Proposition de sujet de thèse : Sur les racines primitives généralisées

Cécile Dartyge

18 février 2018

1 Introduction

Pour tout p premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe cyclique. Un générateur de ce groupe est appelé racine primitive. Une des conjectures les plus célèbres de la théorie des nombres est celle d'Artin sur les racines primitives :

soit $a \in \mathbb{Z} \setminus \{-1, 1\}$ qui ne soit pas un carré ; il existe une infinité de nombres premiers p tels que a soit une racine primitive pour p.

Artin a aussi énoncé un forme "forte" de cette conjecture : il existe $A(a) > 0$ tel que la proportion des nombres premiers admettant a comme racine primitive soit $A(a)$. Cette quantité $A(a)$ a une expression explicite donnée par la formule d'Artin-Heilbronn. Par exemple si a est un entier sans facteur carré, $A(a) = A$ où A est la constante d'Artin :

$$A = \prod_p \Big(1 - \frac{1}{p(p-1)}\Big) = 0.3739558136...$$

Hooley [5] a démontré cette conjecture sous l'hypothèse de Riemann généralisée pour les fonctions ζ de Dedekind de certains corps de nombres.

Gupta et Murty [3] puis Heath-Brown [4] ont obtenu des résultats inconditionnels très surprenants. Une conséquence de celui de Heath-Brown est qu'il existe au plus deux nombres premiers pour lesquels la conjecture faible d'Artin soit fausse. En particulier cette conjecture est vraie pour au moins un entier $a \in \{2, 3, 5\}$. Cependant, à l'heure actuelle, on ne connaît pas de valeur explicite de a pour laquelle que cette conjecture soit vérifiée.

De nombreux travaux ont porté sur les racines primitives ou diverses généralisations des conjectures d'Artin. Ce sujet a fait l'objet de très passionnants articles de synthèse dont celui de Moree [8] de plus d'une centaine de pages.

Dans cette thèse on propose deux variantes autour de ce thème. L'une est relative à la notion de racine primitive généralisée introduite par Carmichael, l'autre porte sur une extension du problème d'Artin à des familles génératrices formées de plusieurs éléments.

Ces problèmes mêlent divers domaines de la théorie des nombres : théorie analytique des nombres notamment les méthodes de crible ; théorie algébrique

des nombres avec le théorème de Chebotaref et aussi la théorie probabiliste des nombres. Dans les deux paragraphes suivants nous présentons les deux axes de recherche de ce projet de thèse.

2 Racines primitives associées à des modules composés

Lorsque $n > 4$ n'est pas de la forme p^k, $2p^k$ avec $k \in \mathbb{N}$ et $p \geq 3$ premier, le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ n'est plus cyclique. Carmichael [2] généralise la notion de racine primitive dans $(\mathbb{Z}/n\mathbb{Z})^*$ de la manière suivante. Un entier a premier avec n est une racine primitive si le sous-groupe engendré par a dans $(\mathbb{Z}/n\mathbb{Z})^*$ a le cardinal le plus grand possible c'est-à-dire est égal à $\lambda(n)$, le nombre d'éléments d'un des plus grands sous-groupes cycliques de $(\mathbb{Z}/n\mathbb{Z})^*$. Cette fonction $\lambda(n)$ est traditionnellement appelée fonction de Carmichael.

Dans ce cadre, 2 est une racine primitive des nombres 3^j. Plus généralement si a est une racine primitive pour p^2 alors a est une racine primitive pour p^j pour tout j. Cependant l'analogue du problème d'Artin n'est pas résolu si on se restreint à des entiers sans facteur carré.

Pour $a \in \mathbb{Z} \setminus \{1, -1\}$, notons $N_a(x)$ le nombre d'entiers n inférieurs à x tels que a soit une racine primitive pour n. Par analogie avec la forme forte de la conjecture d'Artin, on est conduit à penser que si a est en dehors d'un ensemble d'entiers dits *exceptionnels*, il existe une fonction $B(a)$ telle que $N_a(x) \sim B(a)x$. Li et Pomerance ont montré que ce n'était pas le cas : la quantité $N_a(x)/x$ oscille avec x. Li [6] a ainsi montré que

$$\liminf_{x\to\infty} \frac{N_a(x)}{x} = 0$$

tandis que sous l'hypothèse de Riemann généralisée Li et Pomerance [7] montrent que pour tout a n'appartenant pas à l'ensemble des entiers exceptionnels évoqué précédemment,

$$\limsup_{x\to\infty} \frac{N_a(x)}{x} > 0.$$

Dans le même ordre d'idée, si $R(n)$ désigne le nombre de racines primitives pour n, et $\varphi(n)$ le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$ la distribution des valeurs prises par $R(n)/\varphi(n)$ quand n parcourt les entiers est différente de celles des $R(p)/\varphi(p)$ quand p parcourt la suite des nombres premiers.

On propose d'aborder ces questions en restreignant les entiers n à des ensembles $\mathcal{N}$ donnés. Un cas intéressant susceptible d'applications en cryptographie est de considérer les entiers RSA, c'est-à-dire les entiers produits de deux nombres premiers. Plus généralement on propose de considérer les entiers n avec k facteurs premiers pour k donné.

Ces nombres ont d'une part une structure multiplicative proche de celle des nombres premiers et sont parfois appelés nombres presque premiers mais

d'autres part le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ n'est plus cyclique. On est donc dans une situation intermédiaire entre entre celle de la conjecture d'Artin et de la généralisation proposée par Carmichael. Un autre aspect intéressant serait de déterminer s'il n'existe pas un seuil $k_0 = k_0(n)$ où se produirait une transition.

Le cas où l'ensemble $\mathcal{N}$ est un ensemble d'entiers friables, c'est-à-dire sans grand facteur premier semble également très intéressant. Il se peut que les oscillations des quantités correspondantes $N_a(x)/x$ soient de plus grande ampleur que celles relevées par Li et Pomerance dans le cas où $\mathcal{N}$ est l'ensemble des entiers naturels.

3 Variante multidimensionnelle

Soient $a_1, \ldots, a_\ell$ des entiers vérifiant des conditions de type général. Cangelmi et Pappalardi [1], [9] ont étudié la densité de l'ensemble des nombres premiers p tels que le sous-groupe engendré par les classes de $a_1, \ldots, a_\ell$ modulo p soit $(\mathbb{Z}/p\mathbb{Z})^*$.

Ils obtiennent sous la conjecture de Riemann généralisée une extension du résultat de Hooley (qui correspond au cas $k = 1$).

Dans ce deuxième volet on propose d'aborder ce problème pour $(\mathbb{Z}/n\mathbb{Z})^*$ en général. Une première étape consiste à déterminer des formules asymptotiques sous l'hypothèse de Riemann généralisée.

Est-il alors possible d'obtenir des avancées inconditionnelles lorsque ℓ est assez grand par rapport au nombre de facteurs premiers de n ? Là encore il serait particulièrement intéressant de considérer les entiers n de type RSA.

Références

[1] L. Cangelmi & F. Pappalardi – « On the r-rank of Artin conjecture, II », *Journ. of Number Theory* **75** (1999), p. 120–132.

[2] R. D. Carmichael – *The theory of numbers*, Wiley, New York, 1914.

[3] R. Gupta & M. R. Murty – « A remark on Artin's conjecture », *Invent. Math.* **78** (1984), p. 127–130.

[4] D. R. Heath-Brown – « Artin's conjecture for primitive roots, », *Quart. J. Math. Oxford Ser. (2)* **37** (1986), p. 27–38.

[5] C. Hooley – « On Artin's conjecture, », *J. reine angew. Math.* **225** (1967), p. 209–220.

[6] S. Li – « On extending Artin's conjecture for composite moduli », *Mathematika* **46** (1999), p. 373–390.

[7] S. Li & C. Pomerance – « On generalizing Artin's conjecture on primitive roots to composite moduli », *J. reine angew. Math* **556** (2003), p. 205–224.

[8] P. Moree – « Artin's primitive root conjecture-a survey », *Integers* **12** (2012), no. 6, p. 1305–1416.

[9] F. Pappalardi – « On the r-rank Artin conjecture », *Math. Comp.* **66** (1997), p. 853–868.