Se rappeler de cela, Denise Vella-Chemla, début novembre 2024

Il faut que je me rappelle que Gauss voit la relation $a \equiv b$ (mod m) comme une relation d'équivalence sans restriction sur a, b, m (si ce n'est que m est "sans signe", voir image ci-dessous) alors que je l'utilise plutôt systématiquement comme si j'avais :

$$a \bmod m = b \iff \exists q \text{ tel que } \begin{array}{l} a = mq + b \\ \text{et } b \geq 0 \text{ et } b \text{ minimum} \\ \text{et } a \geq 0 \text{ et } a \text{ maximum.} \end{array}$$

i.e. je projette la classe d'équivalence dans $\mathbb{Z}$ sur l'intervalle $[0, m[$; Gauss appelle le résidu modulaire que je considère toujours le "résidu minimum positif de a modulo m".

RECHERCHES

ARITHMÉTIQUES.

SECTION PREMIÈRE.

Des Nombres congrus en général.

1. Si un nombre *a* divise la différence des nombres *b* et *c*, *b* et *c* sont dits *congrus* suivant *a*, sinon *incongrus*. *a* s'appellera le module ; chacun des nombres *b* et *c*, *résidus* de l'autre dans le premier cas, et *non résidus* dans le second.

Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est-à-dire, sans aucun signe.

Ainsi −9 et +16 sont *congrus* par rapport au module 5; −7 est *résidu* de 15 par rapport au module 11, et *non résidu* par rapport au module 3.

Au reste 0 étant divisible par tous les nombres, il s'ensuit qu'on peut regarder tout nombre comme congru avec lui-même par rapport à un module quelconque.

2. Tous les résidus d'un nombre donné *a* suivant le module *m*, sont compris dans la formule $a + km$, *k* étant un entier indéterminé. Les plus faciles des propositions que nous allons exposer

A

FIGURE 1 : article 1 des Recherches arithmétiques de Karl Friedrich Gauss.

4. Il suit de là que chaque nombre aura un résidu, tant dans la suite $0, 1, 2, \ldots (m-1)$, que dans celle-ci $0, -1, -2, \ldots -(m-1)$; nous les appellerons résidus *minima*; et il est clair qu'à moins que 0 ne soit résidu, il y en aura toujours deux, l'un positif, l'autre négatif. S'ils sont inégaux, l'un d'eux sera $< \frac{m}{2}$; s'ils sont égaux, chacun d'eux $= \frac{m}{2}$ sans avoir égard au signe; d'où il suit qu'un nombre quelconque a un résidu qui ne surpasse pas la moitié du module, et que nous appellerons résidu *minimum absolu*.

Par exemple -13 suivant le module 5, a pour résidu *minimum* positif 2, qui est en même temps *minimum absolu*, et -3 pour résidu *minimum* négatif; $+5$, suivant le module 7, est lui-même son résidu *minimum* positif; -2 est le résidu *minimum* négatif et en même temps le *minimum absolu*.

(*) Nous avons adopté ce signe à cause de la grande analogie qui existe entre l'égalité et la congruence. C'est pour la même raison que Legendre, dans des mémoires que nous aurons souvent occasion de citer, a employé le signe même de l'égalité, pour désigner la congruence; nous en avons préféré un autre, pour prévenir toute ambiguité.

FIGURE 2 : article 4 des Recherches arithmétiques de Karl Friedrich Gauss.