

# CURRICULUM VITAE ET STUDIORUM

Nadir Murru

## DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE

(art. 46 del D.P.R. n.445 del 28/12/2000)

## DICHIARAZIONE SOSTITUTIVA DELL'ATTO DI NOTORIETA'

(art. 19 e 47 del D.P.R. n.445 del 28/12/2000)

Il sottoscritto  
consapevole delle sanzioni penali, nel caso di dichiarazioni non verificate e falsità negli atti,  
richiamate dall'art. 76 del D.P.R. 445/200 e dalle leggi speciali in materia

### DICHIARA

che tutto quanto sotto riportato corrisponde a verità.

## Dati Personali

- **Luogo di nascita:** Gattinara (VC)
- **Data di nascita:** 29/09/1983
- **Indirizzo mail:** nadir.murru@gmail.com, nadir.murru@unito.it

## Istruzione

*01/2008 – 02/2011. **Dottorato di Ricerca in Matematica** (con borsa), conseguito in data 28/02/2011 presso Università degli studi di Torino. Settore di Ricerca: Algebra e Teoria dei Numeri, MAT/02. Titolo della Tesi: Approximations of irrationalities by using linear recurrent sequences. Relatore: Prof. Umberto Cerruti.*

**Breve descrizione:** L'argomento della tesi di dottorato si inserisce nel campo dell'approssimazione diofantea e delle frazioni continue. In particolare, sono state studiate approssimazioni di irrazionalità quadratiche e cubiche, trovando nuovi risultati tramite l'utilizzo delle funzioni razionali di Rédei, introdotte in maniera originale come convergenti di particolari frazioni continue. Le approssimazioni di irrazionalità quadratiche sono state anche studiate tramite successioni di punti razionali su particolari coniche (come le coniche di Pell e loro generalizzazioni). Contemporaneamente, sono state fornite nuove rappresentazioni periodiche per radici quadrate e cubiche connesse alle frazioni continue e loro generalizzazioni.

*09/2005 – 07/2007. **Laurea Specialistica in Matematica**, conseguita in data 17/07/2007 presso Università degli Studi di Torino. Votazione: 110/110 Lode e Menzione. Titolo della tesi: Aritmetica delle Frazioni Continue. Relatore: Prof. Umberto Cerruti.*

## Posizioni di Ricerca

*01/05/2019 – In corso. **Ricercatore a Tempo Determinato di tipo A** presso Università di Torino, Dipartimento di Matematica "G. Peano", Torino, Settore Scientifico Disciplinare: MAT/02.*

01/12/2018 – 30/04/2019. **Assegnista di ricerca** (di cui all'art. 22 della legge n.240/2010) presso Politecnico di Torino, Dipartimento di Scienze Matematiche, Torino.  
Titolare di assegno di ricerca "**Crittografia post-quantum**". Responsabile scientifico: Prof. Antonio Di Scala.

01/05/2018 – 31/10/2018. **Borsista** presso Università degli Studi di Torino, Dipartimento di Matematica "G. Peano", Torino.  
Titolare di borsa di ricerca "**Reti neurali e logica fuzzy**". Responsabile scientifico: Prof.ssa Anna Capietto.

01/05/2014 – 30/04/2018. **Assegnista di ricerca** (di cui all'art. 22 della legge n.240/2010) presso Università degli Studi di Torino, Dipartimento di Matematica "G. Peano", Torino.  
Titolare di assegno di ricerca "**Individuazione e sviluppo di nuove tecnologie per favorire la partecipazione attiva agli studi universitari da parte di giovani con disabilità motoria e sensoriale**". Settore Scientifico Disciplinare: MAT/02. Responsabile scientifico: Prof.ssa Anna Capietto.

01/07/2013 – 30/04/2014. **Assegnista di ricerca** (di cui all'art. 22 della legge n.240/2010) presso CNR, Istituto di Scienza e Tecnologie dell'Informazione (ISTI), Pisa.  
Titolare di assegno di ricerca "**Studio di soluzioni matematiche per la caratterizzazione e ottimizzazione di riconfigurazioni di sistemi di distribuzione elettrica, a supporto della modellazione ed analisi di tali sistemi**". Responsabile scientifico: Dott.ssa Felicità Di Giandomenico.

01/06/2011 – 31/05/2012. **Borsista** presso INRIM (Istituto Nazionale di Ricerca Metrologica), Torino.  
Titolare di borsa di addestramento alla ricerca "**Software per il trattamento dati con applicazione alla metrologia dimensionale**". Responsabile scientifico: Dott. Giampaolo E. D'Errico.

## Abilitazione

**Abilitazione Scientifica Nazionale** per il ruolo di *Professore di seconda fascia*, settore concorsuale 01/A2 (Geometria e Algebra), *dal 30-11-2017 al 30-11-2026*.

## Partecipazione a progetti e gruppi di ricerca

- 01/07/2019 – *In corso* **Responsabile** del Progetto di ricerca locale 'Strumenti matematici per le applicazioni', Dipartimento di Matematica G. Peano, Università di Torino, finanziato con 8089,18 euro.
- 01/09/2017 – *In corso* Progetto 'Accessibilità di testi digitali con contenuti scientifici da parte di persone con disabilità visiva', Progetto di ricerca locale, Dipartimento di Matematica G. Peano, Università di Torino.
- 01/05/2014 – *In corso* Progetto 'Per una matematica accessibile e inclusiva', Progetto nazionale del Dipartimento di Matematica G. Peano, Università di Torino.
- 07/03/2017 – 31/07/2019 Progetto 'Algebra e dintorni', Progetto di ricerca locale, Dipartimento di Matematica G. Peano, Università di Torino.
- 15/05/2017 – 31/07/2019 Progetto 'Approssimazione multivariata e algoritmi efficienti con applicazioni a problemi algebrici, differenziali e integrali', Progetto di ricerca locale, Dipartimento di Matematica G. Peano, Università di Torino.

- *01/05/2014 – 30/04/2018* Progetto ‘Individuazione, uso, diffusione e sviluppo di nuove tecnologie per favorire la partecipazione attiva agli studi universitari da parte di giovani con disabilità e con DSA, nell’ottica dei principi dell’accessibilità, della personalizzazione didattica e dell’inclusione’, Progetto di Ateneo, Università di Torino.
- *26/01/2015 – 25/01/2017* Progetto ‘Metodologie, tecnologie, materiali e attività per un apprendimento della matematica accessibile e inclusivo’, Progetto di Ateneo, Università di Torino.
- *01/05/2015 – 31/12/2016* Progetto ‘Algebra e Geometria Algebrica e loro applicazioni’, Progetto di ricerca locale, Dipartimento di Matematica G. Peano, Università di Torino.
- *01/05/2015 – 31/12/2016* Progetto ‘Algebra, Geometria Algebrica e Storia’, Progetto di ricerca locale, Dipartimento di Matematica G. Peano, Università di Torino.
- *01/07/2013 – 30/04/2014* Progetto ‘Tenace: Protecting National Critical Infrastructures from Cyber Threats’, Progetto PRIN n. 20103P34XC.
- *01/07/2013 – 30/04/2014* Progetto ‘SmartC<sup>2</sup>Net: Smart Control of Energy Distribution Grids over Heterogeneous Communication Networks’, Progetto Europeo n. ICT-318023.
- **Membro** del Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni (GNSAGA).
- **Membro** dell’Associazione Nazionale di Crittografia De Componendis Cifris, [www.decifris.it](http://www.decifris.it).
- **Membro** del Gruppo di ricerca in Algebra e Geometria Algebrica del Dipartimento di Matematica dell’Università di Torino.
- **Membro** del Gruppo di ricerca in Geometria Algebrica Computazionale e Differenziale del Politecnico di Torino.
- **Membro** del Gruppo di ricerca in Crittografia e Teoria dei Numeri del Politecnico di Torino.
- **Membro** del CINI (Consorzio Interuniversitario Nazionale per l’Informatica).
- **Membro** del Gruppo di ricerca Tecnologie assistive per le Stem del Dipartimento di Matematica dell’Università di Torino.
- **Membro** del Laboratorio per la Ricerca e Sperimentazione di Nuove Tecnologie Assistive per le STEM ‘S. Polin’ del Dipartimento di Matematica dell’Università di Torino.

## Publicazioni

1. U. Cerruti, S. Dutto, N. Murru, *A symbiosis between cellular automata and genetic algorithms*, Chaos, Solitons and Fractals, To Appear.
2. N. Murru, L. Terracini, *On the finiteness and periodicity of the  $p$ -adic Jacobi–Perron algorithm*, Mathematics of Computation, To Appear.
3. N. Murru, *A note on the use of Rédei polynomials for solving the polynomial Pell equation and its generalization to higher degrees*, The Ramanujan Journal, To Appear. DOI: 10.1007/s11139-019-00233-1.
4. S. Barbero, U. Cerruti, N. Murru, *On polynomial solutions of the Diophantine equation  $(x + y - 1)^2 = wxy$* , Rendiconti del Seminario Matematico, To Appear.

5. S. Barbero, U. Cerruti, N. Murru, *Approximations of algebraic irrationalities with matrices*, Experimental Mathematics, To Appear.  
Ready Online at <https://www.tandfonline.com/doi/full/10.1080/10586458.2018.1526722>.  
DOI: 10.1080/10586458.2018.1526722.
6. C. Havens, S. Barbero, U. Cerruti, N. Murru *Linear fractional transformations and non-linear leaping convergents of some continued fractions*, Research in Number Theory, Vol. 6, Article Number 11, 2020.
7. E. Bellini, N. Murru, *A multifactor RSA-like scheme with fast decryption based on Rédei rational functions over the Pell hyperbola*, Lecture Notes in Computer Science, Vol. 11973, 343–357, 2020.
8. N. Murru, L. Terracini, *On  $p$ -adic multidimensional continued fractions*, Mathematics of Computation, Vol 88, No. 320, 2913–2934, 2019.
9. P. Miska, N. Murru, C. Sanna, *On the  $p$ -adic denseness of the quotient set of a polynomial image*, Journal of Number Theory, Vol. 197, 218–227, 2019.
10. S. Barbero, U. Cerruti, N. Murru, *On the operations over sequences in rings and binomial type sequences*, Ricerche di Matematica, Vol 67, No. 2, 911–927, 2018.
11. S. Barbero, U. Cerruti, N. Murru, *Some combinatorial properties of the Hurwitz series ring*, Ricerche di Matematica, Vol. 67, No. 2, 491–507, 2018.
12. N. Murru, C. Sanna, *On the  $k$ -regularity of the  $k$ -adic valuation of Lucas sequences*, Journal de Théorie des Nombres de Bordeaux, Vol. 29, No. 3, 227–237, 2018.
13. T. Armano, A. Capietto, S. Coriasco, N. Murru, A. Ruighi, E. Taranto, *An automatized method based on LaTeX for the realization of accessible PDF documents containing formulae*, Lecture Notes in Computer Science, Vol. 10896, 583–589, 2018.
14. S. Barbero, U. Cerruti, N. Murru, *An isomorphism between the convolution product and the componentwise sum connected to the D’Arcais numbers and the Ramanujan tau function*, Research in Number Theory, Vol. 4, No. 3, Article 28, 2018.
15. T. Armano, M. Borsero, A. Capietto, N. Murru, A. Panzarea, A. Ruighi, *On the accessibility of Moodle 2 by visually impaired users, with a focus on mathematical content*, Universal Access in the Information Society, Vol. 17, No. 4, 865–874, 2018.
16. N. Murru, F. Saettone, *A novel RSA-like cryptosystem based on a generalization of Rédei rational functions*, Lecture Notes in Computer Science, Vol. 10737, Number Theoretic Methods in Cryptology, 91–103, 2018.
17. U. Cerruti, N. Murru, *If the primes are finite, then all of them divide the number one*, The American Mathematical Monthly, Vol. 124, No. 10, 969, 2017.
18. N. Murru, M. Abrate, S. Barbero, U. Cerruti, *Groups and monoids of Pythagorean triples connected to conics*, Open Mathematics, Vol. 15, No. 1, 1323–1331, 2017.
19. G. Airò Farulla, N. Murru, R. Rossini, *A fuzzy approach to segment touching characters*, Expert Systems with Applications, Vol. 88, 1–13, 2017.
20. N. Murru, *Linear recurrence sequences and periodicity of multidimensional continued fractions*, The Ramanujan Journal, Vol. 44, No. 1, 115–124, 2017.
21. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Linear divisibility sequences and Salem numbers*, Publicationes Mathematicae, Vol. 91, No. 1–2, 247–259, 2017.

22. E. Bellini, N. Murru, *An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics*, Finite Fields and their Applications, Vol. **39**, 179–194, 2016.
23. N. Murru, R. Rossini, *A Bayesian approach for initialization of weights in backpropagation neural net with application to character recognition*, Neurocomputing, Vol. **193**, 92–105, 2016.
24. G. Airò Farulla, T. Armano, A. Capietto, N. Murru, R. Rossini, *Artificial neural networks and fuzzy logic for recognizing alphabet characters and mathematical symbols*, Lecture Notes in Computer Science, Vol. **9759**, Computers Helping People with Special Needs, 7–14, 2016.
25. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *The biharmonic mean*, Mathematical Reports, Vol. **18**, No. **4**, 2016.
26. N. Murru, *On the periodic writing of cubic irrationals and a generalization of Rédei functions*, International Journal of Number Theory, Vol. **11**, No. **3**, 779–799, 2015.
27. S. Chiaradonna, F. Di Giandomenico, N. Murru *On enhancing efficiency and accuracy of particle swarm optimization algorithms*, International Journal of Innovative Computing, Information and Control, Vol. **11**, No. **4**, 1165–1190, 2015.
28. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Polynomial sequences on quadratic curves*, Integers: the Electronic Journal of Combinatorial Number Theory, Vol. **15**, Article **A38**, 2015.
29. N. Murru, *Periodic representations and rational approximations for quadratic irrationalities by means of generalized Rédei rational functions*, Journal of Algebra, Number Theory and Applications, Vol. **33**, No. **2**, 141–154, 2014.
30. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Colored compositions, Invert operator and elegant compositions with the "black tie"*, Discrete Mathematics, Vol. **335**, 1–7, 2014.
31. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Writing  $\pi$  as sum of arctangents with linear recurrent sequences, Golden mean and Lucas numbers*, International Journal of Number Theory, Vol. **10**, No. **5**, doi: 10.1142/S1793042114500286, 1309–1319, 2014.
32. S. Barbero, U. Cerruti, N. Murru, M. Abrate *Identities involving zeros of Ramanujan and Shanks cubic polynomials*, Journal of Integer Sequences, Vol. **16**, Article **13.8.1**, 2013.
33. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Periodic representations and rational approximations of square roots*, Journal of Approximation Theory, Vol. **175**, 83–90, 2013.
34. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Construction and composition of rooted trees via descent functions*, Algebra, Article ID 543913, 2013.
35. G. E. D’Errico, N. Murru, *Fuzzy treatment of candidate outliers in measurements*, Advances in Fuzzy Systems, Article ID **783843**, doi:10.1155/2012/783843, 2012.
36. G. E. D’Errico, N. Murru, *An algorithm for concurrent estimation of time-varying quantities*, Measurement Science and Technology, Vol. **23**, Article **045008**, 2012.
37. G. E. D’Errico, N. Murru, *In-Process Estimation of Time-Variant Contingently Correlated Measurands*, International Journal of Metrology and Quality Engineering, Vol. **3**, No. **3**, 137–143, 2012.

38. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Periodic representations for cubic irrationalities*, The Fibonacci Quarterly, Vol. **50**, No. **3**, 252–264, 2012.
39. S. Barbero, U. Cerruti, N. Murru, *Squaring the magic squares of order 4*, Journal of Algebra, Number Theory: Advances and Applications, Vol. **7**, No. **1**, 31–46, 2012.
40. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Accelerations of generalized Fibonacci sequences*, The Fibonacci Quarterly, Vol. **49**, 255–266, 2011.
41. M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Fixed sequences for a generalization of the Binomial interpolated operator and for some other operators*, Journal of Integer Sequences, Vol. **14**, Article **11.8.1**, 2011.
42. S. Barbero, U. Cerruti, N. Murru, *Solving the Pell equation via Rédei rational functions*, The Fibonacci Quarterly, Vol. **48**, 348–357, 2010.
43. S. Barbero, U. Cerruti, N. Murru, *Generalized Rédei rational functions and rational approximations over conics*, International Journal of Pure and Applied Mathematics, Vol. **64**, 305–316, 2010.
44. S. Barbero, U. Cerruti, N. Murru, *Transforming recurrent sequences by using Binomial and Invert operators*, Journal of Integer Sequences, Vol. **13**, Article **10.7.7**, 2010.
45. S. Barbero, U. Cerruti, N. Murru, *A generalization of the Binomial interpolated operator and its action on linear recurrent sequences*, Journal of Integer Sequences, Vol. **13**, Article **10.9.7**, 2010.

## Preprint

1. S. Barbero, U. Cerruti, N. Murru, *Periodic representations for quadratic irrationalities in the field of  $p$ -adic numbers*, Submitted to Mathematics of Computation.
2. A. Di Scala, N. Murru, C. Sanna, *Lucas pseudoprimes and the Pell conic*, Submitted to Discrete Mathematics and Theoretical Computer Science.
3. N. Murru, L. Terracini, *Simultaneous approximations to  $p$ -adic numbers and algebraic dependence via multidimensional continued fractions*, Submitted to The Ramanujan Journal.
4. E. Bellini, A. Di Scala, M. Elia, N. Murru, *Point-groups over singular cubics*, Submitted to Applied Mathematics and Computation.
5. S. Barbero, U. Cerruti, N. Murru, *Periodic representations and approximations of  $p$ -adic numbers via continued fractions*, Submitted to Experimental Mathematics.
6. D. Bazzanella, A. Di Scala, S. Dutto, N. Murru, *Primality tests, linear recurrent sequences and the Pell equation*, Submitted to Experimental Mathematics.
7. E. Bellini, C. Marcolla, N. Murru, *On the decoding of 1-Fibonacci error correcting codes*, Submitted to Discrete Mathematics, Algorithms and Applications.

## Brevetti

**Titolo:** Method for the management of virtual objects corresponding to real objects, corresponding system and computer program product.

**Inventori Designati:** Marco Abrate, Stefano Barbero, Umberto Cerruti, Nadir Murru, Amedeo Perna.

**International Application No.:** PCT/IB2016/050202

**Pub. No.:** WO/2016/113709

Per ulteriori informazioni: <https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2016113709>.

## Convegni

- *The group's structure of conics with application to public-key cryptography and primality tests*, talk su invito presso Crypto Conference 2020 - Torino, Politecnico di Torino, 28–29 Maggio 2020.
- *RSA cryptanalysis and factoring: a survey*, talk su invito presso The Italian Conference on CyberSecurity (ITASEC 2020), Ancona, Italia, 4 Febbraio 2020.
- *Axessibility 2.0: creating tagged PDF documents with accessible formulae*, talk presso GuIT (gruppo utilizzatori italiani LaTeX) meeting, Torino, Italia, 26 Ottobre 2019.
- *Applicazioni di teoria dei numeri alla crittografia*, talk su invito presso De Cifris incontra Torino: un convegno su crittografia e dintorni, Politecnico e Università di Torino, 14 Ottobre 2019.
- *The Pell conic in cryptography*, talk su invito presso Workshop di Algebra e Crittografia, Dipartimento di Scienze dell'Informazione e Matematica, Università dell'Aquila, 10–11 Ottobre 2019.
- *A multi-factor RSA-like scheme with fast decryption based on Rédei rational functions over the Pell hyperbola*, talk presso The 3rd International Conference on Numerical Computations: Theory and Algorithms, Crotone, 15–22 Giugno 2019.
- *Crittografia, l'arte di nascondere*, talk su invito presso IX Festa di Scienza e Filosofia, Foligno, 13 Aprile 2019.
- *Convergence and periodicity of multidimensional continued fractions*, talk su invito presso Giornate INDAM di Teoria dei Numeri, Genova, 18–19 Dicembre 2017.
- *A novel RSA-like cryptosystem based on a product related to the cubic Pell equation and Rédei rational functions*, talk presso Number Theory Methods in Cryptology Conference, Varsavia, Polonia, 11–13 Settembre 2017.
- *Il LaTeX come soluzione al problema dell'accesso a testi con formule da parte di disabili visivi*, talk presso GuIT (gruppo utilizzatori italiani LaTeX) meeting, Brescia, Italia, 29 Ottobre 2016.
- *Artificial neural networks and fuzzy logic for recognizing alphabet characters and mathematical symbols*, talk presso 15th International Conference on Computers Helping People with Special Needs, Linz, Austria, 13–15 Luglio 2016.
- *A public key cryptosystem based on Rédei rational functions and conics*, poster su invito presso Fifth Welcome home workshop, Dipartimento di Matematica, Università di Torino, Italy, 21–22 Dicembre 2015.
- *Periodic representations and simultaneous approximations of cubic irrationalities*, talk presso Third Italian Number Theory Meeting, Pisa, Italy, 21–24 Settembre 2015.
- *A public-key cryptosystem based on product of points over conics*, poster presso 13-th Conference Effective Methods in Algebraic Geometry (MEGA), Trento, Italy, 15–19 Giugno 2015.
- *Accessibilità e inclusività della matematica in percorsi formativi scolastici e aziendali*, talk presso Convegno Didamatica 2015, 29-esima edizione, Genova, Italy, 15–17 Aprile 2015.

- *An overview on ICT for the accessibility of scientific texts by visually impaired students*, talk presso Convegno Nazionale SIREM/SIE–L 2014, Perugia, Italy, November 13–15, 2014. Atti del convegno, Apertura e flessibilità nella scuola superiore: oltre l’e-learning?, Curatori: Floriana Falcinelli, Tommaso Minerva, Pier Cesare Rivoltella, pp. 119–122, 2014.
- *Sequences of points over conics by means of generalized Rédei functions*, talk su invito presso Mini–Workshop on Coding Theory and Cryptography, Dipartimento di Matematica, Torino, Italy, October 13–14, 2014.

## Seminari

- *Some advancements in number theory and cryptography*, seminario su invito presso il Dipartimento di Matematica G. Peano, Università di Torino, 19 Settembre 2019.
- *An introduction to lattice-based post-quantum cryptography*, seminario su invito presso il Corso di Laurea Triennale, Insegnamento ‘Teoria dell’informazione e della trasmissione’, Dipartimento di Informatica, Università degli Studi di Milano, 31 Maggio 2019.
- *I codici post-quantum basati sui reticoli*, seminario su invito presso PQCifris 2019, evento sulla crittografia post quantum organizzato dall’associazione nazionale di crittografia De Componendis Cifris e CONSOB, Roma, 9 Maggio 2019.
- *Pseudorandom sequences*, seminario su invito presso il Corso di Laurea Magistrale, Insegnamento ‘Crittografia’, Dipartimento di Scienze Matematiche, Politecnico di Torino, 27 Marzo 2019.
- *RSA-like cryptosystems with conics*, seminario su invito presso CNR di Pisa, Istituto di Scienza e Tecnologie dell’Informazione, 7 Novembre 2018.
- *Il LaTeX come soluzione al problema dell’accesso a testi con formule da parte di disabili visivi*, seminario su invito presso XII Edizione Settimana Internazionale della Ricerca, Università di Napoli, 28 Maggio 2018.
- *Introduzione alle tecnologie assistive per disabili visivi*, seminario su invito presso il corso di Laurea Triennale, Insegnamento ‘Tecnologie per la disabilità’, Politecnico di Torino, 16 Maggio 2018.
- *Aritmetica delle frazioni continue e frazioni continue multidimensionali*, seminario su invito presso Corso di Laurea Magistrale, Insegnamento ‘Algebra Computazionale’, Dipartimento di Matematica, Università di Torino, 15 Maggio 2018.
- *Introduzione alle frazioni continue*, seminario su invito presso Corso di Laurea Magistrale, Insegnamento ‘Algebra Computazionale’, Dipartimento di Matematica, Università di Torino, 14 Maggio 2018.
- *Tecnologie assistive per disabili visivi: scrittura in linea per l’accessibilità*, seminario su invito presso Corso di Perfezionamento ‘Optometria geriatrica e Ipovisione’, Università Bicocca di Milano, 8 Gennaio 2018.
- *Introduction to artificial neural networks and their applications*, seminario su invito presso CNR di Pisa, Istituto di Scienza e Tecnologie dell’Informazione, 25 Luglio 2017.
- *Introduzione alle reti neurali e loro utilizzo per lo sviluppo di tecnologie assistive per disabili visivi*, seminario su invito presso il corso di Laurea Triennale, Insegnamento ‘Tecnologie per la disabilità’, Politecnico di Torino, 26 Aprile 2017.

- *Introduzione alla logica fuzzy e applicazione alla segmentazione di caratteri*, seminario presso Seminari di Algebra e Geometria Algebrica del Dipartimento di Matematica dell'Università di Torino e del Dipartimento di Scienze Matematiche del Politecnico di Torino, 5 Ottobre 2016.
- *Introduzione alle reti neurali e loro applicazione nel riconoscimento automatico di caratteri*, seminario presso Seminari di Algebra e Geometria Algebrica del Dipartimento di Matematica dell'Università di Torino e del Dipartimento di Scienze Matematiche del Politecnico di Torino, 10 Giugno 2015.
- *Disabilità e Nuove Tecnologie*, seminario su invito presso Master di I livello in Didattica e psicopedagogia per alunni con disabilità sensoriali, Università degli Studi di Torino, Italy, 13 February 2015.

## Organizzazione Convegni

**Co-organizzatore** dei cicli di seminari *Seminario di Teoria dei Numeri*. Per informazioni:

<https://sites.google.com/unito.it/teoriadeinumeri/>

**24–25/10/2019 Co-organizzatore** del convegno *4th Number Theory Meeting – Torino* presso il Dipartimento di Matematica G. Peano, Università di Torino. Per informazioni:

[http://ntmeeting.polito.it/4th\\_number\\_theory\\_meeting](http://ntmeeting.polito.it/4th_number_theory_meeting).

**14/10/2019 Membro del Comitato Organizzatore** dell'evento 'De Cifris incontra Torino: un convegno su crittografia e dintorni', organizzato dai Dipartimenti di Matematica del Politecnico e dell'Università di Torino. Per informazioni:

[https://crypto.polito.it/eventi/evento\\_la\\_de\\_cifris\\_incontra\\_torino](https://crypto.polito.it/eventi/evento_la_de_cifris_incontra_torino).

**Chairman** presso The 3rd International Conference on Numerical Computations: Theory and Algorithms, Sessione: Pythagorean stream 'Numbers, Algorithms and Applications' (part 1), Crotona, 15–22 Giugno 2019.

**Membro del Comitato Organizzatore** dei cicli di seminari *De Cifris Augustae Taurinorum*, volti a presentare risultati di ricerca nell'ambito della crittografia e applicazioni in ambito industriale/aziendale, anni 2019 e 2020. Per informazioni:

<http://www.decifris.it/seminarilocali/decifrisaugustaetaurinorum.html>

**11–13/02/2019 Membro del Technical Program Committee** dell'*International Conference on Wireless, Intelligent and Distributed Environment for COMMunication* (WIDECOM 2019) presso Università di Milano. Per informazioni:

<http://www.widecomconference.org>.

**15–16/10/2018 Co-organizzatore** del convegno *3rd Number Theory Meeting – Torino* presso il Dipartimento di Matematica G. Peano, Università di Torino. Per informazioni:

[http://ntmeeting.polito.it/3rd\\_Number\\_Theory\\_Meeting.html](http://ntmeeting.polito.it/3rd_Number_Theory_Meeting.html).

**26–27/10/2017 Co-organizzatore** del convegno *2nd Number Theory Meeting – Torino* presso Politecnico di Torino. Per informazioni:

[http://ntmeeting.polito.it/2nd\\_Number\\_Theory\\_Meeting.html](http://ntmeeting.polito.it/2nd_Number_Theory_Meeting.html).

**18/4/2017 Co-organizzatore** del workshop *Uso di strumenti e tecnologie assistive per disabili visivi* presso il Dipartimento di Matematica G. Peano, Università di Torino. Per informazioni:

<http://www.dipmatematica.unito.it/do/home.pl/View?doc=miniworkdis.html>.

4/11/2016 **Organizzatore** del convegno *1st Number Theory Meeting – Torino* presso il Dipartimento di Matematica G. Peano, Università di Torino. Per informazioni: <http://www.dipmatematica.unito.it/do/home.pl/View?doc=teorianumeri.html> e [http://ntmeeting.polito.it/1st\\_Number\\_Theory\\_Meeting.html](http://ntmeeting.polito.it/1st_Number_Theory_Meeting.html).

## Attività didattica

- A.A. 2019–2020 *Aspetti Algebrici della Crittografia*, Corso di Dottorato in Ingegneria e Matematica, presso Politecnico e Università di Torino, titolare del corso.
- A.A. 2019–2020 *Codici Correttori e Crittografia*, Corso di Laurea Triennale in Matematica, presso Università di Torino, co-titolare del corso.
- A.A. 2019–2020 *Matematica Discreta e Logica*, Corso di Laurea Triennale in Informatica, presso Università di Torino, co-titolare del corso.
- A.A. 2019–2020 *Master di I livello in Cybersecurity* organizzato dal Dipartimento di Informatica dell'Università di Torino, 10 ore di lezione su fondamenti di algebra per la crittografia.
- A.A. 2018–2019 *Algebra I*, Corso di Laurea Triennale in Matematica, presso Università di Torino, co-titolare del corso.
- A.A. 2018–2019 *Matematica e biostatistica con applicazioni informatiche*, Corso di Laurea Triennale in Biotecnologie, presso Università di Torino, co-titolare del corso.
- A.A. 2018–2019 *Analisi I*, Corso di Laurea Triennale in Ingegneria, presso Politecnico di Torino, esercitatore.
- A.A. 2018–2019 *Uso scientifico e inclusivo di una moderna stampante 3D*, Corso di Laurea in Matematica, presso Università di Torino, Attività laboratoriale OpenLab, Coordinatore. Per informazioni <https://www.matematica.unito.it/do/didattica.pl/View?doc=OpenLab.html>
- A.A. 2017–2018 *Introduzione alla crittografia*, Corso di Dottorato in Ingegneria e Matematica, presso Politecnico e Università di Torino, co-titolare del corso.
- A.A. 2017–2018 *Analisi I*, Corso di Laurea Triennale in Ingegneria, presso Politecnico di Torino, esercitatore.
- A.A. 2016–2017 *Matematica Discreta e Logica*, Corso di Laurea Triennale in Informatica, presso Università di Torino, tutor in aula.
- A.A. 2010–2011 *Geometria*, Corso di Laurea Triennale in Ingegneria, presso Politecnico di Torino, esercitatore.

## Tesi di Laurea

- A.A. 2018–2019 **Relatore** della tesi di laurea triennale in Matematica *Teoremi sulla distribuzione dei numeri primi*, Università di Torino, Tesista: Dott. Cristian Alaimo.
- A.A. 2018–2019 **Relatore** della tesi di laurea magistrale in Matematica *On the solutions of the Pell equation*, Università di Torino, Tesista: Dott. Sergio Polese.
- A.A. 2018–2019 **Correlatore** della tesi di laurea magistrale in Ingegneria Matematica *Codici correttori e loro applicazioni alla crittografia post-quantum*, Politecnico di Torino, Relatore: Prof. Danilo Bazzanella, Tesista: Dott. Mario Tamietti.

- A.A. 2017–2018 **Relatore** della tesi di laurea triennale in Ingegneria Matematica *Analisi del problema della fattorizzazione di numeri interi nella crittografia a chiave pubblica*, Politecnico di Torino, Tesista: Dott.ssa Alice Morano.
- A.A. 2017–2018 **Correlatore** della tesi di laurea magistrale in Matematica *On a coding theory based on Fibonacci numbers and linear recurrent sequences*, Università di Torino, Relatore: Dott.ssa Cristina Bertone. Tesista: Dott.ssa Silvia Cotignoli.
- A.A. 2017–2018 **Correlatore** della tesi di laurea magistrale in Matematica *Ultrametrics and fuzzy similarities relations*, Università di Torino, Relatore: Prof. Umberto Cerruti. Tesista: Dott. Giulio Di Vincenzo.
- A.A. 2017–2018 **Correlatore** della tesi di laurea magistrale in Ingegneria Informatica *Exploiting Parallel Neural Networks for Automatic Recognition of Characters and Mathematical Symbols*, Politecnico di Torino. Relatore: Prof. Paolo Prinetto, Tesista: Dott. Yu Ye.
- A.A. 2016–2017 **Correlatore** della tesi di laurea magistrale in Matematica *Cellular evolution: a symbiosis between cellular automata and genetic algorithms*, Università di Torino, Relatore: Prof. Umberto Cerruti. Tesista: Dott. Simone Dutto.
- A.A. 2016–2017 **Correlatore** della tesi di laurea magistrale in Scienza in Meccatronica *Experimental validation of backpropagation algorithm for pattern recognition*, Politecnico di Torino. Relatore: Prof. Paolo Prinetto, Tesista: Dott Sajjad Ali.
- A.A. 2015–2016 **Correlatore** della tesi di laurea magistrale in Matematica *Applicazione delle frazioni continue alla crittografia: attacchi al sistema RSA e generazione di sequenze pseudocasuali*, Università di Torino. Relatore: Prof. Umberto Cerruti. Tesista: Dott.ssa Stéphanie Vuillermoz.

## Altri Titoli

**Referee** per le seguenti riviste: *Advances in Applied Clifford Algebras*; *Mediterranean Journal of Mathematics*; *Journal of Integer Sequences*; *Applicable Algebra in Engineering, Communication and Computing*; *Rendiconti del Circolo Matematico di Palermo, Series 2*; *Rendiconti del Seminario Matematico*; *Expert Systems with Applications*; *Symmetry*; *Journal of Information Security and Applications*; *Measurement*; *International Journal of Disaster Risk Reduction*; *International Journal of Information Systems and Change Management*; *Mathematical Reviews (MathSciNet) Database*.

**Editor** della rivista *Journal of Progressive Research in Mathematics* (ISSN: 2395–0218), dal 01/04/2015.

**Guest editor** della rivista *Mathematics* (ISSN: 2227-7390) per la Special Issue *Algebra and Number Theory*.

**Curatore** del volume ‘100 tesi di Crittografia e Codici in Italia 2008-2017’, all’interno Book Series Crittografia, Editore Aracne. Per ulteriori informazioni:  
<http://www.aracneeditrice.it/index.php/publicazione.html?item=9788825527520>.

**Membro** della Commissione giudicatrice per l’assegnazione di n.1 assegni di ricerca ‘post-dottorale’ categoria B dal titolo ‘Crittoanalisi di cifrari ARX’, presso Dipartimento di Scienze Matematiche del Politecnico di Torino, Anno 2019.

**Membro** della Commissione giudicatrice per l’assegnazione di n.1 assegni di ricerca ‘post-dottorale’ categoria B dal titolo ‘Ricorrenze lineari in teoria dei numeri con applicazioni alla crittografia’, presso Dipartimento di Scienze Matematiche del Politecnico di Torino, Anno 2020.

**Membro** di Commissioni giudicatrici per l'assegnazione di Borse di Ricerca di varia natura (e.g., borsa di ricerca nell'ambito della crittografia, borsa di ricerca nell'ambito delle tecnologie assistive per persone con disabilità), presso il Dipartimento di Matematica dell'Università di Torino e il Dipartimento di Scienze Matematiche del Politecnico di Torino.

## Breve Descrizione Attività di Ricerca

La mia attività di ricerca si svolge nell'ambito della **Teoria dei Numeri** e delle sue **applicazioni** trattando temi come crittografia e codici, strutture algebriche e punti razionali su curve, frazioni continue e loro generalizzazioni, trasformazioni algebriche e combinatoriali di sequenze in anelli, approssimazione diofantina. Alcuni miei risultati riguardano lo studio di rappresentazioni periodiche di irrazionalità algebriche, connesse al problema di Hermite (problema aperto di teoria dei numeri dal 1839). In particolare, ho determinato la **prima rappresentazione periodica per ogni irrazionalità cubica** per mezzo di frazioni continue multidimensionali, rispondendo al problema di fornire una scrittura periodica attraverso successioni di razionali o interi per queste irrazionalità. Inoltre, ho fornito un **criterio per la periodicità dell'algoritmo di Jacobi–Perron** e iniziato lo studio di tali oggetti nel campo dei numeri  $p$ -adici. Altre mie ricerche hanno riguardato lo studio di operazioni su coniche, che forniscono loro una struttura di gruppo, e successioni di punti su di esse. Tali studi hanno portato alla costruzione di un **originale sistema crittografico a chiave pubblica** stile RSA con una maggiore efficienza nei tempi di decriptazione e maggiore sicurezza in scenari in cui RSA risulta vulnerabile. Ho iniziato inoltre lo studio di codici correttori d'errore e la loro applicazione nello sviluppo di sistemi crittografici post-quantum. L'attività di ricerca che ho svolto presso INRIM e CNR è stata finalizzata all'**applicazione di strumenti di algebra computazionale**. In particolare presso l'INRIM ho studiato e utilizzato la logica fuzzy per creare un metodo per il trattamento di misure "outlier" inserito in un algoritmo per la stima delle misure di oggetti dimensionali. Presso il CNR mi sono dedicato allo studio di reti di distribuzione elettrica ed in particolare alla loro ottimizzazione e protezione informatica. In questo contesto ho studiato tecniche fuzzy in algoritmi di **ottimizzazione non lineare** e **sistemi crittografici a chiave pubblica**.

## Ulteriore Attività di Ricerca e di Terza missione

Ho svolto varia attività di terza missione per conto dell'Università di Torino dal 2014 ad oggi:

- Corsi di formazione su tecnologie assistive per il supporto a persone con disabilità presso numerosi enti locali (quali Biblioteca Italiana per i Ciechi, Comune di Torino, Camera di Commercio di Torino, Centro Territoriale di Supporto di Torino, Unione Italiana Ciechi).
- Partecipazione a manifestazioni di diffusione delle tecnologie quali: "Handimatica" - presso Istituto Aldini Valeriani Sirani, Bologna, Italia - Dicembre 2017; "Abilitando, Dove la tecnologia incontra la disabilità", presso complesso monumentale di S. Croce a Bosco Marengo, Alessandria, Italia - Ottobre 2017 e Ottobre 2019.
- Referente per il progetto 'Potenziare l'occupabilità di persone con disabilità visiva' in collaborazione con la Città Metropolitana di Torino (Fondo Regionale Disabili) e l'I.Ri.Fo.R. Nell'ambito di tale progetto è stato svolto un corso di 14 ore rivolto a disabili visivi per potenziarne le competenze informatiche indirizzate al mondo del lavoro. Inoltre, sono stati attivati 9 tirocini retribuiti di tre mesi presso alcune aziende torinesi.

- Referente per il progetto D.A.P.A.R.I. (Disabilità in Azienda, Professionalità Avanzata, Ricerca e Integrazione) che si pone l'obiettivo di accompagnare le persone disabili, in particolare cieche o ipovedenti, dalla loro formazione scolastica e universitaria al mondo del lavoro.
- Sviluppo del pacchetto LaTeX 'axessibility.sty', per la creazione di documenti PDF con contenuti scientifici accessibili a persone con disabilità visiva. Per ulteriori informazioni: <https://ctan.org/pkg/axessibility>.
- Attività di formazione del Dipartimento di Matematica di Torino in collaborazione con la Scuola di Formazione Scientifica Luigi Lagrange presso i Campus 'Matematica, Fisica, Astrofisica e Nuove Tecnologie' con corsi relativi ai seguenti argomenti: Teoria dei Numeri, Algoritmi genetici e automi cellulari, Reti neurali artificiali, Crittografia, Codici correttori.