CURRICULUM VITAE ET STUDIORUM

of Francesco Pappalardi

Personal Data:

Birth:	Rome, May 21, 1965
Position:	Associate Professor of Algebra
Address:	Dipartimento di Matematica e Fisica, Università Roma Tre, Largo S. L. Murialdo, 1 I-00146, Roma (ITALIA)
Phone:	+39-06-57.33.82.43
Mobile:	+39-32-90.57.14.88
Fax:	+39-06-57.33.80.80
skype:	francesco.pappalardi
web:	http://www.mat.uniroma3.it/users/pappa
Home Address:	Via S. Jacini, 68, I-00191, Roma (ITALIA)
email:	pappa@mat.uniroma3.it
Citizenship:	Italian
Research Interests:	Analytic Number Theory with Applications to Elliptic Curves and Cryptography

Education:

3/1993	PhD in Math.	McGill University, Montréal (*3-8/1989* Queen's University, Kingston (Ontario))
10/1988	Msc in Math.	Università "La Sapienza", Roma

Fellowships and prizes:

1993	Dean's Honor List	PhD, McGill University
1992	Award	ISM (Institut des Sciences Mathématiques), Montréal
1991	Fellowship	CNR for Italians abroad
1990	Award	WUSC (World University service of Canada)
1989	Fellowship	McGill Steward fellowships for foreign students
1989	Fellowship	Queen's University Baumann fellowship
1988	Fellowship	CNR, for mathematics master students.

Professional Experiences:

2015-	ICTP cunsultant	
2014-	Individual member of the *International Center for Pure and Applied Mathematics* CIMPA	
2014-	*Centro di Ateneo per la Formazione degli Insegnanti delle Scuole* coordinator of the Applied Mathematics Class (A048)	
09/2013	Habilitation to Full Professorship	
01/2002 -	Associate Professor	Università Roma Tre
06/1995-12/2001	Assistant Professor	Università Roma Tre
7/1994-1/1996	Post Doc	European Commission Human Capital and Mobility, Université de Paris Sud - Orsay
1-7/1994	Post Doc	CNR (Consiglio Nazionale delle Ricerche), Università di Roma Tre
08-12/1993	Post Doc	CICMA, Concordia University, Montréal
1989-1993	Teaching Assistant	McGill University - Montréal
1-8/1989	Teaching Assistant	Queen's University - Kingston
1987-1988	Software Consultant	Italian Association Education to Sanitary Contraception - Rome
1986-1987	Software Consultant	Sistema Permanente Servizi srl - Rome
9-12/*1987*	Teacher of Math	High School Istituto Pio XII°, Rome

Grants:

2012-2014	Team Member	**PRIN 2010-2011 (48.000€)** *"Geometria algebrica aritmetica e teoria dei numeri"*
2010-2011	Team Member	**PRIN 2008 (€19.500)** *"Problemi diofantei e analitici in Teoria dei Numeri"*
2007-2008	Team Member	**PRIN 2006 (€18.500)** *"Problemi diofantei e analitici in Teoria dei Numeri"*
2005-2007	Local Team Leader	**INTAS 03-51-5070** *"Analytical and Combinatorial Methods in Number Theory and Geometry"*
2005-2006	Team Member	**PRIN 2004 (€20.000)** *"Funzioni zeta e L e problemi diofantei in teoria dei numeri"*
2003-2004	Local Team Leader	**Italy - México, Scientific and Technological Cooperation Project** *"I gruppi Kleiniani in dimensione alta e la teoria analitica delle frazioni egiziane"*

2003-2004	Team Member	**COFIN 2002 (€22.000)** *"Funzioni zeta e L e problemi diofantei in teoria dei numeri"*
2000-2002	Team Member	**COFIN 2000** *"GVA - Geometria delle varietà algebriche"*
2000-2003	Team Member	**EUROPEAN Grant HPRN-CP-2002-00114** *"GTEM (Galois Theory and Explicit Methods in Arithmetic)"*
1997-1999	Local Team Leader	**Bilateral agreement:** Roma TRE - Macquarie University
1996	Chief Investigator	**Circ. CNR Po. 125.11** *"Programma di scambi internazionali per mobilità di breve durata"*
1994-1995	Chief Investigator	**Human Capital and Mobility Contract number: CHBICT930706** *"The Lang Trotter conjecture for abelian varieties"*
1993-	Group Member	**GNSAGA** from INDAM.

Editor Service:

2014-15	Editor	*Proceedings of the Conference SCHOLAR in honour of Ram Murty* Contemporary Mathematics AMS | CRM, 2015
2012	Guest Editor	A special issue of *Journal of the Australian Mathematical Society* dedicated to Alf van der Poorten Volume 92 - with Igor Shparlinski and Jeffrey Shallit
2003	Editor	Atti della conferenza *Stato della Ricerca e Sviluppi Futuri* with F. Dramis, A. Gambacorta, R. Mignani, A. Trentalance. Aracne Editrice Roma 2003.
1996	Guest Editor	Proceedings of the*"Incontro Italiano Teoria dei Numeri"* with. A. Perelli and C. Viola. Rend. Sem. Mat. Pol. Univ. Torino 53 No. 3-4 (1995)

Organising Conferences, Schools, Workshops:

2017 CIMPA research school on *Artin L-functions, Artin's primitive roots conjecture and applications*, Nesin Mathematics Village, Şirince, Turkey, May 29th–June 12th.

2017 CIMPA research school on *Théorie Algébrique des Nombres et Applications & Cryptographie,* Université Félix Houphouët BOIGNY, Abidjan, Côte d'Ivoire, April 10th–April 22nd

2016 *Leuca2016*, Celebrating Michel Waldschmidt's 70th birthday June 13th–17th, Marina di San Gregorio, Patù (Lecce), Italy

2016 *The Second Mini Symposium* of the Roman Number Teory Association, Università Roma Tre, April 26th

2015 *First Mini Symposium* of the Roman Number Theory Association, Unviversità Europea di Roma, May 7th

2015 *Algebraic Structures, Cryptography, Number Theory and applications.* EMA African Mathematical School. Universidad de Cabo Verde, Praia April 13th–28th Member of Scientific Committee

2014 *NATO ASI, Ohrid 2014 Arithmetic of Hyperelliptic Curves* August 25th–September 5th , Ohrid, the former Yugoslav Republic of Macedonia (scientific committee)

2013 *SCHOLAR - a Scientific Celebration Highlighting Open Lines of Arithmetic Research in honour of Professor M. Ram Murty's mathematical legacy on his 60th birthday,* CRM Montréal, October 15th–17th

2013 CIMPA research school on *Algebraic curves over Finite Fields,* University of the Phillipines Dillman, Manila. July 22nd–August 2nd

2010 CIMPA research school on *Number Theory in Cryptography and Its Applications,* **ICM Satellite Event,** School of Science, Kathmandu University, Dhulikhel, July 12th–31st

2009 "*La Teoria dei Numeri",*Università Roma Tre, May 27th–29th

2002 *"Stato della Ricerca e Sviluppi Futuri",* I primi 10 anni della facoltà di Scienze M.F.N., Università Roma Tre

1999 *"XXI Journées Arithmétiques",*Vatican, July 12th –16th

1995 *"Incontro Italiano Teoria dei Numeri" , Università Rome Tre, January 3rd –5th*

Program Committees

2008 International Workshop on the Arithmetic of Finite Fields *WAIFI08* Siena, Italy. July 6th–9th

Academic Visiting Appointments:

2016 University of Lethbridge (Alberta). **PIMS-Ulethbridge Distinguished Visitor**

2015 National University of Mongolia Ulan Batoor (Mongolia)
Tribuvan University, Kirtipur (Nepal)
Royal University of Phnom Penh (Cambodia)
Can Tho University (Vietnam)

2014 Université de Lomé (Togo)
Unversity of Baghdad (Iraq)

2013 University of Dhaka (Bangladesh)
Université de Lille 1 (France)
Tribuvan University, Kirtipur (Nepal)

2012 KTH Royal Institute of Technology, Stockholm (Sweden)

2011 Eötvös Loránd University, Budapest (Hungary)
Abdus Salam School of Mathematical Sciences, Lahore (Pakistan)
Tribhuvan University, Kirtipur (Nepal)

2010 Harish Chandra Research Institute, Allahabad (India)
Universidad Politécnica de Cataluña, Barcelona (Spain)

2009 Universidad Politécnica de Cataluña, Barcelona (Spain)
Macquarie University, Sydney (Australia)

2008 Harish Chandra Research Institute, Allahabad (India)

2006 Université de Montréal (Canada)
Queen's University, Kingston (Canada)
Mysore University (India)
Punjab University, Chandigarh (India)

2005 University of Missouri, Columbia (USA)
University of Arkansas, Fayetteville (USA)
Macquarie University, Sydney (Australia)
University of Pedagogy, Ho Chi Minh City (Vietnam)
University of Kathmandu (Nepal)
Université de La Polynésie Française, Thaiti (French Polynesia)
Instituto de Matemáticas UNAM, Campus Morelia (Mexico)
Harish Chandra Research Institute, Allahabad (India)

2004 Concordia University, Montréal (Canada)
Macquarie University, Sydney (Australia)
Kinki University, Iizuka, Fukuoka (Japan)

2003 Universiteit Leiden (Netherland)
University of Toronto (Canada)
Harish Chandra Research Institute, Allahabad (India)
Università Federico II, Napoli (Italy)

2002 Macquarie University, Sydney (Australia)
Harish Chandra Research Institute, Allahabad (India)
Université de Caen (France)
American University of Beiruth (Lebanon)
Concordia University, Montréal (Canada)

2001 Harish Chandra Research Institute, Allahabad (India)
Università G. d'Annunzio di Chieti-Pescara (Italy)
Universidad Politécnica de Cataluña, Barcelona (Spain)

2000 Macquarie University, Sydney (Australia)
Concordia University, Montréal (Canada)

1999 Concordia University, Montréal (Canada)
Macquarie University, Sydney (Australia)

1998 Concordia University, Montréal (Canada)
Università di Genova (Italy)

1997 Macquarie University, Sydney (Australia)

1996 Concordia University, Montréal (Canada)
Università di Genova (Italy)

1995 Concordia University, Montréal (Canada)

1993 University of Georgia, Athens (USA)
University of Vermont (USA)

Invited Talks at Conferences and Workshops:

2015 *The Eighth International Conference on Science and Mathematics Education in Developing Countries* Yangon University, Myanmar December 4th-6th

Number Theory and applications in Cryptography and Coding Theory. SEAMS school University of Science, Ho Chi Minh, Vietnam August 31st - September 8th

Algebraic Structures, Cryptography, Number Theory and applications. EMA African Mathematical School. Universidad de Cabo Verde, Praia April 13th –28th

Yearly meeting of the Committee for Developing Countries of the European Mathematical Society. Invited University of Oslo, Norway, April 10th–11th

2014 *CIMPA workshop in Number Theory* at Salahaddin University, Erbil Kurdistan/Iraq, December 1st –9th

Short Course in Algebraic Number Theory (Fields, Units, Galois Groups) , Tribhuvan University, Kirtipur Nepal, October 24th–31th

NATO ASI, Ohrid 2014 - Arithmetic of Hyperelliptic Curves, August 25 - September 5, 2014, Ohrid, the former Yugoslav Republic of Macedonia

Journée Internationale d'Arithmétique Cryptographie at Applications UFRMI Université Félix Houphouet Boigny Cocody, July 24. Abidjan (Ivory Coast)

CIMPA-ICTP-BENIN Research school Algebraic Number Theory and Application, Institute of mathematics and physical Sciences (IMSP), July 7 – 19. Dangbo (Benin)

Frobenius Distribution on Curves, Centre International de Rencontres Mathématiques, February 17 - 22, Luminy (France)

Chaire Jean-Morlet : Unlikely Intersections Centre International de Rencontres Mathématiques , February 3 – 7, Luminy (France)

2013 *Analytic Theory of Automorphic Forms,* Chennai Mathematical Institute (CMI-IMSc), December 9–14, Chennai, (India)

Meeting on Number Theory, Max-Planck Institute for Mathematics MPIM, November 20–22, Bonn (Germany)

2nd International Conference in Mathematics and its Applications, ICMA, October 23–24, Basrah, (Iraq)

Special Semester Méthodes Arithmétiques et Applications, Université de Franche-Comté, September 18–27, Besancon, (France)

CIMPA-ICTP-UNESCO-MESR-MINECO-PHILIPPINES Research School Algebraic Curves over Finite Fields, University of the Phillipines Dillman, July 22 –August 2, Manila (Philippines)

2011 *International Meeting on Number Theory Celebrating the 60th Birthday of Professor R. Balasubramanian*, HRI , December 15–20, Allahabad (India)

2010 *Italy-India Conference on Diophantine and Analytic Number Theory,* Scuola Normale Superiore, March 8–14, Pisa (Italy)

CIMPA research school *Number Theory in Cryptography and its Applications*, Kathmandu University, July 19–31, Dhulikhel (Nepal)

CIMPA research school *Théorie des Nombres et Algorithmique*, University of Bamako, November 15–26, Bamako (Mali)

2009 *International Conference in Number Theory,* Kinki University, October 17–19, Iizuka, Fukuoka (Japan)

1st National School in Number Theory and Cryptography NSNTC, University of Kathmandu, December 2009 – January 2010, Dhulikhel (Nepal)

2007 *International Conference on Number Theory and Smarandache Problems,* Weinan University, March 23–25, Weinan (China)

Ecole d'Eté de Calcul Formel et Théorie des Nombres, Faculté de Sciences de Monastir, August 27–September, Monastir (Tunisia)

2006 *Italian-Polish Number Theory Days,* Uniwersytet im. Adama Mickiewicza, May 17–20, Poznan, (Poland)

Conference devoted to the Memory of Korobov, Lomonosov State University, May 25–31, Moscow (Russia)

WMC 2006, Workshop on Mathematical Cryptology, University of Cantabria, June 29–30, Santander, (Spain)

Mathematics and its Applications, joint SIMAI, SMAI, SMF and UMI meeting Politecnico and Università di Torino, July 3–7, Torino (Italy)

Analysis in Number Theory 2005-2006, Centre de Recherches Mathématiques, Montréal (Canada)

National Conference on Mathematical Foundations of Coding, Complexity, Computation and Cryptography, Annual Tematic year in Coding Theory and Cryptography (IMI), Indian Institute of Science, July 20–22, Bangalore (India)

2004 *Workshop on Industrial Mathematics (IMATH),* King Fahd University of Petroleum and Minerals, February 29 – March 2, Dhahran (Saudi Arabia)

Seminario sulla sicurezza informatic, Università di Campobasso, April 28, Campobasso (Italy)

Analytic Number Theory and Surrounding Areas, Research Institute of Mathematical Science (RIMS), October 18–22, Kyoto (Japan)

2003 *Conference in Honor of K. Ramachandra,* National Institute of Advanced Studies Bangalore, December 12–15, Bangalore (India)

Secondo Convegno Italiano di Teoria dei Numeri, Università di Parma, November 13–15, Parma (Italy)

2002 *Conference in Analytic Number Theory with Special Emphasis on L-functions,* Institute of Mathematical Sciences, January 1–4, Chennai, (India)

Incontro Borsisti di Merito INDAM, Università di Perugia, August 4–7, (Italy)

2001 *Finite Fields and Applications Meeting,* January 8–13, Oberwolfach (Germany)

1999 *Workshop on Cryptography and Computational Number Theory (CCNT'99)*, National University of Singapore, November 22–26, (Singapore)

1997 *Finite Fields and Applications Meeting,* January 20–25, Oberwolfach(Germany)

1995 *Convegno Giornate di Geometria Algebrica ed Argomenti Correlati III,* Università dell'Aquila, May 22–24, L'Aquila (Italy)

Other Conferences/Workshops attended:

2014 *Polynomials over Finite Fields: Functional and Algebraic Properties* Centre de Recerca Matemàtica, May 19 to 24, Bellaterra (Spain)

2013 *SCHOLAR - a Scientific Celebration Highlighting Open Lines of Arithmetic Research In honor of Ram Murty's 60th birthday,* Centre de Recherches Mathematiques (CRM), October 15–16, Montréal (Canada)

CIMPA-UNESCO-MESR-MINECO-MONGOLIA School *Hypergeometric Functions and Representation Theory,* National University of Mongolia, August 5–16, Ulaanbaatar (Mongolia)

3rd Atelier PARI/GP 2013, Institut Mathématiques Bordeaux, January 14–18, Bordeaux (France)

2012 *International Number Theory Conference in Memory of Alf van der Poorten*, CARMA, University of Newcastle, March 12–16, Newcastle (Australia)

2011 *Arctic Number Theory School*, University of Helsinki, May 18–25 (Finland)

2009 *Advances in Mathematics Conference*, Nanyang Technological University, July 20–22, (Singapore)

2008 NATO Advanced Study Institute *New Challenges in Digital Communications*, University of Vlora, April 28 – May 9, Vlora (Albania)

2003 *First Joint AMS-Indian Mathematical Society Meeting.* Indian Institute of Science, December 17–20, Bangalore (India)

Conference in Number Theory in Honour of Professor H.C. Williams, The Banff Centre, May 24–30 , Banff (Canada)

2002 *CNTA-VII, Conference of the Canadian Number Theory Association*, May 19–25 Montréal (Canada)

2000 Clay Mathematics Institute Introductory Workshop in *Algorithmic Number Theory,* MSRI, August 14–23, Berkeley (USA)

Latin American Theoretical Informatics LATIN 2000, April 10–14, Punta del Este (Uruguay)

1996 *CNTA-V, Conference of the Canadian Number Theory Association*, August 17–22 Ottawa (Canada)

1993 *AMS-CMS International Joint Mathematics Meeting #883,* August 15–19, Vancouver (Canada)

1991 *CNTA-III, Conference of the Canadian Number Theory Association*, August 18–24, Kingston (Canada)

Seminars and Conferences:			
Australia (7)	Benin (3)	Cabo Verde (5)	Canada (>10)
China (1)	France (8)	French Polynesia (1)	Germany (4)
Japan (3)	India (>10)	Iraq/Kurdistan (9)	Ivory Coast (1)
Lebanon (2)	FYRO Macedonia (2)	Mali (4)	Mexico (1)
Mongolia (4)	Myanmar (1)	Nepal (>10)	Netherland (1)
Norway (1)	Pakistan (6)	Philippines (6)	Poland (1)
Russia (2)	Saudi Arabia (2)	Singapore (1)	Spain (3)
Sweden (1)	Togo (1)	Tunisia (1)	United States (6)
Vietnam (5)	Italy (>10)		

Referee:

Journals: Acta Arimetica, Algebra and Number Theory, Bullettin of the London Mathematical Society, Mathematics of Computation, Discrete Mathematics, Rendiconti del Seminario Matematico del Politecnico e dell'Univiversità di Torino, Finite Fields and their Applipations, Journal of Number Theory, Bollettino del Unione Matematica Italaliana, Rendiconti di Parma, Journal de Theorié de Nombre Bordeaux, Compositio Mathematica, The Arabian Journal for Science and Engineering, Proceedings of the AMS, Transactions of the AMS, Arkiv fuer Mathematics, Journal of Discrete Algorithms, Integers, Le Matematiche di Catania, Rendiconti dell'Istituto di Matematica dell'Università di Trieste, International Journal of Number Theory, Proceedings of Mathematical Sciences.

Reviewer: Mathematics Reviews, Mathematics of Computation (book review).

Agencies: NSA, Israeli Science Foundation, Commissione Scientifica Regione Calabria (Italy), Minustero Istruzione Università e Ricerca (MIUR), Natural Sciences and Engineering Research Council of Canada (NSERC), INDAM COFUND.

Memberships: Individual Member of the International Center for Pure and Applied Mathematica (CIMPA/ICPAM) , 2014-

Conferences: SODA, WAIFI.

PhD thesis referee: Università Tor Vergata (2015) Università di Roma "Sapienza" (2014) Université de Lille 1 – France (2013)**,** Burdwan University – India (2011-2010) Harish Chandra Research Institute – India (2006-2003), Universiteit Leiden – Netherland (2003)

Thesis Supervised:

Master:	27 thesis since 2000	http://www.mat.uniroma3.it/users/pappa/studenti.html
PhD:	A. Susa	*Some analogous problem to Artin's conjecture (12/04/2006)*
	G. Meleleo	*Questions related to Primitive Points on Elliptic Curves and Statistics for Biquadratic Curves over Finite Fields (8/05/2015)*
	C. Pehlivan	*Some average results connected with reductions of groups of rational numbers (08-05-2015)*
	L. Menici	in progress (due on April 26th, 2015)
	M. Anwar	in progress

Teaching:

students evaluations in **http://www.mat.uniroma3.it/users/pappa/CORSI/corsi.html**

at "Roma TRE"	
1995/1996	Geometry 2 (Point set Topology); Linear Algebra
1996/1997	Calculus for Biologists; Geometry 2 (Point set Topology); Number Theory
1997/1998	Calculus for Biologists; first year Algebra; Number Theory
1998/1999	Multivariate Calculus for Physicists; Public key Cryptography (MA2)
1999/2000	Public key Cryptography (MA2); Finite Groups (AL5)
2000/2001	Public key Cryptography (MA2); Representations of finite groups (GE7)
2001/2002	Public key Cryptography (CR1)
2002/2003	Public key Cryptography (CR1); Galois Theory (TE1)
2003/2004	Analytic Number Theory (TN2); Introduction to Number Theory (TN1)
2004/2005	Elliptic curves Cryptography (CR3); Introduction to Number Theory (TN1); Galois Theory (TE1)
2005/2006	Introduction to Analytic Number Theory (TN2); Topology and Differential Geometry
2006/2007	Analysis for Physics Students; Galois Theory (TE1); Group Theory (AL9)
2007/2008	Public key Cryptography (CR1); Introduction to Analytic Number Theory (TN2)
2008/2009	First year Algebra (AL1); Elliptic curves Cryptography (CR3)
2009/2010	Second year Algebra (AL2); Galois Theory (TE1)
2010/2011	Second year Algebra (AL210); Number Theory (TN510)
2011/2012	Galois Theory (AL310); Public key Cryptography (CR410)
2012/2013	Analytic Number Theory (TN510); Public key Cryptography (CR410)
2013/2014	Elliptic Curve Cryptography (CR510); Public key Cryptography (CR410)
2014/2015	Elementary Number Theory (TN410); Public key Cryptography (CR410)
2015/2016	Number Theory (TN510); Elementary Number Theory (TN410)
at Roma Tor Vergata	
1999/2000	Engineering Linear Algebra
at Concordia	
1993/1994	Several Variables Calculus and Differential Equations (EMAT 212/2)
at McGill	
1992/1993	Calculus I - Section A/B (189-120A/B)
1991/1992	Calculus I - Section A (189-120A)
1990/1991	Calculus I - Section A (189-150A)
1989/1990	Calculus I - Section A/B (189-150A/B)

LIST OF PUBLICATIONS
by Francesco Pappalardi

Journal papers:

1. with A. Susa: *An analogue to Artin's conjecture for multiplicative subgroups of the rationals.* Archiv der Mathematik. **101**, Issue 4, (2013), 319-330

2. *Divisibility of reduction in groups of rational numbers.* Math. Comp. **84**, Issue 291(2015) 385-407

3. with W. Banks and I. Shparlinski: *Possible Group Structures of Elliptic Curves over Finite Fields*. Experimental Mathematics **21**, Issue 1, (2012) 11-25.

4. *On the exponents of the group of points of an Elliptic curve over a finite field.* Proc. Amer. Math. Soc. **139** No. 7 (2011) 2337-2341.

5. with Étienne Fouvry, F. Luca and I. Shparlinski: *Counting dihedral and quaternionic extensions*. Trans. Amer. Math. Soc. **363** No. 6 (2011) 3233-3253.

6. with A. Susa: *On a problem of Schinzel and Wójcik involving equalities between multiplicative orders*. *Math. Proc. Cambridge Philos. Soc.* **146.2** (2009), 303-319.

7. with S. D. Adhikari, R. Balasubramanian and P. Rath: *Some zero-sum constants with weights*. *Proceedings of Indian Academy of Sciences.* **118**, No. 2, (2008), 183-188.

8. with F. Luca: *Composite positive integers with an average prime factor*. *Acta Arithmetica* **129** (2007), 197-201

9. with A. Glibichuk and F. Luca: *On the equation τ(λ(n))=ω(n)+k. Michigan Mathamatical Journal* **55**, Issue 3 (2007), 671-692.

10. with W. Banks, J. B. Friedlander, F. Luca and I. Shparlinski: *Coincidences in the Values of the Euler and Carmichael Functions. Acta Arithmetica* **122.3** (2006), 207-234.

11. with W. Banks: *Powerfree Values of the Euler Function. J. Num. Theory* **120** (2006) 326-348.

12. with S. Konyagin: *Enumerating permutation polynomials over finite fields by degree II. Finite Fields and their Applications* **12** (2006) 26-37.

13. with S. das Adhikari, Y. G. Chen, J. B. Friedlander, S. Konyagin: *Contributions to zero-sum problems. Discrete Math* **306** (2006), 1-10.

14. with W. Banks, K. Ford, F. Luca and I. Shparlinski: *Values of the Euler Function in Various Sequences. Monats. Math.* **146** (2005), 1-19.

15. with Alf van der Poorten: *Pseudo-Elliptic Integrals, Units and Torsion. J. Aust. Math. Soc.* **79** (2005), 335-347.

16. with F. Luca: *Members of binary recurrences on lines of the Pascal triangle. Publ.*

Math. Debrecen **67** 1-2 (2005) 103-113.

17. with C. David: *Average Frobenius Distribution for inerts in* **Q**(*i*). *Journal of the Ramanujan Mathematical Society* **19**, n. 3 (2004), 1-21.

18. with C. Malvenuto: *Enumerating Permutation Polynomials II: k-cycles with minimal degree. Finite Fields and their Applications* **10** (2004) 62-76.

19. *Squarefree Values of the Order Function. New York Journal of Mathematics* **9** (2003), 331-344.

20. with F. Saidak and I. Shparlinski: *Squarefree Values of the Carmichael Function. J. Num. Theory* **103** (2003) 122-131.

21. with S. das Adhikari: *On the visibility problem in the function field case. C. R. Math. Acad. Sci. Soc. R. Can.* **24** (2002), no. 3, 109-116.

22. with S. Konyagin: *Enumerating Permutation Polynomials over finite fields by degree. Finite Fields and their Applications* **8** (2002) 548-553.

23. with C. Malvenuto: *Enumerating Permutation Polynomials I: Permutations with non maximal degree. Finite Fields and their Applications* **8** (2002) 531-547. - *corrigendum* ibid. **13** 1 (2007) 171-174.

24. with B. Mans and I. Shparlinski: *On the spectral Adams property for circulant graphs. Discrete Math.* **254** (2002) 309-329.

25. with E. Croot, D. E. Dobbs, J. B. Friedlander, A. J. Hetzel: *Binary Egyptian Fractions. J. Num. Theory* **84** (2000) 63-79.

26. with L. Cangelmi: *On the r-rank Artin Conjecture II. J. Num. Theory* **75** No.1 (1999) 120-132.

27. with C. David and H. Kisileveski: *Galois representations with non surjective traces. Canad. J. Math.* **51** No. 5 (1999) 936-951.

28. with C. David: *Average Frobenius Distribution of Elliptic Curves. Internat. Math. Res. Notices* **4** (1999) 165-183.

29. *The r-rank Artin Conjecture. Math. Comp.* **66** (1997) 853-868.

30. *On the order of finitely generated subgroups of Q* and divisors of p-1. J. Num. Theory* **57** No. 2 (1996) 207-222.

31. *On Hooley's Theorem with weights. Rend. Sem. Mat. Polit. Univ. Torino* **53** No. 4 (1995) 375-388.

32. with I. Shparlinski: *The Artin Conjecture for function fields. Finite Fields and their Applications* **1** (1995) 399-404.

33. with H. Kisilevsky: *On the exponent of the ideal class group of function fields. Acta Arithmetica* **LXXII** No. 4 (1995) 311-321.

34. *On minimal sets of generators for primitive roots. Bull. Canad. Math. Soc.* **38** No. 4

(1995) 465-468.

35. *On the exponent of the ideal class group of* $\mathbf{Q}(\sqrt{-d})$. *Proc. Amer. Math. Soc.* **123** No. 3 (1995) 663-671.

36. with H. E. Campbell, I. Hughes and P. Selik: *On The ring of Invariants of* $\mathbf{F_2}^{*n}$. *Comment. Math. Helvetici* **66** (1991) 322-331.

Refereed Conference Papers:

1. with Arto Lepistö and Kalle Saari: *Transposition Invariant Words*. *Theoretical Computer Science* **380**, Issue 3 (June 2007) 377-387, Combinatorics on words.

2. with A. Susa *On a problem of Schinzel and Wojcik* (Analytic Number Theory and Surrounding Areas). RIMS Kokyuroku, **1511,** 129-135 (2006).

3. *A survey on k-power freeness.* Proceeding of the Conference in Analytic Number Theory in Honor of Prof. Subbarao at I.M.Sc. Chennai, January 2003. *Number theory, 71-88, Ramanujan Math. Soc. Lect. Notes Ser. 1*, Ramanujan Math. Soc., Mysore, 2005.

4. with J. von zur Gathen: *Density Estimates related to Gauss periods*. Lam, Kwok-Yan (ed.) et al., *Cryptography and computational number theory*. Proceedings of the workshop, CCNT'99, Singapore, November 22-26, 1999. Basel: *Birkhäuser*. Prog. Comput. Sci. Appl. Log. **20**, 33-41 (2001).

5. with C. Malvenuto: *On the Enumeration of Permutation Polynomials*. Proc of Colloque LaCIM 2000 Combinatoire, Informatique et Applications Laboratoire de Combinatoire et d'Informatique Mathématique (*LaCIM*) Université du Québec à Montréal, 7 au 10 septembre 2000.

6. with B. Mans and I. Shparlinski: *On Adams Conjecture for circulant graphs* Hsu, Wen-Lian (ed.) et al., *Computing and combinatorics. 4th annual international conference, COCOON '98, Taipei, Taiwan, ROC, August 12-14, 1998*. Proceedings. Berlin: Springer. *Lect. Notes Comput. Sci.* **1449**, 251-260 (1998).

7. *L'esponente del gruppo delle classi in campi di funzioni.* Estratti Convegno Giornate di Geometria Algebrica ed argomenti Correlati III, L'Aquila 1995.

In Preparation:

1. with Nathan Jones: On never primitive points in elliptic curves over **Q**
2. with Min Sha, Igor Shparlinski and Cam Stewart: *On Multiplicatively Dependent Vectors*
3. with Igor Shparlinski: *Average Schinzel–Wójcick Problem.*
4. with Kalyan Chakraborty and Jorge Jimenez Urroz: *Pairs of integers which are mutually squares.*
5. *On simultaneous primitive roots. Об Одновременно Первообразных Корнях.*
6. with D. Cosentino: *Fast computation of k-dimensional residues and an application to probabilistic encryption.*

Course Notes:

Note di crittografia a chiave pubblica.
Vol 1. *Prerequisiti di Teoria dei Numeri*
Vol 2. *RSA, fattorizzazione e primalità*

Book Reviews:

with P. Mihailescu: "*Elliptic Curves in Cryptography*" by I. Blake, G. Seroussi, N. Smart. Math. Comp. 2001.