

# Martino Borello

---

## PERSONAL DETAILS

Born in Milan, MI, Italy, on July 28<sup>th</sup> 1986  
Citizenship: Italian  
Work Email: [borello@math.univ-paris13.fr](mailto:borello@math.univ-paris13.fr)  
Personal Email: [martino.borello@gmail.com](mailto:martino.borello@gmail.com)  
Homepage: <https://www.math.univ-paris13.fr/~borello/>



## EMPLOYMENT

*Associate professor* (tenure) September 2016 - present  
at Université de Paris 8,  
2 Rue de la Liberté  
93526 Saint-Denis, France  
Équipe MTII at LAGA (Universités Paris 8 et Paris 13, CNRS)

*Scientific Collaborator* (postdoc) September 2014 - August 2016  
at Mathematics Institute for Geometry and Applications,  
EPFL SB MATHGEOM CSAG  
Station 8 - CH-1015 Lausanne  
Director: Prof. Eva Bayer-Fluckiger  
Collaboration with Prof. Peter Jossen, ETH, Zürich

## EDUCATION

*PhD*, Pure and Applied Mathematics January 2011 - January 2014  
Università degli studi di Milano Bicocca, Milan, MI, Italy  
*Automorphism groups of self-dual binary linear codes with a particular regard to the extremal case of length 72*,  
supervisors Prof. Francesca Dalla Volta (Milan) and Prof. Massimiliano Sala (Trento)  
defended on January 16<sup>th</sup> 2014  
Concentration: Algebraic coding theory, Representation Theory,  
Permutation Groups, Automorphisms of combinatorial structures  
Minor: Cryptography

*Master of Science (Msc)*, Mathematics January 2009 - July 2010  
Università degli studi di Milano, Milan, MI, Italy  
*"Gauss class number problem: solution through the theory of L-function associated to elliptic curves"* (written in Italian),  
supervisor Prof. Massimo Bertolini (Milan)  
grade 110/110 cum laude  
Concentration: Algebraic geometry, Arithmetic of elliptic curves

*Bachelor of Science (Bsc)*, Mathematics September 2005 - December 2008  
Università degli studi di Milano, Milan, MI, Italy  
*"Algebraic integers in complex quadratic fields"* (written in Italian),  
supervisor Prof. Vittoria Zambelli (Milan)  
grade 110/110 cum laude  
Concentration: Algebra, Geometry, Number Theory

## VISITING POSITIONS

*Scientific Collaboration* with Prof. W. Willems October 2011 - December 2011  
Otto von Guericke Universität, Magdeburg, Germany

Scientific Collaboration with Prof. W. Willems  
Otto von Guericke Universität, Magdeburg, Germany

April 2012 - June 2012

Scientific Collaboration with Prof. G. Nebe  
RWTH Aachen University, Aachen, Germany

May 2013

Scientific Collaboration with Dr. A. Malevich  
Leibniz Universität Hannover, Hannover, Germany

November 2013

Academic visitor  
at Mathematics Institute for Geometry and Applications  
EPFL, Lausanne, Switzerland

March 2014 - May 2014

## PUBLICATIONS

- M. Borello, *The automorphism group of a self-dual [72, 36, 16] binary code does not contain elements of order 6*, IEEE Transactions on Information Theory 58(12): 7240–7245 (2012)  
(DOI:10.1109/TIT.2012.2211095)
- M. Borello and W. Willems, *Automorphism of order  $2p$  in binary self-dual extremal codes of length a multiple of 24*, IEEE Transactions on Information Theory 59(6): 3378–3383 (2013)  
(DOI:10.1109/TIT.2013.2243802)
- M. Borello, F. Dalla Volta and G. Nebe, *The automorphism group of a self-dual [72, 36, 16] code does not contain  $S_3$ ,  $A_4$  or  $D_8$* , Advances in Mathematics of Communications 7(4): 503–510 (2013)  
(DOI:10.3934/amc.2013.7.503)
- M. Borello, *The automorphism group of a self-dual [72, 36, 16] code is not an elementary abelian group of order 8*, Finite Fields and Their Applications 25: 1–7 (2014)  
(DOI:10.1016/j.ffa.2013.07.007)
- M. Borello, *Automorphism groups of self-dual binary linear codes with a particular regard to the extremal case of length 72*, PhD thesis (Università degli Studi di Milano - Bicocca)
- M. Borello and G. Nebe, *On involutions in extremal self-dual codes and the dual distance of semi self-dual codes*, Finite Fields and Their Applications 33: 80–89 (2015)  
(DOI:10.1016/j.ffa.2014.11.008)
- M. Borello, *On the automorphism groups of binary linear codes*, Topics in Finite Fields, Contemporary Mathematics 632 (2015)  
(DOI:http://dx.doi.org/10.1090/conm/632)
- E. Bayer-Fluckiger, M. Borello and P. Jossen, *Inhomogeneous minima of mixed signature lattices*, Journal of Number Theory 167: 88–103 (2016)  
(DOI:http://dx.doi.org/10.1016/j.jnt.2016.03.010)
- M. Borello and J. de la Cruz, *Some new results on the self-dual [120, 60, 24] code*, Finite Fields and Their Applications 50: 17–34 (2018)  
(DOI:https://doi.org/10.1016/j.ffa.2017.11.004)
- M. Borello and O. Mila, *Symmetries of weight enumerators and applications to Reed-Muller codes*, preprint, (<https://arxiv.org/abs/1707.00575>)

Informative papers:

- M. Borello, *Medaglie Fields 2014 - Storie di matematici esemplari*, EMMECI-quadro 55, December 2014

## REVIEWER

Reviewer for Mathematical Reviews, Journal of Algebra, Journal of Number Theory, Discrete Mathematics, IEEE, Ars Mathematica Contemporanea, Journal of Algebra and its Applications, International Journal of Algebra and Computation, Finite Fields and Their Applications

## INVITED LECTURES

At conferences:

- *On the Euclidean minimum of number fields*, XMaths 2015, Bari
- *Symmetries of weight enumerators*, BunnyTN 2016, Trento
- *Actions de groupes en thorie des codes*, Journe du LAGA 2017, Villetaneuse
- *L'erreur dans la transmission d'informations numériques, comment la corriger?*, Colloque CLI 2017, Saint-Denis

Seminars:

- *On the search of extremal self-dual codes of length 72*, Magdeburg, Germany, December 6<sup>th</sup> 2011
- *The automorphism group of an extremal [72, 36, 16] code does not contain elements of order 6*, Magdeburg, Germany, May 8<sup>th</sup> 2012
- *On the automorphism group of an extremal self-dual code of length 72*, Trento, Italy, August 10<sup>th</sup> 2012
- *On the automorphism group of extremal self-dual codes*, Trento, Italy, August 1<sup>st</sup> 2013
- *Automorphisms of self-dual binary linear codes*, EPFL Lausanne, Switzerland, November 14<sup>th</sup> 2013
- *Automorphisms of self-dual binary linear codes*, Leibniz Universität Hannover, Germany, November 20<sup>th</sup> 2013
- *New bounds for semi self-dual codes*, Milano-Bicocca, Milan, December 19<sup>th</sup> 2013
- *Automorphism groups of self-dual binary linear codes with a particular regard to the extremal case of length 72*, Université de Neuchâtel, Switzerland, April 7<sup>th</sup> 2014
- *On the stabilizer of weight enumerators of linear codes*, Université de Neuchâtel, Switzerland, December 2<sup>nd</sup> 2015
- *Symmetries of weight enumerators*, Università degli Studi di Milano-Bicocca, Italy, January 13<sup>th</sup> 2017
- *Symétries de polynômes énumérateurs*, Université de Paris 8, April 6<sup>th</sup> 2017

## TALKS & POSTERS

- *Ricerca di codici estremali autoduali di lunghezza 72*, Terzo workshop di crittografia BunnyTn 2011, Trento, Italy, March 12<sup>th</sup> 2012
- *Poster The automorphism group of an extremal [72, 36, 16] code does not contain elements of order 6*, Ischia group Theory 2012, Ischia, Italy, 26-29 March 2012

- *On the automorphisms of order  $2p$  in binary self-dual extremal codes with an application to the remarkable case of length 72*, Trends in coding theory, Ascona, Switzerland, October 29<sup>th</sup> 2012
- *Automorphisms of extremal codes*, GTG-Gruppen und Topologische Gruppen 2012, Milan, Italy, January 26<sup>th</sup> 2013
- *Automorphisms of extremal self-dual codes*, Advances in Group Theory and Applications 2013, Porto Cesareo, Italy, June 6<sup>th</sup> 2013
- *Automorphisms of extremal self-dual binary linear codes*, The 11th International Conference on Finite Fields and their Applications, Magdeburg, Germany, July 22<sup>nd</sup> 2013
- *Symmetries of weight enumerators*, The 13th International Conference on Finite Fields and their Applications, Gaeta, Italy, June 6<sup>th</sup> 2017

**WORKSHOPS &** Participation to the following schools/mini-courses:

**SCHOOLS**

- *Crittoanalisi differenziale avanzata*, Trento, Italy, November 29<sup>th</sup>–December 3<sup>rd</sup> 2010  
Lecturer: Prof. Massimiliano Sala (Trento)
- *Simple Lie algebras in prime characteristic*, Milan, Italy, May 4<sup>th</sup>–May 13<sup>th</sup> 2011  
Lecturer: Prof. Joerg Felvdoss (University of South Alabama)
- *PHD School on Elliptic Curves in Number Theory and Cryptography*, Trento, Italy, May 30<sup>th</sup>–June 3<sup>rd</sup> 2011  
Lecturer: Prof. Michele Elia (Politecnico di Torino)
- *Summer School on Finite Groups and Related Geometrical Structures 2011*, Venice, Italy, August 29<sup>th</sup>–September 9<sup>th</sup> 2011  
Lecturers: Prof. Robert Wilson (Queen Mary University of London) and Prof. Alexander Ivanov (Imperial College London)
- *Algebraic Combinatorics*, Milan, Italy, March 15<sup>th</sup>–March 23<sup>rd</sup> 2012  
Lecturer: Prof. Johannes Siemons (University of East Anglia)
- *PHD School on Groebner Bases, Curves, Codes and Cryptography*, Trento, Italy, July 30<sup>th</sup>–August 10<sup>th</sup> 2012  
Lecturers: Prof. Massimiliano Sala (Università degli Studi di Trento), Prof. Michele Elia (Politecnico di Torino), Prof. Massimo Giulietti (Università degli Studi di Perugia) and Prof. Teo Mora (Università degli Studi di Genova)
- *Quadratic forms, lattices and applications*, Les Diablerets, Switzerland, March 10<sup>th</sup>–March 14<sup>th</sup> 2014
- *Young Algebraists' Conference 2014*, Lausanne, Switzerland, June 9<sup>th</sup>–June 13<sup>th</sup>  
Lecturers: Prof. Stephen Donkin (York), Dr. Tim Burness (Bristol) and Dr. Olivier Dudas (Denis Diderot, Paris 7)
- *2014 Bicocca Ph.D. School and Workshop in Representation Theory*, Milan, Italy, June 16<sup>th</sup>–June 20<sup>th</sup> 2014  
Lecturers: Prof. Martin Isaacs (Madison), Prof. Gabriel Navarro (Valencia)
- *Mini-courses on Arithmetic Geometry*, Basel, Switzerland, June 1<sup>st</sup>–June 3<sup>rd</sup> 2015  
Lecturers: Prof. Pietro Corvaja (Udine), Prof. Ulrich Derenthal (Hannover), Prof. Philipp Habegger (Basel)

Participation to the following international workshops:

- *Riemann International School of Mathematics - Advances in Number Theory and Geometry*, Verbania, Italy, April 2009
- *The Seventh International Workshop on Coding and Cryptography 2011 (WCC 2011)*, Paris, France, April 2011
- *Bicocca-Workshop on Linear Groups and Group Representations: Classification Problems*, Milan, Italy, July 2011
- *Kolloquium uber Kombinatorik*, Magdeburg, Germany, November 2011
- *3rd International Castle Meeting on Coding Theory and Applications*, Cardona, Spain, September 2011
- *International Workshop on Coding and Cryptography 2013 (WCC 2013)*, Bergen, Norway, April 2013
- *Zeta functions of groups and related algebraic structures*, Padova, Italy, September 2013
- *Number Theory Days 2014*, Zürich, Switzerland, March 2014
- *Number Theory Days 2015*, Lausanne, Switzerland, May 2015
- *Analytic Aspects of Number Theory*, Zurich, Switzerland, May 2015
- *Effective Methods in Algebraic Geometry*, Trento, Italy, June 2015
- *Lattices and Applications in Number Theory*, Oberwolfach, Germany, January 2016
- *Number Theory Days 2016*, Zürich, Switzerland, April 2016

**TEACHING  
EXPERIENCE**

*Associate professor* September 2016 - present  
 Université de Paris 8, Saint-Denis, France  
 AY 2016-2017

- Course of “Information Theory” (30 hours - grad)
- Course of “Interactions codes/cryptography” (30 hours - grad)
- Course of “Introduction to coding theory” (30 hours - undergrad)
- Course of “Combinatorics” (30 hours - undergrad)
- Course of “Coding theory 1” (30 hours - grad)

AY 2016-2017

- Course of “Information Theory” (30 hours - grad)
- Course of “Algorithms for cryptography” (30 hours - grad)
- Course of “Geometry” (30 hours - undergrad)
- Course of “Combinatorics” (30 hours - undergrad)

*Teaching Assistant* September 2014 - August 2016  
 EPFL, Lausanne, Switzerland  
 AY 2015-2016

- Exercises of “Group Theory” (24 hours - undergrad)
- Exercises of “Rings and Fields” (24 hours - undergrad)

AY 2014-2015

- Exercises of “Algebra I and II” (48 hours - undergrad)

*Teaching Assistant* January 2011 - August 2014  
Università degli studi di Milano-Bicocca, Milan, MI, Italy  
AY 2013-2014

- Exercises of “Principles of Mathematics” (16 hours - undergrad)
- Tutoring of “Recalls of Mathematics”(45 hours - undergrad)

AY 2012-2013

- Exercises of “Algebraic methods for computer science” (24 hours - undergrad)
- Tutoring of “Recalls of Mathematics”(30 hours - undergrad)

AY 2011-2012

- Tutoring of “Fundamentals of Mathematics” (20 hours - undergrad)

*Tutor – Laboratory of Cryptography* March 2014  
Istituto Santa Dorotea, Arcore  
Basic lectures of cryptography and elementary number theory (10 hours)

*Tutor of Mathematics* June 2010 - February 2014  
Camplus (University College), Milan  
Tutoring to freshmen of engineering and architecture (more than 40 hours)

*Tutor – Laboratory of Cryptography* March 2013  
I.I.S. Greppi, Monticello  
Basic lectures of cryptography and elementary number theory (6 hours)

*Tutor – Laboratory of Cryptography* February 2013  
Liceo Scientifico Cremona, Milan  
Basic lectures of cryptography (6 hours)

*Teacher of Mathematics* Summer 2009  
Liceo Scientifico Donatelli-Pascal, Milan  
Remedial courses for high school students (20 hours)

**ADMINISTRATIVE  
EXPERIENCE**

Member of the Advisory Committee (*Comité Consultatif*) 2018 - present  
Department of Mathematics, Université de Paris 8, Saint-Denis, France

Co-organizer of the “Seminaire Protection de l’information” 2017 - present  
Université de Paris 8, Saint-Denis, France

Co-organizer of a working seminar on Bruhat-Tits buildings 2015 - 2016  
EPFL, Lausanne, Switerland

Co-organizer of the “Seminaire d’Algèbre et de Théorie des Nombres” 2015-2016  
EPFL, Lausanne, Switerland

**SUPERVISIONS**

*Semester Project (Master)* of Z. Haddad and T. Benbouabdellah Spring 2017  
*Fonctions de hachage*

*Semester Project (Master)* of I. Benabed and M.H. Benyahia Spring 2017  
*Algorithmes de signature numérique*

*Semester Project (Master)* of A. Kerfi and T. Messous Spring 2017  
*Attaques contre le cryptosystème RSA*

*Semester Project (Master)* of S. Dehl and S. Hamel Spring 2017  
*Chaînes de blocs et bitcoins*

<i>Semester Project (Master) of R. Issaad</i> <i>Entropie de la langue française</i>	Spring 2017
<i>Semester Project (Bachelor) of Quentin Levêque,</i> <i>Sur les groupes simples</i> with Prof. Eva Bayer-Fluckiger	Spring 2016
<i>Semester Project (Bachelor) of Filip Fifka,</i> <i>Ideal Class Group</i> with Prof. Eva Bayer-Fluckiger	Autumn 2015
<i>Master project of Olivier Mila,</i> <i>Invariance for weight enumerators of evaluation codes</i> <i>and counting <math>\mathbb{F}_q</math>-rational points on hypersurfaces</i> with Prof. Eva Bayer-Fluckiger	Spring 2015
<i>Semester Project (Master) of Alessandro Slamitz,</i> <i>Inverse Galois Problem: Intersective Polynomials</i> with Prof. Eva Bayer-Fluckiger	Autumn 2014

**PRIZES AND GRANTS**

- Projet AAP Paris 8, 1800€ 2018
- Projet Exploratoire Premier Soutien (PEPS)  
“Jeunes chercheur-e-s”, 2500€ 2018
- Projet Exploratoire Premier Soutien (PEPS)  
“Jeunes chercheur-e-s”, 3500€ 2017
- “Fondazione Famiglia Legnanese” Scholarship, 3000€ 2009
- “Istituto Nazionale di Alta Matematica” Scholarships, 12000€ 2005-2007
- “Mu Alpha Theta-Fast” Prize for the use of modern mathematics  
project “The minor chord: mathematical harmony of music” 2005
- “Istituto Lombardo, Accademia di Scienze e Lettere”  
Scholarships, 6000€ 2001-2004

**COMPUTER SKILLS**

Excellent knowledge of the document markup language LaTeX and of the computer algebra systems MAGMA and Maple  
Good knowledge of Matlab, Office, Cabri and C  
Basic knowledge of Java, Photoshop

**LANGUAGE SKILLS**

Italian: mother tongue  
English: fluent, written and spoken (First Certificate in English in 2004)  
French: fluent, written and spoken  
German: elementary (A1)

**EXTRA-CURRICULAR ACTIVITIES**

*Co-founder* in 2008 of the cultural group CUMA (“Mathematical culture”) to promote and organize conferences inviting some of the best mathematicians of the world. Two outstanding conferences were with Prof. Enrico Bombieri (Fields Medal in 1974, Professor in the Institute for Advanced Studies in Princeton) and with Prof. Edward Nelson (Professor in the Mathematics Department at Princeton University)

*Organizer* with CUMA of study aids for freshmen of Mathematics, consisting in simulations of some exams (in particular Algebra)

*Co-founder* of the association “Associazione Capitano Grandi”, for the promotion and diffusion of traditional Italian mountains songs in Italy and in Europe (international concerts in Spain, Switzerland and Lithuania)

*Organizer* of a volunteer time at “Sacra Famiglia” of Cesano Boscone, a nursing home for disabled people close to Milan