ARİTHMÉTİQUE

I Division euclidienne

Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.
Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que $a = bq + r$ avec $0 \leq r < b$.

Cette égalité est ce qu'on appelle la division euclidienne de a par b.

q est le quotient, et r le reste, a le dividende et b le diviseur.

Ex : division euclidienne de 27 par 4
$27 = 4 \times 5 + 7$ n'est pas la division euclidienne de 27 par 4 car $7 > 4$.

En revanche, $27 = 4 \times 6 + 3$ est la division euclidienne de 27 par 4 car $0 \leq 3 < 4$.

➔ Cette notion peut s'étendre aux entiers relatifs, et il faut alors que $0 \leq r < |b|$.

Ex : division euclidienne de 35 par -4 :
$35 = -4 \times (-9) - 1$ ne convient pas car $-1 < 0$.

En revanche, $35 = -4 \times (-8) + 3$ est la division euclidienne de 35 par -4.

Cas particulier : On dit que a est un multiple de b lorsque le reste de la division de a par b vaut 0

(c'est-à-dire lorsque $a = b \times q$) *Cela revient à dire que a est dans la table de b*

On dit aussi que b est un diviseur de a ou que a est divisible par b.

Ex : On sait que $35 = 5 \times 7$. On peut donc dire que :

- ⇨ 5 est un diviseur de 35 *ou* 35 est divisible par 5 *ou* 35 est un multiple de 5
- ⇨ 7 est un diviseur de 35 *ou* 35 est divisible par 7 *ou* 35 est un multiple de 7

Propriété : Soient a, b et n trois entiers relatifs.
Si a et b sont des multiples de n, alors la somme $a + b$, la différence $a - b$ et le produit $a \times b$ sont des multiples de n.

Preuve : a est un multiple de n donc $a = nk_1$ où $k_1 \in \mathbb{Z}$.

De même, $b = nk_2$ où $k_2 \in \mathbb{Z}$.

Ainsi, $a + b = nk_1 + nk_2$

$= n(k_1 + k_2)$

Or, $k_1 \in \mathbb{Z}$ et $k_2 \in \mathbb{Z}$ donc $k_1 + k_2 \in \mathbb{Z}$.

Donc $a + b$ est un multiple de n.

On procède de même pour $a - b$ et $a \times b$.

Critères de divisibilité :

Un nombre est divisible par 2 s'il se termine par $0, 2, 4, 6$ ou 8.

Un nombre est divisible par 5 s'il se termine par 0 ou 5.

Un nombre est divisible par 3 si la somme de ses chiffres est divisible par 3.

Un nombre est divisible par 9 si la somme de ses chiffres est divisible par 9.

Ex : $84\,523$ n'est pas divisible par 3 car $8 + 4 + 5 + 2 + 3 = 22$ qui n'est pas divisible par 3.

$473\,652$ est divisible par 9 car $4 + 7 + 3 + 6 + 5 + 2 = 27$ qui est dans la table de 9.

Remarques : 1. Pour savoir si $3\,974\,584\,126$ est divisible par 3, il faut faire la somme de ses chiffres : $3 + 9 + 7 + 4 + 5 + 8 + 4 + 1 + 2 + 6 = 49$
Et on peut recommencer avec 49 en faisant $4 + 9 = 13$, puis une fois encore avec $1 + 3 = 4$
Or, 4 n'est pas dans la table de 3 donc $3\,974\,584\,126$ non plus.

2. Il existe d'autres critères de divisibilité, mais trop compliqués pour être utilisés fréquemment… On peut citer la table de 11 : un nombre est divisible par 11 si la somme alternée (+, puis –, puis +…) de ses chiffres en commençant par les unités est divisible par 11.

Par exemple, pour $81\,653$ on fait $3 - 5 + 6 - 1 + 8 = 11$ donc $81\,653$ est divisible par 11 (et on peut vérifier que $81\,653 = 11 \times 7\,423$)

De même, pour 72 809, on a $9 - 0 + 8 - 2 + 7 = 22$ qui est dans la table de 11 donc 72 809 aussi !

Exercice : montrer que $\frac{1}{3}$ n'est pas un nombre décimal

↪ un nombre décimal est un nombre qui peut s'écrire sous la forme $\frac{a}{10^n}$ où $a \in \mathbb{Z}$ et $n \in \mathbb{N}$

On raisonne par l'absurde : supposons que $\frac{1}{3}$ soit un nombre décimal.

Il existe alors deux entiers naturels a et n tels que $\frac{1}{3} = \frac{a}{10^n}$

On a alors $1 \times 10^n = a \times 3$ ce qui reviendrait à dire que 10^n est un multiple de 3.

Or, une puissance de 10 n'est jamais un multiple de 3 : l'hypothèse de départ amène donc à une contradiction.

Ainsi, $\frac{1}{3}$ n'est pas un nombre décimal.

II Parité

Un nombre est pair s'il est divisible par 2.

⇨ il peut alors s'écrire sous la forme $n = 2k$ où $k \in \mathbb{Z}$.

Un nombre est impair s'il n'est pas divisible par 2.

⇨ il peut alors s'écrire sous la forme $n = 2k + 1$ où $k \in \mathbb{Z}$.

Preuve : Soit $n \in \mathbb{Z}$. Effectuons la division euclidienne de n par 2 :

$$n = 2q + r \text{ où } (q, r) \in \mathbb{Z}^2 \text{ et } 0 \leq r < 2.$$

r étant un entier, il ne peut prendre que deux valeurs : 0 ou 1.

- Si $r = 0$, alors $n = 2q$ ce qui signifie que n est divisible par 2, donc pair.
- Si $r = 1$, alors $n = 2q + 1$ ce qui signifie que n n'est pas divisible par 2, donc impair.

Propriété : La somme de deux nombres pairs est paire.

La somme de deux nombres impairs est paire.

La somme d'un nombre pair et d'un nombre impair est impaire.

Preuve : ❶ Soient a et b deux nombres pairs.

On a alors $a = 2a'$ et $b = 2b'$ avec $(a' ; b') \in \mathbb{Z}^2$

Ainsi, $a + b = 2a' + 2b'$

$= 2(a' + b')$

Donc $a + b$ est un nombre pair car il s'écrit $2q$ avec $q = a' + b' \in \mathbb{Z}$

❷ Soient a et b deux nombres impairs.

On a alors $a = 2a' + 1$ et $b = 2b' + 1$ avec $(a' ; b') \in \mathbb{Z}^2$

Ainsi, $a + b = 2a' + 1 + 2b' + 1$

$= 2a' + 2b' + 2$

$= 2(a' + b' + 1)$

Donc $a + b$ est un nombre pair car il s'écrit $2q$ avec $q = a' + b' + 1 \in \mathbb{Z}$

❸ Soient a un nombre pair et b un nombre impair.

On a alors $a = 2a'$ et $b = 2b' + 1$ avec $(a' ; b') \in \mathbb{Z}^2$

Ainsi, $a + b = 2a' + 2b' + 1$

$= 2(a' + b') + 1$

Donc $a + b$ est un nombre pair car il s'écrit $2q + 1$ avec $q = a' + b' + 1 \in \mathbb{Z}$

Propriété : Si un nombre a est pair, alors son carré a^2 est pair.

De même, si un nombre a est impair, alors son carré a^2 est impair.

Et réciproquement, si a^2 est pair, alors a est pair et si a^2 est impair, alors a est impair.

Preuve : Si a est pair, alors $a = 2k$

Et dans ce cas, $a^2 = (2k)^2 = 4k^2 = 2(2k^2)$ est donc pair.

De même, si a est impair alors $a = 2k + 1$.

On a alors $a^2 = (2k + 1)^2$

$= 4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$ qui est bien un nombre impair.

Réciproquement, soit a^2 un nombre pair.
On effectue un raisonnement par l'absurde : supposons que a soit impair.

Dans ce cas, a^2 serait impair d'après ce qu'on a précédemment démontré.

Or, a^2 est pair par hypothèse donc c'est absurde. Ainsi, a est pair.

Exercice : montrer que $\sqrt{2}$ est un irrationnel
On effectue un raisonnement par l'absurde : supposons que $\sqrt{2}$ soit un nombre rationnel.

On aurait alors $\sqrt{2} = \frac{a}{b}$ où a et b sont des entiers naturels.

On peut même supposer que cette fraction est irréductible : si elle ne l'est pas, il suffit de la simplifier jusqu'à ce qu'elle le soit.

On a alors $\left(\sqrt{2}\right)^2 = \left(\frac{a}{b}\right)^2$

$2 = \frac{a^2}{b^2}$

$2b^2 = a^2$

Ces deux quantités étant égales, elles ont nécessairement le même chiffre des unités.

Chiffre des unités de a	0	1	2	3	4	5	6	7	8	9
Chiffre des unités de a^2	0	1	4	9	6	5	6	9	4	1

Chiffre des unités de b	0	1	2	3	4	5	6	7	8	9
Chiffre des unités de $2b^2$	0	2	8	8	2	0	2	8	8	2

Or, le seul chiffre des unités commun à a^2 et $2b^2$ est 0.

Et dans ce cas, le chiffre des unités de a est 0 donc a est notamment dans la table de 5.

Et le chiffre des unités de b est 0 ou 5, donc b est également dans la table de 5.

Par conséquent, la fraction $\frac{a}{b}$ peut être simplifiée par 5 :elle n'est donc pas irréductible.

Cela contredit l'hypothèse de départ : on en déduit que $\sqrt{2}$ n'est donc pas un nombre rationnel.

III Nombres premiers

1° Définition

Un entier *naturel* est dit premier s'il admet exactement deux diviseurs positifs distincts : 1 et lui-même.

Remarque : tout nombre est divisible par 1 et par lui-même…

« 1 » n'est pas un nombre premier car son seul diviseur est 1.

Liste des nombres premiers : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61\ldots$

Assez rapidement, il n'est pas facile de savoir si un nombre est ou non premier : 221 par exemple n'est pas premier car $221 = 17 \times 13$

⇨ Le « Crible d'Eratosthène » est une méthode classique pour lister les nombres premiers *(cf fin de chapitre)*

⇨ Une fois le début de la liste établi, on dispose d'un « critère de primalité » : un nombre n est premier s'il n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$

Ex : 391 est-il un nombre premier ? Même question pour 709.

$\sqrt{391} \approx 19{,}8$: on va donc tester si 391 est divisible par $2, 3, 5, 7, 11, 13, 17$ et 19.

On constate que $391 : 17 = 23$ donc 391 n'est pas premier.

$\sqrt{709} \approx 26{,}6$: on va donc tester si 709 est divisible par $2, 3, 5, 7, 11, 13, 17, 19$ et 23.

Ce n'est pas le cas : 709 est donc un nombre premier !

2° Utilité

Ces nombres sont fondamentaux dans de nombreux domaines, notamment la cryptographie (messages codés, sécurité des cartes bancaires, etc…) qui utilise de TRÈS grands nombres premiers.

Propriété : tout entier naturel supérieur ou égal à 2 se décompose de manière unique (à l'ordre des facteurs près) en produit de facteurs premiers.

Ex : $360 = 36 \times 10$
$= 6 \times 6 \times 2 \times 5$
$= 2 \times 3 \times 2 \times 3 \times 2 \times 5$
$= 2^3 \times 3^2 \times 5$

$7\,425 = 5 \times 1\,485$
$= 5 \times 5 \times 297$
$= 5 \times 5 \times 9 \times 33$
$= 5 \times 5 \times 3 \times 3 \times 3 \times 11$
$= 3^3 \times 5^2 \times 11$

Là encore, plus les nombres sont grands, et plus leur décomposition en facteurs premiers est compliquée à obtenir : c'est l'un des principes de la cryptographie actuelle…

➔ ces décompositions peuvent par exemple être utiles pour simplifier des fractions, des racines carrées…

Ex : $\sqrt{360} = \sqrt{2^3 \times 3^2 \times 5}$

$= \sqrt{2^2 \times 2 \times 3^2 \times 5}$

$= 2 \times 3\sqrt{2 \times 5}$

$= 6\sqrt{10}$

$\sqrt{104\,976\,000} = \sqrt{2^7 \times 3^8 \times 5^3}$ *admis*

$= \sqrt{2^6 \times 2 \times 3^8 \times 5^2 \times 5}$

$= 2^3 \times 3^4 \times 5\sqrt{2 \times 5}$

$= 3\,240\sqrt{10}$

Complément : le crible d'Eratosthène

- 2 est premier : on barre tous les multiples de 2
- 3 est non barré donc premier : on barre tous ses multiples

- le prochain nombre non barré est 5 : on barre tous ses multiples à partir de $5^2 = 25$

- le prochain nombre non barré est 7 : on barre tous ses multiples à partir de $7^2 = 49$
- etc.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200