On recent Diophantine results

Michel Waldschmidt

Institut de Mathématiques de Jussieu + CIMPA
http://www.math.jussieu.fr/∼miw/

December 21, 2005

SASTRA Kumbakonam December 21, 2005

Ramanujan to Hardy, Don Zagier, SMF—BNF

- Don Zagier (March 16, 2005, BNF/SMF) : "Ramanujan to Hardy, from the first to the last letter..." http ://smf.emath.fr/VieSociete/Rencontres/BNF/2005/
- Mock theta functions
- S. Zwegers – « Mock ϑ-functions and real analytic modular forms. », in *Berndt, Bruce C. (ed.) et al., q-series with applications to combinatorics, number theory, and physics. Proceedings of a conference, University of Illinois, Urbana-Champaign, IL, USA, October 26-28, 2000. Providence, RI : American Mathematical Society (AMS). Contemp. Math. 291, 269-277* . 2001.

Square, cubes...

- A perfect power is an integer of the form a^b where $a \geq 1$ and $b > 1$ are positive integers.
- Squares :

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

- Cubes :

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

- Fifth powers :

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

Perfect powers

The sequence of perfect powers starts with :

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 . . .

Two conjectures

- Catalan's Conjecture : In the sequence of perfect powers, $8, 9$ is the only example of consecutive integers.
- Pillai's Conjecture : In the sequence of perfect powers, the difference between two consecutive terms tends to infinity.
- Alternatively : Let k be a positive integer. The equation
$$x^p - y^q = k,$$
where the unknowns x, y, p and q take integer values, all ≥ 2, has only finitely many solutions (x, y, p, q).

Results

- P. Mihăilescu, 2002. Catalan was right : *the equation* $x^p - y^q = 1$ *where the unknowns* x, y, p *and* q *take integer values, all* ≥ 2, *has only one solution* $(x, y, p, q) = (3, 2, 2, 3)$.
  Previous partial results : J.W.S. Cassels, R. Tijdeman, M. Mignotte. . .
- Higher values of k : nothing known.
- Pillai's conjecture as a consequence of the abc conjecture :

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

with

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

The *abc* Conjecture

- For a positive integer n, we denote by

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

  the *radical* or *square free part* of n.
- The abc Conjecture resulted from a discussion between D. W. Masser and J. Œsterlé in the mid 1980's.
- Conjecture (abc Conjecture). *For each* $\varepsilon > 0$ *there exists* $\kappa(\varepsilon)$ *such that, if* a, b *and* c *in* $\mathbf{Z}_{>0}$ *are relatively prime and satisfy* $a + b = c$, *then*

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

Szpiro's Conjecture

The *abc* Conjecture implies a previous conjecture by L. Szpiro on the conductor of elliptic curves.

Given any $\varepsilon > 0$, there exists a constant $C(\varepsilon) > 0$ such that, for every elliptic curve with minimal discriminant Δ and conductor N,

$$|\Delta| < C(\varepsilon) N^{6+\varepsilon}.$$

Examples

- When a, b and c are three positive relatively prime integers satisfying $a+b=c$, define

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

- Here are the two largest known values for $\lambda(abc)$ (there are 140 known values of $\lambda(a,b,c)$ which are ≥ 1.4).

	$a+b=c$	$\lambda(a,b,c)$	authors
1	$2+3^{10}\cdot 109 = 23^5$	$1.629912\ldots$	É. Reyssat
2	$11^2+3^2 5^6 7^3 = 2^{21}\cdot 23$	$1.625991\ldots$	B.M. Weger

Further examples

- When a, b and c are three positive relatively prime integers satisfying $a+b=c$, define

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

- Here are the two largest known values for $\varrho(abc)$, found by A. Nitaj. There are 46 known triples (a,b,c) with $0<a<b<c$, $a+b=c$ and $\gcd(a,b)=1$ satisfying $\varrho(a,b,c)>4$.

	$a+b=c$	$\varrho(a,b,c)$
1	$13\cdot 19^6+2^{30}\cdot 5=3^{13}\cdot 11^2\cdot 31$	$4.41901\ldots$
2	$2^5\cdot 11^2\cdot 19^9+5^{15}\cdot 37^2\cdot 47=3^7\cdot 7^{11}\cdot 743$	$4.26801\ldots$

Generalized Fermat's equation

The equation $x^p+y^q=z^r$ in positive integers (x,y,z,p,q,r) for which

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

and such that x, y, z relatively prime, has the following 10 solutions (*F. Beukers, D. Zagier*) :

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

Beal's Conjecture

- Beal's Conjecture (R. Tijdeman and D. Zagier). The equation $x^p + y^q = z^r$ has no solution in positive integers (x, y, z, p, q, r) with each of p, q and r at least 3 and x, y, z relatively prime.
- 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.
- Generalized Fermat–Catalan equation. Modular method : Wiles...

Powers with identical digits

- Y. Bugeaud and M. Mignotte (1999) : solution of a conjecture due to Inkeri.
  There is no perfect power with identical digits in its decimal expansion.
  Diophantine equation :

  $$c \cdot \frac{10^k - 1}{9} = a^b$$

  with $1 \le c \le 9$, $a \ge 2$, $b \ge 2$.
- ($2 \le c \le 9$: K. Inkeri, 1972).

Perfect powers in the Fibonacci sequence

- Fibonacci sequence :

  $$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144\ldots$$

  where $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ $(n \geq 3)$.
- Theorem (Bugeaud, Mignotte, Siksek ; 2004). *The only perfect powers in the sequence of Fibonacci numbers are* 1, 8 *and* 144.
- Diophantine equation $F_n = a^b$, with $n \geq 1$, $a \geq 2$, $b \geq 2$.
- T.N. Shorey and F. Luca (2004) : the product of 2 or more consecutive Fibonacci numbers, other than F_1F_2, is never a perfect power.

Hilbert's tenth problem : the role of the Fibonacci sequence

- D. Hilbert (1900) — *Problem :* to give an algorithm in order to decide whether a diophantine equation has an integer solution or not.
- J. Robinson (1952)
- J. Robinson, M. Davis, H. Putnam (1961)
- Yu. Matijasevic (1970)
- The relation $b = F_a$ between two integers a and b is *a diophantine relation with exponential growth.*

Historical survey

- XIXth Century : Hurwitz, Poincaré
- Mordell's Conjecture : rational points
- Siegel's Theorem (1929) : integral points
- Faltings' Theorem(1983) : finiteness of rational points on an algebraic curve of genus ≥ 2 over a number field.
- G. Rémond (2000) : explicit upper bound for the number of solutions.

The Ramanujan–Nagell equation

- $$x^2 + 7 = 2^n$$
  has the solutions
  $$\begin{array}{rcccr} 1^2+7 &=& 2^3 &=& 8 \\ 3^2+7 &=& 2^4 &=& 16 \\ 5^2+7 &=& 2^5 &=& 32 \\ 11^2+7 &=& 2^7 &=& 128 \\ 181^2+7 &=& 2^{15} &=& 32\,768 \end{array}$$
- Nagell (1948) : no further solution

The Ramanujan–Nagell equation (continued)

- Apéry (1960) : for $D > 0$, $D \neq 7$, the equation $x^2 + D = 2^n$ has at most 2 solutions.
- Examples with 2 solutions :

$$D = 23 : \qquad 3^2 + 23 = 32, \quad 45^2 + 23 = 2^{11} = 2\,048$$

$$D = 2^{\ell+1} - 1,\ \ell \geq 3 : \quad (2^\ell - 1)^2 + 2^{\ell+1} - 1 = 2^{2\ell}$$

- Beukers (1980) : at most one solution otherwise.
- M. Bennett (1995) : considers the case $D < 0$.

Ramanujan's approximation for π

- $$\frac{63}{25}\left(\frac{17 + 15\sqrt{5}}{7 + 15\sqrt{5}}\right) = 3.141\,592\,653 \quad 805\ldots$$

  is a root of $P(x) = 168\,125\,x^2 - 792\,225x + 829\,521$.
- The number

$$\pi = 3.141\,592\,653 \quad 589\ldots$$

is transcendental.

Uniform rational approximation to a real number

Let $\xi \in \mathbf{R} \setminus \mathbf{Q}$.

- Dirichlet's box principle : for any real number $X \geq 1$, there exists $(x_0, x_1) \in \mathbf{Z}^2$ satisfying

$$0 < x_0 \leq X \quad \text{and} \quad |x_0\xi - x_1| \leq \varphi(X)$$

  where $\varphi(X) = X^{-1}$.
- there is no $\xi \in \mathbf{R}$ for which the exponent -1 can be lowered.
  Gel'fond's transcendence criterion in 1948.
  Refinements by H. Davenport and W.M. Schmidt in 1970.

Asymptotic rational approximation to a real number

- Liouville 1844 : there exists $\xi \in \mathbf{R}$ such that for any $m > 0$ the system

$$0 < x_0 \leq X, \quad |x_0\xi - x_1| \leq \varphi(X)$$

  has infinitely many solutions with $\varphi(X) = X^{-m}$.
- $$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8 \ldots]$$
- Simultaneous approximation, Diophantine approximation of algebraically dependent quantities.

Simultaneous approximation of ξ and ξ^2

Let $\xi \in \mathbf{R} \setminus \mathbf{Q}$.

- Dirichlet's box principle : for any real number $X \geq 1$, there exists $(x_0, x_1, x_2) \in \mathbf{Z}^3$ satisfying

$$(*) \quad 0 < x_0 \leq X, \quad |x_0\xi - x_1| \leq \varphi(X), \quad |x_0\xi^2 - x_2| \leq \varphi(X)$$

where $\varphi(X) = 1/[\sqrt{X}]$.

- If ξ is algebraic of degree 2, the same is true with $\varphi(X) = c/X$ and $c = c(\xi) > 0$.
- Metrical result : For $\lambda > 1/2$, the set E_λ of ξ which are not quadratic over $\mathbf{Q}$ and for which $(*)$ have a solution for any sufficiently large value of X with $\varphi(X) = X^{-\lambda}$ has Lebesgue measure zero.

Diophantine equations
Diophantine approximation
Diophantine geometry
Irrationality and transcendence
References

Simultaneous approximation of a number and its square

- Consequence of Schmidt's subspace Theorem : For $\lambda > 1/2$, the set E_λ contains no algebraic number.
- H. Davenport and W.M. Schmidt (1969) The set E_λ is empty for $\lambda > \Phi = (-1 + \sqrt{5})/2 = 0.618\ldots$.
- D. Roy (2003) : Examples of transcendental numbers ξ for which the inequalities $(*)$ have a solution for all sufficiently large values of X with $\varphi(X) = cX^{-\Phi}$

Fibonacci word

- Start with $f_1 = b$ and $f_2 = a$ and define (concatenation) : $f_n = f_{n-1}f_{n-2}$.
- Hence $f_3 = ab$ $\quad f_4 = aba$ $\quad f_5 = abaab$
  $f_6 = abaababa$ $\quad f_7 = abaababaabaab$
  $f_8 = abaababaabaababaababa$ ...
- The Fibonacci word

$$w = abaababaabaababaababaabaababaabaab\dots$$

is the fixed point of the morphism $b \mapsto a$, $a \mapsto ab$.

Result of D. Roy (2003)

Let A and B be two distinct positive integers. Let $\xi \in (0,1)$ be the real number whose continued fraction expansion is obtained from the Fibonacci word w by replacing the letters a and b by A and B :

$$[0; A, B, A, A, B, A, B, A, A, B, A, A, B, A, B, A, A, \dots]$$

Then there exists $c > 0$ such that the inequalities

$$0 < x_0 \le X, \quad |x_0\xi - x_1| \le \varphi(X), \quad |x_0\xi^2 - x_2| \le \varphi(X),$$

have a solution for any large value of X with $\varphi(X) = cX^{-\Phi}$ (as above $\Phi = (-1+\sqrt{5})/2 = 0.618\dots$).

Height

- Absolute logarithmic height : for a rational number a/b with $\gcd(a,b)=1$ and $b>0$,

$$h(a/b) = \log \max\{|a|\,,\,b\}.$$

- Lehmer's problem – lower bound for the height of a nontorsion point.
  Generalization to elliptic curves, abelian varieties, commutative algebraic groups.
- Small points : Zariski closure of the set of points of sufficiently small height on a variety, Bogomolov's conjecture.

Diophantine geometry

- Mazur's Conjecture (1992) : density of rational points on algebraic varieties.
- J-L. Colliot-Thélène, A.N. Skorobogatov and P. Swinnerton-Dyer (1997) Counterexample in the general case.
- The special case of abelian varieties reduces to a conjecture from transcendental number theory on which partial results are available.

Irrationality and transcendence

B. Adamczewski, Y. Bugeaud, F. Luca (2004) : *The g-ary expansion*

$$x = \sum_{k\geq 1} \frac{a_k}{g^k}$$

where $a_k \in \{0, 1, \ldots, g-1\}$ ($k \geq 1$) of an algebraic irrational number $x \in (0,1)$ cannot be generated by a finite automaton.

Complexity of the expansion of a real number

Let again $x = \sum_{k\geq 1} a_k g^{-k}$ denote the g-ary expansion of $x \in (0,1)$.

- Complexity function : for each integer $n \geq 1$, $p(n)$ is the number of words of length n which occur in the sequence $(a_1, a_2, \ldots)$.
- A periodic sequence has a bounded complexity.
- The complexity function p of an unbounded sequence satisfies $p(1) > 1$ and $p(n+1) > p(n)$ for all $n \geq 1$, hence $p(n) \geq n+1$ for all $n \geq 1$.
- A Sturmian sequence is a sequence with minimal complexity function : $p(n) = n+1$ for all $n \geq 1$.
- Example : the sequence of letters of the Fibonacci word is Sturmian.

Complexity of the expansion of an algebraic number

- B. Adamczewski, Y. Bugeaud, F. Luca (2004) : *The complexity function p of a real irrational algebraic number x satisfies*

$$\liminf_{n\to\infty} \frac{p(n)}{n} = +\infty.$$

- Example : A number whose sequence of digits is Sturmian is transcendental (S. Ferenczi, C. Mauduit, 1997).
-

Schmidt's subspace Theorem

- W.M. Schmidt (1970) : *For $m \geq 2$ let $L_1, \ldots, L_m$ be independent linear forms in m variables with algebraic coefficients. Let $\epsilon > 0$. Then the set*

$$\{\mathbf{x} = (x_1, \ldots, x_m) \in \mathbf{Z}^m \; ; \; |L_1(\mathbf{x}) \cdots L_m(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}\}$$

is contained in the union of finitely many proper subspaces of $\mathbf{Q}^m$.

- Example : $m = 2$, $L_1(x_1, x_2) = x_1$, $L_2(x_1, x_2) = \alpha x_1 - x_2$.
Roth's Theorem : *for any real algebraic irrational number α, for any $\epsilon > 0$, the set of $p/q \in \mathbf{Q}$ with $|\alpha - p/q| < q^{-2-\epsilon}$ is finite.*

SASTRA Kumbakonam December 21, 2005

http ://www.math.jussieu.fr/∼miw/