Indices (Denise Vella-Chemla, 7.9.2016)

On voudrait fournir les résultats d'un programme qui calcule les indices des nombres au sens de l'article 53 des Recherches arithmétiques de Gauss. Gauss explique que l'intérêt des indices est de faciliter les calculs des puissancs modulaires d'une manière similaire à celle dont l'addition des logarithmes facilite le calcul du logarithme d'un produit.

On peut voir sur l'image extraite du chapitre 3 concernant les résidus des puissances le traitement du cas du nombre premier 19. Pour les nombres premiers p, il y a systématiquement une partition de l'ensemble des nombres de 1 à $p-1$ en parties disjointes selon les diviseurs de $p-1$. Le cardinal de la partie associée à un diviseur donné est fourni par l'indicateur d'Euler du diviseur en question.

53. Pour nous faire entendre plus facilement, nous présenterons d'abord un exemple. Soit $p=19$, les nombres 1, 2, 3...18 peuvent se distribuer de la manière suivante relativement aux diviseurs de 18 :

$$1\{1,\quad 2\{18,\quad 3\{7,11,\quad 6\{8,12,\quad 9\{4,5,6,9,16,17,\quad 18\{2,3,10,13,14,15$$

Ainsi dans cas $\downarrow 1=1$, $\downarrow 2=1$, $\downarrow 3=2$, $\downarrow 6=2$, $\downarrow 9=6$, $\downarrow 18=6$. Avec une légère attention on voit qu'il y en a, relativement à chaque exposant, autant qu'il y a de nombres premiers avec cet exposant et non plus grands que lui, ou bien, en reprenant le signe du n° 40, que $\downarrow d=\phi d$. Mais on peut démontrer généralement cette observation de la manière suivante :

Selon le module 37, les nombres 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35 ont pour indice 36 (leur puissance $36^{ème}$ vaut 1 modulo 37), les nombres 11 et 27 ont pour indice 6 (leur puissance $6^{ème}$ vaut 1 modulo 37) tandis que les nombres 6 et 31 ont pour indice 4.

On calcule par programme pour les nombres n jusqu'à 100 l'indice des nombres compris entre 1 et $n-1$ et on constate, comme indiqué dans la note 53 de Gauss, que les nombres premiers ont la somme des indices des différentes puissances possibles qui vaut $n-1$. On constate par programme que pour les nombres composés, jusqu'à 100 tout du moins, la somme des indices des différentes puissances possibles est *inférieure* à $\frac{n-1}{2}$ (ce qui semble être dit dans l'article 54).