

Remarques sur le théorème de Gauss

L'article de M. THOVERT, dans le dernier *Bulletin* (n° 170, octobre 1955) suggère de comparer la démonstration originale de Gauss à celle de Niewenglowski ; elle en diffère peu quant au fond ; elle se trouve tout au début de la « section seconde » de son célèbre traité de théorie des nombres : « *Disquisitiones arithmeticae* », traduit en français par Pouillet-Delisle, sous le titre : « *Recherches arithmétiques* » (cet ouvrage vient d'être réédité à la librairie A. Blanchard, 7, rue Racine, Paris).

Voici le début de la « section seconde » (dans la « section première », Gauss définit les congruences, dont il est le créateur, et donne leurs propriétés élémentaires).

« THÉORÈME. — Le produit de deux nombres positifs plus petits qu'un nombre premier donné, ne peut être divisé par ce nombre premier. »

Soit p le nombre premier et $a < p$ et > 0 ; je dis qu'on ne pourra trouver aucun nombre positif b , plus petit que p , qui rende $ab \equiv 0 \pmod{p}$.

En effet, s'il peut y en avoir, supposons que ce soient les nombres b, c, d , etc... tous plus petits que p , en sorte qu'on ait $ab \equiv 0, ac \equiv 0$, etc... (mod. p). soit b le plus petit de tous, de sorte qu'on n'en puisse supposer un plus petit que b ; on aura évidemment $b > 1$, car si $b = 1$, on aurait $ab = a < p$ et partant non divisible par p . Or p , comme nombre premier, ne peut être divisé par b , mais tombera entre deux multiples de b , mb et $(m+1)b$. Soit $p - mb = b'$, b' sera positif et $< b$. Or nous avons supposé $ab \equiv 0 \pmod{p}$, on aura donc $mab \equiv 0$, et en retranchant de $ap \equiv 0$ on aura $a(p - mb) = ab' \equiv 0$; donc b' devrait être mis au rang des nombres b, c, d , etc... et serait plus petit que le plus petit de tous, ce qui est contre la supposition.

THÉORÈME. — Si aucun des deux nombres a et b n'est divisible par un nombre premier p , le produit ab ne le sera pas non plus.

Soient α et β les résidus minima positifs des nombres a et b , suivant le module p ; aucun d'eux ne sera nul par hypothèse. Or si l'on avait $ab \equiv 0$, comme $ab \equiv \alpha\beta$ on aurait $\alpha\beta \equiv 0$, ce qui serait contraire au théorème précédent. »

Et Gauss ajoute :

« La démonstration de ce théorème a déjà été donnée par Euclide, El. VII, 32. Nous n'avons pas cependant voulu l'omettre, tant parce que plusieurs auteurs modernes ont présenté des raisonnements vagues au lieu de démonstration, ou bien ont négligé ce théorème ; que dans le but de faire mieux saisir, par ce cas très simple, l'esprit de la méthode que nous appliquerons par la suite à des points difficiles. »

On voit que le théorème cité dans l'article de M. THOVERT se déduit immédiatement du théorème précédent des « *Disquisitiones* » en raisonnant par l'absurde.

Si l'on veut « moderniser » et faire ressortir la structure des démonstrations on peut considérer la notion de « *MODULE de nombres* ».

DÉFINITION. — Un ensemble de nombres réels est appelé « module » si l'ensemble contient avec les nombres x et y les nombres : $x \pm y$.

(Notons que le nombre 0 appartient à n'importe quel module et que, par suite, un module qui contient x contient aussi $-x$ et $m.x$ (m entier positif, négatif ou nul). On a alors le :

THÉORÈME. — Si un module de nombres est tel que dans tout intervalle borné il n'y ait qu'un nombre fini d'éléments du module, ce module est l'ensemble des multiples : $m.d$ d'un nombre positif d du module ($m = 0 ; \pm 1 ; \pm 2 \pm \dots$), ce nombre d est appelé LA BASE du module.

Soit un intervalle contenant zéro et des nombres positifs du module ; il n'en contient qu'un nombre fini ; soit d le plus petit d'entre eux ; si un nombre $h \neq 0$

du module n'était pas de la forme md , il existerait un nombre entier positif, négatif ou nul m_0 tel que $mod < h < (m_0 + 1)d$, d'où $0 < h - m_0d < d$, or, par définition d appartenant au module il en est de même de mod et, par suite, de $h - mod$, ce qui est en contradiction avec la définition de d ; tout nombre du module est donc de la forme $m.d$; la réciproque est immédiate.

CONSÉQUENCE : Si un module de nombres est un module de nombres entiers, il admet nécessairement une base d et les nombres du module sont les multiples de d .

Démontrons alors le théorème suivant :

Si un nombre premier $p > 1$ divise un produit ab sans diviser a , alors il divise b .

On a par hypothèse p premier et $a \equiv 0 \pmod{p}$. Considérons alors l'ensemble (E), évidemment non vide, des entiers x quelconques, tels que : $ax \equiv 0 \pmod{p}$.

Il est immédiat que cet ensemble est un module d'entiers ; il admet donc une base d ($d > 0$) et on a : $x \equiv 0 \pmod{d}$. Or p appartient à (E) et par suite il existe un entier k tel que $p = k.d$.

On a certainement $d > 1$, car $d = 1$ entraînerait : $ad \equiv a \equiv 0 \pmod{p}$, ce qui est contraire à l'hypothèse ; il en résulte alors, puisque p est premier : $k = 1$; $d = p$, donc $x \equiv 0 \pmod{p}$, le théorème est démontré.

Notons que la théorie du P.G.C.D. peut se déduire de la notion de module.

Soient a et b deux nombres entiers ; considérons l'ensemble (F) des nombres de la forme : $ma + nb$, où m et n sont des entiers quelconques, positifs, négatifs ou nuls. Il est immédiat que cet ensemble est un module d'entiers, il admet donc une base g ; tout nombre de (F) est un multiple de g ; en particulier a et b qui correspondent à : $m = 1$; $n = 0$ et $m = 0$; $n = 1$. On a donc :

$$a = ga',$$

$$b = gb'.$$

Tout diviseur de g divise a et b : de plus, il existe deux entiers quelconques m_0 et n_0 , tels que $g = m_0a + n_0b$, donc tout diviseur commun à a et b divise g ; g est le P.G.C.D. de a et b .

En outre, on obtient immédiatement le résultat suivant :

Pour que a et b soient premiers entre eux, il faut et il suffit qu'il existe deux entiers quelconques u et v , tels que : $au + bv = 1$.

Jacques LEGRAND (*Lycée de Biarritz*).