Caractérisation topologique des nombres premiers (Denise Vella-Chemla, 11.5.2019)

Après être revenue à l'article 53 des Recherches arithmétiques de Gauss et au résultat d'un programme de calcul d'indices [1] des nombres qui appartiennent au groupe des unités [2] d'un corps premier, il semblerait qu'on puisse caractériser, d'un point de vue arithmétique puis d'un point de vue topologique, les nombres premiers de la forme $4k+3$, même si cette caractérisation ne permet pas pour l'instant de les distinguer de leurs puissances.

Présentons 4 exemples pour fixer les idées : on travaille dans les corps premiers $\mathbb{Z}/p\mathbb{Z}$ et on indique pour les différentes puissances (avant les signes :) les nombres dont cette puissance est égale à l'unité. Par exemple, dans le tableau ci-dessous, fournissant les puissances associées aux unités dans $\mathbb{Z}/p\mathbb{Z}$ pour $p = 7, 13, 29$ ou 31, les 3 nombres colorés en rouge sont à lire comme $8^4 \equiv 1$ $(mod\ 13)$ (effectivement, $8^4 = 4096 = 315 \times 13 + 1$).

forme 4k + 3	p = 7	p = 31
	6 : 3 5	30 : 3 11 12 13 17 21 22 24
	3 : 2 4	15 : 7 9 10 14 18 19 20 28
	2 : 6	10 : 15 23 27 29
	1 : 1	6 : 6 26
		5 : 2 4 8 16
		3 : 5 25
		2 : 30
		1 : 1
forme 4k + 1	p = 13	p = 29
	12 : 2 6 7 11	28 : 2 3 8 10 11 14 15 18 19 21 26 27
	6 : 4 10	14 : 4 5 6 9 13 22
	4 : 5 8	7 : 7 16 20 23 24 25
	3 : 3 9	4 : 12 17
	2 : 12	2 : 28
	1 : 1	1 : 1

On va appeler "puissances appariées" (ou leur ensemble associé "ensembles appariés") les puissances dont les ensembles de nombres ont même cardinal. Par exemple, pour le module $p = 31$, on dira que la puissance 10 et la puissance 5 sont appariées car leur ensemble associé de nombres sont tous les deux de cardinalité 4.

On effectue les constatations suivantes [3].

Pour les nombres premiers $4k+3$, les ensembles associés aux différentes puissances sont appariés 2 à 2. Ce n'est pas le cas pour les nombres premiers $4k+1$ ou pour leurs puissances, pour lesquels par exemple la plus grande puissance a systématiquement un ensemble de nombres associé qui n'est "apparié à aucun autre ensemble".

Pour les nombres premiers p de la forme $4k+1$, il semblerait que les propriétés suivantes soient systématiquement vérifiées :

- il y a deux fois plus de nombres dont la puissance $p-1$ est égale à l'unité que de nombres dont la puissance $\frac{p-1}{2}$ est égale à l'unité ; il y a autant de nombres dont la puissance $\frac{p-1}{2}$ est égale à l'unité que de nombres dont la puissance $\frac{p-1}{4}$ est égale à l'unité ;

1. i.e. puissances égales à l'unité, cf. http://denise.vella.chemla.free.fr/polyetindices.pdf
2. Les résultats du programme de calcul avait été fournis ici en septembre 2016 : http://denise.vella.chemla.free.fr/indices-RA53.
3. Je ne sais pas si ces constatations découlent de théorèmes voire ont déjà été démontrées.

- pour les ensembles appariés dont les éléments x sont toujours tels que x et $p-x$ sont systématiquement dans des ensembles différents, on a les congruences suivantes (à échange de x et $p-x$ près) :

$$\begin{cases} x^k \equiv 1 \ (mod\ p) \\ (p-x)^{\frac{k}{2}} \equiv 1 \ (mod\ p) \end{cases}$$

- pour les ensembles non appariés avec x et $p-x$ systématiquement dans le même ensemble :

$$\begin{cases} x^k \equiv 1 \ (mod\ p) \\ (p-x)^k \equiv 1 \ (mod\ p). \end{cases}$$

Pour les nombres premiers p de la forme $4k+3$ ou leurs puissances, il semblerait que les propriétés suivantes soient systématiquement vérifiées :

- il y a autant de nombres dont la puissance $p-1$ est égale à l'unité que de nombres dont la puissance $\frac{p-1}{2}$ est égale à l'unité ;
- pour tous les ensembles qui sont tous appariés avec x et $p-x$ systématiquement dans des ensembles différents (à échange de x et $p-x$ près) :

$$\begin{cases} x^k \equiv 1 \ (mod\ p) \\ (p-x)^{\frac{k}{2}} \equiv 1 \ (mod\ p) \end{cases}$$

Ce qui semblerait au premier abord permettre de distinguer les nombres premiers de la forme $4k+1$ (ou leurs puissances) des nombres composés impairs (on ne peut, que ce soit pour les uns ou pour les autres, apparier leurs unités qu'on "quotiente par la puissance les amenant à 1", pour le dire rapidement), c'est le fait que pour les nombres premiers $4k+1$, il y ait exactement moitié moins de nombres associés à la puissance $\frac{p-1}{2}$ qu'à la puissance $p-1$, ce qui n'est pas le cas pour les nombres composés.

On visualise cela dans le tableau des cardinaux d'ensembles d'unités par des couleurs permettant d'observer cette propriété de "exactement moitié moins". Les premiers $4k+1$ sont colorés en bleus, les impairs composés en rouge. Malheureusement, ce qui semblait une caractérisation n'en est pas une : tous les $4k+1$ vérifient cette condition, sauf les $4k+1$ qui sont puissances d'un $4k+3$ (comme 9, 27, etc.). Il semblerait qu'on ait cependant obtenu une condition nécessaire : le fait que la deuxième classe ait un cardinal différent de la moitié du cardinal de la première classe semble impliquer que n est un nombre composé même si l'implication dans l'autre sens n'est pas vraie.

3 : 1/1	29 : 12, 6, 6, 2, 1, 1	55 : 16, 12, 4, 4, 3, 1	81 : 18/18, 6/6, 2/2, 1/1
5 : 2, 1, 1	31 : 8/8, 4/4, 2/2, 1/1	57 : 18, 6, 6, 3, 2, 1	83 : 40/40, 1/1
7 : 2/2, 1/1	33 : 12, 4, 3, 1	59 : 28/28, 1/1	85 : 32, 16, 12, 3, 1
9 : 2/2, 1/1	35 : 8, 6, 4, 3, 2, 1	61 : 16, 8, 8, 8, 4, 4, 4, 2, 2, 2, 1, 1	87 : 24, 18, 6, 4, 3, 1
11 : 4/4, 1/1	37 : 12, 6, 6, 4, 2, 2, 2, 1, 1	63 : 24, 8, 3, 1	89 : 40, 20, 10, 10, 4, 2, 1, 1
13 : 4, 2, 2, 2, 1, 1	39 : 8, 6, 4, 3, 2, 1	65 : 24, 12, 6, 3, 2, 1	91 : 32, 24, 8, 4, 3, 1
15 : 4, 3, 1	41 : 16, 8, 4, 4, 4, 2, 1, 1	67 : 20/20, 10/10, 2/2, 1/1	93 : 24, 12, 8, 6, 4, 3, 2, 1
17 : 8, 4, 2, 1, 1	43 : 12/12, 6/6, 2/2, 1/1	69 : 30, 10, 3, 1	95 : 24, 18, 8, 6, 6, 4, 3, 2, 1
19 : 6/6, 2/2, 1/1	45 : 8, 6, 4, 3, 2, 1	71 : 24/24, 6/6, 4/4, 1/1	97 : 32, 16, 16, 8, 8, 4, 4, 2, 2, 2, 1, 1
21 : 6, 3, 2, 1	47 : 22/22, 1/1	73 : 24, 12, 8, 6, 6, 4, 4, 2, 2, 2, 1, 1	99 : 24, 12, 8, 6, 4, 3, 2, 1
23 : 10/10, 1/1	49 : 12, 12, 6, 6, 2, 2, 1, 1	75 : 16, 12, 4, 4, 3, 1	
25 : 8, 4, 4, 2, 1, 1	51 : 16, 8, 4, 3, 1	77 : 24, 12, 8, 6, 4, 3, 2, 1	
27 : 6/6, 2/2, 1/1	53 : 24, 12, 12, 2, 1, 1	79 : 24/24, 12/12, 2/2, 1/1	

Pour les nombres premiers de la forme $4k+1$, la meilleure caractérisation les concernant semble être le fait qu'ils sont de manière unique somme de 2 carrés d'entiers [4].

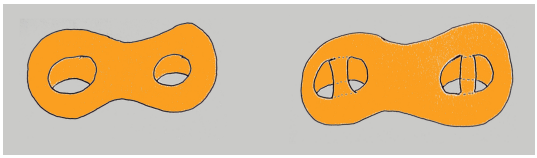
On fournit en annexe une représentation imagée obtenue par programme en python des nombres premiers $4k+1$ sommes de 2 carrés.

Dans tous les cas, la meilleure caractérisation des nombres premiers reste le petit théorème de Fermat : ce sont les seuls nombres pour lesquels tout nombre premier à p est solution pour la puissance $p-1$: $x^{p-1} \equiv 1 \ (mod\ p)$.

4. Ce théorème a été démontré par Fermat, Euler, Gauss et Zagier notamment, cf. la démonstration transcrite des Recherches arithmétiques de Gauss ici : http://denisevellachemla.eu/Gauss-4k+1-RA182.pdf.

Voyons maintenant deux manières de lier les résultats présentés ci-desus concernant les nombres premiers de la forme $4k+3$ à la topologie :

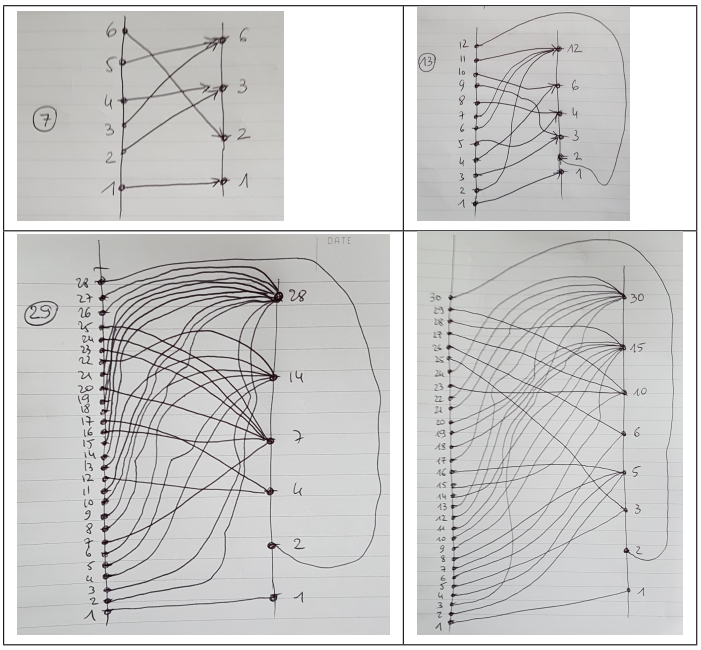
1) *première méthode envisagée* : on trouve dans la littérature qu'il est possible de compter le nombre de solutions d'une équation de la forme $x^p \equiv 1\ (mod\ k)$ sur un tore à p trous. Peut-être peut-on envisager de "dupliquer chaque trou" en comblant une sorte de tunnel de matière au milieu du trou ainsi :



2) *seconde méthode envisagée* : on a l'idée de représenter les nombres et les puissances correspondantes dans les corps premiers par les dessins ci-après (les nombres sur la ligne verticale à gauche sont les unités [5] du corps premier $\mathbb{Z}/p\mathbb{Z}$ considéré et les nombres sur la ligne verticale à droite sont les exposants qui permettent d'amener les nombres de la ligne gauche jusqu'à 1 par élévation à la puissance.

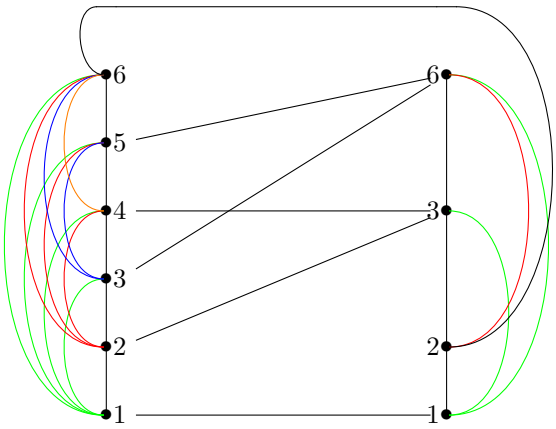
Le fait que 1 soit systématiquement d'indice 1 et $p-1$ d'indice 2 va nous permettre de transformer la représentation de la fonction "puissance qui permet d'atteindre l'unité" en une courbe fermée qui se croisera plusieurs fois elle-même ; les points de croisement seront vus comme des sommets, les éléments de courbe entre sommets seront les arêtes, on aura alors un graphe dans lequel il s'agira de trouver une chaîne eulérienne (dans un graphe connexe - i.e. tel que tout sommet est atteignable par un chemin depuis tout autre-, une chaîne eulérienne existe forcément si seuls deux sommets sont de degré impair ; cette chaîne passe par toutes les arêtes une fois et une seule et permet d'aller de l'un des deux sommets de degré impair à l'autre).

Voici les représentations imagées des fonctions "indices de Gauss".



5. C'est ainsi qu'on appelle les nombres premiers à p, ceux qui n'ont aucun diviseur commun avec p, i.e. les nombres tels que $PGCD(x,p) = 1$; le plus grand diviseur commun de x et y est habituellement simplement noté par le couple (x,y).

Présentons l'ajout d'arêtes sur la représentation associée à $p = 7$. On ajoute autant d'arêtes que nécessaire de façon à ce que tout nombre, qu'il soit sur la ligne verticale à gauche ou sur la ligne verticale à droite, puisse atteindre tout autre nombre sur la ligne en question. On symbolise ces arêtes supplémentaires en rouge, vert, bleu et orange pour améliorer la lisibilité.
Comptons les degrés des sommets (on appelle g_1 à g_6 les sommets à gauche (les indices de Gauss) de bas en haut et d_1 à d_4 les sommets de droite (les éléments du groupe des unités).
Les sommets g_1 à g_6 sont de degrés 6, les sommets d_1 et d_2 sont de degré 4 et les sommets d_3 et d_4 sont de degré 5. Le nombre d'arêtes est la moitié de la somme des degrés, ici 27.
Comme seuls deux sommets sont de degré impair (d_3 et d_4) dans le graphe, la propriété d'Euler est vérifiée, qui permet de parcourir toutes les arêtes une fois et une seule. Comme un tel circuit est difficile à faire apparaître sur le graphe "chargé" en arêtes, on le note par une succession possible de sommets : $d_4\ d_1\ d_3\ d_4\ d_2\ d_1\ g_1\ g_2\ d_3\ g_4\ g_5\ d_4\ g_3\ g_2\ g_4\ g_3\ g_5\ g_6\ g_4\ g_1\ g_3\ g_6\ g_2\ g_5\ g_1\ g_6\ d_2\ d_3$.



Malheureusement, ce qui marchait pour 7 ne marche pas pour 11, 13 : leur graphe contiennent chacun 4 sommets de degré impair, ce qui empêche d'y trouver une chaîne eulérienne. Ce n'est pas une bonne idée que de poursuivre dans cette voie-là.

Annexe 1 : Transcription des articles 53 et 54 des Recherches arithmétiques de Gauss

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

$$1 \left\{ 1, \quad 2 \right\{ 18, \quad 3 \left\{ \begin{matrix} 7 \\ 11 \end{matrix} \right. , \quad 6 \left\{ \begin{matrix} 8 \\ 12 \end{matrix} \right. , \quad 9 \left\{ \begin{matrix} 4,\ 5,\ 6 \\ 9,\ 16,\ 17 \end{matrix} \right. , \quad 18 \left\{ \begin{matrix} 2,\ 3,\ 10 \\ 13,\ 14,\ 15 \end{matrix} \right. .$$

Ainsi dans cas $\psi\ 1 = \ 1, \psi\ 2 = \ 1, \psi\ 3 = \ 2, \psi\ 6 = \ 2, \psi\ 9 = \ 6, \psi\ 18 = \ 6$. 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 $\psi d = \varphi d$. Mais on peut démontrer généralement cette observation de la manière suivante :

1°. S'il y a un nombre a appartenant à l'exposant d, c'est-à-dire dont la puissance d soit congrue à l'unité, et les puissances inférieures incongrues, toutes les puissances de ce nombre, savoir $a, a^2, a^3, a^4 \ldots a^d$, ou leurs résidus *minima*, auront leur puissance d congrue avec l'unité ; et comme cela peut s'exprimer en disant que les résidus *minima* des nombres $a, a^2, a^3, a^4 \ldots a^d$ qui sont tous différents sont les racines de la congruence $x^d \equiv 1$, qui ne peut avoir plus de d racines différentes, il est évident qu'il

n'y a pas de nombres autres que les résidus *minima* de $a, a^2, a^3, a^4 \ldots a^d$ dont les puissances d soient congrues à l'unité ; d'où il suit que les nombres appartenans à l'exposant d se trouvent tous entre les résidus *minima* des nombres $a, a^2, a^3, a^4 \ldots a^d$. On déterminera comme il suit quels ils sont et quel est leur nombre. Si k est un nombre premier avec d, toutes les puissances de a^k, dont les exposans sont $< d$, ne seront pas congrues à l'unité. Soit en effet $\frac{1}{k}$ $(mod.\ d) = m$ (voyez n°31), on aura $a^{km} \equiv a$; donc si la puissance e de a^k était congrue à l'unité, et que l'on eût $e < d$, on aurait aussi $a^{kme} \equiv 1$, et par conséquent $a^e \equiv 1$; ce qui est contre l'hypothèse. Il est évident, d'après cela, que le résidu *minimum* de a^k appartiendra à d ; mais si k a un commun diviseur δ avec d, le résidu *minimum* de a^k n'appartiendra pas à l'exposant d. Car $\frac{kd}{\delta}$ est divisible par d, ou bien $\frac{kd}{\delta} \equiv 0$ $(mod.\ d)$; parconséquent $a^{\frac{kd}{\delta}} \equiv 1$; c'est-à-dire $(a^k)^{\frac{d}{\delta}} \equiv 1$. Nous conclurons de là qu'il y a autant de nombres appartenans à l'exposant d, qu'il y a de nombres premiers avec d dans la série $1, 2, 3 \ldots d$. Mais il faut se souvenir que cette conclusion suppose qu'il existe déjà un nombre a appartenant à l'exposant d ; parconséquent il reste douteux s'il ne pourrait pas se faire qu'aucun nombre n'appartînt à un exposant donné, et la conclusion se réduit à $\psi d = 0$, ou $= \varphi d$.

54. 2°. Soient d, d', d'', etc. les diviseurs de $p-1$; comme tous les nombres $1, 2, 3 \ldots p-1$ doivent être distribués entre ces diviseurs, on aura $\psi d + \psi d' + \psi d'' + etc. = p-1$. Mais (n°40) nous avons démontré que $\varphi d + \varphi d' + \varphi d'' + etc. = p-1$, et du n° précédent il suit que $\psi d = 0$ ou $= \varphi d$; et parconséquent que ψd ne peut pas être $> \varphi d$; ce qui s'étend à $\psi d'$ et $\varphi d'$, etc. Si donc un ou plusieurs des nombres $\psi d, \psi d'$, etc. étaient plus petit que son correspondant parmi les nombres $\varphi d, \varphi d'$, etc., la somme des premiers ne pourrait être égale à la somme des derniers. D'où nous concluons enfin que dans tous les cas, $\psi d = \varphi d$, et que parconséquent ψd ne dépend point de la grandeur de $p-1$.

Annexe 2 : Premiers $4k+1$ sommes de deux carrés