Nombre de solutions de l'équation $xy = -1$ dans les corps premiers (Denise Vella-Chemla, 31.10.2017)

On réalise par programme que dans un corps premier $\mathbb{Z}/p\mathbb{Z}$, le nombre de couples (x, y) solutions de l'équation $xy = -1 \ (mod\ p)$ avec x différent de y est égal à $\frac{p-1}{2}$ si p est de la forme $4k+3$ et à $\frac{p-3}{2}$ si p est de la forme $4k+1$; dans ce second cas, deux nombres sont racines de -1.

Donnons deux exemples :

- pour $p = 13$ de la forme $4k+1$, les couples dont le produit est égal à -1 sont les couples

  $$(1, 12), (2, 6), (3, 4), (7, 11), (9, 10)$$

  et les racines carrées de -1 sont 5 et 8.

  Il y a bien 5 couples de nombres différents avec $5 = \frac{13-3}{2}$;

- pour $p = 19$ de la forme $4k+3$, les couples dont le produit est égal à -1 sont les couples

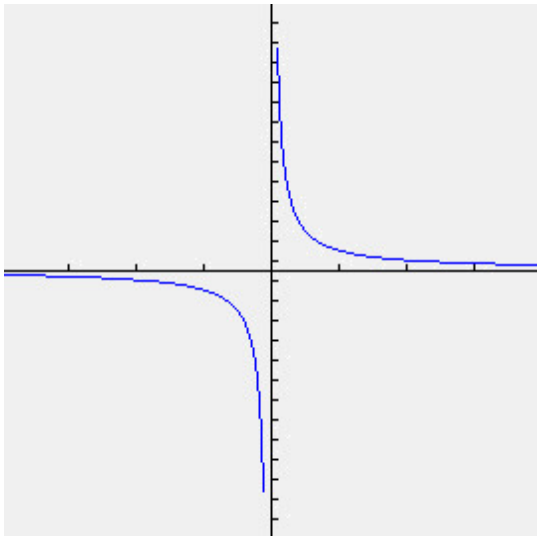
  $$(1, 18), (2, 9), (3, 6), (4, 14), (5, 15), (7, 8), (10, 17), (11, 12), (13, 16).$$

  Il y a bien 9 couples de nombres différents avec $9 = \frac{19-1}{2}$.

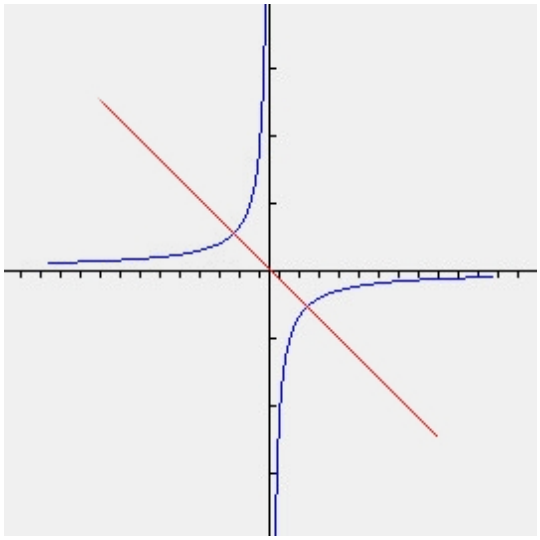
Il est plus simple pour les premiers de la forme $p = 4k+1$ de compter les couples (x, x) avec les autres et de voir les $4k+3$ comme des $4k-1$, cela permet d'unifier les deux cas de la façon suivante : pour les nombres premiers et eux seulement de la forme $4k+1$, il y a $2k+1$ couples (x, y) solutions à l'équation $xy = -1$ tandis que pour les nombres premiers de la forme $4k-1$, il y a $2k-1$ couples (x, y) solutions à cette équation.

(On a bien pour $13 = 4 \times 3 + 1$ un nombre de 7 couples avec $7 = 2 \times 3 + 1$ et pour $19 = 4 \times 5 - 1$ un nombre de 9 couples avec $9 = 2 \times 5 - 1$).

L'équation $xy = -1$, dans le plan cartésien habituel, est l'équation d'une hyperbole toute semblable à l'hyperbole $y = \frac{1}{x}$, cette dernière se trouvant être l'inverse du logarithme. Elle est simplement dans les deuxième et quatrième quadrants du plan cartésien (alors que la courbe de l'inverse du logarithme est dans les premier et troisième quadrants). On peut l'obtenir à partir de l'hyperbole inverse du logarithme par une symétrie verticale, ou bien par une symétrie horizontale, ou bien par une rotation d'un quart ou de trois quarts de tours. Ces deux courbes ont toutes deux deux axes de symétrie et elles sont invariantes par une rotation d'un demi-tour.

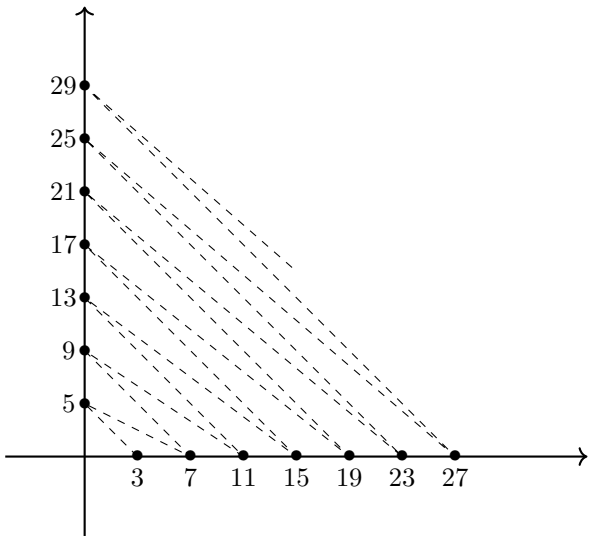


$y = \frac{1}{x}$



$y = -\frac{1}{x}$

On se place dans le plan complexe. Du fait des égalités $4k-1 = (2\sqrt{k}-1)(2\sqrt{k}+1)$ et $4k+1 = (2\sqrt{k}-i)(2\sqrt{k}+i)$, on décide de représente les nombres de la forme $4k-1$ par les nombres entiers successifs k et les seconds (les $4k+1$) par les imaginaires purs successifs ki. Voyons cela sur un diagramme, la "navette" reliant les impairs sucessifs. On ne note pas sur le graphique, pour ne pas l'alourdir, les entiers de la forme $4k$, carrés de $2\sqrt{k}$ ou de la forme $4k+2$ carrés de $2\sqrt{k} - i\sqrt{2}$.



La transformation des coordonnées qui permet de passer du point qui correspond à un nombre impair au point qui correspond au nombre impair suivant est la transformation qui permet d'obtenir la chaîne de points ci-dessous :

$$\binom{1}{0}\binom{0}{1}\binom{2}{0}\binom{0}{2}\binom{3}{0}\binom{0}{3}\binom{4}{0}\cdots$$

On peut obtenir l'opération matricielle de cette opération en ajoutant une troisième coordonnée aux points ; elle transforme $\begin{pmatrix} x_k \\ y_k \\ 1 \end{pmatrix}$ ainsi (on prend comme convention que la coordonnée non nulle ne change pas pour les indices pairs de points) :

$$\begin{pmatrix} x_k \\ y_k \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & \frac{1+(-1)^k}{2} & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_k \\ y_k \\ 1 \end{pmatrix}$$

Il faudrait maintenant essayer de comprendre pourquoi, voire de prouver par récurrence, le nombre de couples $xy = -1\ (mod\ n)$, qui correspond au nombre de triplets solutions d'équations de la forme $xy - z(4k \pm 1) + 1 = 0$ vaut toujours $2k + 1$ pour les $4k + 1$ et $2k - 1$ pour les $4k - 1$ en utilisant la représentation géométrique des nombres qui vient d'être proposée.