Quadrature

Magazine de mathématiques pures et épicées

La mathématique ouvre plus d'une fenêtre sur plus d'un monde

Résultats du prix de fantaisies

Mélanges parfaits (I)

Nombres brésiliens

Sommes de carrés dans un corps fini

n°76

Magazine trimestriel
Avril-Juin 2010
8,50 euros
ISSN 1142-2785

9 782759 805044

EDP SCIENCES

Quadrature n° 76 (2010) 30–38

DOI: 10.1051/quadrature/2010005

Les nombres brésiliens

par Bernard Schott

Résumé.
Les nombres brésiliens sont une curiosité qui amuse les amateurs d'Olympiades mathématiques. Cet article reprend la notion, décrit quelques propriétés élémentaires de ces nombres, puis explore les différents liens avec d'autres concepts arithmétiques. Au fil des paragraphes, il s'intéresse à la question de la primalité, au cas particulier des nombres repunits et développe même quelques arguments de théorie analytique des nombres.

L'Amérique du Sud est non seulement la patrie des footballeurs virtuoses, mais également une terre où fleurissent des nombres bien particuliers :

- Les *nombres colombiens* ou auto-nombres sont des entiers, qui, dans une base donnée, ne peuvent pas s'écrire sous la forme $m + S(m)$, où m est un entier, appelé générateur, et $S(m)$ la somme des chiffres de l'entier m dans cette base[1]. Ces nombres ont été introduits en 1949 par le mathématicien indien **Dattatreya Ramachandra Kaprekar** (1905–1988). Par exemple, 2009 n'est pas colombien en base 10 car $2009 = 1990 + 1 + 9 + 9 + 0$, mais 2007 l'est (vérification laissée au soin du lecteur).
- Les *nombres brésiliens*, qui font l'objet de cet article, ont pour définition : un entier $n > 0$ est dit brésilien s'il existe un entier b, vérifiant $1 < b < n - 1$, pour lequel la représentation de n en base b s'écrit avec des chiffres tous égaux.
- Rappelons que, vers 1500, les Mayas (Pérou-Bolivie) et les Aztèques (Mexique) utilisaient un système de numération de base 20 appelé *système de numération vigésimal*.
- Il existe également les *nombres parfaits Canada*[2] décrits dans [6], mais ceux-ci se situent un peu plus au nord.

Après avoir rappelé l'origine des nombres brésiliens, seront successivement abordées les conditions pour qu'un nombre soit ou non brésilien, l'étude détaillée des nombres premiers brésiliens, avec l'utilisation du crible de Selberg et l'apparition d'une constante des nombres premiers brésiliens, et pour terminer, la recherche des carrés et puissances pures qui sont également brésiliens.

Il est fort possible que ce texte soit le premier jamais publié sur ces nombres brésiliens.

[1] Définition proposée par Alain Legendre.

[2] [6], exercice 700, p. 91.

I Origine des nombres brésiliens

En septembre 1994, lors de la neuvième *Olimpiada Iberoamericana de Matematica* qui se déroulait à Fortaleza, au Brésil, un exercice original, présenté par le Mexique, a été proposé aux étudiants. Cet énoncé a été publié dans [5]. Pierre Bornsztein l'a ensuite repris dans son livre *Hypermath* [3], exercice a35, page 7 :

« Un nombre $n > 0$ est dit « brésilien »[3] s'il existe un entier b vérifiant $1 < b < n-1$, pour lequel la représentation de n en base b s'écrit avec des chiffres tous égaux. Montrer que 1994 est brésilien et que 1993 ne l'est pas. »

Clairement, $b > 1$ car il n'existe pas de système de numération utilisant la base 1, et de plus, $b < n - 1$, sinon tout nombre n serait brésilien car s'écrivant $n = (11)_{n-1}$.

[3] Dans l'énoncé initial proposé en espagnol, le qualificatif utilisé était « sensato », ce qui se traduit littéralement par nombres « sensés » ; la traduction anglaise est devenue « sensible » numbers.

Séduit par cet exercice, je l'ai proposé en octobre 2007 sur le forum des *mathematiques.net*[4]. Cet article reprend et enrichit les résultats obtenus lors des différents messages qui ont été échangés à cette occasion[5]. Suite à cette discussion sur le forum, et à mon intervention auprès de Neil J.A. Sloane, cette séquence de nombres brésiliens figure dans l'OEIS[6] sous la référence A125134. Notons que l'article que vous lisez est proposé comme référence dans l'OEIS.

II Comment prouver qu'un nombre est ou non brésilien ?

II.1 Méthode

Nous sommes amenés à résoudre une succession d'équations diophantiennes :

Pour n donné, existe-t-il m, b et $q \geqslant 2$ dans $\mathbb{N}^*$ vérifiant :

$$n = m(1+b+b^2+\ldots+b^{q-1}) \qquad 1 \leqslant m < b < n-1. \quad (1)$$

Après avoir décomposé n en produit de facteurs premiers, il est alors possible de trouver les valeurs de m possibles $(m_1, m_2, \ldots, m_i, \ldots, m_k)$; en tenant compte des inégalités, ce sont tous les diviseurs de n excepté n lui-même.

Ensuite, pour chaque m_i , avec $i = 1, \ldots, k$, on obtient une nouvelle équation diophantienne à résoudre

$$\frac{n}{m_i} - 1 = b(1 + b + \ldots + b^{q-2}). \qquad (2)$$

Après avoir décomposé $\frac{n}{m_i} - 1$ en produit de facteurs premiers, il est alors possible de trouver les valeurs potentielles de b qui sont strictement supérieures à 1 :

$$1 < b_{i1} < b_{i2} < \cdots < b_{ir}.$$

Ce sont les diviseurs b_{ij} de $\frac{n}{m_i} - 1$ qui, pour $j = 1, \ldots, r$, vérifient la double inégalité provenant de (1) :

$$m_i < b_{ij} < n - 1. \qquad (3)$$

Enfin, pour chaque couple (m_i, b_{ij}) vérifiant cette dernière inégalité (3), on examine s'il existe $q \geqslant 2$ tel que :

$$\frac{n}{m_i} = 1 + b_{ij} + \ldots + b_{ij}^{q-1} = \frac{b_{ij}^q - 1}{b_{ij} - 1}. \qquad (4)$$

[4] URL du forum : http://www.les-mathematiques.net/phorum/.

[5] URL du fil sur les nombres brésiliens : http://www.les-mathematiques.net/phorum/read.php?5,350062,page=1.

[6] OEIS = « The On-Line Encyclopedia of Integer Sequences », URL de OEIS : http://www.research.att.com/~njas/sequences/index.html.

II.2 Application pour 2009

$$2009 = 7^2 \times 41 \Rightarrow m \in \{1, 7, 41, 49, 287\}.$$

Afin de ne pas alourdir le texte, seul le cas $m = 7$ sera étudié en détail.

- $m = 1$, pas de solution.
- $m = 7$, (2) devient

$$\begin{aligned} 286 &= b(1 + b + \ldots + b^{q-2}) \\ &= 2 \times 11 \times 13 \Rightarrow b \in \{2, 11, 13, 22, 26, 286\} \end{aligned}$$

  mais, en tenant compte de la double inégalité (3) $\Rightarrow 7 < b < 2008$, il suffit d'examiner $b = 11, 13, 22, 26, 286$, puis de les porter dans (2) pour vérifier s'il existe une solution q correspondante :
  $b = 11 \Rightarrow 287 \neq 1 + 11 + \ldots + 11^{q-1}$, et pas de solution pour $b = 11$;
  $b = 13 \Rightarrow 287 \neq 1 + 13 + \ldots + 13^{q-1}$, et pas de solution pour $b = 13$;
  $b = 22 \Rightarrow 287 \neq 1 + 22 + \ldots + 22^{q-1}$, et pas de solution pour $b = 22$;
  $b = 26 \Rightarrow 287 \neq 1 + 26 + \ldots + 26^{q-1}$, et pas de solution pour $b = 26$;
  $b = 286 \Rightarrow 287 = 1 + 286 \Rightarrow (b = 286, q = 2)$ est solution, et

$$2009 = 7(1 + 286) = (77)_{286}.$$

- $m = 41$, une seconde solution apparaît nécessitant l'utilisation, par exemple, de la lettre λ pour représenter 41 en base 48. Ainsi :

$$2009 = 41(1 + 48) = (\lambda\lambda)_{48}.$$

- $m = 49, 287 \Rightarrow$ pas de solution.

Finalement, $2009 = (77)_{286} = (\lambda\lambda)_{48}$ avec λ représentant 41 en base 48. Nous dirons que 2009 est 2 fois brésilien.

III Conditions suffisantes pour qu'un nombre soit brésilien

Suite aux exemples et calculs précédents, on constate qu'il existe des nombres brésiliens comme 1994, 2007, 2009, et des nombres non brésiliens comme 1993. On vérifie aisément que $1, 2, 3, 4, 5, 6, 9$ ne sont pas brésiliens, alors que $7 = (111)_2$, qui est ainsi le plus petit nombre brésilien, $8 = (22)_3$ et $10 = (22)_4$ le sont.

Théorème 1. *Si $n > 7$ n'est pas brésilien, alors n est un nombre premier ou le carré d'un nombre premier. Ainsi, tout nombre pair supérieur ou égal à 8 est brésilien.*

→ Tout nombre pair supérieur ou égal à 8 est brésilien.

Si $n \geqslant 8$, alors, $n = 2k = 2(k-1) + 2 = (22)_{k-1}$ avec $k - 1 > 2$ *i.e.* $k > 3$ *i.e.* $k \geqslant 4$.

→ Tout nombre impair s'écrivant $n = ak$, avec $a \geqslant 3$ et $k > a + 1$, est brésilien, car $n = ka = (k-1)a + a = (aa)_{k-1}$.

On en déduit qu'il existe une infinité de nombres brésiliens (suite des nombres pairs $\geqslant 8$).

Notons que la réciproque du théorème 1 est fausse, par exemple : $31 = (111)_5$ et $121 = (11111)_3$ sont brésiliens.

On relève l'existence de nombres dans chacun des quatre sous-ensembles suivants : nombres premiers et brésiliens, nombres premiers et non brésiliens, nombres composés et brésiliens, nombres composés et non brésiliens. Ces quatre ensembles forment d'ailleurs une partition de $\mathbb{N} \setminus \{0, 1\}$ dont les premiers éléments apparaissent dans le tableau ci-dessous.

Entiers	brésiliens	non brésiliens
premiers	7, 13, 31, 43, 73, 127, …	2, 3, 5, 11, 17, 19, …
composés	8, 10, 12, 14, 15, 16, …	4, 6, 9, 25, 49, …

Il existe donc des nombres premiers ou composés qui sont soit brésiliens, soit non brésiliens. Il paraît légitime d'essayer de caractériser les nombres qui sont à la fois premiers et brésiliens, puis ceux qui sont composés et non brésiliens.

IV Les nombres premiers dans la jungle brésilienne

Soit donc p premier et brésilien. Alors, la recherche de m, b et q dans $\mathbb{N}^*$ vérifiant l'équation (1) implique $m = 1$ et $p = 1 + b + b^2 + \ldots + b^{q-1}$. Ainsi, tout nombre premier et brésilien p supérieur ou égal à 7 est un nombre formé de 1 répétés q fois dans une base b.

Définition. Un nombre ne s'écrivant qu'avec des chiffres 1 dans une certaine base s'appelle un entier polymonadique ou encore repunit (rep-unit, répunit)[7].

[7] OEIS : suite A053696.

Nous adopterons la notation suivante pour les repunits afin d'alléger le texte :

$$[R(q)]_b = (\underbrace{11\ldots111}_{q \text{ fois}})_b.$$

Rappel du théorème sur la division des repunits. *Si s divise q, alors le repunit s'écrivant avec s chiffres divise le repunit qui en comprend q, c'est-à-dire que $[R(s)]_b$ divise $[R(q)]_b$.*

Démonstration. En effet, si $q = st$, alors :

$$\frac{[R(q)]_b}{[R(s)]_b} = \frac{b^q - 1}{b^s - 1} = b^{s(t-1)} + b^{s(t-2)} + \ldots + b^s + 1$$

ce qui conclut. □

On en déduit ce **corollaire sur les repunits premiers** :

Corollaire. *Si $p = [R(q)]_b$ est premier, alors nécessairement q est premier.*

De plus, ici, q doit être premier impair, sinon $q = 2$, or $p = (11)_b$ n'est pas brésilien. En conclusion, tout nombre premier brésilien p est de la forme :

$$p = [R(q)]_b = 1 + b + b^2 + \ldots + b^{q-1} = \frac{b^q - 1}{b - 1}$$
$$= (\underbrace{11\ldots111}_{q \text{ fois}})_b. \quad (5)$$

On peut alors énoncer :

Théorème 2 (nombres premiers brésiliens). *Tout nombre premier et brésilien p supérieur ou égal à 7 est un repunit qui s'écrit avec un nombre premier impair de 1 dans une base b.*

Remarquons que la réciproque du théorème 2 est fausse : un repunit peut s'écrire avec un nombre premier de 1 sans être premier. Le plus petit contre-exemple en base 10 est $111 = 3 \times 37$. On ignore s'il existe une infinité de premiers brésiliens.

V Les repunits premiers de la forêt amazonienne

Il nous faut rechercher les entiers polymonadiques s'écrivant avec un nombre premier impair de chiffres 1 dans une base b, et qui sont premiers en base 10. Nous allons d'abord considérer quatre cas particuliers : $b = 10$, $b = 2$, puis $b = q$, et b premier avant d'aborder le cas général $b \geqslant 2$. Enfin, nous établirons quelques propriétés vérifiées par ces repunits premiers.

V.1 Repunits en base $b = 10$

Les repunits premiers[8] en base 10 connus sont assez rares, mais on conjecture cependant qu'il en existe une infinité. On ne connaît que cinq repunits premiers, mais comme 11 n'est pas brésilien par définition, seuls les quatre repunits suivants sont des nombres premiers brésiliens en base 10 : R(19), R(23), R(317) et R(1031). Par ailleurs, on conjecture que R(49 081), R(86 453), R(109 297), R(270 343) sont également des repunits premiers.

Concernant ces quatre derniers repunits, le lecteur pourra se référer à [2, 7, 8, 13].

V.2 Repunits en base $b = 2$

On peut écrire :

$$[R(n)]_2 = 1+2+2^2+\ldots+2^{n-1} = \frac{2^n-1}{2-1} = 2^n-1 = M_n.$$

Ainsi, le repunit qui s'écrit en base 2 avec n fois le chiffre 1 est le n-ième nombre de Mersenne M_n.

Proposition 1. *Tout nombre de Mersenne est brésilien.*

L'historique chronologique du plus grand nombre premier connu montre la présence régulière des nombres de Mersenne dans ce palmarès. En 1876, Édouard Lucas démontrait à la main que M_{127} est premier, ce nombre restera d'ailleurs le plus grand nombre premier connu jusqu'en 1951, date à partir de laquelle la recherche de la primalité des nombres de Mersenne s'effectuera à l'aide d'ordinateurs. En septembre 2008, 46 nombres de Mersenne premiers étaient connus[9]. $M_2 = 3$ n'étant pas brésilien, il subsiste $M_3 = (111)_2 = 7$, $M_5 = 31$, $M_7 = 127$, M_{13}, M_{17}, M_{19}, M_{61}, M_{89}, ..., $M_{37\,156\,667}$, $M_{43\,112\,609}$.

Ce dernier nombre a été découvert le 23 août 2008 et est ainsi devenu le plus grand nombre premier brésilien connu.

V.3 Des nombres premiers brésiliens singuliers $b = q$

Les seuls nombres premiers[10] p pour lesquels $q = b$ dans l'expression (5)

$$p = \frac{q^q-1}{q-1} = (\underbrace{11\ldots111_q}_{q \text{ fois}})$$

correspondent[11] à $q = 2, 3, 19, 31, 7547$. Or si $q = 2$, alors $p = 3$, qui n'est pas brésilien. Il subsiste donc $(111)_3 = 13, [R(19)]_{19}, [R(31)]_{31}, [R(7547)]_{7547}$. On ignore s'il n'existe qu'un nombre fini de tels nombres premiers.

V.4 Repunits premiers en base b, avec b premier

Les résultats de ce paragraphe résultent en grande partie de l'étude réalisée par Paul T. Bateman[12] et Rosemarie M. Stemmler dans [1].

Ces nombres apparaissent dans le cadre de la résolution du problème de Waring, proposé en 1770 par Edward Waring : pour tout entier naturel m, existe-t-il un entier naturel s tel que tout entier soit la somme d'au plus s puissances m-ième d'entiers ?

Soient $\mathbb{K}$ un corps de nombres de degré n (c'est-à-dire une extension algébrique finie de $\mathbb{Q}$ qui est de dimension n lorsqu'elle est considérée comme un $\mathbb{Q}$-espace vectoriel), $O_{\mathbb{K}}$ l'anneau des entiers algébriques de $\mathbb{K}$ et $O_{\mathbb{K}}^m$ le sous-groupe additif engendré par les puissances m-ièmes des éléments de $O_{\mathbb{K}}$. C'est dans $O_{\mathbb{K}}^m$, sous-anneau de $O_{\mathbb{K}}$, que le *problème de Waring* doit être considéré, ce qui justifie son étude. Quand $m = p$ est un nombre premier, il n'est pas trop compliqué de caractériser les corps de nombres pour lesquels $O_{\mathbb{K}}^p = O_{\mathbb{K}}$, sauf quand le nombre premier p peut s'écrire sous la forme[13]

$$p = \frac{b^q-1}{b^s-1} \qquad (*)$$

avec b premier, q étant alors nécessairement une puissance de nombre premier et s le plus grand diviseur de q.

Trois remarques indispensables à la compréhension de ce paragraphe :

1. Les repunits premiers en base b, avec b premier[14], s'écrivent suite à la relation (5) de la page 32 :
$$p = \frac{b^q-1}{b-1} = 1 + b + b^2 + \ldots + b^{q-1}. \qquad (**)$$
Ils sont donc de la forme (*) avec q premier et $s = 1$.
2. Cependant, il existe des nombres premiers de la forme (*) qui ne sont pas des nombres brésiliens car non repunits. Le plus petit contre-exemple que l'on puisse exhiber est $17 = \dfrac{2^8-1}{2^4-1}$.

[8] OEIS : suite A004023.
[9] OEIS : suite A000043.
[10] Ce paragraphe fait suite à une intervention de Claude Becker sur le forum des maths.net.
[11] OEIS : suite A088790.
[12] Spécialiste américain de théorie des nombres ; ne pas confondre avec Harry Bateman (1882–1946).
[13] OEIS : suite A003424.
[14] OEIS : suite A023195.

3. Enfin, il existe des nombres premiers brésiliens s'écrivant sous la forme (**) mais dans une base b qui n'est pas un nombre premier. Nous noterons ces nombres (***), ils seront étudiés au paragraphe 5.5. Le plus petit exemple d'un tel nombre est $43 = \dfrac{6^3-1}{6-1} = (111)_6$.

Il apparaît que les nombres premiers de la forme (*) sont relativement rares, *a fortiori* il en est donc de même pour les nombres premiers brésiliens de la forme (**) avec b premier. Plus précisément, parmi les 9592 nombres premiers inférieurs à 10^5, on n'en dénombre que 28 de la forme (*) dont 20 seulement[15] sont des repunits premiers brésiliens de la forme (**). À l'aide du crible de Selberg (voir plus loin), on démontre le résultat suivant.

Proposition 2. *Soit $H(x)$ le nombre de nombres premiers $p \leqslant x$ et de la forme (*). Alors, pour x suffisamment grand, et en adoptant les notations de Vinogradov*[16]*, on a :*

$$H(x) \ll \frac{x^{1/2}}{(\log x)^2}.$$

On en déduit par sommation d'Abel que la série $\sum p^{-1/2}$ converge, la somme étant prise sur tous les nombres premiers brésiliens de la forme (*). Ceci nous permet d'énoncer :

Corollaire 1. *La série $\sum p^{-1/2}$ converge, la somme étant effectuée sur tous les nombres premiers brésiliens de la forme (**) avec b premier, chacun figurant selon la multiplicité de son écriture*[17] *sous la forme (**).*

Par ailleurs, Bateman et Stemmler ont constaté que parmi les nombres premiers p tels que $p < 1,275 \times 10^{10}$ de la forme (**), il y en a :
→ 776 s'écrivant $p = 1 + b + b^2 = (111)_b$;
→ 16 s'écrivant $p = 1 + b + b^2 + b^3 + b^4 = (11111)_b$;
→ 6 s'écrivant $p = 1 + b + \ldots + b^6 = (1111111)_b$ pour $b = 2$ (M_7), $b = 3, 5, 13, 17, 31$;
→ un seul s'écrivant $p = 1 + b + \ldots + b^{10}$, pour $b = 5$;
→ 3 s'écrivant $p = 1 + b + \ldots + b^{12}$, pour $b = 2$ (M_{13}), $b = 3, 5$;
→ un seul s'écrivant $p = 1 + b + \ldots + b^{16}$, c'est $M_{17} = 2^{17} - 1$;
→ un seul s'écrivant $p = 1 + b + \ldots + b^{18}$, c'est $M_{19} = 2^{19} - 1$;
→ un seul s'écrivant $p = 1 + b + \ldots + b^{60}$, c'est $M_{61} = 2^{61} - 1$.

Il ressort de ces données numériques que la majorité des nombres premiers de la forme (**) semble s'écrire $p = 1 + b + b^2 = (111)_b$. On peut d'ailleurs préciser :

Théorème 3. *Soit $P^3_{br}(N)$ le nombre de nombres premiers brésiliens $p \leqslant N$ et s'écrivant $p = 1+b+b^2$ avec b premier. Alors, pour N entier suffisamment grand, nous avons :*

$$P^3_{br}(N) \ll \frac{N^{1/2}}{(\log N)^2}.$$

Démonstration. On commence par noter que $P^3_{br}(N) \leqslant S(N)$ où l'on définit[18] :

$$S(N) := \sum_{\substack{p \leqslant N^{1/2} \\ p \text{ et } 1+p+p^2 \text{ premiers}}} 1.$$

On traite $S(N)$ en utilisant le théorème de Selberg (1947) que nous rappelons ci-dessous.

Le crible de Selberg. *$M \geqslant 1$ est un entier grand, $1 < z < M$ est un nombre réel, f est un polynôme à coefficients entiers naturels, $\mathcal{A} = \{f(1), f(2), \ldots, f(M)\}$ et on note :*

$$S(\mathcal{A}, M; z) := \sum_{\substack{n \in \mathcal{A} \\ p \mid n \Rightarrow p > z}} 1.$$

Enfin, pour tout entier $d \geqslant 1$, $\omega(d)$ compte le nombre de solutions de la congruence $f(x) \equiv 0 \pmod{d}$. On suppose que, pour tout nombre premier p, on a $1 \leqslant \omega(p) < p$. Selberg obtient alors la majoration suivante :

$$S(\mathcal{A}, M; z) \leqslant M \left(\sum_{m \leqslant z} \frac{\mu(m)^2 \omega(m)}{\varphi(m)} \right)^{-1} + z^2 \prod_{p \leqslant z} \left(1 - \frac{\omega(p)}{p} \right)^{-2} \qquad (6)$$

où μ est la fonction de Möbius et φ le totient d'Euler.

On utilise ce résultat de la façon suivante. Soit $f(x) = x(1 + x + x^2) \in \mathbb{N}[x]$ et $1 < z < N^{1/2}$. Si $p \leqslant N^{1/2}$ est premier tel que $1 + p + p^2$ soit aussi premier, alors :

(i) ou bien $p \leqslant z$,

[15] Ces nombres sont 7, 13, 31, 127, 307, 1093, 1723, 2801, 3541, 5113, 8011, 8191, 10 303, 17 293, 19 531, 28 057, 30 103, 30 941, 86 143 et 88 741.

[16] Notations très utilisées en théorie des nombres ; ainsi, la notation $f \ll g$ signifie $f = O(g)$.

[17] Par exemple : l'inverse de 31 (égal à $1 + 2 + 2^2 + 2^3 + 2^4 = 1 + 5 + 5^2$) est additionné deux fois.

[18] Démonstration ne figurant pas dans [1] et proposée par Olivier Bordellès.

(ii) ou bien $f(p)$ ne possède pas de facteur premier $\leqslant z$,

d'où l'on déduit que :

$$S(N) \leqslant \mathcal{S}\left(\mathcal{A}, N^{1/2}; z\right) + z.$$

La fonction ω est alors déterminée sur les nombres premiers par :

$$\omega(p) = \begin{cases} 1, & \text{si } p \equiv 2 \pmod 3 \\ 2, & \text{si } p = 3 \\ 3, & \text{si } p \equiv 1 \pmod 3. \end{cases}$$

Ainsi :

$$\omega(m) \geqslant \sum_{\substack{d|m \\ d\equiv 1 \bmod 3}} 1.$$

Donc :

$$\begin{aligned}\sum_{m\leqslant z} \frac{\mu(m)^2\omega(m)}{\varphi(m)} &\geqslant \sum_{m\leqslant z} \frac{\mu(m)^2}{\varphi(m)} \sum_{\substack{d|m \\ d\equiv 1 \bmod 3}} 1 \\ &= \sum_{\substack{d\leqslant z \\ d\equiv 1 \bmod 3}} \frac{\mu(d)^2}{\varphi(d)} \sum_{\substack{k\leqslant z/d \\ (k,d)=1}} \frac{\mu(k)^2}{\varphi(k)} \\ &> \sum_{\substack{d\leqslant z \\ d\equiv 1 \bmod 3}} \frac{\mu(d)^2}{d} \log\left(\frac{z}{d}\right) \\ &= \int_1^z \frac{1}{t}\left(\sum_{\substack{d\leqslant t \\ d\equiv 1 \bmod 3}} \frac{\mu(d)^2}{d}\right) \mathrm{d}t.\end{aligned}$$

On peut montrer que, pour tout réel $t \geqslant 2$, on a :

$$\sum_{\substack{d\leqslant t \\ d\equiv 1 \bmod 3}} \frac{\mu(d)^2}{d} > \frac{\log t}{4\zeta(2)}$$

de sorte que :

$$\sum_{m\leqslant z} \frac{\mu(m)^2\omega(m)}{\varphi(m)} > \frac{(\log z)^2}{8\zeta(2)}$$

et comme pour $z \geqslant 5$, on a :

$$\begin{aligned}\prod_{5\leqslant p\leqslant z}\left(1-\frac{3}{p}\right)^{-1} &\leqslant \prod_{5\leqslant p\leqslant z}\left(1-\frac{1}{p}\right)^{-2} \prod_{p\geqslant 5}\left(1-\frac{3}{p^2}\right)^{-1} \\ &< \frac{(\log z)^2}{3}\end{aligned}$$

on obtient en reportant dans (6) que :

$$S(N) < \frac{8\zeta(2)N^{1/2}}{(\log z)^2} + 4z^2(\log z)^4 + z$$

et le choix de $z = N^{1/4}(\log N)^{-3}$ donne le résultat pour N suffisamment grand. □

V.5 Repunits premiers en base b quelconque

Considérons maintenant la suite croissante de tous les nombres premiers brésiliens[19], c'est-à-dire qui s'écrivent sous la forme :

$$p = 1+b+b^2+\ldots+b^{q-1}, \quad b \geqslant 2, \quad q \geqslant 3, \quad q \text{ premier.}$$

On retrouve évidemment les précédents premiers brésiliens s'écrivant avec b premier, complétés par ceux s'écrivant avec b composé, référencés sous la forme (***) en remarque 3 du paragraphe précédent. Parmi les quatorze plus petits premiers brésiliens (ceux inférieurs à 1000), les nouveaux venus, à savoir ceux dont la base b est un nombre composé, sont écrits en gras :
$7 = (111)_2 = M_3$, $13 = (111)_3$, $31 = (111)_5 = (11111)_2 = M_5$, $\mathbf{43 = (111)_6}$, $\mathbf{73 = (111)_8}$, $127 = (1111111)_7$, $\mathbf{157 = (111)_{12}}$, $\mathbf{211 = (111)_{14}}$, $\mathbf{241 = (111)_{15}}$, $307 = (111)_{17}$, $\mathbf{421 = (111)_{20}}$, $\mathbf{463 = (111)_{21}}$, $\mathbf{601 = (111)_{24}}$, $\mathbf{757 = (111)_{27}}$.

L'examen des nombres premiers brésiliens inférieurs à 20 000 montre que, quand b est supérieur ou égal à 2, près de 90 % des nombres premiers brésiliens semblent également s'écrire[20] sous la forme $(111)_b$. Seuls quatre nombres premiers inférieurs[21] à 20 000 ne peuvent s'écrire que sous la forme de repunits contenant plus de trois fois le chiffre 1. Notons que $31 = (11111)_2 = (111)_5$ admet deux écritures brésiliennes.

Un dernier constat[22] : il existe 50 847 534 nombres premiers inférieurs à un milliard. Parmi ceux-ci, seuls 3880 sont premiers brésiliens (soit moins de 0,01 % des nombres premiers), dont 308 sont repunits dans une base b premier, soit environ 8 % des premiers brésiliens, et donc 3572 sont repunits dans une base b composée. Par ailleurs, parmi ces 3880 premiers brésiliens, 3825 sont de la forme $(111)_b$, soit un peu moins de 99 % (on retrouve la même proportion que pour les bases b premiers).

Le lecteur pourra démontrer qu'il n'existe pas de nombres premiers brésiliens repunits en base 9 (réponse à la fin de l'article après la conclusion).

V.6 Théorèmes et conjectures relatifs aux nombres premiers brésiliens

Euclide a le premier démontré qu'il existait une infinité de nombres premiers, puis Euler a démontré

[19] OEIS : suite A085104.
[20] OEIS : suite A002383.
[21] Ce sont $127 = M_7$, $1093 = (1111111)_3$, $2801 = (11111)_7$ et $19\,531 = (1111111)_5$.
[22] Établi à partir de OEIS : suites A023195 et A085104.

en 1737 que la somme des inverses des nombres premiers tendait vers l'infini. La conjecture des nombres premiers jumeaux, nombres tels que p et $p+2$ soient premiers, stipule qu'il existe une infinité de nombres premiers jumeaux, mais Viggo Brun a démontré en 1919 que la série des inverses des nombres premiers jumeaux convergeait.

Nous ignorons s'il existe une infinité de nombres premiers brésiliens, mais que peut-on dire de la somme des inverses de ces mêmes nombres premiers brésiliens ?

Sachant que l'on est confronté ici à un double problème :

1. La représentation $p = 1 + b + b^2 + \ldots + b^q$ avec $b, q \geqslant 2$ et $q+1$ premier n'est pas toujours unique. Par exemple, $31 = 1+2+2^2+2^3+2^4 = 1+5+5^2$.
2. Les entiers b et q dépendent de p.

On peut alors raisonner comme suit[23] : Soit $N \geqslant 1$ un entier fixé. Pour chaque nombre premier brésilien $p \leqslant N$, il existe un entier $b \geqslant 2$ et un entier $q \geqslant 2$ tels que $p \geqslant b^q$ de sorte que :

$$\sum_{\substack{p\leqslant N\\ p \text{ brésilien}}} \frac{1}{p} \leqslant \sum_{\substack{b^q\leqslant N\\ b,q\geqslant 2}} \frac{1}{b^q} \leqslant \sum_{2\leqslant b\leqslant \sqrt{N}} \frac{1}{b^2} \times \frac{1}{1-1/b}$$
$$= \sum_{2\leqslant b\leqslant \sqrt{N}} \left(\frac{1}{b-1} - \frac{1}{b}\right) = 1 - \frac{1}{\left[\sqrt{N}\right]} < 1.$$

On est en mesure d'énoncer le résultat qui suit :

Théorème 4 (la constante des nombres premiers brésiliens). *La série des inverses des nombres premiers brésiliens est convergente, et cette « constante des nombres premiers brésiliens » est comprise*[24] *entre* $0,3$ *et* 1.

Pour finir, en complément aux nombres de Mersenne étudiés dans ce chapitre, examinons rapidement à la loupe brésilienne deux autres ensembles de nombres historiques :

Proposition 3. *Les nombres de Fermat premiers sont non brésiliens, et les nombres de Fermat composés sont tous brésiliens.*

Démonstration. Supposons que F_n soit premier et brésilien. Alors on aurait :

$$1 + 2^{2^n} = 1 + b + \ldots + b^{q-1}$$

avec q premier impair, ce qui impliquerait que $b\left(1 + b + \ldots + b^{q-2}\right) = 2^{2^n}$. Ainsi, il existerait $r \geqslant 1$ tel que $b = 2^r$. Puisque b est pair, l'entier $1 + b + \ldots + b^{q-2}$ serait donc impair, et $b\left(1 + b + \ldots + b^{q-2}\right)$ ne pourrait jamais être une puissance de 2, d'où contradiction.

Supposons maintenant que F_n soit composé. On sait que tout nombre de Fermat n'est jamais égal à une puissance strictement supérieure à 1 de nombre premier[25], donc en particulier F_n n'est jamais un carré de nombre premier. Suite au théorème 1, si F_n est composé, F_n n'étant pas un carré, alors F_n est brésilien. La proposition est démontrée. □

Je propose cette conjecture relative aux nombres premiers de Sophie Germain[26] :

Conjecture 1. *Aucun nombre premier de Sophie Germain n'est brésilien.*[27]

Il est temps de s'intéresser maintenant au carré des nombres premiers.

VI Les nombres composés non brésiliens

À la suite du théorème 1, on vérifie que 4, 9, 25 et 49 ne sont pas brésiliens. Peut-on généraliser ce résultat pour tous les carrés de nombre premier ?

VI.1 Une nouvelle équation diophantienne

Il nous faut résoudre l'équation suivante :

$$p^2 = m(1 + b + b^2 + \ldots + b^n) \qquad (7)$$

$m \mid p^2$ donc $m \in \{1, p, p^2\}$ avec $1 \leqslant m < b < p^2 - 1 < p^2$, et donc $m = 1$ ou p.

→ Supposons $m = p$, alors l'équation (7) devient :

$$p = 1 + b + b^2 + \ldots + b^q$$

$\Rightarrow p - 1 = b[1 + b + \ldots + b^{q-1}]$, ainsi b divise $p - 1$
$\Rightarrow b \leqslant p - 1$;
mézalor, $m = p < b \leqslant p-1$, ce qui s'avère impossible.

→ Reste donc $m = 1$, ce qui nous permet d'énoncer :

Lemme 1. *Si p^2 est brésilien, alors nécessairement l'écriture de p^2 en base b est un repunit vérifiant : $p^2 = (11\ldots11)_b$ avec $1 < b < p^2 - 1$ et p premier.*

On est ainsi amené à résoudre :

[23] Démonstration proposée par Olivier Bordellès.

[24] La somme des inverses des quatorze plus petits premiers brésiliens (paragraphe 5.5) est supérieure à 0,32.

[25] *1001 Problèmes en Théorie Classique des Nombres*, J.M. de Koninck et A. Mercier, exercice 769.

[26] Un nombre premier p est appelé nombre premier de Sophie Germain si $2p + 1$ est également un nombre premier.

[27] Conjecture vérifiée, à l'aide d'une procédure Maple rédigée par Vincent Guenez, par les 3000 premiers nombres premiers de Sophie Germain.

VI.2 L'équation diophantienne $p^2 = 1 + b + \ldots + b^{q-1}$ avec $b,\ q,\ p$ premiers

Cette dernière équation a été résolue par Nagell[28] dans [11] à partir du cas général, avec $p = n$ entier naturel :

$$n^2 = 1+b+b^2+\ldots+b^{q-1}, \quad n > 1,\ b > 1,\ q > 1. \quad (8)$$

Nagell a prouvé que cette équation n'admet que deux solutions :
$[n = 20, b = 7, q = 4]$, soit $20^2 = 400 = (1111)_7$,
$[n = 11, b = 3, q = 5]$, soit $11^2 = 121 = (11111)_3$,
seul le cas $n = 11$, car 11 est premier, nous intéresse ici :

Théorème 5. *Le seul carré de nombre premier qui est brésilien est* $121 = 11^2 = (11111)_3$.

Corollaire 2. *Il existe une infinité de nombres non brésiliens.*

Démonstration. Il suffit de considérer la suite des carrés des nombres premiers, pour $p \geqslant 13$. □

VI.3 L'équation diophantienne $n^t = 1 + b + b^2 + \ldots + b^{q-1}$

Par curiosité, étendons nos recherches vers les puissances pures n^t qui sont des repunits brésiliens en base b. Nous sommes alors amenés à résoudre l'équation diophantienne de Nagell-Ljunggren[29] étudiée dans [9–11] :

$$n^t = 1+b+b^2+\ldots+b^{q-1} = \frac{b^q-1}{b-1}, \quad b,\ n,\ t > 1, q > 2. \quad (9)$$

Dans le cas général de l'équation (9), Yann Bugeaud et Maurice Mignotte émettent dans [4] les deux conjectures 2 et 3 suivantes, réécrites ici sous l'éclairage des nombres brésiliens :

Conjecture 2. *Il n'existe que trois puissances pures qui sont des nombres brésiliens repunits :* 121*,* 343 *et* 400.

Remarque. $343 = (111)_{18} = 7^3$ est la seule solution supplémentaire non carrée vérifiant l'équation (9) pour $n < 10\,000$.

Cependant, la conjecture suivante nous paraît plus réaliste :

Conjecture 3. *Il n'existe qu'un nombre fini de puissances pures qui sont des nombres brésiliens sous forme de repunit.*

T.N. Shorey a démontré dans [12] que cette conjecture 3 est vraie si la conjecture *abc* l'est. Rappelons une des formulations de cette **conjecture *abc*** qui permettrait de démontrer, si elle s'avérait exacte, quelques théorèmes importants en théorie des nombres :
Pour tout $\varepsilon > 0$*, il existe une constante* $K = K_\varepsilon$ *telle que, pour tous* a, b, c *entiers sans diviseur commun et vérifiant* $a + b = c$*, on ait :*

$$\max(|a|, |b|, |c|) \leqslant K_\varepsilon \gamma(abc)^{1+\varepsilon}$$

où $\gamma(n)$ *est le noyau sans facteur carré (ou radical) de* n*, c'est-à-dire le plus grand diviseur sans facteur carré de* n*.*

D'autres résultats ont été obtenus (un « Goldbach » des nombres brésiliens, l'étude des nombres k fois brésiliens...), cependant, il est temps de conclure. Cette étude des nombres brésiliens permet de revisiter différents résultats, conjectures, travaux de recherche actuels et vivants dans le domaine de la théorie des nombres. Une nouvelle fois, derrière un anodin problème d'olympiade, se cachent des domaines d'étude actifs et variés ; d'ailleurs, le lecteur empreint d'un vague à l'âme brésilien est invité à venir discuter du sujet sur le fil référencé au premier chapitre. Enfin, c'est à la suite d'un *« appel à collaborateurs »*[30] lancé sur le forum des mathematiques.net que j'ai proposé ce texte à *Quadrature*...

Réponse à la question du paragraphe 5.5: Il n'existe pas de repunits premiers en base 9 car $[R(q)]_9$ est le $\left(\frac{3^q-1}{2}\right)$-ième nombre triangulaire.

Remerciements

Je remercie l'ensemble des intervenants, parmi lesquels Claude Becker, du fil « 2007 est-il un nombre brésilien ? » ouvert sur le forum des mathematiques.net, ainsi que :

– Olivier Bordellès pour m'avoir invité à proposer un texte à *Quadrature*, puis pour les conseils prodigués pour l'écriture de cet article et les démonstrations des théorèmes 3 et 4 ;

[28] Trygve Nagell (1895–1988), mathématicien norvégien.
[29] Wilhelm Ljunggren (1905–1973), mathématicien norvégien.
[30] URL du fil : http://www.les-mathematiques.net/phorum/read.php?2,462376,462376#msg-462376.

– Yann Bugeaud qui m'a spontanément envoyé les documents dont il est auteur ou co-auteur ;

– Vincent Guenez pour l'écriture de procédures Maple qui m'ont permis d'approcher et de concrétiser quelques résultats divers ;

– Gregory Berhuy, Gilles Boutte, Alain Legendre et Norbert Verdier pour une dernière relecture valorisante de ce document ;

– enfin, le rapporteur de ce texte et Roger Mansuy, qui m'ont guidé avec patience tout au long de la rédaction de cet article.

Références

[1] P.T. Bateman et R.M. Stemmler, « Waring's problem for algebraic number fields and primes of then form $(p^r - 1)/(p^d - 1)$ », *Illinois J. Math.* **6** (1962) 142–156.

[2] L. Baxter, *New Probable Prime Repunit R(86543)*, Number Theory List (26/10/2000).

[3] P. Bornsztein, *Hypermath*, Éditions Vuibert (2001).

[4] Y. Bugeaud et M. Mignotte, « L'équation de Nagell-Ljunggren $(x^n - 1)/(x - 1) = y^q$ », *Enseign. Math.* **48** (2002) 147–168 ; MR 2003f:11043.

[5] *Crux Mathematicorum* **24**, n° 7 (Nov. 1998) 386–387.

[6] J.-M. de Koninck et A. Mercier, *1001 Problèmes en Théorie Classique des Nombres*, Éditions Ellipses (2004).

[7] H. Dubner, *New probable prime repunit R(49081)*, Number Theory List (09/09/1999).

[8] H. Dubner, *New probable prime repunit R(109297)*, Number Theory List (03/04/2007).

[9] W. Ljunggren, « Noen setninger om ubestemte likninger av formen $(x^n - 1)/(x - 1) = y^q$ », *Norsk. Mat. Tidsskr.* **25** (1943) 17–20.

[10] T. Nagell, « Note sur l'équation indéterminée $(x^n - 1)/(x - 1) = y^q$ », *Norsk. Mat. Tidsskr.* **2** (1920) 75–78.

[11] T. Nagell, « Sur l'équation indéterminée $(x^n - 1)/(x - 1) = y^2$ », *Norsk. Mat. Forenings Skrifter*, Sér. I, n°3 (1921) 17.

[12] T.N. Shorey, *Exponential Diophantine equations involving products of consecutive integers and related equations*, *Number Theory*, R.B. Bambah, V.C. Dumir et R.J. Hans-Gill éds., Hindustan Book Agency, 1999, 463–495.

[13] M. Voznyy, *New Probable Prime Repunit R(270343)*, Number Theory List (15/07/2007).

QUADRATURE

Appel à auteurs

Quadrature, magazine de mathématiques pures et appliquées, **s'adresse aux enseignants, étudiants, ingénieurs, amateurs de mathématiques**.

La plupart des articles requièrent un bon niveau de terminale scientifique ou une première année de premier cycle. Les auteurs sont des mathématiciens, des enseignants et des étudiants...

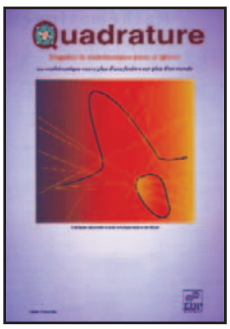
Quadrature est éclectique : certains articles présentent des mathématiques toutes récentes, tandis que d'autres donnent un nouveau point de vue sur des sujets traditionnels ou encore ressuscitent des questions de géométrie ancienne. On trouve également dans le magazine un **forum**, des **nouvelles**, des **notes de lecture**, des **articles d'histoire des mathématiques** et des **articles de réflexion en relation avec l'actualité**. Enfin, un large « coin des problèmes » permet aux lecteurs de poser des questions, qu'ils en connaissent la réponse ou pas.

Quadrature est ouvert, en particulier aux jeunes. Le magazine publie régulièrement des TPE (travaux personnels encadrés) de terminale et premier cycle d'université.

Vous souhaitez contribuer activement à la revue. Venez enrichir nos différentes rubriques et proposez-nous :

- ✔ articles de revue,
- ✔ brèves scientifiques,
- ✔ forum des lecteurs,
- ✔ manifestations,
- ✔ reportages,
- ✔ images mathématiques,
- ✔ analyses d'ouvrages et de logiciels,
- ✔ sites internet spécialisés en mathématiques,
- ✔ nouvelles, fantaisies mathématiques...

N'hésitez pas à prendre contact avec notre bureau de rédaction :



Quadrature
EDP Sciences
PA de Courtabœuf
17 avenue du Hoggar
BP 112
91944 Les Ulis Cedex A
Tél. : 01 69 18 75 75 • Fax : 01 69 07 45 17
E-mail : **quadrature@edpsciences.org**