"Hilbert's problems today"

(April 6, 2001)

Open Diophantine Problems

by

Michel WALDSCHMIDT

Content

§1. Diophantine Equations
§2. Diophantine Approximation
§3. Transcendence
§4. Heights

http://www.math.jussieu.fr/∼miw/articles/ps/odp.ps

1. Diophantine Equations

Hilbert's tenth problem:

> *Given a Diophantine equation with any number of unknown quantities and with integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

`Open problem:`

To answer Hilbert's tenth problem for the special case of plane curve, which means to give an algorithm to decide whether a given Diophantine equation

$$f(x, y) = 0$$

has a solution (in $\mathbb{Z}$, and the same problem for $\mathbb{Q}$).

Problem. *Let $f \in \mathbb{Z}[X, Y]$ be a polynomial such that the equation $f(x, y) = 0$ has only finitely many solutions $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Give an upper bound for* $\max\{|x|, |y|\}$ *when (x, y) is such a solution, in terms of the degree of f and of the maximal absolute value of the coefficients of f.*

Lettre adressée à l'Éditeur par Monsieur E. Catalan, Répétiteur à l'école polytechnique de Paris», published in Crelle Journal (1844):

«*Je vous prie, Monsieur, de bien vouloir énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à le démontrer complètement: d'autres seront peut-être plus heureux:*

Deux nombres entiers consécutifs, autres que 8 *et* 9*, ne peuvent être des puissances exactes; autrement dit: l'équation* $x^m - y^n = 1$*, dans laquelle les inconnues sont entières et positives, n'admet qu'une seule solution.*»

Perfect powers: 1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, 169, ...

Conjecture (Catalan). *The equation*

$$x^p - y^q = 1,$$

where the unknowns x, y, p and q are integers all ≥ 2, has only one solution $(x, y, p, q) = (3, 2, 2, 3)$.

R. Tijdeman (1976): only finitely many solutions.

Conjecture (Pillai). *Let k be a positive integer. The equation*

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

where the unknowns x, y, p and q are integers all ≥ 2, has only finitely many solutions (x, y, p, q).

The Diophantine equation

$$x^p + y^q = z^r$$

has 10 known solutions (x, y, z, p, q, r) in positive integers for which

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

and such that x, y, z are relatively prime:

$$1 + 2^3 = 3^2 \qquad 2^5 + 7^2 = 3^4 \qquad 7^3 + 13^2 = 2^9$$

$$2^7 + 17^3 = 71^2 \qquad 3^5 + 11^4 = 122^2$$

$$17^7 + 76271^3 = 21063928^2$$

$$1414^3 + 2213459^2 = 65^7$$

$$9262^3 + 15312283^2 = 113^7$$

$$43^8 + 96222^3 = 30042907^2$$

$$33^8 + 1549034^2 = 15613^3.$$

R. Tijdeman and D. Zagier Conjecture : *there is no solution with the further restriction that each of p, q and r is ≥ 3.*

$$\boxed{m^2 + m_1^2 + m_2^2 = 3mm_1m_2}$$

- $(1,1,1)$
  - $(2,1,1)$
    - $(5,1,2)$
      - $(29,5,2)$
        - $(433,29,5)$
          - $\vdots$
          - $\vdots$
        - $(169,29,2)$
          - $\vdots$
          - $\vdots$
      - $(13,5,1)$
        - $(194,13,5)$
          - $\vdots$
          - $\vdots$
        - $(34,13,1)$
          - $\vdots$

Markoff Spectrum $\quad x^2 + y^2 + z^2 = 3xyz$

Sequence:

$$1,\ 2,\ 5,\ 13,\ 29,\ 34,\ 89,\ 169,\ 194,$$
$$233,\ 433,\ 610,\ 985,\ 1325,\ 1597,\ldots$$

Conjecture. *Fix a positive integer m for which the equation*

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

has a solution in positive integers (m_1, m_2) with

$$0 < m_1 \le m_2 \le m.$$

Then such a pair (m_1, m_2) is unique.

True for $m \le 10^{105}$.

Connection with Diophantine Approximation:

$$\mu_m = \sqrt{9m^2 - 4}/m :$$

Sequence:

$$\sqrt{5}, \quad \sqrt{8}, \quad \sqrt{221}/5, \quad \sqrt{1517}/13, \ldots$$

$$\limsup_{q\to\infty} \bigl| q(q\alpha_m - p) \bigr| = \frac{m}{\sqrt{9m^2 - 4}}.$$

2. Diophantine Approximation

$\boxed{abc \text{ Conjecture}}$

(D.W. Masser and J. Œsterlé, 1987).

For a positive integer n, denote by

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

the *radical* or *squarefree part* of n.

Conjecture (abc Conjecture). *For each $\epsilon > 0$ there exists a positive number $\kappa(\epsilon)$ which has the following property: if a, b and c are three positive rational integers which are relatively prime and satisfy $a + b = c$, then*

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

Triples (a, b, c) with $0 < a < b < c$, $a + b = c$ and $\gcd(a, b) = 1$.

$- \circ -$

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

(?) Finitely many (a, b, c) with $\lambda(a, b, c) > 1 + \epsilon$.

Largest known value for λ (É. Reyssat):

$$2 + 3^{10} \cdot 109 = 23^5, \qquad \lambda = 1.629912\ldots$$

140 known values of $\lambda(a, b, c)$ which are ≥ 1.4.

$- \circ -$

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

(?) Finitely many (a, b, c) with $\varrho(a, b, c) > 3 + \epsilon$.

Largest known value for ϱ (A. Nitaj):

$$13 \cdot 19^6 + 2^{30} \cdot 5 = 3^{13} \cdot 11^2 \cdot 31, \qquad \varrho = 4.41901\ldots$$

46 known triples (a, b, c) with $0 < a < b < c$ and $\gcd(a, b) = 1$ satisfying $\varrho(a, b, c) > 4$.

Conjecture (Erdős-Woods). *There exists a positive integer k such that, for m and n positive integers, the conditions*

$$R(m+i) = R(n+i) \quad (i = 0, \ldots, k-1)$$

imply $m = n$.

Remark: $k \geq 3$:

$$R(75) = 15 = R(1215), \quad R(76) = 2 \cdot 19 = R(1216).$$

Also $m = 2^h - 2$, $n = 2^h m$, $n + 1 = (m+1)^2$

$$R(m) = R(n) \quad \text{and} \quad R(m+1) = R(n+1)$$

Arithmetic progressions (T.N. Shorey):

(?) *Does there exist a positive integer k such that, for any m, n, d and d' positive integers satisfying* $\gcd(m,d) = \gcd(n,d') = 1$, *the conditions*

$$R(m+id) = R(n+id') \quad (i = 0, \ldots, k-1)$$

imply $m = n$ and $d = d'$?

Remark: $k \geq 4$:

$$R(2) = R(4) = R(8),$$

$$R(2+79) = R(4+23) = R(9),$$

$$R(2 + 2 \cdot 79) = R(4 + 2 \cdot 23) = R(10).$$

Theorem (Thue-Siegel-Roth). *For any $\epsilon > 0$ and any irrational algebraic number α, there is a positive constant $C(\alpha, \epsilon) > 0$ such that, for any rational number p/q,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{C(\epsilon)}{q^{2+\epsilon}}.$$

Consequence of abc (E. Bombieri, M. Langevin):

$$\left|\alpha - \frac{p}{q}\right| > \frac{C(\epsilon)}{R(pq)q^{\epsilon}}.$$

Main Open Problem: Effectivity

(?) *Does there exist an algebraic number of degree ≥ 3 with bounded partial quotients?*

(?) *Does there exist one with unbounded partial quotients?*

Let $\psi(q)$ be a continuous positive real valued function. Assume that the function $q\psi(q)$ is nonincreasing.

Conjecture. *Let θ be real algebraic number of degree at least 3. Then inequality*

$$\left|\theta - \frac{p}{q}\right| > \frac{\psi(q)}{q}.$$

has infinitely many solutions in integers p and q with $q > 0$ if and only if the integral

$$\int_1^\infty \psi(x)dx$$

diverges.

Schmidt's Subspace Theorem
Consequence: finiteness of solutions of the equation

$$x_1 + \cdots + x_n = 1$$

where the unknowns are integers (or S-integers) in a number field and no proper subsum vanishes.

Open problem: effective version for $n \geq 3$?

Waring's problem (1770):

> *"Every integer is a cube or the sum of two, three, ... nine cubes; every integer is also the square of a square, or the sum of up to nineteen such; and so forth. Similar laws may be affirmed for the correspondingly defined numbers of quantities of any like degree."*

$$n = x_1^k + \cdots + x_{g(k)}^k.$$

$$I(k) = 2^k + [(3/2)^k] - 2.$$

Easy to check $g(k) \geq I(k)$:

$$3^k = 2^k q + r \quad \text{with} \quad 0 < r < 2^k, \quad q = [(3/2)^k]$$

$$N = 2^k q - 1 = (q-1)2^k + (2^k - 1)1^k$$

$$I(k) = (q-1) + (2^k - 1)$$

Known: $g(k) = I(k)$ for $2 \leq k \leq 471\,600\,000$.

(?) $$\left\| \left(\frac{3}{2}\right)^k \right\| \geq 2 \cdot \left(\frac{3}{4}\right)^k$$

For $k \geq 2$ let $g(k)$ denote the smallest positive integer g such that any integer is the sum of g elements of the form x^k with $x \geq 0$.

$k =$ 2	3	4	5	6	7
$g(k) =$ 4	9	19	37	73	143
J.L. Lagrange	A. Wieferich	R. Balasubramanian J-M. Deshouillers F. Dress	J. Chen	S.S. Pillai	L.E. Dickson
1770	1909	1986	1964	1940	1936

3. Transcendence

Irrationality Problems:

Euler's constant

$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}-\log n\right)$$
$$= 0.5772157\ldots,$$

Catalan's constant

$$G = \sum_{n\geq 0}\frac{(-1)^n}{(2n+1)^2}$$
$$= \frac{\pi}{4}\int_0^1 {}_2F_1\left(\begin{matrix}1/2\,,\;1/2\\1\end{matrix}\Big| t\right)\frac{dt}{\sqrt{4t}}$$
$$= 0.915965594\ldots,$$

$$\Gamma(1/5) = \int_0^\infty e^{-t}t^{-4/5}dt = 4.59084371\ldots$$

$$e+\pi = 5.8598744\ldots, \qquad e^\gamma = 1.781072\ldots$$

$$\sum_{n\geq 1}\frac{\sigma_k(n)}{n!} \quad (k=1,2) \quad \text{where} \quad \sigma_k(n)=\sum_{d|n}d^k$$

Conjecture (Schanuel). *Let $x_1, \ldots, x_n$ be $\mathbb{Q}$-linearly independent complex numbers. Then the transcendence degree over $\mathbb{Q}$ of the field*

$$\mathbb{Q}\bigl(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}\bigr)$$

is at least n.

Conjecture (Algebraic Independence of Logarithms of Algebraic Numbers). *Let $\lambda_1, \ldots, \lambda_n$ be $\mathbb{Q}$-linearly independent complex numbers. Assume that the numbers $e^{\lambda_1}, \ldots, e^{\lambda_n}$ are algebraic. Then the numbers $\lambda_1, \ldots, \lambda_n$ are algebraically independent.*

D. Roy: $\mathcal{L} = \bigl\{\log \alpha\ ;\ \alpha \in \overline{\mathbb{Q}}^{\times}\bigr\}$

(?) *For any algebraic subvariety V of $\mathbb{C}^n$ defined over the field $\overline{\mathbb{Q}}$ of algebraic numbers, the set $V \cap \mathcal{L}^n$ is the union of the sets $E \cap \mathcal{L}^n$, where E ranges over the set of vector subspaces of $\mathbb{C}^n$ which are contained in V.*

Conjecture (Gel'fond-Schneider). *Let β be an irrational algebraic number of degree d and α a nonzero algebraic number. Let $\log \alpha$ be a nonzero logarithm of α. Then the d numbers*

$$\log \alpha,\ \alpha^{\beta},\ \alpha^{\beta^2}, \ldots, \alpha^{\beta^{d-1}}$$

are algebraically independent.

Elimination Theory

Hilbert Nulstellensatz.

Conjecture (Blum, Cucker, Shub and Smale). *Given an absolute constant c and polynomials $P_1, \ldots, P_m$ with a total of N coefficients and no common complex zeros, there is no program to find, in at most N^c step, the coefficients of polynomials A_i satisfying Bézout's relation*

$$A_1 P_1 + \cdots + A_m P_m = 1.$$

Complexity in theoretical computer science and Diophantine approximation (W.D. Brownawell)

$$\left| x - \frac{p}{q} \right| > \psi(p/q).$$

Polyzeta (or *Multiple Zeta) Values*

L. Euler, K. Nielsen, D. Zagier, A.B. Goncharov, M. Kontsevich, M. Petitot, Minh Hoang Ngoc, P. Cartier,...

$$\zeta(\underline{s}) = \sum_{n_1 > \cdots > n_k \geq 1} n_1^{-s_1} \cdots n_k^{-s_k},$$

$\underline{s} = (s_1, \ldots, s_k) \in \mathbb{Z}^k$ with

$$s_1 \geq 2, \; s_2 \geq 1, \ldots, s_k \geq 1.$$

Let $\mathfrak{Z}_p$ denote the $\mathbb{Q}$-vector subspace spanned by the real numbers $\zeta(\underline{s})$ with $s_1 + \cdots + s_k = p$. Set $\mathfrak{Z}_0 = \mathbb{Q}$ and $\mathfrak{Z}_1 = \{0\}$. The $\mathbb{Q}$-subspace $\mathfrak{Z}$ spanned by all $\mathfrak{Z}_p$, $p \geq 0$, is a subalgebra of $\mathbb{R}$

Conjecture (A.B. Goncharov). *As a $\mathbb{Q}$-algebra, $\mathfrak{Z}$ is the direct sum of $\mathfrak{Z}_p$ for $p \geq 0$.*

Conjecture (D. Zagier). *For $p \geq 3$ the dimension d_p of the $\mathbb{Q}$-vector space $\mathfrak{Z}_p$ is given by*

$$d_p = d_{p-2} + d_{p-3}$$

with $d_0 = 1$, $d_1 = 0$, $d_2 = 1$.

Conjecture. *The numbers*

$$\pi,\ \zeta(3), \zeta(5), \ldots, \zeta(2n+1), \ldots$$

are algebraically independent.

Known:

- (Euler– Lindemann) $\zeta(2n)$ *is transcendental for* $n \geq 1$.
- (Apéry, 1978) $\zeta(3)$ *is irrational*.
- (T. Rivoal, CRAS 2000; K. Ball & T. Rivoal, to appear). *The* $\mathbb{Q}$*-vector space spanned by the* $n+1$ *numbers* $1, \zeta(3), \zeta(5), \ldots, \zeta(2n+1)$ *has dimension*

$$\geq \frac{1-\epsilon}{1+\log 2} \log n$$

for $n \geq n_0(\epsilon)$.

For instance infinitely many of these numbers $\zeta(2n+1)$ $(n \geq 1)$ are irrational.

$\boxed{\textit{Gamma Function}}$

Set

$$G(z) = \frac{1}{\sqrt{2\pi}}\Gamma(z).$$

For $N > 0$ and $x \in \mathbb{C}$ such that $Nx \not\equiv 0 \pmod{\mathbb{Z}}$,

$$\prod_{i=0}^{N-1} G\left(x + \frac{i}{N}\right) = N^{(1/2)-Nx} G(Nx).$$

Then

$$\overline{G} : (\mathbb{Q}/\mathbb{Z}) \setminus \{0\} \to \mathbb{C}^\times/\overline{\mathbb{Q}}^\times$$

is an odd *distribution* on $(\mathbb{Q}/\mathbb{Z}) \setminus \{0\}$:

$$\prod_{i=0}^{N-1} \overline{G}\left(x + \frac{i}{N}\right) = \overline{G}(Nx) \quad \text{for} \quad x \in (\mathbb{Q}/\mathbb{Z}) \setminus \{0\}$$

and

$$\overline{G}(-x) = \overline{G}(x)^{-1}.$$

Conjecture (Rohrlich). *$\overline{G}$ is the universal odd distribution with values in groups where multiplication by 2 is invertible.*

Conjecture. *Three at least of the four numbers*

$$\pi,\ \Gamma(1/5),\ \Gamma(2/5),\ e^{\pi\sqrt{5}}$$

are algebraically independent.

Algebraic Independence and Modular Forms

$$P(q) = 1 - 24\sum_{n=1}^{\infty} \frac{nq^n}{1-q^n},$$

$$Q(q) = 1 + 240\sum_{n=1}^{\infty} \frac{n^3q^n}{1-q^n},$$

$$R(q) = 1 - 504\sum_{n=1}^{\infty} \frac{n^5q^n}{1-q^n}.$$

Conjecture (Nesterenko). *Let $\tau \in \mathbb{C}$ have positive imaginary part. Assume that τ is not quadratic. Set $q = e^{2i\pi\tau}$. Then 4 at least of the 5 numbers*

$$\mathbb{Q}\bigl(\tau,\ q,\ P(q),\ Q(q),\ R(q)\bigr)$$

are algebraically independent.

Fibonacci Numbers

$$F_{n+2} = F_{n+1} + F_n, \qquad F_0 = 0, \quad F_1 = 1.$$

Special values

$$\sum_{n=1}^{\infty} \frac{1}{F_n F_{n+2}} = 1$$

$$\sum_{n=0}^{\infty} \frac{1}{F_{2^n}} = \frac{7-\sqrt{5}}{2}, \qquad \sum_{n=1}^{\infty} \frac{(-1)^n}{F_n F_{n+1}} = \frac{1-\sqrt{5}}{2},$$

$$\sum_{n=1}^{\infty} \frac{1}{F_{2n-1}+1} = \frac{\sqrt{5}}{2}.$$

Each of the numbers

$$\sum_{n=0}^{\infty} \frac{1}{F_n}, \quad \sum_{n=1}^{\infty} \frac{1}{F_n + F_{n+2}} \quad \text{and} \quad \sum_{n\geq 1} \frac{1}{F_1 F_2 \cdots F_n}$$

is irrational (transcendental ?). The numbers

$$\sum_{n=0}^{\infty} \frac{1}{F_{2n-1}}, \quad \sum_{n=0}^{\infty} \frac{1}{F_n^2}, \quad \sum_{n=0}^{\infty} \frac{(-1)^n}{F_n^2}, \quad \sum_{n=0}^{\infty} \frac{n}{F_{2n}},$$

$$\sum_{n=0}^{\infty} \frac{1}{F_{2^n-1} + F_{2^n+1}} \quad \text{and} \quad \sum_{n=0}^{\infty} \frac{1}{F_{2^n+1}}$$

are all transcendental

Series of Rational Fractions

$$\sum_{n=1}^{\infty} \frac{1}{n(n+1)} = 1$$

while

$$\sum_{n=0}^{\infty} \frac{1}{(2n+1)(2n+2)} = \log 2,$$

$$\sum_{n=0}^{\infty} \frac{1}{(n+1)(2n+1)(4n+1)} = \frac{\pi}{3}$$

$$\sum_{n=0}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \qquad \sum_{n=0}^{\infty} \frac{1}{n^2+1} = \frac{1}{2} + \frac{\pi}{2} \cdot \frac{e^{\pi} + e^{-\pi}}{e^{\pi} - e^{-\pi}},$$

$$\sum_{n=0}^{\infty} \frac{1}{(6n+1)(6n+2)(6n+3)(6n+4)(6n+5)(6n+6)} = \frac{1}{4320}(192 \log 2 - 81 \log 3 - 7\pi\sqrt{3})$$

are transcendental.

4. Heights

Mahler's measure of

$$\begin{aligned} f(X) &= a_0X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d \\ &= a_0 \prod_{i=1}^{d} (X - \alpha_i) \end{aligned}$$

is

$$\begin{aligned} \mathrm{M}(f) &= |a_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\} \\ &= \exp\left(\int_0^1 \log |f(e^{2i\pi t})| dt \right). \end{aligned}$$

Lehmer (1933): *Is-it true that for every positive ϵ there exists an algebraic integer α for which*

$$1 < \mathrm{M}(\alpha) < 1 + \epsilon?$$

Smallest known value > 1 for $\mathrm{M}(\alpha)$ is

$$\alpha_0 = 1.1762808\ldots,$$

root of

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

Logarithmic height

$$\mathsf{h}(\alpha) = \frac{1}{d} \log \mathsf{M}(\alpha).$$

Conjecture (Lehmer's Problem). *There exists a positive absolute constant c such that, for any nonzero algebraic number α of degree at most d which is not a root of unity,*

$$\mathsf{h}(\alpha) \geq \frac{c}{d}\cdot$$

Conjecture (Amoroso-David). *For each positive integer $n \geq 1$ there exists a positive number $c(n)$ having the following property. Let $\alpha_1, \ldots, \alpha_n$ be multiplicatively independent algebraic numbers. Define*

$$D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}].$$

Then

$$\prod_{i=1}^{n} \mathsf{h}(\alpha_i) \geq \frac{c(n)}{D}\cdot$$

Heights of Subvarieties

Bogomolov, height of small points, Philippon's alternative heights. Group varieties, height of translate of algebraic subgroups.

Conjecture (Amoroso-David). *For each integer $n \geq 1$ there exists a positive constant $c(n)$ such that, for any algebraic subvariety V of $\mathbb{G}_{\mathrm{m}}^n$ which is defined over $\mathbb{Q}$, which is $\mathbb{Q}$-irreducible, and which is not a union of translates of algebraic subgroups by torsion points,*

$$\hat{V} \geq c(n)\,\mathsf{deg}(V)^{(s-\dim V-1)/(s-\dim V)},$$

where s is the dimension of the smallest algebraic subgroup of $\mathbb{G}_{\mathrm{m}}^n$ containing V.

Mazur Density Problem

Topology of rational points. Connection with the rational version of Hilbert's tenth problem.

Let K be a number field with a given real embedding. Let V be a smooth variety over K. Denote by Z the closure, for the real topology, of $V(K)$ in $V(\mathbb{R})$.

Question (Mazur). *Assume that $K = \mathbb{Q}$ and that $V(\mathbb{Q})$ is Zariski dense; is Z a union of connected components of $V(\mathbb{R})$?*

Colliot-Thélène, Skorobogatov and Swinnerton-Dyer

(?) *Let A be a simple abelian variety over $\mathbb{Q}$. Assume the Mordell-Weil group $A(\mathbb{Q})$ has rank ≥ 1. Then $A(\mathbb{Q}) \cap A(\mathbb{R})^0$ is dense in the neutral component $A(\mathbb{R})^0$ of $A(\mathbb{R})$.*

Conjecture. *Let A be a simple abelian variety over $\mathbb{Q}$, $\exp_A : \mathbb{R}^g \to A(\mathbb{R})^0$ the exponential map of the Lie group $A(\mathbb{R})^0$ and $\Omega = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_g$ its kernel. Let $u = u_1\omega_1 + \cdots + u_g\omega_g \in \mathbb{R}^g$ satisfy $\exp_A(u) \in A(\mathbb{Q})$. Then $1, u_1, \ldots, u_g$ are linearly independent over $\mathbb{Q}$.*