

Rowing Through Numbers

Celebrating Francesco Pappalardi's 60th birthday

May 18-21, 2025, Salahaddin University, Erbil, Kurdistan region, Iraq

Some topics in analytic number theory

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris

*Honorary staff member of the Department of Mathematics,
Salahaddin University, Erbil, Iraq*

<http://www.imj-prg.fr/~michel.waldschmidt/>

Abstract

Analytic number theory is a very active domain of research.
We survey a selection of some of the many recent results



SICME 2019

February 3 - 5, 2019:

The second international conference of mathematics in Erbil,
College of Science, Salahaddin University, Erbil.



Pierre Cartier: A Visionary Mathematician

Alain Connes and Joseph Kouneiher

Pierre Cartier passed away on August 17, 2024,



Pierre Cartier
1932–2024

I could describe myself as a mathematician without borders, borrowing from a well-known saying. By this, I mean crossing boundaries, which allowed me to do mathematics in some rather remarkable countries — Vietnam, Iraq, Kurdistan, and others. Teaching mathematics in such places made the effort worthwhile.

Why is it interesting to cross borders? Because on the other side, things are different. It's always exciting to venture to the other side of the fence, to see what lies in the shade. What may seem uninteresting on one side can be a treasure on the other, offering a fresh perspective. Something that might seem trivial here could be significant there.

<https://doi.org/10.1090/noti3140>

Selected topics in analytic number theory

**A gentle introduction to a few subjects on which
Francesco contributed with original new results.**

- Artin's problem
- Egyptian fractions
- Permutation polynomials
- Elliptic curves
- Arithmetic functions
- Zero sum problems
- Multiplicatively dependent vectors
- Counting dihedral and quaternionic extensions

Some statistics from

<https://zbmath.org/authors/pappalardi.francesco>

Pappalardi, Francesco

Author ID: [pappalardi.francesco](#) 

Published as: Pappalardi, Francesco; Pappalardi, F.

External Links: [MGP](#)  · [Wikidata](#) 

Videos: [carmin.tv](#) 

Documents Indexed: [51 Publications](#) since 1991, including [1 Additional arXiv Preprint](#)
[3 Contributions as Editor](#)

Co-Authors: [44 Co-Authors](#) with [45 Joint Publications](#)
[1,537 Co-Co-Authors](#)

Co-Authors

all ▾

- 9 single-authored
- 9 Luca, Florian
- 9 Shparlinski, Igor E.
- 4 Banks, William David
- 4 David, Chantal
- 3 Adhikari, Sukumar Das

Serials

all ▾

- 6 Finite Fields and their Applications
- 5 Journal of Number Theory
- 4 Acta Arithmetica
- 3 Rendiconti del Seminario Matematico
- 2 Discrete Mathematics

Fields

all ▾

- 48 Number theory (11-XX)
- 5 Algebraic geometry (14-XX)
- 3 General and overarching topics; collections (00-XX)
- 3 Combinatorics (05-XX)
- 3 Commutative algebra (13-XX)

40 Publications have been cited 306 times in 242 Documents

Cited by ▼

Year

Contributions to zero-sum problems. Zbl 1161.11311 Adhikari, Sukumar Das ; Chen, Yonggao ; Friedlander, J. B. ; Konyagin, S. V. ; Pappalardi, F.	47	2006
Average Frobenius distributions of elliptic curves. Zbl 0934.11033 David, Chantal ; Pappalardi, Francesco	30	1999
On the order of finitely generated subgroups of \mathbb{Q}^* (mod p) and divisors of $p - 1$. Zbl 0847.11049 Pappalardi, Francesco	17	1996
A survey on k -freeness. Zbl 1156.11338 Pappalardi, Francesco	17	2005
Some zero-sum constants with weights. Zbl 1207.11030 Adhikari, Sukumar Das ; Balasubramanian, R. ; Pappalardi, F. ; Rath, Purusottam	16	2008

Mathematics Genealogy Project

Francesco Pappalardi

[MathSciNet](#)

Ph.D. [McGill University](#) 1993



Dissertation: On Artin's Conjecture for Primitive Roots

Mathematics Subject Classification: 11—Number theory

Advisor: [M. Ram Pedaprolu \(Maruti\) Murty](#)

Students:

Click [here](#) to see the students listed in chronological order.

Name	School	Year	Descendants
Anwar Mohamed Fouad, Mohammed	Università degli Studi di Roma Tre	2018	
Meleleo, Giulio	Università degli Studi di Roma Tre	2015	
Menici, Lorenzo	Università degli Studi di Roma Tre	2016	
Pehlivan, Cihan	Università degli Studi di Roma Tre	2015	
Susa, Andrea	Università degli Studi di Roma Tre	2006	

According to our current on-line database, Francesco Pappalardi has 5 students and 5 descendants.
We welcome any additional information.

M. Ram Pedaprolu (Maruti) Murty

[MathSciNet](#)

Ph.D. [Massachusetts Institute of Technology](#) 1980



Dissertation: *Artin's Conjecture and Non-Abelian Sieves*

Mathematics Subject Classification: 11—Number theory

Advisor 1: [Harold Mead Stark](#)

Advisor 2: [Dorian Morris Goldfeld](#)

Students:





Click [here](#) to see the students listed in chronological order.

Name	School	Year	Descendants
Cioaba, Sebastian	Queen's University at Kingston	2006	8
Clark, David	McGill University	1992	1
Cojocaru, Alina Carmen	Queen's University at Kingston	2002	4
David, Chantal	McGill University	1993	1
Droll, Andrew	Queen's University at Kingston	2012	
Felix, Adam	Queen's University at Kingston	2011	
Fodden, Brandon	Queen's University at Kingston	2007	
Harper, Malcolm	McGill University	2000	
Kar, Arpita	Queen's University at Kingston	2020	
Myers, Marilyn	Queen's University at Kingston	2007	
Pappalardi, Francesco	McGill University	1993	5
Pasten, Hector	Queen's University at Kingston	2014	1
Pathak, Siddhi	Queen's University at Kingston	2019	
Rundle, Robert	Queen's University at Kingston	2012	
Saidak, Filip	Queen's University at Kingston	2001	1
Séguin, François	Queen's University at Kingston	2018	
Sica, Francesco	McGill University	1998	
Sinha, Kaneenika	Queen's University at Kingston	2006	4
Stefanicki, Tomasz	McGill University	1992	
Vatwani, Akshaa	Queen's University at Kingston	2016	2
Weatherby, Chester	Queen's University at Kingston	2009	
Wong, Peng-Jie	Queen's University at Kingston	2017	
Zhang, Yuanli	McGill University	1994	
























Ram Murty

FUTURE PLANNED MISSIONS

n.	YEAR	COUNTRY	CITY	OCCASION	DATES
-	2024	Georgia	 Tbilisi		
-	2024	Uzbekistan	 Urgench	A CIMPA school on Lattices, Heights and Diophantine Approximation Urgench State University	24/06 - 5/07
-	2024	Senegal			
-	2024	Cameroon			

PAST INTERNATIONAL MISSIONS

n.	YEAR	COUNTRY	CITY	OCCASION	DATES
62	2023	Colombia	 Popayán	CIMPA research school on <i>Isogenies of elliptic curves and their applications to cryptography</i> , Universidad del Cauca	24/7-4/8
61	2023	Vietnam	 Ho Chi Minh	SEAMS school on Number Theory and Applications The Industrial University of Ho Chi Minh City	12-22/6
60	2022	Kurdistan	 Erbil	WAMS School Topics in algebraic number theory , Salahaddin University , Kurdistan Region, Iraq	22-28/08
-			 Sulaimani	WAMS School Topics in commutative algebra , University of Sulaimani , Kurdistan Region, Iraq	3-7/9
59	2022	Benin	 Dangbo	CIMPA research school on Algebra, arithmetic and applications , Institut de Mathématiques et de Sciences Physiques	12-24/06
58	2022	Uzbekistan	 Urgench	WAMS School Lattices, Diophantine Approximation and Heights , Urgench State University	06-10/06
57	2021	Senegal	 M'bour	EMA school on Introduction to Number Theory, Cryptography and related courses , African Institute of Mathematical Sciences	6-9/09 (Lectures ONLINE)
56	2020	Indonesia	 Yogyakarta	CIMPA research school on Group Actions in Arithmetic and Geometry , Universitas Gadjah Mada	17-28/02

54	2019	Laos		Vientiane	The 12 th International Conference on Science and Mathematics Education in Developing Countries, National University of Laos	1-3/11
53	2019	Saudi Arabia		Jeddah	King Abdulaziz University	12-15/6
				Abha	WAMS school: <i>Introductory topics in Number Theory and Differential Geometry</i> , King Khalid University	16-23/6
52	2019	United Kingdom		Oxford	Annual meeting of the Committee for Developing Countries (CDC) of the European Mathematical Society (EMS) University of Oxford	5-6/4
51	2019	UNESCO		Paris	Math day for Development - UNESCO	15/3
50	2019	Uruguay		Montevideo	CIMPA research school on <i>Elliptic curves: arithmetic and computation</i> , Universidad de la República	11-22/2
49	2019	Kurdistan		Erbil	WAMS research school <i>Representation Theory</i> College of Science, University of Sulaymaniyah	7-9/2
					Second International Conference of Mathematics (ICM-Erbil2018) Salahaddin University - Erbil	4-5/2
48	2018	Laos		Vientiane	The 11 th International Conference on Science and Mathematics Education in Developing Countries, National University of Laos	2-4/11
47	2018	Pakistan		Lahore	Riphah Institute of Computing and Applied Sciences One Day Symposium on Algebra & Number Theory, Department of Mathematics, COMSATS University Islamabad, Lahore Campus	13-15/09
46	2018	Nepal		Kathmandu	Tribhuvan University Nepal Algebra Project NAP	September
45	2018	Armenia		Yerevan	WAMS research school on <i>The mathematics of Artin's conjectures</i> Yerevan State University	21-25/5
44	2018	Congo		Kinshasa	CIMPA research school on <i>Arithmétique algorithmique et cryptographie</i> , Université de Kinshasa	7-18/05
43	2018	Sweden		Sigtuna	Annual meeting of the Committee for Developing Countries (CDC) of the European Mathematical Society (EMS)	6-7/04
42	2018	South Africa		Johannesburg	CIMPA research school on <i>Explicit Number Theory</i> , University of the Witwatersrand	8-19/01

Artin's Problem

<https://www.mat.uniroma3.it/users/pappa/>

PhD Thesis:

Remarks on Artin Conjecture on Primitive Roots,

<https://www.mat.uniroma3.it/users/pappa/papers/PhDthesis.pdf>

Department of Mathematics and Statistics

A thesis submitted in partial fulfillment

of the requirements of the degree of

Doctor of Philosophy at McGill University

February 1993

Some of Francesco's coauthors on Artin's Problem



Herish Omer Abdullah



Andam Ali Mustafa



Mohamed Anwar



Igor Shparlinski



Andrea Susa

Decimal expansion of $1/n$ with $n \geq 1$

Dividing 1 by n .

If n has no other prime divisor than 2 and 5, the decimal expansion ends with 0's.

Otherwise, the remainders of the Euclidean division are among 1 and $n - 1$; as soon as one repeats, all the next ones also repeat and the expansion is periodic. Hence the period has at most $n - 1$ digits.

If n is prime to 10 (last decimal digit $\in \{1, 3, 7, 9\}$), it is purely periodic (it repeats as soon as one remainder is 1).

Write a bar for the period:

$$\frac{1}{3} = 0.333\,333\,\dots = 0.\overline{3}.$$

Examples:

$$\frac{1}{24} = 0.041\,666\,\dots = 0.041\,\overline{6}, \quad \frac{1}{88} = 0.011\,36\,36\,\dots = 0.011\,\overline{36}.$$

Decimal expansion of $1/7$

International

$$\begin{array}{r} 142857 \\ 7 \overline{) 1000000} \\ \underline{7} \\ 30 \\ \underline{28} \\ 20 \\ \underline{14} \\ 60 \\ \underline{56} \\ 40 \\ \underline{35} \\ 50 \\ \underline{49} \\ 1 \end{array}$$

French style

$$\begin{array}{r} 1000000 | 7 \\ \underline{7} | 142857 \\ 30 | \\ \underline{28} | \\ 20 | \\ \underline{14} | \\ 60 | \\ \underline{56} | \\ 40 | \\ \underline{35} | \\ 50 | \\ \underline{49} | \\ 1 | \end{array}$$

Remainders: 1,3,2,6,4,5,1...

$$\frac{1}{7} = 0.142857\,142857\,\dots = 0.\overline{142857}$$

Remainders of the division of 1 by 7

Sequence of remainders: 1,3,2,6,4,5,1...

$$10^0 = 1$$

$$10^1 = 10 \equiv 3 \pmod{7}$$

$$10^2 = 30 \equiv 2 \pmod{7}$$

$$10^3 = 20 \equiv 6 \pmod{7}$$

$$10^4 = 60 \equiv 4 \pmod{7}$$

$$10^5 = 40 \equiv 5 \pmod{7}$$

$$10^6 = 50 \equiv 1 \pmod{7}$$

$$\gcd(7, 10) = 1$$

$$10 \cdot 5 \equiv 1 \pmod{7}$$

10 is a generator of the group

$$\mathbb{F}_7^\times = \{1, 2, 3, 4, 5, 6\} = \{1, 3, 2, 6, 4, 5, 1\}$$

10 is a *primitive root* modulo 7.

Decimal expansion of $1/p$ with p prime

$$1/2 = 0.5$$

$$1/3 = 0.\overline{3} \quad \ell = 1$$

$$1/5 = 0.2$$

$$1/7 = 0.\overline{142857} \quad \ell = 6$$

$$1/11 = 0.\overline{09} \quad \ell = 2$$

$$1/13 = 0.\overline{076923} \quad \ell = 6$$

$$1/17 = 0.\overline{0588235294117647} \quad \ell = 16$$

Definition: *Long prime number (long period prime, maximal period prime, full reptend prime)* in decimal basis: when 10 is a primitive root modulo p : $\ell = p - 1$.

Long prime numbers in decimal basis:

7, 17, 19, 23, 29, 47, 59, 61, 97, 109, ...

OEIS A001913

Long prime numbers in binary basis: :

3, 5, 11, 13, 19, 29, 37, 53, 59, 61, ...

OEIS A001122

Primitive root modulo a prime

Let $a > 1$ not a multiple of the prime p . The number of digits of $1/p$ in base a is the order of a modulo p : the smallest $k > 1$ such that $a^k \equiv 1 \pmod{p}$. The remainders are the classes of $1, a, a^2, \dots, a^{k-1}$ modulo p . Hence k divides $p - 1$.

Definition: a is a *primitive root modulo p* if $k = p - 1$:

$$\{1, a, a^2, \dots, a^{p-1}\} = \{1, 2, 3, \dots, p - 1\}.$$

Open Problem: is 2 a primitive root modulo p for infinitely many p ?

Not a single value of a is known for which one can show unconditionally that the set of primes p for which a is a primitive root modulo p is infinite.

Artin's Conjecture

Density of the set of prime numbers p for which a is a primitive root modulo p :

Artin's constant:

<https://oeis.org/A005596>

$$A = \prod_p \left(1 - \frac{1}{p(p-1)} \right) = .3739558 \dots$$



Peter Stevenhagen

Reference: Peter Stevenhagen.

The correction factor in Artin's primitive root conjecture.

J. Théor. Nombres Bordx. **15**, No. 1, 383–391 (2003).

MR2019022

Zbl 1043.11078

Correction needed when the square free part of a is congruent to 1 modulo 4. No need for $a = 2$ nor $a = 10$.

Artin's Conjecture: history



Emil Artin
1898 – 1962



Helmut Hasse
1898 – 1979



Derrick H. Lehmer
1905 – 1991



Emma Lehmer
1906 – 2007



Christopher Hooley
1928 – 2018

1927

Emie Artin,
Helmut Hasse

1957

D.H. and E. Lehmer

1958 correction factor:
letter of Artin to
Emma Lehmer

Christopher Hooley (1967): proof
of the corrected result under GRH

January 6, 1958

Letter of E. Artin to D.H. Lehmer

Dear Professor *Lehmer*:

Since you are interested in the density of primes connected with the factorisation of polynomials I would like to stress the fact that the root of these questions belongs to algebraic number theory and should be viewed from this point of view. Any interpretation in terms of elementary number theory hides very essential insights into the nature of the questions.

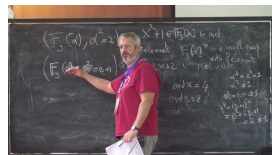
Artin's Problem



Herish Omer Abdullah



Andam Ali Mustafa



Francesco Pappalardi

Let p be a prime and G a multiplicative subgroup of the group of rational numbers.

How large can be the reduction of G modulo p ?

Abdullah, Herish; Ali Mustafa, Andam; Pappalardi, Francesco

Density of the quasi r -rank Artin problem.

Funct. Approximatio, Comment. Math. **65**, No. 1, 73–93 (2021).

Zbl 1489.11004

Abdullah, H. O.; Mustafa, A. Ali; Pappalardi, F.

Divisibility of reduction in groups of rational numbers. II.

Int. J. Number Theory **19**, No. 2, 247–260 (2023).

Zbl 1520.11084

Egyptian fractions



Cyril Banderier



Ernest S. Croot III



David E. Dobbs



John Friedlander



Carlos Alexis Gómez Ruiz



Andrew J. Hetzel




Florian Luca





Enrique Treviño

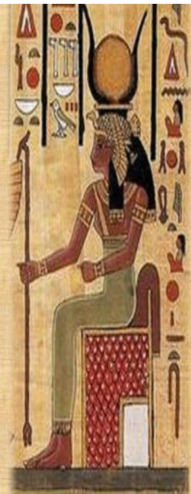
EGYPTIAN FRACTIONS

|||| Four

 one-fourth

Write $\frac{2}{5} = \frac{1}{3} + \frac{1}{15} =$ 

$3.14 = 3 + \frac{1}{10} + \frac{4}{100} = 3 + \frac{1}{10} + \frac{1}{25} =$ 





Egyptian fractions

the Ancient Egyptians only used unit numerator fractions

they turned other fractions into sums of two or more fractions, all with a numerator of **1**

(apart from $\frac{2}{3}$)

they used fractions with different denominators

Egyptian Fractions

Any positive rational number $x/y < 1$ can be written

$$\frac{x}{y} = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_k}$$

with $1 \leq k \leq x$.

Proof.

By induction on x : true for $x = 1$.

Assume $x > 1$. *Greedy algorithm*: take for a_1 the smallest positive integer satisfying

$$\frac{1}{a_1} \leq \frac{x}{y}$$

and define

$$\frac{x_1}{y_1} = \frac{x}{y} - \frac{1}{a_1}.$$

Only need to check: $x_1 < x$.

End of the proof

Since $x/y < 1$ and a_1 is the smallest positive integer satisfying $1/a_1 \leq x/y$, we have

$$\frac{1}{a_1} \leq \frac{x}{y} < \frac{1}{a_1 - 1}.$$

Hence

$$a_1 - 1 < \frac{y}{x} \leq a_1.$$

From

$$a_1 x - x < y \leq a_1 x$$

we deduce the desired estimate for $x_1 = a_1 x - y$:

$$0 \leq a_1 x - y < x.$$

Example: $\frac{x}{y} = \frac{2}{3}$

$$1 < \frac{3}{2} < 2,$$

$$\frac{1}{2} < \frac{2}{3} < 1,$$

$$\frac{2}{3} - \frac{1}{2} = \frac{1}{6}.$$

The greedy algorithm

$$\frac{4}{121} = \frac{1}{33} + \frac{1}{363}.$$

The greedy algorithm gives

$$\frac{4}{121} = \frac{1}{31} + \frac{1}{1250} + \frac{1}{4\,688\,750}.$$

Also

$$\frac{5}{121} = \frac{1}{33} + \frac{1}{121} + \frac{1}{363}$$

but the greedy algorithm gives

$$\frac{5}{121} = \frac{1}{25} + \frac{1}{757} + \frac{1}{763\,309} + \frac{1}{873\,960\,180\,913}$$

$$+ \frac{1}{1\,527\,612\,795\,642\,093\,418\,846\,225}.$$

Sums of two Egyptian fractions

For $n > 1$, the rational numbers $1/n$, $2/n$, are sums of two Egyptian fractions:

$$\frac{1}{n} = \frac{1}{2n} + \frac{1}{2n}, \quad \frac{2}{n} = \frac{1}{n} + \frac{1}{n}.$$

Exercise¹: the rational numbers $3/p$ with p prime $\equiv 1 \pmod{3}$ and $4/p$ with p prime $\equiv 1 \pmod{4}$ are not sums of two Egyptian fractions.

We have seen that the rational numbers $3/n$ with $n > 1$ are sums of three Egyptian fractions.

Is-it true for $4/n$?

¹<https://www.imo.universite-paris-saclay.fr/~daniel.perrin/Divers/APM543-4b.pdf>

Open problem

Open problem. For any $n > 1$, the rational number $4/n$ is the sum of three Egyptian fractions:

$$\frac{4}{n} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

Egyptian fraction

Fix k and n .

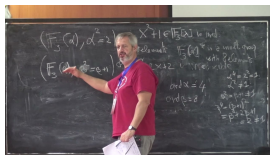
How many x 's are there such that x/n is a sum of reciprocals of k positive integers a_1, \dots, a_k ?

$$\frac{x}{n} = \frac{1}{a_1} + \dots + \frac{1}{a_k}.$$

Ternary Egyptian fractions with prime denominator



Florian Luca



Francesco Pappalardi

For p prime, define

$$A_3(p) = \# \left\{ m \in \mathbb{N} \mid \frac{m}{p} = \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3}, a_1, a_2, a_3 \in \mathbb{N} \right\}.$$

Then as $x \rightarrow \infty$

$$x(\log x)^3 \ll \sum_{p \leq x} A_3(p) \ll x(\log x)^5.$$

Luca, Florian; Pappalardi, Francesco

On ternary Egyptian fractions with prime denominator.

Res. Number Theory **5**, No. 4, Paper No. 34, 14 p. (2019).

Zbl 1455.11057

Permutation polynomials



Sergei Vladimirovich Konyagin



Claudia Malvenuto

Exponential Sums and Enumeration of Permutation Polynomials

Francesco Pappalardi

Conference on Zeta Functions in honor of
Prof. K. Ramachandra on his 70th birthday



National Institute of Advanced Studies
NIAS



Bangalore December 13 - 15, 2003



Bangalore, December 2003

<https://www.mat.uniroma3.it/users/pappa/SLIDES/Slides.html>

- **National Institute of Advanced Studies NIAS Bangalore** (December 15, 2003)
Exponential Sums and Enumeration of Permutation Polynomials (483 Kb)
Conference on Zeta Functions in honor of Prof. K. Ramachandra on his 70th birthday.



Polynomial maps on a finite field

Let \mathbb{F}_q be a finite field with q elements. Given a map $\varphi : \mathbb{F}_q \rightarrow \mathbb{F}_q$, there is a unique polynomial f in $\mathbb{F}_q[X]$ of degree $< q$ such that $f(c) = \varphi(c)$ for all $c \in \mathbb{F}_q$. This polynomial f can be computed via the **Lagrange** interpolation formula (**Vandermonde** determinant).

There is another closed formula which rests on the fact that $z^q = z$ for all $z \in \mathbb{F}_q$ and $1 - z^{q-1} = \delta_{0,z}$ (**Kronecker** symbol):

$$z^{q-1} = \begin{cases} 1 & \text{for } z \neq 0, \\ 0 & \text{for } z = 0. \end{cases}$$

Hence

$$f(X) = \sum_{c \in \mathbb{F}_q} \varphi(c) (1 - (X - c)^{q-1}).$$

For f and g in $\mathbb{F}_q[X]$, we have $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $f - g$ is a multiple of $X^q - X$.

Permutation polynomials

Let $f \in \mathbb{F}_q[X]$. The following equivalent properties define *permutation polynomials*

- (i) The polynomial map $c \mapsto f(c)$ is a permutation of \mathbb{F}_q .
- (ii) The map $c \mapsto f(c)$ from \mathbb{F}_q to \mathbb{F}_q is surjective.
- (iii) The map $c \mapsto f(c)$ from \mathbb{F}_q to \mathbb{F}_q is injective.
- (iv) The map $c \mapsto f(c)$ from \mathbb{F}_q to \mathbb{F}_q is bijective.

If $\sigma \in \mathfrak{S}_q$ is a permutation of \mathbb{F}_q , then the associated polynomial

$$f(X) = \sum_{c \in \mathbb{F}_q} \sigma(c) (1 - (X - c)^{q-1})$$

has degree $\leq q - 2$ if $q > 2$ since $\sum_{c \in \mathbb{F}_q} \sigma(c) = 0$:
the coefficient of X^{q-1} in $X^q - X$ is $\sum_{c \in \mathbb{F}_q} c = 0$.

Permutation polynomials and cryptography

Dickson–Diffie–Hellmann Key
Exchange

Uses Dickson permutation
polynomials (1896).



Leonard Eugene Dickson
1874 – 1954

There is a fast algorithm to compute the values of Dickson permutation polynomials, no fast algorithm is known to compute the Dickson Discrete Logarithm.

Wanted: new explicit permutation polynomials.

Enumerating permutation polynomials with given degree

The number of permutation polynomials over \mathbb{F}_q is $q!$.

Claudia Malvenuto and Francesco Pappalardi:

Almost all permutation polynomials have degree $q - 2$.

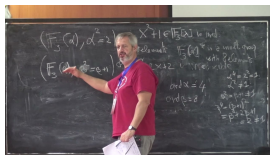
Given q and d , the number $\mathcal{N}(q, d)$ of permutation polynomials of degree $< q - 2$ satisfies

$$|\mathcal{N}(q, d) - (q - 1)!| \leq \sqrt{\frac{2e}{\pi}} q^{q/2}.$$

Enumerating permutation polynomials



Claudia Malvenuto



Francesco Pappalardi

Applications in combinatorics and cryptography

Malvenuto, Claudia; Pappalardi, Francesco

Enumerating permutation polynomials. I: Permutations with non-maximal degree.

Finite Fields Appl. **8**, No. 4, 531–547 (2002).

Zbl 1029.11068

Enumerating permutation polynomials. II: k -cycles with minimal degree.

Finite Fields Appl. **10**, No. 1, 72–96 (2004).

Zbl 1035.11062

Elliptic curves



William Banks



Chantal David



Hershy Kisilevsky



Igor Shparlinski

Counting with elliptic curves over finite fields

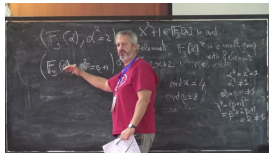
Let E be an elliptic curve over a prime field with p elements. Then the group of points is of cardinality N , where N is in the Hasse interval $[p - 2\sqrt{p} + 1, p + 2\sqrt{p} + 1]$. While its order is well-understood there are finer invariants such as the group structure, the exponent of this group, etc. which are not so well-understood.

Francesco has written a few papers in which he has investigated statistical questions such as how large is the exponent of the group likely to be, or if we fix the structure of the group how many p 's are there for which there exist elliptic curves E with the group of points having that structure, etc.

Rational points on elliptic curves over finite fields



William Banks



Francesco Pappalardi



Igor Shparlinski

Which are the finite groups which can be realized as groups of rational points of an elliptic curve over a finite field?

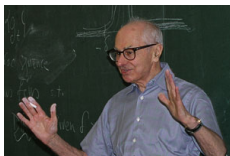
Banks, William D.; Pappalardi, Francesco; Shparlinski, Igor E.

On group structures realized by elliptic curves over arbitrary finite fields.

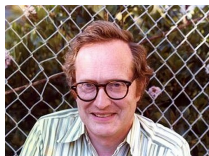
Exp. Math. **21**, No. 1, 11–25 (2012).

Zbl 1257.11060

Lang–Trotter Conjectures



Serge Lang
1927 – 2005



Hale Freeman Trotter
1931 – 2022

In 1976, **Lang** and **Trotter** formulated elliptic analogues of the **Artin** primitive root conjecture. Suppose E is an elliptic curve over \mathbb{Q} with a rational point of infinite order. A natural question is how often does the prescribed point generate $E(\mathbb{F}_p)$, the group of points \pmod{p} ?

More precisely, let a be a rational point of infinite order. The problem is to determine the density of primes p for which $E(\mathbb{F}_p)$ is generated by the reduction of $a \pmod{p}$.

Lang–Trotter Conjectures (continued)

Let E be an elliptic curve over \mathbb{Q} , which does not have complex multiplication over the algebraic closure of \mathbb{Q} . For $x > 0$, let $P(x)$ be the number of primes $p < x$ such that E has good super-singular reduction at p . A conjecture of Lang and Trotter states that

$$P(x) = O(x^{1/2} / \log x).$$



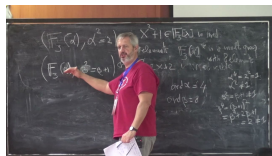
Jean-Pierre Serre

In his paper *Quelques applications du théorème de densité de Chebotarev*, Serre proves $P(x) = O(x^{3/4})$ under the generalized Riemann hypothesis (GRH) for Artin L -functions.

Lang–Trotter Conjectures (continued)



Chantal David



Francesco Pappalardi

In 1999 Chantal David and Francesco Pappalardi prove the Lang–Trotter Conjecture on the average.

David, Chantal; Pappalardi, Francesco.

Average Frobenius distributions of elliptic curves.

Int. Math. Res. Not. No. 4, 165–183 (1999).

Zbl 0934.11033

Arithmetic functions



William Banks



John Friedlander



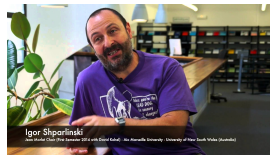
Alexei Glibichuk



Florian Luca



Filip Saidak



Igor Shparlinski

Arithmetic functions

Counting solutions to various equations in arithmetic functions, like the **Euler** function being a square, or the order function (of an element modulo p) being squarefree, etc.

Pappalardi, Francesco

Square free values of the order function.

New York J. Math. **9**, 331–344 (2003).

Zbl 1066.11044

Pappalardi, Francesco; Saidak, Filip; Shparlinski, Igor E.

Square-free values of the Carmichael function.

J. Number Theory **103**, No. 1, 122–131 (2003).

Zbl 1042.11058

Zero sum problems



Sukumar Das Adhikari



R. Balasubramanian



YongGao Chen



John Friedlander



Sergei Vladimirovich Konyagin



Francesco Pappalardi



Purusottam Rath

Zero sum problems

Given a subset A of an abelian group G what is the minimal number $n(A, G)$ of elements of A that we need to choose to make sure that among these there is a zero subsum? What about a zero subsum of a given length k ?

Adhikari, Sukumar Das; Chen, Yonggao; Friedlander, J. B.; Konyagin, S. V.; Pappalardi, F.

Contributions to zero-sum problems.

Discrete Math. **306**, No. 1, 1–10 (2006).

Zbl 1161.11311

Adhikari, Sukumar Das; Balasubramanian, R.; Pappalardi, F.; Rath, Purusottam

Some zero-sum constants with weights.

Proc. Indian Acad. Sci., Math. Sci. **118**, No. 2, 183–188 (2008).

Zbl 1207.11030

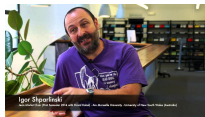
Multiplicatively dependent vectors



Francesco Pappalardi



Min Sha



Igor Shparlinski



Cameron Stewart

Asymptotic formulas are proved for the number of multiplicatively dependent vectors of algebraic numbers of fixed degree, or within a fixed number field, and bounded height.

Pappalardi, Francesco; Sha, Min; Shparlinski, Igor E.; Stewart, Cameron L.

On multiplicatively dependent vectors of algebraic numbers.

Trans. Am. Math. Soc. **370**, No. 9, 6221–6244 (2018).

Zbl 1442.11134

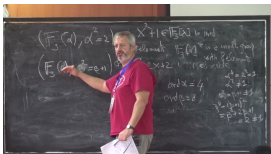
Counting dihedral and quaternionic extensions



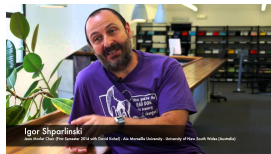
Etienne Fouvry



Florian Luca



Francesco Pappalardi



Igor Shparlinski

Fouvry, Étienne; Luca, Florian; Pappalardi, Francesco; Shparlinski, Igor E.
Counting dihedral and quaternionic extensions.

Trans. Am. Math. Soc. **363**, No. 6, 3233–3253 (2011).

Zbl 1235.11097

Joyeux anniversaire Francesco

