Bulletin
de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

SUR UNE GÉNÉRALISATION DE LA CONJECTURE D'ARTIN PARMI LES PRESQUE-PREMIERS

Paul Péringuey

Tome 152
Fascicule 3

2024

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

pages 377-442

Le *Bulletin de la Société Mathématique de France* est un périodique trimestriel de la Société Mathématique de France.

Fascicule 3, tome 152, septembre 2024

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
commandes@smf.emath.fr

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

Tarifs

Vente au numéro : 43 € ($ 64)
Abonnement électronique : 160 € ($ 240),
avec supplément papier : Europe 244 €, hors Europe 330 € ($ 421)
Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Bulletin de la SMF

Bulletin de la Société Mathématique de France
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 1 44 27 67 99 • Fax : (33) 1 40 46 90 96
bulletin@smf.emath.fr • smf.emath.fr

ISSN 0037-9484 (print) 2102-622X (electronic)

Directeur de la publication : Isabelle GALLAGHER

Bull. Soc. Math. France
152 (3), 2024, p. 377-442

SUR UNE GÉNÉRALISATION DE LA CONJECTURE D'ARTIN PARMI LES PRESQUE-PREMIERS

par Paul Péringuey

Résumé. — Un entier est une racine primitive modulo un premier p s'il génère le sous-groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. En 1927 Artin conjecture qu'un nombre a qui n'est ni -1 ni un carré parfait est racine primitive pour une infinité de nombres premiers, et que l'ensemble de ces premiers a une densité positive parmi tous les premiers. Cette conjecture a été démontrée, sous l'hypothèse de Riemann généralisée (GRH), en 1967 par Hooley.

Plus généralement, on dit qu'un entier est une racine primitive généralisée modulo n s'il génère un sous-groupe de taille maximale dans $(\mathbb{Z}/n\mathbb{Z})^*$. Li et Pomerance ont montré, sous GRH, que l'ensemble des entiers pour lesquels un entier est racine primitive généralisée n'admet pas de densité parmi tous les entiers.

On s'intéresse ici à l'ensemble des entiers ℓ-presque premiers, c'est-à-dire les entiers ayant au plus ℓ facteurs premiers, pour lesquels un entier $a \in \mathbb{Z} \setminus \{-1\}$ donné et différent d'un carré est racine primitive généralisée, et nous montrons, sous GRH, que cet ensemble admet une densité parmi tous les ℓ-presque premiers.

Texte reçu le 1er juin 2023, modifié le 16 février 2024, accepté le 22 février 2024.

Paul Péringuey, University of British Columbia, 1984 Mathematics Road, Vancouver BC V6T 1Z2, Canada • *E-mail :* peringuey@math.ubc.ca

Classification mathématique par sujets (2010). — 11A07, 11N25, 11R42, 11R44.

Mots clefs. — Théorie analytique des nombres, conjecture d'Artin, racines primitives, presque premiers, méthode de Selberg-Delange.

0037-9484/2024/377/$ 5.00
doi:10.24033/bsmf.2892

Abstract (*On a generalization of Artin's conjecture among almost primes*). — An integer is a primitive root modulo a prime p if it generates the whole multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. In 1927 Artin conjectured that an integer a which is not -1 or a square is a primitive root for infinitely many primes, and that the set of those primes has a positive asymptotic density among all primes. This conjecture was proved, under the generalized Riemann hypothesis (GRH), in 1967 by Hooley.

More generally, an integer is called a generalized primitive root modulo n if it generates a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$ of maximal size. Li and Pomerance showed, under GRH, that the set of integers for which a given integer is a generalized primitive root doesn't have an asymptotic density among all integers.

We study here the set of the ℓ-almost primes, i.e. integers with at most ℓ prime factors, for which a given integer $a \in \mathbb{Z} \setminus \{-1\}$, which is not a square, is a generalized primitive root, and we prove, under GRH, that this set has an asymptotic density among all the ℓ-almost primes.

1. Introduction

Soient a un entier et p un nombre premier, on dit que a est une racine primitive modulo p si a engendre le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Une question qui émerge alors est de quantifier le nombre de nombres premiers pour lesquels un entier a est racine primitive. Notons $N_a(x)$ le nombre de premiers plus petits que x pour lesquels a est racine primitive, on cherche alors à apprécier $N_a(x)$ lorsque x tend vers l'infini.

En 1927 Emil Artin conjecture que tout entier a différent de -1 et d'un carré est racine primitive modulo une infinité d'autres entiers. Il stipule qu'un tel entier a serait générateur pour environ 37% des premiers, c'est-à-dire $N_a(x) \sim C_A\pi(x)$, où $C_A = \prod_p \left(1 - \frac{1}{p(p-1)}\right)$ est la constante d'Artin. Une démonstration conditionnelle est fournie par Hooley [6] en 1967, en supposant l'hypothèse de Riemann pour certains corps de nombres. Plus précisément il démontre que $N_a(x) \sim C_A(a)\pi(x)$, la constante dépend donc du nombre a considéré et est la constante conjecturée par Heilbronn (d'après [6]). Concernant des résultats inconditionnels Heath-Brown [4], améliorant un résultat de Gupta et Ram Murty [2], a démontré qu'au plus deux nombres premiers ne sont pas racines primitives pour une infinité de nombres premiers. Plus précisément si (q, r, s) est un triplet d'entiers multiplicativement indépendants tel que aucun élément de $\{q, r, s, -3qr, -3rs, -3qs, qrs\}$ ne soit un carré, alors l'ensemble des premiers pour lesquels au moins un entier parmi q, r et s est racine primitive est asymptotiquement $\gg \frac{x}{(\log x)^2}$. Pour un état de l'art concernant la conjecture d'Artin et les racines primitives généralisées, le lecteur pourra se référer aux articles de synthèse de Moree [13] et de Li et Pomerance [11].

On étend la notion de racine primitive au sous-groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, où n est un entier quelconque, en définissant les racines primitives généralisées modulo n comme étant les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$ générant des sous-groupes de

taille maximale, c'est-à-dire $\{m \in (\mathbb{Z}/n\mathbb{Z})^*,\ |\langle m\rangle| = \lambda(n)\}$, où λ est la fonction lambda de Carmichael [1], définie telle que $\lambda(n)$ est la taille maximale atteinte par les sous-groupes cycliques de $(\mathbb{Z}/n\mathbb{Z})^*$. Il est alors naturel de se demander si des résultats similaires à la conjecture d'Artin existent dans le cadre des racines primitives généralisées. Notons $N'_a(x)$ le nombre d'entiers plus petits que x pour lesquels a est racine primitive généralisée, on espère alors que $N'_a(x) \sim C(a)x$. Malheureusement ce n'est pas le cas. Soit $\mathtt{E}$ l'ensemble des entiers qui sont soit une puissance d'exposant strictement plus grand que 1, soit un carré multiplié par -1 ou ± 2. Li [9] a démontré que pour tout a, $\liminf \frac{N'_a(x)}{x} = 0$ et Li et Pomerance [11] ont démontré que pour les entiers a n'appartenant pas à $\mathtt{E}$ on a, sous l'hypothèse de Riemann généralisée, $\limsup \frac{N'_a(x)}{x} > 0$. Ainsi le nombre d'entiers pour lesquels un certain entier a est racine primitive généralisée n'admet pas de densité parmi tous les entiers. Comme pour le cas classique de la conjecture d'Artin d'autres problèmes surgissent naturellement comme par exemple l'estimation de l'ordre de grandeur de la plus petite racine primitive généralisée pour un entier, dont Martin [12] fournit une majoration pour presque tout entier.

Soit ℓ un entier plus grand que 1. Dans cet article, on étudie une situation intermédiaire, celle de l'ensemble des nombres ℓ-presque premiers pour lesquels un entier a est racine primitive généralisée, et nous montrons qu'il admet une densité parmi tous les ℓ-presque premiers.

Pour le reste de l'article p et q représenteront toujours des nombres premiers, et nous noterons $\mathrm{ord}_n(b)$ l'ordre de b dans $(\mathbb{Z}/n\mathbb{Z})^*$, (b,c) le pgcd de b et c, $[b,c]$ le ppcm de b et c, $\nu_q(b)$ la valuation q-adique de b. On note $\mathscr{P}^*(A)$ l'ensemble des parties non-vides d'un ensemble A. On fixe $a \in \mathbb{Z}\setminus\{-1\}$ un entier différent d'un carré, et on écrit a sous la forme $a = a_1 a_2^2$ où a_1 est sans facteur carré et éventuellement négatif. De plus, on définit h comme le plus grand entier tel que a soit une h-ième puissance :

$$h := \max\{\nu,\ \exists b,\ a = b^\nu\}. \tag{1}$$

Un nombre ℓ-presque premier est un nombre ayant au plus ℓ diviseurs premiers comptés avec multiplicité. Landau [7] a montré que le nombre de ℓ-presque premiers plus petit que x est asymptotiquement $\frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x}$. On s'intéresse ici au comportement asymptotique du nombre de ℓ-presque premiers pour lesquels a est une racine primitive généralisée. Nous obtenons sous l'hypothèse de Riemann généralisée (GRH) le théorème suivant :

THÉORÈME 1.1 (GRH). — *Soient $\ell \geq 1$, $E = \{1,\dots,\ell\}$, a un entier qui n'est ni -1, ni un carré parfait et $\mathcal{N}_{a,\ell}(x)$ le nombre de ℓ-presque premiers plus petits que x et qui ont a comme racine primitive généralisée. On a :*

$$\mathcal{N}_{a,\ell}(x) = \frac{x(\log\log x)^{\ell-1}}{(\ell-1)!\log x}\prod_p (1 - W_\ell(p))\,(1 + V_\ell(a_1))\,(1+o(1))\,,$$

avec les notations suivantes :

1. $W_\ell(p) := \sum_{i=1}^{\ell} \binom{\ell}{i} \sum_{j=0}^{\ell-i} \binom{\ell-i}{j} \frac{(-1)^j p^{i+j} (h,p)^i}{p^{2i}(p-1)^j (p^{i+j}-1)}$, *est la contribution ne dépendant que de* h,
2. $V_\ell(a_1) := \mu(2\tilde{a}_1) \frac{H_2(\ell,a_1)}{1-W_\ell(2)} \prod_{\substack{p \\ p|a_1 \\ p\geq 3}} (1-W_\ell(p))^{-1}$, *est la contribution spécifique dépendant de* a, *où* $\tilde{a}_1 := \frac{a_1}{(2,a_1)}$,
3. $$H_2(\ell,a_1) := \sum_{k=1}^{\ell} \binom{\ell}{k} 2^{-\ell-k} \delta_\ell(k) \mu(\tilde{a}_1)^k \times \prod_{\substack{p|\tilde{a}_1 \\ p\geq 3}} \left(\frac{(p-2)^{\ell-k}}{(p-1)^\ell} \right) \sum_{\prod_{\{i,j\}\in\mathcal{D}} a_{i,j} = \tilde{a}_1} \prod_{\{i,j\}\in\mathcal{D}} G_{i,j}^k(a_{i,j})$$

   où

   $$\delta_\ell(k) = \sigma(a_1,k) + 2^{\ell-2k} \sum_{m=0}^{\ell-k} \binom{\ell-k}{m} 2^{-3m} \sum_{r=0}^{\ell-k-m} \binom{\ell-k-m}{r} \frac{(-1)^r 2^{-r}}{2^{k+m+r}-1},$$

   avec

   $$\sigma(a_1,k) := \begin{cases} 2^{-\ell+k} + 2^{-2\ell+k} 5^{\ell-k} & \text{si } a_1 \equiv 1 \pmod 4 \\ (-1)^k 2^{-\ell+k} + 2^{-2\ell+k} 5^{\ell-k} & \text{si } a_1 \equiv 3 \pmod 4 \\ (-1)^k 2^{-2\ell+k} 5^{\ell-k} & \text{sinon} \end{cases},$$

   $\mathcal{D} = [0,k] \times [0,\ell-k] \setminus \{0,0\}$, *et pour* $(i,j) \in \mathcal{D}$, $G_{i,j}^k$ *est la fonction multiplicative définie pour les nombres premiers impairs par :*

   $$G_{i,j}^k(p) = \binom{k}{i} \binom{\ell-k}{j} \left(\frac{(p-1)(h,p)}{p^2(p-2)} \right)^{i+j} (2-p)^i \left(1 + R_p(k+j)\right),$$

   avec $R_p(m) := \sum_{r=0}^{\ell-m} \binom{\ell-m}{r} \frac{(-1)^r (p-1)^{\ell-m-r}}{(p^{m+r}-1)(p-2)^{\ell-m}}$.

La complexité des termes impliqués dans le résultat ci-dessus provient, en grande partie, du fait qu'un entier peut être racine primitive généralisée modulo $p_1 \cdots p_\ell$ sans pour autant être racine primitive modulo un des p_i (par exemple 1636 est une racine primitive généralisée modulo $4054051 = 1801 \times 2251$ mais n'est pas une racine primitive modulo 1801 ou 2251). Nous montrons dans la section suivante que pour être racine primitive généralisée modulo $p_1 \cdots p_\ell$ un entier doit vérifier des critères plus faibles que celui d'être racine primitive mais cela simultanément modulo chacun des p_i, et donc le résultat ne découle pas immédiatement du résultat de Hooley [6], dont on retrouve ci-dessus le terme principal en prenant $\ell = 1$. En effet ce dernier ramène le problème à compter

les idéaux premiers d'un certain corps de nombres, ce qu'il peut alors faire en étudiant, sous GRH, la fonction zeta de Dedekind associée à ce corps. Dans notre cas, nous ramenons le problème à compter simultanément les idéaux premiers de plusieurs corps de nombres, ce qui n'est pas possible en appliquant classiquement la formule de Perron et en déformant le contour. Pour surmonter cette difficulté, nous démontrons le résultat inconditionnel suivant, qui découle d'une application atypique de la méthode de Selberg-Delange :

THÉORÈME 1.2. — *Soient ℓ un entier non nul, a un entier non nul qui n'est ni -1 ni un carré, C une constante. Soient $v_1, \dots, v_\ell$ des entiers plus petits que C et $\kappa_1, \dots, \kappa_\ell$ des entiers sans facteur carré tels que pour tout $1 \leq i \leq \ell$, $\kappa_i | v_i$, alors :*

$$\sum_{\substack{p_1 \cdots p_\ell \leq x \\ (a, p_1 \cdots p_\ell)=1 \\ \forall i,\ p_i \equiv 1 (v_i) \\ a \in \mathfrak{R}(\kappa_i, p_i)}} 1 = \frac{\ell x}{\log x \prod_i n_i} (\log\log x)^{\ell-1} + \mathcal{O}_C\left(\frac{x}{\log x}(\log\log x)^{\ell-2}\right),$$

où $n_i := [\mathbb{Q}(\sqrt[\kappa_i]{a}, \xi_{v_i}) : \mathbb{Q}]$, ξ_{v_i} est une racine primitive v_i-ième de l'unité et $\mathfrak{R}(\kappa_i, p_i)$ est l'ensemble des entiers dont la classe $\pmod{p_i}$ est une puissance κ_i-ième.

De plus, inconditionnellement, on a la majoration suivante :

THÉORÈME 1.3. — *Avec les mêmes hypothèses que pour le Théorème 1.1, on a :*

$$\mathcal{N}_{a,\ell}(x) \leq \frac{x(\log\log x)^{\ell-1}}{(\ell-1)! \log x} \prod_p (1 - W_\ell(p))\,(1 + V_\ell(a_1))\,(1 + o(1)).$$

Posons $C_\ell(a) = \lim_{x\to\infty} \mathcal{N}_{a,\ell}(x) / \frac{x(\log\log x)^{\ell-1}}{(\ell-1)! \log x}$. Nous avons calculé numériquement plusieurs valeurs particulières, reprises dans le tableau suivant :

ℓ	$\prod_p (1 - W_\ell(p))$, $h = 1$	$C_\ell(2)$	$C_\ell(3)$	$C_\ell(5)$	$C_\ell(10)$
1	$\simeq 0.3739$	$\simeq 0.3739$	$\simeq 0.3739$	$\simeq 0.3936$	$\simeq 0.3739$
2	$\simeq 0.3759$	$\simeq 0.3222$	$\simeq 0.3950$	$\simeq 0.3878$	$\simeq 0.3775$
5	$\simeq 0.3261$	$\simeq 0.1318$	$\simeq 0.3252$	$\simeq 0.3278$	$\simeq 0.3272$
10	$\simeq 0.3051$	$\simeq 0.0293$	$\simeq 0.3053$	$\simeq 0.3046$	$\simeq 0.3047$
20	$\simeq 0.2919$	$\simeq 0.0015$	$\simeq 0.2918$	$\simeq 0.2920$	$\simeq 0.2920$
50	$\simeq 0.2807$	$\simeq 2 \times 10^{-7}$	$\simeq 0.2807$	$\simeq 0.2807$	$\simeq 0.2807$

On retrouve sur la première ligne la constante d'Artin, ainsi que la légère déviation pour $a = 5$. Dans les lignes suivantes, toutes les valeurs présentent une

déviation, qui semble s'estomper quand ℓ grandit, sauf pour $a = 2$ auquel cas $C_\ell(2)$ semble tendre vers 0, ce qui est en accord avec le fait que 2 est dans l'ensemble E décrit par Li et Pomerance [11].

Nous présentons ensuite une approche heuristique analogue à celle du cas classique. Nous transformons le problème en l'évaluation du nombre de ℓ-presque premiers ne vérifiant pas une certaine propriété pour tout nombre premier q. En utilisant l'Hypothèse de Riemann Généralisée nous ramenons le problème à l'évaluation du nombre de ℓ-presque premiers ne vérifiant pas ces propriétés pour q petit. Puis nous montrons que les $p_1 \cdots p_\ell$ comptés sont tels que chaque p_i se décompose comme produit d'idéaux premiers distincts dans un certain corps de nombres. En utilisant la méthode de Selberg-Delange nous évaluons le nombre de $p_1 \cdots p_\ell \leq x$ vérifiant ces propriétés simultanément. Enfin, après avoir contrôlé les termes d'erreurs, nous utilisons des méthodes combinatoires pour obtenir l'expression du terme principal.

2. Caractérisation des racines primitives généralisées

Nous donnons dans ce paragraphe un critère caractérisant les racines primitives généralisées. Ce critère est énoncé dans le lemme 2.2.

Nous commençons par introduire des notations qui nous serviront tout au long de l'article. Pour $l \in \mathbb{N}$ et $n \in \mathbb{N}$ donnés, on notera $\mathfrak{R}(l, n)$ l'ensemble des entiers dont la classe $\pmod n$ est une puissance l-ième :

$$\mathfrak{R}(l,n) = \{c \in \mathbb{Z}, \exists b \in \mathbb{Z}, c \equiv b^l \pmod n\}. \tag{2}$$

Pour $q, p_1, \ldots, p_\ell$ des nombres premiers, on notera $M_q(p_1, \ldots, p_\ell)$ l'ensemble des $p \in \{p_1, \ldots, p_\ell\}$ pour lesquels la valuation q-adique de $p-1$ est maximale parmi les p_i :

$$M_q(p_1,\ldots,p_\ell) = \{p \in \{p_1,\ldots,p_\ell\}, \nu_q(p-1) = \nu_q(\lambda(p_1 \cdots p_\ell))\}. \tag{3}$$

Cet ensemble est toujours non vide. En effet la fonction lambda de Carmichael vérifie les propriétés suivantes :

1. $\lambda(p^r) = \begin{cases} \frac{1}{2}\varphi(p^r) & \text{si } p = 2 \text{ et } r \geq 3 \\ \varphi(p^r) & \text{sinon} \end{cases}$.
2. Si $n = \prod_{i=1}^{k} p_i^{v_i}$ avec $p_i \neq p_j$, alors $\lambda(n) = [\lambda(p_1^{v_1}), \ldots, \lambda(p_k^{v_k})]$.

On commence par donner un résultat classique sur les ordres des éléments dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Lemme 2.1. — *Pour tous a, n_1, n_2 dans $\mathbb{N}$, $(a, n_1 n_2) = 1$:*

$$\operatorname{ord}_{[n_1,n_2]}(a) = [\operatorname{ord}_{n_1}(a), \operatorname{ord}_{n_2}(a)]$$