positif non nul m, $pgcd(ma, mb) = m\ pgcd(a, b)$.

Démonstration

(*i*) Soient a et b deux entiers. D'après le théorème de Bézout, il existe deux entiers u et v tels que $au + bv = \text{pgcd}(a, b)$.
Soit d' diviseur commun de a et de b. Donc $d' \mid au$ et $d' \mid bv$, donc $d' \mid au + bv = \text{pgcd}(a, b)$. Donc tout diviseur commun à a et à b divise $\text{pgcd}(a, b)$.
Soit d un diviseur commun à a et à b tel que tout diviseur commun d' à a et à b divise d. Comme $\text{pgcd}(a, b)$ divise a et b, par définition de d, $\text{pgcd}(a, b) \mid d$ et donc $\text{pgcd}(a, b) \leq d$. Inversement, on vient de démontrer que tout diviseur de a et de b divise $\text{pgcd}(a, b)$. Donc $d \mid \text{pgcd}(a, b)$ et donc $d = \text{pgcd}(a, b)$.

(*ii*) On pose $d = \text{pgcd}(a, b)$. Soit $m \in \mathbb{N}^*$. Supposons que $(a, b) \neq (0, 0)$. Alors $d > 0$. Comme $d \mid a$ et $d \mid b$, donc $md \mid ma$ et $md \mid mb$. D'après le théorème de Bézout, il existe deux entiers u et v tels que $au + bv = d$.
Soit k un entier positif qui divise ma et mb. Donc $k \mid mau$ et $k \mid mbv$, donc $k \mid mau + mbv = md$. Donc tout diviseur commun à ma et à mb divise md, donc $md = \text{pgcd}(ma, mb) = m\ pgcd(a, b)$.

Théorème Théorème de Gauss

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

Démonstration

Soient $a,\ b,\ c \in \mathbb{Z}^*$ tels que $a \mid bc$ et $\text{pgcd}(a, b) = 1$.
D'après la proposition précédente, $\text{pgcd}(ac, bc) = c\ \text{pgcd}(a, b)$ et donc par hypothèse, $\text{pgcd}(ac, bc) = c$. De plus, par définition, $a \mid ac$ et par hypothèse, $a \mid bc$, donc d'après la proposition précédente, $a \mid \text{pgcd}(ac, bc) = c$. □

3. PPCM

Définition-Proposition

Soient $a,\ b \in \mathbb{Z}$. Il existe un unique $m \in \mathbb{N}$ multiple de a et de b et tel que tout $m' \in \mathbb{N}$ multiple de a et b est tel que $m \leq m'$. On l'appelle *plus petit commun multiple* de a et de b.

On le note : $d = \text{ppcm}(a, b)$ ou $d = a \vee b$.

Remarque

$\text{ppcm}(0, 0) = 0$

Démonstration

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

On considère l'ensemble $\mathcal{M} = \{k \in \mathbb{N} \mid a \mid k \text{ et } b \mid k\}$ des multiples communs positifs ou nuls de a et de b. Cet ensemble est une partie de $\mathbb{N}$ non vide puisque $\mid ab \mid \in \mathcal{M}$ et minorée par $\min(\mid a \mid, \mid b \mid)$. Il admet donc un unique plus petit élément. Notons m cet élément. Par définition, tout multiple naturel m' de a et de b appartient à $\mathcal{M}$ et donc, par définition de m, $m \leq m'$. □

Propriétés

- Pour tous $a,\ b \in \mathbb{Z}$, $\text{ppcm}(a, b) = \text{ppcm}(b, a)$.
- Pour tout $a \in \mathbb{Z}$, $\text{ppcm}(0, a) = 0$.
- ~~Pour tout $a \in \mathbb{Z}$, $\text{ppcm}(0, a) = \mid a \mid$.~~

Proposition

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

Alors $ab = \text{pgcd}(a, b) \times \text{ppcm}(a, b)$.

Démonstration

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

Supposons l'un de a et de b au moins est nul. On suppose que $a = 0$. Donc $ab = 0$. On sait aussi que $\text{ppcm}(0, b) = 0$ donc $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = 0 = ab$.

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

On pose $d = \text{pgcd}(a, b)$. $d \neq 0$ puisque $a,\ b \in \mathbb{Z}^*$. On pose $q = \frac{a}{d}$ et $q' = \frac{b}{d}$, i.e. $a = dq$ et $b = dq'$.

$d = \text{pgcd}(a, b) = \text{pgcd}(dq, dq') = d \times \text{pgcd}(q, q')$ donc $\text{pgcd}(q, q') = 1$.

Posons $m = qdq'$. Donc $dm = dqdq' = ab$. De plus, $m = aq'$ et $m = qb$. $a \mid m$ et $b \mid m$ donc $\text{ppcm}(a, b) \leq m$.

Soit ℓ un multiple de a et de b strictement positif. On pose $k = \frac{\ell}{a}$ et $k' = \frac{\ell}{b}$. On a $\ell = ak = bk'$, donc $kqd = k'dq'$.

Comme $d \neq 0$, on a $kq = k'q'$. Donc $q \mid k'q'$ et $q' \mid kq$. Or $\text{pgcd}(q, q') = 1$ donc d'après le lemme de Gauss, $q \mid k'$ et $q' \mid k$.

Donc $m = bq \mid bk' = \ell$ donc $m \leq \ell$. Donc en particulier, comme $\text{ppcm}(a, b)$ est un multiple de a et de b, $m \leq \text{ppcm}(a, b)$.

Donc $m = \text{ppcm}(a, b)$. □

Corollaire

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

a et b sont premiers entre eux si et seulement si $\text{ppcm}(a, b) = ab$.

III. Nombres premiers

Définition

Un entier $p \geq 2$ est dit *premier* lorsqu'il possède pour seuls diviseurs positifs 1 et lui-même.

Exemples

3 est un nombre premier puisque les seuls entiers positifs qui le divisent sont 1 et 3. Néanmoins, on remarque que 3 admet quatre diviseurs $\{-3, -1, 1, 3\}$. 4 n'est pas un nombre premier puisque 2 le divise.

Proposition

Soit n un entier et soit p un nombre premier. Alors soit p divise n soit n et p sont premiers entre eux.

Démonstration

Soit n un entier et soit p un nombre premier. On pose $d = \text{pgcd}(n, p)$.
Donc d est un diviseur positif de p donc $d = 1$ ou $d = p$. Si $d = 1$, alors $\text{pgcd}(n, p) = 1$, i.e. n et p sont premiers entre eux. Si $d = p$ alors $\text{pgcd}(n, p) = p$ et donc p divise n. □

Proposition

Tout nombre entier $n \geq 2$ admet un diviseur premier.

Démonstration

Démontrons cette proposition par récurrence forte.
Initialisation : 2 est un nombre premier et il se divise lui-même donc 2 admet un diviseur premier.
Hérédité : Soit $n \geq 2$ un entier. On suppose que, pour tout entier k tel que $2 \leq k \leq n$, k admet un diviseur premier.
Montrons que $n + 1$ admet un diviseur premier.
Si $n+1$ est un nombre premier, alors $n+1$ se divise lui-même et donc $n+1$ admet un diviseur premier.
Si $n + 1$ n'est pas un nombre premier donc il existe un entier positif r tel que $1 < r < n + 1$ et r divise $n + 1$. Comme $1 < r < n + 1$, donc $2 \leq r \leq n$ et donc par hypothèse de récurrence, r admet un diviseur premier p. Or comme r divise $n + 1$ et que p divise r, donc p divise $n + 1$ et donc $n + 1$ admet p comme diviseur premier.

Ainsi par récurrence, on a démontré que tout nombre entier $n \geq 2$ admet un diviseur premier.

Théorème

Il existe une infinité de nombres premiers.

Démonstration

Démontrons ce théorème par l'absurde.
Supposons qu'il n'existe qu'un nombre fini de nombres premiers. Comme 2 est un nombre premier, le nombre r de nombres premiers est supérieur ou égal à 1.
Soit $\{p_1, p_2, , \ldots, p_r\}$ l'ensemble des r nombres premiers distincts. On pose $m = \prod_{i=1}^{r} p_i + 1$..
m est par définition un nombre entier naturel et donc il admet, d'après la proposition précédente, un diviseur premier. Comme il n'existe qu'un nombre fini de nombres premiers, il existe i_0 tel que p_{i_0} divise m. Donc il existe $k \in \mathbb{Z}$ tel que $m = p_{i_0} k$. Donc $m = p_{i_0} k = \prod_{i=1}^{r} p_i + 1$ soit $p_{i_0} k - \prod_{i=1}^{r} p_i = 1$ et donc

$$p_{i_0} \left(k - \prod_{1 \leq i \leq r, i \neq i_0} p_i \right) = 1$$

Donc p_{i_0} divise 1 , ce qui est impossible parce que p_{i_0} est un nombre premier donc un entier supérieur strictement à 1.

Il existe donc une infinité de nombres premiers.

Lemme Lemme d'Euclide

Soient a et b deux entiers et soit p un nombre premier.
Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

Démonstration

Soient a et b deux entiers et soit p un nombre premier.
Supposons $p \mid ab$. Si $p \nmid a$ alors a et p sont premiers entre eux. D'après le lemme de Gauss, $p \mid b$. Autrement $p \mid a$.

Lemme Contraposée du lemme d'Euclide

Soient a et b deux entiers et soit p un nombre premier.
Si p ne divise pas a et p ne divise pas b, alors p ne divise pas ab.

Théorème Décomposition en facteurs premiers

Soit $n \geq 2$ un entier. Il existe un unique entier $r \geq 1$ et des nombres premiers uniques $p_1 \geq p_2 \geq \ldots \geq p_r$ tel que $n = \prod_{i=1}^{r} p_i$.

Démonstration

Existence :
Démonstration par récurrence : Soit $n \geq 2$ un entier. On pose P_n la proposition "pour tout entier k compris entre 2 et n, k admet une décomposition en facteurs premiers."
Pour $n = 2$: pour k compris entre 2 et 2, $k = 2$. k admet une décomposition en facteurs premiers évidente : $k = p_1 = 2$.
Hérédité : Soit $n \geq 2$ un entier. Supposons P_n. Soit k compris entre 2 et $n+1$. Alors soit k est compris entre 2 et n, et par hypothèse de récurrence k admet une décomposition en facteurs premiers, soit $k = n + 1$.
Supposons $k = n+1$. Comme $n \geq 2$, $k \geq 3$ donc d'après l'un des résultats précédents, k admet un facteur premier p. Si $p = n + 1$, alors $k = n + 1 = p$ est sa décomposition en facteurs premiers. Si $p \neq n + 1$, alors il existe k' entier naturel tel que $k = n + 1 = pk'$. Comme $p \geq 2$ donc $n + 1 = pk' \geq 2k' = k' + k' > k'$ donc k' est compris entre 2 et n et donc k' admet une décomposition en facteurs premiers.
On pose $k' = \prod_{i=1}^{r'} p'_i$ avec $p'_1 \geq p'_2 \geq \ldots \geq p'_{r'}$. Donc $n + 1 = pk' = p \prod_{i=1}^{r'} p'_i$.
On pose $s = r'+1$, on classe p dans la liste des p'_i et on les nomme q_i. On a donc $n+1 = \prod_{i=1}^{s} q_i$.
Unicité :

Soit $n \geq 2$ un entier. On pose Q_n la proposition "pour tout entier k compris entre 2 et n, la décomposition en facteurs premiers de k est unique."
Pour $n = 2$: pour k compris entre 2 et 2, $k = 2$. Soit p un diviseur premier de k. Donc $p \leq k = 2$ et $p \geq 2$ par définition d'un nombre premier, donc $p = 2$. Donc une décomposition en facteurs premiers de 2 est 2^r avec $r \geq 1$. Mais si $r > 1$, $2^r = 2 \times 2^{r-1} > 2$, ce qui est impossible. Donc $k = 2 = p$ est l'unique décomposition en facteurs premiers de 2.
Hérédité : Soit $n \geq 2$ un entier. Supposons Q_n. Soit k compris entre 2 et $n + 1$. Alors soit k est compris entre 2 et n, et par hypothèse de récurrence k admet une unique décomposition en facteurs premiers, soit $k = n + 1$.
Supposons $k = n + 1$. Supposons que k admet deux décompositions en facteurs premiers :

$$n + 1 = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s.$$

Supposons par l'absurde que $p_1 < q_1$. Alors pout tout i entier tel que $1 \geq i \geq s$, $p_1 < q_1 \leq q_i$. Comme $p_1 > 1$ par définition d'un nombre premier, p_1 ne divise aucun des nombres premiers q_i, et donc par la contraposée du lemme d'Euclide p_1 ne divise pas $n+1$: impossible. De même

si $q_1 < p1$, q_1 ne divise pas $n+1$: impossible.
Donc $p_1 = q_1$. Soit n' l'entier tel que $n+1 = p_1 n'$.
Si $n' = 1$ Alors $r = s = 1$ et la décomposition en facteurs premiers de $n+1$ est unique et égale à $n+1 = p_1$.
Si $n' \geq 2$, alors $n+1 = pn' \geq 2n' > n'$ donc $2 \leq n' \leq n$, alors par hypothèse de récurrence, n' admet une unique décomposition en facteurs premiers. On sait aussi par définition de n' que $n' = p_2 \dots p_r = q_2 \dots q_s$. Donc $r = s$ et pour tout $2 \leq i \leq r$, $p_i = q_i$. Donc $n+1$ admet une unique décomposition en facteurs premiers.

IV. Résolution d'équations

1. Équations diophantiennes

Soient a, b et c des entiers tels que a et b sont non nuls.
On cherche à résoudre dans $\mathbb{Z}$ l'équation (E) $ax+by = c$ d'inconnues x et y. Une telle équation est appelée *équation diophantienne*.

On va décrire une méthode de résolution de ce type d'équations en trois étapes.

Étape 1 : Calcul de $d = \text{pgcd}(a, b)$.
Par définition a et b sont non nuls, donc $d \neq 0$ **Si** $d \not| c$ **alors** $ax+by = c$ **n'a pas de solutions.**

Démonstration

Par définition, $d \mid a$ et $d \mid b$ donc $d \mid ax$ et $d \mid by$ et donc $d \mid ax + by = c$.

On suppose à partir de l'étape suivante que $d \mid c$ donc qu'il existe $m \in \mathbb{Z}$ tel que $c = dm$.
Étape 2 : Calcul d'une identité de Bézout entre a et b.
Grâce à l'algorithme d'Euclide étendu, on détermine deux entiers u et v tels que $au + bv = d = \text{pgcd}(a, b)$. Alors

$$a(um) + b(vm) = dm = c.$$

On pose $x_0 = um$ et $y_0 = vm$, alors $ax_0 + by_0 = c$.
Donc si $d \mid c$ **alors** (E) **admet au moins le couple** $(x_0,\ y_0)$ **comme solution**.

Étape 3 : Détermination de l'ensemble des solutions de (E).
On suppose connus $d = \text{pgcd}(a, b)$ et $(x_0,\ y_0)$ une solution particulière de (E), i.e. $ax_0+by_0 = c$.
On pose a' et b' tels que $a = da'$ et $b = db'$.
Alors l'ensemble des solutions de (E) **est** $S = \{(x_0 + kb',\ y_0 - ka') \mid k \in \mathbb{Z}\}$**.**

Démonstration

Comme $d = \text{pgcd}(a,\ b) = \text{pgcd}(da',\ db') = d\,\text{pgcd}(a',\ b')$, alors $\text{pgcd}(a',\ b') = 1$.
Soit $(x,\ y) \in \mathbb{Z}^2$. $(x,\ y)$ est une solution de (E) si et seulement si $ax + by = c = ax_0 + by_0$.
Mais $ax + by = ax_0 + by_0$ si et seulement si $a(x - x0) = b(y_0 - y)$ i.e. $da'(x - x0) = db'(y_0 - y)$.
Comme $d \neq 0$, $ax + by = ax_0 + by_0$ si et seulement si $a'(x - x0) = b'(y_0 - y)$. Ainsi si $(x,\ y)$ est une solution de (E), alors $a' \mid b'(y_0 - y)$ et comme $\text{pgcd}(a',\ b') = 1$, d'après le lemme de Gauss, $a' \mid (y_0 - y)$ donc il existe $\ell_1 \in \mathbb{Z}$ tel que $y = y_0 - \ell_1 a'$. De même, comme $b' \mid a'(x - x_0)$, on a $b' \mid (x - x_0)$ donc il existe $\ell_2 \in \mathbb{Z}$ tel que $x = x_0 + \ell_2 b'$.
Donc $a'(x - x_0) = b'(y_0 - y)$ s'écrit $a'b'\ell_2 = b'a'\ell_1$. Comme $a',\ b' \in \mathbb{Z}^*$, $a'b' \neq 0$ donc $\ell_2 = \ell_1$.
Donc si $(x,\ y)$ est une solution de (E) alors il existe $k \in \mathbb{Z}$ tel que $x = x_0 + kb'$ et $y = y_0 - ka'$.
Donc toute solution de (E) est un élément de S/
Inversement, soit $k \in \mathbb{Z}$. On pose $x = x_0 + kb'$ et $y = y_0 - ka'$. Alors $ax + by = a(x_0 + kb') + b(y_0 - ka') = ax_0 + by_0 + ab'k - ba'k = c + da'b'k - db'a'k = c$. Donc tout élément de S est une solution de (E). □

2. Équations modulaires

Soient a, b et c des entiers tels que a et b sont non nuls.
On cherche à résoudre l'équation (E') $ax \equiv c \mod b$ d'inconnue x. Une telle équation est appelée *équation modulaire*.

On remarque que $ax \equiv c \mod b$ si et seulement si $b \mid ax - c$ si et seulement si il existe $y \in \mathbb{Z}$ tel que $ax - c = by$ i.e. $ax + b(-y) = c$. Résoudre l'équation (E') est équivalent à résoudre l'équation diophantienne $ax + b(-y) = c$. On reprend donc la méthode de résolution vue dans la section précédente.

Étape 1 : Calcul de $d = \text{pgcd}(a, b)$.
Si $d \not| c$ **alors** $ax \equiv c \mod b$ **n'a pas de solutions.**

On suppose à partir de l'étape suivante que $d \mid c$ donc qu'il existe $m \in \mathbb{Z}$ tel que $c = dm$.
Étape 2 : Calcul d'une identité de Bézout entre a et b.
Grâce à l'algorithme d'Euclide étendu, on détermine deux entiers u et v tels que $au + bv = d$. Alors

$$a(um) \equiv c \mod b.$$

Donc si $d \mid c$ **alors** (E') **admet au moins** $x_0 = um$ **comme solution.**

Étape 3 : Détermination de l'ensemble des solutions de (E').
On suppose connus $d = \text{pgcd}(a, b)$ et $(x_0,\ y_0)$ une solution particulière de (E), i.e. $ax_0 + by_0 = c$. On pose b' tel que $b = db'$.
Alors l'ensemble des solutions de (E') **est** $S' = \{x_0 + kb' \mid k \in \mathbb{Z}\}$**.**