Etude probabiliste des p-quotients de Fermat

Georges Gras

ETUDE PROBABILISTE DES p-QUOTIENTS DE FERMAT

GEORGES GRAS

ABSTRACT. Pour $a \geq 2$ fixé, nous suggérons que la probabilité de nullité du p-quotient de Fermat $q_p(a)$ est inférieure à $\frac{1}{p}$ pour tout premier p assez grand. Pour cela nous proposons diverses heuristiques, justifiées par des expérimentations numériques et des formules analytiques, pouvant impliquer la finitude des $q_p(a)$ nuls (Théorème 4.11) et l'existence d'entiers a tels que $q_p(a) \neq 0\ \forall p$. Nous montrons que la densité des entiers A tels que $q_p(A) \neq 0,\ \forall p \leq x$, est en $O\big(\frac{1}{\log(x)}\big)$ (Théorème 4.13).

ABSTRACT. For fixed $a \geq 2$, we suggest that the probability of nullity of the p-Fermat quotient $q_p(a)$ is lower than $\frac{1}{p}$ for any arbitrary large prime p. For this we propose various heuristics, justified by means of numerical computations and analytical results, which may imply the finiteness of the $q_p(a)$ equal to 0 (Theorem 4.11) and the existence of integers a such that $q_p(a) \neq 0\ \forall p$. We show that the density of integers A such that $q_p(A) \neq 0,\ \forall p \leq x$, is about $O\big(\frac{1}{\log(x)}\big)$ (Theorem 4.13).

1. INTRODUCTION

Nous étudions la probabilité de nullité du p-quotient de Fermat $q_p(a)$, de a fixé dans $\mathbb{N}\setminus\{0,1\}$, p étant la variable, à partir du fait que ceci a lieu si et seulement si p^2 divise la valeur en a du m-ième polynôme cyclotomique Φ_m, où $m \,|\, p-1$ est l'ordre de a modulo p (par abus, $q_p(a) = u \in [0, p[$ signifie $\frac{a^{p-1}-1}{p} \equiv u \pmod p$).

D'une manière générale nous convenons, dans toute la suite, de désigner par a un entier fixé (donc "petit" par rapport à p arbitrairement grand), par A un entier quelconque (A est utilisé pour définir des densités sur $\mathbb{N}$ ou $\mathbb{N}\setminus p\,\mathbb{N}$), et enfin par z (resp. Z) un entier de $[1, p[$ (resp. de $[1, p^2[$).

Dans un premier temps, nous utilisons un résultat général de Andrew Granville (1998) qui permet, grâce à un principe local-global diophantien, de déterminer (pour $f \in \mathbb{Z}[X]$) la densité des entiers $A \in \mathbb{N}$ tels que $f(A)$ est sans facteur carré.

Pour Φ_m, la densité relative à la seule condition locale $p^2 \nmid \Phi_m(A)$, pour $p \equiv 1 \pmod m$, est égale à $1 - \frac{\varphi(m)}{p^2}$ où φ est l'indicateur d'Euler, celle relative à la condition $\Phi_m(A)$ sans facteur carré étant égale au produit $\prod_{p \equiv 1 \,(\mathrm{mod}\ m)}(1 - \frac{\varphi(m)}{p^2})$ des densités locales.

Pour tout p, la *densité* des $A \in \mathbb{N}\setminus p\mathbb{N}$ tels que $q_p(A) = 0$ est trivialement $\frac{1}{p}$ (resp. $\frac{p-1}{p^2}$ pour celle des $A \in \mathbb{N}$). Noter que $q_p(1) = 0$ et $q_p(p-1) = 1$ ($\forall\, p > 2$).

Date: 4 Novembre 2014.

1991 *Mathematics Subject Classification.* Primary 11F85; 11R18.

Key words and phrases. Fermat quotients; cyclotomic polynomials; probabilistic number theory.

On en déduit l'heuristique suivante, reposant sur le fait que les probabilités sont inférieures aux densités correspondantes (i.e., lorsque a fixé est remplacé par la variable aléatoire A) : pour a fixé et p arbitraire assez grand, on a la majoration :

$$\mathrm{Prob}\big(q_p(a)=0\big) < \frac{1}{p\,(p-1)^2}\sum_{d\,\mid\,p-1}\varphi(d)^2 < \frac{1}{p},$$

qui ne renseigne que partiellement sur la finitude ou non des $q_p(a)$ nuls.

Dans un second temps, nous montrons comment tenir compte d'avantage du fait que a est fixé une fois pour toutes et que si $q_p(a)=0$ alors $q_p(a^j)=0$ pour les exposants j tels que $a^j \in [2,p-1[$, ce qui introduit un *principe de répétitions* (entiers $z\in[1,p[$ ayant *même* quotient de Fermat $q_p(z)=u$, $u\in[0,p[$ fixé).

En effet, l'expérimentation numérique montre que cette répartition exceptionnelle de $O(\log(p))$ valeurs $z_j=a^j$, par rapport aux $p-1$ solutions $Z\in[1,p^2[$ à $q_p(Z)=0$, est un cas particulier du principe de répétitions général $q_p(z)=u$, $z\in[1,p[$, pour $u\in[0,p[$ fixé ; ce nombre $m_p(u)$ de répétitions peut être au plus aussi en $O(\log(p))$ pour de *très rares* nombres premiers. A priori, le cas $u=0$ n'est pas particulier et on peut avoir $m_p(0)=O(\log(p))$ sans qu'il existe nécessairement $a\ll p$ tel que $q_p(a)=0$ (cf. exemples du § 4.3), ce qui ferait que les célèbres "Wieferich primes" $p=1093, 3511$, ne seraient pas de nature particulière, les valeurs remarquables correspondantes $z_j=2^j\in[2,p-1[$ conduisant à la répétition étant alors anecdotiques.

Le nombre $M_p:=\sup_{u\in[0,p[}\big(m_p(u)\big)$ est au contraire en $O(\log(p))$ *pour tout nombre premier* p, accréditant ainsi l'existence d'une loi de probabilité canonique.

On étudie alors une heuristique stipulant l'existence d'une loi de probabilité binomiale, pour le nombre de $z\in[2,p-1[$ tels que $q_p(z)=u$, à savoir :

$$\mathrm{Prob}\big(\big|\{z\in[2,p-1[,\ q_p(z)=u\}\big|\geq n\big)=1-\sum_{j=0}^{n-1}\tbinom{p-3}{j}\frac{1}{p^j}\Big(1-\frac{1}{p}\Big)^{p-3-j};$$

pour tout $u\in[0,p[$ fixé. Appliquée à $u=0$ et $n\approx\frac{\log(p)}{\log(a)}$ ou plus généralement $n=O(\log(p))$, on obtient, via le principe de Borel–Cantelli et sous cette heuristique, la finitude des p tels que $q_p(a)=0$.

Enfin, en utilisant le fait que le produit formel $\widetilde{\mathcal{P}}(A)=\prod_{m\geq 1}\frac{\Phi_m(A)}{\text{p.g.c.d.}\,(\Phi_m(A),m)}$ est divisible par tous les nombres premiers et que $q_p(A)=0$ si et seulement si $p^2\,|\,\widetilde{\mathcal{P}}(A)$, on obtient la densité des $A\in\mathbb{N}$ tels que $q_p(A)\neq 0\ \forall p\leq x$ (cf. Théorème 4.13).

En toute hypothèse, on peut envisager que la probabilité de nullité de $q_p(a)$ (pour a fixé et $p\to\infty$) est strictement inférieure à $\frac{1}{p}$ et que la conjecture sur la finitude des premiers p tels que $q_p(a)=0$ reste crédible (conjecture qui est un cas particulier des conjectures analogues que nous avons formulées dans le cadre général des régulateurs p-adiques d'un nombre algébrique, cf. [4]).

2. Cyclotomie et quotients de Fermat

2.1. **Rappels sur le quotient de Fermat.** Soit $a\in\mathbb{N}\setminus\{0,1\}$ fixé. Soit p un nombre premier ne divisant pas a. Soit $m=o_p(a)$, divisant $p-1$, l'ordre de a modulo p et soit ξ une racine primitive m-ième de l'unité dans $\mathbb{C}$; alors on peut écrire $a^m-1=\prod_{j=1}^m(a-\xi^j)\equiv 0\pmod p$.

Comme m est l'ordre de a modulo p, c'est le facteur de a^m-1 défini par :

$$\Phi_m(a)=\prod_{t\in(\mathbb{Z}/m\mathbb{Z})^\times}(a-\xi^t)$$

qui est dans $p\,\mathbb{Z}$, où Φ_m est le m-ième polynôme cyclotomique. De façon précise on a la relation $\dfrac{a^m-1}{p}=\dfrac{\Phi_m(a)}{p}\times\prod\limits_{\substack{d\mid m,\\ d\neq m}}\Phi_d(a)$, où $\prod\limits_{\substack{d\mid m,\\ d\neq m}}\Phi_d(a)\not\equiv 0\,(\mathrm{mod}\ p)$; en effet, si l'on avait $p\mid\Phi_d(a)$ pour $d\mid m, d\neq m$, alors on aurait $p\mid a^d-1$ et m ne serait pas l'ordre de a modulo p. On a donc l'implication $m=o_p(a)\Longrightarrow p\mid\Phi_m(a)$.

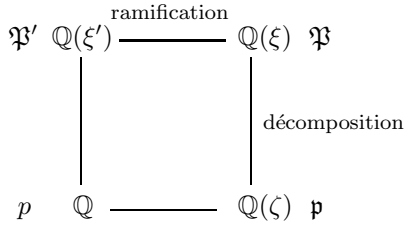
La réciproque est inexacte ; par exemple, si $p=3$, $m=6$, $a=5$, on a $\Phi_m(a)=7\times p$ avec pour ordre de a modulo p, $o_p(a)=2$ et $\Phi_2(a)=2\times p$ comme attendu, mais on a ici $m=p\cdot o_p(a)$ (i.e., p.g.c.d. $(\Phi_m(a),m)=p$). Ce phénomène sera précisé par le Théorème 2.4

Remarque 2.1. On a $q_p(a)\equiv 0\pmod p$ si et seulement si $\Phi_{o_p(a)}(a)\equiv 0\pmod{p^2}$. Pour diverses propriétés des quotients de Fermat on peut se reporter à [1], [2], [6], [8], [13], [10], ainsi qu'à [12], [5], [16] pour les liens avec la conjecture ABC.

2.2. **Utilisation des corps cyclotomiques.** Nous n'utilisons que des propriétés classiques que l'on peut trouver dans [17].

Lemme 2.2. *Soient $a\in\mathbb{N}\backslash\{0,1\}$, $p\nmid a$, et $m\geq 1$. Alors la congruence $\Phi_m(a)\equiv 0\pmod{p^h}$, $h\geq 1$, est équivalente à l'existence d'un couple $(\xi,\mathfrak{P})$, unique à conjugaison près, tel que $a\equiv\xi\pmod{\mathfrak{P}^h}$, où ξ est une racine primitive m-ième de l'unité et $\mathfrak{P}$ un idéal premier de $\mathbb{Q}(\xi)$ au-dessus de p, de degré résiduel 1.*
En outre, lorsque ceci a lieu, m est nécessairement de la forme $p^e\cdot o_p(a)$, $e\geq 0$.

Démonstration. La relation $a\equiv\xi\pmod{\mathfrak{P}^h}$, $h\geq 1$, prouve que $\mathfrak{P}$ est de degré résiduel 1 car l'anneau des entiers de $\mathbb{Q}(\xi)$ est $\mathbb{Z}[\xi]$ et ξ est congrue à un rationnel modulo $\mathfrak{P}$. Un sens est donc évident puisque $\Phi_m(a)=\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(a-\xi)$.
Supposons $\Phi_m(a)\equiv 0\pmod{p^h}$, $h\geq 1$. Comme $\Phi_m(a)=\prod\limits_{t\in(\mathbb{Z}/m\mathbb{Z})^\times}(a-\xi^t)\equiv 0\pmod{p^h}$, il existe $\mathfrak{P}_1\mid p$ dans $\mathbb{Q}(\xi)$ tel que $a-\xi\equiv 0\pmod{\mathfrak{P}_1}$.
Supposons que l'on ait $a-\xi\equiv 0\pmod{\mathfrak{P}_2}$, $\mathfrak{P}_2\mid p$, avec $\mathfrak{P}_2\neq\mathfrak{P}_1$; il existe donc une conjuguaison non triviale $\xi\mapsto\xi^t\neq\xi$ telle que $\mathfrak{P}_2=\mathfrak{P}_1^{t^{-1}}\neq\mathfrak{P}_1$ et on obtient $a-\xi^t\equiv 0\pmod{\mathfrak{P}_1}$, ce qui conduit à $\xi^t-\xi\equiv 0\pmod{\mathfrak{P}_1}$. D'où deux cas :
(i) $p\nmid m$ & $\xi^t\neq\xi$; alors $\xi^t-\xi$ est une unité en p (absurde).
(ii) $p\mid m$ & $\xi^t\neq\xi$.
Donc si $p\nmid m$, un seul idéal premier $\mathfrak{P}\mid p$ intervient et on a $a-\xi\equiv 0\pmod{\mathfrak{P}^h}$.
Examinons le cas $p\mid m$ & $\xi^t\neq\xi$ en considérant le schéma suivant :



Si l'on pose $m=p^em'$, $e\geq 1$, $p\nmid m'$, et $\xi=\zeta\,\xi'$ (ζ d'ordre p^e, ξ' d'ordre m'), il vient $\zeta^t\xi'^t-\zeta\,\xi'\equiv 0\pmod{\mathfrak{P}_1}$. Or on a toujours $\zeta\equiv 1\pmod{\mathfrak{P}_1}$ car dans $\mathbb{Q}(\zeta)$

il y a un unique idéal premier $\mathfrak{p} = (1-\zeta)$ totalement ramifié dans $\mathbb{Q}(\zeta)/\mathbb{Q}$, donc tel que $\mathfrak{P}_1 \,|\, \mathfrak{p}$ et $\mathfrak{P}_2 \,|\, \mathfrak{p}$ (si $p^e = 2$, $\mathbb{Q}(\zeta) = \mathbb{Q}$ et $\mathfrak{p} = (2)$).
D'où $\xi'^t - \xi' \equiv 0 \pmod{\mathfrak{P}'_1 = \mathfrak{P}_1 \cap \mathbb{Z}[\xi']}$ dans $\mathbb{Q}(\xi')$, et par conséquent $\xi'^t = \xi'$ (i.e., $t \equiv 1 \pmod{m'}$) puisque $p \nmid m'$. Mais ceci implique $\mathfrak{P}_2 = \mathfrak{P}_1$ car $\mathbb{Q}(\xi)/\mathbb{Q}(\xi')$ est totalement ramifiée en p et t fixe $\mathbb{Q}(\xi')$ (absurde).

On a donc obtenu dans tous les cas $a - \xi \equiv 0 \pmod{\mathfrak{P}^h}$ pour un unique $\mathfrak{P} \,|\, p$.

Montrons enfin que $m' = o_p(a)$ dans tous les cas. On a à ce stade $m = p^e\, m'$, $e \geq 0$, et $a \equiv \xi' \pmod{\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Z}[\xi']}$ puisque $\zeta \equiv 1 \pmod{\mathfrak{P}}$ (y compris si $e = 0$ où $\zeta = 1$), ce qui implique $a^d \equiv 1 \pmod{p}$ (i.e., $\xi'^d \equiv 1 \pmod{\mathfrak{P}'}$) si et seulement si $\xi'^d = 1$, d'où $d \equiv 0 \pmod{m'}$; d'où le lemme. □

Revenons à l'aspect réciproque de l'implication $m = o_p(a) \Longrightarrow p \,|\, \Phi_m(a)$ en tenant compte des questions de divisibilités par p^h. D'après le lemme précédent, si $p \,|\, \Phi_m(a)$, on a $m = p^e m'$, $e \geq 0$, où $m' = o_p(a)$, et par conséquent $p \,|\, \Phi_{m'}(a)$.
Le cas $p \nmid m$ est donc résolu et conduit à l'équivalence partielle :

$$p \,|\, \Phi_m(a) \ \&\ p \nmid m \iff m = o_p(a).$$

Dans ce cas toute puissance p^h, $h \geq 1$, peut diviser $\Phi_m(a)$ (c'est le problème du quotient de Fermat pour $h \geq 2$).

Lemme 2.3. *Supposons que pour $h \geq 1$, $p^h \,|\, \Phi_m(a)$ avec $m = p^e m'$, $e \geq 1$, $p \nmid m'$. Alors nécessairement $h = 1$ (i.e., $\Phi_m(a) \not\equiv 0 \pmod{p^2}$) sauf si $p^e = m = 2$, auquel cas si $a = -1 + 2^h\, u$, $h \geq 1$ quelconque, on a $\Phi_2(a) = 2^h\ u$, $\Phi_1(a) = -2 + 2^h\, u$.*

Démonstration. On a donc par hypothèse, d'après le Lemme 2.2, $a \equiv \xi \pmod{\mathfrak{P}^h}$, pour $\xi = \zeta\xi'$ d'ordre $p^e m'$ (ζ d'ordre p^e, ξ' d'ordre m'), et $a \equiv \xi' \pmod{\mathfrak{P}'^{h'}}$, $\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Z}[\xi']$, avec $h' \geq 1$ puisque $\zeta \equiv 1 \pmod{\mathfrak{P}}$; on a l'identité :

$$a - \xi = a - \xi' + \xi'\,(1 - \zeta),$$

où les $\mathfrak{P}$-valuations des termes sont respectivement $h,\ h'p^{e-1}(p-1), 1$.

Si $h'p^{e-1}(p-1) > 1$ on a nécessairement $h = 1$. Le cas $h'p^{e-1}(p-1) = 1$ correspond au cas $p = 2$, $h' = e = 1$, donc $o_2(a) = 1$, $\xi' = 1$, $\xi = -1$, $\Phi_2(a) = a + 1$ et p.g.c.d. $(2, \Phi_2(a)) = 2$ (e.g. $p = 2$, $a = 23$, $m = 2$, $\Phi_2(a) = 8 \times 3$, $\Phi_1(a) = 2 \times 11$, $h' = 1$, $h = 3$). En dehors du cas $m = 2$, $p = 2$, $e = 1$, on a $h = 1$. □

En particulier, pour $m = p^e m' \neq 2$, $e \geq 1$, on a $p \,|\, \Phi_m(a)$ et $p^2 \nmid \Phi_m(a)$ (on rappelle que $m' = o_p(a)$). Autrement dit, dans tous les cas où $e \geq 1$, la valeur de $\Phi_m(a)$ ne peut renseigner sur le quotient de Fermat (dans le cas particulier $p = 2$, $m = 2$, $\Phi_2(a) = a + 1$, mais $q_2(a) = 0$ signifie $a \equiv 1 \pmod 4$, or $a + 1 \equiv 2 \pmod 4$).

Théorème 2.4. *Pour tout $m \geq 1$, le p.g.c.d. de $\Phi_m(a)$ et de m est égal à 1 ou à un nombre premier p. Dans ce dernier cas, $m = p^e \cdot o_p(a)$, $e \geq 1$. Réciproquement, pour tout premier p et tout $e \geq 1$, $m = p^e \cdot o_p(a)$ conduit à* p.g.c.d. $(\Phi_m(a), m) = p$. *Autrement dit, on a l'équivalence (pour tout p et tout m) :*

$$p \,|\, \Phi_m(a) \iff m = p^e \cdot o_p(a),\ e \geq 0,$$

Démonstration. Si p et q, $p \neq q$, sont des nombres premiers divisant m et $\Phi_m(a)$, on a nécessairement $m = p^e q^f m''$, $e, f \geq 1$, avec $o_p(a) = q^f m'' \,|\, p - 1$ et $o_q(a) = p^e m'' \,|\, q - 1$, qui suppose $q < p$ et $p < q$ (absurde).

Enfin montrons que tout p premier et $e \geq 1$ conviennent pour $m = p^e \cdot o_p(a)$. Comme $p \,|\, \Phi_{o_p(a)}(a)$, on a $a \equiv \xi' \pmod{\mathfrak{P}'}$ dans $\mathbb{Q}(\xi')$ (ξ' d'ordre $o_p(a)$) ; donc

pour toute racine ζ d'ordre p^e, et pour $\mathfrak{P} \,|\, \mathfrak{P}'$ dans $\mathbb{Q}(\zeta\xi')$, on a $a \equiv \zeta\xi' \pmod{\mathfrak{P}}$ (d'où le résultat par le Lemme 2.2). Il est clair que p.g.c.d. $(m, \Phi_m(a)) = p$. □

Nous réserverons la notation r au cas où $m = r^e \cdot o_r(a)$, $e \geq 1$, car r n'intervient pas pour le calcul des p-quotients de Fermat de a pour $p \,|\, \Phi_m(a)$. Autrement dit la considération de p signifiera $p \,|\, \Phi_m(a)$, $p \nmid m$ (équivalent à $p \neq r$ si m est de la forme précédente avec $e \geq 1$).

2.3. **Définition des nombres $\widetilde{\Phi}_m(a)$, $m \geq 1$.** On peut donc considérer dans tous les cas $\widetilde{\Phi}_m(a) := \dfrac{\Phi_m(a)}{\text{p.g.c.d.}\,(\Phi_m(a), m)}$ qui est égal à $\Phi_m(a)$ ou à $\dfrac{\Phi_{r^e \cdot o_r(a)}(a)}{r}$, $e \geq 1$, pour éliminer le facteur premier r éventuel (ramifié dans $\mathbb{Q}(\xi)/\mathbb{Q}$). Dans le second cas $m = r^e \cdot o_r(a)$, $e \geq 1$, si $p \neq r$ divise $\Phi_m(a)$, alors $m = o_p(a)$ et on a $p \equiv 1 \pmod{r^e \cdot o_r(a)}$.

Dans le cas où p.g.c.d. $(\Phi_m(a), m) = r$, la nullité du r-quotient de Fermat de a est donnée via $\dfrac{\Phi_{o_r(a)}(a)}{r}$ en général distinct des $\dfrac{\Phi_{r^e \cdot o_r(a)}(a)}{r}$ pour $e \geq 1$ puisque dans ce cas, et pour $r^e \cdot o_r(a) \neq 2$, $\Phi_{r^e \cdot o_r(a)}(a) \not\equiv 0 \pmod{r^2}$ (cf. Lemme 2.3).

Par exemple, pour $r = 29$ et $a = 14$ on a $o_{29}(a) = 28$, $\dfrac{\Phi_{29 \cdot 28}(a)}{29} = F \not\equiv 0 \pmod{29}$ mais $\dfrac{\Phi_{28}(a)}{29} = 29 \times F'$ (i.e., $q_{29}(14) = 0$).

Pour $m = 2$ et a impair, on a $r = 2$ et $\widetilde{\Phi}_2(a) = \dfrac{a+1}{2}$ qui peut être divisible par une puissance de 2 arbitraire contrairement au cas général (cf. Lemme 2.3).

2.4. **Décomposition en facteurs premiers de $\widetilde{\Phi}_m(a)$.** Soit $m \neq 2$; d'après les résultats précédents, si l'on pose $\widetilde{\Phi}_m(a) = \prod_{k=1}^{g} \ell_k^{n_k}$, $\ell_1 < \ell_2 < \ldots < \ell_g$, $n_k \geq 1$, tous les premiers ℓ_k sont congrus à 1 modulo m (car de degré 1 et non ramifiés dans $\mathbb{Q}(\mu_m)/\mathbb{Q}$). Il en résulte aussi que pour un tel $\ell = \ell_j$ (en posant $\ell - 1 = t\,m$), ℓ est totalemment décomposé dans l'extension Galoisienne $\mathbb{Q}(\mu_{\ell-1})(\sqrt[t]{a})/\mathbb{Q}$ puisque a est localement de la forme b^t modulo ℓ (ℓ ne divise pas a et n'est pas ramifié dans cette extension). Ces questions d'ordres modulo ℓ sont liées à des techniques issues de la conjecture d'Artin sur les racines primitives et de la démonstration de Hooley, susceptibles de s'appliquer aux quotients de Fermat (voir [9] pour un exposé exhaustif).

Lemme 2.5. *On suppose (m, p) distinct de $(2, 2)$. On a $p^2 \,|\, \widetilde{\Phi}_m(a)$ si et seulement si $m = o_p(a)$ & $p^2 \,|\, \Phi_m(a)$, donc si et seulement si $m = o_p(a)$ & $q_p(a) = 0$.*

Démonstration. En effet, si $p^2 \,|\, \Phi_{o_p(a)}(a)$, comme $p \,|\, \Phi_{o_p(a)}(a)$ et $p \nmid o_p(a)$, on a $\widetilde{\Phi}_{o_p(a)}(a) = \Phi_{o_p(a)}(a)$ et donc $p^2 \,|\, \widetilde{\Phi}_m(a)$.

Réciproquement, si $p^2 \,|\, \widetilde{\Phi}_m(a)$, on peut supposer que p.g.c.d. $(\Phi_m(a), m) = r$ avec $m = r^e\, o_r(a)$, $e \geq 1$, sinon p.g.c.d. $(\Phi_m(a), m) = 1$, $\widetilde{\Phi}_m(a) = \Phi_m(a)$ et nécessairement $m = o_p(a)$. Ainsi $\widetilde{\Phi}_m(a) = \dfrac{\Phi_m(a)}{r}$, donc $p \nmid m$ (i.e., $p \neq r$ car $r^2 \nmid \Phi_m(a)$ par le Lemme 2.3 qui exclue le cas $p^e = m = 2$), d'où $p^2 \,|\, \Phi_m(a) = \Phi_{o_p(a)}(a)$. □

Lemme 2.6. *Pour a fixé, les $\widetilde{\Phi}_m(a)$, $m \geq 1$, sont premiers entre eux deux à deux. Pour tout $p \geq 2$ il existe un et un seul $m \geq 1$ (égal à $o_p(a)$), tel que $p \,|\, \widetilde{\Phi}_m(a)$.*

Démonstration. Si $p \neq 2$ divise $\widetilde{\Phi}_m(a)$ et $\widetilde{\Phi}_{m'}(a)$, d'après le Théorème 2.4 on a $m = p^e o_p(a)$ et $m' = p^{e'} o_p(a)$, $e, e' \geq 0$. Si par exemple $e \geq 1$, on a $p = r$ (absurde car r^2 ne divise pas $\widetilde{\Phi}_m(a)$) ; donc $e = e' = 0$ et $m = m'$.

Si $p = 2$, on obtient encore $m = 2^e$, $m' = 2^{e'}$, $e, e' \geq 0$; le cas e ou $e' \geq 2$ étant impossible car alors $\widetilde{\Phi}_m(a)$ ou $\widetilde{\Phi}_{m'}(a)$ est impair, il reste par exemple le cas $e = 1$, $e' = 0$, mais alors $\widetilde{\Phi}_2(a) = \frac{a+1}{2}$ et $\widetilde{\Phi}_1(a) = \frac{a-1}{2}$ qui ne peuvent être tous deux divisibles par 2. Enfin tout p divise $\Phi_{o_p(a)}(a) = \widetilde{\Phi}_{o_p(a)}(a)$. □

En résumé on a obtenu l'équivalence, plus forte que $q_p(a) = 0 \Longleftrightarrow p^2 \mid \Phi_{o_p(a)}(a)$:

Théorème 2.7. *Soit $a \in \mathbb{N}\backslash\{0, 1\}$ et soit p premier. Alors $q_p(a) = 0$ si et seulement si p^2 divise $\widetilde{\Phi}_{o_p(a)}(a)$ (cf. § 2.3).*

Les cas où $\widetilde{\Phi}_m(a)$ est divisible par le carré d'un nombre premier p sont rarissimes. Rappelons cependant les toutes premières valeurs (a, p) pour lesquelles $q_p(a) = 0$, qui correspondent le plus souvent à des cas triviaux comme $p = 2$ et $a \equiv 1 \pmod 4$, $p = 3$ et $a \equiv 1, 8 \pmod 9$:

$$(a, p) = (3, 11); (5, 2); (7, 5); (8, 3); (9, 2); (9, 11); (10, 3); (11, 71); (13, 2); (14, 29).$$

Remarque 2.8. On utilise $\widetilde{\Phi}_m(a)$ au lieu de $\Phi_m(a)$ car en raison du nombre premier r éventuel, les valeurs $\Phi_m(a)$ sont trivialement non premières entre elles (pour les m de la forme $r^e \cdot o_r(a)$, $e = 0, 1, \ldots$) ; donc on ne peut pas étudier les facteurs carrés du produit formel $\mathcal{P}(a) := \prod_{m \geq 1} \Phi_m(a)$ qui contient pour chaque r les sous-produits $\prod_{e \geq 1} \Phi_{r^e \cdot o_r(a)}(a)$ et donc les facteurs parasites r^∞, ce qui n'est plus le cas de $\widetilde{\mathcal{P}}(a) := \prod_{m \geq 1} \widetilde{\Phi}_m(a)$.

3. Première analyse probabiliste pour $q_p(a) = 0$

3.1. **Remarques sur la somme des probabilités.** Soit $a \geq 2$ fixé et soit p un nombre premier variable. Pour $u = u_p$ donné dans $[0, p[$, l'événement $q_p(a) = u$ est de probabilité a priori voisine de $\frac{1}{p}$. [1] Des probabilités inférieures à $\frac{1}{p}$ en moyenne (pour $u = 0$ par exemple) ne sont pas contradictoires avec une somme (sur u) égale à 1 car une étude numérique montre qu'environ $\frac{1}{3}$ des $u \in [0, p[$ ne sont pas de la forme $q_p(z)$, $z \in [1, p[$ (pour $p = 11$, les $u \in \{3, 6, 8, 9\}$ ne sont pas atteints). Pour $p = 1093$ et $p = 3511$ ($q_p(2) = 0$), on obtient respectivement les proportions exceptionnelles de 0.60348 et 0.60285 de u non atteints. Pour les grands nombres premiers, la proportion moyenne se stabilise autour de 0.3678 qui semble être e^{-1}.

De fait on a des probabilités moyennes lorsque p est la variable aléatoire, car dans l'optique d'estimer le nombre (fini ou infini) de p tels que $q_p(a) = 0$, certains p ont une probabilité importante d'être exclus en raison de la non surjectivité de l'application $z \in [1, p[\mapsto\ q_p(z) \in [0, p[$.

En outre, le cadre probabiliste de recherche des solutions $z \in [2, p - 1[$ est très différent du cas $z = a$ fixé et est plutôt de type "densité" sur un l'intervalle tendant vers l'infini avec p ; or on verra au § 3.5 que ces deux cas de figure sont à distinguer

[1] L'écriture $q_p(\bullet) = u$ a deux sens : ou bien p est fixé et $u = u_p \in [0, p[$, ou bien p est variable et $u \in \mathbb{N}$ est donné indépendant de p, auquel cas $q_p(\bullet) = u$ signifie $q_p(\bullet) \equiv u \pmod p$ qui se confond avec le sens précédent dès que $p > u$. Le cas $u = 0$ est donc universel et à ce titre particulier. Ceci est en rapport avec l'étude cyclotomique de la Section 2 où les cas $q_p(\bullet) = 0$ et $q_p(\bullet) \neq 0$ sont de nature différente en termes de divisibilités des $\widetilde{\Phi}_{o_p(\bullet)}(\bullet)$.

soigneusement, tout se régularisant sur l'intervalle $[1, p^2[$ (existence de $p-1$ solutions canoniques $Z_i \in [1, p^2[$ à $q_p(Z) = 0$ et surjectivité de $Z \in [1, p^2[\mapsto\ q_p(Z) \in [0, p[$, cf. Lemme 3.6).

3.2. **Résultat de A. Granville** [3]**.** Ce résultat a été obtenu, dans le cas le plus général, sous la conjecture ABC. Soit $f \in \mathbb{Z}[X]$ un polynôme tel que l'ensemble des $f(n)$, $n \in \mathbb{Z}$, ait un plus grand commun diviseur égal à 1 (le cas plus complet énoncé dans [3] ne s'applique pas pour nous).

Proposition 3.1. *La densité naturelle des entiers $A \in \mathbb{N}$ tels que $f(A)$ est sans facteur carré non trivial est donnée par l'expression :*

$$\prod_{p\,\text{premier}\,\geq 2} \Big(1 - \frac{c_p}{p^2}\Big),\ \text{où}\ c_p = \Big|\Big\{b \in [0, p^2[,\ \ f(b) \equiv 0 \,(\mathrm{mod}\ p^2)\Big\}\Big|,$$

chaque facteur $1 - \frac{c_p}{p^2}$ étant la densité (dite densité locale associée à p) des $A \in \mathbb{N}$ tels que $p^2 \nmid f(A)$. Dans le cas local, la densité des $A \in \mathbb{N}$ tels que $p^2 \mid f(A)$ étant $\frac{c_p}{p^2}$.

D'une certaine manière on peut dire que les événements $p^2 \nmid f(A)$ sont indépendants par rapport à p.

3.3. **Calcul des coefficients c_p pour les polynômes $\Phi_m(x)$, $m \geq 1$.** Le p.g.c.d. des $\Phi_m(n)$, $n \in \mathbb{Z}$, est égal à 1 car $\Phi_m(0) = \pm 1$ puisque toute racine de l'unité est de norme ± 1. Comme $\Phi_m(0) = \pm 1$, on a pour tout p premier,

$$c_p = \Big|\Big\{A \in [1, p^2[,\ \ \Phi_m(A) \equiv 0 \pmod{p^2}\Big\}\Big|.$$

Proposition 3.2. *Si $p \geq 2$ ne divise pas m, on a $c_p = 0$ pour les $p \not\equiv 1 \pmod m$ et $c_p = \varphi(m)$ pour les $p \equiv 1 \pmod m$, où φ est l'indicateur d'Euler.*
Si $m = p^e m'$, $e \geq 1$, $p \nmid m'$, on a $c_p = 0$ sauf si $m = 2$, auquel cas $c_2 = 1$.

Démonstration. (i) Cas $p \nmid m$. Dans ce cas, la congruence $\Phi_m(A) \equiv 0 \pmod p$ est équivalente à $m = o_p(A)$ et on a $p \equiv 1 \pmod m$; donc pour $p \nmid m$, il y a exactement $\varphi(m)$ nombres distincts $A_i \in [1, p[$ pour lesquels $\Phi_m(A_i) \equiv 0 \pmod p$. Considérons pour i fixé les entiers de la forme $A = A_i + \lambda_i\, p \in [1, p^2[$ (i.e., $\lambda_i \in [0, p[$). On a $\Phi_m(A) \equiv \Phi_m(A_i) + \lambda_i\, p\, \Phi'_m(A_i) \pmod{p^2}$, où Φ'_m est le polynôme dérivé de Φ_m ; dès que $\Phi'_m(A_i) \not\equiv 0 \pmod p$, il existe un unique λ_i modulo p donnant $\Phi_m(A) \equiv 0 \pmod{p^2}$ et dans ce cas, $c_p = \varphi(m)$.
Montrons que $\Phi'_m(A_i) \not\equiv 0 \pmod p$. On a $X^m - 1 = \Phi_m(X) \times Q(X)$, $Q \in \mathbb{Z}[X]$; d'où $m\, X^{m-1} = \Phi'_m(X) \times Q(X) + \Phi_m(X) \times Q'(X)$. Si $\Phi'_m(A_i) \equiv 0 \pmod p$ il vient $m\, A_i^{m-1} \equiv 0 \pmod p$; comme $p \nmid A_i$ par hypothèse, on a $m \equiv 0 \pmod p$ (absurde).

(ii) Cas où $p = r \mid m$. D'après le Lemme 2.3, $m = r^e \cdot o_r(A)$, $e \geq 1$, et $\Phi_m(A) \equiv 0 \pmod{r^2}$ n'a pas de solutions sauf si $m = 2$, auquel cas $c_2 = 1$. □

3.4. **Densités et Probabilités.** De façon générale, $A \in \mathbb{N}$ désigne une variable et $F(A)$ une propriété. On appelle alors densité naturelle (ou, pour simplifier, densité) la limite (si elle existe) :

$$\lim_{y \to \infty}\ \frac{1}{y}\Big|\Big\{A \leq y,\ \ F(A)\Big\}\Big|.$$

Si $F = F_p$ est la propriété locale $p^2 \mid f(A)$, la densité est celle donnée dans la Proposition 3.1, égale à $\frac{c_p}{p^2}$ (celle de $p^2 \nmid f(A)$ étant $1 - \frac{c_p}{p^2}$). Dans ce cadre, la

densité est relative à tous les entiers (y compris ceux divisibles par p). Dans $\mathbb{N}\backslash p\mathbb{N}$ ces densités deviennent respectivement $\frac{c_p}{p\,(p-1)}$ et $1-\frac{c_p}{p\,(p-1)}$.

Il faut distinguer la notion de densité (locale), relative à la propriété :

$$\textit{pour } p \textit{ fixé, } p^2 \mid f(A) \textit{ pour } A \in \mathbb{N} \textit{ variant arbitrairement,}$$

de celle de probabilité définissant l'évenement :

$$\textit{pour } a \textit{ fixé, } p^2 \mid f(a) \textit{ pour } p \textit{ premier variant arbitrairement}$$

(cas de l'étude de $q_p(a)=0$ équivalent à $p^2 \mid \widetilde{\Phi}_{o_p(a)}(a)$ (Théorème 2.7)).

La densité locale ne dépend que de p, tandis que ce que nous définissons comme probabilité est, pour tout a fixé, une fonction de p pour laquelle a est un paramètre.

Analysons sur le cas précis des $q_p(a)$ ce qu'il en est ; soit $d \mid p-1$ un ordre fixé.

Si $p=2$ et $d=1$, $\Phi_1(X)=X-1$ et la densité des A tels que $A-1\equiv 0 \pmod 4$ est trivialement $\frac{\varphi(1)}{p^2}=\frac{1}{4}$ (resp. $\frac{\varphi(1)}{p\,(p-1)}=\frac{1}{2}$ pour les A impairs). Ici l'ordre de grandeur de a ne joue pas encore, mais si l'on veut par exemple $a<p$, la seule solution est $a=1$.

Le cas $p=3$ est plus éloquent car pour $d=1$, la densité des A tels que $A-1\equiv 0 \pmod 9$ est trivialement $\frac{1}{9}$ (resp. $\frac{1}{6}$ pour les A étrangers à 3) et celle correspondant à $d=2$ (i.e., $\Phi_2(X)=X+1$) est aussi $\frac{1}{9}$(resp. $\frac{1}{6}$) ; puisque $A\not\equiv 0 \pmod 3$ peut être d'ordre 1 ou 2 modulo 3, la densité totale pour $q_3(A)=0$ est $\frac{2}{9}$ (resp. $\frac{1}{3}$).

Par contre pour a fixé non divisible par 3, le cas $a-1\equiv 0 \pmod 9$ se produit une fois (solution minimale $a=1$) et le cas $a+1\equiv 0 \pmod 9$ également, mais avec l'unique solution minimale $a=8$; or si a était fixé "assez petit", la probabilité d'avoir $q_3(a)=0$ chute. Le cas $a+1\equiv 0 \pmod 9$ n'est donc plus envisageable avec une probabilité égale à sa densité $\frac{1}{6}$.

Au total la probabilité pour que $q_3(a)=0$ n'est plus la densité totale $\frac{1}{6}+\frac{1}{6}=\frac{1}{3}$ (selon que $o_3(a)=1$ ou 2).

Pour $p=7$, on trouve, pour $A\in[1,7^2[$, $A\not\equiv 0 \pmod 7$, les 6 solutions suivantes à $p^2 \mid \widetilde{\Phi}_d(A)$, selon l'ordre d modulo p considéré :

$$A=1\ (d=1),\ \ A=48\ (d=2),\ \ A=18,30\ (d=3),\ \ A=19,31\ (d=6).$$

Pour $p=101$, on trouve de même les 100 solutions :

$$A=1\ \ (d=1),\ \ A=181\ (d=25),\ \ A=248\ (d=100),\ \ldots,\ A=10020\ (d=50),\ \ A=10200\ (d=2).$$

On voit bien que si a est fixé assez petit lorsque p varie de façon arbitraire, la probabilité de divisibilité de $\widetilde{\Phi}_d(a)$ par p^2 peut même être très faible.

Le cas $q_p(a)=u$ donné dans $\mathbb{N}$ est analogue, même si $u>0$ n'est plus universel comme $u=0$ puisque $q_p(a)=u$ signifie de fait $q_p(a)\equiv u \pmod p$ et une analogie avec le cas $u=0$ suppose $p>u$. On a $q_7(2)=2$, mais les seuls $p>7$, $p<10^8$, tels que $q_p(2)=2$ sont $71, 379, 2659$.

Pour simplifier, nous parlerons par abus de probabilités lorsque a est fixé, et nous écrirons $\mathrm{Prob}\big(f(a)\ \text{s.f.c.}\big)$ et $\mathrm{Prob}\big(p^2\nmid f(a)\big)$ respectivement, puis $\mathrm{Prob}\big(q_p(a)=0\big)$, $\mathrm{Prob}\big(q_p(a)\neq 0\big)$, etc.

A partir de ce principe et d'observations numériques, nous examinerons différentes heuristiques en partant des plus faibles (permettant encore l'infinitude des $q_p(a)$ nuls) pour aller vers les plus fortes impliquant la finitude des $q_p(a)$ nuls.

On peut donc déjà admettre la première heuristique générale suivante :

Heuristique 3.3. *Supposons que pour $A \in \mathbb{N}$ (resp. $A \in \mathbb{N} \setminus p\mathbb{N}$), on ait une propriété "globale" $F(A)$ (resp. la propriété "locale" $F_p(A)$), par exemple du type $f(A)$ a un facteur carré (resp. $p^2 \mid f(A)$), $f \in \mathbb{Z}[X]$.*
Alors la densité correspondante dans $\mathbb{N}$ (resp. $\mathbb{N}\setminus p\mathbb{N}$) est un majorant de $\mathrm{Prob}\big(F(a)\big)$ (resp. $\mathrm{Prob}\big(F_p(a)\big)$ pour a fixé et tout p assez grand.

Par exemple, les densités locales $\frac{\varphi(d)}{p\,(p-1)}$, caractérisant la propriété $F_p(A)$ définie par $p^2 \mid \widetilde{\Phi}_d(A)$ pour les A d'ordre $d \mid p-1$, sont des *majorants* de $\mathrm{Prob}\big(q_p(a)=0\big)$ pour a fixé de même ordre d ($a, A \in \mathbb{N} \setminus p\mathbb{N}$). Ceci sera utilisé au § 3.5.
La Proposition 3.2 a la conséquence suivante concernant la densité globale (on rappelle que $\widetilde{\Phi}_m(A) = \Phi_m(A)$ si p.g.c.d. $(\Phi_m(A), m) = 1$, et $\widetilde{\Phi}_m(A) = \frac{\Phi_{r^e \cdot o_r(A)}(A)}{r}$ sinon, pour un unique nombre premier r et $e \geq 1$) :

Corollaire 3.4. *Pour tout $m \neq 2$, la densité des $A \in \mathbb{N}$ tels que $\widetilde{\Phi}_m(A)$ est sans facteur carré non trivial est $\prod\limits_{p \equiv 1 \,(\mathrm{mod}\, m)} \Big(1 - \frac{\varphi(m)}{p^2}\Big)$. Pour $m = 2$, la densité des $\widetilde{\Phi}_2(A)$ $\big(= A+1$ ou $\frac{1}{2}(A+1)\big)$ sans facteur carré est $\prod_{p \geq 2} \big(1 - \frac{1}{p^2}\big) = \frac{6}{\pi^2} \approx 0.607927$.*

Remarque 3.5. Les valeurs de $P_m = \prod\limits_{p \equiv 1 \,(\mathrm{mod}\, m)} \big(1 - \frac{\varphi(m)}{p^2}\big)$ tendent rapidement vers 1 selon le tableau suivant :

$$\begin{aligned} P_3 &\approx 0.934842023086837134664 \\ P_4 &\approx 0.894841231202923082330 \\ P_{39} &\approx 0.994661340343876645092 \\ P_{40} &\approx 0.989616540587613990799 \\ P_{10003} &\approx 0.999993925954960217571. \end{aligned}$$

3.5. **Densités et probabilités au niveau des p-quotients de Fermat.** Soit $a \in \mathbb{N}\setminus\{0,1\}$ fixé. On écrit que la probabilité d'avoir $q_p(a) = 0$ est de la forme :

$$\mathrm{Prob}\big(q_p(a)=0\big) = \frac{1}{p^{1+\epsilon(p,a)}}, \text{ avec } \epsilon(p,a) \text{ voisin de } 0.$$

Dans l'étude probabiliste de la condition $q_p(a) = 0$, p est variable tendant vers l'infini de sorte que l'on a $a < p$ pour tout p assez grand ; on va donc rechercher, comme expliqué au § 3.4 (cf. Heuristique 3.3), la densité locale associée qui constituera un majorant de la probabilité correspondante. On fixe donc p et on se donne $u \in [0, p[$. La densité des A étrangers à p tels que $q_p(A) = u$ se lit aussi dans l'intervalle $[0, p^2[$ puisque $q_p(A + \Lambda\, p^2) \equiv q_p(A) \pmod p$ pour tout entier Λ.

Lemme 3.6. *Soit $z \in [1, p[$, p premier ; alors il existe un unique $\lambda_u(z) \in [0, p[$ tel que $Z = z + \lambda_u(z)\, p \in [1, p^2[$ vérifie $q_p(Z) = u$. Le nombre $\lambda_u(z)$ est caractérisé par la congruence $\lambda_u(z) \equiv z\,(q_p(z) - u) \pmod p$ et on obtient $Z \equiv z^p - z u\, p \pmod{p^2}$. Par conséquent, la densité des $A \in \mathbb{N}\setminus p\mathbb{N}$ tels que $q_p(A) = u$ est égale à $\frac{p-1}{\varphi(p^2)} = \frac{1}{p}$.*

Démonstration. Pour tout $\lambda \in \mathbb{N}$, $(z + \lambda\, p)^p - (z + \lambda\, p) \equiv z^p - z - \lambda\, p \pmod{p^2}$, d'où $\lambda \equiv z\, q_p(z) - Z\, q_p(Z) \equiv z\, q_p(z) - z\, q_p(Z) \pmod p$. Donc $q_p(Z) = u$ si et seulement si $\lambda = \lambda_u(z) \equiv z\, q_p(z) - z\, u \pmod p$. On a donc pour chaque $z \in [1, p[$ un unique $Z = z + \lambda_u(z)\, p \in [1, p^2[$ tel que $q_p(Z) = u$, d'où la densité (Z est aussi le résidu modulo p^2 de $z^p - z u\, p$). □

Remarques 3.7. (i) Lorsque $z \in [1,p[$, on a les relations $q_p(p-z) \equiv q_p(z) + z^{-1} \pmod p$, $\lambda(p-z)+\lambda(z) = p-1$; ceci n'entre pas en jeu pour $a \ll p$.

(ii) La relation $\lambda(z) \equiv q_p(z)\, z \pmod p$, pour tout $z \in [1,p[$, montre que $q_p(a)$ et $\lambda(a)$ ont des comportements analogues au plan heuristique.

(iii) Pour $u = 0$, l'élément $Z \equiv z \pmod p$ tel que $q_p(Z) = 0$ est caractérisé par $Z \equiv z^p \pmod{p^2}$.

(iv) Comme $q_p(A) = 0$ est équivalent à $p^2 \,|\, \widetilde{\Phi}_{o_p(A)}(A)$ (Théorème 2.7), d'après les résultats "locaux" (cf. §§ 3.2, 3.3, Corollaire 3.4), la densité des $A \in \mathbb{N}\backslash p\mathbb{N}$ tels que $p^2 \,|\, \widetilde{\Phi}_m(A)$ est égale à $\frac{\varphi(m)}{p\,(p-1)}$ (resp. 1) si $m = o_p(A)$ (resp. $m \neq o_p(A)$). En faisant la somme sur les ordres possibles, on retrouve bien la densité $\sum_{d\,|\,p-1} \frac{\varphi(d)}{p\,(p-1)} = \frac{1}{p}$.

Revenons au cas d'un entier $a \geq 2$ fixé ; soit $h_p(a) = \lfloor \frac{\log(p)}{\log(a)} \rfloor$ (partie entière). On a $o_p(a) > h_p(a)$ puisque $a^{o_p(a)} = 1 + \lambda\, p$, $\lambda \geq 1$, et de fait $\mathrm{Prob}\big(o_p(a) = d\big) = 0$ pour les $d \leq h_p(a)$.

On a $o_p(a) \in \{d,\ d\,|\,p-1\}$ et une heuristique raisonnable est que la probabilité correspondante est majorée par la densité relative à la propriété locale $o_p(A) = d$, qui est égale à $\dfrac{\varphi(d)}{p-1}$, car seul le résidu modulo p de A intervient. Mais le phénomène précédent sur les petites valeurs de d rend les "grands" ordres un peu plus probables pour a, ce qui semble pouvoir être négligé dans la mesure où l'on a, en majorant grossièrement, $\sum_{d \leq h_p(a)} \frac{\varphi(d)}{p-1} < O\big(\frac{\log^2(p)}{p}\big)$.

Remarque 3.8. Soient a fixé et p arbitrairement grand ; on a alors le phénomène analogue suivant : soit g, $a < g < p-1$, et soit $G := \big\{g^i,\ 1 \leq i < h_p(g)\big\} \subseteq [2,p-1[$. Cet ensemble est constitué d'éléments plus grands que a, dont les ordres sont certains diviseurs δ_i de $p-1$, et ceci modifie le décompte des ordres possibles pour a, ce qui fait que $\mathrm{Prob}\big(o_p(a) = \delta_i\big)$ est inférieure à $\frac{\varphi(\delta_i)}{p-1}$. Par conséquent, la probabilité correspondante de nullité de $q_p(a)$, pour a fixé et p variable, qui est la somme pondérée des densités, $\displaystyle\sum_{d\,|\,p-1} \mathrm{Prob}\big(o_p(a) = d\big) \times \frac{\varphi(d)}{p\,(p-1)}$, est a priori fortement majorée par $\displaystyle\sum_{d\,|\,p-1} \frac{\varphi(d)}{p-1} \times \frac{\varphi(d)}{p\,(p-1)} = \frac{1}{p\,(p-1)^2} \sum_{d\,|\,p-1} \varphi(d)^2$.

Exemple 3.9. *Prenons $p = 37813$, $a = 2$; alors pour $g = 3$, on a :*

$$G = \{3, 9, 27, 81,\ 243, 729, 2187,\ 6561, 19683\}$$

dont les éléments sont d'ordres respectifs :

$$\delta_i = 18906,\ 9453,\ 6302,\ 9453,\ 18906,\ 3151,\ 18906,\ 9453,\ 6302.$$

Pour $g = 5$ on trouve les ordres $\delta_j = 37812, 18906, 12604, 9453, 37812, 6302$.

On peut construire beaucoup de tels ensembles, jusqu'à $g = 193$ (donnant les ordres $\delta_k = 37812,\ 18906$).

Donc pour $a = 2$ (d'ordre 37812), la probabilité ne peut coïncider avec la densité $\frac{\varphi(p-1)}{p-1} = 0.3165$ puisque cet ordre est aussi celui de nombreux éléments $g > a$.

Le phénomène est difficile à quantifier, mais a une influence importante. En résumé on a obtenu dans ce premier cadre le résultat heuristique suivant :

Heuristique 3.10. *On a, pour $a \in \mathbb{N}\backslash\{0,1\}$ fixé et p assez grand :*

$$\mathrm{Prob}\big(q_p(a)=0\big) := \frac{1}{p^{1+\epsilon(p,a)}} < \frac{1}{p\,(p-1)^2}\sum_{d\,|\,p-1}\varphi(d)^2,$$

ou de façon équivalente $\epsilon(p,a) > \dfrac{1}{\log(p)}\Big(2\log(p-1) - \log\Big(\displaystyle\sum_{d\,|\,p-1}\varphi(d)^2\Big)\Big)$.

Remarque 3.11. Si l'heuristique précédente est vérifiée, alors on obtient :

$$\epsilon(p,a) > 0 \text{ car } \frac{1}{p^{1+\epsilon(p,a)}} < \frac{\sum_{d\,|\,p-1}\varphi(d)^2}{p\,(p-1)^2} < \frac{\big(\sum_{d\,|\,p-1}\varphi(d)\,\big)^2}{p\,(p-1)^2} = \frac{1}{p}$$

(où $\frac{1}{p}$ est la densité des A tels que $q_p(A)=0$). Autrement dit, si $\upsilon(p,a)=\upsilon(p)$ est la fonction $\upsilon(p) = \dfrac{1}{\log(p)}\Big(2\log(p-1) - \log\big(\displaystyle\sum_{d\,|\,p-1}\varphi(d)^2\big)\Big)$, on a $\epsilon(p,a) > \upsilon(p) > 0$ pour tout p assez grand. Afin de proposer de telles fonctions $\epsilon(p,a)$, nous allons donner une condition suffisante de convergence des séries du type $\displaystyle\sum_p \frac{1}{p^{1+\epsilon(p,a)}}$, la série $\displaystyle\sum_p \frac{1}{p^{1+\upsilon(p)}}$ ne l'étant pas comme l'a montré G. Tenenbaum (cf. § 3.7).

3.6. **Une série de référence convergente sur les nombres premiers.** Pour tout $n \geq 1$, désignons par p_n le n-ième nombre premier.

Lemme 3.12. *Soit $C > 1$ une constante et soit $\eta(p) := C \cdot \dfrac{\log_3(p)}{\log(p)}$, où $\log_k$ désigne le k-ième itéré de la fonction* log. *Alors on a $S := \displaystyle\sum_{p\geq 2} \frac{1}{p^{1+\eta(p)}} < \infty$.*

Démonstration. On a $\displaystyle\sum_{p\geq 2} \frac{1}{p^{1+C\,\cdot\,\log_3(p)/\log(p)}} = \sum_{p\geq 2} \frac{1}{p\,\cdot\,\log_2^C(p)} = \sum_{n\geq 1} \frac{1}{p_n\,\cdot\,\log_2^C(p_n)}$. On sait que $p_n > n\log(n)$ (théorème de Rosser) ; donc on peut, à une constante additive près, majorer S par $\displaystyle\sum_{n\geq n_0} \frac{1}{n\log(n)\,\cdot\,\log_2^C(n\log(n))} < \sum_{n\geq n_0} \frac{1}{n\log(n)\,\cdot\,\log_2^C(n)}$ qui a même comportement que $\displaystyle\int_{x_0}^{\infty} \frac{dx}{x\log(x)\,\cdot\,\log_2^C(x)} = \int_{y_0}^{\infty} \frac{dy}{y\,\cdot\,\log^C(y)} < \infty$. □

Cependant il ne faut pas oublier que $\epsilon(p,a) > \upsilon(p)$ et que par conséquent $\epsilon(p,a) > \eta(p)$ reste largement possible. La différence entre $\upsilon(p)$ (situation divergente) et $\eta(p)$ (situation convergente) est très faible comme le montrent les résultats numériques suivants pour p très grand (avec $C = 1.1$) :

$eta - upsilon = 0.010439$, $\quad p = 20000000000000000000000000000000000000243$
$eta - upsilon = 0.007099$, $\quad p = 20000000000000000000000000000000000000477$
$eta - upsilon = 0.004805$, $\quad p = 20000000000000000000000000000000000000513$
$eta - upsilon = -0.004780$, $\quad p = 20000000000000000000000000000000000000593$
$eta - upsilon = 0.008382$, $\quad p = 20000000000000000000000000000000000000723$.

Les rares cas de "croisement des courbes" correspondent aux cas où $p-1$ est divisible par un très grand nombre premier donnant un grand $\varphi(d)$. Ci-dessus, on a celui de $p-1 = 2^4\times 3^2\times 11\times 13\times 971250971250971250971250971250971251$.

3.7. **Première majoration du nombre de solutions p à $q_p(a)=0$.** Une estimation majorante du nombre de $p \leq x$ tels que $q_p(a)=0$ est $\displaystyle\sum_{p\leq x} \frac{1}{p^{1+\upsilon(p)}}$. Or la série $S := \displaystyle\sum_p \frac{1}{p^{1+\upsilon(p)}} = \sum_p \frac{1}{p\,(p-1)^2}\sum_{d\,|\,p-1}\varphi(d)^2$, comme on pouvait s'y attendre, est

divergente, et G. Tenenbaum a démontré que

$$S(x) := \sum_{p\le x} \frac{1}{p\,(p-1)^2} \sum_{d\,|\,p-1} \varphi(d)^2 = O(\log_2(x))$$

lorsque $x \to \infty$ (cf. [15]). Sa démonstration repose, entre autres, sur le théorème de Bombieri–Vinogradov (cf. [14], Théorème II.8.34). On en déduit, en admettant le principe de Borel–Cantelli, que pour a fixé le nombre moyen de solutions $p \nmid a$ à $q_p(a) = 0$ vérifie :

$$\Big|\Big\{p \le x,\ q_p(a) = 0\Big|\Big\} < S(x) = O(\log_2(x)) \approx \frac{1}{2}\log_2(x),\ \text{ pour } x \to \infty,$$

après une estimation de la constante, ce qui reste une croissance très faible mais ne permet pas de conclure dans le cas de a fixé une fois pour toutes (pour $x = 10^8$, $S(x) \approx 1.3380$ et $\frac{1}{2}\log_2(x) \approx 1.4567$). Voir aussi l'heuristique de [1], § 3.

La divergence de $\sum\limits_p \frac{1}{p^{1+\upsilon(p)}}$ n'est pas contradictoire avec une convergence éventuelle de $\sum\limits_p \frac{1}{p^{1+\epsilon(p,a)}}$ puisque chaque terme de S est un majorant strict de $\mathrm{Prob}\big(q_p(a) = 0\big)$ (i.e., $\epsilon(p,a) > \upsilon(p)$ pour tout p assez grand), voire un majorant d'un ordre de grandeur important, et il conviendra de revenir sur ce point, ce qui sera fait Section 4 en partant du point de vue heuristique de l'existence d'une loi de probabilité binomiale sur le nombre de solutions à $q_p(z) = 0$ pour $z \in [2, p-1[$.

Remarque 3.13. Comme expliqué au § 3.4, le fait que $A \in \mathbb{N}$ soit une "variable" dans les calculs de densités est fondamental. En effet, soient $p_1, \cdots, p_n$ des nombres premiers distincts donnés. pour chaque $p \in \{p_1, \ldots, p_n\}$ soit $(Z_p^j)_{j=1,\ldots,p-1}$ la famille des $p-1$ solutions canoniques $Z_p^j \in [1, p^2[$ à $q_p(Z_p^j) = 0$ (cf. Lemme 3.6) ; alors tout A satisfaisant à l'un des systèmes de congruences :

$$\begin{cases} A &\equiv & Z_{p_1}^{j_1} \pmod{p_1^2}, & j_1 \in \{1, \ldots, p_1 - 1\} \\ & \vdots & & \\ A &\equiv & Z_{p_n}^{j_n} \pmod{p_n^2}, & j_n \in \{1, \ldots, p_n - 1\} \end{cases}$$

conduit à $q_{p_1}(A) = \cdots = q_{p_n}(A) = 0$, et c'est en outre une équivalence. Naturellement la solution minimale A devient en général très grande dans $[1, \prod_j p_j^2[$.

Exemple 3.14. *Pour $p_1 = 5$, $p_2 = 7$, on obtient les 24 solutions fondamentales modulo 35^2 :*

$\{1, 18, 68, 99, 226, 276, 293, 324, 374, 393, 557, 607, 618,$
$668, 832, 851, 901, 932, 949, 999, 1126, 1157, 1207, 1224\}$,

la plus petite solution de ce type étant 18.

3.8. **Quotients de Fermat non nuls sur un intervalle – Exemples.** Un des aspects du problème de la finitude ou non des quotients de Fermat nuls est qu'il n'est pas rare de trouver des valeurs de a pour lesquelles $q_p(a) \ne 0$ sur un intervalle $p \in [2, x[$ où x est de l'ordre de 10^{10}, ce qui accrédite la finitude.

Or s'il existe effectivement des a tels que $q_p(a) \ne 0$ pour tout p, un tel cas de finitude (triviale) pour $q_p(a) = 0$ pourrait vouloir dire que tous les entiers $a \in \mathbb{N}\setminus\{0, 1\}$ ont un nombre fini de quotients de Fermat nuls, une heuristique naturelle étant que l'on ne peut avoir deux catégories de nombres fondamentalement différentes.

On abordera cette existence au Théorème 4.13 par le calcul effectif, de type "théorème chinois" (cf. Remarque 3.13 précédente), de la densité des $A \in \mathbb{N}$ tels que $q_p(A) \neq 0$ pour tout $p \leq x$.

Pour $2 \leq a \leq 100$ on trouve les exemples suivants (le cas $p = 2$ éliminant tous les $a \equiv 1 \pmod 4$, $p = 3$ éliminant tous les $a \equiv 1, 8 \pmod 9$, etc.) :

Pour $a = 34$ la première solution est $p = 46145917691$.

Pour $a = 66$, la première solution est $p = 89351671$.

Pour $a = 88$, la première solution est $p = 2535619637$.

Pour $a = 90$, la première solution est $p = 6590291053$.

Pour $a = 47$ et $a = 72$ on ne trouve aucune solution pour $p \leq 10^{11}$.

Dans [8] on trouve les grandes solutions $p \leq 10^{11}$ suivantes, pour $a \in [2, 101]$:

$(a, p) = (5, 6692367337),\ (23, 15546404183),\ (37, 76407520781),\ (97, 76704103313),$

et la solution remarquable $(5, 188748146801)$, ce qui semble indiquer que la finitude éventuelle des $q_p(a) = 0$ n'implique pas nécessairement l'existence d'une borne, pour p, fonction de a.

4. Seconde analyse probabiliste pour $q_p(a) = 0$

L'approche précédente (Section 3), reposant sur des "estimations de densités" relativement à la variable entière $A \in \mathbb{N}$, ne tient pas compte du fait que l'on étudie $q_p(a)$ pour a fixé "petit" et p variable arbitrairement grand. Or, comme on l'a vu, le simple fait que $q_p(a) = 0$ pour $p \gg a$ entraîne de nombreuses solutions dans $[2, p-1[$ puisque $q_p(a^j) = 0$ avec $a^j \in [2, p-1[$ pour $1 \leq j \leq h_p(a) := \lfloor \frac{\log(p)}{\log(a)} \rfloor$ (partie entière). D'où la nécessité d'une première étude sur l'intervalle $[2, p-1[$, étude qui ne dépend alors que de p.

4.1. **Etude des solutions à $q_p(z) = 0$ dans l'intervalle $[2, p-1[$.** Dans cette partie nous allons essayer de justifier l'existence d'une loi de probabilité classique en utilisant un certain nombre d'arguments théoriques et des calculs numériques. En particulier, un résultat de R. Heath-Brown (cf. [7], Theorem 1 & Corollary, p. 2) affirme que les $q_p(z)$, $z \in [1, p[$, sont uniformément répartis modulo p et que les z^p, $z \in [1, p[$, sont uniformément répartis modulo p^2 (cf. Remarque 3.7, (iii)).

4.1.1. *Retour sur l'aspect densités vs probabilités.* Soit p un nombre premier fixé. Pour chaque $z \in [1, p[$ il existe un unique $\lambda(z) \in [0, p[$ tel que $Z := z + \lambda(z)\, p$ vérifie $q_p(Z) = 0$ (on a alors $\lambda(z) \equiv z\, q_p(z) \pmod p$ et $Z \equiv z^p \pmod{p^2}$), d'où la densité des $A \in \mathbb{N} \setminus p\mathbb{N}$ tels que $q_p(A) = 0$ (pour p fixé), égale à $\frac{1}{p}$. Ceci a été vu § 3.5 où le Lemme 3.6 implique que la densité des $A \in \mathbb{N} \setminus p\mathbb{N}$ tels que $q_p(A) = u$ est aussi égale à $\frac{1}{p}$, quel que soit $u \in [0, p[$.

Autrement dit, si l'on fixe provisoirement p, pour $Z \in [1, p^2[$ la probabilité d'avoir $q_p(Z) = 0$ devient exactement la densité $\frac{1}{p}$. Par contre, la même étude dans $[1, p[$ est plus délicate ; elle doit conduire normalement à des probabilités inférieures à la densité $\frac{1}{p}$ mais majorantes de $\mathrm{Prob}\big(q_p(a) = 0\big)$ pour a fixé, $a \ll p$.

Remarques 4.1. (i) Si a est fixé et si $p \gg a$ est tel que $q_p(a) = 0$, on assiste à des "répétitions" dans $[2, p-1[$ puisque $q_p(a^j) = 0$ pour $j = 1, \ldots, h_p(a)$ (aspect qui

sera analysé de façon plus complète dans le § 4.2 où l'on recherchera les $z \in [2, p-1[$ ayant même quotient de Fermat $u \in [0, p[$).

(ii) Plus généralement, lorsque $z \in [2, p-1[$, $z \ll p$, est tel que $q_p(z) = 0$, on a un certain nombre de puissances de z solutions dans $[2, p-1[$, mais on peut supposer que ce phénomène est limité par le fait que pour l'élément canonique $Z = z + \lambda(z)\, p \in [2, p^2 - 1[$, $q_p(Z) = 0$ est d'autant moins probable car si $Z = z$ (i.e., $\lambda(z) = 0$), le nombre de solutions au total dans $[1, p^2[$ est toujours $p-1$ et on a vu que les solutions du type Z sont uniformément réparties modulo p^2 (les cas $z = 1$ et $z = p-1$ introduisent un biais négligeable et on supposera $2 \leq z \leq p-2$).

Par exemple, pour $p = 11$ on a $q_p(Z) = 0$ pour $Z = z = 3, 9 \in [2, p-1[$ et pour $Z = 27, 40, 81, 94, 112, 118, 120 \in]p, p^2[$.

Ceci peut justifier l'existence d'une loi binomiale (cf. Heuristique 4.5 et Remarques 4.7). Comme il y a $p-1$ solutions $Z \in [1, p^2[$, on peut s'attendre en moyenne à une solution $Z = z \in [1, p[$ et à $p-2$ solutions $Z \in [p+1, p^2[$.

Si l'on se base sur l'existence d'une loi de probabilité telle que $\mathrm{Prob}\big(q_p(z) = 0\big) < \frac{1}{p}$ (à comparer à $\mathrm{Prob}\big(q_p(Z) = 0\big) = \frac{1}{p}$ pour $Z \in [2, p^2 - 1[$), on est fondé à énnoncer l'heuristique suivante qui semble légitime au vu du faible nombre moyen de solutions pour chaque p (au plus quelques unités quelle que soit la taille de p et en général zéro ou une solution, cf. § 4.1.2) et des résultats de [7] :

Heuristique 4.2. *Les $p-3$ nombres $Z = z + \lambda(z)\, p \equiv z^p \pmod{p^2}$, $z \in [2, p-1[$, $\lambda(z) \in [0, p[$, tels que $q_p(Z) = 0$, sont aléatoires et indépendants dans $[2, p^2 - 1[$.*

De même que pour les valeurs de $q_p(z)$, non toutes réalisées dans $[0, p[$ (cf. § 3.1), les nombres $\lambda(z) \in [0, p[$ tels que $q_p(z + \lambda(z)\, p) = 0$ ne sont pas tous atteints (il y a aussi environ $\frac{1}{3}$ des valeurs dans ce cas), ce qui est compatible avec le fait que en moyenne $\mathrm{Prob}\big(\lambda(z) = v\big) < \frac{1}{p}$ pour $v \in [0, p[$ (pour $p = 11$, les $v = 1, 4, 5, 6, 9$ ne sont pas atteints).

4.1.2. *Recherche numérique des solutions $z \in [2, p-1[$.* Pour de grandes valeurs de p, on obtient peu (ou pas) de solutions comme attendu ($d = o_p(z)$) :

$$
\begin{aligned}
&p = 10000019\\
&p = 10000079\\
&\qquad\qquad z_1 = 6828481, \quad d = 909098,\\
&\qquad\qquad z_1 = 9659873, \quad d = 5000039,\\
&p = 10000103\\
&\qquad\qquad z_1 = 4578211, \quad d = 386,\\
&\qquad\qquad z_1 = 4215058, \quad d = 10000102,\\
&\qquad\qquad z_2 = 4732368, \quad d = 10000102,\\
&\qquad\qquad z_3 = 8804922, \quad d = 10000102,\\
&p = 10000121\\
&\qquad\qquad z_1 = 1778643, \quad d = 10000120,\\
&\qquad\qquad z_1 = 3601025, \quad d = 5000060,\\
&p = 10000139
\end{aligned}
$$

Pour $p = 1110000127$ (pris au hasard), il y a l'unique solution $z = 723668846$; le nombre premier suivant, $p = 1110000149$, donne 0 solutions dans $[2, p-1[$.

Ceci est assez analogue au cas des petits nombres premiers (nous omettons les $p = 2, 3, 5, 7, 13, 17, 19, 23, 31, 41$ ne conduisant à aucune solution dans $[2, p-1[$) :

$p = 11$ ($z_1 = 3,\ d = 5;\ z_2 = 9,\ d = 5$) ; $p = 29$ ($z_1 = 14,\ d = 28$) ; $p = 37$ ($z_1 = 18,\ d = 36$) ; $p = 43$ ($z_1 = 19,\ d = 42$).

D'après [7], les solutions $z \in [1, p[$ à $q_p(z) = 0$ sont uniformément réparties comme on peut le vérifier numériquement par des comptages cumulés sur les $p \leq x$ en selectionnant des intervalles de longueurs $\frac{p-1}{t}$ où t est un paramètre ajustable.

On note aussi le phénomène suivant. On calcule (sachant que $\lambda(z)+\lambda(p-z) = p-1$, cf. § 3.7) les quantités $\sigma_n(p) := \frac{2\,(n+1)}{(p-1)^{n+1}} \sum_{z=1}^{(p-1)/2} \lambda(z)^n$, pour tout $n \geq 1$, où par définition $\lambda(z)$ est tel que $q_p(z + \lambda(z)\,p) = 0$. On obtient alors une remarquable convergence alternée vers 1 :

$$\begin{aligned} p &= 10001009 & \sigma_{11}(p) &\approx 1.0000467 \\ p &= 10002007 & \sigma_{11}(p) &\approx 1.0013552 \\ p &= 10003001 & \sigma_{11}(p) &\approx 1.0003688 \\ p &= 10004017 & \sigma_{11}(p) &\approx 0.9996190 \\ p &= 10005007 & \sigma_{11}(p) &\approx 0.9987657. \end{aligned}$$

4.1.3. *Classement des nombres premiers p par nombre de solutions* $z \in [2, p-1[$. Le programme suivant (d'exécution assez longue) calcule les proportions de nombres premiers p pour lesquels on a exactement 0, 1, ou 2 solutions, puis lorsque l'on a au moins 3 solutions $z \in [2, p-1[$ telles que $q_p(z) = 0$: [2]

$\{N0 = 0; N1 = 0; N2 = 0; N3 = 0; B = 2 * 10^5; H = 2 * 10^3; p = H; N = 0.0;$
$while(p < H + B, p = nextprime(p + 2); N = N + 1; p2 = p^2; Np = 0;$
$for(z = 2, p - 1, Q = Mod(z, p2)^{(p-1)} - 1; if(Q == 0, Np = Np + 1));$
$if(Np == 0, N0 = N0 + 1); if(Np == 1, N1 = N1 + 1); if(Np == 2, N2 = N2 + 1);$
$if(Np >= 3, N3 = N3 + 1)); print(N0/N, "", exp(-1)); print(N1/N, "", 1 - exp(-1));$
$print(N2/N, "", 1 - 2 * exp(-1)); print(N3/N, "", 1 - 5/2 * exp(-1))\}$

Comme les probabilités indiquées sont d'abord pour 0 solutions, puis pour au moins 1 solution, 2 solutions, 3 solutions, on doit cumuler les nombres de solutions N_1, N_2, N_3 donnés par le programme (naturellement, $N_0 + N_1 + N_2 + N_3 = N$) :

$$\begin{aligned} &\text{cas de 0 solutions :} && \frac{N_0}{N} = 0.3694945\ ; && \text{probabilité} \approx 0.3678794. \\ &\text{au moins 1 solution :} && \frac{N_1 + N_2 + N_3}{N} = 0.6305054\ ; && \text{probabilité} \approx 0.6321205. \\ &\text{au moins 2 solutions :} && \frac{N_2 + N_3}{N} = 0.2646531\ ; && \text{probabilité} \approx 0.2642411. \\ &\text{au moins 3 solutions :} && \frac{N_3}{N} = 0.0805782\ ; && \text{probabilité} \approx 0.0803014. \end{aligned}$$

Dans ce cas, les résultats numériques sont remarquablement cohérents avec la répartition probabiliste que nous allons préciser au § 4.4.

Pour les nombres premiers de l'intervalle $]2.10^3, 2\,(10^3+10^5)[$, il y a 17866 solutions cumulées pour 17845 nombres premiers (une solution en moyenne comme prévu).

4.1.4. *Commentaires au sujet des solutions "exceptionnelles".* Dès que $q_p(a) = 0$ pour $a \ll p$, plusieurs puissances de a fournissent des solutions $z \in [2, p-1[$, solutions exceptionnelles mais non supplémentaires comme il a été mentionné puisqu'en termes de solutions dans $[1, p^2[$, on trouvera toujours $p-1$ solutions $Z = z+\lambda(z)\,p$ à $q_p(Z) = 0$, dont les précédentes, et en un sens on peut considérer qu'il ne s'agit que

[2] Dans tous les programmes PARI [11] proposés, la compatibilité avec TeX oblige à écrire les symboles *par*, & avec un antislash, à placer des *$* et des { } pour les exposants... Sous réserve d'éliminer ces symboles, le fichier tex permet de copier-coller ces programmes.

d'une question de répartition et non d'une dépendance probabiliste. Pour $p = 3511$, on a les solutions $2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048 < p-1$. Pour $p = 40487$, on a les solutions $5, 25, 125, 625, 3125, 15625 < p-1$; comme 4492 est aussi une "petite" solution, on obtient la solution $5 \cdot 4492 = 22460 < p-1$, etc.

De fait le côté "automatique" conduisant à $q_p(a^j) = 0$ pour tout $a^j < p-1$ se rencontre pour d'autres valeurs du quotient de Fermat comme nous allons le vérifier plus systématiquement dans le § 4.2 ; par exemple, pour $p = 59$, on a $q_p(z) = 38$ pour $z = 13, 22, 35, 57$; ce phénomène est d'ailleurs nécessaire puisqu'on sait que beaucoup de valeurs de $q_p(z)$ ne sont pas atteintes (cf. § 3.1).

Remarque 4.3. Ce type d'événement (appelé répétitions) se produit a priori avec la même (faible) probabilité, et on peut analyser ce qui précède de la façon suivante : soit $a \geq 2$ fixé étranger à p, d'ordre d, et soit $a_j \in [2, p-1[$ le résidu modulo p de a^j, $j = 1, \ldots, d-1$; posons $a^j\, a_j^{-1} \equiv 1 + \theta_j\, p \pmod{p^2}$, $\theta_j \in [0, p[$, alors on obtient $q_p(a_j) \equiv j\, q_p(a) + \theta_j \pmod{p}$.

Autrement dit, quel que soit j, le quotient de Fermat de a_j dépend de celui de a au moyen d'une formule canonique, le cas $q_p(a) = 0$ & $\theta_j = 0$ pour tout $a^j < p-1$, n'étant qu'un cas particulier de cette formule.

On peut aussi faire le même genre d'étude sur l'entier $\lambda(z) \in [0, p[$ en donnant la répartition des valeurs de $\lambda(z)$, $z \in [2, p-1[$, et celle du nombre de solutions à $\lambda(z) = v$, v donné ou pris au hasard, sachant que le résultat de [7] donne aussi leur répartition uniforme ; pour $10^3 \leq p \leq 10^3 + 10^4$ il y a 1168 nombres premiers, et on a retenu le nombre K de cas pour lesquels il y a au moins 4 solutions :

En prenant d'abord $v = 0, \ldots, 9$, on obtient $(v, K) = (0, 24)$, $(1, 21)$, $(2, 26)$, $(3, 17)$, $(4, 20)$, $(5, 33)$, $(6, 25)$, $(7, 21)$, $(8, 22)$, $(9, 21)$.

Pour une autre tranche de valeurs de v, on obtient $(v, K) = (123, 21)$, $(124, 11)$, $(125, 27)$, $(126, 23)$, $(127, 32)$, $(128, 19)$, $(129, 17)$, $(130, 21)$, $(131, 18)$, $(132, 21)$.

Dans tous les essais effectués, $v = 0$ ne semble pas jouer un rôle particulier.

La moyenne cumulée observée pour le nombre K est de 22 ; or $\frac{22}{1168} \approx 0.0188356$, et la probabilité que nous définirons pour "au moins 4 solutions à $\lambda(z) = v$" est égale à 0.0189 (cf. Remarque 4.7, (iv)), ce qui constitue une vérification remarquable des arguments précédents. Une expérimentation utilisant la fonction *random* pour $v \in [0, 10^4[$, pour une tranche de 984 nombres premiers $p > 2 \cdot 10^4$, conduit à la valeur 0.019268.

Remarquons aussi que si par exemple $q_p(2)$ était nul pour une infinité de p, alors le nombre h de solutions dans $[2, p-1[$, dûes aux $a_j = 2^j$, tendrait vers l'infini pour une sous-suite de p, ce qui peut paraître excessif au regard de la répartition (i.e., de la densité) sur $[2, p^2-1[$ et du fait que les $q_p(z)$ sont uniformément répartis sur $[0, p[$ (cf. résultats numériques du § 4.1.2).

4.2. **Nombre de répétitions pour $q_p(z) = u$ – Définitions de $m_p(u)$ et de M_p.** Par analogie, un point de vue complémentaire consiste à rechercher, pour p donné, le nombre $m_p(u)$ de $z \in [2, p-1[$ ayant le même quotient de Fermat $u \in [0, p[$ fixé, puis le nombre $M_p = \sup_{u \in [0,p[} \big(m_p(u)\big)$. On obtient alors une stabilité remarquable pour M_p, fonction très régulière de p pouvant faire l'objet de l'heuristique suivante :

Heuristique 4.4. *Le nombre maximum* $M_p = \sup_{u\in[0,p[}\big(m_p(u)\big)$ *de valeurs de* $z \in [2, p-1[$ *ayant même p-quotient de Fermat est en* $O(\log(p))$ *pour tout nombre premier* $p \geq 2$.

Ceci veut dire que pour tout p il existe une ou plusieurs valeurs exceptionnelles $u \in [0, p[$ telles que $q_p(z) = u$ pour environ $O(\log(p))$ valeurs de z. Donnons quelques aspects numériques au moyen du programme suivant :

$\{B = 10^5; b = 300; M = 0.0; N = 0; S = 0.0;$
$p = B; while(p < B + b, p = nextprime(p + 2); p2 = p^2;$
$N = N + 1; S = S + log(p) + log(log(p)); L = listcreate(p);$
$for(k = 1, p, listinsert(L, 0, k));$
$for(a = 2, p - 1, Q = Mod(a, p2)^{(p-1)} - 1; q = component(Q, 2)/p;$
$q1 = q + 1; c = component(L, q1); listput(L, c + 1, q1));$
$m = 0; for(k1 = 1, p, z = component(L, k1);$
$if(z > m, m = z)); print(p, "", m); M = M + m); print("", (M + 0.0)/N, "", S/N, "", M/S)\}$

(α) *Cas des petits nombres premiers.* La régularité a lieu dès le début car on obtient les valeurs (p, M_p) suivantes pour les p tels que $2 \leq p \leq 100$:

$(2,0), (3,1), (5,2), (7,2), (11,2), (13,2), (17,3), (17,3), (17,3), (19,2), (23,3), (29,3), (31,2), (37,3),$
$(41,3), (43,2), (47,3), (53,3), (59,4), (61,4), (67,5), (71,3), (73,4), (79,3), (83,4), (89,4), (97,3).$

(β) *Cas des grands nombres premiers.* On a ensuite les valeurs (p, M_p) suivantes pour les p tels que $100003 \leq p \leq 100313$:

$(100003,7), (100019,7), (100043,8), (100049,9), (100057,8), (100069,7), (100103,8), (100109,8),$
$(100129,7), (100151,8), (100153,7), (100169,8), (100183,8), (100189,7), (100193,9), (100207,9),$
$(100213,8), (100237,8), (100267,8), (100271,7), (100279,7), (100291,8), (100297,8), (100313,8).$

Moyenne des M_p sur les $p \in [100003, 100313]$, égale à $M \approx 7.79$, moyenne des $\log(p)$ égale à $S \approx 13.96$, avec $M/S \approx 0.558$.

Dans la limite des possibilités d'exécution du programme (liste $L =$ listcreate(p) très longue) on obtient pour $p = 48543217$, $M_p = 10$, $\log(p) \approx 17.698$, et $M_p/\log(p) \approx 0.5650$ (qui semble se rapprocher de la constante d'Euler). Noter que $m_p(0) = 3$ pour cet exemple pris au hasard et que les autres $m_p(u)$ sont le plus souvent nuls ou du même ordre de grandeur que $m_p(0)$.

(γ) *Données numériques pour* $p = 100003$. Il est utile de voir quels sont les $u \in [0, p[$ et les $z \in [2, p-1[$ qui réalisent M_p-fois le même quotient de Fermat u.
Pour $p = 100003$ où $M_p = 7$, on obtient les résultats suivants :

$u_1 = 7504$ $\quad z_1 \in \{10670,\ 11850,\ 1700,\ 53108,\ 59887,\ 80486,\ 82613\}$
$u_2 = 9011$ $\quad z_2 \in \{4199,\ 26730,\ 3895,\ 69156,\ 71121,\ 87157,\ 88803\}$
$u_3 = 13940$ $\quad z_3 \in \{646,\ 13662,\ 26364,\ 41841,\ 46741,\ 64523,\ 79877\}$
$u_4 = 79026$ $\quad z_4 \in \{26892,\ 38196,\ 54518,\ 58955,\ 62398,\ 78928,\ 80081\}$
$u_5 = 91190$ $\quad z_5 \in \{3551,\ 9604,\ 15491,\ 20035,\ 63185,\ 80223,\ 82748\}.$

On constate que les valeurs de z ne sont pas spécialement du type "a fixé petit", mais que $M_p = 7$ est réalisé par cinq valeurs de u.

(δ) *Cas des solutions exceptionnelles* $a \ll p$ *avec* $q_p(a) = 0$. Le cas $a = 2$, lorsque $q_p(a) = 0$ pour $p = 1093$, est à peine particulier et conduit par exemple à la série de valeurs suivantes pour (p, M_p) $(1039 \leq p \leq 1163)$:

$(1039,7), (1049,5), (1051,5), (1061,5), (1063,5), (1069,5), (1087,5), (1091,5), (1093,11),$
$(1097,7), (1103,7), (1109,6), (1117,5), (1123,5), (1129,5), (1151,5), (1153,6), (1163,6).$

Pour $p = 1093$, on obtient $M_p = 11$, or on a seulement $h_p(2) = 10$ et $m_p(0) = 10$. Le plus remarquable est que la valeur $q_p(z) = 624$ se produit 11 fois, à savoir pour $z = 9, 18, 36, 71, 72, 142, 144, 284, 288, 568, 576$, et que la valeur $q_p(z) = 960$ se produit aussi 11 fois, pour $z = 13, 26, 52, 93, 104, 186, 208, 372, 416, 744, 832$. On a donc $M_p = m_p(624) = m_p(960) = 11$. Il est clair que $z = 2$ influe en partie sur ces résultats.

Pour $a = 3$, $p = 1006003$, $q_p(a) = 0$ et $h_p(3) = 12$; on a cependant $m_p(u) = 16$ pour $u = 56450, 1004048$, et $M_p = m_p(u) = 17$ pour $u = 297548$; dans ce dernier cas, les valeurs de z qui réalisent $q_p(z) = 297548$, $z \in [2, 1006003[$, sont :

3389, 8102, 10167, 24306, 30501, 51550, 72918, 91503, 154650, 218754, 236000, 274509, 340292, 463950, 656262, 708000, 823527.

Autrement dit, il ne semble pas que le phénomène des petites valeurs de a telles que $q_p(a) = 0$ soit une obstruction à l'existence d'une loi de probabilité puisque les répétitions des quotients de Fermat se produisent avec une grande régularité compatible avec l'Heuristique 4.4.

4.3. **Etude numérique de $m_p(0)$(répétitions de $q_p(z) = 0$, $z \in [2, p-1[$).** Ici, nous imposons la valeur $u = 0$ pour l'étude des répétitions ; donc $m_p(0) \leq M_p$ et a priori, si l'on se restreint aux nombres premiers p tels que $m_p(0) = O(\log(p))$ (i.e., $m_p(0) \approx M_p$), il y a une très importante raréfaction des solutions p. Le résultat pour $u \in \mathbb{N}$ est semblable (à condition de prendre des $p > u$).

4.3.1. *Recherche des $m_p(0)$ en $O(\log(p))$.* Nous allons constater que, en dehors des cas exceptionnels du type $a = 2$, $p = 1093, 3511$, donnant 10 et 11 quotients de Fermat $q_p(z) = 0$, $z \in [2, p-1[$, il existe des valeurs de p où le nombre $m_p(0)$ de répétitions $q_p(z) = 0$ est de l'ordre de $O(\log(p))$ sans que cela ne provienne d'un $a \ll p$ tel que $q_p(a) = 0$.

Les couples correspondants aux répétitions issues d'un $a \ll p$ sont omis et sont pour mémoire $(1093, 10)$, $(3511, 11)$, $(20771, 6)$, $(40487, 8)$, $(66161, 6)$.

Le tableau ci-dessous indique les couples $(p, m_p(0))$ pour un nombre de répétitions $m_p(0) \geq 6$, pour $2 \leq p \leq 2 \times 10^5$, ainsi que les $z \in [2, p-1[$ tels que $q_p(z) = 0$.

(5107, 6)	{560, 1209, 1779, 2621, 4295, 4361}
(51427, 6)	{10364, 14795, 26183, 28411, 34111, 39159}
(52517, 6)	{13425, 18243, 34196, 38462, 39362, 51787}
(61417, 6)	{12947, 15631, 17144, 20287, 41739, 51605}
(103291, 7)	{14866, 27419, 39660, 80408, 92041, 96106, 98404}
(116731, 6)	{5999, 21399, 32127, 61099, 69145, 115067}
(119359, 6)	{25627, 26486, 43165, 57879, 78988, 98633}
(128657, 6)	{28237, 62334, 85135, 120099, 123891, 125137}
(140741, 6)	{44757, 53828, 63099, 107890, 133072, 137002}
(147647, 6)	{198, 39204, 75352, 90252, 98878, 141188}
(150559, 6)	{22349, 34314, 34578, 40446, 67349, 102255}
(199783, 6)	{29626, 61730, 78104, 106439, 124919, 178644}

En continuant ce tableau jusqu'à $p \approx 5 \cdot 10^5$, on obtient les quinze nombres premiers suivants :

203773, 213949, 229939, 237283, 261761, 286751, 288929, 303089,
339139, 342373, 381853, 384611, 385657, 475897, 491531,

pour lesquels on a tout le temps $m_p(0) = 6$ sauf pour $p = 491531$ où $m_p(0) = 7$ (mais dans ce cas, les valeurs de z telles que $q_p(z) = 0$ sont données par six puissances de $a = 7$ et $397783 = 17 \times 23399$) et $M_p = 11$.

4.3.2. *Comparaison des probabilités* $\mathrm{Prob}\big(m_p(0) \geq n\big)$ *et* $\mathrm{Prob}\big(q_p(a') = 0\big)$. On observe une raréfaction des cas issus d'un $a \ll p$. En utilisant la probabilité donnée plus loin dans la Remarque 4.7, (i), on trouve que pour $p \approx 5 \cdot 10^5$ la probabilité d'au moins 6 répétitions $z \in [2, p-1[$ à $q_p(z) = 0$ est égale à $0.000594 \approx \frac{1}{p^{1+\epsilon}}$ avec $\epsilon \approx -0.433916$, ce qui en termes de solutions exceptionnelles provenant d'un $a' \ll p$ (a' fictif) donnerait, pour $h_p(a') = 6$, une valeur de a' égale à 7 ou 8 en moyenne, qui doit être considérée comme "déjà trop grande" ; en effet, on a pour $p \approx 5 \cdot 10^5$ (e.g. $p = 500009$ qui ne sert que d'ordre de grandeur puisque dans ce cas, $m_p(0) = 0$ et $M_p = 9$) :

$h_p(2) = 18$, $h_p(3) = 11$, $h_p(4) = 9$, $h_p(5) = 8$, $h_p(6) = 7$,

$h_p(7) = 6$, $h_p(8) = 6$, $h_p(9) = 5$, etc.

Pour $h_p(a') = 6$ on peut prendre $a' \in \{7, 8\}$.

Autrement dit, le phénomène d'au moins 6 répétitions indifférenciées $q_p(z) = 0$, $z \in [2, p-1[$ (i.e., $m_p(0) \geq 6$), est plus probable dans la mesure où il correspondrait à un a' moyen, non "très petit par rapport à p" (probablement en $O(\log(p))$) ; si l'on écrit les probabilités sous la forme $\mathrm{Prob}\big(q_p(a') = 0\big) = \frac{1}{p^{1+\epsilon}}$ (sous l'hypothèse $m_p(0) \geq 6$), on obtient (pour $p \approx 5 \cdot 10^5$), le tableau suivant :

$a' = 2$, $\epsilon = 1.845$; $a' = 3$, $\epsilon = 0.403$; $a' = 4$, $\epsilon = 0.044$; $a' = 5$, $\epsilon = -0.124$;

$a' = 6$, $\epsilon = -0.284$; $a' = 7$, $\epsilon = -0.434$; $a' = 8$, $\epsilon = -0.434$; $a' = 9$, $\epsilon = -0.572$;

Pour a' assez grand, le ϵ est légèrement négatif, donnant une probabilité supérieure à $\frac{1}{p}$. En decroissant vers $a' = 4$, on commence à obtenir une probabilité inférieure à $\frac{1}{p}$. Quant à $a' = 2$, on obtient une probabilité de la forme $\frac{1}{p^{1+\epsilon}}$ avec $\epsilon \approx 1.845$. Pour $2 \leq a' \leq 4$ on a $9.465 \leq \frac{\log(p)}{\log(a')} \leq 18.931$.

La probabilité $\mathrm{Prob}\big(m_p(0) \geq n\big)$ est supérieure à celle qui proviendrait d'une solution exceptionnelle $a \ll p$ (pour $n = h_p(a)$) et inférieure à celle donnée dans l'Heuristique 3.10.

4.4. **Existence d'une loi de probabilité binomiale pour** $m_p(0)$**.** L'étude précédente conduit à une heuristique utilisant une loi binomiale de paramètres $\big(p-3, \frac{1}{p}\big)$, car on peut considérer que l'on réalise les $p-3$ "tirages" $z \in [2, p-1[$ pour lesquels on regarde combien de fois on obtient l'événement $q_p(z) = 0$ (ou plus généralement $q_p(z) = u$, $u \in [0, p[$, si l'on prend en compte les résultats du § 4.2).

D'après le Lemme 3.6, si $z \in [2, p-1[$ et si $Z = z + \lambda_u(z)\, p \in [2, p^2 - 1[$ est tel que $q_p(Z) = u$, on a les identités $\lambda_u(z) \equiv z\,(q_p(z) - u) \pmod p$ et $Z \equiv z^p - z u\, p \pmod{p^2}$, auquel cas $q_p(z) = u$ si et seulement si $\lambda_u(z) = 0$.

Le paramètre $\frac{1}{p}$ est une approximation de $\mathrm{Prob}\big(q_p(z) = u\big)$ ou de $\mathrm{Prob}\big(\lambda_u(z) = 0\big)$. Cette approximation pour le second paramètre $\frac{1}{p}$ a une incidence négligeable car on est dans une situation de type "densité".

La probabilité d'avoir exactement n cas favorables $z \in [2, p-1[$ est donc :

$$\tbinom{p-3}{n} \frac{1}{p^n} \Big(1 - \frac{1}{p}\Big)^{p-3-n} = \tbinom{p-3}{n} \frac{1}{p^{p-3}} (p-1)^{p-3-n}.$$

Heuristique 4.5. *Soit $u \in [0,p[$. Soit $z \in [2,p-1[$ et soit $Z = z + \lambda_u(z)\,p \in [2,p^2-1[$ tel que $q_p(Z) = u$. Soit $n \in [0,p-2[$; alors la probabilité d'avoir au moins n valeurs $z_1,\dots,z_n \in [2,p-1[$ telles que $q_p(z_j) = u$ (équivalent à $\lambda_u(z_j) = 0$), pour $j = 1,\dots,n$, est donnée par l'expression suivante :*

$$\mathrm{Prob}\Big(\Big|\Big\{z \in [2,p-1[,\ q_p(z) = u\Big\}\Big| \geq n\Big) = \frac{1}{p^{p-3}} \sum_{j=n}^{p-3} \tbinom{p-3}{j} (p-1)^{p-3-j}.$$

Lemme 4.6. *On a pour tout n la majoration $\frac{1}{p^{p-3}} \sum_{j=n}^{p-3} \binom{p-3}{j}(p-1)^{p-3-j} < \frac{1}{p^n}\binom{p-3}{n}$.*

Démonstration. On considère, pour $0 \leq n \leq N$, $t \in [1,\infty[$, la dérivée de la fonction $f_{N,n}(t) = \sum_{j=n}^{N} \binom{N}{j}(t-1)^{N-j} - \binom{N}{n} t^{N-n}$; elle est égale à $N f_{N-1,n}(t)$. On raisonne ensuite par récurrence, à partir de $f_{n,n}(t) = 0$ et de $f_{N,n}(1) < 0$, pour montrer que la dérivée est négative ou nulle sur tout l'intervalle $[1,\infty[$. On aura ensuite à poser $t = p$, $N = p-3$. □

Remarques 4.7. (i) On a, pour les petites valeur de n, la formule plus commode :

$$\mathrm{Prob}\Big(\Big|\Big\{z \in [2,p-1[,\ q_p(z) = u\Big\}\Big| \geq n\Big) = 1 - \Big(1-\frac{1}{p}\Big)^p \Big(\frac{p}{p-1}\Big)^3 \sum_{j=0}^{n-1} \frac{\binom{p-3}{j}}{(p-1)^j}.$$

(ii) La probabilité d'avoir 0 solutions est $\big(1-\frac{1}{p}\big)^p \big(\frac{p}{p-1}\big)^3 \approx 0.3678$.

(iii) La probabilité pour au moins une solution $z \in [2,p-1[$ est $1 - \big(1-\frac{1}{p}\big)^p \big(\frac{p}{p-1}\big)^3$ qui est rapidement proche de $1 - e^{-1}\big(\frac{p}{p-1}\big)^3$ donc de $1 - e^{-1} \approx 0.63212$.

(iv) Pour au moins 2 solutions, la probabilité est proche de $1 - 2\,e^{-1}\big(\frac{p}{p-1}\big)^3 \approx 0.264$; pour au moins 3 (resp. 4) solutions, on obtient 0.0803 (resp. 0.0189).

4.4.1. *Application à l'étude de la probabilité de nullité de $q_p(a)$.* A partir de maintenant nous nous limitons au cas $u = 0$ et a fixé "petit" par rapport à p.

Pour $a \ll p$, $\mathrm{Prob}\big(q_p(a) = 0\big)$ est majorée par $\mathrm{Prob}\big(m_p(0) \geq h\big)$, où $m_p(0)$ est le nombre de solutions $z \in [2,p-1[$ et $h := h_p(a) = \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$, puisque $a,\dots,a^h \in [2,p-1[$ sont h solutions distinctes. Or, lorsque $p \to \infty$, le rapport (majoré par 1) :

$$\frac{\mathrm{Prob}\Big(\Big|\Big\{z \in [2,p-1[,\ q_p(z) = 0\Big\}\Big| \geq h\Big)}{p^{-h}\binom{p-3}{h}}$$

tend vers une constante $C_\infty(a)$, en décroissant, selon le résultat suivant :

Lemme 4.8. *(i) On a pour tout p assez grand l'encadrement (cf. Lemme 4.6) :*

$$\exp\big(-1 + \tfrac{1}{p}(h+\tfrac{5}{2})\big) < \frac{p^{-(p-3)} \sum_{j=h}^{p-3} \binom{p-3}{j}(p-1)^{p-3-j}}{p^{-h}\binom{p-3}{h}} \leq 1.$$

(ii) Il en résulte que pour a fixé on a $\mathrm{Prob}\big(q_p(a) = 0\big) \approx C_\infty(a) \times \frac{1}{p^h}\binom{p-3}{h}$ pour tout p assez grand, où $C_\infty(a)$ est comprise entre $e^{-1} \approx 0.36788$ et 1.

Démonstration. On a la minoration $\quad \frac{p^h}{\binom{p-3}{h}} \times \frac{1}{p^{p-3}} \sum_{j=h}^{p-3} \binom{p-3}{j}(p-1)^{p-3-j}$

$$= \Big(\frac{p-1}{p}\Big)^{p-3} \frac{p^h\,h!}{(p-2-h)\cdots(p-2-1)} \sum_{j=h}^{p-3} \frac{1}{j!} \frac{p-2-j}{p-1} \cdots \frac{p-2-1}{p-1}$$

$$= \Big(\frac{p-1}{p}\Big)^{p-3} \frac{p^h}{(p-1)^h} \sum_{j=h}^{p-3} \frac{h!}{j!} \frac{p-2-j}{p-2-h} \cdots \frac{p-2-1}{p-2-1} \times \frac{1}{(p-1)^{j-h}}$$

$$= \Big(\frac{p-1}{p}\Big)^{p-3-h} \Big[1 + \frac{p-2-(h+1)}{(p-1)(h+1)} + \cdots + \frac{p-2-(h+1)}{(p-1)(h+1)} \cdots \frac{p-2-j}{(p-1)\,j} + \cdots + \frac{p-2-(h+1)}{(p-1)(h+1)} \cdots \frac{p-2-(p-3)}{(p-1)(p-3)}\Big]$$

$$> \Big(\frac{p-1}{p}\Big)^{p-3-h} = \Big(1-\frac{1}{p}\Big)^{p-3-h}.$$

D'où facilement le résultat en considérant la minoration :

$$(p-3-h)\log\Big(1-\frac{1}{p}\Big) = -(p-3-h)\left(\frac{1}{p} + \frac{1}{2p^2} + \cdots\right) > -1 + \frac{1}{p}\Big(h + \frac{5}{2}\Big),$$

tous les termes négligés étant positifs et tendant rapidement vers 0. D'où (i).
Comme $\mathrm{Prob}\big(q_p(a)=0\big)$ est conditionnée à la probabilité d'avoir au moins h solutions, on écrira, par abus, $\mathrm{Prob}\big(q_p(a)=0\big) \approx C_\infty(a) \times \frac{1}{p^h}\binom{p-3}{h}$. □

Pour $p \approx 5 * 10^3$, $a=2$, $h=12$, on obtient les valeurs très proches :

$$\exp(-1) = 0.3678794411 < \exp(-1+(h+5/2)/p) = 0.3689478399 <$$
$$(1-1/p)^{p-3-h} = 0.3689479457 < \mathrm{Prob}\big(m_p(0) \geq h\big) = 0.3994073115 < 1.$$

La quantité $\frac{1}{p^h}\binom{p-3}{h}$ majore $\mathrm{Prob}\big(q_p(a)=0\big)$. On obtiendra, au niveau de la preuve du Lemme 4.10, que cette majoration est en $O\Big(\frac{1}{p^{\log_2(p)/\log(a)}}\Big)$.

Exemple 4.9. *Donnons, sous les heuristiques précédentes, des calculs exacts de probabilités d'avoir au moins $h_p(a) = \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$ solutions, avec $a=2$ pour p croissant ; ceci correspondrait au cas où le quotient de Fermat de a serait nul pour une infinité de p et il convient de voir que c'est numériquement peu compatible.*
On écrit alors cette probabilité sous la forme $\frac{1}{p^{1+\epsilon}}$:

$p = 101$	*probabilité* $= 4.557 \times 10^{-4}$	$\epsilon = 0.667$
$p = 127$	*probabilité* $= 4.819 \times 10^{-4}$	$\epsilon = 0.576$
$p = 10007$	*probabilité* $= 6.294 \times 10^{-11}$	$\epsilon = 1.550$
$p = 200003$	*probabilité* $= 1.094 \times 10^{-15}$	$\epsilon = 1.822$
$p = 1000003$	*probabilité* $= 3.182 \times 10^{-18}$	$\epsilon = 1.916$
$p = 5000011$	*probabilité* $= 3.421 \times 10^{-22}$	$\epsilon = 2.204.$

On confirmera dans la section suivante que cette probabilité est rapidement inférieure à $\frac{1}{p^2}$ et même que ϵ tend vers l'infini très lentement. Pour les petites valeurs de p, ϵ oscille autour de 1 et la dernière valeur de p pour laquelle $\epsilon < 1$ est $p = 1021$.

4.5. **Heuristique principale sur le nombre de p tels que $q_p(a) = 0$.** Soit maintenant $a \geq 2$ fixé. On rappelle les faits suivants :

(i) L'existence de $m_p(0)$ valeurs $z_j \in [2, p-1[$ telles que $q_p(z_j) = 0$ ne dépend que de p. Il n'est pas certain, lorsque $m_p(0) = O(\log(p))$, que ce soit dû à l'existence d'un $a \ll p$ tel que $q_p(a) = 0$ (cf. § 4.3). Cette dernière probabilité ($\{z_1, \ldots, z_{m_p(0)}\}$ contient a) est difficile à estimer, aussi nous l'avons majorée par 1.

(ii) On a obtenu, pour tout p assez grand, $\mathrm{Prob}\big(q_p(a)=0\big) \approx C_\infty(a) \times \frac{1}{p^h}\binom{p-3}{h}$, où $h := \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$ (cf. Lemme 4.8, (ii)).

(iii) Pour $p<a$, on a $h=0$ et $\frac{1}{p^h}\binom{p-3}{h}=1$; donc il est préférable, dans l'optique de l'étude de la sommation sur p, d'utiliser, pour ce nombre fini de p, la densité majorante $\sum_{d\,|\,p-1}\frac{\varphi(d)^2}{p\,(p-1)^2}$ étudiée Section 3.

Lemme 4.10. *Soit $a\geq 2$ fixé. La série $\sum\limits_{p>2}\ \frac{1}{p^h}\binom{p-3}{h}$, où $h:=h_p(a)=\lfloor\frac{\log(p)}{\log(a)}\rfloor$ (partie entière), est convergente.*

Démonstration. On a $\binom{p-3}{h}=\frac{1}{h!}\times(p-2-1)\cdots(p-2-h)$ que l'on peut majorer par $\frac{1}{h!}\times p^h$. En outre, on a par définition $\frac{\log(p)}{\log(a)}-1<h<\frac{\log(p)}{\log(a)}$. Pour tenir compte de ce fait, et afin d'utiliser analytiquement $\frac{\log(p)}{\log(a)}$ au lieu de h dans les formules, on utilise la majoration $\sum\limits_{p>2}\ \frac{\binom{p-3}{h}}{p^h}<\sum\limits_{p>2}\frac{h}{h!}$, où l'on a remplacé $\frac{1}{h!}$ par le majorant $1/\big(\frac{\log(p)}{\log(a)}-1\big)!=\frac{\log(p)}{\log(a)}/\big(\frac{\log(p)}{\log(a)}\big)!$, où h désigne maintenant $\frac{\log(p)}{\log(a)}$ et $\frac{h}{h!}=\frac{1}{\Gamma(h)}$.

On a $\frac{h!}{h}=\sqrt{2\pi}\times h^{h-\frac{1}{2}}\,e^{-h}\times(1+O(\frac{1}{h}))$, d'où en prenant le logarithme :

$$\begin{aligned}\log\Big(\frac{h!}{h}\Big)&=\log\big(\sqrt{2\pi}\big)+\Big(h-\frac{1}{2}\Big)\log(h)-h+\log\Big(1+O\big(\frac{1}{h}\big)\Big)\\&=h(\log(h)-1)-\frac{1}{2}\log(h)+O\big(\frac{1}{h}\big)+\log(\sqrt{2\pi})\\&=\frac{1}{\log(a)}\log(p)\Big(\log_2(p)-\log_2(a)-1\Big)\\&\qquad-\frac{1}{2}\Big(\log_2(p)-\log_2(a)\Big)+O\big(\frac{1}{\log(p)}\big)+\log(\sqrt{2\pi})\\&=\Big[\frac{1}{\log(a)}\Big(\log_2(p)-\log_2(a)-1\Big)\\&\qquad-\frac{1}{2}\frac{1}{\log(p)}\Big(\log_2(p)-\log_2(a)\Big)+O\big(\frac{1}{\log(p)}\big)\Big]\log(p)=:Y\times\log(p).\end{aligned}$$

D'où $\frac{h}{h!}=\frac{1}{p^Y}$ où Y tend vers l'infini comme $\frac{\log_2(p)}{\log(a)}$. Par conséquent, il existe une constante $C>1$ telle que Y est minorée par C pour tout $p\geq p_0$ assez grand et on peut écrire $\sum\limits_{p>2}\ \frac{\binom{p-3}{h}}{p^h}<C_0+\sum\limits_{p>p_0}\frac{1}{p^C}$, où C_0 est une constante égale à la sommation partielle jusqu'à p_0 ; d'où la convergence de la série initiale. □

Théorème 4.11. *Soit $a\geq 2$ fixé. Si l'Heuristique 4.5 est vraie (existence d'une loi de probabilité binomiale), alors il existe $C_\infty(a)$, $0.36788<C_\infty(a)\leq 1$ telle que $\mathrm{Prob}\big(q_p(a)=0\big)\approx C_\infty(a)\times\frac{\binom{p-3}{h}}{p^h}$ qui est majorée par un $O\Big(\frac{1}{p^{\log_2(p)/\log(a)}}\Big)$ pour tout p assez grand, où $h:=h_p(a)=\lfloor\frac{\log(p)}{\log(a)}\rfloor$, et dans le cadre admis du principe de Borel–Cantelli, le nombre de p tels que $q_p(a)=0$ est fini et majoré par la limite de la série $S:=s_0+\sum\limits_{p>a}\ \frac{\binom{p-3}{h}}{p^h}$, où $s_0\approx\sum\limits_{p<a}\ \sum\limits_{d\,|\,p-1}\frac{\varphi(d)^2}{p\,(p-1)^2}<\sum\limits_{p<a}\frac{1}{p}$.*

Remarques 4.12. (i) Les majorations utilisées pour le Lemme 4.10 sont assez grossières car, pour $a=2$, la série $\sum_{p>2}\frac{1}{p^h}\binom{p-3}{h}$ converge vers 0.9578... tandis que $\sum_{p>2}\frac{h}{h!}$ converge vers 6.2761...

(ii) Les résultats précédents restent analogues si l'on remplace h par tout entier de la forme $O(\log(p))$.

(iii) Le fait que l'on puisse choisir C arbitrairement grande dans la preuve du lemme (à condition de sommer à partir d'un p_0 assez grand) montrerait la raréfaction des solutions pour $p \to \infty$. Par exemple, si $a = 2$ et si l'on veut atteindre $C > 1$, il faut avoir $p_0 \geq 79$; pour $C > 2$, il faut $p_0 \geq 4259$. Pour $a = 3$, il faut respectivement $p_0 \geq 24527$ et $p_0 \geq 2669180065451$. Pour $a = 5$ et $C \approx 1.05$, $p_0 = 168116638259$ (peut-on y voir un rapport avec l'exemple $(5, 188748146801)$ donné au § 3.8 ?).
Ces résultats sont obtenus à partir de la série majorante $\sum_{p \geq p_0} \frac{h}{h!} \approx \sum_{p \geq p_0} \frac{1}{p^Y}$; donc les p_0 obtenus sont des majorants des bornes nécessaires pour avoir une série initiale convergente comme celle de terme général $\frac{1}{p^Y}$.

Ce Théorème 4.11 donne une version sans doute favorable du problème, mais il est assez bien vérifiée par l'expérimentation numérique. Le paragraphe suivant, qui utilise des résultats de densités, peut préciser cet aspect.

4.6. **Densité des entiers de p-quotients de Fermat non nuls.** D'après les résultats des §§ 2.3, 2.4, pour a fixé on est amené à étudier le produit infini formel $\widetilde{\mathcal{P}}(a) := \prod_{m \geq 1} \widetilde{\Phi}_m(a)$ qui est tel que tout nombre premier $p \nmid a$ en est un diviseur, à savoir $p \mid \widetilde{\Phi}_m(a)$ pour l'unique indice $m = o_p(a)$ (cf. Lemmes 2.5, 2.6), et qui est tel que $q_p(a) \neq 0$ si et seulement si p^2 ne divise pas $\widetilde{\mathcal{P}}(a)$.
Comme $p \mid \widetilde{\mathcal{P}}(A)$ équivaut à la condition $p \nmid A$ & $p \mid \widetilde{\Phi}_{o_p(A)}(A)$, la densité des $A \in \mathbb{N}$ tels que $p^2 \mid \widetilde{\mathcal{P}}(A)$ est égale à $\frac{\varphi(o_p(A))}{p^2}$; en sommant sur tous les ordres $o_p(A)$ possibles (diviseurs de $p-1$), on obtient la densité $\frac{p-1}{p^2}$; la densité contraire ($p^2 \nmid \widetilde{\mathcal{P}}(A)$) est égale à $D_p := 1 - \frac{p-1}{p^2} = 1 - \frac{1}{p} + \frac{1}{p^2}$.

On note que ces p-densités sont indépendantes (en raison des propriétés des $\widetilde{\Phi}_m(A)$) et que la densité correspondant à plusieurs p est donnée par le produit des densités locales (voir ci-dessous la Remarque 4.14). Il convient donc d'étudier le produit $\prod\limits_{p \leq x} D_p$ qui donne la densité des $A \in \mathbb{N}$ tels que $p^2 \nmid \widetilde{\mathcal{P}}(A)$ pour tout $p \leq x$.
Ecrivons $1 - \frac{1}{p} + \frac{1}{p^2} = \Big(1 - \frac{1}{p}\Big)\Big(1 + \frac{1}{p(p-1)}\Big)$. On a :

$$\prod_{p \leq x} \Big(1 - \frac{1}{p}\Big) = \frac{e^{-\gamma}}{\log(x)} \times \Big(1 + O\big(\tfrac{1}{\log(x)}\big)\Big),$$

où $\gamma \approx 0,577215$ est la constante d'Euler (cf. [14], § I.1.6, formule de Mertens), et $\prod\limits_{p \leq x} \Big(1 + \frac{1}{p(p-1)}\Big) \approx 1.9436$, pour x assez grand, d'où :

$$\prod_{p \leq x} D_p = \frac{1.9436 \times e^{-\gamma}}{\log(x)} \times \Big(1 + O\big(\tfrac{1}{\log(x)}\big)\Big) = \frac{1.09125}{\log(x)} \times \Big(1 + O\big(\tfrac{1}{\log(x)}\big)\Big).$$

On a donc le résultat analytique suivant :

Théorème 4.13. *La densité des $A \in \mathbb{N} \setminus \{0\}$ satisfaisant aux propriétés locales : "$q_p(A) \neq 0$ pour tout premier $p \leq x$", est de l'ordre de $O\Big(\frac{1}{\log(x)}\Big)$. De façon précise, pour x assez grand on a :*

$$\lim_{y \to \infty} \frac{1}{y} \Big|\big\{A \leq y, \quad q_p(A) \neq 0, \ \forall p \leq x\big\}\Big| \approx \frac{1.09125}{\log(x)}.$$

Remarque 4.14. De fait il existe un calcul direct de cette densité par dénombrement de type théorème chinois (cf. Remarque 3.13) avec cette fois des Z_p^j tels que $q_p(Z_p^j) \neq 0$, et ceci pour la suite des nombres premiers $p \leq x$. Si $y = \prod_{p \leq x} p^2$, un calcul standard montre que le nombre de $A \in [1, y[$ tels que $q_p(A) \neq 0$ pour tout $p \leq x$ est exactement $\prod_{p \leq x}(p^2 - p + 1)$, en notant que A est par nature non nécessairement étranger à $\prod_{p \leq x} p$; d'où la densité précédente exacte sur les intervalles de la forme $\big[1, \prod_{p \leq x} p^2\big[$. Ceci constitue une importante vérification des résultats de la Section 3 et montre que la conjecture ABC n'est pas nécessaire dans ce cadre cyclotomique.

Bien que y doive être pris très grand par rapport à x, on peut tester la répartition des solutions sur de petits intervalles ; par exemple, pour $2 \leq A \leq y = 10^4$, on trouve 665 valeurs de A telles que $q_p(A) \neq 0$ pour tout $p \leq x = 10^7$. Or $10^4 \cdot \frac{1.09}{\log(10^7)} \approx 676$.
Du fait que le programme utilisé compte les plus petites solutions A à $q_p(A) \neq 0$ pour tout $p \leq x$, sans doute moins nombreuses[3], le résultat est assez satisfaisant. Prenons $x \approx 10^{10}$, accessible aux calculs ; on a $\frac{1.09}{\log(10^{10})} \approx 0.05$. Pour les entiers $A \in \mathbb{N}\backslash\{0,1\}$, il y en a 95% tels que $q_p(A) = 0$ pour au moins un $p \leq 10^{10}$. Ceci est compatible avec une heuristique de finitude ; les exemples de $a = 47$ et 72 semblent être intéressants de ce point de vue (cf. § 3.8).
Cette étude est de type "densité" et n'informe que partiellement sur le cas d'une valeur a fixée une fois pour toutes. D'après le principe général (Heuristique 3.3), pour a fixé, le cas $q_p(a) \neq 0$ pour tout $p \leq x$ devrait être plus probable que $\frac{1.09125}{\log(x)}$.

4.7. **Heuristique de finitude.** On peut enfin envisager l'heuristique assez radicale suivante, en tenant compte des résultats du § 4.5 :

Heuristique 4.15. *Soit $a \in \mathbb{N}\setminus\{0,1\}$ un entier fixé. Le nombre de quotients de Fermat $q_p(a)$ nuls est en moyenne égal à 2 ou 3.*

Par programme on obtient 2.76 solutions $p < 3 \times 10^9$ en moyenne pour $2 \leq a \leq 101$. Le fait de cumuler une centaine de valeurs de a semble indispensable au vu de la répartition très incertaine des solutions p à $q_p(a) = 0$ pour un seul a.
L'expérimentation numérique semble limiter le nombre de $q_p(a) = 0$ à quelques unités en moyenne, portant en premier lieu sur de petits p (résultant de congruences du type $a \equiv 1 \pmod{p^2}$), puis éventuellement sur un petit nombre de grands nombres premiers accessibles aux ordinateurs actuels, dont la probabilité serait de l'ordre de $\frac{1}{p^2}$ et tendrait rapidement vers 0 pour les très grands nombres premiers comme l'heuristique principale semble l'indiquer (cf. Lemme 4.10, Théorème 4.11).

5. Conclusion

L'Heuristique 3.10, majorant $\mathrm{Prob}\big(q_p(a) = 0\big)$ par l'expression $\frac{1}{p\,(p-1)^2} \sum_{d \,|\, p-1} \varphi(d)^2$, est probablement très raisonnable, mais est insuffisante pour conclure à la finitude des p tels que $q_p(a) = 0$ (a fixé). Si elle est exacte, elle montre que la probabilité $\frac{1}{p}$, souvent admise, pose problème.

[3] La relation $q_p(a) = 0$ engendre les solutions $a^j \in [2, p-1[$, $j = 1, \ldots, h_p(a)$, qualifiées d'exceptionnelles (cf. § 4.1.3), et qui sont ici décomptées des A telles que $q_p(A) \neq 0$, $\forall p \leq x$.

L'Heuristique 4.5, qui stipule l'existence d'une loi de probabilité binomiale pour $\mathrm{Prob}\big(q_p(z)=0\big)$, $z\in[2,p-1[$, et qui conduit à la finitude des p tels que $q_p(a)=0$ (Théorème 4.11), reste le point sensible en raison de l'existence possible de couples (a,p), $a\ll p$, tels que $q_p(a)=0$. Dans ce cas, les $a^j\in[2,p-1[$, $j=1,\dots,h_p(a)$, où $h_p(a)=\big\lfloor\frac{\log(p)}{\log(a)}\big\rfloor$, induisent une répartition exeptionnelle des $p-2$ solutions canoniques $Z\in[2,p^2-1[$, ce qui peut être interprété de deux façons :

(i) ou bien cette loi de probabilité n'est pas la bonne (paramètres à modifier ou nature de la loi elle-même),

(ii) ou bien elle est pertinente pour décrire de façon générale les répétitions de quotients de Fermat et il n'est pas possible que, pour a fixé ($a=2$ par exemple), on ait une infinité de solutions p à $q_p(a)=0$.

Mais différentes observations sont nettement en faveur du point (ii) :

- L'étude numérique des §§ 4.2, 4.3, montre que le nombre $m_p(0)$ des répétitions $q_p(z_j)=0$, $z_j\in[2,p-1[$ pour $j=1,\dots,m_p(0)$, est en $O(\log(p))$ pour de rares nombres premiers p et n'est pas nécessairement dû au cas "$a\ll p$ & $q_p(a)=0$", un peu comme s'il était dû à une circonstance analogue non triviale reposant sur les formules de la Remarque 4.3.
- Les résultats numériques des §§ 4.3.1, 4.3.2, justifient la différence (importante) qu'il y a entre la situation précédente d'un p tel que $m_p(0)=O(\log(p))$, obtenu avec des répétitions $q_p(z_j)=0$, $z_j\in[2,p-1[$, et la probabilité que ce $m_p(0)$ provienne d'une solution exceptionnelle $a\ll p$ ($a=2,3,\dots$).
- Enfin le nombre $M_p=\sup_{u\in[0,p[}\big(m_p(u)\big)$ est très stable en $O(\log(p))$ *pour tout* $p\geq 2$, ce qui constitue certainement le phénomène le plus intéressant.

Ceci dit, l'étude précédente, bien qu'insuffisante, ainsi que les expérimentations numériques, me confortent dans la pertinence des conjectures que j'ai formulées dans le cadre très général du régulateur p-adique d'un élément η d'un corps de nombres K Galoisien sur $\mathbb{Q}$, pour lequel le quotient de Fermat n'est autre que la θ-composante du régulateur de η pour le caractère unité $\theta=1$ de $\mathrm{Gal}(K/\mathbb{Q})$ (cf. [4]).

6. Remerciements

Je remercie Gérald Tenenbaum pour sa disponibilité et ses indications de théorie analytique des nombres, dont sa contribution [15].

Références

[1] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. 66, 217 (1997), 433–449. https://math.dartmouth.edu/~carlp/PDF/paper111.pdf

[2] R. Ernvall and T. Metsänkylä, *On the p-divisibility of Fermat quotients*, Math. Comp. 66, 219 (1997), 1353–1365. http://www.ams.org/journals/mcom/1997-66-219/S0025-5718-97-00843-0/

[3] A. Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices 19 (1998)–991–1009. http://www.dms.umontreal.ca/~andrew/PDF/polysq3.pdf

[4] G. Gras, *Les θ-régulateurs locaux d'un nombre algébrique – Conjectures p-adiques* (submitted), 2014. https://www.researchgate.net/publication/261794953

[5] H. Graves and M.R. Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, Journal of Number Theory 133 (2013), 1809–1813. http://www.sciencedirect.com/science/article/pii/S0022314X12003368

[6] K. Hatada, *Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at* $2 - p$, Comment. Math. Univ. St. Pauli 36 (1987), 41–51. https://zbmath.org/?q=an:04043964
Chi-square tests for mod 1 distribution of Fermat and Fibonacci quotients, Sci. Rep. Fac. Educ., Gifu Univ., Nat. Sci. 12 (1988), 1–2. https://zbmath.org/?q=py:1988+ai:hatada.kazuyuki

[7] R. Heath-Brown, *An Estimate For Heilbronn's Exponential Sum*, In: Conference in honor of Heini Halberstam, Analytic Number Theory, 2 (1996), Birkhüser 1996. http://eprints.maths.ox.ac.uk/157/1/heilbron.pdf

[8] W. Keller and J. Richstein, *Solutions of the congruence* $a^{p-1} \equiv 1 \pmod{p^r}$, Math. Comp., 74, 250 (2004), 927–936.
http://www.ams.org/journals/mcom/2005-74-250/S0025-5718-04-01666-7/
The continuing search for Wieferich primes, Math. Comp., 75, 251 (2005), 1559–1563. http://www.ams.org/journals/mcom/2005-74-251/S0025-5718-05-01723-0/

[9] P. Moree, *Artin's Primitive Root Conjecture – A Survey*, In: The John Selfridge Memorial Volume, Integers, Vol. 12, 6 (2012), 1305–1416. http://www.degruyter.com/view/j/integ.2012.12.issue-6/integers-2012-0043/integers-2012-0043.xml

[10] A. Ostafe and I.E. Shparlinski, *Pseudorandomness and Dynamics of Fermat Quotients*, SIAM J. Discrete Math., 25(1), 50–71. http://dx.doi.org/10.1137/100798466

[11] K. Belabas and al., *Pari/gp, Version 2.5.3*, Laboratoire A2X, Université de Bordeaux I. http://sagemath.org/

[12] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, Journal of Number Theory 30 (1988), 226–237. http://www.sciencedirect.com/science/article/pii/0022314X88900194

[13] I.E. Shparlinski, *On Vanishing Fermat Quotients and a Bound of the Ihara Sum*, Kodai Math. J. Volume 36, Number 1 (2013), 99–108. http://projecteuclid.org/euclid.kmj/1364562722

[14] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 3^e édition revue et augmentée, Coll. Échelles, Belin 2008. http://iecl.univ-lorraine.fr/~Gerald.Tenenbaum/ITAN08/

[15] G. Tenenbaum, *Divergence d'une série liée aux nombres premiers*, Communication privée (juin 2014). https://www.researchgate.net/publication/263200414

[16] M. Waldschmidt, *Lecture on the abc conjecture and some of its consequences*, Abdus Salam School of Mathematical Sciences (ASSMS), Lahore 6th World Conference on 21st Century Mathematics (2013). http://www.math.jussieu.fr/~miw/articles/pdf/abcLahore2013VI.pdf

[17] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer enlarged second edition 1997.

Villa la Gardette, chemin Château Gagnière, F–38520 Le Bourg d'Oisans.
E-mail address: g.mn.gras@wanadoo.fr *url :* https://www.researchgate.net/profile/Georges_Gras/?dbw=true
-- http://monsite.orange.fr/maths.g.mn.gras/