IV. — *Nouvelle manière de présenter la théorie de la divisibilité des nombres*

PAR

F. FOLIE,

DOCTEUR EN SCIENCES, RÉPÉTITEUR A L'ÉCOLE DES MINES, PROFESSEUR A L'ÉCOLE INDUSTRIELLE DE LIÉGE.

En publiant cette note, nous nous sommes proposé un double but :

En premier lieu, de rendre la théorie de la divisibilité des nombres indépendante de celle de la recherche du plus grand commun diviseur, recherche qui n'est qu'un tâtonnement raisonné, comme Lacroix le fait judicieusement remarquer dans son Arithmétique ;

En second lieu, de formuler un principe qui permette de découvrir les caractères de divisibilité d'un nombre par un nombre premier, d'une manière immédiate et applicable à tous les systèmes de numération, sans qu'il soit nécessaire de chercher les restes de la division des puissances de la base par ce nombre premier.

Pour plus de concision, nous n'énoncerons que les principes que nous croyons neufs ou en eux-mêmes, ou par leur mode de démonstration, et nous ferons usage sans scrupule de la notation algébrique, laissant au lecteur familier avec ces théories, le soin de renouer la chaîne des raisonnements, et de leur donner, s'il le veut, la forme usitée dans l'enseignement public.

Il va de soi que nous supposons connues les définitions telles qu'elles sont exposées dans tous les traités. Toutefois,

afin d'éviter la moindre amphibologie, nous dirons que nous appelons *fraction irréductible* une fraction qui ne peut pas se ramener à une autre dont les termes soient *plus petits* que les siens.

§ I. Théorème. — *Une fraction irréductible ne peut être égale à une autre que pour autant que les deux termes de celle-ci soient des équimultiples des deux termes de la première.*

Soit $\frac{a}{b}$ une fraction irréductible ; $\frac{A}{B}$ une fraction égale à celle-là, de sorte que

$$A > a, \quad B > b.$$

Soient m et n les plus grands nombres de fois que a et b sont respectivement contenus dans A et B ; en supposant

$$m < n,$$

posons :

$$A = ma + \alpha, \quad B = mb + \beta ;$$

d'où

$$\alpha < a.$$

Nous aurons ainsi :

$$\frac{a}{b} = \frac{ma + \alpha}{mb + \beta};$$

d'où nous pourrons déduire :

$$\frac{a}{b} = \frac{\alpha}{\beta},$$

ce qui serait contre l'hypothèse, puisque α étant plus petit que a, β doit être plus petit que b, et que la fraction $\frac{\alpha}{\beta}$ serait par suite plus simple que $\frac{a}{b}$.

Donc la fraction $\frac{A}{B}$ ne peut être que de la forme $\frac{ma}{mb}$ (*).

Corollaire. — *Une fraction dont les deux termes sont premiers entre eux est irréductible.*

Car pour qu'elle pût être égale à une fraction plus simple, il faudrait que ses deux termes fussent des équimultiples des deux termes de celle-ci, ce qui serait contre l'hypothèse.

Théorème. — *Lorsqu'un nombre divise un produit de deux facteurs, et qu'il est premier avec l'un deux, il doit diviser l'autre.*

Soit un produit ab divisible par un nombre p premier avec a; je dis que p doit diviser b.

En effet, par hypothèse

$$\frac{ab}{p} = n\ ;$$

(*) On pourrait reprocher à cette démonstration une concision trop grande qui nuirait à sa clarté. Dans ce cas, nous proposerions de la décomposer en deux parties.

1° Soit

$$\frac{a}{b} = \frac{A}{B},$$

$\frac{a}{b}$ étant irréductible; posons

$$A = ma + \alpha, \qquad B = nb + \beta,$$

α et β étant respectivement plus petits que a et b ; je dis qu'on aura

$$m = n.$$

En effet, de

$$\frac{a}{b} = \frac{ma + \alpha}{nb + \beta}$$

on tire :

$$nab + a\beta = mab + \alpha b,$$

qu'on peut écrire, si l'on suppose $n > m$:

$$(n - m)ab = \alpha b - a\beta,$$

d'où

$$(n - m)ab < ab,$$

puisque chacun des termes de la différence est lui-même $< ab$.

d'où

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

Or la première fraction étant irréductible, il résulte du théorème précédent que n et b doivent être des équimultiples de a et de p, c. q. f. d.

C'est là le principe qui se basè, dans tous les traités à notre connaissance, sur la théorie du tâtonnement raisonné.

On sait que, ce principe une fois établi, toute la théorie de la divisibilité des nombres ne présente plus aucune difficulté. Nous ne nous arrêterons donc pas à développer la série des théorèmes qui font suite à ce principe fondamental; et, les supposant connus, nous passerons au second objet de cette note.

Or, ce résultat est évidemment absurde, puisque n étant $> m$ par hypothèse, $n - m$ est au moins égal à 1. Cette hypothèse est donc fausse; il en serait de même si l'on supposait

$$m > n;$$

donc

$$m = n.$$

2° Cela étant, la dernière égalité donne aussi :

$$\alpha b = a\beta;$$

d'où

$$\frac{a}{b} = \frac{\alpha}{\beta},$$

résultat contradictoire avec l'hypothèse que $\frac{a}{b}$ est irréductible, puisque α et β sont respectivement plus petits que a et b.

En premier lieu donc A et B doivent contenir le même nombre de fois respectivement a et b; en second lieu, ils ne peuvent pas être de la forme

$$ma + \alpha, \qquad mb + \beta;$$

par suite on doit poser nécessairement

$$A = ma \quad , \quad B = mb; \text{ c. q. f. d.}$$

§ II. 1° Soit un nombre écrit dans un système de numération à base B :

$$N = AB + C.$$

Cherchons à déterminer les caractères de divisibilité de ce nombre par un nombre premier donné

$$p = aB + c.$$

Si p n'avait que des unités simples, nous formerions un de ses multiples, et nous représenterions ce multiple np par $aB + c$, n étant supposé premier avec p.

Le principe que nous nous proposons d'établir est le suivant :

Théorème. — *Si entre* a *et* c *il existe une relation* $ak' \pm ck = mp$ (*). *le nombre* $AB + C$ *sera divisible par* p *à la condition que*

$$Ak' \pm Ck = mp,$$

pourvu que a, c, k, k', *ne soient pas des multiples de* p.

Pour le démontrer, nous nous appuierons sur ce lemme :

Lemme. — 1° *Si deux nombres* $a.B + c$ *et* $A.B + C$ *sont divisibles par un même nombre premier* p, *on aura* $Ac - aC = m\,p$.

En effet, de

$$aB + c = mp$$
$$AB + C = mp,$$

on déduit :

$$AaB + Ac = mp$$
$$aAB + aC = mp;$$

d'où

$$Ac - aC = mp.$$

2° *Réciproquement si* $aB + c = mp$ *et que* $Ac - aC = mp$, $AB + C$ *le sera aussi, pourvu que* a *et* c *ne le soient pas.*

(*) Par mp nous entendons un *multiple de p* quelconque, ou zéro.

En effet, les égalités supposées peuvent s'écrire :

$$\mathrm{A}a\mathrm{B} + \mathrm{A}c = m.p$$
$$\mathrm{A}c - a\mathrm{C} = m.p$$

d'où par soustraction :

$$a(\mathrm{AB} + \mathrm{C}) = m.p,$$

et par suite

$$\mathrm{AB} + \mathrm{C} = m.p,$$

si a ne l'est pas ; la réciproque est donc démontrée avec ses restrictions ; car si a n'est pas multiple de p, c ne peut pas l'être, à moins que B lui-même ne le soit. Il est inutile de nous occuper de ce dernier cas, qui du reste n'infirme pas le théorème.

Au moyen de ce lemme, la démonstration du principe énoncé plus haut devient fort simple.

Soit donc un nombre premier p ou l'un de ses multiples, représenté d'une manière générale par

$$a\mathrm{B} + c = m.p ;$$

et soit

$$ak' \pm ck = m.p.$$

Je dis que si l'on a :

$$\mathrm{A}k' \pm \mathrm{C}k = m.p,$$

le nombre AB + C sera multiple de p ; a, c, k', k étant premiers avec p.

En effet, des hypothèses posées on tire :

$$\mathrm{A}ak' \pm \mathrm{A}ck = m.p$$
$$a\mathrm{A}k' \pm a\mathrm{C}k = m.p ;$$

d'où, par soustraction :

$$(Ac - aC)\,k = m.p.$$

Si donc k n'est pas multiple de p, $Ac - aC$ doit l'être, et en vertu du lemme précédent $AB + C$ le sera aussi.

Ce lemme suppose a et c premiers avec p ; notre démonstration suppose la même chose relativement à k, et, par suite de ces hypothèses, relativement à k' aussi, en vertu de

$$ak' \pm ck = m.p\,;$$

le principe est donc démontré avec ses restrictions (*).

Nous croyons superflu d'étendre ce principe à la divisibilité d'un nombre par une puissance d'un nombre premier, et nous nous contenterons de quelques brèves applications au système de numération décimale ; nous ne chercherons pas à déduire de nos caractères de divisibilité ceux qui sont habituellement donnés, quelque aisé que ce soit, parce que nous croyons ceux-ci, en général, beaucoup trop compliqués ; enfin, parmi tous les caractères possibles, nous choisirons ceux où le multiplicateur des dizaines est un, comme étant les plus simples dans l'application.

Caractères de divisibilité.

Par 3. Dans $4 \times 3 = 12$, je remarque que $1 + 2 = 3$; donc : un nombre est divisible par 3 si le nombre de ses dizaines augmenté de celui de ses unités est un multiple de 3.

Par 7. Dans $3 \times 7 = 21$, je remarque que $2 - 2 \times 1 = 0$, caractère qui n'appartient pas au facteur 3 ; donc : un nombre est divisible par 7 si le nombre de ses dizaines diminué du double de ses unités est un multiple de 7.

(*) Il va de soi que si l'on recherche le caractère au moyen d'un multiple de p tel que pp', p' étant un facteur premier, il faudra vérifier si le caractère trouvé n'appartient pas à p'.

Par 11. Je remarque que $1 - 1 = 0$; donc : un nombre est divisible par 11 si le nombre de ses dizaines diminué de celui de ses unités est un multiple de 11.

Par 13. Je remarque que $1 + 4 \times 3 = 13$; donc : un nombre est divisible par 13 si le nombre de ses dizaines augmenté du quadruple de ses unités est un multiple de 13.

Par 17. Dans $3 \times 17 = 51$ je remarque que $5 - 5 \times 1 = 0$, caractère qui n'appartient pas au facteur 3; donc : un nombre est divisible par 17 si le nombre de ses dizaines diminué du quintuple de ses unités est un multiple de 17.

Par 19. Je remarque que $1 + 2 \times 9 = 19$; donc : un nombre est divisible par 19 si le nombre de ses dizaines augmenté du double de ses unités est un multiple de 19.

Par 23. Je remarque que $2 + 7 \times 3 = 23$; donc : un nombre est divisible par 23 si le nombre de ses dizaines augmenté du septuple de ses unités est un multiple de 23.

Par 31. Je remarque que $3 - 3 \times 1 = 0$; donc : un nombre est divisible par 31 si le nombre de ses dizaines diminué du triple de ses unités est un multiple de 31.

Par 37. Dans $3 \times 37 = 111$ je remarque que $11 - 11 \times 1 = 0$; donc : un nombre est divisible par 37 si le nombre de ses dizaines diminué de 11 fois ses unités est un multiple de 37.

Nous ne pousserons pas plus loin ces applications; on a pu reconnaître qu'elles présentent une facilité telle que, le principe étant connu, les caractères de divisibilité se trouvent pour ainsi dire *à priori*.

§ II. 2° On se demandera s'il n'existe pas un principe analogue pour un nombre décomposé en unités de différents ordres. Nous allons le chercher encore pour le cas de trois ordres; mais nous verrons qu'il comporte alors des restrictions qui en rendent l'application beaucoup plus difficile, de sorte que le caractère, dans ce cas, ne se trouve pas immédiatement, et que le plus simple sera presque toujours de le déduire du

précédent. Aussi cette extension ne présente-t-elle qu'un intérêt scientifique (*).

Lemme. — 1° p *étant premier*, *si* $aB^2 + cB + d = mp$ *et que* $AB^2 + CB + D = m.p$ *sans que* B *le soit*, *on aura* :

$$(Ad - aD)^2 - (Cd - cD)(Ac - aC) = m.p.$$

Des relations posées on tire :

$$(Ac - aC)B + (Ad - aD) = m.p.$$

$$B\left\{(Ad - aD)B + (Cd - cD)\right\} = m.p.$$

Dans cette dernière relation on peut supprimer le premier facteur B, puisqu'il n'est pas multiple de p ; et l'on pourra écrire, en égalant les valeurs de B tirées de ces deux équations :

$$\frac{m.p - (Ad - aD)}{Ac - aC} = \frac{m.p - (Cd - cD)}{Ad - aD};$$

d'où la relation à démontrer.

2° Réciproquement : *si* $aB^2 + cB + d = m.p$ *et que* $(Ad - aD)^2 - (Cd - cD)(Ac - aC) = m.p$; a, c, d, B *étant pre-*

(*) Le moyen le plus simple en effet de vérifier si un nombre est divisible par un autre est d'employer successivement sur ce nombre et ceux qui en dérivent le caractère fondé sur la décomposition en dizaines et unités.

Montrons par un exemple la rapidité de ce procédé.

Proposons-nous de vérifier si 20748 est divisible par 7, 13, 17, 19.

20748	20748	20748	20748
16	32	40	16
2058	2106	2034	2090
16	24	20	18
189	234	183	38
18	16	15	
0	39	3	

Ce nombre est donc divisible par 7, 13, 19, mais ne l'est pas par 17.

mier avec p, *le nombre* $AB^2 + CB + D$ *sera multiple de* p.

Nous laisserons au lecteur le soin de démontrer cette réciproque.

Théorème. — *Soit un nombre premier* p *ou l'un de ses multiples représenté par* $aB^2 + cB + d = m.p$; *et soit donnée la relation* $ak'' + ck' + dk = mp$, k, k', k'' *étant premiers avec* p; *si*

$$A''k + Ck' + Dk = m.p,$$

le nombre $AB^2 + CB + D$ *sera divisible par* p, *pourvu que* $k'^2 - kk''$ *soit un multiple de* p.

En effet, on déduit des hypothèses posées :

$$(Ac - aC)k' + (Ad - aD)k = m.p.$$
$$(Ad - aD)k'' + (Cd - cD)k' = m.p.$$

et de là, comme plus haut,

$$(Ad - aD)^2 kk'' - (Ac - aC)(Cd - cD)k'^2 = m.p.$$

Mais puisque l'on a aussi

$$k'^2 - kk'' = m.p,$$

il s'ensuit :

$$(Ad - aD)^2 - (Ac - aC)(Cd - cD) = m.p;$$

d'où la preuve du principe, en vertu du lemme précédent.

Les caractères que l'on obtiendra au moyen de ce principe sont les mêmes que ceux qui se déduisent des restes de la division de 100, 10, 1 par le nombre premier donné; ou de 200, 20, 2; 300, 30, 3, etc. En outre, on voit par notre principe que ces restes satisfont toujours à la condition que *le carré du moyen diminué du produit des extrêmes est un multiple du nombre premier*, ce qui est très-aisé à démontrer directement, et peut fournir un moyen très-simple de vérification de ces restes.

Montrons, par un seul exemple, comment le caractère peut s'établir sans tâtonnement, et sans chercher les restes :

Soit un nombre *cdu*, dans le système décimal; son caractère de divisibilité par 7 est, comme nous l'avons vu :

$$cd - 2u = m7;$$

mais ce dernier nombre peut être regardé comme composé de c dizaines en $d - 2u$ unités ; son caractère sera donc :

$$c - 2(d - 2u) = m.7$$

ou

$$c - 2d + 4u = m.7$$

ou encore, puisque

$$4 = 7 - 3 : \qquad c - 2d - 3u = m.7$$

ou enfin

$$-c + 2d + 3u = m.7$$

En partant du caractère suivant, qui appartient aussi aux multiples de 7 :

$$3cd + u = m.7$$

on arriverait à :

$$9c + 3d + u = m.7$$

ou

$$2c + 3d + u = m.7$$

Les multiplicateurs -1, $+2$, $+3$, et $+2$, $+3$, $+1$ satisfont à la condition

$$k'^2 - kk'' = m.7.$$

Nous donnerons la liste des multiplicateurs pour les nombres premiers depuis 3 jusqu'à 37, en désignant respectivement par k'', k', k ceux des chiffres des centaines, dizaines et unités ; on a vu comment on peut les déterminer, et l'on se rappellera que le caractère de divisibilité d'un nombre cdu par p sera

$$k''c + k'd + ku = m.p.$$

CARACTÈRES DE DIVISIBILITÉ PAR p.

p	k''	k'	k	$k'^2 - kk''$
3	1	1	1	0.
7	2	3	1	7.
	-1	2	3	7.
11	1	-1	1	0.
13	-4	-3	1	13.
	-3	1	4	13.
17	-4	3	2	17.
	4	-5	2	17.
19	-9	1	2	19.
	5	-9	1	4×19.
23	1	7	3	2×23.
	-7	-3	2	23.
31	7	10	1	3×31.
	-10	-1	3	31.
37	-7	3	4	37.
	4	-7	3	37.