Racines, chemins pour atteindre l'unité, cardinaux (Denise Vella-Chemla, 10.9.2016)

On voudrait ici fournir les derniers constats qu'on a effectués sur des résultats de programmes. On procède par une méthode assez expérimentale, rappelant celle préconisée par la Fondation La main à la pâte : on programme un résultat dont on a trouvé des exemples simples dans la littérature, on observe les résultats du programme, on émet de nouvelles hypothèses, qu'on cherche à retrouver dans la littérature, le but ultime et idéal étant d'aboutir à une démonstration des conjectures émises au fur et à mesure de l'expérimentation.

Le constat est que de même qu'un nombre premier p a un nombre maximum $\frac{p-1}{2}$ de résidus quadratiques[1], il y a également un nombre maximum (égal à $\varphi(p) = p-1$) de nombres qui sont inférieurs à p et qui ont une puissance égalant l'unité modulo p (cf l'article 54 des Recherches arithmétiques de Gauss).

Le point de départ des travaux en cours est l'article 53 des Recherches arithmétiques. On dispose de deux fichiers résultats de programmes :

- le fichier racunit500.pdf qui fournit pour un nombre n inférieur à 500 ses *"racines de l'unité"* r_i, i.e. les nombres dont une certaine puissance α_i est égale à 1 modulo le nombre n considéré ($r_i^{\alpha_i} \equiv 1\ (mod\ n)$) ;
- le fichier montreplusgrandepuiss2016.pdf qui fournit seulement les exposants qui permettent d'atteindre 1 (sans les racines).

Les constats sont les suivants :

- la puissance $p-1^{ème}$ permet d'atteindre l'unité pour les modules p premiers, c'est un fait connu et démontré ; dans le cas où p est un nombre premier, et seulement dans ce cas, il semblerait que, pour chaque puissance possible α_i, il y a $\varphi(\alpha_i)$ nombres qui élevés à cette puissance permettent d'aboutir à 1 ; Gauss explique cela dans son article 54 ($\varphi(x)$ désigne l'indicateur d'Euler de x, i.e. le nombre de nombres y inférieurs à x et qui lui sont premiers (tels que $(x,y) = pgcd(x,y) = 1)$) ; il y a donc pour les nombres premiers p un nombre maximum $(p-1)$ de nombres qui ont une puissance qui égale l'unité ;
- dans le cas où p est un nombre premier, les puissances successives qui permettent d'atteindre l'unité sont un ensemble de nombres constitué d'un plus grand nombre et de tous ses diviseurs (à l'époque de Gauss, elles étaient appelées les "parties aliquotes" de $p-1$) ; cette propriété n'est pas vérifiée par les nombres composés : par exemple, pour 203, la liste des puissances est $84, 42, 28, 21, 14, 12, 7, 6, 4, 3, 2, 1$;
- les puissances possibles permettant à des nombres d'atteindre l'unité modulo n (qu'il soit premier ou composé) sont toujours des diviseurs de $\varphi(n)$ (cela est dû au théorème d'Euler) ;
- aucun nombre non premier à n (i.e. partageant un facteur supérieur ou égal à 2 avec n) n'a une puissance égale à l'unité ; on imaginerait bien affecter comme puissance aux nombres en question ∞ de manière à ce que tout nombre de 1 à $n-1$ se voit pourvu d'un exposant à la puissance duquel il atteint l'unité (cet exposant fût-il infini) ;
- pour un nombre de la forme 2^k, 2^{k-2} est la plus grande puissance permettant d'atteindre l'unité, les autres puissances étant les puissances décroissantes de 2 ;
- pour un nombre de la forme p^k avec p premier, la plus grande puissance possible qui permet d'atteindre l'unité est $p^k - p^{k-1}$;
- un nombre et son double ont presque toujours le même ensemble de puissances permettant à des racines d'atteindre l'unité (cela n'est pas vérifié pour certains multiples de 16) ;
- pour les nombres impairs dont la factorisation est un produit de plusieurs facteurs premiers différents, c'est un peu plus complexe : il semblerait que les puissances possibles pour atteindre l'unité soient des diviseurs du produit $\prod(p_i - 1)$, les p_i étant les facteurs intervenant dans la factorisation de n. C'est aussi une conséquence du théorème d'Euler.

[1] On s'est intéressé à ce fait dans une note précédente carresimple.pdf.

Observons un phénomène qui nous intrigue, bien qu'il soit certainement connu des mathématiciens, et qui permet encore de distinguer les nombres premiers des nombres composés.

Considérons le nombre composé 203, d'indicateur d'Euler égal à $\varphi(203) = 168$. Les exposants à utiliser pour atteindre l'unité modulo 203 sont les suivants, dont on fournit pour chacun l'indicateur d'Euler corrrespondant entre parenthèses.

84 ($\varphi(84) = 24$) 42 (12) 28 (12) 21 (12) 14 (6) 12 (4) 7 (6) 6 (2) 4 (2) 3 (2) 2 (1) 1 (1)

La somme des indicateurs d'Euler entre parenthèses est égal à 84, inférieur à $\varphi(203)$.

Si on considère plutôt le nombre premier 101, d'indicateur d'Euler égal à $\varphi(101) = 100$. Les exposants à utiliser pour atteindre l'unité modulo 101 sont les suivants, dont on fournit pour chacun l'indicateur d'Euler corrrespondant.

100 ($\varphi(100) = 40$) 50 (20) 25 (20) 20 (8) 10 (4) 5 (4) 4 (2) 2 (1) 1 (1)

La somme des indicateurs d'Euler entre parenthèses est égal à 100, égal à $\varphi(101)$.

Si on observe maintenant les cardinaux des ensembles de racines qui à telle ou telle puissance atteignent l'unité, ils sont bien égaux aux indicateurs d'Euler successifs dans le cas des nombres premiers, mais ils en sont différents dans le cas des nombres composés. Dans le cas du nombre composé 203, les cardinaux des ensembles successifs de racines sont indiqués entre parenthèses ci-dessous et à comparer aux indicateurs d'Euler fournis plus haut.

84 ($\#(84) = 48$) 42 (36) 28 (24) 21 (12) 14 (14) 12 (8) 7 (6) 6 (6) 4 (4) 3 (2) 2 (3) 1 (1)

Concernant l'article 92, on trouve bien, comme l'indique Gauss, pour 1001 comme exposant maximum permettant à des nombres d'atteindre l'unité le nombre 60 qui est le plus petit commun multiple des nombres 6, 10 et 12, les nombres précédents les facteurs de $1001 = 7.11.13$, mais ce n'est pas le ppcm qui fournit la plus grande puissance possible pour le nombre $2009 = 41.7^2$ comme on peut le constater dans le fichier dim20160911am.pdf qui fournit aussi les ppcm des nombres précédents les facteurs du nombre considéré ainsi que la somme des indicateurs d'Euler des exposants possibles pour atteindre l'unité.

Notre objectif serait d'établir des fonctions entre ensembles de mêmes suites de puissances : par exemple, les exposants pour 60 sont 4, 2 et 1 et ce sont les mêmes puissances qui caractérisent le nombre 5. Par contre, les cardinaux des ensembles associés aux exposants sont différents (8,7,1 pour 60 et 2,1,1 pour 5). Il faudrait trouver un moyen d'envoyer les éléments dans les ensembles de 60 sur ceux dans les ensembles de 5.