PROFESSOR Dimitrios Poulakis,
Department of Mathematics, Aristotle University of Thessaloniki,
54124 Thessaloniki, Greece
http://users.auth.gr/~poulakis/
e. mail: poulakis@math.auth.gr
Tel : +30-2310-997908

STUDIES

- B.Sc. in Mathematics, from the Department of Mathematics at University of Ioannina, Greece. Awarded Scholarship from the Greek State Scholarship Foundation.
- DEA of Pure Mathematics, Department of Mathematics at University of Paris XI (Centre d'Orsay).
- Ph.D. of Pure Mathematics, Department of Mathematics at University of Paris XI (Centre d'Orsay).

RESEARCH INTERESTS

Number Theory (Diophantine Equations, Arithmetic Algebraic Geometry, Computational Number Theory) and Public-Key Cryptography.

RESEARCH

1. Points rationnels sur **Q** de la jacobienne de la courbe modulaire $X_0(81)$, C. R. Acad. Sc. Paris, t. 298, Série I, no 18 (1984), 433-436.

2. Points rationnels de la courbe modulaire $X_0(125)$ et de sa jacobienne, J. Number Theory, 25 (1987), 112-131.

3. Evaluation d'une somme cubique de caractères, J. Number Theory, 27 (1987), 41-45.

4. On the homomorphisms of a family of finite rings, Bull. Greek Math. Soc. 30 (1989), 43- 48.

5. Solutions entières de l'équation $Y^m = f(X)$, Sém. Th. des Nombres

Bordeaux 3 (1991), 187-199.

6. Points entiers sur les courbes hyperelliptiques, Acta Arithmetica, 62 (1992), 25-43.

7. Solutions entières de l'équation $f(X,Y)^a = p(X)g(X,Y)$, C. R. Acad. Sc. Paris 315 (1992), 963-968.

8. Courbes elliptiques et 2-extensions Abéliennes, Bull. Greek Math. Soc. 34 (1992), 155-160.

9. Points entiers sur les courbes de genre 0, Colloquim Mathematicum, LXVI (1993), 1-7.

10. Points entiers et modèles des courbes algébriques, Monatshefte für Mathematik 118 (1994), 111-143.

11. Estimation effective des points entiers d'une famille de courbes algébriques, Annales de la Faculté de Sciences de Toulouse, V, no 4, (1996), 691-725.

12. Integer points on algebraic curves with exceptional units, J. Austr. Math. Soc. 63 (1997), 145-164.

13. Polynomial bounds for the solutions of a class of Diophantine equations J. Number Theory 66 (1997), 271-281.

14. Bounds for the size of integral solutions to $Y^m = f(X)$, Proc. Edinburgh Math. Soc. 42 (1999), 127-141.

15. A simple method for solving the diophantine equation $y^2 = x^4+ax^3+bx^2+cx+d$, Elemente der Mathematik 54 (1999), 32-36.

16. Bounds for the minimal solutions of the genus zero diophantine equations, Acta Arithmetica, LXXXVI.1 (1998) 51-90.

17. The number of solutions of the Mordell equation, Acta Arithmetica LXXXVIII.2 (1999), 173-179. Corrigendum, Acta Arithmetica XCII.4 (2000), 387-8.

18. Sur la réduction modulo p des polynômes absolument irréductibles, Monatshefte für Mathematik 129 (2000), 139-145.

19. Sur la réduction modp des courbes algébriques lisses, Archiv der Mathematik 75 (2000), 342-345.

20. Bounds for the size of integral points on curves of genus 0, Acta Mathematica Hungarica, 93 (4) (2001), 327-346.

21. (with E. Voskos) On the practical solution of genus zero diophantine equations, Journal of Symbolic Computation, 30 (2000), 573-582.

22. (with E. Voskos) Solving genus zero diophantine equations with at most two infinite valuations, Journal of Symbolic Computation, 33 (2002), 479-491.

23. Affine curves with infinitely many integral points, Proc. Amer. Math. Soc. 131, 5 (2002), 1357-1359.

24. (with E. Voskos) On the distribution of integer points of rational curves, Periodica Math. Hungarica, 46 (1) (2003), 99-111.

25. Bounds for the smallest integer point of a rational curve, Acta Arith. 107.3 (2003), 251-268.

26. (with M. Laurent) On the global distance between two algebraic points on a curve, J. Number Theory 104 (2004), 210-254.

27. Integer points on rational curves with fixed gcd, Publicationes Mathematicae Debrecen, 64, 3-4 (2004), 369-379.

28. (with G. Walsh) A note on the Diophantine equation $x^2-dy^4 = 1$ with prime discriminant, C. R. Math. Rep.Acad. Sci. Canada, 27 no. 2 (2005), 54-57.

29. (with G. Walsh) A note on the Diophantine equation $x^2-dy^4 = 1$ with prime discriminant II, Colloquium Mathematicum 105, No.1 (2006), 51-55.

30. (with K. Draziotis) Practical solution of the Diophantine equation $y^2 = x(x+2^a p^b)(x-2^a p^b)$, Mathematics of Computation, Vol. 75, no 255 (2006), 1585-1593.

31. (with K. Draziotis) Explicit Chevalley-Weil Theorem for Affine Plane Curves, Rocky Mountain Journal of Mathematics, 39(1) (2009), 49-70.

32. (with K. Draziotis) Solving the Diophantine equation $y^2 = x(x^2 - n^2)$, Journal of Number Theory 129 (2009), 102-121.

33. On the rational solutions of the equation $f(X,Y)^a = h(X)g(X,Y)$, Canadian Mathematical Bulletin, 52 (1) (2009), 117-126.

34. (with P. Alvanos and Y. Bilu) Characterizing Algebraic Curves with Infinitely Many Integral Points, International Journal of Number Theory 5**,** no. 4 (2009), 585 - 590.

35. A variant of Digital Signature Algorithm, Designs, Codes and Cryptography 51, No. 1 (2009), 99-104. Erratum Designs, Codes and Cryptography 58, No. 2, (2011), 219.

36. (with P. Alvanos) Solving Norm Form Equations over Number Fields, Algebraic Informatics, Third International Conference, CAI 2009, Thessaloniki, Greece, May 19-22, 2009, Proceedings, Lecture Notes in Computer Science 5725, pp 136-146.

37. A public key encryption scheme based on factoring and discrete logarithm, Journal of Discrete Mathematical Sciences & Cryptography, 12 (2009) No 6, 745-752.

38. (with K. Draziotis) An Effective Version of Chevalley-Weil Theorem for Projective Plane Curves, Houston Journal of Mathematics, Mathematics Vol. 38, No. 1 (2012), 29-39.

39. (with P. Alvanos) Solving genus zero Diophantine equations over number fields, Journal of Symbolic Computation 46 (2011), 54-69.

40. (with G. Karagiorgos) An algorithm for computing a basis of a finite Abelian group, 4rd International Conference on Algebraic Informatics, Linz, Austria, June 21-24, 2011. LNCS 6742, Springer, Berlin, (2011) 174-184.

41. (with G. Karagiorgos) Linear Time Algorithms for the Basis of Abelian Groups, 17th Annual International Conference in Computing and Combinatorics COCOON 2011, Dallas TX, USA, August 14-16, 2011. LNCS 6842, Springer, Berlin Heidelberg (2011), 456-466.

42. Some Lattice Attacks on DSA and ECDSA, Applicable Algebra in Engineering, Communication and Computing, (2011) 22:347–358.

43. (with G. Karagiorgos) Efficient Algorithms for the Basis of Finite Abelian Groups, Discrete Mathematics, Algorithms and Applications, Vol. 3, No 4 (2011) 537-552.

44. On the Cryptographic Long Term Security, Journal of Applied Mathematics & Bioinformatics, vol.3, no.1, (2013), 1-15.

45. (with K. Draziotis) Lattice Attacks on DSA schemes based on Lagrange's Algorithm, 5rd International Conference on Algebraic Informatics, Island Porcquerolles, France, September 3-6, 2013. LNCS 8080, Springer, Berlin, (2013) 121-133.

46. (with R. Rolland) A Digital Signature Scheme based on two hard problems, in Computation, Cryptography, and Network Security, Chapter 19, pp. 441-450 Springer 2015.

47. (with A. Aubry) Thue Equations and CM Fields, Ramanujan Journal of Mathematics (under publication).

48. (with P. Dospra) Complex Roots of Quaternion Polynomials (submitted)

49. (with P. Dospra) On the roots of quaternion polynomials (submitted).
50. Bounds for the solutions of unit and Thue equations (submitted).
51. Integral points of curves having no real points at infinity (submitted).

SUPERVISION OF PhD THESIS

1. E. Voskos (1-3-2002): Integer Points on Rational Curves.
2. K. Draziotis (1-5-2005). : Unramified Morphisms of Algebraic Curves and Diophantine Equations.
3. P. Alvanos (30-6-2010): Rational Curves over Algebraic Number Fields and Diophantine Equations.

SUPRVISION OF Msc THESIS

1. P. Alvanos (7-3-2005), The Riemann-Roch Theorem.
2. S. Stavropoulos (28-11-2006), Parametrization of algebraic Curves of Genus 0.
3. R. D. Malikiosis (11-9-2007): Elliptic Curves Cryptosystems and Xedni Algorithm.
4. V. Toura (6-11-2007): Elliptic Curves Cryptosystems of RSA Type.
5. K. Chatzigeorgiou (28-2-2008): Digital Signatures and Factorization.
6. G, Saltzis (7-5-2008): Cryptography and Diophantine Equations.
7. Ch. Lampropoulos (2-10-2008): Elliptic Curves and Primality.
8. P. Dospra (30-10-2008): Puiseux Series and Diophantine Equations.
9. Z. Vassiliadou (1-7-2011): Goppa Codes and the cryptosystem of McEliece.
10. E. Theoharopoulou (19-6-2013): Side Channel Attacks on RSA.
11. I. Fragouli (10 – 5 – 2014): Integer Factorization and Cryptography.
12. M. Adamoudis (14-5-2014): The shortest and the closest vector problem in Lattices.
13. I. Chronopoulos (20-9-2014): The LLL and their applications in Cryptanalysis.
14. Marianthi Kikidaki (20-9-2014): Discrete Logarithm and Cryptography.
15. M. Foutzopoulou (24-9-2014): Cryptanalysis with Lattices.
16. F. Kokavesis: (9-5-2015): Continuous Fractions and Applications.
17. M. Zacharea (9-5-2015): Finite Fields and Error Correcting Codes.

TEACHING

Algebra, Algebraic Structures, Algebraic Curves, Linear Algebra, Algebraic Geometry, Number Theory, Cryptography, Coding Theory, Theoretical Informatics.

CONFERENCES, WORKSHOPS etc

1. Journées Arithmétiques, Marseille, France, 17-21 July 1989.
2. Summer School of Number Theory, Athens 18-26 September 1989
3. Intenational Mathematical Meting, Delphes 27 September -2 October 1989.
4. Summer School of Mathematics, Athens 17-24 September 1990.
5. Journées Arithmétiques, Geneva 9-13 September 1991. Title of the talk: Points entiers sur les courbes hyperelliptiques.
6. Complex Analysis, Thessaloniki 23-26 January 1992. Title of the talk: A proof of the Irrationality of π^2 using Complex Analysis.
7. Journées Arithmétiques, Paris, 2-3 July 1992.
8. A' Congrès Européen de Mathématiques, Paris, 6-10 July 1992.
9. Arithmetic of Elliptic Curves, Anogia, Crete, 19-24 July 1993.

10. Journées Arithmétiques, Bordeaux, 13-17 September 1993. Title of the talk: Propriétés de ramification et points entiers sur les courbes algébriques.
11. Number Theory Conference (Diophantine, Computational and Algebraic Aspect) Eger, Hungary, 29 July - 2 August 1996. Title of the talk: Integer points on algebraic curves with exceptional units.
12. 1^{o} Pannelenic Conference of Algebra, Athens 27-28 September 1996. Title of the talk Integer points on algebraic curves with exceptional units.
13. "Devellopments in Language Theory", Thessaloniki 20-23 July 1997.
14. Journées Arithmétiques, Limoges 15-19 September 1997. Title of the talk: Polynomial bounds for the solutions of a class of Diophantine equations.
15. 2^{o} Pannelenic Conference of Algebra and Number Theory, Thessaloniki 13-14 june 1998. Title of the talk: The number of solutions of the Mordell equation.
16. Conference on Algebraic Number Theory and Diophantine Analysis, Graz, Austria, 31 August - 4 September 1998. Title of the talk: Bounds for the minimal solution of the genus zero Diophantine equations.
17. Current Trends and Developments in Fuzzy Logic, Thessaloniki 16-19 October 1998.
18. Journée Arithmétique et Théorie d'Information, Luminy Marseille, France 10 June 1999.
19. Journées Arithmétiques, Rome 12-16 July 1999. Title of the talk: On the reduction modulo p of absolutely irreducible polynomials.
20. Arithmétique, Géometrie et Théorie d'Information, CIRM Luminy, Marseille 25-29 October 1999.
21. Colloquium on Number Theory, Debrecen, Hungary 3-7 July 2000. Title of the talk: On the practical solution of the genus zero diophantine equation.
22. 3^{o} Pannelenic Conference of Algebra and Number Theory, Anogia, Crete, 1-3 September 2000. Title of the talk: On the Hilbert's Irreducibility Theorem.
23. Workshop on effective methods for Diophantine equations, Debrecen, Hungary 21-27 October 2001. Title of the talk: Integer points on rational curves.
24. 4^{o} Pannelenic Conference of Algebra and Number Theory, Patra, 30 May-1 June 2002. Title of the talk: Bounds for the smallest integer point of a rational curve.
25. 5^{o} Pannelenic Conference of Algebra and Number Theory, Ioannina, 1 – 3 October 2004. Title of the talk: The Chevalley-Weil Theorem and Diophantine Analysis.
26. Journées Arithmétiques, Marseille 4-8 June 2005. Title of the talk: Practical solution of the Diophantine equation $y^2 = x(x+2^a p^b)(x-2^a p^b)$.
27. 1st International Conference on Algebraic Informatics, Thessaloniki, 20-23 October 2005.
28. Approximation diophantienne et nombres transcendants, CIRM, Luminy Marseille 4 - 8 September 2006. Title of the talk: On the rational solutions of the equation $f(X,Y)^a = h(X)g(X,Y)$.
29. 2st International Conference on Algebraic Informatics, Thessaloniki 21-25 May 2007.
30. 7^{o} Pannelenic Conference of Algebra and Number Theory, Karlovasi, Samos, 31 May-2 June 2007. Title of the talk: On the rational points of algebraic curves.
31. 2nd Athens Colloquium on Algorithms and Complexity, Athens 23-24 August 2007.
32. 8^{o} Pannelenic Conference of Algebra and Number Theory, Athens 29-31 may 2008. Title of the talk: Solving the Diophantine equation $y^2 = x(x^2 - n^2)$.

33. 8th Central European Conference on Cryptography, Graz, Austria 2 – 4 July 2008. Title of the talk: An Electronic Voting Protocol for General Elections over the Internet.
34. 3nd Athens Colloquium on Algorithms and Complexity, Athens, 25-26 August 2008. Title of my talk: Efficient algorithms for the basis of finite abelian groups.
35. 3st International Conference on Algebraic Informatics, Thessaloniki, 19-22 may 2009. Title of the talk: Solving Norm Form Equations over Number Fields. The talk was given by the coauthor P. Alvanos.
36. 5nd Athens Colloquium on Algorithms and Complexity, Athens, 26-27 August 2010.
37. Approximation diophantienne et nombres transcendants, CIRM, Luminy 6 – 10 September 2010. Title of the talk: Solving genus zero Diophantine equations over number fields.
38. 4st International Conference on Algebraic Informatics, 21–24 Juin 2011, Linz, Austria. Title of the talk: An algorithm for computing a basis of a finite abelian group.
39. 17th Annual International Conference in Computing and Combinatorics COCOON 2011, Dallas TX, USA, August 14-16, 2011. Title of the talk: Linear Time Algorithms for the Basis of Abelian Groups.
40. Workshop on Algebraic Foundations in Computer Science, November 7-8, 2011, Thessaloniki, Greece.
41. Cryptography and Applications in Armed Forces, Hellenic Military Academy, Vari 6 April 2012. Title of the talk: A digital signature scheme for long term security.
42. 7th Athens Colloquium on Algorithms and Complexity, 27-28 August 2012, Athens. Title of the talk: A digital signature scheme for long term security.
43. 6th YACC' 12 (Yet Another Conference in Cryptography 2012) 24-28 September 2012, Porcquerolles Island, France. Invited talk : Primitives for Cryptographic Long Term Security.
44. 2nd International Conference on Applications of Mathematics and Informatics in Military Sciences (2nd AMIMS), Hellenic Military Academy, Vari Attikis, 11-12 April 2013.
45. 8th Athens Colloquium on Algorithms and Complexity, 22-23 August 2013, Athens. Title of the talk: Lattice Attacks on DSA schemes based on Lagrange's Algorithm.
46. 5st International Conference on Algebraic Informatics, 3-6 September 2013, Porcquerolles Island, France. Title of the talk: Lattice Attacks on DSA schemes based on Lagrange's Algorithm.
47. 2th International Conference on Cryptography, Network Security and Applications in Armed Forces (2nd CryptAAF), Hellenic Military Academy, Vari Attikis, 2 April 2014. Title of the talk: A New Lattice Attack on DSA schemes.
48. 7th YACC' 12 (Yet Another Conference in Cryptography 2014) 9-13 Juin 2014, Porcquerolles Island, France. Title of the talk: A New Lattice Attack on DSA Schemes.
49. Approximation diophantienne et nombres transcendants, CIRM, Luminy 15 – 19 Σεπτεμβρίου 2014. Title of the talk: Integral Solutions of Thue Equations.
50. 3nd International Conference on Technological Trends and Scientific Applicationa in Artilery and Military Sciences (3nd TTSAAMS), Nea Peramos Attikis, 5-6 May 2015.
51. Applications of Computer Algebra, Kalamata 20-23 July 2015. Title of the talk: Bezout Matrices and Roots of Quaternion Polynomials. The talk was given by the coauthor P. Dospra.

LECTURES (Total number: 33)
Selected Lectures:

- Department of Mathematics, University of Crete
- Institute H. Poincaré, Paris
- Department of Mathematics, University of Strasburg I
- Department of Mathematics, University of Marseille II
- Departments of Mathematics, Athens University
- Jussieu Institute of Mathematics, Paris
- Research Institute of Symbolic Computation - J.Kepler Linz University
- Center of Technological Research of Eastern Macedonia and Thrace.
- University Aix-Marseille II, Research group ERISCS.
- Department of Mathematics, University of Toulon-Var.

BOOKS (in Greek)

1. Number Theory, Ziti Publisher, 1997.
2. Cryptography, Ziti Publisher, 2004.
3. Introduction to the Geometry of Algebraic Curves, Ziti Publisher, 2006.
4. Algebraic Codes, Ziti Publisher, 2010.
5. Algebra, Ziti Publisher, 2014.
6. Computational Number Theory, SYNDESMOS AKADIMAIKON BIBLIOTHIKON, 2015.

ADMINISTRATIVE POSITIONS

- 1997-2001: Director of the Section of Algebra, Number Theory and Mathematical Logic at the Department of Mathematics, Aristotle University.
- 1999-2003: Vice president of the Department of Mathematics, Aristotle University.
- 2002-2004 and 2008-2014: Member of the Coordinating Committee on Graduate Studies, Department of Mathematics, Aristotle University.
- 2010-2011 and 2012-2015: Director of the Section of Numerical Analysis and Computer Sciences at the Department of Mathematics, Aristotle University.

REVIEWER of “Zentralblatt für Mathematik und ihre Grenzgebiete” and “Mathematical Reviews”.