COLLECTION
ASTROÏDE

MATHÉMATIQUES D'HIER ET D'AUJOURD'HUI

Sous la direction de
Richard PALLASCIO, CIRADE et dép. de mathématiques, UQÀM
et de Gilbert LABELLE, LACIM et dép. de mathématiques, UQÀM

MODULO

Nous reconnaissons l'aide financière du gouvernement du Canada par l'entremise du Programme d'Aide au Développement de l'Industrie de l'Édition (PADIÉ) pour nos activités d'édition.

RÉVISION : Serge Paquin et Corinne Kraschewski
CORRECTION D'ÉPREUVES : Corinne Kraschewski et Marie Théorêt
CONCEPTION GRAPHIQUE : Olena Lytvyn
MONTAGE ET TYPOGRAPHIE : Dominique Chabot et Carole Deslandes
ILLUSTRATIONS : Bertrand Lachance et Diane Mongeau
SURFACES EN 3D DE LA COUVERTURE : Gilbert Labelle

L'astroïde est une courbe mathématique plane ayant la forme d'une étoile à quatre pointes. C'est une hypocycloïde tracée par un point sur la circonférence d'un petit cercle tournant sans glisser à l'intérieur d'un grand cercle (le rayon du grand cercle étant 4 fois plus grand que celui du petit cercle). L'équation de l'astroïde rappelle celle du cercle et celle du théorème de Fermat puisque son équation cartésienne est $x^{2/3} + y^{2/3} = r^{2/3}$ où r est le rayon du grand cercle.

Mathématiques d'hier et d'aujourd'hui

233, av. Dunbar, bureau 300
Mont-Royal (Québec)
Canada H3P 2H4
Téléphone : (514) 738-9818 ou sans frais (888) 738-9818
Télécopieur : (514) 738-5838 ou sans frais (888) 273-5247
Site Internet : http://www.modulo.ca

Dépôt légal — Bibliothèque nationale du Québec, 2000
Bibliothèque nationale du Canada, 2000
ISBN 2-89113-**825**-2

Imprimé au Canada
1 2 3 4 5 04 03 02 01 00

13

Ces nombres qui nous fascinent

Jean-Marie De Koninck et Bernard R. Hodgson
Université Laval

L'anecdote est connue, mais elle vaut qu'on la rappelle, car elle met en lumière l'extraordinaire pouvoir de fascination des nombres. S'étant rendu au chevet de son protégé Srinivasa Ramanujan (1887-1920), le grand mathématicien anglais Godfrey H. Hardy (1877-1947) fit plaisamment remarquer combien le nombre 1729 que portait la voiture taxi qui l'avait amené lui semblait banal. Et de s'entendre rétorquer par son ami malade que, au contraire, ce nombre avait beaucoup d'intérêt, puisque c'était le plus petit entier positif pouvant s'écrire de deux manières différentes comme la somme de deux cubes parfaits :

$$1729 = 12^3 + 1^3 = 10^3 + 9^3.$$

On peut bien sûr considérer ce genre de remarque comme singulière, voire futile, mais pour peu que l'on se prête au jeu, on comprendra combien les nombres, la suite des entiers naturels par exemple, sont une intarissable source d'inspiration et d'émerveillement. C'est à ce genre de découverte que vous convie ce texte dans lequel nous relèverons les propriétés étonnantes de certains nombres fascinants[1] et tirerons au passage des conjectures sur des problèmes ouverts.

Une mise en garde s'impose toutefois. Il ne faut pas croire que le type de résultats présentés ici constitue l'essentiel du travail du mathématicien : le nombre n'est certes pas tout pour le mathématicien, et la plupart des recherches mathématiques actuelles portent sur des objets d'une complexité structurelle beaucoup plus vaste. Mais il reste que les nombres naturels, outre leurs applications abondantes et importantes, ont une vie propre et qu'ils représentent en quelque sorte un territoire commun, que partagent volontiers maints usagers des mathématiques (à tout le moins dans leurs « loisirs » mathématiques).

1. Insistons sur le fait que nous nous intéressons ici aux nombres *naturels* 0, 1, 2, 3, ..., aussi appelés *entiers non négatifs*; nous nous restreindrons parfois aux *entiers positifs* 1, 2, 3, etc.

Voici d'abord quelques balises pour faciliter la lecture du présent texte.

- Plusieurs des problèmes abordés ici se prêtent bien à une exploration systématique au moyen de l'ordinateur.
- Réciproquement, certaines réflexions théoriques viendront parfois guider l'exploration brute avec l'ordinateur et ainsi restreindre l'ampleur du champ d'investigation — sans quoi plusieurs des recherches indiquées deviendraient tout bonnement impraticables en raison de leur trop grande complexité.
- Les preuves présentées, délimitées par ■, ne sont pas essentielles à la poursuite de la lecture.
- Les sections de ce texte sont essentiellement indépendantes les unes des autres, de sorte qu'il n'est pas nécessaire d'avoir lu une section donnée avant de passer à une autre.

1. Quelques produits étonnants

Nous commençons par examiner quelques séries de produits présentant des régularités intéressantes.

A. Première série

Considérons par exemple le tableau suivant :

$$\begin{aligned} 1 \times 9 &= 9 \\ 12 \times 9 &= 108 \\ 123 \times 9 &= 1\,107 \\ 1\,234 \times 9 &= 11\,106 \\ 12\,345 \times 9 &= 111\,105 \end{aligned}$$

Une règle semble s'en dégager; pourriez-vous l'identifier et ainsi écrire d'un trait le résultat de la multiplication $123\,456 \times 9$ (sans effectuer le calcul) ?

Le tableau précédent ne vous a guère semblé frappant ? Modifions-le comme suit[2] :

$$\begin{aligned} 1 \times 9 + 2 &= 11 \\ 12 \times 9 + 3 &= 111 \\ 123 \times 9 + 4 &= 1\,111 \\ 1\,234 \times 9 + 5 &= 11\,111 \\ 12\,345 \times 9 + 6 &= 111\,111 \end{aligned}$$

Il est certainement facile d'écrire directement le résultat de $123\,456 \times 9 + 7$. Mais alors, comment expliquer la régularité apparente ?

Afin d'illustrer les phénomènes sous-jacents, examinons de plus près l'expression $(1\,234 \times 9) + 5$. Réécrivant $1\,234$ sous la forme $1\,111 + 111 + 11 + 1$, nous avons :

$$\begin{aligned} (1\,234 \times 9) + 5 &= ((1\,111 + 111 + 11 + 1) \times 9) + 5 \\ &= 9\,999 + 999 + 99 + 9 + (1 + 1 + 1 + 1 + 1) \\ &= (9\,999 + 1) + (999 + 1) + (99 + 1) + (9 + 1) + 1 \\ &= 10\,000 + 1\,000 + 100 + 10 + 1 \\ &= 11\,111. \end{aligned}$$

2. La régularité qui suit a été observée par le mathématicien français Édouard Lucas (1842-1891) dans ses célèbres *Récréations mathématiques*.

Nous voyons facilement que le même raisonnement[3] s'applique, par exemple, à l'expression $(123\,456\,789 \times 9) + 10$. De là, le passage aux produits du premier tableau, tel $123\,456\,789 \times 9$, se fait aisément.

Nous laissons au lecteur le soin de compléter et d'expliquer les tableaux suivants :

$$\begin{array}{r} (9 \times 9) + 7 = \\ (98 \times 9) + 6 = \\ (987 \times 9) + 5 = \end{array} \qquad \begin{array}{r} (1 \times 8) + 1 = \\ (12 \times 8) + 2 = \\ (123 \times 8) + 3 = \end{array}$$

B. Deuxième série

Les deux produits que voici,

$$37\,037\,037\,037 \times 12 = 444\,444\,444\,444 \text{ et}$$
$$37\,037\,037\,037 \times 21 = 777\,777\,777\,777,$$

laissent manifestement entrevoir l'existence d'une règle. Mais laquelle au juste ?

Le phénomène observable ici repose simplement sur le fait que $37 \cdot 3 = 111$. Il en résulte que, par exemple,

$$37 \cdot 12 = 37 \cdot 3 \cdot 4 = 444,$$
$$37 \cdot 21 = 37 \cdot 3 \cdot 7 = 777.$$

De là, le passage à un nombre de la forme

$$37\,037\,037 \ldots 037$$

(la séquence « 037 » étant répétée un certain nombre de fois) se fait facilement.

C. Troisième série

La dernière série de produits présentée dans cette section repose sur le nombre naturel 142 857. Observons les premiers multiples de ce nombre :

$$142\,857 \times 1 = 142\,857,$$
$$142\,857 \times 2 = 285\,714,$$
$$142\,857 \times 3 = 428\,571.$$

Nous pouvons tout de suite remarquer que les chiffres de ces produits sont toujours les mêmes et qu'ils se succèdent avec régularité. Mais pourquoi en est-il ainsi ?

Le phénomène sous-jacent est lié au développement décimal de la fraction 1/7, la séquence de chiffres « 142857 » constituant justement la *période* de cette fraction :

$$\frac{1}{7} = 0{,}142\,857\,142\,857\,142\,857 \ldots$$

---

3. Voici une façon équivalente de formuler l'argument :

$$\begin{aligned} (1\,234 \times 9) + 5 &= (1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4) \times (10 - 1) + 5 \\ &= 10^4 + 2 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 - 1 \cdot 10^3 - 2 \cdot 10^2 - 3 \cdot 10 - 4 + 5 \\ &= 10^4 + 10^3 + 10^2 + 10 + 1 \\ &= 11\,111. \end{aligned}$$

Il en résulte que

$$\frac{2}{7} = 0{,}285\ 714\ 285\ 714\ 285\ 714\ldots$$

$$\frac{3}{7} = 0{,}428\ 571\ 428\ 571\ 428\ 571\ldots$$

$$\frac{4}{7} = 0{,}571\ 428\ 571\ 428\ 571\ 428\ldots$$

$$\frac{5}{7} = 0{,}714\ 285\ 714\ 285\ 714\ 285\ldots$$

$$\frac{6}{7} = 0{,}857\ 142\ 857\ 142\ 857\ 142\ldots$$

Il peut être utile, pour bien voir ce qui se passe ici, d'effectuer à la main la division $1 \div 7$. Notons que les périodes des fractions précédentes peuvent toutes se lire par permutation cyclique des chiffres de « 142857 »; par exemple, la période de 3/7 est « 428571 ».

Il n'est donc pas surprenant que notre premier tableau se complète comme suit :

$$\begin{aligned}142\ 857 \times 1 &= 142\ 857,\\ 142\ 857 \times 2 &= 285\ 714,\\ 142\ 857 \times 3 &= 428\ 571,\\ 142\ 857 \times 4 &= 571\ 428,\\ 142\ 857 \times 5 &= 714\ 285,\\ 142\ 857 \times 6 &= 857\ 142.\end{aligned}$$

Mais alors, qu'advient-il du produit de $142\ 857 \times 7$? Nous obtenons

$$142\ 857 \times 7 = 999\ 999.$$

Étonnant ? Pas vraiment, s'il est établi qu'il y a un lien avec la fraction $7/7 = 1$; n'oublions pas en effet qu'une des représentations possibles de 1 est[4]

$$1 = 0{,}999\ 999\ 999\ 999\ldots$$

Terminons cette section par quelques remarques.

- Nous pourrions poursuivre le calcul des multiples de 142 857 et trouver ainsi

$$142\ 857 \times 12 = 1\ 714\ 284,$$

le produit présentant de nettes affinités avec le développement décimal de la fraction

$$\frac{12}{7} = 1{,}714\ 285\ 714\ 285\ 714\ 285\ldots$$

4. La manipulation suivante vient étayer cette égalité, qui paraît sans doute bizarre à première vue. Posant $x = 0{,}999\ 999\ldots$, nous avons $10x = 9{,}999\ 999\ldots$, de sorte que $10x - x = 9$ (les deux parties décimales s'annulent); il s'ensuit que $9x = 9$ et que $x = 1$.

- Observez bien le développement décimal suivant :

$$\frac{1}{142\ 857} = 0{,}000\ 007\ 000\ 007\ 000\ 007...,$$

qui n'est guère étonnant si nous multiplions chaque membre de cette égalité par 142 857.

- La très étroite parenté entre les développements décimaux des fractions 1/7, 2/7, ..., 6/7 (ainsi qu'entre les multiples de 142 857) est liée au fait que la longueur de la période de la fraction 1/7 est 6, la longueur maximale possible. Une fraction telle que 1/11 = 0,090 909 090 909..., dont la période n'est pas maximale, ne se prête donc pas à l'expression des mêmes régularités. Après 1/7, la fraction suivante ayant une période maximale est

$$\frac{1}{17} = 0{,}058\ 823\ 529\ 411\ 764\ 705\ 882\ 352\ 941\ 176\ 470\ 588\ 235\ 294\ 117\ 647...$$

Nous laissons le lecteur faire le calcul des développements décimaux des fractions 2/17, 3/17, ..., 16/17, ainsi que des multiples du nombre 588 235 294 117 647.

2. Quelques « gros » nombres

Nous aimerions énoncer ici des problèmes qui relèvent presque du quotidien et comportent quelques « gros » nombres.

A. Le nombre 13 983 816 devrait être connu de millions de personnes : c'est le nombre de façons de choisir 6 boules parmi 49, numérotées de 1 à 49. Autrement dit, il s'agit du nombre de combinaisons possibles à la loterie 6/49; les règles de l'analyse combinatoire nous enseignent en effet que ce nombre est donné par l'expression[5]

$$\frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{6!} = 13\ 983\ 816.$$

Il en résulte que celui ou celle qui joue à la 6/49 a exactement une chance sur 13 983 816 d'obtenir la combinaison gagnante. Vraiment pas fameux !

B. Nous tenons une bande de trois timbres; de combien de façons différentes pouvons-nous plier cette bande de manière à la ramener aux dimensions d'un seul timbre, les trois timbres étant alors superposés ? Dans le cas présent, les plis sont faits le long des deux séries de perforations situées respectivement à la gauche et à la droite du timbre central. Le résultat obtenu dépend des critères que nous avons retenus pour déterminer si deux

---

5. Il y a ici 49 façons de choisir la première boule, 48 pour la deuxième, etc., et ces choix « se multiplient » les uns les autres. Il faut ensuite diviser par 6!, car l'ordre du choix ne compte pas; par exemple, les séquences de boules 10-15-20-25-30-35 et 30-20-10-15-25-35 correspondent à la même combinaison — et il y a 6! façons différentes de nommer ces six boules selon l'ordre d'énumération. Rappelons qu'étant donné le naturel k *la factorielle de* k, notée $k!$, est le produit de la multiplication de tous les entiers positifs jusqu'à k; en symboles, $k! = 1 \cdot 2 \cdot 3... (k-1) \cdot k$. Ainsi $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$.

pliages sont distincts ou non. Nous adoptons ici le point de vue suivant : les timbres sont numérotés consécutivement, leur recto (la figure) étant distinct de leur verso (la face gommée)[6].

Nous vérifions alors qu'une bande de trois timbres donne lieu à six pliages différents; c'est donc dire que toutes les $3! = 6$ permutations des entiers 1, 2 et 3 correspondent à des pliages. Si nous passons à une bande de quatre timbres, nous observons que seulement 16 des $4! = 24$ permutations des entiers 1, 2, 3, 4 correspondent aux pliages d'une bande. Plus généralement, si n_k désigne le nombre de façons de plier une bande de k timbres, nous obtenons la suite de nombres ci-dessous :

$$n_1 = 1,\ n_2 = 2,\ n_3 = 6,\ n_4 = 16,\ n_5 = 50,\ n_6 = 144,$$
$$n_7 = 462,\ n_8 = 1\ 392,\ n_9 = 4\ 536,\ n_{10} = 14\ 060$$

(voir [14], suite M1614). Il est à remarquer qu'aucune formule exacte pour le terme général n_k n'est connue.

Qu'arrive-t-il maintenant si nous utilisons une feuille de timbres, plutôt qu'une bande ? Par exemple, de combien de façons pouvons-nous plier une feuille de timbres de format 2×2 (c'est-à-dire une feuille de quatre timbres), de manière à la ramener aux dimensions d'un seul timbre ? Nous pouvons sans trop de peine identifier huit pliages différents (autrement dit, parmi les $4! = 24$ permutations des entiers 1, 2, 3, 4, seules huit d'entre elles correspondent à un pliage d'une feuille de 4 timbres). Qu'en est-il d'une feuille de timbres de format 3×3 (9 timbres) ou 4×4 (16 timbres) ? Si m_k désigne le nombre de façons de plier une feuille de timbres de format $k \times k$, nous avons la suite de nombres

$$m_1 = 1,\ m_2 = 8,\ m_3 = 1\ 368,\ m_4 = 300\ 608 \text{ et } m_5 = 186\ 086\ 600$$

([14], suite M4587). Ainsi, neuf timbres en forme de bande peuvent être pliés de $n_9 = 4\ 536$ façons différentes, mais ce nombre tombe à $m_3 = 1\ 368$ s'ils forment une feuille de format 3×3. On ne connaît pas la valeur de m_k si $k \geq 6$.

Comme quoi plier une feuille de timbres n'est pas une opération aussi banale qu'on pourrait le penser !

C. La première fois qu'on s'amuse avec un cube de Rubik[7], on a d'abord l'impression qu'on peut rapidement faire le tour de toutes les configurations possibles du cube. Aussi est-on étonné lorsqu'on apprend que le nombre total de configurations du cube de Rubik de format $3 \times 3 \times 3$ est de

$$43\ 252\ 003\ 274\ 489\ 856\ 000 = \frac{8! \cdot 12! \cdot 3^8 \cdot 2^{12}}{2 \cdot 2 \cdot 3}$$

6. Mathématiquement parlant, le pliage d'une bande de k timbres équivaut à l'énumération des entiers 1, 2, ..., k dans un certain ordre; la question consiste donc à identifier parmi les $k!$ énumérations ordonnées, ou *permutations,* des entiers 1 à k, celles qui correspondent au pliage d'une bande de k timbres.

7. Nous supposons ici que le lecteur connaît assez bien cet objet, si populaire durant les années 1980, même s'il est un peu tombé en désuétude.

La démonstration de ce résultat peu banal se retrouve dans de nombreux ouvrages de vulgarisation traitant du cube de Rubik[8].

3. Les nombres de Goodstein

Poursuivons maintenant ces aventures numériques en compagnie d'un nombre extraordinairement gros !

Le nombre $3 \cdot 2^{402\,653\,211} - 3$ est un nombre gigantesque[9] qui a fait son apparition dans la littérature mathématique il y a quelques années, en rapport avec l'étude de la complexité de certains phénomènes combinatoires. En voici l'histoire.

En 1944, le logicien anglais R. L. Goodstein a présenté un processus permettant d'engendrer des suites d'entiers naturels qui, contrairement aux apparences, convergent forcément vers 0. Le nombre $3 \cdot 2^{402\,653\,211} - 3$ correspond justement au nombre d'étapes à franchir avant que la suite de Goodstein obtenue à partir de 4 atteigne 0.

Le processus de Goodstein peut être décrit à l'aide de la notion de *représentation complète* d'un naturel en base b : il s'agit d'écrire ce naturel comme une somme de multiples de puissances de b, puis de faire de même avec les exposants présents dans cette somme, avec les exposants de ces exposants, etc., jusqu'à ce que la représentation devienne stable. Par exemple, la représentation complète en base 2 de 266 (qui peut s'écrire $2^8 + 2^3 + 2^1$) est $2^{2^{2+1}} + 2^{2+1} + 2^1$.

Étant donné l'entier positif n, la *suite de Goodstein* commençant à n est la suite des naturels $g_1(n)$, $g_2(n)$, $g_3(n)$, ... définie comme suit :

- pour obtenir le premier terme, $g_1(n)$, il faut partir de la représentation complète de n en base 2, remplacer partout 2 par 3, puis soustraire 1;
- pour obtenir le second terme, $g_2(n)$, il faut partir de la représentation complète de $g_1(n)$ en base 3, remplacer partout 3 par 4, puis soustraire 1;
- plus généralement, le terme $g_k(n)$ est défini comme suit :
  - si $g_{k-1}(n) = 0$, alors $g_k(n) = 0$;
  - sinon, pour obtenir $g_k(n)$ il faut partir de la représentation complète de $g_{k-1}(n)$ en base $k + 1$, remplacer partout $k + 1$ par $k + 2$, puis soustraire 1.

---

8. Ainsi, pour illustrer la taille de ce nombre assez imposant, Bandelow [1] mentionne qu'en alignant à la queue leu leu des cubes de Rubik de toutes les configurations possibles, chacun ayant une arête de 5,6 cm, on formerait une chaîne de plus de 2 000 000 000 000 000 km de longueur, soit environ 256 années-lumière — par comparaison, *Alpha Centauri*, l'étoile la plus proche du Soleil, est à « seulement » 4,3 années-lumière. Notons cependant que la difficulté du cube de Rubik ne tient pas tant à la taille du nombre de configurations possibles qu'à la structure même du cube; ainsi, il est facile d'ordonner alphabétiquement 21 mots, mais ces mots peuvent être énumérés de 21 ! = 51 090 942 171 709 440 000 façons différentes, soit un nombre supérieur au nombre de configurations du cube de Rubik.
9. Ce nombre est de l'ordre de $10^{121\,210\,695}$ et comprend plus de 121 000 000 de chiffres en écriture décimale usuelle. À raison de 100 chiffres par ligne et de 50 lignes par page, cela ferait un livre de plus de 24 000 pages ! En comparaison, le nombre de configurations du cube de Rubik (*voir* section 2) « n'est que » de l'ordre de 10^{19}.

Après chaque soustraction de 1, il ne faut pas oublier de réécrire le naturel alors en présence comme une somme de multiples de puissances de la base en cours — voir le calcul de $g_4(10)$ ci-après.

Les premiers termes de la suite de Goodstein commençant à $10 = 2^{2+1} + 2^1$ sont

$$\begin{aligned} g_1(10) &= 3^{3+1} + 3^1 - 1 \\ &= 3^{3+1} + 2 \cdot 3^0 \\ &= 83, \end{aligned}$$

$$\begin{aligned} g_2(10) &= 4^{4+1} + 2 \cdot 4^0 - 1 \\ &= 4^{4+1} + 1 \cdot 4^0 \\ &= 1\ 025, \end{aligned}$$

$$\begin{aligned} g_3(10) &= 5^{5+1} + 1 \cdot 5^0 - 1 \\ &= 5^{5+1} \\ &= 15\ 625, \end{aligned}$$

$$\begin{aligned} g_4(10) &= 6^{6+1} - 1 \\ &= 5 \cdot 6^6 + 5 \cdot 6^5 + 5 \cdot 6^4 + 5 \cdot 6^3 + 5 \cdot 6^2 + 5 \cdot 6^1 + 5 \cdot 6^0 \\ &= 279\ 935, \end{aligned}$$

$$\begin{aligned} g_5(10) &= 5 \cdot 7^7 + 5 \cdot 7^5 + 5 \cdot 7^4 + 5 \cdot 7^3 + 5 \cdot 7^2 + 5 \cdot 7^1 + 5 \cdot 7^0 - 1 \\ &= 5 \cdot 7^7 + 5 \cdot 7^5 + 5 \cdot 7^4 + 5 \cdot 7^3 + 5 \cdot 7^2 + 5 \cdot 7^1 + 4 \cdot 7^0 \\ &= 4\ 215\ 754. \end{aligned}$$

Comme le montre cet exemple, la croissance des termes d'une suite de Goodstein semble très rapide. Mais Goodstein [7] a néanmoins démontré que toute suite de Goodstein atteint 0, ce qui, il faut le reconnaître, est tout à fait contraire à l'intuition.

Certaines suites de Goodstein sont plutôt courtes; c'est le cas notamment de la suite obtenue à partir de 3, qui devient rapidement 0. En voici les cinq termes successifs :

$$\begin{aligned} 3 &= 2^1 + 1 \cdot 2^0 \\ &\to g_1(3) = 3^1 + 1 \cdot 3^0 - 1 = 3 = 1 \cdot 3^1 \\ &\to g_2(3) = 1 \cdot 4^1 - 1 = 3 = 3 \cdot 4^0 \\ &\to g_3(3) = 3 \cdot 5^0 - 1 = 2 = 2 \cdot 5^0 \\ &\to g_4(3) = 2 \cdot 6^0 - 1 = 1 = 1 \cdot 6^0 \\ &\to g_5(3) = 1 \cdot 7^0 - 1 = 0. \end{aligned}$$

On obtient donc un terme nul dès $g_5(3)$. Mais le phénomène n'est pas du tout le même si on part de 4 : le plus petit k tel que $g_k(4) = 0$ est justement le nombre $k = 3 \cdot 2^{402\,653\,211} - 3$ mentionné ci-dessus[10]. Et l'effet est encore plus spectaculaire si la source de la suite est un naturel plus grand.

Il n'est pas facile d'expliquer en termes simples le comportement étrange des suites de Goodstein. Nous pouvons quand même souligner que, si la partie exponentielle du processus de Goodstein semble provoquer une véritable explosion numérique, celle-ci n'en

10. Ce résultat n'est pas très difficile à établir et fait l'objet d'un exercice guidé dans [9].

demeure pas moins restreinte car la croissance illimitée n'est qu'apparente. À un certain point, la soustraction de l'unité viendra gruger les nombres gigantesques obtenus. Observons, dans le calcul précédent de la suite de Goodstein à partir de 3, que, le terme $g_2(3) = 3 \cdot 4^0$ étant en quelque sorte indépendant de la base 4, les termes suivants échappent aux changements successifs de base et que la suite décroît alors tout bonnement vers 0.

Kirby et Paris [11] ont établi que la très lente convergence des suites de Goodstein vers 0 est liée au fait que, dans le cadre de ce qu'on appelle l'*arithmétique élémentaire*, il est impossible de démontrer le résultat suivant dû à Goodstein[11] : toute suite engendrée par le processus de Goodstein atteint forcément 0. Ce phénomène est tout à fait analogue à celui des batailles herculéennes dont il est question ailleurs dans ce volume (voir Hodgson [10]).

4. Des nombres et des chiffres

Dans cette section, nous examinerons une série de problèmes relatifs aux chiffres utilisés pour représenter un nombre donné. Notre premier problème fait intervenir les factorielles[12] des chiffres composant un nombre. Observons l'égalité suivante.

$$145 = 1! + 4! + 5!$$

Frappant, n'est-ce pas ? On peut se demander si d'autres nombres sont, comme 145, égaux à la somme des factorielles de leurs chiffres.

Il y a bien sûr les solutions banales $1 = 1!$ et $2 = 2!$. Mais quoi d'autre ?

L'ordinateur peut être d'un grand secours pour résoudre les problèmes de ce type. Il est facile de rédiger un petit programme, dans quelque langage de programmation que ce soit, permettant de tester tous les naturels jusqu'à, disons, 10 000 000; il n'apparaîtra alors dans cet intervalle (après un long calcul de l'ordinateur) qu'une seule nouvelle solution.

$$40\,585 = 4! + 0! + 5! + 8! + 5!$$

Est-ce à dire que nous avons épuisé toutes les possibilités ? Ou existe-t-il au contraire d'autres naturels, au delà de 10 000 000, qui soient égaux à la somme des factorielles de leurs chiffres ?

En fait, les quatre nombres indiqués ci-dessus représentent les seules solutions au problème posé !

Preuve

Pour démontrer cela, supposons que $n = d_1d_2...d_r$ est un tel nombre, où $d_1, d_2, ..., d_r$ désignent les r chiffres de n (par exemple le nombre 145 est de la forme $d_1d_2d_3$ avec $d_1 = 1$, $d_2 = 4$ et $d_3 = 5$). Alors, n doit satisfaire à la double inégalité

$$10^{r-1} < n = d_1! + d_2! + ... + d_r! \leq r \cdot 9! = 362\,880r. \qquad (1)$$

---

11. Pour démontrer son théorème, Goodstein fait appel à la théorie des *nombres ordinaux transfinis,* qui fournit un environnement plus riche que l'arithmétique élémentaire.
12. La notation factorielle a été présentée à la note 5. On pose, par convention, que $0! = 1$.

En effet, l'inégalité de gauche résulte du fait que le plus petit nombre de r chiffres est précisément

$$10^{r-1} = \underbrace{100...0}_{r-1 \text{ fois le chiffre } 0},$$

qui ne satisfait manifestement pas à la propriété considérée; quant à l'inégalité de droite, elle s'obtient à partir du plus grand nombre possible de r chiffres :

$$\underbrace{99...9}_{r \text{ fois le chiffre } 9}.$$

Mais pour que la double inégalité (1) soit vérifiée, il faut que le nombre r de chiffres de n soit inférieur à 8, c'est-à-dire $n < 10^7$; en effet, pour $r \geq 8$, on a $10^{r-1} > 362\,880r$, ce qui contredit (1). N'oublions pas qu'une fonction exponentielle de type $y = a^x$, avec $a > 1$, finit forcément par surpasser toute fonction linéaire de type $y = bx$.

On en conclut donc que les seuls nombres égaux à la somme des factorielles de leurs chiffres sont les nombres 1, 2, 145 et 40 585. ■

On peut imaginer de nombreuses variantes à partir du lien entre un nombre et une certaine somme faisant intervenir ses chiffres. En voici quelques-unes.

A. Le nombre 153 satisfait à l'égalité suivante :

$$153 = 1^3 + 5^3 + 3^3.$$

Étant donné un nombre n de r chiffres, nous convenons de l'appeler nombre *narcissiste* s'il est égal à la somme des puissances r-ièmes de ses chiffres. Outre le cas banal des nombres d'un seul chiffre, 153 est le plus petit nombre narcissiste.
On peut démontrer qu'il existe seulement un nombre fini de nombres narcissistes.

Preuve
En effet, comme ci-dessus, un tel nombre $n = d_1d_2...d_r$ doit satisfaire à

$$10^{r-1} < n = d_1^r + d_2^r + ... + d_r^r \leq r \cdot 9^r,$$

laquelle double inégalité ne tient plus si $r > 60$. Cette dernière observation est facile à vérifier avec un ordinateur qui parcourt les valeurs entières de r. L'ordinateur rend également possible la comparaison entre les graphes des deux fonctions 10^{x-1} et $x\,9^x$; la première surpasse l'autre lorsque $x > 60{,}85$ (approximativement). ■

D. Winter (*voir* E. W. Weisstein [15, p. 1216]) a démontré en 1985 qu'il existe seulement 88 nombres narcissistes et que le plus grand est le nombre de 39 chiffres suivant :

115 132 219 018 763 992 565 095 597 973 971 522 401.

B. Le nombre 598 est tel que

$$598 = 5^1 + 9^2 + 8^3.$$

Étant donné un nombre $n = d_1d_2...d_r$ de r chiffres, demandons-nous s'il est tel que

$$n = d_1^1 + d_2^2 + d_3^3 + ... + d_r^r. \tag{2}$$

Une recherche par ordinateur révélera que la relation (2) est satisfaite dans le cas des nombres suivants : 89, 135, 175, 518, 598, 1 306, 1 676 et 2 427. S'agit-il là des seuls nombres $n > 9$ ayant cette propriété ? À ce jour, la question demeure sans réponse.

C. Qu'arrive-t-il si, dans (2), on inverse la suite des exposants ? Il est facile de démontrer qu'il n'existe aucun nombre $n > 9$ tel que

$$n = d_1d_2...d_r = d_1^r + d_2^{r-1} + d_3^{r-2} + ... + d_{r-1}^2 + d_r^1. \qquad (3)$$

Preuve
En effet, si $n = d_1d_2...d_r$ satisfait à (3), alors

$$n = 10^{r-1}d_1 + 10^{r-2}d_2 + ... + 10d_{r-1} + d_r = d_1^r + d_2^{r-1} + d_3^{r-2} + ... + d_{r-1}^2 + d_r^1,$$

auquel cas il apparaît, si le troisième membre est soustrait du deuxième membre de cette série d'égalités, que

$$0 = d_1(10^{r-1} - d_1^{r-1}) + d_2(10^{r-2} - d_2^{r-2}) + ... + d_{r-1}(10 - d_{r-1}) > d_1 + d_2 + ... + d_{r-1} > 0;$$

mais cette dernière ligne donne $0 > 0$, ce qui est une contradiction. Il n'existe donc pas de nombre $n > 9$ satisfaisant à (3). ■

D. On vérifie aisément que $3\,435 = 3^3 + 4^4 + 3^3 + 5^5$. Y a-t-il un autre nombre $n = d_1d_2...d_r$ tel que

$$n = d_1^{d_1} + d_2^{d_2} + ... + d_r^{d_r} \; ? \qquad (4)$$

Il est même possible de permettre ici que n contienne le chiffre 0, s'il est posé[13] par convention que $0^0 = 0$.

Il s'agit de démontrer qu'il n'existe qu'un nombre fini de naturels satisfaisant à (4); plus précisément, un tel nombre n doit être inférieur à 10^{10}.

Preuve
À partir du type d'argument déjà utilisé, il est facile de voir qu'un tel nombre n doit satisfaire à

$$10^{r-1} < n = d_1^{d_1} + d_2^{d_2} + ... + d_r^{d_r} \leq r \cdot 9^9 = 387\,420\,489r,$$

laquelle double inégalité ne tient plus lorsque $r \geq 11$, c'est-à-dire lorsque $n \geq 10^{10}$. Il s'ensuit donc qu'il ne peut exister qu'un nombre fini de naturels vérifiant l'égalité (4). ■

L'examen par ordinateur de tous les nombres $n < 10^{10}$ en vue d'identifier ceux qui satisfont à (4) nécessiterait plusieurs jours de calcul sur un ordinateur personnel; or, il est possible de réduire cette recherche à quelques minutes de calcul. Supposons en effet

13. Rigoureusement parlant, l'expression 0^0 est une *forme indéterminée*. La convention $0^0 = 0$ n'est choisie ici que par commodité.

qu'un nombre $n = d_1 d_2 \dots d_r > 1$ satisfait à (4); en éliminant d'abord les d_i nuls (s'il en est !) et en réordonnant ensuite les chiffres d_i restants, nous pouvons voir que n s'exprime sous la forme

$$n = e_1^{e_1} + \dots + e_s^{e_s} \text{ avec } 1 \le e_1 \le e_2 \le \dots \le e_s \le 9 \text{ et } s \le r \le 10. \tag{5}$$

Ainsi, $3\,435 = 3^3 + 3^3 + 4^4 + 5^5$. Or, il existe relativement peu de nombres $< 10^{10}$ qui sont de la forme (5); nous pouvons montrer que, en fait, il y en a moins de 100 000. Voici pourquoi.

Preuve

Chaque nombre de la forme (5) correspond en effet à une suite $(e_1, e_2, \dots, e_s)$ de s éléments telle que

$$1 \le e_1 \le e_2 \le \dots \le e_s \le 9 \tag{6}$$

avec $1 \le s \le 10$. Il s'agit donc de compter le nombre de telles suites.

Lorsque $s = 1$, il y a évidemment 9 suites de la forme (e_1). Pour $s = 2$, il est facile de vérifier, par une énumération systématique, qu'il y a exactement 45 suites de la forme (e_1, e_2); voici la liste des nombres n correspondants :

99, 88, 89, 77, 78, 79, 66, ..., 55, ..., 44, ...,
33, ..., 22, ..., 11, 12, 13, 14, 15, 16, 17, 18, 19.

Si on répartit cette liste en fonction du chiffre des dizaines, on voit bien qu'on y trouve

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45$$

éléments[14].

De façon analogue, nous trouvons que, pour $s = 3$, le nombre de suites (e_1, e_2, e_3) est donné par

$$1 + 3 + 6 + 10 + 15 + 21 + 28 + 36 + 45 = 165.$$

Nous laissons au lecteur le soin de vérifier plus généralement que le nombre total de suites $(e_1, e_2, \dots, e_s)$ satisfaisant à (6), lorsque s balaie les valeurs de 1 à 10, est donné par

$$9 + 45 + 165 + 495 + 1\,287 + 3\,003 + 6\,435 + 12\,870 + 24\,310 + 43\,758 = 92\,377,$$

le j-ième terme de la somme, à partir de la gauche, donnant le nombre de suites à j éléments, pour $j = 1, 2, \dots, 10$. ■

Pour chacun de ces 92 377 cas possibles, il reste à vérifier (à l'aide de l'ordinateur) si le nombre $n = e_1^{e_1} + \dots + e_s^{e_s}$, correspondant à la suite $(e_1, e_2, \dots, e_s)$, satisfait à la condition (4), ou encore, ce qui revient au même, si n peut s'écrire exactement à l'aide des s chiffres $e_1, \dots, e_s$ (pas nécessairement dans cet ordre) et éventuellement du chiffre 0. Outre le cas trivial où $n = 1$ et le cas où $n = 3\,435$, mentionné plus haut, il n'y a qu'une situation fructueuse, soit à $n = 438\,579\,088$.

14. Le lecteur aura peut-être reconnu ici un *nombre triangulaire*, c'est-à-dire un nombre de la forme

$$1 + 2 + 3 + \dots + k = \frac{k(k+1)}{2} \text{ (où } k = 9).$$

E. Concluons cette section avec un problème qui nous mènera à d'autres questions à explorer avec l'ordinateur. Les neuf plus petits nombres $n > 1$ qui ne contiennent pas le chiffre 0 et qui sont divisibles[15] à la fois par la somme des carrés de leurs chiffres et par le produit des carrés de leurs chiffres sont les suivants :

$$111,\ 11\,112,\ 1\,122\,112,\ 111\,111\,111,\ 122\,121\,216,\ 1\,111\,112\,112,$$
$$1\,111\,211\,136,\ 1\,116\,122\,112 \text{ et } 1\,211\,162\,112.$$

Il est assez facile de le vérifier avec un ordinateur. Appelons nombres *insolites* les nombres qui jouissent de cette propriété. En existe-t-il une infinité ?
La réponse à cette question est connue : il existe bel et bien une infinité de nombres insolites. À titre de preuve, nous allons montrer que les nombres

$$111,\ \underbrace{111...1}_{9},\ \underbrace{111...1}_{27},\ \underbrace{111...1}_{81},\ ...,\ \underbrace{111...1}_{3^\alpha},\ ...,$$

c'est-à-dire les nombres formés de 3^α fois le chiffre 1, où α prend successivement les valeurs 1, 2, 3, 4, ..., sont tous insolites.

Preuve
D'abord, il est clair que chacun de ces nombres est divisible par le produit des carrés de ses chiffres, car ce produit vaut toujours 1. Il faut donc montrer que chacun de ces nombres est aussi divisible par la somme des carrés de ses chiffres. Or, pour $n = 11 ... 1$ (3^α fois le chiffre 1), la somme des carrés des chiffres de n donne justement 3^α ; par ailleurs, notons que ce même n peut s'écrire sous la forme

$$n = \underbrace{111...1}_{3^\alpha} = \frac{10^{3^\alpha} - 1}{9}.$$

Nous devons donc vérifier que

$$\text{la fraction } \frac{10^{3^\alpha} - 1}{9} \text{ est divisible par } 3^\alpha, \text{ pour chaque entier positif } \alpha. \qquad (7)$$

Il est clair que cette affirmation est vraie pour diverses valeurs concrètes de α, par exemple pour $\alpha = 1$ ou 2. Pour établir la validité générale de l'affirmation (7), nous allons utiliser une technique de démonstration connue sous le nom de *raisonnement par récurrence*[16].

---

15. On dit que a est *divisible* par b s'il existe un entier c tel que $a = bc$. Autres expressions synonymes : a est un *multiple* de b; b est un *diviseur* ou un *facteur* de a, ce qui s'écrit $b \mid a$. Par exemple, 12 est divisible par 3, car $12 = 3 \cdot 4$.

16. Cette technique est aussi dénommée *raisonnement par induction mathématique*; c'est une méthode argumentative souvent efficace quand il faut établir qu'un certain fait est vérifié pour chaque entier positif. Après avoir constaté directement que le fait en question est vrai pour 1 (le cas de base), il faut s'assurer qu'il le demeure lors du passage d'un naturel à son successeur. De proche en proche s'établit alors la validité de ce fait pour n'importe quel entier positif.

Nous supposons à cette fin que l'affirmation (7) est vraie pour une valeur arbitraire de α, disons r, et nous tentons de vérifier qu'elle doit alors être vraie pour l'entier suivant, soit $r + 1$. Or, en posant $x = 10^{3^r}$, nous pouvons écrire

$$\frac{10^{3^{r+1}} - 1}{9} = \frac{(10^{3^r})^3 - 1}{9} = \frac{x^3 - 1}{9} = \frac{(x-1)}{9}(x^2 + x + 1).$$

Si nous posons maintenant que $A = \dfrac{x-1}{9}$ et $B = x^2 + x + 1$, les égalités précédentes deviennent

$$\frac{10^{3^{r+1}} - 1}{9} = A \cdot B.$$

Mais comme $x = 10^{3^r}$, on a donc $A = \dfrac{10^{3^r} - 1}{9}$, de sorte que, selon notre hypothèse de récurrence sur r, $3^r \mid A$. Il nous suffit donc de montrer que $3 \mid B$ pour obtenir le résultat souhaité.

Il est commode, pour établir que $3 \mid B$, de faire appel à la notion de *congruence*[17]. Notons que $10 \equiv 1 \pmod 3$, de sorte que $10^{3^r} \equiv 1^{3^r} \pmod 3$; comme $x = 10^{3^r}$ et $1^{3^r} = 1$, nous en concluons que $x \equiv 1 \pmod 3$, et également que $x^2 \equiv 1 \pmod 3$; il en résulte enfin que

$$B = x^2 + x + 1 \equiv 1 + 1 + 1 \equiv 0 \pmod 3,$$

ce qu'il fallait démontrer. ■

Nous avons donc établi l'existence d'une infinité de nombres insolites. Mais existe-t-il une infinité de nombres insolites contenant au moins un chiffre différent de 1 ? La réponse est oui, car il est possible de démontrer l'existence d'une infinité de nombres insolites contenant tous le chiffre 9; la preuve de ce résultat est toutefois beaucoup plus difficile à apporter.

Voici d'autres questions plus accessibles, que le lecteur peut explorer avec l'ordinateur.

- Le nombre 11 111 113 116 est-il le dixième nombre insolite ? En d'autres mots, existe-t-il un autre nombre insolite entre 1 211 162 112 et 11 111 113 116 ?
- Le nombre 11 121 114 112 est-il le plus petit nombre insolite contenant le chiffre 4 ?
- Quel est le plus petit nombre insolite contenant les chiffres 7, 8, ou 9 ?

17. La notation $a \equiv b \pmod c$, qui se lit « a est congru à b modulo c », signifie que $a - b$ est divisible par c ou, ce qui revient au même, que a et b donnent le même reste après leur division par c. Par exemple, $16 \equiv 1 \pmod 3$. En particulier, $a \equiv 0 \pmod 3$ signifie que $3 \mid a$. Cette notation, qui est un outil de travail fort utile en théorie des nombres, fut introduite en 1801 par le grand mathématicien Carl Friedrich Gauss dans ses *Disquisitiones arithmeticae* (*Recherches arithmétiques*).

5. Entiers positifs et facteurs premiers

Rappelons qu'un nombre *premier* est un entier positif ayant exactement deux diviseurs. Par exemple, 17 est un nombre premier, mais pas 15 (on dit que 15 est *composé*). Voici la liste des nombres premiers jusqu'à 100 :

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

Il est toujours possible d'exprimer un naturel quelconque sous la forme d'un produit dont les facteurs sont tous des nombres premiers. Par exemple,

$$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5.$$

Il est possible de jongler avec toutes sortes de propriétés reliant un nombre et ses facteurs premiers[18]; en voici un exemple.

Observons les égalités suivantes :

$$\begin{aligned}
378 &= 2 \cdot 3^3 \cdot 7 &&= 2^3 + 3^3 + 7^3,\\
2\,548 &= 2^2 \cdot 7^2 \cdot 13 &&= 2^3 + 7^3 + 13^3,\\
2\,836\,295 &= 5 \cdot 7 \cdot 11 \cdot 53 \cdot 139 &&= 5^3 + 7^3 + 11^3 + 53^3 + 139^3.
\end{aligned}$$

Le recours à l'ordinateur révèle que, dans le cas des naturels ne dépassant pas 10^9, ce sont là les seuls nombres n, différents d'un cube, qui correspondent à la somme des cubes de leurs facteurs premiers.

Il en découle alors une autre question : existe-t-il d'autres naturels (au-delà de 10^9) possédant cette propriété ? Il s'agit là d'un problème ouvert qui pourrait s'avérer assez difficile à résoudre. Voici cependant certaines propriétés auxquelles doit satisfaire un naturel n différent d'un cube et égal à la somme des cubes de ses facteurs premiers[19].

- De toute évidence, le plus grand facteur premier de n est inférieur à $n^{1/3}$, soit la racine cubique de n.
- Le nombre n doit avoir un nombre impair de facteurs premiers distincts.

Preuve

En effet, supposons qu'il existe un entier n tel que

$$n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \ldots \cdot q_r^{\alpha_r} = q_1^3 + q_2^3 + \ldots + q_r^3 \qquad (q_1 < q_2 < \ldots < q_r,\ q_i \text{ premiers}),$$

et que r, le nombre de facteurs premiers distincts de n, est un nombre pair. Il y a ici deux cas à considérer.

---

18. Outre, bien entendu, la propriété fondamentale selon laquelle un nombre est le produit de ses facteurs premiers !
19. La recherche par ordinateur se trouvera grandement facilitée par ces propriétés établies à l'aide d'un raisonnement mathématique. (Voilà une autre illustration du bénéfice qu'on retire à allier la puissance de calcul de l'ordinateur à celle de l'« esprit mathématique ».)

1. Si $q_1 = 2$, alors n est évidemment pair, puisqu'il est divisible par 2. Notons par ailleurs que $n = 2^3 + q_2^3 + \ldots + q_r^3$; or, cette somme est impaire, puisque le premier terme, 2^3, est pair et que les $r - 1$ autres termes sont tous impairs (car q_i est impair pour $i \geq 2$) et sont en nombre impair (à savoir, $r - 1$)[20]. Mais alors, n est simultanément pair et impair, ce qui est impossible.
2. Si $q_1 > 2$, alors n est un nombre impair, puisqu'il n'est pas divisible par 2. Mais n est en même temps la somme de r nombres impairs et correspond donc à un nombre pair, dans l'hypothèse où r est pair. Encore une fois, cela est impossible.

Il s'ensuit que r, soit le nombre de facteurs premiers distincts de n, doit forcément être impair. ■

- Le nombre n ne peut être le produit exacte de trois facteurs premiers distincts.

Preuve
Supposons, au contraire, que n est de la forme $n = q_1 q_2 q_3$ avec $q_1 < q_2 < q_3$; il est alors clair que

$$q_1 < q_2 < q_3 < n^{1/3}; \tag{8}$$

on a donc

$$n^{1/3} > q_3 > q_2 = \frac{n}{q_1 q_3} > \frac{n}{q_1 n^{1/3}} = \frac{n^{2/3}}{q_1},$$

ce qui implique que

$$q_1 > \frac{n^{2/3}}{n^{1/3}} = n^{1/3},$$

ce qui contredit (8). ■

Plus généralement, nous pourrions formuler une question analogue pour d'autres puissances des facteurs premiers de n. Par exemple, existe-t-il un nombre qui n'est pas un carré mais qui est la somme des carrés de ses diviseurs premiers ? L'ordinateur nous révèle qu'un tel nombre doit être supérieur à 10^9 ; mais on n'en connaît pas à ce jour. Nous pouvons encore une fois faciliter la recherche par ordinateur en examinant la parité des facteurs premiers d'un tel nombre n. Nous démontrons ainsi que n doit avoir un nombre impair r de facteurs premiers distincts, et aussi que $r \geq 5$, du fait que $r \neq 3$.

Preuve
Comme dernière démonstration, nous justifions le fait que le nombre r de facteurs premiers d'un tel n doit être différent de 3. Supposons au contraire que $r = 3$; il existe alors des nombres premiers $q_1 < q_2 < q_3$ et des entiers positifs α_1, α_2 et α_3 tels que

$$n = q_1^{\alpha_1} q_2^{\alpha_2} q_3^{\alpha_3} = q_1^2 + q_2^2 + q_3^2.$$

20. On répète ici les faits élémentaires suivants : *pair + impair = impair* et *impair + impair = pair.*

Il y a deux cas à considérer, et chacun mène à une contradiction.

1. Si un des q_i est égal à 3, disons $q_1 = 3$, alors $n = 3^2 + q_2^2 + q_3^2$. Or, $3^2 \equiv 0 \pmod 3$; de plus, tout nombre entier x qui n'est pas un multiple de 3 satisfait à $x^2 \equiv 1 \pmod 3$. Il s'ensuit que $n \equiv 1 + 1 = 2 \pmod 3$. Ici surgit la contradiction : nous avons en effet $3 \mid n$, puisque $q_1 = 3$.
2. Si aucun des q_i ne vaut 3, alors
$$n = q_1^2 + q_2^2 + q_3^2 \equiv 1 + 1 + 1 = 0 \pmod 3,$$
et ainsi $3 \mid n$, ce qui est impossible car aucun des facteurs premiers de n n'est égal à 3. ■

6. Les nombres de Sierpinski

Le mathématicien polonais Waclaw Sierpinski (1882-1969) a étudié des nombres qui portent maintenant son nom; le plus petit nombre connu de cette espèce est 78 557.

Un nombre impair k est appelé *nombre de Sierpinski* si l'entier $k \cdot 2^n + 1$ est composé (c'est-à-dire non premier) pour chaque entier $n \geq 1$. Sierpinski a démontré en 1960 qu'il existe une infinité de tels entiers k, et en particulier que 201 446 503 145 165 177 est l'un d'entre eux; en 1962, J. L. Selfridge a démontré que 78 557 est aussi un nombre de Sierpinski. Il est possible qu'il en existe de plus petits, mais on ne le sait pas !

Pour démontrer que 78 557 est un nombre de Sierpinski, Selfridge a montré qu'au moins un des nombres premiers 3, 5, 7, 13, 19, 37, 73 divise n'importe quel entier de la forme $78\,557 \cdot 2^n + 1$, où $n \geq 1$. Plus précisément, il a montré ce qui suit :

$$\begin{aligned}
n &\equiv 0 \pmod 2 \Rightarrow 3 \mid 78\,557 \cdot 2^n + 1,\\
n &\equiv 1 \pmod 4 \Rightarrow 5 \mid 78\,557 \cdot 2^n + 1,\\
n &\equiv 1 \pmod 3 \Rightarrow 7 \mid 78\,557 \cdot 2^n + 1,\\
n &\equiv 11 \pmod{12} \Rightarrow 13 \mid 78\,557 \cdot 2^n + 1,\\
n &\equiv 15 \pmod{18} \Rightarrow 19 \mid 78\,557 \cdot 2^n + 1,\\
n &\equiv 27 \pmod{36} \Rightarrow 37 \mid 78\,557 \cdot 2^n + 1,\\
n &\equiv 3 \pmod 9 \Rightarrow 73 \mid 78\,557 \cdot 2^n + 1.
\end{aligned}$$

Comme ces congruences sont respectivement équivalentes à

$$\begin{aligned}
&n \equiv 0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34 \pmod{36},\\
&n \equiv 1, 5, 9, 13, 17, 21, 25, 29, 33 \pmod{36},\\
&n \equiv 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34 \pmod{36},\\
&n \equiv 11, 23, 35 \pmod{36},\\
&n \equiv 15, 33 \pmod{36},\\
&n \equiv 27 \pmod{36},\\
&n \equiv 3, 12, 21, 30 \pmod{36},
\end{aligned}$$

elles recouvrent tous les cas possibles, modulo 36, ce qui établit bien que $78\,557 \cdot 2^n + 1$ est composé, quel que soit $n \geq 1$.

Il reste encore aujourd'hui 35 entiers positifs impairs $k < 78\,557$ qui sont candidats au titre de nombre de Sierpinski; le plus petit est $k = 4\,847$. Pour chacun de ces nombres k, il a été prouvé que $k \cdot 2^n + 1$ est toujours composé lorsque $n \leq 18\,000$. Le lecteur désireux d'en apprendre davantage sur les nombres de Sierpinski ou de faire connaissance avec les *nombres de Riesel* — ce sont les nombres k tels que les nombres $k \cdot 2^n - 1$ sont composés pour chaque entier $n \geq 1$ — pourra consulter le livre de P. Ribenboim (*voir* bibliographie).

7. Une conjecture d'Euler

Le grand mathématicien suisse Leonhard Euler (1707-1783) fut le premier à établir que l'équation de Fermat[21] $x^3 + y^3 = z^3$ n'a pas de solution où x, y, z sont des entiers positifs. Il en a tiré la conjecture suivante :

> *Tout comme il n'existe pas de solution non triviale de l'équation*
>
> $$x^3 + y^3 = z^3,$$
>
> *il n'en existe pas pour les équations*
>
> $$x^4 + y^4 + z^4 = u^4$$
>
> *et*
>
> $$x^5 + y^5 + z^5 + u^5 = v^5,$$
>
> *et ainsi de suite pour des puissances plus élevées.* (Il est à remarquer que le nombre de termes dans le membre de gauche augmente avec la puissance.)

En 1966, L. J. Lander et T. R. Parkin fournissaient un premier contre-exemple[22] à l'affirmation d'Euler :

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Vers 1988, R. Frye (voir R. K. Guy [8, p. 140] fournissait le contre-exemple suivant :

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4.$$

Même avec les ordinateurs extrêmement puissants et rapides d'aujourd'hui, aucun contre-exemple n'a encore été trouvé pour les puissances égales ou supérieures à 6. Ou serait-ce qu'Euler n'avait pas entièrement tort ?

---

21. Pierre de Fermat (1601-1665) a affirmé que la seule valeur possible de n telle que l'équation $x^n + y^n = z^n$ ait des solutions entières non nulles est $n = 2$. La justification de cette conjecture fameuse n'a été obtenue qu'en 1994 par Andrew Wiles. Euler a donné une démonstration de l'affirmation de Fermat dans le cas particulier où $n = 3$; cette démonstration contenait cependant une erreur méthodologique, car Euler avait omis d'examiner une certaine propriété à laquelle doivent satisfaire les ensembles de nombres qu'il manipulait, propriété qu'il avait acceptée sans vérification. Cet épisode célèbre dans l'histoire de la théorie des nombres a été amplement analysé; on pourra consulter par exemple [5] pour des commentaires généraux et [4] pour un exposé plus détaillé.
22. Notons au passage la différence essentielle entre la *vérification* d'un contre-exemple (facile !) et la *découverte* d'un contre-exemple (difficile !).

8. Hors de portée et (peut-être) sans espoir !

Nous terminons avec deux problèmes qui semblent bien loin d'être résolus.

A. Tout le monde connaît les puissances de 2, les 15 premières étant

2, 4, 8, 16, 32, 64, 128, 256, 512, 1 024, 2 048, 4 096, 8 192, 16 384, 32 768.

Avec un ordinateur, il est facile d'obtenir rapidement le développement décimal d'une puissance de 2. Nous pouvons alors constater que le nombre

$$2^{71} = 2\ 361\ 183\ 241\ 434\ 822\ 606\ 848$$

ne contient pas le chiffre 7, alors que toutes les puissances de 2 qui suivent, tout au moins jusqu'à 2^{3000}, le contiennent. Aussi, il semblerait raisonnable de conjecturer que 2^{71} est la plus grande puissance de 2 qui ne contient pas 7 parmi ses chiffres, comme l'a observé D. Gale [6].

La même question se pose pour tout autre chiffre que 7. Ainsi, le nombre

$$2^{168} = 374\ 144\ 419\ 156\ 711\ 147\ 060\ 143\ 317\ 175\ 368\ 453\ 031\ 918\ 731\ 001\ 856$$

est-il la plus grande puissance de 2 ne contenant pas le chiffre 2 ? Des vérifications expérimentales à l'aide de l'ordinateur le laissent croire !

Voici un tableau donnant les plus grands nombres k connus tels que 2^k ne contient pas le chiffre c :

c	k	c	k
0	86	5	71
1	91	6	93
2	168	7	71
3	153	8	78
4	107	9	108

Bien malin qui montrera que ces nombres ne sont pas les bons !

B. Étant donné un nombre premier p arbitraire, faisons l'exercice d'additionner ses chiffres et désignons cette somme par $s(p)$. Ainsi,

$$s(11) = 2,\ s(13) = 4,\ s(23) = 5,\ s(31) = 4 \text{ et } s(389) = 20.$$

Il est clair que si p est un nombre premier différent de 3, alors $s(p)$ ne sera jamais un multiple de 3; en effet, il est bien connu que, lorsque la somme des chiffres d'un nombre est divisible par 3, ce nombre doit forcément être lui-même un multiple de 3 et ne peut donc être premier.

Quel est le plus petit nombre premier p tel que $s(p) = 14$? On trouve facilement qu'il s'agit de $p = 59$. De manière générale, étant donné un entier positif k qui n'est pas un multiple de 3, quel est le plus petit nombre premier p tel que $s(p) = k$?

Si $\rho(k)$ désigne ce nombre premier « privilégié », le tableau est alors le suivant :

k	$\rho(k)$	k	$\rho(k)$	k	$\rho(k)$	k	$\rho(k)$	k	$\rho(k)$
2	2	19	199	35	8 999	52	799 999	68	59 999 999
4	13	20	389	37	29 989	53	989 999	70	189 997 999
5	5	22	499	38	39 989	55	2 998 999	71	89 999 999
7	7	23	599	40	49 999	56	2 999 999	73	289 999 999
8	17	25	997	41	59 999	58	4 999 999	74	389 999 999
10	19	26	1 889	43	79 999	59	6 999 899	76	689 899 999
11	29	28	1 999	44	98 999	61	8 989 999	77	699 899 999
13	67	29	2 999	46	199 999	62	9 899 999	79	799 999 999
14	59	31	4 999	47	389 999	64	19 999 999	80	998 999 999
16	79	32	6 899	49	598 999	65	29 999 999	82	2 999 899 999
17	89	34	17 989	50	599 999	67	59 899 999	83	3 999 998 999

Un fait est visuellement frappant : le chiffre 9 apparaît très souvent dans ce tableau. La raison est en fait assez simple, et c'est d'ailleurs ce qui nous a permis de construire assez rapidement, à l'aide de l'ordinateur, le tableau ci-dessus. Prenons par exemple $k = 22$, et trouvons d'abord le plus petit nombre n dont la somme des chiffres est 22. Il est facile de voir que ce sera un nombre de trois chiffres, dont les deux derniers sont 9 et dont le premier est $22 - 2 \cdot 9 = 22 - 18 = 4$; il s'agit donc de $n = 499$. Comme 499 est un nombre premier, nous pouvons conclure que $\rho(22) = 499$. Choisissons maintenant $k = 25$; par le même raisonnement, nous trouvons facilement que 799 est le plus petit nombre dont la somme des chiffres est 25; malheureusement, 799 n'est pas premier, car $799 = 17 \cdot 47$. Nous avons tout de même établi que $\rho(25) = 799$; en regardant un peu plus loin que 799, nous concluons que $\rho(25) \geq 997$. En exploitant cette idée, nous pouvons établir une borne inférieure[23] pour $\rho(k)$.

Voilà qui n'était pas trop difficile. Mais il demeure une question beaucoup plus troublante à propos de $\rho(k)$: est-il certain que, pour chaque entier positif k qui n'est pas un multiple de 3, on puisse trouver un nombre premier p dont la somme des chiffres est k ? En d'autres mots, la fonction $\rho(k)$ est-elle bien définie ? Certes, comme en fait foi le tableau ci-dessus, le problème ne se pose pas pour les entiers inférieurs à 84 qui ne sont pas des multiples de 3. Mais qu'en est-il au delà de 83 ? La question dans son ensemble n'a pas encore reçu de réponse.

Tout doute sur le fait que la fonction $\rho(k)$ prend une valeur précise pour tout k qui n'est pas un multiple de 3 peut paraître surprenant; de prime abord, en effet, étant donné un tel nombre $k > 2$, il est tentant de croire qu'il doit exister une infinité de nombres premiers p dont la somme des chiffres est k. Cette « intuition » prend sa source dans quelques constatations. Prenons par exemple $k = 14$; il s'avère que la somme des chiffres de chacun

---

23. Il peut être démontré que $\rho(k) \geq (a + 1)10^b - 1$, où $b = [k/9]$ (c'est-à-dire la partie entière de la fraction $k/9$) et $a = k - 9b$.

des nombres premiers 59, 149, 167, 239, 257, 293, 347, 383, 419, 491 et 509 est 14. Peut-être y a-t-il beaucoup de nombres premiers dont la somme des chiffres est 14, voire une infinité !

Mais considérons maintenant le cas où $k = 2$. Les seuls nombres premiers connus dont la somme des chiffres donne 2 sont 2, 11 et 101; démontrer qu'il y en a une infinité reviendrait à établir l'existence d'une infinité de nombres premiers de la forme $10^m + 1 = 100...01$ ($m - 1$ fois le chiffre 0), ce qui n'a pas été fait.

9. Quelques problèmes ouverts

Voici, pour conclure, deux autres conjectures encore non résolues [3].

A. Nous avons vu à la section 4 qu'il existe quatre entiers positifs qui sont égaux à la somme des factorielles de leurs chiffres. Il est facile de montrer qu'aucun entier $n > 9$ n'est égal au produit de ses chiffres (car il est facile de montrer par récurrence sur r que, pour tout nombre n dont les chiffres sont $d_1, d_2, ..., d_r$, lorsque $r \geq 2$, on a $n > d_1 \cdot d_2 \cdot ... \cdot d_r$). Existe-t-il un nombre entier positif qui soit égal au produit des factorielles de ses chiffres ? Comme les nombres 1!, 2!, ..., 9! ne contiennent que les facteurs premiers 2, 3, 5 et 7, il est facile de voir qu'un tel nombre n doit s'écrire sous la forme

$$n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma \cdot 7^\delta$$

où α, β, γ et δ sont des entiers non négatifs. Et alors, pourquoi un tel nombre ne serait-il pas possible ? Quoi qu'il en soit, on n'en connaît pas.

B. À chaque entier $n > 1$ écrit sous la forme standard du produit de ses facteurs premiers, c'est-à-dire

$$n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot ... \cdot q_r^{\alpha_r},$$

associons le nombre $B(n) = \alpha_1 q_1 + \alpha_2 q_2 + ... + \alpha_r q_r$. Par exemple, $B(12) = 2 \cdot 2 + 1 \cdot 3 = 7$ et $B(15) = 8$. Nous nous posons la question suivante en ce qui concerne la fonction B : est-il possible de trouver trois nombres consécutifs pour lesquels la fonction B prend la même valeur ? En d'autres mots, existe-t-il un nombre n tel que $B(n) = B(n + 1) = B(n + 2)$? La réponse est oui, car[24] $B(417\ 162) = B(417\ 163) = B(417\ 164) = 533$. En utilisant un ordinateur, on constate qu'il n'existe pas d'autre nombre $n < 10^8$ jouissant de cette propriété. Mais en existe-t-il d'autres plus loin ? Et qu'en est-il de plusieurs nombres consécutifs pour lesquels B aurait toujours la même valeur ?

---

24. Ces égalités découlent du fait que les décompositions en facteurs premiers de ces nombres sont

$417\ 162 = 2 \cdot 3 \cdot 251 \cdot 277$,
$417\ 163 = 17 \cdot 53 \cdot 463$,
$417\ 164 = 2^2 \cdot 11 \cdot 19 \cdot 499$.

Bibliographie

[1] BANDELOW, Christoph. *Inside Rubik's Cube and Beyond*, Birkhäuser, 1982.
[2] CONWAY, John H. et Richard K. GUY. *Le Livre des nombres*, Eyrolles, 1998.
[3] DE KONINCK, Jean-Marie. *Ces Nombres qui nous fascinent*, version préliminaire, Québec, Université Laval, 1999, 320 p.
[4] EDWARDS, Harold M. *Fermat's Last Theorem. A Genetic Introduction to Algebric Number Theory*, New York, Springer-Verlag, 1977.
[5] EDWARDS, Harold M. « Pierre de Fermat », dans *Les Mathématiciens*, Paris, Pour la science, 1996, p. 22-31.
[6] GALE, David. « Mathematical Entertainement », *The Mathematical Intelligencer*, 18, 1996, p. 23-27.
[7] GOODSTEIN, Reuben L. « On the Restricted Ordinal Theorem », *Journal of Symbolic Logic*, 9, 1944, p. 33-41.
[8] GUY, Richard K. *Unsolved Problems in Number Theory*, 2e éd., New York, Springer-Verlag, 1994.
[9] HENLE, James M. *An Outline of Set Theory*, New York, Springer-Verlag, 1986.
[10] HODGSON, Bernard R. « Tâches herculéennes ou sisyphéennes ? Un regard neuf sur le phénomène d'incomplétude en logique mathématique », dans *Mathématiques d'hier et d'aujourd'hui*, Mont-Royal, Modulo Éditeur, 2000, 220 p.
[11] KIRBY, Laurie et Jeff PARIS. « Accessible Independence Results for Peano Arithmetic », *Bulletin of the London Mathematical Society*, 14, 1982, p. 285-293.
[12] LE LIONNAIS, François. *Les Nombres remarquables*, Hermann, 1983.
[13] RIBENBOIM, Paulo. *The New Book of Prime Number Records*, New York, Springer-Verlag, 1996, p. 335-360.
[14] SLOANE, Neil J. A. et Simon PLOUFFE. *The Encyclopedia of Integer Sequences*, Academic Press, 1995.
[15] WEISSTEIN, Eric W. *CRC Concise Encyclopedia of Mathematics*, Boca Raton, CRC Press, 1999.
[16] WELLS, David. *Le Dictionnaire Penguin des nombres curieux*, 2e éd., Eyrolles, 1998.

Pour aller plus loin

Le lecteur désireux de découvrir d'autres « nombres fascinants » pourra se régaler en consultant l'un des nombreux ouvrages accessibles qui abordent l'univers numérique sous cet angle. Nous aimerions particulièrement signaler à cet égard les livres de J. H. Conway et R. K. Guy [2], de F. Le Lionnais [12], de D. Wells [16], ainsi que le document de J.-M. De Koninck [3]. Le livre de R. K. Guy [8], quoique plus avancé, est une précieuse source d'information. Pour celui ou celle qui aime les records, le livre de P. Ribenboim [13] est tout à fait indiqué. Enfin, l'encyclopédie de N. J. A. Sloane et S. Plouffe [14] donne une liste de plus de 5 000 suites de nombres naturels[25].

25. On pourra aussi consulter dans Internet le site « L'encyclopédie électronique des suites entières » (http://www.research.att.com/~njas/sequences/indexfr.html).