CURRICULUM VITAE

CARLO SANNA

Contact information

Last update: August 21, 2023

Address	Politecnico di Torino Department of Mathematical Sciences "G. L. Lagrange" Corso Duca degli Abruzzi 24, 10129 Torino, Italy
E-mail	carlo.sanna@polito.it

Positions

01/03/2022 – on going	**Researcher (RTDb)** Politecnico di Torino
01/02/2020 – 31/01/2022	**Postdoctoral Researcher** Politecnico di Torino
01/02/2019 – 31/01/2020	**Postdoctoral Researcher** Unità INdAM dell'Università di Genova

Abilitazione

Abilitazione Scientifica Nazionale per il ruolo di Professore di Seconda Fascia, Settore Concorsuale 01/A2 (Geometria e Algebra), valida dal 11/11/2020 al 11/11/2031.

Education

15/10/2018	**PhD in Pure and Applied Mathematics**, cum laude Università degli Studi di Torino, in association with Politecnico di Torino Thesis title: *"Arithmetic properties of linear recurrences and other topics in Number Theory"* Supervisor: Prof. Danilo Bazzanella Referees: Prof. Giuseppe Molteni, Prof. Alberto Perelli
16/07/2015	**Master of Science, Mathematics**, 110/110 cum laude and "menzione di merito" Università degli Studi di Torino
15/10/2013	**Bachelor of Science, Mathematics**, 110/110 cum laude Università degli Studi di Torino

Awards, prizes, and scholarships

2020	**Award con.Scienze** (€ 1.000) sponsored by "Conferenza Nazionale dei Presidenti e dei Direttori delle Strutture Universitarie di Scienze e Tecnologie", and given to the six best PhD theses in the scientific areas CUN 01-05 (08/2018–07/2019)
2016	**Award Medaglia d'Argento and prize Luciana Picco Botta** (€ 2.000) sponsored by Università degli Studi di Torino, for the best master thesis in Mathematics of the academic year 2014/15

2015 | **PhD scholarship "Contemporary Problems in Mathematics"**
Ranked first over 35 candidates

Research groups and projects

2023 – 2026 | **Quantum-oriented Update to Browsers and Infrastructure for the Post-Quantum Transition (QUBIP) – HORIZON-CL3-2022-CS-01-03**
Responsabile Scientifico di Struttura

2023 – 2025 | **SEcurity and RIghts in the CyberSpace (SERICS) – PNRR, Mission 4**
Responsabile Scientifico Spoke 5

2018 – ongoing | **Member of CrypTO – Group of Cryptography and Number Theory**
Department of Mathematical Sciences "G. L. Lagrange", Politecnico di Torino

2018 – ongoing | **Member of "Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni"**
Istituto Nazionale di Alta Matematica

2017 – 2018 | **Member of the research project "Algebra e Dintorni"**
Department of Mathematics "G. Peano", Università degli Studi di Torino

2017 – 2018 | **Member of the research project "Approssimazione multivariata e algoritmi efficienti con applicazioni a problemi algebrici, differenziali e integrali"**
Department of Mathematics "G. Peano", Università degli Studi di Torino

Conferences

22/09/2021 – 23/09/2021 | **Co-organizer of "6th Number Theory Meeting – Torino"**
Department of Mathematical Sciences "G. L. Lagrange", Politecnico di Torino

26/10/2021 – 27/10/2021 | **Co-organizer of "5th Number Theory Meeting – Torino"**
Department of Mathematical Sciences "G. L. Lagrange", Politecnico di Torino

27/05/2021 – 28/05/2021 | **Co-organizer of "CrypTO Conference 2021"**
Department of Mathematical Sciences "G. L. Lagrange", Politecnico di Torino

24/10/2019 – 25/10/2019 | **Co-organizer of "4th Number Theory Meeting – Torino"**
Department of Mathematics "G. Peano", Università di Torino

15/10/2018 – 16/10/2018 | **Co-organizer of "3rd Number Theory Meeting – Torino"**
Department of Mathematics "G. Peano", Università di Torino

26/10/2017 – 27/10/2017 | **Co-organizer of "2nd Number Theory Meeting – Torino"**
Department of Mathematical Sciences "G. L. Lagrange", Politecnico di Torino

Teaching experiences

2022/23 | **"Linear Algebra and Geometry"** (60 hours)
Politecnico di Torino

2021/22 | **"Linear Algebra and Geometry"** (60 hours)
Politecnico di Torino

2020/21 | **Assistant of "Linear Algebra and Geometry"** (40 hours)
Politecnico di Torino

2019/20 **PhD course "Blockchain and Cryptoeconomy"** (first part, 10 hours)
Politecnico di Torino

2018/19 **Assistant of "Mathematical Methods for Engineers"** (40 hours)
Politecnico di Torino

2018/19 **Assistant of "Mathematics I"** (40 hours)
Corso di Laurea Triennale in Chimica e Tecnologie Chimiche, Università di Torino

2017/18 **Assistant of "Mathematical Analysis I"** (60 hours)
Politecnico di Torino

2016/17 **Assistant of "Mathematical Analysis I"** (60 hours)
Politecnico di Torino

Thesis supervisor

15/03/22 **Sistemi Post-Quantum: Crittografia Multivariata**
Laurea Magistrale in Ingegneria Matematica, Politecnico di Torino
Candidate: Adriano Koleci, Supervisors: Danilo Bazzanella, Carlo Sanna

23/11/21 **Numeri Pseudocasuali: Proprietà e Applicazioni in Crittografia**
Laurea in Matematica per l'Ingegneria, Politecnico di Torino
Candidate: Davide Arnaudo, Supervisors: Danilo Bazzanella, Giuseppe D'Alconzo, Carlo Sanna

11/09/20 **Cifrari Monoalfabetici e Analisi delle Frequenze**
Laurea in Matematica per l'Ingegneria, Politecnico di Torino
Candidate: Matteo Galla, Supervisors: Danilo Bazzanella, Carlo Sanna

Talks and presentations

26/05/23 **Schemi di Firma Digitale Post-Quantum Basati su MinRank**
CrypTO Conference, Torino

04/05/23 **Zeckendorf expansions of multiplicative inverses**
The 7th mini symposium of the Roman Number Theory Association, Rome

05/01/23 (invited) **Some results on the greatest common divisors of terms of linear recurrences**
Faculty of Mathematics and Computer Science of the Jagiellonian University, online

06/12/22 (invited) **Some results on the greatest common divisors of terms of linear recurrences**
Dipartimento di Matematica, Università di Genova

26/05/22 **Membership in random ratio sets**
Combinatorial and Additive Number Theory 2022, New York Number Theory Seminar, online

11/12/21 **On the number of residues of linear recurrences**
Combinatorial Number Theory and Connected Topics (CONTACT-I), online

26/05/21 **Additive bases and Niven numbers**
Combinatorial and Additive Number Theory 2021, New York Number Theory Seminar, online

04/03/21 (invited) **Least common multiples of integer sequences: old and new results**
Number Theory Online, Università di Pisa, Roma Sapienza, Parma, online

18/02/21 (invited) **Cryptanalysis of Multivariate Public Key Cryptosystems**
Technology Innovation Institute, United Arab Emirates, online

05/02/21 (invited) **Introduction to Multivariate Cryptography**
Seminario della serie De Cifris Augustae Taurinorum, online

23/09/20 (invited) **Additive and Xor differential probabilities of Chacha quarter round**
Technology Innovation Institute, United Arab Emirates, online

22/07/20 **On the least common multiple of random terms of binary recurrence sequences**
19th International Conference on Fibonacci Numbers and Their Applications, online

21/05/19 (invited) **On the number of distinct exponents in the prime factorization of an integer**
Seminari di Algebra e Geometria Algebrica, Università di Torino

12/04/19 **Approximations by signed harmonic sums and the Thue–Morse sequence**
5th mini symposium of the Roman Number Theory Association, Università Roma Tre

18/04/18 **Waring's theorem for binary powers**
4th mini symposium of the Roman Number Theory Association, Università Roma Tre

12/04/18 (invited) **Distribution of integral values for the ratio of two linear recurrences**
Giornata dei dottorandi di Teoria dei Numeri, Università degli Studi di Parma

19/12/17 (invited) **A coprimality condition on consecutive values of polynomials**
Giornate INdAM di Teoria dei Numeri, Università degli Studi di Genova

21/09/17 **On the greatest common divisor of n and the nth Fibonacci Number**
20th International Workshop for Young Mathematicians, Jagiellonian University

06/07/17 **On the G.C.D. of n and the nth term of a linear recurrence**
XXXth Journées Arithmétiques, University of Caen

05/06/17 **On the sum of digits of the factorial**
Numeration 2017, Università degli Studi Roma Tre

04/11/16 **A factor of integer polynomials with minimal integrals**
1st Number Theory Meeting - Torino, Università degli Studi di Torino

Preprints

On the distribution of the entries of a fixed-rank random matrix over a finite field
https://arxiv.org/abs/2307.14172

On the inverse of a Fibonacci number modulo a Fibonacci number being a Fibonacci number
http://arxiv.org/abs/2306.08382

Smaller public keys for MinRank-based schemes
(with Antonio J. Di Scala)
https://arxiv.org/abs/2302.12447

Toward a Post-Quantum Zero-Knowledge Verifiable Credential System for Self-Sovereign Identity
(with Simone Dutto, Davide Margaria, and Andrea Vesco)
https://eprint.iacr.org/2022/1297

On the index of appearance of a Lucas sequence
https://arxiv.org/abs/2212.06127

Accepted peer-reviewed papers

RLWE and PLWE over cyclotomic fields are not equivalent
(with Antonio J. Di Scala and Edoardo Signorini)
Applicable Algebra in Engineering, Communication and Computing
https://doi.org/10.1007/s00200-022-00552-9

Finding differential trails on ChaCha by means of state functions
(with Emanuele Bellini, Juan Grados, and Rusydi H. Makarim)
International Journal of Applied Cryptography

Published peer-reviewed papers

2023 **On the greatest common divisor of n and the nth Fibonacci number, II**
(with Abhishek Jha)
Canadian Mathematical Bulletin **66**, 617–625
https://doi.org/10.4153/S0008439522000595

2023 **A note on the distribution of weights of fixed-rank matrices over the binary field**
Finite Fields and Their Applications **87**, 102157
https://doi.org/10.1016/j.ffa.2022.102157

2023 **Zeckendorf representation of multiplicative inverses modulo a Fibonacci number**
(with Gessica Alecci and Nadir Murru)
Monatshefte für Mathematik **201**, 1–9
https://doi.org/10.1007/s00605-022-01724-y

2023 **Pairwise modular multiplicative inverses and Fibonacci numbers**
INTEGERS **23**, article A3
http://math.colgate.edu/~integers/vol23.html

2022 **MR-DSS – Smaller MinRank-based (Ring-)Signatures**
(with Emanuele Bellini, Andre Esser, and Javier Verbel)
PQCrypto 2022: Post-Quantum Cryptography
Lecture Notes in Computer Science, vol. 13512, pp. 144–169
https://doi.org/10.1007/978-3-031-17234-2_8

2022 **An Estimator for the Hardness of the MQ Problem**
(with Emanuele Bellini, Rusydi H. Makarim, and Javier Verbel)
Progress in Cryptology—AFRICACRYPT 2022
Lecture Notes in Computer Science, vol. 13503, pp. 323–347
https://doi.org/10.1007/978-3-031-17433-9_14

2022 **A survey on coefficients of cyclotomic polynomials**
Expositiones Mathematicae **40**, 469–494
https://doi.org/10.1016/j.exmath.2022.03.002

2022 **Greatest common divisors of shifted primes and Fibonacci numbers**
(with Abhishek Jha)
Research in Number Theory **8**, 65
https://doi.org/10.1007/s40993-022-00365-2

2022 **Practical complexities of probabilistic algorithms for solving Boolean polynomial systems**
(with Stefano Barbero, Emanuele Bellini, and Javier Verbel)
Discrete Applied Mathematics **309**, 13–31
https://doi.org/10.1016/j.dam.2021.11.014

2022 **On the divisibility of the rank of appearance of a Lucas sequence**
International Journal of Number Theory **18**, 2145–2156
https://doi.org/10.1142/S1793042122501093

2022 **On the number of residues of linear recurrences**
Research in Number Theory **8**, 7
https://doi.org/10.1007/s40993-021-00305-6

2022 **The largest entry in the inverse of a Vandermonde matrix**
(with Jeffrey Shallit and Shun Zhang)
Linear and Multilinear Algebra **70**, 5634–5641
https://doi.org/10.1080/03081087.2021.1922337

2022 **Membership in random ratio sets**
Indagationes Mathematicae **33**, 1326–1333
https://doi.org/10.1016/j.indag.2022.08.007

2022 **On the l.c.m. of shifted Lucas numbers**
Indagationes Mathematicae **33**, 1001–1011
https://doi.org/10.1016/j.indag.2022.04.006

2022 **On the exponents in the factorizations of r consecutive numbers**
Quaestiones Mathematicae **45**, 1221–1228
https://doi.org/10.2989/16073606.2021.1938277

2022 **Practical central binomial coefficients**
Quaestiones Mathematicae **44**, 1141–1144
https://doi.org/10.2989/16073606.2020.1775156

2021 **A note on the natural density of product sets**
(with Sandro Bettin and Dimitris Koukoulopoulos)
Bulletin of the London Mathematical Society **53**, 1407–1413
https://doi.org/10.1112/blms.12506

2021 **Additive bases and Niven numbers**
Bulletin of the Australian Mathematical Society **104**, 373–380
https://doi.org/10.1017/S0004972721000186

2021 **On the l.c.m. of shifted Fibonacci numbers**
International Journal of Number Theory **17**, 2009–2018
https://doi.org/10.1142/S1793042121500743

2021 **On the least common multiple of shifted powers**
Journal of Integer Sequences **24**, article 21.7.3
https://cs.uwaterloo.ca/journals/JIS/VOL24/Sanna/sanna7.html

2021 **On the least common multiple of random q-integers**
Research in Number Theory **7**, 16
https://doi.org/10.1007/s40993-021-00242-4

2021 **On the condition number of the Vandermonde matrix of the nth cyclotomic polynomial**
(with Antonio J. Di Scala and Edoardo Signorini)
Journal of Mathematical Cryptology **15**, 174–178
https://doi.org/10.1515/jmc-2020-0009

2020 **Greedy approximations by signed harmonic sums and the Thue–Morse sequence**
(with Sandro Bettin and Giuseppe Molteni)
Advances in Mathematics **366**, 107068
https://doi.org/10.1016/j.aim.2020.107068

2020 **On the l.c.m. of random terms of binary recurrence sequences**
Journal of Number Theory **213**, 221–231
https://doi.org/10.1016/j.jnt.2019.12.004

2020 **A note on product sets of random sets**
Acta Mathematica Hungarica **162**, 76–83
https://doi.org/10.1007/s10474-019-01014-4

2020 **On numbers divisible by the product of their nonzero base b digits**
Quaestiones Mathematicae **43**, 1563–1571
https://doi.org/10.2989/16073606.2019.1637956

2020 **Least common multiple of polynomial sequences**
(with Danilo Bazzanella)
Rendiconti del Seminario Matematico Università e Politecnico di Torino **78**, n° 1, 21–25

2020 **Directions sets: A generalization of ratio sets**
(with Paolo Leonetti)
Bulletin of the Australian Mathematical Society **101**, 389–395
https://doi.org/10.1017/S0004972719000959

2020 **Practical numbers among the binomial coefficients**
(with Paolo Leonetti)
Journal of Number Theory **207**, 145–155
https://doi.org/10.1016/j.jnt.2019.07.005

2020 **On the number of distinct exponents in the prime factorization of an integer**
Proceedings of the Indian Academy of Sciences **130**, 27
https://doi.org/10.1007/s12044-020-0556-y

2020 **p-adic denseness of members of partitions of $\mathbb{N}$ and their ratio sets**
(with Piotr Miska)
Bulletin of the Malaysian Mathematical Sciences Society **43**, 1127–1133
https://doi.org/10.1007/s40840-019-00728-6

2019 **Waring's theorem for binary powers**
(with Daniel Kane and Jeffrey Shallit)
Combinatorica **39**, 1335–1350
https://doi.org/10.1007/s00493-019-3933-3

2019 **Practical numbers in Lucas sequences**
Quaestiones Mathematicae **42**, 977–983
https://doi.org/10.2989/16073606.2018.1502697

2019 **On the p-adic denseness of the quotient set of a polynomial image**
(with Piotr Miska and Nadir Murru)
Journal of Number Theory **197**, 218–227
https://doi.org/10.1016/j.jnt.2018.08.010

2019 **On numbers n with polynomial image coprime with the nth term of a linear recurrence**
(with Daniele Mastrostefano)
Bulletin of the Australian Mathematical Society **99**, 23–33
https://doi.org/10.1017/S0004972718000606

2019 **On numbers n relatively prime to the nth term of a linear recurrence**
Bulletin of the Malaysian Mathematical Sciences Society **42**, 827–833
https://doi.org/10.1007/s40840-017-0514-8

2018 **Small values of signed harmonic sums**
(with Sandro Bettin and Giuseppe Molteni)
Comptes Rendus Mathématique **356**, 1062–1074
https://doi.org/10.1016/j.crma.2018.11.007

2018 **On the greatest common divisor of n and the nth Fibonacci number**
(with Paolo Leonetti)
Rocky Mountain Journal of Mathematics **48**, 1191–1199
https://doi.org/10.1216/RMJ-2018-48-4-1191

2018 **The density of numbers n having a prescribed G.C.D. with the nth Fibonacci number**
(with Emanuele Tron)
Indagationes Mathematicae **29**, 972–980
https://doi.org/10.1016/j.indag.2018.03.002

2018 **The moments of the logarithm of a G.C.D. related to Lucas sequences**
Journal of Number Theory **191**, 305–315
https://doi.org/10.1016/j.jnt.2018.03.012

2018 **A note on primes in certain residue classes**
(with Paolo Leonetti)
International Journal of Number Theory **14**, 2219–2223
https://doi.org/10.1142/S1793042118501336

2018 **Central binomial coefficients divisible by or coprime to their indices**
International Journal of Number Theory **14**, 1135–1141
https://doi.org/10.1142/S1793042118500707

2018 **On the k-regularity of the k-adic valuation of Lucas sequences**
(with Nadir Murru)
Journal de Théorie des Nombres de Bordeaux **30**, 227–237
https://doi.org/10.5802/jtnb.1025

2017 **On the closure of the image of the generalized divisor function**
Uniform Distribution Theory **12**, 77–90
https://doi.org/10.1515/udt-2017-0016

2017 **A coprimality condition on consecutive values of polynomials**
(with Márton Szikszai)
Bulletin of the London Mathematical Society **49**, 908–915
https://doi.org/10.1112/blms.12078

2017 **Distribution of integral values for the ratio of two linear recurrences**
Journal of Number Theory **180**, 195–207
https://doi.org/10.1016/j.jnt.2017.04.015

2017 **p-adic quotient sets**
(with Stephan Ramon Garcia, Yu Xuan Hong, Florian Luca, Elena Pinsker, Evan Schechter, and Adam Starr)
Acta Arithmetica **179**, 163–184
https://doi.org/10.4064/aa8579-4-2017

2017 **The quotient set of k-generalised Fibonacci numbers is dense in $\mathbb{Q}_p$**
Bulletin of the Australian Mathematical Society **96**, 24–29
https://doi.org/10.1017/S0004972716001118

2017 **A factor of integer polynomials with minimal integrals**
Journal de Théorie des Nombres de Bordeaux **29**, 637–646
https://doi.org/10.5802/jtnb.994

2017 **On numbers n dividing the nth term of a Lucas sequence**
International Journal of Number Theory **13**, 725–734
https://doi.org/10.1142/S1793042117500373

2017 **On the p-adic valuation of Stirling numbers of the first kind**
(with Paolo Leonetti)
Acta Mathematica Hungarica **151**, 217–231
https://doi.org/10.1007/s10474-016-0680-4

2016 **The p-adic valuation of Lucas sequences**
The Fibonacci Quarterly **54**, 118–124
https://www.fq.math.ca/54-2

2016 **On the p-adic valuation of harmonic numbers**
Journal of Number Theory **166**, 41–46
https://doi.org/10.1016/j.jnt.2016.02.020

2015 **Counting arithmetic formulas**
(with Edinah K. Gnang and Maksym Radziwiłł)
European Journal of Combinatorics **47**, 40–53
https://doi.org/10.1016/j.ejc.2015.01.007

2015 **On the number of arithmetic formulas**
International Journal of Number Theory **11**, 1099–1106
https://doi.org/10.1142/S1793042115500591

2015 **On the sum of digits of the factorial**
Journal of Number Theory **147**, 836–841
https://doi.org/10.1016/j.jnt.2014.09.003

2014 **Covering an arithmetic progression with geometric progressions and vice versa**
International Journal of Number Theory **10**, 1577–1582
https://doi.org/10.1142/S1793042114500456

2014 **On the exponential sum with the sum of digits of hereditary base b notation**
INTEGERS **14**, article A36
https://www.integers-ejcnt.org/vol14.html

2014 **On the asymptotic density of the support of a Dirichlet convolution**
Journal of Number Theory **134**, 1–12
https://doi.org/10.1016/j.jnt.2013.07.012

2013 **Uncertainty principles connected with the Möbius inversion formula**
(with Paul Pollack)
Bulletin of the Australian Mathematical Society **88**, 460–472
https://doi.org/10.1017/S0004972712001128

2012 **On arithmetic progressions of integers with a distinct sum of digits**
Journal of Integer Sequences **15**, article 12.8.1
https://cs.uwaterloo.ca/journals/JIS/VOL15/Sanna/sanna3.html

2012 **A new elementary proof of the inequality** $\varphi(n) > \pi(n)$
Notes on Number Theory and Discrete Mathematics **18**, No. 3, 35–37
https://nntdm.net/volume-18-2012/number-3/35-37

References

Giuseppe Molteni (PhD Thesis Referee)
Università degli Studi di Milano
Department of Mathematics "F. Enriques"
Via Saldini 50, 20133 Milano, Italy
giuseppe.molteni1@unimi.it

Alberto Perelli (PhD Thesis Referee)
Università degli Studi di Genova
Department of Mathematics
Via Dodecaneso 35, 16146 Genova, Italy
perelli@dima.unige.it

Danilo Bazzanella (PhD Supervisor)
Politecnico di Torino
Department of Mathematics "G. L. Lagrange"
Corso Duca degli Abruzzi 24, 10129 Torino, Italy
danilo.bazzanella@polito.it

Umberto Cerruti (MSc Supervisor)
Università degli Studi di Torino
Department of Mathematics "G. Peano"
Via Carlo Alberto 10, 10123 Torino, Italy
umberto.cerruti@unito.it

Paolo Boggiatto (BSc Supervisor)
Università degli Studi di Torino
Department of Mathematics "G. Peano"
Via Carlo Alberto 10, 10123 Torino, Italy
paolo.boggiatto@unito.it