Rappel - arithmétique entière

R. Absil

Année académique 2019 - 2020

Indépendamment de l'existence de nombres rationnels et réels, les nombres entiers sont très étudiés. Certaines de ces études trouvent leur origine depuis l'antiquité. En particulier, une relation fondamentale sur leur écriture a été découverte par Euclide, un mathématicien grec du 3^{e} siècle A.C.N.

Ce résultat s'appelle maintenant la *division euclidienne*. De plus, la technique de calcul écrit que vous avez probablement vu en école primaire permettant de diviser deux nombres porte le nom d'*algorithme de division euclidienne*. Notez que jusqu'à ce jour, aucun algorithme plus efficace n'est connu, plus de deux mille ans plus tard.

Notez que cet algorithme fournit un résultat de division (le *quotient*) et un *reste* uniques. Par exemple, « 7 divisé par 2 égal 3, il reste 1 ». Si l'on fixe les nombres 7 et 2, il ne peut y avoir d'autre résultat dans l'écriture que 3 pour le quotient et 1 pour le reste.

On peut décrire formellement cette propriété de la façon suivante.

Théorème 1. *Soient a et b deux naturels, avec $b \neq 0$, la* division euclidienne *de a par b associe un unique* quotient *q et un unique* reste *r à a et b vérifiant*

$$a = q\,b + r,$$

avec $0 \leqslant r < b$.

Dans cette écriture, on appelle a le *dividende* et b le *diviseur*. Notez qu'on peut facilement adapter cette définition de division euclidienne aux nombres entiers, par simple déduction du signe du quotient.

Ces termes viennent du fait que l'on peut écrire la propriété ci-dessus comme $\frac{a}{b} = q + \frac{r}{b}$. Pour cette raison, la division euclidienne est parfois appelée la *division entière*[1].

Si l'on considère l'algorithme de calcul écrit de division entière vu en école primaire, on remarque donc qu'il donne exactement les nombres q et r comme résultat, et que dans cette technique de résolution, on a systématiquement $r < b$. En effet, si ce n'est pas le cas, on peut encore diviser le résultat par q.

1. Cette terminologie est toutefois un peu restrictive : alors que la division euclidienne fournit à la fois le quotient et le reste de la division, la division entière ne fournit quant à elle que le quotient.

Exemple 1. Le tableau ci-dessous illustre quelques divisions euclidiennes de a par b pour plusieurs valeurs de a et de b.

a	b	q	r
6	3	2	0
16	5	3	1
17	6	2	5
3	7	0	3

Dans ce tableau, on voit donc, par exemple (à la ligne 2), que « 16 divisé par 5 égal 3, il reste 1 ». On peut écrire ceci également comme $16 = 5.3 + 1$. Cette dernière écriture correspond à ce que le théorème 1 affirme.

Notation 2. *Soient a et b deux naturels tels que $a = bq + r$ par la division euclidienne, pour un certain q et r. On définit les opérateurs de* div *et* mod *de la façon suivante :*

$$a \text{ div } b = q$$
$$a \bmod b = r.$$

L'opérateur div *est prononcé « div », et l'opérateur* mod *est lu « modulo ».*

Cette notation permet simplement de retrouver le quotient et le reste issus d'une division entière de a par b.

Exemple 2. On a :

$$5 \text{ div } 3 = 1 \text{ car } 5 = 3 \times \boxed{1} + 2,$$
$$3 \text{ div } 5 = 0 \text{ car } 3 = 5 \times \boxed{0} + 3,$$
$$5 \bmod 3 = 2 \text{ car } 5 = 3 \times 1 + \boxed{2}.$$

1 Diviseurs et multiples

La propriété de division euclidienne permet également de définir des concepts connexes, à savoir ceux de multiples et de diviseurs.

Définition 3. *Soient a et b deux naturels, on dit que*
- *b est un* diviseur *de a si $a \bmod b = 0$;*
- *b est un* multiple *de a si a est un diviseur de b.*

De plus, si b est un diviseur de a, on dit que b *divise* a. Notons qu'en particulier, zéro est un multiple de tout entier, car tous les entiers sont des diviseurs de zéro. Similairement, zéro n'est un diviseur d'aucun entier.

Exemple 3. Les affirmations ci-dessous illustrent les définitions des concepts de multiples et de diviseurs.
- 3 est un diviseur de 6 car la division entière de 6 par 3 a un reste nul.

— 6 est un multiple de 3 car 3 est un diviseur de 6.
— 3 n'est pas un diviseur de 7 car la division entière de 7 par 3 n'a pas un reste égal à zéro.
— 7 n'est pas un multiple de 3 car 3 n'est pas un diviseur de 7.

Exemple 4. On peut énumérer tous les diviseurs de 48 de la façon suivante :
— 1, 48, 2, 24, 3, 16, 4, 12, 6, 8.

Similairement, on peut énumérer les premiers multiples de 12 de la façon suivante :
— 12, 24, 36, 48, 60, 72, 84, 96, etc.

Remarquez que bien qu'un entier n'ait qu'un nombre fini de diviseurs, il a par contre une infinité de multiples.

Dans la technique ci-dessus, notez également que les diviseurs n'ont volontairement pas été énumérés par ordre croissant. En effet, si 48 est divisible par 1, 48 est également divisible par $\frac{48}{1} = 48$. On procède similairement avec les autres diviseurs, et on remarque, à la fin, que 48 est divisible par 6, donc 48 est également divisible par $\frac{48}{6} = 8$. Comme 7 n'est pas un diviseur de 48 et qu'on a déjà énuméré tous les diviseurs de 48 supérieurs à 8, il est inutile de poursuivre l'énumération : on n'a oublié aucun diviseur.

En conséquence, avec cette technique, il est inutile d'énumérer les diviseurs d'un nombre n au delà de $\lfloor\sqrt{n}\rfloor$, où $\lfloor x\rfloor$ dénote le plus grand entier inférieur ou égal à x. Remarquez qu'indépendamment de cette borne supérieure, énumérer les diviseurs d'un nombre prend un temps considérable avec un ordinateur.

Remarque 1. Ne confondez pas le concept de multiple et de diviseur, ce sont des objets bien distincts. Par ailleurs, ne confondez pas « diviseur d'un nombre » et « diviseur » dans une opération de quotient. Ces concepts ont *a priori* peu de points en commun.

2 Nombres premiers

Ls nombres premiers sont un sujet très important en mathématiques pures, mais aussi à cause de leurs applications notamment en informatique, comme en cryptographie. En effet, plusieurs algorithmes de chiffrement, tels que le RSA, trouvent leur robustesse dans des propriétés liées aux nombres premiers, telles que la factorisation de grands nombres.

Définition 4. *Un* nombre premier n *est un naturel strictement plus grand que* 1 *qui n'admet pas de diviseurs positifs autres que* 1 *et* n.

Comme mentionné à la fin de la section précédente, on peut tester si un nombre n est premier en énumérant ses diviseurs jusqu'à $\lfloor\sqrt{n}\rfloor$.

Les premiers nombres premiers sont $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ Cette séquence de nombres est « irrégulière », et jusqu'à présent, on ne connaît pas de formule permettant de donner rapidement le $k^{\text{ième}}$ nombre premier.

Comme mentionné ci-dessus, la sécurité de nombreux systèmes informatiques repose sur des problèmes mathématiques difficiles à résoudre en mathématiques. En particulier, elle repose sur

le fait que les « meilleures » techniques connues à ce jour sont trop lentes pour être utilisées en pratique sur une grande quantité de données, et les mathématiciens conjecturent qu'une telle technique n'existe pas.

3 Factorisation des nombres naturels

En section 1, nous avons vu comment énumérer les diviseurs d'un nombre naturel. On remarque qu'une telle énumération est « rébarbative ». En effet, si 6 divise un naturel n, alors 2 et 3 divisent aussi n, et inversement.

Une façon de remédier à cet inconvénient d'écriture est d'énumérer les diviseurs premiers de n. Une telle énumération s'appelle la *décomposition en facteurs premiers* de n. Plus simplement, cela consiste à écrire n'importe quel nombre naturel comme un produit de nombre premiers.

Exemple 5. Soit $n = 60$, la décomposition en facteurs premiers de n est $2 \times 2 \times 3 \times 5 = 2^2 \cdot 3 \cdot 5$.

Notez que la décomposition en facteurs premiers d'un naturel est unique, à commutativité près. Ce résultat est appelé le *théorème fondamental de l'arithmétique* [**?**]. Remarquez que bien qu'il puisse sembler évident, la preuve d'un tel résultat n'est pas triviale.

L'écriture des nombres naturels en produits de facteurs premiers en facilite la manipulation dans des problèmes de divisibilité, de fraction ou de racine carrée, ou pour la simplification de fractions.

La recherche d'algorithmes de décomposition est d'une importance considérable en mathématique, en cryptologie, en théorie de la complexité des algorithmes, etc. Par exemple, la robustesse de l'algorithme de chiffrement R.S.A. repose sur la difficulté des mathématiciens (et *a fortiori*, des ordinateurs) à factoriser de grands nombres naturels. Cet algorithme, publié en 1977 par R. Rivest, A. Shamir et A. Adelman, permet « d'encoder » un message à l'aide d'une clé dite *publique*, le rendant ainsi illisible pour une tierce personne ne possédant pas la clé *privée* correspondante. Plusieurs garanties reposent sur le problème de factorisation, notamment le fait qu'il soit *difficile*[2] d'obtenir la clé privée à partir de la clé publique, qu'il soit *difficile* de décoder le message sans la clé privée, etc.

2. Ici, « difficile » dénote le fait que ce travail requerrait un temps de calcul immense.