Generalità

Dati anagrafici: nome: **LANGUASCO ALESSANDRO**, nato il 23/12/1966 ad Imperia (IM), Italia, cittadinanza: italiana.
Email: alessandro.languasco@unipd.it - Webpage: https://www.dei.unipd.it/~languasco
Scientific ID-codes: Mathematical Reviews; Zentralblatt; Orcid ID; Scopus Author ID; Web of Science Researcher ID; Researchgate page; Google Scholar profile.
Elenco dei lavori: Lista completa dei lavori; Lista completa dei lavori con gli abstracts.

Posizione accademica: Professore Associato di Analisi Matematica (MATH-03/A) presso il Dipartimento di Ingegneria dell'Informazione DEI, Università di Padova.
In precedenza, dal 26/08/1998 al 30/09/2024, sono stato afferente al Dipartimento di Matematica, Università di Padova, prima in qualità di Ricercatore Universitario a tempo Indeterminato ed in seguito come Professore Associato.

Indicatori bibliografici ASN (in data 21 settembre 2025): Numero articoli ultimi 10 anni: 27; numero citazioni ultimi 15 anni: 333; H-indice ultimi 15 anni: 12; (fonte: Reportistica IRIS-cineca[2009-2024]).

Abilitazioni ASN - Prima Fascia:
- Abilitato per il settore concorsuale 01/A3 (GSD 01/MATH-03) - Analisi Matematica, Probabilità e Statistica Matematica - Prima fascia - dal 30/06/2020 al 30/06/2032.
- Abilitato per il settore concorsuale 01/A2 (GSD 01/MATH-02) - Geometria e Algebra - Prima fascia - dal 08/07/2024 al 08/07/2036.

Lingue conosciute:
- Italiano: lingua madre;
- Inglese: livello C1 (QCER-CEFR); C1 level badge;
- Francese: sola capacità di lettura e comprensione di testi scientifici.

Awards:
2003: Distinguished Award, Hardy-Ramanujan Society.

Formazione

Formazione e carriera universitaria:
- 1989: *Laurea in Matematica*, votazione: 110/110 e lode, Università di Genova, Italia. Tesi di Teoria dei Numeri Computazionale intitolata "Codici a chiave pubblica ed algoritmi di primalità".
- 1994: *Dottorato di Ricerca in Matematica*, sede amministrativa: Università di Torino, Italia. Rilasciato dall'Università di Roma "La Sapienza" in data 21/05/1998. Dissertazione in Teoria Analitica dei Numeri intitolata "La congettura di Goldbach".
- 1998: *Ricercatore Universitario a tempo Indeterminato in Analisi Matematica (MAT/05)*, dal 26/08/1998. Conferma nel ruolo dei Ricercatori di Analisi Matematica (MAT/05), dal 26/03/2002.
- 2006: *Idoneità per il ruolo di Professore Associato di Analisi Matematica (MAT/05)*, giugno 2006. Presa di servizio quale Professore Associato di Analisi Matematica (MAT/05), primo ottobre 2006. Conferma nel ruolo di Professore Associato di Analisi Matematica (MAT/05), primo ottobre 2009.
- 2020: *Abilitato per il settore concorsuale 01/A3 (GSD 01/MATH-03) - Analisi Matematica, Probabilità e Statistica Matematica - Prima fascia* - dal 30/06/2020 al 30/06/2032.
- 2024: *Abilitato per il settore concorsuale 01/A2 (GSD 01/MATH-02) - Algebra e Geometria - Prima fascia* - dal 08/07/2024 al 08/07/2036.

Attività organizzative italiane e internazionali, commissioni

Oltre alle attività seminariali ed i congressi che si trovano in altra sezione, scrivo qui i comitati scientifici di cui ho fatto, o faccio, parte.

Comitati scientifici:
- Dal 2005 partecipo come docente e tutor all'Erasmus Mundus Master "ALGANT" (ALgebra, Geometry And Number Theory) organizzato dalle Università di Bordeaux (Francia), Parigi Sud (Parigi 11, Francia), Leiden (Paesi Bassi), Milano e Padova. Per il Dottorato di Ricerca sono presenti anche partner extra-europei: Chennai (India), Stellenbosch (Sud Africa), Montreal Concordia (Canada).
- Sono stato membro del Comitato Scientifico della mostra "Numeri. Tutto quello che conta, da zero a infinito", curatori C. Bartocci e L. Civalleri, Palazzo delle Esposizioni, Roma, 16/10/2014 - 31/05/2015.
- membro del comitato di programma (PC) della conferenza "Number Theory Methods in Cryptology" (NuTMiC), International conference Number Theory Methods in Cryptology, September 11-13, 2017, Warsaw University, Poland, proceedings pubblicati in: NuTMiC proceedings.
- Membro del comitato organizzatore del convegno "La Decifris incontra Torino"; Politecnico di Torino, 14/10/2019.

Attività organizzative e di alta formazione:

- da novembre 2007 a maggio 2011 sono stato Rappresentante dell'Area Matematica presso la Facoltà di Statistica dell'Università di Padova.
- nel 2007 la fondazione CARIPARO ha finanziato una borsa di studio di Dottorato in Matematica su un tema vincolato da me proposto.
- nel luglio 2009 sono stato nominato membro della "Commissione Assegni di Ricerca" (CAR) dell'Area 01 - Scienze Matematiche, Università di Padova per l'a.a. 2009/2010.
- nel 2010 ho curato la realizzazione della modalità on-line del Precorso di Matematica per la Facoltà di Scienze Statistiche, Università di Padova, mediante l'utilizzo del software dedicato WeBWork, link.
- da febbraio ad aprile 2011 ho fatto parte della "Commissione Nuovo Dipartimento" del Dipartimento di Matematica Pura e Applicata, Università di Padova.
- da giugno 2009 al 2011 ho fatto parte della "Commissione Pagine Web" del Dipartimento di Matematica Pura e Applicata, Università di Padova.
- nel periodo gennaio 2012-maggio 2013 sono stato il coordinatore della "Commissione Comunicazione Esterna" del Dipartimento di Matematica di cui sono stato membro fino al 2014.
- da gennaio 2008 al 30 settembre 2025 ho fatto ininterrottamente parte del Collegio dei Docenti della Scuola di Dottorato in Matematica dell'Università di Padova.

Commissioni d'esame e di concorso:
Oltre ad aver partecipato a varie commissioni d'esame di Laurea della Facoltà di Statistica e della Facoltà di Scienze MM.FF.NN. dell'Università di Padova in qualità di membro o presidente di commissione, sono stato Commissario nelle seguenti occasioni:

- Novembre 2006: Esame di Ammissione alla Scuola di Dottorato in Matematica dell'Università di Padova;
- Gennaio 2007: Esame Finale per il conseguimento del titolo di Dottore di Ricerca in Matematica dell'Università di Torino, candidato Dr. Stefano Barbero.
- Novembre 2007: Esame di Ammissione alla Scuola di Dottorato in Matematica dell'Università di Padova per il tema vincolato "Il problema del logaritmo discreto" finanziato dalla fondazione CARIPARO di Padova.
- Luglio 2009: Referente della Facoltà di Scienze Statistiche per la valutazione dei candidati alla posizione di Tutor presso tale Facoltà per l'a.a. 2009-2010.
- 2009: Valutazione dei "Progetti per Assegni di Ricerca" per l'Area 01 Matematica, Università di Padova.
- Novembre 2010: Esame Finale per il conseguimento del titolo di Dottore di Ricerca in Matematica dell'Università di Trento, candidato Dr. Luca Goldoni.
- 2014: Commissario per la conferma in ruolo di Prof. Associati (settore MAT/05; concorso 11/07/2008, Univ. Padova); nomina con decreto ministeriale del 17/12/2013.
- 2016: Componente Commissione giudicatrice per il concorso INDAM, intitolato a "Ing. Giorgio Schirillo", a n.2 posti di collaborazione ad attività di ricerca, a.a. 2016-2017.
- Aprile 2017: Esame Finale per il conseguimento del titolo di Dottore di Ricerca in Matematica dell'Università di Ferrara, Modena, Parma, Reggio Emilia, candidato Dr. Marco Cantarini.
- Marzo 2019: Esame Finale per il conseguimento del titolo di Dottore di Ricerca in Matematica dell'Università di Ferrara, Modena, Parma, Reggio Emilia, candidato Dr. Mattia Cafferata.
- Novembre 2024: Ph.D. School in Mathematics, Università di Lille (France): Esame Finale per il conseguimento del titolo di Mrs. Thi Thu Nguyen.

Didattica

Corsi innovativi proposti e creati: "Crittografia", poi **"Cryptography"**, poi confluito in **"Cybersecurity and Cryptography: principles and practices"**. Questo corso è stato da me proposto e creato nel 2003 per portare queste tematiche di applicazioni della Teoria dei Numeri algebrica, elementare, analitica e computazionale, da me conosciute a partire dal 1988, all'interno dell'offerta didattica di Padova. A parte due anni sabbatici, e fino a quando ho afferito al Dipartimento di Ingegneria dell'Informazione - DEI (01/10/2024), sono stato l'unico titolare di tale corso presso l'Ateneo padovano. Dal 2005 il corso è stato mutuato da corsi di laurea internazionali, per cui da allora l'ho insegnato in lingua inglese, e da vari corsi di Laurea in Ingegneria e Informatica. Da allora, oltre seicento studenti di varia nazionalità, europea e extraeuropea, e formazione di base (matematica, informatica, ingegneria informatica e telecomunicazioni) hanno potuto conoscere le basi scientifiche di quanto è oggi un aspetto pervasivo della nostra società. A supporto di tale corso ho scritto due testi, in collaborazione con A. Zaccagnini: "Introduzione alla Crittografia" [3] e "Manuale di Crittografia" [4] entrambi editi da Hoepli. Ho anche divulgato tali tematiche all'interno del Progetto Lauree Scientifiche per il Veneto, per il quale ho curato la pubblicazione, con A. Zaccagnini, del testo "Crittografia" [2], edito da CLEUP.

Titolarità: Sono stato titolare dei seguenti corsi:

- a.a. 1999/2000: "Analisi Matematica Uno", (modulo A), corso di Diploma in Informatica, Facoltà di Scienze MM.FF.NN., Università di Padova.

- da a.a. 2001/2002 a a.a. 2003/2004: "Matematica B (Algebra Lineare, Geometria e Calcolo Differenziale in più variabili)", corso di Laurea in Ingegneria Informatica (teledidattica), Facoltà di Ingegneria, Università di Padova.
- a.a. 2003/2004: "Teoria dei Numeri B", Laurea in Matematica, Facoltà di Scienze MM.FF.NN., Università di Padova.
- a.a. 2004/2005: "Metodi Matematici per la Statistica", Laurea Specialistica in Statistica, Facoltà di Statistica, Università di Padova.
- a.a. 2006/2007-2007/2008: "Istituzioni di Analisi Matematica 1", Laurea Triennale in Statistica, Facoltà di Statistica, Università di Padova.
- a.a. 2005/2006-2006/2007 e da a.a. 2008/2009 a a.a. 2011/2012: "Istituzioni di Analisi Matematica 2", Laurea Triennale in Statistica, Facoltà di Statistica, Università di Padova.
- da a.a. 2003/2004 a a.a. 2011/2012; da a.a. 2013/2014 a a.a. 2019/2020: "Crittografia", Laurea Specialistica (e poi Magistrale) in Matematica ed in Informatica, Erasmus Mundus Master ALGANT, Facoltà di Scienze MM.FF.NN. e poi Scuola di Scienze, Università di Padova. Dal 2005/2006 il corso è tenuto in lingua inglese. Nel 2017/2018 il corso è mutuato anche dalla Scuola di Ingegneria, Corso di Laurea Magistrale in Ingegneria per le comunicazioni multimediali e internet (ICT for internet and multimedia), classe di Ingegneria delle telecomunicazioni. In seguito è stato mutuato da Ingegneria Informatica, Scuola di Ingegneria. Confluito poi nel corso "Cybersecurity and Cryptography: principles and practices" della laurea in Cybersecurity.
- da a.a. 2020/2021 a a.a. 2021/2022: "Fondamenti di Analisi Matematica 2", Laurea Triennale in Ingegneria Meccanica, Scuola di Ingegneria, Università di Padova.
- da a.a. 2013/2014 a a.a. 2019/2020; a.a. 2022/2023: "Analisi Matematica Uno", Laurea Triennale in Ingegneria Chimica e dei Materiali, Scuola di Ingegneria, Università di Padova.
- da a.a. 2020/2021 a a.a. 2022/2023: "Cybersecurity and Cryptography: principles and practices", (in lingua inglese), Laurea Magistrale in Cybersecurity, Scuola di Scienze, Università di Padova. Mutuato dalle Lauree Magistrali in Matematica, ALGANT e Informatica della Scuola di Scienze, e dalla Laurea Magistrale in Ingegneria per le comunicazioni multimediali e internet (ICT for internet and multimedia) e Ingegneria Informatica della Scuola di Ingegneria, Università di Padova.
- a.a. 2024/2025 - 2025/2026: "Analisi Matematica Uno (canale E)" (Calculus 1), Laurea Triennale in Ingegneria Informatica, Scuola di Ingegneria, Università di Padova.

Dottorati di Ricerca: Sono stato titolare o ho collaborato ai seguenti corsi di Dottorato:

- a.a. 1998/1999: Dottorato di ricerca in Matematica dell'Università di Padova: corso intitolato "Introduzione alla funzione ζ di Riemann".
- a.a. 1998/1999: Dottorato di ricerca in Matematica dell'Università di Genova (in consorzio con Università e Politecnico di Torino): corso, in collaborazione con il Prof. A. Perelli (Univ. di Genova), intitolato "Introduzione alla teoria dei numeri computazionale ed alla crittografia".
- a.a. 2001/2002 e 2004/2005: Dottorato di ricerca in Statistica dell'Università di Padova: corso, in collaborazione con la Prof. G. Treu (Univ. di Padova), intitolato "Analisi Funzionale".
- a.a. 2005/2006: Scuola di Dottorato in Matematica dell'Università di Padova: corso intitolato "Introduzione alla funzione ζ di Riemann".
- a.a. 2007/2008: Scuola di Dottorato in Matematica dell'Università di Padova: corso intitolato "Funzioni L di Dirichlet e Teoria dei Crivelli".
- a.a. 2015/2016: Scuola di Dottorato in Matematica dell'Università di Parma, consorzio Ferrara-Parma. Minicorso intitolato "Diophantine problems with prime numbers", maggio-giugno 2016.
- a.a. 2025/2026: Scuola di Dottorato in Ingegneria dell'Università di Padova, Corso intitolato "Introduction to Modern Cryptography", (24 h).

Corsi di Master: Sono stato titolare del seguente corso:

- a.a. 2002/2003, 2003/2004: "Un'introduzione alla Teoria dei Numeri e applicazioni alla Crittografia" (14 h), Master in Matematica Applicata, Facoltà di Ingegneria, Università di Padova.

Collaborazioni didattiche e attività di supporto: Ho collaborato alla didattica per i seguenti corsi:

- a.a. 1996/1997 e 1997/1998: sostegno alla didattica per il corso "Geometria e Calcolo Numerico", Facoltà di Ingegneria, Università di Genova.
- da a.a. 1998/1999 a a.a. 2000/2001: collaborazione didattica sul corso "Matematica Generale", Diploma Universitario in Statistica, Facoltà di Statistica, Università di Padova.
- da a.a. 2001/2002 a a.a. 2004/2005: collaborazione didattica sui corsi "Istituzioni di Analisi Matematica I e II", Lauree Triennali in Statistica, Facoltà di Statistica, Università di Padova.
- a.a. 2005/2006: collaborazione didattica sul corso "Istituzioni di Analisi Matematica I" , Lauree Triennali in Statistica, Facoltà di Statistica, Università di Padova.
- a.a. 2005/2006 e a.a. 2008/2009: collaborazione didattica sul corso "Metodi Matematici per la Statistica", Laurea Specialistica in Statistica, Facoltà di Statistica, Università di Padova.

- a.a. 2009/2010-2011/2012: collaborazione didattica sul corso “Analisi Matematica”, Laurea Magistrale in Statistica, Facoltà di Statistica, Università di Padova.
- a.a. 2024/2025: “Analisi Matematica Uno (canale C)” (Calculus 1), Laurea Triennale in Ingegneria Informatica, Scuola di Ingegneria, Università di Padova.

Studenti di Dottorato:

- Sono stato Advisor della Tesi di Dottorato in Matematica della Dott.sa Valentina Settimi, intitolata “On some additive problems with primes and powers of a fixed integer”.
- Sono stato Co-advisor della Tesi di Dottorato in Matematica della Dott.sa Antonella Rossi (advisor: Prof. Alessandro Zaccagnini), Dottorato in Matematica, Consorzio Universitario Milano-Insubria-Parma-Trieste.
- Ho collaborato alla tesi di Dottorato in Matematica del Dott. Marco Cantarini (2016) e del Dott. Alessandro Gambini (2017), Consorzio Universitario Modena-Ferrara-Parma.

Relatore di tesi di Laurea (v.o., triennali, magistrali):

Sono stato relatore di 35 Tesi di Laurea in Teoria dei Numeri, sia per quanto riguarda aspetti teorici che computazionali [n. 4 tesi di laurea vecchio ordinamento; n. 12 tesi di laurea specialistica; n. 9 tesi di laurea magistrale; n. 9 tesi di laurea triennale; n. 1 tesi di diploma universitario]. Gli argomenti spaziano da questione teoriche di Teoria Analitica ed Elementare dei numeri (teorema del numeri primi, congettura di Goldbach, crivello largo, problemi dei primi gemelli) a questioni applicative (protocolli crittografici, crittografia omomorfa, crittografia con curve ellittiche, algoritmi di primalità, algoritmi di fattorizzazione). Due di queste tesi sono sul teorema di Maynard sull’esistenza di infiniti numeri primi consecutivi aventi distanza finita (uno dei risultati per cui Maynard ha ricevuto la medaglia Fields nel 2022).

- relatore, in collaborazione con il Prof. M. Ancona, Università di Genova, della tesi di Laurea in Matematica di A. Caruzzo intitolata “Un approccio computazionale alla congettura di Goldbach e problemi collegati”. (1998)
- relatore, in collaborazione con il Prof. M. Ancona, Università di Genova, della tesi di Laurea in Matematica di F. Motosso intitolata “Aritmetica intera estesa ed applicazioni alla Teoria dei Numeri”. (1999)
- relatore, in collaborazione con la Prof. S. Dulli, Università di Padova, della tesi di Diploma in Statistica e Informatica per la Gestione delle Imprese di N. Orsatti intitolata “Algoritmi in linguaggio C per la rappresentazione di alcuni frattali”. (2000)
- relatore della tesi di Laurea (triennale) in Statistica e Gestione delle Imprese di N. Orsatti intitolata “Alcuni aspetti della Crittografia”. (2002)
- relatore, in collaborazione con il Prof. G. Filé, Università di Padova, della tesi di Laurea (triennale) in Informatica di C. Zanini intitolata “Protocolli di identificazione: Kerberos e sue estensioni mediante la crittografia a chiave pubblica”. (2003)
- relatore della tesi di Laurea (triennale) in Matematica di A. Morra intitolata “Curve ellittiche su campi finiti: alcune applicazioni alla crittografia”. (2004)
- relatore, in collaborazione con il Prof. G. Filé, Università di Padova, della tesi di Laurea (triennale) in Informatica di L. Stoppa intitolata “Kerberos e la crittografia a Chiave Pubblica”. (2005)
- relatore della tesi di Laurea (triennale) in Matematica di V. Settimi intitolata “Pseudocasualità e crittografia: alcuni metodi”. (2005)
- relatore della tesi di Laurea (triennale) in Matematica di D. Cricco intitolata “Il Crivello Quadratico di Pomerance”. (2005)
- relatore della tesi di Laurea in Matematica (vecchio ordinamento) di D. Alessio intitolata “Reticoli: aspetti algoritmici e loro applicazioni crittografiche”. (2006)
- relatore della tesi di Laurea in Matematica (vecchio ordinamento) di L. Doni intitolata “Crittografia classica e moderna: alcuni metodi”. (2006)
- relatore, in collaborazione con il Prof. B. Chiarellotto, Università di Padova, della tesi di Laurea Specialistica in Matematica di C. Anghel (studente ALGANT) intitolata “The Elliptic Curve Discrete Logarithm Problem”. (2007)
- relatore della tesi di Laurea Specialistica in Matematica di T. Majumdar (studente ALGANT) intitolata “On the Large Sieve”. (2008)
- relatore della tesi di Laurea Specialistica in Matematica di U. Frasson (svolta in stage esterno presso l’azienda Elaide) intitolata “Secure Hash Standard: Aspetti implementativi”. (2008)
- relatore della tesi di Laurea Triennale in Matematica di E. Zonta intitolata “Codici, fattorizzazione e primalità con curve ellittiche”. (2008)
- relatore della tesi di Laurea Specialistica in Matematica, in collaborazione con il Prof. R. Colpi, Università di Padova, di M. Placci intitolata “Crittoanalisi del sistema RSA tramite frazioni continue”. (2008)
- relatore della tesi di Laurea Specialistica in Matematica di S. Bettin intitolata “Alcuni problemi equivalenti all’Ipotesi di Riemann”. (2008)
- relatore della tesi di Laurea Specialistica in Matematica di V. Gauthier (studente ALGANT) intitolata “On some polynomial–time primality algorithms”. (2008)
- relatore della tesi di Laurea Specialistica in Matematica di L. Corsi intitolata “Alcuni algoritmi per il Logaritmo Discreto”. (2009)
- relatore della tesi di Laurea Specialistica in Matematica di L. Maggiolo intitolata “Crivelli dei Campi di Numeri”. (2009)

- relatore della tesi di Laurea Specialistica in Matematica di F. Melgrani intitolata “L’algoritmo di Schoof”. (2010)
- relatore della tesi di Laurea Specialistica in Matematica di E. Scipioni intitolata “Alcuni attacchi a RSA e sue varianti”. (2010)
- relatore della tesi di Laurea Specialistica in Matematica, in collaborazione con il Prof. R. Cramer, Università di Leiden e CWI Amsterdam (Paesi Bassi), di D. Orlandi intitolata “A Note on Lossy Trapdoor Functions from Smooth Homomorphic Hash Proof Systems”. (2011)
- relatore della tesi di Laurea Specialistica in Matematica, in collaborazione con il Prof. R. Cramer, Università di Leiden e CWI Amsterdam (Paesi Bassi), di A. Astolfi intitolata “On Proving Permutations in Zero-Knowledge”. (2011)
- relatore della tesi di Laurea Triennale in Matematica, di R. Tonon intitolata “Sulla dimostrazione elementare del Teorema dei Numeri Primi”. (2012)
- relatore della tesi di Laurea Triennale in Matematica, di G. Di Salvo intitolata “Alcune proprietà della trasformata di Mellin”. (2012).
- relatore della tesi di Laurea Magistrale in Matematica di S. Lippiello intitolata “Sulla crittografia omomorfa”, (2013).
- co-relatore, in collaborazione con M.Garuti e L.Zapponi, della tesi di Laurea Magistrale in Matematica di L.Covolo intitolata “Crittografia su curve iperellittiche”, (2013).
- relatore della tesi di Laurea Magistrale in Matematica, di S. Zuliani intitolata “Il decimo problema di Hilbert”. (2014).
- relatore della tesi di Laurea Magistrale in Matematica di M.T. Damir (studente ALGANT) intitolata “Bounded gaps between primes”. (2015).
- relatore della tesi di Laurea Magistrale in Matematica di A. Cracco intitolata “Sul Crivello Quadratico”. (2015).
- relatore della tesi di Laurea Magistrale in Matematica di R. Tonon intitolata “Sulla pair-correlation conjecture di Montgomery”. (2015).
- relatore, in collaborazione con C. Novelli, della tesi di Laurea Magistrale in Matematica di A.Mazzoran intitolata “Curve ellittiche e applicazioni”. (2016).
- relatore della tesi di Laurea Magistrale in Matematica di D. Mastrostefano intitolata “Su recenti risultati relativi a piccole distanze tra primi consecutivi”. (2017).
- relatore, in collaborazione con G. Castagnos (Univ. Bordeaux) della tesi di Laurea Magistrale in Matematica di D. Ciaffi intitolata “A provably secure variant of NTRU cryptosystem”. (2018).

Attività di divulgazione

Monografie:

2004: Ho pubblicato in collaborazione con A. Zaccagnini dell’Università di Parma, il testo “Introduzione alla Crittografia”, [3], Hoepli editrice.
2006: Ho pubblicato in collaborazione con A. Zaccagnini dell’Università di Parma, il testo “Crittografia”, [2], CLEUP, per il Progetto Laureee Scientifiche per il Veneto.
2015: Ho pubblicato in collaborazione con A. Zaccagnini dell’Università di Parma, il testo “Manuale di Crittografia”, [4], Hoepli editrice.
2017: Ho pubblicato il testo “Analisi Matematica 1”, [1], Hoepli editrice.

Conferenze divulgative, interviste, partecipazione a documentari, capitoli di libri:
Elenco per anno tali attività:

- 1998: conferenza per la sezione di Padova dell’associazione “Mathesis” intitolata “Una breve introduzione alla crittografia”.
- 2001: Intervista su “Steganografia e Crittografia” nel programma di divulgazione scientifica “Il sommergibile” di V. Masotti, trasmesso dalla Radio Svizzera Italiana il 02/10/2001, link;
- 2001: Intervista su “Trasmissioni e codici cifrati” nel programma “GR-Scienza” di S. Sciancalepore, trasmesso dal consorzio radiofonico BluSat il 18/10/2001.
- 2005-2007: ho partecipato al Progetto Lauree Scientifiche coordinando il progetto “Crittografia” per quattro diverse Scuole Superiori del Veneto.
- 2009: durante il convegno “Advances in Number Theory and Geometry”, Verbania, sono stato intervistato da U. Rondi per il documentario RAI intitolato ‘‘Caccia ai numeri primi”.
- 2010: Ho presentato la conferenza “Comunicazione sicura nell’era di Internet”, per la serie di conferenze “Eppur si Muove”.
- 2012: Ho presentato la conferenza “Dai messaggi cifrati di Cesare alla comunicazione sicura nell’era di Internet”, per la serie di conferenze “Caffè & Scienza” organizzate dal Circolo ARCI “La mela di Newton”.
- 2014: Sono stato membro del Comitato Scientifico della mostra “Numeri. Tutto quello che conta, da zero a infinito”, curatore C. Bartocci e L. Civalleri, Palazzo delle Esposizioni, Roma, 16/10/2014 - 31/05/2015. Ho scritto il capitolo 11 intitolato “Numeri primi” del volume di presentazione della mostra ed i pannelli relativi, si veda [51].
- 2016: ‘‘Ma la matematica non è un’opinione”, Intervista per “Il Bo”, giornale dell’Università di Padova, che prende spunto da come vengono presentate le notizie relative a (presunte) scoperte scientifiche.

- 2018: Intervista di S. Camisasca per Agorà (pagina culturale del quotidiano Avvenire) pubblicata il 21-02-2018 e riguardante il ruolo della Crittografia nella società odierna.
- 2018: Intervista di S. Camisasca per Agorà (pagina culturale del quotidiano Avvenire) pubblicata il 04-04-2018 e riguardante come l'esempio del lavoro di Ramanujan sia importante per capire il ruolo della matematica nella nostra società attuale.
- 2019: Intervista di S. Camisasca il quotidiano Avvenire pubblicata il 20-02-2019 e riguardante l'influenza della matematica nella nostra società.
- 2020: Intervento sulla vita e le opere di Ramanujan e di Hardy all'interno di "La scienza al cinema" (serie di proiezioni di film su temi scientifici organizzata dal Piano Lauree Scientifiche a Padova) a commento del film "L'uomo che vide l'infinito" di M. Brown.
- 2022: (25 febbraio) Conferenza intitolata "Alla ricerca dei numeri primi" per la sezione di Padova dell'associazione "Mathesis", Locandina.

Collaborazioni con riviste scientifiche

Membro del comitato editoriale:
- Associate Editor di Expositiones Mathematicae, ISSN 0723-0869, dal 15/09/2025.
- Membro del comitato editoriale di Indian Journal of Mathematics, ISSN 0019-5324, dal 01/01/2019.
- Membro del comitato editoriale di Journal of Approximation Software, dal 01/01/2024.
- Già membro del comitato editoriale di Open Mathematics, ISSN 2391-5455, dal 01/09/2016 al 01/02/2024.
- 2003-2005: Managing editor (diffusione e sviluppo della versione elettronica) per la rivista "Rendiconti del Seminario Matematico dell'Università di Padova".

Reviewer:
Dal 1997: Reviewer per la rivista "Mathematical Reviews" per le classi: 11M (teoria analitica delle funzioni zeta e L), 11N (teoria moltiplicativa dei numeri), 11P (teoria additiva dei numeri e partizioni), per un totale di 70 recensioni (fino al 21 settembre 2025).

Referee per le riviste (in ordine alfabetico):

1) Acta Arithmetica;
2) Acta Mathematica Hungarica;
3) Advances in Mathematics;
4) Analysis, Geometry and Number Theory;
5) Annali della Scuola Normale Superiore di Pisa;
6) Applicable Algebra in Engineering, Communication and Computing;
7) Applied Mathematics E-Notes;
8) Atti della Accademia Peloritana dei Pericolanti - Classe di Scienze Fisiche, Matematiche e Naturali;
9) Bollettino dell'Unione Matematica Italiana;
10) Bulletin of the Allahabad Mathematical Society;
11) Canadian Mathematical Bulletin;
12) Communications in Algebra;
13) Complex Variables and Elliptic Equations;
14) Czechoslovak Mathematical Journal;
15) Electronic Research Archive;
16) Experimental Mathematics;
17) Functiones et Approximatio, Commentarii Mathematici;
18) Frontiers of Mathematics;
19) Hacettepe Journal of Mathematics and Statistics;
20) Indagationes Mathematicae;
21) Indian Journal of Mathematics;
22) Integers;
23) International Journal of Number Theory;
24) ISAAC conference;
25) Journal of Algebra and its Applications;
26) Journal of Algebra, Number Theory and Applications;
27) Journal of Inequalities and Applications;
28) Journal of Mathematical Analysis and Applications;
29) Journal of Number Theory;
30) Lithuanian Mathematical Journal;
31) Mathematics of Computation;
32) Mathematica Slovaca;
33) Mathematika;
34) Missouri Journal of Mathematical Sciences;
35) Monatshëfte für Mathematik;
36) Open Mathematics;
37) Quarterly Journal of Mathematics;
38) Periodica Mathematica Hungarica;
39) Publicationes Mathematicae Debrecen;
40) Rendiconti del Circolo Matematico di Palermo;
41) Rendiconti del Seminario Matematico dell'Università di Padova;
42) Rendiconti del Seminario Matematico dell'Università di Torino;
43) Rendiconti per gli studi Economici Quantitativi dell'Università di Venezia;
44) Research in Number Theory;
45) Rivista di Matematica della Università di Parma;
46) Rocky Mountain Journal of Mathematics;
47) Taiwanese Journal of Mathematics;
48) The American Mathematical Monthly;
49) The Ramanujan Journal.

Partecipazione a Conferenze e Convegni; seminari

- Gennaio 1995: Incontro Italiano di Teoria dei Numeri, Roma, Italia, (speaker).
- Luglio 1997: Arithmetical Theory of Elliptic Curves, CIME Course, Cetraro (Cs), Italia.

- Marzo 1999: Matematica e Cultura, Venezia, Italia.
- Luglio 2002: Analytic Number Theory, CIME Course, Cetraro (Cs), Italia.
- Luglio 2003: Journées Arithmétiques 2003, Graz, Austria.
- Novembre 2003: Secondo Incontro Italiano di Teoria dei Numeri, Parma, Italia, (speaker).
- Luglio 2005: Journées Arithmétiques 2005, Marseille, Francia.
- Maggio 2006: Italian-Polish Number Theory Days, Poznań, Polonia (invited speaker).
- Luglio 2006: Special Session in Number Theory of the SIMAI-SMAI-SMF-UMI meeting, Torino, Italia.
- Luglio 2007: Journées Arithmétiques 2007, Edimburgo, Regno Unito, (speaker).
- Settembre 2007: Arithmetic Geometry, CIME Course, Cetraro (Cs), Italia.
- Maggio 2008: Analytic Number Theory Workshop, Parma, Italia, (invited speaker).
- Settembre 2008: A p-adic differential equations: a conference in honor of Gilles Christol, Bressanone (Italia).
- Aprile 2009: Advances in Number Theory and Geometry, Verbania (Italy).
- Maggio 2009: La Teoria dei Numeri, Università di Roma Tre, Roma (Italy), (invited speaker).
- Marzo 2010: International Italy-India Conference on Diophantine and Analytic Number Theory, Scuola Normale Superiore, Pisa (Italy), (invited speaker).
- Agosto-Settembre 2010: Analytic and Combinatorial Number Theory, ICM satellite conference, Institute of Mathematical Sciences, Chennai (India), (invited speaker).
- Ottobre 2010: Number Theory and its applications, An International Conference Dedicated to Kálmán Győry, Attila Pethő, János Pintz, András Sárközy, Institute of Mathematics, University of Debrecen, Hungary, (invited speaker).
- Febbraio 2011: From p-adic differential equations to arithmetic algebraic geometry, on the occasion of Francesco Baldassarri's 60th birthday, 3-5 February 2011, Padova, Italy.
- Agosto 2011: Paul Turán Memorial Conference, 22-26 August 2011, Budapest, Hungary.
- Settembre 2011: Congresso UMI, 12-16 Settembre 2011, Bologna, Italy (chairman di sezione).
- Luglio 2013: Paul Erdős Memorial Conference, 01-05 Luglio 2013, Budapest, Hungary.
- Settembre 2015: Terzo Incontro Italiano di Teoria dei Numeri, Scuola Normale Superiore, Pisa (Italy), (invited speaker), proceedings [44].
- Novembre 2016, Workshop di Teoria dei Numeri, Dipartimento di Matematica, Università di Torino, (invited speaker).
- Marzo 2021: Number Theory Online (invited speaker), link.
- Ottobre 2021: 5th Number Theory Meeting - Torino (invited speaker), link.

Attività seminariale:

- "Il teorema di Bombieri-Vinogradov e sue estensioni, I, II, III", Università di Genova, 1993.
- "Crivello pesato e Teorema di Chen, I,II", Università di Genova, 1994.
- "Alcuni risultati sulla congettura di Goldbach", Incontro Italiano di Teoria dei Numeri, Terza Università di Roma, 1995.
- "Una (breve) introduzione alla crittografia", Associazione Mathesis, Università di Padova, 1998.
- "Approssimazione diofantea e algoritmo LLL, I,II,III", Università di Padova, 2001.
- "Sull'insieme eccezionale in intervalli corti di due problemi additivi con numeri primi", Secondo Incontro Italiano di Teoria dei Numeri, Università di Parma, 2003.
- "Piccole differenze tra primi consecutivi (dopo Goldston, Motohashi, Pintz, Yildirim)" Università di Genova, 08.06.2005.
- "On the sum of a prime and a k-free number", Italian-Polish Number Theory Days, Poznań, Polonia, 18.05.2006.
- "Numeri primi e Crittografia", Università degli studi di Modena, 04.10.2006.
- "On the sum of two primes and k powers of two", Univ. Genova, 15.05.2007 - Univ. Parma 18.05.2007 - Journées Aritmétiques 2007, Edimburgo, UK, 02.07.2007.
- "Alcuni Attacchi a RSA", Università degli studi di Ferrara, 23.05.2007.
- "On the constant in the Mertens product for arithmetic progressions: Numerical values", Univ. Parma 16.05.2008.
- "Sul problema di Goldbach-Linnik", Università di Roma Tre, Roma, 29.05.2009.
- "On the Montgomery-Hooley theorem in short intervals", Marzo 2010: Scuola Normale Superiore, Pisa (Italy).
- "On the average number of Goldbach representation of an integer", Agosto 2010: Institute of Mathematical Sciences, Chennai (India); Ottobre 2010: University of Debrecen, Debrecen (Hungary).
- "Una formula esplicita per i numeri di Goldbach", Settembre 2011: Univ. Bologna, Italy.
- "RSA: firma digitale e attacchi", Novembre 2014, Progetto CAM, Univ. Padova, Italy.
- "On some exponential sums over prime powers and applications", Settembre 2015: Terzo Incontro Italiano di Teoria dei Numeri, Scuola Normale Superiore, Pisa (Italy), proceedings [44].
- "Breve storia del Teorema dei Numeri Primi", Maggio 2016: Associazione Mathesis, Università di Padova.
- "Diophantine problems with prime numbers", Maggio-Giugno 2016: Scuola del dottorato di Matematica, Università di Parma.
- "Formule esplicite per problemi additivi con numeri primi", Workshop di Teoria dei Numeri, Dipartimento di Matematica, Università di Torino, Novembre 2016.

- Marzo 2021: "Calcolo efficiente della costante di Euler-Kronecker per campi ciclotomici (e problemi collegati)", the Number Theory Online conference, invited speaker.
- Marzo 2021: "On computing $\frac{L'}{L}(1,\chi)$ and related problems", Nancy-Metz online Théorie des Nombres Seminaire, invited speaker.
- Ottobre 2021: "On computing $\frac{L'}{L}(1,\chi)$", 5th Number Theory Meeting, Torino, invited speaker.
- Febbraio 2022: "Alla ricerca dei numeri primi", Associazione Mathesis, Università di Padova, 2022.
- 25 Aprile 2023, ore 11.00-12.00: ONLINE talk intitolato: "Computing $\frac{L'}{L}(1,\chi)$ using special functions, their reflection formulae and the Fast Fourier Transform". Per la "Lithe and fast algorithmic number theory" (LFANT) series, INRIA and Institut de Mathématiques de Bordeaux, the Mathematics Institute of CNRS, Université de Bordeaux and Bordeaux INP, link.

Attività scientifica

Awards:
2003: Distinguished Award, Hardy-Ramanujan Society.

Borse di studio e di ricerca:
Vincitore delle seguenti Borse di Studio.
- Marzo 1991 - Novembre 1994: Borsa di studio del dottorato di ricerca (Università di Torino).
- Marzo 1996 - Febbraio 1997: Borsa di studio C.N.R. "ricerca" n. 201.01.121.
- Marzo 1997 - Giugno 1997: Borsa di studio C.N.R. "ricerca" n. 201.01.123.
- Luglio 1997 - Agosto 1998: Borsa di studio post-dottorato dell'Università di Genova.

Partecipazioni a Progetti di Ricerca:
Elenco i progetti di ricerca di interesse nazionale o locale di cui sono stato membro.
- PRIN 2000, MM01118441_001, Funzioni L e numeri primi, Università di Genova;
- PRIN 2002, 2002018334_001, Funzioni L e problemi Diofantei Additivi, Università di Genova;
- PRIN 2004, 2004010549_001, Funzioni L e problemi Diofantei Additivi, Università di Genova;
- PRIN 2006, 2006018391_004, Geometria aritmetica : teorie p-adiche e motivi, Università di Padova;
- PRIN 2008, 2008LMSMTY_005, Metodi differenziali p-adici e motivi, Università di Padova;
- CARIPARO 2008-2009, "Eccellenza", Differential Methods in Arithmetic, Geometry and Algebra, Università di Padova;
- PRIN 2010-2011, 20105LL47Y_001, Geometria algebrica aritmetica e teoria dei numeri, Università di Padova;
- PRIN 2015, 2015XBNXYC_002, Number Theory and Arithmetic Geometry, Università di Padova;
- PRIN 2017, 2017JTLHJR_002, Geometric, algebraic and analytic methods in arithmetic, Università di Padova;
- TRACE4EU, 2023-2025; partecipante all'unità dell'Università di Padova per il progetto TRACE4EU finanziato dalla EU. Topic IP DIGITAL-2022-DEPLOY-02-EBSI-SERVICES. Digital Europe Programme.

Miei lavori citati nella Online Encyclopedia of Integer Sequences:
Fondata nel 1964 da N.J.A. Sloane, contiene un grande numero di dati sulle sequenze intere; per una descrizione dettagliata dei sui scopi si rimanda a alla loro pagina di benvenuto. Alcuni miei contributi scientifici sono citati in tale enciclopedia; essi sono:

1) A000466: $a(n) = 4n^2 - 1$;
2) A002375: From Goldbach conjecture: number of decompositions of 2n into an unordered sum of two odd primes;
3) A014549: Decimal expansion of $1/M(1,\sqrt(2))$ (Gauss's constant).
4) A064533: Decimal expansion of Landau-Ramanujan constant;
5) A073005: Decimal expansion of $\Gamma(1/3)$.
6) A073010: Decimal expansion of $\pi/\sqrt{27}$;
7) A135311: A greedy sequence of prime offsets;
8) A161529: Decimal expansion of negative of constant $M(3,1)$ arising in Mertens and Meissel-Mertens constants for sums over arithmetic progression;
9) A187549: Arises in a Diophantine problem with one prime, two squares of primes and s powers of two;
10) A227158: Second-order term in the asymptotic expansion of $B(x)$, the count of numbers up to x which are the sum of two squares;
11) A242013: Decimal expansion of the Euler-Kronecker constant (as named by P. Moree) for hypotenuse numbers;
12) A242015: Decimal expansion of the Euler-Kronecker constant (as named by P. Moree) for non-hypotenuse numbers;
13) A309520: Primes p for which $h_1(p)/G(p)$ has a record value;
14) A301430: Decimal expansion of an analog of the Landau-Ramanujan constant for Loeschian numbers which are sums of two squares;
15) A335576: Decimal expansion of Mertens constant $C(5,2)$;
16) A336798: Decimal expansion of Mertens constant $C(5,3)$;
17) A336802: Decimal expansion of the constant $\Pi(5,1)$;
18) A338462: Decimal expansion of the constant $\Pi(5,4)$;
19) A340127: Decimal expansion of $\prod_{p\equiv 4 \bmod 5} \frac{p^2}{p^2-1}$;
20) A340628: Decimal expansion of $\prod_{p\equiv 4 \bmod 5} \frac{p^2+1}{p^2-1}$;
21) A340629: Decimal expansion of $\prod_{p\equiv 1 \bmod 5} \frac{p^2+1}{p^2-1}$;
22) A340711: Decimal expansion of $\prod_{p\equiv 3 \bmod 5} \frac{p^2+1}{p^2-1}$;
23) A340839: Decimal expansion of Mertens constant $C(5,1)$;
24) A340866: Decimal expansion of Mertens constant $C(5,4)$;

25) A350763: Decimal expansion of $\gamma + \log 2$, where γ is Euler's constant;
26) A368644: Decimal expansion of the Mertens constant $M(3,2)$ arising in the formula for the sum of reciprocals of primes $p \equiv 2 \bmod 3$;
27) A368645: Decimal expansion of the Mertens constant $M(4,1)$ arising in the formula for the sum of reciprocals of primes $p \equiv 1 \bmod 4$ (negated);
28) A368646: Decimal expansion of the Mertens constant $M(4,3)$ arising in the formula for the sum of reciprocals of primes $p \equiv 1 \bmod 4$.

Attività di ricerca

Elenco dei coautori (in ordine alfabetico):

1) S.S. Al-Haj Baddar (University of Jordan, Amman)
2) D. Bazzanella (Politecnico di Torino, Italy)
3) M. Cantarini (Università di Perugia, Italy)
4) A. Ciolan
5) S. Fan (University of Georgia, USA)
6) A. Gambini (Università di Roma "La Sapienza", Italy)
7) J. Kaczorowski (Poznan University, Poland)
8) N. Kandhil (Hong Kong University, Hong Kong)
9) Y. Lamzouri (Institut Élie Cartan de Lorraine, France)
10) F. Luca (University of the Witwatersrand, South Africa and Max-Planck Institute for Software Systems, Saarbrücken, Germany)
11) R. Lunia (Max Planck Institute für Mathematik, Bonn, Germany)
12) F. Menegazzo
13) P. Moree (Researcher/Scientific Coordinator, Max Planck Institute für Mathematik, Bonn, Germany)
14) M. Migliardi (Università di Padova, Italy)
15) M. Morigi (Università di Bologna, Italy)
16) A. Perelli
17) J. Pintz (Alfred Renyi Mathematical Institute, Budapest, Hungary)
18) L. Righi (IT services, Università di Padova, Italy)
19) S. Saad Eddin (Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria)
20) A. Sedunova (University of Warwick, England)
21) V. Settimi
22) A. Togbé (Purdue University, USA)
23) T. Trudgian (University of New South Wales, Canberra, Australia)
24) A. Zaccagnini (Università di Parma, Italy)

Descrizione dell'attività di ricerca:

In totale la mia produzione scientifica, considerando gli articoli scientifici già pubblicati o in corso di pubblicazione (75), i preprints (9), le monografie (4) e le web-pubblicazioni (5), consta di 93 lavori. Ho scritto anche n. 7 dispense didattiche per alcuni dei corsi che ho tenuto o a cui ho collaborato (elencate nella sezione "Altre pubblicazioni" insieme alle Tesi di Laurea e di Dottorato di Ricerca).
Il mio settore di ricerca principale è la Teoria analitica dei numeri. In particolare ho rivolto la mia attenzione ai problemi additivi con numeri primi ed alla distribuzione degli zeri delle funzioni ζ di Riemann e L di Dirichlet. In alcuni casi mi sono anche interessato degli aspetti computazionali collegati. Nel seguito descrivo alcuni dei filoni principali di ricerca che ho seguito in questi anni. La descrizione delle problematiche sotto riportate è, giocoforza, schematica; maggiori dettagli sono disponibili nel file (list_abstract link) che riporta gli abstract dei miei lavori pubblicati.

Congettura di Goldbach:
Un mio filone principale di ricerca riguarda lo studio della Congettura di Goldbach. Nel 1742, in due lettere indirizzate ad Euler, Goldbach congetturò che *"ogni intero n pari, n > 2, è somma di due numeri primi"*. Talvolta per congettura di Goldbach si intende anche l'affermazione più debole: *"ogni intero n pari, n sufficientemente grande, è somma di due numeri primi"*.
Entrambi i problemi sono, allo stato attuale della ricerca, irrisolti. Chiamerò numeri di Goldbach gli interi pari che sono somma di due numeri primi. Alcuni dei miei lavori riguardano lo studio di risultati parziali sulla congettura di Goldbach. Tra di essi alcuni (i lavori [88], [86] e [74]) riguardano lo studio delle eccezioni a questo problema: ossia, denominato $E = \{n \in \mathbb{N};\ n \text{ non è numero di Goldbach}\}$ e detto X un parametro, ci si chiede quale sia la cardinalità dell'insieme "eccezionale" $E(X) = E \cap (1, X)$ oppure dell'insieme "eccezionale in intervalli corti" $E(X, H) = E \cap (X, X + H)$, dove X ed H sono supposti sufficientemente grandi, ma H è di ordine di grandezza inferiore rispetto ad X. Risultati significativi sono quelli in cui si prova che $|E(X)| = o(X)$ oppure $|E(X, H)| = o(H)$ per $X \to +\infty$. In particolare il lavoro [74] riguarda lo studio dell'insieme eccezionale in intervalli corti senza assumere alcuna ipotesi analitica sulla distribuzione degli zeri non-banali delle funzioni L di Dirichlet.
Un altro tipo di risultato parziale riguarda la distribuzione in intervalli corti dei numeri di Goldbach. Ossia ci si chiede quanto deve essere lungo un intervallo del tipo $(X, X + H)$, dove X ed H sono supposti sufficientemente grandi, ma H è di ordine di grandezza inferiore rispetto ad X, per essere certi che ivi sia contenuto un numero di Goldbach. Alcuni di essi dipendono da congetture analitiche sulla distribuzione degli zeri delle funzioni ζ di Riemann e L di Dirichlet (quali l'Ipotesi di Riemann generalizzata). Ho dimostrato risultati di questo genere nei lavori [85], [83] e [81].
La tecnica adottata per provare i risultati sulla distribuzione dei numeri di Goldbach usa il metodo del cerchio di Hardy, Ramanujan e Littlewood ed è essenzialmente collegata a due fondamentali quantità analitiche: l'Integrale di Selberg (che consente uno studio della distribuzione dei numeri primi) e una media L^2 troncata del polinomio trigonometrico $\sum_{n\le x} \Lambda(n)e(n\alpha)$, dove $\alpha \in (0, 1)$,

$e(\tau) = \exp(2\pi i\tau)$ e $\Lambda(n)$ è la funzione di von Mangoldt (che conta, con un peso logaritmico, i primi e le potenze prime). Lo studio di tali quantità ha portato quindi a formulare risultati indipendenti dalla congettura di Goldbach ma ad essa collegabili. Il lavoro [78] riguarda tali argomenti.
Nel 2010, in collaborazione con A. Zaccagnini (Parma), ho lavorato sull'andamento in media del numero di rappresentazioni di un intero pari come somma di due numeri primi (lavoro [57]). Il lavoro è stato citato nella "On-Line Encyclopedia of Integer Sequences" al numero A002375. In particolare, abbiamo migliorato il termine d'errore della formula esplicita che lega tali medie con gli zeri della funzione zeta di Riemann.

Formula esplicita per i numeri primi:
Sono stato attratto anche da problemi "laterali" a quanto detto sopra. Nello studio delle proprietà della distribuzione dei numeri primi uno strumento fondamentale è la "formula esplicita" per la funzione di Čebicev $\psi(x) = \sum_{n\le x}\Lambda(n)$. Tale formula consente di collegare la distribuzione dei numeri primi alla distribuzione degli zeri non-banali della funzione ζ di Riemann. Nel lavoro [84] si è studiata una variante "pesata" di tale formula che potesse avere ricadute sulla distribuzione dei numeri di Goldbach in intervalli corti. Nel lavoro [82] se ne è studiata, con tecniche analoghe, una variante, la formula di Landau, collegante gli zeri non-banali della funzione ζ di Riemann alla funzione di von Mangoldt.

Il problema additivo di Hardy–Littlewood:
Nel 2001-2002 ho anche studiato l'insieme eccezionale in intervalli corti del problema additivo di Hardy–Littlewood; ossia quello che si occupa della distribuzione degli interi scrivibili come somma di un numero primo e di una potenza naturale di un numero intero. Il lavoro [73] riguarda questo problema.
Nel 2008, in collaborazione con A. Zaccagnini, ho affrontato il problema di determinare la validità di una formula asintotica per la somma in intervalli corti del numero di rappresentazioni di un intero come somma di un primo e di una potenza di un intero, lavoro [66].
In seguito mi sono ancora occupato del problema di Hardy–Littlewood. In particolare ho studiato l'insieme eccezionale in intervalli corti di tale problema assumendo la validità dell'Ipotesi Generalizzata di Riemann. L'articolo [64] riguarda tale argomento.

Media delle rappresentazioni dei numeri di Goldbach e di Hardy–Littlewood:
In questa serie di problemi ho innovato inserendo alcuni pesi all'interno dello studio dell'andamento asintotico e delle formule esplicite per il numero di rappresentazioni dei numeri di Goldbach, di Hardy–Littlewood e di loro generalizzazioni. Ho sviluppato nell'estate del 2010 un metodo di attacco di una serie di problemi additivi con numeri primi che impiega le medie di Cesàro; la tecnica utilizzata è basata sulle trasformate di Laplace anziché sul metodo del cerchio (negli anni '50 del secolo scorso Walfisz la aveva usata per altre tipologie di problemi). Nel 2010 ho poi chiesto a Zaccagnini di collaborare in modo da poter più efficientemente trattare tutti i vari problemi che discendevano dall'impostazione generale da me sviluppata.
Nel 2012, in collaborazione con A. Zaccagnini, ho continuato lo studio dell'andamento in media del numero di rappresentazioni di un intero pari come somma di due numeri primi (lavoro [49]) introducendo questa volta il classico peso di Cesàro. Si ottengono interessanti formule esplicite, ossia che collegano le quantità aritmetiche sopra dette a somme sugli zeri non-banali della funzione zeta di Riemann; tali zeri sono pesati con la funzione Gamma di Euler.
Con una tecnica analoga, ma maggiormente complicata dalla presenza delle funzioni di Bessel di ordine complesso (tale ordine dipende dagli zeri non banali della funzione zeta di Riemann), in collaborazione con A. Zaccagnini, ho studiato l'andamento pesato mediante il peso di Cesàro del numero di rappresentazioni di un intero come somma di un numero primo e del quadrato di un intero, lavoro [52].
Nel 2016, con A. Zaccagnini, ho esteso l'applicabilità del metodo usato in [57] al caso in cui si effettui una media con peso di Cesàro su intervalli corti per le rappresentazioni di un intero come somma di due numeri primi, si veda [41].
In seguito abbiamo migliorato e generalizzato il metodo usato in [49] e [52] dimostrando la validità di una formula esplicita per gli interi rappresentabili come somma di due potenze prime, lavoro [35] o come somma di una potenza prima e di un quadrato, lavoro [36].

Congettura di Montgomery:
La congettura di Montgomery assume la validità dell'Ipotesi di Riemann e riguarda l'ordine di grandezza di una funzione costruita mediante una somma sulle coppie delle parti immaginarie di tali zeri (detta "funzione di correlazione a coppie"). A più riprese a partire dal 1998, si veda [83], ho studiato l'influenza di tale congettura sulla distribuzione dei numeri di Goldbach.
Nel 2000, in collaborazione con A. Perelli (Genova), abbiamo mostrato l'equivalenza tra la formulazione asintotica della Congettura di Montgomery e l'asintotica per le somme esponenziali sui primi coinvolte nelle applicazioni del metodo del cerchio a problemi additivi, [80]. Nel 2013, in collaborazione con Zaccagnini, sono tornato su questo problema raffinando tali risultati nel senso di rendere esplicite le connessioni tra i vari termini d'errore, si veda [50].
Nel 2010-2011 in collaborazione con A. Perelli ed A. Zaccagnini, ho lavorato sulla connessione tra i termini di errore per la funzione di correlazione a coppie degli zeri della funzione ζ di Riemann e per la media dei primi in intervalli corti (lavoro [54]).
Nel 2012-13, in collaborazione con A. Perelli ed A. Zaccagnini, ho studiato una forma generalizzata della funzione di correlazione a coppie degli zeri della funzione ζ di Riemann che permetta lo studio di medie "corte" per i numeri primi in intervalli corti (lavoro

[45]). In seguito abbiamo dimostrato la validità di tale generalizzazione in alcuni intervalli dei parametri principali ed abbiamo raffinato ulteriormente il collegamento con la distribuzione dei numeri primi in intervalli corti (lavoro [40]).

Il prodotto di Mertens sulle progressioni aritmetiche:
Nel 2005-2006, con A. Zaccagnini ho studiato una versione per il prodotto di Mertens nelle progressioni aritmetiche che è uniforme nel modulo q della progressione stessa, lavoro [69]; fino ad allora non erano disponibili risultati uniformi in q. Abbiamo mostrato che la formula asintotica di $\prod_{p\le x; p\equiv a \bmod q}(1-1/p)$ per $x\to+\infty$ vale uniformemente su q fino ad un certo limite che dipende dalle note stime sulle regioni prive di zeri delle funzioni L di Dirichlet. Inoltre detta $C(q,a)$ la costante che governa il primo termine di tale formula asintotica, ne abbiamo determinato una formula esplicita e calcolabile. La centralità del prodotto di Mertens all'interno della Teoria dei numeri primi ha reso molto usati nella letteratura successiva sia questo articolo che quelli computazionali dedicati al calcolo di $C(q,a)$. L'articolo, o sue parti, è citato nella "On-Line Encyclopedia of Integer Sequences" ai numeri A335576-A336798-A340711-A340839-A340866.
Nel 2007, in collaborazione con A. Zaccagnini, ho continuato lo studio del prodotto di Mertens nelle progressioni aritmetiche ottenendo delle stime in media del termine d'errore, articolo [67]. Abbiamo anche esaminato il problema di ottenere alcune formulazioni alternative della costante di Mertens, [62]; il lavoro è citato nella "On-Line Encyclopedia of Integer Sequences" ai numeri A336802-A338462-A340127-A340628-A340629-A340711-A340839-A340866. In altro paragrafo descrivo gli aspetti computazionali collegati a questi problemi.

Problema di Goldbach-Linnik:
Nel 2005-2006 ho lavorato in collaborazione con J. Pintz (Budapest, Ungheria) e A. Zaccagnini sul problema di rappresentare gli interi come somma di due primi e di un certo numero di potenze di due, lavoro [68]. Il risultato, molto forte, permette di far vedere che perturbare il problema di Goldbach con una sola potenza di due permette di ottenere stime per l'insieme eccezionale di tale problema perturbato che, allo stato dell'arte, sono irraggiungibili per il problema di Goldbach.

Interi rappresentabii come somme di più primi:
Nel 2011-2012 ho anche scritto, insieme ad A. Zaccagnini, un articolo che migliora i termini d'errore di una formula esplicita, valida assumendo l'Ipotesi Generalizzata di Riemann, per la funzione che conta il numero di rappresentazioni di un intero come somma di $k\ge 5$ primi, [58].

Approssimazione diofantea con numeri primi e potenze prime:
La principale innovazione inserita in questi lavori è l'inserimento di stime L^2 per le somme esponenziali sui numeri primi, o su potenze prime, all'interno del classico metodo di Davenport-Heilbronn, come ammodernato da Vaughan. Questo ha consentito di estendere l'ampiezza dell'intervallo in cui si riesce a determinare l'esistenza del termine principale per le quantità cercate, rendendo quindi più efficiente il metodo stesso. Per alcuni problemi ho anche implementato un algoritmo di Pintz-Ruzsa per lo studio di valori estremali della somma esponenziale sulle potenze di 2. Tutte queste innovazioni sono state recepite dalla copiosa letteratura scientifica successiva e costituiscono ora uno standard nell'uso del metodo di Davenport-Heilbronn per questi problemi.
Nel 2008, in collaborazione con A. Zaccagnini, ho studiato il problema di valutare le soluzioni della forma lineare formata con primi e potenze di due: $\lambda_1 p_1+\lambda_2 p_2+\mu_1 2^{m_1}+\ldots+\mu_s 2^{m_s}$, in cui i coefficienti λ_i,μ_j sono fissati. Abbiamo migliorato la stima per il numero di potenze di due necessarie ad assicurare l'approssimabilità di un qualunque numero reale mediante i valori raggiunti da tale forma lineare (articolo [61]). Il lavoro è stato citato nella "On-Line Encyclopedia of Integer Sequences" al numero A187549.
Nello stesso periodo, in collaborazione con V. Settimi, ho studiato il problema di valutare le soluzioni della forma lineare formata con primi e potenze di due: $\lambda_1 p_1+\lambda_2 p_2^2+\lambda_3 p_3^2+\mu_1 2^{m_1}+\ldots+\mu_s 2^{m_s}$, in cui i coefficienti λ_i,μ_j sono fissati. Abbiamo sensibilmente migliorato la stima per il numero di potenze di due necessarie ad assicurare l'approssimabilità di un qualunque numero reale mediante i valori raggiunti da tale forma lineare (articolo [55]). Il lavoro è stato citato nella "On-Line Encyclopedia of Integer Sequences" al numero A187549.
Più recentemente in collaborazione con A. Zaccagnini, ho migliorato un risultato sull'approssimabilità di numeri reali con forme del tipo $\lambda_1 p_1+\lambda_2 p_2^2+\lambda_3 p_3^2+\lambda_4 p_4^2$, (articolo [56]), su altri problemi diofantei con numeri primi e potenze prime (articolo [46]) nonché problemi con forme miste in potenze di primi (articolo [53]). Nel 2018 sono tornati a lavorare su questi problemi; in una collaborazione comprendente A. Gambini e A. Zaccagnini, abbiamo migliorato alcuni nostri risultati su problemi di approssimazione diofantea con numeri primi, articolo [39].

Formule asintotiche in media per problemi additivi con numeri primi e potenze prime:
Negli anni immediatamente successivi al 2010, mi sono reso conto che questo problema era affrontabile con le tecniche delle somme esponenziali e adattando il metodo del cerchio. Le principali problematiche da affrontare erano la mancanza di stime per le somme esponenziali su potenze prime. Queste somme esponenziali sono anche utili nello studio di problemi di approssimazione diofantea con numeri primi e potenze prime descritti in altro paragrafo.
Questo ha portato nel 2014, in collaborazione con A. Zaccagnini, a dimostrare, sotto l'assunzione dell'Ipotesi di Riemann, che ogni intervallo del tipo $[N,N+H]$, $H\gg(\log N)^4$, $N\to\infty$, contiene almeno un numero esprimibile come somma di un numero

primo e di due quadrati di primi, lavoro [48]. Più precisamente abbiamo mostrato che in tali intervalli vale una formula esplicita per il numero di rappresentazioni di tali interi.
Nello stesso periodo, con A. Zaccagnini, ho affrontato il problema della rappresentabilità di interi come somma di un primo e di un quadrato, o di un quadrato di un primo; ciò ha portato alla stesura dei due lavori [43] e [47] in cui dimostriamo la validità in intervalli corti di opportune formule asintotiche per la media del numero di rappresentazioni di un intero come somma due addendi di cui uno è un un numero primo (o un suo quadrato) ed l'altro è un quadrato di un intero (o un quadrato di un primo). Inoltre abbiamo generalizzato l'approccio in [43] e [47] a problemi binari di densità ≤ 1, lavoro [38].
Nel 2017-18, in collaborazione con A. Zaccagnini, abbiamo affrontato altri problemi classici in teoria additiva dei numeri quali quelli della somma di quattro cubi di primi (lavoro [37]), diminuendo sensibilmente l'ampiezza dell'intervallo corto in cui se ne ha l'esistenza, e di una potenza prima e due quadrati (lavoro [32]).
Ulteriori miglioramenti di tali risultati sono stati ottenuti raffinando le tecniche già usate in precedenza. Si sono cosí ottenuti risultati in media per il problema di Waring-Goldbach con s addendi e migliorato i risultati su problemi binari con potenze prime [33] (in collaborazione con A. Zaccagnini). In una collaborazione comprendente M. Cantarini, A. Gambini, e A. Zaccagnini abbiamo affrontato un problema ternario avente come addendi potenze prime, [34].

Stime per $\min_{\chi\neq\chi_0} |L'/L(1,\chi)|$:
Nel 2020-2021 ho studiato, in collaborazione con Y. Lamzouri (Lorraine, France), l'ordine di grandezza di $\min_{\chi\neq\chi_0} |L'/L(1,\chi)|$, χ primitivo (lavoro [26]). Il risultato con Lamzouri è il primo che permette di fornire maggiorazioni teoriche su $\min_{\chi\neq\chi_0} |L'/L(1,\chi)|$; inoltre in una parte computazionale, forniamo anche stime dal basso quando $3 \leq q \leq 10^7$, q primo. Queste stime computazionali permettono anche di provare che $L'(1,\chi) \neq 0$ per ogni carattere non banale χ mod q, $3 \leq q \leq 10^7$, q primo, e di fornire la base per congetturare opportune minorazioni per $|L'/L(1,\chi)|$ (al momento non si conoscono stime teoriche per tali minorazioni).

Stime esplicite per $|L(1,\chi)|$:
Nel 2020, in collaborazione con T.S. Trudgian (Canberra, Australia), lavoro [28], ho mostrato la validità delle stime di Lamzouri-Li-Soundararajan per $|L(1,\chi)|$, χ mod q, carattere di Dirichlet non banale, per ogni $q \geq 404$ (il precedente risultato le mostrava valide per $q \geq 10^{10}$). Con una parte computazionale abbiamo poi esteso il range di validità fino a $q \geq 3$.

Formule asintotiche per la funzione dei divisori generalizzata (e altri problemi collegati):
Nel 2021 ho collaborato con A. Ciolan e P. Moree su un problema di comparazione della validità delle formule asintotiche di Landau e di Ramanujan per la funzione che conta il numero di interi n per cui $q \nmid \sigma_k(n)$, dove q è un numero primo e $\sigma_k(n)$ è la funzione generalizzata dei divisori di n, [25]. Nell'articolo, tra cui molti altri risultati legati a classici problemi sulle forme modulari, inseriamo anche il calcolo esatto di ulteriori cifre decimali (130 000, per la precisione) per la costante del secondo ordine dello sviluppo asintotico della funzione che conta il numero di interi esprimibili come somma di due quadrati, si veda anche OEIS: A227158. Il calcolo è stato successivamente migliorato portando at ottenere 130 000 cifre decimali corrette per tale quantità e per altre costanti ad essa collegate come la costante di Landau–Ramanujan: A064533, A227158, A242013, A242015.

Problemi sulla distribuzione di numeri aventi solo due fattori primi:
Nel 2023, nuovamente in collaborazione con Moree, ma questa volta anche con F. Luca e A. Togbé, lavoro [10], abbiamo fornito stime esplicite per le costanti coinvolte nella stima delle differenze di due interi della forma $p^a \cdot q^b$, dove p, q sono due numeri primi distinti. Inoltre, dato $\alpha > 1$, forniamo risultati sia teorici che computazionali sul più piccolo intero m tale che per ogni $n \geq m$ l'intervallo $[n, n\alpha)$ contenga un intero della forma $p^a \cdot q^b$.

Costanti di Euler–Kronecker per campi e sottocampi ciclotomici:
Ho anche ripreso la collaborazione con N. Kandhil, P. Moree, S. Saad Eddin e A. Sedunova, cominciata nel 2019, e riguardante lo studio della congettura di Ihara sulla costante di Euler–Kronecker per sottocampi ciclotomici ed il quoziente di Kummer per il primo fattore del class number del campo ciclotomico. La prima parte dei risultati ottenuti è presentata in [20]. La seconda parte dei risultati, che si focalizza principalmente sull'andamento della quantità $\gamma_q^+ - \gamma_q$, differenza delle costanti di Euler–Kronecker per il massimo sottocampo reale del campo ciclotomico e del campo ciclotomico stesso $\mathbb{Q}(\zeta_q)$, è presentata in [19].

ll Quoziente di Brauer-Siegel:
Nel 2023-2024, collaborando con N. Kandhil e P. Moree [18] abbiamo migliorato un risultato pubblicato di Tatuzawa nel 1953 riguardante l'ordine di grandezza di una opportuna normalizzazione del prodotto tra class number e regolatore di un campo ciclotomico (detto Brauer-Siegel ratio).

Costanti di Eulero ottenuti da primi in progressioni aritmetiche:
Nel 2024, sempre in collaborazione con P. Moree [15], abbiamo trattato il caso delle costanti di Euler ottenuti con prodotti di numeri primi in progressioni aritmetiche, $\gamma(d,a)$. Sono costanti che intervengono spesso in problemi più generali dato che molte serie di Dirichlet di interesse teorico-numerico possono essere scritte come prodotto della serie generatrice $\zeta_{d,a}(s) = \prod_{p\equiv a \pmod d} (1-p^{-s})^{-1}$, dove p varia sui numeri primi appartenenti alla classe residuale primitiva $a \pmod d$, e una funzione $H(s)$ che presenta un buon

comportamento nelle vicinanze del punto $s = 1$. In tale caso la corrispondente costante di Euler viene ad essere espressa mediante le costanti di Euler $\gamma(d, a)$ della serie $\zeta_{d,a}(s)$ (coinvolte nella fattorizzazione menzionata precedentemente) e dalla quantità (più semplice da calcolare numericamente) $H'(1)/H(1)$. Nel lavoro vengono sistematicamente studiate le quantità $\gamma(d, a)$, come esse possano essere calcolate efficientemente ed accuratamente e vengono discusse alcune applicazioni riferite a problemi classici (trattati da Serre, per esempio).
Il lavoro è menzionato cinque volte su OEIS: A073005, A014549, A301430, A227158, A350763.

Una pair correlation conjecture per Dirichlet L-functions e le congetture di Montgomery, Elliott–Halberstam e Chowla:
Nel 2024-25, collaborando con N. Kandhil e P. Moree [11] abbiamo mostrato come una opportuna *pair-correlation conjecture per le funzioni L di Dirichlet* può essere usata, insieme all'Ipotesi Generalizzata di Riemann, per mostrare la veridicità della seguente forma della congettura di Montgomery sulla distribuzione dei numeri primi nelle progressione aritmetiche: per ogni $(a, q) = 1$ si ha

$$\psi(x; q, a) - \frac{x}{\varphi(q)} \ll \sqrt{\frac{x}{q}}\, x^{\varepsilon} \tag{1}$$

uniformemente per $1 \le q \le x^{1-\varepsilon}$. Di conseguenza, sotto le stesse ipotesi, abbiamo mostrato la veridicità di una forma della congettura di Elliott-Halberstam, ossia

$$\sum_{q \le x^{1-4\varepsilon}} \max_{(a,q)=1} \left| \psi(x; q, a) - \frac{x}{\varphi(q)} \right| \ll x^{1-\varepsilon}.$$

È noto che la congettura di Montgomery (riportata in (1)) sulla distribuzione dei numeri primi nelle progressione aritmetiche ha collegamenti con la frequenza con cui $L(\frac{1}{2}, \chi) = 0$. Nel 1980 Chowla congetturò che $L(\frac{1}{2}, \chi) \ne 0$ per ogni carattere quadratico. Si ritiene che $L(\frac{1}{2}, \chi) \ne 0$ per ogni χ, ma, allo stato dell'arte, il problema è aperto. Con tecniche simili a quelle precedentemente descritte, in [11] abbiamo mostrato, sotto le stesse ipotesi, che il numero di caratteri di Dirichlet $\chi \pmod q$ per cui $L(\frac{1}{2}, \chi) = 0$ è di ordine minore a $q^{1/2+\varepsilon}$.

Stime per il numero di ideali interi di estensioni abeliane di $\mathbb{Q}$:
Nel 2025, in collaborazione con Rashi Lunia e Pieter Moree [12], abbiamo migliorato le stime del termine d'errore per la funzione che calcola il numero di ideali interi di una estensione abeliana di $\mathbb{Q}$ avente dimensione maggiore o uguale a 4. Il problema risale a Dedekind e a Weber ed è quindi classico. In particolare, per estensioni di dimensione 4 siamo in grado di mostrare che tale termine d'errore è $O(x^{1/2+\epsilon})$; una stima precedentemente nota solamente assumendo la validità della congettura di Lindelöf generalizzata (ossia per le funzioni L di Dirichlet).

Miscellanea di altri problemi affrontati:
Nel 2001 ho collaborato, con un risultato riguardante la distribuzione della funzione φ di Euler e la distribuzione della funzione $\Omega(n)$ (che conta con molteplicità il numero di fattori primi di n), al lavoro [75].
Nel 2004-2005 ho studiato il problema di rappresentare gli interi come somma di un primo e di un intero privo di potenze k-esime. Il lavoro [70] riguarda tale argomento.
Nel 2009-2010, in collaborazione con D. Bazzanella (Politecnico Torino) e A. Zaccagnini, ho studiato il problema di determinare per quali $\lambda > 1$ esiste una proporzione positiva di intervalli del tipo $(p, p + \lambda \log X]$, p primo, e $(m, m + \lambda \log X]$, m intero e X parametro sufficientemente grande, in cui esiste almeno un numero primo oppure non esiste alcun numero primo. Nel lavoro [63], sviluppiamo una tecnica per stimare i momenti di primi su intervalli del tipo $(p, p + h]$, p primo e $h \le X$, e questo nuovo ingrediente consente di ottenere stime che migliorano quelle note da più di vent'anni.
Nel 2009 ho collaborato con A. Perelli ed A. Zaccagnini al fine di dimostrare la validità in intervalli corti della formula asintotica di Montgomery-Hooley per la media quadratica della distribuzione dei primi in progressioni aritmetiche. Il lavoro è il numero [59].

Articoli di rassegna:
Il lavoro [87] è un survey riguardante la Congettura di Goldbach contenente anche una descrizione dei risultati presentati nella mia Tesi di Dottorato. Il lavoro [72] è un survey che riguarda la presentazione di due risultati sulla congettura di Goldbach e sulla congettura di Hardy–Littlewood. Il lavoro [44] è un survey che riguarda l'uso di somme esponenziali infinite nel metodo del cerchio. Il lavoro [27] espone le idee principali usate per migliorare l'efficienza computazionale del calcolo di $L'/L(1, \chi)$ mediante l'uso di formule di riflessione di funzioni speciali all'interno della Fast Fourier Transform.

Articoli principalmente computazionali o applicativi

Algoritmi sul prodotto di Mertens in progressioni aritmetiche:
Come ho già descritto precedentemente, in collaborazione con A. Zaccagnini ho affrontato il problema di determinare la costante che governa il termine asintotico nel prodotto di Mertens sulle progressioni aritmetiche. Dal punto di vista computazionale, nel 2008-2009, ne abbiamo calcolato gli effettivi valori numerici, perlomeno per tutte le progressioni aritmetiche di modulo $q \le 100$, con una

precisione di almeno 100 cifre decimali, articolo [65]. Il lavoro è stato inserito nella “On-Line Encyclopedia of Integer Sequences” al numero A340711; i risultati computazionali qui ottenuti sono anche menzionati ai numeri A340127-A340839-A340866.
Sempre nel 2009, in collaborazione con A. Zaccagnini, nel lavoro [60] abbiamo studiato le costanti presenti nelle formule asintotiche delle somme di Mertens e di Meissel–Mertens:

$$\sum_{p\equiv a \bmod q}\Big(\log\big(1-\frac{1}{p}\big)+\frac{1}{p}\Big) \qquad \text{e} \qquad \sum_{\substack{p\le x\\ p\equiv a \bmod q}}\frac{1}{p}=\frac{\log\log x}{\varphi(q)}+M(q,a)+\mathcal{O}_q\Big(\frac{1}{\log x}\Big), \quad \text{per } x\to\infty.$$

Vari casi della formula precedente sono stati inseriti nella “On-Line Encyclopedia of Integer Sequences”: A161529, A368644, A368645, A368646.

L’uso della Fast Fourier Transform nel calcolo di $L(1,\chi)$ e di $L'(1,\chi)$ e il calcolo delle costanti di Euler–Kronecker:
Nel 2019 ho rilasciato il lavoro [29], che riguarda lo sviluppo di un nuovo algoritmo per la valutazione delle costanti di Euler–Kronecker per campi ciclotomici $\mathbb{Q}(\zeta_q)$, $q\ge 3$ primo: tale costante è definita come $\gamma_q=\sum_{\chi\ne\chi_0} L'/L(1,\chi)$, dove q è un numero primo dispari. Tale algoritmo combina la Fast Fourier Transform con le formule di riflessione delle funzioni speciali coinvolte nel calcolo di $L(1,\chi)$ e di $L'(1,\chi)$. Queste idee hanno portato a ridurre l’occupazione di memoria richiesta e a migliorare in maniera drastica la complessità computazionale globale del calcolo.
Ciò ha permesso di ottenere un ampio insieme di informazioni relative ai valori di $L(1,\chi)$ e di $L'(1,\chi)$. Dato il ruolo centrale giocato da tali quantità all’interno della Teoria dei Numeri, non è sorprendente il fatto che, usando tali dati, si siano potuti ottenere diversi interessanti risultati.
In [29], ho esteso la conoscenza dei risultati numerici relativi alle costanti di Euler–Kronecker per campi ciclotomici $\mathbb{Q}(\zeta_q)$ fornendole per ogni primo q, $3\le q\le 10^6$. Ho anche determinato nuovi controesempi alla congettura di Ihara sulla positività di tali costanti; tali controesempi sono legati a numeri primi dell’ordine dei 10 miliardi, ossia 10 volte più grandi del precedente esempio di Ford, Luca e Moree. Tali dimensioni costituiscono una notevole sfida computazionale per i noti algoritmi di calcolo della Fast Fourier Transform e le risorse hardware attualmente a disposizione. Il lavoro è stato citato nella “On-Line Encyclopedia of Integer Sequences” al numero A135311.
Nel 2019, in collaborazione con P. Moree (Scientific Coordinator, MPIM, Bonn), S. Saad Eddin (Linz) e A. Sedunova (Purdue), ho studiato il comportamento del rapporto di Kummer $r(q)$ tra il primo fattore del numero delle classi di un campo ciclotomico $\mathbb{Q}(\zeta_q)$, q primo, $q\ge 3$, con il suo atteso ordine di grandezza; la parte computazionale del lavoro, in forma preliminare, è disponibile in questo preprint [93]. In tale parte computazionale, determiniamo anche nuovi estremi per $r(q)$. Il lavoro è stato citato nella “On-Line Encyclopedia of Integer Sequences” al numero A309520. Abbiamo ripreso a lavorare questi problemi nel Febbraio 2023.
In seguito, nel 2020, in collaborazione con L. Righi (Padova), ho sviluppato un algoritmo efficiente per il calcolo della funzione Gamma di Ramanujan-Deninger (lavoro [31]); tale algoritmo ha importanti ricadute anche sul calcolo delle costanti di Euler–Kronecker perché ne migliora enormemente la velocità di calcolo rispetto a quanto precedentemente possibile. Inserendo questo algoritmo di calcolo delle funzione Gamma di Ramanujan-Deninger all’interno dello studio delle costanti di Euler–Kronecker abbiamo ottenuto un ulteriore controesempio alla congettura di Ihara precendentemente menzionata; questa volta esso è legato ad un numero primo dell’ordine dei 50 miliardi, ossia circa 50 volte più grande rispetto agli esempi noti prima dei miei contributi. Abbiamo anche potuto estendere il calcolo di ogni costante di Euler–Kronecker di campi ciclotomici fino a raggiungere ogni primo q, $3\le q\le 10^7$.

Studio numerico delle disuguaglianze di Littlewood per $|L(1,\chi)|$:
Più recentemente (2019-2020) mi sono occupato di studiare numericamente la validità delle disuguaglianze di Littlewood per $|L(1,\chi)|$ (lavoro [30]), χ carattere primitivo non banale di Dirichlet modulo q, q primo, $3\le q\le 10^7$.

Studio numerico di disuguaglianze relative allo zero di Landau–Siegel:
Nel 2023 ho completato un lavoro che fornisce stime computazionali sullo zero di Landau–Siegel, [21].

Algoritmi per il calcolo di alcune funzioni speciali:
Nel 2022 ho sviluppato un nuovo algoritmo per calcolare efficientemente un insieme di funzioni speciali comprendente la funzione Γ di Euler, le funzioni digamma e polygamma, la funzione $\zeta(s,x)$ di Hurwitz e la sua derivata parziale prima $(\partial\zeta/\partial s)(s,x)$, le funzioni L di Dirichlet $L(s,\chi)$ e $L'(s,\chi)$. In particolare, in [23] ho mostrato come calcolare efficientemente $\zeta(s,x)$ per $s>1$ e $x>0$. Combinando tale procedura con la Fast Fourier transform e opportune formule di riflessione, ho ottenuto un algoritmo estremamente efficiente per il calcolo di $L(s,\chi)$, $s>1$, per ogni carattere di Dirichlet non principale definito mod q, dove q è un numero primo dispari. Alcune delle idee esposte in questo articolo sono state recepite all’interno del software PARI/GP.

Applicazioni crittografiche (un protocollo di re-codifica):
Per quanto riguarda le applicazioni crittografiche, il mio lavoro [22] riguardante un protocollo di re-encryption di dati immagazzinati su supporto digitale, è stato pubblicato nei proceedings della “15th International Conference on Ubiquitous Computing & Ambient Intelligence”, (UCAmI 2023).

La funzione di log-verosimiglianza per la distribuzione multinomiale di Dirichlet:
Nel 2020-2021, in collaborazione con M. Migliardi, ho inoltre notevolmente migliorato gli algoritmi esistenti per il calcolo della funzione di log-verosimiglianza per la distribuzione multinomiale di Dirichlet, si veda [24]. Tale distribuzione richiede il calcolo di valori in punti "vicini" della funzione $\log \Gamma$ ed è una quantità utile per interpretare statisticamente dati sperimentali in vari campi (per esempio, in genomica, data science, bayesian statistics, machine learning, natural language processing e per softwares di riconoscimento di immagini).
Negli anni successivi, in collaborazione con S.S. Al-Haj Baddar (University of Jordan) e M. Migliardi (Università di Padova), abbiamo ulteriormente sviluppando le applicazioni del lavoro [24], mostrando la sua applicabilità "pratica", si vedano [16], [17]. La velocità e precisione di calcolo di tale algoritmo lo rende molto interessante in diverse applicazioni quali: bayesian statistics, statistical inference, machine learning, data science, language modeling, facial recognition software, counting data clustering. In particolare, in [14], mostriamo che l'algoritmo in questione consente prestazioni migliori di quelle fornite utilizzando del funzioni predefinite dei packages Python-math e Scipy.

Ricerche in corso di sviluppo (2022-2025)

Valori della funzione τ di Ramanujan:
Nel 2022-2023, in collaborazione con Moree, ho anche studiato la distribuzione dei valori della funzione τ di Ramanujan e della somma dei divisori e divisori generalizzata nelle classi residuali quadratiche e non-quadratiche modulo un numero primo dispari q; si vedano [5], [6] (in preparazione), [13] (sottoposto), [8] (in preparazione).

Problemi applicativi:
Sto lavorando ad estendere il range di applicabilità del mio algoritmo presentato in [23] alla regione $\Re(s) > 0$. In particolare, ciò avrebbe conseguenze sui noti algoritmi per calcolare $L(s, \chi)$ nella striscia critica e sulla linea critica. Un'altra conseguenza riguarda il calcolo delle funzioni L di Dirichlet sulla linea $\Re(s) = 1$. Come già fatto in [23], non solo mostrerò l'algoritmo teorico ma ne fornirò anche una implementazione funzionante.

Articoli divulgativi e monografie; altri skills

Mi sono anche occupato, a più riprese, di divulgazione con particolare attenzione agli aspetti della Teoria dei Numeri maggiormente legati a discipline computazionali ed applicative. I lavori [79], [80], [77], [76] riguardano tale aspetto. In seguito ho collaborato con A. Zaccagnini ad una monografia [3] dedicata alle applicazioni crittografiche della Teoria dei Numeri. Una seconda monografia su tali argomenti, che non solo aggiorna il nostro precedente testo del 2004, ma lo estende ampiamente inserendo la descrizione di nuovi algoritmi e di ulteriori tecniche crittografiche, scritta nuovamente in collaborazione con A. Zaccagnini, è stata pubblicata nel 2015 [4]. Tale monografia è stata citata nella "On-Line Encyclopedia of Integer Sequences" al numero A000466.
Inoltre, su invito del centro PRISTEM-Bocconi, in collaborazione con A. Zaccagnini, ho scritto una serie di articoli divulgativi (identificati da [89], [90], [91] e [92]) su vari aspetti della primalità.
Nel 2014 ho scritto il capitolo 11 del volume di presentazione della mostra "Numeri, tutto quello che conta, da zero a infinito", a cura di C. Bartocci e L. Civalleri, si veda [51].
Nel 2017, in collaborazione con A. Zaccagnini, ho scritto un articolo divulgativo sulla disciplina della Teoria dei Numeri, [42] per la rivista "Sapere", la più antica rivista di divulgazione scientifica italiana.
Nel 2005 ho scritto una colonna dedicata al problema dei primi gemelli per il giornale "La Voz de Almeria" (n. [71]). Nel 2005-2007 ho coordinato il modulo di Crittografia per il "Progetto Nazionale Lauree Scientifiche" per il Veneto. La pubblicazione [2], sviluppata in collaborazione con A. Zaccagnini, riguarda il materiale preparato a tale scopo.
Nel 2016-17, basandomi su parte del materiale accumulato per la didattica nei vent'anni precedenti, ho redatto il testo [1] riguardante un primo corso di Analisi Matematica.

Altri skills: linguaggi di programmazione e di typesetting:
Oltre ad essere esperto nell'uso di LaTeX, fatto che mi ha permesso di scrivere autonomamente tutta la mia produzione scientifica nonché le quattro monografie di cui sono autore (tre delle quali in collaborazione), durante gli ultimi quaranta anni ho usato diversi linguaggi di programmazione per la mia attività di studio e, in seguito, di ricerca. In particolare sono in grado di scrivere programmi in: EDL (IBM series/1 event driven language), Fortran IV, Fortran 77, MS-DOS Basic, Cobol, Digital PDP-11 Assembler, Pascal, Modula-2, LISP, C. Più recentemente ho imparato ad usare alcuni linguaggi di scripting quali Python e quelli dei CAS denominati Pari/GP (per la teoria dei numeri) e MAXIMA (matematica generale). In diverse occasioni ho sfruttato queste abilità in progetti di ricerca; essi sono elencati nella relativa sezione che descrive la mia attività scientifica in progetti computazionali. Tutti i programmi collegati alla mia attività scientifica e di ricerca sono disponibili all'indirizzo web: Programs-Languasco.

Produzione scientifica complessiva

Monografie:

[1] **A. Languasco**. *Analisi Matematica 1*. Ulrico Hoepli editore, 2017. Publisher link.

[2] **A. Languasco** and A. Zaccagnini. *Crittografia*. CLEUP, Padova, 2006. Progetto Lauree Scientifiche per il Veneto.
[3] **A. Languasco** and A. Zaccagnini. *Introduzione alla Crittografia*. Ulrico Hoepli Editore, 2004.
[4] **A. Languasco** and A. Zaccagnini. *Manuale di Crittografia*. Ulrico Hoepli Editore, 2015. Publisher link.

Articoli in preparazione:

[5] **A. Languasco** and P. Moree. Bias of the Ramanujan tau and the sum of divisors function for even moduli. *in preparation*, 2025.
[6] **A. Languasco** and P. Moree. Bias of the Ramanujan tau and the sum of divisors function for odd moduli. *in preparation*, 2025.
[7] **A. Languasco** and P. Moree. Easy counting of irreducible self-reciprocal polynomials over a finite field and partial Euler products. 2025. in preparation.
[8] **A. Languasco** and P. Moree. Quadratic residue bias of the divisor function and fake mu's. *in preparation*, 2025.
[9] S. Fan, **A. Languasco**, R. Lunia, and P. Moree. Coprime and squarefree ideals in infinite families of number fields. 2025. in preparation.

Articoli sottoposti per la pubblicazione:

[10] **A. Languasco**, F. Luca, P. Moree, and A. Togbé. Sequences of integers generated by two fixed primes. *submitted*, 2023. DOI-link:, MR:, ZBL:.
[11] N. Kandhil, **A. Languasco**, and P. Moree. Pair Correlation of zeros of Dirichlet L-Functions: A possible path towards the conjectures of Chowla, Elliott–Halberstam and Montgomery. *submitted*, 2024. DOI.
[12] **A. Languasco**, R. Lunia, and P. Moree. Counting ideals in abelian number fields. *submitted*, 2025. DOI.
[13] **A. Languasco** and P. Moree. Quadratic residue bias of the divisor function, Fekete polynomials and prime gaps. *submitted*, 2025. Computational part.

Articoli in corso di pubblicazione:

[14] S. Al Haj-Baddar, **A. Languasco**, and M. Migliardi. Fast and accurate implementation of the Dirichlet multinomial log-likelihood function. *accepted for the International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA'25), Antalya, Turkiye, on 07-09 August 2025*, 2025. DOI, CodeOcean capsule.

Articoli pubblicati (in ordine cronologico inverso):

[15] **A. Languasco** and P. Moree. Euler constants from primes in arithmetic progression. *Math. Comp.*, 95:363–387, 2026. DOI, Code Ocean capsule, MR:4959026, Google Scholar: 1.
[16] S. Al Haj-Baddar, **A. Languasco**, and M. Migliardi. Efficient analysis of overdispersed data using an accurate computation of the Dirichlet multinomial distribution. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 47:1181–1189, 2025. DOI, CodeOcean capsule.
[17] S. Al Haj-Baddar, **A. Languasco**, and M. Migliardi. Modeling and forecasting overdispersed IoT data using an efficient and accurate computation of the Dirichlet Multinomial distribution. In *2025 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 2025*, pages 28–32, 2025. DOI.
[18] N. Kandhil, **A. Languasco**, and P. Moree. The Brauer–Siegel ratio for prime cyclotomic fields. *Pacific Journal of Mathematics*, 334:167–182, 2025. DOI; extended version, MR:4859074, ZBL:7982969.
[19] N. Kandhil, **A. Languasco**, P. Moree, S. Saad Eddin, and A. Sedunova. Relative class numbers and Euler–Kronecker constants of maximal real cyclotomic subfields. *Math. Comp.*, 2025. electronically published on August 25, 2025, DOI (to appear in print). Computational part.
[20] N. Kandhil, **A. Languasco**, P. Moree, S. Saad Eddin, and A. Sedunova. The Kummer ratio of the relative class number for prime cyclotomic fields. *J. Math. Anal. Appl.*, 538(1):Paper No. 128368, 2024. DOI, MR:4729781, ZBL:7848696.
[21] **A. Languasco**. Numerical estimates on the Landau-Siegel zero and other related quantities. *J. Number Theory*, 251:185–209, 2023. DOI, MR:4598945, ZBL:7695616.
[22] **A. Languasco**. A partially decentralised protocol for a distributed encrypted storage system. In José Bravo and Gabriel Urzáiz, editors, *Proceedings of the 15th International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2023)*, pages 195–204, Cham, 2023. Springer Nature Switzerland. DOI.
[23] **A. Languasco**. A unified strategy to compute some special functions of number–theoretic interest. *J. Number Theory*, 247:118–161, 2023. DOI, MR:4546697, ZBL:7662018.
[24] **A. Languasco** and M. Migliardi. On the fast computation of the Dirichlet-multinomial log-likelihood function. *Comput. Stat.*, 38:1995–2013, 2023. DOI,MR:4672333, ZBL:7800948.
[25] A. Ciolan, **A. Languasco**, and P. Moree. Landau and Ramanujan approximations for divisor sums and coefficients of cusp forms. *J. Math. Anal. Appl.*, 519:1–48, paper n. 126854, 2023. DOI, MR:4511375, ZBL:07624143.
[26] Y. Lamzouri and **A. Languasco**. Small values of $|L'/L(1,\chi)|$. *Exp. Math.*, 32:362–377, 2023. DOI, MR:4592953, ZBL:7708949.

[27] **A. Languasco**. On computing $L'/L(1,\chi)$. *Rendiconti Sem. Mat. Univ. Pol. Torino*, 80:55–71, 2022. Proceedings of the fifth Number Theory Meeting, Università and Politecnico di Torino, October 26–27th, 2021. DOI. MR:4515572, ZBL:7626422.

[28] **A. Languasco** and T. S. Trudgian. Uniform effective estimates for $|L(1,\chi)|$. *J. Number Theory*, 236:245–260, 2022. DOI, MR:4395349, ZBL:7493024.

[29] **A. Languasco**. Efficient computation of the Euler-Kronecker constants for prime cyclotomic fields. *Res. Number Theory*, 7, paper n. 2, 2021. DOI, MR:4194178, ZBL:07304549.

[30] **A. Languasco**. Numerical verification of Littlewood's bounds for $|L(1,\chi)|$. *J. Number Theory*, 223:12–34, 2021. DOI, MR:4213696, ZBL:07329220.

[31] **A. Languasco** and L. Righi. A fast algorithm to compute the Ramanujan–Deninger Gamma function and some number–theoretic applications. *Math. Comp.*, 90:2899–2921, 2021. DOI, MR:4305373; ZBL:07390221.

[32] **A. Languasco** and A. Zaccagnini. Sum of one prime power and two squares of primes in short intervals. *Rocky Mountain J. Math.*, 51:213–224, 2021. DOI, MR:4280109, ZBL:07393760.

[33] **A. Languasco** and A. Zaccagnini. Short intervals asymptotic formulae for binary problems with prime powers, II. *J. Aus. Math. Soc.*, 109:351–370, 2020. DOI, MR:4190085, ZBL:07286548.

[34] M. Cantarini, A. Gambini, **A. Languasco**, and A. Zaccagnini. On a average ternary problem with prime powers. *Ramanujan J.*, 53:155–166, 2020. DOI, MR:4148463, ZBL:07176138.

[35] **A. Languasco** and A. Zaccagnini. A Cesàro average for an additive problem with prime powers. In *Proceedings of the conference "Number Theory Week", Poznań, September 4–8, 2017. Banach Center Publications, Institute of Mathematics, Polish Academy of Sciences, Warszawa*, volume 118, pages 137–152, 2019. DOI, MR:3931260, ZBL:07087893.

[36] **A. Languasco** and A. Zaccagnini. A Cesàro average for generalised Hardy-Littlewood numbers. *Kodai Math. J.*, 42:358–375, 2019. DOI, MR:3981309, ZBL:07108016.

[37] **A. Languasco** and A. Zaccagnini. Sums of four prime cubes in short intervals. *Acta Math. Hungar.*, 159:150–163, 2019. DOI, MR:4003700, ZBL:07119764.

[38] **A. Languasco** and A. Zaccagnini. Short intervals asymptotic formulae for binary problems with prime powers. *J. Théor. Nombres Bordeaux*, 30:609–635, 2018. DOI, MR:3891329, ZBL:3A07081564.

[39] A. Gambini, **A. Languasco**, and A. Zaccagnini. A diophantine approximation problem with two primes and one k-power of a prime. *J. Number Theory*, 188:210–228, 2018. DOI, MR:3778631, ZBL:06855844.

[40] **A. Languasco**, A. Perelli, and A. Zaccagnini. An extended pair-correlation conjecture and primes in short intervals. *Trans. Amer. Math. Soc.*, 369(6):4235–4250, 2017. DOI, MR:3624407, ZBL:06698813.

[41] **A. Languasco** and A. Zaccagnini. Cesàro average in short intervals for Goldbach numbers. *Proc. Amer. Math. Soc.*, 145(10):4175–4186, 2017. DOI, MR:3690604, ZBL:06767077.

[42] **A. Languasco** and A. Zaccagnini. Il fascino discreto della teoria dei numeri. *Sapere*, 1:22–26, 2017. DOI.

[43] **A. Languasco** and A. Zaccagnini. Short intervals asymptotic formulae for binary problems with primes and powers, I: density 3/2. *Ramanujan J.*, 42:371–383, 2017. DOI, MR:3596938, ZBL:06692048.

[44] **A. Languasco**. Applications of some exponential sums on prime powers: a survey. In *Proceedings of the "Terzo Incontro Italiano di Teoria dei Numeri", Scuola Normale Superiore, Pisa, 21–24 Settembre 2015. Rivista di Matematica della Università di Parma*, volume 7, pages 19–37, 2016. DOI, MR:3675401, ZBL:06760984.

[45] **A. Languasco**, A. Perelli, and A. Zaccagnini. An extension of the pair-correlation conjecture and applications. *Math. Res. Lett.*, 23(1):201–220, 2016. DOI, MR:3512883, ZBL:06609432.

[46] **A. Languasco** and A. Zaccagnini. A Diophantine problem with prime variables. In V. Kumar Murty, D. S. Ramana, and R. Thangadurai, editors, *Highly Composite: Papers in Number Theory, Proceedings of the International Meeting on Number Theory, celebrating the 60th Birthday of Professor R. Balasubramanian (Allahabad, 2011)*, volume 23 of *Ramanujan Math. Soc. Lect. Notes Ser.*, pages 157–168. Ramanujan Math. Soc., Mysore, 2016. DOI, MR:3692733, ZBL:1416.11143.

[47] **A. Languasco** and A. Zaccagnini. Short intervals asymptotic formulae for binary problems with primes and powers, II: density 1. *Monatsh. Math.*, 181:419–435, 2016. DOI, MR:3539942, ZBL:1350.11089.

[48] **A. Languasco** and A. Zaccagnini. Sum of one prime and two squares of primes in short intervals. *J. Number Theory*, 159:45–58, 2016. DOI, MR:3412711, ZBL:06497366.

[49] **A. Languasco** and A. Zaccagnini. A Cesàro Average of Goldbach numbers. *Forum Math.*, 27:1945–1960, 2015. DOI, MR:3365783, ZBL:06458901.

[50] **A. Languasco** and A. Zaccagnini. Explicit relations between primes in short intervals and exponential sums over primes. *Funct. Approx. Comment. Math.*, 51:379–391, 2014. DOI, MR:3282634, ZBL:06380131.

[51] **A. Languasco**. Numeri primi. In C. Bartocci and L. Civalleri, editors, *Numeri. Tutto quello che conta. Da zero a infinito*, pages 183–193. Codice Edizioni, Torino, Italy, 2014. (Chapter 11 of the volume).

[52] **A. Languasco** and A. Zaccagnini. A Cesàro Average of Hardy–Littlewood numbers. *J. Math. Anal. Appl.*, 401:568–577, 2013. DOI, MR:3018008, ZBL:06156267.

[53] **A. Languasco** and A. Zaccagnini. On a ternary Diophantine problem with mixed powers of primes. *Acta Arith.*, 159:345–362, 2013. DOI, MR:3080797, ZBL:06184261.

[54] **A. Languasco**, A. Perelli, and A. Zaccagnini. Explicit relations between pair correlation of zeros and primes in short intervals. *J. Math. Anal. Appl.*, 394:761–771, 2012. DOI, MR:2927496, ZBL:06062862.

[55] **A. Languasco** and V. Settimi. On a Diophantine problem with one prime, two squares of primes and s powers of two. *Acta Arith.*, 154:385–412, 2012. DOI, MR:2949876, ZBL:06055436.

[56] **A. Languasco** and A. Zaccagnini. A Diophantine problem with a prime and three squares of primes. *J. Number Theory*, 132:3016–3028, 2012. DOI, MR:2965205, ZBL:06097276.

[57] **A. Languasco** and A. Zaccagnini. The number of Goldbach representations of an integer. *Proc. Amer. Math. Soc.*, 140:795–804, 2012. DOI, MR:2869064, ZBL:1252.11078.

[58] **A. Languasco** and A. Zaccagnini. Sums of many primes. *J. Number Theory*, 132:1265–1283, 2012. DOI, MR:2899803, ZBL:06031097.

[59] **A. Languasco**, A. Perelli, and A. Zaccagnini. On the Montgomery-Hooley theorem in short intervals. *Mathematika*, 52:231–243, 2010. DOI, MR:2678027, ZBL:1238.11087.

[60] **A. Languasco** and A. Zaccagnini. Computing the Mertens and Meissel-Mertens constants for sums over arithmetic progressions. *Exp. Math.*, 19:279–284, 2010. With an appendix by Karl K. Norton. DOI, MR:2743571, ZBL:06074851.

[61] **A. Languasco** and A. Zaccagnini. On a Diophantine problem with two primes and s powers of two. *Acta Arith.*, 145:193–208, 2010. DOI, MR:2733083, ZBL:1222.11049.

[62] **A. Languasco** and A. Zaccagnini. On the constant in the Mertens product for arithmetic progressions. I. Identities. *Funct. Approx. Comment. Math.*, 42:17–27, 2010. DOI, MR:2640766, ZBL:1206.11112.

[63] D. Bazzanella, **A. Languasco**, and A. Zaccagnini. Prime numbers in logarithmic intervals. *Trans. Amer. Math. Soc.*, 362:2667–2684, 2010. DOI, MR:2584615, ZBL:1200.11072.

[64] **A. Languasco**. A conditional result on the exceptional set for Hardy-Littlewood numbers in short intervals. *Int. J. Number Theory*, 5:933–951, 2009. DOI, MR:2569737, ZBL:1251.11068.

[65] **A. Languasco** and A. Zaccagnini. On the constant in the Mertens product for arithmetic progressions. II. Numerical values. *Math. Comp.*, 78:315–326, 2009. DOI, MR:2448709, ZBL:1214.11108.

[66] **A. Languasco** and A. Zaccagnini. On the Hardy-Littlewood problem in short intervals. *Int. J. Number Theory*, 4:715–723, 2008. DOI, MR:2458837, ZBL:1251.11069.

[67] **A. Languasco** and A. Zaccagnini. Some estimates for the average of the error term of the Mertens product for arithmetic progressions. *Funct. Approx. Comment. Math.*, 38:41–47, 2008. DOI, MR:2433787, ZBL:1233.11100.

[68] **A. Languasco**, J. Pintz, and A. Zaccagnini. On the sum of two primes and k powers of two. *Bull. Lond. Math. Soc.*, 39:771–780, 2007. DOI, MR:2365226, ZBL:1137.11066.

[69] **A. Languasco** and A. Zaccagnini. A note on Mertens' formula for arithmetic progressions. *J. Number Theory*, 127:37–46, 2007. DOI, MR:2351662, ZBL:1210.11105.

[70] **A. Languasco**. On the sum of a prime and a k–free number. *Funct. Approx. Comment. Math.*, 34:19–26, 2005. DOI, MR:2269661, ZBL:1228.11156.

[71] **A. Languasco**. Primos Gemelos. *La Voz de Almeria, Seccion Matematica*, 2005. (pubblicato il 04/09/2005 in lingua spagnola, traduzione in Spagnolo di Juan Cuadra Diaz).

[72] **A. Languasco**. The exceptional set in short intervals for two additive problems with primes: a survey. *Riv. Mat. Univ. Parma (7)*, 3*:223–231, 2004. DOI, MR:2128851, ZBL:1166.11348.

[73] **A. Languasco**. On the exceptional set for Hardy-Littlewood's numbers in short intervals. *Tsukuba J. Math.*, 28:169–192, 2004. DOI, MR:2082228, ZBL:1068.11066. *Corrigendum ibid.*, DOI, Tsukuba J. Math., **30** (2006), 237–240, MR:2248294, ZBL:1201.11095.

[74] **A. Languasco**. On the exceptional set of Goldbach's problem in short intervals. *Monatsh. Math.*, 141:147–169, 2004. DOI, MR:2037990, ZBL:1059.11059.

[75] **A. Languasco**, F. Menegazzo, and M. Morigi. On the composition length of finite primitive linear groups. *Arch. Math.*, 79:408–417, 2002. DOI, MR:1966776, ZBL:1015.20034.

[76] **A. Languasco** and A. Perelli. Crittografia e firma digitale. In M. Emmer and M. Manaresi, editors, *Matematica, Arte, Tecnologia, Cinema*, pages 99–106, Bologna, 2002. Springer-Verlag, Milano. English translation in *Mathematics, Art, Technology, and Cinema*, Springer-Verlag, Berlin, Heidelberg, New York, 2003.

[77] **A. Languasco**. An Introduction to Cryptography. *Queen's Papers in Pure and Applied Mathematics*, 119(121–140), 2000. in The Curves Seminar at Queen's , vol. 13, ed. da A.V. Geramita.

[78] **A. Languasco**. Some refinements of error terms estimates for certain additive problems with primes. *J. Number Theory*, 81:149–161, 2000. DOI, MR:1743499, ZBL:1003.11047.

[79] **A. Languasco** and A. Perelli. Numeri Primi e Crittografia. In M. Emmer, editor, *Matematica e Cultura 2000*, pages 227–233, Venezia, 2000. Springer-Verlag, Milano. English translation in *Mathematics and Culture I*, Springer-Verlag, Berlin, Heidelberg, New York, 2003.

[80] **A. Languasco** and A. Perelli. Pair correlation of zeros, primes in short intervals and exponential sums over primes. *J. Number Theory*, 84:292–304, 2000. DOI, MR:1796516, ZBL:0973.11081.

[81] D. Bazzanella and **A. Languasco**. On the asymptotic formula for Goldbach numbers in short intervals. *Studia Sci. Math. Hungar.*, 36:185–199, 2000. DOI, MR:1768230, ZBL:0973.11089.

[82] J. Kaczorowski, **A. Languasco**, and A. Perelli. A note on Landau's formula. *Funct. Approx. Comment. Math.*, 28:173–186, 2000. Dedicated to W lodzimierz Staś on the occasion of his 75th birthday. DOI, MR:1824002, ZBL:1034.11049.

[83] **A. Languasco**. A conditional result on Goldbach numbers in short intervals. *Acta Arith.*, 83:93–103, 1998. DOI, MR:1490641, ZBL:0940.11045.

[84] **A. Languasco**. A note on primes and Goldbach numbers in short intervals. *Acta Math. Hungar.*, 79:191–206, 1998. DOI, MR:1616038, ZBL:0940.11046.

[85] **A. Languasco**. A singular series average and Goldbach numbers in short intervals. *Acta Arith.*, 83:171–179, 1998. DOI, MR:1490647, ZBL:0894.11037.

[86] **A. Languasco** and A. Perelli. A pair correlation hypothesis and the exceptional set in Goldbach's problem. *Mathematika*, 43:349–361, 1996. DOI, MR:1433280, ZBL:0884.11042.

[87] **A. Languasco**. Some results on Goldbach's problem. *Rend. Sem. Mat. Univ. Politec. Torino*, 53(4):325–337, 1995. DOI, MR:1452389, ZBL:0882.11055.

[88] **A. Languasco** and A. Perelli. On Linnik's theorem on Goldbach numbers in short intervals and related problems. *Ann. Inst. Fourier*, 44:307–322, 1994. DOI, MR:1296733, ZBL:0799.11040.

Web-pubblicazioni:

[89] **A. Languasco** and A. Zaccagnini. Alcune proprietà dei numeri primi, I. *Sito web Bocconi–Pristem*, 2005. link1; link2.

[90] **A. Languasco** and A. Zaccagnini. Alcune proprietà dei numeri primi, II. *Sito web Bocconi–Pristem*, 2005. link1; link2.

[91] **A. Languasco** and A. Zaccagnini. Esistono piccoli intervalli fra primi consecutivi! *Sito web Bocconi–Pristem*, 2005. link1; link2.

[92] **A. Languasco** and A. Zaccagnini. Intervalli fra numeri primi consecutivi. *Sito web Bocconi–Pristem*, 2005. link1; link2.

[93] **A. Languasco**, P. Moree, S. Saad Eddin, and A. Sedunova. Computation of the Kummer ratio of the class number for prime cyclotomic fields. *Arxiv*, 2019. DOI (web publication).

Dispense e altre pubblicazioni:

[94] **A. Languasco**. Codici a chiave pubblica ed Algoritmi di Primalità. Master's thesis, Università di Genova, 1989. (italian).

[95] **A. Languasco**. *La congettura di Goldbach*. PhD thesis, Politecnico di Torino, Università di Torino, Università di Genova, 1995. (italian).

[96] **A. Languasco**. Dispense di Analisi Matematica 1. Lecture Notes, Manuscript, (italian), 1999.

[97] **A. Languasco**. Dispense di Algebra Lineare, Geometria e Calcolo Differenziale in più variabili (Matematica B). Lecture Notes, Manuscript, (italian), 2002.

[98] B. Bruno and **A. Languasco**. Dispense integrative per il Corso di Istituzioni di Analisi Matematica II. Lecture Notes, Manuscript, (italian), 2003.

[99] **A. Languasco**. Dispense per il Corso di Metodi Matematici per la Statistica (parte di Analisi Matematica). Lecture Notes, Manuscript, (italian), 2005.

[100] **A. Languasco**. Dispense per il Corso di Fondamenti di Analisi Matematica 2. Lecture Notes, Manuscript, (italian), 2020.

Padova, 21 settembre 2025

Alessandro Languasco

Alessandro LANGUASCO