♦ Chapitre 1. Divisibilité et congruences dans $\mathbb{Z}$

I. — Introduction

L'arithmétique ou théorie des nombres est une branche des mathématiques consacrée à l'étude des nombres entiers. Il existe deux types de nombres entiers : les entiers naturels (0, 1, 2, ...) et les entiers relatifs (..., −2, −1, 0, 1, 2, ...). L'ensemble des entiers naturels se note $\mathbb{N}$ et l'ensemble des entiers relatifs se note $\mathbb{Z}$. Tout entier naturel est un entier relatif mais la réciproque est fausse. Par exemple, $-2 \in \mathbb{Z}$ mais $-2 \notin \mathbb{N}$. Avec une notation ensembliste, $\mathbb{N} \subset \mathbb{Z}$ mais $\mathbb{Z} \not\subset \mathbb{N}$.

Sauf mention explicite du contraire, l'expression *entier* désigne un *entier relatif*.

Dans ce cours, on utilisera deux axiomes i.e. deux propriétés considérées comme des évidences et qui ne demandent pas de démonstration.

Axiome 1

Pour tout nombre réel x, il existe un unique entier n tel que $n \leqslant x < n+1$.

Exemple 2. Si $x = 2{,}4$ alors $n = 2$, si $x = \pi$ alors $n = 3$, si $x = -\sqrt{19}$ alors $n = -5$.

Définition 3

Soit x un réel. L'unique entier n tel que $n \leqslant x < n+1$ est appelé la partie entière de x. On le note $E(x)$.

Exemple 4. $E(2{,}4) = 2$, $E(\pi) = 3$, $E(-\sqrt{19}) = -5$.

Axiome 5

Toute partie non vide de $\mathbb{N}$ admet un plus petit élément. Autrement dit, si A est une partie non vide de $\mathbb{N}$, il existe un élément $a \in A$ tel que, pour tout $n \in A$, $a \leqslant n$.

Exemple 6. Si A est l'ensemble des entiers naturels impairs alors $\min(A) = 1$. Si A est l'ensemble des cubes dont l'écriture décimale contient au moins 2 chiffres alors $\min(A) = 27$.

II. — Divisibilité dans $\mathbb{Z}$

1) Définition et propriétés

Définition 7

Soit a et b deux entiers. On dit que b divise a (ou que b est un diviseur de a ou encore que a est un multiple de b) s'il existe un entier k tel que $a = k \times b$. On note alors $b \mid a$.

L'écriture logique de cette définition est

$$b \mid a \Leftrightarrow \exists k \in \mathbb{Z} \quad a = k \times b.$$

Exemple 8.

1. 3 divise 36 car $36 = 3 \times 12$. On peut remarquer qu'on en déduit également que 12 divise 36. Les diviseurs fonctionnent par paire. L'ensemble des diviseurs de 36 est
$$\mathcal{D}(36) = \{-36, -18, -12, -9, -4, -3, -2, -1, 1, 2, 3, 4, 9, 12, 18, 36\}.$$
2. 1 et -1 sont des diviseurs de tout entier a car $a = 1 \times a = (-1) \times (-a)$. De même, pour tout entier a, a et $-a$ divisent a.
3. Tout entier a divise 0 car $0 = a \times 0$. En revanche, 0 ne divise que 0.

Propriété 9

Soit a et b deux entiers. Démontrer les équivalences suivantes :
$$b \mid a \Leftrightarrow (-b) \mid a \Leftrightarrow b \mid (-a) \Leftrightarrow (-b) \mid (-a).$$

Démonstration. Supposons que b divise a. Alors, il existe un entier k tel que $a = kb$ donc $a = (-k)(-b)$ et, comme $-k$ est un entier, $-b$ divise a. Ainsi,
$$b \mid a \Rightarrow (-b) \mid a.$$
Supposons que $-b$ divise a. Alors, il existe un entier k tel que $a = k(-b)$ donc $-a = kb$ et ainsi b divise $-a$. On a donc montré que
$$(-b) \mid a \Rightarrow b \mid (-a).$$
Supposons que $b \mid (-a)$. Alors, en appliquant le premier point aux entiers b et $-a$, on a que $-b$ divise $-a$. Ainsi,
$$b \mid (-a) \Rightarrow (-b) \mid (-a).$$
Enfin, supposons que $-b$ divise $-a$. Alors, il existe un entier k tel que $-a = k(-b)$ donc $a = kb$ i.e. b divise a. Ainsi,
$$(-b) \mid (-a) \Rightarrow b \mid a.$$
On a donc montré que
$$b \mid a \Rightarrow (-b) \mid a \Rightarrow b \mid (-a) \Rightarrow (-b) \mid (-a) \Rightarrow b \mid a$$
ce qui suffit pour conclure. □

Remarque 10. En conséquence, les diviseurs de a sont exactement les diviseurs de $-a$ et à chaque diviseur positif b de a correspond un et un seul diviseur négatif $-b$.

Propriété 11

Soit a et b deux entiers.

1. Si $b \mid a$ et si $a \neq 0$ alors $|b| \leqslant |a|$. Si, de plus, a et b sont positifs alors b est compris entre 1 et a.
2. Un entier non nul a admet un nombre fini de diviseurs.
3. Si $b \mid a$ et $a \mid b$ alors $|a| = |b|$. Si, de plus, a et b sont positifs alors $a = b$.

Démonstration.

1. Supposons que $b \mid a$ et $a \neq 0$. Alors, il existe un entier k tel que $a = kb$ et, comme $a \neq 0$, $k \neq 0$ et donc $|a| = |kb| = |k|\,|b|$. Comme $|k|$ est un entier naturel non nul, $|k| \geqslant 1$ donc, en multipliant par $|b| \geqslant 0$, $|k|\,|b| \geqslant |b|$ i.e. $|a| \geqslant |b|$.

Si, de plus, a et b sont positifs, $|a| = a$ et $|b| = b$ donc $a \geqslant b \geqslant 0$. Or, comme $a \neq 0$, $b \neq 0$ donc, comme b est entier, $1 \leqslant b \leqslant a$.

2. Soit a un entier non nul. Si b est un diviseur de a alors, d'après le point **1.**, $1 \leqslant |b| \leqslant |a|$ donc a possède, au plus, $2\,|a|$ diviseurs positifs.

3. Supposons que b divise a et a divise b.

1er cas. Si $a = 0$ ou $b = 0$.

Si $a = 0$ alors, comme $a \mid b$, $b = 0$. De même, si $b = 0$, comme $b \mid a$, $a = 0$.

Ainsi, dans les deux cas, $a = b$.

2ième cas. Si $a \neq 0$ et $b \neq 0$.

Alors, d'après le point **1.**, $|b| \leqslant |a| \leqslant |b|$ donc $|a| = |b|$.

Ainsi, dans tous les cas, $|a| = |b|$.

Si, de plus, a et b sont positifs, on a donc $a = b$.

□

Propriété 12

Soit a, b et c des entiers.

1. Si $c \mid b$ et $b \mid a$ alors $c \mid a$ (on dit que la divisibilité est *transitive*).

2. Si a divise b alors, pour tout entier m, $mb \mid ma$.

3. Si c divise a et c divise b alors c divise toute combinaison linéaire de a et b i.e. tout nombre entier de la forme $ua + vb$ où u et v sont des entiers.

Démonstration.

1. Supposons que $c \mid b$ et $b \mid a$. Alors, il existe un entier k tel que $b = kc$ et un entier k' tel que $a = k'b$ donc $a = k'(kc) = (kk')c$. Or, comme k et k' sont des entiers, kk' est un entier donc c divise a.

2. Supposons que $b \mid a$. Alors, il existe un entier k tel que $a = kb$ donc $ma = m(kb) = k(mb)$ donc mb divise ma.

3. Supposons que c divise a et b. Alors, il existe des entiers k et k' tels que $a = kc$ et $b = k'c$. Soit u et v deux entiers. On a alors $ua + vb = u(kc) + v(k'c) = (uk + vk')c$ donc, comme $uk + vk'$ est un entier, c divise $ua + vb$.

□

Remarque 13. En particulier, si c divise a et b alors c divise $a + b$, $a - b$ et ma pour tout $m \in \mathbb{Z}$.

Exercice 14.

1. Déterminer l'ensemble des entiers naturels n tels que $2n + 3$ divise 15.

2. Déterminer l'ensemble des entiers naturels n tels que 15 divise $n + 22$.

3. Déterminer l'ensemble des entiers naturels n tels que $n + 15$ divise $2n + 3$.

solution

1. Pour tout $n \in \mathbb{N}$, $2n + 3 \geqslant 3$ et les diviseurs de 15 supérieurs ou égaux à 3 sont 3, 5 et 15 donc $2n + 3$ divise 15 si et seulement si $2n + 3 \in \{3\,;5\,;15\}$. Ceci équivaut à dire que $n \in \{0\,;1\,;6\}$. Ainsi, l'ensemble des entiers naturels n tels que $2n + 3$ divise 15 est $\{0\,;1\,;6\}$.

2. Soit $n \in \mathbb{N}$. Si 15 divise $n+22$ alors il existe un entier k tel que $n+22 = 15k$ i.e. $n = 15k-22$. Réciproquement, s'il existe un entier k tel que $n = 15k-22$ alors $n+22 = 15k$ donc 15 divise $n+22$. De plus, $15k-22 \geqslant 0$ si et seulement si $15k \geqslant 22$ i.e. $k \geqslant \frac{22}{15}$ soit encore $k \geqslant 2$ car k est entier. Ainsi, l'ensemble des entiers naturels n tels que 15 divise $n+22$ est $\{15k-22 \mid k \in \mathbb{N} \setminus \{0\,;1\}\}$.

3. Soit $n \in \mathbb{N}$ tel que $n+15$ divise $2n+3$. Alors, $n+15$ divise $n+15$ et $2n+3$ donc $n+15$ divise $2(n+15)-(2n+3) = 27$. Or, n est positif donc $n+15 \geqslant 15$ et l'unique diviseur de 27 supérieur ou égal à 15 est 27 donc $n+15 = 27$ i.e. $n = 12$. Réciproquement, si $n = 12$ alors $n+15 = 27$ et $2n+3 = 27$ donc $n+15$ divise $2n+3$. On conclut que l'ensemble des entiers naturels n tels que $n+15$ divise $2n+3$ est $\{27\}$.

2) Division euclidienne

Théorème 15

Soit a et b deux entiers tels que $b > 0$. Alors, il existe un unique entier relatif q et un unique entier naturel r tels que

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

Démonstration. Supposons qu'il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ avec $r < b$ tels que $a = bq+r$. Alors, en divisant par $b > 0$, $\frac{a}{b} = q + \frac{r}{b}$ avec $0 \leqslant \frac{r}{b} < 1$ donc $\frac{a}{b} \leqslant q < \frac{a}{b}+1$. Comme q est entier, par définition, $q = E(\frac{a}{b})$ et alors $r = a - bE(\frac{a}{b})$.

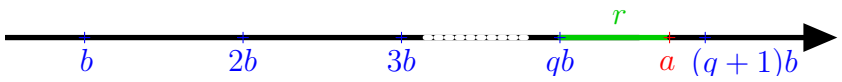
Réciproquement, si on pose $q = E(\frac{a}{b})$ et $r = a-bq$ alors, par définition, q et r sont des entiers tels que $a = bq+r$. De plus, $\frac{a}{b} \leqslant q < \frac{a}{b}+1$ donc, en multipliant par $b > 0$, $a \leqslant bq < a+b$ i.e. $0 \leqslant a-bq < b$ soit $0 \leqslant r < b$.

On conclut que $q = E(\frac{a}{b})$ et $r = a-bq$ sont les seuls entiers tels que $a = bq+r$ et $0 \leqslant r < b$. □

Définition 16

L'écriture $a = bq+r$ avec $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ tel que $r < b$ est appelée la division euclidienne de a par b. Le nombre a est appelé le dividende, le nombre b est appelé le diviseur, le nombre q est appelé le quotient et le nombre r est appelé le reste dans cette division.

Représentation graphique (lorsque $a > b$) :



Exemple 17. Effectuer la division euclidienne de 1315 par 24.

On « pose » la division :

$$\begin{array}{r|l} 1\,3\,1\,5 & 2\,4 \\ \hline 1\,1\,5 & 5\,4 \\ 1\,9 & \end{array}$$

Ainsi, la division euclidienne de 1315 par 24 est $1315 = 24 \times 54 + 19$.

Remarque 18. Lorsque $0 \leqslant a < b$ alors $q = 0$ et $r = a$.

Propriété 19

Soit a et b deux entiers tels que $b > 0$. Alors, b divise a si et seulement si le reste dans la division euclidienne de a par b est nul.

Démonstration. Supposons que b divise a. Alors, il existe un entier k tel que $a = kb$. Ainsi, $a = kb + 0$ avec $0 \leqslant 0 < b$ donc $a = kb + 0$ est la division euclidienne de a par b et donc $r = 0$.

Réciproquement, si le reste dans la division euclidienne de a par b est 0 alors il existe un entier q tel que $a = bq + 0 = bq$ donc b divise a. □

Méthode 20

L'existence de la division euclidienne assure que, si b est un entier naturel non nul, alors tout entier peut s'écrire sous l'une des formes bq, $bq+1$, $bq+2$, ..., $bq+b-1$. En particulier, tout entier s'écrit sous la forme $2q$ ou $2q+1$ (pair/impair), sous la forme $3q$, $3q+1$ ou $3q+2$. Ceci peut être utile dans certains problèmes de divisibilité.

Exemple 21. Soit un entier n. Démontrer que $n(n^2+5)$ est divisible par 3.

On utilise la méthode précédente en procédant par disjonction de cas.

Soit $n \in \mathbb{N}$. Alors, il existe un entier q tel que $n = 3q$ ou $n = 3q+1$ ou $n = 3q+2$.

Si $n = 3q$ alors 3 divise n donc 3 divise $n(n^2+5)$.

Si $n = 3q+1$ alors $n^2+5 = (3q+1)^2+5 = 9q^2+6q+1+5 = 9q^2+6q+6 = 3(3q^2+2q+2)$ et $3q^2+2q+2$ est un entier donc 3 divise n^2+5 et, ainsi, 3 divise $n(n^2+5)$.

Si $n = 3q+2$ alors $n^2+5 = (3q+2)^2+5 = 9q^2+12q+4+5 = 9q^2+12q+9 = 3(3q^2+4q+3)$ et $3q^2+4q+3$ est un entier donc 3 divise n^2+5 et, ainsi, 3 divise $n(n^2+5)$.

Dans tous les cas, n divise $n(n^2+5)$.

III. — Congruences modulo un entier naturel

1) Définition

Définition 22

Soit m un entier naturel et a et b deux entiers relatifs. On dit que a est congru à b modulo m si m divise $a-b$. On note alors $a \equiv b\ (m)$, $a \equiv b\ [m]$, $a \equiv b \mod m$ ou encore $a \equiv b\ (\mathrm{mod}\ m)$.

Remarque 23. Par définition, on a donc $a \equiv b\ [m]$ si et seulement s'il existe un entier k tel que $a - b = km$ i.e. si et seulement s'il existe un entier k tel que $a = b + km$.

Exemple 24.

1. 17 est congru à 2 modulo 3 car $17 - 2 = 15 = 5 \times 3$. On a aussi $17 \equiv -1\ [3]$ car $17 - (-1) = 18 = 6 \times 3$.
2. 1315 est congru à 19 modulo 24 car $1315 - 19 = 1296 = 24 \times 54$.
3. Deux entiers a et b sont congrus modulo 0 si et seulement s'ils sont égaux car 0 divise $a - b$ si et seulement si $a - b = 0$ i.e. $a = b$.
4. Deux entiers sont toujours congrus modulo 1 car, quels que soient a et b, 1 divise $a - b$.

Propriété 25

Soit m un entier naturel et a, b et c des entiers relatifs. Alors,

1. $a \equiv a\ [m]$ (la congruence est *réflexive*) ;
2. si $a \equiv b\ [m]$ alors $b \equiv a\ [m]$ (la congruence est *symétrique*) ;
3. Si $a \equiv b\ [m]$ et $b \equiv c\ [m]$ alors $a \equiv c\ [m]$ (la congruence est *transitive*).

Démonstration.

1. Comme $a - a = 0 = 0 \times m$, m divise $a - a$ donc $a \equiv a\ [m]$.
2. Supposons que $a \equiv b\ [m]$. Alors, m divise $a - b$ donc (voir l'exercice 3), m divise $b - a$ i.e. $b \equiv a\ [m]$.
3. Supposons que $a \equiv b\ [m]$ et $b \equiv c\ [m]$. Alors, m divise $a - b$ et $b - c$ donc m divise $(a - b) + (b - c) = a - c$ i.e. $a \equiv c\ [m]$.

□

Propriété 26

Soit m un entier naturel non nul et a un entier.

1. Si r est le reste dans la division euclidienne de a par m alors $a \equiv r\ [m]$.
2. m divise a si et seulement si $a \equiv 0\ [m]$.
3. Un entier b est congru à a modulo m si et seulement si a et b ont le même reste dans la division euclidienne par m.

Démonstration.

1. Soit r le reste dans la division euclidienne de a par m. Alors, il existe un entier q tel que $a = bq + r$ donc $a - r = bq$. Ainsi b divise $a - r$ donc $a \equiv r\ [m]$.
2. Supposons que m divise a. Alors, m divise $a - 0$ donc $a \equiv 0\ [m]$. Réciproquement, si $a \equiv 0\ [m]$ alors il existe un entier k tel que $a = 0 + mk = mk$ donc m divise a.
3. Soit b un entier. Notons r le reste dans la division euclidienne de a par m et r' le reste dans la division euclidienne de b par m. D'après le point **1.**, $a \equiv r\ [m]$ et $b \equiv r'\ [m]$.

   Supposons que $b \equiv a\ [m]$. Par symétrie, $r' \equiv b\ [m]$ donc, par transitivité, $r' \equiv a\ [m]$ et donc $r' \equiv r\ [m]$. Dès lors, m divise $r' - r$. Or, $0 \leqslant r < m$ donc $-m < -r \leqslant 0$ et $0 \leqslant r' < m$ donc $-m < r' - r < m$. Ainsi, $r' - r$ est un multiple de m strictement compris entre $-m$ et m donc $r' - r = 0$ i.e. $r' = r$.

   Réciproquement, si $r' = r$ alors $a \equiv r\ [m] \equiv r'\ [m] \equiv b\ [m]$ donc a et b sont congrus modulo m.

□

Corollaire 27

Soit m un entier naturel non nul, a un entier quelconque et r le reste dans la division euclidienne de a par m. Alors, r est l'unique entier de $[\![0, m - 1]\!]$ tel que $a \equiv r\ [m]$.

Démonstration. D'après la propriété précédente, $a \equiv r\ [m]$. Supposons que $r' \in [\![0, m-1]\!]$ soit un entier tel que $a \equiv r'\ [m]$. Alors, par symétrie et transitivité de la congruence, $r' \equiv r\ [m]$ donc, toujours par la propriété précédente, r et r' ont même reste dans la division euclidienne par m. Or, comme r et r' sont compris entre 0 et $m-1$, ils sont leurs propres restes dans la division par m donc $r = r'$. Ainsi, r est bien l'unique entier compris entre 0 et $m-1$ tel que $a \equiv r\ [m]$. □

VOCABULAIRE. — Le reste dans la division euclidienne de a par m est aussi appelé le reste de a modulo m.

2) Compatibilité avec les opérations

Théorème 28

Soit a, b, a' et b' des entiers. Soit m un entier naturel. On suppose que $a \equiv b\ [m]$ et $a' \equiv b'\ [m]$. Alors,

1. $a + a' \equiv b + b'\ [m]$;
2. $a - a' \equiv b - b'\ [m]$;
3. $aa' \equiv bb'[m]$;
4. pour tout entier $n \in \mathbb{N}^*$, $a^n \equiv b^n\ [m]$.

Démonstration.

1. On remarque que $(a+a') - (b+b') = (a-b) + (a'-b')$ et, par hypothèse, m divise $a-b$ et $'-b'$ donc m divise $(a+a') - (b+b')$ i.e. $a + a' \equiv b + b'\ [m]$.
2. De même, $(a-a') - (b-b') = (a-b) - (a'-b')$ donc m divise $(a-a') - (b-b')$ i.e. $a - a' \equiv b - b'\ [m]$.
3. De même, $aa' - bb' = (a-b)a' + (a'-b')b$ donc m divise $aa' - bb'$ i.e. $aa' \equiv bb'\ [m]$.
4. Considérons, pour tout $n \in \mathbb{N}^*$, la proposition P_n : « $a^n \equiv b^n\ [m]$ ».
   Par hypothèse, $a \equiv b\ [n]$ donc P_1 est vraie.
   Soit $k \in \mathbb{N}^*$. Supposons que P_k est vraie. Alors, $a^k \equiv b^k\ [m]$ et, par hypothèse $a \equiv b\ [m]$ donc, grâce au point **3.**, $a^k a \equiv b^k b\ [m]$ i.e. $a^{k+1} \equiv b^{k+1}\ [m]$ donc P_{k+1} est vraie.
   On a donc montré par récurrence que, pour tout $n \in \mathbb{N}^*$, $a^n \equiv b^n\ [m]$.

□

Remarque 29.

1. Étant donné que tout entier k est congru à lui-même modulo m, on déduit du point **3.** que, si $a \equiv b\ [m]$ alors $ka \equiv kb\ [m]$.
2. En revanche, même si a et b sont divisible par d, on ne peut en général pas diviser une congruence. Par exemple, $12 \equiv 6\ [2]$ mais $2 \not\equiv 1\ [2]$. Cependant, si a, b et m sont des entiers tels que $a \equiv b\ [m]$ et si a, b et m sont divisibles par un entier $k > 0$ alors $\frac{a}{k} \equiv \frac{b}{k}\ \left[\frac{m}{k}\right]$. En effet, si $a \equiv b\ [m]$ alors m divise $a-b$ donc il existe un entier d tel que $a - b = dm$ et, en divisant par k, $\frac{a}{k} - \frac{b}{k} = d\frac{m}{k}$ donc, comme $\frac{a}{k}$, $\frac{b}{k}$ et $\frac{m}{k}$ sont des entiers, $\frac{a}{k} \equiv \frac{b}{k}\left[\frac{m}{k}\right]$.
3. Le point **4.** reste vrai pour $n = 0$ si a et b sont non nuls.

Exemple 30.

1. Démontrer que, pour tout entier naturel n, $10^n - 1$ est divisible par 9.
   Comme $10 - 1 = 9$, $10 \equiv 1\ [9]$ donc, pour tout entier naturel n, $10^n \equiv 1^n\ [9]$ i.e. $10^n \equiv 1\ [9]$ ce qui signifie que 9 divise $10^n - 1$.

2. Démontrer que, pour tout $n \in \mathbb{N}$, $n(n^2+5)$ est divisible par 3.

On utilise un tableau de reste modulo 3 :

Reste de n modulo 3	0	1	2
Reste de n^2+5 modulo 3	0	0	0
Reste de $n(n^2+5)$ modulo 3	0	0	0

Dans tous les cas, $n(n^2+5) \equiv 0\ [3]$ donc, pour tout $n \in \mathbb{N}$, 3 divise $n(n^2+5)$.

3. Déterminer l'ensemble des entiers x tels que $2x \equiv 4\ [5]$.

On utilise là aussi un tableau de restes modulo 5 :

Reste de x modulo 5	0	1	2	3	4
Reste de $2x$ modulo 5	0	2	4	1	3

On en déduit que $2x \equiv 4\ [5]$ si et seulement si $x \equiv 2\ [5]$ donc l'ensemble des entiers x tels que $2x \equiv 4\ [5]$ est $\{2+5k \mid k \in \mathbb{Z}\}$.

Même question avec $3x \equiv 5\ [6]$.

On raisonne de même :

Reste de x modulo 6	0	1	2	3	4	5
Reste de $2x$ modulo 6	0	3	0	3	0	3

On en déduit que, quel que soit l'entier x, $2x \not\equiv 5\ [6]$ donc l'ensemble des entiers x tels que $2x \equiv 5\ [6]$ est $\varnothing$.

4. Déterminer le chiffre des unités dans l'écriture décimale de $N = 2013^{2014}$.

Remarquons que le chiffre des unités de N est son reste modulo 10. On peut déjà commencer par réduire 2013 modulo 10 : $2013 \equiv 3\ [10]$ donc $N \equiv 2^{2014}\ [10]$.

Ensuite, on cherche une « bonne » puissance de 3 modulo 10 i.e. une puissance dont le reste est 1. On a $3^1 \equiv 3\ [10]$, $3^1 \equiv 3\ [10]$, $3^1 \equiv 3\ [10]$, $3^1 \equiv 3\ [10]$, $3^2 \equiv 9\ [10]$, $3^3 \equiv 7\ [10]$ et $3^4 \equiv 1\ [10]$.

On effectue alors la division euclidienne de 2014 par 4 : $2014 = 4 \times 503 + 2$. On a donc

$$A \equiv 3^{4\times 503+2}\ [10] \equiv \left(3^4\right)^{503} \times 3^2\ [10] \equiv 1^{503} \times 9\ [10] \equiv 9\ [10]$$

et ainsi le chiffre des unités de A est 9.

5. Étudier les restes possibles pour un carré modulo 8 et en déduire que l'équation $x^2 - 5y^2 = 2014$ n'a pas de solutions dans $\mathbb{Z}^2$.

Soit n un entier. On dresse un tableau de restes modulo 8

Reste de n modulo 8	0	1	2	3	4	5	6	7
Reste de n^2 modulo 8	0	1	4	1	0	1	4	1

Ensuite, on dresse un tableau à double entrée donnant les restes possibles pour $x^2 - 5y^2$ modulo 8 :

x^2 \ y^2	0	1	4
0	0	3	4
1	1	4	5
4	4	7	0

Ainsi, si x et y sont deux entiers, les restes possibles pour $x^2 - 5y^2$ sont 0, 1, 3, 4, 5 et 7. Or, s'il existe deux entiers x et y tels que $x^2 - 5y^2 = 2014$ alors le reste de $x^2 - 5y^2$ modulo 8 est le même que celui de 2014. Or, $2014 = 251 \times 8 + 6$ donc le reste de 2014 modulo 8 est 6 et 6 n'est pas un reste possible pour $x^2 - 5y^2$ donc l'équation $x^2 - 5y^2 = 2020$ n'a pas de solution dans $\mathbb{Z}^2$.

IV. — Bases de numération et critères de divisibilité

1) Numération en base $b \geqslant 2$

Lorsque nous écrivons le nombre $N = 72543$, cela représente le nombre $7 \times 10^4 + 2 \times 10^3 + 5 \times 10^2 + 4 \times 10^1 + 3 \times 10^0$. On dit que cette écriture est l'écriture décimale ou encore que c'est l'écriture de N en base 10. Cela signifie qu'on décompose le nombre N comme une somme de puissances entières de 10, les *chiffres* étant alors les entiers naturels strictement inférieurs à 10 : 0, 1, 2, ..., 9.

Cette notation des nombres n'a pas été la seule au cours de l'histoire. Par exemple, les Babyloniens, dès le 2e millénaire avant J.-C., ont été les premiers a utilisé ce type d'écriture (appelée écriture de position) mais ils utilisaient la base 60 : c'est ce qu'on appelle la numération sexagésimale. Dans cette écriture, il y a 60 chiffres qui sont 00, 01, 02, ..., 59. (On écrit 01, 02, ..., 09 plutôt que 0, 1, ..., 9 car il pourrait sinon y avoir ambiguïté, par exemple, pour le nombre 13 qui pourrait aussi bien signifier 13 que $1 \times 60 + 3 = 63$. En fait, les premiers Babyloniens ne disposaient pas du zéro et laissaient un espace entre les tranches de 2 chiffres). Ainsi, l'écriture sexagésimale de $N = 72543$ est 200903 car $72543 = 20 \times 60^2 + 9 \times 60 + 3$. L'écriture sexagésimale a laissé des traces jusqu'à nos jours par exemple dans la mesure du temps (une minute est découpée en 60 secondes) ou dans la mesure des angles en degré (un degré est divisé en 60 minutes).

Pour distinguer les différentes numérations, on utilisera la notation suivante : $\overline{200903}^{60}$ signifie que le nombre est écrit en base 60 alors que $\overline{72543}^{10}$ signifie que le nombre est écrit en base 10. Le plus souvent, pour la base 10, on omet le 10 à côté de la barre.

D'autres bases ont été ou sont utilisées. Les Mayas comptaient en base 20 (numération vicésimal). De nos jours, la base 2 est utilisée en informatique : on parle d'écriture binaire. En binaire, il n'y a que 2 chiffres qui sont 0 et 1. Par exemple, 5 s'écrit en binaire $\overline{101}^2$ car $5 = 1 \times 2^2 + 0 \times 2 + 1$.

Les chiffres ne sont qu'une question de convention. Par exemple, en base 12, on peut décider que les chiffres sont 0, 1, 2, ..., 9, A et B plutôt que 00, 01, 02, ..., 09, 10 et 11 (ce qui évite de rajouter un 0 devant les 10 premiers). Ainsi, avec cette convention, en base 12, 72543 s'écrit $\overline{35B93}^{12}$ car $72543 = 3 \times 12^4 + 5 \times 12^3 + 11 \times 12^2 + 9 \times 12 + 3$.

Méthode 31 : Comment déterminer l'écriture en base entière b ?

1. On cherche la puissance entière k de b telle que $b^k \leqslant N < b^{k+1}$.
2. On effectue la division euclidienne de N par b^k. On note a_k le quotient et r_{k-1} le reste.
3. On effectue la division euclidienne de r_{k-1} par b^{k-1}. On note a_{k-1} le quotient et r_{k-2} le reste.
4. On réitère l'opération pour trouver a_{k-2}, r_{k-3}, puis a_{k-3}, r_{k-4}, ... et enfin a_1, r_0. On pose, de plus, $a_0 = r_0$.
5. L'écriture de N en base b est alors $\overline{a_k a_{k-1} \cdots a_0}^b$. Cette écriture a donc $k+1$ chiffres en base b.

Exemples.

1. Écrire le nombre $N = \overline{72543}$ en base 9.

On a $9^5 \leqslant N < 9^6$ donc $k = 5$. On effectue ensuite les divisions euclidiennes :

$$\begin{aligned} N &= 1 \times 9^5 + 13494 \\ 13494 &= 2 \times 9^4 + 372 \\ 372 &= 0 \times 9^3 + 372 \\ 372 &= 4 \times 9^2 + 48 \\ 48 &= 5 \times 9 + 3 \end{aligned}$$

Ainsi, $N = 1 \times 9^5 + 2 \times 9^4 + 0 \times 9^3 + 4 \times 9^2 + 5 \times 9 + 3 \times 9^0$ donc $N = \overline{120453}^9$.

2. Combien le nombre $N = \overline{72543}$ a-t-il de chiffres dans son écriture binaire ?
Étant donné que $2^{16} \leqslant N < 2^{17}$, l'écriture binaire de N possède 17 chiffres.

2) Critères de divisibilité en base 10

Propriété 32

On considère un entier N écrit en base 10 : $N = \overline{a_k a_{k-1} \cdots a_0}$.

1. N est divisible par 2 si et seulement si a_0 est pair.

2. N est divisible par 3 (resp. par 9) si et seulement si $\sum_{i=0}^{k} a_i$ est divisible par 3 (resp. par 9).

3. N est divisible par 4 si et seulement si l'entier $\overline{a_1 a_0}$ est divisible par 4.

4. N est divisible par 5 si et seulement si $a_0 = 0$ ou $a_0 = 5$.

5. N est divisible par 8 si et seulement si l'entier $\overline{a_2 a_1 a_0}$ est divisible par 8.

6. N est divisible par 11 si et seulement si $\sum_{i=0}^{k} (-1)^i a_i$ est divisible par 11.

Démonstration. Par définition, $N = \sum_{i=0}^{k} a_i 10^i$.

1. Comme $10 \equiv 0\ [2]$, pour tout entier $i \geqslant 1$, $10^i \equiv 0\ [2]$ donc $N \equiv a_0\ [2]$. Ainsi,

$$2 \mid N \Leftrightarrow N \equiv 0\ [2] \Leftrightarrow a_0 \equiv 0\ [2] \Leftrightarrow 2 \mid a_0.$$

Ainsi, 2 divise N si et seulement si a_0 est pair.

2. Comme $10 \equiv 1\ [3]$, pour tout entier $i \geqslant 0$, $10^i \equiv 1\ [3]$ donc $N \equiv \sum_{i=0}^{k} a_i\ [3]$. Ainsi,

$$3 \mid N \Leftrightarrow N \equiv 0\ [3] \Leftrightarrow \sum_{i=0}^{k} a_i \equiv 0\ [3] \Leftrightarrow 3 \mid \sum_{i=0}^{k} a_k.$$

Ainsi, 3 divise N si et seulement si 3 divise $\sum_{i=0}^{k} a_i$.

La démonstration est identique pour la divisibilité par 9 puisque $10 \equiv 1\ [9]$.

3. Comme $100 \equiv 0\ [4]$, pour tout entier $i \geqslant 2$, $10^i = 10^{i-2} \times 100 \equiv 0\ [4]$ donc $N \equiv \overline{a_1 a_0}\ [4]$. Ainsi,

$$4 \mid N \Leftrightarrow N \equiv 0\ [4] \Leftrightarrow \overline{a_1 a_0} \equiv 0\ [4] \Leftrightarrow 2 \mid \overline{a_1 a_0}.$$

Ainsi, 4 divise N si et seulement si $\overline{a_1 a_0}$ est un multiple de 4.

4. Comme $10 \equiv 0\ [5]$, pour tout entier $i \geqslant 1$, $10^i \equiv 0\ [5]$ donc $N \equiv a_0\ [5]$. Ainsi,

$$5 \mid N \Leftrightarrow N \equiv 0\ [5] \Leftrightarrow a_0 \equiv 0\ [5] \Leftrightarrow 5 \mid a_0.$$

Ainsi, 5 divise N si et seulement si 5 divise a_0 i.e. $a_0 = 0$ ou $a_0 = 5$.

5. Comme $1000 \equiv 0\ [8]$, pour tout entier $i \geqslant 3$, $10^i = 10^{i-3} \times 1000 \equiv 0\ [8]$ donc $N \equiv \overline{a_2 a_1 a_0}\ [8]$. Ainsi,

$$8 \mid N \Leftrightarrow N \equiv 0\ [8] \Leftrightarrow \overline{a_2 a_1 a_0} \equiv 0\ [8] \Leftrightarrow 8 \mid \overline{a_2 a_1 a_0}.$$

Ainsi, 8 divise N si et seulement si $\overline{a_2 a_1 a_0}$ est un multiple de 8.

6. Comme $10 \equiv -1\ [11]$, pour tout entier $i \geqslant 0$, $10^i \equiv (-1)^i\ [11] \equiv -1\ [11]$ donc $N \equiv \sum_{i=0}^{k} (-1)^i a_i\ [11]$. Ainsi,

$$11 \mid N \Leftrightarrow N \equiv 0\ [11] \Leftrightarrow \sum_{i=0}^{k} (-1)^i a_i \equiv 0\ [11] \Leftrightarrow 11 \mid \sum_{i=0}^{k} (-1)^i a_i.$$

Ainsi, 11 divise N si et seulement si 11 divise $\sum_{i=0}^{k} (-1)^i a_i$.

□

Exemple 33. Montrer que le nombre $a = 123456789123456789$ (écrit en base 10) est divisible par 9 et par 11.

La somme des chiffres de a est $2 \times \sum_{i=1}^{9} i = 2 \times \dfrac{9 \times 10}{2} = 90 = 9 \times 10$ donc 9 divise a.

La somme alternée des chiffres de a est $9-8+7-6+5-4+3-2+1-9+8-7+6-5+4-3+2-1 = 0 = 0 \times 11$ donc 11 divise a.