Dipartimento di Matematica Pura e Applicata
Via Trieste, 63 - 35121 Padova (PD) - Italy

Prof. Alessandro Languasco, Ph.D.
phone: +39-049-8271385 – fax: +39-049-8271499
email: languasco@math.unipd.it

Università degli Studi di Padova

Padova, 5 ottobre 2009

Al **Servizio Concorsi e Carriere Docenti**
Università di Padova,
Riviera Tito Livio 6 - Padova

Al **Preside della Facoltà di Scienze Statistiche**
Via Cesare Battisti 241 - Padova

Al **Direttore del Dipartimento**
di Matematica Pura ed Applicata
Via Trieste, 63 - Padova

Curriculum e Relazione
sulle attività di Alessandro LANGUASCO
Triennio: 01/10/2006-30/09/2009

Quanto segue è l'attività svolta dal sottoscritto nel triennio di prova quale professore di seconda fascia.

Dati anagrafici:
nome: **Alessandro LANGUASCO**

data di nascita: 23/12/1966

luogo di nascita: IMPERIA (IM)

residenza: via FACCIOLATI 88/3, c.a.p 35126, PADOVA (PD)

cittadinanza: italiana

Posizione attuale:
Professore di seconda fascia del settore scientifico-disciplinare MAT/05 presso la Facoltà di Scienze Statistiche dell'Università di Padova.
Presa di servizio: 01/10/2006; fine periodo di prova: 30/09/2009.

Monografie:
2006: Ho pubblicato in collaborazione con A. Zaccagnini dell'Università di Parma, il testo "Crittografia" 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.

Attività Organizzative e di Alta Formazione:

1) da novembre 2007 sono 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 sul tema vincolato da me proposto "Il problema del Logaritmo Discreto" (indirizzo sito weeb: `http://www.unipd.it/stdoc/elencofinanziatiperweb.pdf`). La borsa di studio è stata attivata nel 2008 e ha durata di tre anni.
3) da gennaio 2008 faccio parte del Consiglio dei Docenti della Scuola di Dottorato in Matematica dell'Università di Padova.

Dipartimento di Matematica Pura e Applicata
Via Trieste, 63 - 35121 Padova (PD) - Italy

Prof. Alessandro Languasco, Ph.D.
phone: +39-049-8271385 – fax: +39-049-8271499
email: languasco@math.unipd.it

Università degli Studi di Padova

4) da giugno 2009 faccio parte della "Commissione Pagine Web" del Dipartimento di Matematica Pura e Applicata, Università di Padova.

5) nel luglio 2009 sono stato nominato membro della "Commissione Assegni di Ricerca" (CAR) dell'Area 01 - Scienze Matematiche, 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, 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.

Attività didattica: Affidamenti

- **da a.a. 2003/2004 a a.a. 2008/2009**: "Crittografia", Laurea Specialistica in Informatica ed in Matematica (con il nome "Teoria dei Numeri e Crittografia"), Master Europeo ALGANT, Facoltà di Scienze MM.FF.NN., Università di Padova. Dal 2005/2006 il corso è tenuto in lingua inglese.
- **a.a. 2006/2007-2007/2008**: "Istituzioni di Analisi Matematica I", Laurea Triennale in Statistica, Facoltà di Statistica, Università di Padova.
- **a.a. 2005/2006-2006/2007 e 2008-2009**: "Istituzioni di Analisi Matematica II", Laurea Triennale in Statistica, Facoltà di Statistica, Università di Padova.
- **a.a. 2008-2009**: collaborazione didattica sul corso "Metodi Matematici per la Statistica", Laurea Specialistica in Statistica, Facoltà di Statistica, Università di Padova

Attività didattica: Corsi per Dottorati di Ricerca

a.a. 2007/2008: Scuola di Dottorato in Matematica dell'Università di Padova: corso intitolato "Funzioni L di Dirichlet e Teoria dei Crivelli".

Tesi seguite:

Sono stato relatore di 21 Tesi di Laurea in Teoria dei Numeri, sia per quanto riguarda aspetti teorici che computazionali; quelle relative al triennio in questione sono in numero pari a 12 e sono di seguito elencate. Sono Advisor della Tesi di Dottorato in Matematica della Dott.sa Valentina Settimi. Sono 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.

2006:
- relatore della tesi di Laurea in Matematica (vecchio ordinamento) di D. Alessio intitolata "Reticoli: aspetti algoritmici e loro applicazioni crittografiche".
- relatore della tesi di Laurea in Matematica (vecchio ordinamento) di L. Doni intitolata "Crittografia classica e moderna: alcuni metodi".

Dipartimento di Matematica Pura e Applicata
Via Trieste, 63 - 35121 Padova (PD) - Italy

Prof. Alessandro Languasco, Ph.D.
phone: +39-049-8271385 – fax: +39-049-8271499
email: languasco@math.unipd.it

Università degli Studi di Padova

2007: 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".

2008:
- relatore della tesi di Laurea Specialistica in Matematica di T. Majumdar (studente ALGANT) intitolata "On the Large Sieve".
- 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".
- relatore della tesi di Laurea Triennale in Matematica di E. Zonta intitolata "Codici, fattorizzazione e primalità con curve ellittiche".
- 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".
- relatore della tesi di Laurea Specialistica in Matematica di S. Bettin intitolata "Alcuni problemi equivalenti all'Ipotesi di Riemann".
- relatore della tesi di Laurea Specialistica in Matematica di V. Gauthier (studente ALGANT) intitolata "On some polynomial–time primality algorithms".

2009:
- relatore della tesi di Laurea Specialistica in Matematica di L. Corsi intitolata "Alcuni algoritmi per il Logaritmo Discreto".
- relatore della tesi di Laurea Specialistica in Matematica di L. Maggiolo intitolata "Crivelli dei Campi di Numeri".
- relatore della tesi di Laurea Specialistica in Matematica di F. Melgrani intitolata "L'algoritmo di Schoof". (tesi in corso di elaborazione).

Attività divulgativa:

- **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 programma televisivo RAI intitolato "La storia siamo noi".

Collaborazione con riviste:

- 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).
- **Referee** per le riviste
  - International Journal of Number Theory;
  - Journal of Number Theory;
  - Monatshëfte für Mathematik;
  - Missouri Journal of Mathematical Sciences;
  - Functiones et Approximatio, Commentarii Mathematici.

Partecipazione a Conferenze e Convegni:

[1] Luglio 2007: Journées Arithmétiques 2007, Edimburgo, Regno Unito, (speaker).

[2] Settembre 2007: Arithmetic Geometry, CIME Course, Cetraro (Cs), Italia.

[3] Maggio 2008: Analytic Number Theory Workshop, Parma, Italia, (invited speaker).

Dipartimento di Matematica Pura e Applicata
Via Trieste, 63 - 35121 Padova (PD) - Italy

Prof. Alessandro Languasco, Ph.D.
phone: +39-049-8271385 – fax: +39-049-8271499
email: languasco@math.unipd.it

Università degli Studi di Padova

[4] Settembre 2008: A p-adic differential equations: a conference in honor of Gilles Christol, Bressanone, Italy.

[5] Aprile 2009: Advances in Number Theory and Geometry, Verbania (Italy).

[6] Maggio 2009: La Teoria dei Numeri, Università di Roma Tre, Roma, (Italy), (invited speaker).

Attività seminariale:

[1] "Numeri primi e Crittografia", Università degli studi di Modena, 04.10.2006.

[2] "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.

[3] "Alcuni Attacchi a RSA", Università degli studi di Ferrara, 23.05.2007.

[4] "On the constant in the Mertens product for arithmetic progressions: Numerical values", Univ. Parma 16.05.2008.

[5] "Sul problema di Goldbach-Linnik", Univ. Roma Tre, 29.05.2009.

Alessandro LANGUASCO

Dipartimento di Matematica Pura e Applicata
Via Trieste, 63 - 35121 Padova (PD) - Italy

Prof. Alessandro Languasco, Ph.D.
phone: +39-049-8271385 – fax: +39-049-8271499
email: languasco@math.unipd.it

Università degli Studi di Padova

Padova, 5 ottobre 2009

Al **Servizio Concorsi e Carriere Docenti**
Università di Padova,
Riviera Tito Livio 6 - Padova

Al **Preside della Facoltà di Scienze Statistiche**
Via Cesare Battisti 241 - Padova

Al **Direttore del Dipartimento**
di Matematica Pura ed Applicata
Via Trieste, 63 - Padova

Relazione sull'attività di ricerca scientifica di Alessandro LANGUASCO
Triennio: 01/10/2006-30/09/2009

Professore di seconda fascia del settore scientifico-disciplinare MAT/05 presso la Facoltà di Scienze Statistiche dell'Università di Padova. Presa di servizio: 01/10/2006; fine periodo di prova: 30/09/2009.

In totale la mia produzione scientifica consta di 36 lavori di cui quelli relativi al triennio di prova e pertanto presentati alla presente procedura di conferma in ruolo sono 12. L'elenco dei soli lavori presentati viene allegato a parte.

Il settore di ricerca in cui si inquadrano i miei lavori 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.

Nel 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 [2]. 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 [1], 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 [4].

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 [6], accettato per la pubblicazione, riguarda tale argomento.

Nel 2007, sempre 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 [3]. Abbiamo anche esaminato il problema di ottenere alcune formulazioni alternative della costante di Mertens, articolo [8]. 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 [5].

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 numeri reali fissati che verificano alcune condizioni tecniche (essenzialmente è necessario che almeno due μ_j siano tali da verificare che $\lambda_1/\mu_{j_1}, \lambda_2/\mu_{j_2} \in \mathbb{Q}$). 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. Il lavoro, attualmente sottoposto per la pubblicazione, è il numero [10].

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,

Dipartimento di Matematica Pura e Applicata
Via Trieste, 63 - 35121 Padova (PD) - Italy

Prof. Alessandro Languasco, Ph.D.
phone: +39-049-8271385 – fax: +39-049-8271499
email: languasco@math.unipd.it

Università degli Studi di Padova

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 [7], 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, attualmente sottoposto per la pubblicazione, è il numero [11].

Sempre nel 2009, in collaborazione con A. Zaccagnini, ho continuato lo studio della computabilità delle costanti di Mertens nelle progressioni aritmetiche. Nel lavoro [9], accettato per la pubblicazione, abbiamo studiato le costanti presenti nelle formule asintotiche delle somme di Mertens e di Meissel-Mertens:

$$\lim_{x\to+\infty} \sum_{\substack{p\le x\\ p\equiv a \bmod q}} \frac{1}{p} \quad \text{e} \quad \sum_{p\equiv a \bmod q} (\log(1-\frac{1}{p})+\frac{1}{p}).$$

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

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

per $x \to +\infty$, è stata inserita nella "On-Line Encyclopedia of Integer Sequences" (`http://www.research.att.com/~njas/sequences/index.html`), al numero A161529; si veda il link `http://www.research.att.com/~njas/sequences/A161529`.

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.
Nel 2005-2007 ho coordinato il modulo di Crittografia per il "Progetto Nazionale Lauree Scientifiche" per il Veneto. La pubblicazione [12], sviluppata in collaborazione con A. Zaccagnini, riguarda il materiale preparato a tale scopo.
Nel 2009, U. Rondi mi ha intervistato per il programma televisivo RAI intitolato "La storia siamo noi".

Alessandro LANGUASCO

Dipartimento di Matematica Pura e Applicata
Via Trieste, 63 - 35121 Padova (PD) - Italy

Prof. Alessandro Languasco, Ph.D.
phone: +39-049-8271385 – fax: +39-049-8271499
email: languasco@math.unipd.it

Università degli Studi di Padova

Pubblicazioni di Alessandro Languasco

nel triennio: 01/10/2006-30/09/2009

Articoli scientifici pubblicati

[1] A. Languasco, 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. (sottoposto il 13/07/2006; rivisto il 06/12/2006).

[2] A. Languasco, J. Pintz, A. Zaccagnini, *"On the sum of two primes and k powers of two"*, Bulletin of the London Mathematical Society, **39** (2007), 771–780, http://dx.doi.org/10.1112/blms/bdm062. (sottoposto il 18/12/2006; rivisto il 26/03/2007).

[3] A. Languasco, A. Zaccagnini, *"Some estimates for the average of the error term of the Mertens product for arithmetic progressions"*, Functiones et Approximatio, Commentarii Mathematici, **38** (2008), 41–48. (sottoposto il 08/05/2007).

[4] A. Languasco, A. Zaccagnini, *"On the Hardy-Littlewood problem in short intervals"*, International Journal of Number Theory, **4** (2008), 715–723. http://dx.doi.org/10.1142/S179304210800164X (sottoposto il 21/11/2006).

[5] A. Languasco, 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 (sottoposto il 11/12/2007; rivisto il 12/02/2008).

Articoli scientifici in corso di pubblicazione

[6] A. Languasco, *"A conditional result on the exceptional set for Hardy-Littlewood numbers in short intervals"*, International Journal of Number Theory, **5** (2009) (sottoposto il 22/03/2007; accettato il 06/03/2008).

[7] D. Bazzanella, A. Languasco, A. Zaccagnini, *"Prime numbers in logarithmic intervals"*, in corso di pubblicazione su Trans. Amer. Math. Soc., http://arxiv.org/abs/0809.2967 (sottoposto il 17/09/2008)

[8] A. Languasco, A. Zaccagnini, *"On the constant in the Mertens product for arithmetic progressions. I. Identities"*, in corso di pubblicazione su Functiones et Approximatio, Commentarii Mathematici. http://arxiv.org/abs/0706.2807. (sottoposto il 26/09/2008)

[9] A. Languasco, A. Zaccagnini, *"Computing the Mertens and Meissel-Mertens constants for sums over arithmetic progressions"*, preprint 2009. in corso di pubblicazione su Experimental Mathematics. http://arxiv.org/abs/0906.2132. (sottoposto il 11/06/2009; rivisto il 23/07/2009).

Prepubblicazioni

[10] A. Languasco, A. Zaccagnini, *"On a Diophantine problem with two primes and s powers of two"*, preprint 2008, sottoposto per la pubblicazione. http://arxiv.org/abs/0811.3663. (sottoposto il 02/04/2009)

[11] A. Languasco, A. Perelli, A. Zaccagnini, *"On the Montgomery-Hooley theorem in short intervals"*, preprint 2009. (sottoposto il 14/09/2009)

Monografie

[12] A. Languasco, A. Zaccagnini, *"Crittografia"*, Progetto Lauree Scientifiche per il Veneto, Ed. CLEUP, Padova, (2006).

Padova, 5 ottobre 2009

Alessandro LANGUASCO