Functiones et Approximatio
54.1 (2016), 115–140
doi: 10.7169/facm/2016.54.1.9

ÉTUDE PROBABILISTE DES QUOTIENTS DE FERMAT

Georges Gras

Abstract: For fixed $a \geqslant 2$, we suggest that the probability of nullity mod p of the Fermat quotient $q_p(a)$ is $\ll \frac{1}{p}$ for $p \to \infty$. For this we propose various heuristics (as the existence of a suitable binomial law of probability), justified by means of numerical computations and analytical results, which may imply, via the Borel–Cantelli heuristic, that $q_p(a) \neq 0$ for all p except a finite number (Th. 4.9). These heuristics are based on the possible existence (with an analogous probability) of $O(\log(p))$ "abundant" solutions $z_i \in [2, p-1[$ which are not necessarily of the "exceptional" form a^k, $1 \leqslant k < \log(p)/\log(a)$, when $q_p(a) = 0$, showing the exceptional solutions as a particular case of abundant solutions, for which a law of probability is natural.

We also compute the density of integers A such that $q_p(A) \neq 0$, $\forall p \leqslant x$ (Th. 4.12).

Keywords: Fermat quotients, cyclotomic polynomials, prime numbers, probabilistic number theory, Borel–Cantelli heuristic.

1. Introduction

Nous étudions la probabilité de nullité modulo p du quotient de Fermat $q_p(a) := \frac{a^{p-1}-1}{p}$, de $a \geqslant 2$ fixé dans $\mathbb{N}$, p premier étant la variable (par abus, l'écriture $q_p(a) = u \in [0, p[$ signifie $q_p(a) \equiv u \pmod p$).

Nous démontrons le résultat probabiliste suivant (Théorème 4.9):

Si l'Heuristique 4.4 est vraie (existence d'une loi de probabilité binomiale sur le nombre d'entiers $z \in [2, p-1[$ tels que $q_p(z) = 0$) alors, pour $p \to \infty$, $\mathrm{Prob}\big(q_p(a) = 0\big) < C_\infty(a) \times p^{-\left(\frac{\log_2(p)}{\log(a)} - \frac{\log_2(a)+1}{\log(a)} + O\left(\frac{\log_2(p)}{\log(p)}\right)\right)}$, *où* $\log_2 = \log \circ \log$ *et où la constante* $C_\infty(a)$ *vérifie* $e^{-1} < C_\infty(a) < 1$. *En admettant le principe de Borel–Cantelli, le nombre de p tels que $q_p(a) = 0$ est fini.*

Nous convenons de désigner par a un entier fixé, par A un entier positif quelconque (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 $[1, p^2[$).

(i) Dans un premier temps, on remarque que $q_p(a) = 0$ si et seulement si p^2 divise la valeur en a du $o_p(a)$-ième polynôme cyclotomique $\Phi_{o_p(a)}$, où

2010 Mathematics Subject Classification: primary: 11K65, 11R18; secondary: 11N37

$o_p(a)\,|\,p-1$ est l'ordre de a modulo p. On utilise la densité des $A \in \mathbb{N}\setminus p\mathbb{N}$ relative à la condition locale $p^2\,|\,\Phi_m(A)$, $m \geqslant 1$ fixé: si ϕ est l'indicateur d'Euler, cette densité est égale à $\frac{\phi(m)}{p(p-1)}$ pour $p \equiv 1 \pmod m$ ou pour $m = p = 2$, à 0 sinon. La densité des $A \in \mathbb{N}\setminus p\mathbb{N}$ tels que $q_p(A) = 0$ est donc $\sum_{d\,|\,p-1} \frac{\phi(d)}{p(p-1)} = \frac{1}{p}$.

On justifie alors au § 3.5 l'heuristique suivante, reposant sur l'idée qu'une *probabilité* portant sur a fixé (resp. sur $z \in [1, p[$), est inférieure à la densité correspondante:

$$\mathrm{Prob}\big(q_p(a) = 0\big) \leqslant \mathrm{Prob}\big(q_p(z) = 0, z \in [1, p[\big) \leqslant \sum_{d\,|\,p-1} \frac{\phi(d)}{p-1}\,\frac{\phi(d)}{p\,(p-1)} < \frac{1}{p}$$

ce qui ne renseigne que partiellement sur la finitude ou non des $q_p(a) = 0$ (Heuristique 3.7, Remarque 3.8, et § 3.7).

(ii) Dans un second temps, nous montrons comment tenir compte du fait que $a \geqslant 2$ est fixé et que si $q_p(a) = 0$ alors $q_p(a^j) = 0$ pour les exposants $j \in \big[1, \frac{\log(p)}{\log(a)}\big[$, pour lesquels $a^j \in [2, p-1[$ (solutions dites *exceptionnelles*). Cette répartition de $O(\log(p))$ solutions $z_j = a^j$, par rapport aux $p-1$ solutions "canoniques" $Z \in [1, p^2[$, est un cas particulier de *répétitions* (entiers $z \in [2, p-1[$ ayant même quotient de Fermat $q_p(z) = u$, $u \in [0, p[$). Si l'on pose $m_p(u) := |\{z \in [2, p-1[,\ q_p(z) = u\}|$, une étude numérique approfondie montre que ce nombre de répétitions est au plus $O(\log(p))$ car $M_p := \sup_{u\in[0,p[}\big(m_p(u)\big)$ est statistiquement très stable en $O(\log(p))$ *pour tout nombre premier* p (point essentiel).

Plus généralement, on peut avoir $m_p(0) = O(\log(p))$, auquel cas on parle de *solutions abondantes* $z_i \in [2, p-1[$, sans qu'il existe nécessairement $a \ll p$ tel que $q_p(a) = 0$ (cf. exemples du § 4.3). Les solutions étant aléatoires (les quotients de Fermat sont uniformément répartis d'après Heath-Brown [H-B]), l'existence d'une loi de probabilité standard est tout à fait crédible et donne, par un calcul analytique simple, une probabilité de cas abondant tendant vers 0 plus vite que $\frac{1}{p}$; or si "par hasard" l'une des solution z_i est égale à $a \ll p$, par ce simple fait d'ordre de grandeur Archimédien, les solutions abondantes sont (presque toutes) exceptionnelles de la forme:

$$z_1 = a, \ldots, z_h = a^h, z_{h+1}, \ldots, z_{m_p(0)},$$

où $h := h_p(a) := \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$ (partie entière), $h \leqslant m_p(0)$, ce qui ferait que les célèbres "Wieferich primes" $p = 1093, 3511$, ne seraient pas de nature particulière, mais encore plus rares que pour le cas abondant (voir les commentaires à la suite de l'Heuristique 4.2, § 4.2).

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

$$\mathrm{Prob}\big(m_p(u) \geqslant n\big) = 1 - \sum_{j=0}^{n-1} \binom{p-1}{j} \frac{1}{p^j} \left(1 - \frac{1}{p}\right)^{p-1-j}, \qquad 0 \leqslant n \ll p,$$

pour tout $u \in [0, p[$ fixé. Appliquée à $u = 0$ et au cas $n = h = O(\log(p))$, on obtient, *via le principe de Borel–Cantelli et sous cette heuristique*, la finitude des p tels que $q_p(a) = 0$ (Théorème 4.9).

(iii) Enfin, en utilisant le fait que $q_p(A) = 0$ si et seulement si p^2 divise $\dfrac{\Phi_{o_p(A)}(A)}{\text{p.g.c.d.}\,(\Phi_{o_p(A)}(A), o_p(A))}$, on démontre que la densité des $A \in \mathbb{N}$ tels que $q_p(A) \neq 0,\ \forall p \leqslant x$, est $O\big(\frac{1}{\log(x)}\big)$ (Théorème 4.12).

2. Cyclotomie et quotients de Fermat

2.1. Rappels sur le quotient de Fermat

Soit $a \geqslant 1$. Soit p un nombre premier, $p \nmid a$. Soit $m = o_p(a)$ 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 $q_p(a) = \frac{a^{p-1}-1}{p} = \frac{\Phi_m(a)}{p} \times F,\ F \not\equiv 0 \pmod p$. On a donc l'implication $m = o_p(a) \Longrightarrow p \,|\, \Phi_m(a)$. 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, avec ici $m = p \cdot o_p(a)$.

Ce phénomène sera précisé par le Théorème 2.3, mais on a toujours $q_p(a) \equiv 0 \pmod p$ 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 [CDP], [EM], [Hat], [KR], [Sh], [OS], ainsi qu'à [Si], [GM], [W] pour les liens avec la conjecture ABC.

2.2. Utilisation des corps cyclotomiques

Nous utilisons des propriétés classiques que l'on peut trouver dans [Wa].

Lemme 2.1. *Soient $a \geqslant 1$, $p \nmid a$, et $m \geqslant 1$. Alors la congruence $\Phi_m(a) \equiv 0 \pmod{p^H}$, $H \geqslant 1$, est équivalente à l'existence d'un couple $(\xi, \mathfrak{P})$, défini à conju-*

[1] Bien que $z = 1$ et $z = p - 1$ introduisent un biais ($q_p(1) = 0$, $q_p(p-1) = 1$), les paramètres $(p-1, 1/p)$ se justifient car on pourrait utiliser un intervalle décalé de $p-1$ résidus de la forme $[-t\,p + 1, (-t+1)\,p[$, $t \in [0, p[$, n'ayant pas ce biais; or ces intervalles ont les mêmes propriétés statistiques (cf. Remarque 4.3). De plus, la loi en $(p-1, 1/p)$ est légèrement majorante pour $\mathrm{Prob}\big(m_p(u) \geqslant n\big)$, ce qui est favorable.

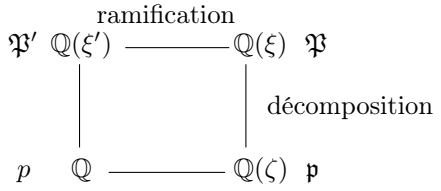
gaison près, tel que $a \equiv \xi \pmod{\mathfrak{P}^H}$*, où* ξ *est une racine primitive* m*-ième de l'unité et* $\mathfrak{P}$ *un idéal premier de* $\mathbb{Q}(\xi)$ *au-dessus de* p*, de degré résiduel* 1*. Lorsque ceci a lieu,* m *est de la forme* $p^e \cdot o_p(a)$*,* $e \geqslant 0$*.*

Démonstration. La relation $a \equiv \xi \pmod{\mathfrak{P}^H}$, $H \geqslant 1$, prouve déjà que $\mathfrak{P}$ est de degré résiduel 1 car 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 $\Phi_m(a) \equiv 0 \pmod{p^H}$, $H \geqslant 1$. Comme $\Phi_m(a) = \prod_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} (a - \xi^t) \equiv 0 \pmod{p^H}$, 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 aussi $a - \xi \equiv 0 \pmod{\mathfrak{P}_2}$, $\mathfrak{P}_2 \mid p$, 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 $a - \xi^t \equiv 0 \pmod{\mathfrak{P}_1}$, d'où $\xi^t - \xi \equiv 0 \pmod{\mathfrak{P}_1}$. 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 $\mathfrak{P} \mid p$ 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 $m = p^e m'$, $e \geqslant 1$, $p \nmid m'$, 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 $\mathfrak{P}_1 \mid \mathfrak{p}$ et $\mathfrak{P}_2 \mid \mathfrak{p}$ (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 obtenu dans tous les cas $a - \xi \equiv 0 \pmod{\mathfrak{P}^H}$ pour un unique $\mathfrak{P} \mid p$.

Montrons enfin que $m' = o_p(a)$ dans tous les cas. On a à, ce stade, $m = p^e \,.\, m'$, $e \geqslant 0$, et $a \equiv \xi' \pmod{\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Z}[\xi']}$ puisque $\zeta \equiv 1 \pmod{\mathfrak{P}}$, 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 $m = o_p(a) \Longrightarrow p \mid \Phi_m(a)$ en tenant compte des questions de divisibilités par p^H. D'après le lemme précédent, si $p \mid \Phi_m(a)$, on a $m = p^e \,.\, o_p(a)$, $e \geqslant 0$, et par conséquent $p \mid \Phi_{o_p(a)}(a)$. Le cas $p \nmid m$ est donc résolu et conduit à l'équivalence partielle $p \mid \Phi_m(a)$ & $p \nmid m \iff m = o_p(a)$. Dans ce cas toute puissance p^H, $H \geqslant 1$, peut diviser $\Phi_m(a) = \Phi_{o_p(a)}(a)$ (c'est le problème du quotient de Fermat pour $H \geqslant 2$). Examinons maintenant le cas où $p \mid m$.

Lemme 2.2. *Supposons que pour $H \geqslant 1$, $p^H \,||\, \Phi_m(a)$ avec $m = p^e m'$, $e \geqslant 1$, $p \nmid m'$ (i.e., $m = p^e \,.\, o_p(a)$). Alors nécessairement $H = 1$ (i.e., $\Phi_m(a) \not\equiv 0 \pmod{p^2}$) sauf si $p^e = m = 2$, auquel cas si $a = -1 + 2^H\,\psi$, $H \geqslant 1$ quelconque, on a $\Phi_2(a) = 2^H\ \psi$, $\Phi_1(a) = -2 + 2^H\,\psi$.*

Démonstration. On a donc par hypothèse, d'après le Lemme 2.1, $a \equiv \xi \pmod{\mathfrak{P}^H}$, pour $\xi = \zeta\xi'$ d'ordre $p^e \,.\, o_p(a)$ (ζ d'ordre p^e, ξ' d'ordre $o_p(a)$), et $a \equiv \xi' \pmod{\mathfrak{P}'^{H'}}$, $\mathfrak{P}' = \mathfrak{P} \cap \mathbb{Z}[\xi']$, avec $H' \geqslant 1$ 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 $H'p^{e-1}(p-1) > 1$, 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 $m = p = 2$, on a $H = 1$. ■

Théorème 2.3. *Pour tout $m \geqslant 1$, 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, $m = p^e \cdot o_p(a)$, $e \geqslant 1$. Réciproquement, pour tout premier p et tout $e \geqslant 1$, $m = p^e \cdot o_p(a)$ conduit à* p.g.c.d. $(\Phi_m(a), m) = p$. *On a donc l'équivalence (pour tout p et tout m) $p \,|\, \Phi_m(a) \iff m = p^e \cdot o_p(a)$, $e \geqslant 0$.*

Démonstration. Si p et q, $p \neq q$, sont des nombres premiers divisant m et $\Phi_m(a)$, on a nécessairement $m = p^e q^f m''$, $e, f \geqslant 1$, 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 tout $e \geqslant 1$ 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 2.1). Il est clair que p.g.c.d. $(m, \Phi_m(a)) = p$. ■

Nous réserverons la notation r au cas où $m = r^e \cdot o_r(a)$, $e \geqslant 1$, car r n'intervient pas pour le calcul des $q_p(a)$ pour les $p \,|\, \Phi_m(a)$. En effet, 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 (mod r) des $\dfrac{\Phi_{r^e \cdot\, o_r(a)}(a)}{r}$ pour $e \geqslant 1$ puisque dans ce cas, et pour $m = r^e \cdot o_r(a) \neq 2$, $\Phi_{r^e \cdot\, o_r(a)}(a) \not\equiv 0 \pmod{r^2}$ (Lemme 2.2). 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., $q_{29}(14) = 0$).

2.3. Définition et propriétés des nombres $\widetilde{\Phi}_m(a)$

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 $\dfrac{\Phi_{r^e \cdot\, o_r(a)}(a)}{r}$, $e \geqslant 1$, pour éliminer le facteur premier r éventuel (ramifié dans $\mathbb{Q}(\xi)/\mathbb{Q}$). Dans le second cas $m = r^e \cdot o_r(a)$, $e \geqslant 1$, si $p \neq r$ divise $\Phi_m(a)$, alors $m = o_p(a)$ et on a $p \equiv 1 \pmod{r^e \cdot o_r(a)}$.

Soit $m \neq 2$; d'après les résultats précédents, tout premier ℓ divisant $\widetilde{\Phi}_m(a)$ est congru à 1 modulo m (car de degré 1 et non ramifiés dans $\mathbb{Q}(\mu_m)/\mathbb{Q}$). Il en résulte aussi que ℓ (en posant $\ell - 1 = t\,m$) est totalement 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. 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; elles sont susceptibles de s'appliquer aux quotients de Fermat (nous renvoyons à [Mo] pour un exposé exhaustif).

Lemme 2.4. *Supposons $(m,p) \neq (2,2)$. On a $p^2 \mid \widetilde{\Phi}_m(a)$ si et seulement si $m = o_p(a)$ & $p^2 \mid \Phi_m(a)$, donc si et seulement si $m = o_p(a)$ & $q_p(a) = 0$.*

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

Réciproquement, si $p^2 \mid \widetilde{\Phi}_m(a)$, on peut supposer p.g.c.d. $(\Phi_m(a), m) = r$ avec $m = r^e\, o_r(a)$, $e \geqslant 1$, 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 2.2 qui exclue le cas $p^e = m = 2$), d'où $p^2 \mid \Phi_m(a) = \Phi_{o_p(a)}(a)$. ■

Lemme 2.5. *Pour a fixé, les $\widetilde{\Phi}_m(a)$, $m \geqslant 1$, sont premiers entre eux deux à deux sauf pour $\widetilde{\Phi}_1(a)$ et $\widetilde{\Phi}_2(a)$ dont le p.g.c.d. est 2 pour $a \equiv 3 \pmod 4$. Pour tout $p > 2$ il existe un et un seul $m \geqslant 1$ (égal à $o_p(a)$), tel que $p \mid \widetilde{\Phi}_m(a)$.*

Démonstration. Si $p \neq 2$ divise $\widetilde{\Phi}_m(a)$ et $\widetilde{\Phi}_{m'}(a)$, d'après le Théorème 2.3 on a $m = p^e o_p(a)$ et $m' = p^{e'} o_p(a)$, $e, e' \geqslant 0$. Si par exemple $e \geqslant 1$, on a $p = r$ (absurde car r^2 ne divise pas $\Phi_m(a)$); donc $e = e' = 0$ et $m = m'$.

Si $p = 2$, on obtient encore $m = 2^e$, $m' = 2^{e'}$, $e, e' \geqslant 0$; le cas e ou $e' \geqslant 2$ 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 $\widetilde{\Phi}_1(a) = a - 1$ sont divisibles par 2 pour $a \equiv 3 \pmod 4$. Enfin tout p divise $\Phi_{o_p(a)}(a) = \widetilde{\Phi}_{o_p(a)}(a)$. ■

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

Théorème 2.6. *Soit $a \geqslant 1$ et soit p premier, $p \geqslant 2$. Alors $q_p(a) = 0$ si et seulement si p^2 divise $\widetilde{\Phi}_{o_p(a)}(a)$.*

Ce résultat ainsi que le Lemme 2.5 seront utilisés, entre autres, au § 4.6.

3. Première heuristique pour Prob $(q_p(a) = 0)$

3.1. Remarques préliminaires sur les probabilités

Soit $a \geqslant 2$ fixé et soit u donné dans $\mathbb{N}$. Pour $p \to \infty$, l'événement $q_p(a) \equiv u \pmod p$ est a priori de probabilité $\frac{1}{p}$ puisque $q_p(a)$ et u sont vus modulo p. Des probabilités inférieures à $\frac{1}{p}$ en moyenne ne sont pas contradictoires car une étude

numérique montre qu'environ un tiers des $u \in [0, p[$ ne sont pas de la forme $q_p(z)$, $z \in [1, p[$. Pour les grands nombres premiers, la proportion moyenne se stabilise autour de $e^{-1} \approx 0.3678...$ (déjà observé dans [EM], § 4), ce qui constituera un bon argument pour l'existence d'une loi de probabilité binomiale car c'est précisément la probabilité (calculée via cette loi) d'avoir 0 solutions $z \in [2, p-1[$ à $q_p(z) = 0$ (Remarque 4.6 (ii)).

Le cadre probabiliste des solutions $z \in [2, p-1[$ à $q_p(z) = 0$ (p fixé) est très différent du cas a fixé (p variable) et est plutôt de type densité; or on verra au § 3.4 que ces deux cas de figure sont à distinguer soigneusement, tout se régularisant sur l'intervalle $[1, p^2[$ où "probabilité = densité" (surjectivité de l'application $Z \in [1, p^2[\mapsto q_p(Z) \in [0, p[$ par l'existence de $p-1$ solutions $Z \in [1, p^2[$ à $q_p(Z) = u$, cf. Lemme 3.4).

3.2. Résultats généraux de densités locales et globales

Citons, à titre d'information, le résultat suivant de Granville [G] (sous la conjecture ABC), dans la mesure où il peut éclairer notre démarche.

Proposition 3.1. *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. La densité naturelle des entiers $A \in \mathbb{N}$ tels que $f(A)$ est sans facteur carré non trivial est $\prod_{p \text{ premier} \geqslant 2} \left(1 - \frac{c_p}{p^2}\right)$, où $c_p = \left| \left\{ b \in [0, p^2[,\ f(b) \equiv 0 \pmod{p^2} \right\} \right|$, chaque facteur $1 - \frac{c_p}{p^2}$ étant la densité (dite densité locale associée à p) des $A \in \mathbb{N}$ tels que $p^2 \nmid f(A)$.*

D'une certaine manière on peut dire que les événements $p^2 \nmid f(A)$ sont indépendants par rapport à p, ce qui constitue une information "probabiliste" intéressante. Par la suite, nous utiliserons essentiellement l'aspect local que l'on retrouve élémentairement dans le cadre cyclotomique.

3.3. Calcul des coefficients c_p pour les polynômes Φ_m

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

Proposition 3.2. *Considérons Φ_m pour $m \geqslant 1$. Si $p \geqslant 2$ ne divise pas m, on a $c_p = 0$ pour les $p \not\equiv 1 \pmod{m}$ et $c_p = \phi(m)$ sinon, où ϕ est l'indicateur d'Euler. Si $m = p^e m'$, $e \geqslant 1$, $p \nmid m'$, on a $c_p = 0$ sauf si $m = p = 2$, 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 $\phi(m)$ nombres distincts $A_i \in [1, p[$ pour lesquels $\Phi_m(A_i) \equiv 0 \pmod{p}$. On vérifie, en dérivant $X^m - 1 = \Phi_m(X) \cdot Q(X)$, qu'il existe un unique $\psi_i \in [0, p[$ tel que $\Phi_m(A_i + \psi_i\, p) \equiv 0 \pmod{p^2}$, pour chaque i.

(ii) Cas $p \mid m$. D'après le Lemme 2.2, $m = p^e \cdot o_p(A)$, $e \geqslant 1$, et $\Phi_m(A) \equiv 0 \pmod{p^2}$ n'a pas de solutions sauf si $m = p = 2$ où $c_2 = 1$. ∎

3.4. Densités et probabilités – généralités

Si F_p est la propriété locale $p^2 \mid f(A)$ (p fixé), la densité des $A \in \mathbb{N} \setminus p\mathbb{N}$, donnée à partir des Propositions 3.1, 3.2, est égale à $\frac{c_p}{p\,(p-1)}$.

Il faut distinguer la notion de densité relative à la propriété:

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

de celle de probabilités définissant l'un des événements suivants:

$$\textit{pour } z \in [2, p-1[,\ p^2 \mid f(z),\ p \textit{ variant arbitrairement,}$$
$$\textit{pour } a \textit{ fixé, } p^2 \mid f(a),\ p \textit{ variant arbitrairement.}$$

La densité locale ne dépend que de p et est de nature *algébrique*, tandis que ce que nous définissons comme probabilités est, pour un unique "tirage" $z \in [2, p-1[$, une fonction de p et, pour a fixé, une fonction de p de paramètre a; c'est le cas de $\mathrm{Prob}\big(q_p(a) = 0\big)$.

Le cas $q_p(a) = u$, u donné dans $\mathbb{N}$, est analogue; par exemple, on a $q_7(2) = 2$, mais les seuls $p < 10^{10}$, tels que $q_p(2) = 2$ sont $7, 71, 379, 2659$.

Chacun des p intervalles $[\lambda p + 1, (\lambda+1)p[$, $\lambda \in [0, p[$, contient a priori $\frac{p-1}{p}$ solutions en moyenne si l'on se réfère à la densité donnée par les $p-1$ solutions canoniques modulo p^2 (de fait $\frac{p-3}{p}$ solutions en raison de l'exclusion des "racines de l'unité" $\pm 1 \pmod{p^2}$ qui ne doivent pas intervenir en termes de probabilités: cas particulier de [Gr1], § 6.1.3, qui reviendrait à utiliser ici le système de représentants plus canonique $[-\frac{p-1}{2}, \frac{p-1}{2}] \setminus \{\pm 1\}$, $p \neq 2$).

On peut donc déjà envisager la première heuristique générale suivante:

Heuristique 3.3. *Supposons donnée une propriété locale $F_p(A)$, $p \to \infty$. Alors, la densité des $A \in \mathbb{N} \setminus p\mathbb{N}$ vérifiant $F_p(A)$ est un majorant de la "densité sur $[1, p[$" (notée par abus $\mathrm{Prob}\big(F_p(z)\big)$) des $z \in [1, p[$ tels que $F_p(z)$, celle-ci étant un majorant de $\mathrm{Prob}\big(F_p(a)\big)$ pour a fixé.*

Par exemple (cf. Théorème 2.6, Lemme 2.4 et Proposition 3.2), les densités locales $\frac{\phi(d)}{p\,(p-1)}$, caractérisant la propriété $p^2 \mid \widetilde{\Phi}_d(A)$ (i.e., $q_p(A) = 0$ pour les A d'ordre d modulo p), sont des *majorants* de $\mathrm{Prob}\big(q_p(z) = 0\big)$ (resp. $\mathrm{Prob}\big(q_p(a) = 0\big)$) pour $z \in [1, p[$ (resp. a fixé), z et a d'ordre d modulo p. Ceci sera utilisé pour justifier l'Heuristique 3.7.

Au plan numérique, pour $10^6 < p < 10^6 + 10^4$, il y a 754 nombres premiers et pour 284 d'entre eux, on a 0 solutions dans $[2, p-1[$. Enfin, si $m_p(0)$ est le nombre de solutions, les sommes $s = \sum_p \frac{m_p(0)}{p-1}$ et $s' = \sum_p \frac{1}{p-1}$ (sur cet intervalle) sont respectivement égales à 0.00012178... et 0.00012417....

3.5. Densités et probabilités des $q_p(\,\bullet\,) = u \in [0, p[$

Le résultat suivant généralise le cas précédent par un calcul direct de densité dans l'intervalle $[0, p^2[$:

Lemme 3.4. *Soit $z \in [1,p[$. Alors il existe un unique entier $\lambda_{p,u}(z) \in [0,p[$ tel que $Z := z + \lambda_{p,u}(z)\,p \in [1,p^2[$ vérifie $q_p(Z) = u$. On a $\lambda_{p,u}(z) \equiv z\,(q_p(z) - u) \pmod p$, d'où $Z \equiv z^p - zu\,p \pmod{p^2}$.*

La densité des $A \in \mathbb{N} \setminus p\mathbb{N}$, d'ordre $d \mid p-1$ modulo p, tels que $q_p(A) = u$ est égale à $\frac{\phi(d)}{p(p-1)}$.

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 $\lambda = \lambda_{p,u}(z) \equiv z\,q_p(z) - z\,u \pmod p$. On a donc pour chaque $z \in [1,p[$ un unique $Z = z + \lambda_{p,u}(z)\,p \in [1,p^2[$ tel que $q_p(Z) = u$ (Z est aussi le résidu modulo p^2 de $z^p - zu\,p$), d'où la densité car $o_p(Z) = d$ équivaut à $o_p(z) = d$. ∎

Remarques 3.5. Posons $\lambda_{p,0}(z) =: \lambda_p(z)$. On a alors les faits suivants:

(i) La relation $\lambda_p(z) \equiv z\,q_p(z) \pmod p$ pour tout $z \in [1,p[$ montre que pour a fixé, $q_p(a)$ et $\lambda_p(a)$ ont des comportements heuristiques analogues. En particulier, $z \in [1,p[\mapsto \lambda_p(z) \in [0,p[$ est non surjective.

(ii) Pour tout $z \in [1,p[$, on a les identités $q_p(p-z) \equiv q_p(z) + z^{-1} \pmod p$ et $\lambda_p(p-z) + \lambda_p(z) = p-1$, ce qui établit des relations de dépendance puisque, par exemple, $q_p(z)$ et $q_p(p-z)$ ne peuvent être nuls simultanément.

Revenons au cas $a \geqslant 2$ fixé. Pour $p \to \infty$ considérons l'intervalle $[1,p[$. D'après l'Heuristique 3.3, $\mathrm{Prob}\big(q_p(a) = 0\big)$ est majorée par la densité des $z \in [1,p[$ tels que $q_p(z) = 0$. Soit alors $d \mid p-1$; comme $o_p(z)$ ne dépend que de la classe de z modulo p, $\mathrm{Prob}\big(o_p(z) = d\big)$ est exactement la densité correspondante, égale à $\frac{\phi(d)}{p-1}$. Ensuite, $\mathrm{Prob}\big(p^2 \mid \widetilde{\Phi}_d(z)\big) \leqslant \frac{\phi(d)}{p\,(p-1)}$ (exemple illustrant l'Heuristique 3.3). Par conséquent, la probabilité de nullité de $q_p(a)$, pour a fixé et $p \to \infty$, est majorée par $\mathrm{Prob}\big(q_p(z) = 0, z \in [1,p[\big)$ qui est la somme pondérée:

$$\sum_{d \mid p-1} \mathrm{Prob}\big(o_p(z) = d\big) \times \mathrm{Prob}\big(p^2 \mid \widetilde{\Phi}_d(z),\, o_p(z) = d\big) \leqslant \sum_{d \mid p-1} \frac{\phi(d)}{p-1} \times \frac{\phi(d)}{p\,(p-1)}.$$

Remarques 3.6.

(i) Soient $z_1, \ldots, z_{\phi(d)}$ les $\phi(d)$ éléments d'ordre d de $[1,p[$. Pour chaque z_i, il existe (Lemme 3.4) $\lambda_i \in [0,p[$ tel que $q_p(z_i + \lambda_i p) = 0$ et λ_i est unique; autrement dit, pour i fixé, les p éléments $Z_\mu := z_i + \mu p$, $\mu \in [0,p[$, ne sont pas indépendants pour la probabilité $\mathrm{Prob}\big(q_p(Z_\mu) = 0\big)$ car la loi de probabilité pour la variable μ (i fixé) est telle que $\mathrm{Prob}\big(q_p(Z_\mu) = 0\big) = \frac{1}{p}$ et $\mathrm{Prob}\big(q_p(Z_{\mu_1}) = q_p(Z_{\mu_2}) = 0\big) = 0$ si $\mu_1 \neq \mu_2$. Mais sur $[1,p[$, une heuristique d'indépendance est possible au vu des résultats numériques (cf. § 4.3) et de l'uniforme distribution des $q_p(z)$.
Ceci explique que si l'on veut retrouver la densité des A tels que $q_p(A) = 0$ par ce raisonnement, à savoir écrire:

$$\sum_{d \mid p-1} \mathrm{Prob}\big(o_p(A) = d\big) \times \mathrm{Prob}\big(p^2 \mid \widetilde{\Phi}_d(A),\, o_p(A) = d\big),$$

le premier facteur est $\frac{p\,\phi(d)}{p\,(p-1)} = \frac{\phi(d)}{p-1}$, mais le second n'est pas la densité $\frac{\phi(d)}{p\,(p-1)}$ car la probabilité conditionnelle porte sur les $o_p(A) = d$ qui se répartissent en $\phi(d)$ classes à p éléments non indépendants comme expliqué ci-dessus.

(ii) La relation $a^{o_p(a)} = 1 + \lambda p > p$, implique $o_p(a) > h_p(a) =: h$, ce qui conduit à $\mathrm{Prob}\big(o_p(a) = d\big) = 0$ pour les petits diviseurs, ce qui favorise les plus grands (somme des probabillités égale à 1). On doit donc considérer une somme de la forme $\Sigma := \sum_{d>h} \left(\frac{\phi(d)}{p-1} + \pi_d\right) \frac{\phi(d)}{p(p-1)}$, où $\sum_{d>h} \pi_d = \sum_{d<h} \frac{\phi(d)}{p-1}$; on admet que l'on peut prendre pour π_d la valeur moyenne $\pi = \frac{1}{N_h} \sum_{d<h} \frac{\phi(d)}{p-1}$, où $N_h := |\{d \,|\, p-1,\ d > h\}|$. On vérifie que π est majoré par $\frac{1}{p^{1-\beta(p)}}$ où $\beta(p) > 0$ est de la forme $O\big(\frac{1}{\log_2(p)}\big)$ et $\sum_{d>h} \pi_d \frac{\phi(d)}{p(p-1)} < O\big(\frac{1}{p^{2-\beta(p)}}\big)$.
On compare Σ et $\frac{1}{p}$ en posant $\Sigma = \alpha_p \frac{1}{p}$. Les extrema locaux de α_p sont obtenus pour les nombres de Sophie Germain $p = 1 + 2\ell$, ℓ premier, où $o_p(a) = 1$ ou 2 est impossible et où l'on peut supposer que $\mathrm{Prob}\big(o_p(a) = \ell\big) = \mathrm{Prob}\big(o_p(a) = 2\ell\big) = \frac{1}{2}$; on a $\pi = \frac{1}{p-1}$, auquel cas $\Sigma = \frac{\ell-1}{2\ell\,p} \sim \frac{1}{2p}$, $p = 1 + 2\ell \to \infty$. Donc $\mathrm{Sup}_p(\alpha_p) = \frac{1}{2}$. Lorsque $p-1$ est très composé, on a toujours $\alpha_p < \frac{1}{2}$, et $\mathrm{Inf}_p(\alpha_p)$ est proche de 0; par exemple, pour $p \in I := [10^6, 11 \times 10^8]$ et pour $a = 3$, on trouve $\mathrm{Inf}_{p\in I}(\alpha_p) = 0.050061...$ (atteint pour $p = 232792561 = 1 + 2^4 \,.\, 3^2 \,.\, 5 \,.\, 7 \,.\, 11 \,.\, 13 \,.\, 17 \,.\, 19$) et $\mathrm{Sup}_{p\in I}(\alpha_p) = 0.499999999090...$ (atteint pour $p = 1099998587 = 1 + 2 \,.\, \ell$, $\ell = 549999293$).

(iii) Si l'on calcule naïvement cette probabilité au moyen du polynôme $X^{p-1} - 1$ pour lequel la densité locale est $\frac{c_p}{p\,(p-1)} = \frac{p-1}{p\,(p-1)} = \frac{1}{p}$, l'expression analogue $\sum_{d\,|\,p-1} \mathrm{Prob}\big(o_p(z) = d\big) \times \mathrm{Prob}\big(p^2 \,|\, z^{p-1} - 1,\ o_p(z) = d\big)$ serait majorée par $\sum_{d\,|\,p-1} \frac{\phi(d)}{p-1} \times \frac{1}{p} = \frac{1}{p}$ indépendamment de toute "corection probabiliste", ce qui montre la pertinence de l'utilisation de $\Phi_d(X)$ au lieu de $X^{p-1} - 1$ qui remplace terme à terme $\frac{1}{p}$ par $\frac{\phi(d)}{p\,(p-1)} < \frac{1}{p}$.

On convient de négliger le phénomène des $d < h$ dans la mesure où seule l'information $\mathrm{Prob}\big(q_p(a) = 0\big) < \frac{1}{p}$ est l'objectif de cette section. On a donc la première heuristique probabiliste suivante pour $q_p(a) = 0$:

Heuristique 3.7. *Pour $a \geqslant 2$ fixé dans $\mathbb{N}$ et tout p assez grand, posons* $\mathrm{Prob}\big(q_p(a) = 0\big) = \frac{1}{p^{1+\epsilon(p,a)}}$. *Alors* $\mathrm{Prob}\big(q_p(a) = 0\big) \leqslant \frac{1}{p\,(p-1)^2} \sum_{d\,|\,p-1} \phi(d)^2$, *ou, de façon équivalente,* $\epsilon(p,a) \geqslant \frac{1}{\log(p)} \big(2\log(p-1) - \log\big(\sum_{d\,|\,p-1} \phi(d)^2\big)\big)$.

Remarque 3.8. Sous l'heuristique précédente, on obtient $\epsilon(p,a) > 0$ car

$$\frac{1}{p^{1+\epsilon(p,a)}} \leqslant \frac{\sum_{d\,|\,p-1} \phi(d)^2}{p\,(p-1)^2} < \frac{\big(\sum_{d\,|\,p-1} \phi(d)\big)^2}{p\,(p-1)^2} = \frac{1}{p}.$$

Autrement dit, si $\upsilon(p) = \frac{1}{\log(p)} \big(2\log(p-1) - \log\big(\sum_{d\,|\,p-1} \phi(d)^2\big)\big)$, on a $\epsilon(p,a) > \upsilon(p) > 0$, $p \to \infty$.

3.6. Une série de référence convergente

Afin de proposer de telles fonctions $\epsilon(p,a)$, rappelons une condition suffisante très classique de convergence des séries du type $\sum_p \frac{1}{p^{1+\epsilon(p,a)}}$, la série $\sum_p \frac{1}{p^{1+\upsilon(p)}}$ ne l'étant pas comme l'a montré G. Tenenbaum (cf. § 3.7).

Lemme 3.9. *Soit* $C>1$ *une constante et soit* $\eta(p) := C \cdot \frac{\log_3(p)}{\log(p)}$, *où* $\log_k$ *désigne le k-ième itéré de la fonction* log. *Alors on a* $S := \sum\limits_{p\geqslant 2} \frac{1}{p^{1+\eta(p)}} < \infty$.

Démonstration. Pour tout $n \geqslant 1$, désignons par p_n le n-ième nombre premier. On a $\sum_{p\geqslant 2} \frac{1}{p^{1+C\,\cdot\,\log_3(p)/\log(p)}} = \sum_{p\geqslant 2} \frac{1}{p\cdot \log_2^C(p)} = \sum_{n\geqslant 1} \frac{1}{p_n \cdot \log_2^C(p_n)}$.

On a $p_n > n\log(n)$ (théorème de Rosser); donc on peut majorer S par $\sum_{n\geqslant n_0} \frac{1}{n\log(n)\cdot \log_2^C(n\log(n))} < \sum_{n\geqslant n_0} \frac{1}{n\log(n)\cdot\log_2^C(n)}$, à une constante près, ce qui a même comportement que $\int_{x_0}^{\infty} \frac{dx}{x\log(x)\cdot \log_2^C(x)} = \int_{y_0}^{\infty} \frac{dy}{y\cdot \log^C(y)} < \infty$. ■

On a $\epsilon(p,a) > \upsilon(p)$ (Remarque 3.8); donc $\epsilon(p,a) > \eta(p)$ reste largement possible. La différence entre $\upsilon(p)$ (situation divergente pour $\sum_p \frac{1}{p^{1+\upsilon(p)}}$) et $\eta(p)$ (situation convergente pour $\sum_p \frac{1}{p^{1+\eta(p)}}$) est très faible comme le montrent les résultats numériques suivants (p très grand, $C = 1.1$):

$$p = 2\times 10^{40}+477 \qquad \mathit{eta}-\mathit{upsilon} = 0.007099...,$$
$$p = 2\times 10^{40}+513 \qquad \mathit{eta}-\mathit{upsilon} = 0.004805...,$$
$$p = 2\times 10^{40}+593 \qquad \mathit{eta}-\mathit{upsilon} = -0.004780...,$$
$$p = 2\times 10^{40}+723 \qquad \mathit{eta}-\mathit{upsilon} = 0.008382....$$

Les "croisements de courbes" (fréquents au début) correspondent aux $p-1$ divisibles par un très grand nombre premier donnant de grands $\phi(d)$ (cas favorables mais non significatifs pour $\sum_p \frac{1}{p^{1+\upsilon(p)}}$). 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

Une estimation majorante du nombre de $p \leqslant x$ tels que $q_p(a) = 0$ est $\sum_{p\leqslant x} \frac{1}{p^{1+\upsilon(p)}}$. Or la série $\widetilde{S} := \sum_p \frac{1}{p^{1+\upsilon(p)}} = \sum_p \frac{1}{p\,(p-1)^2} \sum_{d\,|\,p-1} \phi(d)^2$, comme on pouvait s'y attendre, est divergente, et G. Tenenbaum a démontré que

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

lorsque $x \to \infty$ ([T2]). Sa démonstration repose entre autres sur le théorème de Bombieri–Vinogradov ([T1], Théorème II.8.34).

On en déduit, en admettant le principe de Borel–Cantelli, que pour a fixé le nombre moyen de solutions p à $q_p(a)=0$ vérifie:

$$\big|\{p\leqslant x,\ q_p(a)=0\}\big| < \widetilde{S}(x)=O(\log_2(x)) < 0.452...\times\log_2(x), \qquad \text{pour } x\to\infty,$$

après une estimation majorante de la constante (obtenue pour $x=10^9$), ce qui reste une croissance très faible mais ne permet pas de conclure dans le cas de a fixé.

Remarque 3.10. Soient $p_1,\cdots,p_n$ des nombres premiers distincts donnés. Pour chaque $p\in\{p_1,\dots,p_n\}$ soit $(Z_p^j)_{j=1,\dots,p-1}$ la famille des $p-1$ solutions $Z_p^j\in[1,p^2[$ à $q_p(Z_p^j)=0$ (Lemme 3.4); alors tout A satisfaisant à l'un des systèmes de congruences:

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

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 une autre direction, il n'est pas rare de trouver des valeurs de a pour lesquelles $q_p(a)\neq 0$ sur un intervalle $p\in[2,x[$ où x est de l'ordre de 10^{10}, ce qui accrédite la finitude et on peut se demander s'il existe des a tels que $q_p(a)\neq 0$ pour tout p. On abordera cette existence au Théorème 4.12 par le calcul effectif, de type "théorème chinois" (cf. Remarque 3.10), de la densité des $A\in\mathbb{N}$ tels que $q_p(A)\neq 0$ pour tout $p\leqslant x$.

Pour $2\leqslant a\leqslant 100$ 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 $p\leqslant 10^{11}$.

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

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

et la solution remarquable $(5,188748146801)$ (se reporter à la Remarque 4.10 (ii) pour une analyse possible de ce phénomène).

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

L'approche précédente, reposant en partie sur des calculs de densités, ne tient pas assez compte du fait que l'on étudie $q_p(a)$ pour a fixé et $p\to\infty$. Or $q_p(a)=0$ pour $p\gg a$ conduit à de nombreuses solutions dans $[2,p-1[$ puisque

$$q_p(a^j)=0 \qquad \& \qquad a^j\in[2,p-1[\qquad \text{pour } \ 1\leqslant j\leqslant h_p(a):=\Big\lfloor\frac{\log(p)}{\log(a)}\Big\rfloor.$$

Il se pose également la question de savoir si d'autres solutions sont possibles et quel est leur nombre au vu des propriétés de l'application $z \mapsto q_p(z)$.

Mais on peut supposer, sous peine de répartition inhomogène, que ces phénomènes sont limités par le fait que le nombre total de solutions Z dans $[1, p^2[$ est $p-1$, et comme on l'a vu, on peut s'attendre *en moyenne* à un peu moins d'une solution $z \in [2, p-1[$.

D'où la nécessité d'une première étude sur l'intervalle $[2, p-1[$, étude qui est intermédiaire entre les cas $a \in [2, p-1[$ fixé et $Z \in [2, p^2-1[$ et qui, sur un plan heuristique, caractérise les propriétés du quotient de Fermat.

4.1. Etude des solutions $z \in [2, p-1[$ à $q_p(z) = 0$

Répartition des $q_p(z)$ sur $[1, p[$, pour p fixé

Le résultat de Heath-Brown ([H-B], Theorem 1, Corollary, p. 2) affirme que les $q_p(z)$, $z \in [1, p[$, sont uniformément répartis (mod p) ainsi que les résidus (mod p^2) des z^p, $z \in [1, p[$ (or ce sont les solutions $Z \in [1, p^2[$ à $q_p(Z) = 0$, cf. Lemme 3.4 pour $u = 0$), ce qui renforce notre démarche.

On obtient aussi le curieux phénomène de répartition suivant. On calcule la somme des puissances de $q_p(z)$ vus dans $[0, p[$:

$$\sigma_n(p) := \frac{n+1}{(p-1)^{n+1}} \sum_{z=1}^{p-1} q_p(z)^n,$$

pour tout $n \geqslant 1$. On obtient alors, quel que soit n, une remarquable convergence alternée vers 1 lorsque $p \to \infty$ (couples $(p, \sigma_n(p))$ avec $n = 11$):

(50001037, 1.0000456), (50002037, 0.9997580), (50003039, 0.9998901),
(50004049, 0.9995318), (50005079, 1.0003779), (50006093, 1.0002476),
(50007101, 1.0005291), (50008129, 0.9999471), (50009143, 1.0000493),
(50010157, 0.9998406), (50011019, 0.9997204), (50012029, 1.0002561).

La valeur moyenne des exemples ci-dessus étant 1.000016182....

Pour $n = 100$ les résultats numériques (avec les mêmes nombres premiers) sont quasi-identiques et conduisent à une moyenne de 0.999796908....

Répartition des p par nombre de solutions

Le Programme 1 de [Gr3] (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 $q_p(z) = 0$.

Dans ce cas, les résultats numériques sont remarquablement cohérents avec la répartition probabiliste que nous allons préciser:

cas de 0 solutions:	proportion: 0.3694945...;	probabilité: 0.367879...,
au moins 1 solution:	proportion: 0.6305054...;	probabilité: 0.632120...,
au moins 2 solutions:	proportion: 0.2646531...;	probabilité: 0.264241...,
au moins 3 solutions:	proportion: 0.0805782...;	probabilité: 0.080301....

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).

Cas des solutions "exceptionnelles"

Lorsque $q_p(a) = 0$ pour $p \gg a$, on parlera de *solutions exceptionnelles* pour les puissances $a^j \in [2, p-1[$, $j = 1, \ldots, h_p(a)$; on verra plus loin que l'on peut considérer qu'il ne s'agit que d'une question de répartition et non d'une dépendance probabiliste.

Ce type de "répétitions" se produit aussi en dehors de l'existence de $a \ll p$ tel que $q_p(a) = 0$ (ce qui sera un point fondamental de justification d'une heuristique probabiliste, cf. § 4.2).

Remarque 4.1. On peut aussi faire le même genre d'analyse sur $\lambda_p(z) = z\, q_p(z)$, $z \in [2, p-1[$, en étudiant le nombre de solutions à $\lambda_p(z) = v$, v donné dans $[0, p[$, sachant que le résultat de [H-B] donne aussi leur répartition uniforme; pour $10^3 \leqslant p \leqslant 10^3 + 10^4$ il y a 1168 nombres premiers, et on a retenu le nombre N de cas pour lesquels il y a au moins 4 solutions:

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

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

La moyenne cumulée observée pour le nombre N est de 22; or $\frac{22}{1168} \approx 0.0188...$, et la probabilité pour "au moins 4 solutions à $\lambda_p(z) = v$" (analogue à celle relative à $q_p(z) = u$) est égale à 0.0189... (Remarque 4.6 (iv)).

4.2. Définitions des invariants $m_p(u)$ et M_p

On considère le nombre $m_p(u)$ de répétitions de $z \in [2, p-1[$ ayant le même quotient de Fermat $u \in [0, p[$ fixé, puis $M_p = \sup_{u \in [0,p[} \big(m_p(u)\big)$. On obtient alors une stabilité remarquable pour M_p, fonction très régulière de p pouvant faire l'objet de l'heuristique suivante:

Heuristique 4.2. *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 quotient de Fermat est* $O(\log(p))$ *pour tout nombre premier* $p \geqslant 2$.

Solutions exceptionnelles vs solutions abondantes

Le cas des solutions exceptionnelles pouvant poser question par le fait que les solutions données par les $h := h_p(a)$ premières puissances de a ne sont pas aléatoires et de ce fait semblent dépendantes au plan probabiliste, analysons l'heuristique précédente afin de justifier qu'il n'en est rien.

Soit $g \in \mathbb{Z}$ une racine primitive modulo p. Supposons qu'il existe $m_p(0) = O(\log(p))$ solutions $z_i \in [2, p-1[$ à $q_p(z) = 0$ (on parle alors de *solutions abondantes* dans $[2, p-1[$ car on a $m_p(0) \approx M_p$); on a $z_i \equiv g^{t_i} \pmod p$, $t_i \in \mathbb{Z}/(p-1)\mathbb{Z}$. C'est exclusivement une propriété de p et de l'intervalle $[1, p[$ et on peut admettre que les t_i sont aléatoires. De plus ils ne sont définis qu'à un automorphisme près de $\mathbb{Z}/(p-1)\mathbb{Z}$.

Ensuite, toujours dans le cas de solutions abondantes z_i, on peut se demander si $a \ll p$ (e.g. $a = 2, 3, \ldots$) est tel que $q_p(a) = 0$; ceci implique par exemple $z_i = a^i \in [2, p-1[$, pour tout $i = 1, \ldots, h \leqslant m_p(0)$, et constitue un sous-cas moins probable, l'ensemble $\{t_i,\ 1 \leqslant i \leqslant h\}$ d'exposants correspondant étant *nécessairement* égal à $\{k, 2\,k, \ldots, h\,k\}$ si $a \equiv g^k \pmod p$ (pour a donné, on peut choisir g telle que $k = \frac{p-1}{d}$, $d = o_p(a)$, car $d > h$, auquel cas $i\,k < p\ \forall i$). La situation la plus générale étant que l'ensemble des $m_p(0)$ solutions abondantes est mixte de la forme:

$$\{b, b^2, \ldots, b^{h'}, z_{h'+1}, \ldots, z_{m_p(0)}\}, \qquad \text{avec } 0 \leqslant h' \leqslant m_p(0),$$

où $b \in [2, p-1[$ est la solution minimale, toute valeur $h' \in [0, O(\log(p))]$ étant rencontrée. Noter que la probabilité d'une solution minimale $b < \sqrt{p}$ est inférieure à $\frac{1}{\sqrt{p}}$. Le cas $b = a \ll p$ (cas exceptionnel) n'étant alors qu'un hasard pour lequel on a *mécaniquement* $t_i \equiv i\,k \mod (p-1)\mathbb{Z}$ pour presque tout i en raison de la proximité de h et $m_p(0)$. Autrement dit, on a un contexte "p-adique" sur lequel se greffe une considération Archimédienne. Voir le § 4.3 pour l'aspect numérique des solutions abondantes et la Remarque 4.3 pour un éclairage complémentaire.

Expérimentation numérique sur M_p.

Donnons quelques aspects numériques (Programme 3 de [Gr3]):

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

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

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

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

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 (listes L à p éléments) on obtient pour $p = 48543217$, $M_p = 10$, $\log(p) \approx 17.698...$, et $M_p/\log(p) \approx 0.5650...$.

(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:

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

On constate que les valeurs de z ne sont pas du type $a \ll p$, mais que $M_p = 7$ est réalisé par cinq valeurs de u.

(δ) *Cas des solutions exceptionnelles.* Le cas $a = 2$, avec $q_{1093}(a) = 0$, conduit à la série de valeurs suivantes pour (p, M_p) $(1039 \leqslant p \leqslant 1163)$:

$$\begin{aligned}
&(1039, 7),\ (1049, 5),\ (1051, 5),\ (1061, 5),\ (1063, 5),\ (1069, 5),\\
&(1087, 5),\ (1091, 5),\ (1093, 11),\ (1097, 7),\ (1103, 7),\ (1109, 6),\\
&(1117, 5),\ (1123, 5),\ (1129, 5),\ (1151, 5),\ (1153, 6),\ (1163, 6).
\end{aligned}$$

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 $z = 9, 2.9, 2^2.9, 71, 2^3.9, 2.71, 2^4.9, 2^2.71, 2^5.9, 2^3.71, 2^6.9$, et que la valeur $q_p(z) = 960$ se produit aussi 11 fois, pour $z = 13, 2.13$, $2^2.13$, 93, $2^3.13$, 2.93, $2^4.13$, $2^2.93$, $2^5.13$, $2^3.93$, $2^6.13$. On a donc $M_p = m_p(624) = m_p(960) = 11$.

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 $q_p(z) = 297548$ sont: 3389, 8102, 3.3389, 3.8102, $3^2.3389$, 51550, $3^2.8102$, $3^3.3389$, 3.51550, $3^3.8102$, 236000, $3^4.3389$, 340292, $3^2.51550$, $3^4.8102$, 3.236000, $3^5.3389$.

Il est clair que s'il existe $a \ll p$ tel que $q_p(a) = 0$ (solutions exceptionnelles), ceci peut conduire à une plus grande valeur de $M_p = m_p(u_0)$ puisque si $q_p(z_0) = u_0$, alors on a les solutions $a^j z_0$ pour tout $j \leqslant \lfloor \frac{\log(p)}{\log(a)} - \frac{\log(z_0)}{\log(a)} \rfloor$. Dans le cas $q_p(2) = u_0 \neq 0$, on obtient systématiquement $O(\log(p))$ solutions à $q_p(z) = u_0$ en plus peut-être des $O(\log(p))$ solutions attendues. Mais ceci ne modifie pas l'heuristique en $O(\log(p))$ pour M_p.

4.3. Etude numérique de $m_p(0)$

Ici, nous imposons la valeur $u = 0$ pour l'étude des répétitions; si l'on se restreint aux nombres premiers p tels que $m_p(0) = O(\log(p))$ (solutions abondantes), il y a une très importante raréfaction des nombres premiers p.

Recherche des solutions abondantes ($m_p(0) = O(\log(p))$)

Nous allons constater qu'il existe des valeurs de p où $m_p(0) = O(\log(p))$ sans que cela ne provienne d'un $a \ll p$ tel que $q_p(a) = 0$.

Les couples $(p, m_p(0))$ correspondants, pour $p < 10^5$, 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 $m_p(0) \geqslant 6$ et $2 \leqslant p \leqslant 1.5 \times 10^5$, ainsi que les solutions $z \in [2, p-1[$ à $q_p(z) = 0$ (Programme 2 de [Gr3]):

(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}

En continuant jusqu'à $p \approx 10^6$, on obtient les nombres premiers suivants:

150559, 199783, 203773, 213949, 229939, 237283, 261761, 286751, 288929, 303089, 339139, 342373, 381853, 384611, 385657, 475897, 491531, 528679, 534851, 553699, 559831, 560317, 565937, 571933, 577069, 584791, 587123, 602227, 602627, 616513, 622159, 631549, 634609, 634979, 663587, 728471, 733277, 747871, 757403, 767071, 778187, 781283, 785779, 787079, 797897, 800677, 804367, 824753, 879239, 893609, 907589, 921001, 997961,

pour lesquels on a $m_p(0) = 6$ sauf pour $p = 491531$ où $m_p(0) = 7$ et où les solutions z sont données par six puissances de $b = 7$ et $397783 = 17 \times 23399$; de même pour $p = 534851$, où $m_p(0) = 7$, les solutions z sont données par sept puissances de $b = 6$ (cas avec solutions en partie exceptionnelles).

Par contre, on a $m_p(0) = 7$ pour $p = 804367$ et la liste des solutions {100933, 434207, 586707, 654355, 677456, 750045, 751958}, puis $m_p(0) = 8$ pour $p = 728471$ et la liste {36709, 159316, 241830, 288664, 418571, 443653, 653451, 679977} et enfin $m_p(0) = 7$ pour $p = 997961$ et la liste {196462, 324572, 505976, 517837, 612235, 636080, 990873}.

Comparaison de $\mathbf{Prob}(m_p(0) \geqslant n)$ et $\mathbf{Prob}(q_p(a') = 0)$

En utilisant la probabilité donnée plus loin (Remarque 4.6 (i)), on trouve que pour $p \approx 5 \times 10^5$ la probabilité d'un cas de solutions abondantes avec $m_p(0) = 6$ est

égale à $0.000594... \approx \frac{1}{p^{1+\epsilon}}$ avec $\epsilon \approx -0.433916...$, ce qui en termes de solutions exceptionnelles qui proviendraient d'un $a' \ll p$ (a' fictif fixé) donnerait, pour $h_p(a') = 6$, $a' = 8$ ou 9 en moyenne, qui doit être considérée comme déjà "trop grand" si l'on avait prévu d'étudier le cas de a donné petit ($a = 2$ par exemple); en effet, on a pour $p \approx 5 \times 10^5$:

$$h_p(2) = 18, \quad h_p(3) = 11, \quad h_p(4) = 9, \quad h_p(5) = 8, \quad h_p(6) = 7,$$
$$h_p(7) = \lfloor 6.743... \rfloor, \quad h_p(8) = \lfloor 6.310... \rfloor, \quad h_p(9) = \lfloor 5.972... \rfloor, \qquad \text{etc.}$$

Autrement dit, $m_p(0) \geqslant 6$ (dans le cadre abondant) est plus probable que l'existence de a' fixé tel que $q_p(a') = 0$, dans la mesure où il correspondrait à un a' moyen (fictif), non "très petit par rapport à p" (probablement $a' = O(\log(p))$).

Si l'on écrit les probabilités sous la forme $\text{Prob}\big(q_p(a') = 0\big) = \frac{1}{p^{1+\epsilon}}$, on obtient (pour $p \approx 5 \times 10^5$), le tableau suivant:

$$(a' = 2, \epsilon \approx +1.845); \qquad (a' = 3, \epsilon \approx +0.403); \qquad (a' = 4, \epsilon \approx +0.044);$$
$$(a' = 5, \epsilon \approx -0.124); \qquad (a' = 6, \epsilon \approx -0.284); \qquad (a' = 7, \epsilon \approx -0.434);$$
$$(a' = 8, \epsilon \approx -0.434); \qquad (a' = 9, \epsilon \approx -0.572).$$

Pour a' assez grand, le ϵ est négatif, donnant une probabilité supérieure à $\frac{1}{p}$. En décroissant 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 $\epsilon \approx 1.845...$. La probabilité $\text{Prob}\big(m_p(0) \geqslant n\big)$ est supérieure à celle qui proviendrait d'une solution exceptionnelle $a' \ll p$ fictive fixée assez petite.

Remarque 4.3. On pourrait se placer dans n'importe quel intervalle de $\mathbb{Z}$, translaté modulo p, $I_p^{(t)} := [-t\,p + 1, (-t+1)\,p[$, $t \in [0, p[$, en renormalisant de la façon suivante: on remplace $q_p(x)$ par $x\,q_p(x) = \lambda_p(x)$ (cf. Lemme 3.4 et Remarque 4.1) et on considère l'application T définie par $T(z) = z - t\,p$ pour tout $z \in [1, p[$. Si $a \in [1, p[$ est fixé et est tel que $aq_p(a) = 0$, il vient facilement:

$$T(a^j)\,q_p(T(a^j)) \equiv a^j\,q_p(a^j) + t \equiv t \pmod{p},$$

pour tout j tel que $a^j \in [1, p[$; comme $T(a^j) \in I_p^{(t)}$, on a bien translaté les solutions exceptionnelles (relatives à $u = 0$ dans $I_p^{(0)}$) en des solutions exceptionnelles relatives à $u = t$ dans $I_p^{(t)}$. Un calcul identique montre que les éventuelles solutions abondantes $z_i \in [1, p[$ (pour $u = 0$) sont translatées dans $I_p^{(t)}$ par l'opération T en solutions abondantes (pour $u = t$) et inversement, ce qui relativise les deux notions abondantes/exceptionnelles, ainsi que le phénomène Archimédien à l'origine des solutions exceptionnelles.

Une étude numérique (non reproduite ici) montre que les valeurs statistiques $(m_p(\bullet), M_p)$ sur $I_p^{(t)}$, sont analogue à celle sur $I_p^{(0)}$, ce qui fait que nous pouvons supposer $t = 0$ avec les données et définitions habituelles.

4.4. Sur l'existence d'une loi binomiale pour $m_p(0)$

L'étude précédente conduit à une heuristique utilisant une loi binomiale (majorante) de paramètres $\big(p-1, \frac{1}{p}\big)$, car on peut considérer que l'on réalise n "tirages" $z \in [1, p[$ (ensemble à $p-1$ éléments) pour lesquels on regarde combien de fois on obtient l'événement $q_p(z) = 0$ (ou plus généralement $q_p(z) = u$, $u \in [0, p[$ fixé, si l'on prend en compte les résultats du § 4.2). On néglige le biais provenant de $z = 1$ et $z = p-1$. La relation de dépendance rappelée Remarque 3.5 (ii) conduit à supposer n assez petit ($n \ll p$). Le second paramètre $\frac{1}{p}$ est une approximation de $\mathrm{Prob}\big(q_p(z) = u\big)$. Par conséquent, on devrait remplacer $\frac{1}{p}$ par $\frac{1}{p^{\kappa(z)}}$, $\kappa(z) > 1$.

On vérifie que cela ne modifie pas la nature des résultats ultérieurs (Lemmes 4.5, 4.7, 4.8, Théorème 4.9) et conduit à des probabilités majorantes. Aussi on conservera $(p-1, \frac{1}{p})$ par commodité.

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

$$\binom{p-1}{n} \frac{1}{p^n} \left(1 - \frac{1}{p}\right)^{p-1-n} = \binom{p-1}{n} \frac{1}{p^{p-1}} (p-1)^{p-1-n}.$$

Heuristique 4.4. *Soit $u \in [0, p[$ fixé. Soit $n \geqslant 0$, $n \ll p$; alors la probabilité d'avoir au moins n valeurs $z_1, \ldots, z_n \in [2, p-1[$ telles que $q_p(z_j) = u$ pour $j = 1, \ldots, n$ (i.e., $m_p(u) \geqslant n$), est donnée par l'expression:*

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

Lemme 4.5. *On a*

$$\frac{1}{p^{p-1}} \sum_{j=n}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} < \frac{1}{p^n} \binom{p-1}{n}$$

pour tout $n \leqslant p-1$.

Démonstration. Vérifions que $\sum_{j=n}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} < \binom{p-1}{n} p^{p-1-n}$ pour tout $n \leqslant p-1$. On considère, pour $0 \leqslant n \leqslant N$, $t \in]1, \infty[$, 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 $t = p$, $N = p-1$. ∎

Remarques 4.6.

(i) On a, pour $n \ll p$, la formule plus commode ($p \to \infty$) $\mathrm{Prob}\big(m_p(u) \geqslant n\big) = 1 - \big(1 - \frac{1}{p}\big)^p \frac{p}{p-1} \sum_{j=0}^{n-1} \frac{1}{(p-1)^j} \binom{p-1}{j}$.

(ii) La probabilité d'avoir 0 solutions est $\big(1 - \frac{1}{p}\big)^p \frac{p}{p-1} \approx e^{-1} \approx 0.36788....$

(iii) Celle d'au moins une solution est proche de $1 - e^{-1} \approx 0.63212....$

(iv) Celle d'au moins 2 solutions est proche de $1 - 2\,e^{-1} \approx 0.264...$; pour au moins 3 (resp. 4) solutions, on obtient 0.0803... (resp. 0.0189...).

Application à la probabilité de nullité de $q_p(a)$

Maintenant, nous supposons que $u = 0$, que a est fixé et que $p \to \infty$. On a $\mathrm{Prob}\big(q_p(a) = 0\big) < \mathrm{Prob}\big(m_p(0) \geqslant h\big)$, où $h = \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$, puisque alors $a, \dots, a^h \in [2, p-1[$ sont h solutions distinctes. Or, lorsque $p \to \infty$, le rapport $\dfrac{\mathrm{Prob}\big(m_p(0) \geqslant h\big)}{p^{-h}\binom{p-1}{h}}$ (majoré par 1 d'après le Lemme 4.5) tend rapidement vers une constante $C_\infty(a)$, en décroissant, selon le résultat suivant:

Lemme 4.7.

(i) *On a pour p assez grand l'encadrement:*

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

(ii) *Il en résulte* $\mathrm{Prob}\big(q_p(a) = 0\big) < \mathrm{Prob}\big(m_p(0) \geqslant h\big) \approx C_\infty(a) \times \frac{1}{p^h}\binom{p-1}{h}$ *pour tout p assez grand, où la constante $C_\infty(a)$ vérifie $e^{-1} \leqslant C_\infty(a) < 1$.*

Démonstration. On a la minoration

$$\begin{aligned}
&\frac{p^h}{\binom{p-1}{h}} \times \frac{1}{p^{p-1}} \sum_{j=h}^{p-1} \binom{p-1}{j} (p-1)^{p-1-j} \\
&\quad = \Big(\frac{p-1}{p}\Big)^{p-1} \frac{p^h\, h!}{(p-h)\cdots(p-1)} \sum_{j=h}^{p-1} \frac{1}{j!} \frac{p-j}{p-1} \cdots \frac{p-1}{p-1} \\
&\quad = \Big(\frac{p-1}{p}\Big)^{p-1} \frac{p^h}{(p-1)^h} \sum_{j=h}^{p-1} \frac{h!}{j!} \frac{p-j}{p-h} \cdots \frac{p-1}{p-1} \times \frac{1}{(p-1)^{j-h}} \\
&\quad = \Big(\frac{p-1}{p}\Big)^{p-1-h} \Big[1 + \frac{p-(h+1)}{(p-1)(h+1)} + \cdots + \frac{p-(h+1)}{(p-1)(h+1)} \cdots \frac{p-j}{(p-1)\,j} + \cdots \\
&\qquad \cdots + \frac{p-(h+1)}{(p-1)(h+1)} \cdots \frac{p-(p-1)}{(p-1)(p-1)}\Big] > \Big(\frac{p-1}{p}\Big)^{p-1-h} = \Big(1 - \frac{1}{p}\Big)^{p-1-h}.
\end{aligned}$$

D'où facilement le résultat en considérant la minoration:

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

tous les termes négligés étant positifs et tendant vers 0 comme $O(\frac{\log(p)}{p^2})$. ∎

On écrira par abus $\mathrm{Prob}\big(q_p(a) = 0\big) < C_\infty(a) \times \frac{1}{p^h}\binom{p-1}{h}$, qui est le majorant obtenu lorsque $m_p(0) = h$. On obtiendra, au niveau de la preuve du Lemme 4.8, que ce majorant est $p^{-\left(\frac{\log_2(p)}{\log(a)} - \frac{\log_2(a)+1}{\log(a)} + O\left(\frac{\log_2(p)}{\log(p)}\right)\right)}$.

Donnons, sous les heuristiques précédentes, des majorants des probabilités d'avoir au moins $h_p(a) = \big\lfloor \frac{\log(p)}{\log(a)} \big\rfloor$ solutions exceptionnelles avec $a = 2$, pour p

croissant; ceci correspondrait au cas où le quotient de Fermat de a serait nul pour des p arbitrairement grands et il convient de voir que c'est numériquement peu compatible.

On écrit alors ces majorants sous la forme $\frac{1}{p^{1+\epsilon}}$ qui correspond à la probabilité exacte de au moins $h_p(a)$ solutions abondantes:

$p = 101$	probabilité $< 5.075... \times 10^{-4}$	$\epsilon = 0.6437...$
$p = 127$	probabilité $< 5.245... \times 10^{-4}$	$\epsilon = 0.5591...$
$p = 10007$	probabilité $< 6.310... \times 10^{-11}$	$\epsilon = 1.5498...$
$p = 200003$	probabilité $< 1.094... \times 10^{-15}$	$\epsilon = 1.8222...$
$p = 1000003$	probabilité $< 3.182... \times 10^{-18}$	$\epsilon = 1.9162...$
$p = 5000011$	probabilité $< 3.421... \times 10^{-22}$	$\epsilon = 2.2043....$

On confirmera dans la section suivante que ϵ tend vers l'infini très lentement. La dernière valeur de p pour laquelle $\epsilon < 1$ est $p = 1021$.

4.5. Conséquence principale – finitude des solutions

Soit $a \geqslant 2$ fixé. Sous l'Heuristique 4.4 on a, pour $p \to \infty$, $\mathrm{Prob}\big(q_p(a) = 0\big) < \mathrm{Prob}\big(m_p(0) \geqslant h\big) \approx C_\infty(a) \times \frac{1}{p^h}\binom{p-1}{h}$, où $h := \lfloor \frac{\log(p)}{\log(a)} \rfloor$ (Lemme 4.7 (ii)).

Lemme 4.8. *Soit $a \geqslant 2$ fixé. La série $\sum_{p>2} \frac{1}{p^h}\binom{p-1}{h}$ est convergente.*

Démonstration. On a $\frac{1}{p^h}\binom{p-1}{h} = \frac{1}{h!} \times \frac{(p-1)\cdots(p-h)}{p^h}$ que l'on peut majorer par $\frac{1}{h!}$. 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 $\frac{1}{p^h}\binom{p-1}{h} < \frac{h}{h!}$, où l'on a remplacé $\frac{h}{h!}$ par $\frac{\log(p)}{\log(a)}/\big(\frac{\log(p)}{\log(a)}\big)!$ où h désigne maintenant $\frac{\log(p)}{\log(a)}$ et $\frac{h}{h!} = \frac{1}{\Gamma(h)}$.

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

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

D'où $\frac{h}{h!} = \frac{1}{p^Y}$, où $Y = \frac{\log_2(p)}{\log(a)} + O(1)$ tend vers l'infini comme $\frac{\log_2(p)}{\log(a)}$, et la convergence de la série initiale. Pour toute constante $E > 1$, il existe p_0 assez grand tel que $Y > E$ et $\frac{h}{h!} < \frac{1}{p^E}$ pour tout $p \geqslant p_0$. ■

Rappelons que l'on parle de solutions abondantes si le nombre $m_p(0)$ de $z \in [2, p-1[$ tels que $q_p(z) = 0$ est au moins $O(\log(p))$. Les calculs précédents obtenus avec $h_p(a)$ sont valables pour toute expression en $O(\log(p))$ et on peut énoncer:

Théorème 4.9. *Soit $a \geqslant 2$ fixé. Si l'Heuristique 4.4 est vraie (existence d'une loi de probabilité binomiale pour $m_p(0)$), on a la majoration:*

$$\mathrm{Prob}\big(q_p(a) = 0\big) < C_\infty(a) \times \frac{1}{p^h} \binom{p-1}{h} < C_\infty(a) \times p^{-\left(\frac{\log_2(p)}{\log(a)} - \frac{\log_2(a)+1}{\log(a)} + O\left(\frac{\log_2(p)}{\log(p)}\right)\right)},$$

pour $p \to \infty$, où $h = \left\lfloor \frac{\log(p)}{\log(a)} \right\rfloor$ (partie entière) et $e^{-1} < C_\infty(a) < 1$.

Sous le principe de Borel–Cantelli, le nombre de p tels que l'on ait un cas de solutions abondantes dans $[2, p-1[$ est fini; a fortiori, le nombre de p tels que l'on ait $q_p(a) = 0$ est fini.

Remarques 4.10.

(i) Les majorations utilisées pour le Lemme 4.8 sont assez bonnes car, pour $a = 2$, les séries $\sum_{p \geqslant 2} \mathrm{Prob}\big(m_p(0) \geqslant h\big)$, $\sum_{p \geqslant 2} \frac{1}{p^h} \binom{p-1}{h}$, et $\sum_{p \geqslant 2} \frac{h}{h!}$, convergent respectivement vers 1.65613..., 2.09444..., 6.27613.... Lorsque a augmente, la limite de la série $\sum_{p \geqslant 2} \mathrm{Prob}\big(m_p(0) \geqslant h\big)$ (censée donner une approximation du nombre de solutions) devient assez grande en raison du terme négatif dans l'exposant $\frac{\log_2(p)}{\log(a)} - \frac{\log_2(a)+1}{\log(a)} + O\big(\frac{\log_2(p)}{\log(p)}\big)$. Un calcul exact de $\binom{p-1}{h}$ via la fonction Γ donne:
$Y = \frac{\log_2(p)}{\log(a)} - \frac{\log_2(a)+1}{\log(a)} + \frac{1}{2}\frac{\log_2(p)}{\log(p)} - \frac{1}{2}\frac{\log_2(a) - \log(2\,\pi)}{\log(p)} + \frac{O(1)}{\log^2(p)}$.

(ii) Le fait que l'on puisse choisir E arbitrairement grande dans la preuve du lemme (à condition de sommer à partir d'un p_0 extrêmement grand) montrerait une loi de raréfaction brutale des solutions pour $p \to \infty$. En utilisant l'expression de Y ci-dessus, on obtient les exemples suivants (mais p_0 dépend beaucoup de l'approximation choisie pour Y):
Si $a = 2$ et si l'on veut atteindre $E = 1$, il suffit d'avoir $p_0 \geqslant 17$; pour $E = 2$, il faut $p_0 \geqslant 577$. Pour $a = 3$, il suffit d'avoir $p_0 \geqslant 1399$ (resp. $p_0 \geqslant 46505941763$). Pour $a = 5$ et $E = 1$, $p_0 = 168991001$, et pour $E = 2$, on obtient $p_0 \approx 4.817... \times 10^{45}$. Dès que a augmente, p_0 devient inaccessible: pour $a = 13$, on a $p_0 \approx 6.607... \times 10^{36}$ pour $E = 1 + 10^{-6}$, et $p_0 \approx 6.268... \times 10^{507}$ pour $E = 2$; pour $a = 23$, on a $p_0 \approx 4.476... \times 10^{81}$ pour $E = 1 + 10^{-6}$ et $p_0 \approx 3.491... \times 10^{1952}$ pour $E = 2$.

Cette rapide croissance de p_0, pour E raisonnable, laisse la possibilité d'avoir $q_p(a) = 0$ pour de très grands $p < p_0$, inaccessibles par ordinateur, mais en nombre conjecturalement fini; on peut y voir un rapport avec l'exemple donné au § 3.7 ($a = 5, p = 188748146801$) car si l'on calcule Y pour ces données, on trouve $Y = 1.17773...$ qui, de façon remarquable, définit une probabilité seulement en $\frac{1}{p^{1.17773...}}$.

(iii) Pour tout p assez grand on a, en posant $\mathrm{Prob}\big(m_p(0) \geqslant h\big) = \frac{1}{p^{1+\epsilon(p,a)}}$, $\epsilon(p,a) < Y-1 \approx \frac{\log_2(p)}{\log(a)} - 1 - \frac{\log_2(a)+1}{\log(a)}$. La constante $\theta(a) := \frac{\log_2(a)+1}{\log(a)}$ prend les valeurs approchées suivantes: $\theta(2) \approx 0.914...$, $\theta(3) \approx 0.996...$, $\theta(4) \approx 0.957...$, $\theta(5) \approx 0.917...$, $\theta(6) \approx 0.884...$, ...

4.6. Densité des entiers A de quotients de Fermat $\neq 0$

D'après les résultats du § 2.3, appliqués à $A \in \mathbb{N}$, on est amené à considérer (par simple commodité) le produit infini formel $\widetilde{\mathcal{P}}(A) := \prod_{m \geqslant 1} \widetilde{\Phi}_m(A)$ qui est tel que tout nombre premier p impair, $p \nmid A$, en est un diviseur, à savoir $p \,|\, \widetilde{\Phi}_m(A)$ pour l'unique indice $m = o_p(A)$ (Lemmes 2.4, 2.5); on a alors $q_p(A) \neq 0$ si et seulement si p^2 ne divise pas $\widetilde{\mathcal{P}}(A)$ (Théorème 2.6). Pour $p = 2$, $q_2(A) \neq 0$ si et seulement si $A \equiv 3 \pmod 4$.

Comme $p^2 \,|\, \widetilde{\mathcal{P}}(A)$ équivaut à $p^2 \,|\, \widetilde{\Phi}_{o_p(A)}(A)$ ($p \neq 2$), la densité des $A \in \mathbb{N}$ tels que $p^2 \,|\, \widetilde{\mathcal{P}}(A)$ est égale à $\frac{\phi(o_p(A))}{p^2}$; en sommant sur tous les ordres $o_p(A)$ possibles, on obtient la densité $\frac{p-1}{p^2}$; la densité contraire ($p^2 \nmid \widetilde{\mathcal{P}}(A)$) est égale à $D_p := 1 - \frac{p-1}{p^2} = 1 - \frac{1}{p} + \frac{1}{p^2}$ (valable pour $p = 2$).

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; en particulier, le produit $\prod_{p \leqslant x} D_p$ donne la densité des $A \in \mathbb{N}$ tels que $p^2 \nmid \widetilde{\mathcal{P}}(A)$ pour tout $p \leqslant x$.

Remarque 4.11. De fait il existe un calcul direct de cette densité par dénombrement de type théorème chinois (Remarque 3.10) avec cette fois des Z_p^j tels que $q_p(Z_p^j) \neq 0$, et ceci pour la suite des nombres premiers $p \leqslant x$. Si $y = \prod_{p \leqslant x} p^2$, un calcul standard montre que le nombre de $A \in [1, y[$ tels que $q_p(A) \neq 0$ pour tout $p \leqslant x$ est exactement $\prod_{p \leqslant x}(p^2 - p + 1)$; d'où la densité précédente, exacte sur les intervalles de la forme $\big[1, \prod_{p \leqslant x} p^2\big[$.

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 $\prod\limits_{p \leqslant x} \big(1 - \frac{1}{p}\big) = \frac{e^{-\gamma}}{\log(x)} \times \big(1 + O\big(\frac{1}{\log(x)}\big)\big)$, où $\gamma \approx 0,577215...$ est la constante d'Euler (cf. [T1], § I.1.6, formule de Mertens), et $\prod\limits_{p \leqslant x} \big(1 + \frac{1}{p(p-1)}\big) \approx 1.9436...$, pour x assez grand, d'où $\prod\limits_{p \leqslant x} D_p = \frac{1.9436... \times e^{-\gamma}}{\log(x)} \times \big(1 + O\big(\frac{1}{\log(x)}\big)\big) = \frac{1.09125...}{\log(x)} \times \big(1 + O\big(\frac{1}{\log(x)}\big)\big)$. On a donc le résultat analytique suivant:

Théorème 4.12. *La densité des $A \in \mathbb{N}$ tels que $q_p(A) \neq 0$ pour tout nombre premier $p \leqslant x$, est égale à $O\Big(\frac{1}{\log(x)}\Big)$. De façon précise, pour x assez grand on a*

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

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 $2 \leqslant A \leqslant y = 10^4$, on trouve 665 valeurs de A telles que $q_p(A) \neq 0$ pour tout $p \leqslant x = 10^7$. Or $10^4 \times \frac{1.09...}{\log(10^7)} \approx 676...$ et 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 $A \in \mathbb{N}$, il y en a 95% tels que $q_p(A) = 0$ pour au moins un $p \leqslant 10^{10}$. Mais dans ces calculs $A \to \infty$ et, par exemple, $\frac{\log_2(p_0)}{\log(A)} \approx E > 1$ équivaut à $p_0 \approx \exp(A^E)$ si l'on fait référence à l'aspect probabilités.

Ceci est compatible avec une heuristique de finitude pour a fixé; les cas de $a = 47$ et 72 semblent être intéressants de ce point de vue (cf. § 3.7).

Par programme on obtient 2.76 solutions $p < 3 \times 10^9$ en moyenne pour $2 \leqslant a \leqslant 101$. On obtient 2.8 solutions $p < 10^{10} + 5 \times 10^9$ en moyenne pour $a \in \{5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$.

5. Conclusion

L'Heuristique 3.7, majorant $\mathrm{Prob}\big(q_p(a) = 0\big)$ par $\frac{1}{p\,(p-1)^2} \sum_{d\,|\,p-1} \phi(d)^2 < \frac{1}{p}$, est 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.

L'Heuristique 4.4, qui stipule l'existence d'une loi de probabilité binomiale pour $\mathrm{Prob}\big(m_p(0) \geqslant n\big)$, $n \ll p$, et qui implique la finitude des p conduisant à des solutions abondantes dans $[2, p-1[$ (Théorème 4.9), reste le point crucial pour interpréter l'existence possible de couples (a, p), $a \ll p$, tels que $q_p(a) = 0$, induisant une répartition exceptionnelle des $p-1$ solutions $Z \in [1, p^2[$.

Mais différentes observations justifient cette heuristique:

- Le tableau du § 4.1 montre l'adéquation avec les probabilités théoriques relatives au nombre de solutions à $q_p(z) = 0$, $z \in [2, p-1[$.
- L'étude numérique des §§ 4.2, 4.3, montre que le nombre $m_p(0)$ des répétitions $q_p(z_i) = 0$, $z_i \in [2, p-1[$ pour $i = 1, \ldots, m_p(0)$, est aussi $O(\log(p))$ (solutions abondantes) 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 cachée analogue, non triviale, reposant sur la construction même des $q_p([g^k]_p)$, $1 \leqslant k \leqslant p-1$, lorsque g est une racine primitive et $[\ ]_p$ la fonction résidu modulo p.
- Les résultats numériques du §§ 4.3, justifient la différence (importante) qu'il y a entre la situation précédente où $m_p(0) = O(\log(p))$ (solutions abondantes),

et la probabilité que ce $m_p(0)$ provienne de solutions exceptionnelles avec $a \ll p$ et $q_p(a) = 0$ $(a = 2, 3, \ldots)$. Autrement dit, rien n'empêche que la probabilité d'avoir $q_p(a) = 0$ ne soit très inférieure à celle d'avoir des solutions abondantes dans $[1, p[$, et une heuristique forte de finitude pourrait être que, en moyenne, $q_p(a) = 0$ pour 3 nombres premiers p.

- Enfin le nombre $M_p = \sup_{u\in[0,p[}\big(m_p(u)\big)$ est très stable en $O(\log(p))$ *pour tout nombre premier* $p \geqslant 2$, ce qui constitue certainement le phénomène le plus intéressant (voir en complément le calcul heuristique de [Gr2]). Une preuve de ce fait serait importante car elle entraînerait trivialement que $m_p(0)$ ne dépasse jamais $O(\log(p))$ ce qui renforcerait les observations précédentes.

Ceci dit, cette étude ainsi que les expérimentations numériques, me confortent dans la pertinence des conjectures de finitude que j'ai formulées dans le cadre très général du régulateur p-adique (normalisé) d'un élément η d'un corps de nombres K, Galoisien sur $\mathbb{Q}$ (cf. [Gr1], § 8). De plus, l'équivalent probabiliste

$$p^{-\left(\frac{\log_2(p)}{\log(a)} - \frac{\log_2(a)+1}{\log(a)} + O\left(\frac{\log_2(p)}{\log(p)}\right)\right)}, \qquad p \to \infty,$$

est universel pour tout corps K et tout élément η (engendrant un Galois module de $\mathbb{Z}$-rang $[K : \mathbb{Q}]$) en remplaçant a par le maximum des valeurs absolues des conjugués de η ([Gr1], Théorème 1.1).

Remerciements. Je remercie Gérald Tenenbaum pour sa contribution [T2], ainsi que l'Editeur de la revue pour ses suggestions de publication, et le Rapporteur pour ses remarques.

Références

[CDP] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. 66, 217 (1997), 433–449.

[EM] R. Ernvall and T. Metsänkylä, *On the p-divisibility of Fermat quotients*, Math. Comp. **66** (1997), no. 219, 1353–1365.

[G] A. Granville, *ABC allows us to count squarefrees*, Internat. Math. Res. Notices **19** (1998), 991–1009.

[Gr1] G. Gras, *Les θ-régulateurs locaux d'un nombre algébrique – Conjectures p-adiques*, Canadian Journal of Mathematics, to appear (2016). http://dx.doi.org/10.4153/CJM-2015-026-3

[Gr2] G. Gras, *Complément : Estimation numérique de M_p pour la loi de probabilité binomiale de paramètres* $(p-1, \frac{1}{p})$. https://www.researchgate.net/publication/277588496

[Gr3] G. Gras, *Programmes PARI*, https://www.researchgate.net/publication/294260146

[GM] H. Graves and M.R. Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, Journal of Number Theory **133** (2013), 1809–1813.

[Hat] 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.

[Hat] K. Hatada, *Chi-square tests for mod 1 distribution of Fermat and Fibonacci quotients*, Sci. Rep. Fac. Educ., Gifu Univ., Nat. Sci. **12** (1988), 1–2.

[H-B] 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

[KR] W. Keller and J. Richstein, *Solutions of the congruence* $a^{p-1} \equiv 1 \pmod{p^r}$, Math. Comp. **74** (2004), no. 250, 927–936.

[KR] W. Keller and J. Richstein, *The continuing search for Wieferich primes*, Math. Comp. **75** (2005), no. 251, 1559–1563.

[Mo] P. Moree, *Artin's Primitive Root Conjecture - A Survey*, In: The John Selfridge Memorial Volume, Integers **12** (2012), no. 6, 1305–1416.

[OS] A. Ostafe and I.E. Shparlinski, *Pseudorandomness and Dynamics of Fermat Quotients*, SIAM J. Discrete Math. **25** (2011), no. 1, 50–71.

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

[Si] J.H. Silverman, *Wieferich's criterion and the abc-conjecture*, Journal of Number Theory **30** (1988), 226–237.

[Sh] I.E. Shparlinski, *On Vanishing Fermat Quotients and a Bound of the Ihara Sum*, Kodai Math. J. **36** (2013), no. 1, 99–108.

[T1] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 3^e édition revue et augmentée, Coll. Échelles, Belin 2008.

[T2] G. Tenenbaum, *Divergence d'une série liée aux nombres premiers.* https://www.researchgate.net/ publication/263200414

[W] 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

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

Address: Georges Gras: Villa la Gardette, Chemin Château Gagnière, F–38520 Le Bourg d'Oisans, France.

E-mail: g.mn.gras@wanadoo.fr

Received: 19 November 2014; **revised:** 11 September 2015