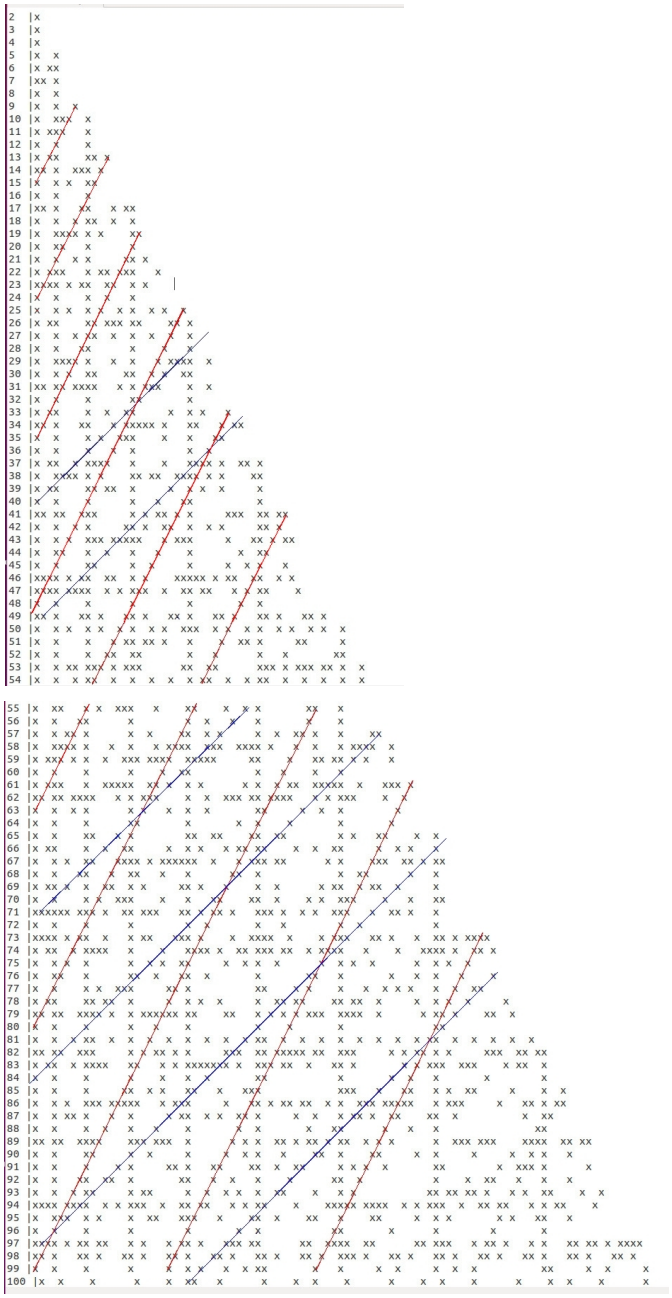
Suites de relations "est résidu quadratique de" en miroir (Denise Vella-Chemla, 31.10.2017)

Les deux graphiques ci-dessous rappellent le contenu de la table de l'annexe des Recherches arithmétiques de Gauss[1] et fournissent pour un nombre ses résidus quadratiques (compter une croix par colonne, la première correspondant à 1).



Le trait rouge qui démarre à la croix $(48, 1)$ correspond aux équation de la forme $7^2 - a - b = 0$ avec $a + b = 49$. On a de la même manière un trait rouge qui débute à chaque croix $(x^2 - 1, 1)$. Si on note[2] R la relation *"est un résidu quadratique de"*, les traits rouges correspondent à l'équivalence $b\ R\ a \iff (b + i)\ R\ (a - i)$.

Les traits bleus identiquement correspondent au fait qu'un certain nombre d'équations quadratiques sont simultanément vérifiées (il s'agit, comme pour ce que nous avons proposé au sujet de la conjecture de Goldbach, de lier entre elles deux assertions logiques, l'une correspondant au fait qu'une équation soit ou non vérifiée par les coordonnées d'un point, et l'autre correspondant au fait qu'*une autre équation* soit ou non vérifiée par *un autre point*. Prenons par exemple la ligne reliant les points $(71, 2)$, $(70, 4)$, $(69, 6)$, $(68, 8), \ldots$, ces points représentent les équations $12^2 - 71 \times 2 - 2 = 0, 12^2 - 70 \times 2 - 4 = 0, 12^2 - 69 \times 2 - 6 = 0, 12^2 - 68 \times 2 - 8 = 0, \ldots$. On a fixé dans l'équation $x^2 - zy - t = 0$ les valeurs de x et y à 12 et 2 et z et t sont les coordonnées de points alignés. On remarque que ces droites passent par des points dont les ordonnées sont toutes impaires $1, 3, 5, \ldots$ ou toutes paires $2, 4, 6$ suivant que le carré est impair ou pair.

[1] Table II, n°99, p.499 de l'édition Jacques Gabay.
[2] comme Gauss.

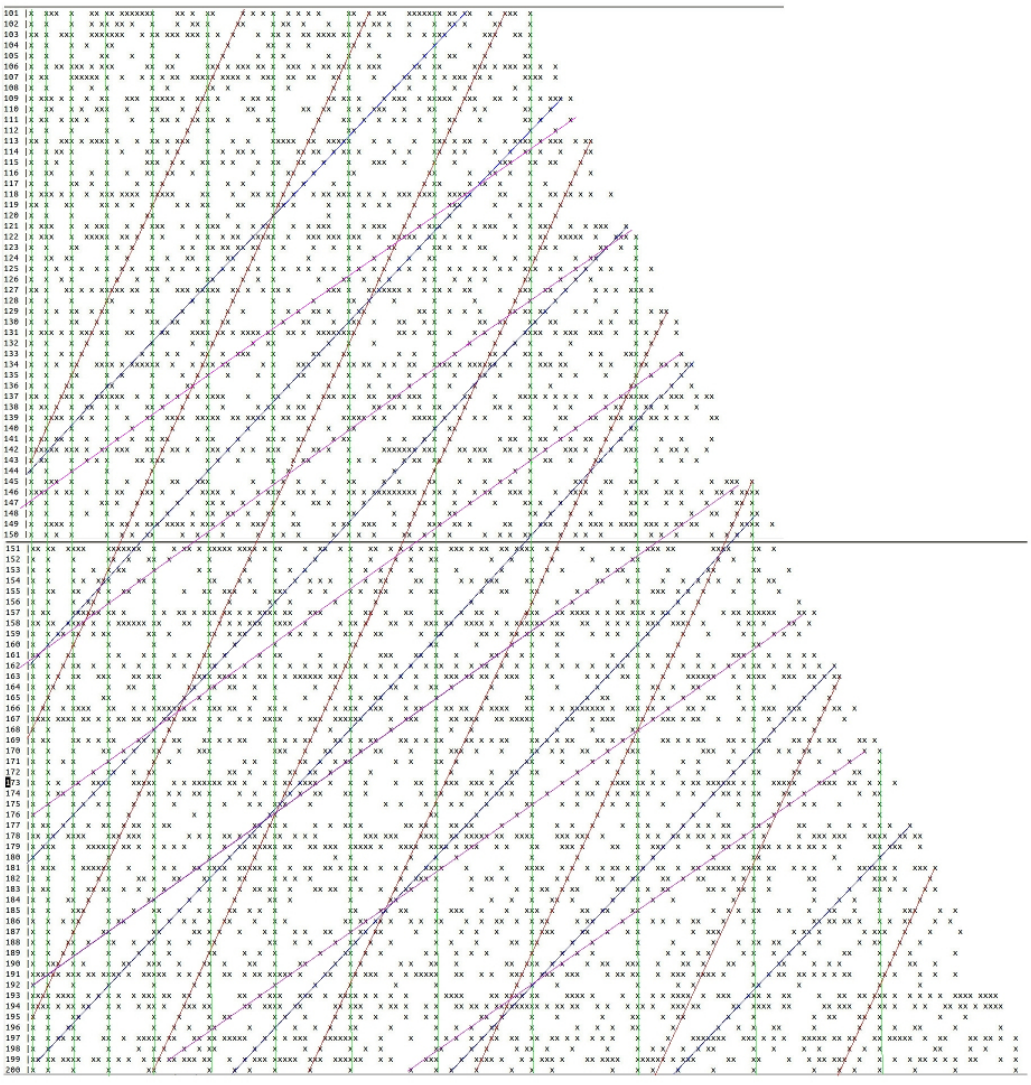
Il faut insister sur le fait que chaque croix représente une assertion logique contenant deux quantificateurs existentiels. Par exemple, les 3 points $(71, 2), (70, 4)$ et $(69, 6)$ représentent les 3 assertions logiques :

- $\exists x_1, 1 \leqslant x_1 < 71, \exists y_1, 1 \leqslant y_1 < 71$, tels que $x_1^2 - 71y_1 - 2 = 0$ (que l'on peut écrire $x_1^2 \equiv 2 \ (mod\ 71)$) ;
- $\exists x_2, 1 \leqslant x_2 < 70, \exists y_2, 1 \leqslant y_2 < 70$, tels que $x_2^2 - 70y_2 - 4 = 0$ (que l'on peut écrire $x_2^2 \equiv 4 \ (mod\ 70)$) ;
- $\exists x_3, 1 \leqslant x_3 < 69, \exists y_3, 1 \leqslant y_3 < 69$, tels que $x_3^2 - 69y_3 - 6 = 0$ (que l'on peut écrire $x_3^3 \equiv 6 \ (mod\ 69)$) ;

Ces trois assertions sont simultanément vérifiées par $x_1 = x_2 = x_3 = 12$ et $y_1 = y_2 = y_3 = 2$.

Le nombre de résidus quadratiques d'un nombre premier p est égal à $\frac{p-1}{2}$, c'est un fait démontré par Gauss. On peut relier les résultats présentés ici à ce fait en distinguant les deux sortes de nombres premiers :

- pour un nombre premier p de la forme $4k - 1$, il y a autant de couples (x, y) de produit $xy \equiv -1 \ (mod\ p)$ que de résidus quadratiques de p (i.e. $2k - 1 = \frac{p-1}{2}$) ; chacun des couples en question contient un résidu quadratique et un non-résidu quadratique
- pour un nombre premier p de la forme $4k + 1$, si on note r le nombre de résidus quadratiques de p (égal à $\frac{p-1}{2}$), alors il y a $r+1$ couples (x, y) de produit $xy \equiv -1 \ (mod\ p)$ (i.e. $\frac{p+1}{2}$) : deux résidus quadratiques sont systématiquement de carré congru à $-1 \ (mod\ p)$ tandis que les autres couples de produit -1 font intervenir deux résidus quadratiques chacun.



En fixant 2 variables sur 4 dans les équations de la forme $x^2 - yz - t = 0$, on explique les droites de pente 1, 2 ou 3 qui apparaissent sur la table de résiduosité quadratique de Gauss pour les modules compris entre 100

et 200. On pourrait, de la même manière qu'on cherche des droites, chercher des points à coordonnées entières appartenant à certains cercles : ce qui importe, ce sont les liens que les points établissent entre 4 variables, pour ce qui concerne la résiduosité quadratique.

On voit clairement par les concentrations horizontales de points, le fait que les nombres premiers maximisent le nombre de résidus quadratiques (un nombre premier p a $\frac{p-1}{2}$ résidus quadratiques).