IX Entiers relatifs et arithmétique de $\mathbb{Z}$

2 décembre 2016

Dans tout ce chapitre, a, b, c, d, m, n, p, q et r sont des entiers relatifs, sauf mention contraire.

1 Divisibilité

1.1 Définition

Définition 1.1.1.
On dit que n *divise* m, que n *est un diviseur de* m ou que m *est un multiple de* n et on note $n|m$ si et seulement s'il existe $k \in \mathbb{Z}$ vérifiant $m = kn$.

Proposition 1.1.2. (i) La relation $|$ est réflexive, transitive, mais pas symétrique (sur $\mathbb{Z}$ comme sur $\mathbb{N}$). Elle n'est pas antisymétrique sur $\mathbb{Z}$ mais l'est sur $\mathbb{N}$: plus précisément on a sur $\mathbb{Z}$:

$$a|b \text{ et } b|a \iff |a| = |b| \iff a = \pm b$$

(ii) Si a divise b et c, il divise toute combinaison linéaire à coefficients entiers de b et c :

$$a|b \text{ et } a|c \Rightarrow a|bn + cm$$

(iii) La relation $|$ est compatible avec le produit :

$$a|b \text{ et } c|d \Rightarrow ac|bd$$

En particulier, pour tout $k \in \mathbb{N}$, $a|b$ implique $a^k|b^k$;

(iv) Si $c \neq 0$, $a|b \Leftrightarrow ac|bc$.

Démonstration. (i) on ne montre que la dernière partie (le reste a déjà été fait dans le chapitre VIII). Soient $a, b \in \mathbb{Z}$ tels que $a|b$ et $b|a$. Alors il existe $k, \ell \in \mathbb{Z}$ tels que $a = kb$ et $b = a\ell$, donc $b = bk\ell$. Si $b = 0$, alors $a = 0$ également, car $b|a$. Si $b \neq 0$, alors $k\ell = 1$, et donc $k \neq 0$, $\ell \neq 0$, et $|k| \leqslant 1$, ainsi que $|\ell| \leqslant 1$. Par conséquent $k = \ell = 1$ ou $k = \ell = -1$, et donc $a = b$ ou $a = -b$.

(ii) Élémentaire.

(iii) Élémentaire.

(iv) Élémentaire.

□

Exercice 1.1.3.
Montrer que si $a \in \mathbb{Z}$ vérifie $a|1$, alors $a = \pm 1$.

Définition 1.1.4.
On dit que a *est congru à* b *modulo* n et on note $a \equiv b \quad [n]$ (voire $a = b \quad [n]$) si et seulement si n divise $a - b$:

$$a \equiv b \quad [n] \iff n|a - b.$$

Remarque 1.1.5.
Pour tout entier n, la relation de congruence modulo n est une relation d'équivalence.

Proposition 1.1.6.
La relation de congruence modulo n est compatible avec l'addition et la multiplication : si $a \equiv b[n]$ et $c \equiv d[n]$, alors $a + c \equiv b + d[n]$ et $ac \equiv bd[n]$.

Démonstration.
On sait qu'il existe $(k, \ell) \in \mathbb{Z}^2$ vérifiant $a = b + nk$ et $c = d + n\ell$. On a alors $a + c = b + d + n(k + \ell)$, donc $a + c \equiv b + d[n]$, et $ac = bd + n(b\ell + dk + nk\ell)$, donc $ac \equiv bd[n]$. □

Remarque 1.1.7.
Attention, ce n'est pas le cas de la relation usuelle de congruence modulo 2π. Ainsi, $2\pi \equiv 0 \quad [2\pi]$ mais $4\pi^2 \not\equiv 0 \quad [2\pi]$.

Remarque 1.1.8.
On a $n|a$ si et seulement si $a \equiv 0[n]$.

Exercice 1.1.9.
Retrouver les critères de divisibilité énoncés au collège.

1.2 Division euclidienne

Théorème 1.2.1.
Soient $a \in \mathbb{Z}$, et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tels que $a = bq + r$ et $0 \leqslant r < b$. q et r sont respectivement appelés le quotient et le reste de la division euclidienne de a par b. b

est appelé le diviseur et a le dividende de cette division.

Démonstration.
On montre l'existence puis l'unicité.

Existence : On note $A = \{ k \in \mathbb{Z} \mid kb \leqslant a \}$. Alors :
- A est non vide car si $a \geqslant 0$, $0 \in A$, et si $a < 0$ on a $a \in A$ car $b \geqslant 1$.
- De plus A est majoré, par 0 si $a \leqslant 0$ et par a si $a > 0$.

A a donc un plus grand élément noté q. Alors par construction $qb \leqslant a < (q+1)b$, d'où le résultat en posant $r = a - qb$.

Unicité : Soit (q, r) et (q', r') deux couples vérifiant les conditions considérées.
Alors $a = qb + r = q'b + r'$, donc $b(q - q') = r' - r$ et ainsi $b|q - q'| = |r - r'|$. Or on a $0 \leqslant r < b$ et $-b < -r' \leqslant 0$, donc $|r - r'| < b$, donc $|q - q'| < 1$, or $q - q'$ est un entier donc $q = q'$, donc $r = r'$.

□

Remarque 1.2.2.
On a donc $r \equiv a[b]$.

Exemple 1.2.3.
Poser une division à la main. Par exemple 360 divisé par 7.

Remarque 1.2.4.
Dans la pratique, pour $a \geqslant 0$, un algorithme naïf de calcul consiste à soustraire b de a autant de fois que nécessaire pour qu'il reste un nombre plus petit que b. Ainsi :
- Si $a < b$, le quotient est 0 et le reste est a. Sinon on calcule $a_1 = a - b$
- Si $a_1 < b$, le quotient est 0 et le reste est a_1. Sinon on calcule $a_2 = a_1 - b$.
- Si $a_2 < b$, le quotient est 0 et le reste est a_2. Sinon on calcule $a_3 = a_2 - b$.

Et ainsi de suite par récurrence : on s'arrête dès que $a_n < b$. On a alors soustrait n fois b, et il reste a_n : $a = nb + a_n$.

Dans le cas où $a < 0$, on ajoute b jusqu'à obtenir un nombre positif ou nul.

Théorème 1.2.5 (Fonction Python)**.**

```
def diveuclide (a, b) :
    """Précondition : b > 0"""
    q = 0
    r = a
    while r >= b :
        # Invariant : a = b*q + r
        # Variant : r
        r = r-b
        q = q+1
    # Invariant : r < b
    while r < 0 :
        # Invariants :
        # a = b*q + r
        # r < b
        # Variant : -r
        r = r+b
        q = q+1
    # Invariants :
    # 0 <= r < b
    # a = b*q + r
    return(q,r)


def quotient (a, b) :
    """Précondition b > 0"""
    (q, r) = diveuclide (a, b)
    return q


def reste (a, b) :
    """Précondition b > 0"""
    (q, r) = diveuclide (a, b);
    return r

print(reste(11**42424244,7))
```

Démonstration.
- Les boucles `while` terminent : dans la première, la valeur de `r` est un entier qui décroît strictement à chaque itération et sera donc strictement inférieure à celle de b à partir d'un certain moment ; dans la seconde, la valeur de `r` est toujours entière et croît strictement à chaque itération et sera donc strictement positive à partir d'un certain moment.
- Le premier invariant de boucle est vrai à l'arrivée dans la boucle et est préservé au cours de son exécution.

— En sortie de la première boucle, la condition de boucle est fausse donc on a nécessairement `r` $<$ `b`.
— À l'entrée de la seconde, l'invariant annoncé est vrai, il est également préservé. De plus, au début de chaque itération, on a `r` < 0 donc à la fin de chaque itération, on a `r` $<$ `b`.
— À la sortie de la seconde boucle, la condition de boucle est fausse donc on a nécessairement `r` $\geqslant 0$. De plus l'invariant de boucle est encore vrai et `r` $<$ `b`. □

Remarque 1.2.6.
Dans la pratique, au lieu d'enlever b un par un, on peut l'enlever paquets par paquets : c'est ce que l'on fait en posant la division usuelle.

Exemple 1.2.7.
$2356 = 18 \times 125 + 106$.

Proposition 1.2.8.
Soit $n \in \mathbb{N}^*$, alors $a \equiv b[n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n.

Démonstration.
Si a et b ont le même reste dans la division euclidienne par n, on écrit $a = nq_1 + r$ et $b = nq_2 + r$, avec $(q_1, q_2) \in \mathbb{Z}^2$ et $0 \leqslant r < n$. On a donc bien $a - b = n(q_1 - q_2)$, donc $n|(a-b)$.

Réciproquement, si $a \equiv b[n]$, on écrit les divisions euclidiennes de a et b par n : $a = nq_1 + r_1$ et $b = nq_2 + r_2$, avec $(q_1, q_2) \in \mathbb{Z}^2$ et $(r_1, r_2) \in \mathbb{N}^2$ vérifiant, pour tout $i \in \{1, 2\}$, $0 \leqslant r_i < n$. On a alors $a - b - n(q_1 - q_2) = r_1 - r_2$, donc $n|(r_1 - r_2)$. Or, $-n < r_1 - r_2 < n$ et il existe un seul entier dans $[\![-n+1, n-1]\!]$ divisible par n (le montrer !) : c'est 0. Ainsi, $r_1 = r_2$. □

Exemple 1.2.9.
Exercice classique : calculer à la main le reste de la division euclidienne de $11^{42424244}$ par 7.

2 PGCD, PPCM

Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a est noté $a\mathbb{Z}$. C'est donc $\{ak | k \in \mathbb{Z}\}$. Remarquons que, si $a \neq 0$, $|a|$ est le plus petit entier strictement positif de $a\mathbb{Z}$.

On notera aussi $\mathscr{D}(a)$ l'ensemble des diviseurs de a : c'est donc $\{k \in \mathbb{Z} \mid \exists \ell \in \mathbb{Z}, a = k\ell\}$. On remarquera que, si $a \neq 0$, $\mathscr{D}(a)$ est borné par $|a|$.

2.1 PGCD de deux entiers

Dans cette partie, pour tout couple $(a, b) \in \mathbb{Z}$, on note $\mathscr{D}(a, b)$ l'ensemble des diviseurs communs à a et b. Ainsi, $\mathscr{D}(a, b) = \mathscr{D}(a) \cap \mathscr{D}(b)$.

Remarque 2.1.1.
Si $b = 0$, alors $\mathscr{D}(a, b) = \mathscr{D}(a)$.

Définition 2.1.2.
Soit a et b deux entiers avec $(a, b) \neq (0, 0)$, alors on appelle plus grand diviseur commun de a et b (pgcd de a et b) et on note $\mathrm{PGCD}(a, b)$ ou $a \wedge b$ le plus grand élément de $\mathscr{D}(a, b)$.

Remarque 2.1.3.
L'un des deux entiers est non nul, donc $\mathscr{D}(a, b)$ est majoré par la valeur absolue de cet entier. Par ailleurs, $1 \in \mathscr{D}(a, b)$. Donc $\mathscr{D}(a, b)$ est un ensemble d'entiers non vide majoré, donc il admet un plus grand élément, ce qui justifie la définition.

Lemme 2.1.4 (Lemme d'Euclide)**.**
Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, r le reste de la division euclidienne de a par b. Alors $\mathscr{D}(a, b) = \mathscr{D}(b, r)$.

Démonstration.
Soit $d \in \mathscr{D}(a, b)$. Alors a s'écrit sous la forme $bq + r$ donc $r = a - bq$, or $d|a$ et $d|b$, donc d divise toute combinaison linéaire de a et b, donc divise r. Donc $\mathscr{D}(a, b) \subset \mathscr{D}(b, r)$.

Réciproquement, soit $d \in \mathscr{D}(b, r)$, alors a s'écrit sous la forme $bq + r$ or $d|b$ et $d|r$ donc $d|a$, donc $\mathscr{D}(b, r) \subset \mathscr{D}(a, b)$. □

Théorème 2.1.5.
Soit $(a, b) \in \mathbb{Z}^2$ avec $(a, b) \neq (0, 0)$. Alors il existe un unique entier $d > 0$ tel que $\mathscr{D}(a, b)$ soit l'ensemble des diviseurs de d. Cet entier est $a \wedge b$.

Démonstration.
Montrons tout d'abord l'unicité sous réserve d'existence. Soit d et d' deux entiers strictement positifs tels que $\mathscr{D}(a, b)$ soit l'ensemble des diviseurs de d et soit également l'ensemble des diviseurs de d'. Alors on a $d \in \mathscr{D}(a, b)$. Or $\mathscr{D}(a, b)$ est l'ensemble des diviseurs de d', donc $d|d'$. De même $d'|d$. Or $d > 0$ et $d' > 0$ donc $d = d'$.

L'existence repose sur un algorithme, appelé algorithme d'Euclide. En Python, il s'écrit :

```
def euclide (a,b) :
    """Précondition (a,b) != (0,0)"""
    R0 = abs(a)
    R1 = abs(b)
    while R1 > 0 :
        # Invariant : D(R0,R1) = D(a,b)
        # et R0 >= 0 et R1 >= 0
        # et (R0, R1) != (0,0)
        # Variant : R1
        (q, R2) = diveuclide (R0,R1)
        R0 = R1
        R1 = R2
    # Sortie de boucle : R1 == 0
    return R0
```

Soit a et b deux entiers relatifs non tous les deux nuls. Il est clair que l'appel `euclide(a,b)` termine. La valeur d retournée vérifie $\mathscr{D}(a,b) = \mathscr{D}(d,0)$, $d \geqslant 0$ et $(d,0) \neq (0,0)$. Or $\mathscr{D}(d,0)$ est l'ensemble des diviseurs de d donc $\mathscr{D}(a,b)$ est bien l'ensemble des diviseurs d'un entier $d > 0$.

Un autre point de vue sur cet algorithme est la suite r définie de la façon suivante :

$$\begin{cases} r_0 = |a| \\ r_1 = |b| \\ \forall n \in \mathbb{N} \quad r_{n+2} = \begin{cases} \texttt{reste}(r_n, r_{n+1}) & \text{si } r_{n+1} \neq 0 \\ 0 & \texttt{sinon} \end{cases} \end{cases}$$

Il est clair que cette suite est à valeurs positives ou nulles. À partir d'un certain rang, cette suite est nulle, sinon r serait strictement décroissante (du moins à partir du rang 1), ce qui serait absurde. Par ailleurs, pour toutes les valeurs de n pour lesquelles $(r_n, r_{n+1}) \neq (0,0)$, on a $\mathscr{D}(r_n, r_{n+1}) = \mathscr{D}(a,b)$. En particulier, pour la dernière valeur non-nulle r_n, on a $\mathscr{D}(r_n, 0) = \mathscr{D}(a,b)$.

L'algorithme d'Euclide n'est rien d'autre que le calcul des termes successifs de la suite (r_n) : en numérotant les tours de boucle (à partir de 0) dans l'algorithme précédent, on peut d'ailleurs noter qu'au n^{e} tour de boucle, R_0 contient la valeur de r_n, et R_1 celle de r_{n+1}. □

Remarque 2.1.6. — Sur $(\mathbb{N}^*)^2$, le pgcd de deux nombres a et b est donc la borne inférieure de $\{a,b\}$ pour l'ordre $|$. C'est donc aussi le maximum de $\mathscr{D}(a,b) \cap \mathbb{N}^*$ pour l'ordre $|$ et pour l'ordre $\leqslant$.

— Sur $\mathbb{Z}^*$, la relation $|$ n'est pas un ordre car elle n'est pas antisymétrique : on a à la fois $1|-1$ et $-1|1$ (on dit qu'on à affaire à un préordre). L'ensemble des diviseurs de a et b a alors deux «plus grands» éléments pour la relation de divisibilité : $a \wedge b$ et $-(a \wedge b)$. On peut donc en fait considérer que a et b ont deux pgcd : $a \wedge b$ et $-(a \wedge b)$; lorsqu'on parle *du* pgcd, on considère alors qu'il s'agit du pgcd positif.

On peut donner la caractérisation suivante :

Proposition 2.1.7.
Soient $a, b, d \in \mathbb{Z}$, avec $(a,b) \neq (0,0)$. On a l'équivalence :

$$\Big(d \text{ est le PGCD de } a \text{ et } b\Big)$$
$$\Leftrightarrow \Big(d|a,\ d|b,\ d \geqslant 0 \text{ et } \forall n \in \mathbb{Z},\ (n|a \text{ et } n|b) \Rightarrow n|d\Big)$$

Démonstration.
Le sens $\Rightarrow$ découle du théorème précédent.

Réciproquement, si $d \in \mathbb{N}$ vérifie $d|a$, $d|b$ et $\forall n \in \mathbb{N}$, $n|a$ et $n|b \Rightarrow n|d$. Alors d'après les deux premiers points $d|a \wedge b$ et d'après le dernier, $a \wedge b|d$. On conclut avec $d \geqslant 0$ et $a \wedge b \geqslant 0$. □

Théorème 2.1.8 (Théorème de Bézout, première partie)**.**
Soient $a, b \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Il existe deux entiers u, v tels que $au + bv = a \wedge b$. Un tel couple est appelé un couple de Bézout de a et b.

Démonstration.
L'idée de la démonstration est de regarder ce qui se passe dans l'algorithme d'Euclide. On constate qu'à chaque étape, les variables R_0 et R_1 sont des combinaisons linéaires de a et b. À la fin de l'algorithme, le pgcd R_0 est donc une combinaison linéaire de a et b.

Pour calculer les coefficients de Bézout, on aura recours à l'algorithme d'Euclide étendu. Celui-ci est un simple ajout à l'algorithme vu précédemment ; on introduit en effet des variables U_i et V_i pour $i = 0, 1$ qu'on va modifier au fur et à mesure de l'exécution de façon à garantir $R_0 = U_0 a + V_0 b$ et $R_1 = U_1 a + V_1 b$.

```
def euclide_etendu (a, b) :
    """Précondition (a,b) != (0,0)"""
    R0 = abs(a)
    if a < 0 :
        U0 = -1
    else :
        U0 = 1
    V0 = 0
    # Invariant : R0 == U0*a + V0*b
```

```
R1 = abs(b)
U1 = 0
if b < 0 :
    V1 = -1
else :
    V1 = 1
# Invariant : R1 == U1*a + V1*b
# Invariant : D(R0,R1) == D(a,b)
while R1 > 0 :
    # Invariants :
    # D(R0,R1) == D(a,b)
    # R1>=0 et R2>=0
    # (R1,R2) != (0,0)
    # R0 == U0*a + V0*b
    # R1 == U1*a + V1*b
    # Variant : R1
    (q,R2) = diveuclide(R0,R1)
    # donc R2 = R0 - q*R1
    U2 = U0-q*U1
    V2 = V0-q*V1
    # R2 = U2*a + V2*b
    R0, U0, V0 = R1, U1, V1
    R1, U1, V1 = R2, U2, V2
# R1 == 0
return (R0,U0,V0)
```

Là encore, une autre façon de considérer cet algorithme est de regarder les suites r, u et v, où r est la suite considérée précédemment, où u et v vérifient $r_i = u_i a + v_i b$ pour $i = 0, 1$ et pour n tel que r_{n+1} soit non nul, $u_{n+2} = u_n - aq_{n+1}$ et $v_{n+2} = v_n - qv_{n+1}$, où q est le quotient de la division euclidienne de r_n par r_{n+1}. Là encore, il n'est pas difficile de montrer par récurrence double que tant que $(r_n, r_{n+1}) \neq (0,0)$, on a $r_n = u_n a + v_n b$. □

 Le couple des coefficients de Bézout n'est pas unique. Par exemple on a $-1 \times 2 + 1 \times 3 = 1$ et $2 \times 2 + (-1) \times 3 = 1$.

Exemple 2.1.9.
Calcul d'un couple de Bézout pour 1750 et 644.

On peut alors faire la remarque suivante :

Corollaire 2.1.10.
Soit $(a,b) \in \mathbb{Z}^2 \setminus \{ (0,0) \}$. Alors

$$a\mathbb{Z} + b\mathbb{Z} = \left\{ au + bv \;\middle|\; (u,v) \in \mathbb{Z}^2 \right\} = (a \wedge b)\mathbb{Z}$$

Démonstration.
L'inclusion gauche-droite découle du fait que, a et b étant des multiples de $a \wedge b$, toute combinaison linéaire de a et b est également un multiple de $a \wedge b$.

L'inclusion droite-gauche découle du fait que $a \wedge b$ s'écrit comme combinaison linéaire à coefficients entiers de a et b (d'après le théorème de Bézout) et que tout multiple d'une combinaison linéaire de a et b à coefficients entiers est encore une combinaison linéaire à coefficients entiers. □

Corollaire 2.1.11.
Soient $a, b, c \in \mathbb{Z}$. Alors $(ac) \wedge (bc) = |c|(a \wedge b)$.

Démonstration.
Posons $p = (ac) \wedge (bc)$ et $q = |c|(a \wedge b)$. On a $p > 0$ et $q > 0$ donc p et q sont respectivement les plus petits éléments strictement positifs de $p\mathbb{Z}$ et $q\mathbb{Z}$.

Il suffit donc de montrer $p\mathbb{Z} = q\mathbb{Z}$.

Or d'après ce qui précède, on a successivement :

$$\begin{aligned}(a \wedge b)\mathbb{Z} &= \left\{ au + bv \;\middle|\; (u,v) \in \mathbb{Z}^2 \right\} \\ q\mathbb{Z} &= \left\{ |c|(au + bv) \;\middle|\; (u,v) \in \mathbb{Z}^2 \right\} \\ &= \left\{ cau + cbv \;\middle|\; (u,v) \in \mathbb{Z}^2 \right\} \\ &= p\mathbb{Z}\end{aligned}$$

□

2.2 PGCD d'une famille finie d'entiers

Les définitions et résultats de la section précédente se généralisent à une famille finie d'entiers.

Ainsi, si $a_1, \ldots, a_p$ sont p entiers non tous nuls, on note $\mathscr{D}(a_1, \ldots, a_p)$ l'ensemble des diviseurs communs à tous les entiers $a_1, \ldots, a_p$. Cet ensemble étant non vide (il contient 1) et fini, il admet un plus grand élément, appelé *plus grand commun diviseur* des entiers $a_1, \ldots, a_p$ et noté $\bigwedge_{i=1}^{p} a_i$, ou $a_1 \wedge \ldots \wedge a_p$.

Proposition 2.2.1.
Soient $(a_1, \ldots, a_p) \in \mathbb{Z}^p$, avec $a_1 \neq 0$ et $p \in \mathbb{N}^*$.

(i) Soit $k \in \mathscr{D}(a_1, \ldots, a_p)$, alors $k | a_1 \wedge \ldots \wedge a_p$.

(ii) $a_1 \wedge \ldots \wedge a_p = (a_1 \wedge \ldots \wedge a_{p-1}) \wedge a_p$.

Démonstration.
Démontrons les deux résultats en une récurrence, en posant pour chaque $p \in \mathbb{N}^*$:

(H_p) : pour tout $(a_1, \dots, a_p) \in \mathbb{Z}^p$, avec $a_1 \neq 0$, on a (i) et (ii).

Le résultat est connu pour $p = 1$ et $p = 2$.
Soit $p \in \mathbb{N}^*$ tel (H_p) soit vraie.
Soient $a_1, \dots, a_{p+1} \in \mathbb{N}$ tels que $a_1 \neq 0$.
Notons $d = a_1 \wedge \dots \wedge a_p$, $D = a_1 \wedge \dots \wedge a_p \wedge a_{p+1}$ et $D' = d \wedge a_{p+1}$.
Par définition, D divise $a_1, \dots, a_p$: par hypothèse de récurrence (i), D divise donc d. De plus, D divise a_{p+1}, donc $D|D'$.
Par définition, D' divise d et a_{p+1}, et d divise $a_1, \dots, a_p$. Par transitivité de la relation de divisibilité, D' est donc un diviseur de $a_1, \dots, a_{p+1}$. Par définition de D', on a donc $D' \leqslant D$: il vient donc $D = D'$.
Soit k un autre diviseur de $a_1, \dots, a_{p+1}$. En particulier, k est un diviseur de $a_1, \dots, a_p$, donc $k|d$. Et comme $k|a_{p+1}$, alors $k|D'$, et donc $k|D$: (H_{p+1}) est bien démontrée. □

Remarque 2.2.2.
La proposition précédente assure que l'on peut calculer le PGCD d'une famille $a_1, \dots, a_p$ d'entiers en plusieurs étapes : on calcule d'abord $a_1 \wedge a_2$ puis $(a_1 \wedge a_2) \wedge a_3$, et ainsi de suite. Par commutativité du PGCD, on peut aussi choisir les entiers dans un autre ordre, et tout ceci prouve l'associativité du PGCD et assure que la notation $a_1 \wedge \dots \wedge a_p$ est sans ambiguïté.

Le théorème de Bézout peut alors se généraliser par récurrence :

Théorème 2.2.3.
Soient $a_1, \dots, a_p$ des entiers non tous nuls. Alors il existe des entiers $u_1, \dots, u_p$ tels que

$$u_1 a_1 + \dots + u_p a_p = a_1 \wedge \dots \wedge a_p.$$

Démonstration.
Montrons-le par récurrence sur p.
On sait déjà que la propriété est vraie pour $p = 2$.
Soit $p \geqslant 2$ tel que la propriété soit vraie, et soient $a_1, \dots, a_p, a_{p+1}$ des entiers, avec par exemple $a_1 \neq 0$.

Si $a_1 = \dots = a_p = 0$, alors $a_1 \wedge \dots \wedge a_{p+1} = a_{p+1}$, ce qui est bien une relation de Bézout.

Sinon, par hypothèse de récurrence, il existe des entiers $u_1, \dots, u_p$ tels que $u_1 a_1 + \dots + u_p a_p = a_1 \wedge \dots \wedge a_p$. Mais $a_1 \wedge \dots \wedge a_p \wedge a_{p+1} = (a_1 \wedge \dots \wedge a_p) \wedge a_{p+1}$ et d'après le théorème de Bézout pour deux entiers, il existe $b, c \in \mathbb{Z}$ tels que $b.a_1 \wedge \dots \wedge a_p + c.a_{p+1} = a_1 \wedge \dots \wedge a_{p+1}$. D'où $a_1 \wedge \dots \wedge a_{p+1} = bu_1 a_1 + \dots + bu_p a_p + ca_{p+1}$, et l'hérédité est démontrée. □

Exemple 2.2.4.
Trouver trois entiers a, b, c tels que $72a + 180b + 120c = 12$.

Remarque 2.2.5.
Le corollaire 2.1.11 se généralise : soient $a_1, \dots, a_n$ une famille finie d'entiers et $c \in \mathbb{Z}$. Alors $\bigwedge_{i=1}^{n} (ca_i) = |c| \bigwedge_{i=1}^{n} a_i$.

2.3 Nombres premiers entre eux

Définition 2.3.1.
Deux entiers relatifs a et b sont dit premiers entre eux si et seulement si $(a, b) \neq (0, 0)$ et $a \wedge b = 1$.

Remarque 2.3.2.
Deux entier a et b sont premiers entre eux si et seulement si leurs seuls diviseurs communs sont 1 et -1, en d'autres termes si et seulement si $\mathscr{D}(a, b) \subset \{ -1, 1 \}$ (ce qui est équivalent à $\mathscr{D}(a, b) = \{ -1, 1 \}$).

Théorème 2.3.3 (Théorème de Bézout, seconde partie)**.**
Soient $a, b \in \mathbb{Z}$. Alors, a et b sont premiers entre eux si et seulement s'il existe deux entiers u et v tels que $au + bv = 1$.

Démonstration.
Le cas $(a, b) = (0, 0)$ est direct : les deux propositions sont fausses, donc équivalentes. Considérons donc $(a, b) \in \mathbb{Z}^2 \setminus \{ (0, 0) \}$.

Supposons a et b premiers entre eux. Alors, d'après le théorème de Bézout (première partie), on a le résultat.

Réciproquement, supposons qu'il existe deux entiers u et v vérifiant $au + bv = 1$. Soit alors $d \in \mathscr{D}(a, b)$. On a $d|a$ et $d|b$, donc $d|(au + bv)$, donc $d|1$, donc $d = \pm 1$. Donc $\mathscr{D}(a, b) \subset \{ -1, +1 \}$. □

Remarque 2.3.4.
On a donc $a \wedge b = 1$ si et seulement si a est inversible modulo b (*i.e.* il existe $k \in \mathbb{Z}$ vérifiant $ak = 1[b]$).

 $au + bv = 1$ implique $a \wedge b = 1$, mais $au + bv = d$ n'implique pas $a \wedge b = d$, mais simplement $(a \wedge b)|d$.

Corollaire 2.3.5.
Soit $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Alors en posant $d = a \wedge b$, $a' = a/d$ et $b' = b/d$, on a

$$a' \wedge b' = 1$$

Démonstration.
On utilise les deux versions du théorème de Bézout : On sait qu'il existe u et v vérifiant $d = au + bv$, d'où $1 = a'u + b'v$, d'où a' et b' sont premiers entre eux. □

Remarque 2.3.6.
Ce corollaire est très fréquemment utilisé.

Corollaire 2.3.7. (i) Soient a premier avec k entiers relatifs b_1, b_2, ..., b_k. Alors a est premier avec $b_1 \times b_2 \times \ldots \times b_k$.

(ii) Si a et b sont premiers entre eux, alors pour tous $m, n \in \mathbb{N}^*$, a^m et b^n sont également premiers entre eux.

Démonstration. (i) On traite le cas $k = 2$, le cas général s'en déduit immédiatement par récurrence. Il existe u_i et v_i vérifiant $au_i + b_i v_i = 1$ pour $i = 1, 2$. En multipliant ces deux relations, il vient successivement

$$1 = (au_1 + b_1v_1)(au_2 + b_2v_2)$$
$$1 = a^2u_1u_2 + au_1b_2v_2 + b_1v_1au_2 + b_1v_1b_2v_2$$
$$1 = a(au_1u_2 + u_1b_2v_2 + b_1v_1u_2) + b_1b_2(v_1v_2)$$

D'où le résultat.

(ii) On applique (i) à a et $b \times b \times b \times \ldots \times b$, puis (i) à b^n et $a \times a \times a \times \ldots \times a$.

□

Théorème 2.3.8 (Lemme de Gauss)**.**
Soient $a, b, c \in \mathbb{Z}$. On suppose $a|bc$ et $a \wedge b = 1$. Alors $a|c$.

Démonstration.
Ce résultat est une généralisation d'un lemme d'Euclide . On a $a \wedge b = 1$ donc 1 s'écrit comme combinaison linéaire $au + bv$ de a et b. Donc $c = c \times 1 = a(cu) + (bc)v$. Donc c est combinaison linéaire de a et bc. Or bc est un multiple de a donc c est un multiple de a.

On peut aussi le voir d'un point de vue plus algébrique : le théorème de Bézout (2e partie) nous indique que $a \wedge b = 1$ si et seulement si b est inversible modulo a (*i.e*, il existe $k \in \mathbb{Z}$ tel que $kb = 1[a]$). On a alors $bc = 0[a]$, donc $kbc = c = 0[a]$. □

Corollaire 2.3.9 (Forme irréductible d'un rationnel)**.**
Soit $r \in \mathbb{Q}$. Il existe un unique couple $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \dfrac{p}{q}$ et $p \wedge q = 1$. Ce couple est appelé *la forme irréductible de* r.

Démonstration.Existence C'est une conséquence directe du corollaire 2.3.5.

Unicité Soit (p,q) et (p',q') deux formes irréductibles d'un même rationnel r. Alors $p/q = p'/q'$ donc $pq' = p'q$. Donc $q|pq'$ et $p \wedge q = 1$. Donc d'après le théorème de Gauss, on a $q|q'$. De même $q'|q$. Donc $q = q'$ ou $q = -q'$. Or q et q' sont tous deux positifs, donc $q = q'$, donc $p = p'$.

□

Définition 2.3.10.
On dit que des entiers $a_1, \ldots, a_p$ sont *premiers entre eux dans leur ensemble* si leur PGCD vaut 1.

Remarque 2.3.11.
Ne pas confondre « premiers entre eux dans leur ensemble » et « premiers deux à deux ».

Remarque 2.3.12.
La deuxième partie du théorème de Bézout se généralise sans problème à une famille finie d'entiers : soient $a_1, \ldots, a_p$ des entiers. Ces entiers sont premiers entre eux dans leur ensemble si et seulement si il existe des entiers $u_1, \ldots, u_p$ tels que $u_1a_1 + \ldots + u_pa_p = 1$.

2.4 PPCM

Définition 2.4.1.
Soit a et b deux entiers relatifs. L'ensemble de leurs multiples communs est $a\mathbb{Z} \cap b\mathbb{Z}$. Si a et b sont tous deux non nuls, alors cet ensemble possède un plus petit élément strictement positif. Celui-ci est appelé ppcm de a et b et est noté $\mathrm{PPCM}(a,b)$ ou $a \vee b$.

Remarque 2.4.2.
$|ab|$ est un multiple commun à a et b. De plus, comme a et b sont non nuls, c'est un nombre strictement positif. L'ensemble des multiples communs de a et de b strictement positifs est donc non vide. Il est évidemment minoré (par 0), donc il admet un plus petit élément.

Théorème 2.4.3.
Soit a et b deux entiers relatifs. Alors il existe un unique $m \geqslant 0$ vérifiant $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Dans le cas où a et b sont non-nuls, cet entier m est le ppcm de a et b et vaut $\frac{|ab|}{a \wedge b}$

Démonstration.
Le cas ou a ou b est nul est trivial : on a alors $a\mathbb{Z} \cap b\mathbb{Z} = \{0\} = 0\mathbb{Z}$. On suppose donc dans la suite de cette démonstration que a et b sont non nuls. Posons $d = a \wedge b$, $a' = a/d$ et $b' = b/d$. a' et b' sont premiers entre eux.

Posons $m = |ab/d| = |a'b'd|$. m est un multiple de a et de b, donc tout multiple de m est un multiple commun de a et b : $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$.

Soit alors p un multiple de a et de b. Alors p s'écrit à la fois sous la forme au et sous la forme bv. On a donc $p = au = bv$, donc $a'du = b'dv$, donc $a'u = b'v$. Donc $a'|b'v$, or $a' \wedge b' = 1$ donc $a'|v$. Donc il existe k vérifiant $v = ka'$. On a alors $p = bv = bka' = ka'b'd$, donc p est un multiple de m. Donc $a\mathbb{Z} \cap b\mathbb{Z} \subset m\mathbb{Z}$.

On a donc $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. De plus, m est le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$ et pour tout $m' \geqslant 0$ vérifiant $m'\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, m' est également le plus petit élément strictement positif de $a\mathbb{Z} \cap b\mathbb{Z}$, donc $m' = m$. □

Remarque 2.4.4.
— Sur $(\mathbb{N}^*)^2$, le ppcm de deux nombres a et b est donc la borne supérieure de $\{a, b\}$ pour l'ordre $|$. C'est donc aussi le minimum de $a\mathbb{N} \cap b\mathbb{N}$ pour l'ordre $|$ et pour l'ordre $\leqslant$.
— De même que pour le pgcd, sur $\mathbb{Z}^*$, l'ensemble des diviseurs de a et b a deux «plus petits» éléments pour la relation de divisibilité : $a \vee b$ et $-(a \vee b)$. On peut donc en fait considérer que a et b ont deux ppcm : $a \vee b$ et $-(a \vee b)$; lorsqu'on parle *du* ppcm, on considère alors qu'il s'agit du ppcm positif.

On peut donner la caractérisation suivante :

Proposition 2.4.5.
Soient $a, b, m \in \mathbb{Z}$. On a l'équivalence :

$$\Big(m \text{ est le PPCM de } a \text{ et } b\Big)$$
$$\Leftrightarrow \Big(a|m,\ b|m,\ m \geqslant 0$$
$$\text{et : } \forall n \in \mathbb{Z},\ (a|n \text{ et } b|n) \Rightarrow m|n\Big)$$

Et également (le point (ii) a d'ailleurs été démontré au cours de la démonstration du théorème 2.4.3) :

Proposition 2.4.6.
Soient $a, b, c \in \mathbb{Z}$. Alors :
(i) $(ac) \vee (bc) = |c|(a \vee b)$.
(ii) si $(a, b) \neq (0, 0)$, alors $|ab| = (a \wedge b).(a \vee b)$.

Exemple 2.4.7.
Calculer $1750 \vee 644$.

Remarque 2.4.8.
Là encore, si $a_1, \ldots, a_n$ est une famille finie d'entiers et $c \in \mathbb{Z}$, alors $\bigvee_{i=1}^{n}(ca_i) = |c| \bigvee_{i=1}^{n} a_i$.

3 Nombres premiers

Définition 3.0.1.
Soit $p \in \mathbb{N}^*$. On dit que p est *premier* si $p \neq 1$ et si ses seuls diviseurs positifs sont 1 et p. On dit que p est *composé* si $p \neq 1$ et p est non premier.

Exemple 3.0.2.
Les premiers nombres premiers : $2, 3, 5, 7, 11, 13, 17, 19, 23, 2$
2 est le seul nombre premier pair.

Remarque 3.0.3.
On appelle *diviseur strict* de n tout entier naturel diviseur de n différent de n. Un nombre premier est donc un entier autre que 1 sans diviseur strict autre que 1.

Remarque 3.0.4.
Soit p et q sont deux nombres premiers distincts. Alors p et q sont premiers entre eux.

Démonstration.
Par l'absurde, supposons $p \wedge q \neq 1$. Alors $p \wedge q$ est un diviseur de p et de q autre que 1. p et q étant premiers, ce ne peut être un diviseur strict, donc $p = p \wedge q = q$. Or $p \neq q$, donc c'est absurde. □

Le résultat suivant, fondamental, ainsi que la démonstration donnée, sont connus depuis Euclide :

Théorème 3.0.5.
L'ensemble des nombres premiers est infini.

Démonstration.
En effet, soient $p_1, \ldots, p_n$ n nombres premiers, avec $n \geqslant 1$. Montrons qu'il en existe nécessairement un autre.

On considère la quantité $p_1.p_2.\ldots.p_n+1$. Cette quantité est un entier strictement supérieur à 1. L'ensemble de ses diviseurs (positifs) différents de 1 est donc non vide et possède donc un plus petit élément q, différent de 1, qui ne peut posséder aucun diviseur strict autre que 1 : q est donc premier.

Alors q est nécessairement différent de tous les p_i. Car si $q = p_i$ pour un certain $i \in [\![1, n]\!]$, q divise $p_1.p_2.\ldots.p_n$ d'une part, et divise $p_1.p_2.\ldots.p_n + 1$ d'autre part, donc divise la différence qui vaut 1, ce qui est impossible.

q est donc un $(n+1)$ème nombre premier. □

Théorème 3.0.6.
Tout entier naturel supérieur ou égal à 1 se décompose de manière unique (à l'ordre des facteurs près) en un produit de nombres premiers (ce produit est éventuellement réduit à zéro ou un terme, et peut avoir plusieurs facteurs égaux). Plus précisément, pour tout $n \in \mathbb{N}\backslash\{0, 1\}$, il existe $k \in \mathbb{N}^*$, des entiers premiers $p_1, \ldots, p_k$ distincts et $\alpha_1, \ldots, \alpha_k \in \mathbb{N}^*$ tels que

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}.$$

Démonstration.Existence on en donne trois démonstrations

Principe de la descente infinie de Fermat Si n est un nombre ne se décomposant pas en facteurs premiers, alors n n'est lui-même pas premier (sinon, $n = n$ est une décomposition). Donc, n s'écrit $n = ab$, avec $1 < a < n$ et $1 < b < n$. n ne se décomposant pas en facteurs premiers, nécessairement, a ou b ne se décompose pas en facteurs premiers. On trouve donc, pour tout entier ne se décomposant pas en facteurs premiers, un entier strictement plus petit ne se décomposant pas en facteurs premiers. Ce qui est impossible, car en itérant le procédé, on construirait une suite strictement décroissante d'entiers.

Principe du bon ordre Soit A l'ensemble des entiers n'admettant pas de décomposition. Nous voulons montrer que A est vide. S'il était non vide, il y aurait un plus petit élément a. Si a n'admet pour diviseur que 1 et lui-même, a est premier. $a = a$ est une décomposition de a en facteurs premiers, ce qui est contraire à l'hypothèse. Donc a s'écrit $b \times c$ où b et c sont des entiers différents de a et de 1. a étant le minimum de A, b et c ne sont pas éléments de A et se décomposent donc en produit de facteurs premiers. Il en est donc de même de a.

Principe de récurrence On suppose que tout entier inférieur ou égal à n se décompose en produits de facteurs premiers (ce qui est vrai pour $n \leqslant 2$). Considérons $n + 1$:

- Si $n + 1$ est premier, alors $n + 1 = n + 1$ est une décomposition.
- Sinon, $n + 1 = ab$, avec $1 < a < n + 1$, et $1 < b < n + 1$. L'hypothèse de récurrence s'applique sur a et b, qui se décomposent donc en produits de facteurs premiers. Il en est donc de même de $n + 1$.

Unicité Commençons par remarquer que pour tout entier non nul p, $p^0 = 1$. Ainsi si $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}$ et si p_{k+1} est un nombre premier distinct des k précédents, on peut écrire $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}.p_{k+1}^{\alpha_{k+1}}$, avec $\alpha_{k+1} = 0$.

On suppose que n a deux décompositions en facteurs premiers, que l'on peut donc écrire $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k} = p_1^{\beta_1}.p_2^{\beta_2}.\ldots.p_k^{\beta_k}$, les deux membres étant éventuellement complétés par p^0 pour avoir les mêmes facteurs premiers dans les deux membres. Le théorème de Gauss permet de dire que $p_1^{\alpha_1}$ divise le membre de droite, mais puisqu'il est premier avec $p_2, \ldots, p_k$ car tous ces nombres premiers sont distincts, il divise $p_1^{\beta_1}$, et donc $\alpha_1 \leqslant \beta_1$. Symétriquement, $\alpha_1 \geqslant \beta_1$, et ainsi $\alpha_1 = \beta_1$. Il en est de même pour les autres puissances.

□

Définition 3.0.7.
Pour un nombre premier p on définit l'application

$$\begin{array}{rccl} \nu_p & : & \mathbb{Z} & \to & \mathbb{N} \cup \{ +\infty \} \\ & & n & \mapsto & \left\{ \begin{array}{l} +\infty \text{ si } n = 0 \\ \max \left\{ k \in \mathbb{N} \;\middle|\; p^k | n \right\} \quad \text{sinon} \end{array} \right. \end{array}$$

qui à un entier n associe l'exposant de p dans la décomposition de n en facteurs premiers, avec la convention $\nu_p(0) = +\infty$. Cette fonction est appelée *valuation p-adique sur* $\mathbb{Z}$.

Démonstration.
Il faut démontrer que $\max \left\{ k \in \mathbb{N} \;\middle|\; p^k | n \right\}$ existe bien. L'ensemble $\left\{ k \in \mathbb{N} \;\middle|\; p^k | n \right\}$ est non vide car il contient 0 ; de plus $p^k \xrightarrow[k \to +\infty]{} +\infty$, donc il existe $K \in \mathbb{N}$ tel que $p^K > n$, donc cet ensemble est majoré. Comme c'est une partie de $\mathbb{N}$, il admet bien un maximum. □

Exemple 3.0.8.
$\nu_5(50) = 2$, $\nu_3(50) = 0$.

Proposition 3.0.9.
Soient $a, b \in \mathbb{Z}$. On note $\mathscr{P}$ l'ensemble des nombres premiers.

(i) Pour tout entier p premier, p divise a si et seulement si $\nu_p(a) > 0$.

(ii) Si $a \neq 0$, $|a| = \prod_{p \in \mathscr{P}} p^{\nu_p(a)}$.

(iii) On a $a|b$ si et seulement si, pour tout $p \in \mathscr{P}$, $\nu_p(a) \leqslant \nu_p(b)$.

(iv) Si $(a, b) \neq (0, 0)$, $a \wedge b = \prod_{p \in \mathscr{P}} p^{\min(\nu_p(a), \nu_p(b))}$.

(v) si $a \neq 0$ et $b \neq 0$, $a \vee b = \prod_{p \in \mathscr{P}} p^{\max(\nu_p(a), \nu_p(b))}$

(vi) Les entiers a et b sont premiers entre eux si et seulement si ils n'ont aucun facteur premier en commun (*i.e.* pour tout p, $\nu_p(a) = 0$ ou $\nu_p(b) = 0$).

Démonstration. (i) Évident.

(ii) C'est une simple réécriture de la décomposition de a en facteurs premiers.

(iii) Si $a|b$, soit $p \in \mathscr{P}$. Alors, $p^{\nu_p(a)}$ divise a donc p, donc $\nu_p(b) \geqslant \nu_p(a)$.
Réciproquement, supposons que pour tout $p \in \mathscr{P}$, $\nu_p(a) \leqslant \nu_p(b)$. On voit alors dans la décomposition en facteurs premiers de b que l'on peut factoriser a dans b, donc $a|b$.

(iv) Commençons par remarquer que le produit considéré est bien défini : c'est un produit faisant intervenir une infinité de termes car $\mathscr{P}$ est infini, mais en fait seul un nombre fini de ces termes sont différents de 1. En effet, les diviseurs premiers de a sont en nombre fini, donc la valuation de a n'est non nulle que pour un nombre fini d'entiers premiers. Il en est de même pour b, et donc $\min(\nu_p(a), \nu_p(b))$ n'est non nulle que pour un nombre fini d'entiers premiers p.
On note $d = \prod_{p \in \mathscr{P}} p^{\min(\nu_p(a), \nu_p(b))}$. Alors :

$$d \times \prod_{p \in \mathscr{P}} p^{\nu_p(a) - \min(\nu_p(a), \nu_p(b))} = \prod_{p \in \mathscr{P}} p^{\nu_p(a)} = a$$

$$\text{et } d \times \prod_{p \in \mathscr{P}} p^{\nu_p(b) - \min(\nu_p(a), \nu_p(b))} = \prod_{p \in \mathscr{P}} p^{\nu_p(b)} = b$$

donc d est un diviseur commun à a et b.
Soit d' un autre diviseur commun à a et b. Alors d' s'écrit nécessairement : $d' = \prod_{p \in \mathscr{P}} p^{\delta(p)}$, avec pour tout p, $\delta(p) \in \mathbb{N}$, et il n'y a qu'un nombre fini d'entiers premiers p tels que $\delta(p) > 0$. Mais si $d'|a$, on doit avoir pour tout $p \in \mathscr{P}$, $\delta(p) \leqslant \nu_p(a)$. De même, $d'|b$ donc pour tout $p \in \mathscr{P}$, $\delta(p) \leqslant \nu_p(b)$. On a donc pour tout $p \in \mathscr{P}$, $\delta(p) \leqslant \min(\nu_p(a), \nu_p(b))$, et par conséquent $d'|d$, et d est bien le pgcd de a et b.

(v) S'inspirer de la démonstration du point précédent.

(vi)
a et b sont premiers entre eux
$\Leftrightarrow$ $a \wedge b = 1$
$\Leftrightarrow$ pour tout entier premier p, $\nu_p(a \wedge b) = 0$
$\Leftrightarrow$ pour tout entier premier p, $\min(\nu_p(a), \nu_p(b)) = 0$
$\Leftrightarrow$ pour tout entier premier p, $\nu_p(a) = 0$ ou $\nu_p(b) = 0$
$\Leftrightarrow$ pour tout entier premier p, p ne divise pas a ou p ne divise pas b
$\Leftrightarrow$ ils n'ont aucun facteur premier en commun.

□

Finissons par un dernier résultat classique, le petit théorème de Fermat (Pierre de, Beaumont-de-Lomagne, première décennie du XVIIe siècle - Castres, 1665) (le grand n'est malheureusement pas à notre portée), qui a deux formulations équivalentes :

Théorème 3.0.10 (Petit théorème de Fermat, 1640)**.**
Soit p un nombre premier. Alors on a :

(i) pour tout $a \in \mathbb{Z}$, p divise $a^p - a$.

(ii) pour tout $a \in \mathbb{Z}$ qui n'est pas un multiple de p, p divise $a^{p-1} - 1$.

Démonstration.
Ce théorème admet plus de 100 démonstrations. Fermat disait en connaître une mais ne l'a jamais publiée et elle n'est pas parvenue jusqu'à nous. La première démonstration est dûe à Leibniz en 1683, dans un manuscrit qui lui non plus n'a pas été publié. Il faut attendre 1736 pour qu'Euler donne la première démonstration publique, qui est essentiellement la même que celle de Leibniz.
Un petit nombre de ces démonstrations ainsi qu'une introduction historique peuvent être lus à l'adresse suivante, sur le site de l'ENS :

http ://preview.tinyurl.com/pm49tb4

Donnons-en encore une autre :

Commençons par montrer l'équivalence des deux énoncés [1] :
Si (i) est vrai et que a n'est pas un multiple de p, alors puisque p est premier, a et p sont premiers entre eux. Par conséquent, grâce au théorème de Gauss, $p|a(a^{p-1} - 1)$ donc $p|a^{p-1} - 1$.
Si (ii) est vrai, soit $a \in \mathbb{Z}$. Si a est un multiple de p, $p|a$ donc $p|a(a^{p-1} - 1)$. Et si a n'est pas un multiple de p, alors avec (ii) $p|a^{p-1} - 1$ donc $p|a(a^{p-1} - 1)$. Dans tous les cas, (i) est vrai.

Montrons maintenant le point (ii).
Soit a un entier non multiple de p. Posons $N = a(2a)(3a)...((p-1)a)$. Nous allons calculer N modulo p de deux manières.

1. Ici, nous n'avons besoin que de montrer que (ii) implique (i) puisque nous allons montrer (i) par la suite.

Tout d'abord, réécrivons $N = a^{p-1} \times (p-1)!$.

Ensuite, pour tout $i \in [\![1, p-1]\!]$, appelons r_i le reste de la division euclidienne de ia par p. Alors $N \equiv r_1 r_2 \dots r_{p-1}$ $[p]$. Supposons qu'il existe $i, j \in [\![1, p-1]\!]$ tels que $r_i = r_j$. Alors $ia \equiv ja$ $[p]$ donc $p|(i-j)a$. Or $a \wedge p = 1$ donc avec le théorème de Gauss, $p|(i-j)$. Mais $|i-j| < p$ donc nécessairement $i - j = 0$, donc $i = j$. Ainsi les $r_1, \dots, r_{p-1}$ sont deux à deux distincts. Mais comme ils sont tous dans l'intervalle $[\![1, p-1]\!]$, qui contient exactement $p-1$ éléments, $\{r_1, \dots, r_{p-1}\} = [\![1, p-1]\!]$, et donc $r_1 r_2 \dots r_{p-1} = (p-1)!$.

Finalement, $N = a^{p-1} \times (p-1)! \equiv (p-1)!$ $[p]$, donc $p|(p-1)!(a^{p-1} - 1)$. Or p est premier avec tous les entiers de 1 à $p-1$, donc il est premier avec $(p-1)!$, et à nouveau avec le théorème de Gauss, il vient bien $p|a^{p-1} - 1$. □

Le Petit théorème de Fermat donne donc une condition nécessaire pour qu'un nombre entier soit premier. Il est d'ailleurs très largement utilisé dans les tests de primalité, comme celui de Rabin-Miller. Mais, sa réciproque étant fausse, il n'est pas possible de savoir de manière certaine qu'un nombre est premier en n'utilisant que ce théorème. Ainsi, on appelle *nombres de Carmichael* ou *menteurs de Fermat* les nombres entiers qui ne sont pas premiers mais vérifient tout de même le Petit théorème de Fermat. Le plus petit nombre de Carmichael est 561, et a été découvert par Carmichael en 1910, bien que les propriétés de tels nombres aient déjà été énoncées en 1899 par Korselt. Les nombres de Carmichael étant relativement rares par rapport aux nombres premiers, un test de primalité basé sur le petit théorème de Fermat aura peu de chances de donner un résultat erroné, mais il n'est cependant pas considéré comme un test suffisament fiable. C'est pourquoi on le combine avec d'autres tests pour obtenir des tests de primalité probabilistes plus fiables.