Plus de la moitié ?

Denise Vella-Chemla

16.8.16

On souhaiterait ici montrer une manière enfantine de présenter le lemme de Gauss associé à la loi de réciprocité quadratique. Ce travail peut présenter un intérêt dans la mesure où le comptage des "petits" résidus quadratiques d'un nombre permet de savoir s'il est premier ou composé.

L'énoncé du lemme de Gauss est :

Soit p un nombre premier et a un entier non divisible par p. On considère les entiers

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

et leur plus petit résidu positif modulo p. Parmi ces $(p-1)/2$ entiers distincts compris entre 1 et $p-1$, soit n le nombre de ceux qui sont plus grands que $p/2$. Alors,

$$\left(\frac{a}{p}\right) = (-1)^n$$

où $\left(\frac{a}{p}\right)$ est le symbole de Legendre.

Pour visualiser ce lemme, utilisons des tables de multiplication modulaire et comptons les éléments "supérieurs à la moitié" (à la manière de Gauss, on utilise la lettre R pour noter $x\ R\ y$ le fait que x est un résidu quadratique de y et la lettre N pour noter $x\ N\ y$ le fait que x n'est pas un résidu quadratique de y).

Modulo 7 : (comptage en couleur cyan des nombres supérieurs à $(7-1)/2 = 3$)

	1	2	3	
1	1	2	3	0 est pair $\rightarrow$ 1 R 7
2	2	4	6	2 est pair $\rightarrow$ 2 R 7
3	3	6	2	1 est impair $\rightarrow$ 3 N 7

Modulo 11 : (comptage en couleur cyan des nombres supérieurs à $(11-1)/2 = 5$)

	1	2	3	4	5	
1	1	2	3	4	5	0 est pair $\rightarrow$ 1 R 11
2	2	4	6	8	10	3 est impair $\rightarrow$ 2 N 11
3	3	6	9	1	4	2 est pair $\rightarrow$ 3 R 11
4	4	8	1	5	9	2 est pair $\rightarrow$ 4 R 11
5	5	10	4	9	3	2 est pair $\rightarrow$ 5 R 11

Modulo 19 : (comptage en couleur cyan des nombres supérieurs à $(19-1)/2 = 9$)

	1	2	3	4	5	6	7	8	9	
1	1	2	3	4	5	6	7	8	9	0 est pair → 1 R 19
2	2	4	6	8	10	12	14	16	18	5 est impair → 2 N 19
3	3	6	9	12	15	18	2	5	8	3 est impair → 3 N 19
4	4	8	12	16	1	5	9	13	17	4 est pair → 4 R 19
5	5	10	15	1	6	11	16	2	7	4 est pair → 5 R 19
6	6	12	18	5	11	17	4	10	16	6 est pair → 6 R 19
7	7	14	2	9	16	4	11	18	6	4 est pair → 7 R 19
8	8	16	5	13	2	10	18	7	15	5 est impair → 8 N 19
9	9	18	8	17	7	16	6	15	5	4 est pair → 9 R 19

Modulo 23 : (comptage en couleur cyan des nombres supérieurs à $(23-1)/2 = 11$)

	1	2	3	4	5	6	7	8	9	10	11	
1	1	2	3	4	5	6	7	8	9	10	11	0 est pair → 1 R 23
2	2	4	6	8	10	12	14	16	18	20	22	6 est pair → 2 R 23
3	3	6	9	12	15	18	21	1	4	7	10	4 est pair → 3 R 23
4	4	8	12	16	20	1	5	9	13	17	21	6 est pair → 4 R 23
5	5	10	15	20	2	7	12	17	22	4	9	5 est impair → 5 N 23
6	6	12	18	1	7	13	19	2	8	14	20	6 est pair → 6 R 23
7	7	14	21	5	12	19	3	10	17	1	8	5 est impair → 7 N 23
8	8	16	1	9	17	2	10	18	3	11	19	4 est pair → 8 R 23
9	9	18	4	13	22	8	17	3	13	21	7	6 est pair → 9 R 23
10	10	20	7	17	4	14	1	11	21	8	18	5 est impair → 10 N 23
11	11	22	10	21	9	20	8	19	7	18	6	5 est impair → 11 N 23

La parité du nombre d'éléments "supérieurs à la moitié" par ligne exprime le caractère de résiduosité quadratique du nombre indice de la ligne au module considéré. On a indiqué ce caractère en regard des lignes, à droite. On appellera *lignes paires* les lignes dont le nombre d'éléments supérieurs à la moitié du module considéré est pair et *lignes impaires* les autres.

Voyons sur le module 15 que le comptage ne permet pas de déduire le caractère de résiduosité quadratique à un module composé :

Modulo 15 : (comptage en couleur cyan des nombres supérieurs à $(15-1)/2 = 7$)

	1	2	3	4	5	6	7	
1	1	2	3	4	5	6	7	0 est pair → 1 R 15
2	2	4	6	8	10	12	14	4 est pair or 2 N 15
3	3	6	9	12	0	3	6	2 est pair or 3 N 15
4	4	8	12	1	5	9	13	4 est pair → 4 R 15
5	5	10	0	5	10	0	5	2 est pair or 5 N 15
6	6	12	3	9	0	6	12	3 est impair or 6 R 15
7	7	14	6	13	5	12	4	3 est impair → 7 N 15

Outre le fait que 3 et 15, par comptage, seraient considérés comme résidus quadratiques de 15 alors qu'ils le divisent, on voit que 2 a un nombre pair d'éléments supérieurs à 7 dans sa ligne alors qu'il n'est pas résidu quadratique de 15 ou bien on voit que 6 a un nombre impair d'éléments supérieurs à 7 dans sa ligne alors qu'il est quant à lui effectivement résidu quadratique de 15 (il est son propre carré modulo 15 car $6 \times 6 = 36 \equiv 6\ (mod\ 15)$).

Ce qu'il faudrait comprendre et démontrer, c'est pourquoi le nombre de lignes "paires" (correspondant au nombre de résidus quadratiques *inférieurs ou égaux*[1] à $n/2$) est toujours supérieur à $n/4$ pour les nombres premiers de la forme $4k+3$.

Il faudrait également démontrer une hypothèse qu'on a émise et vérifiée jusqu'à 3.10^5. Le nombre de résidus quadratiques de n inférieurs ou égaux à $n/2$ est toujours inférieur à $n/4$ pour les nombres composés. Cette hypothèse peut présenter un intérêt par sa simplicité : elle correspond au fait de compter le nombre de points à coordonnées entières et dont la seconde coordonnée est inférieure ou égale à une certaine valeur $(n/2)$, ces points appartenant à une surface définie par une équation quadratique de la forme $x^2 - y - nz = 0$.

1. Attention à l'inversion ici, il s'agit effectivement de compter les *petits* résidus quadratiques, i.e. ceux qui sont *inférieurs ou égaux* à la moitié du module.