

Dati anagrafici: nome: **LANGUASCO ALESSANDRO**, nato il 23/12/1966 ad Imperia (IM), Italia, cittadinanza: italiana.

Posizione attuale: Professore Associato confermato di MAT/05 (Analisi Matematica) presso la Facoltà di Statistica dell'Università di Padova dal 1 ottobre 2009.

Afferenza: Dal 01/01/2012 sono afferente al Dipartimento di Matematica, Università di Padova. Dal 26/08/1998 al 31/12/2011 sono stato afferente al Dipartimento di Matematica Pura e Applicata, Università di Padova.

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

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”; relatore Prof. A. Perelli.

1994: *Dottorato di Ricerca in Matematica*, Università di Torino, Italia. Dissertazione in Teoria Analitica dei Numeri intitolata “La congettura di Goldbach”, sotto la supervisione del Prof. A. Perelli.

1998: *Ricercatore 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.

2009: *Conferma nel ruolo di Professore Associato di Analisi Matematica (MAT/05)*, primo ottobre 2009.

Monografie: 2004: Ho pubblicato in collaborazione con A. Zaccagnini dell'Università di Parma, il testo “Introduzione alla Crittografia”, [42], pubblicato dalla Hoepli editrice.

2006: Ho pubblicato in collaborazione con A. Zaccagnini dell'Università di Parma, il testo “Crittografia”, [43], pubblicato dalla CLEUP per il Progetto Lauree Scientifiche per il Veneto.

Attività Internazionali: 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 ex-terra-europei: Chennai (India), Stellenbosch (Sud Africa), Montreal Concordia (Canada).

Attività Organizzative e di Alta Formazione: 1) da novembre 2007 a maggio 2011 sono stato Rappresentante dell'Area Matematica presso la Facoltà di Statistica dell'Università di Padova.

2) Nel 2007 la fondazione CARIPARO ha finanziato una borsa di studio di Dottorato in Matematica (indirizzo sito web: <http://www.unipd.it/stdoc/elencofinanziatiperweb.pdf>).

3) da gennaio 2008 faccio parte del Consiglio dei Docenti della Scuola di Dottorato in Matematica dell'Università di Padova.

4) da giugno 2009 faccio parte della “Commissione Pagine Web” del Dipartimento di Matematica Pura e Applicata, Università di Padova. Da Gennaio 2012 ne sono il coordinatore.

5) 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.

6) 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 <http://webwork.maa.org>

7) da febbraio ad aprile 2011 ho fatto parte della “Commissione Nuovo Dipartimento” del Dipartimento di Matematica Pura e Applicata, 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:

1) Novembre 2006: Esame di Ammissione alla Scuola di Dottorato in Matematica dell'Università di Padova;

2) Gennaio 2007: Esame Finale per il conseguimento del titolo di Dottore di Ricerca in Matematica dell'Università di Torino, candidato Dr. Stefano Barbero.

3) 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.

4) 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.

5) 2009: Valutazione dei “Progetti per Assegni di Ricerca” per l'Area 01 Matematica, Università di Padova.

- 6) Novembre 2010: Esame Finale per il conseguimento del titolo di Dottore di Ricerca in Matematica dell'Università di Trento, candidato Dr. Luca Goldoni.

Borse di studio e di ricerca: Sono risultato vincitore delle seguenti Borse di Studio.

- 1) Marzo 1991 - Novembre 1994: Borsa di studio del dottorato di ricerca (Università di Torino).
- 2) Marzo 1996 - Febbraio 1997: Borsa di studio C.N.R. "ricerca" n. 201.01.121.
- 3) Marzo 1997 - Giugno 1997: Borsa di studio C.N.R. "ricerca" n. 201.01.123.
- 4) Luglio 1997 - Agosto 1998: Borsa di studio post-dottorato dell'Università di Genova.

Attività didattica:

Affidamenti: Sono stato titolare per Affidamento 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 (Teoria della funzione ζ di Riemann ed applicazioni)", 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:** "Crittografia", Laurea Specialistica in Informatica ed in Matematica, Erasmus Mundus Master ALGANT, Facoltà di Scienze MM.FF.NN., Università di Padova. Dal 2005/2006 il corso è tenuto in lingua inglese.

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".

Corsi di Master: Sono stato titolare dei seguenti corsi per varie Scuole di Master:

- 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: 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.

- Studenti di Dottorato:** 1) Sono stato Advisor della Tesi di Dottorato in Matematica della Dott.ssa Valentina Settimi, intitolata “On some additive problems with primes and powers of a fixed integer”.
- 2) Sono stato Co-advisor della Tesi di Dottorato in Matematica della Dott.ssa Antonella Rossi (advisor: Prof. Alessandro Zaccagnini), Dottorato in Matematica, Consorzio Universitario Milano-Insubria-Parma-Trieste.

Tesi di Laurea Triennale o Magistrale: Sono stato relatore di 26 Tesi di Laurea in Teoria dei Numeri, sia per quanto riguarda aspetti teorici che computazionali.

- 1) 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)
- 2) 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)
- 3) 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)
- 4) relatore della tesi di Laurea (triennale) in Statistica e Gestione delle Imprese di N. Orsatti intitolata “Alcuni aspetti della Crittografia”. (2002)
- 5) 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)
- 6) relatore della tesi di Laurea (triennale) in Matematica di A. Morra intitolata “Curve ellittiche su campi finiti: alcune applicazioni alla crittografia”. (2004)
- 7) 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)
- 8) relatore della tesi di Laurea (triennale) in Matematica di V. Settimi intitolata “Pseudocasualità e crittografia: alcuni metodi”. (2005)
- 9) relatore della tesi di Laurea (triennale) in Matematica di D. Cricco intitolata “Il Crivello Quadratico di Pomerance”. (2005)
- 10) relatore della tesi di Laurea in Matematica (vecchio ordinamento) di D. Alessio intitolata “Reticoli: aspetti algoritmici e loro applicazioni crittografiche”. (2006)
- 11) relatore della tesi di Laurea in Matematica (vecchio ordinamento) di L. Doni intitolata “Crittografia classica e moderna: alcuni metodi”. (2006)
- 12) 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)
- 13) relatore della tesi di Laurea Specialistica in Matematica di T. Majumdar (studente ALGANT) intitolata “On the Large Sieve”. (2008)
- 14) 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)
- 15) relatore della tesi di Laurea Triennale in Matematica di E. Zonta intitolata “Codici, fattorizzazione e primalità con curve ellittiche”. (2008)
- 16) 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)
- 17) relatore della tesi di Laurea Specialistica in Matematica di S. Bettin intitolata “Alcuni problemi equivalenti all’Ipotesi di Riemann”. (2008)
- 18) relatore della tesi di Laurea Specialistica in Matematica di V. Gauthier (studente ALGANT) intitolata “On some polynomial-time primality algorithms”. (2008)
- 19) relatore della tesi di Laurea Specialistica in Matematica di L. Corsi intitolata “Alcuni algoritmi per il Logaritmo Discreto”. (2009)
- 20) relatore della tesi di Laurea Specialistica in Matematica di L. Maggiolo intitolata “Crivelli dei Campi di Numeri”. (2009)
- 21) relatore della tesi di Laurea Specialistica in Matematica di F. Melgrani intitolata “L’algoritmo di Schoof”. (2010)
- 22) relatore della tesi di Laurea Specialistica in Matematica di E. Scipioni intitolata “Alcuni attacchi a RSA e sue varianti”. (2010)
- 23) 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)
- 24) relatore della tesi di Laurea Triennale in Matematica, di R. Tonon intitolata “Sulla dimostrazione elementare del Teorema dei Numeri Primi”. (2012)
- 25) relatore della tesi di Laurea Magistrale in Matematica, di S. Zuliani intitolata “Il decimo problema di Hilbert”. (2012), in corso di elaborazione.
- 26) relatore della tesi di Laurea Triennale in Matematica, di G. Di Salvo intitolata “Sul Teorema dei Numeri Primi”. (2012),

in corso di elaborazione.

- Attività divulgativa:** 1) **1998:** conferenza per la sezione di Padova dell'associazione "Mathesis" intitolata "Una breve introduzione alla crittografia".
- 2) **2001:** - Intervista su "Steganografia e Crittografia" nel programma di divulgazione scientifica "Il sommergibile" di V. Masotti, trasmesso dalla Radio Svizzera Italiana.
- Intervista su "Trasmissioni e codici cifrati" nel programma "GR-Scienza" di S. Sciancalepore, trasmesso dal consorzio radiofonico BluSat.
- 3) **2005-2007:** ho partecipato al Progetto Lauree Scientifiche coordinando il progetto "Crittografia" per quattro diverse Scuole Superiori del Veneto.
- 4) **2009:** durante il convegno "Advances in Number Theory and Geometry", Verbania, sono stato intervistato da U. Rondi per il programma RAI intitolato "La storia siamo noi".
- 5) **2010:** Ho presentato la conferenza "Comunicazione sicura nell'era di Internet", per la serie di conferenze "Eppur si Muove".
- 6) **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".

- Collaborazione con riviste:** 1) 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 37 recensioni (fino al 20 aprile 2012).
- 2) **2003-2005:** Managing editor (diffusione e sviluppo della versione elettronica) per la rivista "Rendiconti del Seminario Matematico dell'Università di Padova".
- 3) **Referee** per le riviste Rendiconti del Seminario Matematico dell'Università di Padova; International Journal of Number Theory; Journal of Number Theory; Monatshäfte für Mathematik; Missouri Journal of Mathematical Sciences; Functiones et Approximatio, Commentarii Mathematici; Bollettino dell'Unione Matematica Italiana; Rendiconti del Seminario Matematico dell'Università di Torino; Acta Arithmetica.

- Partecipazione a Conferenze e Convegni:** 1) Gennaio 1995: Incontro Italiano di Teoria dei Numeri, Roma, Italia, (speaker).
- 2) Luglio 1997: Arithmetical Theory of Elliptic Curves, CIME Course, Cetraro (Cs), Italia.
- 3) Marzo 1999: Matematica e Cultura, Venezia, Italia.
- 4) Luglio 2002: Analytic Number Theory, CIME Course, Cetraro (Cs), Italia.
- 5) Luglio 2003: Journées Arithmétiques 2003, Graz, Austria.
- 6) Novembre 2003: Secondo Incontro Italiano di Teoria dei Numeri, Parma, Italia, (speaker).
- 7) Luglio 2005: Journées Arithmétiques 2005, Marseille, Francia.
- 8) Maggio 2006: Italian-Polish Number Theory Days, Poznań, Polonia (invited speaker).
- 9) Luglio 2006: Special Session in Number Theory of the SIMAI-SMAI-SMF-UMI meeting, Torino, Italia.
- 10) Luglio 2007: Journées Arithmétiques 2007, Edimburgo, Regno Unito, (speaker).
- 11) Settembre 2007: Arithmetic Geometry, CIME Course, Cetraro (Cs), Italia.
- 12) Maggio 2008: Analytic Number Theory Workshop, Parma, Italia, (invited speaker).
- 13) Settembre 2008: A p -adic differential equations: a conference in honor of Gilles Christol, Bressanone (Italia).
- 14) Aprile 2009: Advances in Number Theory and Geometry, Verbania (Italy).
- 15) Maggio 2009: La Teoria dei Numeri, Università di Roma Tre, Roma (Italy), (invited speaker).
- 16) Marzo 2010: International Italy-India Conference on Diophantine and Analytic Number Theory, Scuola Normale Superiore, Pisa (Italy), (invited speaker).
- 17) Agosto-Settembre 2010: Analytic and Combinatorial Number Theory, ICM satellite conference, Institute of Mathematical Sciences, Chennai (India), (invited speaker).
- 18) 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).
- 19) 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.
- 20) Agosto 2011: Paul Turán Memorial Conference, 22-26 August 2011, Budapest, Hungary.
- 21) Settembre 2011: Congresso UMI, 12-16 Settembre 2011, Bologna, Italy (chairman di sezione).

- Attività seminariale:** 1) "Comologia di Čech", per il corso di Algebra Commutativa (Prof. P. Valabrega) del Dottorato di Ricerca del consorzio UniTo, PoliTo, UniGe, 1991.
- 2) "Analisi non-standard" per il corso di Logica Matematica (Prof. G. Lolli) del Dottorato di Ricerca del consorzio UniTo, PoliTo, UniGe, 1991.
- 3) "Il teorema di Bombieri-Vinogradov e sue estensioni, I, II, III", Università di Genova, 1993.
- 4) "Crivello pesante e Teorema di Chen, I, II", Università di Genova, 1994.

- 5) “Alcuni risultati sulla congettura di Goldbach”, Incontro Italiano di Teoria dei Numeri, Terza Università di Roma, 1995.
- 6) “Una (breve) introduzione alla crittografia”, Associazione Mathesis, Università di Padova, 1998.
- 7) “Approssimazione diofantea e algoritmo LLL; I, II, III”, Università di Padova, 2001.
- 8) “Sull’insieme eccezionale in intervalli corti di due problemi additivi con numeri primi”, Secondo Incontro Italiano di Teoria dei Numeri, Università di Parma, 2003.
- 9) “Piccole differenze tra primi consecutivi (dopo Goldston, Motohashi, Pintz, Yildirim)” Università di Genova, 08.06.2005.
- 10) “On the sum of a prime and a k -free number”, Italian-Polish Number Theory Days, Poznań, Polonia, 18.05.2006.
- 11) “Numeri primi e Crittografia”, Università degli studi di Modena, 04.10.2006.
- 12) “On the sum of two primes and k powers of two”, Univ. Genova, 15.05.2007 - Univ. Parma 18.05.2007 - Journées Arithmétiques 2007, Edimburgo, UK, 02.07.2007.
- 13) “Alcuni Attacchi a RSA”, Università degli studi di Ferrara, 23.05.2007.
- 14) “On the constant in the Mertens product for arithmetic progressions: Numerical values”, Univ. Parma 16.05.2008.
- 15) “Sul problema di Goldbach-Linnik”, Università di Roma Tre, 29.05.2009.
- 16) “On the Montgomery-Hooley theorem in short intervals”, Marzo 2010: Scuola Normale Superiore, Pisa (Italy).
- 17) “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).
- 18) “Una formula esplicita per i numeri di Goldbach”, Settembre 2011: Univ. Bologna, Italy.

Attività scientifica: In totale la mia produzione scientifica consta di 39 lavori.

Il settore di ricerca in cui essi si inquadrano è quello della 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.

Il mio filone principale di ricerca riguarda lo studio della Congettura di Goldbach. Nel 1742, in due lettere indirizzate ad Eulero, 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.

I miei lavori riguardano lo studio di alcuni risultati parziali sulla congettura di Goldbach.

Tra di essi alcuni (i lavori [1], [3] e [17]) 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 inferiore rispetto ad X . Risultati significativi sono quelli in cui si prova che $E(X) = o(X)$ oppure $E(X, H) = o(H)$.

In particolare il lavoro [17] riguarda lo studio dell’insieme eccezionale in intervalli corti senza assumere alcuna ipotesi analitica. Per questo articolo l’Hardy-Ramanujan Society mi ha conferito, nel 2003, il suo “Distinguished Award”.

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 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 [6], [4] e [10].

La tecnica adottata per provare i risultati sulla distribuzione dei numeri di Goldbach 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 $\sum_{n \leq x} \Lambda(n)e(n\alpha)$, 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. I lavori [12] e [11] riguardano tali argomenti.

Sono stato attratto anche da problemi “lateral” 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 $\psi(x) = \sum_{n \leq x} \Lambda(n)$. Tale formula consente di collegare la distribuzione dei numeri primi alla distribuzione degli zeri non-banali della funzione ζ di Riemann.

Nel lavoro [5] si è studiata una variante “pesata” di tale formula che potesse avere ricadute sulla distribuzione dei numeri di Goldbach in intervalli corti.

Nel lavoro [8] 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.

Nel 2001 ho collaborato, con un risultato riguardante la distribuzione della funzione φ di Eulero e la distribuzione della funzione $\Omega(n)$ (che conta con molteplicità il numero di fattori primi di n), al lavoro [14].

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 [16] riguarda questo problema.

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 l'Ipotesi Generalizzata di Riemann. L'articolo [28], accettato per la pubblicazione, riguarda tale argomento.

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 [23] riguarda tale argomento.

Nel 2005-2006 ho lavorato in collaborazione con J. Pintz e A. Zaccagnini sul problema di rappresentare gli interi come somma di due primi e di un certo numero di potenze di due, lavoro [25]. Nello stesso periodo, con A. Zaccagnini ho studiato una versione per il prodotto di Mertens nelle progressioni aritmetiche che è uniforme nel modulo della progressione stessa, lavoro [24], ed 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 [26], in corso di pubblicazione.

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 [27]. Abbiamo anche esaminato il problema di ottenere alcune formulazioni alternative della costante di Mertens, [32]. Inoltre abbiamo affrontato il problema di calcolarne gli effettivi valori numerici, perlomeno per tutte le progressioni aritmetiche di modulo $q \leq 100$, con una precisione di almeno 100 cifre decimali, articolo [29].

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: $\lambda_1 p_1 + \lambda_2 p_2 + \mu_1 2^{m_1} + \dots + \mu_s 2^{m_s}$, 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 [31]). Il lavoro è stato citato nella "On-Line Encyclopedia of Integer Sequences" al numero A187549; si veda il link <http://oeis.org/A187549>.

Nello stesso periodo, in collaborazione con D. Bazzanella 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 [34], sviluppiamo una tecnica per stimare i momenti di primi su intervalli del tipo $(p, p + h]$, p primo e $h \leq X$, 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 [33].

Sempre nel 2009, in collaborazione con A. Zaccagnini, ho continuato lo studio della computabilità delle costanti di Mertens nelle progressioni aritmetiche. Nel lavoro [30], abbiamo studiato le costanti presenti nelle formule asintotiche delle somme di Mertens e di Meissel-Mertens:

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \frac{1}{p} \quad \text{e} \quad \sum_{p \equiv a \pmod{q}} \left(\log\left(1 - \frac{1}{p}\right) + \frac{1}{p} \right).$$

La sequenza $M(3, 1)$ risultante dalla formula asintotica

$$\sum_{\substack{p \leq x \\ p \equiv 1 \pmod{3}}} \frac{1}{p} = \frac{\log \log x}{2} + M(3, 1) + \mathcal{O}\left(\frac{1}{\log x}\right),$$

è stata inserita nella "On-Line Encyclopedia of Integer Sequences" al numero A161529; si veda il link <http://oeis.org/A161529>.

Nel 2010, in collaborazione con A. Zaccagnini, ho lavorato sull'andamento in media del numero di rappresentazioni di un intero pari come somma di due numeri primi (lavoro [39]). Il lavoro è stato citato nella "On-Line Encyclopedia of Integer Sequences" (<http://oeis.org/>), al numero A002375; si veda il link <http://oeis.org/A002375>.

Sempre nel 2010-2011 in collaborazione con A. Perelli ed A. Zaccagnini, ho lavorato sulla connessione tra i termini di errore per la funzione di pair-correlation degli zeri della funzione ζ di Riemann e per la media dei primi in intervalli corti (lavoro [37]).

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 $k \geq 5$ primi, [41].

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: $\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^3 + \mu_1 2^{m_1} + \dots + \mu_s 2^{m_s}$, 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 [40]). Il lavoro è stato citato nella "On-Line Encyclopedia of Integer Sequences" al numero A187549; si veda il link <http://oeis.org/A187549>.

Più recentemente in collaborazione con A. Zaccagnini, ho migliorato un risultato sull'approssimabilità di numeri reali con forme del tipo $\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^3 + \lambda_4 p_4^4$, (articolo [35]), su altri problemi diofantei con numeri primi e potenze prime (articolo [36]) e ho studiato le medie L^2 di somme esponenziali sulle potenze prime (articolo [38]).

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 [9], [7], [13] riguardano tale aspetto. In seguito ho collaborato con A. Zaccagnini ad una monografia [42] dedicata alle applicazioni crittografiche della Teoria dei Numeri. Inoltre, su invito del centro PRISTEM-Bocconi, in collaborazione con A. Zaccagnini, ho scritto una serie di articoli divulgativi (identificati da [18], [19], [20] e [21]) su vari aspetti della primalità. Nel 2005 ho scritto una colonna dedicata al problema dei primi gemelli per il giornale "La Voz de Almeria" (n. [22]). Nel 2005-2007 ho coordinato il modulo di Crittografia per il "Progetto Nazionale Lauree Scientifiche" per il Veneto. La pubblicazione [43], sviluppata in collaborazione con A. Zaccagnini, riguarda il materiale preparato a tale scopo.

Il lavoro [2] è un survey riguardante la Congettura di Goldbach contenente i risultati presentati nella mia Tesi di Dottorato. Il lavoro [15] è un survey che riguarda la presentazione di due risultati sulla congettura di Goldbach e sulla congettura di Hardy-Littlewood.

Inoltre ho anche curato la stesura di dispense didattiche dei corsi che ho tenuto o a cui ho collaborato (elencate nella successiva sezione "Altre pubblicazioni" insieme alle Tesi di Laurea e di Dottorato di Ricerca).

PUBBLICAZIONI

- [1] A. Languasco and A. Perelli, *On Linnik's theorem on Goldbach numbers in short intervals and related problems*, Ann. Inst. Fourier **44** (1994), 307–322, http://archive.numdam.org/article/AIF_1994__44_2_307_0.pdf, MR1296733 (95g:11097).
- [2] A. Languasco, *Some results on Goldbach's problem*, Rend. Sem. Mat. Univ. Politec. Torino **53** (1995), no. 4, 325–337, <http://seminariomatematico.dm.unito.it/rendiconti/cartaceo/53-4/325.pdf>, MR1452389 (98f:11106).
- [3] A. Languasco and A. Perelli, *A pair correlation hypothesis and the exceptional set in Goldbach's problem*, Mathematika **43** (1996), 349–361, <http://dx.doi.org/10.1112/S0025579300011827>, MR1433280 (98g:11113).
- [4] A. Languasco, *A conditional result on Goldbach numbers in short intervals*, Acta Arith. **83** (1998), 93–103, <http://matwbn.icm.edu.pl/ksiazki/aa/aa83/aa8327.pdf>, MR1490641 (98k:11139a).
- [5] A. Languasco, *A note on primes and Goldbach numbers in short intervals*, Acta Math. Hungar. **79** (1998), 191–206, <http://dx.doi.org/10.1023/A:1006553707162>, MR1616038 (99g:11104).
- [6] A. Languasco, *A singular series average and Goldbach numbers in short intervals*, Acta Arith. **83** (1998), 171–179, <http://matwbn.icm.edu.pl/ksiazki/aa/aa83/aa8321.pdf>, MR1490647 (98k:11139b).
- [7] A. Languasco, *An Introduction to Cryptography*, Queen's Papers in Pure and Applied Mathematics **119** (2000), no. 121-140, in "The Curves Seminar at Queen's", vol. 13, ed. da A.V. Geramita.
- [8] J. Kaczorowski, A. Languasco, and A. Perelli, *A note on Landau's formula*, Funct. Approx. Comment. Math. **28** (2000), 173–186, Dedicated to Włodzimierz Staś on the occasion of his 75th birthday. <http://www.staff.amu.edu.pl/~fa/XXVIII/fa-28-1-173.pdf>, MR1824002 (2001m:11156).
- [9] A. Languasco and A. Perelli, *Numeri Primi e Crittografia*, Matematica e Cultura 2000 (Venezia) (M. Emmer, ed.), Springer-Verlag, Milano, 2000, trad. inglese in *Mathematics and Culture I*, Springer-Verlag, Berlin, Heidelberg, New York, 2003, pp. 227–233.
- [10] D. Bazzanella and A. Languasco, *On the asymptotic formula for Goldbach numbers in short intervals*, Studia Sci. Math. Hungar. **36** (2000), 185–199, <http://dx.doi.org/10.1556/SScMath.36.2000.1-2.14>, MR1768230 (2001j:11096).
- [11] A. Languasco and A. Perelli, *Pair correlation of zeros, primes in short intervals and exponential sums over primes*, J. Number Theory **84** (2000), no. 2, 292–304, <http://dx.doi.org/10.1006/jnth.2000.2511>, MR1796516 (2001m:11151).
- [12] A. Languasco, *Some refinements of error terms estimates for certain additive problems with primes*, J. Number Theory **81** (2000), 149–161, <http://dx.doi.org/10.1006/jnth.1999.2468>.
- [13] A. Languasco and A. Perelli, *Crittografia e firma digitale*, Matematica, Arte, Tecnologia, Cinema (Bologna) (M. Emmer and M. Manaresi, eds.), Springer-Verlag, Milano, 2002, trad. inglese in *Mathematics, Art, Technology, and Cinema*, Springer-Verlag, Berlin, Heidelberg, New York, 2003, pp. 99–106.
- [14] A. Languasco, F. Menegazzo, and M. Morigi, *On the composition length of finite primitive linear groups*, Arch. Math. **79** (2002), 408–417, <http://dx.doi.org/10.1007/BF02638376>, MR1966776 (2004a:20051).
- [15] A. Languasco, *The exceptional set in short intervals for two additive problems with primes: a survey*, Riv. Mat. Univ. Parma (7) **3*** (2004), 223–231, MR2128851 (2006a:11130).
- [16] A. Languasco, *On the exceptional set for Hardy-Littlewood's numbers in short intervals*, Tsukuba J. Math. **28** (2004), 169–192, <http://www.tulips.tsukuba.ac.jp/limedio/dlam/M73/M735867/11.pdf>, MR2082228 (2005d:11145). *Corrigendum ibid.*, Tsukuba Journal of Mathematics, **30** (2006), 237–240, MR2248294 (2007e:11124).
- [17] A. Languasco, *On the exceptional set of Goldbach's problem in short intervals*, Monatsh. Math. (2004), <http://dx.doi.org/10.1007/s00605-003-0038-1>, MR2037990 (2004m:11162).

- [18] A. Languasco and A. Zaccagnini, *Alcune proprietà dei numeri primi, I*, Sito web Bocconi-Pristem (2005), <http://matematica-old.unibocconi.it/LangZac/home.htm>.
- [19] A. Languasco and A. Zaccagnini, *Alcune proprietà dei numeri primi, II*, Sito web Bocconi-Pristem (2005), <http://matematica-old.unibocconi.it/LangZac/home2.htm>.
- [20] A. Languasco and A. Zaccagnini, *Esistono piccoli intervalli fra primi consecutivi!*, Sito web Bocconi-Pristem (2005), <http://matematica-old.unibocconi.it/LangZac/risultatoteorianumeri.htm>.
- [21] A. Languasco and A. Zaccagnini, *Intervalli fra primi consecutivi*, Sito web Bocconi-Pristem (2005), <http://matematica-old.unibocconi.it/LangZac/introduzione3.htm>.
- [22] A. Languasco, *Primos Gemelos*, La Voz de Almeria, Seccion Matematica (2005), (pubblicato il 04/09/2005 in lingua spagnola, traduzione di Juan Cuadra Diaz).
- [23] A. Languasco, *On the sum of a prime and a k -free number*, *Functiones et Approximatio, Commentarii Mathematici* **34** (2006), 19–26, <http://www.staff.amu.edu.pl/~fa/XXXIV/fa-34-1-019.pdf>, MR2269661 (2007j:11142).
- [24] A. Languasco and A. Zaccagnini, *A note on Mertens' formula for arithmetic progressions*, *Journal of Number Theory* **127** (2007), 37–46, <http://dx.doi.org/10.1016/j.jnt.2006.12.015>, MR2351662 (2009g:11136).
- [25] A. Languasco, J. Pintz, and A. Zaccagnini, *On the sum of two primes and k powers of two*, *Bull. London Math. Soc.* **39** (2007), 771–780, <http://dx.doi.org/10.1112/blms/bdm062>, MR2365226 (2008k:11107).
- [26] A. Languasco and A. Zaccagnini, *On the Hardy-Littlewood problem in short intervals*, *Int. J. Number Theory* **4** (2008), no. 5, 715–723, <http://dx.doi.org/10.1142/S179304210800164X>, MR2458837 (2010a:11202).
- [27] 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** (2008), 41–47, <http://projecteuclid.org/euclid.facm/1229624650>, MR2433787 (2009f:11119).
- [28] A. Languasco, *A conditional result on the exceptional set for Hardy-Littlewood numbers in short intervals*, *International Journal of Number Theory* **5** (2009), 9333–951, <http://dx.doi.org/10.1142/S179304210900247X>, MR2569737 (2010j:11146).
- [29] A. Languasco and A. Zaccagnini, *On the constant in the Mertens product for arithmetic progressions. II. Numerical values*, *Math. Comp.* **78** (2009), 315–326, <http://dx.doi.org/10.1090/S0025-5718-08-02148-0>, MR2448709 (2010g:11164).
- [30] A. Languasco and A. Zaccagnini, *Computing the Mertens and Meissel-Mertens constants for sums over arithmetic progressions*, *Experimental Mathematics* **19** (2010), no. 3, 279–284, With an appendix by Karl K. Norton. <http://www.informaworld.com/smpp/content-db=all-content=a933386262-frm=titlelink>, MR2743571 (2011j:11247).
- [31] A. Languasco and A. Zaccagnini, *On a Diophantine problem with two primes and s powers of two*, *Acta Arith.* **145** (2010), 193–208, <http://journals.impan.gov.pl/cgi-bin/aa/pdf?aa145-2-07>, MR2733083 (2011i:11046).
- [32] A. Languasco and A. Zaccagnini, *On the constant in the Mertens product for arithmetic progressions. I. Identities*, *Functiones et Approximatio, Commentarii Mathematici* **42** (2010), no. 1, 17–27, <http://projecteuclid.org/euclid.facm/1269437065>, MR2640766 (2011b:11127).
- [33] A. Languasco, A. Perelli, and A. Zaccagnini, *On the Montgomery-Hooley theorem in short intervals*, *Mathematika* **52** (2010), 231–243, <http://dx.doi.org/10.1112/S0025579310000628>, MR2678027 (2011g:11179).
- [34] D. Bazzanella, A. Languasco, and A. Zaccagnini, *Prime numbers in logarithmic intervals*, *Trans. Amer. Math. Soc.* **362** (2010), no. 5, 2667–2684, <http://dx.doi.org/10.1090/S0002-9947-09-05009-0>, MR2584615 (2011a:11171).
- [35] A. Languasco and A. Zaccagnini, *A Diophantine problem with a prime and three squares of primes*, submitted, 2012.
- [36] A. Languasco and A. Zaccagnini, *A Diophantine problem with prime variables*, submitted, 2012.
- [37] A. Languasco, A. Perelli, and A. Zaccagnini, *Explicit relations between pair correlation of zeros and primes in short intervals*, to appear in *Journal of Mathematical Analysis and Applications*, 2012.
- [38] A. Languasco and A. Zaccagnini, *L^2 -norms of exponential sums over prime powers*, submitted, 2012.
- [39] A. Languasco and A. Zaccagnini, *The number of Goldbach representations of an integer*, *Proc. Amer. Math. Soc.* **140** (2012), 795–804, <http://dx.doi.org/10.1090/S0002-9939-2011-10957-2>.
- [40] A. Languasco and V. Settimi, *On a Diophantine problem with one prime, two squares of primes and s powers of two*, preprint, to appear in *Acta Arithmetica* (2012), <http://arxiv.org/abs/1103.1985>.
- [41] A. Languasco and A. Zaccagnini, *Sums of many primes*, *Journal of Number Theory* **132** (2012), 1265–1283, <http://dx.doi.org/10.1016/j.jnt.2011.11.004>.
- [42] A. Languasco and A. Zaccagnini, *Introduzione alla Crittografia*, Ulrico Hoepli Editore, 2004.
- [43] A. Languasco and A. Zaccagnini, *Crittografia*, CLEUP, Padova, 2006, Progetto Lauree Scientifiche per il Veneto.

Altre Pubblicazioni:

- [1] A. Languasco, “*Codici a chiave pubblica ed Algoritmi di Primalità*”, tesi per il conseguimento della Laurea in Matematica (1989).
- [2] A. Languasco, “*La congettura di Goldbach*”, tesi per il conseguimento del Dottorato di Ricerca (1995).
- [3] A. Languasco, “*Dispense di Analisi Matematica I*”, manoscritto, (1999).
- [4] A. Languasco, “*Dispense di Algebra Lineare, Geometria e Calcolo Differenziale in più variabili (Matematica B)*”, (2002).
- [5] B. Bruno, A. Languasco “*Dispense integrative per il Corso di Istituzioni di Analisi Matematica II*”, (2003).
- [6] A. Languasco, “*Dispense per il Corso di Metodi Matematici per la Statistica (parte di Analisi Matematica)*”, (2005), in corso di revisione per l’a.a. 2008-2009.

La lista delle pubblicazioni e dei relativi abstract è disponibile al seguente indirizzo: <http://www.math.unipd.it/~languasc/lavoripdf/list-abstracts.pdf>.

Padova, 20 aprile 2012

Alessandro LANGUASCO