Danilo Bazzanella

Curriculum vitae

Sono nato a Imperia nel 1966. Mi sono laureato in Matematica presso l'Università di Genova (1989), ho conseguito il Dottorato di Ricerca in Matematica presso il consorzio Università di Genova, Politecnico di Torino e Università di Torino (1995) e sono ricercatore di Analisi Matematica presso il Politecnico di Torino dal 1994.

La mia tesi di laurea è stata dedicata alla crittografia (titolo "*Codici a Chiave Pubblica ed Algoritmi di Fattorizzazione*", relatore Prof. Perelli), ma poi nel proseguo della mia carriera mi sono interessato soprattutto di Teoria dei Numeri, con particolare interesse per la distribuzione dei numeri primi e la distribuzione delle più note funzioni aritmetiche. Mi sono interessato anche di alcune delle più famose congetture del settore, quali la Congettura di Goldbach e la Congettura di Legendre.

Negli ultimi anni sono tornato ad interessarmi di crittografia, dal punto di vista della ricerca, della didattica e del trasferimento tecnologico. Sono attualmente a capo del gruppo CrypTo, gruppo interateneo di Crittografia e Teoria dei Numeri - Politecnico di Torino e Università di Torino (https://crypto.polito.it).

Dal 1999 sono titolare di insegnamenti per la laurea triennale, la laurea magistrale e per il dottorato di ricerca in varie discipline tra cui: Crittografia, Teoria dei Numeri, Analisi Matematica, Analisi Complessa, Metodi Matematici per l'Ingegneria, Calcolo delle Probabilità e Statistica.

Sono impegnato a livello nazionale nella politica universitaria attraverso l'adesione, come uno dei referenti del Politecnico di Torino, alla Rete29Aprile (http://www.rete29aprile.it) e a livello locale prima come membro del Coordinamento dei Ricercatori e poi del nuovo Coordinamento PoliTo. Sono inoltre il moderatore della mailing list lista_discussione@polito.it, che dal 2010 è un luogo di discussione e di confronto all'interno del nostro Ateneo e gestore del blog http://coordinamentopolito.wordpress.com/, strumenti che utilizzo per diffondere i resoconti delle sedute degli Organi di Governo e delle commissioni di cui faccio parte nella convinzione che la trasparenza e la diffusione dell'informazione sia il necessario presupposto per un vero sistema democratico.

Dall'inizio del 2010 ho partecipato alla mobilitazione universitaria contro la riforma proposta dall'allora Ministro Gelmini e contro il progetto di destrutturazione e conseguente affossamento dell'Università pubblica, a carico di un sistema universitario notoriamente e pesantemente già molto sotto finanziato rispetto alle realtà internazionali confrontabili con il nostro paese.

Forte dell'esperienza acquisita come membro della comunità accademica del Politecnico e dell'impegno attivo nella vita politica dell'Ateneo, sono stato eletto nelle elezioni suppletive del Senato Accademico del gennaio del 2011, come rappresentante dei ricercatori.

Nel 2013 sono stato eletto nel Consiglio di Amministrazione, con un programma che metteva al centro l'Università Pubblica come sistema coordinato di comunità accademiche e come bene pubblico al servizio dei nostri studenti e della società (vedi http://tiny.cc/elezioni2013).

Con l'intento di aprire uno spazio di discussione e di proposta a livello nazionale, nel 2015 ho contribuito a curare l'organizzazione del convegno ***Ruolo Unico: una rivoluzione necessaria? – Discussione nazionale***

nella prospettiva di una riforma dello stato giuridico della docenza universitaria (vedi https://coordinamentopolito.wordpress.com/convegno/), con l'obiettivo dichiarato di favorire *"… una discussione nazionale nella prospettiva di una riforma complessiva dello stato giuridico della docenza universitaria*", a cui hanno partecipato membri del CUN, del MIUR, della CRUI… e che ha visto la presentazione di una proposta di riforma complessiva dell'Università.

Nelle 2016 mi sono nuovamente candidato alle elezioni del Consiglio di Amministrazione (http://tiny.cc/elezioni2016) e sono stato confermato nella carica, che ho ricoperto fino a fine mandato a ottobre 2020.

Negli ultimi anni ho continuato la mia attività politica nella nostra comunità accademica come componente del Coordinamento PoliTo (https://coordinamentopolito.wordpress.com), continuando le battaglie sostenute per anni in prima persona dentro gli organi di governo.

Progetti di ricerca

- Name of the project: "Crittografia Post-Quantum per applicazioni cloud"
Company: Telsy SpA (TIM Group) - https://www.telsy.com/
Duration: 9 months
Period: 2019-20

- Name of the project: "Cryptanalysis of ARX ciphers"
Company: DarkMatter - https://www.darkmatter.ae
Duration: 12 months
Period: 2019-20

- Name of the project: "Cryptanalysis of multivariate-based cryptosystems and Machine learning applied to cryptanalysis"
Company: TII - Technology Innovation Institute - https://tii.ae
Duration: 12 months
Period: 2020-21

- Name of the project: " Design and cryptanalysis of post-quantum signature schemes and Automatic methods for key recovery attacks in symmetric ciphers "
Company: TII - Technology Innovation Institute - https://tii.ae
Duration: 12 months
Period: 2021-22

- Name of the project: "Design di piattaforme decentralizzate user-rewarding"
Company: SEA Soluzioni Eco Ambientali - https://www.seaeco.it
Duration: 12 months
Period: 2021-22

Attività divulgativa

- 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 Univ. 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 Univ. 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", The Ramanujan Journal (2021).
- D. Bazzanella, S. Bettin, A. Perelli, A. Zaccagnini, "Proceedings of Second Symposium on Analytic Number Theory" Cetraro (2021).
- D. Bazzanella, T. Serra, A. Tagliaferro, "Integers in a Rational Sequence", Rendiconti Sem. Mat. Univ. Pol. Torino Vol. 79, 2021 (2021), 25-29.
- S. Barbero, D. Bazzanella, E. Bellini, "Rotational cryptanalysis in the presence of constants applied to ChaCha stream cipher", to appear on Symmetry (2022).

Danilo Bazzanella