Rappels sur le nombre de racines de -1 dans les corps premiers (Denise Vella-Chemla, 4.11.2017)

On rappelle que :

- si p est de la forme $4k+1$, deux nombres et deux seulement ont pour carré -1 dans $\mathbb{Z}/p\mathbb{Z}$; ces nombres ont pour somme p et pour produit 1 ;
- il y a exactement $2k-1$ (respectivement $2k+1$) couples (x,y) tels que $xy \equiv -1\ (mod\ p)$.

Pour n composé, soit on trouve 0 ou 4 racines de -1 et non 2, soit on trouve, comme pour les nombres premiers, deux telles racines (par exemple, pour les carrés de nombres premiers de la forme $4k+1$) mais alors, le nombre de couples (x,y) tels que $xy \equiv -1\ (mod\ p)$ n'est pas égal à $2k-1$ si n est de la forme $4k-1$ ou n'est pas égal à $2k+1$ si n est de la forme $4k+1$.

Fournissons quelques valeurs pour fixer les idées :

- dans $\mathbb{Z}/5\mathbb{Z}$, 2 et 3 ont pour carré -1 ;
- dans $\mathbb{Z}/13\mathbb{Z}$, 5 et 8 ont pour carré -1 ;
- dans $\mathbb{Z}/17\mathbb{Z}$, 4 et 13 ont pour carré -1 ;
- dans $\mathbb{Z}/29\mathbb{Z}$, 12 et 17 ont pour carré -1 ;
- dans $\mathbb{Z}/37\mathbb{Z}$, 6 et 31 ont pour carré -1 ;
- dans $\mathbb{Z}/41\mathbb{Z}$, 9 et 32 ont pour carré -1 ;
- dans $\mathbb{Z}/53\mathbb{Z}$, 23 et 30 ont pour carré -1 ;
- dans $\mathbb{Z}/61\mathbb{Z}$, 11 et 50 ont pour carré -1 ;
- dans $\mathbb{Z}/73\mathbb{Z}$, 27 et 46 ont pour carré -1 ;
- dans $\mathbb{Z}/89\mathbb{Z}$, 34 et 55 ont pour carré -1 ;
- dans $\mathbb{Z}/97\mathbb{Z}$, 75 et 22 ont pour carré -1.

Dans $\mathbb{Z}/n\mathbb{Z}$ lorsque $n = 9, 21, 33, 45, 49, 57, 69, 77, 81, 93$, il n'y a pas de racine de -1.

Dans $\mathbb{Z}/n\mathbb{Z}$ lorsque $n = 65$ ou $n = 85$, il y a 4 racines de -1 (deux à deux de somme n et de produit 1), qui sont les nombres 8 et 57 ou bien 18 et 47 si $p = 65$ ou qui sont 13 et 72 ou bien 38 et 47 si $p = 85$.

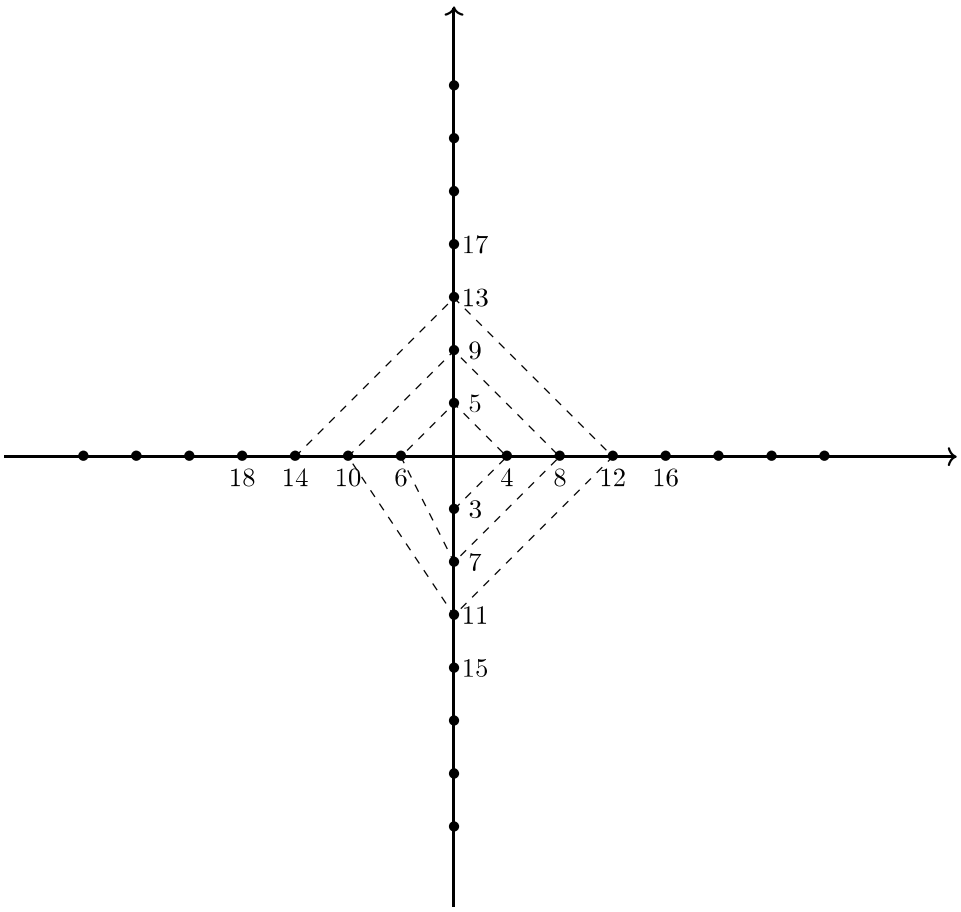
Pour 25 $(= 4 \times 6 + 1)$, carré d'un nombre premier de la forme $4k+1$, il y a, comme pour les nombres premiers de la forme $4k+1$, 2 racines carrées de -1 (7 et 18) mais ce qui exclut la primalité alors, c'est le nombre de couples (x,y) dont le produit est égal à -1 qui s'élève à 10, différent de 13 $(= 2 \times 6 + 1)$.

Pour les carrés de nombres premiers de la forme $4k+3$ (49, 121, 361), il n'y a pas de racine de -1.

Dans une note toute récente, on avait proposé un positionnement des nombres par des points du plan complexe qui les faisaient "faire la navette" entre les deux demi-axes positifs des coordonnées. On omettait les points associés aux nombres pairs parce qu'on ne voyait pas trop où les placer.

Essayons de proposer une nouvelle représentation graphique, qui pourrait peut-être être utile pour étudier la primalité.

On se place dans le plan complexe. On positionne les nombres sur une spirale selon le graphique suivant :



La transformation des coordonnées qui permet de passer d'un point de la spirale au suivant est la transformation qui permet d'obtenir la chaîne de points ci-dessous :

$$\begin{pmatrix}0\\-i\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\i\end{pmatrix}\begin{pmatrix}-1\\0\end{pmatrix}\begin{pmatrix}0\\-2i\end{pmatrix}\begin{pmatrix}2\\0\end{pmatrix}\begin{pmatrix}0\\2i\end{pmatrix}\begin{pmatrix}-2\\0\end{pmatrix}\cdots$$

Cette transformation a pour opérateur :

$$\begin{pmatrix}x\\y\end{pmatrix}\mapsto\begin{pmatrix}0&i\\i&0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}iy\\ix\end{pmatrix}$$

faux : cela ne fait pas augmenter le rayon.

On doit pour représenter les points de la spirale utiliser un complexe en première coordonnée (qui vaut k, $-k$, ki ou $-ki$ selon le graphique ci-dessus, i.e. $k=\left\lfloor\frac{n+1}{4}\right\rfloor$) et 3 booléens en $2^{ème}$, $3^{ème}$ et $4^{ème}$ coordonnées. Les booléens servent à se promener sur un carré de sommets $(1,1),(0,1),(0,0),(1,0)$ qui sont des points tels qu'effectuer un $\wedge$ logique entre leurs coordonnées permet d'obtenir un 1 une fois sur 4 (on voit dans la chaîne de bipoints fournie un peu plus haut qu'il fallait augmenter la valeur de la coordonnée non nulle tous les 4 points et que l'opérateur proposé n'effectuait pas cette augmentation périodique). La transformation corrigée devient :

$$\begin{pmatrix}x\\y\\z\\t\end{pmatrix}\mapsto\begin{pmatrix}ix+yz\\1-z\\y\\yz\end{pmatrix}$$

x est un $\pm k$ ou un $\pm ki$, y et z sont les booléens et yz calcule leur $\wedge$ logique)

Il faudrait maintenant essayer de démontrer les éléments rappelés en se basant sur cette représentation.