Danilo Bazzanella

Curriculum vitae

Position

Aggregate Professor at the Department of Mathematical Science of Politecnico di Torino, Scientific Sector MAT/02 - Algebra.

Web site: https://crypto.polito.it/danilo_bazzanella

Education

- Master's degree with honors in Mathematics (Università di Genova 1989) with the thesis: *Codici a Chiave Pubblica ed Algoritmi di Fattorizzazione* (tutor Prof. A. Perelli).

- Ph. D. in Mathematics (Università di Genova, Università di Torino, Politecnico di Torino 1995) with the thesis: *Metodo delle Coppie di Esponenti e applicazioni* (tutor Prof. A. Perelli).

Teaching activities

- I was and still I am in charge of numerous teaching courses for the bachelor's degree, for the master's degree and for the Ph. D. program, including Cryptography, Blockchain and Cryptoeconomy, Mathematical Analysis 1, Mathematical Analysis 2, Analytic Number Theory, Complex Analysis, Mathematical Methods for Engineering and Theory of Probability and Statistics.

- I was tutor of numerous theses in the fields of Cryptography and Number Theory.

- I was and still I am supervisor of various Ph. D. students: Carlo Sanna (31° cycle - Title of the thesis: *Arithmetic Properties of Linear Recurrences and Other Topics in Number Theory*), Simone Dutto (34° cycle), Guglielmo Morgari and Andrea Gangemi (35° cycle), Matteo Rossi, Gessica Alecci, Giuseppe D'Alconzo and Edoardo Signorini (36° cycle).

- I was a member of the selection committee for the admission to the Ph. D. program in Pure and Applied Mathematics of Politecnico di Torino e Università di Torino.

- Teaching Books: *Serie di Funzioni e Trasformate*, D. Bazzanella, P. Boieri, L. Caire, A. Tabacco, CLUT (2001).

Management activities

- I was a member of the Academic Senate of Politecnico di Torino (2011-2012), as a representative of assistant professors. During my tenure I was a member of the Research Strategy Commission and the Commission for the Statute of the University.

- I was a member of the Board of Governors (2013-2020). During my tenure I was a member of the Strategic Plan Commission, Student Project and University Fees Commission, Budget Commission, Commission for Monitoring Researchers and Fellows, Staff Planning Commission, Interdepartmental Centers Commission, Commission for Teaching Strategies, Commission for Research Strategies and the General Regulation Commission.

- I am the coordinator of the Commission for the Website of the Department of Mathematical Sciences of Politecnico di Torino.

- I am the head of the research group CrypTO (https://crypto.polito.it/en), the interuniversity research group of Cryptography and Number Theory of the Department of Mathematical Sciences of Politecnico di Torino and the Department of Mathematics of Università di Torino. The CrypTO group is made up of 5 professors, 3 research fellows and 7 Ph. D. students. The activities of the group concern teaching (courses for the master's degree, for the Ph. D., thesis, student teams...), research (Symmetric and Asymmetric Cryptography, Post-Quantum Cryptography, Cryptanalysis, Blockchain, Number Theory...), dissemination (series of seminars and conferences) and technology transfer (projects in collaboration with technology companies).

Scientific activities

My research field is Number Theory and its application to Cryptography. In the early years my research was mainly oriented towards the distribution of prime numbers and additive diophantine problems with primes. In particular I started my research activity with the study of the estimation of exponential sums, a problem closely linked to various questions about the distribution of prime numbers, to which I have dedicated my Ph. D. thesis.

Later on I became interested in the study of irregularities about the distribution of prime numbers, in particular I studied the exceptional set of the distribution of primes in short intervals, say, the set of the x in [X, 2X] such that the interval [x, x + H(x)] does not contain the expected number of primes. This study led to a paper titled *The exceptional set for the number of primes in short intervals* J. Number Theory 80 (2000), 109-124, written in collaboration with Prof. A. Perelli (Univ. of Genova).

At the same time, I started the collaboration with Prof. A. Languasco on the study of the distribution of Goldbach numbers, which led to the paper *On the asymptotic formula for Goldbach numbers in short intervals* Stud. Math Sci. Hung. 36 (2000) No.1-2, 185-199, that improves the previous best known result due to H. Mikawa dating back to 1993.

Next I became interested in the classical conjecture about the existence of a prime number between two consecutive squares. The proof of this conjecture is quite out of reach at present, even under the assumption of the Riemann Hypothesis. At that time the best known result was still Goldston's 1990 result. I improved this classical result in *Primes Between consecutive squares* Arch. Math. 75th (2000), 29-34, and then I generalized my results considering intervals between two consecutive powers in the form $[n^a, (n+1)^a]$.

Still on the distribution of primes in short intervals I improved a very famous result of A. E. Ingham, published in 1937, in which he showed that all intervals of the form $[x, x + x^a]$ contain the expected number of primes for a>1/2, under the assumption of the Lindelöf hypothesis. I improved the result of Ingham the first time in 2008 and then in 2011.

Another topic that I treated was the distribution of prime numbers in very short intervals. Thanks to a new bound for the k-th moments of primes in intervals of logarithmic length obtained in collaboration with A. Languasco and A. Zaccagnini, we were able to improve the best known result of that time (Cheer and Goldston 1987). The results on this subject were published in 2010 on Transactions of the American Mathematical Society.

More recently I have been interested in studying the distribution of the divisor function and I obtained a generalization of some classical results of Jutila.

Next, I worked to deepen my knowledge about the general structure of the exceptional sets, from the point of view of Descriptive Set Theory and this work led to an article in collaboration with R. Camerlo.

Later on I was fascinated by the surprising relationship between the integrals of polynomials with integer coefficients and the distribution of primes, as discovered by Gelfond-Shnirelman-Nair, see M. Nair *A new method in elementary prime number theory*, J. London Math. Soc., (2), 25 (1982), 385-391. I have approached the problem with both algebraic and analytical methods and I obtained some results which I published in three articles.

In recent years I have shifted my attention to the applications of Number Theory to Cryptography and in particular to Post-Quantum Cryptography and Cryptanalysis. The first research topic in which I became interested was primality tests, a subject closely linked to the construction of many cryptosystems. Following this subject, my collaborative paper with A. Di Scala, S. Dutto, and N. Murru *"Primality tests, linear recurrent sequences and the Pell equation"* was recently accepted for publication in The Ramanujan Journal.

I am a member of UMI (Italian Mathematical Union) and I am part of the “Cryptography and codes” UMI group (https://umi.dm.unibo.it/gruppi-umi-2/gruppo-umi-crittografia-e-codici/).

I am a referee of various Number Theory and Cryptography Journals.

Research projects

- Name of the project: *Crittografia Post-Quantum per applicazioni cloud*
Company: Telsy SpA (TIM Group) - https://www.telsy.com/

- Name of the project: *Cryptanalysis of ARX ciphers*
Company: DarkMatter - https://www.darkmatter.ae

- Name of the project: *Cryptanalysis of multivariate-based cryptosystems and Machine learning applied to cryptanalysis*
Company: TII - Technology Innovation Institute - https://tii.ae

I have research and dissemination collaborations with various companies: Telsy SpA, Quadrans Foundation, Foodchain, INRiM - Istituto Nazionale di Ricerca Metrologica, Young Platform… (https://crypto.polito.it/en/partners).

I was a member of the following PRIN projects:

- Geometria Algebrica - Coordinator: Pedrini C. (1998-2000)
- Funzioni L e Numeri Primi - Coordinator: Perelli A. (2000-2003)
- Funzioni L e Problemi Diofantei Additivi - Coordinator: Perelli A. (2002-2004)
- Funzioni L e Problemi Diofantei Additivi - Coordinator: Perelli A. (2004-2006)
- Teoria Analitica dei Numeri e Funzioni L - Coordinator: Zannier U. (2007-2009)
- Funzioni L e Problemi Analitici in Teoria dei Numeri - Coordinator: Zannier U. (2010-2012)
- Geometria Algebrica Aritmetica e Teoria dei Numeri - Coordinator: Chiarellotto B. (2013-2016)

Dissemination

- Conference “*CrypTO Conference 2021*” (https://crypto.polito.it/conference).

- Series of seminars "*CRYPTOGRAPHY: From Theory to Applications*", in collaboration with Telsy SPA, a company of the TIM group specialized in cybersecurity (https://crypto.polito.it/en/eventi/crittografia_dalla_teoria_alle_applicazioni).

- Series of seminars “*De Cifris Augustae Taurinorum*”, in collaboration with the national cryptography association De Componendis Cifris, Telsy SpA and Quadrans Foundation (https://crypto.polito.it/en/eventi/seminari_di_de_cifris_augustae_taurinorum).

- Periodic conferences named “*Number Theory Meeting”* (http://ntmeeting.polito.it), dedicated to number theory and its applications, in years 2016, 2017, 2018 and 2019. Next event scheduled for 2021.

- I was one of the organizers of the “*Second Symposium on Analytic Number Theory*” - Cetraro, 8-12 July 2019 (https://www.dima.unige.it/ant/symposium/).

Pubblications

- **D. Bazzanella** *Codici a Chiave Pubblica ed Algoritmi di Fattorizzazione*, Master’s Degree Thesis (1989 Università di Genova) - Tutor: Prof. A. Perelli.
- **D. Bazzanella** *Primes in almost all short intervals*, Boll. U.M.I.(7), 9-B (1995), 233-249.
- **D. Bazzanella** *Il Metodo delle Coppie di Esponenti ed Applicazioni*, Ph. D. Thesis (1995 Università di Genova) - Tutor: Prof. A. Perelli.
- **D. Bazzanella, A. Perelli** *The exceptional set for the number of primes in short intervals*, Journal of Number Theory 80 (2000) n.1, 109-124.
- **D. Bazzanella, A. Languasco** *On the asymptotic formula for Goldbach numbers in short intervals*, Stud. Sci. Math.

Hung. 36 (2000) n.1-2, 185-199.

- **D. Bazzanella** *Primes in almost all short intervals II*, Boll. U.M.I. (8) 3-B (2000), 717-726.
- **D. Bazzanella** *Primes between consecutive squares*, Arch. Math. (Basel) 75 (2000) n.1, 29-34.
- **D. Bazzanella, P. Boieri, L. Caire, A. Tabacco** *Serie di Funzioni e trasformate,* CLUT (2001).
- **D. Bazzanella** *Prime numbers between squares*, Riv. Mat. Univ. Parma (7) 3* (2004), 159-164.
- **D. Bazzanella** *The exceptional set for the distribution of primes between consecutive powers*, Acta Math. Hungar. 116 (3) (2007), 197-207.
- **D. Bazzanella** *A note on primes in short intervals*, Arch. Math. (Basel) 91 (2008) n. 2, 131-135.
- **D. Bazzanella** *Primes between consecutive powers*, Rocky Mountain J. Math. 39 (2009), n. 2, 413-421.
- **D. Bazzanella** *A note on primes between consecutive powers*, Rend. Semin. Mat. Univ. Padova 121 (2009) 223-231.
- **D. Bazzanella** *Prime numbers in intervals starting at a fixed power of the integers*, J. Australian Math. Soc. 87 (2009) 83-99.
- **D. Bazzanella, A. Languasco, A. Zaccagnini** *Prime numbers in logarithmic intervals*, Transactions of the American Mathematical Society 362 (2010), n. 5, 2667-2684.
- **D. Bazzanella** *Two conditional results about primes in short intervals*, Int. J. Number Theory 7 (2011), n. 7, 1753-1759.
- **D. Bazzanella** *On the divisor function in short intervals*, Arch. Math. (Basel) 97 (2011), n. 5, 453-458.
- **D. Bazzanella** *Some conditional results on primes between consecutive squares*, Funct. Approx. Comment. Math. 45, n. 2 (2011), 255-263.
- **D. Bazzanella** *Primes between consecutive squares and the Lindelöf hypothesis*, Period. Math. Hungar. 66, n. 1 (2013), 111-117.
- **D. Bazzanella** *Conditional results about primes between consecutive powers*, Riv. Mat. Univ. Parma 4, n. 1 (2013), 61-69.
- **D. Bazzanella** *A note on integer polynomials with small integrals*, Acta Math. Hungar. 141 (2013), n. 4, 320-328.
- **D. Bazzanella, R. Camerlo** *The class of the exceptional sets for a general asymptotic formula*, Funct. Approx. Comment. Math. 51 (2014), n. 2, 347-362.
- **D. Bazzanella** *A note on integer polynomials with small integrals. II*, Acta Math. Hungar. 149 (2016), n. 1, 71-81.
- **D. Bazzanella** *Integer polynomials with small integrals*, Riv. Mat. Univ. Parma, vol 7 (2016), n. 1, 165-179.
- **D. Bazzanella, C. Sanna** *Least common multiple of polynomial sequences*, Rendiconti del Seminario Matematico, vol. 78 (2020), n. 1, 21-25.
- **D. Bazzanella, A. Di Scala, S. Dutto, N. Murru** *Primality tests, linear recurrent sequences and the Pell equation*, to appear in The Ramanujan Journal (2021).