Arithmétique

1 Nombres entiers, divisibilité

1.1 Nombres entiers

On appelle $\mathbb{N}$ l'ensemble des nombres entiers positifs $0, 1, 2, 3, \ldots$. Cet ensemble est infini. La somme et le produit de deux éléments de $\mathbb{N}$ est un élément de $\mathbb{N}$. En revanche, la différence et le quotient de deux éléments de $\mathbb{N}$ n'est pas en général un élément de $\mathbb{N}$.

Exemple : 5-12=-7 n'est pas dans $\mathbb{N}$.

L'ensemble des nombres entiers $\ldots, -3, -2, -1, 0, 1, \ldots$ s'appelle $\mathbb{Z}$. Cet ensemble contient $\mathbb{N}$ et est donc infini. La somme, le produit et la différence de deux nombres entiers est un entier. En revanche, le quotient de deux nombres entiers n'est pas en général un nombre entier.

Exemple : $3/4$ n'est pas dans $\mathbb{Z}$.

Lorsque le quotient d'un entier b par un entier a non-nul est lui-même un entier, on dit que a divise b et on écrit $a|b$. Comme

$$\frac{b}{a} = n$$

implique, en multipliant à gauche et à droite par a, que

$$b = an$$

l'entier a divise l'entier b si et seulement s'il existe un entier $n \in \mathbb{Z}$ tel que b puisse s'écrire $b = an$. Si a ne divise pas b, on écrit $a \nmid b$. Remarquons que si $a|b$ et si a et b sont strictement positifs, alors $a \leq b$.

Exemple : 3 divise 6, 12 ne divise pas 25.

Voici quelques propriétés élémentaires de la relation de divisibilité.

Lemme 1.1. *1. L'entier* 1 *divise tous les entiers.*

2. Tout entier non-nul divise 0*.*

3. Un entier a non-nul se divise lui-même.

4. Si a divise b, alors $-a$ divise b et a divise $-b$.

5. Si $a|b$ et $a|c$ alors $a|(b+c)$.

6. Si $a|b$ et $b|a$ alors $a = \pm b$.

7. *Si $a|b$ et $b|c$, alors $a|c$.*

Démonstration. 1. Soit $a \in \mathbb{Z}$. Alors a s'écrit $a = a \times 1$ donc $1|a$.

2. Soit $a \in \mathbb{Z}$ non-nul. Alors 0 s'écrit $0 = a \times 0$ donc $a|0$.

3. Soit $a \in \mathbb{Z}$. Alors a s'écrit $a = a \times 1$ donc $a|a$.

4. Soit a et b deux entiers avec $a|b$. Alors b s'écrit $b = na$ avec $n \in \mathbb{Z}$. Donc $b = (-n)(-a)$ donc $-a|b$ et $-b = (-n)a$ donc $a| - b$.

5. Soit a, b, c trois entiers avec $a|b$ et $a|c$. Alors b s'écrit $b = na$ avec $n \in \mathbb{Z}$ et c s'écrit $c = ma$ avec $m \in \mathbb{Z}$ donc $b + c$ s'écrit $b + c = ma + na = (m + n)a$ et $(m + n) \in \mathbb{Z}$.

6. Soit a et b deux entiers avec $a|b$ et $b|a$. Alors b s'écrit $b = na$ avec $n \in \mathbb{Z}$ et a s'écrit $a = mb$ avec $m \in \mathbb{Z}$. Donc b s'écrit $b = nmb$. Comme $b \neq 0$, on peut diviser des deux côtés de cette égalité par b et l'on obtient $nm = 1$. Les seuls entiers dont le produit est 1 sont 1 et 1 ou bien -1 et -1. Donc $a = \pm b$.

7. Soit a, b, c trois entiers avec $a|b$ et $b|c$. Alors b s'écrit $b = na$ avec $n \in \mathbb{Z}$ et c s'écrit $c = mb$ avec $m \in \mathbb{Z}$. Donc c s'écrit $c = mna$ avec $mn \in \mathbb{Z}$ donc $a|c$.

□

Si b est un entier positif et si a est un entier positif vérifiant $a|b$, on dit que a est un diviseur de b. A part l'entier 0, tous les entiers positifs ont un nombre fini de diviseurs et en ont au moins 1. Ceci permet de définir quatre grandes catégories d'entiers positifs : 0 (qui a un nombre infini de diviseurs), 1 (qui n'a qu'un seul diviseur, lui-même), les nombres premiers et les nombres composés. Un entier positif est dit premier si et seulement s'il a exactement deux diviseurs (1 et lui-même). Un entier positif est dit composé si et seulement s'il a strictement plus de deux diviseurs. Les 15 premiers nombres premiers sont :

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$$

Les 15 premiers nombres composés sont :

$$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25$$

Lemme 1.2. *Tout entier non-nul peut s'écrire comme le produit de ± 1 et un produit fini de nombres premiers.*

Démonstration. Soit a un entier non-nul. Si $a < 0$, alors on pose $a' = -a$. Il suffit de démontrer le résultat pour a'. Il n'y a donc pas de perte de généralités à supposer que $a > 0$. Le résultat est alors vrai pour $a = 1$ car 1 s'écrit comme le produit de 1 et de zéro nombres premiers. Soit n un entier strictement supérieur à 1. Supposons le résultat vrai pour tous les entiers strictement positifs strictement inférieur à n. Si n est premier, alors n s'écrit $n = n$ donc est un produit fini de nombres premiers. Sinon, n a au moins un diviseur qui ne soit ni 1 ni n. Donc n peut s'écrire $n = ab$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$. Les entiers a et b sont plus petits que n donc peuvent s'écrire $a = p_1 \cdots p_s$ et $b = q_1 \cdots q_t$ où les p_i et les q_j sont des nombres premiers. Donc $n = p_1 \cdots p_s q_1 \cdots q_t$ donc s'écrit comme un nombre fini de nombres premiers. □

1.2 Division euclidienne

La proposition suivante caractérise de façon fondamentale l'arithmétique des nombres entiers.

Proposition 1.3. *Soit a un entier et b un entier strictement positif. Il existe un unique couple d'entiers (q, r) tel que $a = bq + r$ avec $0 \leq r < b$.*

Démonstration. Considérons l'ensemble des entiers de la forme $a - xb$ avec $x \in \mathbb{Z}$. Cet ensemble contient des éléments positifs, et contient un unique élément positif de taille minimal que nous notons r. Soit $q \in \mathbb{Z}$ tel que $a - qb = r$. Alors a s'écrit $a = bq + r$ avec $0 \leq r$. Il suffit donc de démontrer que $r < b$ et que (q, r) est le seul couple d'entiers vérifiant cette propriété.

Les inégalités

$$a - xb \geq b > 0$$

impliquent :

$$0 \leq a - (x + 1)b < a - xb$$

L'élément r, qui est minimal parmi les $a - xb$, est donc strictement inférieur à b. Si (q', r') est un autre couple d'entiers tel que $a = q'b + r'$ et $0 \leq r' < b$, alors $q'b + r' = qb + r$ donc $b(q' - q) = r - r'$ donc b divise $r - r'$ et $r' - r$. L'un des deux entiers $r - r'$ et $r' - r$ est positif, disons $r - r'$. L'entier $r - r'$ est une différence positive d'entiers strictement inférieurs à b. C'est donc un entier strictement inférieur à b. Le seul entier strictement inférieur à b que b divise est 0 donc $r = r'$. Donc $b(q - q') = 0$ donc $q = q'$. □

L'entier q s'appelle le quotient et l'entier r s'appelle le reste de la division euclidienne de a par b.

Remarque : Si l'on veut faire la division euclidienne de a par b avec $b < 0$, il suffit de réaliser la division euclidienne de a par $-b$ pour d'écrire $a = q(-b) + r$ puis de remarquer que cela signifie que $a = (-q)b + r$. On se permettra donc de réaliser des division euclidiennes sans toujours vérifier le signe de b. On remarque que dans tous les cas $0 \leq r < |b|$.

1.3 Plus grand diviseur commun

Soit $a, b \in \mathbb{Z}$ deux entiers. On note (a) l'ensemble des nombres entiers qui peuvent s'écrire sous la forme ax avec $x \in \mathbb{Z}$. C'est donc aussi l'ensemble des entiers que a divise. On note (a, b) l'ensemble des nombres entiers qui peuvent s'écrire sous la forme $ax + by$ avec $x, y \in \mathbb{Z}$.

Lemme 1.4.

1. $(a, 0) = (a)$.
2. $(a, b) = (\pm a, \pm b)$.
3. $(a, b) = (a)$ *si et seulement si* $a|b$.
4. $(a, 1) = \mathbb{Z}$.
5. $(a, a + b) = (a, b)$.
6. *Soit $a, b \in \mathbb{Z}$. Soit r le reste de la division euclidienne de a par b. Alors* $(a, b) = (b, r)$.

Démonstration. 1. L'ensemble des nombres entiers qui peuvent s'écrire sous la forme $ax + y0$ avec $x, y \in \mathbb{Z}$ est l'ensemble des nombres entiers qui peuvent s'écrire sous la forme ax avec $x \in \mathbb{Z}$.

2. L'ensemble des nombres entiers qui peuvent s'écrire sous la forme $ax + by$ avec $x, y \in \mathbb{Z}$ est égal à l'ensemble des nombres entiers qui peuvent s'écrire sous la forme $(-a)x + (-b)y$ avec $x, y \in \mathbb{Z}$.
3. Si $a|b$, alors $b = na$ donc l'ensemble des nombres entiers qui peuvent s'écrire sous la forme $ax + by$ avec $x, y \in \mathbb{Z}$ est égal à l'ensemble des nombres entiers qui peuvent s'écrire sous la forme $ax + nay = a(x + ny) = az$. Si $(a, b) = (a)$, alors b appartient à (a) donc b peut s'écrire $b = na$ donc $a|b$.
4. D'après l'assertion précédente, $(a, 1) = (1) = \mathbb{Z}$.
5. L'ensemble des nombres entiers qui peuvent s'écrire sous la forme $ax+(a+b)y$ avec $x, y \in \mathbb{Z}$ est égal à l'ensemble des nombres entiers qui peuvent s'écrire sous la forme $a(x+y)+by = az+by$ avec $z, y \in \mathbb{Z}$, donc à (a, b).
6. D'après les assertions précédentes, $(a, b) = (a - b, b) = (a - 2b, b) = \cdots = (a - qb, b) = (b, r)$.

□

Proposition 1.5. *Soit $a, b \in \mathbb{Z}$. Soit c le plus petit élément strictement positif de (a, b). Alors $(a, b) = (c)$.*

Démonstration. L'entier c appartient à (a, b) donc peut s'écrire sous la forme ax_0+by_0. Tout élément de la forme cz avec $z \in \mathbb{Z}$ peut donc s'écrire sous la forme $ax_0z + by_0z$ et appartient donc à (a, b). Il suffit donc de montrer réciproquement que tout élément de la forme $ax + by$ avec $x, y \in \mathbb{Z}$ s'écrit sous la forme cz avec $z \in \mathbb{Z}$. Écrivons la division euclidienne de $ax + by$ par c.

$$ax + by = qc + r,\ 0 \leq r < c$$

Donc r s'écrit $r = ax + by - q(ax_0 + by_0) = a(x - qx_0) + b(y - qy_0)$ donc appartient à $\mathbb{Z}$. Comme $r < c$, r est nul. Donc $ax + by = qc$ donc $ax + by$ appartient à (c). □

Lemme 1.6. *Soit $a, b \in \mathbb{Z}$ et soit c l'entier positif tel que $(c) = (a, b)$. L'entier c est le plus grand entier divisant à la fois a et b.*

Démonstration. Tout d'abord, $a \in (c)$ et $b \in (c)$ donc $c|a$ et $c|b$. Soit d un diviseur commun à a et b. Alors d divise a et d divise b donc $c = ax_0 + by_0$ peut s'écrire $c = dnx_0 + dmy_0 = d(nx_0 + my_0)$ donc d divise c. □

L'entier c s'appelle le plus grand diviseur commun de a et b. On peut aussi le noter $a \wedge b$. Lorsque $a \wedge b = 1$, on dit que a et b sont premiers entre eux.

Exemples : 5 et 23 sont premiers entre eux, 6 et 35 sont premiers entre eux, 26 et 91 ne sont pas premiers entre eux (car $26 \wedge 91 = 13$). Deux nombres premiers distincts sont premiers entre eux.

Lemme 1.7. *Soit $a, b, c \in \mathbb{Z}$. Supposons que $a|bc$ et que $a \wedge b = 1$. Alors $a|c$. En particulier, si p est un nombre premier et si $p|ab$ alors $p|a$ ou $p|b$. Si $p \nmid a$ et si $p \nmid b$ alors $p \nmid ab$*

Démonstration. De $a \wedge b = 1$, on déduit qu'il existe des entiers x, y tels que $ax + by = 1$. Donc $c = axc + byc$. De $a|bc$, on déduit que bc peut s'écrire $bc = an$. Donc $c = axc + any = a(xc + ny)$. Donc $a|c$. La deuxième assertion découle de la première et du fait que si p est premier, alors $p \wedge a = 1$ ou $p \wedge a = p$. La troisième assertion est une reformulation de la deuxième. □

Soit $a, b \in \mathbb{Z}$ et $d = a \wedge b$. Écrivons $a = da'$ et $b = db'$. Alors $a' \wedge b' = 1$. En effet, d peut s'écrire $d = ax + by$ donc $1 = a'x + b'y$.

1.4 Le théorème fondamental de l'arithmétique

Théorème 1. *Tout nombre entier non-nul peut s'écrire de manière unique (à l'ordre près) comme un produit d'un signe et d'un produit fini de nombres premiers.*

Démonstration. Soit n un entier. Si $n = \pm 1$, alors n s'écrit comme dans le théorème. Nous savons déjà que n peut s'écrire sous la forme :

$$n = (-1)^{\epsilon} \prod_i p_i^{n_i}$$

Dans le produit ci-dessus, les p_i sont des nombres premiers distincts. Supposons que n s'écrive également sous la forme :

$$n = (-1)^{\epsilon} \prod_j q_j^{m_j}$$

Soit q l'un des q_j. Alors $q|n$. Comme $q^m \wedge p^n = 1$ si $p \neq q$, l'un des p_i est égal à q et $p_i^{n_i}$ est divisible par q^m. Donc les q_j sont des p_i et les n_i sont inférieurs aux m_j. Par symétrie, les p_i sont des q_j et $n_i = m_j$. □

L'écriture d'un entier comme produit de nombres premiers peut aussi se présenter sous la forme suivante :

$$n = (-1)^{\alpha} \prod_p p^{n_p}$$

Ici, le produit est pris sur tous les nombres premiers, mais les n_p sont tous égaux à zéro sauf un nombre fini.

Corollaire 1.8. *Soit n et m deux entiers dont les écritures en produit de nombres premiers s'écrivent :*

$$n = (-1)^{\alpha} \prod_p p^{n_p}, m = (-1)^{\beta} \prod_p p^{m_p}$$

1. *L'entier n est un diviseur de m si et seulement si $n_p \leq m_p$ pour tout nombre premier.*
2. *Pour tout nombre premier p, on dénote par d_p le minimum de n_p et m_p. L'entier $n \wedge m$ s'écrit alors :*

$$n \wedge m = \prod_p p^{d_p}$$

Démonstration. 1. Si $n_p \leq m_p$ pour tout p, alors

$$n' = (-1)^{\alpha+\beta} \prod_p p^{m_p - n_p}$$

est un entier qui vérifie $nn' = m$. Réciproquement, si m s'écrit $m = nn'$ et si n' s'écrit

$$n' = (-1)^{\alpha'} \prod_p p^{n'_p}$$

alors m s'écrit :

$$m = (-1)^{\alpha} \prod_p p^{n_p} (-1)^{\gamma} \prod_p p^{n'_p} = (-1)^{\alpha+\alpha'} \prod_p p^{n_p + n'_p}$$

Par unicité de l'écriture en produit de nombres premiers, on a $\alpha' = \beta - \alpha$ et $n'_p = m_p - n_p$. Donc $m_p - n_p \geq 0$ pour tout p.

2. L'entier

$$d = \prod_p p^{d_p}$$

divise n et m d'après la première assertion. Si $d'|n$ et $d'|m$, alors $d'_p \leq n_p$ et $d' \leq m_p$ pour tout p donc $d'_p \leq \min(n_p, m_p)$ pour tout p donc $d'|d$ d'après la première assertion. Donc $d = n \wedge m$.

□

2 L'algorithme d'Euclide et l'équation $ax + by = c$

2.1 L'algorithme d'Euclide

Soit $a, b \in \mathbb{Z}$. Soit (q, r) le quotient et le reste de la division euclidienne de a par b. Nous avons déjà vu que $(a, b) = (b, r)$. Ceci suggère l'algorithme suivant pour calculer $a \wedge b$. L'algorithme prend en entrée un couple d'entiers (a, b).

1. Réaliser la division euclidienne de a par b. Ceci produit des entiers q et r.
2. Si $r = 0$, alors rendre comme résultat b.
3. Sinon, remplacer a par b et b par r.
4. Retourner en 1.

Exemple : Calculons $51 \wedge 187$ par ce procédé. L'algorithme prend donc $(51, 85)$ comme entrée. Après la première étape, ceci produit les entiers $q = 0$ et $r = 51$. La troisième étape produit alors $(187, 51)$. On retourne à la première étape qui produit $q = 3$ et $r = 34$. La troisième étape produit alors $(51, 34)$. La première étape produit alors $q = 1$ et $r = 17$. La troisième étape produit alors $(34, 17)$. La première étape produit alors $q = 2$ et $r = 0$. La deuxième étape rend alors comme résultat 17.

2.2 L'équation $ax + by = c$

Soit a, b, c trois entiers. Supposons que l'on souhaite trouver tous les couples d'entiers (x, y) tel que $ax + by = c$.

Remarque : L'ensemble des points (x, y) du plan (identifié avec $\mathbb{R}^2$) qui vérifient $ax + by = c$ est une droite. La question que l'on se pose est donc de trouver les points à coordonnées entières sur les droites.

Par définition, si l'équation $ax + by = c$ admet des solutions avec x, y entiers, alors c appartient à $(a, b) = (a \wedge b)$. Donc $a \wedge b$ divise c. Réciproquement, si $a \wedge b$ divise c, alors c s'écrit $c = nd$ et $d = ax_0 + by_0$ donc $nax_0 + nbx_0 = c$ est une solution entière de l'équation $ax + by = c$.

Proposition 2.1. *Soit a, b, c trois entiers et $d = a \wedge b$. Si $d \nmid c$, alors l'équation $ax + by = c$ n'admet pas de solution entière. Si $d|c$, écrivons $a = a'd$, $b = b'd$ et $c = c'd$. Soit (x_0, y_0) une solution de $a'x_0 + b'y_0 = 1$. Les solutions de l'équation $ax + by = c$ sont :*

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

Démonstration. Nous avons déjà vu que si $d \nmid c$, alors l'équation $ax+by = c$ n'admet pas de solution entière. Supposons donc $d|c$. Un couple d'entier (x, y) est une solution de $ax+by = c$ si et seulement si c'est une solution de $a'x + b'y = c'$. Une solution est donc donnée par $(c'x_0, c'y_0)$. Soit (x_1, y_1) une autre solution. Alors :

$$a'x_1 - a'c'x_0 = b'c'y_0 - b'y_1$$

Soit encore :

$$a'(x_1 - c'x_0) = b'(c'y_0 - y_1)$$

Donc a' divise $b'(c'y_0 - y_1)$. Comme $a' \wedge b' = 1$, a' divise $c'y_0 - y_1$. Il existe donc $k \in \mathbb{Z}$ tel que $y_1 = c'y_0 - ka'$. Mais alors $(x_1 - c'x_0) = kb'$. Finalement, $x_1 = c'x_0 + kb'$ et $y_1 = c'y_0 - ka'$. Réciproquement, le couple $(c'x_0 + kb', y_1 = c'y_0 - ka')$ avec k entier est bien une solution. □

Pour compléter la proposition précédente, il suffit de détermine un moyen de trouver une solution entière à l'équation $ax + by = d$ lorsque $d = a \wedge b$. Nous allons pour cela adapter l'algorithme d'Euclide. Ce nouvel algorithme prend en entrée un couple d'entier (a, b).

1. Initialiser n à la valeur 0. Transformer le couple (a, b) en quintuplet :

$$(r_0, r_1, q_0, u_0, u_1, v_0, v_1) = (a, b, 0, 1, 0, 0, 1)$$

2. Réaliser la division euclidienne de r_n par r_{n+1}. Ceci produit des entiers q_{n+1} et r_{n+2}. Transformer le quintuplet $(r_n, r_{n+1}, q_n, u_n, u_{n+1}, v_n, v_{n+1})$ en :

$$(r_{n+1}, r_{n+2}, q_{n+1}, u_{n+1}, u_n - q_{n+1}u_{n+1}, v_{n+1}, v_n - q_{n+1}v_{n+1})$$

3. Si le deuxième terme de ce quintuplet est nul, alors rendre comme résultat le triplet $(r_{n+1}, u_{n+1}, v_{n+1})$.

4. Sinon, ajouter 1 à n et retourner en 2.

Lemme 2.2. *Dans l'algorithme précédent, on a pour tout n, $r_n = au_n + bv_n$. En particulier, le résultat rendu vérifie $a \wedge b = au + bv$.*

Démonstration. Si $n = 0$, $r_0 = a$, $u_0 = 1$ et $v_0 = 0$ donc l'égalité est vérifiée. Si $n = 1$, $r_1 = b$, $u_1 = 0$ et $v_1 = 1$ donc l'égalité est vérifiée. Si la relation est vraie pour n et $n-1$, alors $r_{n-1} = q_n r_n + r_{n+1}$ donc :

$$\begin{aligned} r_{n+1} &= r_{n-1} - q_n r_n = au_{n-1} + bv_{n-1} - q_n au_n + q_n bv_n \\ &= a(u_{n-1} - q_n u_n) + b(v_{n-1} - q_n v_n) = au_{n+1} + bv_{n+1} \end{aligned}$$

Appliquer ceci au dernier reste non-nul démontre la deuxième assertion. □

On peut de façon commode présenter les calculs dans un tableau de la manière suivante :

	q_1	q_2	$\cdots$	q_{n-1}	q_n
$r_0 = a$	$r_1 = b$	r_2	$\cdots$	r_{n-1}	r_n
1	0	u_2	$\cdots$	u_{n-1}	u_n
0	1	v_2	$\cdots$	v_{n-1}	v_n

Exemple : Calculons $d = 17640 \wedge 525$ ainsi qu'une relation $17640a + 525b = d$.

$$\begin{aligned} 17640 &= 33 \cdot 525 + 315 \\ 525 &= 315 + 210 \\ 315 &= 210 + 105 \\ 210 &= 2 \cdot 105 \end{aligned}$$

Donc $d = 105$.

	33	1	1	2
17640	525	315	210	105
1	0	1	-1	2
0	1	-33	34	-67

Donc $2 \cdot 17640 - 67 \cdot 525 = 105$.

En pratique, pour des petits entiers (disons plus petits que 10 000), il est en général plus rapide de calculer la plus grand diviseur commun de deux entiers en utilisant la décomposition en facteurs premiers qu'en utilisant l'algorithme d'Euclide. L'avantage de l'algorithme d'Euclide est de produire une solution à l'équation $ax + by = d$. En revanche, pour des entiers plus grands (ou même pour des entiers relativement petit si l'on a pas de chance), l'algorithme d'Euclide est considérablement plus rapide.

3 $\mathbb{Z}/n\mathbb{Z}$

3.1 Définition

Soit n un entier strictement positif. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble $\mathbb{Z}$ dans lequel on décide que deux entiers x et y sont égaux si et seulement si $x - y$ est divisible par n. On écrit

$$x \equiv y \bmod n$$

et l'on dit que x et y sont égaux modulo n ou encore que x modulo n est égal à y.

Exemples : Le calcul modulo 12 (ou 24) est relativement commun : on sait bien que 5 heures après 20 heures, il est 1 heure du matin, et non 25 heures. De la même façon, le calcul modulo 7 peut s'interpréter comme le calcul du jours de la semaine : si le premier janvier tombe un dimanche (comme ce sera le cas en 2012), cela implique qu'il était tombé un samedi en 2011 et qu'il tombera un mardi en 2013 (car 2012 est une année bisextile).

Proposition 3.1. *Soit a un entier et n un entier strictement positif.*

1. *Soit r le reste de la division euclidienne de a par n. Alors $a \equiv r \bmod n$.*
2. *Il existe n entiers $x_1, \cdots, x_n$ que l'on peut choisir égaux à $0, \cdots, n-1$ tels que pour tout $x \in \mathbb{Z}$, il existe un x_i avec $x \equiv x_i \bmod n$.*

Démonstration. 1. En effet, $a - r$ s'écrit $a - r = qn$ donc $n|(a - r)$.

2. D'après la première assertion, on peut prendre pour les x_i les restes possibles de la division euclidienne par n.

□

3.2 Compatibilité avec les opérations usuelles

Proposition 3.2. *Soit $(a, b) \in \mathbb{Z}^2$ deux entiers et n un entier strictement positif. Supposons $a \equiv x \bmod n$ et $b \equiv x \bmod n$. Alors $a + b \equiv x + y \bmod n$ et $ab \equiv xy \bmod n$. En particulier $a^s \equiv x^s \bmod n$ pour tout $s \geq 0$. L'équation $ax \equiv b \bmod n$ admet des solutions si et seulement si $a \wedge n$ divise b.*

Démonstration. Par définition, $n|(a - x)$ et $n|(b - y)$. Donc $n|(a + b - x - y)$. Écrivons x et y en fonction de a, b et n.

$$a = qn + x$$
$$b = q'n + y$$

Alors $ab = n(qq'n + xq' + yq) + xy$. Donc $n|(ab - xy)$. En appliquant de façon répétée ce résultat, on obtient que $a^s \equiv x^s \bmod n$. L'équation $ax \equiv b \bmod n$ admet des solutions si et seulement si $ax - ny = b$ admet des solutions. Nous savons que cela est le cas si et seulement si $a \wedge n$ divise b. □

Ceci permet de calculer modulo n, ou dans $\mathbb{Z}/n\mathbb{Z}$, comme si on calculait dans $\mathbb{Z}$, mais en simplifiant grandement les opérations.

3.3 Preuves par $3, 9, 11, n$

Soit n un entier strictement positif. Soit $x = \overline{c_s c_{s-1} \cdots c_0}$ un entier écrit en base 10. Par définition, $x = 10^s c_s + 10^{s-1} c_{s-1} + \cdots + 10c_1 + c_0$. Pour calculer $x \bmod n$, il suffit donc de calculer les $c_i \bmod n$ et les $10^{s_i} \bmod n$. Donnons quelques exemples.

Le cas $n = 2, 5$ Dans ce cas, $10^{s_i} \bmod n$ est égal à zéro dès que $s_i \neq 0$. Donc $x \equiv c_0 \bmod n$. Ceci implique que x est pair si et seulement si c_0 est pair et que x est divisible par 5 si et seulement si c_0 est divisible par 5.

Le cas $n = 4, 25$ Dans ce cas, $10^{s_i} \bmod n$ est égal à zéro dès que $s_i \geq 1$. Donc $x \equiv \overline{c_1 c_0} \bmod n$. Ceci implique que x est divisible par 4 si et seulement si $\overline{c_1 c_0}$ est divisible par 4 et que x est divisible par 25 si et seulement si $\overline{c_1 c_0}$ est divisible par 25.

Le cas $n = 3, 9$ Dans ce cas, $10 \equiv 1 \bmod n$ donc $10^s \equiv 1 \bmod n$ pour tout $s \geq 0$ donc $x \equiv c_s + c_{s-1} + \cdots + c_1 + c_0$. Ceci implique qu'un entier moins la somme de ses chiffres est divisible par 9.

En comparant ces résultats avec la proposition 3.2, on en déduit qu'une addition, une multiplication ou une soustraction ne peut être juste que si elle est juste sur les deux derniers chiffres (preuve par 4) et si elle demeure juste lorsque que l'on l'effectue sur la somme des chiffres (preuve par 9).

Le cas $n = 11$ Dans ce cas, $10 \equiv -1 \bmod n$ donc $10^s \equiv (-1)^s \bmod n$ pour tout $s \geq 0$ donc $x \equiv (-1)^s c_s + (-1)^{s-1} c_{s-1} + \cdots - c_1 + c_0$. Ceci implique qu'un entier est divisible par 11 si et seulement si la somme alternée de ses chiffres est divisible par 11.

Le cas général

Proposition 3.3. *Soit $n > 0$ un entier premier à 10. Il existe un entier $s > 0$ tel que $10^s \equiv 1 \bmod n$. Soit t un entier et $r(t)$ le reste de la division euclidienne de t par s. Alors $10^t \equiv 10^r \bmod n$. Donc $x \equiv c_t 10^{r(t)} + c_{t-1} 10^{r(t-1)} + \cdots + 10c_1 + c_0 \bmod n$.*

Démonstration. Les puissances successives de 10 sont congrues à des éléments de $\mathbb{Z}/n\mathbb{Z}$. Parmi les $n+1$ premières puissances de 10-à savoir $1, 10, \cdots, 10^n$-deux sont nécessairement égales. Disons que $10^s \equiv 10^{s'} \bmod n$ avec $s > s'$. L'équation $10z \equiv 1 \bmod n$ admet une solution donc, en multipliant par $z^{s'}$ à gauche et à droite, $10^{s-s'} \equiv 1 \bmod n$. Donc $10^t \equiv 10^{qs+r(t)} \equiv (10^s)^q 10^{r(t)} \equiv 10^{r(t)} \bmod n$. □

Traitons le cas $n = 7$.

$$\begin{aligned} 10 &\equiv 3 \bmod 7 \\ 10^2 &\equiv 2 \bmod 7 \\ 10^3 &\equiv 6 \bmod 7 \\ 10^4 &\equiv 4 \bmod 7 \\ 10^5 &\equiv 5 \bmod 7 \\ 10^6 &\equiv 1 \bmod 7 \end{aligned}$$

Donc $10^t \equiv 10^{t \bmod 6} \bmod 7$. Donc $x \equiv c_s 10^{s \bmod 6} + \cdots + 2c_2 + 3c_1 + c_0 \bmod 7$. Pour $x = 87654392$, par exemple, on obtient :

$$\begin{aligned} x &\equiv 2 + 9.3 + 3.2 + 4.6 + 5.4 + 6.5 + 7.1 + 8.3 \bmod 7 \\ &\equiv 2 + 27 + 6 + 24 + 20 + 30 + 7 + 24 \bmod 7 \\ &\equiv 0 \bmod 7 \end{aligned}$$