December 16, 2014

Winter School on modular functions in one and several variables,

December 2014, Goa University.

Algebraic independence of periods of elliptic curves

Michel Waldschmidt

References

[1] S. Bruiltet – "D'une mesure d'approximation simultanée à une mesure d'irrationalité: le cas de $\Gamma(1/4)$ et $\Gamma(1/3)$", *Acta Arith.* **104** (2002), no. 3, p. 243–281.

[2] G. V. Chudnovsky – "Algebraic independence of constants connected with the exponential and the elliptic functions", *Dokl. Akad. Nauk Ukrain. SSR Ser. A* **8** (1976), p. 698–701, 767.

[3] — , "Indépendance algébrique des valeurs d'une fonction elliptique en des points algébriques. Formulation des résultats", *C. R. Acad. Sci. Paris Sér. A-B* **288** (1979), no. 8, p. A439–A440.

[4] — , "Algebraic independence of the values of elliptic function at algebraic points", *Invent. Math.* **61** (1980), no. 3, p. 267–290, Elliptic analogue of the Lindemann-Weierstrass theorem.

[5] — , "Algebraic independence of values of exponential and elliptic functions", in *Proceedings of the International Congress of Mathematicians (Helsinki, 1978)* (Helsinki), Acad. Sci. Fennica, 1980, p. 339–350.

[6] — , "Indépendance algébrique dans la méthode de Gelfond-Schneider", *C. R. Acad. Sci., Paris, Sér. A* **291** (1980), p. 365–368, *see* Zbl 0456.10016.

[7] — , *Contributions to the theory of transcendental numbers*, Mathematical Surveys and Monographs, vol. 19, American Mathematical Society, Providence, RI, 1984.

[8] D. W. Masser – *Elliptic functions and transcendence*, Springer-Verlag, Berlin, 1975, Lecture Notes in Mathematics, Vol. 437.

[9] D. W. Masser & G. Wüstholz – "Fields of large transcendence degree generated by values of elliptic functions", *Invent. Math.* **72** (1983), no. 3, p. 407–464.

[10] — , "Algebraic independence of values of elliptic functions", *Math. Ann.* **276** (1986), no. 1, p. 1–17.

[11] J. V. Nesterenko – "Modular functions and transcendence problems", *C. R. Acad. Sci. Paris Sér. I Math.* **322** (1996), no. 10, p. 909–914.

[12] — , "Modular functions and transcendence questions", *Mat. Sb.* **187** (1996), no. 9, p. 65–96.

[13] — , "On the measure of algebraic independence of values of Ramanujan functions", *Tr. Mat. Inst. Steklova* **218** (1997), no. Anal. Teor. Chisel i Prilozh., p. 299–334.

[14] — , "Algebraic independence of π and e^{π}", in *Number theory and its applications (Ankara, 1996)*, Lecture Notes in Pure and Appl. Math., vol. 204, Dekker, New York, 1999, p. 121–149.

[15] — , "On the algebraic independence of values of Ramanujan functions", *Vestnik Moskov. Univ. Ser. I Mat. Mekh.* **2** (2001), p. 6–10, 70.

[16] Y. V. Nesterenko & P. Philippon – *Introduction to algebraic independence theory*, Lecture Notes in Mathematics, vol. 1752, Springer-Verlag, Berlin, 2001, With contributions from F. Amoroso, D. Bertrand, W. D. Brownawell, G. Diaz, M. Laurent, Yuri V. Nesterenko, K. Nishioka, Patrice Philippon, G. Rémond, D. Roy and M. Waldschmidt, Edited by Nesterenko and Philippon.

[17] G. Philibert – "Une mesure d'indépendance algébrique", *Ann. Inst. Fourier (Grenoble)* **38** (1988), no. 3, p. 85–103.

[18] R. Tubbs – "Algebraic groups and small transcendence degree. I", *J. Number Theory* **25** (1987), no. 3, p. 279–307.

[19] — , "Algebraic groups and small transcendence degree. II", *J. Number Theory* **35** (1990), no. 2, p. 109–127.

[20] M. Waldschmidt – "Propriétés arithmétiques des valeurs de fonctions méromorphes algébriquement indépendantes", *Acta Arith.* **23** (1973), p. 19–88.

[21] — , "Les travaux de G. V. Chudnovsky sur les nombres transcendants", in *Séminaire Bourbaki, Vol. 1975/76, 28e année, Exp. No. 488*, Springer, Berlin, 1977, p. 274–292. Lecture Notes in Math., Vol. 567.

[22] — , "Nombres transcendants et fonctions sigma de Weierstrass", *C. R. Math. Rep. Acad. Sci. Canada* **1** (1978/79), no. 2, p. 111–114.

[23] — , *Nombres transcendants et groupes algébriques*, Astérisque, vol. 69, Société Mathématique de France, Paris, 1979, With appendices by Daniel Bertrand and Jean-Pierre Serre.

[24] — , "Algebraic independence of values of exponential and elliptic functions", *J. Indian Math. Soc. (N.S.)* **48** (1984), no. 1-4, p. 215–228 (1986).

[25] — , "Sur la nature arithmétique des valeurs de fonctions modulaires", *Astérisque* **245** (1997), p. Exp. No. 824, 3, 105–140, Séminaire Bourbaki, Vol. 1996/97.

[26] — , "Transcendance et indépendance algébrique de valeurs de fonctions modulaires", in *Number theory (Ottawa, ON, 1996)*, CRM Proc. Lecture Notes, vol. 19, Amer. Math. Soc., Providence, RI, 1999, p. 353–375.

[27] — , "Algebraic independence of transcendental numbers: a survey", in *Number theory*, Trends Math., Birkhäuser and Hindustan Book Agency, Basel and New-Delhi, 2000, p. 497–527.

[28] — , "Elliptic Functions and Transcendence" in *Developments in Mathematics* **17**, Surveys in Number Theory, §7, Springer Verlag (2008), 143-188.

Some of these paper are available on the internet. See in particular

http://www.imj-prg.fr/~michel.waldschmidt/texts.html

Michel WALDSCHMIDT
UPMC Univ Paris 06, UMR 7586-IMJ
F–75005 Paris
FRANCE
e-mail: michel.waldschmidt@imj-prg.fr
URL: http://www.imj-prg.fr/~michel.waldschmidt

Keywords: elliptic curves, addition, doubling, explicit formulas, register allocation, scalar multiplication, multi-scalar multiplication, side-channel countermeasures, unied addition formulas, complete addition formulas, ecient implementation, performance evaluation.Â Several subsequent papers analyzed the performance of other forms of elliptic curves proposed in the mathematical literature. See, e.g., [18] for the speed of several dialects of the Weierstrass form, [34] for the speed of Jacobi intersections, [28] for the speed of Hessians, and [9] for the speed of Jacobi quartics; see also [38] and [23], which introduced the Montgomery and Doche/Icart/Kohel forms and analyzed their speed. An elliptic curve over k is a nonsingular projective algebraic curve E of genus 1 over k with a chosen base point O âˆˆ E. Remark. There is a somewhat subtle point here concerning what is meant by a point of a curve over a non-algebraically-closed eld.Â Any elliptic curve E over k is isomorphic to the curve in P2k dened by some generalised Weierstrass equation, with the base point O of E being mapped to. (0 : 1 : 0). Conversely any non-singular generalised Weierstrass equation denes an. elliptic curve, with this choice of basepoint. Proposition 1.6.Â called periods of E and let Î› = ZÏ‰1 + ZÏ‰2. It can be shown that Ï‰1, Ï‰2 are linearly independent over R and hence Î› is a lattice. Fix a point P0 âˆˆ E(C) and dene the map. Ïˆ : E(C) âˆ’â†’ C/Î›. ag.algebraic-geometry elliptic-curves complex-multiplication. share|cite|improve this question|.Â For further accounts of these types of results and their history, I highly recommend Waldschmidt's articles "Transcendence of periods: the state of the art," Pure Appl. Math. Q. 2 (2006), no. 2, part 2, 435-463, and "Elliptic functions and transcendence," Surveys in number theory, Dev.