

## Curriculum dell'attività scientifica e didattica

dott. Andrea Susa

(Aggiornato al 21 marzo 2014)

### Dati Personali

- **Luogo e data di nascita:** Roma, 26 luglio 1974
- **Residenza:** Via Copenhagen 18 F12 - 00054 FIUMICINO
- 
- 

### Posizioni attuali

- Libero professionista - consulente IT e Docente;
- Cultore della materia di "Metodi Matematici per l'Economia - SSD SECS-S/06", presso l'Università Europea di Roma, A.A. 2013/14;
- Didattica integrativa di "Matematica con elementi di statistica", presso l'Università della Tuscia (DIBAF), A.A. 2013/14;
- Docente di "Matematica e Statistica", per ITS Agroalimentare di Viterbo

### Posizioni precedenti

- Professore a Contratto di Istituzioni di Matematica presso la Facoltà di Scienze Organizzative e Gestionali - Università degli Studi della Tuscia (A.A. 2008/09 - 2010/11, 2012/13)
- Professore a Contratto di "Metodi Matematici per l'Economia - SSD SECS-S/06", presso l'Università Europea di Roma (sede distaccata di tutoraggio di Pomezia) (A.A. 2011/12 - 2012/13)
- Docente di corsi di specializzazione in crittografia, crittanalisi e sicurezza delle informazioni e delle reti presso lo Stato Maggiore della Difesa (2006 - 2011)
- Professore a Contratto di Analisi Matematica presso la Facoltà di Scienze MM FF NN - Università degli Studi di "Roma TRE" (A.A. 2006/07 - 2008/09)

- Esercitatore di Geometria presso la Facoltà di Ingegneria - Università degli Studi di Roma "Tor Vergata" (A.A. 2007/08 - 2009/10)
- Esercitatore di Analisi Matematica e Statistica presso la Facoltà di Economia - Università Europea di Roma (A.A. 2007/08 - 2009/10)
- Assegnista di ricerca in crittografia e sicurezza delle reti - CIVV Università degli Studi di Roma Tor Vergata (2006 - 2007)

## Titoli di Studio

- Dottorato di Ricerca in Matematica, conseguito il 12 aprile 2006 presso l'Università degli Studi "Roma TRE" (SSD MAT/02 - MAT/05)
- Laurea in Matematica (indirizzo GENERALE) conseguita il 16 febbraio 2001 presso l'Università degli Studi "Roma TRE" con votazione 110/110 e lode (SSD MAT/02 - MAT/05).
- Maturità scientifica conseguita presso il Liceo-Ginnasio Sperimentale "V. Bachelet" di Roma, con votazione 60/60.

## Aree di interesse scientifico:

- Teoria algebrica ed analitica dei Numeri. Congettura di Artin per radici primitive e problemi analoghi. L-Serie di Artin ed applicazioni. Funzioni aritmetiche. Curve ellittiche (settori disciplinari MAT/02 - MAT/03 - MAT/05).
- Crittografia a chiave pubblica e privata. Crittosistemi su curve ellittiche. Il problema del Logaritmo Discreto su campi e su curve. Analisi di sistemi di streaming mediante attacchi algebrici e statistici (settori disciplinari MAT/02 - MAT/03 - ING-INF/05 - INF/01)
- Metodologie e Processi per la Sicurezza. Modelli e Piani per la sicurezza delle Informazioni. Piani per Business Continuity e Disaster Recovery. Privacy

## Borse di Studio e di Ricerca

- Assegno di Ricerca semestrale presso l'Università degli Studi di Roma "Tor Vergata" - Centro Vito Volterra (gennaio - giugno 2007).
- Borsa di studio annuale presso l'Università degli Studi di Roma "Tor Vergata" - Centro Vito Volterra (Fente Finanziatore esterno FILAS, progetto: Algoritmi crittografici) (novembre 2005 - ottobre 2006).

- Borsa di Dottorato in Matematica, XVIII ciclo triennale (2002-2005) presso l'Università degli Studi "Roma TRE".
- Borsa di Collaborazione presso la Segreteria Didattica - Dipartimento di Matematica, Università degli Studi "Roma TRE", per l'A.A.1999-2000.
- Borsa di Studio "ADISU/Roma TRE" per il biennio accademico 1997-1999.
- Borsa di Studio l'Università degli Studi "Roma TRE" per il biennio accademico 1994-1996.

### Soggiorni di Ricerca all'estero

- 1 febbraio - 1 marzo 2006 - CRM Montreal (Canada) - partecipazione all'anno speciale *Analysis in Number Theory*
- 10-30 gennaio 2006 - IHP "Institut H. Poincaré" Parigi (Francia) - periodo di ricerca su problemi di Teoria Analitica dei Numeri
- 10 ottobre - 20 novembre 2005 - CRM Montreal (Canada) - partecipazione all'anno speciale *Analysis in Number Theory*
- 23-29 giugno 2005 - Anogia (Grecia) - partecipazione alla scuola estiva "Number fields and curves over finite fields"
- settembre/ dicembre 2004 - IHP "Institut H. Poincaré" Parigi (Francia) - partecipazione al Trimestre speciale: *Explicit Methods in Number Theory*.

### Partecipazione a Convegni:

La (\*) indica che si è tenuta una comunicazione/seminario.

- 27 - 29 Maggio 2009 (Roma TRE), III convegno italiano di Teoria dei numeri
- 27-31 Ottobre 2008 (Forschungsinstitut für Mathematik of ETH Zurich) *Random matrices, L-functions and primes*
- 23 Ottobre (IRMA, Strasbourg) *Journé diophantienne, October 23, 2008,*
- 9-13 Luglio 2007 (Technical University of Graz) *Summer School on Dynamical Systems and Number Theory*
- 23-27 Febbraio 2007 (Harish-Chandra Research Institute, Allahabad) *Workshop: International conference on Number Theory and Cryptography*

- (\*) 11–15 Ottobre 2004 (IHIP Parigi) Workshop: **Explicit algebraic number theory** - titolo della comunicazione: "On a problem of Schinzel and Wojcik"
- (\*) 20 Maggio 2004 (Parma) Giornata di Teoria dei Numeri - titolo del seminario: "Problemi analoghi alla Congettura di Artin per radici primitive"
- 18-20 Dicembre 2003 (Roma) Meeting on Algebraic Varieties
- 13-15 Novembre 2003 (Parma) II Convegno Italiano di Teoria dei Numeri

### Seminari su invito:

- 22–25 giugno 2007 - Università degli Studi "Roma Tre" - Dipartimento di Matematica. Seminario dal titolo: "*A new approach to pseudorandom number generators, 1 e 2*"
- 13 aprile 2005 - Università degli Studi "Roma Tre" - Dipartimento di Matematica. Seminario dal titolo: "*Su un problema di Schinzel-Wojcik*"
- 10 novembre 2005 - CRM Montreal (Canada). Seminario dal titolo: "*Some problems analogous to Artin's conjecture*"

### Tesi, pubblicazioni e pre-print, pubblicazione didattica:

- **Tesi di Laurea e Dottorato**
  1. **Tesi di Laurea:** "*Sui coefficienti dei polinomi ciclotomici*" - Relatore Prof. F. Pappalardi
  2. **Tesi di Dottorato:** "*Some problems analogous to Artin's Conjecture*" - Advisor Prof. F. Pappalardi
- **Pubblicazioni**
  1. con F. Pappalardi, "*On a problem of Schinzel and Wojcik involving equalities between multiplicative orders*", Math. Proc. Cambridge Philos. Soc. 146.2 (2009), 303-319.
  2. con F. Pappalardi, "*An analogue to Artin's conjecture for multiplicative subgroups of the rationals*", Archiv der Mathematik Volume 101 (2013), Issue 4, pp 319-330
- **Pre-print**

1. "On a problem of Schinzel and Wjciak involving equalities between multiplicative orders, II", pre-print.
2. "On a problem of distribution of subgroups with fixed index" pre-print.

- **Publicazioni didattiche**

1. Note di Crittografia a chiave pubblica, vol 3. "Campi finiti, logaritmi discreti e crittosistemi derivati" disponibile on line.
2. con M. Mento: Corso di Matematica Propedeutico alla Crypto materiale multimediale per il CIFI/GE/Stato Maggiore della Difesa.
3. Note di Crittografia, vol.1 "Storia dei sistemi di cifratura" materiale multimediale per il CIFI/GE/Stato Maggiore della Difesa.

## Attività didattica:

### Contratti incarico insegnamento - docente titolare

- A.A. 2013/14
  1. Corso di "Matematica - 2 CFU" PAS A059 - DEB - Dipartimento di Scienze Ecologiche e Biologiche, Università della Tuscia
  2. Corso di "Matematica e Statistica - 24 ore" Istituto Tecnico Superiore Agroalimentare - Viterbo
- A.A. 2012/13
  1. Corso di "Istituzioni di Matematica" (SSD MAT/05) - Facoltà di Scienze organizzative e Gestionali, Università della Tuscia
  2. Corso di "Metodi Matematici per l'Economia" (SSD SECS-S/06) - Ambito di Economia, Università Europea di Roma (sede distaccata di tutoraggio di Pomezia)
- A.A. 2011/12
  1. Corso di "Metodi Matematici per l'Economia" (SSD SECS-S/06) - Ambito di Economia, Università Europea di Roma (sede distaccata di tutoraggio di Pomezia)
- A.A. 2010/11
  1. Corso di "Analisi Matematica" (SSD MAT/05) - Facoltà di Scienze Organizzative e Gestionali, Università degli Studi della Tuscia
  2. Docenza corso "Crittanalisi del Sistema BlowFish" presso Stato Maggiore della Difesa
- A.A. 2009/10

1. Precorso di "Matematica" (SSD MAT/05) - Corso di Laurea in Ingegneria, Università degli Studi "Roma Tre"
  2. Corso di "Analisi Matematica" (SSD MAT/05) - Facoltà di Scienze Organizzative e Gestionali, Università degli Studi della Tuscia
- A.A. 2008/09
    1. Corso di "Matematica IP" (SSD MAT/05) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre"
    2. Corso di "Matematica" (SSD MAT/05) - Facoltà di Scienze Organizzative e Gestionali, Università degli Studi della Tuscia
  - A.A. 2007/08
    1. Corso di "Crittanalisi di sistemi di streaming mediante attacchi algebrici e statistici" (MAT/02 - MAT/03) DISP - Facoltà di Ingegneria, Università degli Studi di Roma "Tor Vergata"
    2. Corso di "Matematica IB" (SSD MAT/05) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre"
    3. Corso di "Analista Crypto 3" (MAT/02 - MAT/03) - CIFI GE Centro Interforze di Formazione Intelligence/GE presso Stato Maggiore della Difesa
    4. Corso di "Sicurezza dei dati e delle reti" - (SSD ING-INF/05) CIFI GE Centro Interforze di Formazione Intelligence/GE presso Stato Maggiore della Difesa
  - A.A. 2006/07
    1. Corso di "Matematica IB" (SSD MAT/05) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre"
    2. Corso di "Analista Crypto 2" (MAT/02 - MAT/03) - CIFI GE Centro Interforze di Formazione Intelligence/GE presso Stato Maggiore della Difesa
    3. Corso di "Sicurezza dei dati e delle reti" (SSD ING-INF/05) - CIFI GE Centro Interforze di Formazione Intelligence/GE presso Stato Maggiore della Difesa
  - A.A. 2005/06
    1. Corso di "Analista Crypto 1" (MAT/02 - MAT/03) - CIFI GE Centro Interforze di Formazione Intelligence/GE presso Stato Maggiore della Difesa

## Supporto alla Didattica ed Esercitazioni

- A.A. 2013/14
  1. Esercitazioni di "Metodi Matematici per l'Economia" (SECS-S/06) Università Europea di Roma
  2. "Precorso di Matematica" per la preparazione al test di accesso per la Facoltà di Economia - Università degli Studi "La Sapienza" di Roma
  3. "Precorso di Matematica" per la preparazione al test di accesso per la Facoltà di Ingegneria - Università degli Studi "Roma TRE"
  4. Didattica integrativa di "Matematica con elementi di fisica - SSD MAT/05", presso l'Università della Tuscia (DIBAF)
  5. Docente corso di "Matematica - PAS classe A059", presso l'Università della Tuscia (DEB), A.A. 2013/14;
  6. Docente di Matematica e Fisica - Progetto "Orientamento in rete - corsi di preparazione alla prova di accesso programmato per il corso di Laurea in Medicina" - Facoltà di Medicina e Psicologia - Università "La Sapienza"
- A.A. 2009/10

Esercitazioni di "Analisi Matematica I" (SSD MAT/05) - Corso di Laurea in Economia, Università Europea di Roma, sotto la direzione della Prof.ssa M. Monsurrò (24 ore)
- A.A. 2008/09

Esercitazioni di "Analisi Matematica I" (SSD MAT/05) - Corso di Laurea in Economia, Università Europea di Roma, sotto la direzione della Prof.ssa M. Monsurrò (24 ore)

Esercitazioni di "Geometria ed Algebra" (SSD MAT/03) - Corso di Laurea in Ingegneria, Università degli Studi di Roma "Tor Vergata" sotto la direzione del Prof. G. Pareschi (32 ore)
- A.A. 2007/08

Esercitazioni di "IN1 - Introduzione alla Teoria dei Numeri" (SSD MAT/02) - Corso di Laurea in Matematica, Università degli Studi "Roma Tre" sotto la direzione della Prof.ssa F. Girolami (12 ore)

Esercitazioni di "Geometria I e II" (SSD MAT/03) - Corso di Laurea in Ingegneria, Università degli Studi di Roma "Tor Vergata" sotto la direzione del Prof. G. Pareschi (32 ore)
- A.A. 2006/07

Esercitazioni di "GE2 - Geometria 2" (SSD MAT/03) - Corso di Laurea in Matematica, Università degli Studi "Roma Tre" sotto la direzione del Prof. A. Verra (12 ore)

- Esercitazioni di "CR1 - Crittografia 1" (SSD MAT/02 - INF/01) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre" sotto la direzione del Prof. F.ssa Tartarone (12 ore)
- Esercitazioni di "Geometria I" (SSD MAT/03) - Corso di Laurea in Ingegneria, Università degli Studi di Roma "Tor Vergata" sotto la direzione della Prof. Ciriza (16 ore)
- Esercitazioni di "Geometria e algebra" (SSD MAT/03) - Corso di Laurea in Ingegneria, Università degli Studi di Roma "Tor Vergata" sotto la direzione del Prof. F. Flamini (16 ore)
- A.A. 2005/06
 

Esercitazioni di "Matematica I" (SSD MAT/05) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre" sotto la direzione del Prof. V. Talamanca (24 ore)

Esercitazioni di "CR1 - Crittografia 1" (SSD MAT/02 - INF/01) - Corso di Laurea in Matematica, Università degli Studi "Roma Tre" sotto la direzione della Prof.ssa F. Tartarone (24 ore)
  - A.A. 2004/05
 

Esercitazioni di "Matematica I" (SSD MAT/05) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre" sotto la direzione del Prof. D. Vergni (24 ore)

Esercitazioni di "Matematica II" (SSD MAT/05) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre" sotto la direzione della Prof.ssa V. Orlandi (24 ore)

Esercitazioni di "CR1 - Crittografia 1" (SSD MAT/02 - INF/01) - Corso di Laurea in Matematica, Università degli Studi "Roma Tre" sotto la direzione della Prof.ssa F. Tartarone (24 ore)
  - A.A. 2003/04
 

Esercitazioni di "Matematica II" (SSD MAT/05) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre" sotto la direzione del Prof. G. Pontrelli (24 ore)

Esercitazioni di "CR1 - Crittografia 1" (SSD MAT/02 - INF/01) - Corso di Laurea in Matematica, Università degli Studi "Roma Tre" sotto la direzione del Prof. F. Tartarone (24 ore)
  - A.A. 2002/03
 

Esercitazioni di "Matematica II" (SSD MAT/05) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre" sotto la direzione della Prof.ssa V. Orlandi (24 ore)

Esercitazioni di "CR1 - Crittografia 1" (SSD MAT/02 - INF/01) - Corso di Laurea in Matematica, Università degli Studi "Roma Tre" sotto la direzione del Prof. F. Pappalardi (24 ore)

- A.A. 2001/02

Esercitazioni di "Matematica II" (SSD MAT/05) - Corso di Laurea in Geologia, Università degli Studi "Roma Tre" sotto la direzione del Prof. A. Pellegrinotti (24 ore)

Esercitazioni di "AL1 - Algebra 1" (SSD MAT/02) - Corso di Laurea in Matematica, Università degli Studi "Roma Tre" sotto la direzione del Prof. M. Fontana (24 ore)

- A.A. 2000/01

Esercitazioni di "NUC - Numeri e Complementi" (SSD MAT/05) - Corso di Laurea in Matematica, Università degli Studi "Roma Tre" sotto la direzione del Prof. A. Bruno (12 ore)

Il sottoscritto autorizza la raccolta ed il trattamento dei dati personali ai sensi del D.Lgs n. 196/2003.

data

Roma, 25/06/2014

<sup>firma</sup>  


