22/06/2019

Abha. Saudi Arabia, King Khalid University,
Wams school on Introductory topics in Number Theory and Differential Geometry.
June 17 – 23, 2019

Diophantine Equations

Michel Waldschmidt

http://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/DiophantineEquationsAbha2019.pdf

Syllabus: http://www.rnta.eu/Abha2019/

- Classical Diophantine equations in two variables, their theory, relations with Diophantine Approximation and with Algebraic Number Theory
  - linear equation
  - Pell equation
  - Thue equation
  - elliptic, hyperelliptic, superelliptic equations
  - general equation, Siegel's finiteness theorem.
- Baker's method, effective results
- From effective to explicit: the Las-Vegas Principle
- Continued Fractions and Baker-Davenport Lemma
- Explicit solution of simultaneous Pell equations
- Explicit solutions of Thue equations.
- Elliptic curves, Mordell-Weil Theorem. Solving elliptic equations using elliptic logarithms.

First course: *Thursday, June 20, 2019; 8:30 – 9:15*

- The linear recurrent sequence $u_{n+2} = u_{n+1} + u_n$ with $u_0 = 1$ and $u_1 = (1 - \sqrt{5})/2$. Sensitivity to initial conditions.

Reference:
https://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/SensitivityInitialConditions.pdf

- Thue Diophantine equation $x^3 - 2y^3 = k$ and irrationality measure for $\sqrt[3]{2}$.
  Liouville's estimate for the rational Diophantine approximation of $\sqrt[3]{2}$:

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{cq^3}$$

with $c = 5$ for all p/q, and any $c > 3\sqrt[3]{4} = 4.7622\ldots$ for q sufficiently large.

Proof: write

$$1 \leq |p^3 - 2q^3| = |p - \sqrt[3]{2}q|(p^2 + \sqrt[3]{4}pq + \sqrt[3]{4}q^2).$$

We may assume $0 < p \leq q\sqrt[3]{2} + (1/cq^2)$. Then

$$0 < p^2 + \sqrt[3]{4}pq + \sqrt[3]{4}q^2 < 3\sqrt[3]{4}q^2 + \frac{3\sqrt[3]{2}}{cq} + \frac{1}{c^2q^4} < cq^2.$$

Explicit refinement by M. Bennett: *for any* $p/q \in \mathbf{Q}$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{1}{4\ q^{5/2}}.$$

Application: *for any* $(x, y) \in \mathbf{Z}^2$ *with* $x > 0$,

$$|x^3 - 2y^3| \geq \sqrt{x}.$$

Lemma 1. *Let* η *be a positive real number. The two following properties are equivalent:*
(i) *There exists a constant* $c_1 > 0$ *such that, for any* $p/q \in \mathbf{Q}$ *with* $q > 0$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{c_1}{q^\eta}.$$

(ii) *There exists a constant* $c_2 > 0$ *such that, for any* $(x, y) \in \mathbf{Z}^2$ *with* $x > 0$,

$$|x^3 - 2y^3| \geq c_2 x^{3-\eta}.$$

True for $\eta > 2$, false for $\eta < 2$, unknown for $\eta = 2$. Effective for $\eta > 5/2$ only.

Liouville estimate for $|\alpha - (p/q)|$. Improvement by Thue. Application to Thue equation $F(x, y) = k$ where $F \in \mathbf{Z}[X, Y]$ is a homogeneous form with at least 3 distinct linear factors in $\mathbf{C}$.

Statement of the Thue – Siegel – Roth Theorem. Not effective.

References:

§ 2.2.5 of
https://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/IntroductionDiophantineMethods.pdf
§ 3 of
https://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/IntroductionDiophantineApproximationBerhampur2018.pdf

22/06/2019

Second course: *Thursday, June 20, 2019; 12:00 – 12:45*

• Basic facts from algebraic number theory.

Number field, degree, examples: $\mathbf{Q}(\sqrt{d})$, $\mathbf{Q}(\alpha)$, $\mathbf{Q}(e^{2i\pi/n})$.

The field of algebraic numbers, the ring of algebraic integers, the ring of integers of a number field, the group of units of a number field. Dirichlet's Unit Theorem: *the group of units of a number field is finitely generated.*

Quadratic fields: ring of integers, roots of unity, units, connection with Pell's equation.

• Statement of the assertions (T) = Thue, (M) = Mordell, (E) = Elliptic, (HE) = Hyperelliptic, (SE) = Superelliptic and (S) = Siegel Unit Theorem

Their equivalence:

$$\begin{array}{ccccc} (\mathrm{SE}) & \Longrightarrow & (\mathrm{M}) & \Longleftarrow & (\mathrm{E}) \\ \Uparrow & & \Downarrow & & \Uparrow \\ (\mathrm{T}) & \Longleftarrow & (\mathrm{S}) & \Longrightarrow & (\mathrm{HE}) \end{array}$$

Trivial implications (HE)⇒(E), (E)⇒(M) and (SE)⇒(M).
Proofs of the easy implications (M)⇒(S) and (T)⇒(S).
Proof of the not too difficult implication (S)⇒(T).
The two implications which are not so easy to prove are

$$(\mathrm{T}) \Longrightarrow (\mathrm{SE}) \quad \text{and} \quad (\mathrm{S}) \Longrightarrow (\mathrm{HE}).$$

`References:`

M.W. – Diophantine equations and transcendental methods (written by Noriko Hirata). in: Transcendental numbers and related topics, RIMS Kôkyûroku, Kyoto, **599** (1986), N°8, 82–94.

`https://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/DiophEqnNoriko1986.pdf`

C. Levesque and M.W. – Some remarks on diophantine equations and diophantine approximation, 26 p. Vietnam Journal of Mathematics, 39:3 (2011) 343-368.
arXiv:1312.7200 [math.NT].

`https://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/CLMW-DEDA2011.pdf`

M.W. – Thue Diophantine equations - a survey. Proceedings of the International Conference on Class Groups of Number Fields and Related Topics (ICCGNFRT-2017), HRI Allahabad, September 2017, 14 p. Springer Verlag.

`https://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/ProcHRI2017ThueEquations.pdf`

Third course: *Saturday, June 22, 2019; 8:30 – 9:15*

• Statement of Siegel's finiteness Theorem for integral points on curves of genus ≥ 1. Effective (by Baker's method using lower bounds for linear forms in logarithms) only for genus 1. Statement of Falting's Theorem (Mordell's Conjecture) for rational points on curves of genus ≥ 2. Upper bounds for the number of solutions.

• Lower bounds for linear forms in logarithms. Liouville–type bound: e^{-cB}. Gel'fond – Baker method: B^{-c}.

• Sketch of proof of Siegel Theorem (S) on the unit equation using a lower bound for linear forms in logarithms.

The next lemma (see for instance the book by Y. Bugeaud, Th. 4.3) follows from the equivalence of two norms on a finite dimensional vector space.

Lemma 2. *Let K be a number field, $\epsilon_1, \ldots, \epsilon_r$ a basis of the unit group of K modulo torsion. There exists a constant $c > 0$ such that, if u is a unit of K with*

$$u = \zeta \epsilon_1^{t_1} \cdots \epsilon_r^{t_r}$$

where ζ is a root of unity and $b_1, \ldots, b_r$ are in $\mathbf{Z}$, then there exists a conjugate u' of u in $\mathbf{C}$ such that

$$\max\{|t_1|, \ldots, |t_r|\} \leq c \log |u'|.$$

Sketch of proof of Siegel Theorem (S). Assume $a_1 u_1 + a_2 u_2 = 1$. Write

$$u_1 = \zeta_1 \epsilon_1^{s_1} \cdots \epsilon_r^{s_r}, \quad u_2 = \zeta_2 \epsilon_1^{t_1} \cdots \epsilon_r^{t_r}.$$

We may assume $\max\{|t_1|, \ldots, |t_r|\} \geq \max\{|s_1|, \ldots, |s_r|\}$. Let

$$B = \max\{|t_1|, \ldots, |t_r|\}.$$

By Lemma 2, there is an embedding of K into $\mathbf{C}$ for which $\log |u_2| \geq c_1 B$. Write

$$\frac{-a_1 u_1}{a_2 u_2} - 1 = \frac{-1}{a_2 u_2}.$$

The modulus of the right hand side is $\leq \mathrm{e}^{-c_2 B}$ with some constant $c_2 > 0$. Setting $b_i = s_i - t_i$, $\alpha_i = \epsilon_i$ $(i = 1, \ldots, n)$, $\alpha_0 = -a_1 \zeta_1 / a_2 \zeta_2$, $b_0 = 1$, we write the left hand side as

$$\alpha_0^{b_0} \alpha_1^{b_1} \cdots \alpha_r^{b_r} - 1.$$

By the results from the theory of linear forms in logarithms, the modulus of this number is bounded from below by B^{-c_3} with another constant $c_3 > 0$. Hence B is bounded and the set of u_1, u_2 is finite.

□

References:

Y. Bugeaud. – Linear Forms in Logarithms and Applications. IRMA Lectures in Mathematics and Theoretical Physics Vol. **28** 2018.

M.W. — Diophantine approximation and Diophantine equations.
https://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/HRI2011.pdf

Fourth course: *Saturday, June 22, 2019; 9:20 – 10:05*

• Elliptic curves.

Weierstrass model of the elliptic curve E with a parametrisation by Weierstrass $\wp$ function.

Mordell–Weil Theorem: the group of rational points of an elliptic curve over a number field is finitely generated.

Linear forms in elliptic logarithms: lower bound for $|v| = |b_0u_0+\cdots+b_nu_n|$ when $x = \wp(v) \in \mathbf{Z}$. Trivial $|x| \geq 1$ yields e^{-cB}, where $B = \max\{|b_i|\}$. Transcendence methods yields B^{-c}.

Sketch of proof of Siegel's Theorem (E) on the finiteness of integer points on an elliptic curve using lower bounds for linear forms in elliptic logarithms.

Sketch of proof of Siegel Theorem (E). Let $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ satisfy

$$y^2 = 4x^3 - g_2x - g_3.$$

Write $x = \wp(v)$. Assume $|x|$ is sufficiently large. Then there exists a period ω of $\wp$ such that $0 < |v - \omega| < c_1/v^2$.

Let $u_1, \ldots, u_r$ be a basis of the Mordell–Weil group $E(K)$ modulo torsion. Write

$$v = w + b_1u_1 + \cdots + b_ru_r$$

where w is an elliptic logarithm of a torsion point (a small multiple of w is a period) and $b_1, \ldots, b_r$ are in $\mathbf{Z}$. From the theory of Néron–Tate height it follows that the number $B = \max\{|b_1|, \ldots, |b_r|\}$ satisfies $B \leq c_2 \log |v|$. On the other hand, using a lower bound for linear forms in elliptic logarithms, we have

$$|b_1u_1 + \cdots + b_ru_r + w - \omega| \geq B^{-c_3}.$$

Combining the upper and the lower bound yields an upper bound for B, hence $|v|$ belongs to a finite set, and finally $|x|$ is bounded. □

• Elliptic binomial Diophantine equations.

Reference:
http://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/EllipticBinomialDiophantineEquations.pdf

R.J. Stroeker and N. Tzanakis. — *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arithmetica **67** (1994), 177 – 196.

R.J. Stroeker and N. Tzanakis. — *On the Elliptic Logarithm Method for Elliptic Diophantine Equations: Reflections and an Improvement.* Experimental Mathematics, **8** (1999), No. 2, 135 – 149.

R.J. Stroeker and N. Tzanakis. — *Elliptic binomial Diophantine equations*, Mathematics of Computation, **68**, 227 (1999), 1257 – 1281.

Michel WALDSCHMIDT
Sorbonne Université
Faculté Sciences et Ingenierie
CNRS, Institut Mathématique de Jussieu Paris Rive Gauche, IMJ-PRG
F – 75005 Paris, France
michel.waldschmidt@imj-prg.fr
http://www.imj-prg.fr/~michel.waldschmidt