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. 337-344

<http://www.numdam.org/item?id=NAM_1844_1_3__337_0>

THÉORIE ÉLÉMENTAIRE DES NOMBRES

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

(Suite, v. p. 219.)

28. $\alpha+1$ est un nombre premier ; car, s'il était le produit de deux facteurs mn, alors $2^{mn}-1$ serait divisible par 2^m-1 et par 2^n-1 ; et par conséquent $2^{\alpha+1}-1$ n'étant plus un nombre premier, N ne sera plus un nombre parfait. Faisons $2^\alpha = x$; alors $N = 2x^2 - x$; lorsque $x = 1$, N devient égal à l'unité ; donc $N-1$ est divisible par $x-1$; et l'on a $N-1 = (x-1)(2x+1)$; remplaçant x par sa valeur, on a l'identité $N = 2^\alpha(2^{\alpha+1}-1) = (2^\alpha-1)(2^{\alpha+1}+1)+1$, α est essentiellement pair, et $2^\alpha = (3-1)^\alpha$; donc 2^α est de la forme $\dot{3}+1$; par conséquent $2^\alpha-1$ est divisible par 3 ; il en est de même de $2^{\alpha+1}+1$; donc N est de la forme $\dot{9}+1$. Soit N_1 la somme des chiffres de N ; N_2 la somme des chiffres de N_1 ; N_3 la somme des chiffres de N_2, et ainsi de suite ; tous ces nombres, en vertu de la propriété connue du diviseur 9 dans la numération décimale, sont de la forme $\dot{9}+1$. Ces nombres vont toujours en diminuant ; le dernier de ces nombres est donc l'unité, et l'avant-dernier est dix ou une puissance de dix.

Nous devons à l'obligeance de M. le professeur Wantzel la démonstration de cette observation de Krafft (27).

Le premier chiffre à droite de 2^α étant 4 ou 6, il en résulte que le premier chiffre à droite d'un nombre parfait est 6 ou 8.

Résidus négatifs; diviseur commun maximum; multiple minimum.

29. Dans la division, si la partie entière du quotient est trop faible à moins d'une unité près, on dit que la division se fait *en dedans*, et dans ce cas le résidu est positif; si la partie entière est trop forte à moins d'une unité près, la division est dite *en dehors*, et le résidu est négatif.

L'équation $a = bq + r$ (§ 13, p. 214) peut s'écrire

$$a = b(q+1) + r - b;$$

$q+1$ est le quotient en dehors, et $r - b$ est le résidu négatif correspondant; exemple :

$$15 = 4.3 + 3 = 4.4 - 1;$$

ainsi dans la division de 15 par 4, 3 est le résidu positif et -1 le résidu négatif. Les théorèmes 5, 6, 7 ont également lieu pour les résidus négatifs.

30. La somme du résidu positif et du résidu négatif pris positivement, est égale au diviseur; car $r + (b - r) = b$; donc, lorsqu'un de ces résidus est plus grand que la moitié du diviseur, l'autre est nécessairement plus petit que cette moitié; ils ne peuvent être égaux que lorsque le diviseur est pair.

31. *Problème* 5. Trouver le plus grand commun diviseur de deux nombres A et B.

1re *solution. Méthode d'Euclide.* Elle est fondée sur le théorème 5 (p. 216); si $A = B$, le diviseur commun maximum est A; si $A > B$, soit r_1 leur résidu; ainsi le diviseur cherché divise r_1 (théor. 5), et *vice versâ* le diviseur de r_1 et de B divise A; soit r_2 le résidu de B et de r_1. On démontre de même que le diviseur commun cherché appartient aussi à r_1 et r_2; les résidus r_1, r_2, r_3.... allant en diminuant, on parviendra nécessairement à zéro ou à l'unité Dans le premier cas, le diviseur correspondant au résidu nul est le diviseur

commun maximum cherché ; dans le second cas, les deux nombres n'ayant d'autres diviseurs que l'unité, sont premiers entre eux. (Euclide, liv. VII, prop. 2 ; liv. X, prop. 3.)

2^e *solution. Méthode de décomposition.* On décompose chaque nombre en ses facteurs premiers. On prend tous les facteurs communs aux deux ; on donne à chacun de ces facteurs le plus petit exposant qu'il a dans les deux nombres ; le produit de ces puissances est le plus grand commun diviseur cherché. Exemple :

$$504 = 2^3.3^2.7\ ;\quad 2880 = 2^6.3^2 5\ ,$$

ainsi le diviseur commun maximum de 504 et de 2880 est $2^3.3^2 = 72$.

32. *Problème* 6. Trouver une limite pour le nombre d'opérations à effectuer dans la recherche du plus grand commun diviseur, par la méthode d'Euclide.

Solution. Soient A et B les deux nombres ; $A > B$; et $r_1, r_2, r_3 \ldots r_n$ les résidus ; n indique le nombres d'opérations et r_n le dernier résidu. On suppose qu'on prend toujours les résidus les plus petits, et au besoin des résidus négatifs. Ainsi on a donc

$$r_1 < \frac{B}{2};\quad r_2 < \frac{r_1}{2};\quad r \ldots r_n < \frac{r_{n-1}}{2};$$

sans exclure l'égalité (30). Donc

$$r_2 < \frac{B}{2^2};\quad r_3 < \frac{B}{2^3};\ \ldots\ r_n < \frac{B}{2^n};$$

or r_n étant un nombre entier, on a necessairement

$$2^n < B\ ;\quad \text{ou}\quad n < \frac{\log.B}{\log.2};\quad \text{or}\quad \frac{1}{\log.2} < \frac{10}{3};$$

donc

$$n < \frac{10}{3}\log.B\ ;$$

si B a m chiffres, alors $m > \log.B$: donc $n < \frac{10}{3}m$.

Le plus souvent, le nombre d'opérations est bien au-dessous de cette limite; ainsi dès qu'on parvient à un résidu premier avec le diviseur correspondant, l'opération se termine là. (*Voir* t. I, p. 355.)

32 (*bis*). *Théorème de M. Gauss.* Les carrés des modules des termes de la série A, B, r_1, r_2, r_3.... r_n vont toujours en diminuant.

Démonstration. La proposition est évidente quand A et B ont des nombres réels. Si A et B sont imaginaires, soit $\frac{A}{B} = b + ci$, b et c sont réels, et $i = \sqrt{-1}$; soient b' et c' les entiers les plus rapprochés à $\frac{1}{2}$ près de b et c; de sorte que $(b - b')^2 < \frac{1}{4}$; $(c - c')^2 < \frac{1}{4}$; on a $A = Bq_1 + r_1$. Faisons

$$q_1 = b' + c'i; \quad B = h + ki; \quad r_1 = f + gi;$$

h, k, f, g sont des nombres réels. De ces diverses équations on tire

$$\frac{r_1}{B} = b - b' + i(c - c') = \frac{f + gi}{h + ki},$$

et passant aux modules,

$$(b - b')^2 + (c - c') = \frac{f^2 + g^2}{h^2 + k^2}.$$

Le premier membre est plus petit que $\frac{1}{2}$; donc $f^2 + g^2$, carré du module de r_1, ne surpasse pas la moitié de $h^2 + k^2$, carré du module de B. Ce qu'il fallait démontrer.

Observation. M. Gauss appelle *norme* le carré d'un module : cette expression abrége beaucoup d'énoncés. Le théorème précédent sert de base à la théorie des racines complexes des équations.

Corollaire. r_n est diviseur commun de A et B, et si l'on a $r_n = \pm 1$ ou bien $r_n = \pm i$, les nombres A et B n'ont pas de diviseur commun.

33. Problème 7. Trouver le plus grand commun diviseur des nombres A, B, C, D, etc.

1re *Solution. Méthode d'Euclide.* Soit M le plus grand commun diviseur entre A et B ; on cherche le plus grand commun diviseur entre M et C, et ainsi de suite. (Euclide, liv. VII, prop. 3 ; liv. X, prop. 2-4.)

2e *Solution. Méthode de décomposition.* On prend les facteurs premiers communs, avec leurs plus petits exposants ; on en forme un produit qui est le plus grand commun diviseur cherché.

Corollaire. En divisant tous ces nombres par leur plus grand commun diviseur, les quotients n'ont plus de commun diviseur.

34. Problème 8. Trouver le plus petit multiple de deux nombres A et B.

1re *Solution. Méthode d'Euclide.* Soit D le plus grand commun diviseur, a le quotient de $\frac{A}{D}$ et b le quotient de $\frac{B}{D}$, le plus petit multiple est abD. (Euclide, liv. VII, prop. 36.)

2e *Solution. Méthode de décomposition.* On fait le produit de tous les facteurs premiers élevés chacun au plus haut exposant.

35. Problème 9. Trouver le plus petit multiple des nombres A, B, C, D.....

1re *Solution. Méthode d'Euclide.* Soit M le plus petit multiple de A et B ; on cherche le plus petit multiple M_1 de M et C, et ainsi de suite. Le dernier plus petit multiple satisfait à la question. (Euclide, liv. VII, prop. 38, seulement pour trois nombres.)

2e *Solution. Méthode de décomposition.* Comme pour le problème précédent.

Observation. Les problèmes 5, 7, 8, 9 servent à simplifier

les fractions et à les ramener au moindre dénominateur commun.

Nombres congruents, modules et congruences.

36. *Définition.* Deux nombres sont dits *congruents* relativement à un troisième nombre, lorsque, étant divisés chacun par ce troisième nombre, ils laissent des résidus égaux, et ce troisième nombre est dit le *module* des deux nombres *congruents*.

37. Si a et b sont congruents par rapport au module p, on aura $a - b = \dot{p}$ (th. 6, p. 216); et réciproquement, si l'on a $a - b = \dot{p}$, a et b sont congruents par rapport au module p. Une telle équation se nomme une *congruence*.

Pour exprimer que $a - b$ n'est pas divisible par p, nous écrirons $a - b > \dot{p}$; et dans ce cas, a et b ne sont pas congruents relativement à p. Ainsi $a > \dot{p}$ signifie que a n'est pas divisible par p. Si $a > \dot{x}$, x désignant un nombre quelconque supérieur à l'unité, a est un nombre premier.

Remarque. Euclide, au livre X, prop. 80, dit qu'une ligne est *congrue* (προσαρμόζει) à une autre, lorsqu'elle satisfait à certaine condition de commensurabilité. M. Gauss a transporté cette locution en arithmétique et en a fait la base d'une doctrine qui fait époque dans la théorie des nombres; l'illustre géomètre écrit ainsi les congruences $a \equiv b \pmod{p}$; les notations étant purement conventionnelles, lorsqu'elles n'ont pas encore acquis la sanction des siècles, on peut et on doit les changer, s'il y a avantage. Legendre a adopté cette forme $a - b = \mathrm{M}(p)$, où M est la lettre initiale du mot multiplicateur; quelquefois encore, il emploie cette forme $\frac{a-b}{p} = e$, e étant la lettre initiale du mot entier. Nous avons pensé que le point, étant déjà admis pour désigner une multiplica-

tion, pourrait par analogie encore servir dans les congruences. On fait ce signe facilement et promptement ; ce qui est un avantage pour le calculateur et aussi sous le rapport typographique.

M. Cauchy s'est servi des mots *équivalents* et *équivalence*, pour remplacer les mots *congruents* et *congruence*. Ces nouvelles dénominations ne paraissent pas avoir été adoptées.

Théorie des résidus dans les progressions arithmétiques ; congruences du 1er degré.

38. Lemme 1. Etant données n quantités quelconques, disposées dans un ordre quelconque sur une ligne horizontale, la dernière moins la première est égale à la somme des $n-1$ restes qu'on obtient en retranchant chaque quantité de celle qui la précède.

Démonstration. Soient a, a_1, a_2, a_3 . . . a_{n-1}, a_n les n quantités, on a l'identité

$$a_n - a = (a_1 - a) + (a_2 - a_1) + (a_3 - a_2) + \ldots . (a_n - a_{n-1}).$$

Corollaire. Si ces différences sont toutes égales, on a

$$a_n - a = (n-1)(a_1 - a) ;$$

ce qui a lieu dans les progressions arithmétiques.

Observation. Ce lemme est la base du calcul aux différences finies.

39. Lemme 2. Lorsque les n quantités étant réelles sont écrites suivant leur ordre de grandeur, la différence des quantités extrêmes est plus grande qu'aucune différence entre des quantités intermédiaires.

Démonstration. Soient a_1, a_2, a_3,... a_p.... a_q.... a_n, n quantités écrites suivant un ordre ascendant, on aura

$$a_n - a_1 > a_q - a_p ;$$

car $a_q - a_p$ est égale à la somme de toutes les différences in-

termédiaires, et $a_n - a_1$ est égale à cette même somme, plus les différences comprises entre a_p et a_1 ; et encore entre a_n et a_q. Donc, etc.

40. Lemme 3. Si n nombres inégaux se succèdent suivant un ordre ascendant, deux quelconques de ces nombres ne peuvent être congruents par rapport à un module plus grand que la différence des nombres extrêmes.

Démonstration. Le module étant plus grand que la différence des extrêmes, est plus grand *à fortiori* qu'une différence entre deux nombres intermédiaires (lemme 2) ; le module ne peut donc diviser cette différence ; les deux nombres ne sont donc pas congruents.

Corollaire. Divisant donc tous les nombres par ce module, on obtient n restes différents.

41. Théorème 11. n nombres entiers consécutifs étant divisés chacun par n, donnent les résidus $0, 1, 2, 3 \ldots n-1$, dans un ordre quelconque.

Démonstration. Ce théoreme est une conséquence immédiate du lemme précédent. (Disq. arith., sec. 1, § 3.)

42. Théorème 12. Soit la progression arithmétique $a, 2a, 3a \ldots (n-1)a$, n étant premier avec a ; si l'on divise chaque terme par n, on obtient les résidus $1, 2, 3 \ldots n-1$.

Démonstration. La différence de deux termes quelconques est ka, ou $k < n$; et a étant premier avec n, ka n'est donc pas divisible par n. Par conséquent, aucune différence n'est divisible par n ; tous les restes sont donc différents et moindres que n, et aucun reste n'est nul. Donc, etc.

(*La suite prochainement.*)