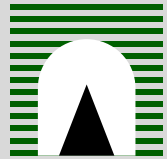
Propriétés des réductions de groupes de nombres rationnels

Introduction à la Conjecture d'Artin

Séminaire de Théorie des Nombres
Université de Lomé
21 Juillet 2014

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre



Histoire de la Conjecture d'Artin

La question de Gauss sur les longueurs de périodes

Quels sont les nombres premiers p tels que $1/p$ a une longueur $p-1$?

Par exemple:

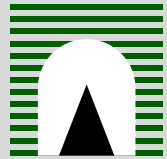
$$\frac{1}{7} = 0.\overline{142857},$$
$$\frac{1}{17} = 0,\overline{0588235294117647},$$
$$\frac{1}{19} = 0.\overline{0526315789473684 21},$$
$$\vdots$$
$$\frac{1}{47} = 0.\overline{0212765957446808510638297872340425531914893617}$$

Quelques nombres premiers avec cette propriété:

$7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, \ldots$

Soit $k_p :=$ la longueur de la période de $1/p$

$k_3 = 1,\ k_{11} = 2,\ k_{13} = 6,$ k_2 et k_5 sont pas définis



La question de Gauss sur les longueurs de périodes

La longueur de période de la fraction $1/p$ est le plus petit k tel que

$$\frac{1}{p} = 0.\overline{a_1 \cdots a_k} = 0.a_1 \cdots a_k \; a_1 \cdots a_k \; \ldots$$

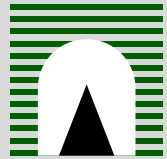
En d'autres termes

$$\begin{aligned} \frac{1}{p} &= \left(\frac{a_1}{10} + \cdots + \frac{a_k}{10^{k+1}}\right) \times \left(1 + \frac{1}{10^k} + \frac{1}{10^{2k}} + \cdots\right) \\ &= \frac{M}{10^k - 1} \end{aligned}$$

D'où

$$M \times p = 10^k - 1$$

Donc k_p est le plus petit entier k tel que $10^k - 1$ est divisible par p!

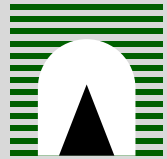


Propriétés algébrique des longueurs de périodes

- La longueur de la période k_p de $1/p$ est le plus petit entier k tel que $10^k - 1$ est divisible par p
- Le petit Théorème de Fermat affirme que $10^{p-1} - 1$ est divisible par p
- Donc $k_p \leq p - 1$
- En effet, il n'est pas difficile de montrer que k_p est un diviseur de $p - 1$
- Parfois, la longueur de la période est petite:

$$1/1111111111111111 = 0,\overline{0000000000000009}$$

- la plupart du temps $k_p > \sqrt{p}$ (pas évident!)
- Gauss a, en particulier, demandé quelles sont les fréquences des périodes



Quelques statistiques sur la longueur de la période:

Soit k_p la longueur de la période de $1/p$. Le tableau suivant contient

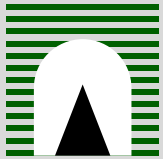
$$\delta_m = \frac{\{p < 2^{31} : k_p = \frac{p-1}{m}\}}{\#\{p \leq 2^{31}\}}$$

pour $m = 1, \ldots, 40$.

m	1	2	3	4	5	6	7
δ_m	0.37393	0.28047	0.06649	0.07133	0.01890	0.04986	0.00893
m	8	9	10	11	12	13	14
δ_m	0.01660	0.00739	0.01416	0.00340	0.01268	0.00240	0.00669
m	15	16	17	18	18	20	21
δ_m	0.00335	0.00415	0.00136	0.00553	0.00109	0.00235	0.00158
m	22	23	24	25	26	27	28
δ_m	0.00255	0.00073	0.00294	0.00075	0.00180	0.00081	0.00171
m	29	30	31	32	33	34	35
δ_m	0.00046	0.00251	0.00039	0.00103	0.00060	0.00103	0.00044

Remarque

$2,94\%$ des nombres premiers $p \leq 2^{31}$ ont une longueur de période $k_p = \frac{p-1}{m}$ avec $m > 35$



Propriétés algébriques des longueurs de périodes

- Les périodes sont également définies par rapport à n'importe quelle base $a \in \mathbb{N}$
- La longueur de la période de $1/p$ en base a est le plus petit $k_p(a)$ tel que $a^k - 1$ est divisible par p (c'est donc un diviseur de $p-1$)
- Il n'est pas difficile de voir que:
  la longueur de la période $k_p(a)$ *vérifie* $k_p(a) = p-1$ *si et seulement si l'ensemble*

$$\{a^j : \ j = 1, \ldots, p-1\}$$

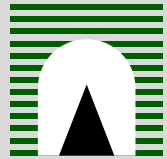
  contient $p-1$ ***éléments distincts modulo*** p
- *en d'autres termes, la longueur de la période vérifie* $k_p(a) = p-1$ *si et seulement si*

p est pas un diviseur de $a^s - a^r \quad \forall r, s : \ 1 \leq r < s \leq p-1$

- nous exprimons cette condition par

$$\langle a \bmod p \rangle = \mathbb{F}_p^* \quad \text{ou encore} \quad \#\langle a \bmod p \rangle = p-1$$

- Si la longueur de la période en base a de $1/p$ est $p-1$ (c'est-à-dire $k_p(a) = p-1$), nous disons que a *est une racine primitive modulo* p



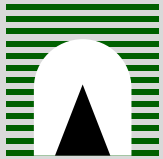
Propriétés algébriques des longueurs de périodes

(De la longueur des périodes aux racines primitives)

- Donc a *est une racine primitive modulo* p si et seulement si $\langle a \bmod p \rangle = \mathbb{F}_p^*$
  (c'est-à-dire s'il y a $p-1$ puissances distinctes de a modulo p)
- Il n'est pas difficile de vérifier que, si p est un diviseur de a, alors l'écriture de $1/p$ en base a est finie.
- par exemple $1/2 = 0.5, \quad 1/5 = 0.2$ en base décimale, $1/10 = 0.1$ en base binaire
- on peut étendre la définition de a *est une racine primitive modulo* p au cas où a est un nombre rationnel et où p ne divise pas le numérateur, ni le dénominateur de a (c'est-à-dire $v_p(a) = 0$)
- a *est une racine primitive modulo* p si et seulement si

  Pour tout nombre premier ℓ qui divise $p-1$, p ne divise pas $a^{(p-1)/\ell} - 1$
- C'était l'intuition d'Artin sur la

Conjecture des Racines Primitives



La Conjecture d'Artin (1927)

Remarque

Heuristiquement, etond donné un nombre premier ℓ, la probabilité qu'un nombre premier p vérifie les deux propriétés

1. ℓ divise $p-1$,
2. p divise $a^{(p-1)/\ell}-1$,

est $1/\ell(\ell-1)$.
Par conséquent, la probabilité pur p que, pour tout premier ℓ qui divise $p-1$, $a^{(p-1)/\ell}-1$ ne soit pas divisible par p, est

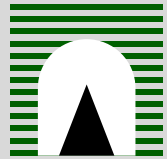
$$A=\prod_{\ell\geq 2}\left(1-\frac{1}{\ell(\ell-1)}\right)=0,373955\ldots$$

Définition (A est appelé la *Constante d'Artin*)

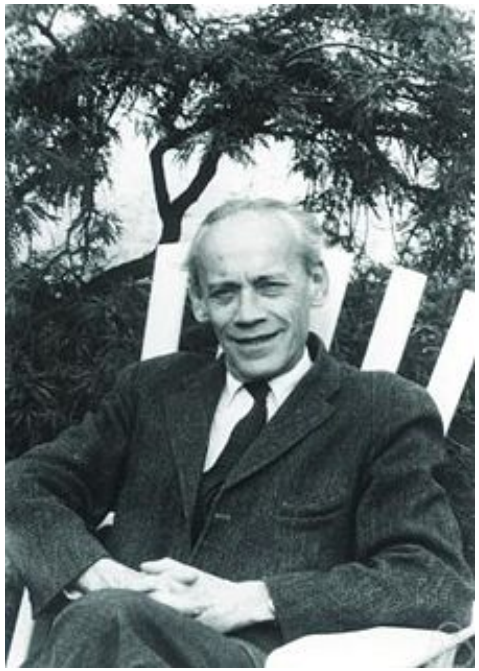
Conjecture

$$\lim_{x\to\infty}\frac{\#\{p\leq x:\ p\neq 2,5,\ \langle 10 \bmod p\rangle=\mathbb{F}_p^*\}}{\#\{p\leq x\}}=A$$

Qu'est-ce si au lieu de 10, nous considérons un $a\in\mathbb{Z}\setminus\{-1,0,1\}$?



La conjecture d'Artin (1927)



Emil Artin (Mars 3, 1898 - Décembre 20, 1962)

Conjecture (La conjecture d'Artin – (première version))

Si $a \in \mathbb{Q} \setminus \big(\{-1, 0, 1\} \cup \{b^2 : b \in \mathbb{Q}\}\big)$, alors

$$\#\{p \leq x : \ v_p(a) = 0, \ \langle a \bmod p \rangle = \mathbb{F}_p^*\} \sim A\pi(x)$$

ici $\pi(x) = \#\{p \leq x\}$ et $A = \prod_{\ell \geq 2} 1 - \dfrac{1}{\ell(\ell-1)} = 0,37395\ldots$

Certains tests numériques pour la conjecture d'Artin

Soit

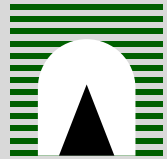
$$S_a = \{p \leq 2^{29} : \langle a \bmod p \rangle = \mathbb{F}_p^*\}, \quad d_a = \#S_a/\pi(2^{29})$$

Noter que $\pi(2^{29}) = 28192750$ et $A = 0,373955\ldots$.

a	S_a	d_a	a	S_a	d_a
-15	10432805	0.37005	2	10543421	0.37397
-14	10543340	0.37397	3	10543631	0.37398
-13	10542796	0.37395	5	11098098	0.39365
-12	12653339	0.44881	6	10543607	0.37398
-11	10639090	0.37736	7	10544579	0.37401
-10	10543135	0.37396	8	6325893	0.22438
-9	10542743	0.37395	10	10542876	0.37395
-8	6325704	0.22437	11	10542933	0.37395
-7	10799148	0.38304	12	10545029	0.37403
-6	10543575	0.37398	13	10611720	0.37639
-5	10542080	0.37392	14	10542946	0.37395
-4	10543032	0.37396	15	10544134	0.37400
-3	12651353	0.44874	17	10582932	0.37537
-2	10542194	0.37393	18	10545385	0.37404

Ces résulats numériques ne sont pas toujours totalement convaincants!

Notamment pour $a \in \{-15, -12, -11, -8, -7, -3, 5, 8, 13, 17\}$



La conjecture d'Artin

La correction de Lehmer

Derrick Henry Lehmer (Février 1905 - Mai 1991)

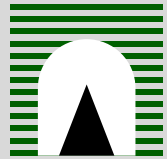
Remarque (Lehmer)

Étant donnés deux nombres premiers ℓ_1 et ℓ_2, les probabilités pour un nombre premier p de vérifier

1. ℓ_i divise $p-1$
2. p divise $a^{(p-1)/\ell_i}-1$

pour $i=1,2$ ne correspondent pas toujours à des événements indépendants!!

Donc, il faut un facteur de correction
(le *facteur d'enchevêtrement*)



La conjecture d'Artin

après la correction de Lehmer

Conjecture (La conjecture d'Artin – forme finale)

Soit $a \in \mathbb{Q}^* \setminus \{1, -1\}$, alors $p - 1 = \#\langle a \mod p \rangle$ pour une proportion de nombres premiers δ_a où

$$\delta_a = r_a \times t_a,$$

où si $h = \max\{j : a = b^j, b \in \mathbb{Q}\}$, $\partial(a) = \mathrm{disc}(\mathbb{Q}(\sqrt{a}))$,

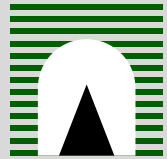
$$t_a = \prod_{\ell \geq 2} \left(1 - \frac{\gcd(h, \ell)}{\ell(\ell - 1)}\right)$$

et $r_a = 1$ si $\partial(a)$ est pair , tandis que si $\partial(a)$ est impair on a:

$$r_a = 1 - \prod_{\ell | \partial(a)} \frac{-1}{\ell(\ell-1)/\gcd(\ell,h)-1}$$

Noter que

- t_a est un multiple rationnel de la constante d'Artin A
- $\delta_a = 0$ si et seulement si a est un carré parfait
- $\partial(a)$ est facile mais technique à définir



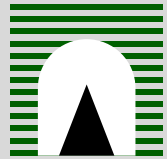
La conjecture d'Artin

Effet de l'enchevêtrement Lehmer

Nous n'avons pas été convaincus par les valeurs correspondant à $a \in \{-15, -12, -11, -8, -7, -3, 5, 8, 13, 17\}$

a	δ_a	d_a
-15	0.37001	0.37005
-12	0.44875	0.44881
-11	0.37709	0.37736
-8	0.22437	0.22437
-7	0.38308	0.38304
-3	0.44875	0.44874
5	0.39363	0.39365
8	0.22437	0.22438
13	0.37636	0.37639
17	0.37533	0.37537

Pour toutes les autres valeurs de a dans le tableau précédent, $\delta_a = A$



La conjecture d'Artin

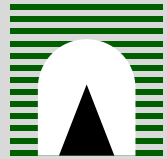
ce qui est connu sur la conjecture d'Artin

Théorème (C. Hooley (1965))

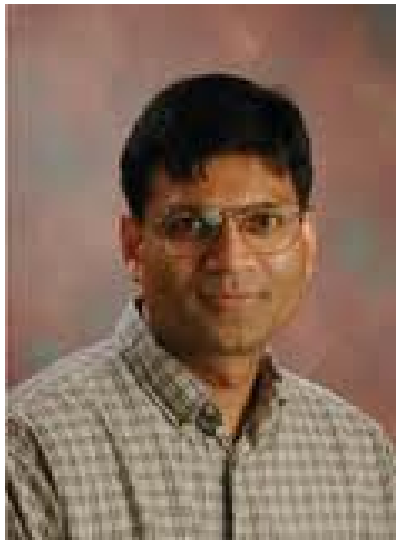
Si l'Hypothèse de Riemann Généralisée (GRH) est valable pour les corps $\mathbb{Q}(a^{1/\ell})$ (ℓ nombre premier) alors la conjecture d'Artin (forme finale) est valable pour cette valeur de a

Qu'est-ce que GRH?

- C'est une conjecture compliquée en théorie des nombres, si puissante que souvent on suppose qu'elle est vraie
- Elle est au delà du niveau de ce séminaire
- Il y a beaucoup de formulations différentes:
- *tous les zéros non triviaux de la fonction zêta de Dedekind sont sur la droite* $\Re s = 1/2$
- *Les nombres premiers peuvent être comptés très précisément*



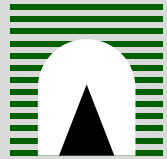
La conjecture d'Artin
la quasi–résolution



Théorème (R. Gupta, R. Murty & R. Heath–Brown (1984/86))

$\exists g \in \{2, 3, 5\}$ t.q.

$$\#\{p \leq x : \ p > 5, \langle g \bmod p \rangle = \mathbb{F}_p^*\} \gg \frac{\pi(x)}{\log x}$$



La Conjecture d'Artin pour les racines quasi–primitives en rang plus élevé

travail conjoint avec Andrea Susa

Notations:

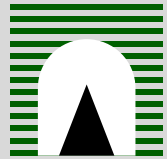
- $\Gamma \subset \mathbb{Q}^*$ Sous-groupe de type fini
- r rang de Γ
- $m \in \mathbb{N}^+$
- $\sigma_\Gamma = \prod_{p:v_p(x)=0, \exists x \in \Gamma} p$
- $\forall p \nmid \sigma_\Gamma$

$$\Gamma_p = \{g (\mathrm{mod} p) : g \in \Gamma\} \subset \mathbb{F}_p^*$$

et on définit

- $N_\Gamma(x,m) := \#\{p \leq x : p \nmid \sigma_\Gamma, |\Gamma_p| = \frac{p-1}{m}\}$
- Γ_p généralise la notion de $\langle a \bmod p \rangle$.
- si $\Gamma = \langle a \rangle$ est de rang 1, alors

$$N_{\langle a \rangle}(x,m) = \#\{p \leq x : \frac{1}{p} \text{ a une période de longueur } \frac{p-1}{m}\}$$

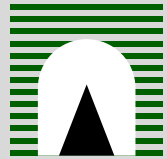


La Conjecture d'Artin pour les racines quasi–primitives en rang plus élevé

travail conjoint avec Andrea Susa

Dip. Mat. & Fis.

Università Roma Tre



Théorème

Soit $\Gamma \subset \mathbb{Q}^*$ avec rang $r \geq 2$. Soit $m \in \mathbb{N}$ et supposons GRH vérifié pour $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ ($k \in \mathbb{N}$). Alors, $\forall \epsilon > 0$ et $m \leq x^{\frac{r-1}{(r+1)(4r+2)}-\epsilon}$,

$$N_\Gamma(x,m) = \left(\rho(\Gamma,m) + O\left(\frac{1}{\varphi(m^{r+1})\log^r x}\right)\right)\pi(x),$$

où

$$\rho(\Gamma,m) = \sum_{k\geq 1} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/mk}) : \mathbb{Q}]}.$$

Un analogue du résultat ci-dessus est également valable, dans le cas où $\Gamma \subset \mathbb{Q}^*$ est de rang infini.

La Conjecture d'Artin pour les racines quasi–primitives en rang plus élevé

travail en commun avec Andrea Susa

Théorème

Soit $\Gamma \subset \mathbb{Q}^+ = \{q \in \mathbb{Q}; q > 0\}$ de rang $r \geq 2$ et soit $m \in \mathbb{N}$. Soit $\Gamma(m) := \Gamma(\mathbb{Q}^*)^m/(\mathbb{Q}^*)^m$,

$$A_{\Gamma,m} = \frac{1}{\varphi(m)|\Gamma(m)|} \times \prod_{\substack{\ell>2 \\ \ell\nmid m}} \left(1 - \frac{1}{(\ell-1)|\Gamma(\ell)|}\right) \times \prod_{\substack{\ell>2 \\ \ell\mid m}} \left(1 - \frac{|\Gamma(\ell^{v_\ell(m)})|}{\ell|\Gamma(\ell^{1+v_\ell(m)})|}\right)$$

et

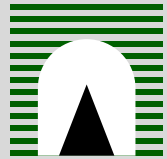
$$B_{\Gamma,k} = \sum_{\substack{\eta\mid\sigma_\Gamma \\ \eta^{2^{v_2(k)-1}}\cdot\mathbb{Q}^{*2^{v_2(k)}} \in \Gamma(2^{v_2(k)}) \\ v_2(\partial(\eta))\leq k}} \prod_{\substack{\ell\mid\partial(\eta) \\ \ell\nmid k}} \frac{-1}{(\ell-1)|\Gamma(\ell)|-1}.$$

Alors

$$\rho(\Gamma,m) = A_{\Gamma,m}\left(B_{\Gamma,m} - \frac{|\Gamma(2^{v_2(m)})|}{(2,m)|\Gamma(2^{1+v_2(m)})|}B_{\Gamma,2m}\right).$$

Dip. Mat. & Fis.

Università Roma Tre



La Conjecture d'Artin pour les racines quasi–primitives en rang plus élevé

densité nulle

Théorème

Soit $\Gamma \subset \mathbb{Q}^+$ de type fini, $m \in \mathbb{N}$. Alors

$$\rho(\Gamma, m) = 0$$

si l'une des conditions suivantes est remplie::

1. $2 \nmid m$ et pour tous $g \in \Gamma, \partial(g) \mid m$;
2. $2 \mid m, 3 \nmid m, \Gamma(3) = \{1\}$ et $\exists \eta \mid \sigma_\Gamma$,
   - $\eta^{2^{v_2(m/2)}} \cdot \mathbb{Q}^{*2^{v_2(m)}} \in \Gamma(2^{v_2(m)})$
   - $\partial(-3\eta) \mid m$

(si $2 \nmid m$, (1) est également nécessaire pour $\rho(\Gamma, m) = 0$). Si $\Gamma \subset \mathbb{Q}^+$ et m vérifie (1) ou (2) ci–dessus, alors

$$\{p : \mathrm{ind}_p \Gamma = m\} \quad \text{est fini.}$$

Par conséquent, sous GRH, si $2 \nmid m$,

$$\{p : \mathrm{ind}_p \Gamma = m\} \quad \text{finie} \iff \forall g \in \Gamma, \partial(g) \mid m.$$