20 janvier 2009

Cours de Théorie des Nombres MM020

Équations Diophantiennes

Michel Waldschmidt

Institut de Mathématiques de Jussieu & CIMPA

http ://www.math.jussieu.fr/∼miw/

Plan

- Équations de Catalan et Pillai
- Conjecture abc
- Équation de Fermat généralisée
- Problème de Waring
- Équation de Markoff

Carrés, cubes...

Une puissance parfaite est un entier de la forme a^b où $a \geq 1$ et $b > 1$ sont des entiers.

Carrés :

$1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 49,\ 64,\ 81,\ 100,\ 121,\ 144,\ 169,\ 196\ldots$

Cubes :

$1,\ 8,\ 27,\ 64,\ 125,\ 216,\ 343,\ 512,\ 729,\ 1\,000,\ 1\,331\ldots$

Puissances cinquièmes :

$1,\ 32,\ 243,\ 1\,024,\ 3\,125,\ 7\,776,\ 16\,807,\ 32\,768\ldots$

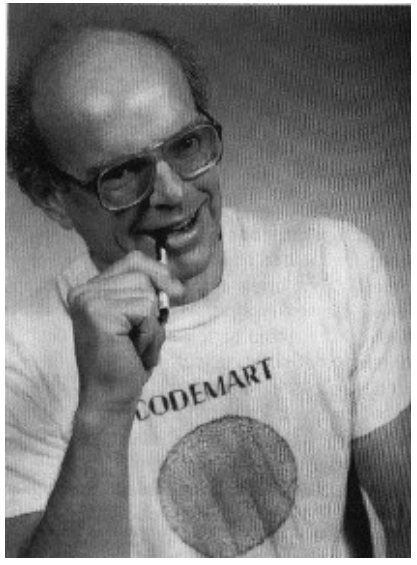
Encyclopédie des suites

1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, 196, 216, 225, 243, 256, 289, 324, 343, 361, 400, 441, 484, 512, 529, 576, 625, 676, 729, 784, 841, 900, 961, 1000, 1024, 1089, 1156, 1225, 1296, 1331, 1369, 1444, 1521, 1600, 1681, 1728, 1764 . . .

On trouve la suite des puissances parfaites sur la toile

The On-Line Encyclopedia of Integer Sequences

Neil J. A. Sloane



http ://www.research.att.com/∼njas/sequences/A001597

Puissances parfaites

1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125,
128, 144, 169, 196, 216, 225, 243, 256, 289, 324, 343,
361, 400, 441, 484, 512, 529, 576, 625, 676, 729, 784,
841, 900, 961, 1000, 1024, 1089, 1156, 1225, 1296,
1331, 1369, 1444, 1521, 1600, 1681, 1728, 1764 . . .

Difference 1 : $(8, 9)$

Difference 2 : $(25, 27)$

Difference 3 : $(1, 4)$, $(125, 128)$

Difference 4 : $(4, 8)$, $(32, 36)$, $(121, 125)$

Difference 5 : $(4, 9)$, $(27, 32)$ . . .

Deux conjectures

Conjecture de Catalan (1844). Dans la suite des puissances parfaites, $8, 9$ sont les seuls entiers consécutifs.

Conjecture de Pillai (1945). Dans la suite des puissances parfaites, la différence entre deux termes consécutifs tend vers l'infini.
Autrement dit : Soit k un entier positif. L'équation

$$x^p - y^q = k,$$

où les inconnues x, y, p et q sont des entiers tous ≥ 2, n'a qu'un nombre fini de solutions (x, y, p, q).

Catalan (1844)

$x^p - y^q = 1$

Pillai (1945)

$x^p - y^q = k$

Résultats

P. Mihăilescu, 2002. Catalan avait raison : *l'équation* $x^p - y^q = 1$ *où les inconnues* x, y, p *et* q *sont des entiers* ≥ 2, *a pour seule solution* $(x, y, p, q) = (3, 2, 2, 3)$.
Résultats précédents de J.W.S. Cassels, R. Tijdeman, M. Mignotte...
Autres valeurs de k : rien n'est connu.
La conjecture de Pillai est une conséquence de la conjecture abc :

$$|x^p - y^q| \geq c(\epsilon) \max\{x^p, y^q\}^{\kappa - \epsilon}$$

avec

$$\kappa = 1 - \frac{1}{p} - \frac{1}{q}.$$

Le radical d'un entier

Quand n est un entier positif, on définit le radical $R(n)$ de n par

$$R(n) = \prod_{p|n} p$$

On dit encore que c'est la partie sans facteurs carrés de n.

Si la décomposition de n en facteurs premiers est $n = p_1^{a_1} \cdots p_k^{a_k}$ où les p_i sont des nombres premiers distincts et les a_i des entiers ≥ 1, alors

$$R(n) = p_1 \cdots p_k.$$

n	$=$	1	2	3	4	5	6	7	8	9	10	11	12	$\ldots$
$R(n)$	$=$	1	2	3	2	5	6	7	2	3	10	11	6	$\ldots$

La conjecture *abc*

La conjecture *abc* a son origine dans une discussion entre D. W. Masser et J. Œsterlé dans les années 1980.

Conjecture *abc*. *Pour tout* $\varepsilon > 0$ *il existe* $\kappa(\varepsilon)$ *tel que, si* a, b *et* c *sont des éléments de* $\mathbf{Z}_{>0}$ *premiers entre eux satisfaisant* $a + b = c$, *alors*

$$c < \kappa(\varepsilon) R(abc)^{1+\varepsilon}.$$

Quand $a + b = c$, on a $\text{PGCD}(a, b) = 1$ si et seulement si $\text{PGCD}(a, b, c) = 1$.

Le théorème de Mason

Théorème (R. Mason). *Soient K un corps, A, B, C trois polynômes de $K[X]$ premiers entre eux vérifiant $A+B=C$ et a, b, c leurs degrés. Soit r le nombre de zéros sans multiplicités du produit ABC. Alors*

$$\max\{a,b,c\} \leq r-1.$$

Le nombre r est le degré du *radical* R de ABC, c'est-à-dire du produit des facteurs irréductibles unitaires de ABC :

$$R = \prod_{P|ABC} P$$

où P décrit l'ensemble des polynômes irréductibles unitaires de $K[X]$.

Démonstration du théorème de Mason

Posons $f = A/C$, $g = B/C$, de sorte que la relation $A + B = C$ devient $f + g = 1$. En dérivant on obtient $f' + g' = 0$, relation que l'on peut écrire

$$\frac{A}{B} = \frac{f}{g} = -\frac{g'/g}{f'/f}.$$

Soit R le radical du produit ABC : son degré est r, comme nous l'avons vu. On remarque que $A_1 = -Rg'/g$ et $B_1 = Rf'/f$ sont deux polynômes de degrés $r - 1$, qui vérifient

$$\frac{A}{B} = \frac{A_1}{B_1}.$$

Comme A/B est une fraction rationnelle irréductible, il en résulte que les polynômes A et B sont tous deux de degré $\leq r - 1$.

Conjecture *abc*

Si a, b et c sont des entiers positifs premiers entre eux satisfaisant $a + b = c$, on pose

$$\alpha(a, b, c) = \frac{\log c}{\log R(abc)}.$$

La conjecture *abc* revient à dire que pour $\alpha_0 > 1$, il n'y a qu'un nombre fini de triplets (a, b, c) avec $\text{PGCD}(a, b, c) = 1$ vérifiant $\alpha(a, b, c) \geq \alpha_0$.

Conjecture *abc* : de bons exemples

On connaît

- 13 valeurs de $\alpha(abc)$ qui sont $\geq 1,5$
- 221 qui sont $> 1,4$.

Voici les deux plus grandes

$a+b=c$	$\alpha(a,b,c)$	auteurs
$2+3^{10}\cdot 109=23^5$	$1.629912\ldots$	É. Reyssat
$11^2+3^2 5^6 7^3=2^{21}\cdot 23$	$1.625991\ldots$	B.M. Weger

Le site de la conjecture *abc* :

`http ://www.math.unicaen.fr/~nitaj/abc.html`

Conséquences de la conjecture *abc*

1. Le Dernier Théorème de Fermat sous forme *asymptotique* : si n est un entier > 3, alors l'équation $x^n + y^n = z^n$ n'a qu'un nombre fini de solutions (x, y, z) en entiers positifs premiers entre eux.

2. Équation de Fermat généralisée : étant donnés des entiers positifs A, B, C, l'équation $Ax^r + By^s = Cz^t$ n'a qu'un nombre fini de solutions en entiers x, y, z, r, s, t satisfaisant $\text{PGCD}(x, y, z) = 1$ et $1/r + 1/s + 1/t < 1$
Remarque. Si r, s, t sont fixés avec $1/r + 1/s + 1/t < 1$, on sait que l'équation $Ax^r + By^s = Cz^t$ n'a qu'un nombre fini de solutions en entiers x, y, z, r, s, t satisfaisant $\text{PGCD}(x, y, z) = 1$.

Conséquences de la conjecture *abc*

3. Un nombre premiers de Wieferich. est un nombre premier p tel que p^2 divise $2^{p-1} - 1$. Les seuls exemples connus sont 1093 et 3511. Il n'y en a pas d'autre inférieur à $4 \cdot 10^{12}$.

La conjecture *abc* apporterait une réponse positive au problème ouvert suivant :

Étant donné un entier $a > 1$, il y a une infinité de nombres premiers p tels que p^2 ne divise pas $a^{p-1} - 1$.

Une liste de 30 conséquences de ce genre se trouve sur la page de Abderrahmane Nitaj
`http ://www.math.unicaen.fr/~nitaj/abc.html`

Équation de Fermat généralisée

L'équation $x^p + y^q = z^r$ en entiers positifs (x, y, z, p, q, r) tels que

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1,$$

avec x, y, z premiers entre eux possède les 10 solutions suivantes (*F. Beukers, D. Zagier*) :

$$1 + 2^3 = 3^2, \quad 2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2,$$
$$1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7,$$
$$43^8 + 96222^3 = 30042907^2, \quad 33^8 + 1549034^2 = 15613^3.$$

Conjecture de Beal

Conjecture de Beal (R. Tijdeman et D. Zagier). L'équation $x^p + y^q = z^r$ n'a pas de solution en entiers positifs (x, y, z, p, q, r) avec chacun des exposants p, q et r au moins 3 et x, y, z premiers entre eux.

Mauldin, R. D. – *A generalization of Fermat's last theorem : the Beal conjecture and prize problem.* Notices Amer. Math. Soc. **44** N°11 (1997), 1436–1437.

Le problème de Waring

Soit $k \geq 2$ un entier rationnel. On définit $g(k)$ comme le plus petit des entiers $g \geq 1$ tels que tout entier positif soit somme d'au plus g puissances k-ièmes.

Par exemple $g(4) \geq 19$ car pour écrire le nombre 79 comme somme de puissances 4-ièmes (bicarrés) il faut au moins 19 termes (comme $79 = 4 \times 16 + 15$, le plus économique est d'ajouter 4 fois 2^4 et 15 fois 1).

Le problème de Waring

Divisons 3^k par 2^k, ce qui veut dire qu'on écrit $3^k = 2^k q + r$ avec $0 < r < 2^k$. Ainsi $q = [(3/2)^k]$ (où $[\cdot]$ désigne la partie entière). Le nombre $I(k) = 2^k + q - 2$ est appelé *constante de Waring idéale*. L'écriture de $2^k q - 1$ comme somme de puissances k-ième nécessite au moins $I(k)$ termes, à savoir $q - 1$ termes 2^k et $2^k - 1$ termes 1, donc $g(k) \geq I(k)$. L'égalité $g(k) = I(k)$ est vérifiée pour de nombreuses valeurs de k (notamment toutes les valeurs de k "suffisamment grandes" ainsi que pour $2 \leq k \leq 4,716 \cdot 10^8$).

L'égalité $g(k) = I(k)$ pour k suffisamment grand est une conséquence de la conjecture *abc*.

L'équation de Markoff $x^2 + y^2 + z^2 = 3xyz$

Il est facile de montrer que l'équation $x^2 + y^2 + z^2 = 3xyz$, dans laquelle les trois inconnues x, y, z sont des entiers positifs, possède une infinité de solutions. Un algorithme permet de les déterminer toutes. Cela ne résout pas tous les problèmes : en particulier Frobenius a conjecturé que pour tout entier $z > 0$ il existe au plus une solution (x, y, z) satisfaisant $x < y < z$. Cette question fait l'objet de recherches actuelles, elle est encore ouverte.

L'équation de Markoff $x^2 + y^2 + z^2 = 3xyz$

Cette équation est apparue dans l'étude de minima de formes quadratiques (travaux de Lagrange, Hermite, Korkine, Zolotarev, Markoff, Frobenius, Hurwitz, Cassels notamment) et l'approximation rationnelle de nombres réels. Les solutions correspondent aux nombres quadratiques qui possèdent les moins bonnes approximations rationnelles, ce qui donne lieu au spectre de Lagrange–Markoff. Elle intervient aussi dans l'étude de groupes Fuchsiens et de surfaces de Riemann hyperboliques (Ford, Lehner, Cohn, Rankin, Conway, Coxeter, Hirzebruch et Zagier...).

La suite des nombres de Markoff

Un *nombre de Markoff* est un nombre entier positif z tel qu'il existe des entiers positifs x et y satisfaisant

$$x^2 + y^2 + z^2 = 3xyz.$$

Par exemple 1 est un nombre de Markoff, puisque $(x, y, z) = (1, 1, 1)$ est une solution.

Andrei Andreyevich Markoff
(1856–1922)

Crédit photos :
http ://www-history.mcs.st-andrews.ac.uk/history/

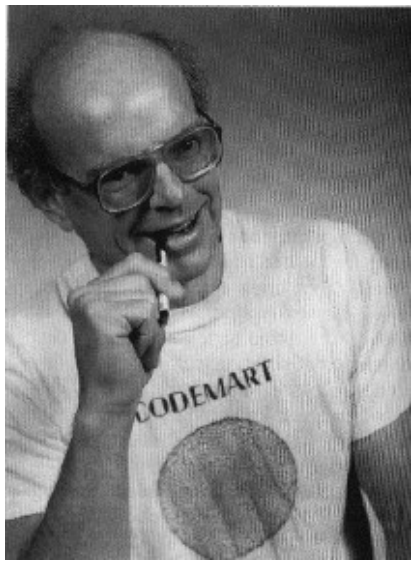
Encyclopédie des suites

1, 2, 5, 13, 29, 34, 89, 169, 194, 233, 433, 610, 985, 1325, 1597, 2897, 4181, 5741, 6466, 7561, 9077, 10946, 14701, 28657, 33461, 37666, 43261, 51641, 62210, 75025, 96557, 135137, 195025, 196418, 294685, ...

On trouve la suite des nombres de Markoff sur la toile

The On-Line Encyclopedia of Integer Sequences

Neil J. A. Sloane



http ://www.research.att.com/∼njas/sequences/A002559

Points entiers sur une surface

Étant donné un nombre de Markoff z, il existe une infinité de couples d'entiers positifs x et y satisfaisant

$$x^2 + y^2 + z^2 = 3xyz.$$

C'est une équation de degré 3 en les 3 variables (x, y, z) dont on connaît une solution $(1, 1, 1)$.

Un algorithme permet de déterminer toutes les solutions entières.

La cubique de Markoff

La surface cubique définie par l'équation de Markoff

$$x^2 + y^2 + z^2 = 3xyz.$$

est une variété algébrique avec beaucoup d'automorphismes : permutation des variables, changements de signes et

$$(x, y, z) \mapsto (3yz - x, y, z).$$

A.A. Markoff (1856–1922)

Algorithme donnant toutes les solutions

Soit (m, m_1, m_2) une solution de l'équation de Markoff :

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2.$$

Fixons deux des coordonnées de cette solution, disons m_1 et m_2. Il reste une équation en la troisième coordonnée m dont on connait une solution, donc l'équation

$$x^2 + m_1^2 + m_2^2 = 3xm_1m_2.$$

a deux solutions, $x = m$ et $x = m'$, avec $m + m' = 3m_1m_2$ et $mm' = m_1^2 + m_2^2$ – c'est le *procédé de la corde et de la tangente.*

Ainsi une *autre* solution est (m', m_1, m_2) avec $m' = 3m_1m_2 - m$.

Trois solutions à partir d'une

Partant d'une solution (m, m_1, m_2) on en déduit trois *nouvelles* solutions :

$$(m', m_1, m_2), \quad (m, m_1', m_2), \quad (m, m_1, m_2').$$

Si la solution dont on part est $(1, 1, 1)$, on ne trouve en fait qu'une nouvelle solution, $(2, 1, 1)$ (à permutation près).

Si la solution dont on part est $(2, 1, 1)$, on ne trouve en fait que deux *nouvelles* solutions, $(1, 1, 1)$ et $(5, 2, 1)$ (à permutation près).

Nouvelle = différente de la solution de départ.

Nouvelles solutions

On va montrer que toute solution autre que $(1, 1, 1)$ et $(2, 1, 1)$ produit trois nouvelles solutions différentes, et aussi que pour toute solution autre que $(1, 1, 1)$ et $(2, 1, 1)$, les trois nombres m, m_1 et m_2 sont distincts.

On dit que deux solutions sont *voisines* si deux de leurs composantes sont les mêmes.

Cet algorithme les produit toutes

Supposons que la solution initiale (m, m_1, m_2) satisfasse $m > m_1 > m_2$. On va vérifier

$$m_2' > m_1' > m > m'.$$

On peut ordonner les solutions par leur plus grande composante. Alors deux des voisins de (m, m_1, m_2) sont plus grands, le troisième est plus petit.

Ainsi quand on part de $(1, 1, 1)$ on produit une infinité de solutions, qu'on dispose en un arbre : *l'arbre de Markoff*.

On obtient toutes les solutions

Inversement quand on part d'une solution autre que $(1, 1, 1)$, l'algorithme lui associe une solution plus petite, et par récurrence on trouve une suite de solutions de plus en plus petites qui aboutit sur $(1, 1, 1)$. Donc la solution dont on est partie était dans l'arbre de Markoff.

Premières branches de l'arbre de Markoff

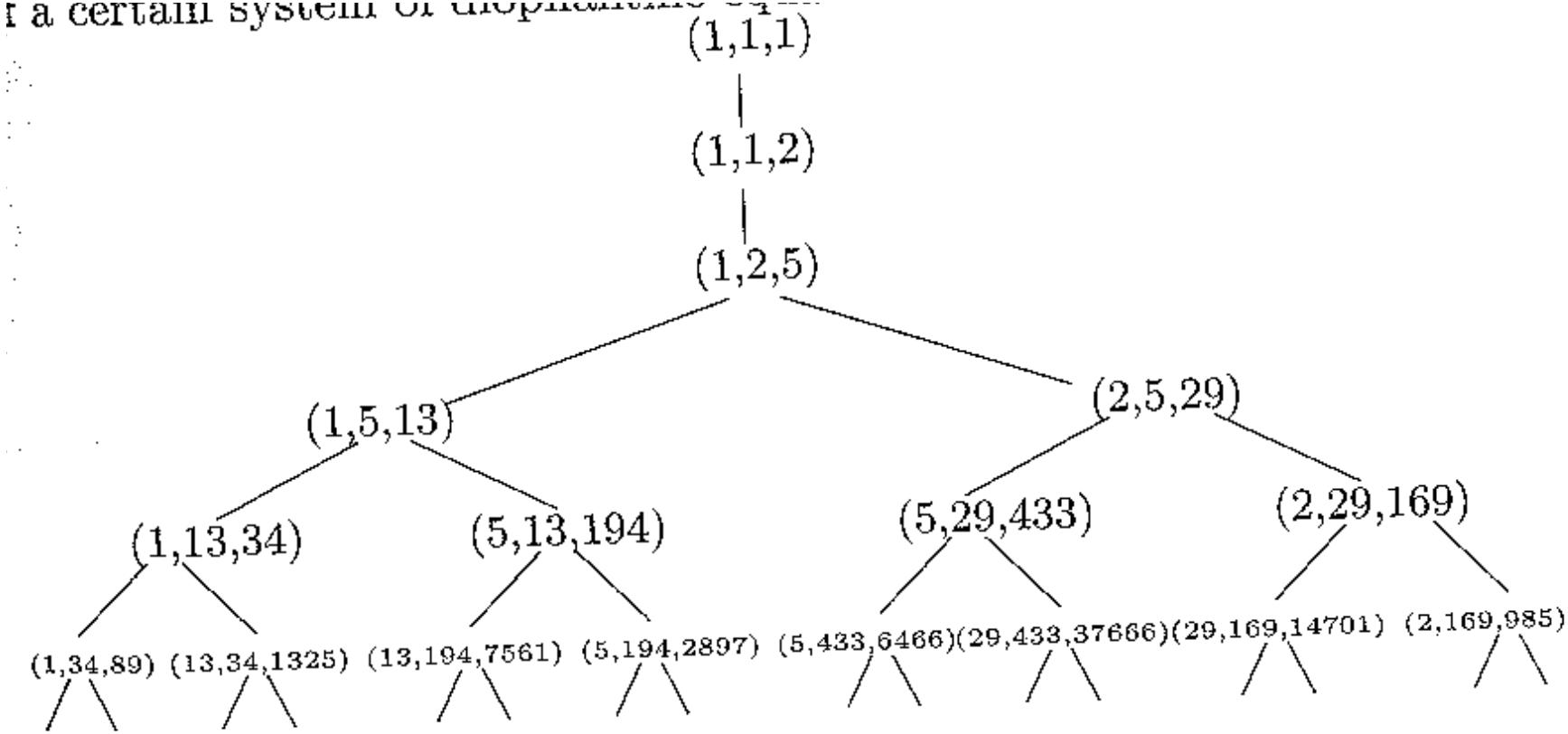
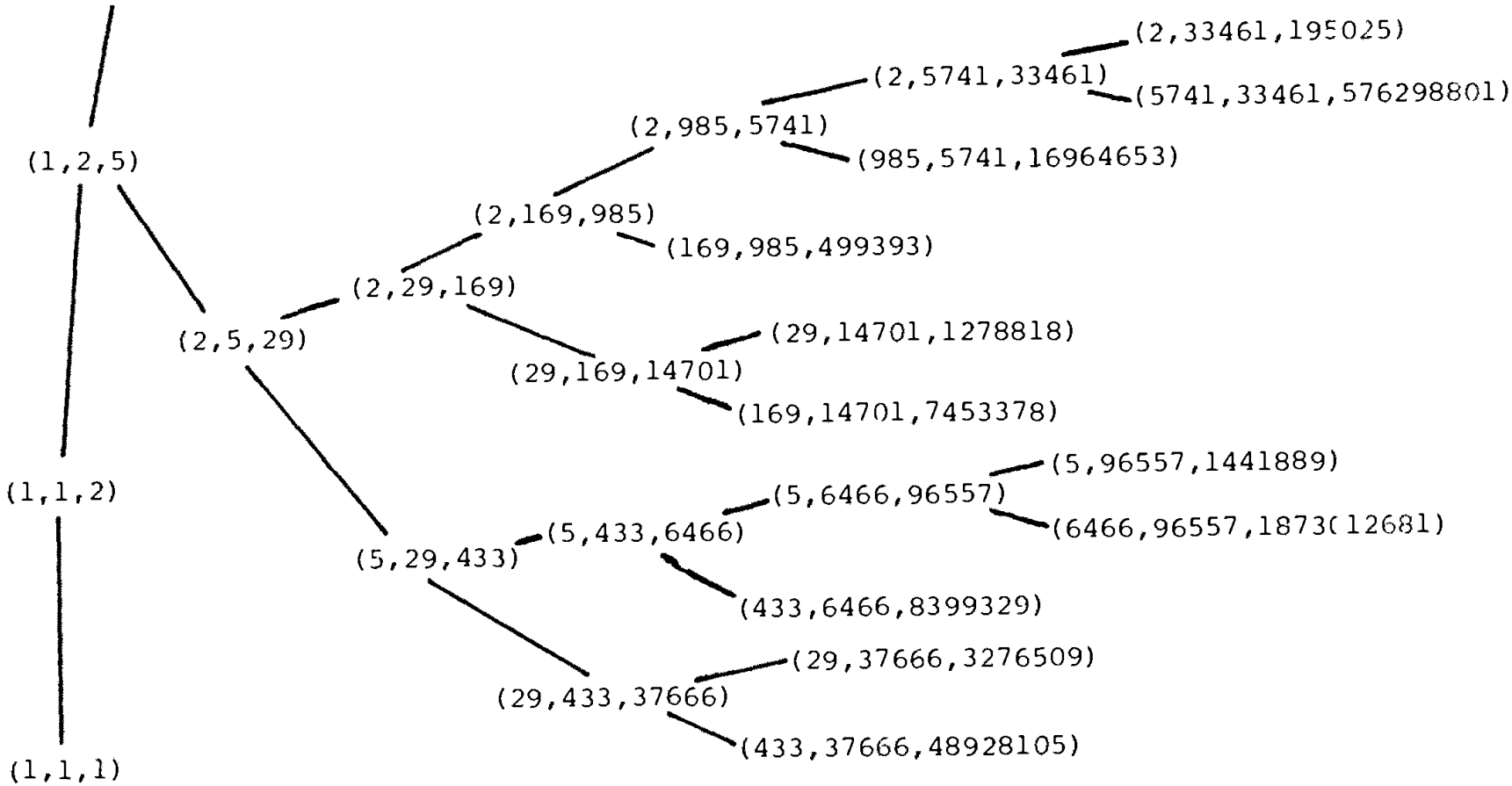


Figure 10. The Tree of Markoff Solutions.

Arbre de Markoff partant de $(2, 5, 29)$



Arbre de Markoff jusqu'à 100 000

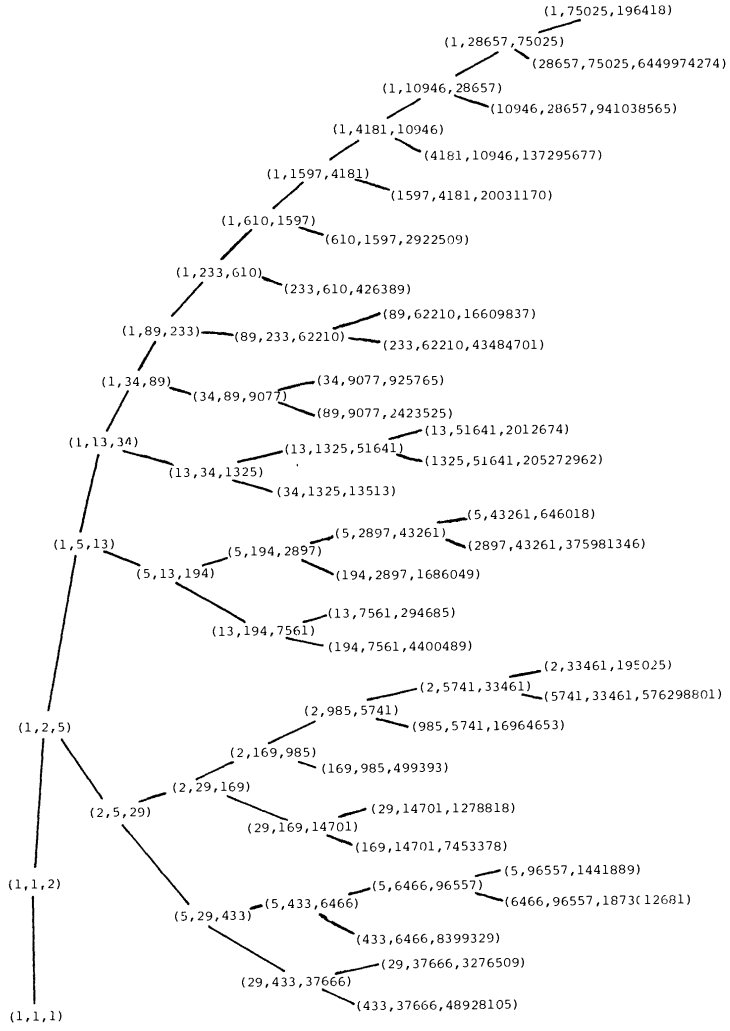


FIGURE 2
Markoff triples (p, q, r) *with* $\max(p, q) \leqslant 100000$

Don Zagier,
On the number of Markoff numbers below a given bound.
Mathematics of Computation, **39** 160 (1982), 709–723.

Fractions continues et arbre de Markoff

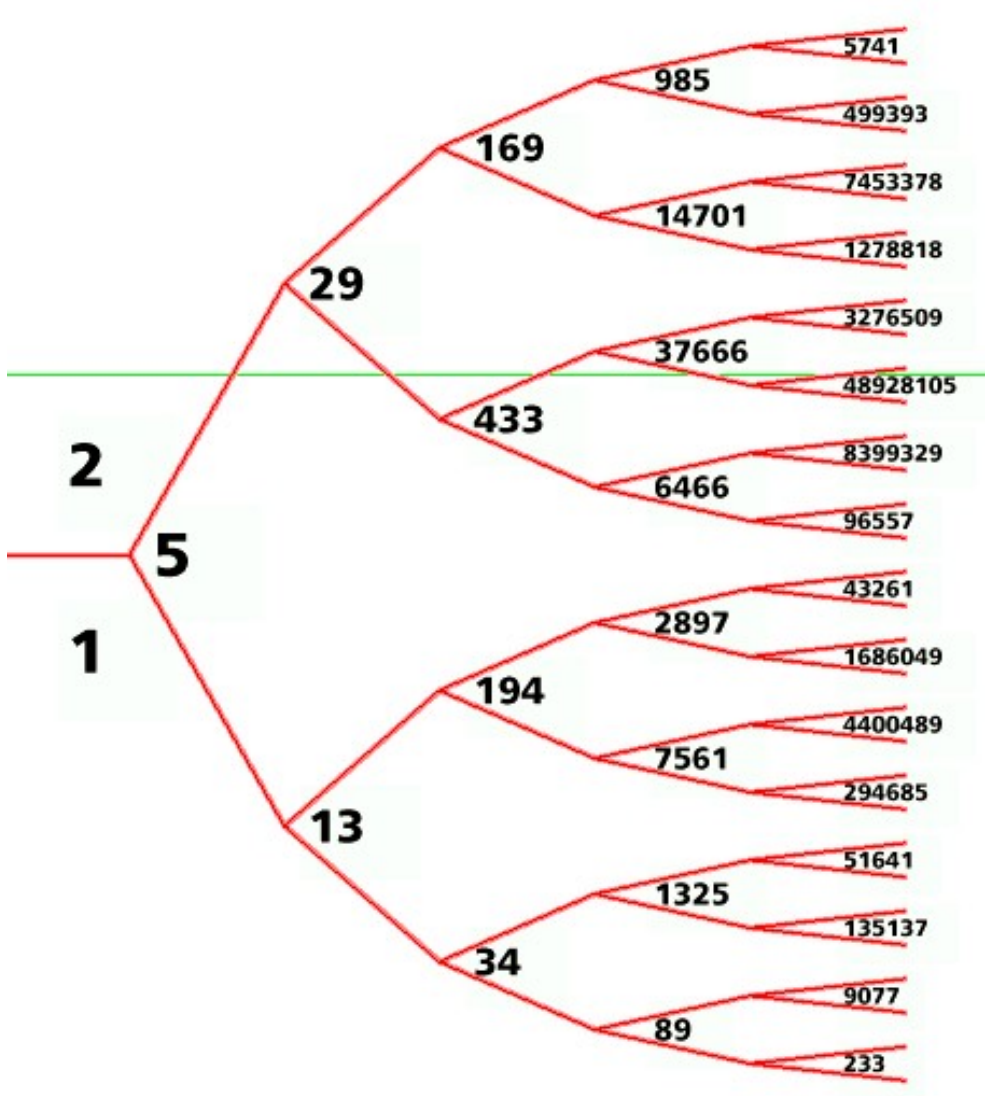
E. Bombieri,

Continued fractions and the Markoff tree,

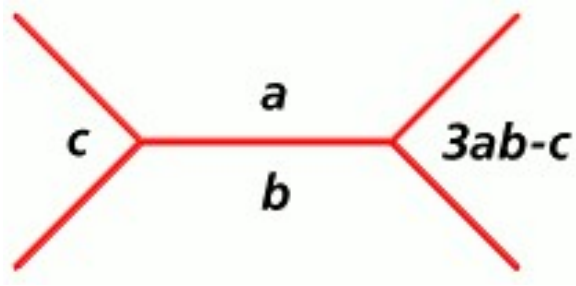
Expo. Math. **25** (2007),

no. 3, 187–213.

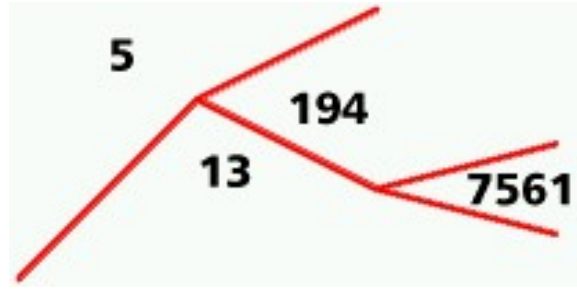
L'arbre de Markoff

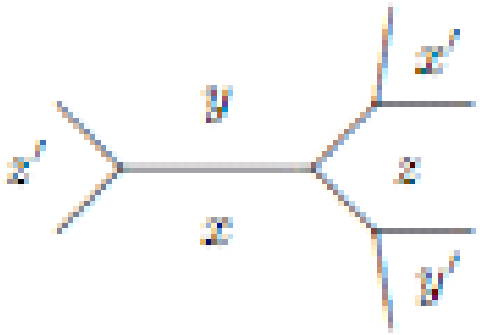


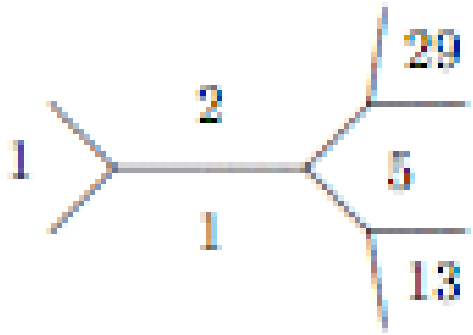
$$a^2 + b^2 + c^2 = 3abc$$



$$X^2 - 3abX + a^2 + b^2 =$$
$$(X - c)(X - 3ab + c)$$







La suite de Fibonacci et l'équation de Markoff

Le plus petit nombre de Markoff est 1. Quand on fixe $z = 1$ dans l'équation de Markoff $x^2 + y^2 + z^2 = 3xyz$, on obtient l'équation

$$x^2 + y^2 + 1 = 3xy.$$

En décrivant l'arbre de Markoff à partir de $(1, 1, 1)$, on obtient une sous–suite de la suite de Markoff

$$1,\ 2,\ 5,\ 13,\ 34,\ 89,\ 233,\ 610,\ 1597, 4181,\ 10946,\ 28657,\ \ldots\ldots$$

qui est la suite des nombres de Fibonacci d'indices impairs

$$F_1 = 1,\ F_3 = 2,\ F_5 = 5,\ F_7 = 13,\ F_9 = 34,\ F_{11} = 89,\ \ldots$$

Leonardo Pisano Fibonacci

La suite de Fibonacci $(F_n)_{n\geq 0}$:

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,$$

$$34,\ 55,\ 89,\ 144,\ 233\ldots$$

est définie par

$$F_0 = 0,\ F_1 = 1,$$

$$F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

Leonardo Pisano Fibonacci
(1170–1250)

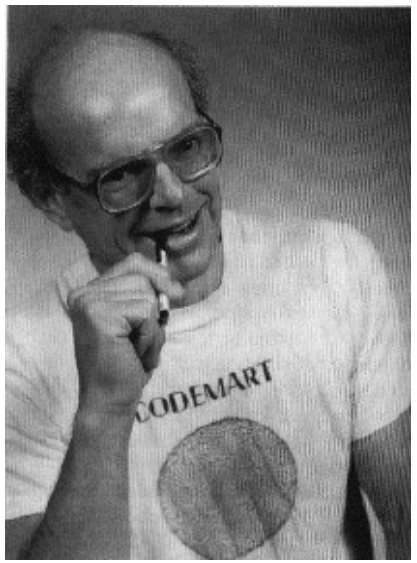
Encyclopédie des suites (suite)

0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025, 121393, 196418, 317811, 514229, 832040, 1346269, 2178309, 3524578, 5702887, 9227465, ...

On trouve la suite de Fibonacci sur la toile

The On-Line Encyclopedia of Integer Sequences

Neil J. A. Sloane



http ://www.research.att.com/~njas/sequences/A000045

Suite de Fibonacci et nombre d'or

- Construction géométrique de la suite de Fibonacci

- Comparaison avec la construction géométrique du développement en fraction continue du nombre d'or.

$$\Phi = \frac{1}{\Phi - 1}, \quad \Phi = \frac{1+\sqrt{5}}{2} = 2\cos(\pi/5).$$

`http ://images.math.cnrs.fr/`
`Le-nombre-d-or-en-mathematique.html`

- $\Phi^2 = 1 + \Phi$,

$$\Phi = \sqrt{1+\Phi} = \sqrt{1+\sqrt{1+\Phi}} = \cdots = \sqrt{1+\sqrt{1+\sqrt{1+\cdots}}}$$

Nombres de Fibonacci d'indices impairs

Les nombres de Fibonacci d'indices impairs sont des nombres de Markoff :

$$F_{m+3}F_{m-1} - F_{m+1}^2 = (-1)^m \quad \text{pour} \quad m \geq 1$$

et

$$F_{m+3} + F_{m-1} = 3F_{m+1} \quad \text{pour} \quad m \geq 1.$$

Posons $y = F_{m+1}$, $x = F_{m-1}$, $x' = F_{m+3}$. Alors, pour m pair, on a

$$x + x' = 3y, \quad xx' = y^2 + 1$$

et

$$X^2 - 3yX + y^2 + 1 = (X - x)(X - x').$$

Ordre des *nouvelles* solutions

Soit (m, m_1, m_2) une solution de l'équation de Markoff

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2.$$

Désignons par m' la seconde racine du polynôme quadratique

$$X^2 - 3m_1m_2X + m_1^2 + m_2^2.$$

Ainsi

$$X^2 - 3m_1m_2X + m_1^2 + m_2^2 = (X - m)(X - m')$$

et

$$m + m' = 3m_1m_2, \quad mm' = m_1^2 + m_2^2.$$

$m_1 \neq m_2$

Montrons que *si* $m_1 = m_2$, *alors* $m_1 = m_2 = 1$ *:*
ceci ne se produit que pour les deux solutions $(1, 1, 1)$, $(2, 1, 1)$.

Supposons $m_1 = m_2$. On a

$$m^2 + 2m_1^2 = 3mm_1^2 \quad \text{donc} \quad m^2 = (3m - 2)m_1^2.$$

Alors m_1 divise m. Soit $m = km_1$. On a $k^2 = 3km_1 - 2$, donc k divise 2.
Quand $k = 1$ on obtient $m = m_1 = 1$.
Quand $k = 2$ on trouve $m_1 = 1$, $m = 2$.

Considérons désormais une solution autre que $(1, 1, 1)$ ou $(2, 1, 1)$: on a $m_1 \neq m_2$.

Deux plus grandes et une plus petite

Supposons $m_1 > m_2$.
Question : *a-t-on* $m' > m_1$ *ou bien* $m' < m_1$ *?*

Considérons le nombre $a = (m_1 - m)(m_1 - m')$.

Comme $m + m' = 3m_1m_2$, et $mm' = m_1^2 + m_2^2$ on a

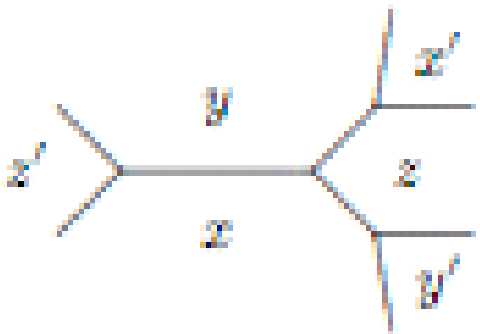
$$\begin{aligned} a &= m_1^2 - m_1(m + m') + mm' \\ &= 2m_1^2 + m_2^2 - 3m_1^2m_2 \\ &= (2m_1^2 - 2m_1^2m_2) + (m_2^2 - m_1^2m_2). \end{aligned}$$

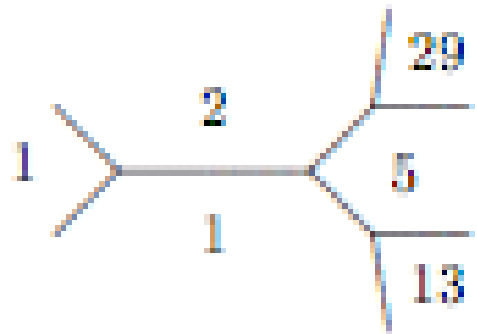
Mais $2m_1^2 < 2m_1^2m_2$ et $m_2^2 < m_1^2m_2$, donc $a < 0$.

Autrement dit $\boxed{m_1 \text{ est entre } m \text{ et } m'.}$

Ordre des solutions

Si $m > m_1$ on a $m_1 > m'$ et la nouvelle solution (m', m_1, m_2) est plus petite que la solution initiale (m, m_1, m_2).
Si $m < m_1$ on a $m_1 < m'$ et la nouvelle solution (m', m_1, m_2) est plus grande que la solution initiale (m, m_1, m_2).





Facteurs premiers

Remarque. Soit m un nombre de Markoff :

$$m^2 + m_1^2 + m_2^2 = 3mm_1m_2.$$

Le même argument montre que le PGCD de m, m_1 et m_2 est 1 : en effet, si p divise m_1, m_2 et m, alors p divise les *nouvelles* solutions produites par le procédé de la corde et de la tangente - en descendant dans l'arbre on trouve que p doit diviser 1.
Les facteurs premiers impairs de m sont tous congrus à 1 modulo 4 (ils divisent une somme de deux carrés premiers entre eux).
Si m est un nombre de Markoff pair, alors les nombres

$$\frac{m}{2}, \quad \frac{3m-2}{4}, \quad \frac{3m+2}{8}$$

sont entiers et impairs.

La conjecture de Markoff

On dispose donc d'un algorithme donnant la suite des nombres de Markoff. Chaque nombre de Markoff apparaît une infinité de fois dans l'arbre comme une des composantes de la solution de l'équation.

Par définition, pour un nombre de Markoff $m > 2$, il existe un couple (m_1, m_2) d'entiers positifs avec $m > m_1 > m_2$ tels que $m^2 + m_1^2 + m_2^2 = 3mm_1m_2$.

Question : *Étant donné m, un tel couple (m_1, m_2) est-il unique ?*

La réponse est oui tant que $m \leq 10^{105}$.

Travaux de Frobenius

La *conjecture de Markoff* n'apparaît pas dans les travaux de Markoff en 1879 et 1880 mais dans ceux de Frobenius en 1913.

Ferdinand Georg Frobenius
(1849–1917)

Cas particuliers

La conjecture est démontrée pour certains nombres de Markoff m comme
p^n, $(p^n \pm 2)/3$, p premier
A. Baragar (1996),
P. Schmutz (1996),
J.O. Button (1998),
M.L. Lang, S.P. Tan (2005),
Ying Zhang (2007).

Arthur Baragar

http ://www.nevada.edu/∼baragar/

Puissance d'un nombre premier

Anitha Srinivasan, 2007
A really simple proof of the Markoff conjecture for prime powers

Number Theory Web
Created and maintained by
Keith Matthews, Brisbane, Australia
www.numbertheory.org/pdfs/simpleproof.pdf

État de la conjecture

10/09/2007, 04/12/2007 : Norbert Riedel

http ://fr.arxiv.org/abs/0709.1499v2

A triple (a, b, c) of positive integers is called a Markoff triple iff it satisfies the diophantine equation $a^2 + b^2 + c^2 = abc$. Recasting the Markoff tree, whose vertices are Markoff triples, in the framework of integral upper triangular 3×3 matrices, it will be shown that the largest member of such a triple determines the other two uniquely. This answers a question which has been open for almost 100 years.

Erreur décelée par Serge Perrine.

Pourquoi le coefficient 3 ?

Soit n un entier positif.
Hurwitz (1907) : *Si l'équation* $x^2 + y^2 + z^2 = nxyz$ *a une solution en entiers positifs, alors*
ou bien $n = 3$ *et* x, y, z *sont premiers entre eux,*
ou bien $n = 1$ *et le* PGCD *des nombres* x, y, z *est* 3.

Friedrich Hirzebruch & Don Zagier,
The Atiyah–Singer Theorem and elementary number theory,
Publish or Perish (1974)

Équations de type Markoff

Bijection entre les solutions de l'équation avec $n = 1$ *et celles avec* $n = 3$ *:*

- si $x^2 + y^2 + z^2 = 3xyz$, alors $(3x, 3y, 3z)$ est solution de $X^2 + Y^2 + Z^2 = XYZ$, car $(3x)^2 + (3y)^2 + (3z)^2 = (3x)(3y)(3z)$.

- si $X^2 + Y^2 + Z^2 = XYZ$, alors X, Y, Z sont multiples de 3, et $(X/3)^2 + (Y/3)^2 + (Z/3)^2 = 3(X/3)(Y/3)(Z/3)$.

Les carrés modulo 3 sont 0 et 1, si X, Y et Z ne sont pas multiples de 3, alors $X^2 + Y^2 + Z^2$ est multiple de 3.

Si un ou deux seulement parmi X, Y, Z est multiple de 3, alors $X^2 + Y^2 + Z^2$ n'est pas multiple de 3.

Équations $x^2 + ay^2 + bz^2 = (1 + a + b)xyz$

Si on impose que $(1, 1, 1)$ soit une solution, il n'y a (à permutation près) que deux autres équations diophantiennes du type

$$x^2 + ay^2 + bz^2 = (1 + a + b)xyz$$

ayant une infinité de solutions entières : ce sont celles avec $(a, b) = (1, 2)$ et $(2, 3)$:

$$x^2 + y^2 + 2z^2 = 4xyz \quad \text{et} \quad x^2 + 2y^2 + 3z^2 = 6xyz.$$

- $x^2 + y^2 + z^2$: pavage du plan par des triangles équilatéraux,
- $x^2 + y^2 + 2z^2 = 4xyz$: pavage du plan par des triangles isocèles rectangles,
- $x^2 + 2y^2 + 3z^2 = 6xyz$: pavage ?

Le phénomène de Laurent

Lien avec les polynômes de Laurent.

James Propp, *The combinatorics of frieze paterns and Markoff numbers,* http ://fr.arxiv.org/abs/math/0511633

Si f, g, h sont des polynômes de Laurent en deux variables x et y, c'est-à-dire des polynômes en x, x^{-1}, y, y^{-1}, en général

$$h\big(f(x,y),g(x,y)\big)$$

n'est pas un polynôme de Laurent :

$$f(x)=\frac{x^2+1}{x}=x+\frac{1}{x},$$

$$f\big(f(x)\big)=\frac{\left(x+\dfrac{1}{x}\right)^2+1}{x+\dfrac{1}{x}}=\frac{x^4+3x^2+1}{x(x^2+1)}.$$

Équation de Hurwitz (1907)

Pour chaque entier $n \geq 2$, l'ensemble K_n des entiers positifs k pour lesquels l'équation

$$x_1^2 + x_2^2 + \cdots + x_n^2 = k x_1 \cdots x_n$$

a une solution en entiers positifs est fini.

Le plus grand élément k de K_n est n — avec la solution

$$(1, 1, \ldots, 1).$$

Exemples :

$$K_3 = \{1,\ 3\},$$
$$K_4 = \{1,\ 4\},$$
$$K_7 = \{1,\ 2,\ 3,\ 5,\ 7\}.$$

Équation de Hurwitz

$$x_1^2 + x_2^2 + \cdots + x_n^2 = k x_1 \cdots x_n$$

Quand il y a une solution en entiers positifs, il y en a une infinité, qui se répartissent en un nombre fini d'arbres.

On conjecture qu'*il existe de telles équations nécessitant un nombre d'arbres arbitrairement grand* (analogue de la situation pour le rang des courbes elliptiques).

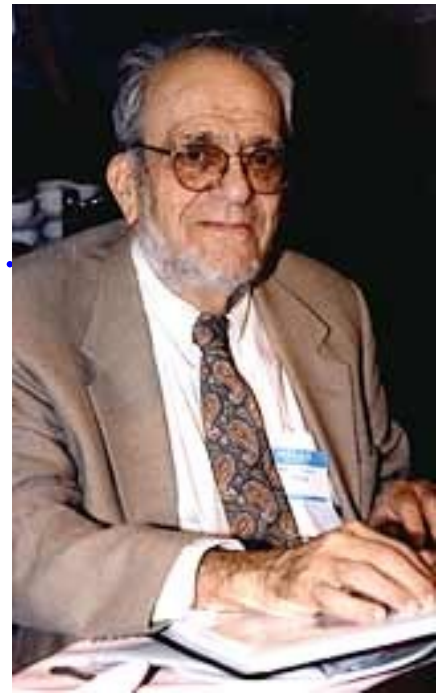
Nombre maximal connu d'arbres nécessaires : 14 (D. Zagier).

Croissance de la suite de Markoff

1978 : ordre de grandeur de m, m_1 et m_2 pour $m^2 + m_1^2 + m_2^2 = 3mm_1m_2$ avec $m_1 < m_2 < m$,

$$\log(3m_1) + \log(3m_2) = \log(3m) + o(1).$$

Harvey Cohn



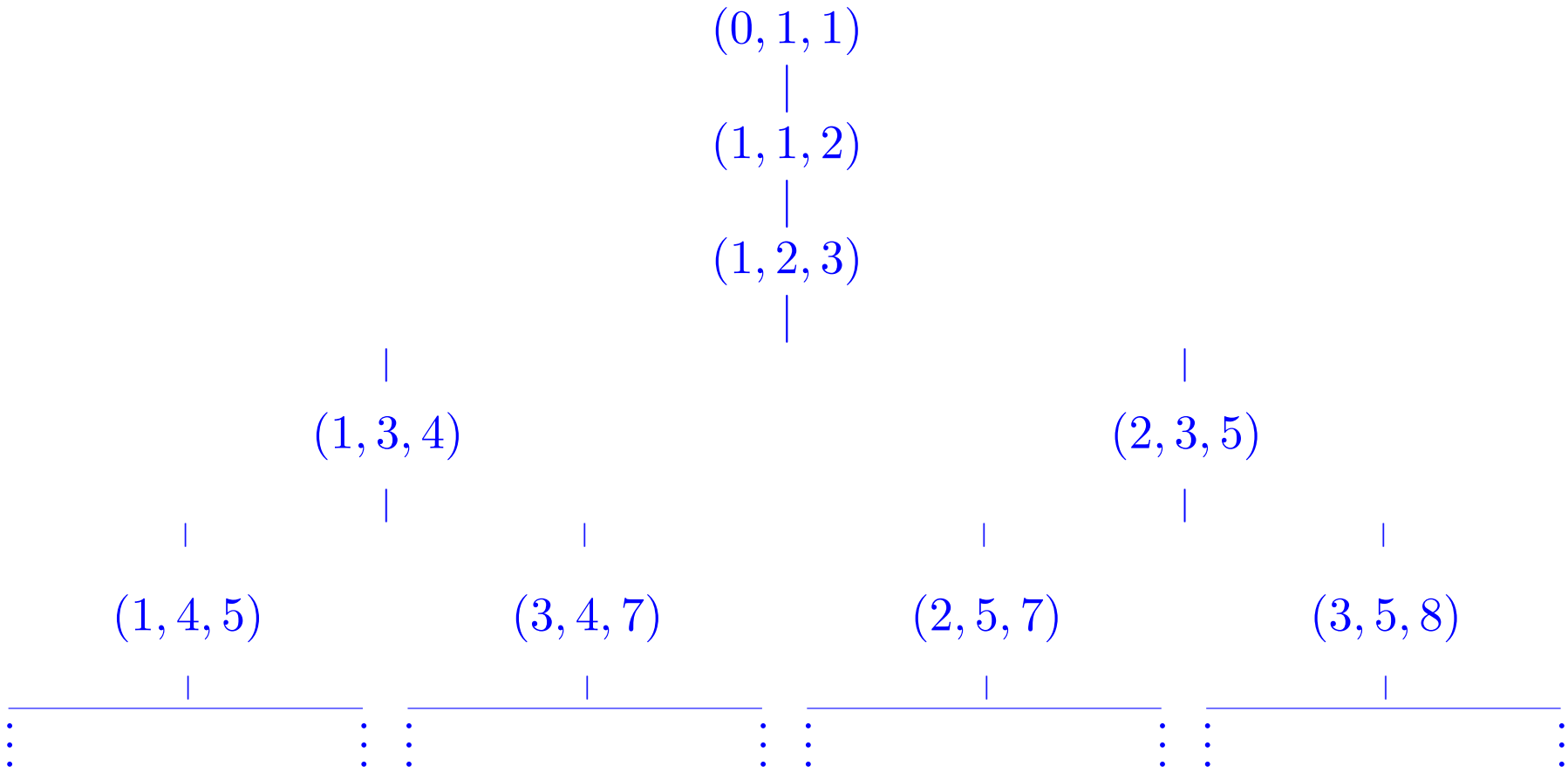
Identifier des mots primitifs dans un groupe libre à deux générateurs

Markoff forms and primitive words

$x \mapsto \log(3x) : (m_1, m_2, m) \mapsto (a, b, c)$ avec $a + b \sim c$.

Arbre d'Euclide

On part de $(0, 1, 1)$. Quand on a un triplet (a, b, c) avec $a + b = c$ et $a \leq b \leq c$, on en déduit deux autres plus grands $(a, c, a + c)$ et $(b, c, b + c)$ et un plus petit $(a, b - a, b)$ ou $(b - a, a, b)$.



Arbre de Markoff et arbre d'Euclide

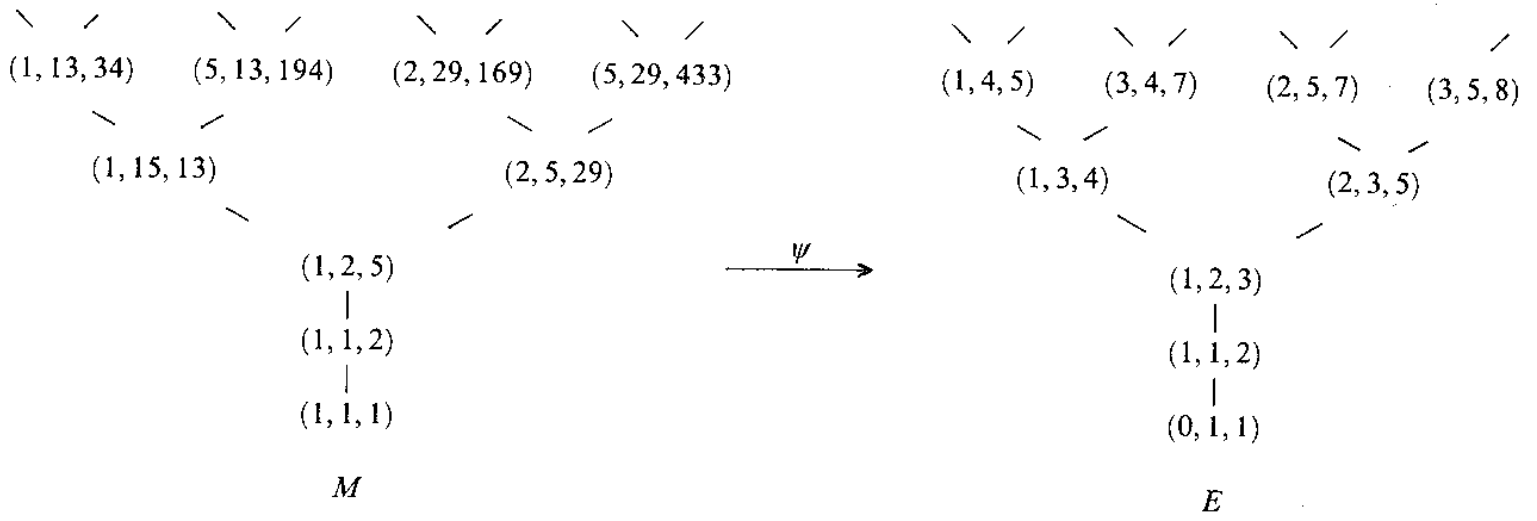


FIGURE 2. THE MARKOFF TREE AND THE EUCLID TREE

Tom Cusik & Mary Flahive,
The Markoff and Lagrange spectra,
Math. Surveys and Monographs **30**, AMS (1989).

Croissance de la suite de Markoff

Don Zagier (1982)
estimation du nombre de
triplets de Markoff majorés
par x :

$$c(\log x)^2 + O\big(\log x(\log\log x)^2\big),$$

$$c = 0,18071704711507\ldots$$

Conjecture : le n-ième nombre de Markoff m_n vérifie

$$m_n \sim A^{\sqrt{n}} \quad \text{avec} \quad A = 10,5101504\cdots$$

Origine historique : approximation rationnelle

Théorème de Hurwitz
(1891) : *Pour tout nombre réel irrationnel x, il existe une infinité de p/q tels que*

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{\sqrt{5}q^2}.$$

Nombre d'Or
$\Phi = (1+\sqrt{5})/2 = 1,6180339887498948482\ldots$
ce résultat est optimal.

Adolf Hurwitz
(1859–1919)

Énoncé de Hurwitz

L'énoncé de Hurwitz peut se formuler :

$$\liminf_{q\to\infty} q \min_{p\in\mathbf{Z}} |qx-p| \leq \frac{1}{\sqrt{5}} \quad \text{pour tout } x \in \mathbf{R}\setminus\mathbf{Q}$$

avec égalité pour $x = \Phi$ le Nombre d'Or.

Remarque : on montre que pour tout nombre réel irrationnel x,

$$\limsup_{q\to\infty} \left(\min_{p\in\mathbf{Z}} |qx-p|\right) = \frac{1}{2} \quad \text{pour tout } x \in \mathbf{R}\setminus\mathbf{Q}.$$

Plus précisément la suite $(qx)_{q\geq 1}$ est *équirépartie modulo* 1.

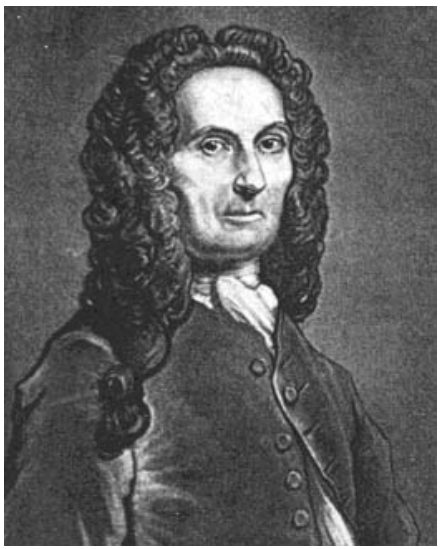
La suite de Fibonacci et le Nombre d'Or

Formule de A. De Moivre (1730), L. Euler (1765), J.P.M. Binet (1843) :

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

La formule de De Moivre – Euler – Binet

Abraham de Moivre (1667–1754)



Leonhard Euler (1707–1783)

Jacques Philippe Marie Binet (1786–1856)

F_n est l'entier le plus proche de $\frac{1}{\sqrt{5}}\Phi^n$.

Relation quadratique

On vérifie, par récurrence,

$$F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n \quad \text{pour tout} \quad n \geq 0.$$

Le membre de gauche est la valeur en (F_{n+1}, F_n) de la forme quadratique

$$X^2 - XY - Y^2 = (X - \Phi Y)(X + \Phi^{-1}Y).$$

La suite $u_n = F_{n+1}/F_n$, $n \geq 1$ converge vers le Nombre d'Or Φ et

$$F_{n+1}^2 - F_{n+1}F_n - F_n^2 = F_n^2(u_n - \Phi)(u_n + \Phi^{-1}).$$

La suite u_n des quotients de Fibonacci

On en déduit

$$F_n^2|\Phi - u_n| = \frac{1}{\Phi^{-1} + u_n} \to \frac{1}{\Phi^{-1} + \Phi} = \frac{1}{\sqrt{5}}.$$

D'où

$$\lim_{n\to\infty} F_n^2 \left|\Phi - \frac{F_{n+1}}{F_n}\right| = \frac{1}{\sqrt{5}}.$$

Fractions continues

La suite $u_n = F_{n+1}/F_n$ est aussi définie par

$$u_1 = 1,\ u_n = 1 + \frac{1}{u_{n-1}},\quad (n \geq 2).$$

Donc

$$u_n = 1 + \frac{1}{1 + \frac{1}{u_{n-2}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{u_{n-3}}}} = \cdots$$

$$= 1 + \frac{1|}{|1} + \frac{1|}{|1} \cdots + \frac{1|}{|1} + \frac{1|}{|1}$$

$$= [1, 1, \ldots, 1] \quad n \text{ termes}$$

$$\Phi = [\overline{1}]$$

Le résultat de Hurwitz est optimal

L'énoncé de Hurwitz

$$\liminf_{q\to\infty} q \min_{p\in\mathbf{Z}} |qx-p| \leq \frac{1}{\sqrt{5}} \quad \text{pour tout } x \in \mathbf{R}\setminus\mathbf{Q}$$

est optimal : il y a égalité dans le cas $x = \Phi$.
Pour $|q\Phi - p| \leq 1$, on a

$$1 \leq |q^2 + pq - p^2| = |q\Phi - p| \cdot (q\Phi^{-1} + p)$$

avec

$$q\Phi^{-1} + p = q(\Phi + \Phi^{-1}) + p - q\Phi \leq q\sqrt{5} + 1,$$

donc

$$1 \leq |q\Phi - p| \cdot (q\sqrt{5} + 1).$$

Noter que $P(X) = X^2 - X - 1$ a pour discriminant 5 et $P'(\Phi) = \sqrt{\Delta} = \sqrt{5}$.

Inégalité de Liouville

Inégalité de Liouville.
Soient α un nombre algébrique de degré $d \geq 2$, $P \in \mathbf{Z}[X]$ son polynôme minimal, $c = |P'(\alpha)|$ et $\epsilon > 0$. Il existe un entier q_0 tel que, pour tout $p/q \in \mathbf{Q}$ avec $q \geq q_0$,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(c+\epsilon)q^d}.$$

Joseph Liouville, 1844

Inégalité de Liouville

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(c+\epsilon)q^d}, \qquad c = |P'(\alpha)|.$$

Quand α est un nombre réel irrationnel quadratique ($d = 2$) de discriminant $\Delta > 0$, on a $c = \sqrt{\Delta}$.

Remarque : pour un polynôme quadratique irréductible $P(X) = aX^2 + bX + c$ à coefficients entiers de discriminant $\Delta = b^2 - 4ac > 0$, on a $\Delta \geq 5$.

Démonstration de l'inégalité de Liouville

Soient q un entier suffisamment grand, p l'entier le plus proche de $q\alpha$:

$$|q\alpha - p| \leq \frac{1}{2}.$$

Soit $a_0 > 0$ le coefficient directeur de P et $\alpha_1, \ldots, \alpha_d$ ses racines, avec $\alpha_1 = \alpha$:

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_d),$$

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^{d} \left(\frac{p}{q} - \alpha_i\right),$$

et

$$P'(\alpha) = a_0 \prod_{i=2}^{d} (\alpha - \alpha_i).$$

Démonstration de l'inégalité de Liouville

On a $q^d P(p/q) \in \mathbf{Z} \setminus \{0\}$.

Pour $i \geq 2$ on a

$$\left|\alpha_i - \frac{p}{q}\right| \leq |\alpha_i - \alpha| + \frac{1}{2q}.$$

Donc

$$1 \leq q^d a_0 \left|\alpha - \frac{p}{q}\right| \prod_{i=2}^{d} \left(|\alpha_i - \alpha| + \frac{1}{2q}\right).$$

Pour q suffisamment grand on déduit

$$1 \leq q^d \left|\alpha - \frac{p}{q}\right| (|P'(\alpha)| + \epsilon).$$

Constante de Markoff

Pour $x \in \mathbf{R} \setminus \mathbf{Q}$, notons $\lambda(x) \in [\sqrt{5}, +\infty]$ la borne supérieure des $\gamma > 0$ tels qu'il existe une infinité de $p/q \in \mathbf{Q}$ satisfaisant

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{\gamma q^2}.$$

Autrement dit

$$\frac{1}{\lambda(x)} = \liminf_{q \to \infty} q \min_{p \in \mathbf{Z}} |qx - p| .$$

Hurwitz : $\lambda(x) \geq \sqrt{5}$ pour tout x et $\lambda(\Phi) = \sqrt{5}$.
trois opérations $x \mapsto x + 1$, $x \mapsto -x$ et $x \mapsto 1/x$, alors $\lambda(x) = \lambda(y)$.

Nombres mal approchables

Un nombre réel irrationnel x est *mal approchable* par les nombres rationnels si sa constante de Markoff est finie : cela signifie qu'il existe $\gamma > 0$ tel que, pour tout $p/q \in \mathbf{Q}$,

$$\left| x - \frac{p}{q} \right| \geq \frac{1}{\gamma q^2}.$$

Par exemple les nombres de Liouville ont une constante de Markoff infinie.

Un nombre réel irrationnel est mal approchable si et seulement si la suite $(a_n)_{n \geq 0}$ des quotients partiels de son développement en fractions continues

$$x = [a_0,\ a_1,\ a_2,\ \ldots, a_n,\ \ldots]$$

est bornée.

Nombres mal approchables

Tout nombre réel quadratique irrationnel a une constante de Markoff finie.

On ignore s'il existe des nombres algébriques réels de degré ≥ 3 qui soient mal approchables.

On ignore aussi s'il n'en existe pas...

On conjecture que *tout nombre réel irrationnel non quadratique mal approchable est transcendant.*

Mesure de Lebesgue

Les nombres mal approchables forment un ensemble de mesure nulle pour la mesure de Lebesgue.

Henri Léon Lebesgue
(1875–1941)

Propriétés de la constante de Markoff

On a

$$\lambda(x+1) = \lambda(x) : \qquad \left| x + 1 - \frac{p}{q} \right| = \left| x - \frac{p+q}{q} \right|$$

et

$$\lambda(-x) = \lambda(x) : \qquad \left| -x - \frac{p}{q} \right| = \left| x + \frac{p}{q} \right|,$$

On a aussi $\lambda(1/x) = \lambda(x)$:

$$p^2 \left| \frac{1}{x} - \frac{q}{p} \right| = q^2 \left| \frac{p}{qx} \right| \cdot \left| x - \frac{p}{q} \right|.$$

Le groupe modulaire

Le groupe multiplicatif engendré par les trois matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

est le groupe des matrices 2×2

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients dans $\mathbf{Z}$

de déterminant ± 1.

J-P. Serre – *Cours d'arithmétique*, Coll. SUP, Presses Universitaires de France, Paris, 1970.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} x = \frac{ax+b}{cx+d}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} x = x+1 \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} x = -x \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x = \frac{1}{x}$$

$$\lambda(x+1) = \lambda(x) \qquad \lambda(-x) = \lambda(x) \qquad \lambda(1/x) = \lambda(x)$$

Conséquence : *Soit* $x \in \mathbf{R} \setminus \mathbf{Q}$ *et soient* a, b, c, d *des entiers rationnels satisfaisant* $ad - bc = \pm 1$. *On pose*

$$y = \frac{ax+b}{cx+d}.$$

Alors $\lambda(x) = \lambda(y)$.

Travaux de Hurwitz (suite)

L'inégalité $\lambda(x) \geq \sqrt{5}$ *pour tout* x *irrationnel* est optimale pour le Nombre d'Or et pour tous les nombres *nobles* dont le développement en fraction continue termine par une suite infinie de 1, qui sont les racines de polynômes quadratiques de discriminant 5.

$$\Phi = [1, 1, 1, \ldots] = [\overline{1}].$$

Adolf Hurwitz, 1891

Le début du spectre

Pour tous les nombres qui ne sont pas associés au Nombre d'Or par une homographie à coefficients entiers de déterminant ± 1, une inégalité plus forte que celle de Hurwitz

$$\lambda(x) \geq \sqrt{5} = 2,236\,;067\,977\ldots$$

est valable, à savoir

$$\lambda(x) \geq 2\sqrt{2} = 2,828\,427\,125\ldots$$

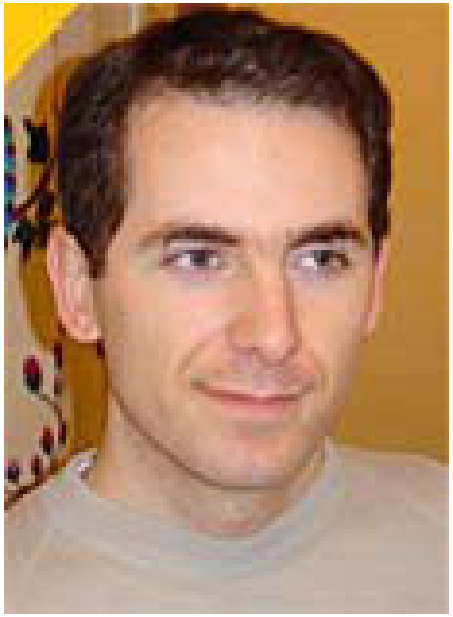
C'est optimal pour

$$\sqrt{2} = 1,414213562373095048801688724209698078\ldots$$

dont le développement en fraction continue est

$$[1;\ 2,2,2,\ldots] = [1;\ \overline{2}].$$

Le fabuleux destin de $\sqrt{2}$



Éditions
Le Pommier

- Benoît Rittaud, Éditions *Le Pommier* (2006).

http://www.math.univ-paris13.fr/∼rittaud/RacineDeDeux

$\lambda(\sqrt{2}) = 2\sqrt{2}$

Comme le discriminant de $X^2 - 2$ est 8, on a $\lambda(\sqrt{2}) \geq 2\sqrt{2}$.
Montrons l'égalité.

On pose $G_0 = 0$, $G_1 = 1$, et par récurrence on définit
$G_n = 2G_{n-1} + G_{n-2}$ pour $n \geq 2$.
Pour tout $n \geq 1$, on a

$$G_n^2 - 2G_nG_{n-1} - G_{n-1}^2 = (-1)^{n-1}.$$

La suite $(G_n/G_{n-1})_{n\geq 2}$ converge vers $1 + \sqrt{2}$ quand $n \to \infty$.

Donc il existe une suite $(p_n/q_n)_{n\geq 1}$ de nombre rationnels telle que

$$\lim_{n\to\infty} q_n \left| q_n\sqrt{2} - p_n \right| = \frac{1}{2\sqrt{2}}.$$

La suite du spectre

Pour tous les nombres x associés au Nombre d'Or par une homographie à coefficients entiers de déterminant 1, on a

$$\lambda(x) = \sqrt{5} = 2,236\ 067\ 977\ldots$$

Pour tous les nombres associés à $\sqrt{2}$, on a

$$\lambda(x) = 2\sqrt{2} = 2,828\ 427\ 125\ldots$$

Pour tous les autres nombres réels irrationnels x, on a

$$\lambda(x) \geq \frac{\sqrt{221}}{5} = 2,973\ 213\ 749\ldots$$

C'est optimal pour les racines du polynôme $5x^2 + 11x - 5$ et ses associés, dont le développement en fraction continue termine par la période $\overline{2211}$.

La suite du spectre

La suite de nombres commençant par $\lambda_1 = \sqrt{5}$, $\lambda_2 = 2\sqrt{2}$, $\lambda_5 = \sqrt{221}/5$,... continue avec

$$\lambda_{13} = \frac{\sqrt{1517}}{13}, \quad \lambda_{29} = \frac{\sqrt{7565}}{29} \ldots$$

et plus généralement

$$\lambda_m = \sqrt{9 - \frac{4}{m^2}}$$

où m décrit la suite des nombres de Markoff.

Les polynômes quadratiques

La suite de polynômes quadratiques commençant par

$$f_1(x) = x^2 - x - 1,$$

$$f_2(x) = 2x^2 + 4x - 2,$$

$$f_5(x) = 5x^2 + 11x - 5,$$

continue avec

$$f_{13}(x) = 13x^2 + 29x - 13,$$

de discriminant 1517. Ses racines et leurs associés ont un développement en fraction continue qui termine par la période $\overline{221111}$.

Les polynômes quadratiques

Soient m un nombre de Markoff. On pose

$$\Delta_m = 9m^2 - 4.$$

Soit (m_1, m_2) une solution de l'équation de Markoff

$$m_1^2 + m_2^2 + m^2 = 3m_1 m_2 m, \quad (m_1 \leq m_2 \leq m).$$

Soit $k \in \mathbf{Z}$, $0 < k < m$, tel que $km_1 \equiv m_2 \pmod{m}$.
Comme $m_1^2 + m_2^2 \equiv 0 \pmod{m}$, on a $k^2 + 1 \equiv 0 \pmod{m}$
et le nombre

$$\ell = \frac{k^2 + 1}{m}$$

est entier.

Les polynômes quadratiques

Le polynôme

$$f_m(X) = mX^2 + (3m - 2k)X + \ell - 3k$$

a pour discriminant $9m^2 - 4 = \Delta_m$.

Soient ξ_m et ξ'_m ses racines. Alors

$$\lambda(\xi_m) = \frac{\sqrt{\Delta_m}}{m^2}.$$

De plus les développements en fraction continue de ξ_m et ξ'_m ne comportent que des 1 et des 2.

Minima de formes quadratiques

Considérons une forme quadratique $f(X,Y) = aX^2 + bXY + cY^2$ à coefficient réels. Soit $\Delta(f)$ son discriminant $b^2 - 4ac$.

On s'intéresse au minimum $m(f)$ de $|f(x,y)|$ sur $\mathbf{Z}^2 \setminus \{(0,0)\}$. On suppose donc $\Delta(f) \neq 0$ et on pose

$$C(f) = m(f)/\sqrt{|\Delta(f)|}.$$

Soient α et α' les racines de $f(X,1)$:

$$f(X,Y) = a(X - \alpha Y)(X - \alpha' Y),$$

$$\{\alpha, \alpha'\} = \frac{1}{2a}\left\{-b \pm \sqrt{\Delta(f)}\right\}.$$

Exemple avec $\Delta < 0$

La forme quadratique

$$f(X, Y) = X^2 + XY + Y^2$$

a pour discriminant $\Delta(f) = -3$ et minimum $m(f) = 1$, donc

$$C(f) = \frac{m(f)}{\sqrt{|\Delta(f)|}} = \frac{1}{\sqrt{3}}.$$

Pour $\Delta < 0$, la forme quadratique

$$f(X, Y) = \sqrt{\frac{|\Delta|}{3}}(X^2 + XY + Y^2)$$

a pour discriminant Δ et minimum $\sqrt{|\Delta|/3}$. De nouveau

$$C(f) = \frac{1}{\sqrt{3}}.$$

Formes quadratiques définies ($\Delta < 0$)

Si le discriminant est négatif, J.L. Lagrange et Ch. Hermite (lettre à Jacobi, 6 Août 1845) ont montré que $C(f) \leq 1/\sqrt{3}$ avec égalité pour $f(X,Y) = X^2 + XY + Y^2$. Pour chaque $\varrho \in (0, 1/\sqrt{3}]$, il existe une telle forme f avec $C(f) = \varrho$.

Joseph-Louis Lagrange (1736–1813)

Charles Hermite (1822–1901)

Carl Gustav Jacob Jacobi (1804–1851)

Exemple avec $\Delta > 0$

La forme quadratique

$$f(X, Y) = X^2 - XY - Y^2$$

a pour discriminant $\Delta(f) = 5$ et minimum $m(f) = 1$, donc

$$C(f) = \frac{m(f)}{\sqrt{\Delta(f)}} = \frac{1}{\sqrt{5}}.$$

Pour $\Delta > 0$, la forme quadratique

$$f(X, Y) = \sqrt{\frac{\Delta}{5}}(X^2 - XY - Y^2)$$

a pour discriminant Δ et minimum $\sqrt{\Delta/5}$. De nouveau

$$C(f) = \frac{1}{\sqrt{5}}.$$

Formes quadratiques indéfinies ($\Delta > 0$)

Supposons $\Delta > 0$

A. Korkine et E.I. Zolotarev ont montré en 1873 $C(f) \leq 1/\sqrt{5}$ avec égalité pour $f_0(X, Y) = X^2 - XY - Y^2$.
Pour toutes les formes qui ne sont pas équivalentes à f_0 sous $\mathrm{GL}(2, \mathbf{Z})$ ils montrent $C(f) \leq 1/\sqrt{8}$.
$1/\sqrt{5} = 0,447\,213\,595\ldots$
$1/\sqrt{8} = 0,353\,553\,391\ldots$

Trou !

Egor Ivanovich Zolotarev
(1847–1878)

Formes quadratiques indéfinies ($\Delta > 0$).

Les travaux de Korkine et Zolotarev ont incité A.A. Markoff à étudier la question. Il décrit une infinité de valeurs de $C(f_i)$, $i = 0, 1, \ldots$, entre $1/\sqrt{5}$ et $1/3$, possédant la même propriété que f_0. Ces valeurs convergent vers $1/3$. Il les construit grâce à l'arbre des solutions de l'équation de Markoff.

A. Markoff, 1879 et 1880.

Formes quadratiques indéfinies ($\Delta > 0$)

Soit f une forme quadratique de discriminant $\Delta > 0$.

Si $|f(x, y)|$ est petit avec $y \neq 0$, alors x/y est proche d'une racine de $f(X, 1)$, disons de α.

Par conséquent

$$|x - y\alpha'| \sim |y| \cdot |\alpha - \alpha'|$$

et $\alpha - \alpha' = \sqrt{\Delta}/a$.

Donc

$$|f(x, y)| = |a(x - \alpha y)(x - \alpha' y)| \sim \sqrt{|\Delta|} \left|\alpha - \frac{x}{y}\right|.$$

Spectre de Lagrange et spectre de Markoff

Spectre de Markoff = valeurs atteintes par

$$\frac{1}{C(f)} = \sqrt{\Delta(f)}/m(f)$$

quand f décrit les formes quadratiques binaires $ax^2 + bxy + c$ à coefficients réels de discriminant $\Delta(f) = b^2 - 4ac > 0$ et $m(f) = \inf_{(x,y)\in\mathbf{Z}^2\setminus\{(0,0)\}} |f(x,y)|$.

Spectre de Lagrange = valeurs atteintes par la constante de Markoff (!) :

$$\lambda(x) = 1/\liminf_{q\to\infty} q \min_{p\in\mathbf{Z}} |qx - p|$$

quand x décrit les nombres réels.

Le spectre de Markoff contient le spectre de Lagrange.

Les intersections des deux spectres avec l'intervalle $[\sqrt{5}, 3)$ coïncident : *suite discrète*.

20 janvier 2009

Cours de Théorie des Nombres MM020

Équations Diophantiennes

Michel Waldschmidt

Institut de Mathématiques de Jussieu & CIMPA

http ://www.math.jussieu.fr/∼miw/