

Théorie élémentaire des nombres.

D'APRÈS EULER, LEGENDRE, MM. GAUSS ET CAUCHY.

(Suite et fin.)

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.) 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.

1^{re} solution. Méthode d'Euclide. Elle est fondée sur le théorème 5 ; 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 versa, 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 $r_1, r_2, r_3, \dots$ 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 :

$$504 = 2^3.3^2.7 ; 2880 = 2^5.3^3.5,$$

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 $r_1, r_2, r_3, \dots, r_n$ les résidus ; n indique le nombre 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. On a donc

$$r_1 < \frac{B}{2} ; r_2 < \frac{r_1}{2} ; r_3 < \frac{r_2}{2} ; \dots ; r_n < \frac{r_{n-1}}{2} ;$$

sans exclure l'égalité (30). Donc

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

or r_n étant un nombre entier, on a nécessairement

$$2^n < B ; \text{ ou } n < \frac{\log B}{\log 2} ; \text{ or, } \log 2 \text{ étant } 0.3, \text{ on a } n < \frac{1}{0.3} \log B ;$$

donc

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

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

(Voir plus loin REMARQUE I.)

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.

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

Démonstration. La proposition est évidente quand A et B sont des nombres réels. Si A et B sont imaginaires, soit

$$\frac{A}{B} = b + ci, \quad b \text{ et } c \text{ sont réels, et } i = \sqrt{-1} ; \text{ soient } b' \text{ et } c'$$

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

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

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,

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

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 abrégée 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 $r = \pm 1$ 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.

1^{re} 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.)

2^e 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.

1^{re} 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.)

2^e 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, etc.

1^{re} solution. Méthode d'Euclide. Soit M le petit multiple de A et B ; on cherche le plus petit multiple M₁ 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.)

2^e solution. Méthode de décomposition. Comme pour le problème précédent.