Curriculum Didattico e Scientifico

Generalità

Nome: Previtali Andrea

Indirizzo: Dipartimento di Scienza e Alta Tecnologia
Università dell'Insubria-Como
Via Valleggio, 11 - 22100
Como Italia
andrea.previtali@uninsubria.it
http:\\scienze-como.uninsubria.it/previtali

Posizione attuale: Professore Associato Confermato

Data di nascita: 28 Dicembre 1965

Luogo di Nascita: Vimercate (MB)

Nazionalità: Italiana

Titoli

1984: Diploma linguistico (Inglese, Francese e Tedesco) **60/60**

1990: Laurea in Matematica presso l'Università di Milano **110/110 e lode**

1990: Dottorato in Matematica presso l'Università di Pisa **120/120**

Impieghi

1993: Abilitazione all'insegnamento di Matematica nella scuola superiore **100/100**

2000: Ricercatore in Matematica presso l'Università dell'Insubria

2003: Ricercatore Confermato in Matematica presso l'Università dell'Insubria

2006: Professore Associato in Matematica presso l'Università dell'Insubria

2009: Professore Associato Confermato in Matematica presso l'Università dell'Insubria

Incarichi organizzativo-amministrativi

2000: Organizzatore del bimestre intensivo Indam presso l'Università di Milano-Bicocca

2005-2012: Coordinatore locale del Progetto Lauree Scientifiche

2009: Organizzatore del convegno in occasione del 70-simo compleanno del Prof. A.E. Zalesskii presso l'Università di Milano-Bicocca

Borse di Studio

1991-1995: Borsa quadriennale per il Dottorato dell'Università di Pisa

1995: Borsa annuale dell'Istituto dell'Alta Matematica

1996: Borsa semestrale di Perfezionamento all'estero dell'Università di Padova

1996: Borsa annuale Fulbright

1996: Borsa annuale del Consiglio Nazionale delle Ricerche

1997-1998: Borsa biennale Postdottorato dell'Università di Pisa

1999: Borsa annuale del Consiglio Nazionale delle Ricerche per l'estero

2000-2001: Assegni di Ricerca erogati dall'Università di Milano-Bicocca

Posizioni come Visitatore

1991-1992: Studente di Dottorato presso l'Università di Pisa

1993-1994: Studente di Dottorato presso l'Università di Mainz, Germania, supervisore Prof. Dr. B. Huppert

1995: Borsista Indam presso l'Università di Roma, supervisore Prof. C. M. Scoppola

1996-1997: Borsista Postdottorato presso l'Università di Wisconsin-Madison, USA, supervisore Prof. M. I. Isaacs

1999, 2002: Due visite bimestrali presso la University College of Dublin, Irlanda, collaboratore Prof. R. Gow

2002, 2003: Due visite bimestrali presso Institute for experimental Mathematics a Essen, Germania, collaboratore Prof. G. O. Michler

2004, 2005: Due visite bimestrali presso University of Cornell, collaboratore Prof. G. O. Michler

2007-2008: Visita semestrale presso University of Sydney, collaboratori Dott. C. Fieker e Prof. J. Cannon

Comunicazioni

1994: "Sylow p–subgroups of finite linear groups and their character degrees" al convegno "Linear Groups" organizzato dal CIRM in Levico (TN)

1995: "Character degrees of some p–groups" alla Tagung "Gruppen und topologischen Gruppen" a Friburgo

1997: "Theorems like Hall's" alla conferenza dell'American Mathematical Society di Detroit

1997: "Theorems like Hall's" al Ph. D. Centennial dell'Università del Wisconsin a Madison

1997: “Operator groups fixing chain of subgroups” all’Università di Firenze

1997: “Operator groups fixing chain of subgroups” all’Università de L’Aquila

1998: “Maps behaving like exponentials” al convegno di Teoria dei Gruppi di Firenze

1998: “Maps behaving like exponentials” all’Università de L’Aquila

2000: “Unitriangular action on sesquilinear and quadratic forms” al convegno di Teoria dei Gruppi di Milano

2000: ”Minimally irreducible groups” al convegno di Teoria dei Gruppi di Lecce

2001: ”Irreducible modules of modular exceptional simple Lie algebras” all’Università Cattolica di Brescia

2001: ”Graph methods in Lie theory” all’Università di Milano-Bicocca

2001: ”Almost-simple irreducible groups of Lie type” all’Università de L’Aquila

2001: ”Minimally irreducible semisimple groups” al Workshop in group theory dell’Università di Oxford

2002: ”Carter subgroups” all’Università de L’Aquila

2002: ”Galois automorphisms in classical groups” all’University College Dublin

2002: ”Conjugacy problem for Carter subgroups” all’Università di San Pietroburgo

2002: ”Existence and Uniqueness of some sporadic groups” al Convegno di Teoria dei Gruppi di Ischia

2003: ”On the construction of Higman-Sims simple group” all’Institut fuer experimentelle Mathematik di Essen

2003: ”Classical groups and their Carter subgroups” alla Summer school in Combinatorics and Representation theory presso l’Università di Lisbona

2003: ”Esistenza ed Unicità del gruppo di O’Nan” XVII convegno dell’Unione Matematica Italiana

2003: ”Gruppi generati da trasvezioni” al Convegno di Teoria dei Gruppi di Udine

2004: ”On the Existence and uniqueness of Thompson sporadic simple group” al Convegno in onore di M. Herzog, Ischia

2004: ”Il metodo RSA” Licei Fermi, Galilei, Giovio, Badoni e Terragni

2004: ”Nuovi metodi per stabilire quando un intero primo” Licei Fermi, Galilei, Giovio, Badoni e Terragni

2004: ”Computing Character Tables: Old and new methods” al convegno di Teoria dei gruppi di Napoli

2005: ”Classical Groups, Character Degrees, Unitriangular Actions, and Quadratic Forms” al convegno ”p-gruppi: vecchi problemi, nuove tecniche” at the Domus galileiana in Pisa

2005: "Seven questions and one lie" Licei Fermi, Galilei, Giovio, Grassi, Terragni e Facchinetti

2005: "Matematica Sperimentale: tra utile e dilettevole" Insubria Open Days

2006: "Magma, gruppi di permutazione e curve ellittiche", Universita' di Milano

2006: "Magma, basi di Groebner e curve ellittiche", Universita' di Milano-Bicocca

2006: "Irreducible characters of monomial representations", Technische Universitaet zu Berlin

2006: "Cyclotomic polynomials and generation of finite fields", Palazzo della Regione Abruzzo

2006: "Irreducible characters of monomial representations", University of Padua

2007: "Constructing representations with a given character", School of Mathematics and Statistics, University of Sydney

2009: "Class Sizes of Unipotent Subgroups in Good Characteristic", al Convegno per 70-simo compleanno del Prof. M.I. Isaacs, Universidad de Valencia

2009: "Galois Invariance, Trace and Subfield Subcodes", al convegno "Gruppen und topologischen Gruppen", Università Statale di Milano

2010: "Galois Invariance, Trace and Subfield Subcodes", al convegno "Teoria dei Gruppi e Applicazioni", Ischia

2011: "Sistemi Assiomatici", Liceo Grassi, Saronno

2011: "Dimostrazioni Automatiche di Teoremi in Geometria Elementare", Liceo Vanoni, Menaggio

Convegni

1989 & 1990: Corsi estivi di Perugia in Algebra, Analisi Numerica e Geometria Algebrica

1991: "Arithmetic Algebraic Geometry" organizzato dal CIME a Povo (TN)

1991: "Modular Representation Theory" organizzato dal CIRM a Povo (TN)

1992: "Arithmetic Algebraic Geometry" organizzato dall'ICTP a Trieste

1993: "Group Theory" organizzato dal CIRM a Povo (TN)

1995: "Linear Groups" organizzato dal CIRM a Levico (TN)

1995: "Gruppen und topologischen Gruppen" a Friburgo

1997: Convegno dell'American Mathematical Society a Detroit

1997: Ph. D. Centennial dell'Università del Wisconsin a Madison

1998: Convegno di Teoria dei Gruppi a Firenze

1998: Corso estivo di Cortona su Gruppi lineari

2000: Convegno di Teoria dei Gruppi a Milano-Bicocca

2000: Convegno di Teoria dei Gruppi a Lecce

2001: Conferenza su "Algebraic groups", Bielefeld

2001: Norddeutsches Kolloquium

2001: Corsi estivi al Workshop in group theory, Oxford

2001: Convegno di Teoria dei Gruppi a Brescia

2002: Corso estivo di Cortona sulla Classificazione dei gruppi semplici

2002: Convegno di Teoria dei Gruppi a Ischia

2003: Scuola estiva in Combinatoria e teoria della rappresentazione a Lisbona

2003: XVII convegno dell'Unione Matematica Italiana

2003: Conferenza in onore di Walter Feit presso la Yale University

2003: Convegno di Teoria dei Gruppi a Udine

2004: Convegno di Teoria dei Gruppi in onore di M. Herzog a Ischia

2004: Convegno di Teoria dei Gruppi a Naples

2005: Conferenza "p-groups: old problems new techniques" alla Domus galileiana di Pisa

2006: Magma conference 2006 Technische Universitaet zu Berlin

2006: Sicurezza nella pubblica amministrazione, Palazzo della Regione de L'Aquila, Abruzzo

2006: Convegno di Teoria dei Gruppi a Padova

2007: Summer School on Finite Groups and Related Geometrical Structures, Venezia

2007: Convegno su Magma, School of Mathematics and Statistics, University of Sydney

2009: Convegno per 70-simo compleanno del Prof. A.E. Zalesskii, Università di Milano-Bicocca

2009: Convegno per 70-simo compleanno del Prof. M.I. Isaacs, Universidad de Valencia

2009: Convegno "Gruppen und topologischen Gruppen", Universita' Statale di Milano

2010: Summer School on Finite Groups and Related Geometrical Structures, Venezia

2012: Convegno per 75-simo compleanno del Prof. B. Fischer, Universität zu Bielefeld

2012: Convegno di Teoria dei Gruppi a Ischia

Didattica

1989-1990: Supplenze di Matematica presso l'I.T.C. Ghandi

1993: Precorsi di Matematica presso il Politecnico di Milano

1993-1994: Cattedra di Matematica presso l'I.T.C. Ghandi

1998: Precorsi di Matematica presso il Politecnico di Como

1999: Precorsi di Matematica presso il Politecnico di Milano

1999: Esercitazioni di Geometria presso il Politecnico di Milano

1999: Esercitazioni di Geometria presso il Politecnico di Como

2000: Esercitazioni di Matematica Discreta presso l'Università di Milano-Bicocca

2000: Esercitazioni di Algebra presso l'Università dell'Insubria

2001: Corso di Teoria di Galois presso l'Università dell'Insubria

2001: Corso di Algebra presso l'Università dell'Insubria

2001: Esercitazioni di Algebra presso l'Università dell'Insubria

2002: Esercitazioni di Algebra presso l'Università dell'Insubria

2002: Corso di Crittografia presso l'Università dell'Insubria

2002: Corso di Matematica Discreta presso l'Università di Milano-Bicocca

2003: Corso di Algebra I presso l'Università dell'Insubria

2003: Corso di Combinatoria presso l'Università dell'Insubria

2003: Corso di Matematica Discreta presso l'Università di Milano-Bicocca

2004: Corso di Teoria dei Codici presso l'Università dell'Insubria

2004: Corso di Matematica Discreta presso l'Università di Milano-Bicocca

2005: Corso di Dottorato sulla Teoria delle Rappresentazioni Modulari presso l'Università di Milano-Bicocca

2005-2012: Corsi di Matematica Discreta, Algebra 1,2 e 3, Teoria dei Codici, Teoria di Galois, Crittografia presso l'Università dell'Insubria

2006-2012: Stage estivo di Matematica Discreta e Crittografia

Attività di Ricerca

1990: Tesi di Laurea in Matematica dal titolo "Rappresentazioni matriciali di interi algebrici"; relatore Prof. M. Sce

1990: Borsa di Dottorato presso l'Università di Pisa

1994: Tesi di Dottorato relativa alla risoluzione di una congettura di R. Thompson riguardante i gradi dei caratteri dei sottogruppi unipotenti massimali dei gruppi di tipo Lie; relatore Prof. Dr. B. Huppert presso l'Università di Mainz

1995: Analisi dei p-gruppi con piccola ampiezza; collaboratori Prof. C. Scoppola dell'Università La Sapienza di Roma, Prof. A. Mann dell'University of Jerusalem; finanziato dall'Istituto dell'Alta Matematica

1996: Risolubilità o nilpotenza di alcuni gruppi di automorfismi; collaboratore Prof. M. I. Isaacs dell'Università del Wisconsin; supporto borse di perfezionamento, Fulbright e postdottorato

1997: Estendendo tecniche sviluppate durante la stesura della tesi di Dottorato, ho determinato le classi di coniugio nei gruppi unipotenti massimali dei gruppi finiti di tipo Lie

1997: Determinazione del gruppo degli automorfismi di grafi che generalizzano quello di Petersen; collaboratori Dr. W. Pacco e Dr. M. Lovrečič

1998: Esistenza di partizioni in gruppi aventi ordine potenza di primo, collaboratore Prof. N. Gavioli dell'Università de L'Aquila.

1999: Analisi dei caratteri dei gruppi unipotenti massimali dei gruppi simplettici in caratteristica 2 e azioni unitriangolari su forme quadratiche e sesquilineari; collaboratore Prof. R. Gow dell'University College Dublin

2000: Determinazione dei gruppi minimamente irriducibili; collaboratori Proff. L. Di Martino e F. Dalla Volta dell'Università di Milano-Bicocca

2001: Coniugio dei sottogruppi di Carter di gruppi finiti; collaboratori Prof. M. C. Tamburini dell'Università di Brescia e Dr. E. P. Vdovin dell'University of Novosibirsk

2002: Generazione di gruppi classici mediante trasvezioni; collaboratori Prof. L. Di Martino dell'Università di Milano-Bicocca e Dr. R. Radina dell'Università di Milano

2002: Riduzioni modulari della rappresentazione di Steinberg; collaboratore Prof. R. Gow dell'University College Dublin

2002: Esistenza ed Unicità dei gruppi sporadici; collaboratore Prof. Dr. G. O. Michler dell'Institut für experimentelle Mathematik zu Essen

2003: Costruzione dei gruppi sporadici di Higman-Sims e Thompson; collaboratore Prof. Dr. G. O. Michler della Cornell University NY

2004: Gruppi speciali lineari generati da trasvezioni; collaboratori Prof. L. Di Martino dell'Università di Milano-Bicocca e Dr. R. Radina dell'Università di Milano

2004: Costruzione della tavola dei caratteri di gruppi di permutazioni di grado elevato mediante l'uso dell'algoritmo di Lenstra-Lenstra-Lovasz (LLL) e di Michler-Weller; collaboratore Prof. Dr. G. O. Michler della Cornell University NY;

2004: Automorfismi di grafi supergeneralizzati di Petersen e geometrie proiettive; collaboratori Dr. W. Pacco e Dr. M. Lovrečič;

2005: Relazioni ricorsive per la lunghezze delle orbite di forme sesquilineari e quadratiche rispetto all'azione del gruppo unitriangolare e gradi dei caratteri di sottogruppi unipotenti massimali di gruppi finiti di tipo Lie;

2006: Determinazione delle costituenti irriducibili di rappresentazioni monomiali di gruppi finiti in caratteristica coprima

2006: Costruzione del gruppo sporadico di O'Nan; collaboratore Prof. Dr. G. O. Michler della Cornell University NY

2007: Minimizzazione del grado del campo di realizzazione per rappresentazioni irriducibili in caratteristica zero: caso ciclico e non-ciclico, collaboratore Dr. C. Fieker (University of Sydney);

2007: Costruzione di reppresentazioni con assegnato carattere mediante Magma, collaboratore Prof. J. Cannon (University of Sydney);

2007: Determinazione delle classi di coniugio di sottogruppi unipotenti massimali di gruppi finiti di tipo Lie in caratteristica buona, collaboratore Prof. T. Weigel (Università di Milano-Bicocca);

2008: Determinazione dei gradi dei caratteri irriducibili di sottogruppi unipotenti massimali di gruppi finiti di tipo Lie in caratteristica buona, collaboratore Prof. T. Weigel (Università di Milano-Bicocca);

2008: Classi di equivalenza d codici di Goppa rispetto ad azioni monomiali, collaboratori Prof. F. Dalla Volta (Università di Milano-Bicocca) e Dott.ssa M.Giorgetti (Universitdell'Insubria-Como)

2009: Estensioni di scalari su codici, discese di galois e codici traccia, collaboratore Dott.ssa M.Giorgetti (Università dell'Insubria-Como)

2009: Generalizzazioni di protocolli crittografici quali LUC e XTR utilizzando polinomi ciclotomici, tori algebrici e sottogruppi irriducibili su un campo finito, collaboratori Dott. Pelosi (Politecnico di Milano) e Dott.ssa Fragneto (ST Microelectronics)

2009: Equivalenza di funzioni booleane a meno di permutazioni, collaboratore Dott. Pelosi (Politecnico di Milano)

2010-11: Costruzione esplicita di mappe birazionali per tori algebrici definiti su campi finiti per estensioni di grado primo, Congettura di Voskresenskii e applicazioni crittografiche, collaboratore Dott. Montanari (Università di Perugia)

Collaborazioni Esterne

2006-2012: Collaborazioni con la Dott.ssa Fragneto e l'Ing. Bertoni della ST Microelectronics per l'implementazione di protocolli crittografici con conseguente contratto di consulenza dell'importo di €20.000

2011: Collaborazione per l'analisi di codici BCH con la Dott.ssa Marelli, Qimonda Italy srl Design Center

Abilità

Discreta conoscenza di linguaggi di programmazione (Turbopascal, Basic) e di alcuni pacchetti di manipolazione simbolica (Maple 15, Mathematica 8.0, Magma 2.18, Pari 2.4 e Gap 4.4).