NOUVELLES ANNALES DE MATHÉMATIQUES

TERQUEM

Théorie élémentaire des nombres, d'après Euler, Legendre, MM. Gauss et Cauchy

Nouvelles annales de mathématiques 1re série, tome 3 (1844), p. 214-219

<http://www.numdam.org/item?id=NAM_1844_1_3__214_0>

THÉORIE ÉLÉMENTAIRE DES NOMBRES,

D'après Euler, Legendre, MM. Gauss et Cauchy.

(Suite, v. page 204.)

—

Division, diviseurs, résidus.

13. La division est une opération par laquelle on trouve combien de fois on peut soustraire un nombre d'un autre jusqu'à ce que le reste soit devenu plus petit que le nombre soustrait. Le *dividende* est le nombre duquel on soustrait; le *diviseur*, le nombre qu'on soustrait; le *quotient* marque le nombre de soustractions à effectuer; le *résidu* de deux nombres est le reste de la division du grand nombre par le petit. Ainsi, pour les deux nombres 19 et 5, 19 est le dividende, 5 le diviseur, 3 le quotient et 4 le résidu.

Soient a, dividende; p, diviseur; q, quotient; r, résidu, on a l'identité $a = pq + r$.

Observation. La division et la multiplication sont deux opérations *inverses* et peuvent se contrôler mutuellement.

14. Lorsque le résidu de deux nombres est zéro, le dividende est dit *multiple* du diviseur, et le diviseur est un *sous-multiple* du dividende. On dit aussi, dans un sens restreint, qu'un nombre est *diviseur* d'un autre, lorsque leur résidu est nul; ainsi 5 est diviseur de 15, et 15 est un multiple de 5. Zéro est divisible par un nombre quelconque.

15. *Notation.* Nous proposons de désigner le multiple quelconque d'un nombre par un point placé sur ce nombre; ainsi $\dot{5}$, $\dot{p}$ désignent des multiples quelconques de 5 ou de p, et l'équation $a = \dot{p}$ signifie que a est un multiple de p.

Observation. Le point est déjà employé pour désigner une multiplication quand il est placé à côté du nombre.

$E\left(\frac{a}{b}\right)$ désigne la partie entière du quotient de a divisé par b; ainsi $E\left(\frac{20}{7}\right) = 2$, $E\left(\frac{31}{5}\right) = 6$.

16. Lorsque le même nombre divise d'autres nombres, on dit qu'il est *diviseur commun* à ces deux nombres; ainsi 3 est diviseur commun à 15, 21, 36.

Un est diviseur commun à tous les nombres.

17. Un nombre premier est celui qui n'est divisible que par lui-même, 7, 11, 13, 17, etc., sont des nombres premiers; les autres nombres sont dits non premiers ou composés. 2 est le seul nombre premier pair; 1.2.3 sont trois nombres premiers consécutifs, il ne saurait y en avoir d'autres aussi consécutifs.

18. Deux nombres sont premiers entre eux lorsqu'ils n'ont d'autres diviseurs communs que l'unité; ainsi 25 et 36 sont *premiers entre eux*.

Corollaire 1. Un est premier à l'égard de tous les autres nombres.

Corollaire 2. Un nombre premier est nécessairement premier avec tout nombre plus petit; avec un nombre plus grand, il est premier ou il en est un sous-multiple.

19. *Théorème* 3. La somme algébrique de tant de nombres qu'on voudra, multiples chacun du même nombre, est un multiple de ce nombre.

Ce théorème peut s'écrire ainsi : $a = \dot{p}$, $b = \dot{p}$, $c = \dot{p}$, etc.; on a $a + b + c + \ldots = \dot{p}$.

20. *Théorème* 4. La somme algébrique de tant de multiples d'un même nombre qu'on voudra, et affectés chacun d'un coefficient entier, est un multiple de ce même nombre.

Ce théorème peut s'écrire ainsi : $a = \dot{p}$, $b = \dot{p}$, $c = \dot{p}$, etc., on a aussi $ma + nb + rc + \ldots = \dot{p}$.

Corollaire. Si $a=\dot{p}$, $b=\dot{p}$, $c=\dot{p}$... on a $a^m b^n c^r \ldots =\dot{p}$, m, n, r étant des exposants entiers positifs.

Observation. Nous omettons la démonstration trop facile de ces théorèmes.

21. *Théorème* 5. Le diviseur commun à deux nombres est aussi commun à leur résidu.

Démonstration. Ce résidu est égal au dividende, moins le diviseur multiplié par le quotient ; donc..... (théorème 4).

Corollaire. Le résidu de deux nombres premiers entre eux est toujours premier avec le diviseur.

22. *Théorème* 6. Le résidu de la somme algébrique de plusieurs nombres relativement à un même diviseur, est égal à la somme des résidus.

Démonstration. Soit $a=\dot{p}+r$, $b=\dot{p}+s$, $c=\dot{p}+t$, etc. ; p étant le diviseur et r, s, t les résidus, on a

$$a+b+c+\ldots\ldots=\dot{p}+r+s+t\ldots\ldots ;$$

donc, etc.

Observation. Si la somme des résidus surpasse le diviseur p, on prend le résidu de cette somme.

23. *Théorème* 7. Le résidu d'un produit est égal au produit des résidus des facteurs.

Démonstration. Soient a, b, c les facteurs, p un diviseur, $a=\dot{p}+r$, $b+\dot{p}+s$, $c=\dot{p}+t$, on a $abc\ldots\ldots=\dot{p}+rst\ldots$. si $rst\ldots$ est plus grand que p, on en prend le résidu.

Observation. Les preuves dites par 9 dont on se sert pour contrôler les opérations de l'arithmétique sont fondées sur les deux théorèmes précédents.

24. *Théorème* 8. Le produit de deux facteurs premiers avec un troisième est premier avec ce troisième nombre.

Démonstration. Soient a, b les deux facteurs premiers avec p, et admettons, s'il est possible, que q soit un facteur commun entre ab et p, de sorte qu'on a $ab=\dot{q}$, $p=\dot{q}$.

Supposons d'abord $p \not> a$, on a donc $p = \dot{a} + r$; le résidu r est plus petit que a. Cette équation donne celle-ci : $pb = \dot{a}b + br$; pb et $\dot{a}b$, par hypothèse, ont le facteur commun q; ce même facteur divise donc br. De ce produit, on déduirait semblablement un produit br' divisible par q, et où $r' < r$; on parviendrait donc enfin à un produit $1 \times b$, divisible par q; p et b auraient donc le diviseur commun q, ce qui est impossible; donc ab et p n'ont pas de diviseur commun.

2° Si $a > p$, on a $a = \dot{p} + r$, où r est plus petit que p et premier avec p; $ab = \dot{b}p + br$; si ab n'est pas premier avec p, alors br ne serait pas non plus premier avec p; mais r étant plus petit que p, br est nécessairement premier avec p; donc, etc.

Ce théorème 8 est la proposition 26 du septième livre d'Euclide.

25. *Théorème* 9. Si tous les facteurs d'un produit sont premiers avec le nombre p, le produit sera premier aussi avec ce nombre p.

Ce théorème est un corollaire du précédent; propositions 16, 17, 18, 19 du neuvième livre d'Euclide.

Corollaire. Si a est premier avec p, a^m est aussi premier avec p; on en déduit qu'il est impossible que la racine d'un indice quelconque d'un nombre entier soit un nombre fractionnaire, et de là l'existence des quantités irrationnelles.

26. *Théorème* 10. Un nombre composé ne peut se résoudre que d'une seule manière, en facteurs premiers.

Démonstration. Soient a, b, c, d..... les nombres premiers, suivant l'ordre de grandeur, qui divisent le nombre composé N; ainsi $N = a^\alpha b^\beta c^\gamma d^\delta \ldots\ldots$; soit un autre nombre premier a', différent de a, b, c, d.....; étant premier avec a, b, c, d. ... il sera premier avec N; ainsi N n'admet

pas d'autres nombres premiers. Soit donc $N = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots\ldots$, et $\alpha' > \alpha$; on aura $b^{\beta'} c^{\gamma'} \ldots\ldots = a^{\alpha'-\alpha} b^{\beta} c^{\gamma} \ldots\ldots$ Mais cette équation est impossible, car le second membre est divisible par a et le premier ne l'est pas; donc, etc.

27. *Problème* 4. Combien un nombre composé a-t-il de diviseurs, et quelle est la somme de ces diviseurs?

Solution. Soit comme dans le théorème précédent,

$$N = a^{\alpha} b^{\beta} c^{\gamma} \ldots\ldots$$

Effectuant le produit des polynômes

$$(1 + a + a^2 + \ldots. a^{\alpha})(1 + b + b^2 + \ldots. b^{\beta})(1 + \ldots. c^{\gamma}) \ldots.$$

tous les termes de ce produit sont inégaux; chacun est diviseur de N, et réciproquement tout diviseur de N est nécessairement un de ces termes; or le nombre de ces termes est évidemment $(1+\alpha)(1+\beta)(1+\gamma)\ldots.$; tel est donc le nombre des diviseurs de N, l'unité comprise, et la somme de tous ces diviseurs est donc égale à

$$\frac{(a^{\alpha+1}-1)(b^{\beta+1}-1)(c^{\gamma+1}-1)\ldots}{(a-1)(b-1)(c-1)\ldots}.$$

Coroll. Soit $N = 2^{\alpha}(2^{\alpha+1}-1)$, et supposons que $2^{\alpha+1}-1$ soit un nombre premier; ainsi $a = 2$; $b = 2^{\alpha+1}-1$; $\beta = 1$; la somme de tous les diviseurs est donc, toute réduction faite, égale à $2N$; le nombre N, qui jouit de cette propriété d'être égale à la somme de ses diviseurs, est dit un nombre *parfait;* ces nombres sont ainsi dénommés à raison de leur rareté; voici les 11 premiers nombres :

Valeurs de α.

0 — 1
1 — 6
2 — 28
4 — 496
6 — 8128

12 — 33 550 336
16 | 85 898 691 328
18 | 137 438 691 328
30 | 2 305 843 008 139 952 128
40 | 2 417 851 639 228 158 837 784 756
46 | 9 903 520 314 282 971 830 448 816 128.

Si, dans un nombre parfait, on ajoute ensemble tous les chiffres, on obtient un second nombre; si on a fait de même pour ce second nombre, on obtient un troisième nombre qui est divisible par 10. Observation de Kraft. (M. de Pétᵍ, 1734—35). Sans démonstration.

Entre 1 et un sextillion, il n'y a que 10 nombres parfaits. Cette solution se trouve dans Euclide. (Prop. 36, liv. 9.)

La suite prochainement.