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/

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 . . .

Cubes :

1, 8, 27, 64, 125, 216, 343, 512, 729, 1 000, 1 331 . . .

Puissances cinquièmes :

1, 32, 243, 1 024, 3 125, 7 776, 16 807, 32 768 . . .

Plan

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

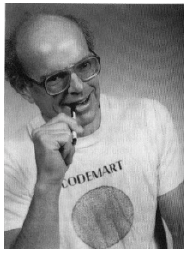
Encyclopédie des suites

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 *:* $(4, 9)$, $(27, 32)$ . . .

Catalan (1844)

$x^p - y^q = 1$

Pillai (1945)

$x^p - y^q = k$

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).

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	...
$R(n)$	$=$	1	2	3	2	5	6	7	2	3	10	11	6	...

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 $K[X]$.

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 $\text{PGCD}(a, b, c) = 1$.

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 $\alpha(a,b,c)\geq\alpha_0$.

Conséquences de la conjecture *abc*

1. Le Dernier Théorème de Fermat sous forme *asymptotique* : Il existe un entier N (non effectif, dépendant de $\kappa(\varepsilon)$) tel que pour tout $n>N$, il n'existe aucune solution de l'équation $x^n+y^n=z^n$.

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 $\text{PGCD}(x,y,z)=1$.

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*

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*) :

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

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*.