Chapitre 12

Arithmétique dans $\mathbb{Z}$

I Divisibilité

1. Généralités

Définition - Multiples, diviseurs

Soient $a, b \in \mathbb{Z}$. On dit que a divise b et on note $a \mid b$ s'il existe un entier $k \in \mathbb{Z}$ tel que $b = ka$. On dit alors que b est un *multiple* de a et a est un *diviseur* de b.

On note $a\mathbb{Z} = \{ka,\ k \in \mathbb{Z}\}$ les multiples de a.

Théorème - Propriétés de la relation de divisibilité

i. La relation de divisibilité est une relation d'ordre sur $\mathbb{N}$.

ii. Si $a \mid b$ et $a \mid c$, alors pour tous $u, v \in \mathbb{Z}$, $a \mid bu + cv$.

iii. Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$, et en particulier, $a^k \mid b^k$ pour tout $k \in \mathbb{N}$.

iv. Si $m \neq 0$, alors $a \mid b \iff ma \mid mb$.

Démonstration.

i. Nous avons déjà montré ce résultat dans le chapitre Applications et relations binaires.

ii. Soient $k, l \in \mathbb{Z}$ tels que $b = ka$ et $c = la$. Si $u, v \in \mathbb{Z}$, alors on a $bu + cv = (ku + lv)a$, donc $a \mid bu + cv$.

iii. Soient $k, l \in \mathbb{Z}$ tels que $b = ka$ et $d = lc$. Alors, on a $bd = kl\,ac$, donc $ac \mid bd$.

iv. Le sens direct est immédiat. S'il existe $k \in \mathbb{Z}$ tel que $mb = k\,ma$, alors en divisant par m, on a $b = ka$. □

Remarque. La relation de divisibilité n'est pas une relation d'ordre sur $\mathbb{Z}$, car elle n'est pas antisymétrique : si $a, b \in \mathbb{Z}$, on a $a \mid b$ et $b \mid a \iff |a| = |b| \iff a = \pm b$.

2. Division euclidienne

Théorème - Division euclidienne

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

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

Une telle écriture est appelée *division euclidienne* de a par b, et on appelle q le *quotient* et r le *reste* de la division euclidienne.

Remarques.

- Si q est le quotient dans la division euclidienne de a par b, alors $q = \left\lfloor \frac{a}{b} \right\rfloor$.
- On peut étendre ce résultat au cas où $b \in \mathbb{Z}^\star$: il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leqslant r < |b|$.

Démonstration.

- *Existence.* On suppose $a \geqslant 0$, et on considère l'ensemble $A = \{k \in \mathbb{N},\ a - kb \geqslant 0\}$. Si $k \in A$, on a $k \leqslant kb \leqslant a$, donc A est majoré par a. Ainsi, A possède un plus grand élément, qu'on note q. Par ailleurs, on a $a-(q+1)b < 0$, donc $a - bq < b$. Comme on a aussi $a - bq \geqslant 0$, on obtient le résultat en posant $r = a - bq$.
  Si $a < 0$, on raisonne de la même manière en considérant $m = \min\{k \in \mathbb{N},\ a + kb \geqslant 0\}$, et on pose $q = -m$. On a alors $a - bq \geqslant 0$ et comme $a + (m-1)b < 0$, on a $a - bq < b$.

  Unicité. Supposons qu'il existe deux couples (q_1, r_1) et (q_2, r_2) comme dans l'énoncé. Alors $bq_1 + r_1 = bq_2 + r_2$, donc $b(q_1 - q_2) = r_2 - r_1$. Comme $r_1, r_2 \in [\![0, b[\![$, on a $-b < r_2 - r_1 < b$, d'où $-1 < q_2 - q_1 < 1$. Par conséquent, l'entier $q_1 - q_2$ est nul, ce qui donne $q_1 = q_2$, puis $r_1 = r_2$. □

Remarque. On peut généraliser le résultat de la division euclidienne au cas où $b \in \mathbb{Z}^\star$, de la manière suivante : il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leqslant r < |b|$.

Corollaire - Caractérisation de la divisibilité dans $\mathbb{Z}$

Si $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^\star$, alors $b \mid a$ si et seulement si le reste dans la division euclidienne de a par b est nul.

Démonstration. Par unité du quotient et du reste dans la division euclidienne, le reste dans la division euclidienne de a par b est nul si et seulement s'il existe $q \in \mathbb{Z}$ tel que $a = bq$, c'est-à-dire si et seulement si $b \mid a$. □

3. Congruences

Définition - Congruence modulo un entier

Soient $a, b, n \in \mathbb{Z}$. On dit que a est *congru* à b *modulo* n s'il existe un entier $k \in \mathbb{Z}$ tel que $a = kn + b$, autrement dit : n divise $a - b$. On note alors $a \equiv b\ [n]$.

Remarques.

- Si $a, n \in \mathbb{Z}$, on a : $n \mid a \iff a \equiv 0\ [n]$.
- Si $a \in \mathbb{Z}$ et $n \in \mathbb{N}^\star$, le reste r dans la division euclidienne de a par n est l'unique entier de $[\![0, n-1]\!]$ tel que $a \equiv r\ [n]$.

Théorème - Compatibilité avec les opérations

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

(i) Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $a + a' \equiv b + b'\ [n]$.
(ii) Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $aa' \equiv bb'\ [n]$. En particulier, $a^k \equiv b^k\ [n]$ pour tout $k \in \mathbb{N}$.
(iii) Si $m \neq 0$, alors $a \equiv b\ [n]$ si et seulement si $ma \equiv mb\ [mn]$.

Démonstration.

- (i) et (ii). Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, on considère $k, l \in \mathbb{Z}$ tels que $a = kb + n$ et $a' = lb + n$. On a alors $a + a' = (k + l)b + n$ donc $a + a' \equiv b + b'\ [n]$, et $aa' = (kln + kb' + lb)n + bb'$, donc $aa' \equiv bb'\ [n]$.
- (iii). Le sens direct est clair, la réciproque s'obtient en divisant l'égalité $ma = kmb + mn$ pour un entier $k \in \mathbb{Z}$ par m qui est non nul. □

Exemple. Pour tout $n \in \mathbb{N}$, 7 divise $2^{3n} - 1$.

On remarque que $2^3 \equiv 1\ [7]$. Ainsi, pour tout $n \in \mathbb{N}$, on obtient en élevant à la puissance n que $2^{3n} \equiv 1 \equiv\ [7]$, c'est-à-dire $2^{3n} - 1 \equiv 0\ [7]$.

Théorème

La relation de congruence modulo un entier est une relation d'équivalence sur $\mathbb{Z}$.

Démonstration. Si $n \in \mathbb{N}$ et $a, b, c \in \mathbb{Z}$, on a pour commencer, si $a \equiv b\ [n]$, il existe $k \in \mathbb{Z}$ tel que $a = kn + b$, donc $b = -kn + a$ et $b \equiv a\ [n]$, donc $\equiv$ est symétrique. Ensuite, $a = 0\,n + a$, donc $a \equiv a\ [n]$, et $\equiv$ est réflexive. Par ailleurs, si $a \equiv b\ [n]$ et $b \equiv c\ [n]$, il existe $k, l \in \mathbb{Z}$ tels que $a = kn + b$ et $b = ln + c$, donc $a = (k + l)n + c$, donc $a \equiv c\ [n]$, donc $\equiv$ est transitive. □

4. Nombres premiers

Définition - Nombre premier

On dit qu'un entier $p \geqslant 2$ est *premier* si ses seuls diviseurs positifs sont 1 et p. Si $p \geqslant 2$ n'est pas premier, on dit qu'il est *composé*. On note $\mathscr{P}$ l'ensemble des nombres premiers.

Exemple. Les entiers $2, 3, 5, 7, 11, 13, 17, 19, 23$ sont premiers.

Remarque. Un entier $n \geqslant 2$ est composé si et seulement s'il possède un diviseur $d \in [\![2, n-1]\!]$.

Théorème - Factorisation première (existence)

Tout nombre entier $n \geqslant 2$ est un produit de facteurs premiers.

Démonstration. Montrons par récurrence forte que tout entier $n \geqslant 2$ est un produit de facteurs premiers.

- *Initialisation.* 2 est premier, donc un produit d'un seul facteur premier.
- *Hérédité.* Soit $n \geqslant 2$. On suppose que tout entier $k \in [\![2, n]\!]$ est un produit de facteurs premiers, et on considère l'entier $n+1$. Soit $n+1$ est premier, donc produit d'un seul facteur premier, soit il ne l'est pas, et s'écrit donc $n+1 = ab$ avec $a, b \in [\![2, n]\!]$. Par hypothèse de récurrence, les entiers a et b s'écrivent comme facteurs de nombres premiers, donc $n+1 = ab$ également, ce qui conclut. □

Remarque. Il y a aussi unicité de cette décomposition en produits de facteurs premiers, à ordre près des facteurs. Nous démontrerons ce résultat plus loin dans ce chapitre.

Théorème - $\mathscr{P}$ est infini

Il existe une infinité de nombres premiers.

Démonstration. Supposons qu'il existe un nombre fini r de nombres premiers, qu'on écrit $p_1, \ldots, p_r$. On considère alors l'entier $n = p_1 \ldots p_r + 1$. Comme n n'est pas premier, il possède un diviseur premier, qui est p_i pour un certain $i \in [\![1, r]\!]$. Par conséquent, p_i divise $n - p_1 \ldots p_r$, ce qui entraîne que $p_i \mid 1$, ce qui est contradictoire. □

Théorème

Si un entier $n \geqslant 2$ n'est pas premier, alors il possède un diviseur premier $p \leqslant \sqrt{n}$.

Démonstration. Soit $n \geqslant 2$ non premier. On sait que n admet un diviseur premier p. Si $p \leqslant \sqrt{n}$, alors le résultat est prouvé. Sinon, on peut écrire $n = pk$ avec $k < \sqrt{n}$. L'entier k possède lui aussi un diviseur premier q qui vérifie $q \leqslant k < \sqrt{n}$. Comme q est aussi un diviseur de n, ceci conclut. □

Le résultat ci-dessus permet d'obtenir un procédé algorithmique pour trouver tous les nombres premiers inférieurs à un entier donné.

Crible d'Ératosthène. Pour obtenir tous les nombres premiers inférieurs à un entier donné n, on peut procéder de la manière suivante.

- On commence par 2 dont on sait qu'il est premier, et on élimine tous les entiers de $[\![2, n]\!]$ qui sont multiples de 2, et ne sont donc pas premiers.
- On s'intéresse au premier entier non éliminé, qu'on identifie comme étant premier (il n'a pas de diviseur premier qui lui est strictement inférieur), et on élimine tous ses multiples dans $[\![2, n]\!]$.
- On répète ainsi l'opération tant qu'on considère les multiples d'entiers k tels que $k \leqslant \sqrt{n}$.

On aura alors sélectionné tous les nombres premiers de $[\![2, n]\!]$ car on a vu que tout nombre composé de cet ensemble possède un diviseur premier inférieur à $\sqrt{n}$. Le tableau ci-dessous donne l'exemple du cas $n = 100$.

	2	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

II Plus grand diviseur commun, plus petit multiple commun

1. PGCD de deux entiers

Dans la suite, on note D_a l'ensemble des diviseurs d'un entier $a \in \mathbb{Z}$.

Remarques.

- Pour tout $a \in \mathbb{Z}$, $1 \in D_a$ et $-1 \in D_a$.
- Si $a \neq 0$, alors D_a est majoré par $|a|$: pour tout $k \in D_a$, il existe $d \in \mathbb{Z}^\star$ tel que $a = kd$, on a donc $|k| \leqslant |kd| = |a|$.
- On a $D_1 = \{-1, 1\}$ et $D_0 = \mathbb{Z}$.

Définition-théorème - PGCD

Si $a, b \in \mathbb{Z}$ ne sont pas tous deux nuls, l'ensemble $D_a \cap D_b$ des diviseurs communs à a et b admet un plus grand élément appelé PGCD de a et b, qu'on note $a \wedge b$. En d'autres termes, $a \wedge b = \max(D_a \cap D_b)$.

On convient par ailleurs que $0 \wedge 0 = 0$.

Démonstration. Si $a \neq 0$, l'ensemble $D_a \cap D_b$ est majoré par $|a|$ car D_a l'est. Il est par ailleurs non vide car il contient 1, donc admet un plus grand élément. Si $a = 0$, alors $b \neq 0$ et $D_a \cap D_b$ est majoré par $|b|$ donc la situation est similaire. □

Exemples.
- Si $a \in \mathbb{Z}$, on a $a \wedge 1 = 1$ et $a \wedge 0 = |a|$, du fait que $D_a \cap D_1 = D_1$, et $D_a \cap D_0 = D_a$.
- Si $a, b \in \mathbb{Z}$, on a $a \wedge b = |a| \wedge |b|$.
- Si $a \in \mathbb{Z}$ et d est un diviseur positif de a, alors $a \wedge d = d$: comme $D_d \subset D_a$, on a $D_a \cap D_d = D_d$.

Théorème - PGCD d'un entier avec un nombre premier

Soient $a \in \mathbb{Z}$ et p un nombre premier. Alors :
- soit $p \mid a$ et $a \wedge p = p$,
- soit $p \nmid a$ et $a \wedge p = 1$.

Démonstration. Si $p \mid a$, alors $a \wedge p = p$ d'après ce qui précède. Si maintenant $p \nmid a$, comme $D_p = \{-p, -1, 1, p\}$, on a $D_a \cap D_p = \{-1, 1\}$, donc $a \wedge p = 1$. □

Théorème

Si $a, b, r \in \mathbb{Z}$ et $a \equiv r\ [b]$, alors $D_a \cap D_b = D_b \cap D_r$, et donc $a \wedge b = b \wedge r$.

Démonstration. On peut écrire $a = bq + r$, où $q \in \mathbb{Z}$. Ainsi, si d divise b et r, alors d divise a, ce qui donne $D_b \cap D_r \subset D_a \cap D_b$. L'autre inclusion est obtenue de la même manière : si d divise a et b, alors d divise $r = a - bq$. □

Le résultat ci-dessus justifie l'utilisation de l'algorithme d'Euclide détaillé ci-dessous pour calculer le PGCD de deux entiers.

Algorithme d'Euclide pour le calcul du PGCD.

Si $a, b \in \mathbb{N}$, on note $r_0 = a$ et $r_1 = b$, et on effectue la procédure suivante.

Pour $k \in \mathbb{N}^\star$:

- Si $r_k \neq 0$: on effectue la division euclidienne de r_{k-1} par r_k, et on note r_{k+1} son reste. On a alors $r_{k-1} \equiv r_{k+1}\ [r_k]$, ce qui entraîne que $r_{k+1} < r_k$, et $r_k \wedge r_{k-1} = r_{k+1} \wedge r_k$.
- Si $r_k = 0$, la procédure s'arrête, et $a \wedge b = r_{k-1}$.

Ainsi, $a \wedge b$ est le *dernier reste non nul* de la famille des restes successifs de l'algorithme d'Euclide.

Cas où $a, b \in \mathbb{Z}$: comme $a \wedge b = |a| \wedge |b|$, on se ramène au cas précédent.

Remarques.

- La propriété $r_{k+1} < r_k$ si $r_k \neq 0$, assure l'existence d'un entier k_0 tel que $r_{k_0} = 0$. En d'autres termes, l'algorithme s'arrête.

– Comme, $r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$ pour tout k, on a par récurrence immédiate que $r_{k-1} \wedge r_k = r_0 \wedge r_1 = a \wedge b$. Ainsi,
$$a \wedge b = r_{k_0-1} \wedge r_{k_0} = r_{k_0-1},$$
car $r_{k_0} = 0$. En d'autres termes, l'algorithme fournit le bon résultat. On dit que "$a \wedge b = r_{k-1} \wedge r_k$" est un invariant de boucle.

Exemple. Calcul du PGCD de 660 et 126 :

On a $660 \wedge 126 = 6$:
$$\begin{aligned} 660 &= 126 \times 5 + 30 \\ 126 &= 30 \times 4 + \boxed{6} \\ 30 &= 6 \times 5 + 0 \end{aligned}$$

L'algorithme peut s'écrire de la manière suivante en PYTHON.

Algorithme d'Euclide.

```python
def pgcd(a,b):
    while (b!=0):
        a,b = b,a%b
    return a
```

Une conséquence du résultat ci-dessus est que les diviseurs communs à a et b sont exactement les diviseurs de $a \wedge b$, ce qu'exprime le théorème suivant.

Théorème

Si $a, b \in \mathbb{Z}$ et $d = a \wedge b$, alors $D_a \cap D_b = D_d$.

Démonstration. En reprenant les notations de l'algorithme d'Euclide, on a $r_{k-1} \equiv r_{k+1}\ [r_k]$ pour tout k. Ainsi, nous avons vu que $D_{r_{k-1}} \cap D_{r_k} = D_{r_k} \cap D_{r_{k+1}}$. Une récurrence immédiate montre alors que
$$D_a \cap D_b = D_{r_{k_0}-1} \cap D_{r_{k_0}} = D_{r_{k_0}-1},$$
où k_0 est l'entier tel que $r_{k_0} = 0$. Comme $d = r_{k_0} - 1$, ceci conclut. □

Remarque. On retiendra que si $d \mid a$ et $d \mid b$, alors $d \mid a \wedge b$.

Théorème - Factorisation du PGCD

Si $a, b, k \in \mathbb{Z}$, alors $(ka) \wedge (kb) = |k|\, a \wedge b$.

Démonstration. Le cas $k = 0$ étant clair, on suppose que $k \neq 0$.

– On remarque que $|k| a \wedge b$ divise ka et kb, donc on sait que $|k| a \wedge b$ divise $(ka) \wedge (kb)$.
– Comme k divise ka et kb, on en déduit que k divise $(ka) \wedge (kb)$: il existe $d \in \mathbb{Z}$ tel que $(ka) \wedge (kb) = kd$. Ainsi, comme kd divise ka et kb et $k \neq 0$, on déduit que $d \mid a$ et $d \mid b$, donc $d \mid a \wedge b$. Finalement, kd divise $|k| a \wedge b$.

Finalement, $(ka) \wedge (kb)$ et $|k|\, a \wedge b$ sont des entiers naturels qui se divisent mutuellement, ils sont égaux. □

2. Relations de Bézout

Théorème - Relation de Bézout pour deux entiers

Soient $a, b \in \mathbb{Z}$. Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$. Une telle relation est appelée *relation de Bézout*.

Remarque. Le couple (u, v) d'une relation de Bézout n'est pas unique, loin s'en faut ! Par exemple $9 \wedge 6 = 3$, et $3 = 1 \times 9 + (-1) \times 6 = (-5) \times 9 + 8 \times 6$.

Démonstration. On reprend les notations de l'algorithme d'Euclide : $r_0 = a$, $r_1 = b$, et pour tout $k \in \mathbb{N}^\star$ tel que $r_k \neq 0$, on écrit $r_{k-1} = q_{k+1} r_k + r_{k+1}$, division euclidienne de r_{k-1} par r_k. On montre ensuite par récurrence double que pour tout $k \in \mathbb{N}$, il existe $u_k, v_k \in \mathbb{Z}$ tels que $r_k = u_k a + v_k b$.

– *Initialisation* : en posant $u_0 = 1$, $v_0 = 0$, $u_1 = 0$ et $v_1 = 1$, on a bien $r_0 = u_0 a + v_0 b$ et $r_1 = u_1 a + v_1 b$.
– *Hérédité* : soit $k \in \mathbb{N}^\star$, on suppose qu'il existe $u_{k-1}, v_{k-1}, u_k, v_k \in \mathbb{Z}$ tels que $r_{k-1} = u_{k-1}a + v_{k-1}b$ et $r_k = u_k a + v_k b$. Ainsi,

$$r_{k+1} = r_{k-1} - q_{k+1}r_k = (u_{k-1} - q_{k+1}u_k)\, a + (v_{k-1} - q_{k+1}v_k)\, b.$$

On obtient le résultat en posant $u_{k+1} = u_{k-1} - q_{k+1}u_k$ et $v_{k+1} = v_{k-1} - q_{k+1}v_k$.

Comme on sait qu'il existe un entier k_0 tel que $r_{k_0} = 0$ et $a \wedge b = r_{k_0-1}$, on a donc $a \wedge b = u_{k_0-1}a + v_{k_0-1}b$. □

Remarque. La preuve ci-dessus fournit en fait des relations de récurrence permettant de calculer u_k et v_k à chaque étape. En ajoutant ce calcul à l'algorithme d'Euclide, ceci permet d'obtenir en plus une relation de Bézout. Ce nouvel algorithme porte le nom d'algorithme d'Euclide étendu, et peut se schématiser de la manière suivante.

Algorithme d'Euclide étendu.

On peut synthétiser la réalisation de l'algorithme d'Euclide étendu dans un tableau contenant les restes successifs, les quotients, ainsi que les entiers u_k et v_k.

On commence par écrire r_0, r_1 et les premières valeurs u_0, v_0, u_1, v_1, puis on utilise les relations de récurrence.

r_k	q_k	u_k	v_k
a		1	0
b		0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Exemple. Recherche d'une relation de Bézout pour les entiers $a = 323$ et $b = 119$.

◇ $323 = 119 \times 2 + 85$,
◇ $119 = 84 \times 1 + 34$,
◇ $85 = 34 \times 2 + 17$,
◇ $34 = 17 \times 2 + 0$.

On obtient $a \wedge b = 17$, et $17 = 3 \times 323 - 8 \times 119$.

r_k	q_k	u_k	v_k
323		1	0
119		0	1
85	2	1	−2
34	1	−1	3
$\boxed{17}$	2	3	−8

Corollaire

Si $a, b \in \mathbb{Z}$ et $d = a \wedge b$, alors $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

Démonstration. On sait qu'il existe une relation de Bézout $au_0 + bv_0 = d$. Ainsi, $d \in a\mathbb{Z} + b\mathbb{Z}$, donc les multiples de d appartiennent à $a\mathbb{Z} + b\mathbb{Z}$. Autrement dit, $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$.

Si $n \in a\mathbb{Z} + b\mathbb{Z}$, on peut écrire $n = au + bv$ avec $u, v \in \mathbb{Z}$. Comme $d \,|\, a$ et $d \,|\, b$, on a $d \,|\, au + bv$, donc $au + bv \in d\mathbb{Z}$. □

Remarque. La réciproque est vraie : si $d \in \mathbb{N}$ est tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, alors $d = a \wedge b$.

3. PGCD d'une famille finie d'entiers

On peut aisément généraliser la notion de PGCD à un nombre fini d'entiers.

Définition - PGCD d'un nombre fini d'entiers

Soient $a_1, \ldots, a_n \in \mathbb{Z}$ non tous nuls. On appelle PGCD de $a_1, \ldots, a_n$ le plus grand des diviseurs communs de $a_1, \ldots, a_n$, noté $a_1 \wedge \ldots \wedge a_n$. En d'autres termes, $a_1 \wedge \ldots \wedge a_n = \max D_{a_1} \cap \ldots \cap D_{a_n}$.

On convient que $0 \wedge \ldots \wedge 0 = 0$.

Remarques.

– Il découle de la définition que le PGCD est associatif : si $a, b, c \in \mathbb{Z}$, alors $a \wedge b \wedge c = a \wedge (b \wedge c) = (a \wedge b) \wedge c$. Ceci fournit un moyen de calculer le PGCD d'un nombre fini d'entiers en calculant une succession de PGCD de deux entiers.
– De même que pour le cas de deux entiers, on a $D_{a_1} \cap \ldots \cap D_{a_n} = D_{a_1 \wedge \ldots \wedge a_n}$.
– Le résultat de factorisation se généralise : si $a_1, \ldots, a_n, k \in \mathbb{Z}$, alors $(ka_1) \wedge \ldots \wedge (ka_n) = |k| a_1 \wedge \ldots \wedge a_n$.

Théorème - Relation de Bézout pour une famille finie d'entiers

Soient $a_1, \ldots, a_n \in \mathbb{Z}$. Il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que $a_1u_1 + \ldots + a_nu_n = a_1 \wedge \ldots \wedge a_n$. On dit qu'une telle égalité est une *relation de Bézout* de $a_1, \ldots, a_n$.

Exercice 1. Déterminer une relation de Bézout des entiers 4, 6 et 9.

4. PPCM

Définition-théorème - PPCM de deux entiers

Soient $a, b \in \mathbb{Z}^\star$. L'ensemble $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^\star$ admet un plus petit élément, appelé PPCM de a et b. On le note $a \vee b$. En d'autres termes, $a \vee b = \min(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^\star)$.
On convient par ailleurs que $a \vee b = 0$ si $a = 0$ ou $b = 0$.

Démonstration. Si $a, b \in \mathbb{Z}^\star$ sont non nuls, l'ensemble $a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^\star$ contient l'entier ab. En tant que sous-ensemble non vide de $\mathbb{N}^\star$, il admet bien un plus petit élément. □

Théorème

Si $a, b \in \mathbb{Z}$ et $m = a \vee b$, alors $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. En d'autres termes, les multiples communs à a et b sont exactement les multiples de $a \vee b$.

Démonstration. Si l'un des deux entiers a et b est nul, le résultat est clair : $a\mathbb{Z} \cap b\mathbb{Z} = \{0\}$.
Si $a, b \in \mathbb{Z}^\star$, on remarque que comme m est multiple de a et b, tous ses multiples le sont, autrement dit, $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$. Montrons maintenant que $a\mathbb{Z} \cap b\mathbb{Z} \subset m\mathbb{Z}$. On raisonne par l'absurde et on suppose qu'il existe $k \in a\mathbb{Z} \cap b\mathbb{Z}$ tel que $k \notin m\mathbb{Z}$. On écrit alors $k = mq + r$ la division euclidienne de k par m, on a ainsi $r \in [\![1, m-1]\!]$. Comme k et mq sont des éléments de $a\mathbb{Z} \cap b\mathbb{Z}$, on en déduit que $r \in a\mathbb{Z} \cap b\mathbb{Z}$, ce qui est une contradiction car $0 < r < \min(a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^\star)$. □

Remarque. On retiendra que pour tout $n \in \mathbb{Z}$, si $a \mid n$ et $b \mid n$, alors $(a \vee b) \mid n$.

III Nombres premiers entre eux

Définition - Nombres premiers entre eux

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

Remarques.

- Les entiers a et b sont premiers entre eux si et seulement si $D_a \cap D_b = \{-1, 1\}$.
- Les entiers a et b sont premiers entre eux si et seulement s'ils n'ont aucun facteur premier en commun.

Théorème

Soient $a, b \in \mathbb{Z}$ non tous deux nuls et $d = a \wedge b$. Il existe a' et b' premiers entre eux tels que $\begin{cases} a = da' \\ b = db' \end{cases}$

Démonstration. Comme a, b sont non tous deux nuls, on a $d = a \wedge b \neq 0$. On note a', b' les entiers tels que $a = da'$ et $b = db'$. Comme $d = (da') \wedge (db')$, on a $1 = a' \wedge b'$. □

Définition - Nombres premiers entre eux deux à deux – nombres premiers entre eux dans leur ensemble

Soient $a_1, \ldots, a_n \in \mathbb{Z}$.

- On dit que $a_1, \ldots, a_n$ sont *premiers entre eux deux à deux* si pour tous $i, j \in [\![1, n]\!]$ avec $i \neq j$, $a_i \wedge a_j = 1$.
- On dit que $a_1, \ldots, a_n$ sont *premiers entre eux dans leur ensemble* si $a_1 \wedge \ldots \wedge a_n = 1$.

⚠ Si $a_1, \ldots, a_n$ sont premiers entre eux deux à deux, alors ils sont premiers entre eux dans leur ensemble, mais la réciproque est fausse.

Par exemple, les nombres 2, 4 et 5 sont premiers entre eux dans leur ensemble (ils n'ont pas de diviseurs communs autre que 1 et -1), mais ils ne sont pas premiers entre eux deux à deux, car $2 \wedge 4 = 2$.

Théorème - Théorème de Bézout

Soient $a, b \in \mathbb{Z}$. Les entiers a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$.

Démonstration. Si a et b sont premiers entre eux, on sait qu'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b = 1$. Réciproquement, s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$, alors tout diviseur commun de a et b divise 1, ce qui donne $D_a \cap D_b = \{-1, 1\}$, puis $a \wedge b = 1$. □

Exemple. Pour tout $n \in \mathbb{Z}$, les entiers n et $n+1$ sont premiers entre eux : $(n+1) - n = 1$ est une relation de Bézout.

Remarque. Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^\star$. Si $a \wedge n = 1$, alors le théorème de Bézout donne l'existence de $u \in \mathbb{Z}$ tel que $au \equiv 1\ [n]$. On dira que a est inversible modulo n.

Exercice 2. Résoudre dans $\mathbb{Z}$ l'équation $3x \equiv 2\ [7]$.

On a $3 \times 5 - 7 \times 2 = 1$, donc $3 \times 5 \equiv 1\,[7]$ (on a inversé 3 modulo 7). Ainsi,

$$3x \equiv 2\ [7] \iff 5 \times 3x \equiv 5 \times 2\ [7] \iff x \equiv 3\ [7].$$

Les solutions sont donc tous les entiers de la forme $7k + 3$, où $k \in \mathbb{Z}$.

Théorème - Lemme de Gauss, lemme d'Euclide

- *Lemme de Gauss.* Soient $a, b, c \in \mathbb{Z}$. Si $a \,|\, bc$ et $a \wedge b = 1$, alors $a \,|\, c$.
- *Lemme d'Euclide.* Soient $a, b \in \mathbb{Z}$ et p un nombre premier. Si $p \,|\, ab$, alors $p \,|\, a$ ou $p \,|\, b$.

Démonstration.

- Par hypothèse, il existe $k \in \mathbb{Z}$ tel que $bc = ka$, et on une relation de Bézout : $au + bv = 1$ avec $u, v \in \mathbb{Z}$. En multipliant par c, on obtient $acu + bcv = c$, donc $acu + kav = c$, soit $a(cu + kv) = c$, donc $a \,|\, c$.
- Comme p est premier, si $p \nmid a$, alors $p \wedge a = 1$. On peut donc appliquer le lemme de Gauss : comme $p \,|\, ab$, on a $p \,|\, b$. □

Remarque. Une conséquence du lemme de Gauss est que si $ma \equiv mb\ [c]$ et $m \wedge c = 1$, alors $a \equiv b\ [c]$. En effet $ma \equiv mb\ [c]$ se récrit $c \,|\, m(a - b)$. Si $m \wedge c = 1$, alors $c \,|\, a - b$, autrement dit $a \equiv b\ [c]$.

Alternativement, on peut aussi voir le résultat en remarquant que comme $m \wedge c = 1$, il existe un inverse u de m modulo c. Ainsi $mu\,a \equiv mu\,b\,[c]$, *i.e.* $a \equiv b\,[c]$.

Théorème

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

(i) Si $a \wedge n = 1$ et $b \wedge n = 1$, alors $ab \wedge n = 1$.

(ii) Si $a \wedge b = 1$, $\ a \,|\, n$ et $b \,|\, n$, alors $ab \,|\, n$.

Démonstration.

(i) Raisonnons par l'absurde et supposons que ab et n ont un facteur premier p commun. Alors $p \,|\, ab$ donc, par le lemme d'Euclide, soit $p \,|\, a$, soit $p \,|\, b$. Dans le premier cas, $p \in D_a \cap D_n$, ce qui est impossible, et dans le second cas, $p \in D_b \cap D_n$, ce qui est également impossible.

(ii) Par hypothèse, il existe $k, l \in \mathbb{Z}$ tels que $n = ka = lb$. Ainsi, $a \,|\, lb$, et comme $a \wedge b = 1$, le lemme de Gauss entraîne que $a \,|\, l$, c'est-à-dire qu'il existe $m \in \mathbb{Z}$ tel que $l = ma$. Par conséquent, $n = mab$, et $ab \,|\, n$. □

Remarque. Les deux résultats ci-dessus se généralisent aisément au cas d'un nombre fini d'entiers, par des récurrences assez immédiates : pour $a_1, \ldots, a_k, n \in \mathbb{Z}$,

(i) si $a_1 \wedge n = \ldots = a_k \wedge n = 1$, alors $(a_1 \ldots a_k) \wedge n = 1$,

(ii) si $a_1, \ldots, a_k$ premiers entre eux deux à deux, et $a_1 \,|\, n, \ldots, a_k \,|\, n$, alors $a_1 \ldots a_n \,|\, n$.

Exemple. Si p est un nombre premier et $k \in [\![1, p-1]\!]$, alors p divise $\binom{p}{k}$.

Démonstration. On remarque que $k!\binom{p}{k} = p(p-1)\ldots(p-k+1)$, donc p divise $k!\binom{p}{k}$. Comme p est premier et $k < p$, les entiers $i \leqslant k$ sont premiers avec p, donc leur produit également : $k! \wedge p = 1$. Par le lemme de Gauss, on en déduit donc que $p \,|\, \binom{p}{k}$. □

Théorème - Petit théorème de Fermat

Si p est un nombre premier et $n \in \mathbb{Z}$, alors :

i. $n^p \equiv n\ [p]$,

ii. si $p \wedge n = 1$, alors $n^{p-1} \equiv 1\ [p]$.

Démonstration.

i. On monte le résultat pour $n \in \mathbb{N}$ en raisonnant par récurrence.

- Si $n = 0$, on a $n^p = 0$, donc le résultat est vrai.
- Soit $n \in \mathbb{N}$. On suppose que $n^p \equiv n\ [p]$. On a alors

$$(n+1)^p \ = \ n^p + \sum_{k=1}^{p-1} \binom{p}{k} n^k + 1 \ \equiv \ n^p + 1; \equiv \ n+1\ [p],$$

car pour tout $k \in [\![1, p-1]\!]$, on sait que p divise $\binom{p}{k}$, donc $\sum\limits_{k=1}^{p-1} \binom{p}{k} n^k \equiv 0\ [p]$.

Si $n \in \mathbb{Z}$, on a $n \equiv r\ [p]$ avec $r \in [\![0, p-1]\!]$. Comme $r^p \equiv r\ [p]$, on a aussi $n^p \equiv n\ [p]$.

ii. Si de plus $p \wedge n = 1$, alors il existe $u \in \mathbb{Z}$ inverse de n modulo p, c'est-à-dire que $nu \equiv 1\ [p]$, donc en multipliant l'égalité précédente par u, on obtient $n^{p-1} \equiv 1\ [p]$. □

IV Factorisation première

1. Décomposition en produit de facteurs premiers

Théorème - Factorisation première

Si $n \in \mathbb{N}$ avec $n \geqslant 2$, alors n s'écrit de manière unique sous la forme

$$n \ = \ p_1^{\alpha_1} \dots p_r^{\alpha_r},$$

où $p_1, \dots, p_r$ sont des nombres premiers tels que $p_1 < \dots < p_r$ et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^\star$.

Démonstration.

- L'existence a été prouvée plus haut.
- *Unicité.* On suppose que n possède deux décompositions en produits de facteurs premiers comme dans l'énoncé. Quitte à choisir des exposants nuls dans les décompositions, on peut supposer que les facteurs premiers sont les mêmes :

$$n \ = \ p_1^{\alpha_1} \dots p_r^{\alpha_r} \ = \ p_1^{\beta_1} \dots p_r^{\beta_r}, \quad \text{où} \ \ \alpha_1, \dots, \alpha_r,\ \beta_1, \dots, \beta_r \in \mathbb{N}.$$

Soit $i \in [\![1, r]\!]$. On a alors $n \ = \ p_i^{\alpha_i} a \ = \ p_i^{\beta_i} b$, où a et b sont des produits de nombres premiers distincts de p_i, donc premiers avec p_1. Par conséquent, on a $p_i \wedge a = 1$, puis $p_i^{\beta_i} \wedge a = 1$. Le lemme de Gauss donne alors $p_i^{\beta_i} \,|\, p_i^{\alpha_i}$, donc $\beta_i \leqslant \alpha_i$. De même, $p_i^{\alpha_i} \wedge b = 1$, donc $p_i^{\alpha_i} \,|\, p_i^{\beta_i}$, et $\alpha_i \leqslant \beta_i$. Finalement, $\alpha_i = \beta_i$, ce qui conclut. □

2. Valuation p-adique

Définition - Valuation p-adique

Soient p un nombre premier et $n \in \mathbb{Z}^\star$. On appelle *valuation p-adique* de n et on note $v_p(n)$ le plus grand entier $k \in \mathbb{N}$ tel que $p^k \,|\, n$.

Remarque. En d'autres termes, si $p \in \mathscr{P}$ et $n \in \mathbb{N}^\star$, alors $v_p(n)$ est l'exposant de p dans la factorisation première de n (en retenant un exposant nul si p ne divise pas n). On peut écrire la factorisation première de $n \in \mathbb{N}^\star$:

$$n = \prod_{p \in \mathscr{P}} p^{v_p(n)}.$$

On note que le produit est fini, car il existe un nombre fini de nombres premiers p tels que $v_p(n) \neq 0$.

Exemple. Comme $20 = 2^2 \times 5$, on a $v_2(20) = 2$ et $v_5(20) = 1$.

Remarque. Si $n \in \mathbb{Z}$ et $p \in \mathscr{P}$, alors :
- $v_p(n) = \alpha$ si et seulement si n s'écrit $n = p^\alpha n'$, où p ne divise pas n',
- $v_p(n) > 0$ si et seulement si $p \mid n$.

Théorème - Valuation et produit

Si $n, m \in \mathbb{Z}$ et p est un nombre premier, alors $v_p(nm) = v_p(n) + v_p(m)$.

Démonstration. On peut écrire $n = p^{v_p(n)}n'$ et $m = p^{v_p(m)}m'$, où p ne divise ni n' ni m'. Ainsi, on obtient que $nm = p^{v_p(n)+v_p(m)}n'm'$. Par le lemme d'Euclide, p ne divise pas $n'm'$, ce qui assure que $v_p(nm) = v_p(n) + v_p(m)$. ☐

Remarque. Ceci fournit une manière plus directe de présenter la preuve de l'irrationalité de $\sqrt{2}$ rencontrée dans le chapitre Rudiments de logique :

> Supposons que $\sqrt{2} \in \mathbb{Q}$, et notons $\sqrt{2} = \frac{p}{q}$ avec $p, q \in \mathbb{N}^\star$. On a alors $p^2 = 2q^2$, ce qui entraîne que $v_2(p^2) = v_2(2q^2)$, c'est-à-dire $2v_2(p) = 2v_2(q) + 1$, qui entraîne $0 \equiv 1\ [2]$, il y a contradiction.

Théorème - Valuation et divisibilité

Si $a, b \in \mathbb{Z}$, alors $a \mid b$ si et seulement si pour tout $p \in \mathscr{P}$, $v_p(a) \leqslant v_p(b)$.

Démonstration. Si $a \mid b$, il existe $k \in \mathbb{Z}$ tel que $b = ka$. Ainsi, si $p \in \mathscr{P}$, on a $v_p(b) = v_p(k) + v_p(a) \geqslant v_p(a)$. La réciproque est claire en considérant les factorisations premières de a et b. ☐

Remarques.

- Si $n \geqslant 2$ a pour factorisation première $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, alors ses diviseurs positifs sont exactement les entiers de la forme $p_1^{\beta_1} \dots p_r^{\beta_r}$ avec $\beta_i \leqslant \alpha_i$ pour tout $i \in [\![1, r]\!]$.
- On en déduit que le nombre de diviseurs positifs d'un entier $n \in \mathbb{N}^\star$ est donné par
$$\prod_{p \in \mathscr{P}} (v_p(n) + 1).$$
En effet, si la factorisation première de n s'écrit $p_1^{v_{p_1}(n)} \dots p_r^{v_{p_r}(n)}$, il y a autant de diviseurs positifs que de choix de r-uplets d'exposants $(\alpha_1, \dots, \alpha_r)$ avec $\alpha_i \in [\![0, v_{p_i}(n) - 1]\!]$, c'est-à-dire $(v_{p_1}(n) - 1) \dots (v_{p_r}(n) - 1)$.

Théorème - Valuations et PGCD, PPCM

Si $a, b \in \mathbb{Z}^\star$, alors $a \wedge b = \prod\limits_{p \in \mathscr{P}} p^{\min(v_p(a), v_p(b))}$, et $a \vee b = \prod\limits_{p \in \mathscr{P}} p^{\max(v_p(a), v_p(b))}$.

Démonstration. Pour tout $p \in \mathscr{P}$, on note $\alpha_p = v_p(a)$ et $\beta_p = v_p(b)$.

- On considère un entier d dont on note la factorisation première $d = \prod_{p \in \mathscr{P}} p^{\gamma_p}$. On a $d \in D_a \cap D_b$ si et seulement si pour tout $p \in \mathscr{P}$, $\gamma_p \leqslant \alpha_p$ et $\gamma_p \leqslant \beta_p$, c'est-à-dire $\gamma_p \leqslant \min(\alpha_p, \beta_p)$, d'où le résultat.
- De même, si $m \in \mathbb{N}$ a pour factorisation première $m = \prod_{p \in \mathscr{P}} p^{\gamma_p}$, alors $m \in a\mathbb{Z} \cap b\mathbb{Z}$ si et seulement si pour tout $p \in \mathscr{P}$, $\gamma_p \geqslant \alpha_p$ et $\gamma_p \geqslant \beta_p$, c'est-à-dire $\gamma_p \geqslant \max(\alpha_p, \beta_p)$, d'où le résultat. ☐

Corollaire - Produit du PGCD et du PPCM

Si $a, b \in \mathbb{Z}$, $d = a \wedge b$ et $m = a \vee b$, alors $dm = |ab|$.

Démonstration. Si $a = 0$ ou $b = 0$, alors $m = 0$, donc $dm = |ab|$. Si $a, b \in \mathbb{Z}^\star$, il suffit d'utiliser les factorisations premières : $|a| = \prod_{p \in \mathscr{P}} p^{\alpha_p}$ et $|b| = \prod_{p \in \mathscr{P}} p^{\beta_p}$:
$$dm = \prod_{p \in \mathscr{P}} p^{\min(\alpha_p, \beta_p) + \max(\alpha_p, \beta_p)} = \prod_{p \in \mathscr{P}} p^{\alpha_p + \beta_p} = \prod_{p \in \mathscr{P}} p^{\alpha_p} \prod_{p \in \mathscr{P}} p^{\beta_p} = |ab|.$$ ☐

Exemple. On a $300 = 2^2 \times 3 \times 5^2$ et $168 = 2^3 \times 3 \times 7$, donc $300 \wedge 168 = 2^2 \times 3 = 12$, et $300 \vee 168 = 2^3 \times 3 \times 5^2 \times 7 = 4200$.

Remarque. On peut alors trouver le PPCM de deux entiers à partir de leur PGCD.